Principles, Standards, & Implementation

Regulations

EU Directives and Legislation

The purpose of this section is to act as a guide for anyone concerned with machine safety especially guarding and protective systems in the European Union. It is intended for designers and users of industrial equipment.

In order to promote the concept of an open market within the European Economic Area (EEA) (which comprises all EU Member States plus three other countries) all member states are obliged to enact legislation that defines essential safety requirements for machinery and its use.

Machinery that does not meet these requirements cannot be supplied into or within EEA countries.

There are several European Directives that can apply to the safety of industrial machinery and equipment but the two that are of the most direct relevance are:

1. The Machinery Directive
2. The Use of Work Equipment by Workers at Work Directive

These two Directives are directly related as the Essential Health and Safety Requirements (EHSRs) from the Machinery Directive can be used to confirm the safety of equipment in the Use of Work Equipment Directive.

This section deals with aspects of both directives and it is strongly recommended that anyone concerned with the design, supply, purchase or use of industrial equipment within or into the EEA and also certain other European countries should familiarize themselves with their requirements. Most suppliers and users of machinery will simply not be allowed to supply or operate machinery in these countries unless they conform to these directives.

There are other European Directives that may have relevance to machinery. Most of them are fairly specialized in their application and are therefore left outside the scope of this section but it is important to note that, where relevant, their requirements must also be met. Examples are: The EMC Directive 2004/108/EC and the ATEX Directive 94/9/EC.

The EU Machinery Directive

The Machinery Directive covers the supply of new machinery and other equipment including safety components. It is an offense to supply machinery within the EU unless the provisions and requirements of the Directive are met.

The broadest definition of “machinery” given within the Directive is a follows: an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application.

Detailed information and guidance on the definition and all other aspects of the Machinery Directive can be found at the official EU website:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm

The current Machinery Directive (2006/42/EC) replaced the former version (98/37/EC) at the end of 2009. It clarifies and amends but does not introduce any radical changes to its Essential Health and Safety Requirements (EHSRs). It does introduce some changes to take account of changes in technology and methods. It extends its scope to cover some extra types of equipment (e.g. construction site hoists). There is now an explicit requirement for a risk assessment for the determination of which EHSRs are applicable and there are changes made to the conformity assessment procedures for Annex IV equipment.

The key provisions of the original Directive (98/37/EC) came into force for machinery on January 1, 1995 and for Safety Components on January 1, 1997.

The provisions of the current Directive (2006/42/EC) became applicable on December 29, 2009. It is the responsibility of the manufacturer or his authorized representative to ensure that equipment supplied is in conformity with the Directive. This includes:

Figure 1: CE Marking Affixed to Machine

- Ensuring that the applicable EHSRs contained in Annex I of the Directive are fulfilled
- A technical file is prepared
- Appropriate conformity assessment is carried out
- An “EC Declaration of Conformity” is given
- CE Marking is affixed where applicable
- Instructions for safe use are provided

Essential Health and Safety Requirements

Annex 1 of the Directive gives a list of Essential Health and Safety Requirements (referred to as EHSRs) to which machinery must comply where relevant. The purpose of this list is to ensure that the machinery is safe and is designed and constructed so that it can be used, adjusted and maintained throughout all phases of its life without putting persons at risk. The following text provides a quick overview of some typical requirements but it is important to consider all of the EHSRs given in Annex 1.

A risk assessment must be carried out to determine which EHSRs are applicable to the equipment under consideration.

The EHSRs in Annex 1 provides a hierarchy of measures for eliminating the risk:

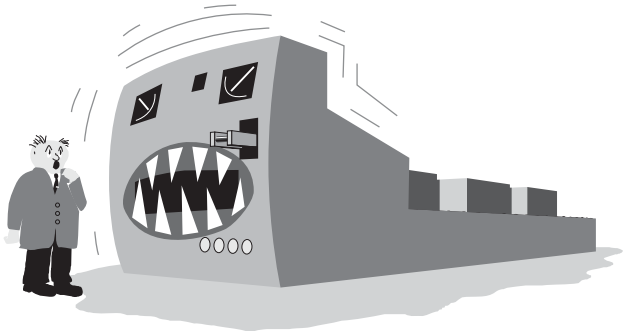


Figure 2: Machine Must Meet EHSRs

(1) Inherently Safe Design—Where possible the design itself will prevent any hazards.

Where this is not possible **(2) Additional Protective Measures**, e.g., Guards with interlocked access points, non-material barriers such as light curtains, sensing mats etc., should be used.

Any residual risk which cannot be dealt with by the above methods must be contained by **(3) Personal Protective Equipment and/or Training**. The machine supplier must specify what is appropriate.

Suitable materials should be used for construction and operation. Adequate lighting and handling facilities should be provided. Controls and control systems must be safe and reliable. Machines must not be capable of starting up unexpectedly and should usually have one or more emergency stop devices fitted. Consideration

must be given to complex installations where processes upstream or downstream can affect the safety of a machine. Failure of a power supply or control circuit must not lead to a dangerous situation. Machines must be stable and capable of withstanding foreseeable stresses. They must have no exposed edges or surfaces likely to cause injury.

Guards or protection devices must be used to protect risks such as moving parts. These must be of robust construction and difficult to bypass. Fixed guards must be mounted by methods that can only be removed with tools. Movable guards should be interlocked. Adjustable guards should be readily adjustable without the use of tools.

Electrical and other energy supply hazards must be prevented. There must be minimal risk of injury from temperature, explosion, noise, vibration, dust, gases or radiation. There must be proper provisions for maintenance and servicing. Sufficient indication and warning devices must be provided. Machinery shall be provided with instructions for safe installation, use, adjustment etc.

The Machinery Directive—Conformity Assessment and Standards

A harmonized European (EN) Standard that is listed in the Official Journal of the European Union (OJ) under the Machinery Directive, and whose date of cessation of presumption of conformity has not expired, confers a presumption of conformity with certain of the EHSRs. (Many recent standards listed in the OJ include a cross-reference identifying the EHSRs that is covered by the standard).

Therefore, where equipment complies with such current harmonized European standards, the task of demonstrating conformity with the EHSRs is greatly simplified, and the manufacturer also benefits from the increased legal certainty. These standards are not legally required, however, their use is strongly recommended since proving conformity by alternative methods can be an extremely complex issue. These standards support the Machinery Directive and are produced by CEN (the European Committee for Standardization) in cooperation with ISO, and CENELEC (the European Committee for Electrotechnical Standardization) in cooperation with IEC.

A thorough, documented risk assessment must be conducted to ensure that all potential machine hazards are addressed. It is the responsibility of the machine manufacturer to ensure that all EHSRs are satisfied, even those that are not addressed by harmonized EN Standards.

Technical File

The manufacturer or his authorized representative must prepare a Technical File to provide evidence of conformity with the EHSRs. This file should include all relevant information such as test results, drawings, specifications, etc.

It is not essential that all the information is permanently available as hard copy but it must be possible to make the entire Technical File available for inspection on request from a competent authority (a body appointed by an EU country to monitor the conformity of machinery).

At the minimum, the following documentation must be included in a Technical File:

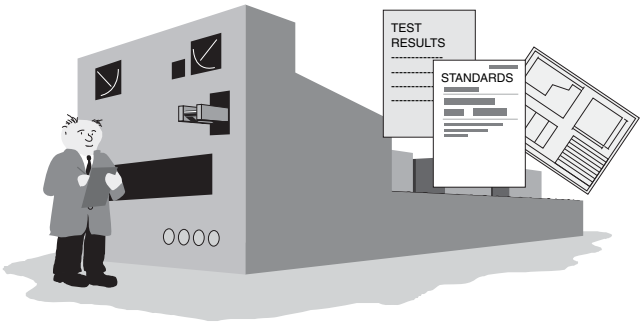


Figure 3: Document Assessment Results

1. Overall drawings of the equipment including control circuit drawings.
2. Detailed drawings, calculation notes, test results, etc. required for checking the conformity of the machinery with the EHSRs.
3. Risk assessment documentation, including a list of the essential health and safety requirements which apply to the machinery and a description of the protective measures implemented.
4. A list of the standards and other technical specifications used, indicating the essential health and safety requirements covered.
5. A description of methods adopted to eliminate hazards presented by the machinery.
6. If relevant, any technical reports or certificates obtained from a test facility or other body.
7. If conformity is declared with a Harmonized European Standard, any technical report giving test results for it.
8. A copy of the instructions for the machinery.
9. Where appropriate, the declaration of incorporation for included partly completed machinery and the relevant assembly instructions for such machinery.
10. Where appropriate, copies of the EC declaration of conformity of machinery or other products incorporated into the machinery.
11. A copy of the EC declaration of conformity.

For series manufacture, details of internal measures (quality systems, for example) to ensure all machinery produced remains in conformity:

- The manufacturer must carry out necessary research or tests on components, fittings or the completed machinery to determine whether by its design and construction it is capable of being erected and put into service safely.
- The technical file need not exist as a permanent single file, but it must be possible to assemble it to make it available in a reasonable time. It must be available for ten years following production of the last unit.

The technical file does not need to include detailed plans or any other specific information regarding sub-assemblies used for the manufacture of the machinery, unless they are essential to verify conformity with the EHSRs.

Conformity Assessment

Certain types of equipment are subject to special measures. This equipment is listed in Annex IV of the Directive and includes dangerous machines such as some woodworking machines, presses, injection molding machines, underground equipment, vehicle servicing lifts, etc.

Annex IV also includes certain safety components such as Protective devices designed to detect the presence of persons (e.g. light curtains) and logic units for ensuring safety functions.

Figure 4: Conformity Assessments

For Annex IV machines that are not in full conformity with the relevant Harmonized European Standards the manufacturer or his authorized representative must apply one of the following procedures:

1. **EC Type Examination**. A Technical File must be prepared and an example of the machine must submitted to a notified body (test house) for EC type examination. If it passes, the machine will be given an EC type examination certificate. The validity of the certificate must be reviewed every five years with the Notified Body.
2. **Full Quality Assurance**. A Technical File must be prepared and the manufacturer must operate an approved quality system for design, manufacture, final inspection and testing. The quality system must ensure conformity of the machinery with the provisions of this Directive. The quality system must be periodically audited by a Notified Body.

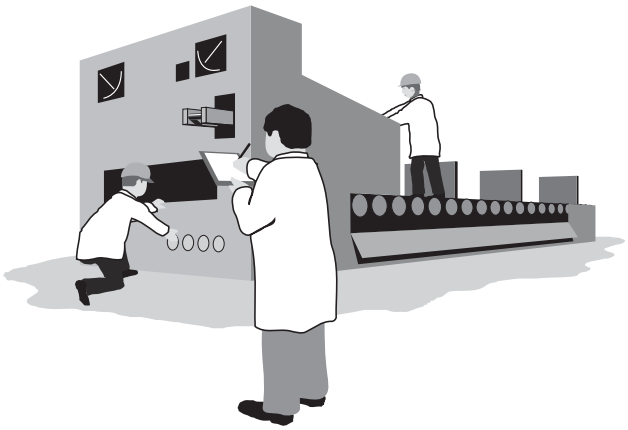


Figure 5: Notified Body Examinations

For machines that are not included in Annex IV or machines that are included in Annex IV but are in full conformity with the relevant Harmonized European Standards, the manufacturer or his authorized representative also has the option prepare the Technical and self assess and declare the conformity of the equipment. There must be internal checks to ensure that the manufactured equipment remains in conformity.

Notified Bodies

A network of notified bodies that communicate with each other and work to common criteria exists throughout the EU. Notified Bodies are appointed by governments (not by industry) and details of organizations with notified body status can be obtained from: *http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm*

EC Declaration of Conformity Procedure

The CE Marking must be applied to all machines supplied. The machines should also be supplied with an EC Declaration of Conformity.

CE

Figure 6: CE Mark

The CE Mark indicates that the machine conforms to all applicable European Directives and that the appropriate conformity assessment procedures have been completed. It is an offense to apply the CE Mark for the Machinery Directive unless the machine satisfies the relevant EHSRs.

The EC Declaration of Conformity must contain the following information:

- Business name and full address of the manufacturer and, where appropriate, the authorized representative;
- Name and address of the person authorized to compile the technical file, who must be established in the Community (in the case of a manufacturer outside the EU this may be the "Authorized Representative") ;
- Description and identification of the machinery, including generic denomination, function, model, type, serial number and commercial name;
- A sentence expressly declaring that the machinery fulfills all the relevant provisions of this Directive and where appropriate, a similar sentence declaring the conformity with other Directives and/or relevant provisions with which the machinery complies;
- Where appropriate, a reference to the harmonized standards used;
- Where appropriate, the reference to other technical standards and specifications used;
- (For an Annex IV machines) where appropriate, the name, address and identification number of the notified body which carried out the EC type-examination referred to in Annex IX and the number of the EC type-examination certificate;
- (For an Annex IV machines) where appropriate, the name, address and identification number of the notified body which approved the full quality assurance system referred to in Annex X;
- The place and date of the declaration;
- The identity and signature of the person empowered to draw up the declaration on behalf of the manufacturer or the authorized representative.

EC Declaration of Incorporation for Partly Completed Machinery

Where the equipment is supplied for assembly with other items to form a complete machine at a later date, a DECLARATION OF INCORPORATION should be issued with it. The CE mark should not be applied. The declaration should state that the equipment must not be put into service until the machine into which it has been incorporated has been declared in conformity. A Technical File must be prepared and the partly completed machinery must be supplied with information containing a description of the conditions which must be met with a view to correct incorporation in the final machinery, so as not to compromise safety.

This option is not available for equipment which can function independently or which modifies the function of a machine.

The Declaration of Incorporation must contain the following information:

- Business name and full address of the manufacturer of the partly completed machinery and, where appropriate, the authorized representative;
- Name and address of the person authorized to compile the relevant technical documentation, who must be established in the Community (in the case of a manufacturer outside the EU this may be the "Authorized Representative");
- Description and identification of the partly completed machinery including generic denomination, function, model, type, serial number and commercial name;
- A sentence declaring which essential requirements of this Directive are applied and fulfilled and that the relevant technical documentation is compiled in accordance with part B of Annex VII, and, where appropriate, a sentence declaring the conformity of the partly completed machinery with other relevant Directives;
- An undertaking to transmit, in response to a reasoned request by the national authorities, relevant information on the partly completed machinery. This shall include the method of transmission and shall be without prejudice to the intellectual property rights of the manufacturer of the partly completed machinery;
- A statement that the partly completed machinery must not be put into service until the final machinery into which it is to be incorporated has been declared in conformity with the provisions of this Directive, where appropriate;
- The place and date of the declaration;
- The identity and signature of the person empowered to draw up the declaration on behalf of the manufacturer or the authorized representative.

Machinery Supplied from Outside the EU—Authorized Representatives

If a manufacturer based outside the EU (or EEA) exports machinery into the EU they will need to appoint an Authorized Representative.

An Authorized Representative means any natural or legal person established in the European Community who has received a written mandate from the manufacturer to perform on his behalf all or part of the obligations and formalities connected with the Machinery Directive.

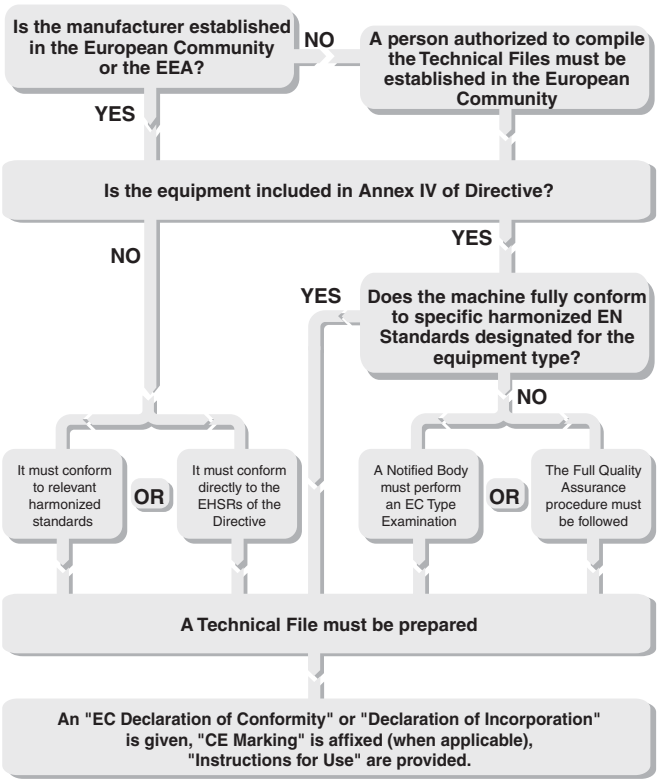


Figure 7: Overview of Procedures for the Machinery Directive

It is important to study the Directive (2006/42/EC) for full details.

The EU Use of Work Equipment Directive (U.W.E. Directive)

Whereas the Machinery Directive is aimed at suppliers, this Directive (89/655/EEC as amended by 95/63/EC, 2001/45/EC and 2007/30/EC) is aimed at users of machinery. It covers all industrial sectors and it places general duties on employers together with minimum requirements for the safety of work equipment. All EU countries are enacting their own forms of legislation to implement this Directive.

For example it is implementation in the UK under the name of The Provision and Use of Work Equipment Regulations (often abbreviated to P.U.W.E.R.). The form of implementation may vary between countries but the effect of the Directive is retained.

The articles of the Directive give details of which types of equipment and workplaces are covered by the Directive.

They also place general duties on employers such as instituting safe systems of working and providing suitable and safe equipment that must be properly maintained. Machine operators must be given proper information and training for the safe use of the machine.

New machinery (and second hand machinery from outside the EU) provided after January 1, 1993 should satisfy any relevant product directives, e.g., The Machinery Directive (subject to transitional arrangements). Second hand equipment from within the EU provided for the first time in the workplace must immediately provide minimum requirements given in an annex of the U.W.E. Directive.

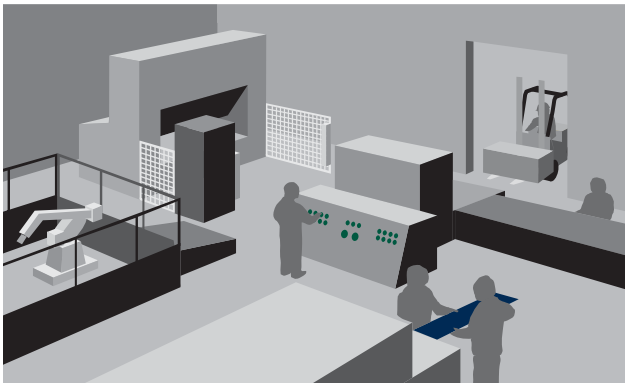


Figure 8: Directive Covers Use of Equipment

Note: Existing or second-hand machinery which is significantly overhauled or modified will be classified as new equipment, so the work carried out on it must ensure compliance with the Machinery Directive (even if it is for a company's own use).

Suitability of work equipment is an important requirement of the directive and it highlights the employer's responsibility to carry out a proper process of risk assessment.

It is a requirement that machinery must be properly maintained. This will normally mean that there must be a routine and planned preventive maintenance schedule. It is recommended that a log is compiled and kept up to date. This is especially important in cases where the maintenance and inspection of equipment contributes to the continuing safety integrity of a protective device or system.

The Annex of the U.W.E. Directive gives general minimum requirements applicable to work equipment.

If the equipment conforms to relevant product directives, e.g., The Machinery Directive, they will automatically comply with the corresponding machine design requirements given in the minimum requirements of the Annex.

Member states are allowed to issue legislation regarding the use of work equipment that goes beyond the minimum requirements of the U.W.E. Directive.

Detailed information on the Use of Work Equipment Directive can be found at the official EU website:
http://europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11116_en.htm

U.S. Regulations

This section introduces some of the industrial machine guarding safety regulations in the U.S. This is only a starting point; readers must further investigate the requirements for their specific applications and take measures to ensure that their designs, uses and maintenance procedures and practices meet their own needs as well as national and local codes and regulations.

There are many organizations that promote industrial safety in the United States. These include:

1. Corporations, which use established requirements as well as establish their own internal requirements;
2. The Occupational Safety and Health Administration (OSHA);
3. Industrial organizations like the National Fire Protection Association (NFPA), the Robotics Industries Association (RIA), the Association of Manufacturing Technology (AMT) and the suppliers of safety products and solutions such as Rockwell Automation.

Occupational Safety and Health Administration

In the United States, one of the main drivers of industrial safety is the Occupational Safety and Health Administration (OSHA). OSHA was established in 1970 by an Act of the U.S. Congress. The purpose of this act is to provide safe and healthful working conditions and to preserve human resources. The act authorizes the Secretary of Labor to set mandatory occupational safety and health standards applicable to businesses affecting interstate commerce. This Act shall apply with respect to employment performed in a workplace in a State, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, American Samoa, Guam, the Trust Territory of the Pacific Islands, Wake Island, Outer Continental Shelf Lands defined in the Outer Continental Shelf Lands Act, Johnston Island, and the Canal Zone.

Article 5 of the Act sets the basic requirements. Each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees; and shall comply with occupational safety and health standards promulgated under this Act.

Article 5 also states that each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.

The OSHA Act places the responsibility on both the employer and the employee. This is quite divergent from Machinery Directive, which requires suppliers to place machines on the market that are free from hazards. In the U.S., a supplier can sell a machine without any safeguarding. The user must add the safeguarding to make the machine safe. Although this was a common practice when the Act was approved, the trend is for suppliers to provide machines with the safeguarding, as designing safety into a machine is far more cost effective than adding the safeguarding after the machine is designed and built. Standards are now attempting to get the supplier and user to communicate requirements for safeguarding so that machines are made not only safe but more productive.

The Secretary of Labor has the authority to promulgate as an occupational safety or health standard any national consensus standard, and any established Federal standard, unless the promulgation of such a standard would not result in improved safety or health for specifically designated employees.

OSHA accomplishes this task by publishing regulations in Title 29 of the Code of Federal Regulation (29 CFR). Standards pertaining to industrial machinery are published by OSHA in Part 1910 of 29 CFR. They are freely available on the OSAH website at www.osha.gov. Unlike most standards, which are voluntary, the OSHA standards are laws.

Some of the important parts as they pertain to machine safety are as follows:

A General
B Adoption and Extension of Established Federal Standards
C General Safety and Health Provisions
H Hazardous Materials
I Personal Protective Equipment
J General Environmental Controls—includes Lockout/Tagout
O Machinery and Machine Guarding
R Special Industries
S Electrical

Some OSHA standards reference voluntary standards. The legal effect of incorporation by reference is that the material is treated as if it were published in full in the Federal Register. When a national consensus standard is incorporated by reference in one of the subparts, that standard is considered the law. For example, NFPA 70, a voluntary standard known as the US National Electric Code, is referenced in Subpart S. This makes the requirements in the NFPA70 standard mandatory.

The 29 CFR 1910.147, in Subpart J, covers the control of hazardous energy. This is commonly known as the Lockout/Tagout standard. The equivalent voluntary standard is ANSI Z244.1. Essentially, this standard requires power to the machine to be locked out when undergoing service or maintenance. The purpose is to prevent the unexpected energization or startup of the machine which would result in injury to employees.

Employers must establish a program and utilize procedures for affixing appropriate lockout devices or tagout devices to energy isolating devices, and to otherwise disable machines or equipment to prevent unexpected energization, start up or release of stored energy in order to prevent injury to employees.

Minor tool changes and adjustments, and other minor servicing activities, which take place during normal production operations, are not covered by this standard if they are routine, repetitive, and integral to the use of the equipment for production, provided that the work is performed using alternative measures which provide effective protection. Alternative measures are safeguarding devices like light curtains, safety mats, gate interlocks and other similar devices connected to a safety system. The challenge to the machine designer and user is to determine what is “minor” and what is “routine, repetitive and integral.”

Subpart O covers “Machinery and Machine Guarding.” This subpart lists the general requirements for all machines as well as requirements for some specific machines. When OSHA was formed in 1970, it adopted many existing ANSI standards. For example B11.1 for mechanical power presses was adopted as 1910.217.

The 1910.212 is the general OSHA standard for machines. It states that one or more methods of machine guarding shall be provided to protect the operator and other employees in the machine area from hazards such as those created by the point of operation, ingoing nip points, rotating parts, flying chips and sparks. Guards shall be affixed to the machine where possible and secured elsewhere if for any reason attachment to the machine is not possible. The guard shall be such that it does not offer an accident hazard in itself.

The “point of operation” is the area on a machine where work is actually performed upon the material being processed. The point of operation of a machine, whose operation exposes an employee to injury, shall be guarded. The guarding device shall be in conformity with any appropriate standards or, in the absence of applicable specific standards, shall be so designed and constructed as to prevent the operator from having any part of his body in the danger zone during the operating cycle.

Subpart S (1910.399) states the OSHA electrical requirements. An installation or equipment is acceptable to the Assistant Secretary of Labor, and approved within the meaning of this Subpart S if it is accepted, certified, listed, labeled, or otherwise determined to be safe by a nationally recognized testing laboratory (NRTL).

What is Equipment? A general term including material, fittings, devices, appliances, fixtures, apparatus, and the like, used as a part of, or in connection with, an electrical installation.

What is “Listed”? Equipment is “listed” if it is of a kind mentioned in a list which, (a) is published by a nationally recognized laboratory which makes periodic inspection of the production of such equipment, and (b) states such equipment meets nationally recognized standards or has been tested and found safe for use in a specified manner.

As of August 2009, the following companies are recognized by OSHA as NRTLs:
Canadian Standards Association (CSA)
Communication Certification Laboratory, Inc. (CCL)
Curtis-Straus LLC (CSL)
FM Approvals LLC (FM)
Intertek Testing Services NA, Inc. (ITSNA)
MET Laboratories, Inc. (MET)
NSF International (NSF)
National Technical Systems, Inc. (NTS)
SGS U.S. Testing Company, Inc. (SGSUS)
Southwest Research Institute (SWRI)
TÜV America, Inc. (TÜVAM)
TÜV Product Services GmbH (TÜVPSG)
TÜV Rheinland of North America, Inc. (TÜV)
Underwriters Laboratories Inc. (UL)
Wyle Laboratories, Inc. (WL)

Some states have adopted their own local OSHAs. Twenty-four states, Puerto Rico and the Virgin Islands have OSHA-approved State Plans and have adopted their own standards and enforcement policies. For the most part, these States adopt standards that are identical to Federal OSHA. However, some States have adopted different standards applicable to this topic or may have different enforcement policies.

Employers must report incident history to OSHA. OSHA compiles incident rates and transmits the information to local offices, and uses this information to prioritize inspections. The key inspection drivers are:

- Imminent Danger
- Catastrophes and Fatalities
- Employee Complaints
- High Hazardous Industries
- Local Planned Inspections
- Follow-up Inspections
- National and Local Focus Programs

Violations of OSHA standards can result in fines. The schedule of fines is:

- Serious: up to $7000 per violation
- Other than Serious: discretionary but not more than $7000
- Repeat: up to $70,000 per violation
- Willful: up to $70,000 per violation
- Violations resulting in death: further penalties
- Failure to abate: $7000/day

The table below shows the top 14 OSHA citations from October 2004 to September 2005.

Standard	Description
1910.147	The control of hazardous energy (lockout/tagout)
1910.1200	Hazard communication
1910.212	General requirements for all machines
1910.134	Respiratory protection
1910.305	Wiring methods, components, and equipment for general use
1910.178	Powered industrial trucks
1910.219	Mechanical power transmission
1910.303	General requirements
1910.213	Woodworking machinery
19102.215	Abrasive wheel machinery
19102.132	General requirements
1910.217	Mechanical power presses
1910.095	Occupational noise exposure
1910.023	Guarding floor and wall openings and holes

Table 1

Canada Regulations

In Canada, Industrial Safety is governed at the Provincial level. Each province has its own regulations that are maintained and enforced. For example, Ontario established the Occupational Health and Safety Act, which sets out the rights and duties of all parties in the workplace. Its main purpose is to protect workers against health and safety hazards on the job. The Act establishes procedures for dealing with workplace hazards, and it provides for enforcement of the law where compliance has not been achieved voluntarily.

Within the Act there is regulation 851, Section 7 that defines the Pre-Start Health and Safety review. This review is a requirement within Ontario for any new, rebuilt or modified piece of machinery and a report needs to be generated by a professional engineer.

Standards

This section provides a list of some of the typical international and national standards that are relevant to machinery safety. It is not intended to form an exhaustive list but rather to give an insight on what machinery safety issues are the subject of standardization.

This section should be read in conjunction with the Regulation section.

The countries of the world are working towards global harmonization of standards. This is especially evident in the area of machine safety. Global safety standards for machinery are governed by two organizations: ISO and IEC. Regional and country standards are still in existence and continue to support local requirements but in many countries there has been a move toward using the international standards produced by ISO and IEC.

For example, the EN (European Norm) standards are used throughout the EEA countries. All new EN standards are aligned with, and in most cases have identical text with ISO and IEC standards.

IEC covers electrotechnical issues and ISO covers all other issues. Most industrialized countries are members of IEC and ISO. Machinery safety standards are written by working groups comprised of experts from many of the world's industrialized counties.

In most countries standards can be regarded as voluntary whereas regulations are legally mandatory. However standards are usually used as the practical interpretation of the regulations. Therefore the worlds of standards and regulations are closely interlinked.

ISO (International Organization for Standardization)

ISO is a non-governmental organization comprised of the national standards bodies of most of the countries of the world (157 countries at the time of this printing). A Central Secretariat, located in Geneva, Switzerland, coordinates the system. ISO generates standards for designing, manufacturing and using machinery more efficiently, safer and cleaner. The standards also make trade between countries easier and fairer.

ISO standards can be identified by the three letters ISO.

The ISO machine standards are organized in the same fashion as the EN standards, three levels: Type A, B and C (see the later section on EN Harmonized European Standards).

