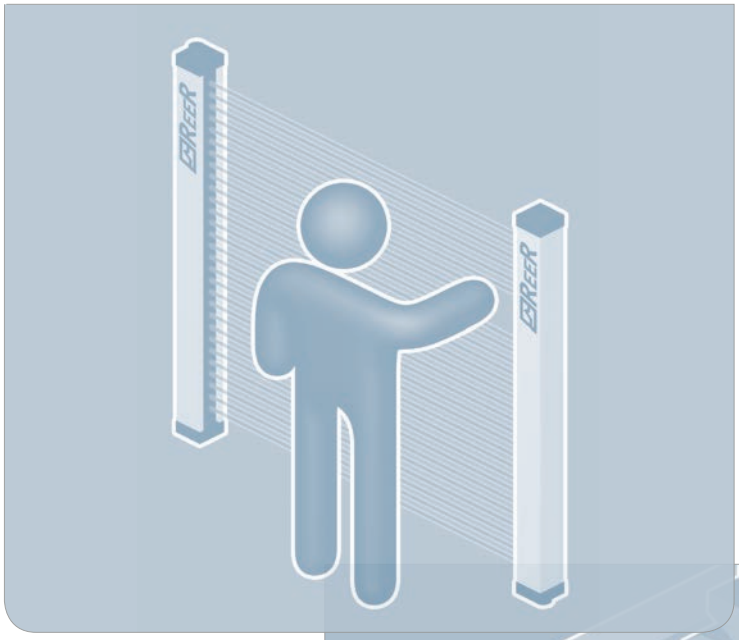
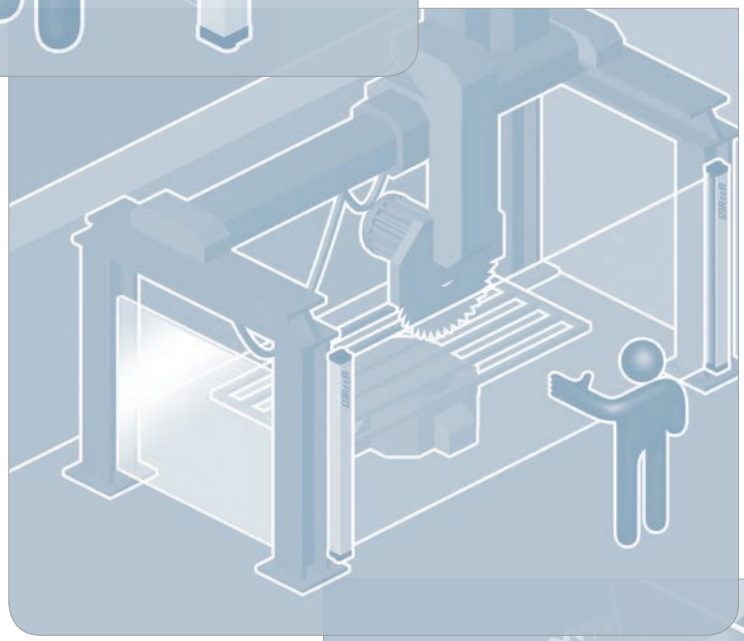
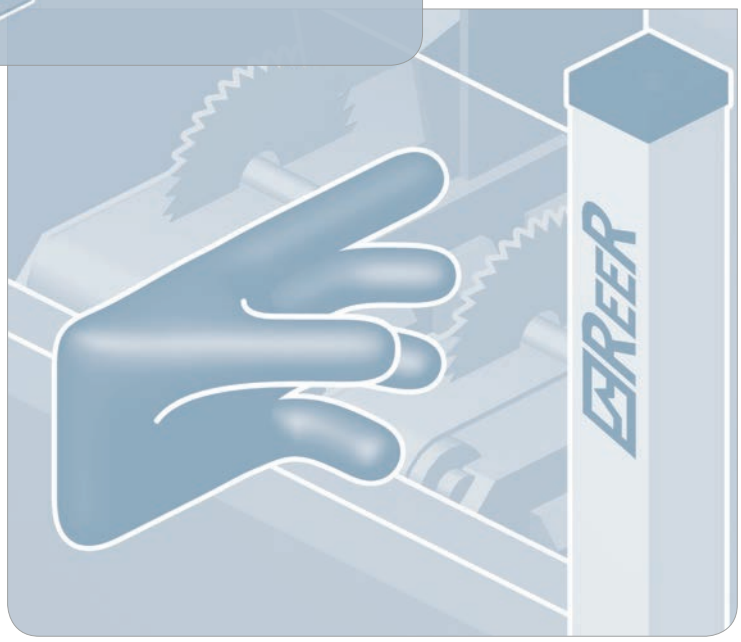
SAFETY GUIDE







SAFETY IN THE WORKING ENVIRONMENT

INTERNATIONAL STANDARD

Many important changes have been introduced in regulations on safety of machinery, starting from 2010. In practice several of these have already had some impact since 2005 and 2006, when the overlap period began for Standards on safety-related machine control systems.

In particular, this concerns the crucial family of Standards under the umbrella of ISO 13849, and IEC 61508 which impacts safety of machinery especially through IEC 62061. Thus, important statistical concepts derived from process safety and 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 PLs (Performance Levels, for ISO) and SILs (Safety Integrity Levels, for IEC). PL and SIL come next to and in many ways replace the now familiar concept of Category featuring in the 'old' EN 954-1.

In 2008 IEC finished the second edition of IEC TS 62046, a specification providing guidelines on the use of safety sensors for machinery protection applications.

This is a novelty the impact of which will be felt worldwide.

Looking nearer home in Europe, the new Machinery Directive 2006/42/EC is effective starting from December 29, 2009. This Directive introduces a number of innovations compared to 98/37/EC.

EUROPEAN DIRECTIVES

The aim of the EC 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, service and people within the European Union.

In particular, where the safety of workers is concerned, the harmonization of legal provisions has resulted in the formulation and approval of Directives and Standards of great importance.

DIRECTIVES Define the objectives to be achieved.

STANDARDS Define the means and methods by which to achieve the objectives established by the Directives.

A product/service that complies with the harmonized Standards is presumed to conform to the Directives.

Stages for the realization of a Standard:

- Creation of a Working Group (WG) made by experts of the subject to be treated, which represent the Member States
- Preparation of a draft version of the Standard (prEN) to be examined by the various national Committees involved, for comments, proposals and the subsequent final approval
- Drafting of the definitive formulation of the text of the Standard (EN), official publication, and acceptance by the individual Member States.

The Directives concerning the protection of workers are:

- 89/391/EC "Health and safety at work - Framework directive"
- 2009/104/EC "Use of work equipment" and amendments / additions

The Directives governing safety components are:

- 2006/42/EC "Machinery directive"
- 2006/95/EC "Low Voltage Directive"
- 2004/108/EC "Electromagnetic Compatibility Directive"

SOCIAL DIRECTIVES

"Social Directives" 2009/104/EC and 89/391/EC, are aimed at the improvement of safety in working environment.

The Directives:

- Determine the preventive measures to be adopted in the working environment.
- Supply information on:
  - risk analysis;
  - program of prevention and achievement of compliance of the machines;
  - procedures concerning the compliance of machines;
  - responsibilities of the employer;
  - education and training of the people in charge of system operation.
- Imposes the adaptation of existing machinery in compliance with the provisions of the Machinery Directive.

THE MACHINERY DIRECTIVE

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

- 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, construction and marketing in the European Union of safety 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:

- It applies to all new machines and safety components that are sold, lent or hired, and to used machinery in the event of sale, rental or loan.
- It sets forth the essential safety requirements relating to the design and construction 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 Directive:

- Lays down stringent procedures for safety components and highly hazardous machines which are listed in Annex 4.
- Lays down simplified procedures for low and medium risk machines not included in annex 4.
- Requires that manufacturers prepare a technical dossier for each product stating the safety principles adopted in the design, manufacture, transport, use and maintenance of the machine or 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 attesting compliance to the Directive.

THE MACHINERY DIRECTIVE 2006/42/EC

Main objectives of the revision

Clarity

- The list of products covered by the Directive is more explicit.
- New product classes have been added.
- Borderline relative to other Directives have been clarified.
- Definitions have been improved.

Legal certainty

The fourth Proviso states: "In order to ensure legal certainty for users, the scope of this Directive and the concepts relating to its application should be defined as precisely as possible".

Improved applicability

- The criteria used for the nomination of Notified Bodies are more rigorous.
- Market surveillance. The obligations of the Member States are defined more accurately.
- Rules have been added for the withdrawal of dangerous products.

The conformity evaluation procedures have been revised

- It will no longer be possible to submit a technical file to a notified body without undergoing any verification of the content by the latter.
- Internal inspection of manufacturing process (Annex VIII) is required for all conformity evaluation procedures. Responsibility for inspection lies with the manufacturer.

Note on the annexes listing dangerous machinery and safety-related components
Annex 4 - which lists dangerous machinery and safety-related components – also includes safety-related logic blocks (e.g. programmable control units, PLCs, etc.). Annex 5 includes a non-exhaustive list of safety-related components.

Certifications

- CE type examination certificates issued by notified bodies must be updated.
- The CE type certificates is valid for 5 years (Annex IX para. 9.3), the five-year period starting from the revision date of the certificate.

LOW VOLTAGE DIRECTIVE

2006/95/EC is aimed at ensuring that electrical materials are designed and manufactured so as to guarantee the protection of people against any risk of injury arising from the use of such materials.

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

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

The last revision of the directive is in force starting from 16/01/2007.

ELECTROMAGNETIC COMPATIBILITY DIRECTIVE

The aim of "Electromagnetic Compatibility Directive" 2004/108/EC 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 purpose
- The level of built-in immunity to external disturbances enables them to operate according to their intended purpose.

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

The last revision of the directive is in force starting from 20/01/2005

ATEX DIRECTIVE

Atex DIRECTIVE 94/9/EC applies to all products for use in explosive atmosphere.

The Directive specifies minimum safety requirements for electrical devices used in environments classified as dangerous regarding the aspect of risk of explosion from gas or dust.

The risk of explosion consists of three levels:

- Category 1 : maximum risk level (areas 0 and 20)
- Category 2 : high risk level (areas 1 and 21)
- Category 3 : risk level defined as "normal" (areas 2 and 22).

The ATEX Directive is in force since 1/07/2003.

SAFETY IN THE WORKING ENVIRONMENT

ACCREDITED BODIES

In each Member State, the role of the accredited Bodies is to assess and verify the compliance and the application of the Directives concerning machines and safety components.

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

The Accredited Bodies must have the expertise and the resources which are necessary to perform their activities of inspection, analysis, technical support, measuring, etc.

NOTIFIED BODIES

Notified Bodies are authorized to examine and certify machines and safety components in compliance with the applicable Directives.

Each Member State of the European Union is required to:
- Appoint the Notified Bodies by specifying their tasks
- Submit a list of the Notified Bodies to the European Commission and to the other Member States.

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

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

HARMONIZED STANDARDS

- They are technical Standards conceived to meet the essential requirements of the Directives
- They are written by the 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.

Status of the Standards

prEN... a proposed standard (draft) which has not yet been definitely approved

EN... an approved standard already in force

TS... a technical specification.

The European Standards concerning safety are subdivided into 3 groups:

TYPE A STANDARDS

They specify the general design principles applying to all types of machine:

e.g...	**EN 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 - 1	Safety distances for the protection of the upper limbs.
	EN 60204	Safety of machinery. Electrical equipment of machine.
	EN ISO 13849 - 1,2	Safety related parts of control systems.

- **type B2 Standards: concerning safety devices**

e.g...	**EN 61496-1**	Electro-sensitive protective equipment - general requirements and tests-
	EN 61496-2	Electro-sensitive protective equipment- Particular requirements for equipment using active optoelectronics protective devices (i.e. light curtains)-
	EN 61496-3	Electro-sensitive protective equipment-Particular requirements for Active Optoelectronics Devices responsive to diffuse reflection (i.e. laser scanner)-
	EN ISO 13850	Emergency stop - Principles for design.

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.
- If no C type Standards exist, compliance with the Directive can be attained on the basis of type A and type B Standards.

What is IEC TS 62046 – Application and integration of electrosensitive protection devices
IEC TS 62046 Ed. 2 - 2008, specifies recommendations for the installation and use of Electro-sensitive Protective Equipment (ESPE).
It applies mainly to Light Curtains, Laser Scanners, Borders and pressure–sensitive mats. Its purpose is to meet machinery manufacturers' and users' needs.
IEC TS 62046 specifies the precise positioning of electrosensitive devices relative to the machine and their correct interfacing with the machine rather than their construction. Its goal is to ensure that the risk for the operator is minimized through a correct selection and application of protection devices.
IEC TS 62046 details crucial aspects linked to the use of ESPEs, such as selection criteria, use, integration with the machine control system and also provides information on special functions of safety light curtains including Muting and Blanking.


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 particular aspects of their construction or operation. For the preparation of these standards ANSI often relies on the contribution of non-profit 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 When Referenced by other B11 Machine Tool Safety Standards (design, construction, maintenance and operation criteria for protection devices specified in Std. B11 covering machine tools)

SAFETY IN THE WORKING ENVIRONMENT

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 in question must be inspected by the Authorities Having Jurisdiction (AHJ).
If the device in question is already listed 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 is a non-profit organization listing industrial components which have been tested and proven to be safe and reliable in terms of electrical safety and fire resistance.

UL Listed Certification Mark means that the product in question 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 and with Std. ANSI/1998. 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.

RISK ASSESSMENT

The European Standard **EN ISO 12100** puts forward a systematic procedure for the examination of the hazards associated with machinery with the aim of selecting and adopting the most suitable safety measures to reduce or eliminate the risks.

For USA an equivalent procedure is described in the **ANSI Technical Report B11.TR3**.

