



*Your future's safe!*



# Safety Guide

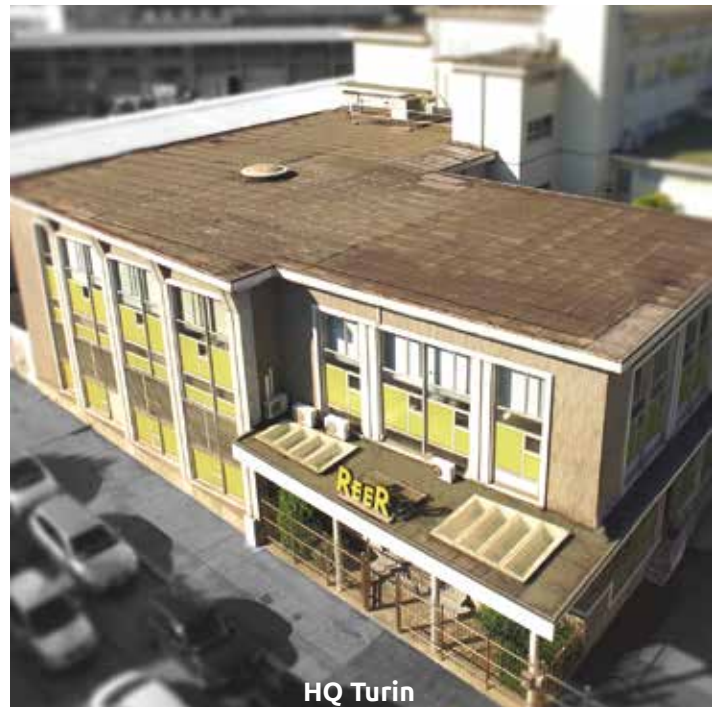
*safety in the working environment*

## Your technological partner since 1959

ReeR was established in 1959 with a mission to distribute automation products for industrial, lighting, and home applications. By the mid-1970s, the first safety sensors were developed. Not long after, the first light curtains were produced.

Today, ReeR is the **leading Italian company** in the industry and one of the **largest manufacturers in the world of optoelectronic sensors** for industrial safety.

The Safety Division has the expertise to support customers all over the world. Its talented network of distributors provides industry-leading support services to customers in more than 50 countries.



## Safety and Automation

Safety is essential in every workplace. It becomes even more crucial in highly automated environments.

Thanks to our collaboration with world-leading companies in the machine-tool, automotive, packaging, and palletization industries, **ReeR is able to offer a wide range of safety devices** such as light curtains, programmable controllers, photocells, laser scanners, and interfaces able to meet the demands of any application.

ReeR specializes in the field of optoelectronic curtains for automation, measurement, and control.

## ReeR's Industry Expertise

Technological excellence and application know-how embody the spirit of ReeR.

Fourteen percent (14%) of ReeR's workforce is employed in the R&D department with expertise in safety hardware, software, and firmware.

In addition to developing its own technology and devices, the experts at ReeR work hard to participate in the standardization development process for the industry. As one of the main players in the space, **ReeR plays a vital role in national and international organizing committees** on machinery safety requirements.





## Key words

### Quality



ReeR is committed to continuously improving its quality management system by minimizing defective returns and ensuring high product reliability.

Product traceability and production process control are delivered using ReeR's proprietary management software.

Product quality is guaranteed by the TÜV certified Quality System according to the ISO 9001 standard.



### ReeR supports the environment



All internal electrical consumption origins from renewable sources.

The 2002/95/CE RoHS directive restricts the use of hazardous substances in electric and electronic devices.



### Health and safety in the workplace



In order to reduce incident risks in the workplace, ReeR has implemented a management system for the monitoring of all health and safety issues in the workplace, as regulated by ISO 45001.

### Innovative manufacturing process

Constant investment in manufacturing technologies

- Manufacturing process control system regulated by Lean Manufacturing principles
- Continuous improvement
- Slim production
- Waste reduction
- Delivery times improvement
- Fast-moving part-numbers management



## Products

### Safety devices

- Type 4 and Type 2 Safety light curtains
- Photocells
- Magnetic and RFID switches
- Incremental encoder

### Configurable Safety interfaces

- Inputs for Type 4 and Type 2 light curtains
- Inputs for light curtains with integrated Muting function
- Analogue signal inputs
- Inputs for interlocking devices
- Inputs for two-hand control
- Safety speed monitoring (SIL 3, PL e)
- Emergency stop buttons and safety switches control

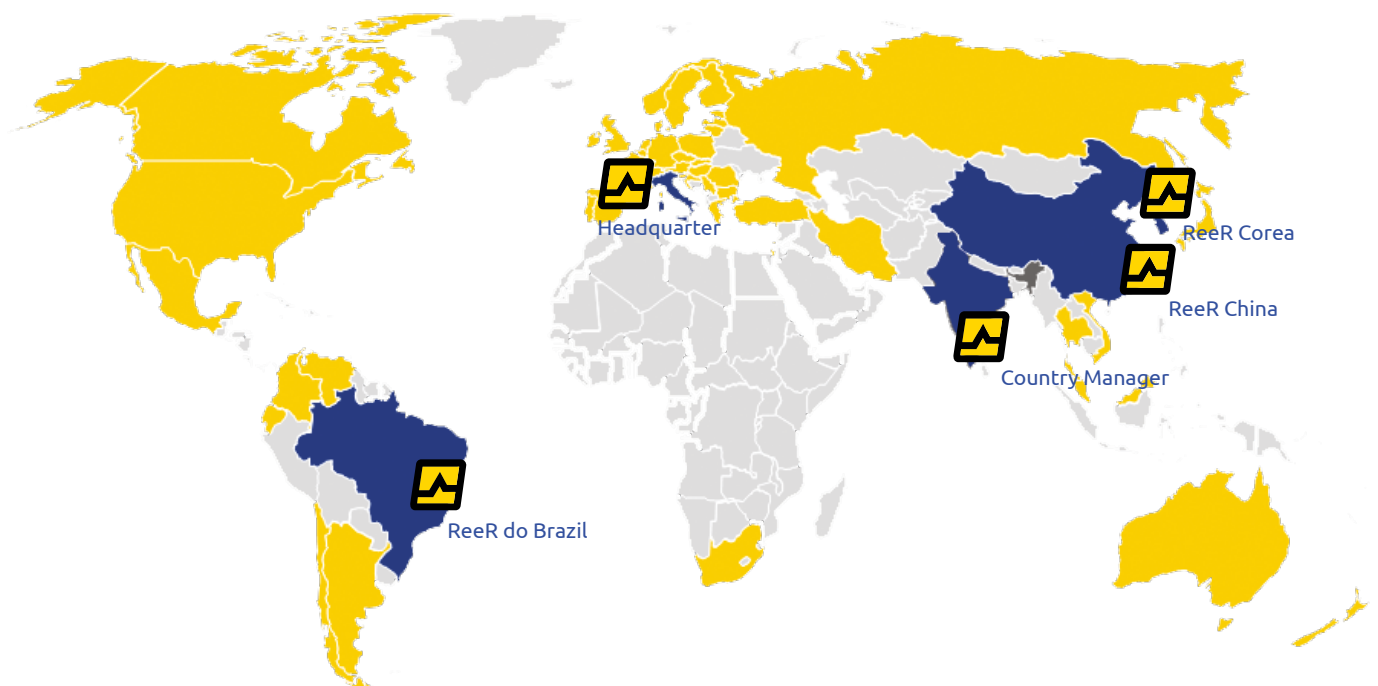
### Laser scanners

### Measurement, control and automation devices

### Accessories

## Sales network

Direct sales network in Italy, Brazil, China, India and South Korea; 65 distributors in the world



## CONTENTS

Introduction	9
European directives	9
Social directives	9
Product directives	9
Low voltage directive	10
Electromagnetic compatibility directive	10
ATEX directive	11
Accredited bodies	11
Notified bodies	11
Harmonized standards	12
Steps for the development of a Standard	12
Structure of a safety-related Product Standard	12
Northern American standard and test bodies	13
OSHA is the body authorized to approve NRTLs.	14
ISO 12100:2012 - Safety of machinery - General principles for design - Risk assessment and risk reduction	15
Strategy for risk assessment and risk reduction	15
1 - Risk analysis	16
2 - Risk evaluation	17
3 - Risk reduction principles	18
Step 1 - integration of safety concepts at the design stage	19
Step 2 - Risk reduction by means of protective measures	20
Step 3 - Risk reduction by administrative measures	21
Functional safety standards	25
EN ISO 13849-1,2 Safety of Machinery - Safety Related Parts of Control Systems - General principles for design	25
Risk assessment and required Performance Level - PL r assignment	26
Overlapping of hazards	28
Identification of the safety function and design specification	29
Realization of a safety function with an SRP/CS	31
PL of the SRP/CS	32
Categories and their relationship with the MTTF <sub>D</sub> with the DC and with the CCFs	34
Computation of the MTTF <sub>D</sub> of the SRP/CS	37
Simplified method for estimating the quantifiable part of the PL	41
IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control system.	47
Management of functional Safety	47
Safety Integrity Level (SIL)	47
SIL allocation	47
Assignment of the safety requirements specification (SRS) and functional requirements specifications	50

# TABLE OF CONTENTS

Design process of an SCS	50
Use of a pre-designed subsystem	51
PFH as a target parameter to measure the hardware safety integrity of the SCS	52
Determining the PFH of the SCS	52
Determining the SIL of the SCS	52
Requirements for systematic safety integrity	53
Safety measures with regards to electromagnetic phenomena	53
Safety-related application software	54
Design and development of subsystems	56
Step one - Choice of the architecture (structure).	56
Step two - Determination of the parameters $\lambda$ , $\lambda_d$ , $\lambda_s$ , $\lambda_{dd}$ , $\lambda_{du}$	60
Step 3 - Determination of Diagnostic Coverage (DC) and of the parameters $\lambda_{dd}$ and $\lambda_{du}$	63
Step 4- Estimation of safe failure fraction	65
Methodology for the estimation of susceptibility to common cause failures	66
Estimation of the effect of CCF	66
EN ISO 14119 Safety of machinery - Interlocking devices associated with guards - Principles for design and selection	67
Overall system stopping performance and access time (The guards distance)	68
Logical series connection of interlocking devices	68
Interlocking devices based on "fault exclusion"	69
Guard lock and Guard interlock	69
Measures to prevent the defeat of the interlock device	69
Safety speed monitoring	70
Sensors and certified speed monitoring combinations	70
Mosaic analog safety modules (MA2 - MA4) and analog sensors	74
MA2, MA4 modules used with safety analog sensors	75
Glossary	82
<b>SENSORS - PHOTOELECTRIC SAFETY LIGHT CURTAINS</b>	<b>85</b>
Characteristic elements	85
New safety parameters for Type 2 light curtains	85
Protected height	85
Range	85
Response time	85
Resolution	86
Advantages of light curtains	86
The technical specification IEC 62046: Safety of machinery –	
Application of protective equipment to detect the presence of persons	87
Selection process	87
Machine characteristics	88
Environmental characteristics	88
Dimensions and characteristics of the human body	89
Uses of protective equipment	89
Use of an ESPE for Trip function	89

Definition of type of detection	90
Determination of the safety distance	91
GENERAL FORMULA FOR THE DETERMINATION OF THE MINIMUM SAFETY DISTANCE	91
DIRECTION OF APPROACH PERPENDICULAR TO THE PROTECTED PLANE WITH $\alpha=90^\circ (\pm 5^\circ)$	92
Determination of the minimum safety distance:	92
Determination of the minimum safety distance:	94
Direction of approach parallel to the protected plane with $\alpha=0^\circ (\pm 5^\circ)$	95
Light curtains protected height - Determination criteria	97
Using the ESPE as a presence sensing device	97
Muting function	99
MUTING: palletizers and materials handling systems	100
Common solutions for Muting sensor positioning	101
Muting with 2 crossed-beam or parallel-beam sensors – Configuration type L with timing monitoring and one-way only(exit from dangerous area) pallet operation:	102
Protection of two transport systems operating in a coordinated way	103
Blanking function	105
<b>SENSORS - LASER SCANNER</b>	<b>106</b>
Characteristic elements	106
Controlled areas	107
Applications	108
Area control	108
Access control	108
Protection of Automatic Guided Vehicles (AGV)	108
<b>SENSORS - CONTACTLESS SAFETY SENSORS</b>	<b>109</b>
RFID safety sensors	109
Magnetic safety sensors	109
Inductive safety sensors	109
<b>GUARD LOCK AND GUARD INTERLOCK DEVICES</b>	<b>110</b>
Safety switch with guard locking	110
<b>SELECTION GUIDE</b>	
Rules for correct interconnection of protection devices to machine control system	116

# TABLE OF CONTENTS

<b>INSIGHTS</b>	<b>118</b>
Placement of the acces control light curtains in the paletizer plant	118
Using mechanical obstacles	119
Industrial thermal processes	120
Standard	121
Perimeter protection	123
<b>CUSTOMER SERVICE</b>	<b>125</b>



## Introduction

This safety guide refers to the set of rules governing the safety of machinery. In particular, this concerns the crucial family of standards under the umbrella of:

- ISO 13849 "Safety of machinery"
- IEC 61508 "Functional safety of electrical / electronic / programmable electronic safety related systems" which impacts safety of machinery especially through IEC 62061 "Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems"
- IEC 61496 "Safety of machinery - Electro sensitive protective equipment"

Important statistical concepts related, in varying degrees, to probability of dangerous failure, are covered by machine safety, resulting in new classifications of safety-related control systems for machinery and protection devices. These include PL (Performance Levels, for ISO) and SILs (Safety Integrity Levels, for IEC). PL and SIL come next to and in many ways replace the familiar concept of category of the 'old' EN 954-1.

The second edition of the Technical Specification IEC TS 62046 "Application of protective equipment to detect the presence of persons", is a useful guide for players who want to use electro-sensitive protective devices for the realization of control systems for machine safety.



## European directives

The aim of the EU Directives is to harmonize the national legislation of the Member States so as to have common regulations concerning technical, economic, social aspects, etc. and to facilitate the free circulation of goods, services and people within the European Union.

A Directive is a legislative act that establishes the objectives that all EU countries must achieve. For this reason it is mandatory to transpose it without modification to national legislation; however, each country can decide how to transpose. In particular, with regard to safety at workplace, the legislation distinguishes between two types of measures:

- Social directive
- Product directive

### Social directives

Social directives are addressed to the employer and have as their goal the improvement of safety in the workplace environment. Are examples of social directive: the General Directive 89/391 / EEC, concerning the implementation of measures aimed at the improvement of safety and health of workers and the particular Directive related to it, 2009/104 / EC, on the use of work equipment. Other social directives of interest are:

- 2019/1832/UE "Personal protective equipment"
- 90/269 CEE "Manual handling of loads"
- 90/270 CEE "VDT equipment"

### Product directives

Product Directives establish:

- The Essential Safety Requirements of products in order to guarantee the free movement of safe products within the European market
- Attestation conformity criteria

The fundamental directives for safety work equipment are:

- 2006/42/EC "Machinery directive"
- 2014/35/EU "Low Voltage Directive"
- 2014/34/EU "Electromagnetic Compatibility Directive"
- 2014/34/EU "ATEX directive"

Compliance with technical safety requirements of the directives is mandatory.

## Machinery directive

The “Machinery Directive” 2006/42/EC is meant for the manufacturers of machines and safety components, and has the following goals:

- The definition of safety and health protection requirements for the improvement of the degree of protection offered to the operators of hazardous machinery
- The design, manufacture and marketing in the European Union of machines and components complying with the minimum safety requirements laid down by the Directive itself
- The free circulation in the Member States of machines and safety components complying with the Directive

The Machinery Directive:

- Applies to all new machines and safety components that are sold, lent or hired, and to used machinery in case they are sold, rent or lent.
- It sets forth the essential safety requirements relating to the design and manufacturing of machines and safety components and it defines the respective certification procedures.
- It is mandatory for machines and for safety components.
- Only products conforming to the Directive can be marketed or commissioned in the European Union

## Certification procedures

The machinery directive:

- Lays down stringent procedures for safety components and highly hazardous machines which are listed in Annex IV
- Lays down simplified procedures for low and medium risk machines not included in Annex IV
- Requires machine builders to draw up a technical file stating the safety principles adopted in the design, manufacture, transport, use and maintenance of the machine or of the safety component

## Declaration of conformity

In order to certify the conformity of a product to the Directive, the manufacturer must:

- Affix the CE mark to the product
- Attach the CE declaration of conformity certifying compliance to the Directive

## Certifications

The CE type certificates is valid for 5 years (Annex IX para. 9.3), the five-year period starting from the date of issue of the certificate. After which a new verification will be required to maintain the certification.

## Low voltage directive

2014/35/EU is aimed at ensuring that electrical materials are designed and manufactured so as to guarantee the protection of people against any risks of electrocution resulting from their use or from the influence of external agents on the electrical materials themselves.

This Directive applies to all electrical materials meant for use at a nominal voltage between:

- 50V and 1000V for alternating current
- 75V and 1500V for direct current

## Electromagnetic compatibility directive

The aim of “Electromagnetic Compatibility Directive” 2014/30/EU is to ensure that electrical devices are designed and manufactured so that:

- Electromagnetic emissions are limited and low enough to permit other electrical devices to operate according to their intended use
- The level of built-in immunity to external electromagnetic disturbances enables them to operate according to their intended use

This Directive applies to all electrical and electronic devices able to cause electromagnetic disturbances and whose operation can be affected by external electrical factors.

## ATEX directive

The ATEX Directive 2014/34/EU applies to all equipment intended for use in potentially explosive atmosphere. It is in force since 30 March 2014.

The ATEX Directive 2014/34/EU specifies minimum safety requirements for electrical devices used in environments classified as dangerous regarding the aspect of risk of explosion due to the presence of gas or dust.

The Directive allocates equipment into group and categories.

The manufacturer must decide, according to the use, the Group and the Category to which the equipment belongs.

- Group 1: equipment intended for use in underground works, mines and their above ground installations
- Group 2: equipment intended for use in environments where explosive atmospheres are likely to occur
- These product groups are then categorized according to the level of protection against the risk of ignition of potentially explosive atmospheres.

The products in the Group 2 are divided into three Categories:

- Category 1: equipment intended for high-risk zones where an explosive atmosphere is present for long periods
- Category 2: equipment intended for medium-risk zones where an explosive atmosphere may occur under normal operating conditions
- Category 3: equipment intended for zones where an explosive atmosphere is only likely under abnormal circumstances

## Accredited bodies

In each Member State, Accredited Bodies are appointed with the role to assess and verify the compliance and the application of the European Directives.

Each State is responsible for the appointment and control of its own Bodies.

## Notified bodies

Notified Bodies are third party organisations which have been officially designated by their national authority to assess the conformity to the applicable Directives of machines and safety components before being placed on the market.

Each Member State of the European Union is required to:

- Appoint the Notified Bodies by specifying their tasks
- Submit a list of Notified Bodies to the European Commission and to the other Member States

The European Commission publishes on the Official Journal a Directory of all Notified Bodies, together with a list of the services, the machines and/or the safety components on which they are authorised to assess compliance.

The Member States of the European Union must ensure that these Bodies respect specified ethical and technical criteria.



## Harmonized standards

- They are technical Standards conceived to meet the essential safety requirements of the Directives
- They are written by various Technical Committees on a mandate by the Commission of the European Union
- They are approved and adopted:
  - by the CEN (European Committee for Standardization)
  - or the CENELEC (European Committee for Electrotechnical Standardization)
- Then they are translated and published in the Official Journal of the European Committee and the Official Gazette of each Member State.

Compliance with a harmonized standard confers on the products or services the presumption of compliance with the Directives. In most cases, the use of harmonized standards is optional. It is also possible to choose another technical solution. However, the Essential Safety Requirements of the applicable directives must be guaranteed.

### Steps for the development of a Standard

- A draft standard (NP, New work item proposal) is prepared that will be examined by the various concerned national Committees, for comments, proposals and subsequent approval
- Upon approval of the NP, a Working Group (WG) made of experts on the subject being discussed is set up. Experts (industry experts, experts from test laboratories, representatives of workers' organizations, consumer representatives) are appointed by the Member States
- Production of a first WD (Working Draft).
- Through subsequent processing of the text of the WD the following document are produced:
  - In IEC organization: CD (Committee Draft), CDV (Committee Draft for Voting), FDIS (Final Draft International Standard)
  - In ISO organization: CD (Committee Draft), DIS (Draft International Standard), FDIS (Final Draft International Standard).
- Upon reaching the consensus (expressed by a positive majority vote on the FDIS document expressed by Member States), the final text of the Standard is finalized, officially published and implemented by each Member State.

A published Standard remain in force for five years unless there is a need to review its contents.

### Structure of a safety-related Product Standard

To facilitate use and reading, most of safety-related Product Standards have the following structure:

- Preface
- Index
- Introduction
- Field of application
- Standard references
- Terms and Definitions (symbols and abbreviations)
- Safety requirements (risk reduction measures)
- Tests (test methods by testing or analysis for verifying safety requirements)
- Marking (for correct identification)
- Information for safe use
- Optional Annexes (they provide additional provisions beyond those found in the body text of the Standard)
- Optional information annexes (provide additional information intended to improve understanding and use of the document) and only for European Harmonized Standards
- Annex ZA (regulatory): regulatory references between International Publications and the corresponding European Publications (this annex lists international or European documents that are essential for the application of the standard)
- Annex ZZ (informative): correspondence between the paragraphs, sub-paragraphs of the Standard and the Essential Safety Requirements of the applicable Directives. Once the standard is referred to in the Official Journal of the European Union, compliance with the clauses of the Standard that are reported in the Table of Annex ZZ confers, within the limits of the scope of the Standard, a presumption of conformity with the corresponding requirements of the Directive.



The European Standards concerning safety are subdivided into 3 groups:

TYPE A STANDARDS - They specify the general design principles applicable to all types of machine

e.g... **ISO 12100** Safety of machinery - General principles for design - Risk assessment and risk reduction

TYPE B STANDARDS - They are divided into two classes:

Type B1 Standards: concerning a specific aspect of safety

e.g... **EN ISO 13855** Positioning of safeguards with respect to approach speeds of parts of the human body  
**EN ISO 13857** Safety distances for the protection of the upper limbs  
**IEC EN 60204-1** Safety of machinery. Electrical equipment of machine  
**EN ISO 13849 - 1,2** Safety of machinery. Safety related parts

Type B2 Standards: concerning safety devices

e.g... **IEC EN 61496-1** Electrosensitive protective equipment - general requirements and tests -  
**IEC EN 61496-2** Electrosensitive protective equipment-Particular requirements for equipment using active optoelectronics protective devices (i.e. light curtains)  
**IEC EN 61496-3** Electrosensitive protective equipment-Particular requirements for Active Optoelectronics Devices responsive to diffuse reflection (i.e. laser scanner) -  
**ISO 13850** Emergency stop - Principles for design  
**ISO 14119** Safety of machinery - Interlocking devices associated with guards - Principles for design and selection

TYPE C STANDARDS - They concern specific types of machine:

e.g... **EN 692** Mechanical presses  
**EN 693** Hydraulic presses  
**EN 415** Packaging machines  
**EN 415-4** Palletizing and de-palletizing systems  
**EN ISO 10218** Industrial robot

A type C Standard takes priority over type A and B Standards.

The type C standard identifies the significant hazards generally associated with the category of machinery and provides the protective measures to address them. However, the application of harmonized standards does not completely exempt the machine manufacturer from the obligation to carry out a risk assessment. The manufacturer must ensure that the harmonized standard is suitable for the particular machine and covers all the risks it presents. If the machine presents hazards that are not covered by a type C standard, a full risk assessment is required for those hazards and adequate protective measures must be taken to face them. In this case, type A and B standards can help.



## Northern American standard and test bodies

The Body overseeing health and safety in the workplace in the USA is the Occupational Health and Safety Administration (OSHA). Individual States may have their own safety regulatory organizations which may enforce stricter regulations than OSHA. OSHA oversees the application of laws and regulations in force at the Federal level, and in turn issues safety standards covering the use and construction of safety devices and/or machine tools.

An important example of such activity is Standard OSHA 1910.217 – Mechanical Power Presses.

The American National Standard Institute (ANSI) issues standards on the safety of machine tools or aspects of their construction or operation. For the preparation of these standards ANSI often relies on the contribution of nonprofit organizations such as the Robotic Industry Association (RIA), or the Association for Manufacturing Technology (AMT).

### Examples of major ANSI standards:

B11 Standards including:

**B11.1** Mechanical Power Presses  
**B11.2** Hydraulic Power Presses  
**B11.3** Power Press Brakes  
**B11.4** Shears  
**B11.19** Performance Criteria for the Design, Construction, Care and Operation of Safeguarding

Other ANSI standards:

**B20.1** Conveyor Belts  
**ANSI/RIA R15.06** Safety Requirements for Industrial Robots

Contrary to Europe, North America does not accept a certificate of conformity as an approval to sell and install electrical equipment. Prior to installation the device or system must be inspected by the Authorities Having Jurisdiction (AHJ). If the device is already approved by a Nationally Recognized Testing Laboratory (NRTL), the competent authority is dispensed from inspecting the product. The mark of a NRTL assures product conformity to safety standards in force.

Although not mandatory in North America, certification facilitates marketing as retailers, inspectors, users and local authorities readily approve any product bearing a NRTL mark. Certified installations enjoy advantages in terms of insurance benefits and freedom from potential industrial disputes, as Workers Unions might prevent members from operating non-certified, and therefore possibly dangerous, machinery.

## OSHA is the body authorized to approve NRTLs.

NRTLs shall obtain approval for all national and foreign facilities for all products for which they are authorized to award certification. To obtain accreditation, the applicant shall also, but not only, prove to be independent of any users, suppliers or retailers of the products for which certification is sought. NRTLs may develop and apply for approval of its own developed standards or adopt standards produced by other NRTLs. Each NRTL has its own unique mark.

Underwriters Laboratories Inc. (UL) is a leading NRTL among those authorized to issue certification of electrical systems and equipment



UL Listed Certification Mark means that the product was tested and verified to be in line with USA safety requirements. UL Listed General Mark certifies conformance to fire resistance and electrical safety requirements.



UL certification also includes components such as safety light curtains which are covered by Std. UL 61496-1 and Std. UL 61496-2 derived from international Std. IEC 61496-1,2. Systems incorporating safety software can be also certified as per Std. ANSI/UL 1998. Safety light curtains (ESPE) are covered by a specific marking certifying compliance with the appropriate product standard. ReeR safety curtains are in line with all these requirements and bear the associated mark of approval.



UL may also certify conformity to CSA Canadian Standards (through C-UL mark or C-UL-US mark for products to be marketed in Canada and in the USA).

The Canadian Standard Association (CSA) is the main Canadian standardization body and acting certification authority competent for verification of conformance of safety components to Canadian regulations.

As Nationally Recognized Test Laboratory (NRTL) for the USA, CSA is authorized to verify conformance of all products under OSHA jurisdiction and award the CSA mark of NRTL/C, equivalent to C-US UL, which applies for example to safety light curtains.



## ISO 12100:2012 - Safety of machinery - General principles for design - Risk assessment and risk reduction

As a result of their functionality, machines and plants represent potential risks for the workers. If a machine may present hazards, a risk assessment is required and, if relevant, a risk reduction shall be undertaken to reduce the risk to an acceptable level.

ISO 12100 provides a methodology for the design of machines that shall be safe for their intended use. It gives provisions:

- For identification of the hazards
- For estimation and evaluation of the risks associated with the machine
- On how to remove hazards or provide sufficient risk reduction

ISO 12100 is a type-A standard.

For USA equivalent information is given in ANSI 12100.

### Strategy for risk assessment and risk reduction

Risk assessment is comprehensive method to enable in a systematic way the analysis and evaluation of risks. It must be carried out during the design, construction and commissioning of the machinery and every time are made modifications. It can also be used for the evaluation of existing machinery if, for example, there have been accidents or malfunctions.

To implement risk assessment and risk reduction the following actions shall be taken

1. **Risk analysis**  
to determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse, and to identify the hazards and associated hazardous situations associated to the person's activities (all safeguards should be ignored while hazard identification is performed).
2. **Risk evaluation**  
To evaluate the risk for each identified hazard and hazardous situation and take decisions about whether there is a need to reduce risk.
3. **Risk reduction**  
If the hazard cannot be removed, reduce the associated risk by implementing protective measures.

The process is iterative, and several successive applications can be necessary.

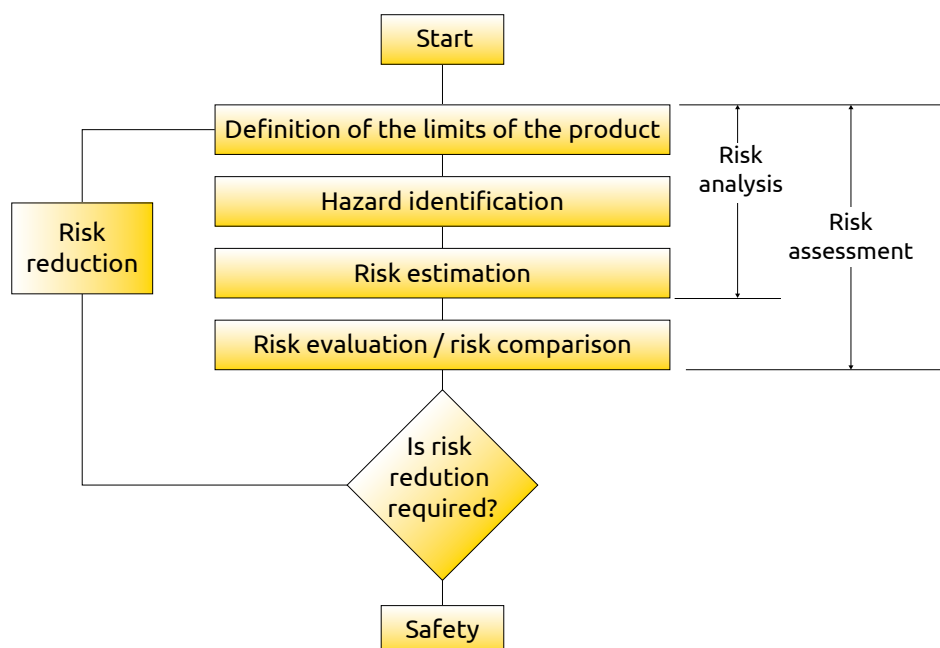


Fig. 1. Strategy for risk assessment and risk reduction

The goal to be met is to reduce risk to an acceptable (tolerable) level considering that the risk reduction achieved: should be effective throughout all phases the machine life cycle and should not impair machinery functions and usability.

When changes are made to the process or to the machine or if protective measures are added, all steps of the risk assessment should be repeated to check whether:

- There have been changes to the operating limits of the machine
- New hazards or dangerous situations have been introduced
- The level of risks of any existing dangerous situations has been increased
- Protective measures added are effective in reducing the risk
- The risk reduction intended has been achieved

Achieving the required risk reduction is only one of the inputs to the decision to stop the iterative risk reduction process. This decision should involve additional considerations such as regulations, national laws, and work organization.

## 1 - Risk analysis

Determination of the limit of the machine

The first step of the risk analysis consist in providing a clear description of the mechanical, physical and functional capabilities of the machinery; to determine the space limits of the machinery which means to determine the range of movements, the space requirements for persons interacting with the machine (also during maintenance) the kind of human interaction, the environmental operating limits (minimum and maximum temperatures, dry or wet weather, tolerance to dust etc.), different operating modes, power supply interface.

### Identification of the hazards

After determination of the limits of the machinery, the essential step in any machinery risk assessment is the systematic identification of reasonably foreseeable hazards that may arise during the whole machine life cycle (transport, installation, commissioning, use, disabling, dismantling). Only if all the hazards are correctly identified action can be taken to reduce the associated risks. Unidentified hazards can lead to injury. It is therefore important to ensure that the identification of hazards is systematic and complete.

To accomplish the hazard identification, it is necessary to identify:

- The operations to be performed by the machinery
- The tasks to be performed by persons who interact with the machine, considering unintended behavior or reasonably foreseeable misuse of the machine
- The characteristics of the materials to be processed
- The environment in which the machine can be used

Hazards generated by man-machine interaction	Hazards generated by the machine
Setting	Electrical hazards
Testing	Mechanical hazards
Programming	Thermal hazards
Manual loading-unloading	Hazards generated by noise
Tool changeover	Hazards generated by vibrations
Starting, stopping the machine	Hazards generated by radiation
Restart after unscheduled stop	Hazards generated by materials
Cleaning and housekeeping	Hazards related to the environment
Preventive and corrective maintenance	Hazards related to emission of substances



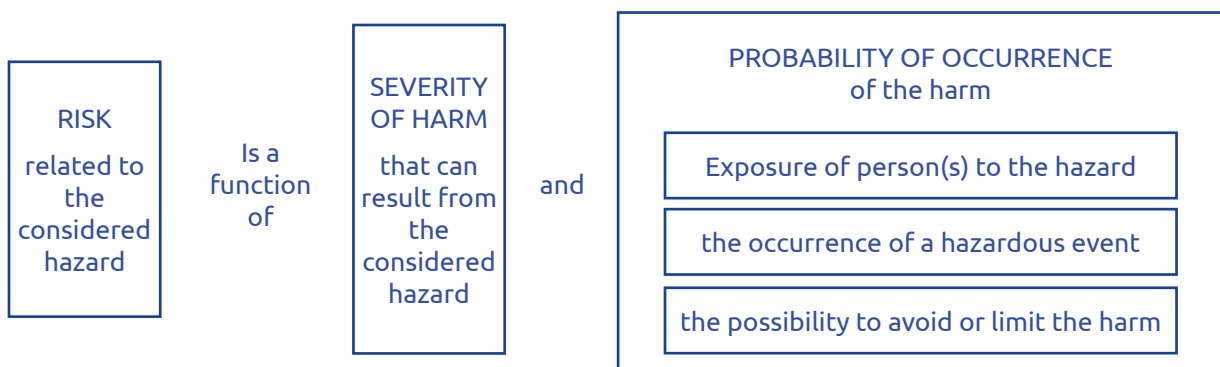
## 2 - Risk evaluation

Once the hazards and hazardous situations have been identified, an estimate of the risks associated with each hazard and each hazardous situation must be carry out. Converting the impact of risk into numerical terms is a difficult task because there is no universal scale of risk. ISO 12100 has decided to define the risk as a combination of the severity of harm and the probability of occurrence of that harm.

Risk can thus be measured by creating a scale based on the product of consequence (in terms of injury to persons) and probability of occurrence (likelihood of an event causing injury).

$$\text{Risk} = \text{Consequence of harm} \times \text{probability of occurrence}$$

Typically, to improve the accuracy of the estimate of the probability of occurrence of harm, additional parameters are added such as the frequency and duration of exposure to the hazard, the probability of occurrence of a hazardous event and the technical and human possibilities to avoid or limit the harm.

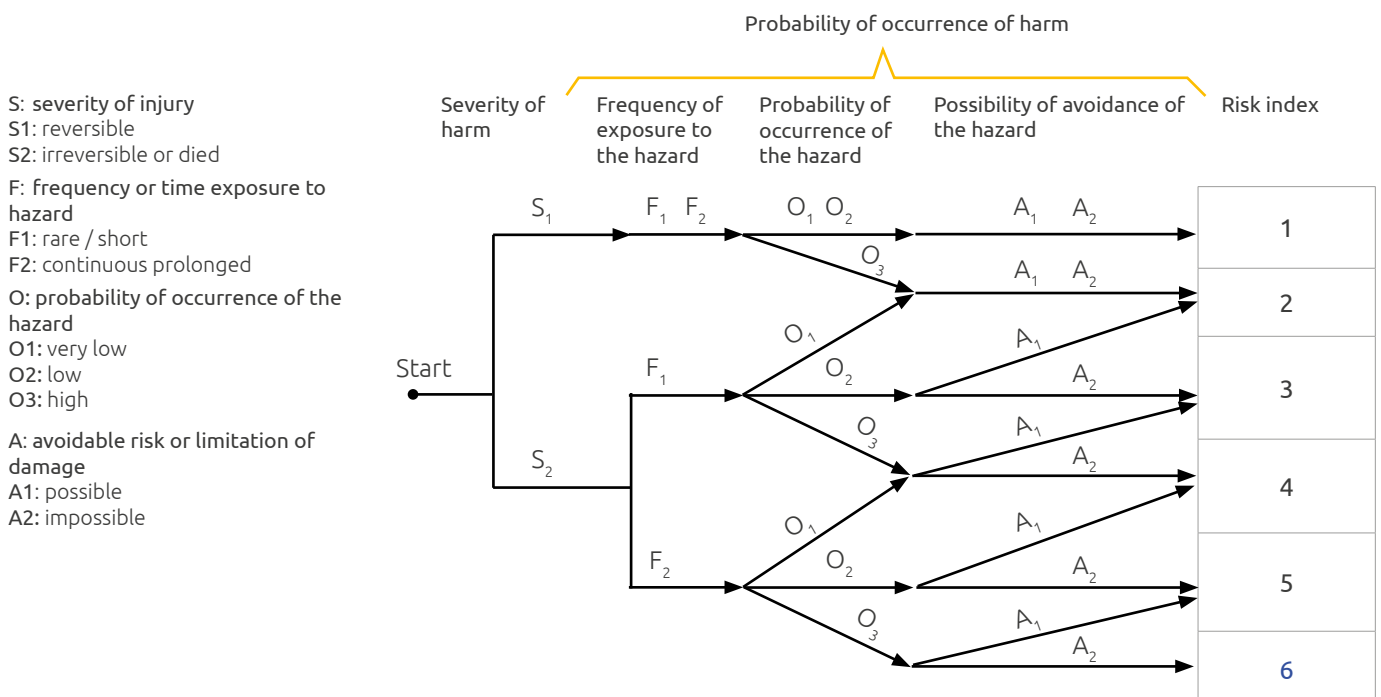


The formula then becomes:

$$\text{Risk} = \text{Consequence of harm} \times (\text{time of exposure} + \text{probability of occurrence} + \text{possibility of avoiding the risk or limiting the harm})$$

A variety of tools have been developed to assist with this process, these include tables, risk graphs, numeric methods.

Example of Risk graph



Example of risk matrix

Consequences	Severity	Class Cl (Fr+P+Av)				
	G	3-4	5-7	8-10	11-13	14-15
Dead, losing an eye or arm	4					
Permanent injury: losing a finger	3					
Reversible injury, medical attention	2					
Reversible injury, first aid	1					

Unacceptable risk
  Moderate risk
  Tolerable risk

Frequency of exposure, Fr		Probability of occurrence, P		Probabilities of avoiding or limiting harm, Av	
≥ 1 per hour	5	Very high	5	Impossible	5
< 1 per hour ≥ 1 per day	5	Probable	4	Possible	3
< 1 per day ≥ 1 per 2 week	4	Possible	3	Probable	1
< 1 per 2 week ≥ 1 per 1 year	3	Low	2		
< 1 per year	2	Very low	1		

Fig. 2. Example of risk matrix

The choice of the method to be used for risk estimation is largely linked to the type of machinery and the nature of the hazards. It is also necessary to take into account the skills, experience and preferences of the team making the assessment.

Compliance with the rules for the estimation of the risk is more important than trying to achieve absolute accuracy of the results.

### 3 - Risk reduction principles

After risk evaluation has been completed, an analysis shall be carried out to determine if any dangerous situations require further risk reduction. Implementing risk reduction means to reduce risk to persons to an “acceptable” level of residual risk.

**Safety does not mean zero risk**

**Zero risk only possible when the hazard is FULLY removed**

**Safety means freedom from unacceptable risk**

In general, there is industry agreement that a risk reduction strategy should utilize a hierarchical approach referred to as the three-step method.