For more information, visit the ISO website: *www.iso.org*

IEC (International Electrotechnical Commission)

The IEC prepares and publishes international standards for electrical, electronic and related technologies. Through its members, the IEC promotes international cooperation on all questions of electrotechnical standardization and related matters, such as the assessment of conformity to electrotechnical standards.

For more information, visit the IEC website: *www.iec/ch*.

EN Harmonized European Standards

These standards are common to all EEA countries and are produced by the European Standardization Organizations CEN and CENELEC. Their use is voluntary but designing and manufacturing equipment to them is the most direct way of demonstrating compliance with the EHSRs of the Machinery Directive.

They are divided into 3 types: A, B and C standards.

Type A. STANDARDS: Cover aspects applicable to all types of machines.

Type B. STANDARDS: Subdivided into 2 groups.

Type B1 STANDARDS: Cover particular safety and ergonomic aspects of machinery.

Type B2 STANDARDS: Cover safety components and protective devices.

Type C. STANDARDS: Cover specific types or groups of machines.

It is important to note that complying with a C Standard gives automatic presumption of conformity with the EHSRs. In the absence of a suitable C Standard, A and B Standards can be used as part or full proof of EHSR conformity by pointing to compliance with relevant sections.

Agreements have been reached for cooperation between CEN/CENELEC and bodies such as ISO and IEC. This should ultimately result in common worldwide standards. In most cases an EN Standard has a counterpart in IEC or ISO. In general the two texts will be the same and any regional differences will be given in the forward of the standard.

This section lists some of the EN, ISO, IEC and other national and regional Standards relevant to machinery safety. Where an EN standard is shown in brackets it is identical or very closely aligned with the ISO or IEC standard. For a complete list of EN Machinery Safety standards go to:
http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm

ISO and EN Standards (Type A)

EN ISO 12100

Safety of machinery. Basic concepts, general principles for design. Pts 1 & 2

This is an A standard which outlines all the basic principles including risk assessment, guarding, interlocking, emergency stops, trip devices, safety distances, etc. It references to other standards that provide greater levels of detail.

In the near future it is likely that EN ISO 12100 and EN ISO 14121 will be combined into one standard.

EN ISO 14121

Principles for risk assessment.

This principle outlines the fundamentals of assessing the risks during the life of the machinery. It summarizes methods for hazard analysis and risk estimation.

An ISO Technical Report: ISO/TR 14121-2 is also available. It gives practical guidance and examples of methods for risk assessment.

ISO and EN Standards (Type B)

EN ISO 11161

Safety of Integrated Manufacturing Systems—Basic Requirements.

This standard was published in its revised form in 2007. It was significantly updated making it very useful for contemporary integrated machinery.

EN ISO 13849-1:2008 Safety related parts of control systems—Pt 1: General principles for design

This standard is the result of the significant revision of the old EN 954-1 (which is due for withdrawal at the end of 2011). It introduced many new aspects for Functional Safety of control systems. The term “PL” (Performance Level) is used to describe the level of integrity of a system or a subsystem.

It is available as an alternative to IEC/EN 62061 (see later). Note that EN ISO 13849-1 covers all technologies of control system whereas IEC/EN 62061 only covers electrical technology.

EN ISO 13849-1 is intended to provide a direct transition path from the categories of the previous EN 954-1. It has a relatively simple methodology compared to IEC/EN 62061 but this is at the expense of some constraints and restrictions. Either the revised ISO/EN 13849-1 or IEC/EN 62061 can be applied to machinery electrical safety related systems and the user should choose whichever one is best suited to their needs but EN ISO 13849-1 is often preferred when transitioning from Categories.

Note: Recent to the time of publication of this text, CEN (European Committee for Standardisation) announced that the final date for presumption of conformity of EN 954-1 will be extended to the end of 2011 to facilitate transition to the later standards. This replaces the original date of December 29, 2009.

For the latest information on the use and status of EN 954-1 visit: *http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx*. In the meantime it is advised that the extension of the transition period is used to move over to the use of the later standards (EN ISO 13849-1 or IEC/EN 62061) in a timely manner.

EN ISO 13849-2

Safety related parts of control systems—Pt 2: Validation

This standard provides details for validation of safety related parts of control systems. It has annexes that give details safety components, principles and fault exclusion.

EN ISO 13850

Emergency Stop devices, functional aspects—Principles for design.

Provides design principles and requirements.

ISO 13851 (EN 574)

Two-hand control devices—Functional aspects—Principles for design.

Provides requirements and guidance on the design and selection of two-hand control devices, including the prevention of defeat and the avoidance of faults.

EN ISO 13857

Safety distances to prevent danger zones being reached by the upper and lower limbs.

Provides data for calculation of safe aperture sizes and positioning for guards, etc.

ISO 13854 (EN 349)

Minimum distances to avoid crushing parts of the human body.

Provides data for calculation of safe gaps between moving parts, etc.

ISO 13855 (EN 999)

The positioning of protective equipment in respect to approach speeds of parts of the human body.

Provides methods for designers to calculate the minimum safety distances from a hazard for specific safety devices, in particular for electrosensitive devices (e.g., light curtains), pressure sensitive mats/floors and two-hand controls. It contains a principle for the positioning of safety devices based on approach speed and machine stopping time that can reasonably be extrapolated to cover interlocked guard doors without guard locking.

ISO 13856-1 (EN 1760-1)

Pressure Sensitive Safety Devices—Pt 1: Mats & Floors.

Provides requirements and test procedures.

ISO 13856-2 (EN 1760-2)

Pressure Sensitive Safety Devices—Pt 2: Edges & Bars.

Provides requirements and test procedures

ISO 14118 (EN 1037)

Prevention of unexpected start-up—Isolation and energy dissipation

Defines measures aimed at isolating machines from power supplies and dissipating stored energy to prevent unexpected machine startup and allow safe intervention with machinery.

ISO 14119 (EN 1088)

Interlocking devices associated with guards—Principles for design and selection.

Provides principles for the design and selection of interlocking devices associated with guards.

In order to verify mechanical switches it refers to IEC 60947-5-1—Low voltage switch gear—Pt 5: Control circuit devices and switching elements—Section 1: Electromechanical control circuit devices.

In order to verify non-mechanical switches it refers to IEC 60947-5-3—Particular requirements for proximity devices with defined behavior under fault conditions.

ISO 14120 (EN 953)

General Requirements for the Design and Construction of Guards.

Provides definitions, descriptions and design requirements for fixed and movable guards.

ISO and EN Standards (Type C)

There is a large range of Type C Standards that cover specific types of machinery. For example:

EN ISO 10218-1

Industrial robots

EN 415-4

Safety of packaging machines. Palletizers and depalletizers.

IEC and EN Standards

IEC/EN 60204-1

Electrical equipment of machines—Pt 1 General requirements.

This is a very important standard that outlines recommendations for safety related aspects of wiring and electrical equipment on machines. A significantly revised version was published in 2006. This revision removed the former preference for electromechanical safety circuits.

IEC/EN 61508

Functional safety of electrical, electronic and programmable electronic safety-related systems.

This standard is important because it contains the requirements and provisions that are necessary for the design of complex electronic and programmable systems and subsystems. The standard is generic so it is not restricted to the machinery sector. It is a lengthy and complex document comprising seven parts. Within the machinery sector, its use is mostly for the design of complex devices such as safety PLCs. For system level design and integration aspects for machinery the sector specific standards such as IEC/EN 62061 or EN ISO 13849-1 are probably the most suitable. IEC 61508 has mapped out the approach for a new generation of sector and product specific standards that is now emerging. It introduced the term SIL (safety integrity level) and gives a hierarchy of 4 SILs which are applied to a safety function. SIL 1 is the lowest and SIL 4 is the highest. SIL 4 is not usually applicable to the machinery sector because it is intended to be related to very high risk levels more associated with sectors such as petrochemical or nuclear.

IEC 62061 (EN 62061)

Functional safety of safety related electrical, electronic and programmable electronic control systems.

This standard is one of the new generations of standards that use the term SIL (safety integrity level). It is the machinery specific implementation of IEC/EN 61508. It specifies requirements and makes recommendations for the design, integration and validation of electrical safety related control systems for machines. This standard provides an alternative approach to EN ISO 13849-1 and is intended to be useful for the increasingly complex safety functionality required for today's current and future machinery For less complex safety functionality EN ISO 13849-1 may be easier to implement. The use of these standards requires the availability of data such as PFH_D (probability of dangerous failure per hour) or MTTFd (mean time to dangerous failure).

IEC 61496 (EN 61496)

Electro-sensitive protective equipment Pt 1: General requirements and tests.

General requirements and tests.

Pt 2: Particular requirements for equipment using active optoelectronic protective devices.

Part 1 gives requirements and test procedures for the control and monitoring aspects for electrosensitive protective equipment. Subsequent parts deal with aspects particular to the sensing side of the system. Part 2 gives particular requirements for safety light curtains.

IEC 61800-5-2 (EN 61800-5-2)

Functional safety of power drive systems.

This standard deals with drives that have safety functionality.

US Standards

OSHA Standards

Where possible, OSHA promulgates national consensus standards or established Federal standards as safety standards. The mandatory provisions (e.g., the word shall implies mandatory) of the standards, incorporated by reference, have the same force and effects as the standards listed in Part 1910. For example, the national consensus standard NFPA 70 is listed as a reference document in Appendix A of Subpart S-Electrical of Part 1910 of 29 CFR. NFPA 70 is a voluntary standard, which was developed by the National Fire Protection Association (NFPA). NFPA 70 is also known as the National Electric Code (NEC). By incorporation, all the mandatory requirements in the NEC are mandatory by OSHA.

The following is a list of some of the OSHA standards relevant to machinery safety,

1910 Subpart O - Machinery and Machine Guarding

1910.211 - Definitions.

1910.212 - General requirements for all machines.

1910.213 - Woodworking machinery requirements.

1910.214 - Cooperage machinery. [Reserved]

1910.215 - Abrasive wheel machinery.

1910.216 - Mills and calendars in the rubber and plastics industries.

1910.217 - Mechanical power presses.

1910.217 App A - Mandatory requirements for certification/ validation of safety systems for presence sensing device initiation of mechanical power presses

1910.217 App B - Nonmandatory guidelines for certification/ validation of safety systems for presence sensing device initiation of mechanical power presses

1910.217 App C - Mandatory requirements for OSHA recognition of third-party validation organizations for the PSDI standard

1910.217 App D - Nonmandatory supplementary information

1910.218 - Forging machines.

1910.219 - Mechanical power

1910.255 - Resistance welding.

1910 Subpart R - Special Industries

1910.261 - Pulp, paper, and paperboard mills.

1910.262 - Textiles.

1910.263 - Bakery equipment.

1910.264 - Laundry machinery and operations.

1910.265 - Sawmills.

1910.266 - Logging operations.

ANSI Standards

The American National Standards Institute (ANSI) serves as the administrator and coordinator of the United States private sector voluntary standardization system. It is a private, nonprofit, membership organization supported by a diverse constituency of private and public sector organizations.

ANSI, itself, does not develop standards; it facilitates the development of standards by establishing consensus among qualified groups. ANSI also ensures that the guiding principles of consensus, due process and openness are followed by the qualified groups. Below is a partial list of industrial safety standards that can be obtained by contacting ANSI.

These standards are categorized as either application standards or construction standards. Application standards define how to apply a safeguarding to machinery. Examples include ANSI B11.1, which provides information on the use of machine guarding on power presses, and ANSI/RIA R15.06, which outlines safeguarding use for robot guarding.

National Fire Protection Association

The National Fire Protection Association (NFPA) was organized in 1896. Its mission is to reduce the burden of fire on the quality of life by advocating scientifically based consensus codes and standards, research and education for fire and related safety issues. The NFPA sponsors many standards to help accomplish its mission. Two very important standards related to industrial safety and safe-guarding are the National Electric Code (NEC) and Electrical Standard for Industrial Machinery.

The National Fire Protection Association has acted as sponsor of the NEC since 1911. The original code document was developed in 1897 as a result of the united efforts of various insurance, electrical, architectural, and allied interests. The NEC has since been updated numerous times; it is revised about every three years. Article 670 of the NEC covers some details on industrial machinery and refers the reader to the Electrical Standard for Industrial Machinery, NFPA 79.

NFPA 79 applies to electrical/electronic equipment, apparatus, or systems of industrial machines operating from a nominal voltage of 600 volts or less. The purpose of NFPA 79 is to provide detailed information for the application of electrical/electronic equipment, apparatus, or systems supplied as part of industrial machines that will promote safety to life and property. NFPA 79, which was officially adopted by ANSI in 1962, is very similar in content to the standard IEC 60204-1.

Machines, which are not covered by specific OSHA standards, are required to be free of recognized hazards which may cause death or serious injuries. These machines must be designed and maintained to meet or exceed the requirements of applicable industry standards. NFPA 79 is a standard that would apply to machines not specifically covered by OSHA standards.

ANSI/NFPA 70

US National Electrical Code

ANSI/NFPA 70E

Electrical Safety Requirements for Employee Workplaces

ANSI/NFPA 79

Electrical Standard for Industrial Machinery

Association for Manufacturing Technology

ANSI B11.1

Machine Tools - Mechanical Power Presses - Safety Requirements for Construction, Care, and Use

ANSI B11.2

Machine Tools - Hydraulic Power Presses, Safety Requirements for Construction, Care, and Use

ANSI B11.3

Power Press Brakes, Safety Requirements for the Construction, Care, and Use

ANSI B11.4

Machine Tools - Shears - Safety Requirements for Construction, Care, and Use

ANSI B11.5

Machine Tools - Iron Workers - Safety Requirements for Construction, Care, and Use

ANSI B11.6

Lathes, Safety Requirements for the Construction, Care, and Use

ANSI B11.7

Machine Tools - Cold Headers and Cold Formers, Safety Requirements for Construction, Care, and Use

ANSI B11.8

Drilling, Milling, and Boring Machines, Safety Requirements for the Construction, Care, and Use

ANSI B11.9

Grinding Machines, Safety Requirements for the Construction, Care, and Use

ANSI B11.10

Metal Sawing Machines, Safety Requirements for Construction, Care, and Use

ANSI B11.11

Gear Cutting Machines, Safety Requirements for the Construction, Care, and Use

ANSI B11.12

Machine Tools - Roll-Forming and Roll-Bending Machines - Safety Requirements for the Construction, Care, and Use

ANSI B11.13

Machine Tools - Single- and Multiple-Spindle Automatic Bar and Chucking Machines - Safety Requirements for Construction, Care and Use

ANSI B11.14

Machine Tools - Coil-Slitting Machines Safety Requirements for Construction, Care, and Use – Withdrawn and rolled into B11.18

ANSI B11.15

Pipe, Tube, and Shape Bending Machines, Safety Requirements for Construction, Care, and Use

ANSI B11.16

Metal Powder Compacting Presses, Safety Requirements for Construction, Care, and Use

ANSI B11.17

Machine Tools - Horizontal Hydraulic Extrusion Presses - Safety Requirements for Construction, Care, and Use

ANSI B11.18

Machine Tools - Machines and Machinery Systems for Processing Strip, Sheet, or Plate from Coiled Configuration - Safety Requirements for Construction, Care, and Use

ANSI B11.19

Machine Tools - Safeguarding When Referenced by Other B11 Machine Tool Safety Standards-Performance Criteria for the Design, Construction, Care and Operation

ANSI B11.20

Machine Tools - Manufacturing Systems/Cells – Safety Requirements for Construction, Care, and Use

ANSI B11.21

Machine Tools - Machine Tools Using Lasers for Processing Materials - Safety Requirements for Design, Construction, Care, and Use

ANSI B11.TR3

Risk assessment and risk reduction – A guide to estimate, evaluate and reduce risks associated with machine tools

ANSI B11.TR4

This technical report covers the application of programmable controllers to safety applications.

ANSI B11.TR6

This technical report, currently in development, will provide circuit examples of safety functions to accommodate various levels of risk Reduction.

ANSI ISO 12100

Safety of machinery. Basic concepts, general principles for design. Pts -1 and -2

The standard ISO 12100 has been adopted in the US by AMT as an identical ANSI standard. ISO 12100 is a globally applicable top level basic principles standard that forms the framework for most of the ISO, IEC and EN machinery safety standards. It provides a risk assessment approach as opposed to a prescriptive and restrictive approach. The aim is to avoid cost and trade barrier problems caused by a multiplicity of different national standards covering the same subject in different ways.

Robot Industries Association

ANSI RIA R15.06

Safety Requirements for Industrial Robots and Robot Systems

ANSI RIA R15.06

Safety Requirements for Industrial Robots and Robot Systems

Packaging Machinery Manufacturer's Institute

ANSI PMMI B155.1

Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery

The packaging standard was recently revised to incorporate risk assessment and risk reduction.

American Society of Safety Engineers

Z224.1

Control of Hazardous Energy, Lockout/Tag out and Alternative Methods

This standard is similar to OSHA 1910.147. It provides a method (risk assessment) to determine the appropriate alternative method when energy cannot be locked out.

Society of Plastics Industry

ANSI B151.1

Horizontal Injection Molding Machines – Safety Requirements for Manufacture, Care and Use

ANSI B151.15

Extrusion Blow Molding Machines – Safety Requirements

ANSI B151.21

Injection Blow Molding Machines - Safety Requirements

ANSI B151.26

Plastics Machinery - Dynamic Reaction - Injection Molding Machines - Safety Requirements for the Manufacture, Care and Use

ANSI B151.27

Plastics Machinery - Robots used with Horizontal Injection Molding Machines - Safety Requirements for the Integration, Care and Use

ANSI B151.28

Plastics Machinery - Machines to Cut, Slit, of Buff Plastic Foams - Safety Requirements for the Manufacture, Care and Use

Canada Standards

CSA Standards reflect a national consensus of producers and users – including manufactures, consumers, retailers, unions and professional organizations, and government agencies. The standards are used widely by industry and commerce and often adopted by municipal, provincial, and federal governments in their regulations, particularly in the fields of health, safety, building and construction, and the environment.

Individuals, companies, and associations across Canada indicate their support for CSA's standards development by volunteering their time and skills to CSA Committee work and supporting the Association's objectives through sustaining memberships. The more than 7000 committee volunteers and the 2000 sustaining memberships together form CSA's total membership.

The Standards Council of Canada is the coordinating body of the National Standards system, a federation of independent, autonomous organizations working towards the further development and improvement of voluntary standardization in the national interest.

CSA Z432-04

Safeguarding of Machinery

CSA Z434-03

Industrial Robots and Robot Systems - General Safety Requirements

CSA Z460-05

Control of hazardous energy – Lockout and other methods

CSA Z142-02

Code for Power Press Operation: Health, Safety, and Guarding Requirements

Australia Standards

Most of these standards are closely aligned with the equivalent ISO/IEC/EN standards

Standards Australia Limited
286 Sussex Street,
Sydney,
NSW 2001
Phone: +61 2 8206 6000
Email: mail@standards.org.au
Website: www.standards.org.au

To purchase copies of standards:

SAI Global Limited
286 Sussex Street
Sydney
NSW 2001
Phone: +61 2 8206 6000
Fax: +61 2 8206 6001
Email: mail@sai-global.com
Website: www.saiglobal.com/shop

AS 4024.1-2006

Safeguarding of machinery. Part 1: General principles

AS 4024.1101-2006 Terminology – General

AS 4024.1201-2006 Basic terminology and methodology

AS 4024.1202-2006 Technical principles

AS 4024.1301-2006 Principles of risk assessment

AS 4024.1302-2006 Reduction of risks to health and safety from hazardous substances emitted by machinery

AS 4024.1401-2006 Design principles – Terminology and general principles

AS 4024.1501-2006 Design of safety related parts of control systems – General principles

AS 4024.1502-2006 Design of safety related parts of control systems – Validation

AS 4024.1601-2006 General requirements for the design and construction of fixed and movable guards

AS 4024.1602-2006 Principles for the design and selection of interlocks

AS 4024.1603-2006 Prevention of unexpected start-up

AS 4024.1604-2006 Emergency stop – Principles for design

AS 4024.1701-2006 Basic human body measurements for technological design

AS 4024.1702-2006 Principles for determining the dimensions required for openings for whole body access to machinery

AS 4024.1703-2006 Principles for determining the dimensions required for access openings

AS 4024.1704-2006 Anthropometric data

AS 4024.1801-2006 Safety distances – Upper limbs

AS 4024.1802-2006 Safety distances – Lower limbs

AS 4024.1803-2006 Minimum gaps to prevent crushing of parts of the human body

AS 4024.1901-2006 General principles for human interaction with displays and control actuators

AS 4024.1902-2006 Displays

AS 4024.1903-2006 Control actuators

AS 4024.1904-2006 Requirements for visual, auditory and tactile signs

AS 4024.1905-2006 Requirements for marking

AS 4024.1906-2006 Requirements for the location and operation of actuators

AS 4024.1907-2006 System of auditory and visual danger and information signals

AS4024.2-1998

Safeguarding of machinery. Part 2: Installation and commissioning requirements for electro-sensitive systems—Optoelectronic devices

The basis of this standard is IEC 61496-1 and -2. Part 2 covers the installation and commissioning of light curtains specifically related to machinery safety.

AS 4024.3-1998

Safeguarding of machinery. Part 3: Manufacturing and testing requirements for electro-sensitive systems— Optoelectronic devices

The basis of this standard is IEC 61496-1 and -2. Part 3 covers the manufacturing and testing of light curtains specifically related to machinery safety.

AS4024.4-1998

Safeguarding of machinery. Part 4: Installation and commissioning requirements for electro-sensitive systems—Pressure-sensitive devices

The basis of this standard is EN 1760-1 and EN 1760-2. Part 4 covers the installation and commissioning of mats, floors, edges and bars that are used with machinery, regardless of the energy used.

AS 4024.5-1998

Safeguarding of machinery. Part 5: Manufacturing and testing requirements for electro-sensitive systems— Pressure-sensitive devices

The basis of this standard is EN1760-1 and EN1760-2. Part 5 covers the manufacturing and testing mats, floors, edges and bars that are used with machinery, regardless of the energy used.

Safety Strategy

From a purely functional point of view the more efficiently a machine performs its task of processing material then the better it is. But, in order for a machine to be viable it must also be safe. Indeed safety must be regarded as a prime consideration.

In order to devise a proper safety strategy there must be two key steps, which work together as shown in Figure 9.

Risk Assessment based on a clear understanding of the machine limits and functions and the tasks that may be required to be performed at the machine throughout its life.

Risk Reduction is then performed if necessary and safety measures are selected based on the information derived from the risk assessment stage.

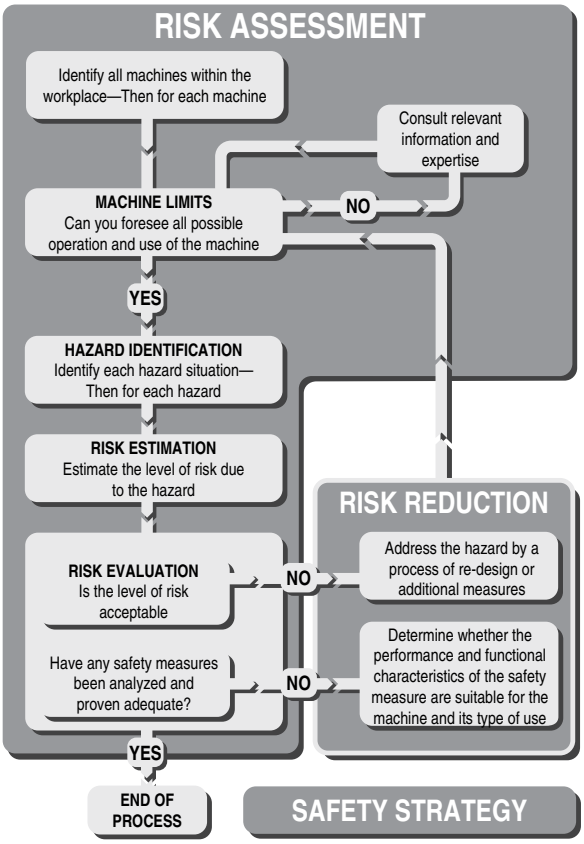


Figure 9: Safety Strategy

The manner in which this is done is the basis of the Safety Strategy for the machine.

We need a checklist to follow and ensure that all aspects are considered, and that the overriding principle does not become lost in the detail. The whole process should be documented. Not only will this ensure a more thorough job, but it will also make the results available for checking by other parties.

This section applies both to machine manufacturers and to machine users. The manufacturer needs to ensure that his machine is capable of being used safely. The risk assessment should be started at the machine design phase and it should take account of all the foreseeable tasks that will need to be performed on the machine. This task based approach at the early iterations of the risk assessment is very important. For example, there may be a regular need for adjustment of moving parts at the machine. At the design phase it should be possible to design in measures that will allow this process to be carried out safely. If it is missed at the early stage it may be difficult or impossible to implement at later stage. The result could be that the adjustment of moving parts still has to be performed but must be done in a manner that is either unsafe or inefficient (or both). A machine on which all tasks have been taken account of during the risk assessment will be a safer machine and a more efficient machine.

The user (or employer) needs to ensure that the machines in their working environment are safe. Even if a machine has been declared safe by the manufacturer, the machine user should still perform a risk assessment to determine whether the equipment is safe in their environment. Machines are often used in circumstances unforeseen by the manufacturer. For example, a milling machine used in a school workshop will need additional considerations to one that is used in an industrial tool room.

It should also be remembered that if a user company acquires two or more independent machines and integrates them into one process they are the manufacturer of the resulting combined machine.

So now let us consider the essential steps on the route to a proper safety strategy. The following can be applied to an existing factory installation or a single new machine.

Risk Assessment

It is wrong to regard risk assessment as a burden. It is a helpful process that provides vital information and empowers the user or designer to take logical decisions about ways of achieving safety.

There are various standards that cover this subject. ISO 14121: “Principles for risk assessment” and ISO 12100: “Safety of machinery—Basic principles” contain the most globally applied guidance.

Which ever technique is used to carry out a risk assessment, a cross functional team of people will usually produce a result with wider coverage and better balance than one individual.

Risk assessment is an iterative process; it will be performed at different stages of the machine life cycle. The information available will vary according to the stage of the life cycle. For example, a risk assessment conducted by a machine builder will have access to every detail of the machine mechanisms and construction materials but probably only an approximate assumption of the machine’s ultimate working environment. A risk assessment conducted by the machine user would not necessarily have access to the in-depth technical details but will have access to every detail of the machines working environment. Ideally the output of one iteration will be the input for the next iteration.

Machine Limit Determination

This involves collecting and analyzing information regarding the parts, mechanisms and functions of a machine. It will also be necessary to consider all the types of human task interaction with the machine and the environment in which the machine will operate. The objective is to get a clear understanding of the machine and its usage.

Where separate machines are linked together, either mechanically or by control systems, they should be considered as a single machine, unless they are “zoned” by appropriate protective measures.

It is important to consider all limits and stages of the life of a machine including installation, commissioning, maintenance, decommissioning, correct use and operation as well as the consequences of reasonably foreseeable misuse or malfunction.

Task and Hazard Identification

All the hazards at the machine must be identified and listed in terms of their nature and location. Types of hazard include crushing, shearing, entanglement, part ejection, fumes, radiation, toxic substances, heat, noise, etc.

The results of the task analysis should be compared with the results of the hazard identification. This will show where there is a possibility for the convergence of a hazard and a person i.e. a hazardous situation. All the hazardous situations should be listed. It may be possible that the same hazard could produce different type of hazardous situation depending on the nature of the person or the task. For example, the presence of a highly skilled and trained maintenance technician may have different implications than the presence of an unskilled cleaner who has no knowledge of the machine. In this situation if each case is listed and addressed separately it may be possible to justify different protective measures for the maintenance technician than the ones for the cleaner. If the cases are not listed and addressed separately then the worst case should be used and the maintenance and the cleaner will both be covered by the same protective measure.

Sometimes it will be necessary to carry out a general risk assessment on an existing machine that already has protective measures fitted (e.g., a machine with dangerous moving parts protected by an interlocked guard door). The dangerous moving parts are a potential hazard that may become an actual hazard in the event of failure of the interlocking system. Unless that interlock system has already been validated (e.g., by risk assessment or design to an appropriate standard), its presence should not be taken into account.

Risk Estimation

This is one of the most fundamental aspects of risk assessment. There are many ways of tackling this subject and the following pages illustrate the basic principles.

Any machinery that has potential for hazardous situations presents a risk of a hazardous event (i.e. of harm). The greater the amount of risk, the more important it becomes to do something about it. At one hazard the risk could be so small that we can tolerate and accept it but at another hazard the risk could be so large that we need to go to extreme measures to protect against it. Therefore in order to make a decision on "if and what to do about the risk," we need to be able to quantify it.

Risk is often thought of solely in terms of the severity of injury at an accident. Both the severity of potential harm AND the probability of its occurrence have to be taken into account in order to estimate the amount of risk present.

The suggestion for risk estimation given on the following pages is not advocated as the definitive method as individual circumstances may dictate a different approach. IT IS INTENDED ONLY AS A GENERAL GUIDELINE TO ENCOURAGE A METHODICAL AND DOCUMENTED STRUCTURE.

The point system used has not been calibrated for any particular type of application therefore is not necessarily suitable for any specific application. ISO TR (Technical Report) 14121-2 "Risk assessment – Practical guidance and examples of methods" provides practical guidance and some shows different methods for quantification of risk.

The following factors are taken into account:

- THE SEVERITY OF POTENTIAL INJURY.
- THE PROBABILITY OF ITS OCCURRENCE.

The probability of occurrence includes two factors:

- FREQUENCY OF EXPOSURE.
- PROBABILITY OF INJURY.

Dealing with each factor independently we will assign values to each of these factors.