The risk assessment can thus be broken down into 4 stages:

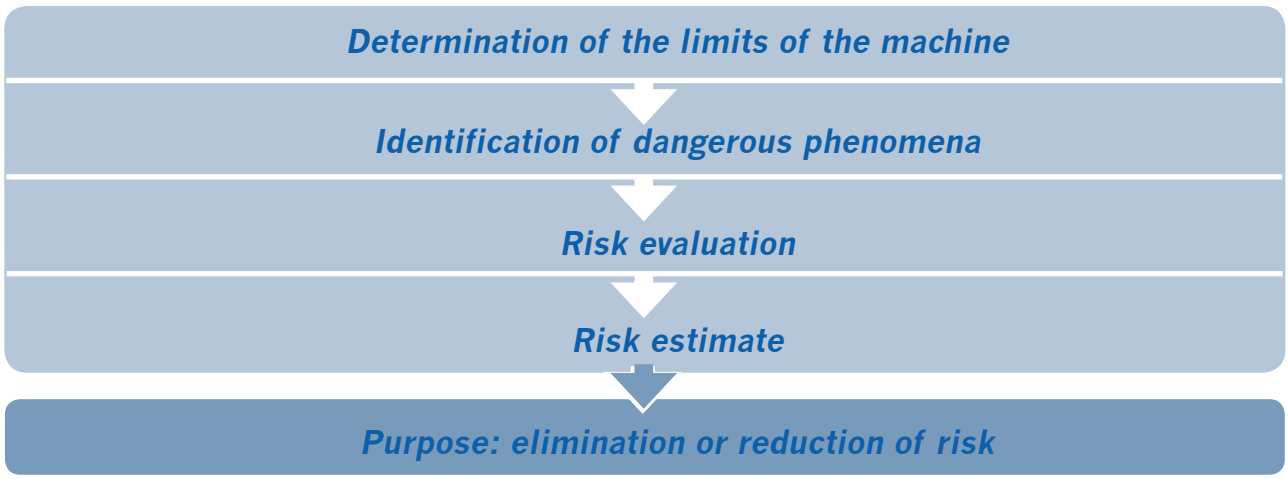


Fig. 1 - Stages of risk assessment

1. Determination of the limits of the machine
Consists in the examining of the intended use and of all the reasonably foreseeable misuses in relation to the level of training, experience and attitude of the user.

2. Identification of the hazards
Consists in the listing of:
The risks and the hazardous elements (mechanical, electrical, chemical, etc.)
Hazardous situations (manual loading-unloading, access to the system, etc.)
Events that might cause damages (machine failures or anomalies).

3. Risk estimation
Each hazardous situation identified is derived from a combination of the following elements:
Severity of injuries or damage to health (reversible, irreversible, fatal)
Probability of occurrence of that injury, which is a function of frequency and duration of exposure to danger
Possibility of avoiding danger with reference to:

- rapidity of occurrence of the event,
- possibility by the operator to perceive hazards and react promptly,
- possibility to escape.

4. Risk evaluation
Following the risk estimation a risk evaluation is required to determine if a risk reduction is necessary or whether safety has been achieved. If risk reduction is required, the protective measures selected and applied shall be evaluated to determine if an adequate risk reduction has been achieved.

SAFETY-RELATED CONTROL SYSTEM FOR MACHINERY

Where safety is based on the proper operation of the 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 the harmonized standards developed by mandate of the European Commission (assumption of conformity).

In the event of an accident, using the 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 new standards ISO 13849-1 and IEC 62061 which supersede EN954-1 as regulatory instruments covering machine control systems.

The old EN 954-1 Safety Related Parts of Control Systems, Part 1: General principles for design.

Up to December 31, 2011, safety-related parts of the machine control system designed according to Std. EN 954-1 shall be acceptable. As from 31st December 2011, compliance with Std. ISO 13849-1 or IEC 62061 will be mandatory.

Standard **EN 954-1** is harmonized since 1996. The safety-related control system is classified in five Categories.

Safety categories

For different parts of the machine the risk evaluation may lead to different levels. Therefore, the degree (category) of safety actions to be taken shall depend on the actual risk involved in each part.

To select the optimum category in relation to actual risk, use shall be made of the well-known risk graph.

Selection of the Categories

S Severity of injury
S1 Slight injury (usually reversible).
S2 Serious injury (usually irreversible) or death.

F Frequency and duration of exposure to hazard
F1 Seldom to more often and/or short exposure.
F2 Frequent to continuous and/or long exposure duration.

P Possibility of Avoiding hazard
P1 Possible under certain conditions (escape or action by others).
P2 Hazard almost unavoidable (occurs quickly).

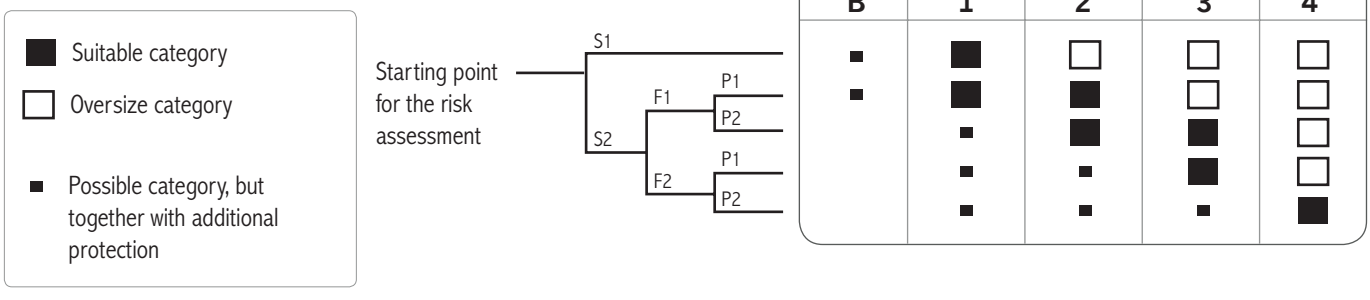


Fig. 2 - Category selection

For Cat. B and Cat.1 the ability to resist failure is due to robustness of components (avoid failures as far as possible).

For Cat. 2,3,4 the ability to resist failure is due to the system structure (control of the failure). Failure is controlled through cycle monitoring for Cat.2, redundancy for Cat.3 , redundancy plus monitoring for Cat.4.

Operational requirements are specified for each Category. The failure modes of the electric components are defined and listed. The relationship among Categories and the safety performance of the control system in case of failure is well defined (deterministic approach).

Note: categories are not necessarily totally hierarchical.

CATEGORY	REQUIREMENTS	BEHAVIOUR	SAFETY PRINCIPLES
B	Devices designed, manufactured and combined in compliance with the reference Standards so as to be able to cope with foreseeable events.	A fault may result in the loss of the safety functions.	Use of selected components.
1	Same requirements as for category B, but with the use of reliable and well-tested safety principles and components.	A fault may result in the loss of the safety functions, but with lower probability than in category B.	
2	The requirements of category 1 apply. Moreover: the safety function of the device is based on cyclic control managed by the control system of the machine.	A fault may result in the momentary loss of the safety function. The fault is detected when performing the test before starting the next working cycle, and the start of a new machine cycle is disabled.	Use of structures and safety circuits able to detect the fault and stop the machine.
3	The requirements of category 1 apply. Moreover: a single fault shall not lead to the loss of the safety function. Whenever possible, the individual fault must be detected.	Not all faults can be detected. When an individual fault occurs, the safety function is always active. The build up of un-detected faults may result in the loss of the safety function.	
4	The requirements of category 1 apply. Moreover: a single fault shall not result in the loss of the safety function. An individual fault is detected before or at the time of the request for the safety function. If this is not possible, the build up of faults shall not lead to the loss of the safety function.	Fault detection shall occur in time to prevent the loss of the safety function.	

Restricted use of EN 954-1

System behaviour upon failure cannot be the only way to assess the performance of the safety-related control system.

Other factors, such as component reliability, may have an important, even crucial, role.

Such concept is recognized in Std. EN 954-1 stating that (Annex B) “component reliability and the technology used in the application concerned may result in deviation from the Category envisaged.”

The Category selection process should be as follows:

- Identify the nominal or reference Category based on risk analysis (through risk graph)
- Modify selection of Category based on component reliability, technology used, etc.

SAFETY IN THE WORKING ENVIRONMENT

Phase two of the process is mainly empirical, and little information is given in the Standard.

Category is almost invariably selected referring to the risk graph disregarding changes due to other factors, or the changes introduced are subjective to the point where proving system safety becomes difficult.

Also, the extensive use of programmable electronics in the field of machine control systems has further highlighted the shortcomings of the deterministic model, impracticable for complex control systems, i.e. systems which use PLCs, communication lines, variable-speed actuators and programmable sensors.

To evaluate the safety-related performance of a complex system it is better to estimate its probability of being able to provide protection when needed. Or, in other words, estimate the probability of occurrence of a dangerous failure in a given period of time considering component reliability.

The new Standards

To offset the applicability limitations of Std. EN 954-1 two new standards were adopted, namely ISO 13849-1:2006 and IEC 62061:2005 which combine probability and known deterministic concepts to cope with technological progress in the field of industrial machinery.

Both these standards are harmonized to Directive 2006/42/EC regarding the following mandatory safety requirement:

Annex I : 1.2 Controls systems.

The two Standards exhibit a number of differences and overlaps, especially as regards the application criteria.

ISO 13849-1 may be used regardless of the type of technology and power used, i.e. mechanical, hydraulic, pneumatic, electric. It applies only to the five designated architectures.

IEC 62061 applies only to electric powered control systems. Subsystem reliability calculation formulas are given only for the four types of architecture specified therein and considered typical of industrial machinery, but may be applied also to other architectures. It allows the integration of subsystem designs in line with the requirements of ISO 13849-1: 1999 (EN 954-1).

ISO 13849-1 Safety Related Parts of Control Systems, Part 1: General principles for design

ISO 13849-1 is a revised version of EN 954-1

The complex mathematical formulas of the system reliability theory were replaced with pre-calculated tables.

Some concepts of EN 954 were retained, i.e. categories, redundancy, monitoring.

A number were modified, i.e. risk graph, selection of Categories.

The role of Categories is no longer crucial as in EN 954-1.

To assess the resistance to dangerous failure, the Category concept is replaced by Performance Level (PL) as the ability of the safety-related machine control system (hereinafter called SRP/CS) to assure protection in specified operating conditions.

The parameter used to evaluate the PL of the safety-related system is the Average probability of dangerous failure/hour. A failure is considered to be dangerous where it inhibits the system protection function if undetected.

There are 5 levels, PLa to PLe.

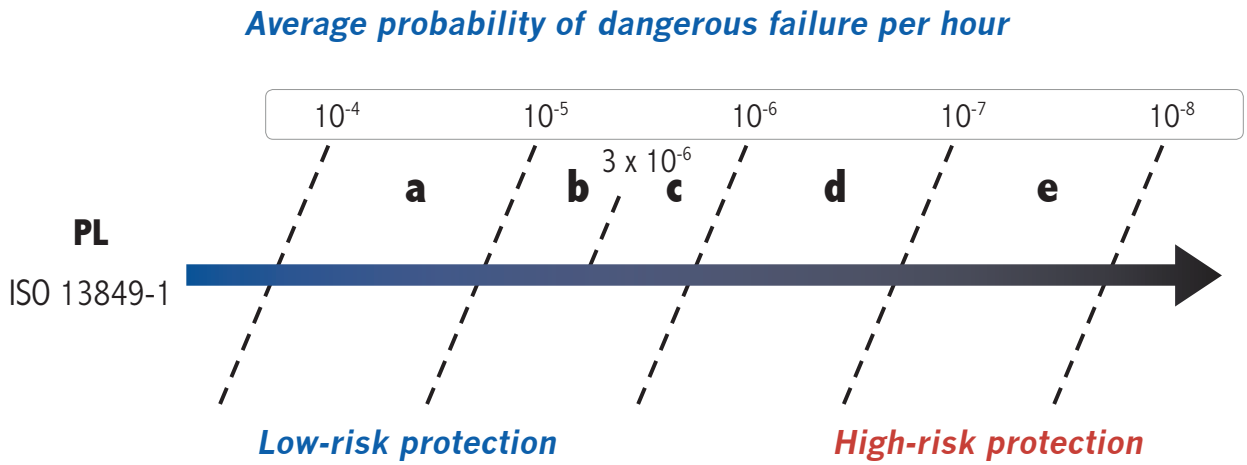


Fig. 3 - Table of ISO 13849-1

The greater the contribution to reducing risk the lower the **Average probability of dangerous failure/hour**.

PL is a function of control system architecture, component reliability, ability to promptly detect internal failure potentially affecting the safety function and quality of the design.

The table below summarizes mandatory qualitative and quantitative requirements to be met for safe control system design to ISO 13849-1.

► **See also glossary on page 28**

PL

Quantity aspects

$MTTF_d$ for individual components	**(measure of reliability)**
DC_{avg}	**(measure of diagnosticability)**
CCF	**(measure of ability to resist dangerous failure)**
Categories	**(description of structure)**

Quality aspects

Safety system performance in failure conditions
Monitoring of Systematic failure
Safety related software
Implementability of safety function in specific environmental conditions

Fig. 4 - Mandatory qualitative and quantitative requirements to be met for safe control system design to ISO 13849-1

SAFETY IN THE WORKING ENVIRONMENT

To claim a given PL, in addition to evaluating the Average probability of dangerous failure/hour for the control system in question, it will also be necessary to prove compliance with quality requirements specified by the standard.

The claimed PL must be validated using ISO 13849-2 Safety Related Parts of Control Systems - Validation defining procedures tests and analysis, for the assessment of:

- Safety function provided
- Category attained
- Performance level reached.

IMPORTANT!

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

- Monitoring of systematic failures
- Using robust and reliable components (in line with Product Standards if available)
- Working according 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 the Standard ISO 13849-1 and meeting development requirements for applications and built-in SW.