The three-step method shall be applied in the following sequence:

- Step 1 integration of safety concepts at the design stage
- Step 2. add protective measures against risks that cannot be removed by design
- Step 3 inform and warn about residual risks

### Step 1 - integration of safety concepts at the design stage

Inherently safe design is the first and most important step in the risk reduction process because protective measures which are integral to the machine design are likely to remain effective, while experience has shown that even well-designed safeguarding can fail or can be violated or information for use may not be followed. Inherently safe design measures are achieved:

- a. By a suitable choice of mechanical design features for example, by avoiding sharp edges, corners, and protruding parts, by avoiding crushing points, shearing points, and entanglement points
- b. By designing machines to have sufficient stability in their specified conditions of use.  
Factors to be considered include
  - The geometry of the base and the weight distribution, including loading
  - The dynamic forces due to movements of parts of the machine or of elements held by the machine which can result in an overturning moment
  - Vibration, oscillations
- c. By reducing the interaction between the exposed persons and the machine. This objective can be achieved by limiting the time to exposure to the hazard, for example, by means of:
  - Automatic loading and unloading stations
  - Setup and maintenance work from outside the hazardous zones
  - Use of reliable components to reduce maintenance work
  - Clear and unambiguous operating concept (e.g., precise marking of controls)
  - Use of Lock-Out/Tag-Out procedure
- d. By limiting the exposure to electrical power (direct and indirect contact) A stable power supply is particularly important in safety-related applications. Voltage supplies must withstand brief power failures. A power supply isolation device must be provided for every power supply connection. For 24 V DC power supplies, use Class 2 circuit which offers protection for fire initiation and electric shock. Another option to provide protection against electric shock is to use safety extra-low voltage (SELV, PELV).
- e. By using suitable enclosures for protections for electric components. Electrical equipment enclosures must meet the requirement for enclosure ratings. Two widely accepted rating systems are the NEMA types/number and the IP rating code.

The enclosure ratings describe the protection against the ingress of water and foreign objects (dust). In addition, they describe protection against direct contact with live parts.

NEMA (National Electric Manufacturers' Association) is commonly specified at installations in the U.S. IP (International Protection), is derived from the IEC and is typically used in Europe.

Typically, control cabinets should be NEMA 13 or IP 54.

- f. By selecting components that are immune to the disturbances to be expected. The machine and the components used shall be selected so that they are immune to the expected electromagnetic disturbances. Increased requirements apply to safety components.

The following design guidelines will help to prevent EMC problems:

- Continuous equipotential bonding by means of conductive connections between parts of machinery and systems
  - Physical separation from the supply unit (power supply/ actuator systems/inverters)
  - Screen shall not be used to carry equipotential bonding currents
  - Connect any grounding/functional earth (FE) provided
  - Use of twisted cables to transmit data (fieldbus)
- g. By preventing unexpected start-up. The connection to mains electricity supply or switching-on of an external power supply shall not result in the starting of working parts of a machine.

A spontaneous restart of a machine after power interruption shall be prevented (for example, by use of a self-maintained relay, contactor, or valve).

Every machine shall be equipped with a control for stopping the machine in normal operation.

A command to stop the machine shall have a higher priority than the commands for putting the machine into operation.

A Category 0 stop function shall be available as a minimum.

*Stop Category 0:* uncontrolled stop by immediately removing power to the machine actuators (drive elements)

*Stop Category 1:* controlled stop with power available to the machine actuators to achieve the stop, then power is removed when the stop is achieved

*Stop Category 2:* controlled stop with power left available to the machine actuator

## Step 2 - Risk reduction by means of protective measures

If the hazards cannot be removed or the risks cannot be adequately reduced by inherently safe design measures, additional protective measures must be applied, arranged in a way to reduce the probability of occurrence of the hazardous event by suppressing probable causes or to impose a limitation on exposure to the hazards or to enhance the possibility of avoiding the harm or at least by reducing its intensity.

Protective measures can be passive, active, complementary.

### Passive protective measures

They are independent from the machine control system and do not need to be activated to attain their function of risk reduction, they are effective continuously. Are used when access to the hazard zone is not required during normal operation.

Examples of passive protective measures are permanent guards (welded into the body of the machine) and removable fences that can only be removed when the machine is stopped with special tool not easily available to operators.

They provide protection by reducing the duration of exposure to the hazard.

### Active protective measures

Active protective measures are turned on in response to a defined change in a measurable property of an input (e.g., a sensor or a switch). They are intended to reduce the risk generated by the following events:

#### a. Human interaction with the machine

It is possible that a person, which is involved in a certain machine process, with its behaviour exposes himself to dangerous movements of the machine.

Examples of active protective measures suitable to reduce risks generated by human interaction with the machine are ESPEs, safety mats, enabling devices, hold-to-run control devices, interlocking guards.

They provide protection by reducing the probability of occurrence of the harm.

They are intended to work immediately upon a specific initiating event. Their role is to ensure that persons or parts of human body are not injured by the dangerous parts of the machine.

The "demand" of protection is generated by the person with its interaction (operations) with the machine process

#### b. Failures of the machine automation control system (MCS)

It is possible that a failure of a component of the machine automation control system which is involved in a certain machine process can generate dangerous situations such as rise of hot surfaces, flames, excessive vibrations, explosions etc.

Examples of active protective measures suitable to reduce risk due to components failures of the machine automation control system are torque limiters, pressure or temperature limiting devices, overspeed limiters, monitoring devices for the emission of radiation or gas, fire, and smoke detectors.

They provide protection by reducing the probability of occurrence of the harm.

They are employed as a means of prevention and are intended to work before a specific initiating event takes place. Their role is to ensure that the accident does not happen, or at least to slow down its development or to limit to an acceptable level the deviation of the process.

The "demand" is generated because of a failure of the machine automation system.



c. Improper use of the machine.

It is possible that intense usage of the machine due to time pressure or high stress due to excessive loads or due to the processing of unsuitable material can bring the machine to work outside its design limits which in turn can generate mechanical failures of the machine itself or damage to the goods to be processed and, in a second step, can generate risks to the persons.

Examples of active protective measures suitable to reduce risk due to improper use are torque limiters, pressure limiting devices, overspeed limiters, strain gauge sensors, current overload sensors.

They provide protection by reducing the probability of occurrence of the harm.

The “demand” is generated by the overload of the machine because of its improper use.



**NOTE:** Where a protective measure is implemented through the safety-related control system of the machine, it is advisable to use the methods described in ISO EN ISO 13849-1 or EN IEC 62061 for risk estimation because they automatically provide the correspondence between the PL / SIL required and the estimated risk.

### Complementary protective measures

To achieve further risk reduction, it may be necessary to use complementary protection measures considering the intended use and reasonably foreseeable improper use of the machine.

Complementary protection measures whose main effect is to avoid or limit the harm are emergency stop, measures to allow a safe access to machinery, measures for the escape and rescue of trapped people.



**NOTE:** Emergency stop is not considered a primary safeguard because it does not prevent or detect access to a hazard zone. The safety level shall be defined based on the risk assessment of the machine.

Complementary protection whose main effect is to reduce the duration of exposure to the hazard are devices suitable for energy isolation like isolation valves and isolation switches, devices suitable for energy dissipation like pressure relief valves, mechanical locks to prevent movements.

### Step 3 - Risk reduction by administrative measures

To make sure that passive, active and complementary protective measures implemented remain effective all over the machine life cycle additional actions based on procedures and organization are needed.

a. Procedures for maintenance.

Lack of maintenance (poor lubrication and loss of cooling liquid) can lead to mechanical failures or errors. To reduce these type of hazards, detailed maintenance instructions should be developed and implemented.

b. Administrative measures - Organizational work procedures.

At least the following organizational measures should be operative:

- Well defined roles and responsibilities of workers, supervisors and management
- A plan for periodic trainings of workers
- Availability of suitable tools for maintenance and verifications
- A plan for periodic inspections to check the integrity of the protections
- A plan for escape and for Emergency procedures
- Means to keep track of periodic verifications

c. Information for use.

Information for use is an integral part of the design of a machine

- Shall inform the user about the intended use of the machine
- Shall contain all directions required to ensure safe and correct use of the machine
- Shall inform and warn the user about residual risk
- Shall indicate, as appropriate, the need for personal protective equipment

Visual signals, such as flashing lights and audible signals such as sirens may be used to warn of an impending hazardous event such as machine start-up or overspeed.

Such signals shall be emitted before the occurrence of the hazardous event and be differentiated from all other signals used.

Where information for use is kept in electronic form (CD, DVD, tape, hard disk, etc.), information on safety-related issues that need immediate action shall always be backed up with a hard copy that is readily available.

## Safety function as “active” protective measure

Active protective measures are usually implemented by selecting and combining in an appropriate way hardware components (such as sensors, switches, logic units, relays etc.) to build up a Safety Related Control System.

A control system that executes an active protective measure is said to carry out a **safety function** and the control system itself is called **Safety Related Control System**. In complex machines it can happen that multiple hazardous movements can potentially injury the operator. For each hazard for which an active protective measure is required, a correspondent safety function must be implemented.

It may therefore happen that the same safety related control system must handle several safety functions.

When a safety function is activated, the machine is brought to a safe state in time before a dangerous situation for persons can occur.

List of typical safety functions suitable to reduce risk originated by man-machine interactions.

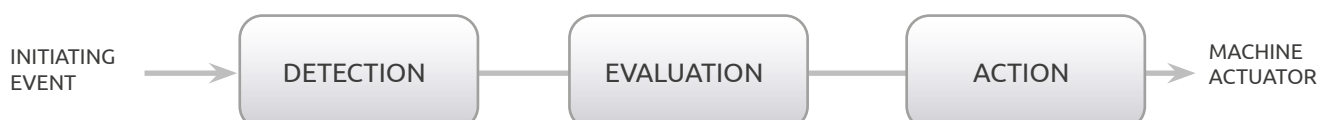
Safety function	Example of application
Safety –related stop function initiated by a safeguard	Stop a motor in response to tripping of a protective device
Manual reset function	Intended action to re-establishes the safeguard after its actuation. Acknowledgement that risk is no more present
Start/restart function	Start of a dangerous movement can take place only when an hazardous situation no more exists
Muting function	Automatic temporary suspension of a safety function
Hold-to-run function	Hazardous machine movements can be controlled from a position within the hazard zone, e.g., inching mode during setup
Prevention of unexpected start-up	Keeping a machine in a stopped condition while persons are present in danger zones
Operating mode selection	Activation of safety functions by an operating mode selector switch
Safe motion, safe position	Overspeed, overtravel control

List of typical safety functions suitable to reduce risks originated by failures of the MCS

Monitoring or limiting of	
Speed	temperature
torque	position
power	stopping time
pressure	stopping distance

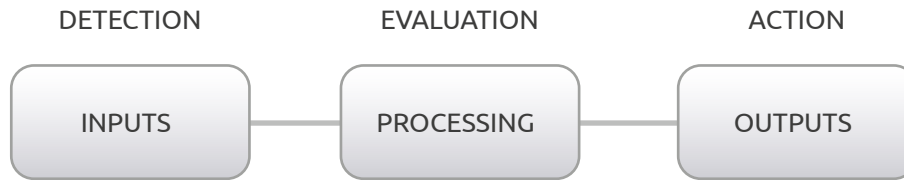
## Structure of a safety function

A safety function is typically starting with a detection and evaluation of an ‘initiation event’ and ending with an output causing an action to a ‘machine actuator’



### Realization of a Safety function

A safety function is usually made by a series combination of three sub-functions performing respectively the tasks of Detection, Evaluation and Action.



Each sub-function can be implemented by:

- Using previously validated subsystems
- Designing new subsystems
- A combination of both alternatives above

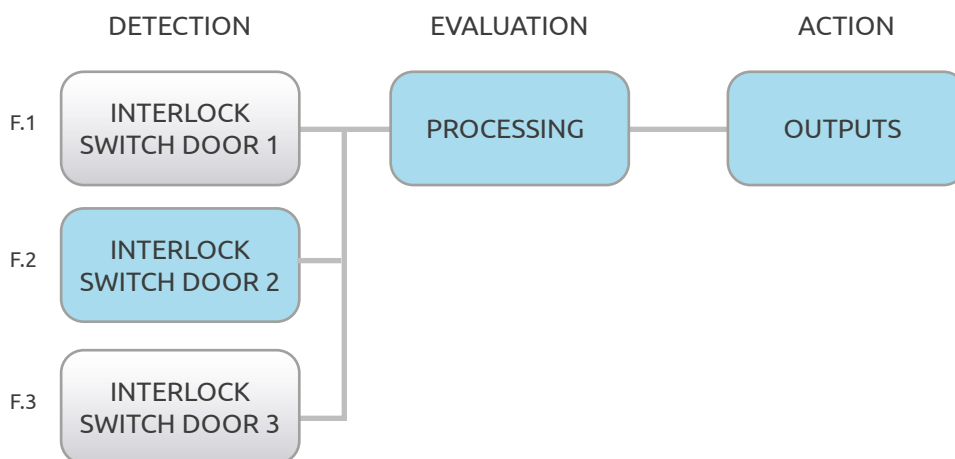
Any of the technologies available (electric, hydraulic, pneumatic, mechanical) individually or in combination may be used.

The risk reduction provided by each safety function does not cover the overall risk of the machine, but only that part of the risk resulting from the application of that safety function. This measure helps to avoid an unduly increase of complexity in the execution of calculations because the reliability data of components of the safety-related control system that do not contribute to that safety function are not considered.

Example:

A hazardous movement is safeguarded by a fence fitted with five guards. The opening of any of the five guards stops the dangerous movement.

Four separate safety functions can be considered, one for each door, if it is assumed that only one door is opened at a time.



E.g. For the safety function F. 2, which refers to door n°2, only the blocks highlighted blue are considered in the computation of the safety function.

### Integration of a safety-related control system into the machine control system

For the integration of a safety-related control system into the machine control system (MCS) the following principles should be applied:

- The safety-related control system is separated and independent from the MCS
- The safety-related control system is only intended for direct or indirect protection of persons; it does not take active part in the machine process and is activated only when a dangerous situation occurs

- The reliability of the MCS does not take any role for the execution of the safety function. It is the reliability of the safety-related control system that is of concern; the greater is the probability that a person will be exposed to the risk, the greater should be the availability of the safety-related control system
- When a dangerous fault occurs in the safety-related control system the machine is brought to a safe state. Restarting the machine process is accepted only after repair and restoration of the safety related control system
- It is also possible that a safety-related control system executes safety functions and machine command functions (for example a safety light curtain or a two-hand control device can be used for both protection and cycle restart).

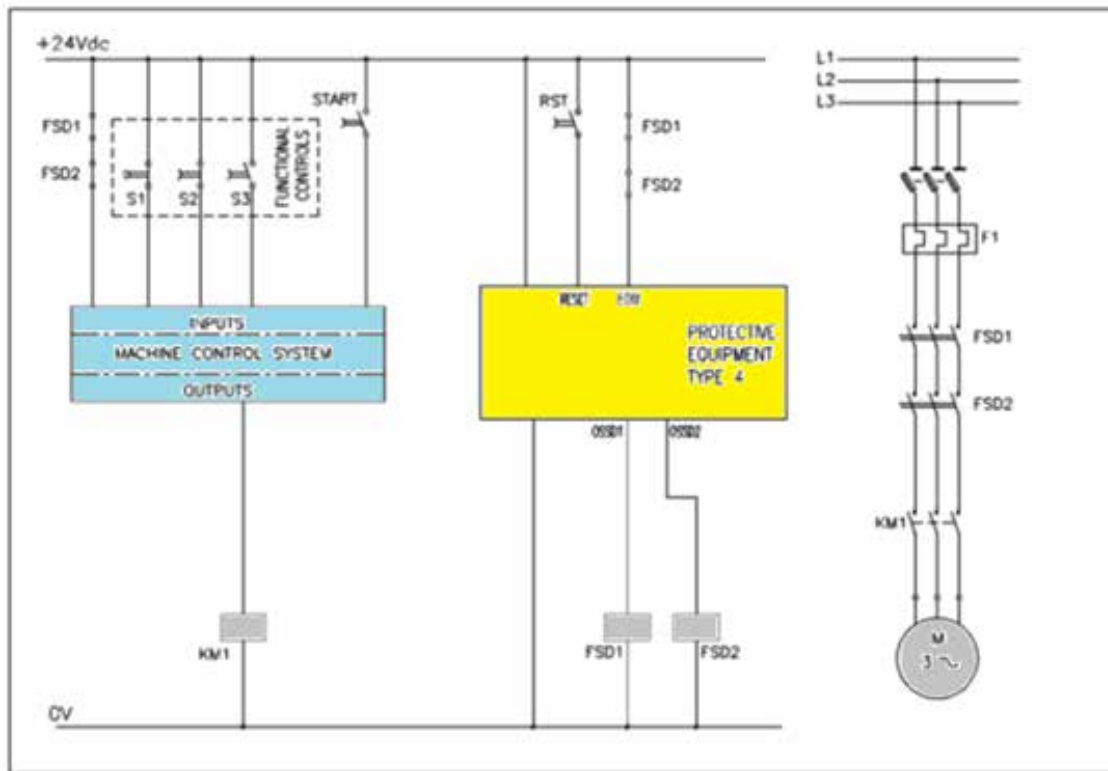
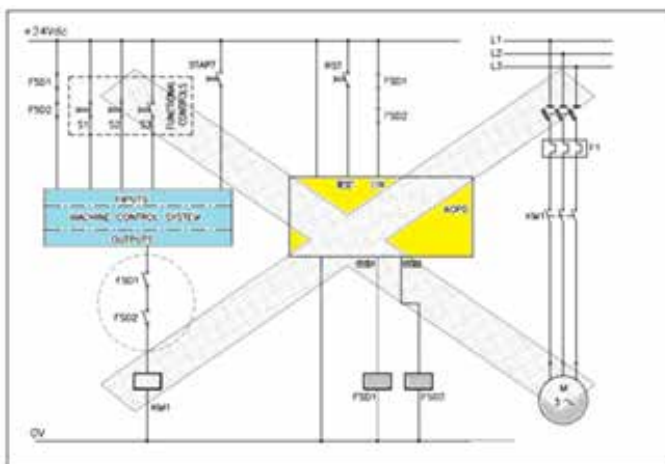
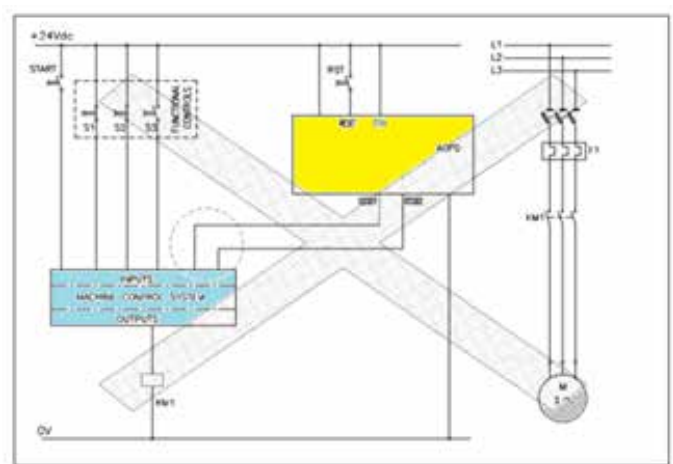


Fig. 3. Example of integration of a safety-related control system with a PLC



A failure to open (e.g. due to welded contacts) of KM1 prevents stopping of the motor.



If the outputs of the SRP/CS are connected TO the inputs of a standard (non-safety) PLC, hw and sw faults within the PLC or the failure of KM1 can prevent stopping of the motor.

Fig. 4. Examples of an incorrect integration



## Functional safety standards

Where safety is based on the proper operation of the safety-related machine control system, it shall be designed so that to ensure a minimal probability of functional errors. Otherwise, any errors shall not lead to the loss of the safety function. In Europe, to meet these requirements it is highly recommended to use harmonized standards developed by mandate of the European Commission (presumption of conformity). Using harmonized standards saves extra time and costs where proof of conformity of the safety-related control system to the essential requirements of the Machinery Directive shall be demonstrated.

Given hereunder are the basic concepts of the standards **ISO 13849-1** and **IEC 62061** which are the most used for the design of the safety functions implemented by the safety related machine control system.

Within the limits of scope, these two Standards provide presumption of conformity with essential requirements of clause 1.2.1 of Annex I of the machinery Directive 2006/46/EC.

### **EN ISO 13849-1,2      Safety of Machinery - Safety Related Parts of Control Systems - General principles for design**

EN ISO 13849-1,2 are used as part of the systematic risk reduction described in ISO 12100 for the part concerning the design of the machine safety-related control system.

ISO 13849-1 is a standard for designing the parts of the control system that implement the safety functions. It can be used for all types of machinery regardless of the type of technology used (electrical, hydraulic, pneumatic, etc.). These parts can be made up of hardware and / or software and can be separated from the machine control system or be an integral part of it.

ISO 13849-1 is applicable only if the safety function is demanded with a frequency higher than once a year (operation in High demand mode) or if it is demanded continuously (Continuous mode of operation) because the tables and formulas provided in the standard relate to these two modes of operation.

Examples of products that are commonly integrated into a safety-related control system are: relays, solenoid valves, position switches, configurable PLCs, safety modules, motor drives, two-hand control devices, pressure sensitive equipment, photoelectric barriers, laser scanner.

The parts of the machine control system that perform safety-related tasks are designated with the acronym SRP / CS (Safety Related Parts of Control System).

In addition to implementing safety functions, an SRP / CS can also provide operational functions, but only the parts that are safety-related fall within the scope of the standard

For the evaluation of the safety performance of an SRP / CS, ISO the term PL (Performance Level) is used which specifies the ability of an SRP / CS to ensure adequate risk reduction within predefined operating conditions.

The performance level is measured on a 5-level scale, from PL a to PL e; each level is associated with a range of values of mean probability of dangerous failure (PFH<sub>D</sub>).

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

Fig. 5. Table from ISO 13849 standard: Performance levels (PL)

## Risk assessment and required Performance Level - PL r assignment

For each safety function identified, the designer must decide what is the contribution to risk reduction the safety function should provide.

This contribution does not cover the overall machine risk but only the part of risk related to the application of that particular safety function.

The parameter, that is used to establish what is the amount of risk reduction that the safety function is required to provide is the PL r (Performance Level Required).

Parameter PL, instead, represents the Performance Level reached by the hardware implementing the safety function. PL of the hardware must be equal to or higher than specified PL r.

After deciding the necessary PL r, it is necessary to design a suitable SRP / CS, calculate the resulting PL of that piece of hardware and check if it is greater than or equal to the PL r.

To get the contribution to risk reduction that must be provided by the safety-related function a graph of decisions is used, leading to univocal identification of the PL r. If more than one safety-related function are identified, PL r shall be identified for each of them.

### S: severity of injury

- S1: Slight injury generally reversible
- S2: Serious injury generally irreversible or died

### F: frequency or time exposure to hazard

- F1: From rare to short and or short exposure time
- F2: From frequent to continuous and or long exposure time

P: avoidable risk or limitation of damage  
(it depends on the speed of the event, the possibility of perception of the hazard and the possibility of escape)

- P1: avoidable within given conditions
- P2: almost unavoidable

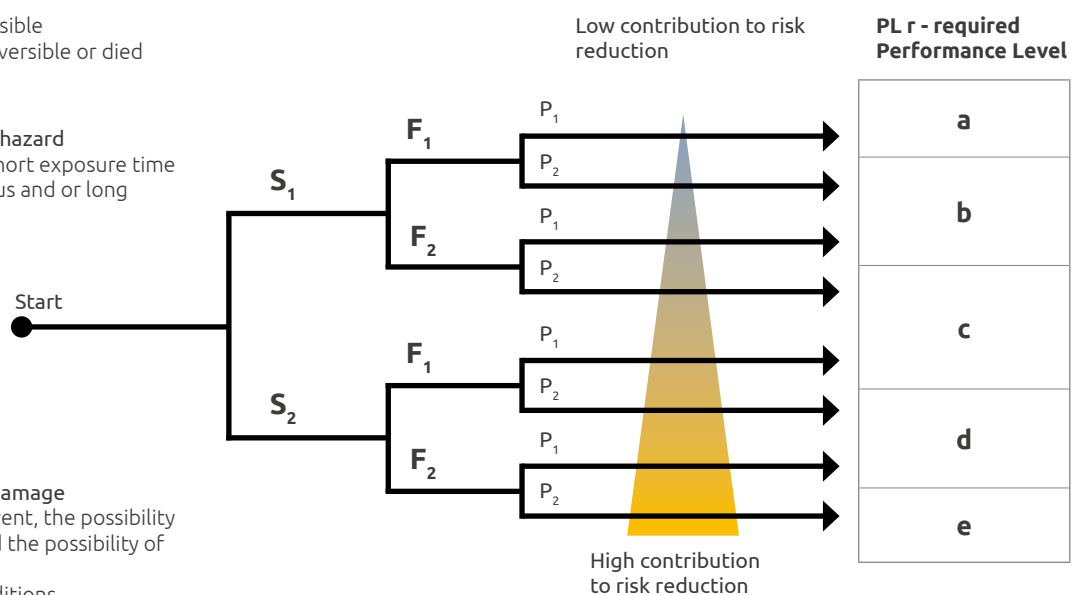


Fig. 6. Graph of decisions for evaluation of the PL r



PL r(e) provides the greatest contribution to risk reduction, whereas PL r(a) makes the lowest contribution.

### Considerations on the S parameter

It is necessary to make an assessment on the type of injuries that could result from a failure of the safety function. EN 13849-1 proposes only two possibilities:

- S1 = slight injury
- S2 = severe injury

Slight injuries are considered to be scratches, peeling, bruising, lacerations without complications. Amputations, loss of function of a limb, loss of an eye, death are considered serious injuries.

### Considerations on parameter F

The distinction between F1 and F2 can be formulated as follows:

F2 is chosen if the frequency of exposure to the hazard is greater than once every 15 minutes. F1 is chosen if the frequency of exposure to the hazard is not greater than once every 15 minutes and the accumulated exposure time does not exceed 1/20 of the overall operating time.

### Considerations on the probability of occurrence of the dangerous event

The probability of the occurrence of a dangerous event depends on both human behaviour and technical failures, it should be based on factors such as:

- Reliability data of the control system
- History of accidents on similar machines (with the same risk, same process, same operator action and same technology causing the hazard).

The probability of occurrence is always evaluated to be equal to 1 because in most cases, the correct probability is not known or is difficult to estimate.

If the probability of occurrence of a dangerous event can be judged low, the PL r can be reduced by one level.

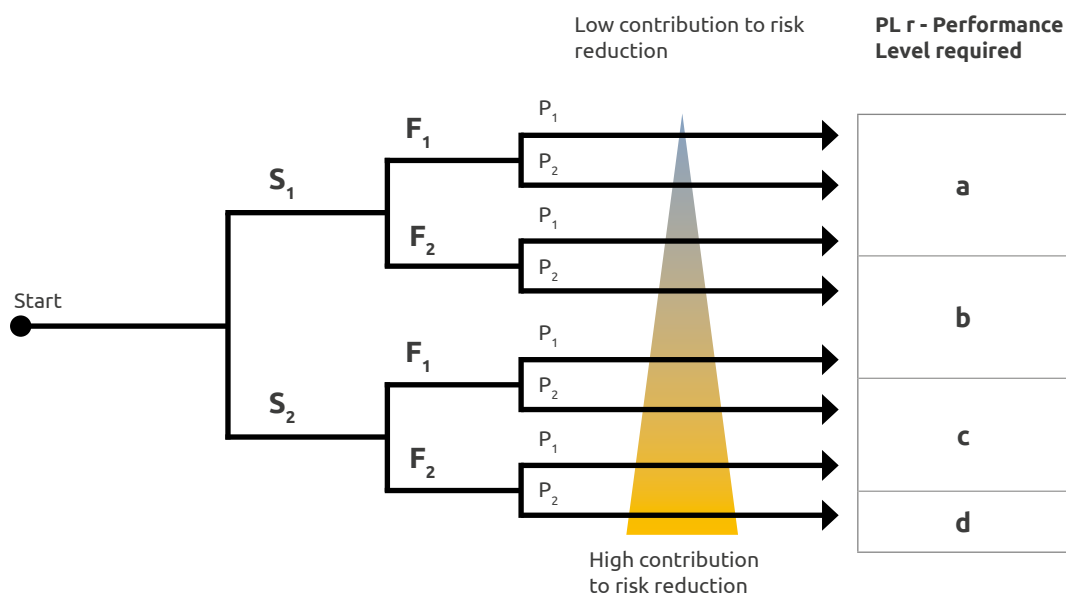


Fig. 7. Graph of decisions for evaluation of the PLr if (P) probability of occurrence of a dangerous event can be judged low

## Overlapping of hazards

It is possible that the same person may be subjected to the simultaneous interaction of multiple hazards due, for example, to the presence of multiple dangerous movements of the machine that could potentially create harm.

If the evaluation of the probability of failure were made by taking into account all the hardware components of the overall safety related control system, very high  $PFH_D$  values would soon be reached (even if components with very high  $MTTF_D$  values were used) with consequent impossibility to stay within the required PL r.

Things get even more complicated if the individual risks require different PL r.

To overcome the problem it is allowed to separate the risks, if this is possible, and to assign to each of them a separate safety function.

The designer must analyse this possibility during the risk assessment process. First, the dangerous zone is identified, then all dangerous movements of the machine parts that are located in the same dangerous zone are identified, then all the operations carried out by the machine in the same zone are considered and which are the parts of the body that are subjected to risk.

If the analysis shows the possibility of separating the various dangerous movements, then a separate safety function is assigned to each dangerous movement and the relevant PL is calculated.

### Example 1

In a working cell that involves several robots on different operations, the stopping function following the actuation of the light curtain can be evaluated individually for each robot.

For the example of the machining cell shown in the picture, the following safety functions can be identified:

SF1: The actuation of the safety light curtain involves the stopping of all robot 1 drives

SF2: The actuation of the safety light curtain involves the stopping of all the robot 2 drives

SF3: The actuation of the safety light curtain involves the stopping of all robot 3 drives



Fig. 8. Working cell involving multiple robots on different operations

The same consideration applies for example to a rotary table equipped with several clamping devices; the risk assessment can be done separately for each clamp.

### Example 2

In a welding robot the operator is exposed simultaneously to the risk of crushing due to the movement of the robot head and to the risk of burning due to the tool mounted on the head. In this case the robot head and tool must be taken into account at the same time in the evaluation of the safety function.

### Example 3

For a robot in learning mode it is possible to keep power to the robot when the entrance door of the cell is open, only if a local enabling device (hold-to-run control) is used and that the robot is operated at a reduced safety speed.

The probability of failure of all three devices (door interlock, hold-to-run and speed monitor) must therefore be included in the calculation of the  $PFH_D$  because the dangerous failure of one of them immediately leads to a dangerous condition.

## Identification of the safety function and design specification

To decide which safety functions are required, the intended use of the machine must be considered (including reasonably foreseeable misuse). For each safety function, a document must be drawn up in which at least the following specifications are detailed:

- Result of the risk assessment for each hazard (PL r value)
- Behaviour that is intended to be achieved or prevented with the safety function (e.g. when the guard is opened the machine performs a stop Cat.0)
- Intended use of the machine and reasonably foreseeable misuse
- Operation in emergency conditions
- Safety function response time
- Restart after a protective action (automatic or manual restart)
- Actuation mode (related to a section or part of the machine)
- Need to suspend the safety function (muting, banking)
- By-pass mode of the safety function for repair, tuning, cleaning, troubleshooting, etc.
- Description of connections between different safety function, if any
- Safety function actuation frequency
- Priority of functions which, if active at the same time, can cause operating conflicts

To help the designer, the standard lists the main safety functions that are generally implemented in an SRP / CS and for some of them it provides the main safety requirements:

- Safety related stop function started by a safety measure
- Manual restart function
- Start / Restart function
- Local command function
- Muting function
- Hold-to-run control function
- Enable device
- Prevention of unexpected start-up
- Escape and rescue of trapped people
- Isolation function and energy dissipation
- Command mode and enable mode
- Emergency stop function

### Safety-related stop function

The stop function activated by the actuation of a protective device must bring the machine to a safe state in the shortest time possible.

The safety-related stop function has priority over a stop for operational reasons.

When a group of machines work together, it is necessary to report to the supervisory control and / or to the other machines the existence of the safety stop.

After the actuation of a stop command by a protective device, the stop condition must be maintained until a safe condition exist for restarting.

## Manual restart function

Reset command restarts the protective device and cancels the safety stop command. If established by the risk assessment, this cancellation must be confirmed through a manual, separate and deliberate action (manual reset). The manual reset function:

- It must be authorized through a separate device, included in the SRP / CS and operated manually
- It must be enabled only if all protective devices are operational
- The manual restart must not initiate a movement or a dangerous situation
- It must take place through deliberate action
- It must enable the control system to accept the start command
- It must be enabled only when the machine actuator is in the OFF state

## Muting function

Muting function must not expose people to dangerous situations. During Muting, the safety conditions must be guaranteed by other protection devices. At the end of Muting, all the safety functions of the SRP / CS must be reset automatically. The PL of the parts of the SRP / CS that perform the Muting function must not decrease the safety level of the protective device to which are connected.

## Safety related parameters

When the deviation of parameters such as position, speed, temperature or pressure, beyond the set limits can cause safety problems, the control system must implement appropriate measures (for example, stopping, warning signal, alarm).

## Fluctuations, loss and restoration of power sources

When fluctuations in power levels exceed the designed operating range, including loss of power, the SRP / CS must continue to provide or send output signals that allow other parts of the machine system to maintain a safe state.

## E – Stop

The E-Stop is defined as a "complementary protection measure" (it is not a safety function).

It is used to reduce the risk of unreasonably foreseeable failure or accidents in parts of the machine, including failure of protective devices. Since it must be available in case of failure of the other protective devices, it is also advisable to consider it in EN ISO 13849-1.

It must be available and operational at all times and must bypass all other functions and operating modes of the machine (without compromising any structures designed for the escape of trapped peoples). Any start command (voluntary, unintentional, or unexpected) must not have effect on those parts of the machine stopped by the E-stop command until the device is manually reset.

The PL r of the E-Stop function should be the same of the safety function with the highest PL r involved in the realisation of the SRP / CS.

## Local control function

When a machine is locally controlled, e.g. by means of a portable control device it is necessary that:

- The local control device selector must be located outside the danger zone
- Local control must be active only in the part of the dangerous area identified by the risk analysis
- The change from local control to main control must not create a dangerous situation

## Response time

When, following the risk assessment, it is found that the response time of the SRP / CS can be decisive for safety purposes, its response time must be added to the response time of the other devices of the safety loop in order to get the overall response time of the machine.

The overall response time required for stopping the machine can affect the design of the SRP/CS, e.g for some applications it can be necessary to add a braking system.



## Realization of a safety function with an SRP/CS

A safety function can be done using one or more SRP/CS.

All available technologies can be used, also in combination; electrical, hydraulic, pneumatic, mechanical etc.

It is also possible for an SRP/CS to implement safety functions and normal command functions (for example a photo-electric light curtain or two-hand control can be used for both protection and start cycle).

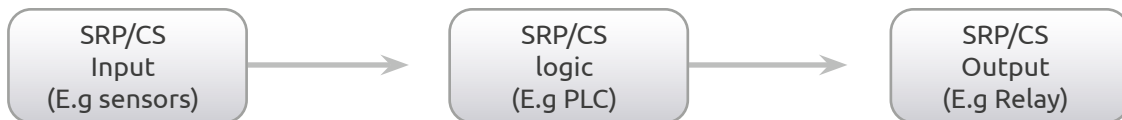


Fig. 9. Typical architecture of the SRE / CS

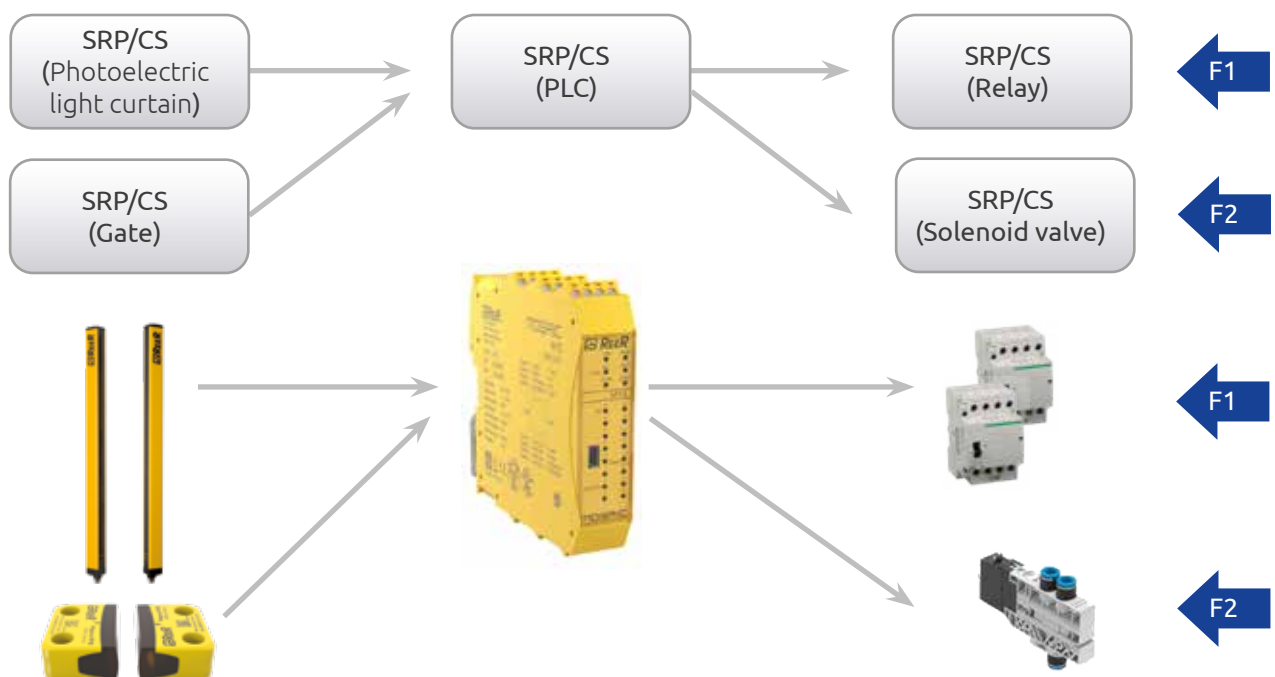


Fig. 10. Several safety functions can share one or more SRP/CS

The designer has to decide the required contribution to risk reduction for each safety function.

The evaluation of PL r must be carried out separately for each individual safety function.

## SRP/CS design phase - Organisational aspects

Before creating an SRP/CS, in order to reduce as much as possible the introduction of systematic failures during the design phase or as a result of subsequent modifications, it is necessary to have a management organization that follows structured procedures covering the entire life cycle of the SRP/CS. Each design activity should be properly specified, documented and verified.

## PL of the SRP/CS

PL is a function of several factors such as :

- Hardware and software architecture
- Ability to promptly detect internal failures potentially affecting the safety function
- Component reliability, the ability to limit common cause failures
- Quality of the design
- Environmental conditions and operational stresses
- The operating cycle of the machine.

Intended use and reasonably foreseeable misuse must be considered.

The table below summarizes the quantitative requirements, assigning them an overall value of probability of dangerous failure, and the qualitative aspects that must be met in order to obtain a PL.

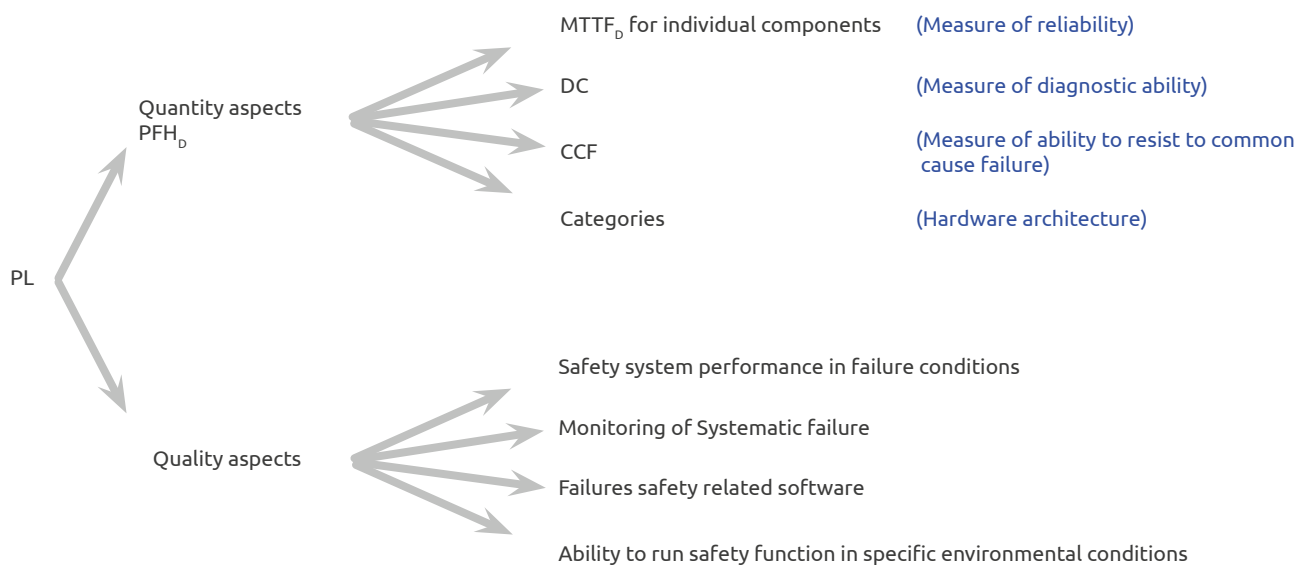


Fig. 11. Mandatory qualitative and quantitative requirements to be met for safe control system design according to ISO 13849-1

### Remember

*Average Probability of Dangerous Failure/Hour is only one of the parameters contributing to assignment of PL. To claim a PL rating, it is also mandatory to prove having considered and complied with all requirements, including:*

- *Monitoring of systematic failures*
- *Using robust and reliable components (according to Product Standards if available)*
- *Use of good engineering practice*
- *Considering environmental conditions in which the safety-related system will operate*
- *In the case of new software, adopting all organisational aspects of V-type development model shown in Figure 6 of ISO 13849-1 and meeting development requirements for application SW and embedded SW.*

### PFH<sub>d</sub> calculation

The method used for the evaluation of the part of the PL linked to the quantitative aspects is the computation of the probability that a dangerous failure may occur to the SRP/CS in a certain period of time, considering the reliability of its components.