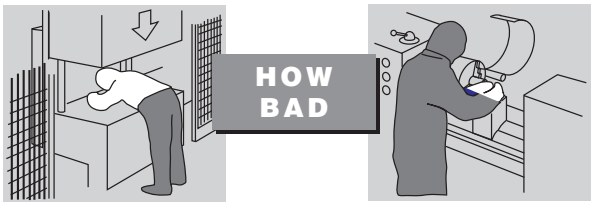
Make use of any data and expertise available to you. You are dealing with all stages of machine life, so to avoid too much complexity base your decisions on the worst case for each factor.

It is also important to retain common sense. Decisions need to take account of what is feasible, realistic and plausible. This is where a cross functional team approach is valuable.

Remember, for the purposes of this exercise you should usually not take account of any existing protective system. If this risk estimation shows that a protective system is required there are some methodologies as shown later in this chapter that can be used to determine the characteristics required.

1. Severity of potential injury

For this consideration we are presuming that the accident or incident has occurred, perhaps as a result of the hazards shown in Figure 10. Careful study of the hazard will reveal what is the most severe injury possible.



In this example most severe injury would be "fatal."

In this example the probable most severe injury would be "serious," with the possibility of bruising, breakage, finger amputation or injury from ejected chuck key, etc.

Figure 10: Potential Injury

Remember: For this consideration we are presuming that an injury is inevitable and we are only concerned with its severity. You should assume that the operator is exposed to the hazardous motion or process.

The severity of injury should be assessed as:

- **FATAL:** Death
- **MAJOR**: (Normally irreversible) Permanent disability, loss of sight, limb amputation, respiratory damage, etc.
- **SERIOUS**: (Normally reversible) Loss of consciousness, burns, breakages, etc.
- **MINOR**: Bruising, cuts, light abrasions, etc.

Each description could be assigned a points value (shown in Figure 11).

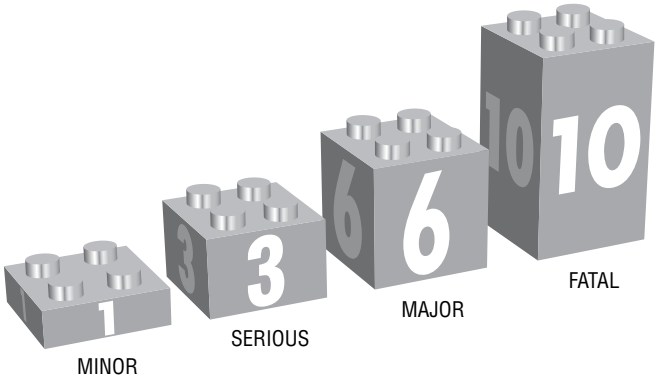


Figure 11: Points Assigned to Severity

2. Frequency of exposure

Frequency of exposure answers the question of how often is the operator or the maintenance person exposed to the hazard (Figure 12).

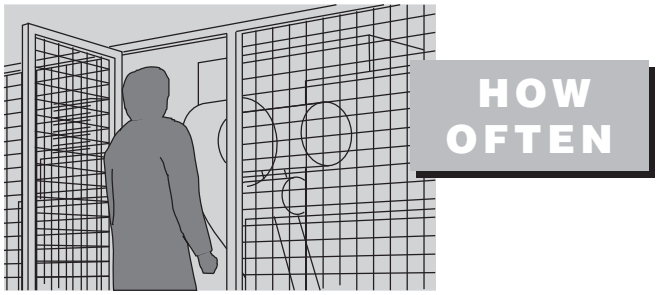


Figure 12: Frequency of Exposure

The frequency of exposure to hazard can be classified as:

- **FREQUENT**: Several times per day
- **OCCASIONAL**: Daily
- **SELDOM**: Weekly or less

Each description could be assigned a points value (shown in Figure 13).

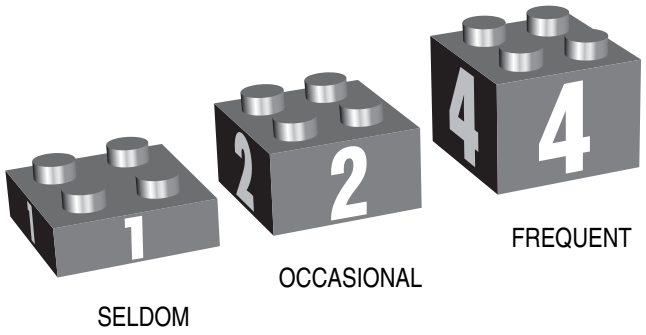
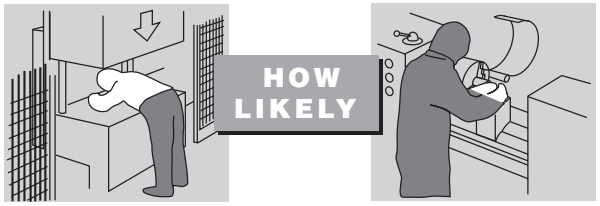


Figure 13: Points Assigned to Frequency of Exposure

3. Probability of injury

You should assume that the operator is exposed to the hazardous motion or process (Figure 14).



In this example the probability of injury could be rated as "certain" because of the amount of body in the hazard area and the speed of machine operation.

In this example the probability of injury may be rated as "possible" as there is minimal contact between the hazard and the operator. There may be time to withdraw from the danger.

Figure 14: How Likely

By considering the manner in which the operator is involved with the machine and other factors (speed of start up, for example) the probability of injury can be classified as:

- Unlikely
- Probable
- Possible
- Certain

Each description could be assigned a points value shown in Figure 15.

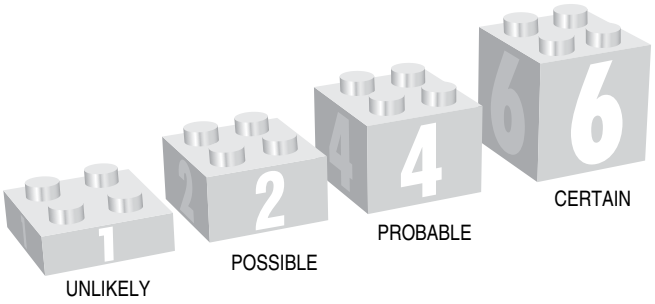


Figure 15: Points Assigned to Probability of Injury

All headings are assigned a value and they are now added together to give an initial estimate. Figure 16 shows the sum of the three components adds up to a value of 13. But we must consider a few more factors.

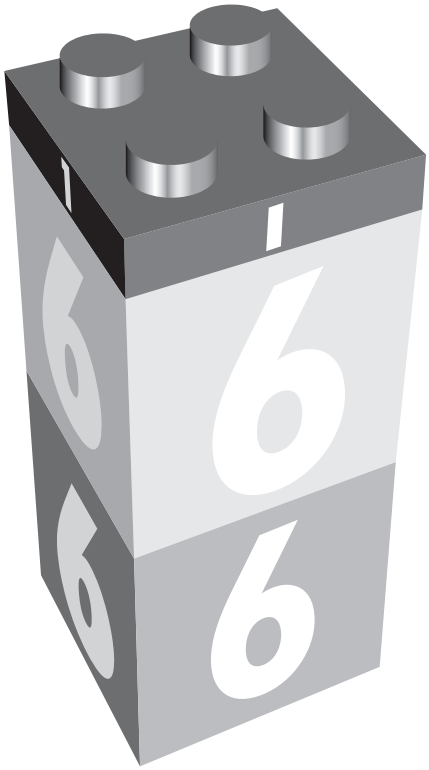


Figure 16: Initial Estimate

(**Note**: This is not based necessarily on the previous example pictures.)

The next step is to adjust the initial estimate by considering additional factors such as those shown in Table 2. Often they can only be properly considered when the machine is installed in its permanent location.

Typical Factor	Suggested Action
More than one person exposed to the hazard	Multiply the severity by the number of people
Protracted time in the danger zone without complete power isolation	If time spent per access is more than 15 minutes, add 1 point to the frequency factor.
Operator is unskilled or untrained	Add 2 points to the total.
Very long intervals (e.g., one year) between accesses. (There may be progressive and undetected failures particularly in monitoring systems.)	Add points equivalent to the maximum frequency factor.

Table 2: Additional Considerations for Risk Estimate

The results of any additional factors are then added to the previous total as shown in Figure 17.

Visit our website: www.ab.com/catalogs
Publication S117-CA001A-EN-P

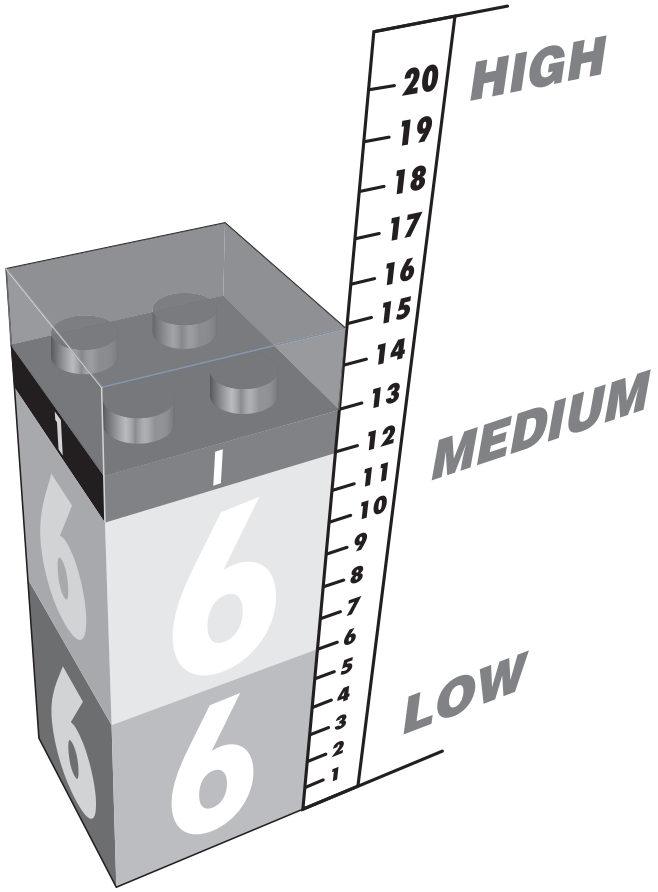


Figure 17: Final Value with Adjustments

Risk Reduction

Now we must consider each machine and its respective risks in turn and take measures to address all of its hazards.

The chart shown in Figure 18 is a suggestion for part of a documented process of accounting for all safety aspects of the machinery being used. It acts as a guide for machinery users, but machine manufacturers or suppliers can also use the same principle to confirm that all equipment has been evaluated. It will also act as an index to more detailed reports on risk assessment.

It shows that where a machine carries the CE Mark it simplifies the process as the machine hazards have already been evaluated by the manufacturer and that all the necessary measures have been taken. Even with CE Marked equipment there may still be hazards due to the nature of its application or material being processed which the manufacturer did not foresee.

Hierarchy of Measures for Risk Reduction

There are three basic methods to be considered and used in the following order:

1. Eliminate or reduce risks as far as possible (inherently safe machinery design and construction).
2. Install the necessary protective systems and measures (e.g. interlocked guards, light curtains etc) in relation to risks that cannot be eliminated by design.
3. Inform users of the residual risks due to any shortcomings of the protection measures adopted, indicate whether any particular training is required and specify any need to provide personal protection equipment.

Each measure from the hierarchy should be considered starting from the top and used where possible. This will usually result in the use of a combination of measures.

Company - MAYKIT WRIGHT LTD
Facility - Tool room - East Factory.
Date - 8/29/95
Operator profile - skilled.

Equipment Identity & Date	Directive Conformity	Risk Assessment Report Number	Accident History	Notes	Hazard Identity	Hazard Type	Action Required	Implemented and Inspected - Reference
Bloggs center lathe. Serial no. 8390726 Installed 1978	None claimed	RA302	None	Electrical equipment complies with BS EN 60204 E-Stops fitted (replaced 1989)	Chuck rotation with guard open	Mechanical Entanglement Cutting	Fit guard interlock switch	11/25/94 J Kershaw Report no 9567
					Cutting fluid	Toxic	Change to non toxic type	11/30/94 J Kershaw Report no 9714
					Swarf cleaning	Cutting	Supply gloves	11/30/94 J Kershaw Report no 9715
Bloggs turret head milling m/c Serial no 17304294 Manuf 1995 Installed May 95	M/c Dir. EMC Dir	RA416	None		Movement of bed (towards wall)	Crushing	Move machine to give enough clearance	4/13/95 J Kershaw Report no 10064

Figure 18: Risk Assessment Matrix

Inherently Safe Design

At the machine design phase it will be possible to avoid many of the possible hazards simply by careful consideration of factors such as materials, access requirements, hot surfaces, transmission methods, trap points, voltage levels, etc.

For example, if access is not required to a dangerous area, the solution is to safeguard it within the body of the machine or by some type of fixed enclosing guard.

Protective Systems and Measures

If access is required, then life becomes a little more difficult. It will be necessary to ensure that access can only be gained while the machine is safe. Protective measures such as interlocked guard doors and/or trip systems will be required. The choice of protective device or system should be heavily influenced by the operating characteristics of the machine. This is extremely important as a system that impairs machine efficiency will render itself liable to unauthorized removal or bypassing.

The safety of the machine in this case will depend on the proper application and correct operation of the protective system even under fault conditions.

The correct operation of the system must now be considered. Within each type there is likely to be a choice of technologies with varying degrees of performance of fault monitoring, detection or prevention.

In an ideal world every protective system would be perfect with absolutely no possibility of failing to a dangerous condition. In the real world, however, we are constrained by the current limits of knowledge and materials. Another very real constraint is cost. Based on these factors it becomes obvious that a sense of proportion is required. Common sense tells us that it would be ridiculous to insist that the integrity of a safety system on a machine that may, at the worst case, cause mild bruising to be the same as that required to keep a jumbo jet in the air. The consequences of failure are drastically different and therefore we need to have some way of relating the extent of the protective measures to the level of risk obtained at the risk estimation stage.

Whichever type of protective device is chosen it must be remembered that a “safety related system” may contain many elements including the protective device, wiring, power switching device and sometimes parts of the machine’s operational control system. All these elements of the system (including guards, mounting, wiring etc.) should have suitable performance characteristics relevant to their design principle and technology. IEC/EN 62061 and EN ISO 13849-1 classify hierarchical levels of performance for safety related parts of control systems and they provide risk assessment methods in their annexes to determine the integrity requirements for a protective system.

ISO 13849-1:2006 provides an enhanced risk graph in its Annex A. This graph is shown in Figure 19.

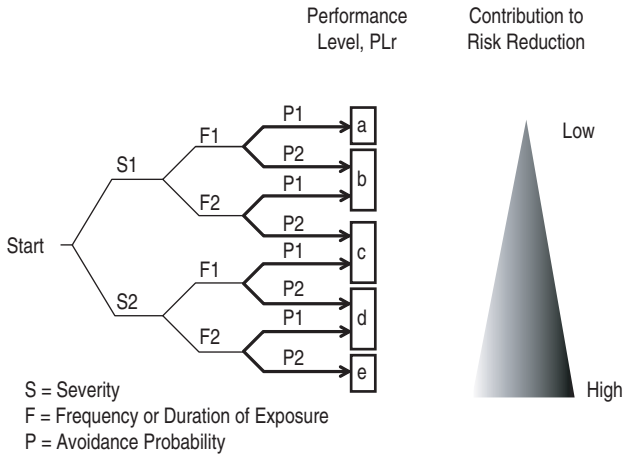


Figure 19: Risk Graph for Determining the Required Performance Level for a Safety Function—from ISO 13849-1:2006

IEC 62061 also provides a method in its Annex A, it takes the form shown in Figure 20.

The use of either of the above methods should provide equivalent results. Each method is intended to take account of the detailed content of the standard to which it belongs.

In both cases it is extremely important that the guidance provided in the text of the standard is used. The Risk Graph or Table must not be used in isolation or in an overly simplistic manner.

Evaluation

After the protective measure has been chosen and before it is implemented it is important to repeat the risk estimation. This is a procedure that is often missed. It may be that if we install a protective measure, the machine operator may feel that they are totally and completely protected against the original envisaged risk. Because they no longer have the original awareness of danger, they may intervene with the machine in a different way. They may be exposed to the hazard more often, or they may enter further into the machine for example. This means that if the protective measure fails they will be at a greater risk than envisaged before. This is the actual risk that we need to estimate. Therefore the risk estimation needs to be repeated taking into account any foreseeable changes in the way that people may intervene with the machine. The result of this activity is used to check whether the proposed protective measures are, in fact, suitable. For further information Annex A of IEC/EN 62061 is recommended.

Training, Personal Protective Equipment, etc.

It is important that operators have the necessary training in the safe working methods for a machine. This does not mean that the other measures can be omitted. It is not acceptable to merely tell an operator that they must not go near dangerous areas (as an alternative to guarding them).

It may also be necessary for the operator to use equipment such as special gloves, goggles, respirators, etc. The machinery designer should specify what sort of equipment is required. The use of personal protective equipment will not usually form the primary safeguarding method but will complement the measures shown above.

Risk assessment and safety measures

Document No.:
Part of:

Product:
Issued by:
Date:

☐ Pre risk assessment
☐ Intermediate risk assessment
☐ Follow up risk assessment

Black area = Safety measures required
Grey area = Safety measures recommended

Consequences	Severity Se	Class Cl 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Frequency and duration, Fr		Probability of hzd. event, Pr		Avoidance Av	
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hour	5	Common	5		
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3	> 1 h - <=day	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1day - <= 2wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	> 2wks - <= 1 yr	3	Rarely	2	Possible	3
							> 1 yr	2	Negligible	1	Likely	1

Ser. No.	Hzd. No.	Hazard	Se	Fr	Pr	Av	Cl	Safety measure	Safe

Comments

Figure 20: Table for Determining the Required Safety Integrity Level for a Safety Function—from IEC 62061

Standards

Many standards and technical reports provide guidance on risk assessment. Some are written for wide applicability, and some are written for specific applications. The following is a list of standards that include information on risk assessment.

ANSI B11.TR3: Risk assessment and risk reduction—A guide to estimate, evaluate and reduce risks associated with machine tools

ANSI PMMI B155.1: Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery

ANSI RIA R15.06: Safety Requirements for Industrial Robots and Robot Systems

AS 4024.1301-2006: Principles of risk assessment

CSA Z432-04: Safeguarding of Machinery

CSA Z434-03: Industrial Robots and Robot Systems—General Safety Requirements

IEC/EN 61508: Functional safety of electrical, electronic and programmable electronic safety-related systems.

IEC/EN 62061: Safety of machinery—Functional safety of safety related electrical, electronic and programmable electronic control systems.

EN ISO 13849-1: Safety of machinery—Safety related parts of control systems

EN ISO 14121-1: Principles for risk assessment

ISO TR 14121-2: Risk assessment—Practical guidance and examples of methods

Protective Measures and Complementary Equipment

When the risk assessment shows that a machine or process carries a risk of injury, the hazard must be eliminated or contained. The manner in which this is achieved will depend on the nature of the machine and the hazard. Protective measures in conjunction with guarding either prevent access to a hazard or prevent dangerous motion at a hazard when access is available. Typical examples of protective measures are interlocked guards, light curtains, safety mats, two-hand controls and enabling switches.

Emergency stop devices and systems are associated with safety related control systems but they are not direct protective systems, they should only be regarded as complementary protective measures.

Preventing Access

Fixed Enclosing Guards

If the hazard is on a part of the machinery which does not require access, a guard should be permanently fixed to the machinery as shown in Figure 21. These types of guards must require tools for removal. The fixed guards must be able to 1) withstand their operating environment, 2) contain projectiles where necessary, and 3) not create hazards by having, for example, sharp edges. Fixed guards may have openings where the guard meets the machinery or openings due to the use of a wire mesh type enclosure.

Windows provide convenient ways to monitor machine performance, when access to that portion of the machine. Care must be taken in the selection of the material used, as chemical interactions with cutting fluids, ultra-violet rays and simple aging cause the window materials to degrade over time.

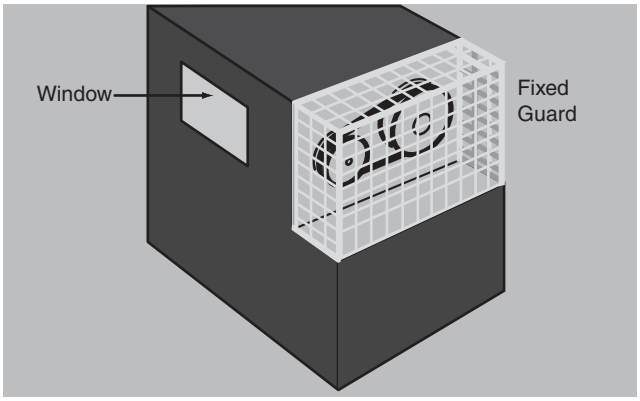


Figure 21: Fixed Guards

The size of the openings must prevent the operator from reaching the hazard. Table O-10 in U.S. OHSA 1910.217 (f) (4), ISO 13854, Table D-1 of ANSI B11.19, Table 3 in CSA Z432, and AS4024.1 provide guidance on the appropriate distance a specific opening must be from the hazard.

Detecting Access

Protective measures can be used to detect access to a hazard. When detection is selected as the method of risk reduction, the designer must understand that a complete safety system must be used; the safeguarding device, by itself, does not provide necessary risk reduction.

This safety system generally consists of three blocks: 1) an input device that senses the access to the hazard, 2) a logic device that process the signals from the sensing device, checks the status of the safety system and turns on or off output devices, and 3) an output device that controls the actuator (for example, a motor). Figure 22 shows the block diagram of a simple safety system.

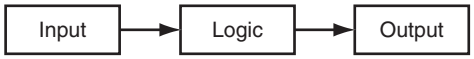


Figure 22: Simple Safety System Block Diagram

Detection Devices

Many alternative devices are available to detect the presence of a person entering or inside a hazard area. The best choice for a particular application is dependent on a number of factors.

- Frequency of access,
- Stopping time of hazard,
- Importance of completing the machine cycle, and
- Containment of projectiles, fluids, mists, vapors, etc.

Appropriately selected movable guards can be interlocked to provide protection against projectiles, fluids, mists and other types of hazards, and are often used when access to the hazard is infrequent. Interlocked guards can also be locked to prevent access while the machine is in the middle of the cycle and when the machine takes a long time to come to a stop.

Presence sensing devices, like light curtains, mats and scanners, provide quick and easy access to the hazard area and are often selected when operators must frequently access the hazard area. These types of devices do not provide protection against projectiles, mists, fluids, or other types of hazards.

The best choice of protective measure is a device or system that provides the maximum protection with the minimum hindrance to normal machine operation. All aspects of machine use must be considered, as experience shows that a system that is difficult to use is more liable to be removed or by-passed.

Presence Sensing Devices

When deciding how to protect a zone or area it is important to have a clear understanding of exactly what safety functions are required.

In general there will be at least two functions.

1. Switch off or disable power when a person enters the hazard area.
2. Prevent switching on or enabling of power when a person is in the hazard area.

At first thought these may seem to be one and the same thing but although they are obviously linked, and are often achieved by the same equipment, they are actually two separate functions. To achieve the first point we need to use some form of trip device. In other words a device which detects that a part of a person has gone beyond a certain point and gives a signal to trip off the power. If the person is then able to continue past this tripping point and their presence is no longer detected then the second point (preventing switching on) may not be achieved.

Figure 23 shows a full body access example with a vertically mounted light curtain as the trip device. Interlocked guard doors may also be regarded as a trip only device when there is nothing to prevent the door being closed after entry.

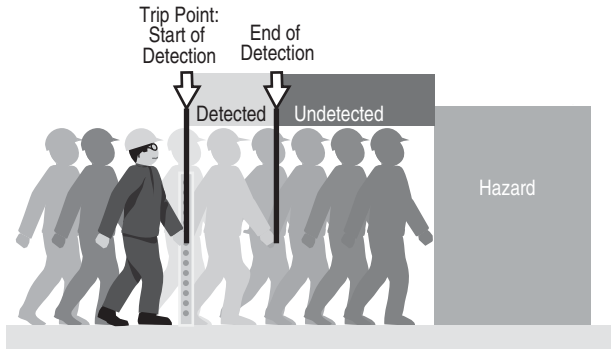


Figure 23: Full Body Access

If whole body access is not possible, so a person is not able to continue past the tripping point, their presence is always detected and the second point (preventing switching on) is achieved.

For partial body applications, as shown in Figure 24, the same types of devices perform tripping and presence sensing. The only difference being the type of application.

Presence sensing devices are used to detect the presence of people. The family of devices includes safety light curtains, single beam safety barriers, safety area scanners, safety mats and safety edges.

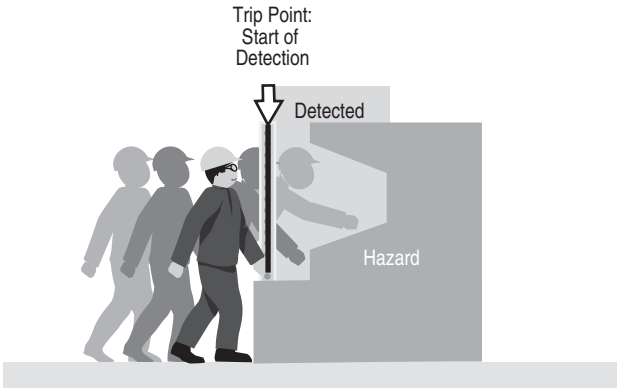


Figure 24: Partial Body Access

Safety Light Curtains

Safety light curtains are most simply described as photoelectric presence sensors specifically designed to protect personnel from injuries related to hazardous machine motion. Also known as AOPDs (Active Opto-electronic Protective Devices) or ESPE (Electro Sensitive Protective Equipment), light curtains offer optimal safety, yet they allow for greater productivity and are the more ergonomically sound solution when compared to mechanical guards. They are ideally suited for applications where personnel need frequent and easy access to a point of operation hazard.

Light curtains are designed and tested to meet IEC 61496-1 and -2. There is no harmonized EN version of part 2 so Annex IV of the European Machinery Directive requires third party certification of light curtains prior to placing them on the market in the European Community. Third parties test the light curtains to meet this international standard. Underwriter's Laboratory has adopted IEC 61496-1 as a U.S. national standard.

Operation

Safety light curtains consist of an emitter and receiver pair that creates a multi-beam barrier of infrared light in front of, or around, a hazardous area. The emitter is synchronized with the receiver by the photoelectric beam nearest one end of the housing. To eliminate susceptibility to false tripping attributed to ambient light and interference (crosstalk) from other opto-electronic devices, the LEDs in the emitter are pulsed at a specific rate (frequency modulated), with each LED pulsed sequentially so that an emitter can only affect the specific receiver associated with it. When all the beams have been checked, the scan starts over again. An example of a basic light curtain system is shown in Figure 25.

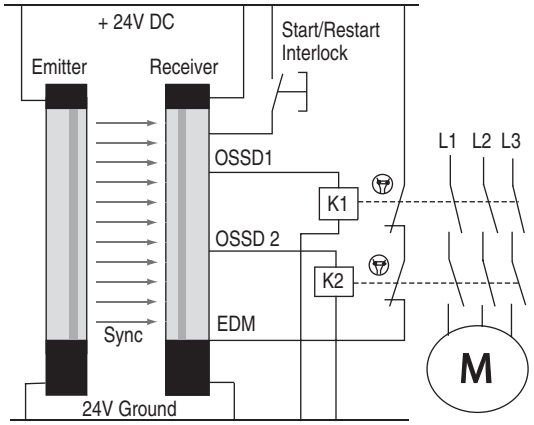


Figure 25: Basic Light Curtain Safety System

When any of the beams are blocked by intrusion into the sensing field, the light curtain control circuit turns its output signals off. The output signal must be used to turn the hazard off. Most light curtains have OSSD (Output Signal Switching Devices) outputs. The OSSDs are PNP type transistors with short circuit protection, overload protection and cross fault (channel to channel) detection. They can switch DC powered devices, like safety contactors and safety control relays, usually up to 500 mA.

Start/Restart Interlock: Light curtains are designed to interface directly with either low power machine actuators or logic devices like monitoring safety relays or programmable safety controllers. When switching machine actuators directly, the Start/Restart interlocking input of the light curtain must be used. This prevents the light curtain from re-initiating the hazard when the light curtain is initially powered or when the light curtain is cleared.

EDM: Light curtains also have an input that allows them to monitor the machine actuators. This is known as EDM (external device monitoring). After the light curtain is cleared, the light curtain determines if the external actuator is off before enabling any restart.

The emitter and receiver can also be interfaced to a control unit that provides the necessary logic, outputs, system diagnostics and additional functions (muting, blanking, PSDI) to suit the application.

The light curtain system must be able to send a stop signal to the machine even in the event of a component failure(s). Light curtains have two cross monitored outputs that are designed to change state when the safety light curtain sensing field is broken. If one of the outputs fails, the other output responds and sends a stop signal to the controlled machine and as part of the cross monitored system detects that the other output did not change state or respond. The light curtain would then go to a lock out condition, which prevents the machine from being operated until the safety light curtain is repaired. Resetting the safety light curtains or cycling power will not clear the lock out condition.

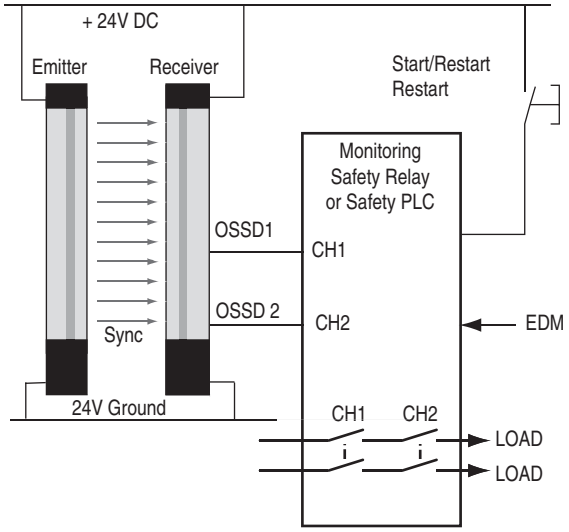


Figure 26: Light Curtain Interfacing with MSR or Safety PLC

Light curtains are often integrated into the safety system by connecting them to a monitoring safety relay (MSR) or safety PLC, as shown in Figure 26. In this case, the MSR or safety PLC handles the switching of the loads, the start/restart interlock and the external device monitoring. This approach is used for complex safety functions, and large load switching requirements. This also minimizes the wiring to the light curtain.