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

1. Identification of safety-related function through risk analysis
2. Assignment of Performance Level requested (PLr) through risk graph
3. Selection of system structure (architectures) and self-diagnostic techniques
4. Technical development of control system
5. Calculation of MTTFd, DCavg and verification of CCF
6. Calculation of PL using Table 5
7. Verification of PL (if calculated PL is below PLr return to Step 3)
8. Validation.

Identification of safety related item and assignment of Performance Level required - PLr

For each safety-related function identified the designer of the SRP/CS decides the contribution to reduction of risk to be provided, i.e. PLr.

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

Parameter PLr represents the Performance Level required for the safety-related function in question.

Parameter PL represents the Performance Level of implementation hardware. PL of hardware must be equal to or higher than specified PLr.

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 PLr. If more than one safety-related function are identified, PLr shall be identified for each of them.

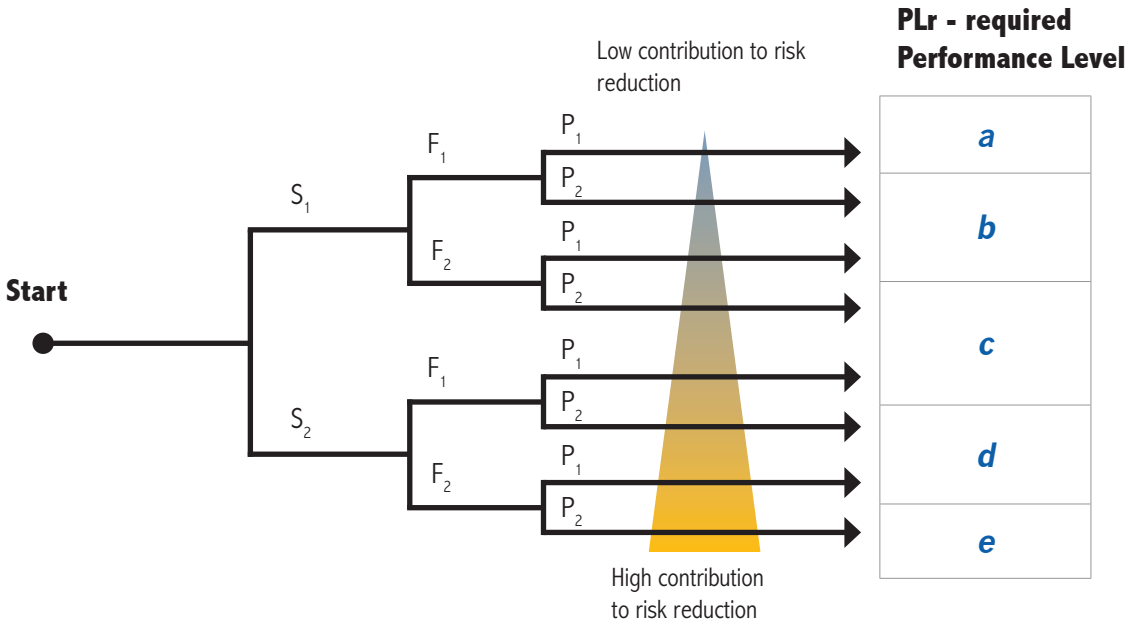


Fig. 5 - Tree type graph of decisions

S severity of injury
S1 reversible
S2 irreversible

F frequency or time exposure to hazard
F1 rare / short
F2 continuous / prolonged

P avoidable risk or limitation of damage
P1 avoidable within given conditions
P2 almost unavoidable

Note: contrary to EN954-1 as regards Categories, here PLrs are totally "hierarchical".
PLr(e) provides the greatest contribution to risk reduction, whereas PLr(a) makes the lowest contribution.

Design of the safety related control system and evaluation of the PL

After deciding on the PLr needed, a suitable SRP/CS is designed, calculating the resulting PL and ensuring that it is higher than or equal to PLr.

Fig. 3 shows that, to obtain the PL, the Average probability of dangerous failure/hour of the SRP/CS designed must be calculated

The Average probability of dangerous failure/hour for a safety-related control system may be estimated in various ways.

Using such methods implies that for each components the following are known:

- Failure rate (λ)
- Percent distribution of failure rate for all component failure modes, (e.g. if for a positive action switch the failure modes are: the contact will not open when required = 20% of cases and the contact will not close when required = 80% of cases.
- The effect of each failure on safety-related system performance, (e.g. dangerous failure = λd, or non-dangerous failure = λs)
- Percent of dangerous failures detected (by automatic self-diagnostic techniques implemented) out of total dangerous failures: λdd = λd x DC.
- Percent of dangerous failures not detected (by automatic self-diagnostic techniques implemented) out of total dangerous failures: λdu = λd x (1-DC).

SAFETY IN THE WORKING ENVIRONMENT

ISO 13849-1 simplifies calculation by providing a table based on Markov modelling in which average probability of dangerous failure per hour is pre-calculated for various Category combinations and range values of MTTFd and DCavg which are in turn obtained using tables.

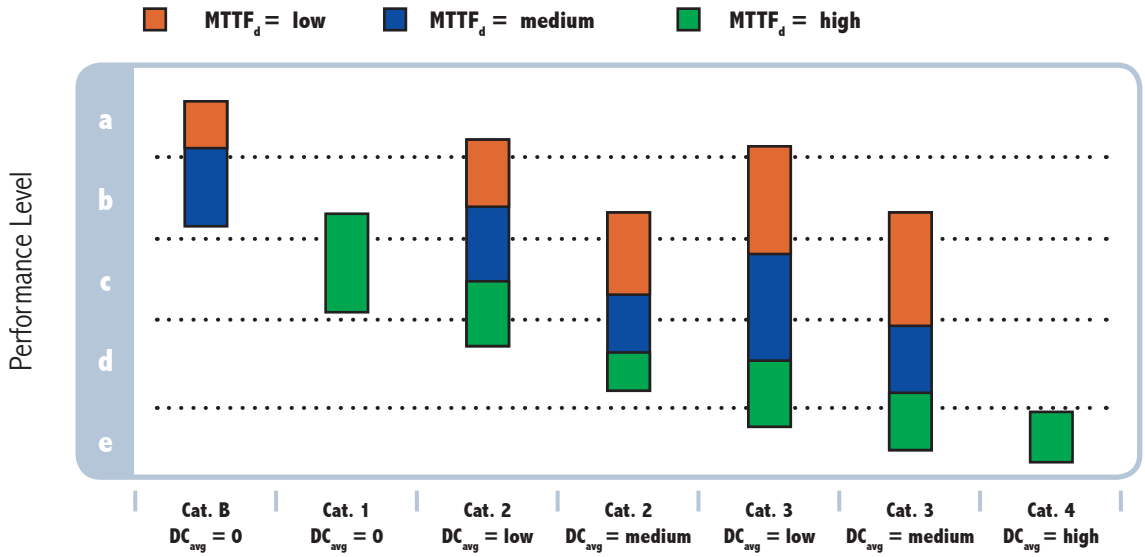
Denotations of $MTTF_d$	Range of $MTTF_d$
Low	3 years $\leq MTTF_d <$ 10 years
Medium	10 years $\leq MTTF_d <$ 30 years
High	30 years $\leq MTTF_d <$ 100 years

Denomination DCavg	Range of values DC / DCavg
None	DC < 60%
Low	60% $\leq$ DC < 90%
Medium	90% $\leq$ DC < 99%
High	99% $\leq$ DC

The problem is thus reduced to: selecting the architecture, calculating DC_{avg} in relation to self-diagnostic techniques implemented, calculating simplified $MTTF_d$ of circuit designed and verifying compliance with requirements for independent channel operation (CCF) for redundant architectures (Cat. 2, 3 and 4).

The combination of Category plus DC_{avg} adopted, is shown in one of the seven columns of fig. 5 of ISO 13849-1. Calculated $MTTF_d$ determines which part of the column is to be considered. Corresponding PL is shown on the left of the table.

Fig. 6 - figure of ISO 13849-1



The part of column selected may include two or three possible values of PL, e.g. for Cat. 3, DC_{avg} = Medium and $MTTF_d$ = Low, the following three values are possible: PLb, PLc, PLd. In these cases, to obtain the correct PL use is made of Table K.1 of Annex K of the Standard (not shown) providing detailed values of Average probability of dangerous failure per hour and PL in relation to actual value of $MTTF_d$ and the combination Category-plus-DC_{avg} implemented.

The Standard may be adopted only if the control system is designed using one (or more) of the five architectures specified.

Each architecture corresponds to one of the Categories defined in EN 954-1.

For systems designed to EN 954-1, category selection is directly linked to risk through the risk graph.

ISO 13849-1 is more flexible, as several options are available for each Performance Level specified.

An example is given in Table 5 where for a system having PL of "c" the following five alternatives are possible:

1. Category 3 with $MTTF_d$ = Low and DC_{avg} medium.
2. Category 3 with $MTTF_d$ = Medium and DC_{avg} low.
3. Category 2 with $MTTF_d$ = Medium and DC_{avg} medium.
4. Category 2 with $MTTF_d$ = High and DC_{avg} low.
5. Category 1 with $MTTF_d$ = High.

Combination of several SRC/PS to achieve the overall PL

The safety-related function may include one or more SRP/CSs, and several safety-related function may use the same SRP/CSs.

Individual SRP/CSs could also be obtained using other architectures.

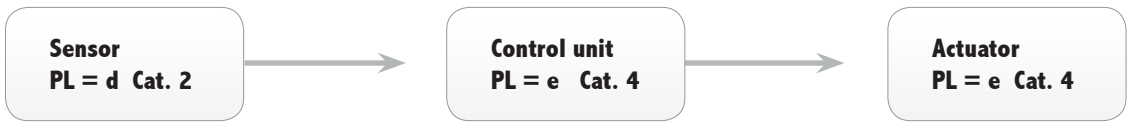
Where the safety-related function is obtained by a series connection of several SRP/CSs, e.g. safety light curtains, control logics, power output, and for each of these the PL is known, the Standard provides a simple method for calculating overall PL.

Locate the part with PL = PL low
Find the number of parts having PL = PL low
Enter data in the following table to obtain total PL

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

The PL obtained using this table refers to reliability values at mid-position for each of the intervals in Table 3 of ISO 13849-1.

Example:



We have: **PL low = d** **N low = 1 (< 3)**
Therefore: **PL total = d**

and average probability of dangerous failure per hour for the entire system will be a number somewhere between 1 x 10-6 and 1 x 10-7 (see Table 3 of ISO 13849-1).

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.

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

IEC 62061 retains the features of IEC 61508, but simplifies safety requirements (of 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 more than once per year.

The standard is based on two basic concepts:
- Management of Functional Safety
- Safety Integrity Level.

SAFETY IN THE WORKING ENVIRONMENT

Management of Operational Safety

Specifies all design aspects needed to attain the required level of functional safety, from assignment of safety requirements to documentation, design management up to validation.

Each design shall have its own Functional Safety Plan properly written, documented and duly updated as necessary.

The Functional Safety Plan shall identify people, functions and resources needed for design and implementation of the safety system.

Safety Integrity Level (SIL)

Methodology and requirements is given for:
- specifying functional requirements of each safety-related function to be implemented
- assigning the Safety Integrity Level (SIL) for each safety-related function envisaged
- allow the design of a SRECS suitable for the safety-related function to be implemented
- validating the SRECS.

SIL assignment

For SIL assignment use the method of Annex A (although the Standard also accepts the techniques of IEC 61508-5).

For each risk identified the following must be assessed:
- Degree of severity (Se) of possible damage
- Frequency and time (Fr) of exposure to danger
- Probability of dangerous event (Pr) linked to machine operating mode
- Avoidability (Av) of danger. The more difficult to avoid danger the higher the number representing avoidability.

The following table, extracted from the form in Figure A.3 of the Standard IEC 62061, will help in obtaining the SIL to be assigned to the safety–related function.

Consequences	**Severity Se**	**Class Cl**					**Frequency and duration Fr**		**Probability of hazardous event Pr**		**Avoidance Av**	
		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**	≥ 1 hour	5	Very high	5		
Permanent: losing fingers	3		**OM**	**SIL 1**	**SIL 2**	**SIL 3**	< 1 hour ≥ 1 day	5	Likely	4		
Reversible: medical attention	2			**OM**	**SIL 1**	**SIL 2**	< 1 day ≥ 1 2 weeks	4	Possible	3	Impossible	5
Reversible: first aid	1				**OM**	**SIL 1**	< 1 2 weeks ≥ 1 1 year	3	Rarely	2	Possible	3
							< 1 1 year	2	Negligible	1	Probable	1

OM (Other Measures) = The use of other parameters is recommended.

The sum of marks obtained for attributes of frequency, probability and avoidability provides the probability class of danger:

$$Cl = Fr + Pr + Av$$

To obtain the SIL align actual Cl to level of severity (Se) identified.

This is an iterative process. In fact, depending on the protective action undertaken, some parameters might change, e.g. Fr or Pr, in which case the SIL assignment process will have to be repeated using new values for changed parameters.

Three levels are envisaged: **SIL 1**, **SIL 2**, **SIL 3**.

Average probability of serious failure per hour (PFH_d)

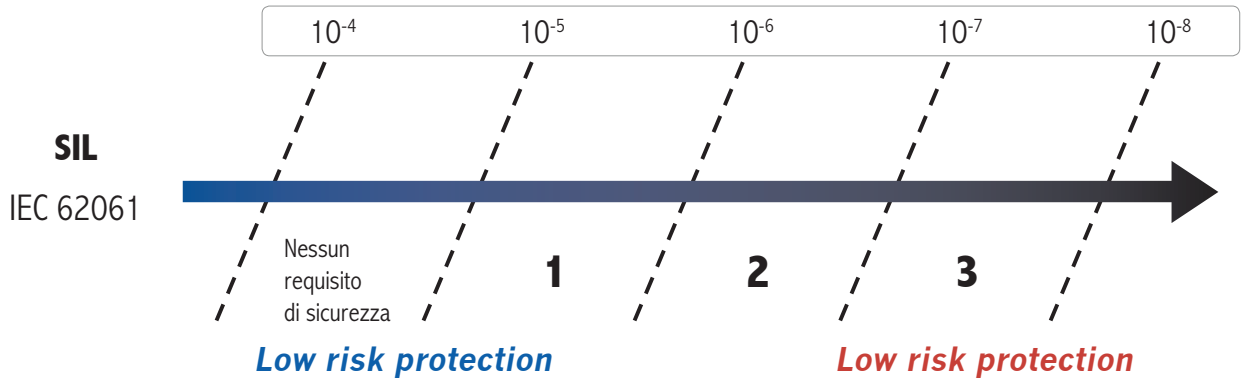


Fig. 7 - Table 3 of IEC 62061

Thus, the SIL represents the safety level to be assigned to a SRECS for attainment of its safety integrity in the operating conditions and all the way through the time specified.