The greater the contribution to risk reduction provided by the safety function the lower must be the PFH<sub>d</sub> (average probability of dangerous failure) of the SRP/CS.

A fault is considered dangerous if it inhibits the protection function of the safety related control-system.

The Average probability of dangerous failure for a safety-related control system, or for a sub-system, may be estimated in various ways. These methods require the use of complex mathematical formulas which typically belong to the field of system reliability theory. The use of such methods implies that for each components the following are known:

- Failure rate ( $\lambda$ )
- Percent distribution of failure rate for each component failure modes, (example: for a positive action switch the failure modes are: the contact will not open when required = 20% of the times and the contact will not close when required = 80% of the times)
- The effect of each failure on safety-related system performance, (e.g dangerous failure or not dangerous failure)
- Percent of dangerous failures detected (by automatic self-diagnostic techniques implemented) out of total dangerous failures
- Percent of dangerous failures not detected (by automatic self-diagnostic techniques implemented) out of total dangerous failures

ISO 13849-1 simplifies this process by replacing the mathematical formulas with precalculated tables for different combinations of Categories, average MTTF<sub>d</sub> and DC values which are also determined through tables

Design of an SRP/CS as per ISO 13849-1 may be summarized in the following eight steps:

1. Selection of system structure (architectures)
2. Calculation of MTTF<sub>d</sub>
3. Selection of the self-diagnostic techniques and DC calculation
4. Verification of CCF for redundant architecture
5. Calculation of PL using Table 5 or Table K.1
6. Verification of PL (if calculated PL is below PL<sub>r</sub> return to Step 1)
7. Validation.

## Categories and their relationship with the $MTTF_D$ with the DC and with the CCFs

EN / ISO 13849 uses a methodology based on 5 particular structures called "Categories" which constitute the backbone on which all the quantifiable aspects that contribute to the formation of the PL are based.

The categories describe the performance of an SRP/CS in relation to:

- Structural arrangement of its parts
- Its fault tolerance
- Its behaviour under fault conditions
- Reliability of its components

This means that the safety performance is achieved not only through particular hardware architectures (which the standard defines as designated architecture), but also through a careful use of reliable components and, if necessary, of adequate monitoring techniques. The choice of a category mainly depends on:

- Amount of risk reduction needed
- Required performance level (PL r)
- Technology used
- Type of risk due to the failure of the SRP/CS
- Possibility to avoid systematic failures in the SRP/CS
- Probability of failures in the SRP/CS
- Mean Time to Dangerous Failure ( $MTTF_D$ )
- Diagnostic coverage (DC)
- Common Cause Failures (CCF) in the case of categories 2, 3 and 4

It should be noted that the designated architectures give a logical representation of the system structure, while the technical implementation and the functional circuit diagram may appear completely different.

Designated architectures can also be used to describe a part or a sub-part of a control system responding to certain input signals and generating safety output signals. Therefore the "input" block can represent, for example, a photo-electric light curtain (AOPD) or switch contacts. The "output" block can represent, for example, a safety-related output (OSSD) or a combination of relay contacts.

For categories 3 and 4 the dual channel representation does not mean that all parts need to be physically redundant but that redundant means exist to ensure that a single fault cannot lead to the loss of the safety function.

There are certainly several ways to create architectures that can satisfy the requirements established by the categories. If the structure of the control system is made by one (or more) of the 5 categories, then for the computation of the safety performance level (PL) it is possible to use the simplified procedures described in the standard.

If an architecture deviates from those of the Categories, then its PL cannot be evaluated with the simplified method of the standard, but must be justified by other analytical means, for example by Markov modeling, in order to show that through this non designated architecture it is possible to achieve the required performance level (PL r). Markov offers a remarkable ability to manage many of the technical characteristics that are implemented in modern safety devices, for example it is possible to model periodic events such as automatic fault diagnostics tests.

## Overview of the main safety requirements and functional characteristics of the 5 categories

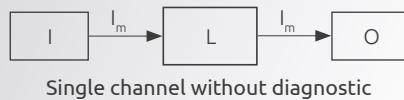
The categories reflect what is already happening in the industrial machinery world. Most of the controls implemented on machines can be traced back to a limited number of safety-related control topologies, which are:

- Untested single-channel systems using reliable components (goal is to avoid a fault)
- Single-channel systems with testing (goal is to detect the fault)
- Dual-channel systems with self-diagnosis (single fault is detected)
- Dual-channel systems with high quality self-diagnosis (even multiple faults are detected)

**NOTE:** The lines and arrows in the following figures represent logical, functional, and diagnostic interconnections.

## Cat. B

Fault tolerance = 0



Single channel without diagnostic

$PL_{max} = b$

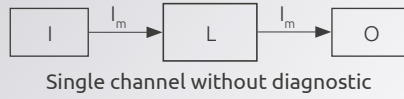
DC = 0

$MTTF_D$  = from low to medium

Use of **basic safety principles** (components must withstand the expected operating stresses)

## Cat. 1

Fault tolerance = 0



Single channel without diagnostic

$PL_{max} = c$

DC = 0

$MTTF_D$  = alto

Use of **basic safety principles** and **"well tried" safety principles**;

Use of **"well tried" components**; no complex components (PLC, Asic).

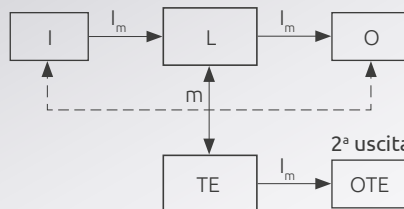
A "well tried component" is a component that has been:

- Widely used in the past with positive results in similar applications
- Built and verified using principles that demonstrate its suitability, reliability and robustness for safety related applications

The qualification of a component as well tried depends on its application. Example, a position switch with open contacts can be well tested for a machine tool and at the same time inappropriate for application in the food industry.

## Cat. 2

Fault tolerance = 0



Single channel with diagnostic

$PL_{max} = d$

DC = from low to medium

$MTTF_D$  = from low to medium (functional channel components only)

$MTTF_D$  of TE at least higher than half the  $MTTF_D$  of the functional channel.

If this is not the case, the  $MTTF_D$  of the channel must be downgraded.

Use of **basic safety principles**

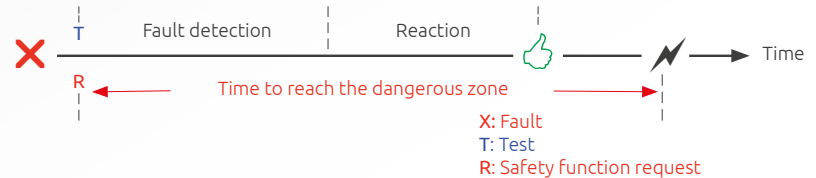
Use of **"well tried" safety principles**

The test must not produce a dangerous situation (e.g increase in the response time).

The safety function must be tested at least during the start-up and before a dangerous condition may occur (starting a new cycle). The frequency of the functional channel test has to be at least 100 times higher than the demand rate of the safety function.

For ratios greater than 25 and less than 100 it is possible to use the  $PFH_D$  values (shown in table K.1 for Cat. 2) multiplied by a factor of 1.1.

The test can also be performed at the same time as the safety function request, but the overall time to detect the fault and to bring the machine to a safe condition (usually when the machine is stopped) must be shorter than the time taken by a person to reach the dangerous point.

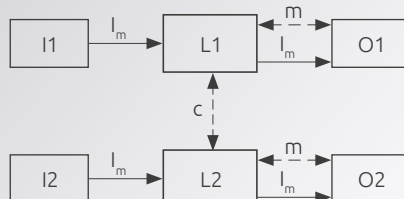


For  $PL_r = a$  and up to  $PL_r = c$ , when, upon detection of the fault, it is not possible to initiate a safe state (for example due to the welding of the contact in the output device), it may be sufficient that the output OTE only provides a warning signal.

For  $PL_r = d$ , the OTE output must initiate a safe state which is maintained until the fault is cleared.

## Cat. 3

Fault tolerance = 1



Dual channel with diagnostic

$PL_{max} = e$

DC = from low to medium

$MTTF_D$  = from low to medium

Use of **basic safety principles**

Use of **"well tried" safety principles**

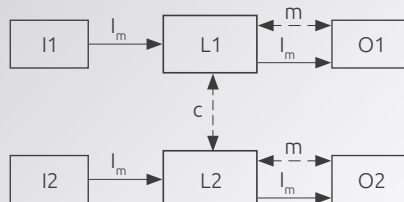
A single fault does not lead to the loss of the safety function.

When reasonably practicable, the single fault must be detected during or before the next safety function request.

Not all faults can be detected. The accumulation of undetected faults leads to the loss of the safety function.

## Cat. 4

Fault tolerance = 1



Dual channel with diagnostic

$PL_{max} = e$

DC = High

$MTTF_D$  = High

Use of **basic safety principles**

Use of **"well tried" safety principles**

A single fault does not lead to the loss of the safety function.

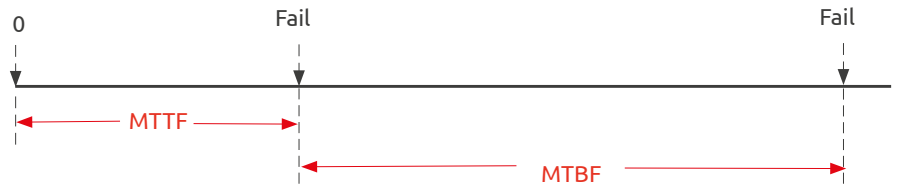
Faults must be detected in time before the loss of safety function. For example, immediately upon their occurrence, or when the machine is turned on, or at the end of the operating cycle. If this detection is not possible, the combination of two independent faults must not lead to the loss of the safety function.

## Computation of the $MTTF_D$ - Average time before a dangerous failure occurs

The true reliability of a component is never exactly known, but statistics and reliability theory give us the tools for its estimation.

The failure rate  $\lambda$  is the measure of reliability of a component; it gives the number of failures per unit time (hour).

Its reciprocal, called mean time between failures, is commonly indicated with the short form MTBF (mean time between failures) or MTTF (mean time to failure) in case of the first failure after the initial start-up. MTTF is measured in years.



For the computation of the  $PFH_D$ , it is important to know only the  $MTTF_D$ , i.e. only the faults that can cause a dangerous system operation.

To help the designer to select which faults to consider, EN ISO 13849-2 (Annexes A to D) provides, for each technology, a list of relevant faults and the conditions under which it is possible to assume that they cannot occur (faults exclusion).

The list is not exhaustive and, if necessary, additional faults can be added depending on the particular application.

In practice, for each SRP / CS it is advisable to build a list of all components used and for each of them establish the faults to be considered on the basis of the list of faults provided in EN ISO 13849-2, then determine if the type of fault is a dangerous fault, or if has no safety relevance or if can be excluded a priori.

For ease of computation or in case of uncertainty, the standard makes it possible to consider, for each component, 50% of possible faults as dangerous (worst case), therefore:

$$MTTF_D = 2 \times MTTF$$

Furthermore, to simplify, the following criterion was adopted:

- If a "first fault" directly triggers a second fault, the probability of occurrence of this second fault is the same as that of the first fault; it follows that the first fault and all those originated by it must be considered as a single fault. If, in some circumstances, two faults have the same common origin, they must be considered as a single fault (CCF).
- The simultaneous occurrence of two or more faults due to separate causes is highly unlikely (product of two probabilities extremely low on their own) and therefore is not considered. This means that it is generally acceptable that the simultaneous occurrence of multiple independent faults can generate a hazard.
- Each SRP / CS must be reasonably reliable so that the probability of a "first failure" is low; therefore,  $MTTF_D$  values of less than 3 years are not considered.

### $MTTF_D$ : where to get data?

The hierarchical procedure for finding reliability data should be as follow:

- a. Use of manufacturer's data
- b. Use of data of table C.1 of the Standard for most commonly used mechanical, hydraulic, pneumatic, electrical components for which the failure mechanism is due to wear of materials
- c. Use of data of tables C.2 to C.7 for electronic components
- d. Select 10 years

The use of data of table C.1 is allowed only if it is possible to prove that good engineering practices have been followed. This means:

- The components selected have been designed and manufactured according to basic safety principles and well tried safety principles according to ISO 13849-2 or other relevant standard. (Confirmed in component's data sheet).
- The manufacturer specifies that the component is appropriate for the application and operating conditions of the user.
- The manufacturer of the SRP/CS, declares that the component is used respecting basic and well tried safety principles according to ISO 13849-2.



### MTTF<sub>D</sub> of parts whose failures are mainly due to wear

For all electromechanical and pneumatic components subject to wear (e.g relays, solenoid valves, switches) the failure rate increases with the number of worked cycles, therefore their reliability is generally not referred to the working time but to the number of worked cycles.

The parameter provided by the manufacturers is B<sub>10</sub> (numbers of cycles until 10% of the components have failed in a life test, under specified load).

The percentage of B<sub>10</sub> for which the component has failed dangerously is indicated with B<sub>10D</sub>.

In the absence of detailed information, EN ISO 13849-1 recommends considering 50% of failures as dangerous:

$$B_{10D} = 2 \times B_{10}$$

Knowing the B<sub>10D</sub> and the average number of operations in a year (N<sub>op</sub>), the value of MTTF<sub>D</sub> is derived as follows:

$$MTTF_D = \frac{B_{10D}}{0,1 \times N_{op}}$$

Then, the useful life of the component must be limited to T<sub>10D</sub> (time within which 10% of the components under consideration fail dangerously).

$$T_{10D} = \frac{B_{10D}}{N_{op}}$$

This time must be compared with the mission time of the machine (20 years, established by the standard). If the useful life T<sub>10D</sub> of the component is less than 20 years, the component must be replaced before the expire of its useful life.

Relay example:

B<sub>10</sub> = 3.000.000 cycles

Workload

d<sub>op</sub> = 220 dd/year

h<sub>op</sub> = 16 h/day (two shifts of work)

t<sub>ciclo</sub> = 15 s (machine cycle)

$$N_{op} = \frac{220 \times 16 \times 3600}{15} = 0,84 \times 10^6$$

$$MTTF_{op} = \frac{B_{10D}}{0,1 \times N_{op}} = \frac{2 \times 3 \times 10^6}{0,84 \times 10^6} = 71 \text{ years}$$

$$T_{10D} = \frac{B_{10D}}{N_{op}} = \frac{2 \times 3 \times 10^6}{0,84 \times 10^6} = 7,1 \text{ years}$$

The useful life of the relay is just over 7 years. The relay must be replaced in the seventh year of operation.

### Computation of the MTTF<sub>D</sub> of the SRP/CS

The relationship between the reliability of the components, their number in a channel and the total MTTF<sub>D</sub> of the channel is the following:

$$\frac{1}{MTTF_D} = \sum_{i=1}^N \frac{1}{MTTF_{Di}}$$

Where MTTF<sub>Di</sub> is the MTTF<sub>D</sub> value of each component

The formula is also valid for several SRP/CS connected in series to form a channel where the failure of one component causes the failure of the whole channel.

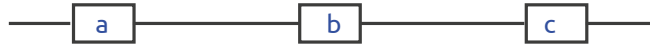
The MTTF<sub>D</sub> of a channel greater than 100 years are not acceptable since the PFHD of the SRP/CS must not depend only on the reliability of the components. An exception is Category 4 where the limit is extended up to 2500 years.



Individual components of a channel may have MTTF<sub>D</sub> values higher than 100 years.

Example: channel consisting of three components a, b and c

- a)  $MTTF_D = 228$
- b)  $MTTF_D = 45662$
- c)  $MTTF_D = 14269$



$$\frac{1}{MTTF_D} = \frac{1}{228} + \frac{1}{45662} + \frac{1}{14269} = 4,38 \times 10^{-3} + 2,19 \times 10^{-5} + 7 \times 10^{-5} = 4,5 \times 10^{-3}$$

$$MTTF_{op} = \frac{1}{4,5 \times 10^{-3}} \approx 223 \text{ years} \quad \text{It should be limited to 100 years up to PL d}$$

In the case of dual channel systems (Cat. 3 and Cat. 4) only one channel needs the computation of the  $MTTF_D$ , but if the overall  $MTTF_D$  of each of the two channels have different values (not homogeneous channels), there are two possibilities:

- a. The lower  $MTTF_D$  value of the two is selected (worst case)
- b. The following formula is used which “re-homogenizes” the two channels. The dual channel system is replaced with an equivalent architecture having identical  $MTTF_D$ s for both channels.

$$MTTF_D = \frac{2}{3} \left[ MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}} \right]$$

$MTTF_{DC1}$  e  $MTTF_{DC2}$  are the  $MTTF_D$  values of the two channels.

Once the calculation is completed, the  $MTTF_D$  class is chosen by means of the following table:

Denotations of $MTTF_D$	Range in years
Low	$3 \leq MTTF_D < 10$
Medium	$10 \leq MTTF_D < 30$
High	$30 \leq MTTF_D < 100$

## Fault exclusion

The possibility of a fault exclusion is linked to the compromise between the requirement to consider all dangerous faults and the theoretical possibility that certain type of dangerous fault could not occur.

Fault exclusion is based on:

- The very low probability of occurrence of some faults
- The accepted technical robustness of a certain type of component, regardless of the application considered
- The technical requirements concerning the application and the type of risk

Since a fault exclusion can lead to a very high PL, a detailed justification of the exclusion must be provided in the technical documentation.

For new components or components that are not in the lists of ISO 13849-2, an FMEA analysis (see IEC 60812) must be carried out to establish the faults that must be considered for these components and those that can be excluded.

If dangerous faults can be excluded for a component, the contribution of the component to the  $MTTF_D$  is zero.

For electromechanical components, the analysis on the fault exclusion must be conducted separately for the mechanical part and for the electrical part, considering the environmental conditions and possible external influences.

### Choice of diagnostic techniques and DC computation

If it is supposed:

- That a failure can always occur (otherwise there would be no reason to define the MTTF)
- That the mechanisms for faults detection are not all equally efficient and immediate (it depends on the type of fault, for some faults it may take longer time) and that it is not possible to be able to detect all faults
- However, by adopting suitable circuit arrangements, it is possible to detect most of the dangerous faults

then it's possible to define a DC parameter that specifies how efficient the system is in detecting its own malfunctions "in time" (in time means before a second dangerous fault can occur).

### DC computation - General rule

The DC parameter is expressed as the ratio between the failure rate of dangerous failures detected by the implemented self-diagnostic measures,  $\lambda_{dd}$ , and the failure rate of all possible dangerous failures  $\lambda_d$  (detected and undetected).

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d}$$

Knowing  $\lambda_d$  and the percentage of fault coverage provided by the diagnostic measures implemented, it is possible to derive  $\lambda_{dd}$  (detectable) and  $\lambda_{du}$  (not detectable) and then compute the value of DC for the entire subsystem.

### DC computation -Simplified method

This simplified method is based on the diagnostic techniques listed in Table E.1 of the Standard. Table E: 1 provides a list of 34 different diagnostic techniques divided into three families (for input circuits, for processing logic, for output circuits). If the designer decides to use diagnostic techniques to increase fault coverage, he can choose the preferred techniques among those listed in Table E.1 that best suit its application. A variable fraction of DC coverage ranging from 0% to 99% is assigned to each technique.

- 0% = the selected technique does not detect dangerous faults
- 60% = a low fraction of dangerous failures is detected
- 90% = an average fraction of dangerous failures is detected
- 99% = a very high fraction of dangerous failures is detected

It is also possible to select diagnostic techniques with different DC values for the individual parts. The formula that allows the computation of the DC of the entire system (DC) is

$$DC = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \dots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \dots + \frac{1}{MTTF_{DN}}}$$

Where  $MTTF_{Di}$  and  $DC_N$  are the values of  $MTTF_D$  and DC of the individual individual components of the subsystem

A part with a low DC and a low  $MTTF_D$  has great weight and leads to a low DC value. A part that is not tested gets a DC = 0 and contribute only to the value of the denominator. Once the calculation is completed, a DC class is chosen by means of the following table:

As was done for the choice of the  $MTTF_D$ , also for the DC the Standard does not require knowledge of the exact value for the computation of the PFH<sub>d</sub>, but that a choice is made among four ranges of values.

Denomination DC	Range of values DC
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

## CCF evaluation for redundant architectures

CCFs (Common Cause Failures) are failures due to a single cause that can affect multiple components at the same time.

CCFs can occur simultaneously on multiple components due to a shock, or due to an increase in system stress (e.g increase in temperature, humidity, vibration), or due to electromagnetic interference, or due to design errors.

It is important to consider whether common cause failures can occur. These failures can nullify the effects of redundancy. Indeed, if two or more distinct channels in a multichannel system are simultaneously in a faulty state because of common cause failures, the entire safety-related control system could lose the protective effect.

For Cat. 2, Cat. 3 and Cat. 4 it is therefore necessary to implement defence strategies in order to reduce the probability of having CCF. Reduction of the coupling factor between two independent channels, choice of robust components, increase of the inherent reliability of the system and keeping the operating environment within the design constraints are some of the defence strategies.

ISO 13849-1 presents a list of 10 measures in Table F.1.

The measures are grouped into the following categories:

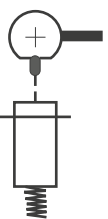

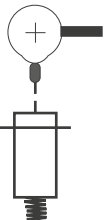
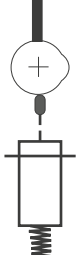
Physical design	Separation / segregation
	Diversity / redundancy
	Complexity / design / application / maturity / experience
Analysis	Data evaluation / analysis and feedback
Human problems	Expertise / training / safety culture of designers
Environment problems	EMC / Environmental control / pollution of fluidic systems

A score is assigned to each of the measure listed in the table. The total sum is 100. A score of 65 or better must be achieved. With a score of 65 it is conceivable that the residual fraction of common cause failures is less than or equal to 2%. If, on the other hand, the total score is less than 65, further measures must be taken.

The highest credits are assigned to measures against environmental influences (25 points) and to the use of different technologies / physical principles for the two channels in a two channel system (20 points).

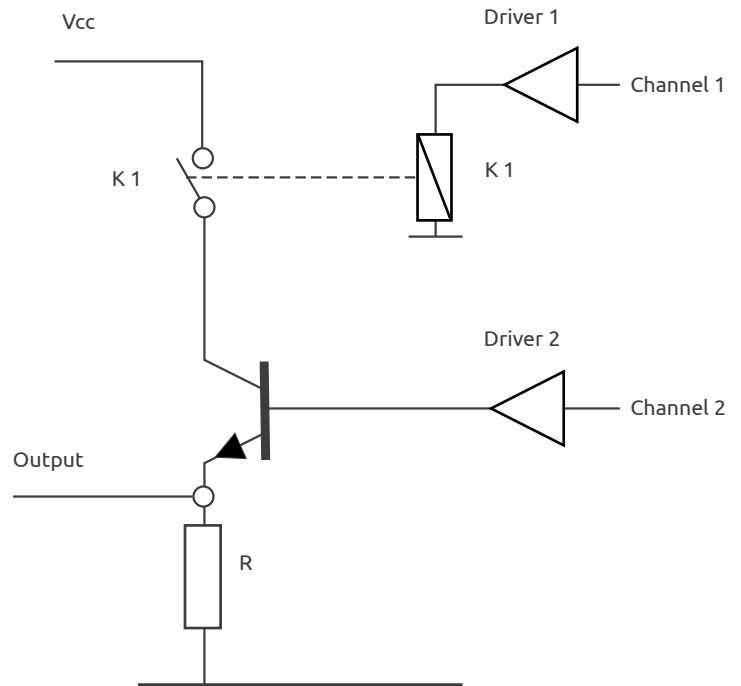
### Diversity example:

Two position switches used in combination, one directly mechanically operated and one indirectly mechanically operated as shown in the table below:

Mechanic Drive	Guard close	Guard open	Working mode	Behaviour example in case of failure
Direct			<p>The plunger (actuator) is held down by a cam until the guard is not closed.</p> <p>When the guard is closed, the output changes status spring breaks. as a result of the action of the return spring.</p>	The output will remain in the safe state when the guard is open even if the spring breaks.
Indirect			<p>The plunger (actuator) is held down by a cam until the guard is closed.</p> <p>When the guard is not closed, the output changes status as a result of the action of the return spring.</p>	If the spring breaks, the output may be in an unsafe state even if the guard is open.

Output made by a combination of a mechanical switch in series with an electronic switch.

Each measure on Table F.1 must be evaluated. The related score is assigned only if the measure has been fully applied; in the case of partial adoption, the associated scoring is zero.



### Simplified method for estimating the quantifiable part of the PL

After having chosen the category, verified that CCF scoring has been respected (for redundant architectures), found  $MTTF_D$ , and DC values, the PL and the  $PFH_D$  can be derived directly from table K.1 of the Standard.

The values of table K.1 have been computed by applying Markov analysis to the designated architectures of the 5 categories. Therefore, if the simplified method of the Standard is used, it is not possible to make exceptions regarding the Categories. The values of table K.1 have been calculated assuming that:

- Mission time = 20 years
- Constant failure rate throughout the mission time
- For Category 2: The test frequency is at least 100 times higher than the frequency of demand of the safety function and the  $MTTF_D$  of the test channel is greater than half the  $MTTF_D$  of the functional channel

Table K.1 is read as follows:

The calculated  $MTTF_D$  value is identified in a row of the left column and, after identifying the column corresponding to the implemented Category and the calculated DC, the PL and the  $PFH_D$  value are found.

MTTF <sub>D</sub> di ogni canale anni	Probabilità media di un guasto pericoloso per ora (1/h) e corrispondente livello di prestazione (PL)									
	Cat. B DC <sub>avg</sub> = nessuna	PL	Cat. 1 DC <sub>avg</sub> = nessuna	PL	Cat. 2 DC <sub>avg</sub> = bassa	PL	Cat. 2 DC <sub>avg</sub> = media	PL	Cat. 3 DC <sub>avg</sub> = bassa	PL
15	$7,61 \times 10^{-6}$	b			$4,53 \times 10^{-6}$	b	$3,01 \times 10^{-6}$	b	$1,82 \times 10^{-6}$	c
16	$7,13 \times 10^{-6}$	b			$4,21 \times 10^{-6}$	b	$2,77 \times 10^{-6}$	c	$1,67 \times 10^{-6}$	c
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d	$4,53 \times 10^{-7}$	d
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d	$3,87 \times 10^{-7}$	d
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$	c	$6,49 \times 10^{-7}$	d	$3,35 \times 10^{-7}$	d
51			$2,24 \times 10^{-6}$	c	$1,13 \times 10^{-6}$	c	$5,80 \times 10^{-7}$	d		
56			$2,04 \times 10^{-6}$	c	$1,02 \times 10^{-6}$	c				
62			$1,84 \times 10^{-6}$	c						
68										

If it is needed only the PL value, then the graph of figure 5 of the standard can be used.

The combination of category and DC identifies one of the seven columns; the calculated  $MTTF_D$  range determines which part of the column to consider. The corresponding PL value can then be read directly on the left side of the graph.

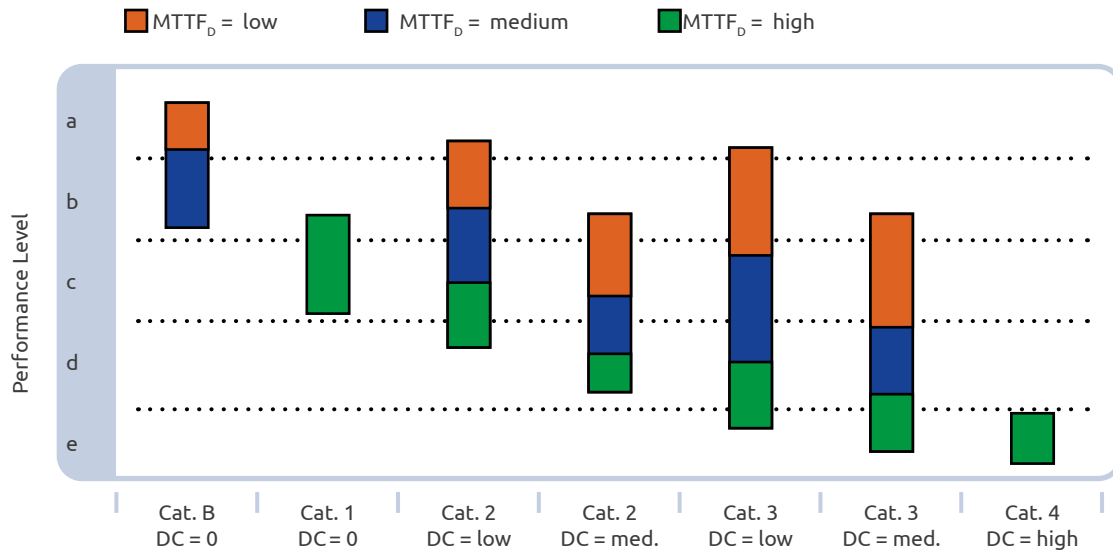


Fig. 12. ISO 13849-1 - Figure 5

It may happen that the part of the column chosen includes two or three possible PL values (e.g in the case of Cat. 3, DC = medium and  $MTTF_D$  = low, the following three values are possible: PL b, PL c, PL d) in these cases, table K.1 is used to get the correct PL value. As can be seen from Figure 5 for each Performance Level specified are available different choices. As an example from Table 5 it can be seen that for a system having PL of "c" the following five alternatives are possible:

- Category 3 with  $MTTF_D$  = Low and DC medium
- Category 3 with  $MTTF_D$  = Medium and DC low
- Category 2 with  $MTTF_D$  = Medium and DC medium
- Category 2 with  $MTTF_D$  = High and DC low
- Category 1 with  $MTTF_D$  = High

## Estimation of the PL based only on the Category information

This method is applicable only to the output subsystem of an SRP/CS. If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application-specific reliability data are available, the machine manufacturer may evaluate the quantifiable aspects of the PL without any  $MTTF_D$  calculation.

For such cases, the safety-related performance level (PL) is assured by the Category and by the measures against CCF. The next table shows the relationship between achievable PL and Categories.

	PFH <sub>d</sub> (1/h)	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	$2 \cdot 10^{-5}$	*	0	0	0	0
PL b	$5 \cdot 10^{-6}$	*	0	0	0	0
PL c	$1,7 \cdot 10^{-6}$	-	*2	*1	0	0
PL d	$2,9 \cdot 10^{-7}$	-	-	-	*1	0
PL e	$4,7 \cdot 10^{-8}$	-	-	-	-	*1

\* Applied category is recommended

0 Applied category is optional  
- category is not allowed

\*1 Proven in use or well-tried (confirmed by the component manufacturer to be suitable for particular application) components and well-tried safety principles must be used

\*2 Well-tried components and well-tried safety principles must be used. For safety-related components that are not monitored in the process, the T10<sub>d</sub> value can be determined based on proven in use data by the machine manufacturer.



PL a and PL b can be reached by using Category B; PL c can be reached by using Category 1 or Category 2; PL d can be reached by using Category 3; PL e can be reached by using Category 4.

Furthermore:

- if Category 1 is used to get a PL c, it is essential:
  - to determine, for the components involved, the  $T_{100}$  value. This value can be determined on the basis of “proven in use” data provided by the machine manufacturer
- if Category 2 is used:
  - well tried safety principles and well tried components declared suitable by the component manufacturer for the particular application must be used
  - $MTTF_D$  of the test channel must be at least 10 years
  - DC must be low or medium
  - Measures to control CCF must be in place
- if Category 3 is used:
  - well tried safety principles and well tried components must be used
  - DC must be low or medium
  - measures to control CCF must be in place
- if Category 4 is used:
  - well tried safety principles and well tried components must be used
  - DC must be high
  - measures to control CCF must be in place

Since formula E.1 of the standard cannot be used for the computation of the DC due to the unavailability of the  $MTTF_D$  values, the DC must be derived simply as the arithmetic average of the individual DC values of the components of the output subsystem.

Proof that the component is “proven-in-use” is based on the failure analysis of the component over a long period of time used in the same specific configuration and for that particular application. There must be documented evidence that the probability of dangerous systematic failure of that component in that specific application is low enough for the required PL value.

The concept of a “proven in use” component is a concept of the IEC 61508 standard.

#### Combination of several SRC/PS to achieve the overall PL

Where the safety-related function is made by a series connection of several subsystem, e.g safety light curtains, control logics, power output, and if the  $PFH_D$  values of the subsystem are known, then the  $PFH_D$  of the combined SRP/CS is the sum of all  $PFH_D$  values of the N individual subsystem.

The standard proposes two methods; a detailed one if for the single subsystem, in addition to the PL, also the  $PFH_D$  is known and a simplified one if only the PL is available.

#### Detailed method

If the  $PFH_D$  of the single subsystem is known, the total  $PFH_D$  is equal to the sum of the  $PFH_D$  values of each subsystem.



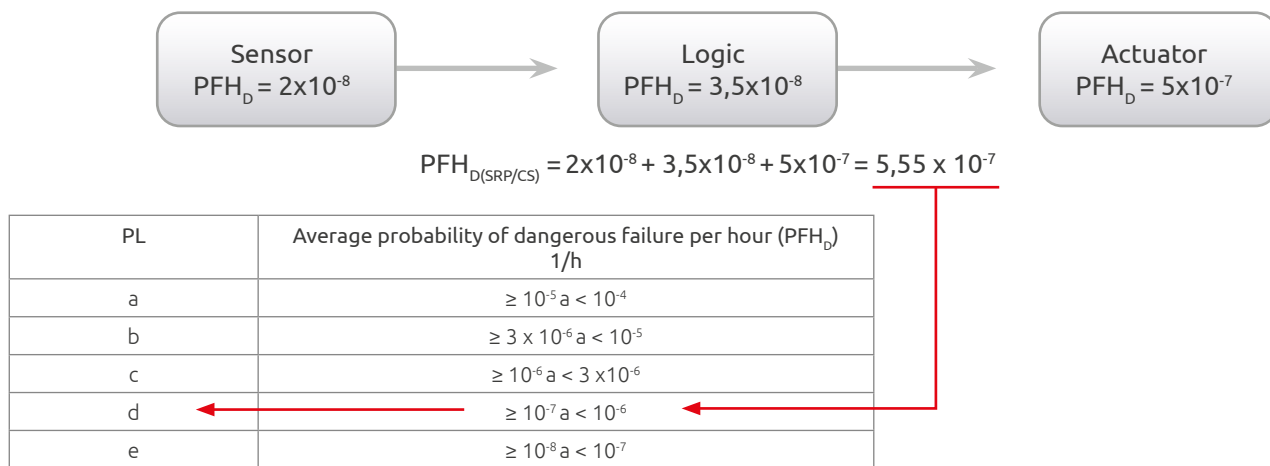
$$PFH_D = PFH_{D1} + PFH_{D2} + PFH_{D3}$$

The PL of the SRP/CS is derived by entering the total PFHD value in the following table.

PL	Average probability of dangerous failure (PFH <sub>D</sub> )
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

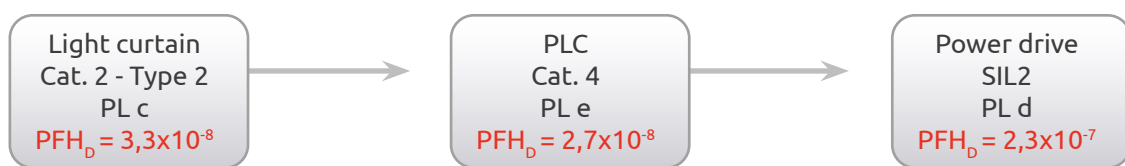
Fig. 13. Table 3 of ISO 13849-1 standard: Performance levels (PL)

Numerical Example:



The PL corresponding to the PFH<sub>D</sub> thus calculated is then limited by systematic constraints. The total PL cannot be greater than the lowest PL of all the subsystems that realize the safety function.

Limitation example:



The safety function consists of a Type 2 Photoelectric light curtain, PL c, a PL e control unit and a PL d drive

Summing the PFH<sub>D</sub> values it results:

$$PFH_D = 3.3 \times 10^{-8} + 2.7 \times 10^{-8} + 2.3 \times 10^{-7} = 5.33 \times 10^{-7}$$

Entering  $5.33 \times 10^{-7}$  into the table, it follows that the resulting PL should be PL d

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

However, remembering the constraints due to systematic failures to which Type 2, photoelectric light curtains are subjected::

ESPE TYPE	PL	SIL
2	a, b, c	1
3	a, b, c, d	1, 2
4	a, b, c, d, e	1, 2, 3

Fig. 14. Maximum PL for a safety function using safety light curtains

It comes that the maximum PL that can be reached by the safety function is limited to PL c

### Simplified method

If it is known only the PL of the individual subsystems, an estimate PL of the combination can be derived by using the following table:

PL (low)	n (low)		PL
a	>3		-
	≤ 3	-->	a
b	>2	-->	a
	≤ 2	-->	b
c	>2	-->	b
	≤ 2	-->	c
d	>3	-->	c
	≤ 3	-->	d
e	>3	-->	d
	≤ 3	-->	e

Fig. 15. Table for total PL computation

If the PFH<sub>d</sub> values of all individual SRP/CSs are not known: Locate the part with PL = PL low. Find the number of parts having PL = PL low

1. Identify the part with the lowest PL "PL (low)" first column
2. Identify the number of parts with the lowest PL "n (low)" second column
3. The total PL is found in the corresponding row of the third column



The PL found through this approximation refers to PFH<sub>d</sub> values that are in the middle of the range of the corresponding PL

In the proposed example of Fig. 15:

PL (low)	n (low)		PL	
a	>3		-	
	≤ 3	-->	a	
b	>2	-->	a	
	≤ 2	-->	b	
c	>2	-->	b	
	≤ 2	-->	c	←
d	>3	-->	c	
	≤ 3	-->	d	
e	>3	-->	d	
	≤ 3	-->	e	

PL low = c

N Low = 1

Total PL = c

$PFH_D = 2 \times 10^{-6}$

## Subsystem interconnections

It is also necessary to give particular attention to the interfaces between subsystems:

The safety aspects related to the interfaces and connections between SRP/CS (e.g conductors or data communication bus) must be included in the PL of one of the associated subsystems, otherwise connection errors must be excluded or negligible.

The cascade of safety subsystems must have compatible interfaces. Each subsystem output must be suitable for initiating the safe state of the downstream subsystem.

## IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control system.

IEC 62061 is derived from IEC 61508 – Functional safety of safety-related electric/electronic/programmable electronic control systems.



IEC 61508 is the international reference standard on functional safety of electric, electronic and programmable electronic systems. This Standard consists of seven sections. The first three sections specify the safety requirements for hardware, software and safety management, the rest are of an informative nature and offer support for the correct application of the former parts.

IEC 62061 retains the features of IEC 61508, but simplifies safety requirements (both hardware and software) adapting them to the specific needs of industrial machinery.

Safety requirements are considered only for “high demand mode”, i.e. request of the safety function greater than once a year.

### Management of functional Safety

All design aspects needed to attain the required level of functional safety, starting from assignment of the safety requirements specifications to the design management, to validation up to the instructions for safe use, shall be decided and defined before initiating the design.

Each design shall have its own Functional Safety Plan properly written, documented and duly updated as necessary. The Functional Safety Plan shall identify individuals, departments and resources needed for design and implementation of the safety system.

### Safety Integrity Level (SIL)

A Safety Control System (SCS), in order to be suitable to perform the assigned safety function in the specified operating conditions and all the way through the mission times shall have some degree or level of safety integrity (SIL). Three levels are defined, where safety integrity level 3 has the highest level of safety integrity and safety integrity level 1 has the lowest. The SIL must be defined for each safety-related function resulting from risk analysis.