Resolution:

One of the important selection criteria for light curtain is its resolution. Resolution is the theoretical maximum size that an object must be to always trip the light curtain. Frequently used resolutions are 14 mm, which is commonly used for finger detection; 30 mm, which is commonly used for hand detection; and 50 mm, which is commonly used for ankle detection. Larger values are used for full body detection.

The resolution is one of the factors that determine how close the light curtain can be placed to the hazard. See the section on "Safety Distance Calculation" for more information.

Vertical Applications:

Light curtains are most often used in vertically mounted applications. The light curtains must be placed at such distance as to prevent the user from reaching the hazard before the hazard stops.

In reach-through applications, the breaking of the light curtain initiates a stop command to the hazard. While continuing to reach through, to load or unload parts for example, the operator is protected because some part of their body is blocking the light curtain and preventing a restart of the machine.

Fixed guards or additional safeguarding must prevent the operator from reaching over, under or around the light curtain. Figure 27 shows an example of a vertical application.

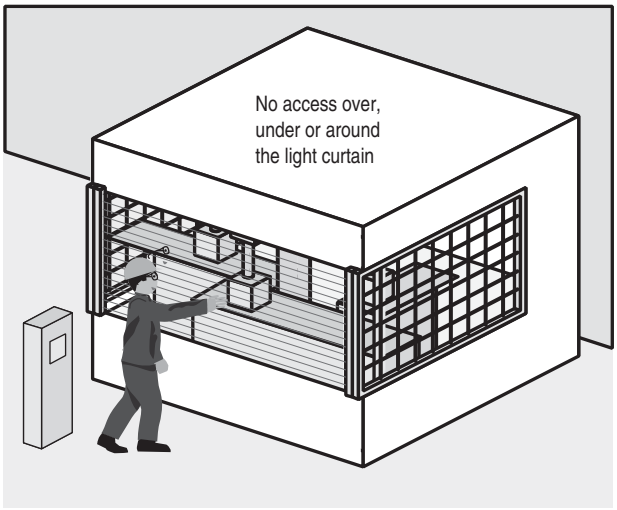


Figure 27: Vertical Application

Cascading

Cascading is a technique of connecting one set of light curtains directly to another set of light curtains like that shown in Figure 28. One set acts as the host, and the other set acts as a guest. A third light curtain can be added as the second guest. This approach saves cabling costs and input terminals at the logic device. The tradeoff is that the response time of the cascaded light curtains is increased as more beams have to be checked during each scan of the cascaded light curtain.

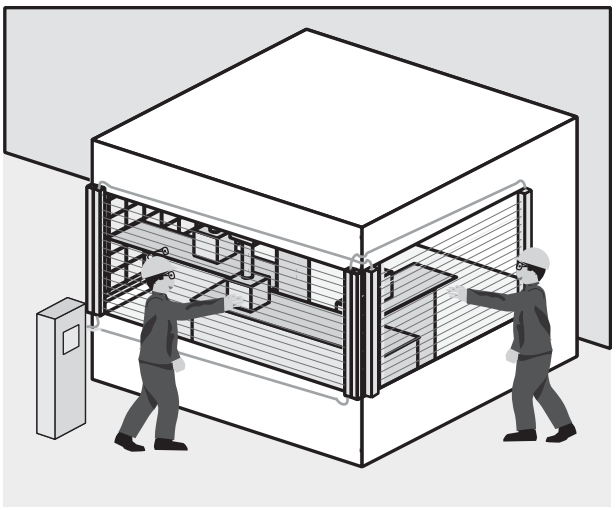


Figure 28: Cascaded Light Curtains

Fixed Blanking

Blanking allows portions of a light curtain's sensing field to be disabled to accommodate objects typically associated with the process. These objects must be ignored by the light curtain, while the light curtain still provides detection of the operator.

Figure 29 shows an example where the object is stationary. Mounting hardware, machine fixture, tooling, or conveyor are in the blanked portion of the light curtain. Known as monitored fixed blanking, this function requires that the object be in the specified area at all times. If any of the beams programmed as “blanked” are not blocked by the fixture or work piece, a stop signal is sent to the machine.

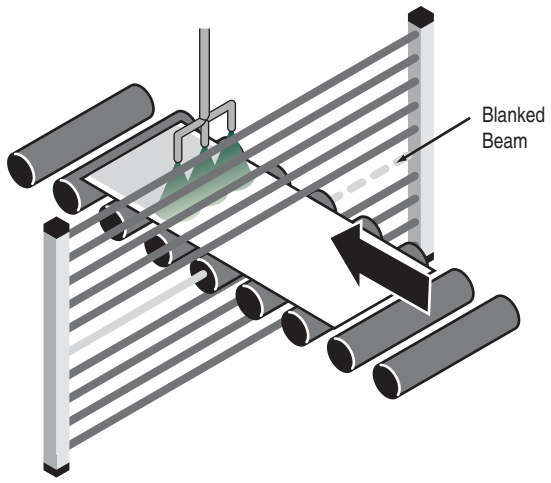


Figure 29: LIght Curtain Is Blanked Where Conveyor Is Fixed

Floating Blanking

Floating blanking allows an object such as feed stock to penetrate the sensing field at any point without stopping the machine. This is accomplished by disabling up to two light beams anywhere within the sensing field. Instead of creating a fixed window, the blanked beams move up and down, or “float,” as needed.

The number of beams that can be blanked depends on the resolution. Two beams can be blanked with a resolution of 14 mm, whereas only one beam can be blanked when a resolution of 30 mm is used. This restriction maintains a smaller opening to help prevent the operator from reaching through the blanked beams.

The beam(s) can be blocked anywhere in the sensing field except the sync beam without the system sending a stop signal to the protected machinery. A press brake, shown in Figure 30, provides a good example. As the ram moves down, the sheet metal bends and moves through the light curtain, breaking only one or two contiguous beams at a time.

Visit our website: www.ab.com/catalogs
Publication S117-CA001A-EN-P

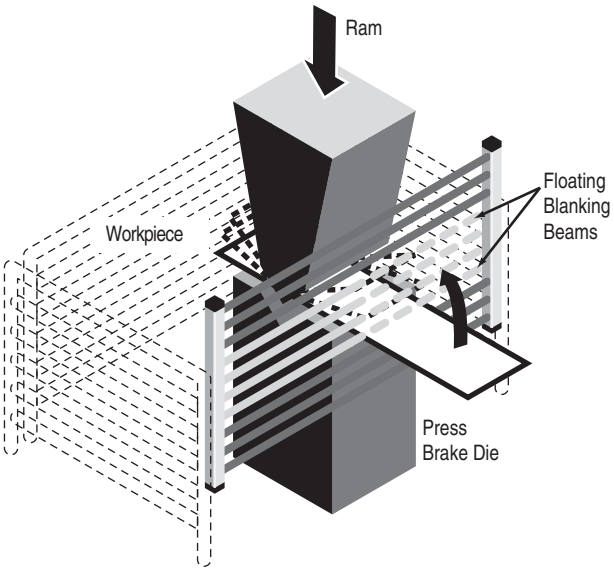


Figure 30: Floating Blanking

When using blanking, fixed or floating, the Safety Distance (the minimum distance the light curtain can be from the hazard such that an operator cannot reach the hazard before the machine stops) is affected. Since blanking increases the minimum object size that can be detected, the minimum safety distance must also increase based on the formula for calculating the minimum safety distance (see the Safety Distance Calculation section).

Horizontal Applications

After calculating the safety distance, the designer might find that the machine operator can fit in the space between the light curtain and the hazard. If this space exceeds 300 mm (12 in.), additional precautions must be considered. One solution is to mount a second light curtain in a horizontal position. These can be two independent sets of light curtains or a cascaded pair of light curtains. Another alternative is to mount a longer light curtain on an angle to the machine. These alternatives are shown in Figure 31. In either alternative, the light curtains must be located a safe distance away from the hazard.

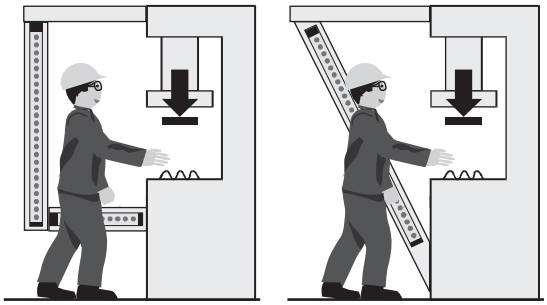


Figure 31: Alternative Solutions for Space between Light Curtain and Hazard

For longer safety distances or for area detection, light curtains can be mounted horizontally, as shown in Figure 32. The light curtains must not be mounted too close to the floor to prevent them from getting dirty, nor too high so as to allow someone to crawl under the light curtain. A distance of 300 mm (12 in.) off the floor is often used. Additionally, the light curtains must not be used as foot steps to gain access. The resolution of the light curtain must be selected to at least detect a person's ankle. No larger than 50 mm resolution is used for ankle detection. If the light curtain does not protect the whole cell, then a manual rest function must be used. The reset button must be located outside the cell with full view of the cell.

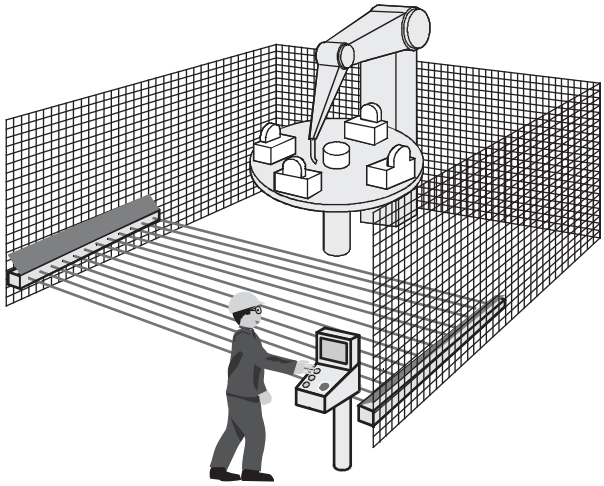


Figure 32: Horizontal Application of a Light Curtain

Perimeter or Area Access Control

Perimeter access control is often used to detect access along the outside edge of a hazard area. Light curtains used to detect perimeter access have resolutions that detect full bodies, as shown in Figure 33. This can be accomplished by a couple different ways. Multi-beam light curtains consisting of two or three beams or a single beam device that is reflected off mirrors to create a dual beam pattern are regularly used. In either case, the lowest beam should be 300 mm (12 in.) off the ground, and the highest beam should prevent a person from simply climbing over the light curtain.

Mirrors can be used to deflect the light beam around a cell. The distance the light curtain can cover is reduced due to the losses in the mirror reflections. Alignment of the light curtain is more difficult and a visible laser alignment tool is often needed during installation.

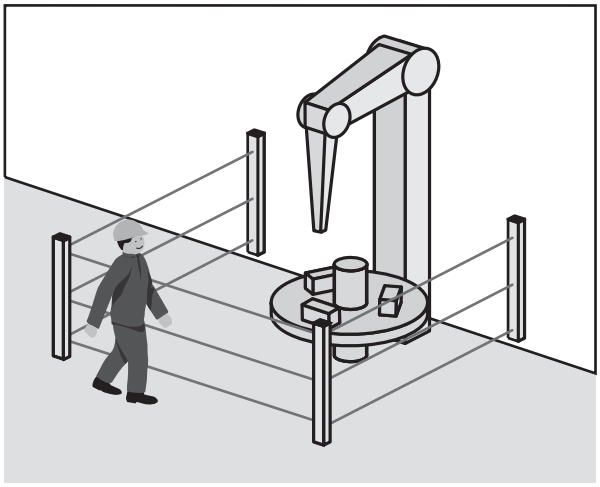


Figure 33: Mirrors Create Perimeter

Mirrors can be used to deflect the light beam around a cell. The distance the light curtain can cover is reduced due to the losses in the mirror reflections. Alignment of the light curtain is more difficult and a visible laser alignment tool is often needed during installation.

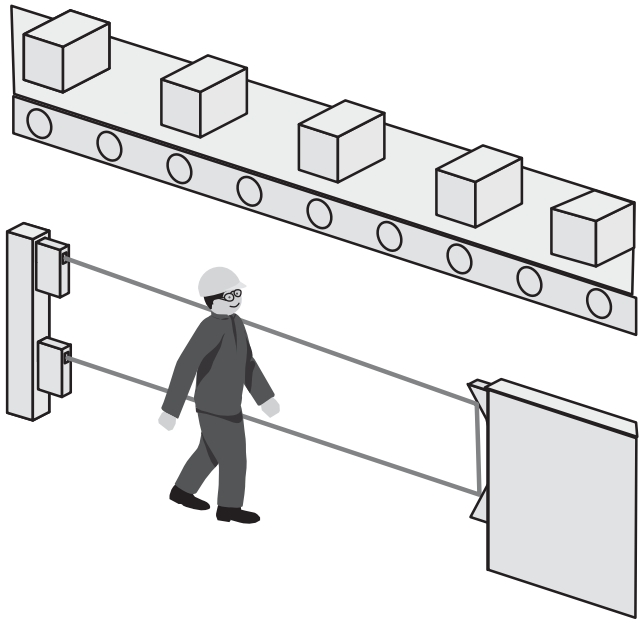


Figure 34: Single Beam Devices for Low Risk Applications

Some single beam devices have extensive (up to 275 feet) sensing distances. This allows a single beam device to create a protective barrier around hazardous machines. Since only a single or dual beam arrangement can be made, this approach is limited to low risk applications. The “Safety Distance Calculation” section (page) discussed beam placement and spacing to achieve adequate protective fields. Figure 34 shows an example of a single beam application. This approach is generally used in low risk applications, due to the larger beam spacing. Breakage of the beam is used to stop the hazardous machine motion.

Safety Laser Scanners

Safety laser scanners use a rotating mirror that deflects light pulses over an arc, creating a plane of detection. The location of the object is determined by the angle of rotation of the mirror. Using a “time-of-flight” technique of a reflected beam of invisible light, the scanner can also detect the distance the object is from the scanner. By taking the measured distance and the location of the object, the laser scanner determines the exact position of the object.

Laser scanners create two zones: 1) a warning zone and 2) a safety zone. The warning zone provides a signal that does not shut down the hazard and informs people that they are approaching the safety zone as shown in Figure 35. Objects entering or inside the safety zone cause the laser scanner to issue a stop command; the OSSD outputs turn off.

The shape and size of the protected area is configured by an accompanied software program and downloaded to the scanner. The safety distance calculation must be used to determine the appropriate size of the safety zone.

One advantage of the laser scanner over a horizontal light curtains or mats is the ability to reconfigure the area. Figure 35 shows an example of the warning field configured to ignore structural objects.

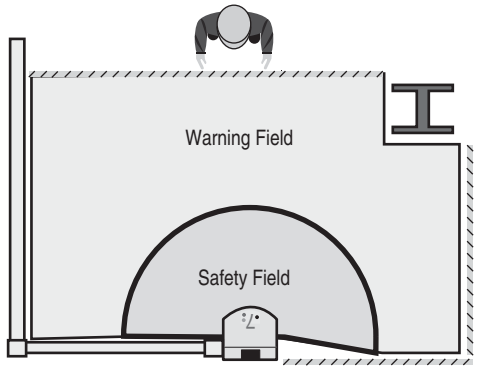


Figure 35: Warning Field Configured Around Structural Objects

Developments in laser scanner technology allow a single scanner to cover multiple zones. In Figure 36, the laser scanner allows operator access to one side (shown as Case 1) while the robot is busy on the other side (Case 2).

Older scanners have electro-mechanical outputs. Newer scanners adopt the same principles as light curtains and provide OSSD outputs with cross checking, external device monitoring and restart interlock for standalone use. The OSSD outputs can also be connected to logic devices when needed as part of a larger system.

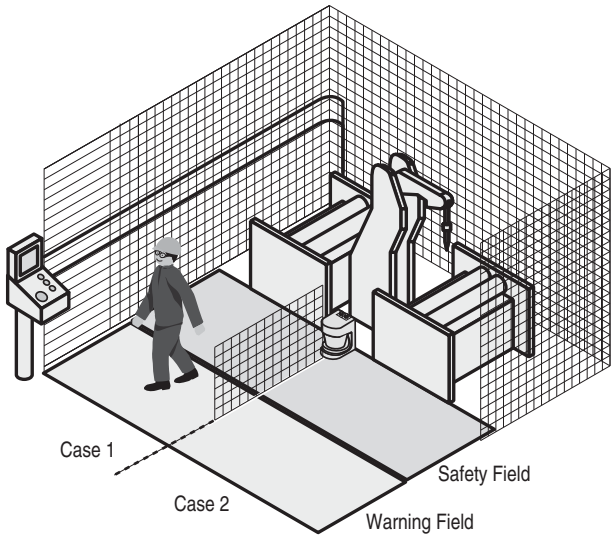


Figure 36: Multizone Application of Laser Scanner

Muting

Muting is characterized as the automatic, temporary suspension of a safety function. Sometimes the process requires that the machine stop when personnel enters the area, yet remain running when automatically-fed material enters. In such a case, a muting function is necessary. Muting is permitted during the non-hazardous portion of the machine cycle or must not expose people to a hazard.

Sensors are used to initiate the muting function. The sensors may be safety rated or non-safety rated. The types, number and location of muting sensors must be selected to meet the safety requirements determined by the risk assessment.

Figure 37 shows a typical conveyor material handling muting arrangement using two sensors. The sensors are arranged in an X pattern. Some logic units require a specific order in which the sensors are blocked. When order is important, the X pattern must be asymmetrical. For those logic units that use the sensor inputs as pairs, the X pattern can be symmetrical. Polarized, retroreflective photosensors are often used to prevent spurious reflections from falsely initiating the muting function, or causing nuisance trips. Other sensing technologies, such as inductive sensors and limit switches may also be use.

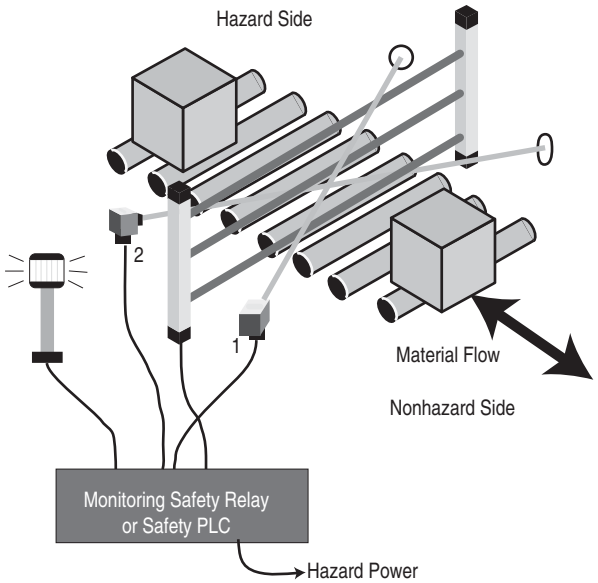


Figure 37: Conveyor 2 Sensor Muting

Another commonly applied approach is to use four sensors, as shown in Figure 38. Two sensors are mounted on the hazard side and two on the non hazard side. The sensors look directly across the conveyor. The shape and position of the object is less important in this approach. The length of the object is important as the object must block all four sensors.

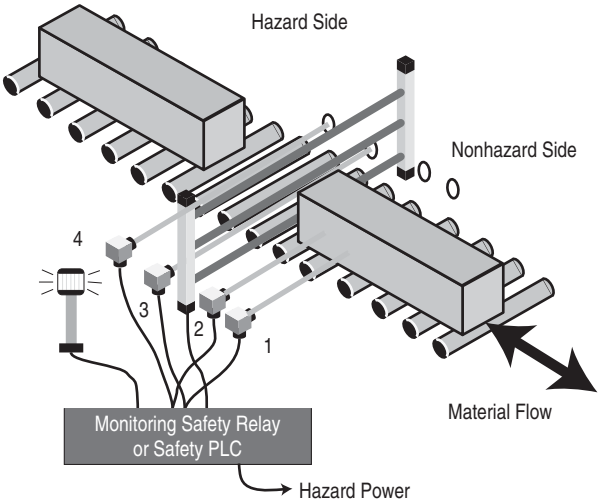


Figure 38: Conveyor 4 Sensor Muting

A common application is for a fork truck to access a conveyor. In order to mute the light curtain, the fork truck must be detected by sensors. The challenge is to locate the sensors so they detect the fork truck and not a person. Figure 39 shows an example of this application.

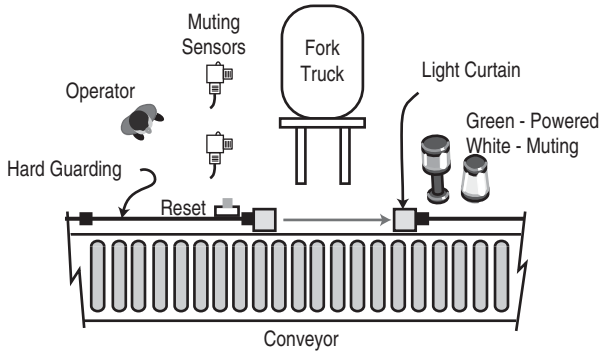


Figure 39: Fork Truck 2 Sensor Muting

Access to robot cells is also accomplished by muting. As shown in Figure 40, limit switches, located on the base of the robot, indicate the position of the robot. The safeguarding devices (the light curtains and safety mats) are muted when the robot is not in a hazardous position.

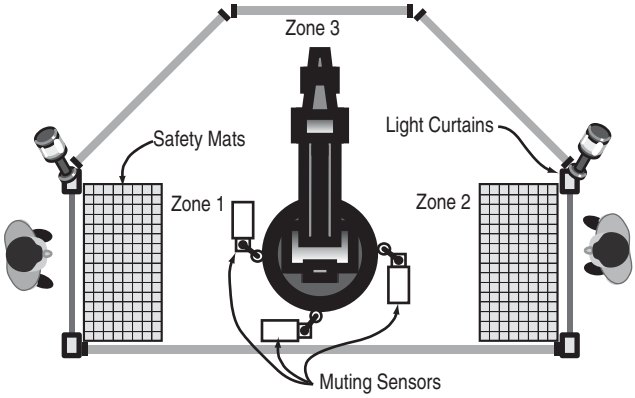


Figure 40: Muting of a Robot Cell

Presence Sensing Device Initiation (PSDI)

Also known as single break, double break, or stepping operating mode, PSDI involves the use of a light curtain not only as a safety device, but as the control for machine operation. PSDI initiates a machine cycle based on the number of times the sensing field is broken. For example, as an operator reaches toward the hazard to insert a work piece, breakage of the beams immediately stops the machine or prevents restart of the machine until the operator removes his hand from the area, at which time the machine automatically initiates its next cycle. This process can be accomplished by safety programmable logic devices or by monitoring relays specifically designed for this function.

Auto initiation allows the machine to start and stop based on the number of times the light curtain beams are broken and cleared. Illustrated in Figures 41 to 43 is an auto initiation double break mode (after initial start-up sequence).

In Step 1, the operator breaks the light curtain. The machine is stopped and the operator removes the processed material. The operator clears the light curtain, making the first break.

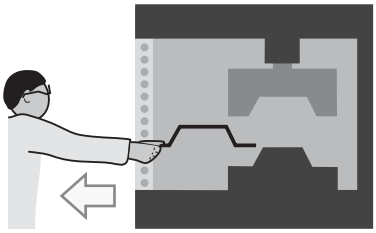


Figure 41: Step 1 of Double Break PSDI

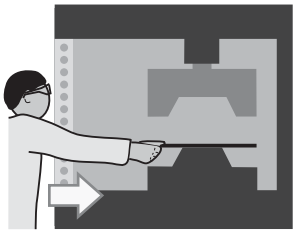


Figure 42: Step 2 of Double Break PSDI

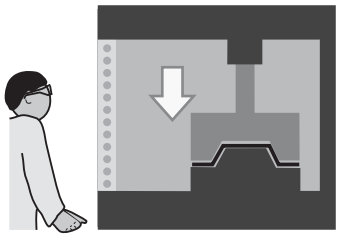


Figure 43: Step 3 of Double Break PSDI

In Step 2, the operator breaks the light curtain a second time and loads new material. The machine remains in stop mode.

In Step 3, the machine starts automatically after the second clearing of the light curtain.

Pressure Sensitive Safety Mats

These devices are used to provide guarding of a floor area around a machine, as shown in Figure 44. A matrix of interconnected mats is laid around the hazard area and pressure applied to the mat (e.g., an operator's footstep) will cause the mat controller unit to switch off power to the hazard.

There are a number of technologies used to create safety mats. One of the more popular technologies is using two parallel metal plates, as shown in Figure 45. The plates are separated by spacers. The metal plates and spacers are encapsulated in a nonconductive material with its surface designed to prevent slipping.

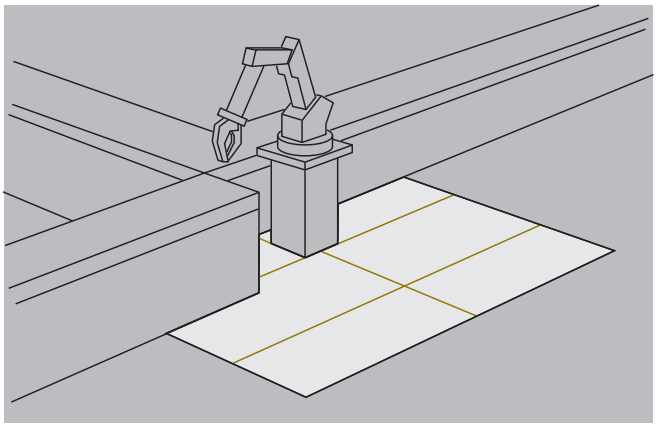


Figure 44: Safety Mats Surrounding a Robot

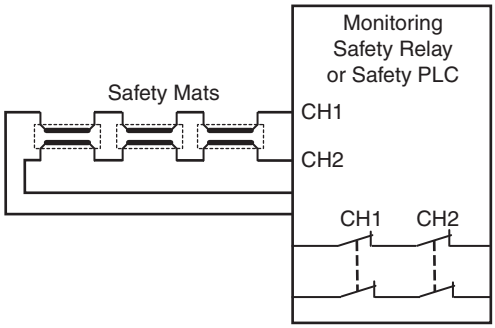


Figure 45: Safety Mat Interfacing

To ensure that the safety mat is available for use, an electrical current is passed through both plates. If an open-circuit wiring fault occurs, the safety system shuts down. To accommodate the parallel plates into a safety system, either two or four conductors are used. If two conductors are used, then a terminating resistor is used to differentiate the two plates. The more popular approach is to use four conductors. Two conductors, connected to the top plate are assigned one channel. Two conductors connected to the bottom plate are assigned to a second channel. When a person steps on the mat, the two plates create a short circuit from Channel 1 to Channel 2. The safety logic device must be designed to accommodate this short circuit. Figure 46 shows an example of how multiple 4-wire mats are connected in series to ensure the safety mats are available for use.

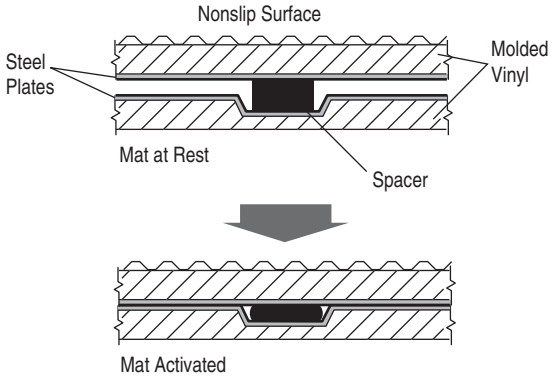


Figure 46: Typical Safety Mat Construction

Pressure sensitive mats are often used within an enclosed area containing several machines—flexible manufacturing or robotics cells, for example. When cell access is required (for setting or robot “teaching,” for example), they prevent dangerous motion if the operator strays from the safe area, or must get behind a piece of equipment, as shown in Figure 47.

The size and positioning of the mat must take the safety distance into account (see Safety Distance Calculation).

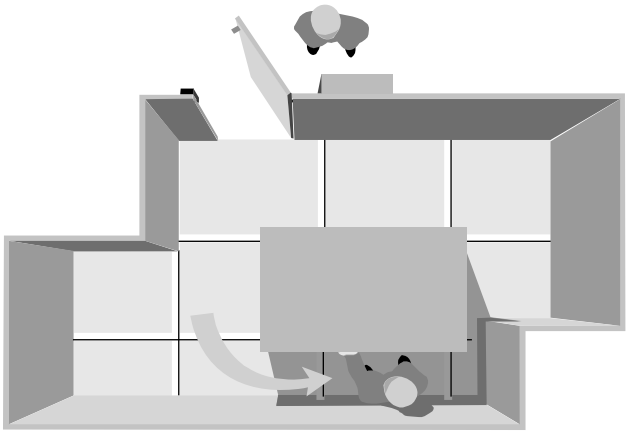


Figure 47: Safety Mat Detects Operator Behind Equipment

Pressure Sensitive Edges

These devices are flexible edging strips that can be mounted to the edge of a moving part, such as a machine table or powered door that poses a risk of a crushing or shearing, as shown in Figure 48.