The parameter used to define the SIL (Safety Integrity Level) is the probability of dangerous failure/hour (PFH_d).

The higher the SIL, the lower the probability of the SRECS not performing as safely as expected.

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

Development and design process

Each safety-related function identified through risk analysis shall be described in terms of:

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

Each safety-related function shall be broken down into functional blocks, e.g. functional block of input data, functional block of logic data processing, functional block of output data.

A subsystem is associated with each functional block.

In turn, subsystems will consist of electrical components interconnected with one another. Electrical components are known as subsystem elements.

Implementation of the SRECS technique will result in a typical architecture as shown (in this instance access control through photoelectric curtain)

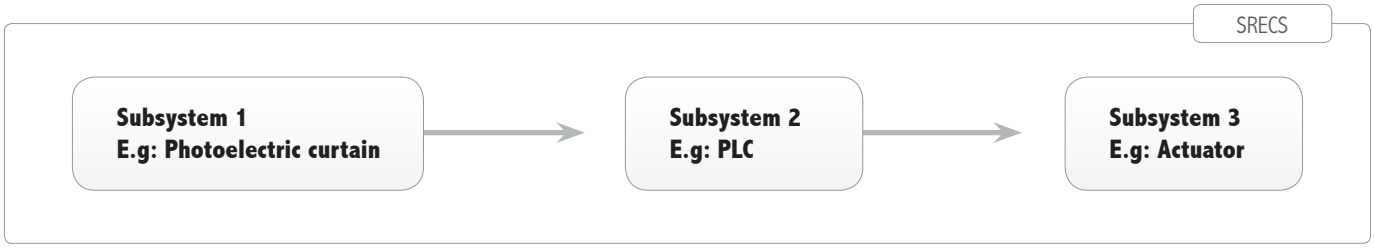
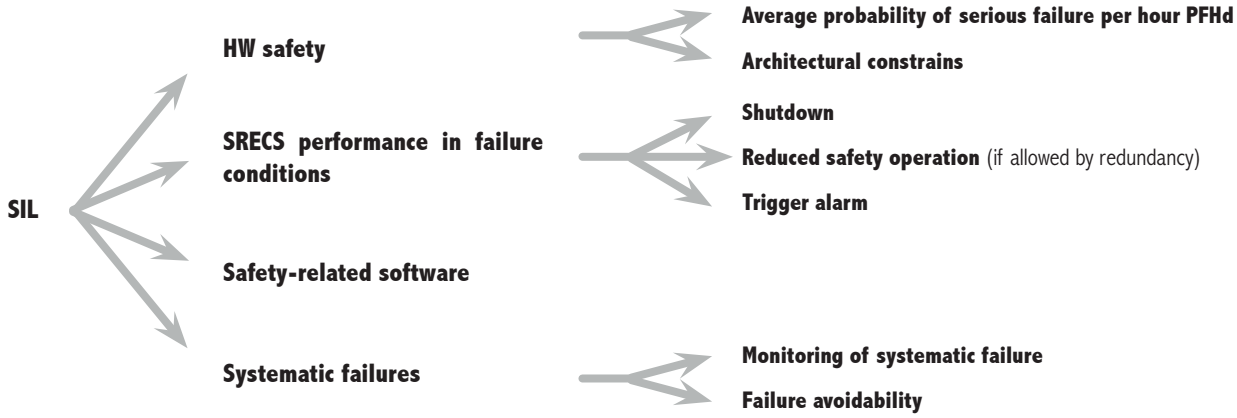


Fig. 8 - Typical architecture of the SRECS

SAFETY IN THE WORKING ENVIRONMENT

For SRECS to comply with identified operational and safety requirements, the following requirements shall be met:



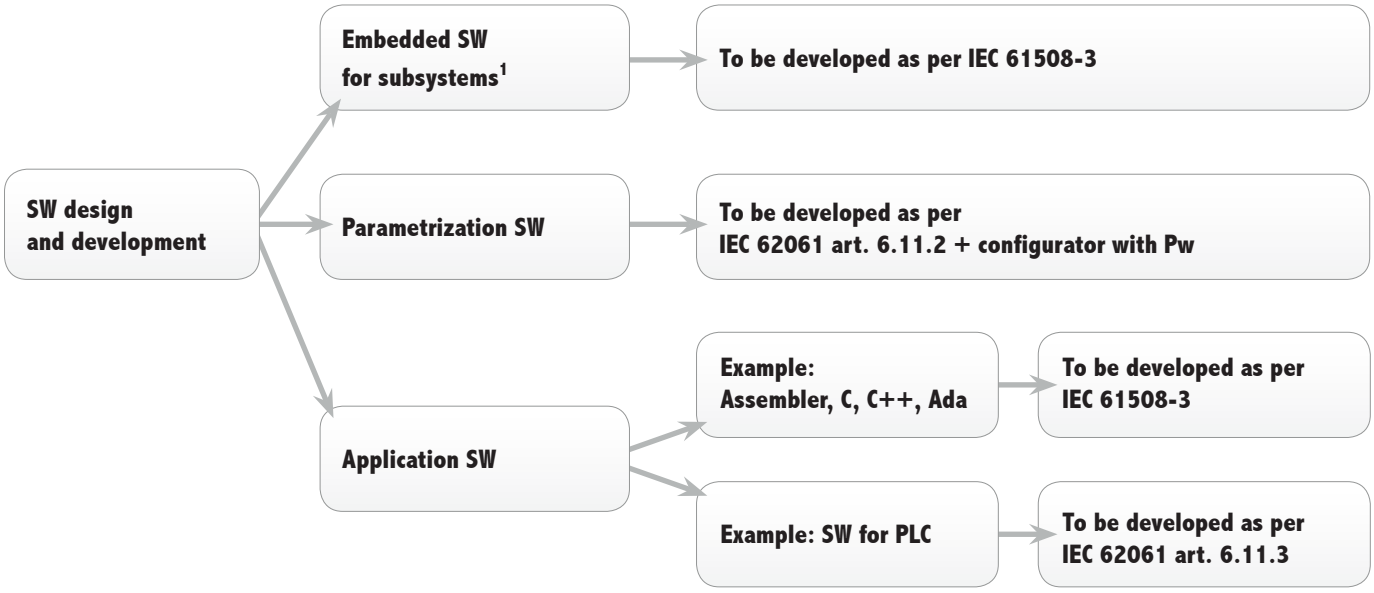
Each subsystem shall consist of electrical circuits suited to attain the required SIL.

The maximum SIL attainable by a subsystem is identified as SILCL (SIL claim).

Subsystem SILCLs depend on PFH_d, architecture constraints, performance under failure conditions and on the ability to control and avoid systematic failure.

Safety-related software

For software design, the code must be developed as per reference standards depending on the type of software in question as follows:



Note: Safety-related PLCs, safety bus, actuators, safety light curtains and in general all complex safety-related devices with integral programmable logics and embedded software, if used to build a SRECS, shall comply with the requirements of the appropriate Product Standards (if applicable) and with IEC 61508 as regards functional safety.

IMPORTANT!

The probability aspect is only one of the elements contributing to assignment of SIL.
To claim a specific SIL applicants must prove and document having:

- adopted adequate management actions and techniques to attain the required level of operational safety
- in place a documented and up-to-date Operational Safety Plan
- avoided systematic failure as far as possible
- evaluated (through inspections and tests) safety system performance in actual environmental conditions
- developed the software after adopting all organisational aspects required.

Calculation of subsystem PFH_d

To calculate subsystem PFH_d select first the type of architecture (structure). The Standard suggests four pre-defined architectures, providing a different simplified formula for each of them.

This calculation requires the use of the following parameters:

λ_d = Dangerous failure rate of each subsystem element.
Obtained from its known failure rate λ, percent distribution of failure rate for all failure modes and analysis of subsystem performance after failure (Dangerous Failure = λ_d or Non-dangerous Failure = λ_s).

T1 = Proof Test. Proof test interval (external inspection and repair returning the system to as-new condition) for industrial machinery usually coincides with life time (20 years).

T2 = Test interval of the diagnostic functions. Depending on design or devices used the diagnostic functions can be executed by internal circuitry of the same SRECS or by other SRECSs..

DC = Diagnostic Coverage:
Parameter representing the percent of dangerous failures detected out of all possible dangerous failures.
DC depends on self-diagnostic techniques implemented.
Assuming that failure is always possible (otherwise there would be no point in defining λ), that mechanisms for detecting failures are not necessarily all equally effective and responsive (depending on type of failure some may take longer), that it is impossible to detect all failures, that suitable circuitry architectures and effective testing may permit detection of most dangerous failures, a DC parameter may be defined for estimating the effectiveness of implemented self-diagnostic techniques.
IEC 62061 does not provide data for obtaining DC in relation to implemented diagnostic techniques. However, data of IEC 61508-2 Annex A may be used.

β = Common cause failure factor. Provides a measure of the degree of independence of operation of redundant channel systems.

Having calculated subsystem PFH_d by means of the formulas from the IEC 62061, it is important to ensure that the associated SILCL obtained from Table 3 of IEC 62061 (see page 21) is compatible with the constraints imposed by the architecture as the maximum SILCL attainable by a given subsystem is restricted by the hardware fault tolerance of the architecture and by SFF as listed in the following table

(Table 5 of IEC 62061)

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 safety failure fraction (SFF) is, by definition, the fraction of overall failure rate not involving dangerous failure

$$SFF = (\Sigma\lambda s + \Sigma\lambda dd) / (\Sigma\lambda s + \Sigma\lambda dd + \Sigma\lambda du).$$

λdd (failure rate of detectable dangerous failures) and λdu (failure rate of undetectable dangerous failures) are obtained from known effectiveness of implemented diagnostic techniques.

If PFH_d and SILCL of each subsystem are known, it will be possible to calculate the overall SIL of SRECS.

The overall probability of dangerous failure/hour of SRECS will equal the sum of the probabilities of dangerous failure/hour of all subsystem involved and shall include, if necessary, also the probability of dangerous failure per hour (PTE) of any safety-related communication lines:

$$PFH_d = PFH_{d1} + ... + PFH_{dN} + P_{TE}$$

Known the PFH_d, the resulting SIL of the SRECS is obtained from Table 3.

The SIL shall than be compared to the SILCL of each subsystem, as the SIL that can be claimed for the SRECS shall be less or equal to the lowest value of the SILCL of any of the subsystems.

Example:

$$PFH_d(system) = PFH_d\,(ss1) + PFH_d\,(ss2) + PFH_d\,(ss3) + P_{TE} = 5{,}56x10^{-7}/h$$

$$SIL = 2$$

Where a subsystem involves two or more safety-related functions requiring different SILs, the highest SIL shall apply.

CONCLUSIONS

The procedures specified in EN ISO 13849-1 simplify the estimation of Average Probability of Dangerous Failure per Hour compared to IEC 61508, offering a pragmatic approach more in line with the needs of the machine tool industry.

By retaining Categories and other basic concepts, such as safety-related function and risk graph, seamless continuity with EN 954: 1996 is assured.

Maintaining a closely linear approach with EN 954-1:1996 however, shows the limits of EN ISO 13849-1 / EN 954-1. Where the adoption of complex technology is anticipated , e.g. programmable electronics, safety-related bus applications, different architectures, etc., it will be more appropriate to design to IEC 62061.

Where devices and/or subsystems designed in accordance with EN ISO 13849-1 are used, Std. IEC 62061 shows how to integrate them in SRECS.

A precise bi-univocal equivalence between PL and SIL cannot be identified.

However, the probabilistic side of PL and SIL can be compared as they use the same concept, namely the Average Probability of Dangerous Failure per Hour, to define the extent to failure resistance.

Also, although the probability concept used in the two Standards is the same, the result may differ as the rigor of calculation is not the same.

In fact, for evaluating PFH_d, IEC 62061 specifies a procedure based on formulas derived from the system reliability theory. The results may in some cases, e.g. reduced number of components, high-efficiency of self-diagnostic techniques implemented, turn out to be very low, i.e. very good.

To simplify and speed up evaluation of Probability of Dangerous Failure per Hour, ISO 13849-1 uses approximation tables which must necessarily consider worst case scenarios, with consequently higher results, i.e. inferior to, than those calculated using IEC 62061.

Therefore, extra care must be exercised when calculating overall PL of a serial system such as the following:

If the resulting Probability of Dangerous Failure per Hour for the entire system is calculated as the sum of the PFH_d values of the parts computed by means of IEC 62061 and not using the calculation procedure as per ISO 13849-1, the limitations imposed to the parts by the categories which restrict max. PL attainable to that actually specified by ISO 13849-1 (see Table 5 of the Standard) must be taken into account.

Otherwise, a higher than actual system PL could result.

The following table may be used as a general guideline, noting that the ranges of Probability of Dangerous Failure per Hour should be compared, not the actual values of SIL and PL.