For each safety function a methodology is given for:

- The allocation of the Safety Integrity Level (SIL)
- The assignment of the safety requirements specification (SRS) and functional requirements specifications
- The design of the SCS implementing the safety function
- The validation of the SCS

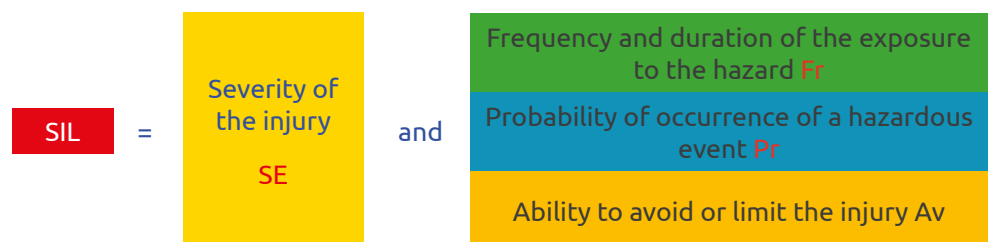
### SIL allocation

A method for SIL allocation is given in Annex A (although the Standard accepts in addition the techniques described in IEC 61508-5). According to Annex A, The SIL is determined by the following risk parameters:

- Severity of the injury -Se
- Probability of occurrence of such injury

The probability of occurrence of the injury being a function of:

- frequency and duration of the exposure to the hazard, Fr
- probability of occurrence of a hazardous event Pr
- ability to avoid or limit the injury, Av



It comes that for each identified hazard the the following parameters must be assessed:

- Degree of severity (Se) of the harm
- Frequency and time (Fr) of exposure to the hazard
- Probability of occurrence of the dangerous event (Pr) associated for each machine operating mode
- Possibility to avoid the hazard (Av). The more difficult it is to avoid the hazard the higher is the number representing AV

## Severity (Se)

The severity is decided on the basis of the consequences of an injury.

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

Fig. 16. Table A1 - Severity (Se) classification

## Frequency and duration of the exposure (Fr)

- The average interval between exposures and therefore the average frequency of exposure is estimated by considering the following aspects:
  - All modes of use (normal operation, maintenance)
  - The nature of access (manual feed of materials, settings)
  - Time spent in the hazard zone
  - Frequency of access

Frequency and duration of exposure (Fr) classification		
Frequency of exposure	Duration of exposure ≥ 10 min	Duration of exposure < 10 min
≥ 1 per h	5	5
< 1 per h to ≥ 1 per day	5	4
< 1 per day to ≥ 1 per 2 weeks	4	3
< 1 per 2 weeks to ≥ 1 per year	3	2
< 1 per year	2	1

Fig. 17. Table A2 - Frequency and duration of the exposure (Fr)

## Probability of occurrence of a hazardous event (Pr)

This parameter can be estimated by taking into account the human behaviour (stress, skills, machine complexity) with regard to interaction with the parts of the machine relevant to the hazard.

Very high probability of occurrence of a hazardous event should be selected to consider the worst case.

For any lower values to be used, high level of user competences and well-defined knowledge of the application are required.

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Fig. 18. Table A3 - Probability (Pr) classification



### Probability of avoiding or limiting harm (Av)

Takes into account:

- Sudden, fast or slow speed of appearance of the hazardous event
- Spatial possibility to withdraw from the hazard
- The nature of the component
- Possibility of recognition of a hazard

Probability of avoiding or limiting harm (Av)	
Impossible	5
Rarely	3
Probable	1

Fig. 19. Table A4 - Probability of avoiding or limiting harm (Av) classification

**Warning:** the choice probable should be selected only if the hazard is clearly recognizable and if there is sufficient time to take counteractions or to leave the hazardous area.

The sum of the scores for the attributes of frequency, probability and avoidance provides the probability class (Cl) of the hazard:

$$Cl = Fr + Pr + Av$$

The following SIL allocation matrix, will help finding the SIL to be assigned to each safety-related function by cross-referencing on the matrix the actual Cl to the identified degree of severity (Se) identified.

Table A.6 – Matrix for SIL assignment

Consequences	Severity Se	Class Cl				
		4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent: losing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible: medical attention	2			OM	SIL 1	SIL 2
Reversible: first aid	1				OM	SIL 1

Fig. 20. Table 3 of IEC 62061

## Assignment of the safety requirements specification (SRS) and functional requirements specifications

Safety requirements specification (SRS) must include at least the following machine characteristics:

- Cycle time
  - response time performance
  - environmental conditions
  - switching frequency and duty cycle for electromechanical devices, if used.
- Man-machine interactions
- Machine behavior under normal working conditions
- Required reaction of the safety function

Functional requirements specification shall describe details of each safety function, in particular:

- Description of the safety function
- Conditions of reset and conditions of re-starting after actuation of the safety function
- Response time
- Interfaces of the safety function with the other parts of the machine control system
- Operating mode of the machine in which the safety function shall be active or disabled

## Design process of an SCS

Each safety function shall be described in terms of:

- Operational requirements (mode of operation, cycle time, environmental conditions, response time, type of interface with other components or subsystems, EMC level, etc.)
- Safety requirements (SIL).

Each safety-related function shall be broken down into subfunctions, e.g. subfunction for input signals, subfunction for logic data processing, subfunction for output signals.

A subsystem is then associated to each subfunction.

Subsystems may be made of components of any technology, electrical, electronic, pneumatic, hydraulic, interconnected each another. Single components are called subsystem elements.

The technical implementation of a SCS will therefore assume a typical structure as shown in the figure (example of an access control implemented via a photoelectric barrier).

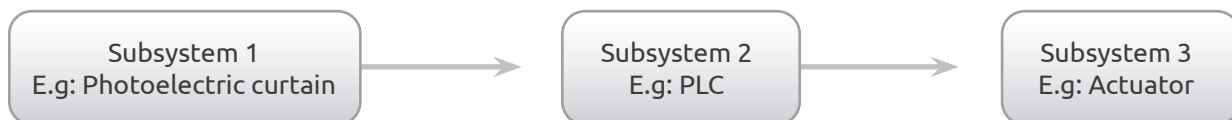


Fig. 21. Typical structure of a SCS

An SCS can implement more safety functions. Each safety function can be made of several subsystems. A subsystem can share more subfunctions.

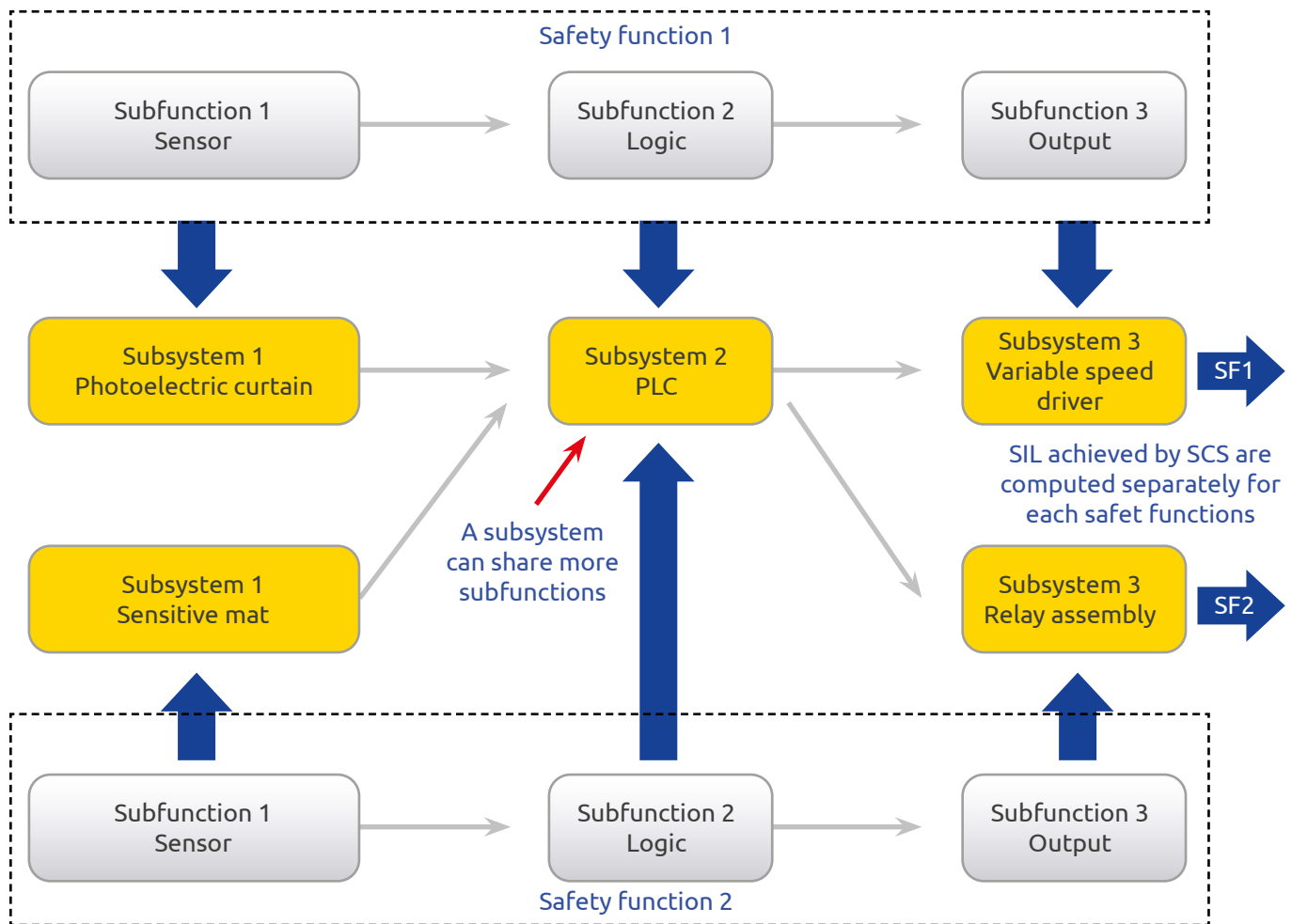


Fig. 22. Fig. 3 General structure of an SCS

If a subsystem shares safety functions of different safety integrity levels, its hardware and software shall be treated as requiring the highest safety integrity level.

If a subsystem implements both safety functions and other functions, then all its hardware and software shall be treated as safety-related unless the safety functions and other functions are sufficiently independent.

If digital data communication is used as a part of an SCS, it shall satisfy the relevant requirements for functional safety fieldbuses (IEC 61784-3) in accordance with the SIL target of the safety function.

### Use of a pre-designed subsystem

It is possible to combine subsystems designed with this standard with subsystems designed with other safety standards. Table 4 of IEC 62061 provides a correspondence with SIL or PL values of subsystems designed with other standards.

IEC 62061	IEC 62061	IEC 61508	ISO 13849
PFH	SIL	at least...	at least...
$< 10^{-5}$	SIL 1	SIL 1	PL b,c
$< 10^{-6}$	SIL 2	SIL 2	PL d
$< 10^{-7}$	SIL 3	SIL 3	PL e

Fig. 23. Table S4 - Required SIL and PFH of pre-designed subsystems

Column IEC 61508 includes SIL-based standards that fulfil the same architectural constraints, such as IEC 61800-5-2 and IEC 60947-5-3.

It is not possible to identify a perfect one-to-one correspondence between PL and SIL; however, it is possible to compare the probabilistic part of PL and SIL because they use the same concept to define the degree of resistance to failures, i.e. the PFH, even if it is possible to compare the ranges but not the exact values because the calculation methods used are not the same in both standards.

Moreover, some restrictions are imposed:

- The correspondence with ISO 13849-1 does not apply to subsystems using complex components and PLb does not correspond to SIL1 in case of a Category B structure.
- No correspondence can be assumed between IEC 62061 and IEC 61511 (all parts) or ISO 26262

## PFH as a target parameter to measure the hardware safety integrity of the SCS

The parameter used to define the safety performance of the SIL (Safety Integrity Level) is the probability of dangerous failure/hour (PFHd). The higher the SIL, the less likely the SCS does not perform the required safety function.

The SIL must be defined for each safety-related function resulting from risk analysis.

Table 3 of the Standard gives a correspondence between SIL and PFH

SIL limits and PFH values	
SIL	PFH values
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

Fig. 24. Table 3 -SIL limits and PFH values

## Determining f the PFH of the SCS

The PFH of an SCS is the sum of the individual values of all subsystems' PFH participating in the realization of the SCS and shall include the probability of dangerous transmission errors (PTE) for any digital data communication involved.

$$PFH_{scs} = PFH_{subsystem\ 1} + ... + PFH_{subsystem\ n} + PTE$$

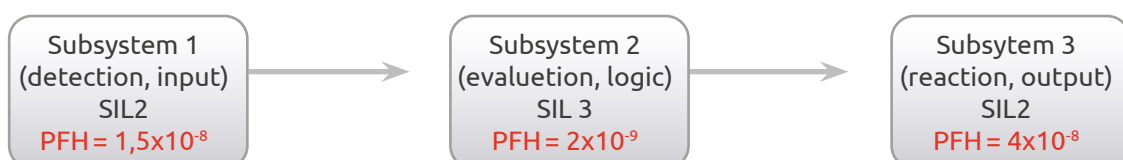
Hardware wiring connecting subsystems are part of systematic integrity and possible dangerous failures on the wiring shall be detected by online diagnostics.

## Determining the SIL of the SCS

After having derived the PFH of the SCS, the resulting SIL is found from Table 3. It comes that the maximum SIL is limited by the sum of the PFH values of all subsystems.

The SIL of the SCS can only be equal to or less than the lowest SIL of any of the subsystems participating in the realization of the SCS. However, the PFH values of the single subsystems are not restricted (for example, a SIL 2 subsystem can have a PFH lower than  $10^{-7}$ ).

Example:



$$PFH_{CS} = 1,5 \times 10^{-8} + 2 \times 10^{-9} + 4 \times 10^{-8} = 5,7 \times 10^{-8}$$

SIL limits and PFH values

SIL	limits and PFH values
1	< $10^{-5}$
2	< $10^{-6}$
3	< $10^{-7}$

It comes that the SIL of this SCS, despite the overall PFH value being suitable for a SIL 3, is limited to SIL 2, being SIL 2 the lower SIL of the three subsystems.

In addition, the safety integrity of the SCS is limited also by the systematic capabilities (for example, environmental influences, EMC, and detection principle).

### Requirements for systematic safety integrity

The value of PFH is only one of the parameters that contribute to SIL assignment.

In order to claim a SIL, it is also necessary to prove that all the requirements relating to:

- The avoidance of systematic hardware failures
- The control of systematic failures
- The use of robust and reliable components (complying with product standards, where available)
- The environmental conditions in which the safety system will have to operate

have been taken into consideration and complied with and, if it was necessary to write software, to have adopted all the organizational and design aspects relevant for the target SIL.

### Safety measures with regards to electromagnetic phenomena

The SCS shall not be affected by electromagnetic Interference to the point of disturbing or making the safety function ineffective in a way that could lead to an unacceptable risk.

Adequate performance with respect to electromagnetic disturbances is therefore mandatory.

When available, only electrical and/or electronic devices or apparatus which meet the requirements of the relevant product standard regarding immunity against electromagnetic phenomena should be used. Examples of such product standards are IEC 61326-3-1, IEC 61800-5-2, IEC 61496-1, IEC 60947-5-3 (CD stage).

If no dedicated product standard exist addressing electromagnetic influences on functional safety aspects, the generic standard IEC 61000-6-7:2014 should be applied. A comprehensive safety analysis regarding the effects of electromagnetic disturbances on the SCS shall be carried out to derive the immunity limits that are required for the SIL needed.

For pre-designed subsystems according to this standard, the foreseeable electromagnetic threats in the real environment of the equipment should be considered in the SRS. The immunity requirements should be based on the generic standard IEC 61000-6-7:2014 if for the subsystem no relevant dedicated product-family or product standard addressing electromagnetic influences on functional safety exists. For pre-designed subsystems designed according to PL a or PL b of ISO 13849-1 follow the EMI standard applicable is IEC 61000-6-2:2014.

For the integration of SCS into the electrical equipment of the machine EMI measures according to Annex H of IEC 60204-1 should be applied. In particular:

- Avoid large conductive loops, do not install different electrical wiring systems in common routes, (e.g., power supply, communication, control and signal cables)
- Use RF-filter and overvoltage and transient protection for safety related input/output signals
- If applicable, shielded and earthed cables for motors or sine filter between motor and inverter or equivalent measures

## Safety-related application software

When developing application SW, it is preferable to separate SW performing non-safety basic machine functions from safety related functions. Where the software performs both non-safety and safety functions, then all the software shall be treated as safety related.

Configuration management processes and modifications management processes shall be defined and documented.

Software configuration management shall allow a precise and unique software version identification.

Modifications or changes to SW shall be subject to an impact analysis that identifies all software parts affected and the necessary re-design, re-review and re-test activities to confirm that the relevant software safety requirements are still satisfied.

The Standard describes two different levels of application software: SW level 1 and SW level 2. SW level 3 is not addressed in this Standard.

### SW Level 1

This is an application software making use of a limited variability language (LVL) due to the use of pre-designed hardware and software modules. Example of systems using LVL: Safety PLC with LVL or Safety programmable relay.

The following languages are LVL: ladder diagram, function block diagram and sequential function chart.

Clause 8.3 of the standard gives detailed requirements regarding the SW safety life cycle, SW design, Module design, coding, testing, modification management and documentation.

Software safety requirements specification shall be developed for each subsystem based on the SCS specification and architecture, documented, and managed throughout the lifecycle of the SCS.

A SW safety lifecycle model like the simplified V-model can be used.

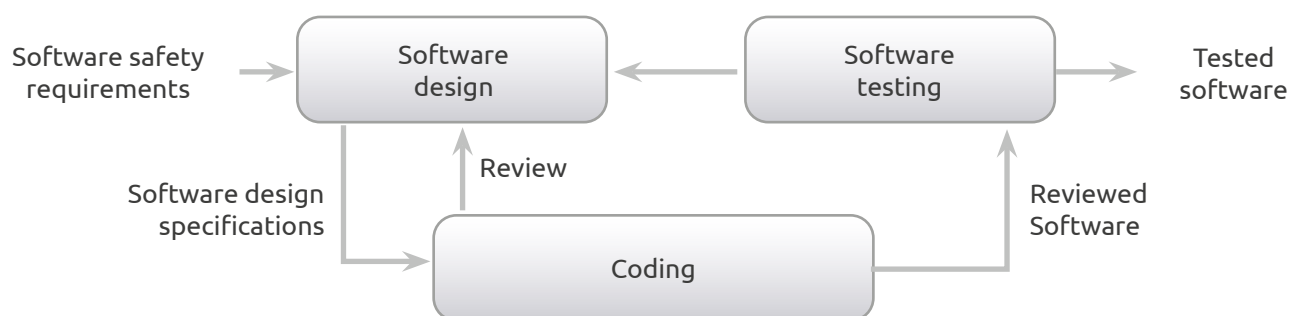


Fig. 25. V-model for SW Level 1

The left side represents requirements i.e., things to achieve. The right-side details testing of the software.

The output of each phase shall be checked against the requirements of the input of the same phase.

It is recommended to use pre-designed approved software modules wherever possible but, if the library modules provided by the manufacturer is not satisfactory, the design of customized software modules can also be developed according to this simplified V-model.

Each module which was not previously assessed shall be tested against the test cases. Software testing shall include failure simulation and the associated failure reaction depending on the required safety integrity.

## SW Level 2

Software Level 2 is introduced to support Full Variability Language (FVL). Example of systems using FVL: Safety PLC with FVL complying with this Standard.

The following languages are FVL: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, and SQL.

The maximum achievable SIL for SW level 2 is SIL 2.

SW levels 2 is of increased complexity in comparison with SW level 1 due to the use of fully variable programming languages. Therefore, a more detailed V-model shall be used.

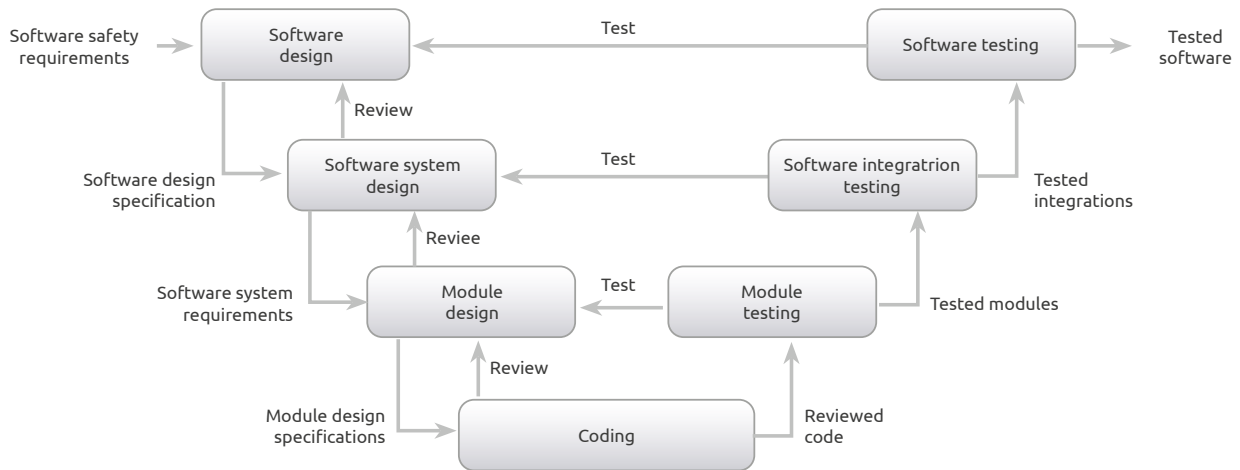


Fig. 26. V-model of software safety lifecycle for SW level 2

The left side represents requirements, i.e., things to achieve. The right-side details testing of the software.

Clause 8.4 of the standard gives detailed requirements regarding the SW safety life cycle, SW design, Module design, coding, testing, modification management and documentation.

The design shall include self-monitoring of control flow and data flow appropriate to the SIL of the SCS.

The inputs of the software design specification must be related in a straightforward manner to the desired outputs and vice versa.

The SW system design shall follow a modular approach with a limited module size, a fully defined interface and one entry/one exit point in subroutines and functions. Each module shall have a single, clearly understood function. The maximum module size shall be limited to one complete safety function.

Where previously developed software library modules are to be used as part of the design, their suitability in satisfying the safety requirement specifications of the SW shall be demonstrated.

Integration test cases of the SW shall be performed and documented.

Software testing shall also include failure simulation and the related failure reaction. Functional testing as a basic measure shall be applied. Code should be tested by simulation where feasible.

Testing of software includes two types of activities: both Static analysis and dynamic analysis shall be performed.

## SW level 3

For application SW compliant with SIL 3, IEC 61508-3 must be applied.

A high level of competence is required to design according to SW level 3. Factors that make the use of IEC 61508-3 for SW level 3 more appropriate than the use of SW 2 are:

- High degree of complexity of the safety function
- Large number of safety functions
- Large project size.

## Design and development of subsystems

### Step one - Choice of the architecture (structure)

The standard proposes four predefined architectures and for each of them provides a simplified formula for computation of the PFH.

The four architectures are differentiated by the hardware fault tolerance (HFT), and for the presence (or absence) of diagnostics.

The four architectures correspond to the most popular configurations used in the field of safety of machinery.

A hardware fault tolerance of N means that the subsystem tolerates up to N failures before losing his safety performance. N + 1 faults could cause a loss of the safety function.

When defining the fault tolerance of an architecture no credit is given to additional measures that can control the effects of faults, such as diagnostics.

For architecture B and D the two channels must be sufficiently independent; i.e. designed in such a way that a single channel is able to carry out the function independently from the other. The same apply to the architecture C for the functional channel with respect to the diagnostic channel.

#### Subsystem architecture A:

HFT = 0 - Single channel without diagnostic function



Fig. 27. Basic subsystem architecture A

Any dangerous failure of a subsystem element causes the loss of the safety function.

$$(1) \quad PFH = \lambda_{De1} + \dots + \lambda_{Den}$$

$\lambda_{Dei}$  is the dangerous failure rate of an element of the single channel.

Comparison with EN ISO 13849-1:



Cat. B (PLmax = b) e Cat. 1 (PLmax = c)



## Subsystem architecture B

HFT = 1 - Dual channel without diagnostic function

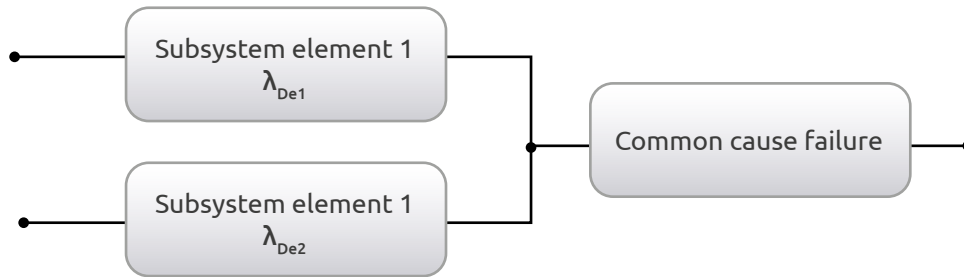


Fig. 28. Basic subsystem architecture B

A single failure of any subsystem element does not cause a loss of the safety function

$$(2) \quad PFH = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$

- $\lambda_{De1}$  is the dangerous failure rate of an element of the first functional channel.
- $\lambda_{De2}$  is the dangerous failure rate of an element of the second functional channel.
- $T_1$  is the useful lifetime or the proof test interval, whichever is the smaller. In any case not exceeding 20y
- $\beta$  is the susceptibility to common cause failures.

No correspondence with the categories of EN ISO 13849-1

## Subsystem architecture C:

HFT = 0 Single channel with a diagnostic function

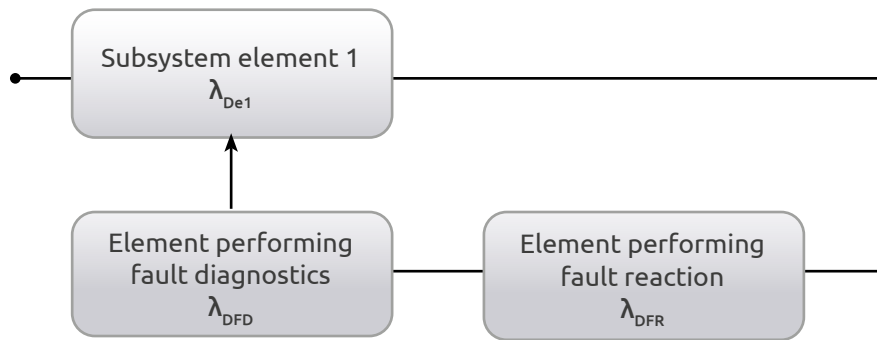


Fig. 29. Basic subsystem architecture C

Any undetected dangerous fault of a subsystem element of the functional channel leads to the loss of the safety function. When a dangerous fault of a subsystem element of the functional channel is detected by the diagnostic function, the diagnostic function itself initiates a fault reaction.

$$(3) \quad PFH = \sum_{i=1}^n \lambda_{Dei} - DC \times \left( \sum_{i=1}^n \lambda_{Dei} - \lambda_{cc} \right) \times \left\{ 1 - \frac{1}{2} \left[ \sum_{i=1}^n \lambda_{DFHj} - \lambda_{cc} \right] \times T_1 \right\}$$

With

$$(4) \quad \lambda_{cc} = \beta \times \min \left( \sum_{i=1}^n \lambda_{Dei}, \sum_{i=1}^n \lambda_{DFHj} \right)$$

and

$$(5) \quad DC = \frac{\sum_{i=1}^n (DC_i \times \lambda_{Dei})}{\sum_{i=1}^n \lambda_{Dei}}$$

where:

T1 is the useful lifetime or the proof test interval, whichever is the smaller. In any case not exceeding 20y

$\lambda_{Dei}$  is the dangerous failure rate of element ei within the single functional channel.

n is the number of elements of the single functional channel.

$\lambda_{DFHj} = \lambda_{DFDj} + \lambda_{DFRj}$  is the failure rate of the elements number j within the single channel that realizes the fault handling function.

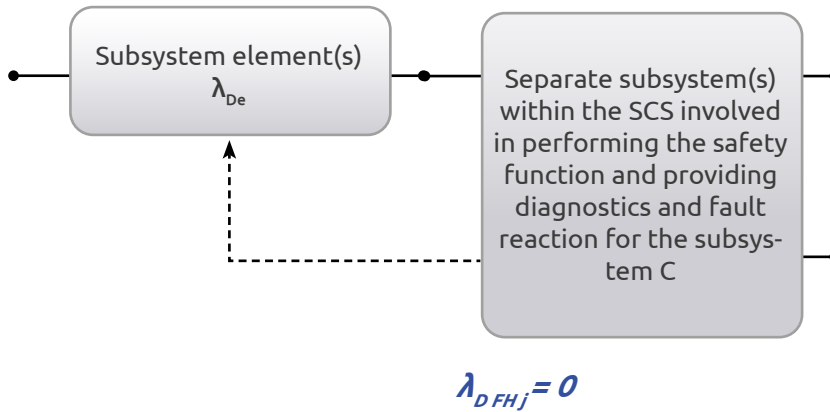
m is the number of elements of the single channel that realizes the fault handling function(s)

$DC_i$  is the diagnostic coverage for element ei of the single functional channel.

$\beta$  is the susceptibility to common cause failures of the functional channel and of the diagnostic channel.

If the diagnostic function is performed by a separate subsystem within the SCS

Then;



$\beta < 2\%$ - due to the separation of the two subsystems and the equations simplify to:

$$(6) \quad PFH = (1 - DC_1) \times \lambda_{De1} + \dots + (1 - DC_n) \times \lambda_{Den}$$

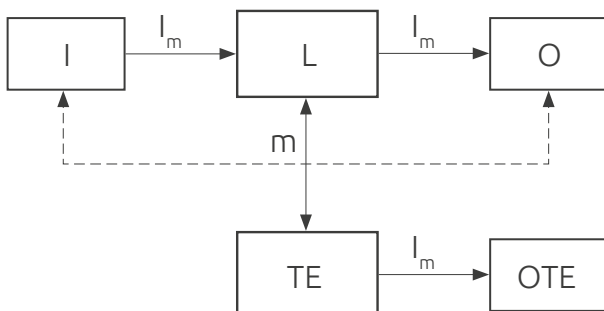
The test rate of the diagnostic functions must be at least a factor of 100 higher than the demand rate of the safety function and the time needed for the fault reaction must be short to bring the system to a safe state before a hazardous event occurs.

Alternatively, the test can be performed periodically. In this case the sum of the test interval, plus the time needed to detect a fault plus the time needed to bring the system to a safe state is shorter than the process safety time.

The test can also be performed immediately upon any demand of the safety function. In this case the time needed to detect a fault and to bring the system to a safe state must be shorter than the process safety time.

Comparison with EN ISO 13849-1

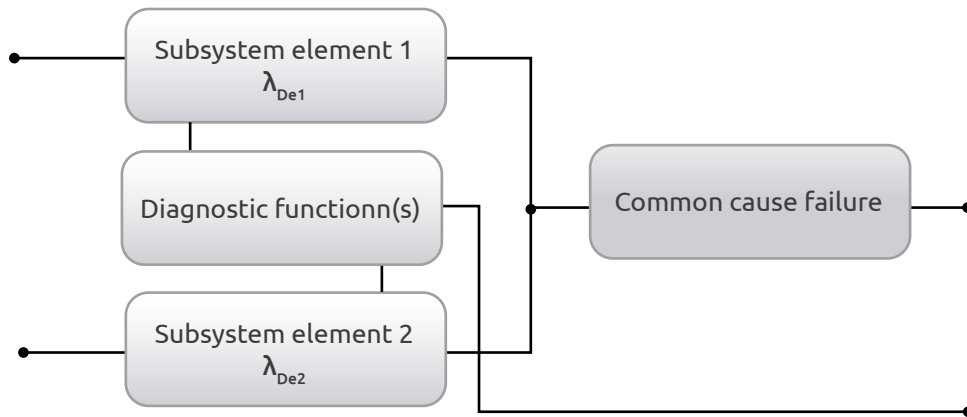
Subsystem architecture D



Cat. 2 (PLmax = d)

HFT = 1 Dual channel with a diagnostic function

Fig. 30. Subsystem architecture D



For subsystem elements of the same design:

$$(7) \text{ PFH} = (1-\beta)^2 \times [DC \times T_2 + (1-DC) \times T_1] \times \lambda_{De2} + \beta \times \lambda_{De}$$

For subsystem elements of different design

$$(8) \text{ PFH} = (1-\beta)^2 \times [\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2 / 2 + \lambda_{De1} \times \lambda_{De2} \times (2-DC_1-DC_2) \times T_2 / 2 + \beta \times (\lambda_{De1} \times \lambda_{De2}) / 2]$$

Where

$T_2$  is the diagnostic test interval.

$T_1$  is the useful lifetime or the proof test interval, whichever is the smaller. In any case not exceeding 20y

$\beta$  is the susceptibility to common cause failures.

$\lambda_{De1}$  is the dangerous failure rate of subsystem element 1.

$\lambda_{De2}$  is the dangerous failure rate of subsystem element 2.

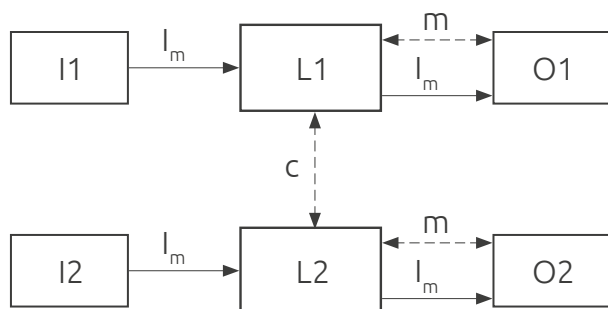
$DC_1$  is the diagnostic coverage for subsystem element 1.

$DC_2$  is the diagnostic coverage for subsystem element 2.

A single dangerous fault of any subsystem element does not cause a loss of the safety function. Where a fault of a subsystem element is detected by the diagnostic function, the diagnostic function itself initiates a fault reaction.

The diagnostic function is performed continuously, and the sum of the diagnostic test interval and the time needed to perform the specified fault reaction, in order to bring the system to a safe state, must be shorter than the process safety time.

Comparison with EN ISO 13849-1



Cat. 3 ( $PL_{max} = d$ )

Cat. 4 ( $PL = e$ )

## Step two - Determination of the parameters $\lambda$ , $\lambda_d$ , $\lambda_s$ , $\lambda_{dd}$ , $\lambda_{du}$

### General considerations

For purpose of determining the failure rates of subsystem elements, the following fault criteria shall be considered:

- If, because of a fault, further components fail, the first fault together with all following faults shall be considered as a single fault
- Two or more separate faults having a common cause shall be considered as a single fault
- The simultaneous occurrence of two or more faults having separate causes is considered highly unlikely and therefore need not be considered
- Certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements of the subsystem

A basis for fault consideration is given in ISO 13849-2 (Annexes A to D).

For the list of components/elements included in Annexes A to D, are provided:

- The faults to be considered
- The permitted fault exclusions, considering environmental and application aspects and conditions under which fault exclusion are permitted

### Electrical/electronic components

#### Determination of $\lambda$

In general, for this type of components the manufacturer does not provide reliability data because they strongly depend on how the component is used and on the characteristics of the environment.

Reliability data can be found in the set of standards SN 29500 or in the MIL-HDBK 217F or OREDA 2015 or even in the EXIDA reliability handbook.

Failure rates are expressed in FIT (failure in time)

1 FIT =  $1 \times 10^{-9}$  hours

FIT values are given at reference operating conditions (voltage, current, dissipation etc..) and at the ambient temperature of 40 °C. The value given is  $\lambda_{ref}$  in FIT.

Example: for a metal film resistor is  $\lambda_{ref} = 0,2$  FIT

If the actual operating conditions are different respect to the reference ones, it is necessary to make corrections using formulas that are provided in the same document for each family of components.

#### Determination of $\lambda_d$ and $\lambda_s$

After having determined  $\lambda$  for each subsystem element (e.g. derived by one of the data base mentioned), the different failure modes of the subsystem element should be considered. It is typically assumed that not all failures modes lead to a dangerous failure. To determine the failures to consider for each element and to decide whether they are safe failures or dangerous failures, an analysis technique, such as failure mode and effect analysis (FMEA) or fault tree analysis (FTA) should be carried out.

In order to undertake this technical analysis, the following information is necessary:

- The hardware schematics of the subsystem describing each component and interconnections between components
- For each component the failure modes and associated percentages of the total failure probability

To help the designer, several recognised industry sources are available where to find a list of failure modes together with the failure mode ratio.

Example of typical failure modes and failure ratio (%) of some electronic components

Component	Shorts	Opens	Drift
Bipolar transistors	80	20	—
Field effect transistors	80	10	10
Diodes general purpose	80	20	—
Zener	70	20	—
Optocoupler	10	50	40
Resistors, fixed (film)	—	60	40
Capacitors foil	15	80	5
ceramic	70	10	20
Al	30	30	40
Coils	20	80	—

Fig. 31. Failure modes and failures ratio

The process should be as follows:

Categorize each failure mode according to whether it leads to

- A safe failure (fault has no influence or the fault leads to a safe state without a diagnostic measure)
- A dangerous failure (leads without diagnostic to a dangerous malfunction)
- Components that are not a part of a safety function or of a diagnostic measure, and that do not have any influence on the safety function are not considered.

Doing this analysis, do not consider the effects of diagnostic techniques implemented! The effects of diagnostics are considered separately; see the clause: computation of DC.

From the estimate of  $\lambda$  of each component and the categorization of the failures (safe, dangerous) calculate the probability of safe failure ( $\lambda_s$ ) and the probability of dangerous failure ( $\lambda_d$ ).

Example, just to describe how to apply the method:

Let's take for ease of computation the case of two components, a ceramic capacitor and a metal film resistor that are part of the components of a functional channel.

For the capacitor we get from SN 29500 a failure rate of 2 FIT ( $\lambda = 2 \times 10^{-9}$ ). From the analysis of the circuit, it comes that a short circuit of the capacitor or a drift leads to a dangerous failure, while an open circuit leads to a safe failure.

For the resistor we get from SN 29500 a failure rate of 0,2 FIT ( $\lambda = 0,2 \times 10^{-9}$ ). From the analysis of the circuit, it comes that an open circuit of the metal film resistor or a drift leads to a dangerous failure, a short circuit leads to a safe failure, but this type of failure for a metal film resistor is excluded, due to the technology. (see ISO 13849-2).

For the capacitor:

$$\lambda_{Scap} = 2 \times 10^{-9} \times 0,1 = 2 \times 10^{-10}$$

$$\lambda_{Dcap} = 2 \times 10^{-9} \times (0,7 + 0,2) = 1,8 \times 10^{-9}$$

For the resistor:

$$\lambda_{Dres} = 0,2 \times 10^{-9} \times (0,6 + 0,4) = 0,2 \times 10^{-9}$$

Obviously, the same calculations must be carried out for all components of the channel.

The overall values of  $\lambda_s$  and  $\lambda_d$  for the channel are then derived by summing the values of  $\lambda_s$  and  $\lambda_d$  of each component.

Limited to the components of our example:

$$\lambda_{\text{Schannel}} = 2 \times 10^{-10}$$

$$\lambda_{\text{Dchannel}} = 1,8 \times 10^{-9} + 0,2 \times 10^{-9} = 2 \times 10^{-9}$$

Alternative method:

If no specific information is available concerning the failure modes, 50 % of the failures can be estimated as dangerous, in this case  $\lambda_s$  and  $\lambda_d$  are approximated to:

For the capacitor:

$$\lambda_{\text{Scap}} = 2 \times 10^{-9} \times 0,5 = 1 \times 10^{-9}$$

$$\lambda_{\text{Dcap}} = 2 \times 10^{-9} \times (0,5) = 1 \times 10^{-9}$$

For the resistor:

The technology used excludes the fault of short circuit; if no additional information is available, all the other faults must be considered dangerous:

$$\lambda_{\text{Dres}} = 0,2 \times 10^{-9}$$

## Determination of $\lambda_d$ for electromechanical components

For electromechanical, pneumatic and mechanical components subject to wear (eg. relay and solenoid valves) the failure rate increases with the number of cycles processed.

For this reason, their reliability is usually related to the number of cycles performed and not to the time for which they have been working.