If the moving part strikes the operator (or vice versa), the flexible sensitive edge is depressed and will initiate a command to switch off the hazard power source. Sensitive edges can also be used to guard machinery where there is a risk of operator entanglement. If an operator becomes caught in the machine, contact with the sensitive edge will shut down machine power.

There are a number of technologies used to create safety edges. One popular technology is to insert essentially what is a long switch inside the edge. This approach provides straight edges and generally uses the four-wire connection technique.

Figure 48: Edge on Machine Table and Powered Door

The Allen-Bradley Guardmaster Safedge uses conductive rubber, with two wires running the length of edge (Figure 49). At the end of the edge, a terminating resistor is used to complete the circuit. Depressing the rubber reduces the circuit resistance.

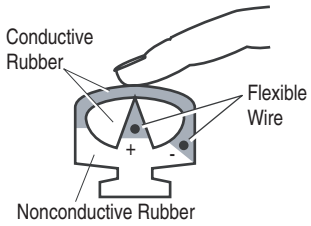


Figure 49: Conductive Rubber Safety Edge

Since a change in resistance must be detected, the monitoring safety relay must be designed to detect this change. An example wiring of this two-wire design with a terminating resistor is shown in Figure 50. One advantage of the conductive rubber technology is that it provides active corners.

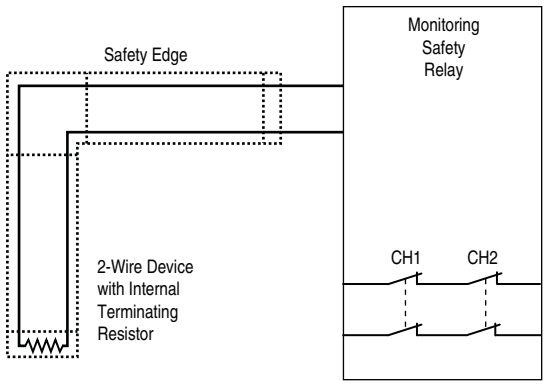


Figure 50: Conductive Rubber Safety Edge Circuit

Light curtains, scanners, floor mats and sensitive edges are classified as “trip devices.” They do not actually restrict access but only “sense” it. They rely entirely on their ability to both sense and switch for the provision of safety. In general they are only suitable on machinery which stops reasonably quickly after switching off the power source. Because an operator can walk or reach directly into the hazard area it is obviously necessary that the time taken for the motion to stop is less than that required for the operator to reach the hazard after tripping the device.

Safety Switches

When access to the machine is infrequent, movable (operable) guards are preferred. The guard is interlocked with the power source of the hazard in a manner which ensures that whenever the guard door is not closed the hazard power will be switched off. This approach involves the use of an interlocking switch fitted to the guard door. The control of the power source of the hazard is routed through the switch section of the unit. The power source is usually electrical but it could also be pneumatic or hydraulic. When guard door movement (opening) is detected the interlocking switch will initiate a command to isolate the hazard power supply either directly or via a power contactor (or valve).

Some interlocking switches also incorporate a locking device that locks the guard door closed and will not release it until the machine is in a safe condition. For the majority of applications the combination of a movable guard and an interlock switch with or without guard locking is the most reliable and cost effective solution.

Tongue Interlock Switches

Tongue operated interlocks require a tongue-shaped actuator to be inserted and removed from the switch. When the tongue is inserted, the internal safety contacts close and allow the machine to run. When the tongue is removed, the internal safety contacts open and send a stop command to the safety related parts of the control system. Tongue operated interlocks are versatile as they can be used on sliding, hinged or removable guards as shown in Figure 51.

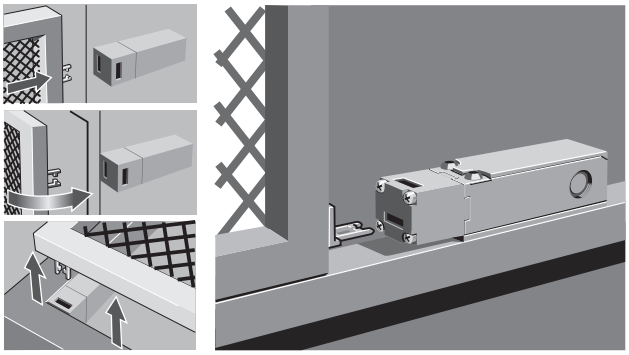


Figure 51: Tongues Interlocks on Sliding, Hinge or Removable Guards

Some of the latest functional safety standards focus on the need for complete fault tolerance as part of the requirements for device that is being used for high risk levels (e.g. SIL 3 or PLe). Because, in theory, mechanical tongue operated switches have single points of failure (e.g. the tongue actuator) even though they have two electrical switching channels. This means that non-contact switches may be preferred in these cases because they do not generally have the single mechanical failure points.

Tongue interlocks have three basic features that allow them to have a safety rating: defeatability, galvanic isolation, and direct opening action.

Defeatability

The security of an interlock switch is dependent on its ability to withstand attempts to "cheat" or defeat the mechanism. An interlock switch should be designed so that it cannot be defeated by simple tools or materials which may be readily available (like screwdrivers, coins, tape, or wire).

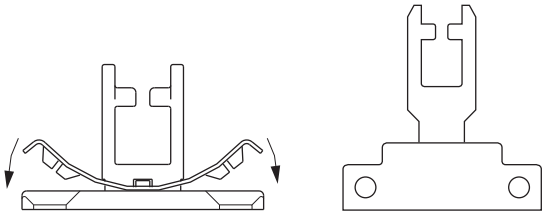


Figure 52: Tongue Shaped Actuators with Dimensional Features to Help Prevent Defeatability

This is accomplished by making the actuator a special shape, as shown in Figure 52. When maintenance is required on the machine, the interlocks may have to be bypassed. If this is done, other safeguarding methods for protection must be provided. Access to spare actuators must be controlled by management operating procedures. Some actuators, like the one on the left in Figure 52, have a spring that prevents the tongue from fully entering and operating the interlock switch unless it is correctly fixed to the guard.

In some circumstances personnel may be tempted to override the switch in some way. Information concerning the use of the machine, gathered at the risk assessment stage, will help to decide whether this is more likely or less likely to happen. The more likely it is to happen then the more difficult it should be to override the switch or system. The level of estimated risk should also be a factor at this stage. Switches are available with various levels of security ranging from resistance to impulsive tampering, to being virtually impossible to defeat.

It should be noted at this stage that if a high degree of security is required it is sometimes more practical to achieve this by the way in which it is mounted.

For example, if the switch is mounted as in Figure 53 with a covering track, there is no access to the switch with the guard door open. The nature of any "cheating" prevention measures taken at the installation will depend on the operating principle of the switch.

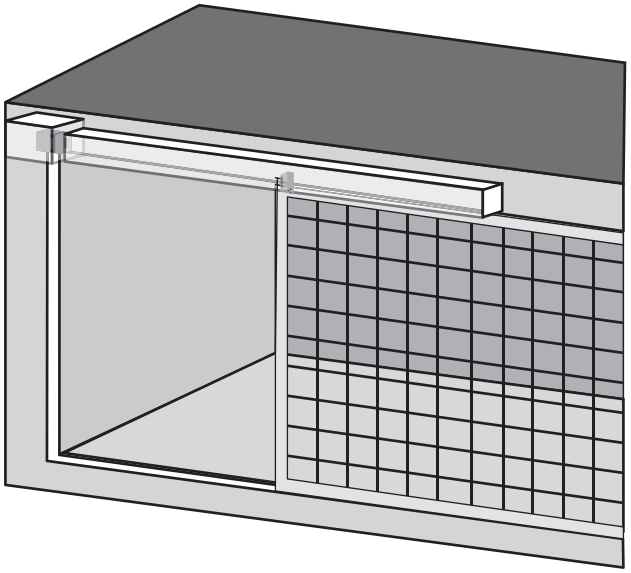


Figure 53: Switch and Actuator Hidden

Direct Opening Action

ISO 12100-2 explains that if a moving mechanical component inevitably moves another component along with it, either by direct contact or via rigid elements, these components are said to be connected in the positive mode. IEC 60947-5-1 uses the term Direct Opening Action and defines it as achievement of contact separation as the direct result of a specified movement of the switch actuator through non-resilient members (for example not dependent upon springs). This standard provides a set of test that can be used to verify Direct Opening Action. Products that meet the requirements of Direct Opening Action display the symbol shown in Figure 54 on their enclosure.

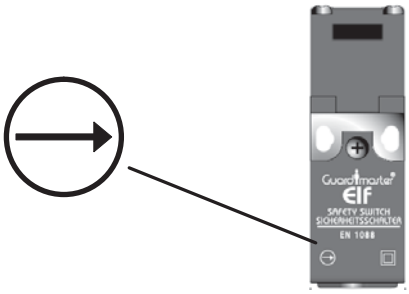


Figure 54: Symbol of Direct Opening Action

Figure 55 shows an example of positive mode operation giving forced disconnection of the contacts. The contacts are considered normally-closed (N.C.) when the actuator is inserted into the switch (i.e., guard closed). This closes an electrical circuit and allows current to flow through the circuit when the machine is allowed to run. The closed circuit approach allows for the detection of a broken wire which will initiate a stop function. These switches are typically designed with double break contacts. When the guard is opened, the tongue is removed from the operating head and rotates an internal cam. The cam drives the plunger which forces the spanner to open both contacts, breaking potentially welded contacts.

Visit our website: www.ab.com/catalogs
Publication S117-CA001A-EN-P

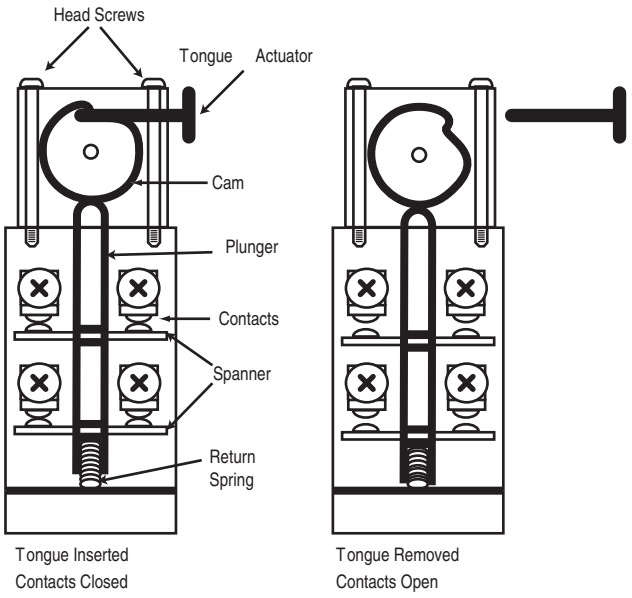


Figure 55: Double-Break with Direct Opening Action

Most tongue interlocks also have a set of normally-open (N.O.) contacts. These contacts typically close by the force of the return spring. If the spring breaks, proper contact operation cannot be performed with a high enough degree of reliability. Therefore, they are typically used to signal the machine control system that the guard is open.

Normally-open spring-return contacts can be used as a secondary channel in a safety system. This approach provides diversity to the safety system to help prevent common cause failures. The monitoring safety relay or safety PLC must be designed to accommodate this diverse N.O. + N.C. approach.

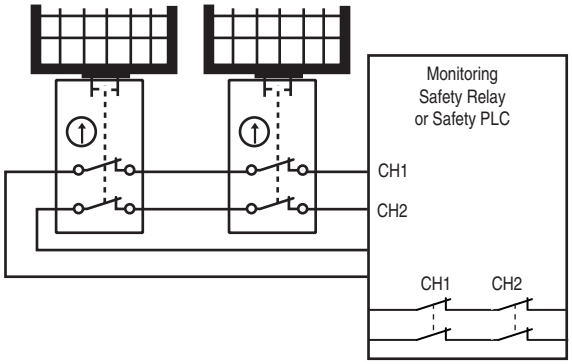


Figure 56: Daisy Chain of Multiple Two N.C. Interlocks

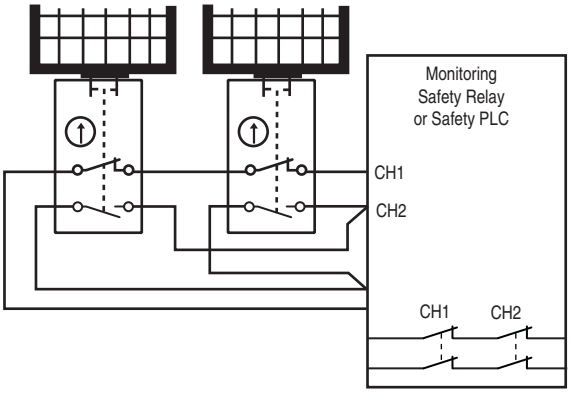


Figure 57: Multiple Interlocks with N.C. and N.O. Contacts

One advantage of using two normally closed contacts with interlocks is reduction in the wiring when multiple gates must be monitored. Figure 56 shows how multiple gates can be daisy chained. This may be practical for a small number of gates, but becomes more challenging to troubleshoot when too many gates are connected in series.

Where the risk assessment deems the use of diverse contacts, the N.C. contacts are connected in series and the N.O. contacts are connected in parallel. Figure 57 shows a basic schematic of this approach when multiple interlocks are monitored by a monitoring safety relay. The N.O. contacts in the Channel 2 circuit are connected in parallel.

Duplication (also referred to as Redundancy)

If components which are not inherently safe are used in the design, and they are critical to the safety function, then an acceptable level of safety may be provided by duplication of those components or systems. In case of failure of one component, the other one can still perform the function. It is usually necessary to provide monitoring to detect the first failure so that, for example, a dual channel system does not become degraded to a single channel without anybody being aware of it. Attention also must be given to the issue of common cause failures.

Protection must be provided against failure, which will cause all duplicated components (or channels) to fail at the same time Suitable measures may include using diverse technologies for each channel or ensuring an oriented failure mode.

Galvanic Isolation

Figure 58 shows contact blocks with two sets of contacts. A galvanic isolation barrier is required if it is possible for the contacts to touch each other back to back in the event of contact weld or sticking.

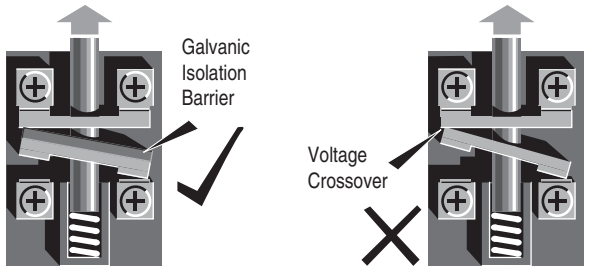


Figure 58: Galvanic Isolation of Contacts

Mechanical Stops

Interlock switches are not designed to withstand the stopping of a gate. The machine designer must provide an adequate stop while also providing enough travel for the actuator to fully insert into the switch (Figure 59).

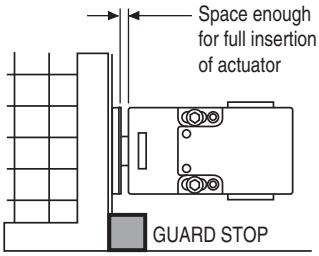


Figure 59: Mechanical Stops

The guard-mounted tongue needs to remain reasonably well aligned with the entry hole in the switch body. Over time, hinges may wear and guards may bend or twist. This adversely affects the alignment of the actuator to the head. The machine designer should consider metal bodied interfaces and flexible actuators, as shown in Figure 60.

Figure 60: Metal Interface with Flexible Actuator

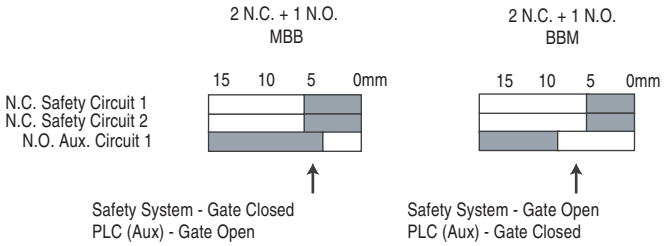


Figure 61: MBB and BBM Contacts—Conflicting Messages

Due to wear, damaged, or other changes to the guarding over time, pressure may be applied to the door forcing it open slightly. If the door moves between to the point where the change-over occurs, the safety system and machine control system will get conflicting messages, as shown in Figure 61.

Fixes for this include latching the door closed or using snap acting contacts. Selection of the appropriate tongue interlock involves many considerations: plastic or metal body, number of contacts, contact operation, size of guard, alignment of guard, movement of the guard, space available and washdown. Tongue operated switches can be difficult to clean thoroughly. Thus, food/beverage and pharmaceutical industries generally prefer non contact interlocks.

Guard Locking Switches

In some applications, locking the guard closed or delaying the opening of the guard is required. Devices suitable for this requirement are called guard locking interlock switches. They are suited to machines with run down characteristics but they can also provide a significant increase of protection level for most types of machines.

For most types of guard locking interlock switches, the unlocking action is conditional on the receipt of some form of electrical signal, for example an electrical voltage to energize a lock release solenoid. This principle of conditional release makes the solenoid controlled guard locking switch a very useful and adaptable device. Whereas with most devices the safety function is achieved by stopping the machine, guard locking switches also prevent access to the machine and prevent restart of the machine whenever the lock is released. Therefore these devices can perform two separate but inter-related safety functions: prevention of access and prevention of dangerous movement. This means that these switches are fundamentally important in the field of machinery safety. The following text describes some typical application based reasons why guard locking interlock switches are commonly used:

Protection of machine and people: In many situations tool or work piece damage can be caused or significant process disruption incurred if a machine is stopped suddenly at the wrong point in its operating sequence. A typical example of this would be the opening of an interlocked guard door of an automated machine tool in mid cycle. This situation can be avoided by using a solenoid controlled guard locking switch. If access through the guard door is required a lock release request signal is sent to the machine controller which will then wait for a properly sequenced stop before sending the release signal to the guard locking switch.

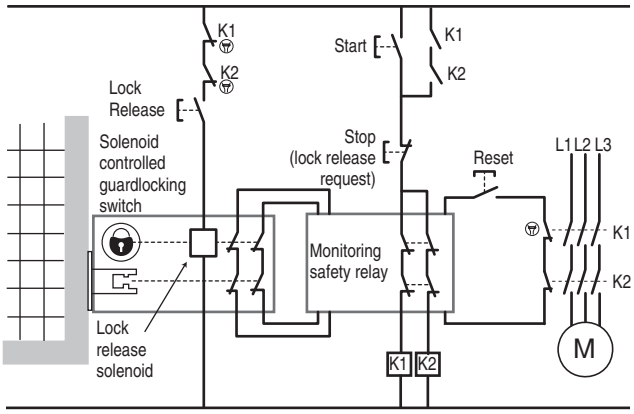


Figure 62: Simplified Basic Solenoid Guard Locking Switch Scheme

Figure 62 shows a very simplified schematic view of the principle. In practice, the start, stop and lock release functions of the push switches shown would typically be achieved by inputs and outputs of the machine's PLC. The PLC would accept a lock release request input at any point in the machine cycle but would only action a release command at the end of that cycle. The release command would be the equivalent of pressing the stop and lock release push switches.

When the lock is released and the guard door is opened, the switch contacts open causing the isolation of power to the hazard.

This type of approach can be further developed by using a key operated switch or button as the lock release request. In this way it can be possible to control not only when the guard can be opened but also who can open it.

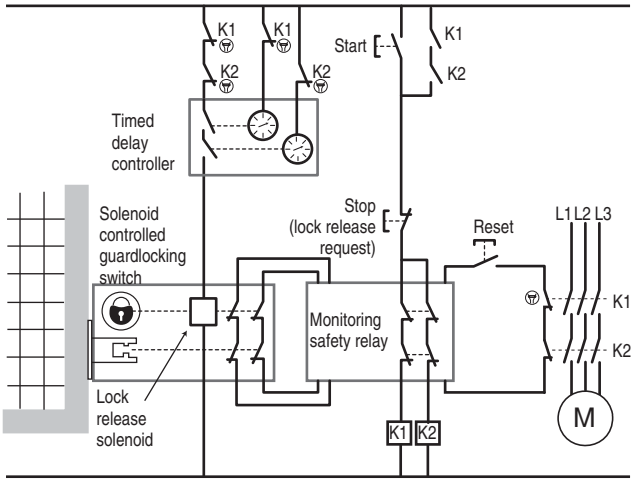


Figure 63: Timed Delay Controlled Solenoid Guard Locking Switch Scheme

Protection against machine run down: On many machines, removal of power to the motor or actuator will not necessarily cause a reliable and immediate stopping of the dangerous motion. This situation can be addressed by using a solenoid controlled guard locking switch with its release conditional on implementation of some form of delay that ensures that all dangerous motion has stopped before the lock is released.

Timed delay: The simplest method is to use a timed delay function configured so that the switch will not release the guard until the contactor is OFF and a preset time interval has elapsed. This is shown in Figure 63. The timed delay function can be provided by a Safety PLC or a dedicated controller. It is important that it is safety rated because failure that causes a shorter time delay than specified could result in exposure to dangerous moving parts.

The timed delay interval should be set at least to the worst case stopping time of the machine. This stopping time must be predictable, reliable and not dependant on braking methods that may degrade with use.

Stopped motion confirmation: It is also possible to make the lock release conditional on the confirmation that motion has stopped. The advantages with this approach are that even if the machine takes longer than expected to stop the lock will never be released too early. It also provides better efficiency than a timed delay because the lock is released as soon as the motion has stopped without having to always wait for the worst case stopping time. An example of this approach is shown in Figure 64.

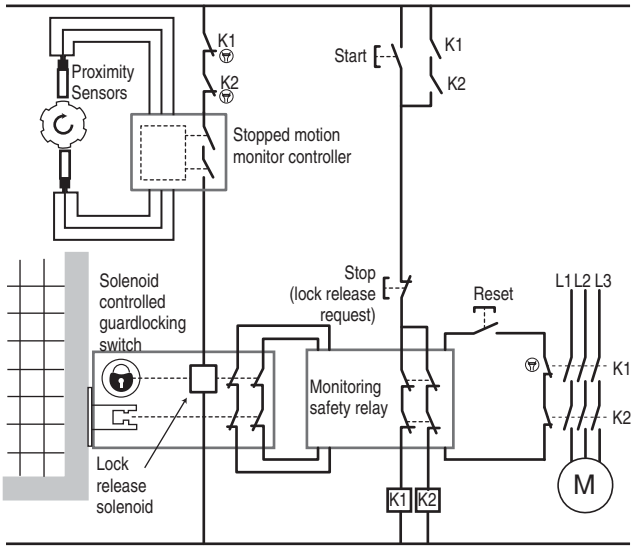


Figure 64: Simplified Stopped Motion Controlled Solenoid Guard Locking Switch Scheme

This stopped motion monitoring function must be safety rated and is usually achieved by one of the following methods:

Proximity sensors or shaft encoders combined with a dedicated controller or safety PLC.

Back EMF detection using a dedicated control unit.

Future generations of variable speed drives and motion control systems will also provide this functionality as safety rated.

Slow speed safety: For some types of machinery it may be necessary to have access to some moving parts in order to perform certain tasks such as maintenance, setting, feeding or threading. This type of activity is only considered if adequate safety can be provided by other measures. Typically these other measures will take the form of at least both of the following:

a) Access is only allowed under conditions of a safe slow speed

b) Any person with access to the moving parts must have personal local control for stopping, or prevention of starting, of the motion. The local control must override any other control signals.

This should be taken as a minimum. Whether this is acceptable or not will depend on risk assessment and relevant safety standards and regulations. However where it is found to be acceptable this type of safety functionality is often implemented using a solenoid controlled guard locking interlock switch in combination with a slow speed monitoring unit and a three position enabling device.

The safe slow speed monitoring unit constantly checks the speed of the moving parts via its input sensors and will only allow the sending of the lock release signal when the speed is not greater than its preset threshold value. After the lock has been released the slow speed unit continues to monitor the speed. If its preset threshold is exceeded while access is allowed, power to the motor will be switched off immediately. Also the safe slow speed can only continue while the enabling switch is held in the middle position (see Figure 70 for more information). It is clear that the guard locking switch, the safe slow speed unit and the enabling device must be connected to some form of safety rated logic solver in order implement the required functionality for both safety and production. In its most simple form this can simply be the way that the units are hardwired together, typically switchable via a manual mode selector switch. This switch is often key operated to restrict the safe slow speed access mode to authorized people. Greater operating efficiency and flexibility can be gained by using a configurable or programmable device for the logic solving function. This could be anything from modular configurable relay through to a Safety PLC.

This type of safe slow speed functionality is often required on complex integrated machinery systems where the equipment is divided into different operating zones each with different and interdependent operating modes. In these types of applications a Safety PLC or a dedicated configurable control unit such as the MSR57 is often a more suitable solution than individual relays and control units.

Most guard locking switches are adaptations of tongue interlocks. A solenoid is added to the interlock. The solenoid locks the actuator in place. There are two types of solenoid locking:

1. Power-to-unlock
2. Power-to-lock

Power-to-unlock devices require power to the solenoid to unlock the actuator. As long as power is applied to the solenoid, the door can be opened. With power removed from the actuator, the guard locks as soon as it is closed.

During a power loss, the gate remains closed and locked. If the guard locking device is used in full body access applications, a method of escape must be provided in case someone becomes locked in the hazard area. This is accomplished by providing a rotating lever, a pushbutton, or mechanical methods, as shown in Figure 65.

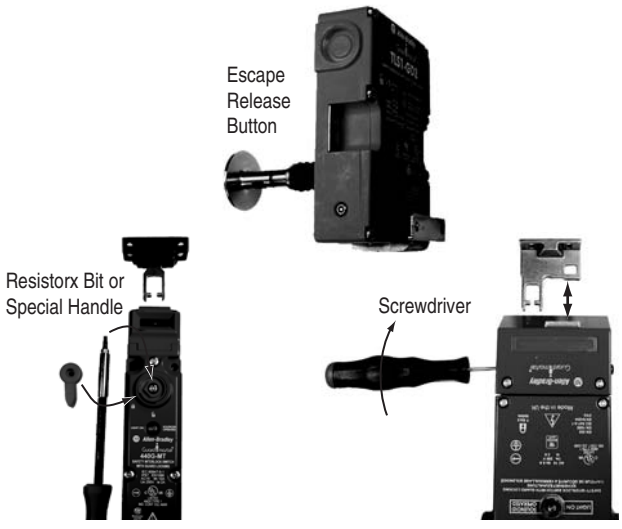


Figure 65: Escape Methods for Guard Locking

The power-to-lock requires power to the solenoid to lock the guard. A risk assessment must consider the potential hazardous situations that may arise if power is lost and the gate becomes unlocked while the machine is running down.

An important criterion when selecting guard locking interlocks is the holding force. How much force is required to hold the guard locked? When the door is manually operated, holding force can be minimal. Depending on where the guard locking switch is installed, operating leverage may suggest higher holding forces. Motorized doors may require higher holding forces.

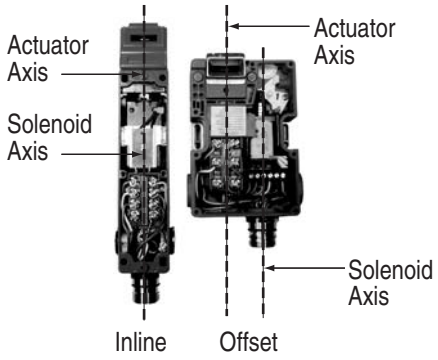


Figure 66: Inline and Offset Solenoid

Another important criterion for the selection process involves the relationship of the solenoid and the actuator. Two relationships exist: inline and offset, as shown in Figure 66. The solenoid is in the same axis as the actuator contacts or the solenoid is offset from the actuator contacts. The offset arrangement provides separate contacts that provide status of the solenoid.

The inline arrangement does not provide separate contacts for the solenoid. The inline arrangement is a little easier to apply. The offset arrangement provides more information on the operation of the switch. With the offset arrangement, the machine designer must ensure the solenoid status is monitored by the safety system. Selection of either arrangement is based on user preference.

A second type of guard locking device is manually operated and the guard can be opened at any time. A handle or knob that releases the guard lock also opens the control circuit contacts.

On a device such as the bolt switch, a time delay is imposed. The bolt which locks the guard in place operates the contacts and is withdrawn by turning the operating knob. The first few turns open the contacts but the locking bolt is not fully retracted until the knob is turned many more times (taking up to 20 seconds). These devices are simple to apply and they are extremely rugged and reliable. The time delay bolt switch is suitable mainly for sliding guards.

The stopping time of the hazard must be predictable and it must not be possible for the bolt to be withdrawn before the hazard has ceased. It must only be possible to extend the bolt into its locked position when the guard is fully closed. This means that it will be necessary to add stops to restrict the travel of the guard door, as shown in Figure 67.

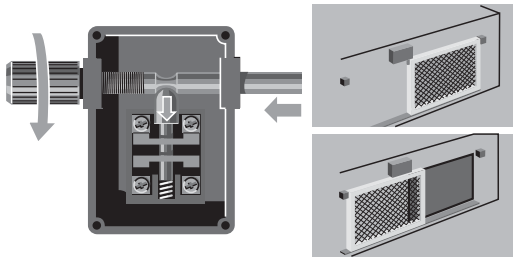


Figure 67: Sliding Bolt Interlock

Non-Contact Interlock Switches

Some of the latest functional safety standards focus on the need for complete fault tolerance as part of the requirements for device that is being used for high risk levels (e.g. SIL 3 or PLe). Because, in theory, mechanically actuated switches have single points of failure (e.g. the tongue actuator) even though they have two electrical switching channels. This means that dual channel non-contact switches may be preferred in these cases because they do not generally have the single mechanical failure points.

For non-contact interlocks, no physical contact (under normal conditions) takes place between the switch and actuator. Therefore positive mode operation cannot be used as the way of ensuring the switching action, and we need to use other methods to achieve equivalent performance.