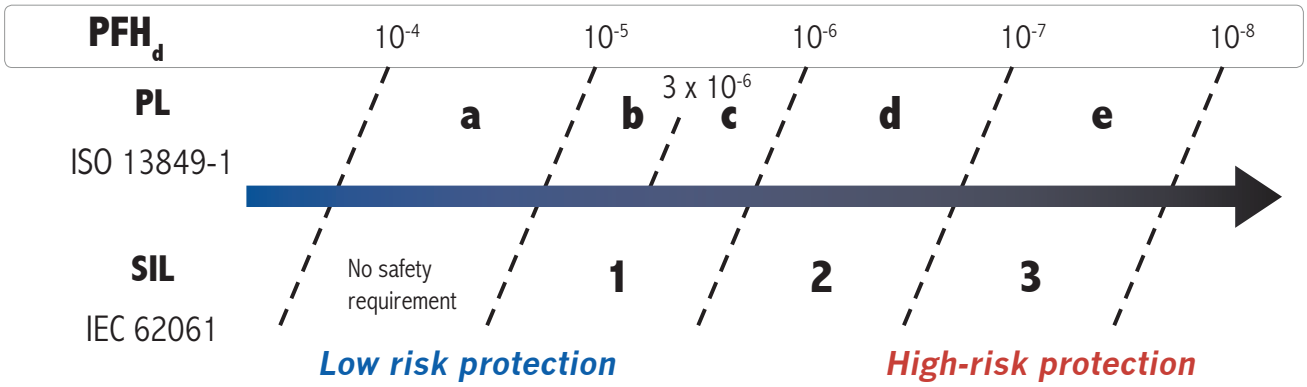


Fig. 9 - Requirements be met to satisfy the functional requirements and safety

Glossary

Initials	Definition	Standard	Description
β (Beta)	Common cause failure factor	IEC 62061	Degree of operational independence of channels of a multi-channel system. Ranging from 0.1 to 0.01 depending on CCF attained.
λ (Lambda)	Failure rate	IEC 62061	Random failure frequency. The time-random failure frequency of a component is usually known as Failure Rate, described as number of failures per unit of hour. Its inverse is known as Mean Time Between Failures (MTBF), expressed in hours. Random failures are the result of sudden stress accumulation above maximum design strength of a component. May occur at random intervals and entirely unexpectedly. Frequency of failure over sufficiently long periods is virtually constant. PFH_d calculation methods given in both Standards refer only to the assessment of random failures. 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).
λs	Safe failure rate	IEC 62061	Failure rate for non-dangerous failures. Non-dangerous failures which have no adverse safety-related effect on control system. The control system continues to ensure protection.
λd	Dangerous failure rate	IEC 62061	Failure rate of failures which may involve dangerous operation. Dangerous failures prevent the control system from continuing to provide protection.
λdd	Dangerous detected failure rate	IEC 62061	Failure rate for detectable dangerous failures. Detectable dangerous failures may be detected by automatic self-diagnostic systems.
λdu	Dangerous undetected failure rate	IEC 62061	Failure rate for undetectable dangerous failures. Undetectable dangerous failures cannot be detected by internal automatic self-diagnostic systems. They determine the value of PFH_d and, consequently, the value of SIL or PL.
Cat.	Category	ISO 13849-1	The Category is the main parameter to consider to attain a given PL. Describes the SRP/CS performance in relation to its ability to resist failure and resulting performance in failure conditions. Five Categories are envisaged depending on structural positioning of components.
CCF	Common Cause Failure	ISO 13849-1 IEC 62061	Failure resulting from common causes. Failure resulting from one or more events causing simultaneous malfunction of channels of a multi-channel system. Provides a measure of the degree of independence of redundant channel operation. Assessed by assigning marks. Maximum possible score is 100.
DC	Diagnostic Coverage	ISO 13849-1 IEC 62061	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%.
$MTTF_d$	Mean Time to dangerous Failures	ISO 13849-1	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.

Initials	Definition	Standard	Description
PFH_d	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, PLa to PLe. PLe represents the highest level of risk reduction, PLa the lowest level.
PLr	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. PLr 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.

PHOTOELECTRIC SAFETY LIGHT CURTAINS

CHARACTERISTIC ELEMENTS

Light curtains are electro sensitive devices using one or more light beams, emitted by an Emitter and received by a Receiver, to create an intangible controlled area. Fundamental characteristics are:

Safety type

- defines the self-monitoring and safety principles contained in the device;
- it must be chosen as a function of the risk level characterising the machine.

When the chosen safety device is a photo-electric barrier (**AOPD** Active Optoelectronic Protective Device), it shall necessary belong to **TYPE 2** or **TYPE 4** as established by the International Standard **IEC 61496 1-2**.

NOTE: why "Type" and not "Category"?
When talking about light curtains and laser scanners, we normally refer to their "safety type"; while for all other safety devices the term of choice is "safety category". This distinction is due to the International Standard IEC 61496, in which the term "type" is introduced to determine the safety level of optoelectronics protective equipment. In practice, "type" adds some optical requirements to the requirements which define categories for non-optical safety devices. Therefore, a type 2 light curtain is a light curtain which complies with the requirements for category 2 safety electronics and furthermore whose beams have certain characteristics, among which a given aperture angle, immunity to light interference and so on. The same applies for type 4 light curtains and type 3 laser scanners.

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%.

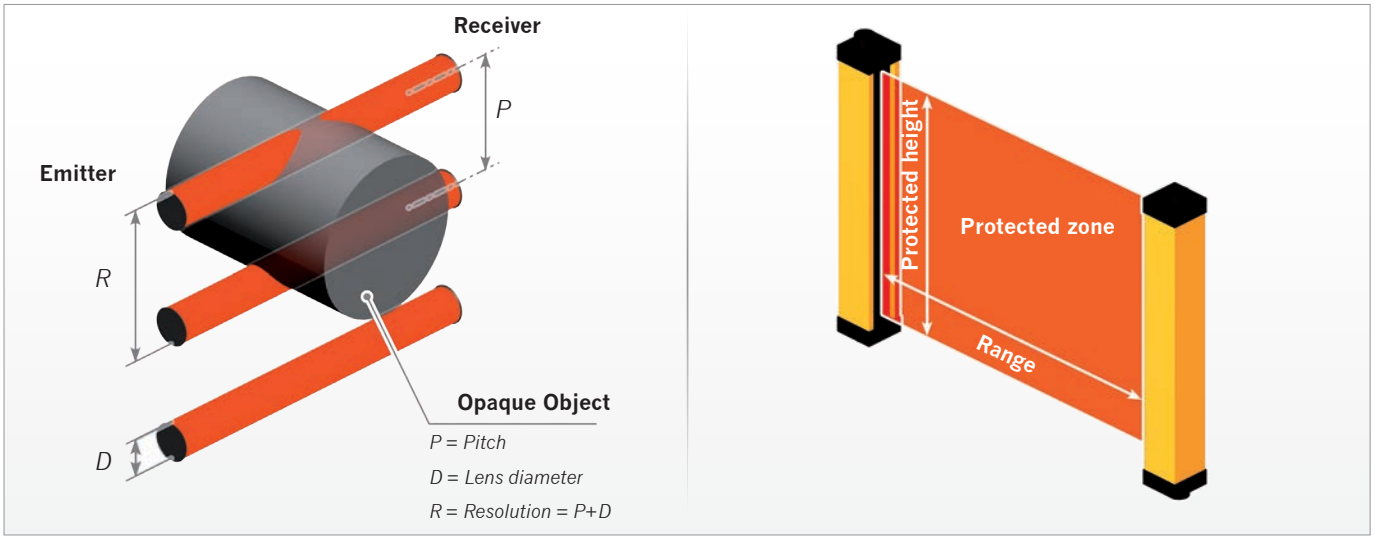
Response time

This is the time it takes for the light curtain to transmit the alarm signal from the time the protected zone is interrupted.

Resolution

The resolution of a light curtain 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. **R = D**
- Multibeam light curtains: their resolution **R** is the same as the sum of the lens diameter + the distance between two adjacent lenses. **R = P + D**



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.

CONDITIONS OF USE

For the photoelectric safety protections to be effective, it is necessary to verify that:

- It must be possible to electrically interface them to the control unit of the machine.
- It must be possible to stop the hazardous movements of the machine at once. In particular, it is important to know the machine stopping time to place the light curtain at the correct distance.
- The time taken to reach the hazardous point must be greater than the time necessary to stop the hazardous movement.
- The machine must not create secondary dangers due to the projection or fall from above of materials. If this danger exists, additional protections of a mechanical nature have to be provided.
- The minimum size of the object to be detected must be equal to or greater than the chosen light curtain resolution.

PHOTOELECTRIC SAFETY LIGHT CURTAINS

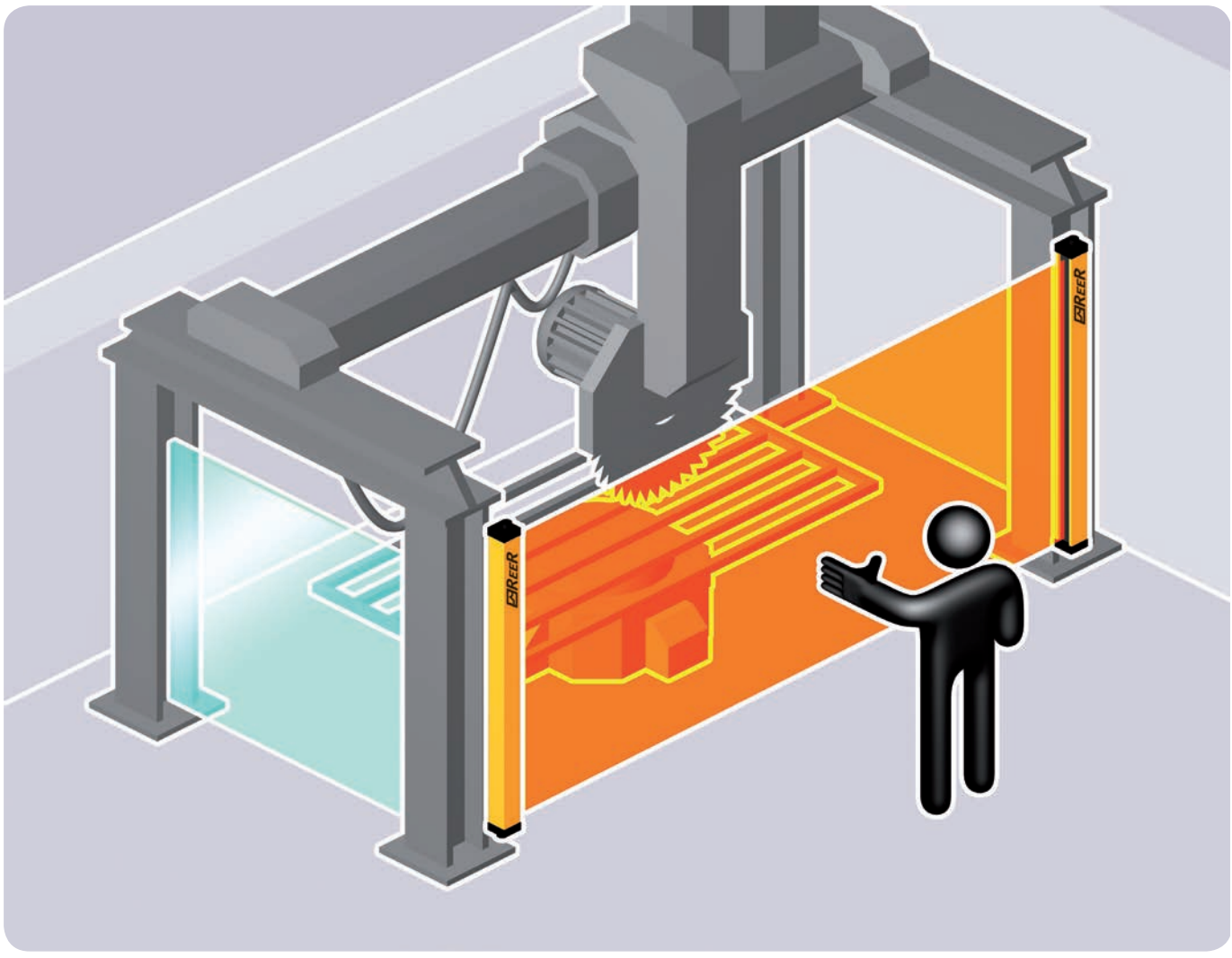
SELECTION CRITERIA OF A SAFETY LIGHT CURTAIN

1. **Definition of the zone to be protected.**
2. **Definition of the parts of the body to be detected:**
   - fingers or hands
   - approaching body of a person
   - presence of a person in a hazardous area.
3. **Definition of the safety distance between the light curtain and the hazardous point.**
4. **Definition of the safety category Level/Type to be adopted according to ISO 13849-1, IEC 62061, IEC 61496**

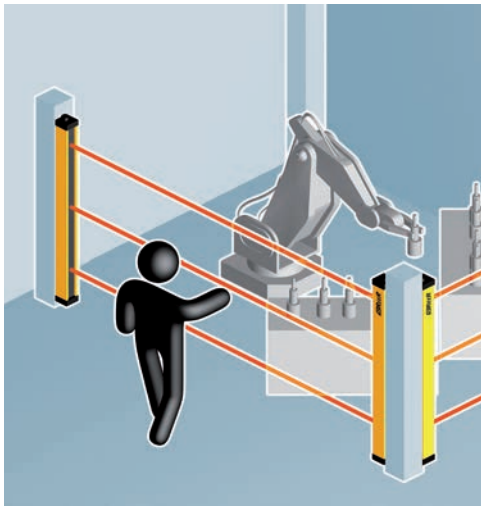
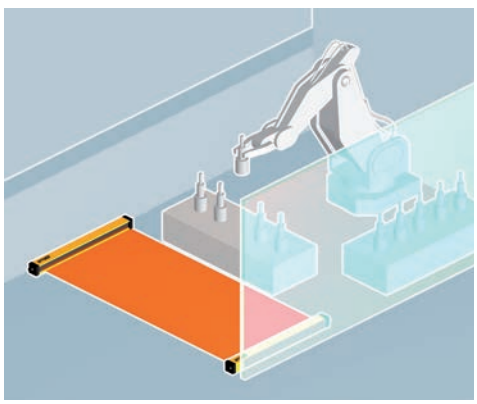
DEFINITION OF THE ZONE TO BE PROTECTED

- Take into account the configuration of the zone:
  - shape and dimensions: width and height of the access area
  - positions of hazardous parts
  - possible access points.
- The light curtain must be positioned so as to prevent the access to the dangerous area from above, from below, and from the sides without having intercepted the field protected by the light curtain.