The parameter given by the manufacturer is the  $B_{10}$  or the  $B_{10d}$  expressed in numbers of operations; this is the number of operations after which failures occur in 10% of the components tested (endurance test under specified load).

If manufacturer data are not available, for a list of hydraulic, pneumatic, and electromechanical components, it is also possible to use the  $B_{10d}$  or  $MTTF_d$  values given in Table C.1 of the standard. The use of these values is allowed only under the following conditions:

- Basic and well-tried safety principles according to ISO 13849-2 have been used for the design of the component (confirmed in the data sheet of the component)
- The manufacturer of the component specifies that the component can be used for safety related applications
- The subsystem designer confirm that the component is utilized fulfilling basic and well-tried safety principles according to ISO 13849-2.

Hydraulic components listed in Table C.1 are characterized with  $MTTF_d$ . For the conversion of  $MTTF_d$  into a  $\lambda_d$  value the following basic equation can be used:

$$(9) \quad \lambda_d = \frac{1}{MTTF_d \times 8760 \text{ h/a}}$$

Note:  $MTTF_d$  is given in years; one year is approximatively 8760 ours.

For the conversion of  $B_{10d}$  into a  $\lambda_d$  value the following equation can be used:

$$(10) \quad \lambda_d = (0.1 \times C) / B_{10d}$$

where

$C = n_{op} / 8760$  (mean number of operations per hour)

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{T_{cycle}} \quad (\text{mean number of annual operations})$$

$h_{op}$  = mean operation, in hours per day

$d_{op}$  = mean operation, in days per year

$t_{cycle}$  = time between the beginning of two successive cycles in seconds per cycle.

8760 = number of hours in a year

The operating time of the component must then be limited to T10d which is the average time within which 10% of the components undergoes a dangerous failure.

$$(11) \quad T_{10d} = 0,1 / \lambda_d$$

If only B<sub>10</sub> is available (the number of operations after which 10% of the components under test undertake a failure), B10d can be derived knowing the ratio of dangerous failures (RDF)

$$(12) \quad B_{10d} = B_{10} / RDF$$

If no other information is available, RDF is estimated as 0,5 (50 % dangerous failure).

Example:

For a low duty relay the manufacturer specifies a B<sub>10</sub> = 10 M cycles when used at small load (20% of the nominal load).

The relay is used on a machine operated as follows:

220 days/year; 16 h/day (two shifts); machine cycle: 1 min (60 cycles/h)

From the above formulas it comes:

Mean number of annual operations  $n_{op} = 211200$

Mean operation per hour  $C = 24,11 / h$

No information is given regarding B<sub>10d</sub>, therefore is assumed  $B_{10d} = 2 \times B_{10}$   
then:  $\lambda_d = 0,1 * 24,11 / 20 * 10^6 = 1,2 * 10^{-7} / h$

A more precise analysis can be carried out by retrieving from a reliability data base the list of failure modes and failure mode ratios of the relay and analysing, for the given application, which are the dangerous failures:

Example:

Component	Failure mode	Typical failure mode ratios %	
Relay	All contacts remain in the energized position when the coil is de-energized	25	D
	All contacts remain in the de-energized position when the coil is energized	25	S
	Contact will not open	10	D
	Contact will not close	10	S
	Simultaneous short circuit between three contacts of a change-over contact	10	D
	Simultaneous closing of normally open and normally closed contact	10	D
	Short circuit between two pairs of contacts and/or between contact and coil terminal	10	D

Ratio of dangerous failures (RDF) = 65%

From equation :  $B_{10d} = 10M / 0,65 = 15,38 M$  operations

Then  $\lambda_d = 0,1 * 24,11 / 15,38 * 10^6 = 1,57 * 10^{-7} / h$

### Step 3 - Determination of Diagnostic Coverage (DC) and of the parameters $\lambda_{dd}$ and $\lambda_{du}$

Assuming that

- A failure can always happen (otherwise there would be no reason to define  $\lambda$ )
- Is not possible to detect all faults because the mechanisms for the detection of faults are not all equally effective and immediate (for some faults may take longer)
- But taking appropriate diagnostic measures most of the dangerous faults can be detected

It is possible to define a parameter DC which gives an estimate of the efficiency of the diagnostic measure implemented.

DC is defined as the ratio between the failure rate of dangerous failures detected ( $\lambda_{dd}$ ) compared to all dangerous failures detected and not detected ( $\lambda_d$ ).

$$(13) \quad DC = \lambda_{dd} / \lambda_d$$

Calling  $\lambda_{du}$  the fraction of dangerous failures that remain undetected it comes that

$$(14) \quad \lambda_d = \lambda_{dd} + \lambda_{du}$$

And:

$$(15) \quad \lambda_{dd} = \lambda_d \times DC$$

$$(16) \quad \lambda_{du} = \lambda_d \times (1 - DC)$$

IEC 62061 provides a list of different diagnostic techniques in Annex D and for each of them a parameter DC is given representing the fraction of dangerous failures that can be detected by the application of that diagnostic technique.

DC range is from 0% to 99%

DC = 0% representing no dangerous fault is detected

DC = 99% representing very high fraction of dangerous faults detected

The designer must select for each subsystem element, the diagnostic technique that would be better suited to its application (for input signals, for processing logic, for the outputs) and at the same time ensuring the DC level needed.

Example: if the diagnostic measure implemented for the control of dangerous failures of the relay of the previous example is implemented by monitoring the functioning of the relay by a mechanically linked NC contact, from Table D.1 it follows DC = 99%:

Then

$$\lambda_{dd} = 1,2 \times 10^{-7} \times 0,99 = 1,188 \times 10^{-7}$$

$$\lambda_{du} = 1,2 \times 10^{-7} \times 0,01 = 1,2 \times 10^{-9}$$

## Realization of diagnostic functions

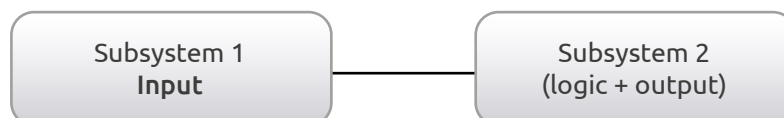
$$(17) \quad DC = \frac{\sum \lambda_{dd}}{\sum \lambda_d}$$

where:

$\sum \lambda_{dd}$  is the sum of the rate of dangerous failures detected of all subsystem elements and

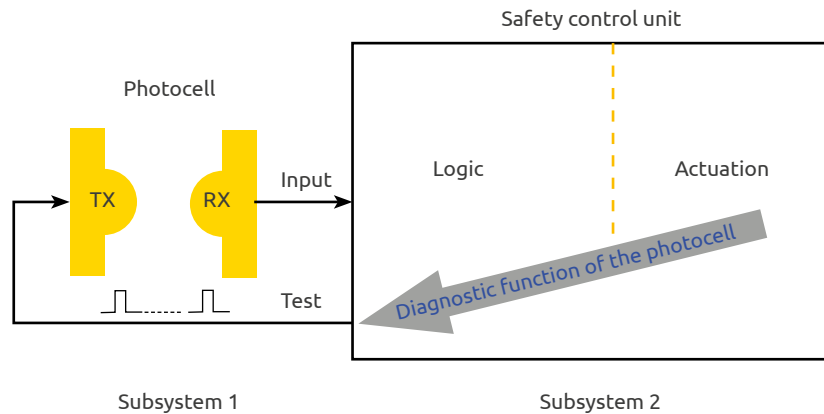
$\sum \lambda_d$  is the sum of the rate of dangerous failures of all subsystem elements

The diagnostic functions are considered as separate functions that may have also a different structure than the SCS and may be performed by:



- The same subsystem which requires diagnostics
- Or subsystems of the SCS not performing the SCF





c. Or other subsystems of the SCS

Example of diagnostic function of type c)

The SCS is made of two subsystems:

Subsystem 1 is a photocell with an MTBF = 10 years (emitter + receiver)

Subsystem 2 is an AU SX safety control unit SIL 2 rated with a PFH =  $5 \times 10^{-9}$

Diagnostic measure selected: online monitoring with check of the response time of the Photocell

From Table D.1: Cyclic test stimulus by dynamic change of the input signals DC = 90%.

Subsystem 1:

For calculation purposes, MTBF can be assumed equal to MTTF,

The ratio of dangerous failures is estimated as 0,5, therefore

$$MTTF_d = 2 \times MTTF$$

$$\lambda_d = 5,7 \times 10^{-6}$$

HFT = 0 (architecture C)

$$\beta \leq 2\%$$

As the diagnostic function is performed by the separate subsystem 2 within the SCS, formula (6) can be applied for the estimation of the PFH:

$$PFH(\text{subsystem 1}) = (1-DC) \times 5,7 \times 10^{-6} = 5,7 \times 10^{-7}$$

The overall PFH of the SCS is:

$$PFH(\text{scs}) = 5,7 \times 10^{-7} + 5 \times 10^{-9} = 5,75 \times 10^{-7}$$

#### Step 4- Estimation of safe failure fraction

After having derived for each subsystem the PFH it is important to ensure that the associated SIL is compatible with the limitations imposed by the architecture. The highest safety integrity level that can be claimed for subsystem is limited by the safe failure fractions (SFF) as specified in the following table

Safe failure fraction (SFF)	Hardware fault tolerance		
	0	1	2
SFF < 60%	Not allowed	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 3
SFF ≥ 99%	SIL 3	SIL 3	SIL 3

Subsystem safe failure fraction (SFF) is, by definition, the fraction of the overall failure rate that does not result in a dangerous failure.

It is therefore the ratio between the sum of the overall safe failures and dangerous failures detected by the diagnostic techniques implemented and the sum of all possible failures (safe, dangerous detected and dangerous not detected).

$$(18) \quad SFF = (\Sigma\lambda_s + \Sigma\lambda_{dd}) / \Sigma\lambda_s + \Sigma\lambda_d$$

For the calculation, all the components including electrical, electronic, electromechanical, mechanical etc, which are necessary to allow the subsystem to process the safety function shall considered.

## Methodology for the estimation of susceptibility to common cause failures

In case of redundant structures, the methodology used for calculating the PFH assumes a sufficient operating independence of the two channels.

However, if the channels are not fully independent, common cause failures due to a single occurrence or condition can cause a critical malfunction simultaneously on both channels in a dual channel architecture.

Examples of failures due to common causes such common-cause faults are:

- Power surges (a surge strong enough to cause multiple catastrophic failures one channel will likely destroy the other at the same time)
- Impurity of the fluid medium (valves of both channels fail to open)
- Overtemperature (due to a failure of the cooling fans).

## Estimation of the effect of CCF

The likelihood of common cause failure introduces the problem of estimating the rates of simultaneous failure for multiple components in addition to their Individual failure rates.

IEC 62061 overcome this problem by using the scoring method proposed in Annex E.

Table E.1 of this Annex gives a list of measures and for each measure an associated values is assigned which represent the contribution of each measure to the reduction of common cause failures.

All the factors having an impact on the design of the subsystem must be added to provide an overall score.

For each listed measure, only the full score or nothing can be claimed.

If a measure is only partly fulfilled, the score according to this measure is zero.

Where it can be shown that equivalent means of avoiding of CCF can be achieved through the use of specific design measures (e.g. the use of opto-isolated devices rather than shielded cables), then the relevant score can be claimed as this can be considered to provide the same contribution to the avoidance of CCF.

If equivalent means of avoiding of CCF can be achieved through the use of specific design measures (e.g. the use of opto-isolated devices rather than shielded cables), then the relevant score can be claimed.

The overall score is used to determine the common cause failure factor  $\beta$  from table F.2 as a percentage value.

Overall score	Common cause failure factor ( $\beta$ )
$\leq 35$	10% (0,1)
36 to 65	5% (0,05)
66 to 85	2% (0,02)
86 to 100	1% (0,01)

This  $\beta$  factor will be used in formulas 2, 4, 7, 8 for the calculation of the PFH of a subsystem.

## EN ISO 14119 Safety of machinery - Interlocking devices associated with guards - Principles for design and selection

### New subdivision of the interlocking devices

Interlocking device interlock (ISO 14119:2013, § 3.1) - Mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions (generally as long as a guard is not closed).

#### Type 1 devices - Uncoded

These can be:

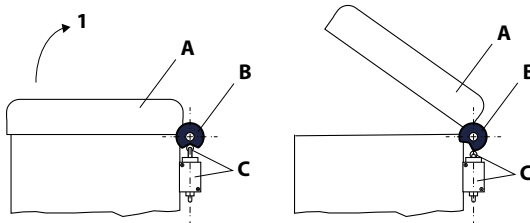
- Rotary cam
- Linear cam
- Hinge.

Linear cam

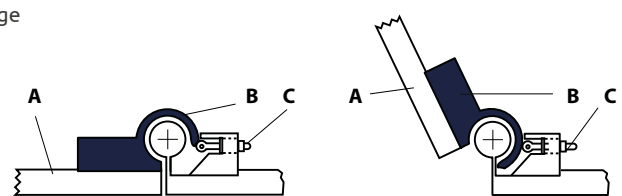


A: Movable guard  
B: Actuator (cam)  
C: Position switch  
1: Opening direction

#### Rotary cam



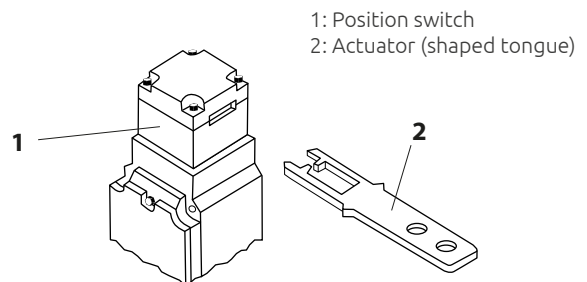
Hinge



#### Type 2 - Coded

Coded actuator (ISO 14119:2013, § 3.13). Actuator which is specially designed (e.g. by shape) to actuate a certain position switch.

- Low level coded actuator: coded actuator for which 1 to 9 variations in code are available.
- Medium level coded actuator: coded actuator for which 10 to 1000 variations in code are available.
- High level coded actuator: coded actuator for which more than 1000 variations are available.

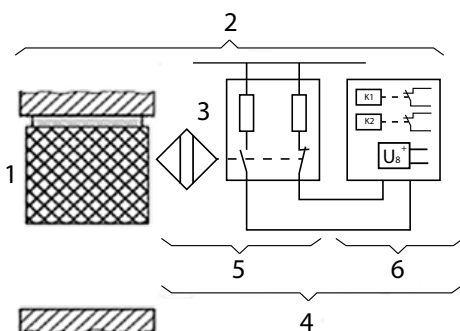


1: Position switch  
2: Actuator (shaped tongue)

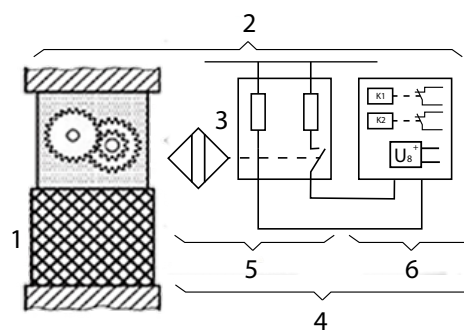
#### Type 3 - Uncoded

These can be:

- Inductive - Actuated by metal of the guard
- Magnetic - Actuated by uncoded magnet
- Capacitive - Ultrasonic or optical



Movable guard closed



Movable guard not closed

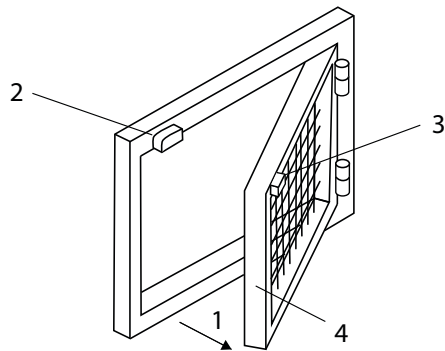
1: Movable guard  
2: Interlocking device  
3: Actuator (inductive, magnetic or capacitive)  
4: Proximity switch  
5: Actuating system  
6: Output system

## Type 4 - Coded

These can be:

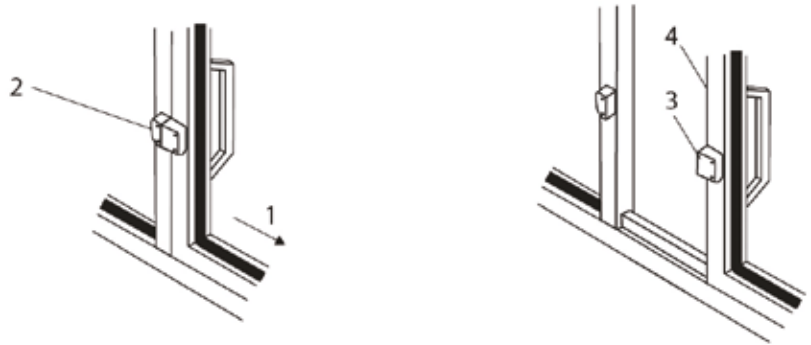
- Magnetic - Actuated by coded magnet
- RFID
- Optical - Actuated by coded optics

Position switch RFID



- 1: Opening direction
- 2: Type 4 interlocking device
- 3: coded magnet actuator
- 4: Movable guard

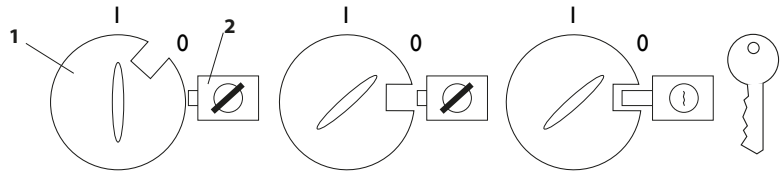
Type 4 interlocking device with position switch actuated by coded magnetic actuator



- 1: Opening direction
- 2: Type 4 interlocking device
- 3: coded RFID tag actuator
- 4: Movable guard

## Type 5 - Coded

These can be: position switch with trapped key interlocking



## Overall system stopping performance and access time (The gards distance)

The access time shall be calculated by using the distance between the hazard zone and the guard together with the approach speed (see ISO 13855:2010 for typical values).

## Logical series connection of interlocking devices

Logical series connection of interlocking device means for NC contacts wired in series or for NO contacts wired in parallel.

Up to now, for a logical series of NC contacts, it is considered a DC = 60%, allowing you to get a PL d (not a PL e). The masking of faults, could lead to a lower diagnostic coverage, so nothing.

Based on  $DC = \lambda_{dd} / \lambda_d$  (ratio of detected dangerous failures and total) can easily lead to a DC <60%.

## Interlocking devices based on “fault exclusion”

The standard specifies that the maximum safety level reached by interlocking devices based on “fault exclusion” is generally PL d. In fact there is the possibility that a single mechanical failure resulting in the loss of the safety function.

For example a mechanical failure relating to the key (actuator), or some part of the mechanical device, can generate false information on the electrical contact output.

In some cases it is still possible reach the safety level PL e. These are cases of “fault exclusion for the guard locking”.

The safety level reached in these cases is not necessarily limited by the faults exclusion of the mechanical locking device.

However, specific requirements must be verified: the holding force specified (FZH) of the protection guard locking device must be sufficient to withstand static forces planned on locking bolt, it is also necessary to prevent any effect on the protection locking device determined by the forces dynamic due to movement of the protection guard.

## Guard lock and Guard interlock

The standard emphasizes the fact that the interlock function and the lock function are two separate safety functions with PL r that can also be different (PL r Locking < PL r interlock).

## Measures to prevent the defeat of the interlock device

Guards and protection devices of the machines should not be easy to by-pass or render non-operational (Directive 2006/42/EC §1.4.1). Measures required to minimize tampering.

### Defeat (ISO 14119:2013, § 3.7 and § 3.8)

Defeat: action that makes interlocking devices inoperative or bypasses them with the result that a machine is used in a manner not intended by the designer or without the necessary safety measures.

Defeat in a reasonably foreseeable manner: defeat of an interlocking device either manually or by using readily available objects. Measures to reduce the defeat of interlocking devices may be adopted:

Prevent access to the elements which constitute the interlock device:

- Mounting out of reach, physical obstruction / shielding, Mounting in hidden position)
- Preventing substitution of the actuators using encoded interlocking devices
- Prevent disassembly or moving of the interlocking devices (welding, gluing, riveting, etc ..)
- Status monitoring or cyclic testing of the interlocking device
- Adding an additional interlock device with a different principle of implementation. In this case, you will testing dividing the plausibility of the state of both devices

The table 3 of the standard ISO 14119:2013 specify the additional measures against defeating interlocking devices depending on type.

### The anti-tampering measures in case of magnetic sensors low level coding (MAGNUS)

Mandatory:

- Mounting out of reach places, or mounting recesses and not visible in the machine, or status monitoring
- Mounting the actuator so that it is difficult to remove

Advice:

- Second magnetic sensor
- Plausibility check of both sensors

## Safe speed monitoring

The safe speed monitoring using sensors (encoders, proximity switch) for the measurement of speed, must be able to detect possible dangerous failures of the sensors themselves.

### Sensors and certified speed monitoring combinations



The Encoder is a safety related sensor SIL certified. The Mosaic controller (MV1 or MV2) monitor:

- The information provided by the sensor
- Failures on the connecting cables (short circuit, open circuit, power supply failure)

Loss of mechanical coupling between the motor shaft and the encoder cannot be detected by the safety module. The coupling system shall be designed, constructed and validated as specified in Table D8 of the IEC 61800-5-2:2016 standard in order to exclude the fault due loss of mechanical fastening of the encoder.

**Note:** if the safety integrity level of the encoder is SIL 2, then the result of the combination (Encoder + MV1 or MV2) will be SIL 2 - PL d.



The two non-safety related sensors composes a dual-channel subsystem.

The Mosaic controller (MV1 or MV2) monitor

- The information provided by the two sensors (e.g., deviation between the two measured values)
- Failures on the connecting cables (short circuit, open circuit, power supply failure)

The subsystem  $DC_{avg} = 90\%$  (medium).

The mechanical coupling of the encoder shall be designed, constructed and validated as specified in IEC 61800-5-2:2016 standard in order to exclude the fault due loss of mechanical fastening of the encoder. Mechanical coupling faults of the Sensor / Phonic Wheel combination must be excluded as well by means of a suitable fixing solution.

The dual channel solution forms a Cat. 3.

The two channels are not homogeneous as the two sensors are of different technology. This reduces the possibility of common cause failures by improving the CCF (Common Cause Failure) factor score

For the calculation of the PL, it is necessary to know the  $MTTF_D$  values of both sensors.



The two Proximity non-safety related sensors creates a dual-channel subsystem.

- The two Proximity sensors shall be installed so that to generate interleaved signals.
- The Mosaic module (MV0) verifies that the two sensors measure the same speed. Failure of one of the two channels (electrical or mechanical) causes a difference in the values measured by the controller which generates an alarm signal. Failures on the connecting cables are also detected
- Loosening or loss of mechanical coupling of the phonic wheel to the motor must be avoided by means of suitable fixing solutions.

If the above conditions are fulfilled, the subsystem  $DC_{avg} = 90\%$  (medium).

The dual channel solution forms a Cat. 3 subsystem

The two channels are homogeneous as the two sensors are of the same technology. This aspect requires more precautions to achieve the minimum score (65) of the CCF factor than the Encoder + Proximity solution. In this case it is necessary more attention in the wiring layout, in the choice of power supplies, in the quality of the cables (EMC susceptibility). It is necessary to ensure that the sensors always work within the limits of temperature, humidity and vibrations specified in the data sheet.

For the calculation of the PL, it is necessary to know the  $MTTF_D$  values of the sensors.



The two non-safety related sensors creates a dual-channel system.

- The Mosaic modules (MV1 or MV2) verifies that the two sensors measure the same speed. Failure of one of the two channels (electrical or mechanical) causes a difference in the values measured by the controller which generates an alarm signal.
- Loss of mechanical coupling between the motor shaft and the encoder cannot be detected by the safety module. The coupling system shall be designed, constructed and validated as specified in Table D8 of the IEC 61800-5-2:2016 standard in order to exclude the fault due loss of mechanical fastening of the encoder.

The subsystem  $DC_{avg} = 90\%$  (diagnostic coverage = medium). The dual channel solution forms a Cat. 3

The two channels are homogeneous as the two sensors are of the same technology. This aspect requires more precautions to achieve the minimum score (65) of the CCF factor. It is necessary more attention in the wiring layout, in the choice of power supplies, in the quality of the cables (EMC susceptibility). It is necessary to ensure that the sensors always work within the limits of temperature, humidity and vibrations specified in the data sheet.

For the calculation of the PL, it is necessary to know the  $MTTF_D$  values of the encoders.



One single non-safety related encoder is used, thus making a single channel subsystem. No monitoring means are implemented.

The Mosaic module MV1 cannot make comparisons or plausibility checks as only one single information is available.

Single failures of the encoder, regardless of the cause (electrical or mechanical), may not be detected. Faults of the connecting cable are detected. There is no diagnostic coverage, therefore  $DC_{avg} = 0$ .

The solution is Cat.B. This limits the maximum achievable safety level to PL b.

Loosening or loss of mechanical coupling with the motor shall be avoided by means of suitable fixing solutions.

For the calculation of the PL, it is necessary to know the  $MTTF_D$  values of the encoder.

The solution could reach SIL 1 -PL c- Cat.1 only if the encoder used can be considered a Well-Tried Component for safety related applications (ref. EN ISO 13849-1 and the  $MTTF_d$  of the encoder is higher than 30 years. Even if theoretically possible, this solution is not recommended for the following reasons:

- ISO EN 13849-1 (§6.2.4) gives the following definition:  
A "well-tried component" for a safety-related application is a component which has been either  
- widely used in the past with successful results in similar applications, or  
- made and verified using principles which demonstrate its suitability and reliability for safety related applications.  
The decision to accept a particular component as being "well-tried" depends on the application. Example, a position switch with positive opening contacts can be well tested for a machine tool and at the same time inappropriate for application in the food industry.
- Complex electronic components (e.g., PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to "well tried".
- Table D.3 of ISO EN 13849-2 supply a list of "well-tried" components.  
Encoders are not comprised in the list of "well-tried" components
- An encoder may be declared as well-tried for safety related purposes in a given application, if the user of the encoder is able to demonstrate and document its correct behaviour and high reliability under all environmental conditions that can be assumed for the entire mission time of the device, for a sufficient quantity of parts and for a suitably long time.



1 Proximity

+



Safety speed monitoring unit MV0

=

Cat. B  
PL b

The proximity must have two antivalents outputs.

This is a single channel subsystem because one single non-safety related proximity is used. No monitoring means are implemented. The controller cannot make comparisons or plausibility checks, as only one single information is available.

Single failures of the channel, regardless of the cause (electrical or mechanical), may not be detected. Some faults of the connecting cable are detected. There is no diagnostic coverage, therefore  $DC_{avg} = 0$ .

The solution is Cat.B. This limits the maximum achievable safety level to PL b.

Loosening or loss of mechanical coupling with the motor shall be avoided by means of suitable fixing solutions.

For the calculation of the PL, it is necessary to know the  $MTTF_d$  value of the sensor.

**Warning:** When using phonic wheels, reading error may occur due to sensor hysteresis. If the phonic wheel stops at a position where the part detected by the sensor is at the limit (right or left) of the detectable part (e.g., tooth of the wheel), the system may still perform counts.

The solution could reach SIL 1 -PL c- Cat.1 only if the proximity used can be considered a Well-Tried Component for safety related applications (ref. EN ISO 13849-1 and the  $MTTF_d$  of the proximity is higher than 30 years. Even if theoretically possible, this solution is not recommended for the same reasons of the previous point. As indicated for the encoder is also true for the proximity

## General safety principles for all combinations

The sensors shall be fixed, installed, and wired in accordance with the sensor manufacturer's instructions. Observe the basic mechanical and electrical safety principles (only for parts not covered by the sensor manufacturer user manual).

- Mechanical
  - Correct dimensioning and shaping
  - Proper selection, combination, arrangements, assembly, and installation of components/system
  - Proper fastening
- Electrical
  - Proper selection, combination, arrangements, assembly and installation of components/system
  - Correct protective bonding
  - Withstanding environmental conditions
  - Secure fixing of input devices
  - Protection of the control circuit Failure mode orientation.

## Additional safety principles for safety integrity level combinations SIL1 - PL c, SIL2 - PL d, SIL 3 - PL e

Observe the well-tried mechanical and electrical safety principles (only for parts not covered by the sensor manufacturer).

- Mechanical:
  - Over dimensioning /safety factor
  - Safe position
  - Careful selection, combination, arrangement, assembly and installation of components/system related to the application
  - Careful selection of fastening related to the application
  - Limited range of force and similar parameters
  - Limited range of speed and similar parameters
- Electrical
  - Fault avoidance in cables
  - Limitation of electrical parameters



- No undefined states
- Oriented failure mode

<p>Loss or loosening of attachment during standstill or during motion:</p> <ul style="list-style-type: none"> <li>- sensor housing from motor chassis</li> <li>- sensor shaft from motor shaft</li> <li>- mounting of the read head</li> </ul>	<p>Preparing FMEA and prove:</p> <ul style="list-style-type: none"> <li>- permanent fastness for form-locked connections</li> <li>- fastness for force-locked connections</li> </ul>	<p>The maximum permissible loading of the sensor is known or limited on the sensor's data sheet.</p> <p>a) <u>For form-locked connections:</u></p> <p>1) Design for permanent fastness in accordance with generally acknowledged technical experience with a high safety factor</p> <ul style="list-style-type: none"> <li>- Verification is performed by calculation and with a suitable test.</li> <li>- Example for steel components: Overdimensioning with a safety factor <math>S \geq 2</math> against fatigue fracture.</li> </ul> <p>or</p> <p>2) Overdimensioning with a safety factor <math>S \geq 5</math> against fatigue fracture</p> <ul style="list-style-type: none"> <li>- Verification is performed by calculation.</li> </ul> <p>b) <u>For force-locked connections:</u></p> <p>1) Overdimensioning with a safety factor <math>S \geq 4</math> against slipping</p> <ul style="list-style-type: none"> <li>- Detailed measures for application and maintaining the preloading force are to be defined in the user documentation (e.g. defined pairs of materials, surfaces and torque-controlled tightening methods).</li> <li>- Verification is performed by calculation and with a suitable test.</li> </ul> <p>or</p> <p>2) Overdimensioning with a safety factor <math>S \geq 10</math> against slipping</p> <ul style="list-style-type: none"> <li>- Measures for application and maintaining the preloading force are to be defined in the user documentation</li> <li>- Verification is performed by calculation.</li> </ul>
--	--	--

- Minimizing possibility of faults

Fig. 32. Extracted from Table D.8 of the IEC EN 61800-5-2: 2016 standard

## Mosaic analog safety modules (MA2 - MA4) and analog sensors

Often, in machines and industrial plants, there are process that require safety functions capable of reaching PL or SIL levels. For example, the EN528 standard for stacker cranes requires a weight control with a performance level PL r = d. To meet this need, the MA2 and MA4 modules, capable of carrying out a safe evaluation of analog quantities, have been added to the Mosaic range.

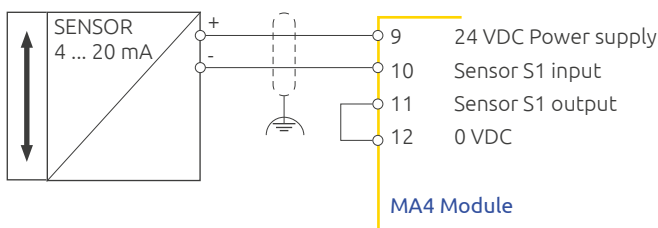
The MA2 and MA4 modules are certified according to the 2006/42/EC Machinery Directive. They also comply with the standards of the EN IEC 61508 series, so they can also be used in process plants, for SIS systems and SIF functions.

The MA2 and MA4 modules can manage 2 or 4 analog input channels. These inputs can be used individually or in pairs.

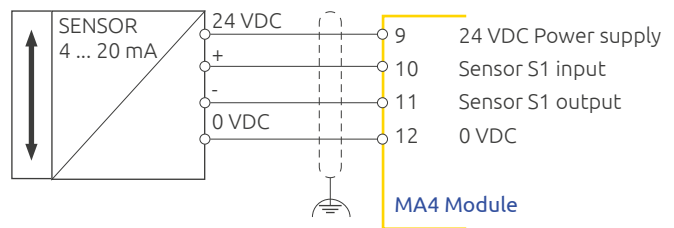
- When the inputs are used individually, depending on the sensors connected, the system can reach a safety level up to SIL 2 / PL d.
- When the inputs are used in pairs, depending on the sensors connected, the system can reach a safety level SIL 3 / PL e.

Each analog input is fully isolated up to 500 VDC. MA2 and MA4 can be configured to be connected to 1 or 2 sensors having a current output (0 ÷ 20 mA, 4 ÷ 20 mA) or having a voltage output (0 ÷ 10 V). In addition, various connection configurations are possible.

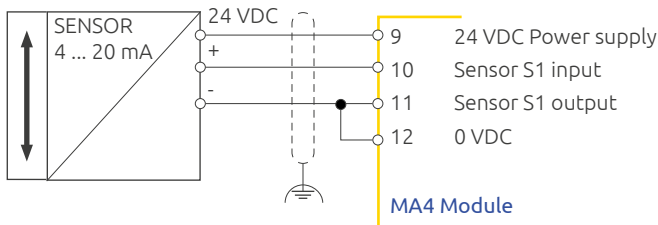
Sensors with current output 2 wires



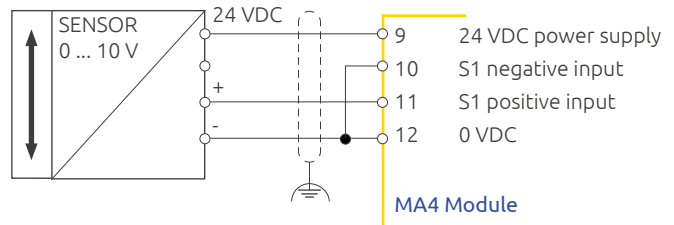
Sensors with current output 4 wires




Sensors with current output 3 wires



Sensor with voltage output 3 wires



 **Sensors** Sensors with 0-5V voltage outputs. These sensors can be connected to modules configured for voltage input by selecting in the MSD Software a full scale value two times higher. Example: if full scale is 100 kg at 5V, 200 kg must be selected. In this case, 1 bit of resolution will be lost out of the 16 available.

There are also sensors capable of measuring both positive and negative values. Mosaic analog modules can also accept negative values from the sensors (for example a flow in both directions, the pressure can also be negative - vacuum, etc.).

In this case the output signal may have, for example:

- A minimum full scale that refers to a negative value (4 mA)
- A maximum full scale that refers to a positive value (20 mA)
- The zero value will be placed in the centre of the scale (12 mA)

## MA2, MA4 modules used with safety analog sensors

On the market are available analog sensors already certified SIL (Typically IEC 61508). These standard is mainly used in the world of process industry and less known in the world of machines and industrial automation where EN ISO 13849-1 /2 and EN 62061 are used. For example:

- Temperature sensors
- Flow sensors
- Pressure sensors
- Lower explosive limit (LEL) sensors for Atex zones
- Weight sensors
- Flame sensors
- Transducers of physical quantities in current signals from 4 to 20 mA always with SIL certifications.

The use of these sensors already SIL rated makes it easier the calculation of the overall safety integrity of the safety function.

Simplifying as much as possible, let's look at example.

Safety level according to IEC 61508

Sensors	MA2, MA4	Application Safety level
1 sensor SIL 3	SIL3	SIL 3
2 sensors SIL 2 in parallel	SIL3	SIL 3
2 sensors SIL 1 in parallel	SIL3	SIL 2
1 sensor SIL 2	SIL3	SIL 2
1 sensor SIL 1	SIL3	SIL 1

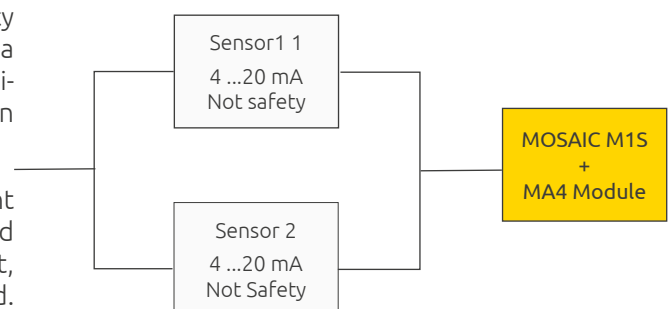
## MA2, MA4 modules used with non-safety analog sensors

There are non-safety analog sensors on the market. Using the Mosaic MA2 and MA4 analog modules, these sensors can also be used for safety functions according to EN ISO 13849. We consider EN ISO 13849-1 as it is the standard that is most frequently used in the field of machines.

The characteristics of the MA2 MA4 modules allow to connect 2 measurement sensors, to put them in relation to each other, creating redundancy and cross monitoring to increase the total safety level of the system. In this way it is possible to verify the measurement and obtain a security level higher than that obtainable using a single sensor.

Automation sensors can be used, e.g. without the PL / SIL safety level declared by the manufacturer and in any case achieve a very high safety level, up to SIL 3 / PL e, satisfying all the conditions required by the standards. Beside a logical representation of the system.

An example will be presented below where the most important aspects of the assessments to be performed will be analysed and the procedures that must be performed to ensure that, with the Mosaic system, the required level of safety is achieved.



The example shows: Non-safety sensors (without PL / SIL declared by the manufacturer) 4-20 mA and Mosaic M1S with MA4 module.

We will then analyse which is the achievable PL and under what conditions.

This architecture represents a pair of analog sensors that measure the same physical quantity.

It is necessary to verify that:

- The safety function SF, generates a stop signal (not represented here) when a certain threshold value is exceeded
- The behaviour in case of failure has been well identified. With safety systems that measure analog quantities, the evaluation of the behaviour in the event of a fault is more complex. Behaviour must be evaluated and the decision is often not unique. In general, in case of a component failure, The system must consider the signal coming from the faulty component as if it had exceeded the threshold beyond which the machine must be stopped (safety-oriented fault).
- The safety related software has been created according to EN ISO13849-1 §4.6
- Systematic failures are checked and excluded (EN ISO13849-1 Annex G)
- The ability to perform the safety function under the expected environmental conditions is verified

The architecture with 2 sensors indicates a category 3 or 4 due to the presence of redundancy. We will check which conditions must be met to obtain Category 4 or Category 3.

Reference should be made to table 10 of ISO 13849-1, which deals with making a first classification:

Category	Summary of requirements	System Behaviour	Principles used to achieve safety	MTTF <sub>D</sub> of each channel	Diagnostic coverage (DC)	Common cause failure (CCF)
B	Design according to the basic safety principles	The occurrence of a fault can lead to the loss of safety function	Mainly characterized by selection of components	Low	None	Not relevant
1	Requirement of B + well tried components and well tried safety principles shall be used	The occurrence of a fault can lead to the loss of safety function but the probability of occurrence is lower than for category B	Mainly characterized by selection of components	High	None	Not relevant
2	Requirement of B + Safety function test at "appropriate" intervals	The occurrence of a fault can lead to the loss of safety function between one test and another. The test recognizes the loss of the safety function.	Architecture	Low	Low - Medium	Check
3	Requirement of B + a single fault must not lead to the loss of the safety condition and if possible, the single fault must be identified	A single fault must not lead to the loss of the safety condition. Some faults need to be identified. The accumulation of faults can lead to the loss of the safe condition.	Architecture	Low	Low - Medium	Check
4	Requirement of B + a single fault must not lead to the loss of the safety condition. The single fault must be identified before the need for intervention and in any case the accumulation of faults must not lead to the loss of the safety condition	A single fault must not lead to the loss of the safety condition. The identification of accumulated faults (high DC) reduces the probability of loss of the safe condition	Architecture	High	High and includes the accumulation of faults	Check

Following the instructions in the table, we need to:

- Compliance with relevant standards for resistance to expected influences (Check sensor manufacturer's datasheet).
- Use of basic safety principles.
- Use of well-tried safety principles.
- Single fault tolerance and reasonably foreseeable fault detection

## MTTF<sub>D</sub> value

We determine the average duration of operation, expressed in years, before a potentially dangerous random failure or "Mean Time to dangerous Failures" (MTTF<sub>D</sub>) occurs. Normally the manufacturer of the sensors does not provide data of "Performance Level" (PL) / "Probability of dangerous Failure per Hour" (PFH<sub>D</sub>) or of "Mean Time to dangerous Failures" (MTTF<sub>D</sub>) but only the value of "Mean time between failure" (MTBF) which, in this example, we assume 54 years (real figure obtained from a manufacturer). If this value is not available, it is possible to obtain standard values from the EN ISO13849-1 Annex C. In this case it is possible to make the following assumptions

$$MTTF = MTBF + MTTR \text{ (Mean Time To Restoration)}$$



"Mean time to restoration" (MTTR) or average repair time, is the time interval during which an equipment is in a state of unavailability due to a fault. The MTTR includes the time for diagnosis, the time for the arrival of the maintenance technician, the arrival of the component to be replaced and the actual repair. For electronic equipment MTTR can be considered negligible (it is not repaired, it is replaced).

$$MTTF \approx MTBF$$

When the dangerous failure rate is not known, EN13849-1 allows us to assume that these are 50% of all failures, therefore:

$$MTTF_D = 2 \times MTBF$$

$$MTTF_D = 2 \times 54 = 108 \text{ years}$$

This evaluation refers to the single sensor.