Redundancy

Just as described in the section on tongue interlock switches, a high level of safety can be provided by non-contact devices designed with component duplication (or redundancy). In case of a failure of one component there is another one ready to perform the safety function and also a monitoring function to detect that first failure. In some cases it can be an advantage to design devices with components that have the same function but different failure mechanisms. This is referred to as diverse redundancy. A typical example is the use of one normally open contact and one normally closed contact.

Oriented Failure Mode

With simple devices we can use components with an oriented failure mode as explained in ISO 12100-2. This means using components in which the predominant failure mode is known in advance and always the same. The device is designed so that anything likely to cause a failure will also cause the device to switch off.

An example of a device using this technique is a magnetically actuated non-contact interlock switch. The contacts are connected with an internal non-reset overcurrent protection device. Any overcurrent situation in the circuit being switched will result in an open circuit at the protection device that is designed to operate at a current well below that which could endanger the safety-related contacts.

Due to the use of special components, the safety-critical fault likely to occur would be a welding of the reed contacts due to excessive current being applied to the switch as illustrated in Figure 68. This is prevented by the non-reset overcurrent protection device. There is a large margin of safety between the rating of this device and the reed contacts. Because it is non-reset, the switch should be protected by a suitably rated external fuse. The Allen-Bradley Guardmaster Ferrogard interlocks use this technique.

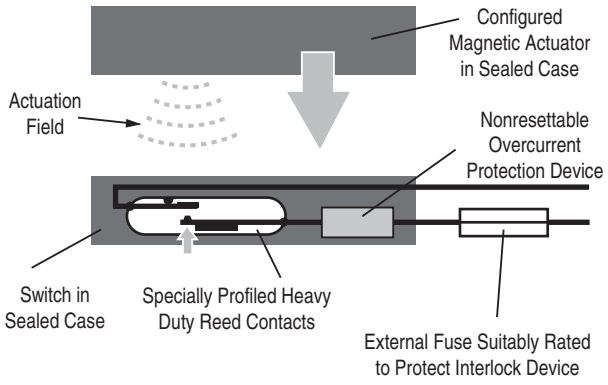


Figure 68: Simple Magnetic Operated Noncontact Interlock

Non-contact devices are designed with smooth enclosures and are fully sealed, making them ideal for food and beverage applications as they have no dirt traps and can be pressure cleaned. They are extremely easy to apply and have a considerable operating tolerance so they can accept some guard wear or distortion and still function properly.

One important consideration when applying non-contact switches is their sensing range and tolerance to misalignment. Each product family has an operating curve showing sensing range and tolerance to misalignment, as shown in Figure 69.

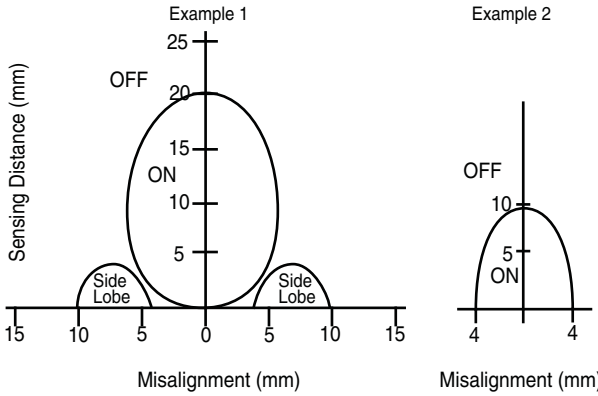


Figure 69: Non-Contact Operating Curve

Another important consideration for applying non-contact switches is the direction of approach of the actuator, as shown in Figure 70. The coding techniques determine which approaches are acceptable.

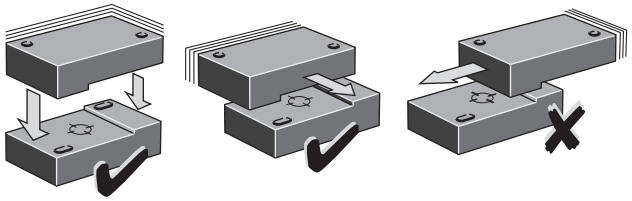


Figure 70: Approach of Actuator Affects Performance

Defeatability—Non-Contact Interlock Switches

It is important that the switch is only operated by its intended actuator. This means that ordinary proximity devices which sense ferrous metal are not appropriate. The switch should be operated by an "active" actuator.

When protection against defeatability by simple tools (a screwdriver, pliers, wire, coin, or a single magnet) is deemed necessary by the risk assessment, the noncoded actuation types must be installed so that they cannot be accessed while the guard is open. An example of this is shown in Figure 71. They should also be installed where they are not subjected to extraneous interference by magnetic/electric fields.

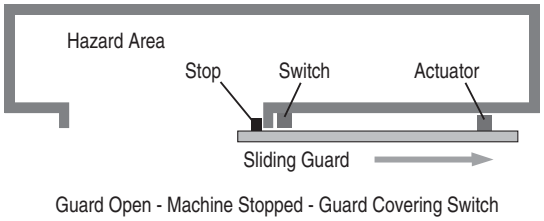


Figure 71: Sliding Guard Protects Access to Sensor

A high security against defeat can be achieved by using a coded actuator and sensor. For magnetically actuated and coded devices the actuator incorporates multiple magnets arranged to create multiple specific magnetic fields. The sensor has multiple reed switches specifically arranged to operate only with the specific magnetic fields of the actuator. Unique coding is generally not feasible using magnetic coding techniques. Unique coding, where an individual actuator is “tuned” to an individual sensor.

The reed switches used with magnetically coded switches are often small. To avoid the risk of welded contacts some switches use one normally open contact and one normally closed contact as outputs. This is based on the premise that you cannot weld an open contact. The logic device or control unit must be compatible with the N.C. + N.O. circuit arrangement and must also provide overcurrent protection. The Allen-Bradley Guardmaster Sipha interlocks use the coded magnetic technique.

RFID Non-Contact Interlock Switches

Non-contact interlock switches based on RFID (Radio Frequency Identification) technology can provide a very high level of security against defeat by “simple” tools. This technology can also be used to provide devices with unique coding for applications where security is paramount.

The use of RFID technique has many other important advantages. It is suitable for use with high integrity circuit architectures such as Category 4 or SIL 3.

It can be incorporated into devices with fully sealed IP69K enclosures manufactured from plastic or stainless steel.

When RFID technology is used for coding, and inductive technology for sensing, a large sensing range and tolerance to misalignment can be achieved, typically 15…25 mm. This means that these devices can provide very stable and reliable service combined with high levels of integrity and security over a wide range of industrial safety applications.

The Allen-Bradley Guardmaster SensaGuard interlocks use the RFID technique.

Hinge Switches

The device is mounted over the hinge-pin of a hinged guard as shown in Figure 72. The opening of the guard is transmitted via a positive mode operating mechanism to the control circuit contacts.

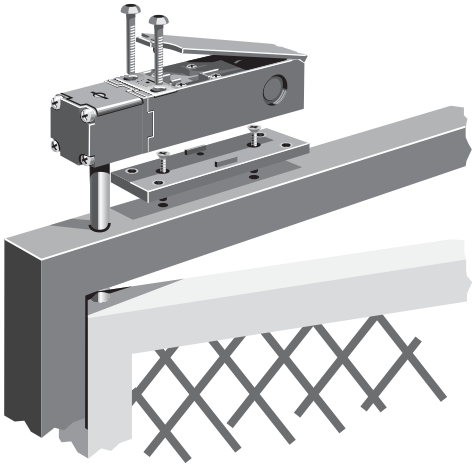


Figure 72: Hinge Switch Installation

When properly installed these types of switches are ideal for most hinged guard doors where there is access to the hinge center line. They can isolate the control circuit within 3° of guard movement and they are virtually impossible to defeat without dismantling the guard.

Care must be taken since an opening movement of only 3° can still result in a significant gap at the opening edge on very wide guard doors. It is also important to ensure that a heavy guard does not put excessive stress on the switch actuator shaft.

Position (Limit Switch) Interlocks

Cam operated actuation usually takes the form of a positive mode limit (or position) switch and a linear or rotary cam (as shown in Figure 73). It is generally used on sliding guards. When the guard is opened, the cam forces the plunger down to open the control circuit contacts. The simplicity of the system allows the switch to be both small and reliable.

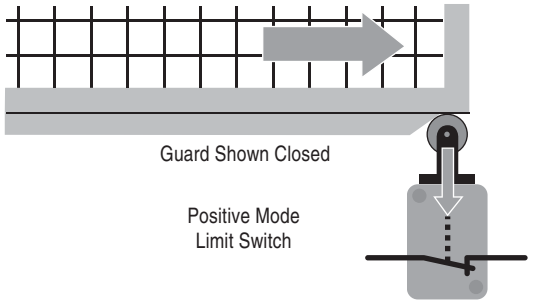


Figure 73: Positive Mode Limit Switch

Position (limit) interlocks must not be used on lift-off or hinged guards.

It is extremely important that the switch plunger can only extend when the guard is fully closed. This means that it may be necessary to install additional stops to limit the guard movement in both directions.

It is necessary to fabricate a suitably profiled cam that will operate within defined tolerances. The guard-mounted cam must never become separated from the switch as this will cause the switch contacts to close. Such a system can be prone to failures due to wear, especially when badly profiled cams or the presence of abrasive materials is a factor.

It is often advisable to use two switches as shown in Figure 74. One operates in positive mode (direct action to open contact), and one operates in negative mode (spring return).

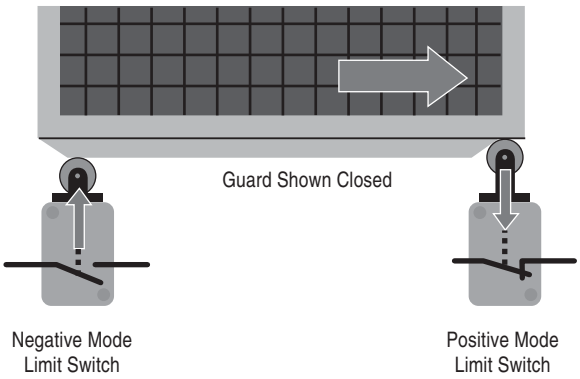


Figure 74: Diverse Redundant Position Switches

Trapped Key Interlocks

Trapped keys can perform control interlocking as well as power interlocking. With “control interlocking,” an interlock device initiates a stop command to an intermediate device, which turns off a subsequent device to disconnect the energy from the actuator. With “power interlocking,” the stop command directly interrupts the energy supply to the machine actuators.

The most practical method of power interlocking is a trapped key system (see Figure 75). The power isolation switch is operated by a key that is trapped in position while the switch is in the ON position. When the key is turned, the isolation switch contacts are locked open (isolating the power supply) and the key can be withdrawn.

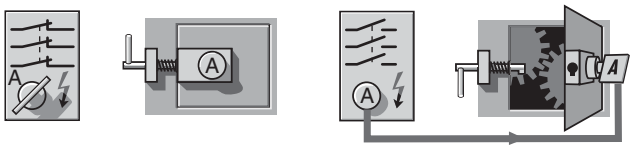


Figure 75: Power Interlocking with Trapped Key System

The guard door is locked closed and the only way to unlock it is by using the key from the isolator. When turned to release the guard locking unit, the key is trapped in position and cannot be removed until the guard is closed and locked again.

Therefore it is impossible to open the guard without first isolating the power source and it is also impossible to switch on the power without closing and locking the guard.

This type of system is extremely reliable and has the advantage of not requiring electrical wiring to the guard. The main disadvantage is that because it requires the transfer of the key every time, it is not suitable if guard access is required frequently.

Whenever whole body access is required, the use of a personnel key is recommended. As shown in Figure 76, the “B” key is the personnel key. The “B” key is taken by the operator into the hazard area. The trapped key range is available in double, triple, and quad key versions for multiple access points. The use of a personnel key ensures that the operator cannot be locked in the guarded area. The key can also be taken into the cell and inserted into another switch to enable functions like robot teach and machine jog modes.

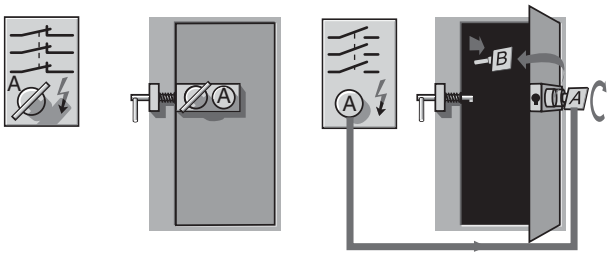


Figure 76: Full Body Access—Operator Takes "B" Key

In another example shown in Figure 77, rotate and remove Key “A” from the power isolator. Power is then OFF. To gain access through guard doors Key “A” is inserted and rotated in the Key Exchange Unit. Both “B” Keys are then released for guard locks. Key “A” is trapped preventing power from being switched on. Two “C” Keys are released from the guard door locks for use in the next sequence step or as personnel keys.

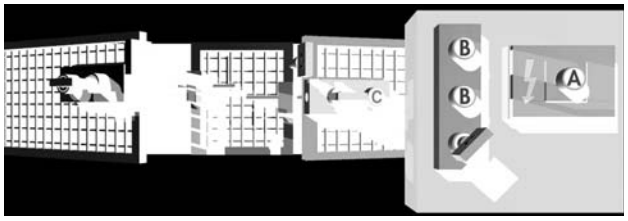


Figure 77: Multiple Doors Are Accessible

Figures 78 shows another example of trapped key interlock applications by using both single and double key locking units and keys with different codes together with a key exchange unit, complex systems can be formed. Besides ensuring that the power is isolated before access can be gained it is also possible to use the system to enforce a pre-defined sequence of operation.

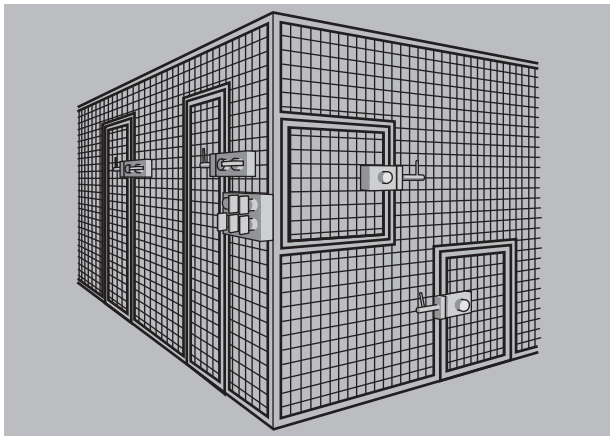


Figure 78: Defined Sequence of Events

Because the entire safety of this type of system depends on its mechanical operation it is critical that the principles and materials used are suitable for the expected demand made on them.

If an isolation switch is part of the system it should have positive mode operation and it should satisfy the requirements of the relevant parts of IEC 60947.

The integrity and security of the system revolves around the fact that under certain conditions the keys are trapped in place, therefore two basic features need to be ensured:

1. THE LOCK CAN ONLY BE OPERATED BY THE DEDICATED KEY.

This means that it should not be possible to “cheat” the lock by using screwdrivers, etc., or defeat the mechanism by mistreating it in any straightforward manner. Where there is more than one lock on the same site it also means that the specifying of key codes must in itself prevent any possibility of spurious operation.

2. IT IS NOT POSSIBLE TO OBTAIN THE KEY IN ANY WAY OTHER THAN THE INTENDED MANNER.

This means that, for example, once the key is trapped, any excessive force applied to it will result in a broken key as opposed to a broken lock.

Operator Interface Devices

Stop Function

In the U.S., Canada, Europe, and at the international level, harmonization of standards exist with regard to the descriptions of stop categories for machines or manufacturing systems.

NOTE: these categories are different to the categories from EN 954-1 (ISO 13849-1). See standards NFPA79 and IEC/EN60204-1 for further details. Stops fall into three categories:

- Category 0 is stopping by immediate removal of power to the machine actuators. This is considered an uncontrolled stop. With power removed, braking action requiring power will not be effective. This will allow motors to free spin and coast to a stop over an extended period of time. In other cases, material may be dropped by machine holding fixtures, which require power to hold the material. Mechanical stopping means, not requiring power, may also be a used with a category 0 stop. The category 0 stop takes priority over category 1 or category 2 stops.
- Category 1 is a controlled stop with power available to the machine actuators to achieve the stop. Power is then removed from the actuators when the stop is achieved. This category of stop allows powered braking to quickly stop hazardous motion, and then power can be removed from the actuators.
- Category 2 is a controlled stop with power left available to the machine actuators. A normal production stop is considered a category 2 stop.

These stop categories must be applied to each stop function, where the stop function is the action taken by the safety related parts of the control system in response to an input, category 0 or 1 should be used. Stop functions must override related start functions. The selection of the stop category for each stop function must be determined by a risk assessment.

Emergency Stop Function

The emergency stop function must operate as either a category 0 or category 1 stop, as determined by a risk assessment. It must be initiated by a single human action. When executed, it must override all other functions and machine operating modes. The objective is to remove power as quickly as possible without creating additional hazards.

Until recently, hardwired electro-mechanical components were required for e-stop circuits. Recent changes to standards such as IEC 60204-1 and NFPA 79 mean that safety PLCs and other forms of electronic logic meeting the requirements of standards like IEC61508, can be used in the e-stop circuit.

Emergency Stop Devices

Wherever there is a danger of an operator getting into trouble on a machine there must be a facility for fast access to an emergency stop device. The e-stop device must be continuously operable and readily available. Operator panels should contain at least one e-stop device. Additional e-stop devices may be used at other locations as needed. E-Stop devices come in various forms. Pushbutton switches and cable pull switches are examples of the more popular type devices. When the e-stop device is actuated, it must latch in and it must not be possible to generate the stop command without latching in. The resetting of the emergency stop device must not cause a hazardous situation. A separate and deliberate action must be used to re-start the machine.

For further information on e-stop devices, read ISO/EN13850, IEC 60947-5-5, NFPA79 and IEC60204-1, AS4024.1, Z432-94.

Emergency Stop Buttons

Emergency stop devices are considered complimentary safeguarding equipment. They are not considered primary safeguarding devices because they do not prevent access to a hazard nor do they detect access to a hazard.

The usual way of providing this is in the form of a red-colored mushroom-headed push button on a yellow background which the operator strikes in the event of an emergency (see Figure 79). They must be strategically placed in sufficient quantity around the machine to ensure that there is always one in reach at a hazard point.

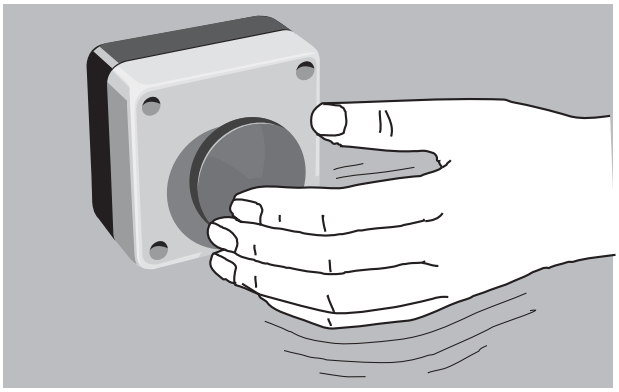


Figure 79: E-Stop Push Button—Red Colored Mushroom Head on a Yellow Background

E-Stop buttons must be readily accessible and must be available in all modes of machine operation. When a pushbutton is used as an e-stop device, it must be a mushroom (or palm operated) shaped, red colored, with a yellow background. When the button is pressed, the contacts must change state at the same time the button latches in the depressed position.

One of the latest technologies to be applied to e-stops is a self-monitoring technique. An additional contact is added to the back e-stop that monitors whether the back of the panel components are still present. This is known as a self-monitoring contact block. It consists of a spring actuated contact that closes when the contact block is snapped into place onto the panel. Figure 80 shows the self-monitoring contact connected in series with one of the direct opening safety contacts.

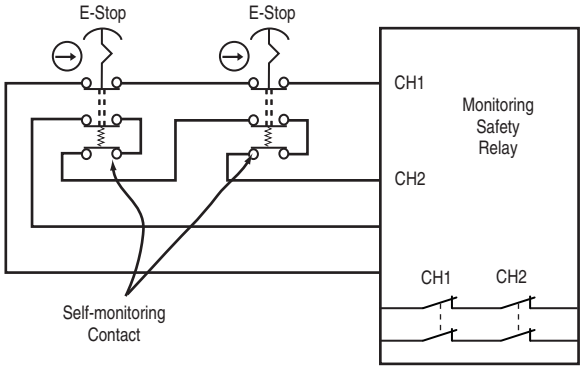


Figure 80: Self-Monitoring Contacts on E-Stop

Cable Pull Switches

For machinery such as conveyors, it is often more convenient and effective to use a cable pull device along the hazard area (as shown in Figure 81) as the emergency stop device. These devices use a steel wire rope connected to latching pull switches so that pulling on the rope in any direction at any point along its length will trip the switch and cut off the machine power.

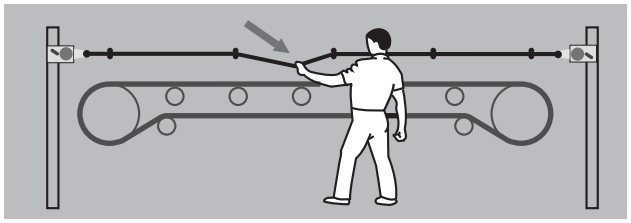


Figure 81: Cable Pull Switches

The cable pull switches must detect both a pull on the cable as well as when the cable goes slack. Slack detection ensures that the cable is not cut and is ready for use.

Cable distance affects performance of the switch. For short distances, the safety switch is mounted on one end and a tension spring mounted at the other. For longer distances, a safety switch must be mounted at both ends of the cable to ensure that a single action by the operator initiates a stop command.

The required cable pull force should not exceed 200 N (45 lb) or a distance of 400 mm (15.75 in.) at a position centered between two cable supports.

Two-Hand Controls

The use of two-hand controls (also referred to as bi-manual controls) is a common method of preventing access while a machine is in a dangerous condition. Two controls must be operated concurrently (within 0.5 s of each other) to start the machine. This ensures that both hands of the operator are occupied in a safe position (i.e., at the controls) and therefore cannot be in the hazard area. The controls must be operated continuously during the hazardous conditions. Machine operation must cease when either of the controls are released, if one control is released, the other control must also be released before the machine can be restarted.

A two-hand control system depends heavily on the integrity of its control and monitoring system to detect any faults, so it is important that this aspect is designed to the correct specification. Performance of the two-hand safety system is characterized into Types by ISO 13851 (EN 574) as shown and they are related to the Categories from ISO 13849-1. The types most commonly used for machinery safety are IIIB and IIIC. Table 4.1 shows the relationship of the types to the categories of safety performance.

	Types				
			III		
Requirements	I	II	A	B	C
Synchronous actuation			X	X	X
Use of Category 1 (from ISO 13849-1)	X		X		
Use of Category 3 (from ISO 13849-1)		X		X	
Use of Category 4 (from ISO 13849-1)					X

Table 3: Two-Hand Control Types and Categories

The physical design spacing should prevent improper operation (e.g., by hand and elbow). This can be accomplished by distance or shields as the examples shown in Figure 82.

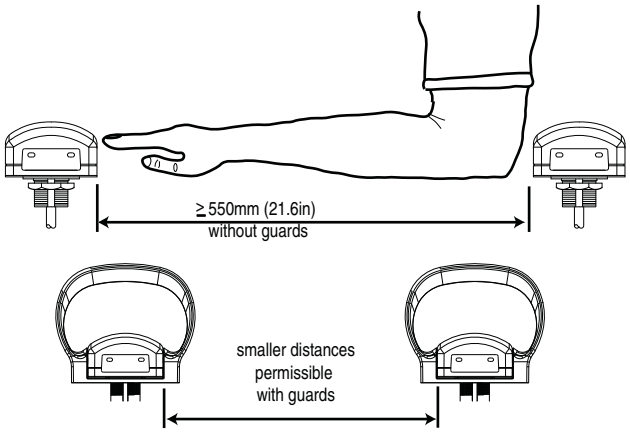


Figure 82: Separation of Two hand Controls

The machine should not go from one cycle to another without the releasing and pressing of both buttons. This prevents the possibility of both buttons being blocked, leaving the machine running continuously. Releasing of either button must cause the machine to stop.

The use of two-hand control should be considered with caution as it usually leaves some form of risk exposed. The two-hand control only protects the person using them. The protected operator must be able to observe all access to the hazard, as other personnel may not be protected.

ISO 13851 (EN574) provides additional guidance on two-hand control.

Enabling Devices

Enabling devices are controls that allow an operator to enter a hazard area with the hazard running only while the operator is holding the enabling device in the actuated position. Enabling devices use either two-position or three position types of switches. Two position types are off when the actuator is not operated, and are on when the actuator is operated. Three position switches are off when not actuated (position 1), on when held in the center position (position 2) and off when the actuator is operated past the mid position (position 3). In addition, when returning from position 3 to 1, the output circuit must not close when passing through position 2. This concept is shown in Figure 83.

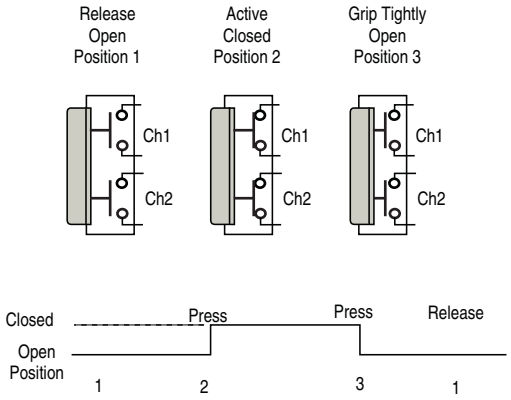


Figure 83: Three-Position Enabling Switch Operation

Enabling devices must be used in conjunction with other safety related function. A typical example is placing the motion is a controlled slow mode. Once in slow mode, an operator can enter the hazard area holding the enabling device.

When using an enabling device, a signal must indicate that the enabling device is active.

Logic Devices

Logic devices play the central role of the safety related part of the control system. Logic devices perform the checking and monitoring of the safety system and either allow the machine to start or execute commands to stop the machine.

A range of logic devices are available to create a safety architecture that meets the complexity and the functionality required for the machine. Small hardwired monitoring safety relays are most economical for smaller machines where a dedicated logic device is needed to complete the safety function. Modular and configurable monitoring safety relays are preferred where a large and diverse number of safeguarding devices and minimal zone control are required. The medium to large and more complex machine will find programmable systems with distributed I/O to be preferable.

Monitoring Safety Relays

Monitoring safety relay (MSR) modules play a key role in many safety systems. These modules are usually comprised of two or more positively guided relays with additional circuitry to ensure the performance of the safety function.

Positive guided relays are specialized “ice-cube” relays. Positively guided relays must meet the performance requirements of EN50025. Essentially, they are designed to prevent the normally closed and normally open contacts from being closed simultaneously. Newer designs replace the electromechanical outputs with safety rated solid state outputs.

Monitoring safety relays perform many checks on the safety system. Upon power-up, they perform self-checks on their internal components. When the input devices are activated, the MSR compares the results of redundant inputs. If acceptable, the MSR checks external actuators. If okay, the MSR awaits a reset signal to energize its outputs.

The selection of the appropriate safety relay is dependent on a number of factors: type of device it monitors, the type of reset, the number and type of outputs.

Inputs Types

Safeguarding devices have different types of methods of indicating something has happened:

- Contact Interlocks and E-stops:
  Mechanical contacts, single channel with one normally closed contact or dual channel, both normally closed. The MSR must be able to accept single or dual channel and provide cross fault detection for the dual channel arrangement.
- Non-Contacts Interlocks and E-stops
  Mechanical contacts, dual channel, one normally open and one normally closed contact. The MSR must be able to process diverse inputs.
- Output Solid State Switching Devices
  Light curtains, laser scanners, solid-state non-contacts have two sourcing outputs and perform their own cross fault detection. The MSR must be able to ignore the devices cross fault detection method.
- Mats:
  Mats create a short circuit between two channels. The MSR must be able to withstand the repeated short circuits.
- Edges:
  Some edges are designed like 4-wire mats. Some are two wire devices that create a change in resistance. The MSR must be able to detect a short circuit or the change resistance.
- Voltage
  Measures the Back EMF of a motor during rundown. The MSR must be able to tolerate high voltages as well as detect low voltages as the motor spins down.
- Stopped Motion
  The MSR must detect pulse streams from diverse, redundant sensors.
- Two-hand Control
  The MSR must detect normally open and normally closed diverse inputs as well as provide 0.5s timing and sequencing logic.

Input Impedance

The input impedance of the monitoring safety relays determines how many input devices can be connected to the relay and how far away the input devices can be mounted. For example, a safety relay may have a maximum allowable input impedance of 500 ohms (Ω). When the input impedance is greater than 500Ω, it will not switch on its outputs. Care must be taken by the user to ensure that the input impedance remains below the maximum specification. The length, size and type of wire used affects input impedance. Table 4 shows typical resistance of annealed copper wire at 25°C.

ISO Cross Section mm²	AWG Size	Ω per 1000 m	Ω per 1000 ft
0.5	20	33.30	10.15
0.75	18	20.95	6.385
1.5	16	13.18	4.016
2.5	14	8.28	2.525
4	12	5.21	1.588

Table 4: Wire Resistance Values

Number of Input Devices

The risk assessment process should be used to help determine how many inputs devices should be connected to a monitoring safety relay unit MSR and how often the input devices should be checked. To assure that E-Stops and gate interlocks are in an operational state, they should be checked for operation at regular intervals, as determined by the risk assessment. For example, a dual channel input MSR connected to an interlocked gate that must be opened every machine cycle (e.g., several times per day) may not have to be checked. This is because opening the guard causes the MSR to check itself, its inputs and its outputs (depending on configuration) for single faults. The more frequent the guard opening the greater the integrity of the checking process.