It is possible to install one or more deflection mirrors in order to protect areas with access from several sides. This results in a considerable reduction in costs, as this solution eliminates the need of installing many separate 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.

Note: 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 in compliance with IEC 61496-1.
- 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.

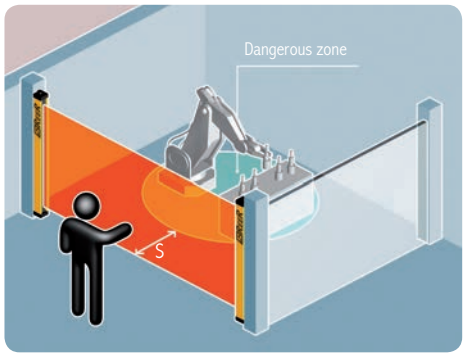
The light curtain must be positioned so that:

- 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).

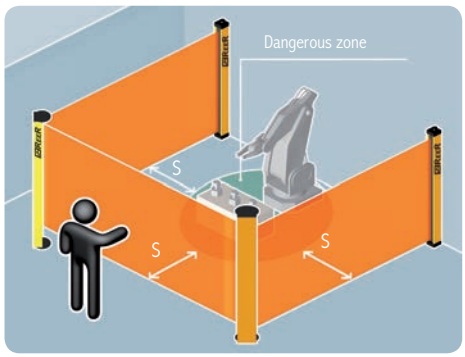
European Standard EN ISO 13855 provides the elements for the determination of the safety distance.

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:
a) to reduce the total stopping time of the machine,
b) to improve the detection capability (resolution) of the light curtain.



One-side protection



Three-side protection using deflection mirrors

GENERAL FORMULA FOR THE DETERMINATION OF THE MINIMUM SAFETY DISTANCE

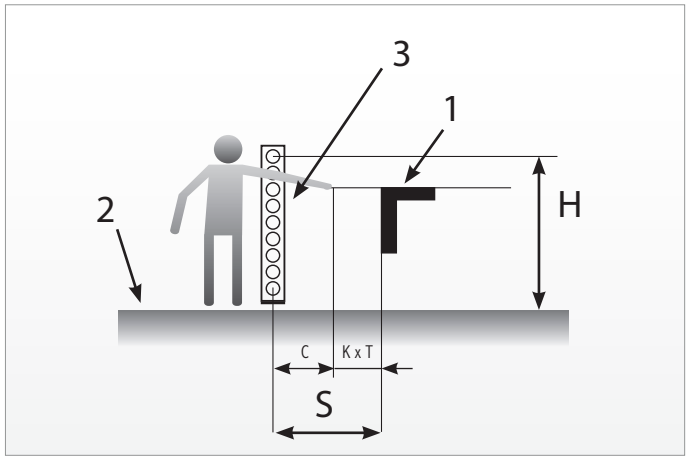
$$S = K \times T + C$$

S	minimum safety distance between the protection and hazardous point, expressed in mm.
K	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).
T	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.
C	additional distance in mm.

C takes into account:

1. Possible intrusion of parts of the body in the sensitive area before they are detected.
   For example**:**

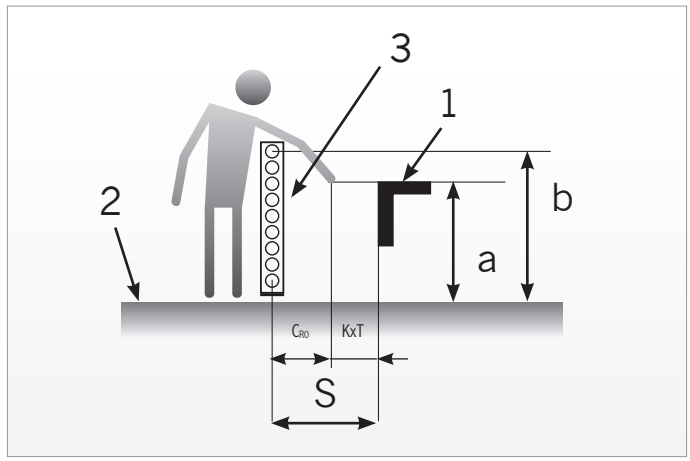
   - **C** = 8 x (d-14) If **d** (light curtain resolution) ≤ 40 mm
   - **C** = 850 If **d** (light curtain resolution) > 40 mm and for 2 - 3 - 4 beam light curtains
   - **C** = 1200 - (0,4 x H) for horizontal light curtains (**See pag. 38**)



1 = Dangerous area **2** = Reference plane **3** = Light curtain

2. The dangerous point can be reached by leaning over the upper edge of the sensitive area of a vertical light curtain.
   In this case C, called "$\mathbf{C_{RO}}$" is obtained from the following Table 2 of EN ISO 13855 / EN 999.

   Note:
   - Interpolation is not allowed.
   - If distances a, b or C_{RO} fall between values listed in the table, use the higher.
   - $\mathbf{C_{RO}}$ (reaching over) calculated using Table 2 of EN ISO 13855 / EN 999 must be compared to **C** as conventionally calculated (see paragraph 1).
     Always select the higher value.



1 = Dangerous area **2** = Reference plane **3** = Light curtain

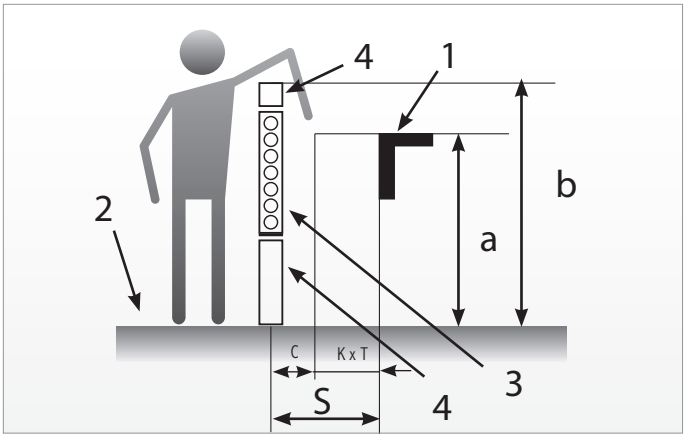
Height of Hazard zone "a"	**Height "b" of upper edge of area protected by photoelectric curtain**											
	900	1000	1100	1200	1300	1400	1600	1800	2000	2200	2400	2600
	Alternative distance C_{RO}											
2600	0	0	0	0	0	0	0	0	0	0	0	0
2500	400	400	350	300	300	300	300	300	250	150	100	-
2400	550	550	550	500	450	450	400	400	300	250	100	-
2200	800	750	750	700	650	650	600	550	400	250	-	-
2000	950	950	850	850	800	750	700	550	400	-	-	-
1800	1100	1100	950	950	850	800	750	550	-	-	-	-
1600	1150	1150	1100	1000	900	800	750	450	-	-	-	-
1400	1200	1200	1100	1000	900	850	650	-	-	-	-	-
1200	1200	1200	1100	1000	850	800	-	-	-	-	-	-
1000	1200	1150	1050	950	750	700	-	-	-	-	-	-
800	1150	1050	950	800	500	450	-	-	-	-	-	-
600	1050	950	750	550	-	-	-	-	-	-	-	-
400	900	700	-	-	-	-	-	-	-	-	-	-
200	600	-	-	-	-	-	-	-	-	-	-	-
0	-	-	-	-	-	-	-	-	-	-	-	-

(Tabel 2 of ISO 13855/EN 999)

PHOTOELECTRIC SAFETY LIGHT CURTAINS

3. For combined mechanical and electrosensitive protections (as shown), where it would be possible to lean against the mechanical protection and bypass the light curtain, for the calculation of the parameter **C** should use the Table 1 (for low risk applications) or the 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.



1 = Dangerous area **2** = Reference plane **3** = Light curtain
4 = Mechanical protection

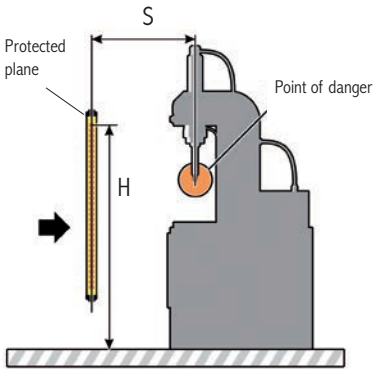
When calculating the safety distance, also consider installation tolerances, accuracy of the measured response time and possible decay of the brake system performance of the machine.

Where brake system decay is possible, use a stopping performance monitor device (SPM).

PHOTOELECTRIC SAFETY LIGHT CURTAINS

DIRECTION OF APPROACH PERPENDICULAR TO THE PROTECTED PLANE WITH α=90° (± 5°)

Light curtains with resolution for the detection of hands and fingers.
Light curtains resolution (d) ≤ 40 mm



Determination of the minimum safety distance (**S**)

Refer to the general formula for the determination of the minimum safety distance.

S = K x T + C

S = 2000xT + 8x(d-14)

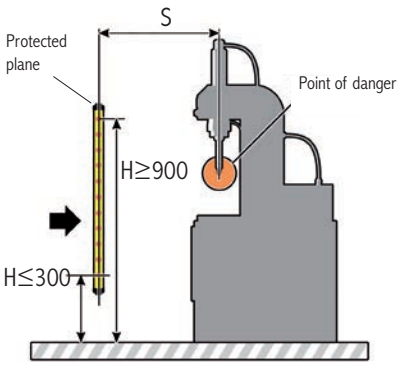
if the formula as a result: **S**> 500 you can use K = 1600

S = 1600xT + 8x(d-14)

► **For C values see pag. 35**

- 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.
- In these circumstances, the distance must in no case be lower than 500 mm.

Light curtains with a resolution for detection of arms and legs.
40 mm < Light curtains resolution (d) ≤70 mm



Refer to the general formula for the determination of the minimum safety distance.

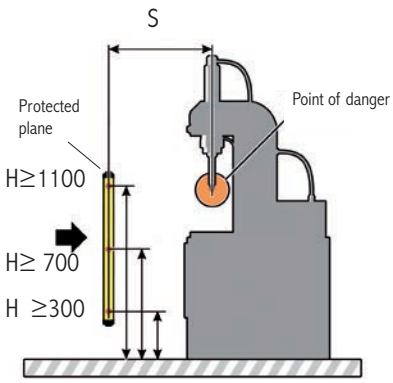
S = K x T + C

S = 1600xT + 850

► **For C values see pag. 35**

- The height of the lowest beam must be equal to or lower than 300 mm.
- The height of the uppest beam must be equal to or higher than 900 mm.

Light grids for body detection through access control.
Light curtains resolution (d) >70 mm



Refer to the general formula for the determination of the minimum safety distance.

S = K x T + C

S = 1600xT + 850

► **For C values see pag. 35**

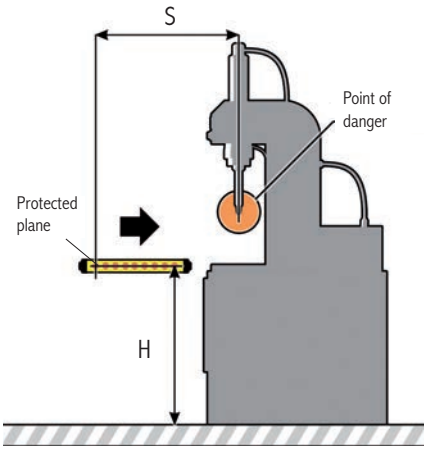
Number and height of the beams

N.	Recommended height
2	400 - 900 mm
3	300 - 700 - 1100 mm
4	300 - 600 - 900 - 1200 mm.

PHOTOELECTRIC SAFETY LIGHT CURTAINS

DIRECTION OF APPROACH PARALLEL TO THE PROTECTED PLANE WITH α=0° (± 5°)

Horizontal light curtains for presence control in a dangerous area.



Refer to the general formula for the determination of the minimum safety distance.

S = K x T + C

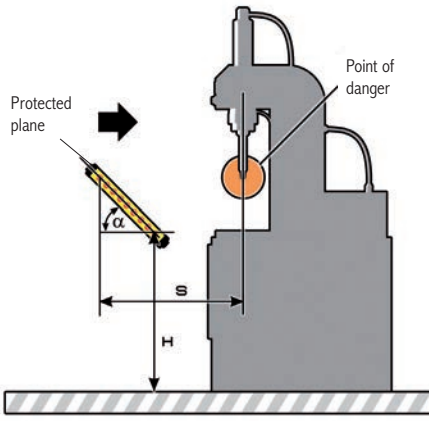
S = 1600xT + (1200-0,4xH)

► **For C values see pag. 35**

- C = 1200 - (0,4 x 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 x (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.

DIRECTION OF APPROACH ANGLED TO THE PROTECTED PLANE WITH 5°< α <85°

Slanted light curtains to detect hands and arms and for presence control in the dangerous area.