## Diagnostic coverage considerations

We now determine the value of the "Diagnostic Coverage" (DC)

The Diagnostic Coverage specifies how efficient the system is in determining its malfunctions in real time ie before another failure occurs.

We will use the ISO 13849 Table E1 (shown right), which provides a list of 34 different diagnostic techniques that can be used to increase the fault detection capability of a circuit.

The techniques are divided into three families (input circuits, signal processing logic and output circuits).

A percentage score between 0% and 99% is assigned for each technique.

Mosaic MA4 and MA2 perform cross monitoring [A] as required by the table, then the system reaches 99% DC.

This is still not enough for the system to reach Category 4.

### E.1 Examples of diagnostic coverage (DC)

See Table E.1

Table E.1 — Estimates for diagnostic coverage (DC)

Measure	DC
<b>Input device</b>	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

A

## Accumulated faults

To obtain the Category 4, Table 10 of ISO 13849-1 (see previous page) requires the DC to be High (99%) and includes the accumulation of faults, e.g. multiple faults can occur, one after the other, without degrades the safety function.

The single fault must be detected when it occurs or before the next request from the safety function. If this is not possible, an accumulation of undetected faults must not lead to the loss of the safety function.

To meet this requirement, the choice of sensors or how to use them also matters.

1. A sensor with 0-10 V output has the minimum value at 0 VDC which is indistinguishable from a short circuit at 0 VDC. Furthermore both sensors could have this type of fault resulting in an accumulation of faults.
2. Sensors with 0-20 mA current output follow the same logic but with a dangerous fault represented by an open circuit (for example a disconnected cable).

In safety applications, if we want to reach Category 4, these type of sensors must be avoided or a threshold must be programmed for which below a certain value, for example 0.5 VDC or 2 mA, the system reacts as if to a fault. With the Mosaic system, for example, it is possible to configure the operating parameters through the MSD software to increase the DC. Intermediate controls can be implemented such as:

- Measurement error between the 2 sensors.
- Time control of out of range.

An important aspect remains regarding the diagnostic coverage and the accumulation of faults. The case where the sensor output value does not change for a period of time.

Let's assume that sensors, for example for temperature, measure the same value for a long time, always transmitting the same current value, e.g. 5 mA. One of the possible faults that could occur is that in which both sensors, in sequence, break, always transmitting the same current value. Such a fault could not be detected by the safety system.

To be sure to also detect this type of accumulated faults, it is necessary to carry out dynamic tests, for example by varying the temperature in the part of the machine to which the sensors are connected, with a predetermined frequency (for example 4 times per hour). This type of test is mandatory for category 4.

To conclude these assessments on accumulated failures, we must point out:

1. It is often impossible to force changes into a process. As for our example, it could be difficult to change the temperature of a part of the machine.
2. All this is required for Category 4 ONLY.
3. The use of adequately sensors and thresholds to avoid short circuits or undetected open circuits is also important in the calculation of CCFs, described below.

If we want to obtain a Category 4, we must increase the Diagnostic Coverage (DC) or at least verify that the use of our safety system is the best possible. There are methods to evaluate what the time interval must be between 2 successive changes in the values measured by the sensors:

- Statistical mathematical evaluations of the reliability characteristics of the sensors used and their configuration. There are established but complex calculation methods to analyse them in this guide. However, the use of complex mathematical tools does not guarantee the accuracy of the result.
- Consider the practical application of the sensors and aim for a significantly lower test interval than the duration of inactivity of the sensors. Or carry out a test before using the machine and the need for the safety function.

The ultimate goal is that the accumulation of faults, even not detected, never leads to the loss of the safety function. This is the mandatory requirement of Category 4, it is often impossible to fully comply.

## Common Cause Failure (CCF) considerations

This is the fault resulting from one or more events that causes the simultaneous malfunction of the channels of a two or more channel system.

It provides an indication of the degree of operational independence of the channels of a redundant system.

Using the table F1 (shown on the right) of the ISO 13849 standard, a score is assigned in relation to any measure against common cause failures. The maximum achievable score is 100.

The calculation and verifications are common for all categories.

### 1. Separation / Segregation

*Use of shielded cables* - With the use of analog outputs, shielded cables are already normally used, and it is the single cable that is shielded.

*Detection of faults such as short circuits or open circuits* - The detection characteristics of analog signals, current (0 ... 20 mA) or voltage (0 ... 10 V) allow to satisfy the indicated measurements.

This can be done easily by excluding values such as 0 V or 0 mA. So it's easy to get the 15 points.

### 2. Diversity

*Use of different sensors* - For example, with the Mosaic MA2 MA4 modules, 2 sensors can be used not only with different full scale but, even, with different types of outputs (voltage or current).

It's easy to get the 20 points.

### 3. Design / Application / Experience

*Use of protections* - By inserting the appropriate and necessary protections (Over-Voltage and Over-Current) 15 points can be obtained.

*Use of well tried components* - Devices with analog output are not among the well tried components (EN 13849-2 table D.4). So 0 points.

### 4. Evaluation / Analysis

Failure mode and effect analysis (FMEA) analyses are required.

This type of analyses would require a lot of time, for this measure we assign 0 points by not carrying out any activity.



However, a FMEA is not necessarily a mathematical calculation of the probability of risk, but it is an analysis of all types of failure to evaluate their effects. An evaluation of this type must however be carried out when choosing and installing sensors, so it might be worthwhile to document it and get the few 5 points it deserves.

### 5. Competence / Training

Considering the designers prepared to understand the generation of CCFs and their consequences, we assign 5 points

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
<b>1</b>	<b>Separation/ Segregation</b>	
	Physical separation between signal paths, for example:	<b>15</b>
	— separation in wiring/piping;	
	— detection of short circuits and open circuits in cables by dynamic test;	
	— separate shielding for the signal path of each channel;	
	— sufficient clearances and creepage distances on printed-circuit boards.	
<b>2</b>	<b>Diversity</b>	
	Different technologies/design or physical principles are used, for example:	<b>20</b>
	— first channel electronic or programmable electronic and second channel electromechanical hardwired,	
	— different initiation of safety function for each channel (e.g. position, pressure, temperature),	
	and/or	
	digital and analog measurement of variables (e.g. distance, pressure or temperature)	
	and/or	
	Components of different manufactures.	
* Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.		

Table F.1 (continued)

No.	Measure against CCF	Score
3	Design/application/experience	
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15
3.2	Components used are well-tried.	5
4	Assessment/analysis	
	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	5
5	Competence/training	
	Training of designers to understand the causes and consequences of common cause failures.	5
6	Environmental	
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326-3-1).  Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium.  NOTE For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Other influences  Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10
Total		[max. achievable 100]
Total score		
65 or better		Meets the requirements
Less than 65		Process failed ⇒ choose additional measures
* Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.		



## 6. Environment

The system must be immune to the effects of the surrounding environment, such as dirt. Furthermore, the system must be immune to EMC disturbances, in particular to EMC disturbances generating CCF (Common mode and / or differential disturbances). Only if it can be proven (also documented with tests), we have 25 points.

All other environmental conditions (temperature, humidity, vibrations...) must be taken into consideration. Only if immunity can be demonstrated, we have 10 points.

At least 65 points must be obtained. It is quite clear that the conditions for reaching Category 3 are quite easy. The achievement of System Category 4 (not to be confused with that of the module) is more critical due to the difficulty of detecting the accumulation of faults.

Basically:

1. If it is demonstrable that  $DC = 99\%$  and the accumulation of faults is detected, the requirements of Category 4 are met.
2. In the event that it is demonstrable that  $DC > 90\%$  and the accumulation of faults is not detected, the requirements of Category 3 are met.

## Conclusion

Based on table K1 of EN 13849-1, the safety function in our example, with 62 years sensor  $MTTF_D$ , high DC but, for example, without the conditions required by Category 4 because we are unable to test sensors at regular intervals, PL e is reached (green box).

MTTF <sub>D</sub> di ogni canale anni	Probabilità media di un guasto pericoloso per ora (1/h) e corrispondente livello di prestazione (PL)							
	Cat. B DC <sub>avg</sub> = nessuna	PL	Cat. 1 DC <sub>avg</sub> = nessuna	PL	Cat. 2 DC <sub>avg</sub> = bassa	PL	Cat. 2 DC <sub>avg</sub> = media	PL
15	$7,61 \times 10^{-6}$	b			$4,53 \times 10^{-6}$	b	$3,01 \times 10^{-6}$	b
16	$7,13 \times 10^{-6}$	b			$4,21 \times 10^{-6}$	b	$2,77 \times 10^{-6}$	c
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$	c	$6,49 \times 10^{-7}$	d
51			$2,24 \times 10^{-6}$	c	$1,13 \times 10^{-6}$	c	$5,80 \times 10^{-7}$	d
56			$2,04 \times 10^{-6}$	c	$1,02 \times 10^{-6}$	c	$5,10 \times 10^{-7}$	d
62			$1,84 \times 10^{-6}$	c	$9,06 \times 10^{-7}$	d	$4,43 \times 10^{-7}$	d
68			$1,68 \times 10^{-6}$	c	$8,17 \times 10^{-7}$	d	$3,90 \times 10^{-7}$	d
75			$1,52 \times 10^{-6}$	c	$7,31 \times 10^{-7}$	d	$3,40 \times 10^{-7}$	d
82			$1,39 \times 10^{-6}$	c	$6,61 \times 10^{-7}$	d	$3,01 \times 10^{-7}$	d
91			$1,25 \times 10^{-6}$	c	$5,88 \times 10^{-7}$	d	$2,61 \times 10^{-7}$	d
100			$1,14 \times 10^{-6}$	c	$5,28 \times 10^{-7}$	d	$2,29 \times 10^{-7}$	d

From the table, the sensor subsystem will have:

$$PL=e \text{ with } PFH_D=4,22 \times 10^{-8}$$

the other component of the safety system is Mosaic.

From the Mosaic report a combination of M1S master module + MA4 analog module have the value:

$$PFH_D=2,97 \times 10^{-8}$$



To calculate the total PL we have to add the  $PFH_D$

$$PFH_{D\_total} = PFH_{D\_sensor} + PFH_{D\_Mosaic} = 4,22 \times 10^{-8} + 2,97 \times 10^{-8} = 7,29 \times 10^{-8}$$

Always PL=e

**Table 2 — Performance levels (PL)**

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

Use of not safety sensors for safety functions according to EN IEC 62061

The same considerations can also be repeated with this standard for process automation. However, the calculation and analysis methods are much more complex.

For a simplified approach it is possible to refer to this table of EN ISO 13849 which proposes a relationship between the final values achieved

**Table 4 — Relationship between performance level (PL) and safety integrity level (SIL)**

PL	SIL (IEC 61508-1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

## Glossary

Initials	Definition	Standard	Description
$\beta$ (Beta)	Common cause failure factor	IEC 62061	<p>Degree of operational independence of channels of a multi-channel system. Ranging from 0.1 to 0.01 depending on CCF attained.</p> <p>Random failure frequency.</p> <p>The time-random failure frequency of a component is usually known as Failure Rate, described as number of failures per unit of hour.</p> <p>Its inverse is known as Mean Time Between Failures (MTBF), expressed in hours.</p>
$\lambda$ (Lambda)	Failure rate	IEC 62061	<p>Random failures are the result of sudden stress accumulation above maximum design strength of a component. May occur at random intervals and entirely unexpectedly.</p> <p>Frequency of failure over sufficiently long periods is virtually constant. PFHd calculation methods given in both Standards refer only to the assessment of random failures.</p> <p>The unit of measure for failure rate is FIT (Failure In Time) equivalent to one failure per billion of operating hours (F=1 means one failure every 109 hours).</p>
$\lambda_s$	Safe failure rate	IEC 62061	<p>Failure rate for non-dangerous failures.</p> <p>Non-dangerous failures which have no adverse safety-related effect on control system. The control system continues to ensure protection.</p>
$\lambda_d$	Dangerous failure rate	IEC 62061	<p>Failure rate of failures which may involve dangerous operation.</p> <p>Dangerous failures prevent the control system from continuing to provide protection.</p>
$\lambda_{dd}$	Dangerous detected failure rate	IEC 62061	<p>Failure rate for detectable dangerous failures.</p> <p>Detectable dangerous failures may be detected by automatic self-diagnostic systems.</p>
$\lambda_{du}$	Dangerous undetected failure rate	IEC 62061	<p>Failure rate for undetectable dangerous failures. Undetectable dangerous failures cannot be detected by internal automatic self-diagnostic systems.</p> <p>They determine the value of PFHd and, consequently, the value of SIL or PL.</p>
Cat.	Category	ISO 13849-1	<p>The category is the main parameter to consider to attain a given PL.</p> <p>Describes the SRP/CS performance in relation to its ability to resist failure and resulting performance in failure conditions.</p> <p>Five Categories are envisaged depending on structural positioning of components.</p>
CCF	Common Cause Failure	ISO 13849-1 IEC 62061	<p>Failure resulting from common causes.</p> <p>Failure resulting from one or more events causing simultaneous malfunction of channels of a multi-channel system.</p> <p>Provides a measure of the degree of independence of redundant channel operation. Assessed by assigning marks. Maximum possible score is 100.</p>
DC	Diagnostic Coverage	ISO 13849-1 IEC 62061	<p>Reduced probability of dangerous hardware failure due to automatic self-diagnostic system operation. A measure of system effectiveness in promptly detecting its own possible malfunction. Expressed as 60% to 99%.</p>
MTTF <sub>D</sub>	Mean Time to dangerous Failures	ISO 13849-1	<p>Average operating time, expressed in years, to potentially dangerous random failure (not generic failure). May refer to a single component, or to a single channel, or to the entire safety-related system.</p>

Initials	Definition	Standard	Description
PFH <sub>d</sub>	Probability of dangerous Failure /Hour	IEC 62061	Average probability of dangerous failure per hour. Quantitative representation of risk reduction factor provided by the safety-related control system.
PL	Performance Level	ISO 13849-1	Level of performance. In ISO 13849-1, the extent to which failures are controlled is assessed using the Performance Level concept (PL). Represents SRP/CS ability to perform a safety-related function within predictable operating conditions. There are 5 levels, PL a to PL e. PL e represents the highest level of risk reduction, PL a the lowest level.
PL r	Performance Level required	ISO 13849-1	Level of performance required. Represents the contribution to risk reduction by each safety-related part implemented in SRP/CS. PL r is obtained using the risk curve.
SIL	Safety Integrity Level	IEC 62061	Level of integrity of a safety-related function. Discrete level (one of three) used to describe the ability of a safety-related control system to resist failure as per IEC 62061, where level 3 assures the highest protection and level 1 the lowest.
SILCL	SIL Claim	IEC 62061	Max. SIL attainable by a subsystem in relation to architecture and ability to detect failure.
SRP/CS	Safety Related Parts of Control Systems	ISO 13849-1	Part of machine control system able to maintain or achieve machine safety status in relation to the status of certain safety-related sensors.
SRECS	Safety Related Electrical, electronic and programmable electronic Control System	IEC 62061	Electrical, electronic and programmable electronic control system the failure of which immediately increases the risk factor associated with machine operation.
T1	Proof test interval	IEC 62061	Interval of proof test. The Proof Test is an external manual inspection for detecting component failure and performance decay, undetectable by internal self-diagnostic systems. The unit of measure is time (months or, more usually, years).
T2	Diagnostic test interval	IEC 62061	Test interval of self-diagnostic functions. Time elapsed between one test for the detection of possible internal failure and the next. Tests are carried out in automatic mode by dedicated circuitry which may be internal to the SRECS in question or may belong to other SRECSs. The unit of measure is time (milliseconds to hours).
SFF	Safe Failure Fraction	IEC 62061	Fraction of overall failure rate which does not involve dangerous failure. Represents the percentage of non-dangerous failures relative to total number of failures of the safety-related control system.

# SENSORS

## PHOTOELECTRIC SAFETY LIGHT CURTAINS



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

## Characteristic elements

Light curtains are protective electro sensitive devices (ESPE) using one or more light beams, emitted by an Emitter and received by a Receiver, to create an intangible controlled area.

When the chosen safety device is a photo-electric barrier (AOPD Active Optoelectronic Protective Device), it shall necessarily belong to TYPE 2 or TYPE 4 as established by the International Standard IEC 61496 1-2.

**Why “Type” and not “category”?**

The two “Types” differ in their safety related performance and are related to the categories of ISO 13849-1 but do not have the same meaning as here, to define the degree of safety integrity, further parameters in addition to the the architecture of the system and to the types of hardware and software failures are taken into account that are related to the detection technology used (substantially optical); they mainly concern immunity to light interference and the design characteristics of the Optical systems.

## New safety parameters for Type 2 light curtains

With the publication of Edition 3 of the harmonized EN 61496-1 standard it is no longer possible to use a Type 2 safety light curtains for safety functions assessed as SIL 2 / PL d. If a safety level of SIL 2 / PL d (or higher) is required and it is nevertheless intended to use a safety light curtain, then it will be necessary to use a Type 4 safety light curtain.

This regulatory requirement derives from the fact that the reduction of risk that can be obtained via a photoelectric safety light curtain is not only a function of the safety level of its electronic parts, but is also determined by its systematic capabilities (for example: environmental influences, EMC, optical performance and detection principle).

The systematic capability of a Type 2 photoelectric light curtain may in fact not be sufficient to ensure adequate risk reduction for SIL 2 / PL d applications. The standard also establishes that the labelling of Type 2 safety light curtains must indicate such limitation to SIL 1 / PL c.

The  $PFH_d$  values declared for the electronic control part of the device, on the other hand, are not limited and therefore it is possible to use the  $PFH_d$  value provided by the manufacturer of the device in the global assessment of the safety function, even if it exceeds the SIL 1 / PL c range.

## Protected height

This is the height controlled by the light curtain. If it is positioned horizontally, this value shows the depth of the protected zone.

## Range

This is the maximum working distance that may exist between the emitter and the receiver. When deflection mirrors are used, it is necessary to take into account the attenuation factor introduced by each of them, which it is about 15%.

## Response time

This is the time it takes for the light curtain to transmit the alarm signal from the time the protected zone is interrupted.

## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### Resolution

The resolution, for all ReeR safety light curtains, is the minimum size of an object that, placed into the controlled area, will obscure the controlled zone and hence stop the hazardous movement of the machine.

- Single beam light barriers: their resolution  $R$  is the same as the diameter of the lens.
- Multibeam light curtains: their resolution  $R$  is the same as the sum of the lens diameter + the distance between two adjacent lenses.

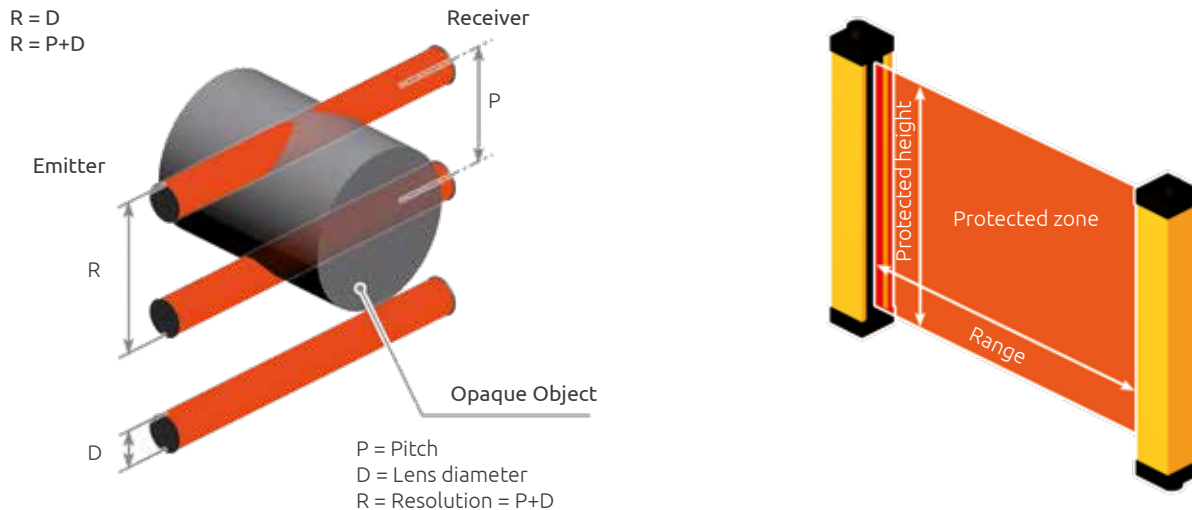


Fig. 33. Resolution

### Advantages of light curtains

- Effective protection in the event of fatigue or distraction of the operator.
- Increase in the productive capacity of the machine as the light curtain does not require the manual handling of physical guards or waiting for them to open.
- Faster machine loading/unloading operations.
- Reduced times of approach to the working areas.
- Elimination of the risk of tampering since any irregular intervention on the light curtain stops the machine.
- Simple and quick installation, with greater flexibility of adjustment on the machine, even in the case of subsequent repositioning.
- Possibility to build up large sized protections, either linear or along a perimeter, on several sides, at greatly reduced costs.
- Facilitated and fast maintenance of the machine, as there is no need to remove physical guards, such as grids, gates, etc.
- Improved appearance and ergonomic effectiveness of the machine.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

**The technical specification IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons**

This technical specification provides recommendations for the installation and use of ESPEs.

It is therefore mainly applied to Safety light curtains and Safety Laser Scanners, Safety Mats

This technical specification meets the needs of the machine manufacturers and of the machine users. Indeed it gives requirements for the selection of the most suitable model, its correct positioning and its correct interfacing to the machine.

**Selection process**

The purpose of the Selection Process of the Protective Device (ESPE) is to ensure that, through proper choice and application of the device (and if necessary through the integration of other safety measures) the risk of injury to the operator is reduced to the acceptable minimum.

In order to make a correct choice, the following factors must be taken into account which may adversely affect the effectiveness of protection:

- machine characteristics
- environmental characteristics
- human characteristics
- type of use of the protective equipment
- protective equipment characteristics.

## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### Machine characteristics

For optoelectronic safety devices to be effective, it is necessary to verify that they are suitable for the shape and size of the detection zone (e.g. width and height of the access area).

However, some characteristics of particular machines can preclude the use of protective equipment as the sole protective measure.

Examples of these machine characteristics are:

- possibility that the machinery will eject materials, swarf or component parts
- risk of injury from thermal or other radiation unacceptable noise levels
- an environment likely to adversely affect the function of the protective equipment
- a material being processed that can influence the effectiveness of the protective measure
- it is impossible to stop the machine immediately when it is started because this could introduce additional risks or because the machine can only be stopped at the end of the processing cycle due to the particular type of operation

Or the ESPE is poorly efficient if:

- The machine stopping time is unknown or is randomly variable due to unquantifiable delays introduced by the control circuit or due to under dimensioned braking systems
- The machine cannot be stopped at any point in its working cycle

### Environmental characteristics

Care must be taken to assess the environment in which the machine is expected to work. Before choosing the device, all the necessary information about the working environment and the possible variations that are reasonable to expect during the life of the machine should be available.

A non-exhaustive list of environmental conditions that may adversely affect the operation of an optoelectronic device are as follows.

- electromagnetic interference
  - electrostatic discharge
  - radio frequency interference, for example mobile telephones
  - lightnings
- vibration/shock
- light interference
  - ambient light
  - reflective surfaces
  - infra-red, for example remote controls or other ESPEs that can emit interfering light
- pollution
  - water
  - dust
  - corrosive chemicals
  - smoke
- temperature
- humidity
- weather conditions
- radiation

If there are special operating conditions such as outdoor operation (fog, rain, snow) or operation in potentially explosive or flammable atmospheres (paints, sawdust), then further environmental requirements may be needed that will normally have to be agreed upon with the manufacturer of the device.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### Dimensions and characteristics of the human body

Since the main function of the ESPE is to detect the human body or parts of the human body, it should be taken into account its anatomy (fingers, hands, legs), the predictable maximum speed, how it interact with the machine.

The resolution, that is, the detectable minimum object, must be the function of the body part to be protected (eg fingers, hands, legs, arms). Typically, this choice is made by referring to the ESPE manufacturer's catalog or user manual.

### Uses of protective equipment

A protective equipment may be used to provide:

- trip function
- presence sensing function
- combination trip function and presence sensing function

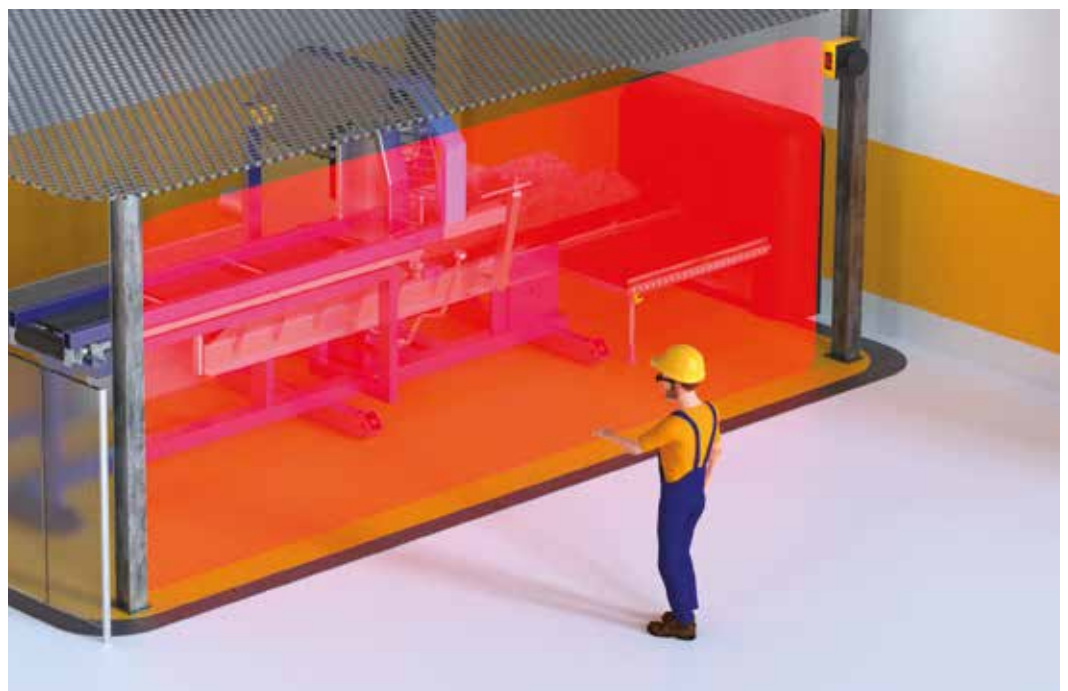
### Use of an ESPE for Trip function

Where the protective equipment is used to provide a trip function, it shall be positioned at a sufficient distance from the specific machine hazard(s) to ensure the machine can stop or otherwise reach a safe condition before any part of an approaching person can reach the hazard zone.

This safety distance shall take into account:







- protective equipment detection capability in relation to human characteristics
- approach speed
- body part penetration/encroachment
- reaching over or under the sensing zone
- possibility of circumvention
- the response time of the ESPE
- the stopping time of the machine measured under the worst operating conditions (maximum load, maximum speed, any factors that may lead to deterioration of the braking performance, low temperatures etc.)
- any reflective surfaces that could, under certain conditions, generate an optical bypass of the beams and consequently prevent the detection of the person


The minimum distance shall be maintained for all foreseeable directions of approach considering also the furthest extension of the moving part towards the direction of approach.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### Definition of type of detection

	DETECTION	CHARACTERISTICS	ADVANTAGES
	Finger or hand 	Detection necessary when the operator must work close to the danger.  Barrier resolution must be between 14 mm and 40 mm	Possibility to lower the dimensions by reducing at the top the space between the protection and the dangerous zone.  Short time for machine charging and discharging.  Less operator fatigue, more productivity.
	Body (use as trip device) 	Ideal detection for access control and protections of several sides, also for long scanning distances.  The barrier must be placed at least at 850 mm from the danger.  Barrier normally composed by 2, 3, 4 beams.	Protection costs reduced by the restricted number of beams.  Possibility to protect zones with big dimensions by using deflection mirrors.  See note below
	Presence in a dangerous zone 	Detection realized by positioning the light curtains horizontally to control continuously the presence of an object in a definite zone.  The light curtains resolution depends on the height of the detection plane, anyway it cannot be higher than 116 mm.	Possibility to control zones not visible from where the machine's push button controls are located.  Possibility of preventing unintended start of the machine while the operator is in the danger zone

 Accidental start-up of the machine shall not be possible when anyone crosses the sensitive area and stays undetected in the dangerous area. Suitable ways of eliminating this type of risk include the following:

- Use of start / restart-interlock function positioning the command so that the dangerous area is in full view and so that the command cannot be reached by anyone from inside the dangerous area. The Restart command has to be safe.
- Use of additional presence sensing detectors for the detection of the operator inside dangerous area.
- Use of obstacles preventing the operator from remaining undetected in the space between the sensing zone of the protective device and the dangerous area.

PHOTOELECTRIC SAFETY LIGHT CURTAINS

Determination of the safety distance

The effectiveness of the protection depends greatly on the correct positioning of the light curtain with respect to the danger.

The light curtain must be located at a distance greater than or equal to the minimum safety distance *S*, so that reaching the dangerous point will be possible only when the dangerous action of the machine has been stopped.

The light curtain must be positioned so that:

- It is impossible to reach the dangerous point without going through the zone controlled by the light curtain.
- A person cannot be present in the dangerous zone without his/her presence being detected. To this end, it might be necessary to resort to additional safety devices (i.e.: photoelectric light curtains arranged horizontally).

European Standard EN ISO 13855 provides the elements for the determination of the safety distance.

If the machine in object is governed by a specific C type Standard, it shall be taken into due account.

If the distance *S* determined in this manner is too big, it is necessary:

- to reduce the total stopping time of the machine,
- to improve the detection capability (resolution) of the light curtain.



Fig. 34. One-side protection



Fig. 35. Three-side protection using deflection mirrors

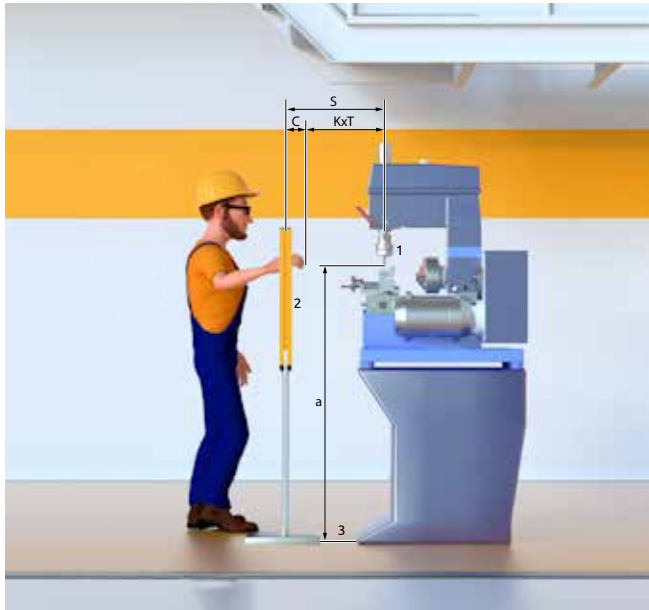
GENERAL FORMULA FOR THE DETERMINATION OF THE MINIMUM SAFETY DISTANCE

$$S = K \times T + C$$

<i>S</i>	minimum safety distance between the protection and hazardous point, expressed in mm.
<i>K</i>	speed of approach of the body or parts of the body, expressed in mm / sec. The K values can be: K = 2000 mm / sec. for safety distance up to 500 mm (forearm movement speed) K = 1600 mm / sec. for safety distance higher than 500 mm (body movement speed).
<i>T</i>	total stopping time of the machine, consisting of: t1 reaction time of the protective device in seconds t2 reaction time of the machine in seconds, until it stops the hazardous action.
<i>C</i>	additional distance in mm.

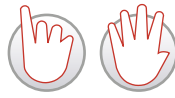
## PHOTOELECTRIC SAFETY LIGHT CURTAINS

DIRECTION OF APPROACH PERPENDICULAR TO THE PROTECTED PLANE WITH  $A=90^\circ (\pm 5^\circ)$



- 1. Hazardous point
- 2. Sensitive area
- 3. Reference plane
- S. Safety distance
- a. Height of the hazardous point

Fig. 36. Scenario 1 - Possibility to reach the hazardous point only through the sensitive area



Light curtains with resolution for the detection of hands and fingers. Light curtains resolution (d): 14 - 20 - 30 - 40 mm

Determination of the minimum safety distance:

$$S = K \times T + C$$

$K = 2000$  or  $1600$  (see following calculations)

$T = t_1 + t_2$  "General formula for the determination of the safety distance" on page 41

$$C = 8 \times (d - 14)$$

$$S = 2000 \times T + 8 \times (d - 14)$$

- the distance S must not be lower than 100 mm
- If the distance S is greater than 500 mm it is possible to re-calculate the distance using  $K=1600$  but in these circumstances, the distance must in no case be lower than 500 mm

$$S = 1600 \times T + 8 \times (d - 14)$$



Light curtains with a resolution for detection of arms and legs. Light curtains resolution (d): 50 - 90 mm

Determination of the minimum safety distance:

$$S = K \times T + C$$

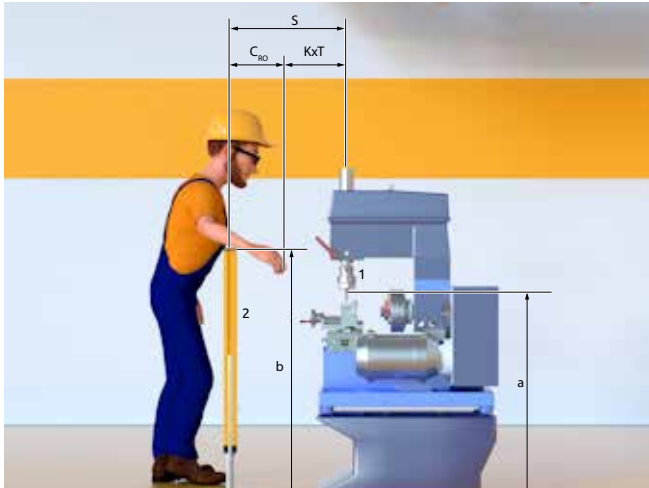
$$K = 1600$$

$T = t_1 + t_2$  "General formula for the determination of the safety distance" on page 41

$$C = 850$$

$$S = 1600 \times T + 850$$

## PHOTOELECTRIC SAFETY LIGHT CURTAINS



- 1. Hazardous point
- 2. Sensitive area
- 3. Reference plane
- a. Height of the hazardous point
- b. Height of the highest beam
- S. Safety distance

Fig. 37. Scenario 2 - Possibility to reach the hazardous point by leaning over the edge of the sensitive area

Possibility to reach the hazardous point by leaning over the edge of the sensitive area

In this case C, called " $C_{RO}$ " is obtained from the following Table 1 of ISO 13855:2010.

Determination of the minimum safety distance:

$$S = K \times T + C_{RO}$$

K = 2000 or 1600 (see following calculations)

T = t1 + t2 "General formula for the determination of the safety distance" on page 41

$C_{RO}$  = see the following Table 1

Note:

- Interpolation is not allowed.
- If distances a, b or  $C_{RO}$  fall between values listed in the table, use the higher.
- $C_{RO}$  (reaching over) calculated using Table 1 of of ISO 13855:2010 must be compared to C as conventionally calculated (see paragraph 1). Always select the higher value.

Height of Hazard zone "a"	Height "b" of upper edge of area protected by photoelectric light curtain											
	900	1000	1100	1200	1300	1400	1600	1800	2000	2200	2400	2600
	Alternative distance $C_{RO}$											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	0
2400	550	550	550	500	450	450	400	400	300	250	100	0
2200	800	750	750	700	650	650	600	550	400	250	0	0
2000	950	950	850	850	800	750	700	550	400	0	0	0
1800	1100	1100	950	950	850	800	750	550	0	0	0	0
1600	1150	1150	1100	1000	900	800	750	450	0	0	0	0
1400	1200	1200	1100	1000	900	850	650	0	0	0	0	0
1200	1200	1200	1100	1000	850	800	0	0	0	0	0	0
1000	1200	1150	1050	950	750	700	0	0	0	0	0	0
800	1150	1050	950	800	500	450	0	0	0	0	0	0
600	1050	950	750	550	0	0	0	0	0	0	0	0
400	900	700	0	0	0	0	0	0	0	0	0	0
200	600	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0

(Table 1 della 13855:2010)

For combined mechanical and electrosensitive protections (as shown), where it would be possible to lean against the



## PHOTOELECTRIC SAFETY LIGHT CURTAINS



- 1. Hazardous point
- 2. Sensitive area
- 3. Reference plane
- a. Height of the hazardous point
- b. Height of the upper edge
- S. Safety distance

Fig. 38. Scenario 3 - Possibility to reach the hazardous point by leaning against the mechanical protection and bypass the light curtain



- 1. Hazardous point
- 3. Reference plane
- S. Safety distance
- Hra. Height of the highest beam
- Hrb. Height of the lower beam

Fig. 39. Scenario 1 - Possibility to reach the hazardous point only through the sensitive area. Light curtains with 2, 3, 4 beams

### mechanical protection and bypass the light curtain

For the calculation of the parameter C should use

- Table 1 (for low risk applications) or
- Table 2 (for high-risk applications)

of ISO 13857:2007 (formerly EN 294) in place of the table on the previous page.

In this catalog the two tables of ISO 13857:2007 (formerly EN 294) - Safety distances to prevent danger zones being reached by upper and lower limbs - are not mentioned.



Light curtains for the detection of the presence of the body in a dangerous area. Light curtains with 2 - 3- 4 beams

Determination of the minimum safety distance:

$$S = K \times T + C$$

K = 1600

T = t1 + t2 "General formula for the determination of the safety distance" on page 41

C = 850

$$S = 1600 \times T + 850$$

Note for 2 beams light curtains:

- H lower beam = 400 mm (can be used if allowed by risks analysis).
- H higher beam = 900 mm

Note for 3 beams light curtains:

- H lower beam = 300 mm
- H middle beam = 700 mm
- H higher beam = 1100 mm

Note for 4 beams light curtains:

- H lower beam = 300 mm
- H middle beam 1 = 600 mm
- H middle beam 2 = 900 mm
- H higher beam = 1200 mm

Height of the beams from the reference plane (eg. floor).