Another example might be E-Stops. Since E-Stops are typically used only for emergencies, they are likely to be rarely used. Therefore a program should be established to exercise the E Stops and confirm their effectiveness on a scheduled basis. Exercising the safety system in this way is called performing a Proof Test, and the time in between Proof Tests is called the Proof Test Interval. A third example might be access doors for machine adjustments, which like E-Stops might be rarely used Here again a program should be established to exercise the checking function on a scheduled basis.

The risk assessment will help determine whether the input devices need to be checked and how often they should be checked. The higher the level of risk, the greater integrity required of the checking process. And the less frequent the "automatic" checking, the more frequent should be the imposed "manual" check.

Input Crossfault Detection

In dual channel systems, channel-to-channel short circuit faults of the input devices, also known as cross faults, must be detected by the safety system. This is accomplished by the sensing device or the monitoring safety relay.

Microprocessor based monitoring safety relays, like light curtains, laser scanners and the advanced non-contact sensors detect these shorts in a variety of ways. One common way of detecting cross faults is by using diverse pulse testing shown in Figure 84. The output signals are pulsed very quickly. The channel 1 pulse is offset from the channel 2 pulse. If a short occurs, the pulses occur concurrently and are detected by the device.

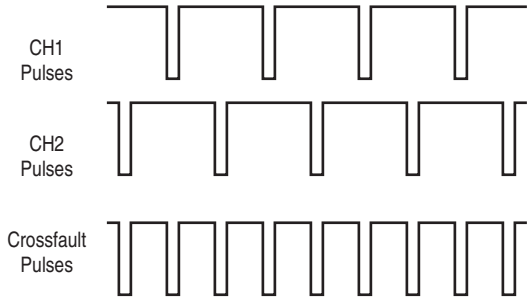


Figure 84: Pulse Testing to Detect Crossfaults

Electro-mechanical based monitoring safety relays employ a different diversity technique: one pull-up input and one pull-down input. This is shown in Figure 85. A short from Channel 1 to Channel 2 will make the overcurrent protection device active and the safety system will shut down.

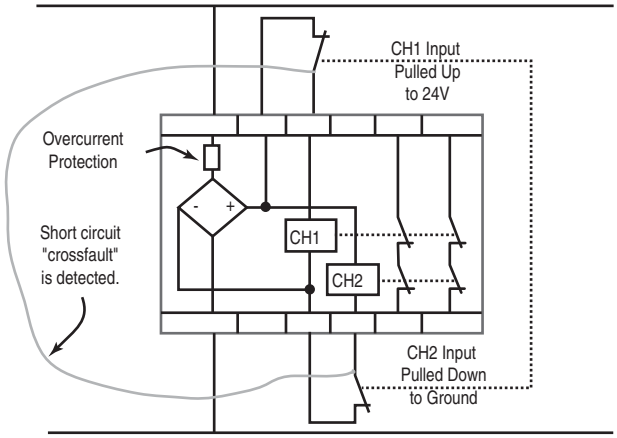


Figure 85: Diverse Inputs Detect Crossfaults

Outputs

MSRs come with various numbers of outputs. The types of outputs help determine which MSR must be used in specific applications.

Most MSRs have at least 2 immediately operating safety outputs. MSR safety outputs are characterized as normally-open. These are safety rated due to the redundancy and internal checking.

A second type of output is delayed outputs. Delayed outputs are typically used in Category 1 stops, where the machine requires time to execute the stopping function before allowing access to the hazard area. Figure 86 shows the symbols used for immediate and delayed contacts.

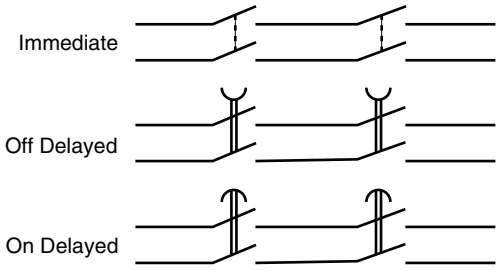


Figure 86: Symbols for Contact Types

MSRs also have auxiliary outputs. Generally these are considered normally closed. Figure 87 shows three arrangements of normally closed contacts. The circuit on the left only allows the normally closed contacts to be used as auxiliary circuits as a single fault in CH1 or CH2 will close the circuit. The middle arrangement can be auxiliary usage as shown or safety usage if connected in series. The circuit on the right shows the normally closed contacts in a redundant arrangement, so they can be used in safety related circuits.

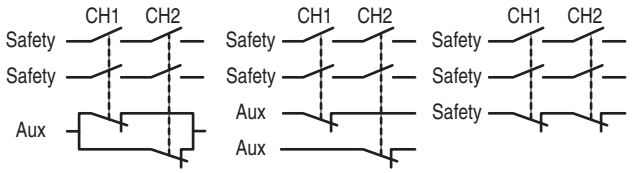


Figure 87: NC Contact Usage

Output Ratings

Output ratings describe the ability of the safeguarding device to switch loads. Typically, the ratings for industrial devices are described as resistive or electromagnetic. A resistive load may be a heater type element. Electromagnetic loads are typically relays, contactors, or solenoids; where there is a large inductive characteristic of the load. Annex A of standard IEC 60947-5-1, shown in Table 5 describes the ratings for loads.

Designation Letter: The designation is a letter followed by a number, for example A300.

The letter relates to the conventional enclosed thermal current and whether that current is direct or alternating. For example A represents 10 amps alternating current. The number stands for the rated insulation voltage. For example, 300 represents 300V.

Designation	Utilization	Enclosed Thermal Current	Rated Operational Current Ie at the Rated Operational Voltage Ue						VA	
			120V	240V	380V	480V	500V	600V	Make	Break
A150	AC-15	10	6	—	—	—	—	—	7200	720
A300	AC-15	10	6	3	—	—	—	—	7200	720
A600	AC-15	10	6	3	1.9	1.5	1.4	1.2	7200	720
B150	AC-15	5	3	—	—	—	—	—	3600	360
B300	AC-15	5	3	1.5	—	—	—	—	3600	360
B600	AC-15	5	3	1.5	0.95	0.92	0.75	0.6	3600	360
C150	AC-15	2.5	1.5	—	—	—	—	—	1800	180
C300	AC-15	2.5	1.5	0.75	—				1800	180
C600	AC-15	2.5	1.5	0.75	0.47	0.375	0.35	0.3	1800	180
D150	AC-14	1.0	0.6	—	—	—	—	—	432	72
D300	AC-14	1.0	0.6	0.3	—	—	—	—	432	72
E150	AC-14	0.5	0.3	—	—	—	—	—	216	36
Direct Current			125V	250V		400V	500V	600V		
N150	DC-13	10	2.2	—		—	—	—	275	275
N300	DC-13	10	2.2	1.1		—	—	—	275	275
N600	DC-13	10	2.2	1.1		0.63	0.55	0.4	275	275
P150	DC-13	5	1.1	—		—	—	—	138	138
P300	DC-13	5	1.1	0.55		—	—	—	138	138
P600	DC-13	5	1.1	0.55		0.31	0.27	0.2	138	138
Q150	DC-13	2.5	0.55	—		—	—	—	69	69
Q300	DC-13	2.5	0.55	0.27		—	—	—	69	69
Q600	DC-13	2.5	0.55	0.27		0.15	0.13	0.1	69	69
R150	DC-13	1.0	0.22	—		—	—	—	28	28
R300	DC-13	1.0	0.22	0.1		—	—	—	28	28

Table 5: Contact Ratings for Inductive Load Switching

Utilization: The Utilization describes the types of loads the device is designed to switch. The utilizations relevant to IEC 60947-5 are shown in Table 6.

Utilization	Description of Load
AC-12	Control of resistive loads and solid-state loads with isolation by opto-couplers
AC-13	Control of solid-state loads with transformer isolation
AC-14	Control of small electromagnetic loads (less than 72 VA)
AC-15	Electromagnetic loads greater than 72 VA
DC-12	Control of resistive loads and solid-state loads with isolation by opto-couplers
DC-13	Control of electromagnets
DC-14	Control of electromagnetic loads having economy resistors in circuit

Table 6: Utilization Categories

Thermal Current, Ith: The conventional enclosed thermal current is the value of current used for the temperature-rise tests of the equipment when mounted in a specified enclosure.

Rated Operational Voltage Ue and Current Ie; The rated operational current and voltage specify the making and breaking capacities of the switching elements under normal operating conditions. The Allen-Bradley Guardmaster products are specifically rated at 125V AC, 250V AC and 24V DC. Consult the factory for usage at voltages other than these specified ratings.

VA: The VA (Voltage x Amperage) ratings indicate the ratings of the switching elements when making the circuit as well as breaking the circuit.

Example 1: An A150, AC-15 rating indicates that the contacts can make a 7200V A circuit. At 120V AC, the contacts can make a 60 amp inrush circuit. Since the AC-15 is an electromagnetic load, the 60 amp is only for a short duration; the inrush current of the electromagnetic load. The breaking of the circuit is only 720V A because the steady state current of the electromagnetic load is 6 A, which is the rated operational current.

Example 2: An N150, DC-13 rating indicates that the contacts can make a 275V A circuit. At 125V AC, the contacts can make a 2.2 amp circuit. DC electromagnetic loads do not have an inrush current like AC electromagnetic loads. The breaking of the circuit is also 275V A because the steady state current of the electromagnetic load is 2.2, which is the rated operational current.

Machine Restart

If, for example, an interlocked guard is opened on an operating machine, the safety interlock switch will stop that machine. In most circumstances it is imperative that the machine does not restart immediately when the guard is closed. A common way of achieving this is to rely on a latching contactor start arrangement as shown in Figure 88. An interlocked guard door is used as an example here but the requirements apply to other protection devices and emergency stop systems.

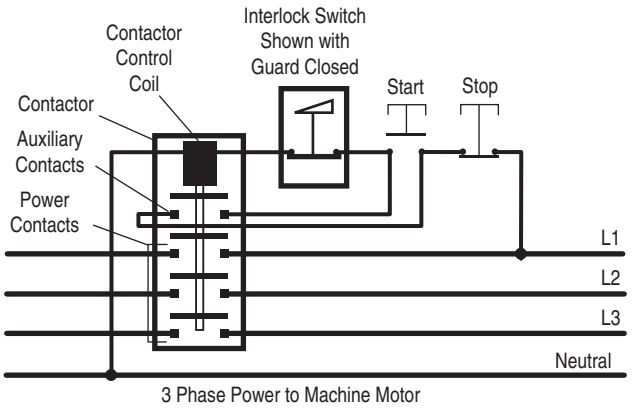


Figure 88: Simple Machine Start Stop Interlock Circuit

Pressing and releasing the start button momentarily energizes the contactor control coil which closes the power contacts. As long as power is flowing through the power contacts the control coil is kept energized (electrically latched) via the contactor's auxiliary contacts which are mechanically linked to the power contacts. Any interruption to the main power or control supply results in the de-energizing of the coil and opening of the main power and auxiliary contacts. The guard interlock is wired into the contactor control circuit. This means that restart can only be achieved by closing the guard and then switching “ON” at the normal start button which resets the contactor and starts the machine.

The requirement for normal interlocking situations is made clear in ISO 12100-1 Paragraph 3.22.4 (extract).

When the guard is closed, the hazardous machine functions covered by the guard can operate, but the closure of the guard does not by itself initiate their operation.

Many machines already have either single or double contactors which operate as described above (or have a system which achieves the same result). When fitting an interlock to existing machinery it is necessary to determine whether the power control arrangement meets this requirement and take additional measures if necessary.

Reset Functions

Allen-Bradley Guardmaster monitoring safety relays are designed with either monitored manual reset or automatic/manual reset.

Monitored Manual Reset

A monitored manual reset requires a change of state of the reset circuit after the gate is closed or the E-Stop is reset. Figure 89 shows a typical configuration of a reset switch connected in the output monitoring circuit of a safety relay with a monitored manual reset function. The mechanically linked normally closed auxiliary contacts of the power switching contactors are connected in series with a momentary push button. After the guard has been opened and closed again, the safety relay will not allow the machine to be restarted until there is a change of state at the reset button. This is in compliance with the intent of the requirements for additional manual reset as given in EN ISO 13849-1. i.e., the reset function ensures that both contactors are OFF and that both interlock circuits (and therefore the guards) are closed and also (because a change of state is required) that the reset actuator has not been bypassed or blocked in any way. If these checks are successful the machine can then be restarted from the normal controls. EN ISO 13849-1 cites the change of state from energized to de-energized but the same protective principle can also be achieved by the opposite effect.

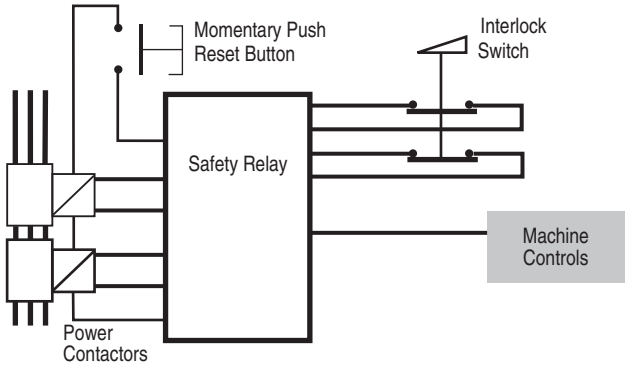


Figure 89: Monitored Manual Reset

The reset switch should be located in a place that provides a good view of the hazard so that the operator can check that the area is clear before operation.

Auto/Manual Reset

Some safety relays have automatic/manual reset. The manual reset mode is not monitored and reset occurs when the button is pressed. A short circuited or jammed in reset switch will not be detected. With this approach it may not be possible to achieve the requirements for additional manual reset as given in EN ISO 13849-1 unless additional means are used.

Alternatively the reset line can be jumpered allowing an automatic reset. The user must then provide another mechanism for preventing machine start-up when the gate closes.

The reset switch should be located in a place that provides a good view of the hazard so that the operator can check that the area is clear before operation.

Auto/Manual Reset

Some safety relays have automatic/manual reset. The manual reset mode is not monitored and reset occurs when the button is pressed. A short circuited or jammed in reset switch will not be detected. With this approach it may not be possible to achieve the requirements for additional manual reset as given in EN ISO 13849-1 unless additional means are used.

Alternatively the reset line can be jumpered allowing an automatic reset. The user must then provide another mechanism for preventing machine start-up when the gate closes.

An auto-reset device does not require a manual switching action but after de-actuation it will always conduct a system integrity check before resetting the system. An auto-reset system should not be confused with a device without reset facilities. In the latter the safety system will be enabled immediately after de-actuation but there will be no system integrity check.

Control Guards

A control guard stops a machine when the guard is opened and directly starts it again when the guard is closed. The use of control guards is only allowed under certain stringent conditions because any unexpected start-up or failure to stop would be extremely dangerous. The interlocking system must have the highest possible reliability (it is often advisable to use guard locking). The use of control guards can ONLY be considered on machinery where there is NO POSSIBILITY of an operator or part of his body staying in or reaching into the danger zone while the guard is closed. The control guard must be the only access to the hazard area.

Safety Programmable Logic Controls

The need for flexible and scaleable safety applications drove the development of safety PLCs/controllers. Programmable safety controllers provide users the same level of control flexibility in a safety application that they are accustomed to with standard programmable controllers. However there are extensive differences between standard and safety PLCs. Safety PLCs, shown in Figure 90 come in various platforms to accommodate the scalability, functional and integration requirements of the more complex safety systems.

Figure 90: Safety PLC Platforms

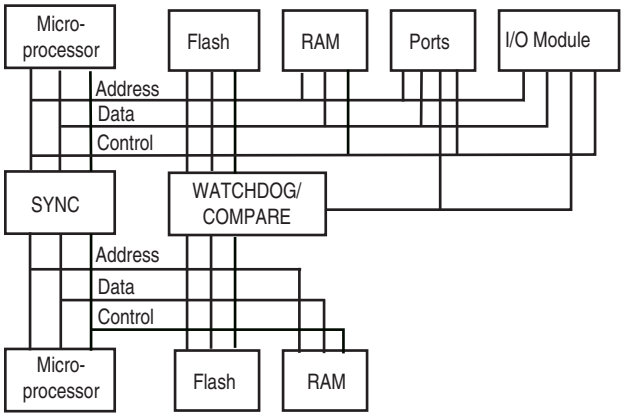


Figure 91: 1oo2D Architecture

Multiple microprocessors are used to process the I/O, memory, and safe communications. Watchdog circuits perform diagnostic analysis. This type of construction is known as 1oo2D, because either one of the two microprocessors can perform the safety function, and extensive diagnostics are performed to ensure that both microprocessors are operating in sync.

Also, each input circuit is internally tested many times each second to make sure that it is operating correctly. Figure 92 shows a block diagram of an input. You may only hit the E-Stop once a month; but when you do, the circuit has been continuously tested so that the E-Stop will be sensed correctly internal to the safety PLC.

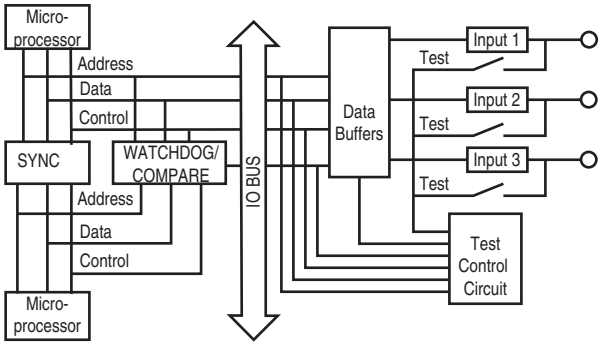


Figure 92: Block Diagram of a Safety Input Module

Safety PLC outputs are electromechanical or safety rated solid state. Figure 93 shows multiple switches in every output circuit of a safety PLC. Like the input circuits, the output circuits are tested multiple times every second to make sure that they can turn the output off. If one of the three fails, the output is turned off by the other two, and the fault is reported by the internal monitoring circuit.

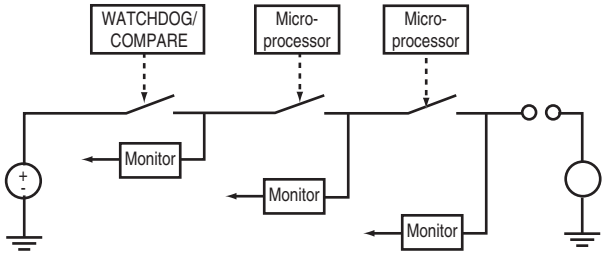


Figure 93: Safety Output Module Block Diagram

When using safety devices with mechanical contacts (E-stops, gate switches, etc), the user can apply pulse test signals to detect cross faults. To not use up expensive safety outputs, many safety PLCs provides specific pulsing outputs that can be connected to mechanical contact devices. A wiring example is shown in Figure 94. In this example, outputs O1, O2, O3, and O4 are all pulsing at different rates. The safety PLC expects to see these different pulse rates reflected in the inputs. If identical pulse rates are detected, a cross fault has occurred and appropriate action is taken in the safety PLC.

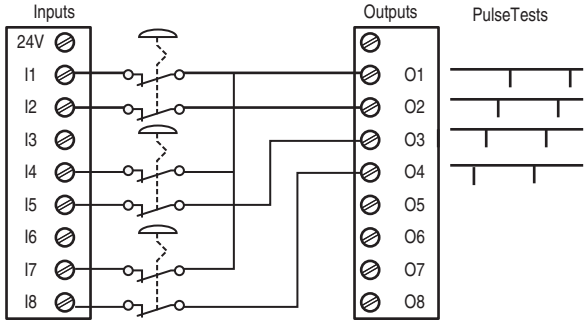


Figure 94: Pulse Testing of 2 N.C. Mechanical Inputs

Software

Safety PLCs program very much like standard PLCs do. All of the additional diagnostics and error checking mentioned earlier is done by the operating system, so the programmer is not even aware that it is happening. Most safety PLCs will have special instructions used to write the program for the safety system, and these instructions tend to mimic the function of their safety relay counterparts. For example, the Emergency Stop instruction in Figure 95 operates very much like an MSR127. Though the logic behind each of these instructions is complex, the safety programs look relatively simple because the programmer simply connects these blocks together. These instructions, along with other logical, math, data manipulation, etc. instructions are certified by a third party to ensure their operation is consistent with the applicable standards.

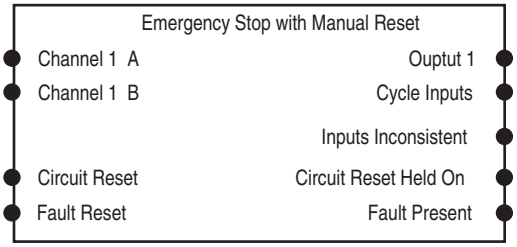


Figure 95: E-Stop Function Block

Visit our website: www.ab.com/catalogs
Publication S117-CA001A-EN-P

Function blocks are the predominant methods for programming safety functions. In addition to Function Blocks and Ladder Logic, safety PLCs also provide certified safety application instructions. Certified safety instructions provide application specific behavior. This example shows an emergency stop instruction. To accomplish the same function in ladder logic would require approximately 16 rungs of ladder logic. Since the logic behavior is embedded in the E-Stop instruction, the embedded logic does not have to be tested.

Certified function blocks are available to interface with almost all safety devices. One exception to this list is the safety edge that uses resistive technology. Here is a list of certified application instructions available in the GuardPLC.

1. Diverse (1 N.O. + 1 N.C.) Input with Auto Reset
2. Diverse (1 N.O. + 1 N.C.) Input with Manual Reset
3. Emergency Stop with Auto Reset
4. Emergency Stop with Manual Reset
5. Redundant (2 N.C.) Input with Auto Reset
6. Redundant (2 N.C.) Input with Manual Reset
7. Redundant Output with Positive Feedback
8. Redundant Output with Negative Feedback
9. Enable Pendant with Auto Reset
10. Enable Pendant with Manual Reset
11. Two Hand Run Station with Active Pin
12. Two Hand Run Station without Active Pin
13. Light Curtain with Auto Reset
14. Light Curtain with Manual Reset
15. Five Position Mode Selector
16. Single Pulse Test Output
17. Redundant Pulse Test Output

Safety PLCs generate a “signature” that provides the ability to track whether changes were made. This signature is usually a combination of the program, input/output configuration, and a time stamp. When the program is finalized and validated, the user should record this signature as part of the validation results for future reference. If the program needs modification, revalidation is required and a new signature must be recorded. The program can also be locked with a password to prevent unauthorized changes.

Wiring is simplified with programmable logic systems as compared to monitoring safety relays. Unlike wiring to specific terminals on monitoring safety relays, input devices are connected to any input terminals and output devices are connected to any output terminals. The terminals are then assigned through software.

Integrated Safety Controllers

Safety control solutions now provide complete integration within a single control architecture where safety and standard control functions reside and work together. The ability to perform motion, drive, process, batch, high speed sequential, and SIL 3 safety in one controller provides significant benefits. The integration of safety and standard control provides the opportunity to utilize common tools and technologies which reduce costs associated with design, installation, commissioning and maintenance. The ability to utilize common control hardware, distributed safety I/O or devices on safety networks and common HMI devices reduce purchase and maintenance costs, and also reduce development time. All of these features improve productivity, the speed associated with troubleshooting and the lowering of training costs due to commonality.

Figure 96 shows an example of the integration of control and safety. The standard non-safety related control functions reside in the Main Task. The safety related functions reside in the Safety Task.

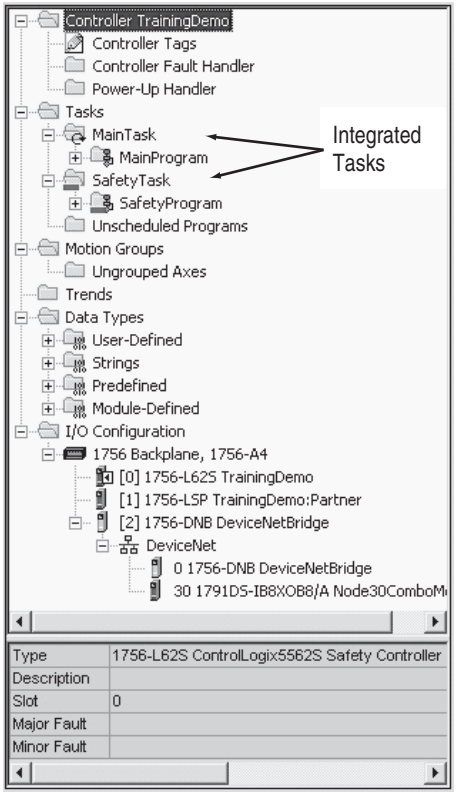


Figure 96: Integrated Safety and Nonsafety Tasks

All standard and safety related functions are isolated from each other. Figure 97 shows a block diagram of allowed interaction between the standard and safety portions of the application. For example, safety tags can be directly read by the standard logic. Safety tags can be exchanged between GuardLogix controllers over EtherNet, ControlNet or DeviceNet. Safety tag data can be directly read by external devices, Human Machine Interfaces (HMI), personal computers (PC) or other controllers.

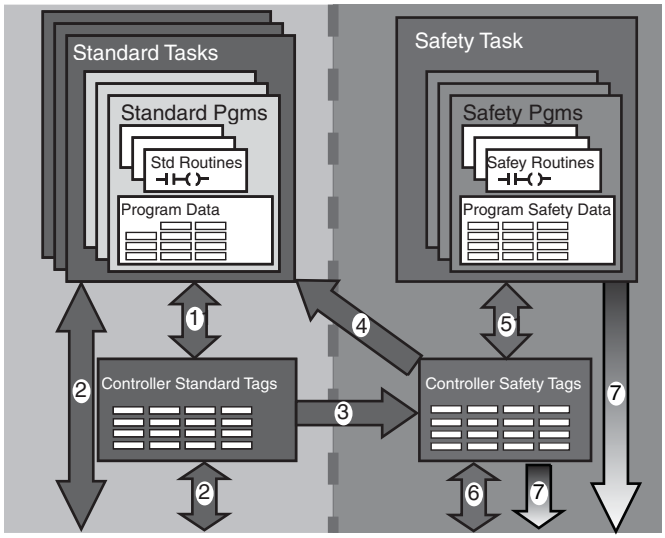


Figure 97: Standard and Safety Task Interaction

1. Standard tags and logic behave the same as ControlLogix.
2. Standard tag data, program or controller scoped and external devices, HMI, PC's, other controllers, etc.
3. As an integrated controller, GuardLogix provides the ability to move (map) standard tag data into safety tags for use within the safety task. This is to provide users the ability read status information from the standard side of GuardLogix. This data must not be used to directly control a safety output.
4. Safety tags can be directly read by standard logic.
5. Safety tags can be read or written by safety logic.
6. Safety tags can be exchanged between GuardLogix controllers over EtherNet.
7. Safety tag data, program or controller scoped can be read by external devices, HMIs, PCs, other controllers, etc. Note, once this data is read, it is considered standard data, not safety data.

Safety Networks

Plant floor communication networks have traditionally provided manufacturers the capability to improve flexibility, increase diagnostics, increase distance, reduce installation and wiring cost, ease maintainability and generally improve the productivity of their manufacturing operations. These same motivations are also driving the implementation of industrial safety networks. These safety networks allow manufacturers to distribute safety I/O and safety devices around their machinery using a single network cable, reducing installation costs while improving diagnostics and enabling safety systems of increased complexity. They also enable safe communications between safety PLCs/controllers, allowing users to distribute their safety control among several intelligent systems.

Safety networks do not prevent communication errors from occurring. Safety networks are more capable of detecting transmission errors and then allow safety devices to take the appropriate actions. Communication errors that are detected include: message insertion, message loss, message corruption, message delay, message repeat, and incorrect message sequence.

For most applications, when an error is detected the device will go to a known de-energized state, typically called a "safety state." The safety input or output device is responsible for detecting these communication errors and then going to the safe state if appropriate.

Early safety networks were tied to a particular media type or media access scheme, so manufacturers were required to use specific cables, network interface cards, routers, bridges, etc. that also became part of the safety function. These networks were limited in that they only supported communication between safety devices. This meant that manufacturers were required to use two or more networks for their machine control strategy (one network for standard control and another for safety related control) increasing installation, training and spare parts costs.

Modern safety networks allow a single network cable to communicate with safety and standard control devices. CIP (Common Industrial Protocol) Safety is an open standard protocol published by ODVA (Open DeviceNet Vendors Association) that allows for safety communications between safety devices on DeviceNet, ControlNet and EtherNet/IP networks. Because CIP Safety is an extension to the standard CIP protocol, safety devices and standard devices can all reside on the same network. Users can also bridge between networks containing safety devices, allowing them to subdivide safety devices to fine-tune safety response times, or to simply make distribution of safety devices easier. Because the safety protocol is solely the responsibility of the end devices (safety PLC/controller, safety I/O module, safety component), standard cables, network interface cards, bridges, and routers are used, eliminating any special networking hardware and removing these devices from the safety function.

Figure 98 shows a simplified example of a distributed I/O system. The operator opens the gate. The interlock switch, connected to the local Safety I/O block, sends its safety data over the DeviceNet network to the Safety PLC. The Safety PLC sends a signal back to the Safety I/O block to shut down the equipment inside of the gate and sends a standard output to a stack light to annunciate the gate is open. The HMI and the standard PLC monitors the safety data for display and additional control measures, like performing a cycle stop of adjacent equipment.

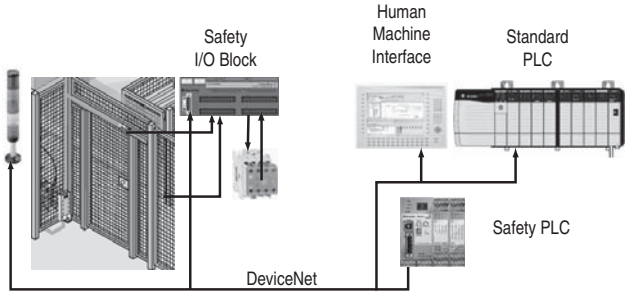


Figure 98: Example of a Simple Distributed Safety Network

For larger manufacturing systems, where safety information and control must be shared, Ethernet/IP can also be used. Figure 99 shows an example of communications between two safety controllers while DeviceNet is used for local distribution of I/O within a smaller subsystem.