- With angle α >30° refer to the case of approach perpendicular to the protected plane. (Previous case)
- With angle α <30° refer to the case of approach parallel to the protected plane. (cases of previous page)

With α >30°:

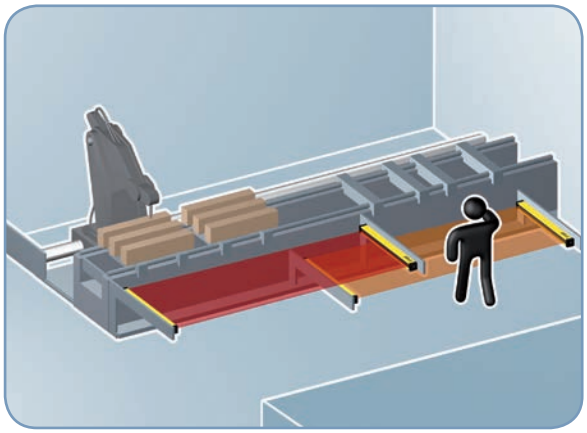
- The distance S refers to the beam farthest away from the hazardous point.
- The height of the beam farthest away from the hazardous point must not be greater than 1000 mm.
- For the determination of height H or resolution d apply the following formulas to the lowermost beam:
  H = 15 x (d - 50)
  d = H / 15 + 50

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:

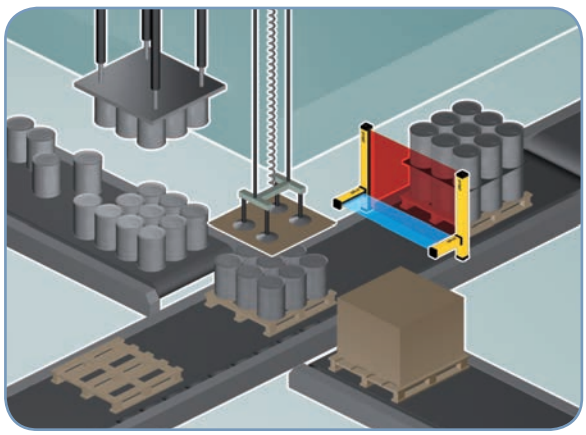
1. Enabling personnel access inside dangerous area during the non-dangerous part of machine cycle.



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 415-4	"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 hardwired signals triggered by a correct time or space sequence.
- 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:

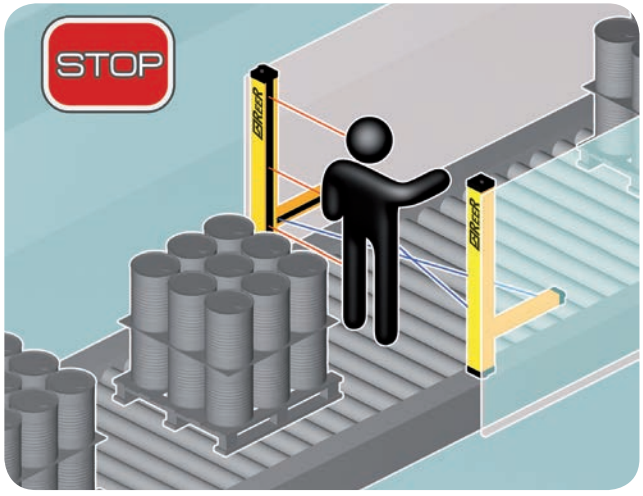
- Monitor the load, not the pallet, otherwise the operator might go into the hazardous zone being dragged by the pallet.
- Muting time must be restricted to the actual time taken by the material to pass through the opening.
- Muting must be time-restricted.
- Sensor mismatch with effect similar to their 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.

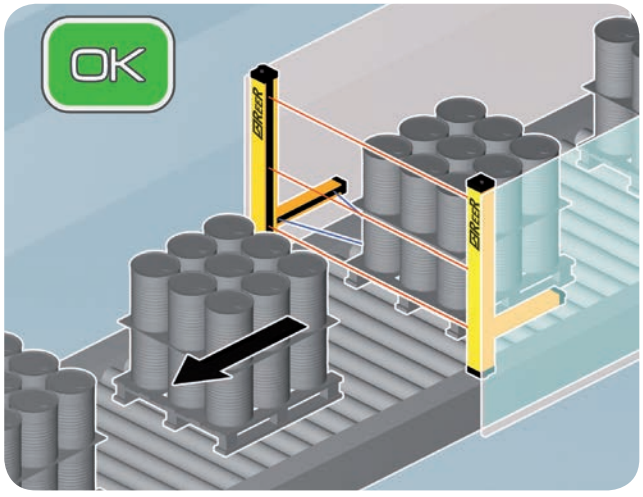
Therefore it is necessary to realise a safety system able to distinguish between:

- **authorized materials**
- **non authorized people**

→ **to go through the light curtain**

The Muting function can be present on both type 2 and type 4 safety light curtains.

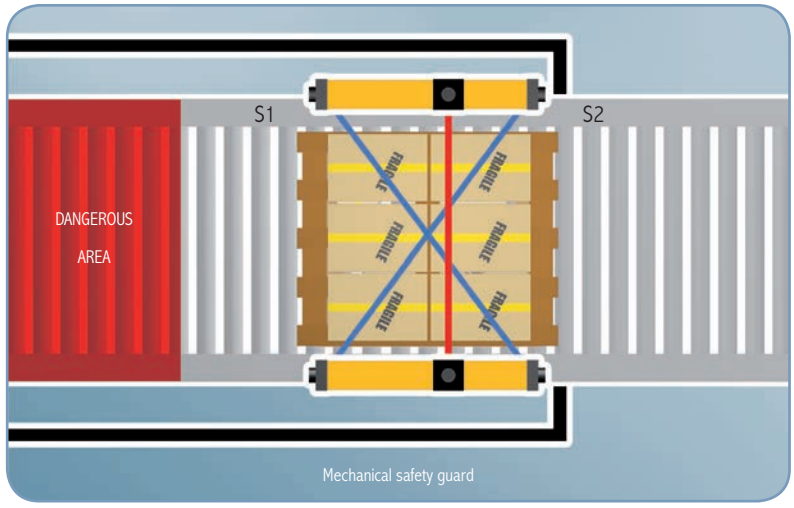




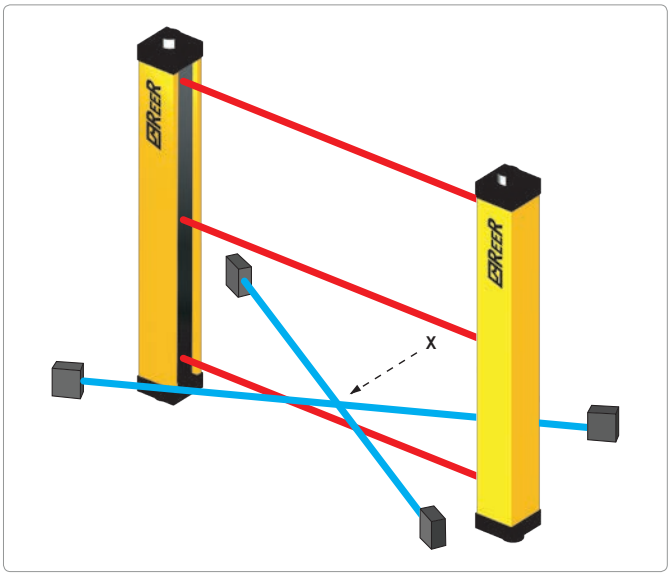
Common solutions for Muting sensor positioning

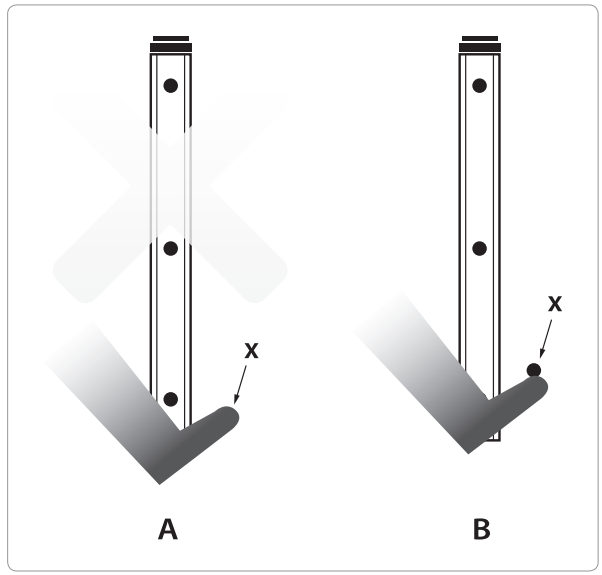
Muting with 2 crossed-beam sensors – Configuration type T with timing monitoring and two-way pallet operation:

- 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: (t2(S2) – t1(S1) = 4 seconds max.).
- The two beams shall be continuously interrupted by the pallet throughout the transit through the sensors.
- A matt cylindrical object D=500 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.

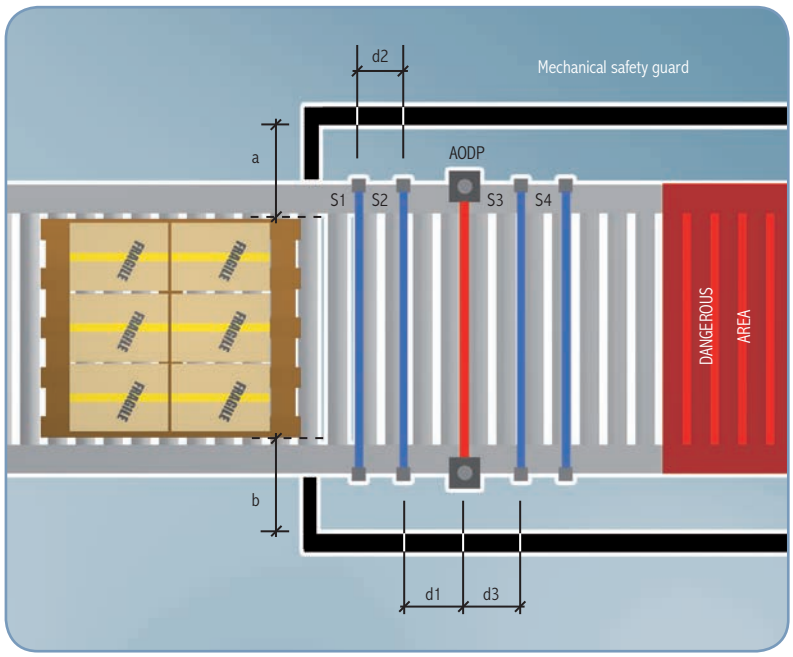




PHOTOELECTRIC SAFETY LIGHT CURTAINS

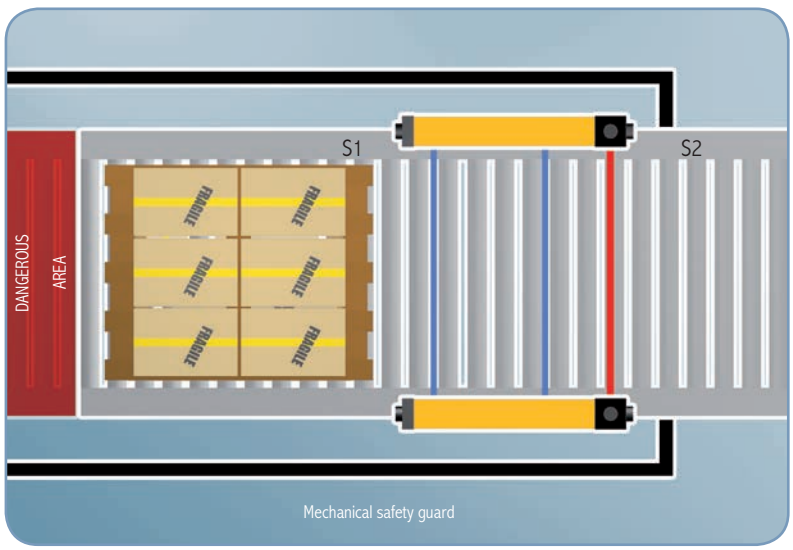
Muting with 4 parallel-beam sensors – Configuration type T with timing and/or sequence monitoring - Two-way pallet operation:

- 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.



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 and in accordance with a configurable operating logic.

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.

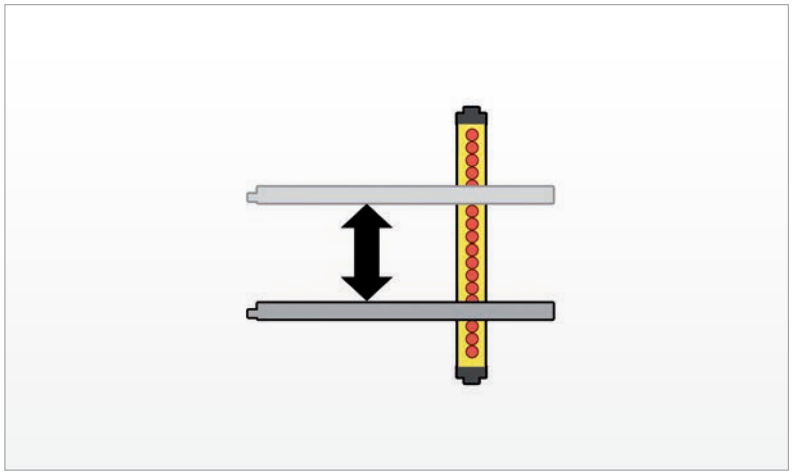
In practice, it is possible to keep the light curtain's safety outputs in an ON condition, and the machine working, even if a pre-determined number of beams within the protection fields are being intercepted.

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 that may be 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.
ReeR SpA does not assume responsibility for the improper use of the blanking function nor for the possible damages deriving from it.
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 Safety Laser Scanner is an electro-sensitive device for the protection of operators against the risk of accidents caused by industrial machines and plants with potentially dangerous moving parts and against possible collisions with Automatic Guided Vehicles (AGV).

For **EN 61496-3**, Laser Scanners must be certified in accordance to **type 3** or lower (**AOPDDR** Active Optoelectronics Protective Device responsive to Diffuse Reflection).

For **IEC 61508, IEC 62061, ISO 13849-1**, they must be certified as **SIL 2 - PLd** 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.