## PHOTOELECTRIC SAFETY LIGHT CURTAINS



- 1. Hazardous point
- 2. Sensitive area
- 3. Reference plane
- a. Height of the hazardous point
- x. Distance between end of the detection zone and machine edge
- S. Safety distance
- H. Height of the sensitive area

Fig. 40. Horizontal light curtains for presence control in a dangerous area

Direction of approach parallel to the protected plane with  $\alpha=0^\circ (\pm 5^\circ)$



Horizontal light curtains for presence control in a dangerous area

Determination of the minimum safety distance:

$$S = K \times T + C$$

$$K = 1600$$

$T = t_1 + t_2$  "General formula for the determination of the safety distance" on page 41

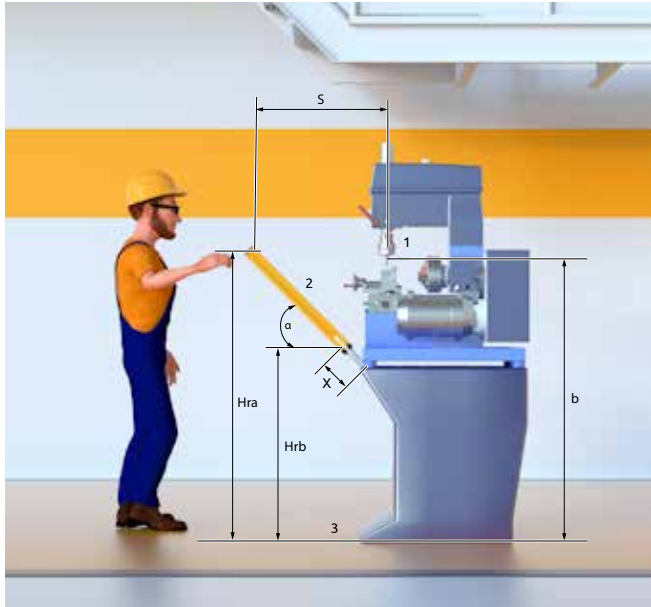
$$C = 1200 - (0,4 \times H)$$

$$S = 1600 \times T + (1200 - 0,4 \times H)$$

Note:

- $C = 1200 - (0,4 \times H)$  must be equal to or greater than 850 mm
- The maximum height allowed is:  $H_{max} = 1000$  mm
- The height  $H$  depends on the resolution  $d$  of the light curtains and is determined through the following formula:  
 **$H = 15 \times (d - 50)$**
- This formula can also be used to determine the maximum resolution that can be used at the different heights  
 **$d = H / 15 + 50$**
- For example, the maximum resolution limits will be:  
for  $H = 1000$  mm  $d = 116$  mm  
for  $H = 0$  mm  $d = 50$  mm
- If  $H$  is greater than 300 mm, at the stage of risk assessment it becomes necessary to take into consideration the possibility of access from beneath the beams
- When using the light curtain as a combination of trip and presence sensing device, the distance  $x$  must be less than or equal to the detection capability

## PHOTOELECTRIC SAFETY LIGHT CURTAINS



- 1. Hazardous point
- 2. Sensitive area
- 3. Reference plane
- a. Height of the hazardous point
- S. Safety distance
- x. Distance between end of the detection zone and machine edge
- Hra. Height of the highest beam
- Hrb. Height of the lower beam

direction of approach angled to the protected plane with  $5^\circ < \alpha < 85^\circ$



Slanted light curtains to detect hands and arms and for presence control in the dangerous area

With angle  $\alpha > 30^\circ$  refer to the case of "Approach perpendicular to the protected plane". (Previous case).

With angle  $\alpha < 30^\circ$  refer to the case of "Approach parallel to the protected plane". (Previous case page 45).

Note:

- The distance S refers to the beam farthest away from the hazardous point
- The height of the beam farthest away from the hazardous point must not be greater than 1000 mm
- For the determination of height H or resolution d apply the following formulas to the lowermost beam:  

$$H = 15 \times (d - 50)$$

$$d = H / 15 + 50$$
- When using the light curtain as a combination of trip and presence sensing device, the distance x must be less than or equal to the detection capability.

Fig. 41. Possibility to reach the hazardous point only through the sensitive area



When calculating the safety distance, also consider installation tolerances, accuracy of the measured response time and possible decay of the brake system performance of the machine.

It is advisable to increase the calculated value by at least 10% in order to take into account installation tolerances, accuracy in response time and possible degradation of brake system performance.

As can be seen from the formulas, the total stopping time plays an important role in calculating the safety distance; When a deterioration in braking time is expected, a Stopping Time monitoring device (SPM) is required. Checking of the stopping time is not necessary when:

- The system is very reliable and not subject to deterioration
- The machine is only rarely stopped
- Effective preventive control of the braking systems of the machine is implemented.

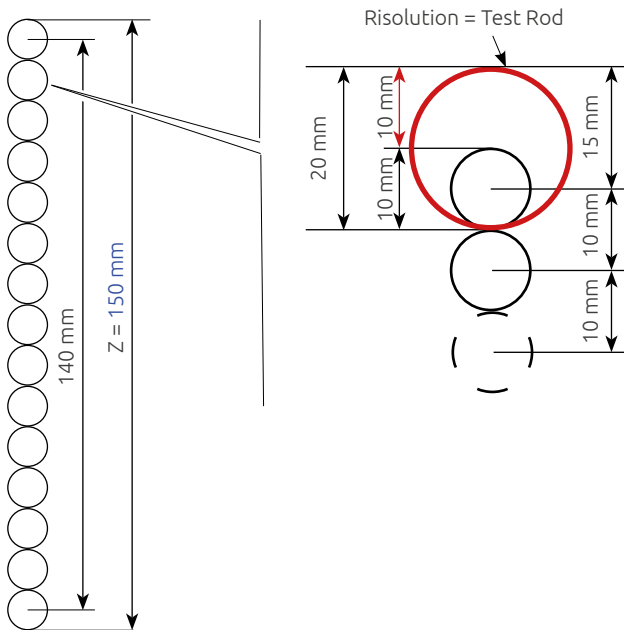


## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### Light curtains protected height - Determination criteria

The following calculation, for the correct definition of the light curtains protected height are related to these models of light curtains:

- model: EOS 152 A
- Nominal protected height: 160 mm
- Resolution: 20 mm
- Numbers of beams: 15
- Lens diameter: 10 mm



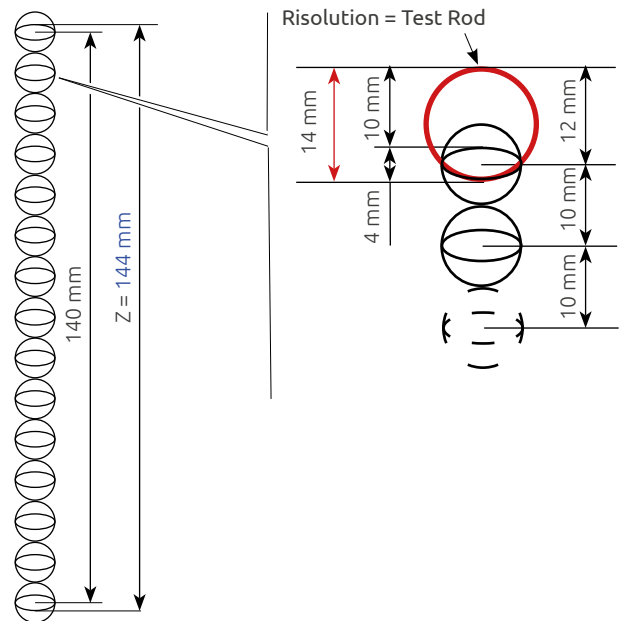
In order to keep in account the dimension of the "Test Rod" (resolution), it is necessary to add 10 mm for each side to the Z dimension.

Protected height =  $150 + 10 + 10 = 170$  mm.

This value is conventionally rounded to 160 mm (Nominal protected height).

We can use the same nominal protected height value (160 mm) for all other resolutions.

- model: EOS 151 A
- Nominal protected height: 160 mm
- Resolution: 14 mm
- Numbers of beams: 15
- Lens dimensions: 10 x 4 mm



In order to keep in account the dimension of the "Test Rod" (resolution), it is necessary to add 10 mm for each side to the Z dimension.

Protected height =  $144 + 10 + 10 = 164$  mm.

This value is conventionally rounded to 160 mm (Nominal protected height).

You can see that we can use the same nominal protected height value (160 mm) also for the 14 mm resolution.

### Using the ESPE as a presence sensing device

The main function of a protective device used for presence sensing is to keep the machine in a safe state as long as a person or part of it is within its sensing area.

The sensing area must therefore be configured so as not to allow for a person to remain within the hazardous area or to a distance below the stated safety distance without being detected.

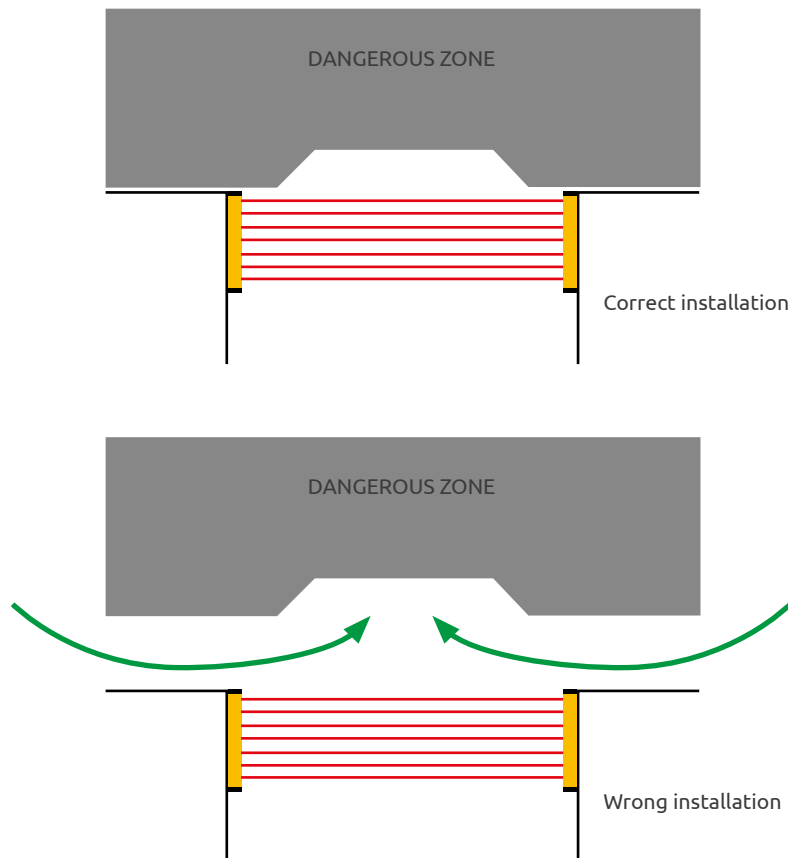
If the ESPE only performs the presence sensor function, it must be used in combination with other safety measures (eg interlocked shield or crossover sensor) to ensure that the machine is in a safe state before it is possible access it.

## PHOTOELECTRIC SAFETY LIGHT CURTAINS

In dimensioning the protected area, additional protective measures shall be implemented in addition to computing the safety distance, to prevent that a person can circumvent the protected area.

It shall not be possible to reach the dangerous area by climbing on the machine or crawling below the sensitive area or leaning over the edge of the sensitive area.

The parts of the machine not guarded by the ESPE, shall be protected by means of solid repairs (e.g. interlocked guards if can be removed to allow access for maintenance).



Unexpected start-up of the machine shall be prevented after a person has passed through the detection zone of the trip device to the hazardous zone of the machine.

Suitable methods are:

- barriers to ensure that a person cannot approach the machine hazard from directions not protected by the protective equipment
- provision of a restart interlock
- provision of a presence sensing device
- measures to prevent a person being present between the protective equipment and the hazardous zone.

## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### Muting function

The Muting function is the provisional and automatic cut-out of the light curtain protective function in relation to the machine cycle. Muting can only occur in a safety condition. Two types of applications are envisaged:

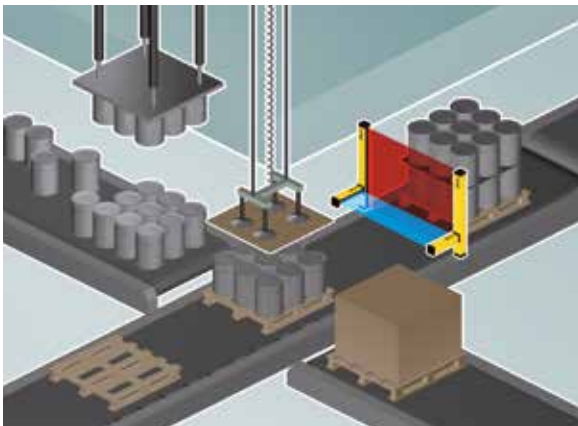
1. Enabling personnel access inside dangerous area during the non-dangerous part of machine cycle.



Example: Positioning or removal of workpiece

Depending on the position of the tool, which is the most dangerous part, one of the two curtains (the one facing the tool working area) is active whereas the other is in Muting mode to enable the operator to load/unload the workpiece. Muting mode of the light curtains is subsequently reversed when the tool works on the opposite side of the machine.

2. Enabling access to material and preventing access to personnel.



Example: Pallet exit from dangerous area

The safety light curtain incorporates Muting sensors able to discriminate between personnel and materials. Only the material is authorized to pass through the monitored area.

The essential requirements regarding the Muting Function are described by the followings Standards:

**IEC TS 62046** "Application of the protective equipment to detect the presence of persons"

**EN 415-10** "Safety of the Machinery - automatic palletizing systems"

**IEC 61496-1** "Electro-Sensitive Protective Equipment"

General Requirements:

- Muting is a temporary suspension of the safety-related function and it must be activated and de-activated automatically.
- The safety integrity level of the circuit implementing the Muting function shall be equal to that of the safety function temporarily suspended, so that the protection performance of the entire system is not adversely affected.
- Muting should be activated and de-activated only by means of two or more separate and independent hardwired signals triggered by a correct time or space sequence. Such that a signal fault cannot be considered a muting condition.
- It shall not be possible to trigger Muting while the ESPE outputs are in the off state.
- It shall not be possible to initiate Muting by turning the device off and then on again.
- Muting shall be only activated in an appropriate point of the machine cycle, i.e. only when there is no risk for the operator.
- Muting sensors shall be mechanically protected to prevent mismatch in case of impact.

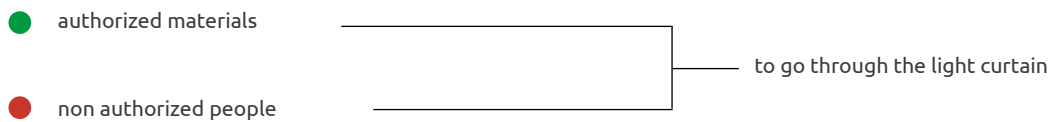
## PHOTOELECTRIC SAFETY LIGHT CURTAINS

### MUTING: palletizers and materials handling systems

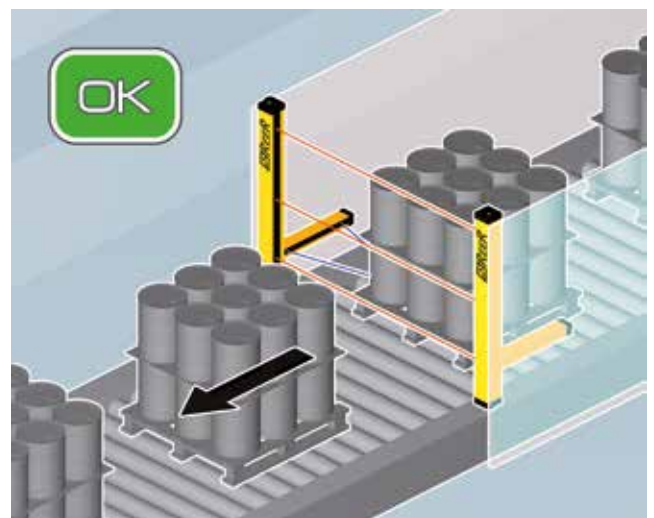
Requirements for the monitoring of the openings:

- Monitor the load, not the pallet, otherwise the operator might go into the hazardous zone being dragged by the pallet.
- Muting time must be restricted to the actual time taken by the material to pass through the opening.
- Muting must be time-restricted.
- Sensor mismatch with effect similar to their actuation shall not allow a condition of permanent Muting.
- The configuration and positioning of the Muting sensors shall ensure reliable differentiation between personnel and material.
- The layout of the opening, the positioning of the Muting sensors and the additional side protections shall prevent personnel access to the dangerous area for all the time the Muting function is activated and throughout the time the pallet crosses the opening.

Therefore it is necessary to realise a safety system able to distinguish between:



The Muting function can be present on both type 2 and type 4 safety light curtains.

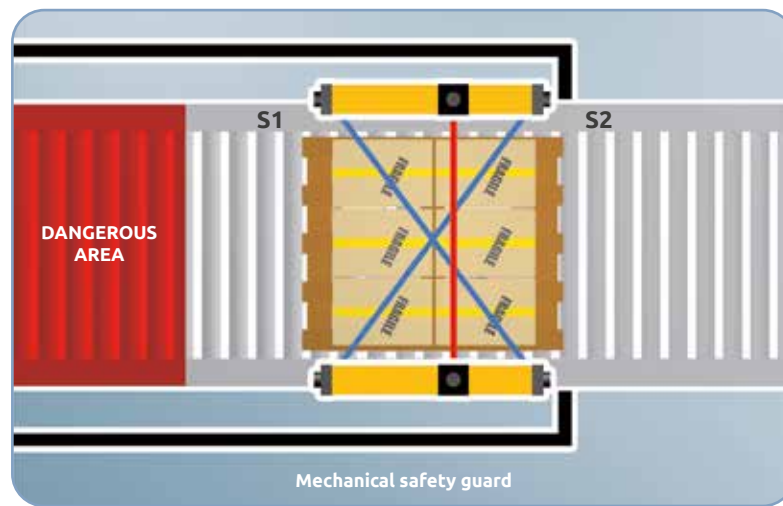


## PHOTOELECTRIC SAFETY LIGHT CURTAINS

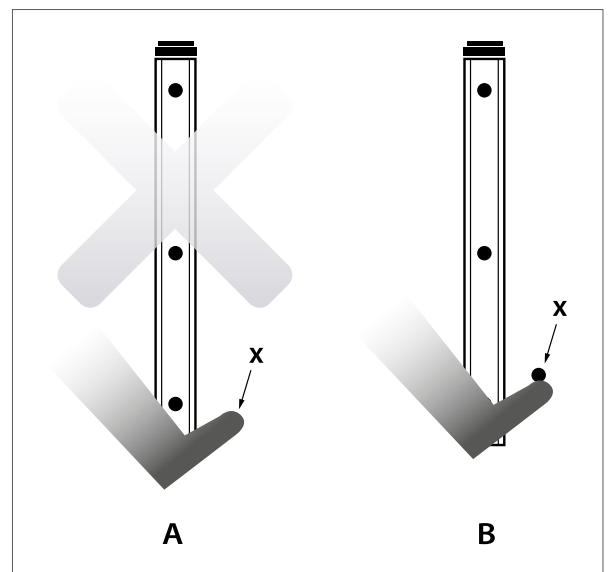
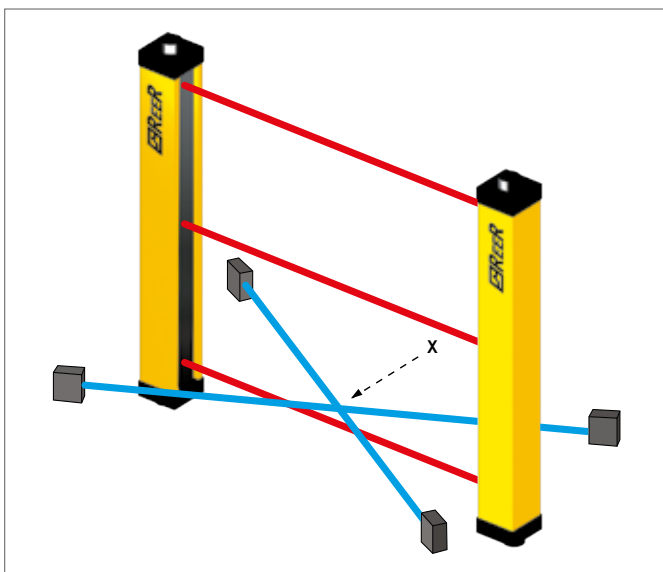
### Common solutions for Muting sensor positioning

Muting with 2 crossed-beam sensors – Configuration type T with timing monitoring and two-way pallet operation:

- The point of intersection of the two beams shall lie in the segregated dangerous area beyond the light curtain.
- A fail safe timer shall be provided to restrict Muting to the time needed for the material to cross the opening.
- The Muting function shall be activated only if the Muting sensors are contemporaneously intercepted: ( $t_2(S_2) - t_1(S_1) = 4 \text{ seconds max.}$ ).
- The two beams shall be continuously interrupted by the pallet throughout the transit through the sensors.
- A matt cylindrical object  $D=500 \text{ mm}$  (simulating the size of a human body) shall not trigger the Muting function.



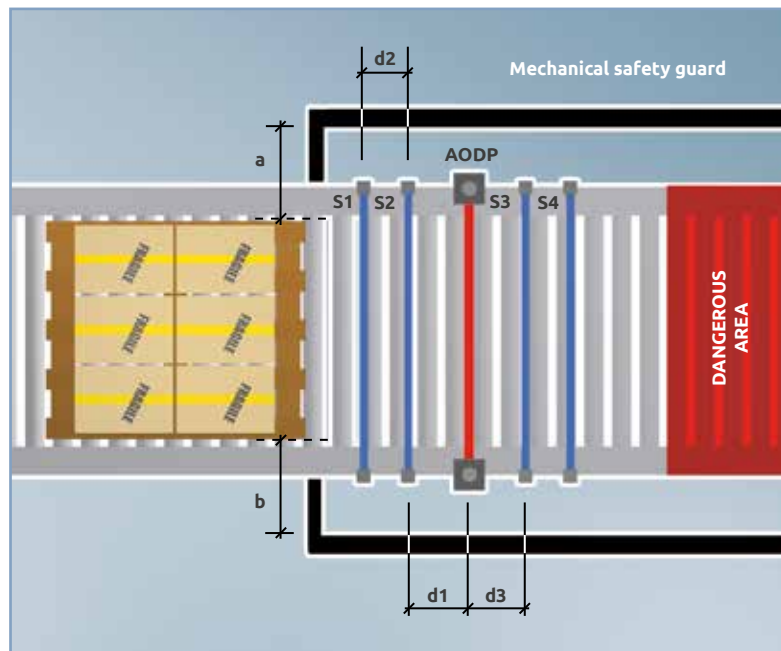
Muting sensor beam intersection shall be positioned the higher up or equal than level of the lower light curtain beam to avoid possible tampering or accidental triggering of Muting.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

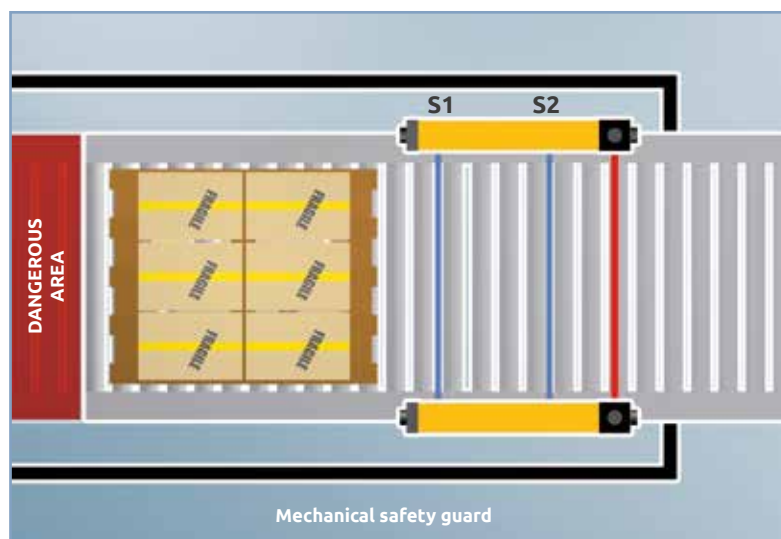
Muting with 4 parallel-beam sensors – Configuration type T with timing and/or sequence monitoring - Two-way pallet operation:

- The 4 Muting sensors shall be all actuated together for a brief moment (sequential actuation and de-activation of the 4 sensors).
- The distance between sensors and the sensing field of the light curtain shall be:
  - $d1$  and  $d3 < 200$  mm to prevent undetected personnel access by preceding or following immediately after the pallet during Muting.
  - $d2 > 250$  mm to prevent personnel limb, garment, etc. from enabling Muting by triggering two sensors simultaneously.



Muting with 2 crossed-beam or parallel-beam sensors – Configuration type L with timing monitoring and one-way only(exit from dangerous area) pallet operation:

- Muting sensors shall be positioned beyond the light curtain in the dangerous area.
- Muting shall be disabled as soon as the light curtain is cleared and not later than 4 seconds max. from the instant the first of the two Muting sensor is cleared. The timer monitoring the 4 seconds shall be a safety-related item.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

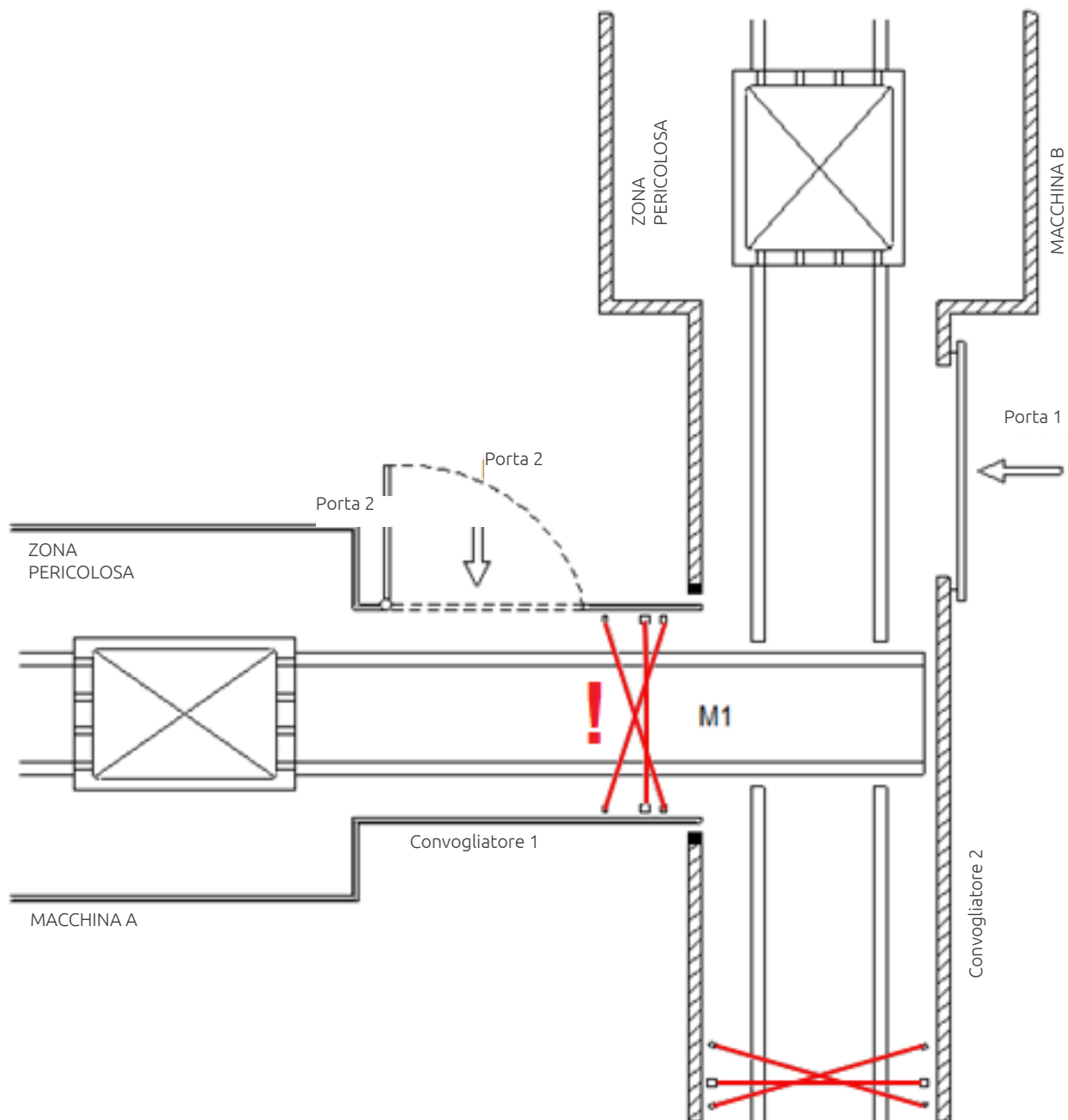
### Protection of two transport systems operating in a coordinated way

The example shows a part of a production line comprising two machines, A and B, and two transport lines. The pallets move from the dangerous area associated with conveyor 1 to the dangerous area associated with conveyor 2.

The M1 Muting system with two T-shaped sensors allows pallets to pass from conveyor 1 to conveyor 2.

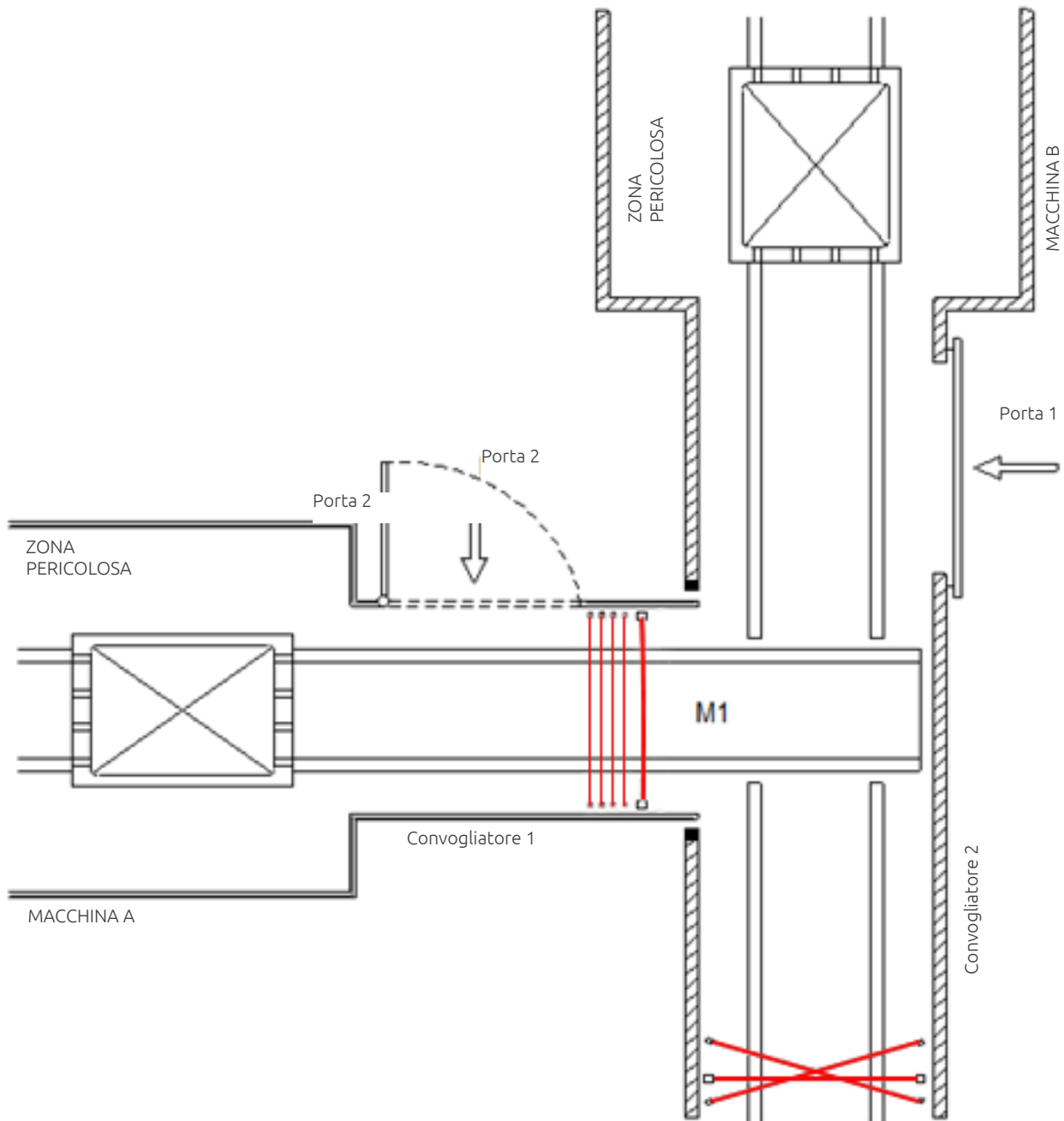
If the operator opens door 1, the dangerous area associated with machine B is made safe while the Muting system M1 will prevent the operator from accessing the dangerous area associated with machine A.

If the operator opens door 2 instead, the dangerous area associated with machine A is made safe, but the system of Muting M1 cannot provide any protection to the operator if he tries to reach the dangerous area associated with Machine B by passing on the transport system since the operator can activate the Muting before having interrupted the sensitive area of the barrier, for example by passing at the point of intersection of the two muting sensors. The Muting system with two T-sensors is therefore not suitable.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

For this application it is necessary to use a four sensor muting system with timing or sequence control.



The barriers with 4 muting sensors with parallel beams:

- allow the bidirectional transit of pallets between one machine and another
- they do not activate muting and if a person tries to cross the protected passage in both directions.



## PHOTOELECTRIC SAFETY LIGHT CURTAINS

## Blanking function

Blanking is an auxiliary function of safety light curtains for which the introduction of an opaque object inside parts of the light curtain's protection field is allowed without causing the stoppage of the machine. Blanking is only possible in the presence of determined safety conditions.

The blanking function is therefore particularly useful when the light curtain's protection field must be inevitably intercepted by the material being worked or by a fixed or mobile part of the machine.

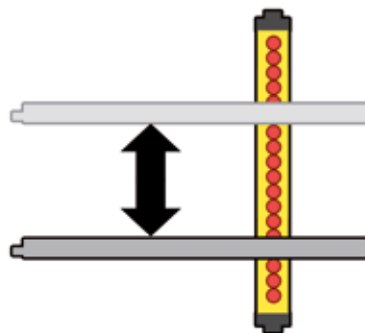
In practice, it is possible to keep the light curtain's safety outputs in an ON condition, and the machine working, even if a pre-determined number of beams within the protection fields are being intercepted.

**Fixed Blanking** allows a fixed portion of the protection field (i. e. a fixed set of beams) to be occupied, while all the other beams operate normally.

**Floating Blanking** allows the object to move freely inside the light curtain's protection field occupying a given number of beams, at the condition that the occupied beams are adjacent and that their number is not higher than the configured one.

**Floating Blanking with compulsory object presence** makes the light curtain work in a reverse way within the blanked portion of the protection field. That is, the blanked beams must be occupied during blanking and therefore the object has to be inside the protection field for the light curtain to remain in the ON state. In this case too the object can move freely within the protection field if the above conditions are respected.

Requirements for the blanking function can be found in the Technical Specification IEC/TS 62046 describing additional means required to prevent a person from reaching into the hazard through the blanked areas of the detection zone.

**WARNING!**

*The use of the blanking function can be allowed depending on the characteristics of the application to be protected. Based on the risk analysis of your application, check whether the use of the blanking function is allowed for that particular application and with what features.*

*The use of the blanking function may need a recalculation of the safety distance due to the modified detection capability.*

## SAFETY LASER SCANNER

### Characteristic elements

The Laser scanner (Active Opto-electronic Protective Device responsive to Diffuse Reflection) measures the distance between the objects that fall into its sensing field by means of the small fraction of energy that is re-diffused by the objects themselves in axis with the direction of emission.

AOPDDRs do not need a cooperating target for their operation, especially where the protected area is mobile, as is the case with AGVs, or where it is necessary to vary the position and size of the protected area during the production process

For [EN 61496-3](#), Laser Scanners must be classified in accordance to type 3 or lower safety sensors.

For [IEC 61508](#), [IEC 62061](#), [ISO 13849-1](#), they must be used to realize safety functions up to SIL 2 - PL d or lower.

Using the Safety Laser Sensor, precise programmable horizontal protected areas of variable shape can be created (i. e. semi-circular, rectangular or segmented), suitable for all applications with no need of a separate reflective or receiving element.

It is also possible to use the Laser Scanner in a vertical position for the access protection to a dangerous area, in that case detection of the edge of the gate is mandatory ([IEC TS 62046](#)).



Any person or object entering or remaining in the safety zone during survey causes, through the self-monitored static safety outputs of the device, an emergency stop command to the control system of the protected machine. The machine's hazardous movement will thus be interrupted.

If the warning zone is instead occupied, thanks to a non-safety dedicated solid state output, a signal is sent to the machine control system, which can be used to activate a light or a sound signal in order to prevent operators to break into the safety zone and stop the machine. Or, on an AGV application, the warning signal can be used to slow the vehicle down, so that a possible further break of the safety zone will not force it to stop abruptly, thus reducing the mechanical wear of the AGV.

The profiles of the controlled areas, as well as all the other configurable parameters, are programmable through a dedicated user interface software, installed on a laptop or PC and connected with the scanner via a serial interface.

The Laser Scanner is also able to automatically detect the controlled area by means the teach-in function.

## SAFETY LASER SCANNER

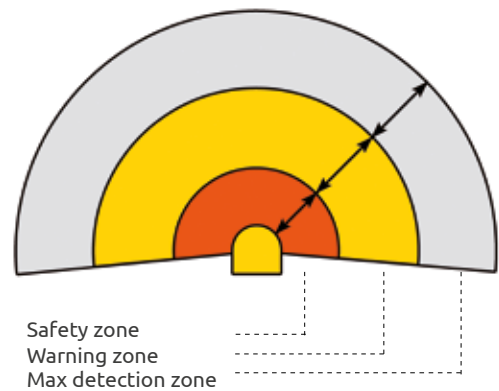
### Controlled areas

#### Safety zone

This is the effective protection zone, in which the laser scanner assures the detection of any obstacle having a minimum reflectivity to infrared light of 1.8%. This means any human body in any possible clothing.

The occupation of this zone causes the switching of the two safety outputs that control the emergency stopping of the machine.

The shape of the zone can be programmed according to the application requirements.



#### Warning zone

This is the zone in which the laser scanner is able to detect the presence of an obstacle approaching the safety zone.

The occupation of this zone causes the switching of the auxiliary output that can be used to activate light or sound signals or in order to slow down the hazardous movement.

This zone is generally larger than the safety zone. In this case also the shape of the zone can be programmed according to the application requirements.

#### Advantages of the laser scanner

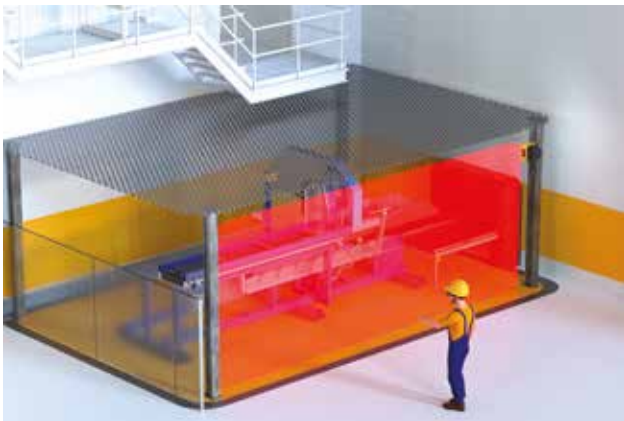
- No receiving and reflecting elements
- Simple programming of differently-shaped controlled areas
- Monitoring and protection of large areas
- Horizontal mount for the detection of the body in a dangerous area
- Vertical mount for the detection of hands and arms or for the detection of the body in access control
- Use on moving vehicles (AGVs)
- Measurement of object size, shape and position
- Fast and reliable installation

### Applications



#### Area control

Example of an horizontally mounted protective field permanently monitored by Pharo. In this way a larger area can be monitored through the detection of the lower limbs of the body.



#### Access control

If the controlled plane is installed in a vertical position, even very large accesses can be protected. Hands, arms or the whole body can be detected, depending on the chosen resolution.

Note: the contour detection is mandatory for the vertical mount / accesscontrol applications.



#### Protection of Automatic Guided Vehicles (AGV)

The vast size of the controlled area allows the AGV to travel at higher speeds with respect to bumper protection.

The warning area permits speed reduction in the presence of obstacles.

The data measured by the sensor can be sent to the vehicle on the serial interface and used as navigation aid.

#### Dimensional measurement

The sensor is first of all a measurement device. Therefore, the measurement data of the surrounding environment, which are always available during operation, can also be used for object profile, position and dimensions measurement in industrial automation.

## CONTACTLESS SAFETY SENSORS

### RFID safety sensors

The RFID technology enables Magnus RFID sensors to be individually coded in three different ways to allow the appropriate tampering protection in all applications. The highest configurations allow each sensor to be paired with one only assigned actuator.

The RFID technology used allows to reach safety levels up to PL e / SIL 3 (EN ISO 13849-1 directive) also when connecting the sensors in series.



### Magnetic safety sensors

Magnus series safety switches can be connected to Mosaic safety configurable controller (PL e) or to the dedicated safety control unit MG d1 (PL d).

MG switches connected to Mosaic safety controller form a certified PL e safety system.



### Inductive safety sensors

A complete range of sensors for position detection.

- Certified according to the EN 60947-5-3 standard
- It guarantees the safety of people and machinery
- It does not require a specific actuator
- Connecting sensors to interfaces, controllers or Safety PLCs (for example: AD SR1, Mosaic)

All the models in the range reach the safety level PL d / SIL2.

The PI M30 NF K model reaches safety level PL e / SIL3



## GUARD LOCK AND GUARD INTERLOCK DEVICES

### Safety switch with guard locking

Interlocking device (ISO 14119:2013, § 3.1) - Mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions (generally as long as a guard is not closed).

The reference standard is EN 14119. The standard emphasizes the fact that the interlock function and the lock function are two separate safety functions, with PLR that can also be different. Often the safety level required for the interlock function is lower than that required for the interlock function.

As an example, we will analyse the protection of a machine's dangerous movement through a perimeter protection gate by carrying out a risk analysis (simplified) according to EN 13849.



A tree type graph of decisions is used to find the contribution to risk reduction that must be provided by the safety related function, leading to univocal identification of PL r. If more than one safety-related function are identified, PL r shall be identified for each of them.

#### Interlock safety related function

1. When the gate opens, the dangerous movement must be stopped and remain still.
2. Referring to the graph above, In case of accident, we assume that:
  - The injury that can be generated is irreversible,  $S_2$
  - Frequency exposure to hazard is continuous (Machine always in run),  $F_2$
  - Possibility of limiting the damage is low and the risk is unavoidable in case of unexpected start of the machinery,  $P_2$ .

Then, the required Performance Level (PL r) of the interlock safety function must be PL e.

#### Lock safety related function

We have also to consider the machinery inertia. The safety distance (calculated according to EN 13855) is greater than the distance between the gate and the dangerous area. In this case, it is possible to open the gate and reach the machinery still in motion. For this reason, it is advisable to use a lock device that locks the gate safely, preventing entry until the machinery is moving.

Therefore, safety systems able to perform this function must be used. For example:

- Safety speed monitoring able to check the stand still of the moving parts before allowing the gate or guard opening
- Authorize opening only after a delay following a stop command.

Therefore we have a new safety function, the gate or guard lock

Always using the previous page graph, we analyze the risks even for the lock function. Let's assume that:

1. The injury that can be generated is irreversible,  $S_2$
2. Frequency exposure to hazard is rare (entry into dangerous zone is rare),  $F_1$
3. Possibility of limiting the damage is high and the risk is avoidable,  $P_1$ . This for two reasons:
  - The operator can see the dangerous movement of the machinery (humane behavior) and decide to not entry
  - Very reliable systems to control the movement of the machine are used (Safety speed monitor, Safety PLC....)

Then, the required Performance Level (PL r) of the lock safety function must be PL c.



## GUARD LOCK AND GUARD INTERLOCK DEVICES

### Safety levels

In this type of device, a single failure resulting in the loss of the safety function. Typically mechanical breakage of the actuator tongue or some other part of the mechanical connection. Therefore, a single mechanical failure can compromise the safety of the gate or guard or can it may cause a transmission error. The contacts transmit an incorrect signal about the state of closure or opening of the gate or guard.

The lock interlock safety function of these devices is (in general) of category Cat. 1:

- There is no redundancy, therefore Cat. 4 and Cat. 3 must be excluded. The single fault resulting in the loss of the safety function
- Cat. 2 is impractical because it is impossible to test the functioning of the mechanical retention
- Cat. 1 can only be reached thanks to the reliability of the components (high MTTF<sub>d</sub>)
- From ISO 13849-1 - Table 5, we can see that the safety levels PL c and PL d correspond to Cat. 1.

### How to increase the safety level of the interlock function?

To increase the safety level of this function there are several alternatives:

- **Redundancy**, i.e. duplicating the interlocking device (electromechanical)
- Again to obtain redundancy, we can combine the electromechanical device with a more refined technology sensor, for example an RFID sensor, to be used as an interlocking device.
- **Fault exclusion**, i.e. carry out a detailed analysis of all dangerous failures and take measures to exclude all cases in which they can occur. With this method, using only one device, it is possible to reach Cat. 3 / PL d (PL e does not plan to use the fault exclusion). It is a complex activity that must be carried out according to EN 13849-1 / 2 and justified in all its aspects.

Let's summarize these concepts now with an example based on ReeR products.

- Safelock Safety switch with guard locking and electromagnetic lock
- Magnus RFID Contactless RFID sensor with OSSD outputs used as interlock sensor
- Magnus Contactless magnetic Reed sensor with 2 N.O. contacts used as interlock sensor
- Safety realys (ADSR3, ADS4, AD SR1)
- MOSAIC Safety controller

Lock function Category / Safety level	Interlock function Category / Safety level	Coding	Devices
Up to Cat. 1 / PL c (Note)	Up to Cat. 1 / PL c	Low	Safelock + PL d safety interfaces for emergency stop buttons and safety switches ADSR3 or 1 Mosaic input
Up to Cat. 1 / PL c (Note)	Up to Cat. 3 / PL d	Low	Safelock + PL d safety interfaces for emergency stop buttons and safety switches ADSR3 or 2 Mosaic inputs + Fault exclusion (note)
Up to Cat. 1 / PL c (Note)	Up to Cat. 4 / PL e	High	Safelock + Magnus + 2 PL e safety interfaces for emergency stop buttons and safety switches ADSR4 or 4 Mosaic inputs
Up to Cat. 1 / PL c (Note)	Up to Cat. 4 / PL e	High	Safelock + Magnus RFID + Safety relay AD SR1 or 2 Mosaic inputs (only for Magnus)
Up to Cat. 4 / PL e	Up to Cat. 3 / PL d	Low	2 Safelock + PL d safety interfaces for emergency stop buttons and safety switches ADSR3 or 2 + 1 Mosaic inputs (FBK needed)
Up to Cat. 4 / PL e	Up to Cat. 4 / PL e	Low	2 Safelock + 2 PL e safety interfaces for emergency stop buttons and safety switches ADSR4 or 4 + 2 Mosaic inputs (FBK needed)

(Note) Cat. 3 / PL d can be reached through fault exclusion. The exclusion of faults is allowed according to point 7.3 of EN ISO 13849-1 of which an extract is reported.

## SELECTION GUIDE



	EOS 4 A	EOS 4 X	ADMIRAL AD	ADMIRAL AX	ADMIRAL AX BK
Sensor	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain
Safety level	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e
Resolution (mm)	14	14	14	14	14
Controlled area heights (mm)	160 ... 1960	160 ... 1960	160 ... 1810	160 ... 1810	160 ... 1810
Max. range (m)	6	6	5	5	5
Start/Restart interlock integrato	-	yes	-	yes	-
EDM integrato	-	yes	-	yes	-
Blanking	-	-	-	-	yes, floating
Versioni Master/Slave	-	yes (1/2 slave)	-	yes (1 slave)	yes, master



	EOS 4 A	EOS 4 X	SAFEGATE SM - SMO	SAFEGATE SMPO	ADMIRAL AD	ADMIRAL AX	ADMIRAL AX BK	JANUS M
Sensor	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain
Safety level	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e	Type 4 SIL 3 – PL e
Resolution(m)	20, 30, 40	20, 30, 40	30, 40	30, 40	20, 30, 40	20, 30, 40	20, 40	30, 40
Controlled area heights(mm)	160 ... 2260	160 ... 2260	310 ... 2260	310 ... 2260	160 ... 2260**	160 ... 2260**	160 ... 2260**	310 ... 1810
Max. range (m)	12 or 20	12 or 20	4 or 12	4 or 12	18	18	18	16 or 60
Start/Restart Interlock	-	yes	yes	yes	-	yes	-	yes
EDM	-	yes	yes	yes	-	yes	-	yes
Blanking	-	-	-	-	-	-	yes, floating	-
Muting	-	-	yes	yes	-	-	-	yes
Master, Slave	-	yes (1/2 slave)	-	-	-	yes (1 slave)	yes master	-
Integrated Muting lamp	-	-	SMO model	yes	-	-	-	-
Programmable	-	-	-	yes	-	-	-	-
TRX version with pas-seive elment	-	-	yes	yes	-	-	-	yes
Long Range	-	-	-	-	-	-	-	yes (up tp 60 m)



\*\* Are available, on request, ADMIRAL series safety light curtains (AX, AD and AX BK models) with protected height up to 2260 mm. Resolutions (30 mm, 40 mm, 50 mm and 90 mm).

In detail the new protected heights are: 1960 mm, 2110 mm and 2260 mm.

Master and Slave models are not available for these new heights.

\* VISION VXL and VISION MXL 30 mm resolution models: maximum controlled area height 1210 mm.

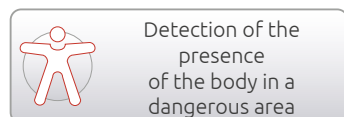




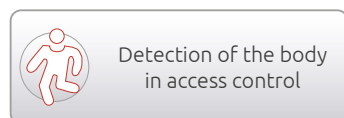
Finger detection



Hand detection



Detection of the presence of the body in a dangerous area



Detection of the body in access control

### GLOSSARY

Start/Restart interlock	Interlock function (manual restart required) at machine start or restart.
EDM	External Device Monitoring: controls the switching of external contactors via feedback input.
Master/Slave	Two or three light curtains can be connected in cascade; all the outputs are managed by only one of these (Master).
Blanking	The light curtain can be programmed to ignore a single object of defined dimensions that may also be greater than the resolution (see "Blanking function")
Muting	The protective function of the light curtain can be inhibited under certain safety conditions (see "Muting function")
Modelli I	Models with connections for external Muting sensors
Modelli L, T	Models with built-in Muting sensors in pre-assembled kits for pallet outfeed only (L) or infeed/outfeed (T).

JANUS J	LASER SCANNER UAM	LASER SCANNER PHARO	EOS 2 A	EOS 2 X	VISION V	VISION VX	VISION VXL	VISION MXL
Light curtain	Laser scanner	Laser scanner	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain
Type 4 SIL 3 – PL e	Type 3 SIL 2 – PL d	Type 3 SIL 2 – PL d	Type 2 SIL 1 – PL c	Type 2 SIL 1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c
40	30, 40, 70 select.	30, 40 select.	30, 40	30, 40	20, 30, 40	20, 30, 40	30, 40	30, 40
610 ... 1210	-	-	160 ... 2260	160 ... 2260	160 ... 1810	160 ... 1810	160 ... 1810*	160 ... 1810*
16 or 60	5 (radius)	2,6 (radius)	12	12	16	18	8	8
yes	yes	yes	-	yes	-	yes	yes	yes
yes	yes	yes	-	yes	-	yes	yes	yes
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	yes
-	-	-	-	yes (1/2 slave)	-	yes (1 slave)	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-
yes	-	-	-	-	-	-	-	-
yes (up to 60 m)	-	-	-	-	-	-	-	-

## SELECTION GUIDE



	EOS 4 A	EOS 4 X	ADMIRAL AD	ADMIRAL AX	ADMIRAL AX BK	JANUS M	JANUS J
Sensor	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain
Safety level	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e
Resolution (mm)	50, 90	50, 90	50, 90	50, 90	40, 90	40, 90	40
Controlled area heights(mm)	160 ... 2260	160 ... 2260	310 ... 2250**	310 ... 2250**	310 ... 2250**	310 ... 1810	610 ... 1210
Max. range (m)	12 or 20	12 or 20	18	18	18	16 or 60	16 or 60
Start/Restart interlock	-	yes	-	yes	-	yes	yes
EDM	-	yes	-	yes	-	yes	yes
Blanking	-	-	-	-	yes, floating	-	-
Muting	-	-	-	-	-	yes	-
Master/Slave	-	yes (1/2 slave)	-	yes (1 slave)	yes (master)	-	-
Long Range	-	-	-	-	-	yes (up to 60 m)	yes (up to 60 m)



	EOS 4 A	EOS 4 X	SAFEGATE SM - SMO	SAFEGATE SMPO	ADMIRAL AD	ADMIRAL AX	JANUS M	JANUS J
Sensor	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain	Light curtain
Safety level	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e	Type 4 SILCL3 – PL e	Type 4 SILCL3 – PL e	Type 4 SIL 3 – PL e	Type 4 SIL 3 – PL e
Number of beams	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4
Resolution (mm)	-	-	-	-	-	-	-	-
Controlled area heights(mm)	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910
Max. range (m)	12 or 20	12 or 20	4 or 12	4 or 12	18	18 or 60	16 or 60	16 or 60
Start/Restart interlock	-	yes	yes	yes	-	yes	yes	yes
EDM	-	yes	yes	yes	-	yes	yes	yes
Muting	-	-	yes	yes	-	-	yes, I, L and T models	-
Master/Slave	-	yes (1/2 slave)	-	-	-	yes	-	-
Integrated Muting lamp	-	-	SMO Model	yes	-	-	-	-
Programmable	-	-	-	yes	-	-	-	-
TRX versions with passive retroreflector elements	-	-	yes	yes	-	-	yes	yes
Long Range	-	-	-	-	-	yes (fino a 80 m)	yes (up to 60 m)	yes (up to 80 m)

LASER SCANNER UAM	LASER SCANNER PHARO	EOS 2 A	EOS 2 X	VISION V	VISION VX
Laser scanner	Laser scanner	Light curtain	Light curtain	Light curtain	Light curtain
Type 3 SIL 2 – PL d	Type 3 SIL 2 – PL d	Type 2 SIL 1 – PL c	Type 2 SIL 1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c
30, 40, 70 select.	50, 70 select.	50, 90	50, 90	50, 90	50, 90
-	-	160 ... 2260	160 ... 2260	310 ... 1810	310 ... 1810
5 (radius)	2,6 (radius)	12	12	16	18
yes	yes	-	yes	-	yes
yes	yes	-	yes	-	yes
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	yes (1/2 slave)	-	yes (1 slave)
-	-	-	-	-	-

LASER SCANNER UAM	LASER SCANNER PHARO	EOS 2 A	EOS 2 X	VISION V	VISION VX	VISION VXL	VISION MXL	ILION	ULISSE
Laser scanner	Laser scanner	Light curtain	Light curtain	Light curtain	Light curtain	Light cur- tain	Light curtain	Single beam	Single beam
Type 3 SIL 2 – PL d	Type 3 SIL 2 – PL d	Type 2 SIL 1 – PL c	Type 2 SIL 1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c	Type 2 SILCL1 – PL c
-	-	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4	1, 2, 3, 4	1, 2, 3, 4
-	-	-	-	-	-	-	-	-	-
-	-	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	510 ... 910	-	-
5 (radius)	2,6 (radius))	12	12	16	18 or 60	8	8	8 or 20	6
yes	yes	-	yes	-	yes	yes	yes	yes with AU SX or AU SXM	yes with AU SX or AU SXM
yes	yes	-	yes	-	yes	yes	yes	yes with AU SX or AU SXM	yes with AU SX or AU SXM
-	-	-	-	-	-	-	yes	yes with AU SXM	yes with AU SXM
-	-	-	yes (1/2 slave)	-	yes (1 slave)	-	-	-	-
-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	yes (up tp 60 m)	-	-	-	-

## SELECTION GUIDE

As the ESPE will be integrated in the machine safety-related control system, the choice of its safety level will depend on the result of risk analysis and, consequently, on parameters such as PL, SIL or category resulting from the related safety function.

Product Standards (Type C) usually recommend the most suitable ESPE type for each safety-related function involved. If type C Standards are not available, adopt the recommendations of ISO 13849-1 and IEC 62061. Also consider that the overall safety integrity of the serial connection: input – control unit – actuators, shall necessarily be equal to or lower than that of the weaker device.

### Rules for correct interconnection of protection devices to machine control system

The interconnections between safety outputs of ESPE (OSSD) and the machine primary control elements, the positioning and selection of reset push buttons shall not reduce or eliminate the extent of safety integrity assigned to the safety-related machine control system.

Next figure shows the most common example, i.e. where the machine control and monitoring system (e.g. the PLC) has no safety-related function. In this case, the safety-related control system monitoring the protective devices connected to it must operate autonomously and must be inserted between the machine control system and the machine primary control elements.

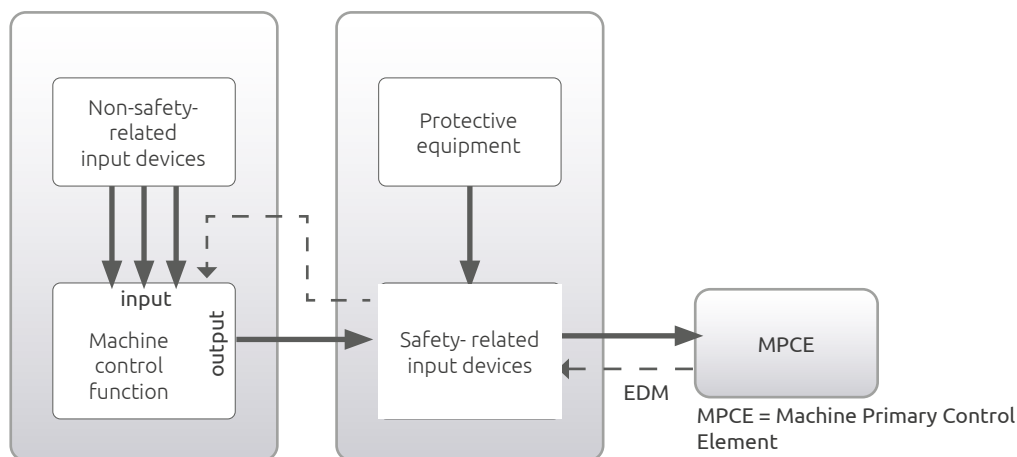


Fig. 42. Machine control and monitoring system (e.g. the PLC) has no safety-related function

If the machine is equipped with an integrated safety-related control and management system (safety-related PLC), see figure 15, machine operational functions and safety-related functions should be governed through the centralized safety-related system.

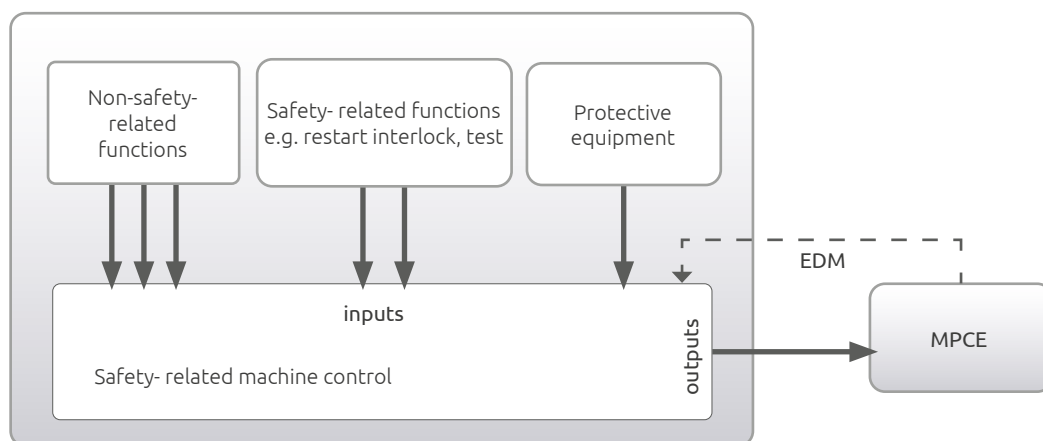


Fig. 43. integrated safety-related control and management system (safety-related PLC)



## Placement of the access control light curtains in the paletizer plant

This standard study tries to answer these two questions:

- how high, compared with to reference plane, it must be the first beam of the light curtains?
- What is the selection criterion to determine the number of the beams of the light curtains?

Below there are three examples of palletizers where the safety light curtains are positioned:

- Example 1  
at the ground floor,
- Example 2  
on a conveyor placed near the ground,
- Example 3  
on a conveyor in the case of a raised conveyor if its surface is flat and, moreover, easily accessible by stairs.



For each of these conditions the EN 415-19 defines:

3. how high must be positioned the first beam of the light curtain
4. the number of beams of the same light curtain.

When the opening includes the floor or an easily accessible platform as in follow example, the AOPDs must have at least 3 beams positioned at 300mm, 700mm and 1100mm from the access plane.

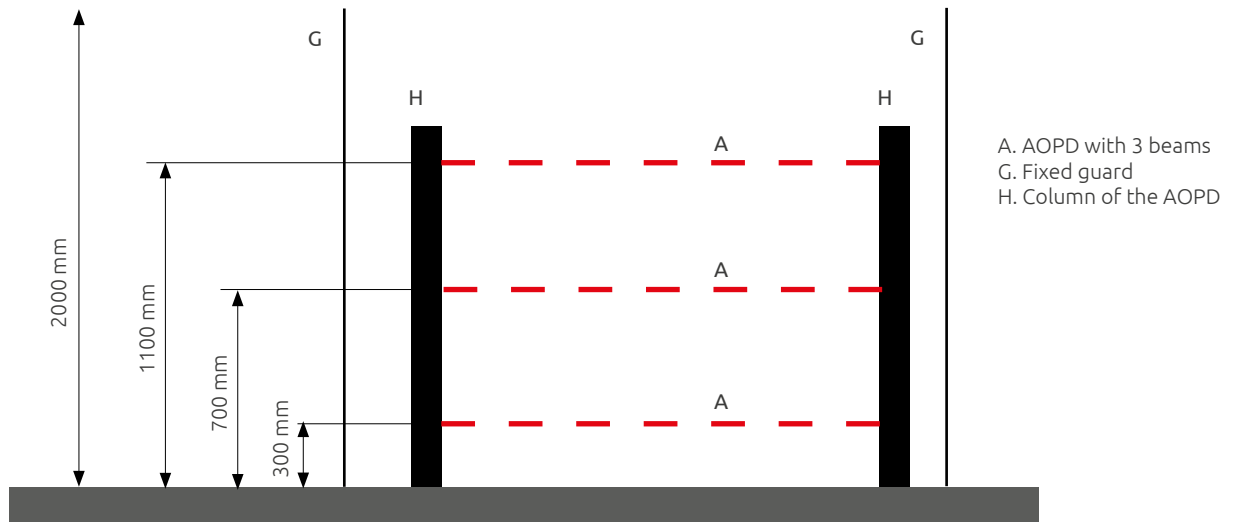


Fig. 44. Positioning of the AOPD - General

When the opening is on a conveyor, the AOPDs must have at least 2 beams positioned at 400mm and 900mm from the conveyor plane.

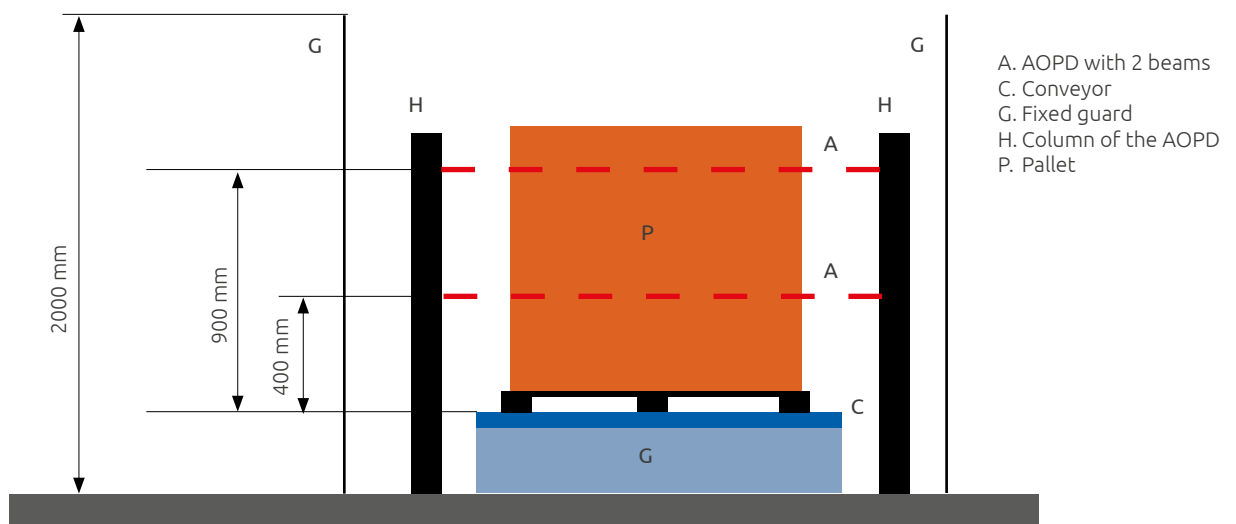


Fig. 45. Positioning of the AOPD - Above the roller conveyor

The safety distance must be calculated using the formula:  $S = 1600 \times T + 850$  (see ISO 13855: 2010)

If it is possible to reach the dangerous point by leaning over the edge of the higher beam then the following formula must be used:  $S = 1600 \times T + C_{ro}$  (Where  $C_{ro}$  comes from Table 1 of ISO 13855: 2010)

Or an ESPE with a larger number of beams must be selected.

### Using mechanical obstacles

To prevent a person from crawling below the lower beam and reaching the dangerous area without being intercepted by the AOPD, mechanical obstacles can be used.





## Industrial thermal processes

Control of all applications where burners are used or, in general, in industrial thermal processes. Example: ovens, dryers for ceramic or cereals, shrink-sleeve wrappers & spreading lines, etc..

The most common requests for this kind of applications are the following:

- Flame monitoring, according to ISO 13849-1 standard, must reach PL e safety level.
- Gas and burning oil pressure control (PL d).
- Post-purge monitoring of gas presence in pipes (PL d).
- Combustive-air ventilation turn-off control (PL d).



With regards to these type of applications, a key factor should be highlighted: there should be no confusion between the actual “burner” and the plant or thermal process in which the burner is used.

Burners must comply with specific standards requiring analogic reading functions of air-gas mixture and many other relating logic functions.

Instead, standard EN 746-2 regulates burner’s applications defining the thermal process required safety levels and regulations applicable.

### Sensors required by the EN 746-2 standard

- Flame extinction monitoring: flame-presence detector sensors are normally used (often optical, non-safety) instead of the required SIL3-type or 2x SIL2-type flame detectors. More commonly, certified integrated burner monitoring systems (BMS), including flame control, are used. The SIL3-type or the 2x SIL2-type digital signal generated by the BMS can be used as input.
- Gas pressure monitoring: pressure switches (SIL2-type, SIL3 not available).
- Pilot-flame temperature control: temperature detectors (SIL3).
- Gas pipes purging control: gas detector (SIL3 or SIL2).
- Air-vent fans monitoring: flow sensors (SIL2).
- Air/fuel ratio monitoring: pressure switches (SIL2).





The block diagram shown below indicates the relationships between system's components.

The diagram clearly shows where Mosaic safety controller can take action. Based on the input received from sensors and safety systems, Mosaic OSSDs acts on the combustion-gas and combustible-air nozzles, controlling and adjusting the combustion process.

#### Process control (a)

1. Control and instrumentation system / Operator control level
  - Process control level
  - Control level (local)
  - Control (non-fail-safe)
  - Tuning and adjustments
  - Monitoring
2. Protective systems
  - E-stop
  - Safety interlock
  - Purge and pipe monitoring
  - Tightness control
  - Automatic burner control unit
  - Flue gas venting
  - Air/fuel ratio
  - Flow and pressure detectors
  - High temperature limits

#### Heated system (b)

3. Fuel supply (gas)
4. Combustion air supply
5. Burner system and ignition device
6. Combustion chamber
7. Processing chamber
8. Flue gas system.

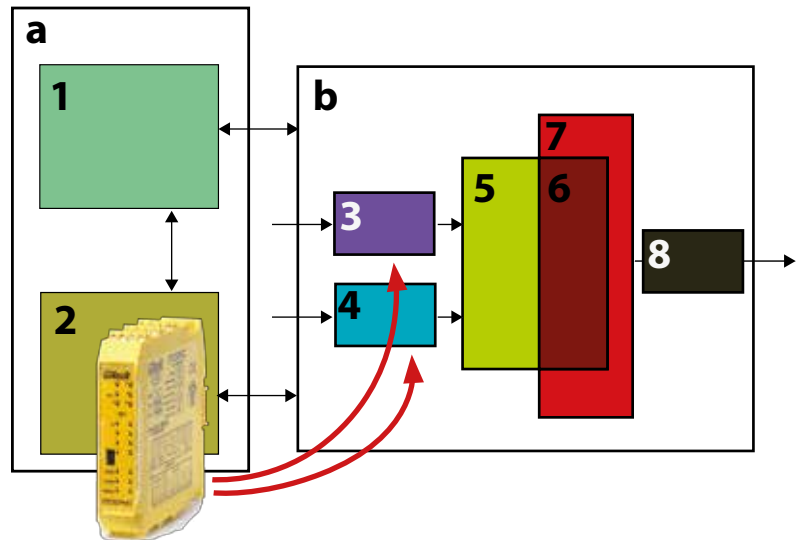


Fig. 46. Block diagram showing equipment for industrial thermal process

## Standard

These types of systems are regulated by European Standard EN 746-2 - "Industrial thermoprocessing equipment safety requirements for combustion and fuel handling systems" May 2010.

This Type C standard and is part of the 8 standards forming the EN 746 safety standards "Industrial Thermoprocessing Equipment".



The EN 746-2 assumes that all equipments are not creating any potential explosive atmosphere and are located in a normally ventilated area.

EN 746-2 defines the requirements for the protective-and-safety systems of these devices:

- The protective-and-safety system is a group of devices, control units and safety circuits whose main purpose is the protection of the personnel, the plant and the environment.
- The protective-and-safety system includes all components required to carry out the safety function:
  - Sensors for monitoring safety-related parameters (e.g. flame temperature, air pressure, etc..)
  - Combustion-gas and combustible-air blocking devices (valves)
  - Combustion-chamber ventilation control and burner protection devices (e.g. temperature level monitoring).

A protective-and-safety system is typically made up of sensors, control logics, actuator devices and a multi-channel system allowing communication between all elements. The required safety monitoring of the whole system can be performed by Mosaic.

The standard also defines the conditions that the protective-and-safety system should fulfill, indicating 4 possible scenarios as shown in the following table:

Condition	Device	Standard
Hardwired system in which all components comply with the relevant product standards as specified in 5.2 to 5.6	Automatic burner control systems	EN 298
	Valve testing systems	EN 1643
	Pressure sensing devices	EN 1854
	Automatic shut-off valves	EN 161
	Gas/Air ratio controls	EN 12067-2
Hardwired system with a combination of: components complying with the relevant product standards as specified in 5.2 to 5.6 components complying with defined SIL/PL level in accordance respectively with EN 62061 and EN ISO 13849-1	Automatic burner control systems	EN 298
	Valve testing systems	EN 1643
	Pressure sensing devices	EN 1854
	Automatic shut-off valves	EN 161
	Gas/Air ratio controls	EN 12067-2
	Guarding functions (e.g. gas pressure, temperature) performed by components for which no relevant product standards are existing shall comply with at least: SIL 2 / PL d	IEC 62061 (SIL)
	Functions which will lead to immediate hazard in case of failure (e.g. flame detector device, ratio monitoring) performed by components for which no relevant product standards are existing shall comply with at least: SIL 3 / PL e	EN ISO 13849 (PL)
PLC based system with a combination of: components complying with the relevant product standards as specified in 5.2 to 5.6 components complying with defined SIL/PL level in accordance respectively with EN 62061 and EN ISO 13849-1	Automatic burner control systems	EN 298
	Valve testing systems	EN 1543
	Pressure sensing devices	EN 1854
	Automatic shut-off valves	EN 161
	Gas/Air ratio controls	EN 12067-2
	Guarding functions (e.g. gas pressure, temperature) performed by components for which no relevant product standards are existing shall comply with at least: SIL 2 / PL d	
	Functions which will lead to immediate hazard in case of failure (e.g. flame detector device, ratio monitoring) performed by components for which no relevant product standards are existing shall comply with at least: SIL 3 / PL e	IEC 62061 (SIL)
	Software for safety functions should be separate from other functions (e.g. control functions) the software for safety functions shall be designed in accordance with the requirements of EN ISO 13849 and EN 62061. A PLC used for safety functions shall comply with EN ISO 13849-1 and EN 62061.	EN ISO 13849 (PL)
PLC based system in which all components comply with defined SIL 3 /PL e and with a defined SIL 3/PL e of hard and software.	In this case EN ISO 13849-1 and EN 62061 shall be applied for the protective system in general	IEC 62061 (SIL)
		EN ISO 13849 (PL)

## Perimeter protection

Combined application of safety light curtains and deflector mirrors. For perimeter protections up to 4 sides, floor support columns with deflection mirrors can be used in combination with safety light curtains. An example of application is illustrated in the following figure.



Fig. 47. Machine for laser cutting perimeter protection

Columns with deflection mirrors range offer from ReeR is the following:

Models	FMC-S2	FMC-SB2	FMC-S3	FMC-SB3	FMC-S4	FMC-SB4	FMC-S1700	FMC-S2000
Ordering codes	1200620	1200645	1200621	1200646	1200622	1200647	1200625	1200623
Description	single mirror for 2 beams light curtains	2 mirrors for 2 beams light curtains	single mirror for 3 beams light curtains	3 mirrors for 3 beams light curtains	single mirror for 4 beams light curtains	four mirrors for 4 beams light curtains	controlled height up to 1360 mm	controlled height up to 1660 mm
Overall height with base (mm)	1055		1255		1385		1725	2025

The SP deflection mirrors make it possible to create perimeter protection of areas with access point on multiple sides with large distances between the protection elements.

Normally the light curtains used in this type of applications are those with 2, 3 and 4 beams for detecting the presence of the body in a hazardous area. However, You can also use light curtains with different resolutions. In this case, do not apply the measures listed in the table of the next page. For these applications it is necessary to assess the safety distances depending on the type of plant. The layout of safety light curtains and columns with the deflection mirrors clearly depend on the type and the specific requirements of the protection system we intend to create.

There are three factors to take into account in calculating the distances between safety barriers and columns:

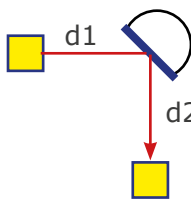
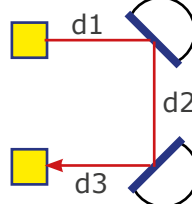
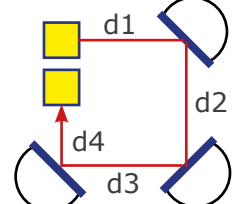
- Divergence between the beams - Should be taken into account that the beams emitted from the light curtain emitter present a certain degree of divergence, so there are never perfectly parallel.
- Any problems of flatness of the mirror - This factor, as the previous increases its influence with increasing distances.
- Absorption coefficient of mirrors - For each mirror used is necessary to take into account the reduction in power of the optical beam emitted from the light curtain emitter. Refer to the following diagram:
  - FMC (S2 - S3 - S4)
    - 15% for light curtains with range up to 20 m
    - 20% for light curtains with range higher than 20 m.
  - FMC (SB2 - SB3 - SB4)
    - 10% for light curtains with range up to 20 m
    - 15% for light curtains with range higher than 20 m.

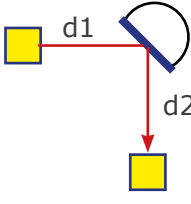
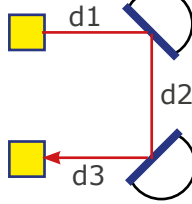
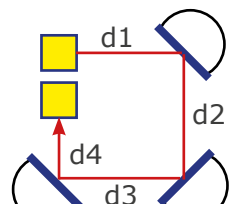
This reduction is due to the specific characteristics of the mirror and takes account of the dirt and dust that settles on the same, especially in industrial environments. This reduces the range of the system mirror/light curtains.

These three factors determine the choice of the barrier model and the minimum distances for the positioning of the elements of the protection system.

The following table is intended to provide a guide for:

- choice of the type of column and light curtain to be used;
- define the maximum distance allowed for the correct placement of the devices taking into account the factors mentioned above and the maximum range of the light curtain used.

			INSTALLATION TYPE		
COLUMN WITH DEFLECTION MIRROR TYPE	LIGHT CURTAINS MODEL	LIGHT CURTAINS RANGE			
			Max. Distance	Max. Distance	Max. Distance
FMC S2 FMC S3 FMC S4	EOS SAFEGATE	4 - 12 m	$(d1+d2) < 10 \text{ m}$	$(d1+d2+d3) < 8,5 \text{ m}$	$(d1+d2+d3+d4) < 6,5 \text{ m}$
	EOS H	10 - 20 m	$(d1+d2) < 17 \text{ m}$	$(d1+d2+d3) < 14,5 \text{ m}$	$(d1+d2+d3+d4) < 12 \text{ m}$
	ADMIRAL	6 - 18 m	$(d1+d2) < 15 \text{ m}$	$(d1+d2+d3) < 13 \text{ m}$	$(d1+d2+d3+d4) < 11 \text{ m}$
	VISION	6 - 16 m	$(d1+d2) < 13,5 \text{ m}$	$(d1+d2+d3) < 11,5 \text{ m}$	$(d1+d2+d3+d4) < 9,5 \text{ m}$
	JANUS LR	30 - 60 m			
	ADMIRAL LR	22 - 60 m	$(d1+d2) < 48 \text{ m}$	$(d1+d2+d3) < 38 \text{ m}$	$(d1+d2+d3+d4) < 30 \text{ m}$
	VISION LR	22 - 60 m			
	JANUS LR ILP	40 - 80 m	$(d1+d2) < 64 \text{ m}$	$(d1+d2+d3) < 51 \text{ m}$	$(d1+d2+d3+d4) < 41 \text{ m}$

			INSTALLATION TYPE		
COLUMN WITH DEFLECTION MIRROR TYPE	LIGHT CURTAINS MODEL	LIGHT CURTAINS RANGE			
			Max. Distance	Max. Distance	Max. Distance
FMC SB2 FMC SB3 FMC SB4	EOS SAFEGATE	4 - 12 m	$(d1+d2) < 11 \text{ m}$	$(d1+d2+d3) < 10 \text{ m}$	$(d1+d2+d3+d4) < 9 \text{ m}$
	EOS H	10 - 20 m	$(d1+d2) < 18 \text{ m}$	$(d1+d2+d3) < 16 \text{ m}$	$(d1+d2+d3+d4) < 14,5 \text{ m}$
	ADMIRAL	6 - 18 m	$(d1+d2) < 16 \text{ m}$	$(d1+d2+d3) < 14,5 \text{ m}$	$(d1+d2+d3+d4) < 13 \text{ m}$
	VISION	6 - 16 m	$(d1+d2) < 14,5 \text{ m}$	$(d1+d2+d3) < 13 \text{ m}$	$(d1+d2+d3+d4) < 11,5 \text{ m}$
	JANUS LR	30 - 60 m			
	ADMIRAL LR	22 - 60 m	$(d1+d2) < 51 \text{ m}$	$(d1+d2+d3) < 43 \text{ m}$	$(d1+d2+d3+d4) < 36,5 \text{ m}$
	VISION LR	22 - 60 m			
	JANUS LR ILP	40 - 80 m	$(d1+d2) < 68 \text{ m}$	$(d1+d2+d3) < 58 \text{ m}$	$(d1+d2+d3+d4) < 49 \text{ m}$



For small distances the column with single mirror is enough; for longer distances, which amplify all the factors mentioned above, are required multiple mirrors that let you retrieve the divergence of beams parallelism.



## **REEER** *Customer Service*

**We put our Customers always first**

ReeR after sales service is committed to support all customers that need technical guidance regarding functionality, handling and installation of our products.

**Customer Service Hotline**

**+39 011 24 82 215**

**Monday to Friday 8.30 - 12.30 and 13.30-18.00 (CET)**

or contact

**[aftersales@reer.it](mailto:aftersales@reer.it)**

For product returns please visit [www.reersafety.com](http://www.reersafety.com) for further information.



*Your future's safe!*

### More than 60 years of quality and innovation

Founded in Turin (Italy) in 1959, ReeR distinguished itself for its strong commitment to innovation and technology.

A steady growth throughout the years allowed ReeR to become a point of reference in the safety automation industry at a worldwide level.

The Safety Division is in fact today a world leader in the development and manufacturing of safety optoelectronic sensors and controllers.

ReeR is ISO 9001, ISO 14001 and ISO 45001 certified.



ReeR SpA  
Via Carcano, 32  
10153 Torino, Italy

T +39 011 248 2215  
F +39 011 859 867

[www.reersafety.com](http://www.reersafety.com) | [info@reer.it](mailto:info@reer.it)



Issue 2 - Rev 1.4

June 2022

8946230

SAFETY GUIDE - English

*Printed in Italy*



ReeR SpA does not guarantee that product information in this catalogue are the most current available. ReeR SpA reserves the right to make changes to the products described without notice and assumes no liability as a result of their use or application. Our goal is to keep the information on this catalogue timely and accurate, however ReeR SpA accepts no responsibility or liability whatsoever with regard to the information on this catalogue. Reproduction is not authorised, except with the expressed permission of ReeR SpA.