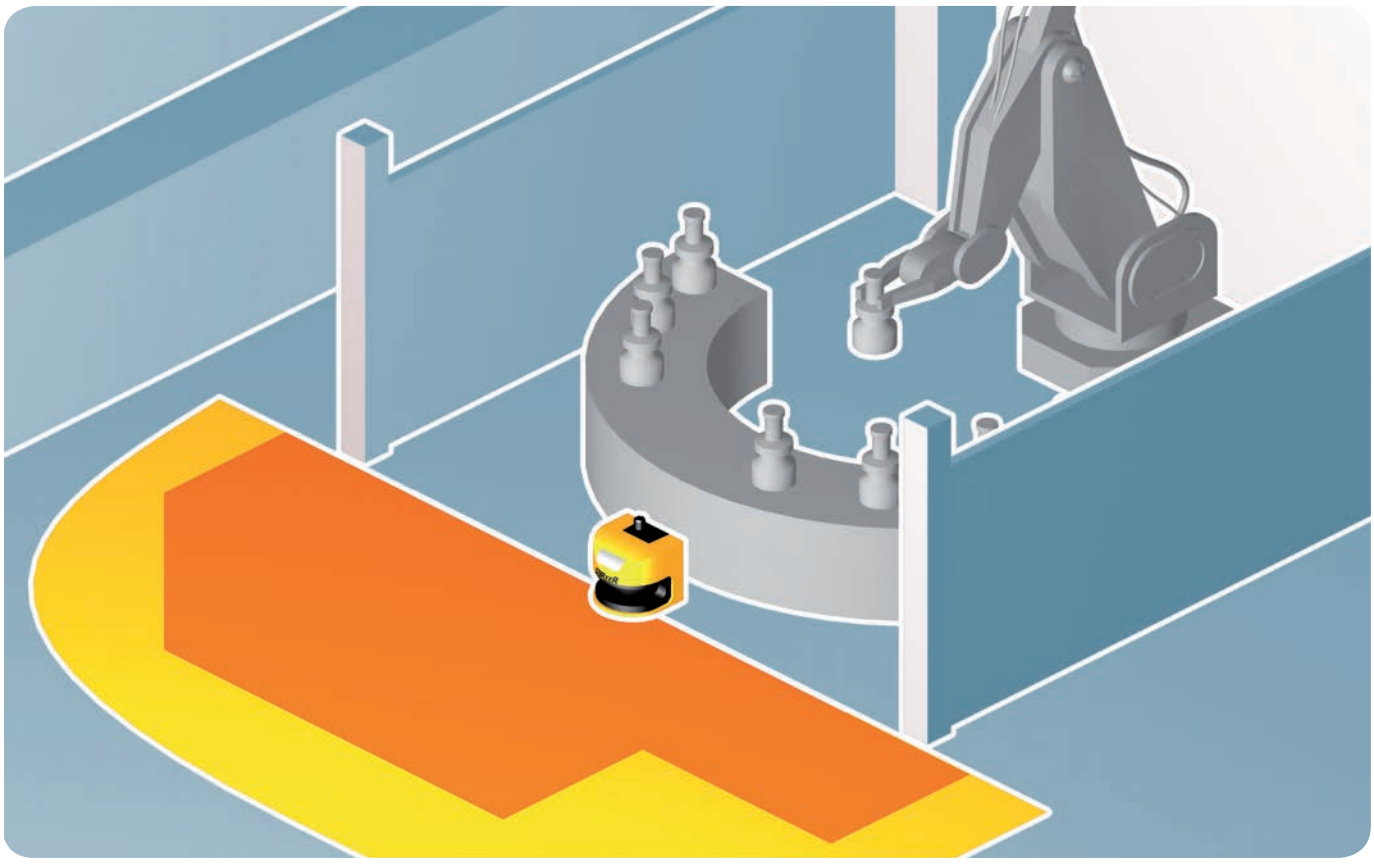
It is also possible to use the Laser Scanner in a **vertical** position for the access protection to a dangerous area, in that case detection of the edge of the gate is mandatory (**IEC TS 62046**).

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.

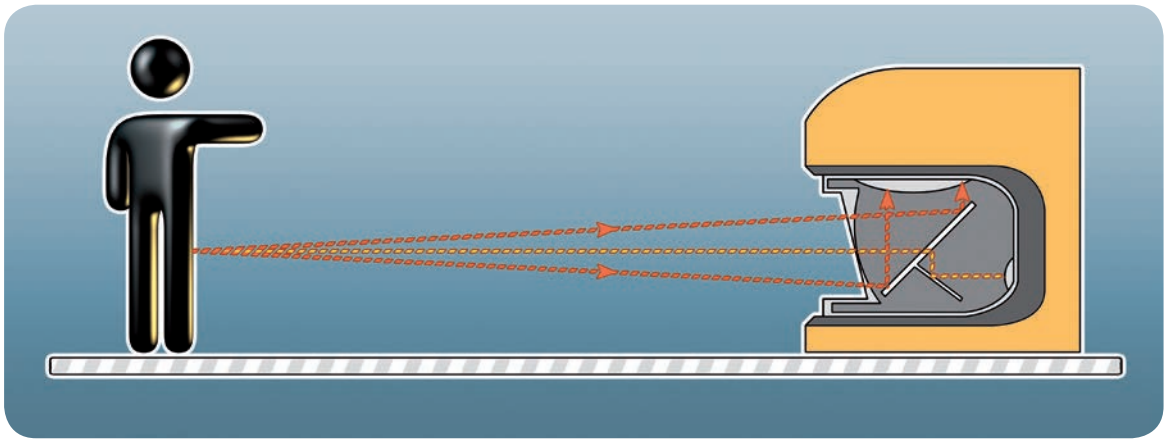
The Laser Scanner is also able to automatically detect the controlled area by means the teach-in function.



OPERATING PRINCIPLE OF THE LASER SCANNER PHARO

The Safety Laser Scanner Pharo emits ultra-short infrared laser light pulses. If the emitted beam hits an obstacle inside the controlled zone, then part of the light is reflected back towards the point of emission.

With its state-of-the-art technology, the Laser Scanner is able to measure the time (billionth of second) taken by the light to travel across the space between the sensor and the obstacle and back and to convert it into a distance with a precision of 3 cm.

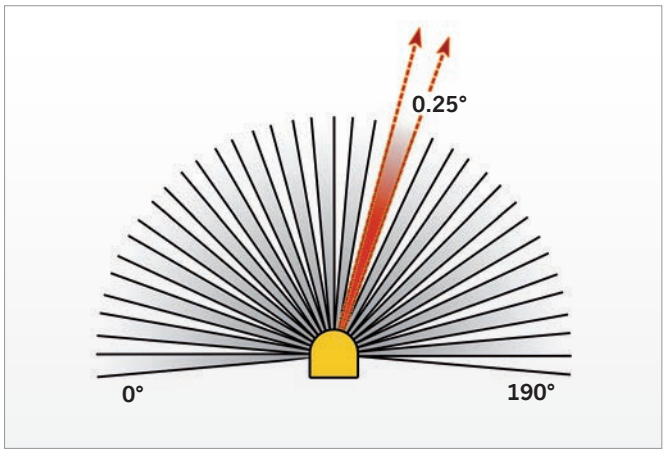


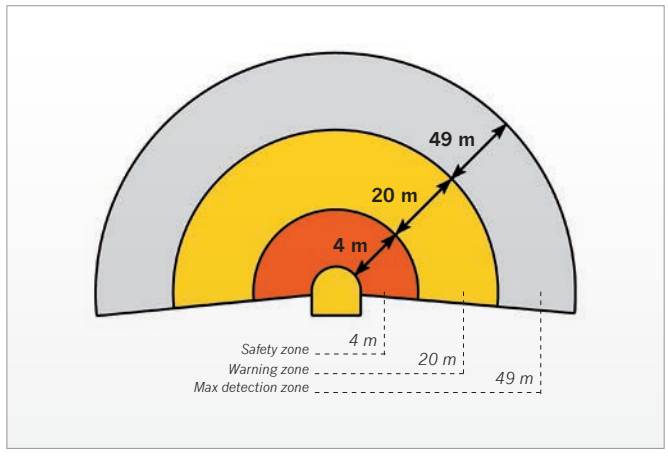
Using a rotating optical system, these measurements are made on a 190° semi-circular area every 0.25° for a total of 760 measurements per scan. The device performs 33 scans per second.

The Safety Laser Scanner Pharo creates a **controlled safety area with a maximum radius of 4 meters and a warning area with a maximum radius of 20 meters**. The safe detection of a person inside the safety zone is assured independently from the reflectivity of its clothes or skin.

The shape of the two controlled areas is fully programmable. Therefore, for each of the 760 measurements per scan, the laser scanner will compare the programmed distance to the measured distance.

If the measured distance is less than the programmed one, this means that an obstacle is inside the safety zone. A stop command will thus be sent to the machine.





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.

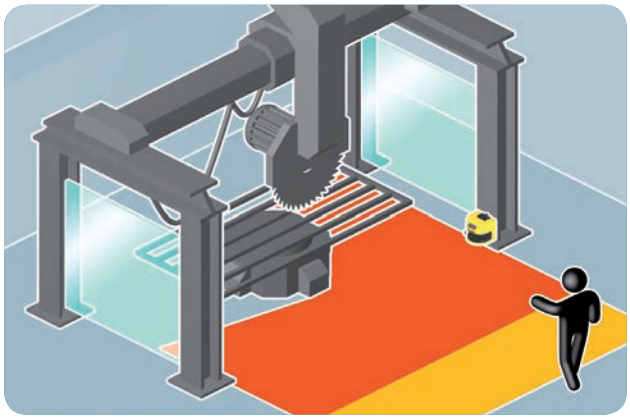
The occupation of this zone causes the switching of the auxiliary output that can be used to activate light or sound signals or in order to slow down the hazardous movement.

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

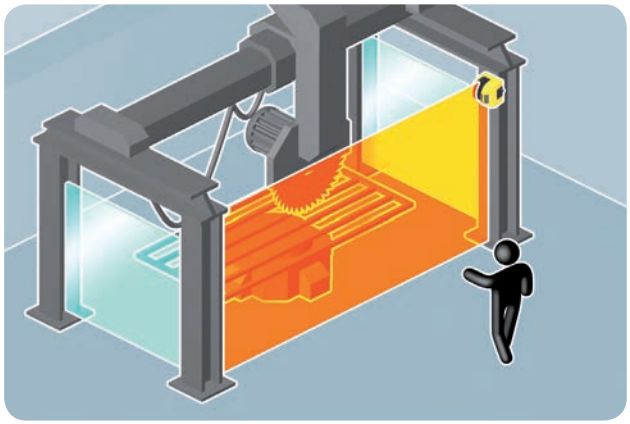
- No receiving and reflecting elements.
- Simple programming of differently-shaped controlled areas.
- Monitoring and protection of large areas.
- Horizontal mount for the detection of the body in a dangerous area.
- Vertical mount for the detection of hands and arms or for the detection of the body in access control.
- Use on moving vehicles (AGVs).
- Measurement of object size, shape and position.
- Fast and reliable installation.

APPLICATIONS



Area control

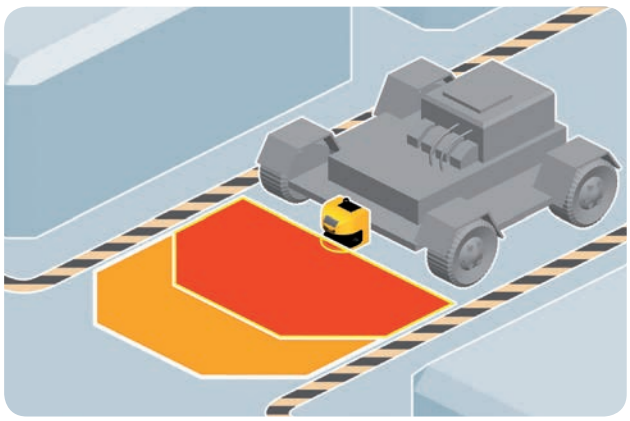
Example of an horizontally mounted protective field permanently monitored by Pharo. In this way a larger area can be monitored through the detection of the lower limbs of the body.



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 / access control 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.

INTEGRATION OF THE ESPE

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 this analysis.

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.

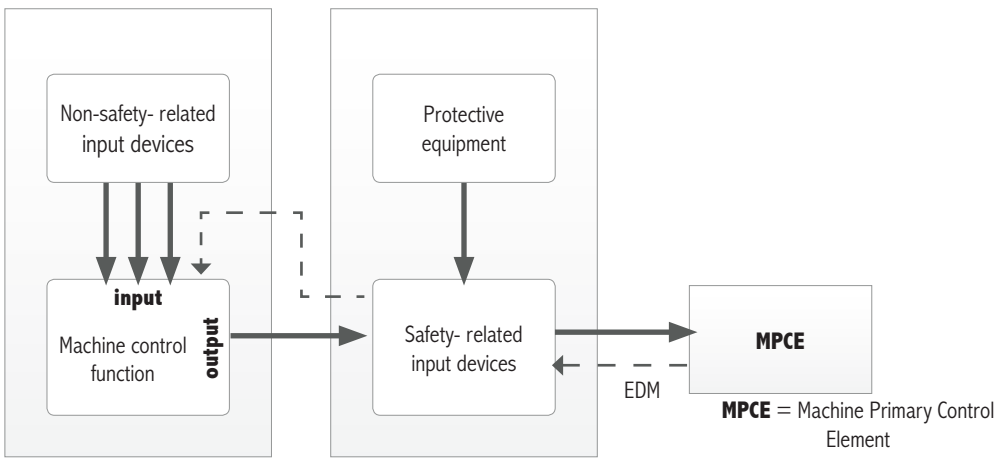
Also consider that the overall safety integrity of the serial connection: input – control unit – actuators, shall necessarily be equal to or lower than that of the weaker device.

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.

Figure 1 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.

Figure 1



If the machine is equipped with an integrated safety-related control and management system (safety-related PLC), see figure 2, machine operational functions and safety-related functions should be governed through the centralized safety-related system.

Figure 2