Output Devices

Safety Control Relays and Safety Contactors

Control Relays and Contactors are used to remove power from the actuator. Special features are added to control relays and contactors to provide the safety rating.

Mechanically linked normally closed contacts are used to feed back the status of the control relays and contactors to the logic device. The use of mechanically linked contacts helps ensure the safety function. To meet the requirements of mechanically linked contacts, the normally closed and the normally open contacts cannot be in the closed state at the same time. IEC 60947-5-1 defines the requirements for mechanically linked contacts. If the normally open contacts were to weld, the normally closed contacts remain open by at least 0.5 mm. Conversely, if the normally closed contacts were to weld, then the normally open contacts remain open. If the product meets this requirement, the symbol shown in Figure 100 is applied to the product.

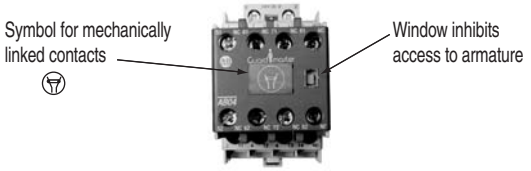


Figure 100: Mechanically Linked Contact Symbol

Safety systems must only be started at specific locations. Standard rated control relays and contactors allow the armature to be depressed to close the normally open contacts. On safety rated devices, the armature is protected from manual override to mitigate unexpected startup.

On safety control relays, the normally closed contact is driven by the main spanner. Safety contactors use an adder deck to locate the mechanically linked contacts. If the contact block were to fall off the base, the mechanically linked contacts remain closed. The mechanically linked contacts are permanently affixed to the safety control relay or safety contactor.

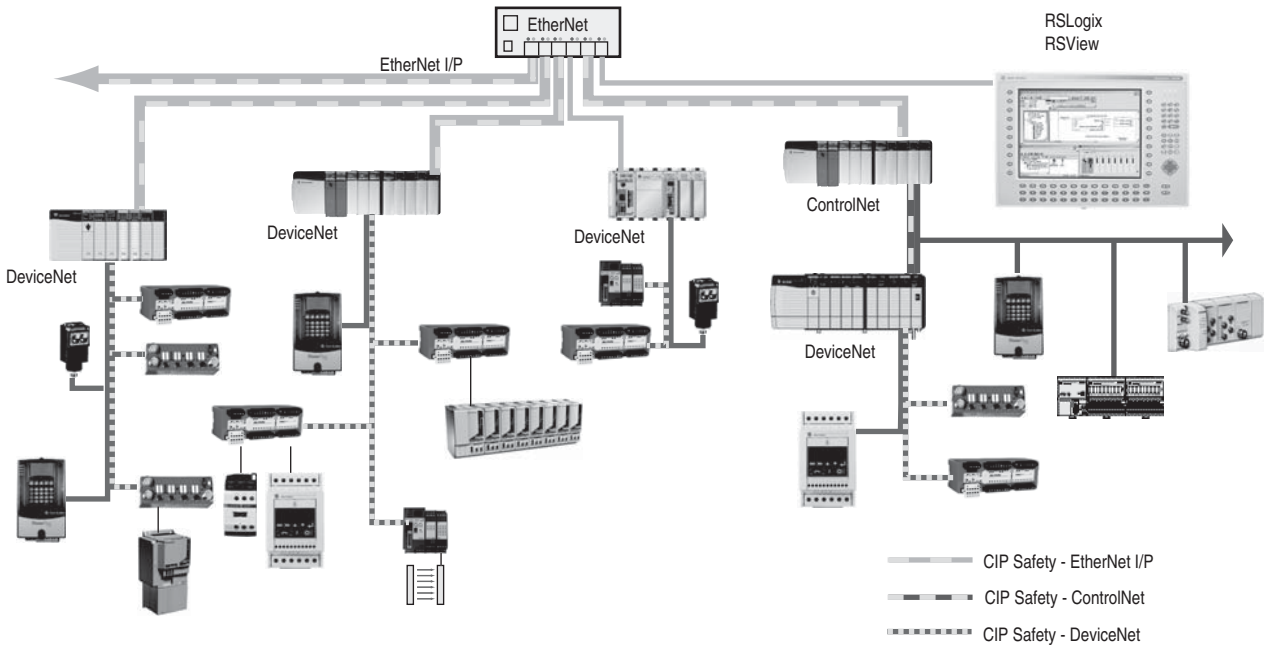


Figure 99: Example of a Complex Distributed Safety Network

On the larger contactors, an adder deck is insufficient to accurately reflect the status of the wider spanner. Mirrored contacts, shown in Figure 101 are located on either side of the contactor are used.

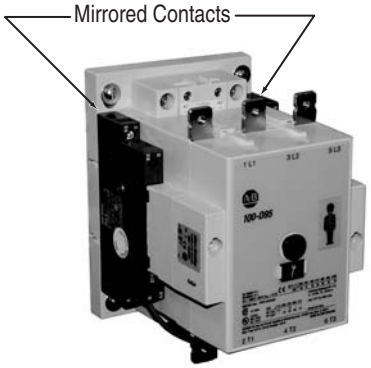


Figure 101: Mirrored Normally Closed Contacts

Dropout time of control relays or contactors play a role in the safety distance calculation. Often, a surge suppressor is placed across the coil to improve the life of the contacts driving the coil. For AC powered coils, the drop out time is not affected. For DC powered coils, the drop out time is increased. The increase is dependent on the type of suppression selected.

Control relays and contactors are designed to switch large loads, anywhere from 0.5 A to over 100 A. The safety system operates on low currents. The feedback signal generated by the safety system logic device can be on the order of a few milliamps to tens of milliamps, usually at 24V DC. The safety control relays and safety contactors use gold plated bifurcated contacts to reliably switch this small current.

Overload Protection

Overload protection for motors is required by electrical standards. Diagnostics provided by the overload protection device enhances not only equipment safety but operator safety as well. Technologies available today can detect fault conditions like an overload, phase loss, ground fault, stall, jam, under-load, current imbalance and over-temperature. Detecting and communicating abnormal conditions prior to tripping help to improve production up time and help prevent operators and maintenance people from unforeseen hazardous conditions

Figure 102 shows examples of overload protection devices. When dual contactors are used to ensure the switching off of a motor in Category 3, 4 or Control reliable solution, only one overload protection device is needed for each motor.

Figure 102: Contactor Overload Protection

Drives and Servos

Safety rated drives and servos can be used to prevent rotational energy from being delivered to achieve a safety stop as well as an emergency stop.

AC drives achieve the safety rating with redundant channels to remove power to the gate control circuitry. One channel is the Enable signal, a hardware signal that removes the input signal to the gate control circuitry. The second channel is positive guided relay that remove the power supply from the Gate control circuitry. The positive guided relay also provides a status signal back to the logic system. A block diagram of the implementation of safe off feature in the PowerFlex drive is shown in Figure 103.

This redundant approach allows the safety rated drive to be applied in emergency stop circuits without the need for a contactor.

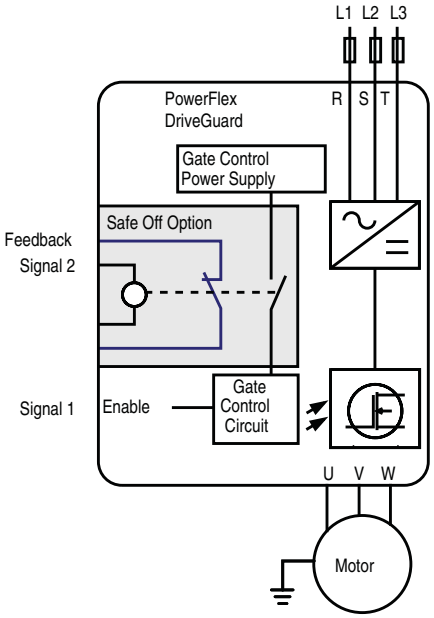


Figure 103: Drive Safety Signals

The Servo achieves a result in a manner similar to the AC drives. Figure 104 shows that redundant safety signals are used to achieve the safety function. One signal interrupts the drive to the Gate Control Circuitry. A second signal interrupts power to the power supply of the Gate control circuitry. Two positive guided relays are used to remove the signals and provide feedback to the safety logic device as well.

Connection Systems

Connection systems add value by reducing the installation and maintenance costs of safety systems. Designs must take into account consideration of single channel, dual channel, dual channel with indication and multiple types of devices.

When a series connection of dual channel interlocks is needed, a distribution block can simplify installation. Figure 105 shows a simple example of a series of interlocks connected to one port. With an IP67 rating, these types of boxes can be mounted on the machine at remote locations.

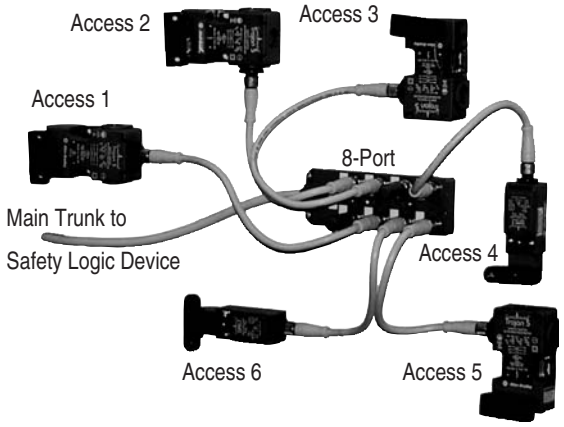


Figure 105: Safety Distribution Block

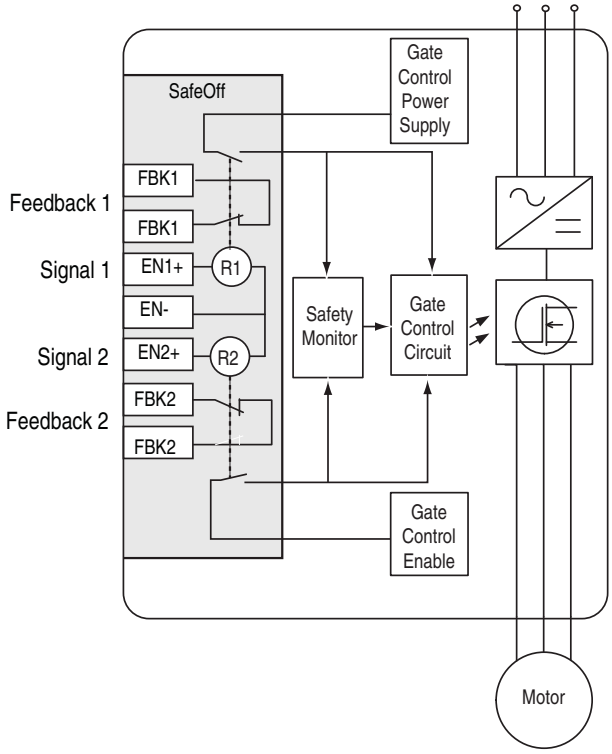


Figure 104: Kinetix Drive Safety Signals

When a diverse set of devices is required, an ArmorBlock Guard I/O box can be used. Figure 106 shows an eight port and four port block with an IP67 rating, which can be mounted directly on the machine without an enclosure. The inputs can be configured by software to accommodate various types of devices.

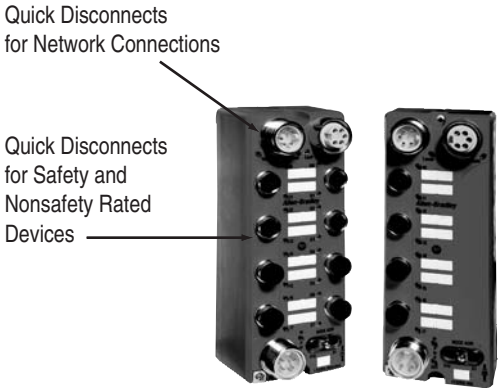


Figure 106: ArmorBlock Guard I/O

Safety Distance Calculation

Hazards must come to a safe state prior to an operator reaching the hazard. For the safety distance calculation, there are two groups of standards that have proliferated. In this chapter, these standards are grouped as follows:

ISO EN: (ISO 13855 and EN 999)

US CAN (ANSI B11.19, ANSI RIA R15.06 and CAN/CSA Z434-03)

Formula

The minimum safety distance is dependent on the time required to process the Stop command and how far the operator can penetrate the detection zone before detection. The formula used throughout the world has the same form and requirements. The differences are the symbols used to represent the variables and the units of measure.

The formulas are:

ISO EN:S =K x T+ C

US CAN: Ds =K x(Ts + Tc + Tr + Tbm) + Dpf

Where:

Ds and S are the minimum safe distance from the danger zone to the closest detection point.

Directions of Approach

When considering the safety distance calculation where a light curtains or area scanner is used, the approach to the detection device must be taken into consideration. Three types of approaches are considered:

Normal: an approach perpendicular to the detection plane

Horizontal: an approach parallel to the detection plan

Angled: an angled approach to the detection zone.

Speed Constant

K is a speed constant. The value of the speed constant is dependent on movements of the operator (i.e. hand speeds, walking speeds, and stride lengths). This parameter is based on research data showing that it is reasonable to assume a 1600 mm/sec (63 in./s) hand speed of an operator while the body is stationary. The circumstances of the actual application must be taken into account. As a general guideline, the approach speed will vary from 1600 mm/s (63 in./s) to 2500 mm/sec (100 in./s). The appropriate speed constant must be determined by the risk assessment.

Stopping Time

T is the overall stopping time of the system. The total time, in seconds, starts from the initiation of the stop signal to the cessation of the hazard. This time can be broken down to its incremental parts (Ts, Tc, Tr and Tbm) for easier analysis. Ts is the worst stopping time of the machine/equipment. Tc is the worst stopping time of the control system. Tr is the response time of the safeguarding device, including its interface. Tbm is additional stopping time allowed by the brake monitor before it detects stop-time deterioration beyond the end users' predetermined limits. Tbm is used with part revolution mechanical presses. Ts + Tc + Tr are usually measured by a stop-time measuring device if the values are unknown.

Depth Penetration Factor

The Depth Penetration Factors is represented by the symbols C and Dpf. It is the maximum travel towards the hazard before detection by the safeguarding device. Depth penetration factors will change depending on the type of device and application. Appropriate standard must be checked to determine the best depth penetration factor. For a normal approach to a light curtain or area scanner, whose object sensitivity is less than 64 mm (2.5 in.), the ANSI and Canadian standards use:

Dpf = 3.4 x (Object Sensitivity – 6.875 mm), but not less than zero.

For a normal approach to a light curtain or area scanner, whose object sensitivity is less than 40 mm (1.57 in.), the ISO and EN standards use:

C = 8 x (Object Sensitivity – 14 mm), but not less than 0

Figure 107 shows a comparison of these two factors. These two formulas have a cross over point at 19.3 mm. For object sensitivity less than 19 mm, the US CAN approach is more restrictive, as the light curtain or area scanner must be set back further from the hazard. For object sensitivities greater than 19.3 mm, the ISO EN standard is more restrictive. Machine builders, who want to build one machine for use throughout the world, must take the worst case conditions from both equations.

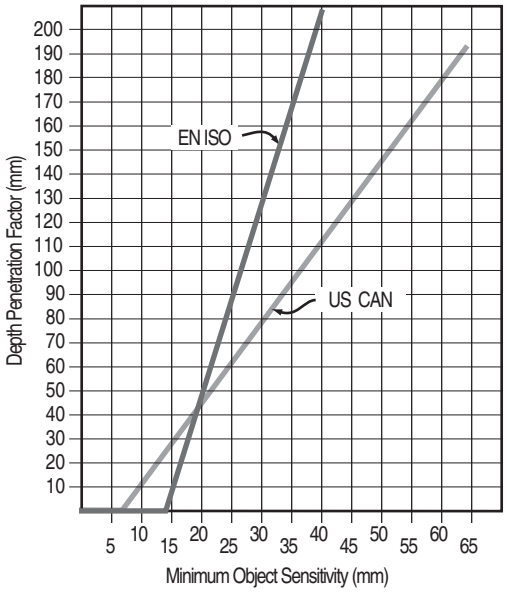


Figure 107: Depth Penetration vs. Object Sensitivity

Reach Through Applications

When larger object sensitivities are used, the US CAN and ISO EN standards differ slightly on the depth penetration factor and the object sensitivity. Figure 108 summarizes the differences. The ISO EN value is 850mm where the US CAN value is 900 mm. The standards also differ in the object sensitivity. Where the ISO EN standard allows for 40 to 70 mm, the US CAN standard allows up to 600 mm.

Safety Distance Calculation

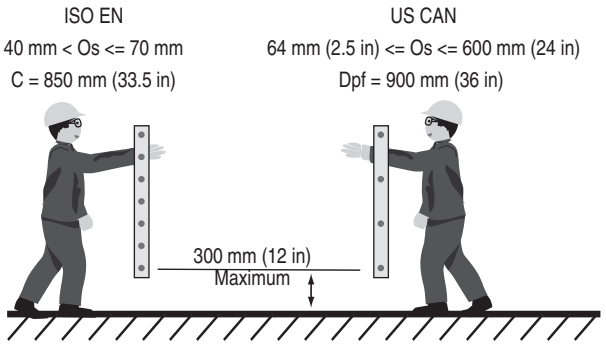


Figure 108: Depth Penetration Factors for Reach-Through Applications

Reach-Over Applications

Both standards agree that the minimum height of the lowest beam should be 300 mm, but differ with respect to the minimum height of the highest beam. The ISO EN states 900 mm, whereas the US CAN states 1200 mm. Figure 109 summarizes the differences.

The value for the highest beam seems to be moot. When considering this to be a reach-through application, the height of the highest beam will have to be much higher to accommodate an operator in a standing position. If the operator can reach over the detection plane, then the reach over criteria applies.

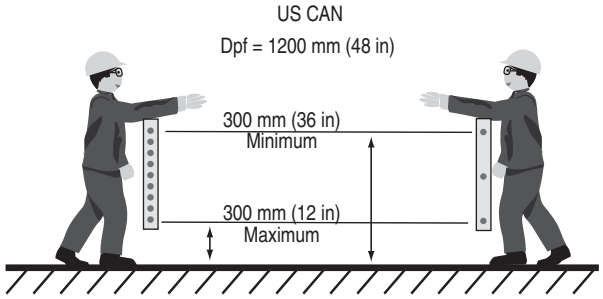


Figure 109: Depth Penetration Factors for Reach-Over Applications

Single or Multiple Beams

Single or multiple separate beams are further defined by the ISO EN standards. Table 5.1 shows the “practical” heights of multiple beams above the floor. The depth penetration is 850 mm for most cases and 1200 mm for the single beam usage. In comparison, the US CAN approach takes this into account by the Reach-Through requirements. Getting over, under or around the single and multiple beams must always be taken into consideration.

No. of Beams	Height Above the Floor [mm (in.)]	C [mm (in.)]
1	750 (29.5)	1200 (47.2)
2	400 (15.7), 900 (35.4)	850 (33.4)
3	300 (11.8), 700 (27.5), 1100 (43.3)	850 (33.4)
4	300 (11.8), 600 (23.6), 900 (35.4), 1200 (47.2)	850 (33.4)

Table 7: Single and Multiple Beam Heights and Depth Penetration Factor

Distance Calculations

For the normal approach to light curtains, the safety distance calculation for the ISO EN and U.S. CAN are close, but differences do exist. For the normal approach to vertical light curtains where the object sensitivity is a maximum of 40 m, the ISO EN approach requires two steps. First, calculate S using 2000 for the speed constant.

S = 2000 x T + 8 x (d -1 4)

The minimum distance that S can be is 100 mm.

A second step can be used when the distance is greater than 500 mm. Then the value of K can be reduced to 1600. When using K=1600, the minimum value of S is 500 mm.

The U.S. CAN approach uses a one step approach:

Ds = 1600 x T * Dpf

This leads to differences greater than 5% between the standards, when the response time is less than 560 ms. Figure 110 shows the minimum safety distance as a function of the total stopping time for 14 and 30 mm object sensitivity. A combination of both approaches needs to be examined to achieve the worst case scenario for globally designed machines.

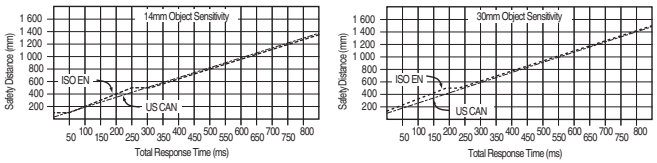


Figure 110: Safety Distance Comparisons

Angled Approaches

Most applications of light curtains and scanners are mounted in vertical (normal approach) or horizontal (parallel approach). These mountings are not considered angled if they are within ±5° of the intended design. When the angle exceeds ±5°, the potential risks (e.g. shortest distance) of foreseeable approaches must be taken into consideration. In general, angles greater than 30° from the reference plane (e.g. floor) should be consider normal and those less than 30 considered parallel. This is depicted in Figure 111.

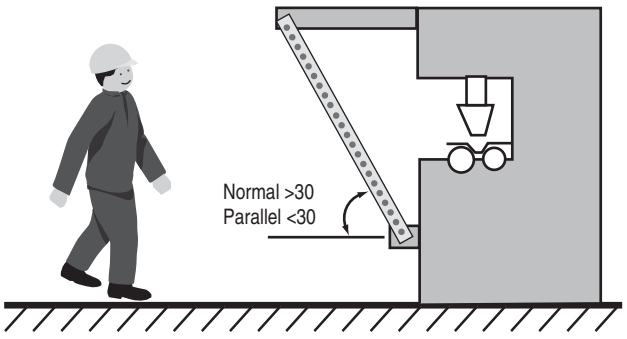


Figure 111: Angle Approach to the Detection Field

Safety Mats

With safety mats, the safety distance must take into account the operators pace and stride. Assuming the operator is walking and the safety mats are mounted on the floor. The operator's first step onto the mat is a depth penetration factor of 1200 mm or 48 in. An example arrangement is shown in Figure 112.

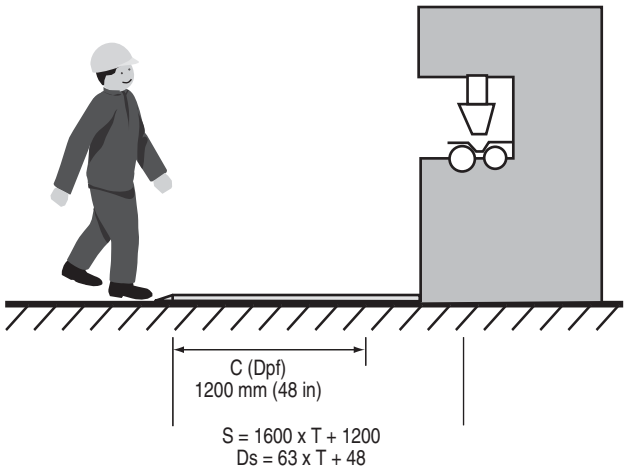


Figure 112: Safety Mat Mounted on Floor

If the operator must step up onto a platform, then the depth penetration factor can be reduced by a factor of 40% of the height of the step (see Figure 113).

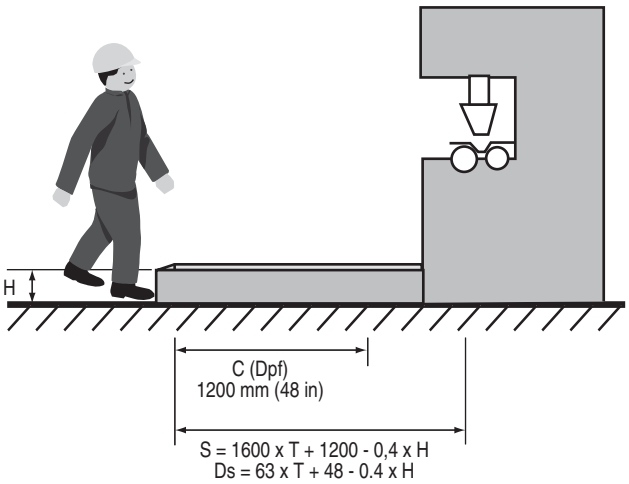


Figure 113: Step Up to Safety Mat Mounted on a Platform

Examples

Example: An operator uses a normal approach to a 14 mm light curtain, which is connected to a monitoring safety relay which is connected to a DC powered contactor with a diode suppressor. The safety system response time, Tr, is 20 + 15 + 95 = 130 ms. The machine stopping time, Ts+Tc, is 170 ms. A brake monitor is not used. The Dpf value is 1 inch, and the C value is zero. The calculation would be as follows:

Dpf = 3.4 (14 - 6.875) = 24.2 mm (1 in) C = 8 (14-14) = 0
Ds = K x (Ts + Tc + Tr + Tbm) + Dpf S = K x T + C
Ds = 63 x (0.17 + 0.13 + 0) + 1 S = 1600 x (0,3) + 0
Ds = 63 x (0.3) + 1 S = 480 mm (18.9 in)
Ds = 18.9 + 1
Ds = 19.9 in (505 mm)

Therefore, the minimum safe distance the safety light curtain must be mounted from the hazard is 508 mm (20 in.) for a machine to be used anywhere in the world.

Prevention of Unexpected Power Up

Prevention of unexpected power up is covered by many standards. Examples include ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05, and AS 4024.1603. These standards have a common theme: the primary method of preventing unexpected power up is to remove the energy from the system and to lock the system in the off state. The purpose is to safely allow people to enter a machine's danger zones.

Lockout/Tagout

New machines must be built with lockable energy isolating devices. The devices apply to all types of energy, including electrical, hydraulic, pneumatic, gravity, and lasers. Lockout refers to applying a lock to an energy isolating device. The lock must only be removed by its owner or by a supervisor under controlled conditions. When multiple individuals must work on the machine, each individual must apply their locks to the energy isolating devices. Each lock must be identifiable to its owner.

In the U.S., tagout is an alternative to lockout for older machines where a lockable device has never been installed. In this case, the machine is turned off and a tag is applied to warn all personnel to not start the machine while the tag holder is working on the machine. Beginning in 1990, machines that are modified must be upgraded to include a lockable energy isolating device.

An energy isolating device is a mechanical device that physically prevents the transmission or release of energy. These devices can take the form of a circuit breaker, a disconnect switch, a manually operated switch, a plug/socket combination or a manually operated valve. Electrical isolating devices must switch all ungrounded supply conductors and no pole can operate independently.

The purpose of lockout and tagout is to prevent the unexpected startup of the machine. Unexpected startup may be the result of various causes: a failure of the control system; an inappropriate action on a start control, sensor, contactor, or valve; a restoration of power after an interruption; or some other internal or external influences. After completion of the lockout or tagout process, the dissipation of the energy must be verified.

Safety Isolation Systems

Safety isolation systems execute an orderly shutdown of a machine and also provide an easy method of locking off the power to a machine. This approach works well for larger machines and manufacturing systems, especially when multiple energy sources are located on a mezzanine level or at distant locations.

Figure 114 shows an overview of the system layout. Lockable stations are remotely located at convenient access points throughout the machine. When necessary, an operator uses the remote station to turn off the machine and lock the machine in the off state. The control box disconnects electrical and pneumatic power and provides a signal back to the operator that the energy has been disconnected.

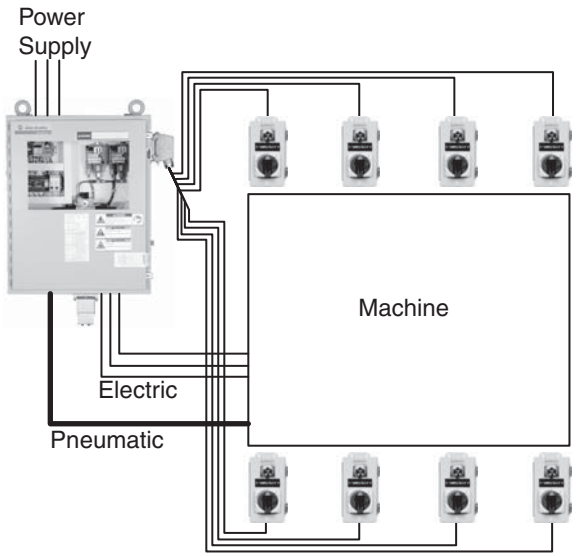


Figure 114: Layout of Safety Isolation System

Figure 115 shows that the safety isolation system not only removes power from the machine but also grounds the load side. The operator gets a monitored, visible signal at the remote station that the machine is in a safe state, and the energy is dissipated.

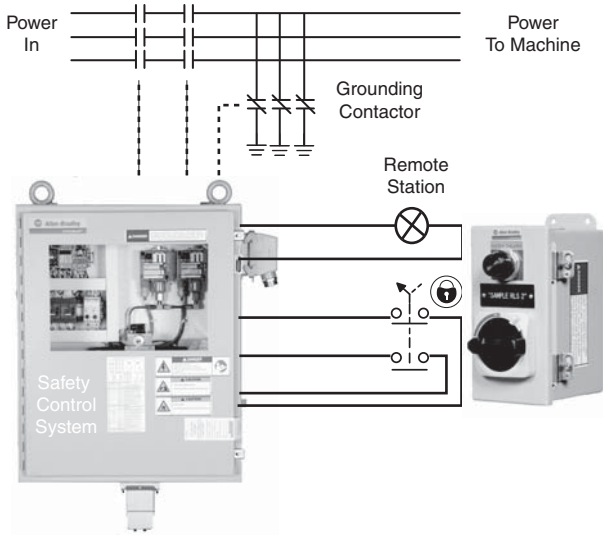


Figure 115: Machine side is grounded with signal to operator.

Load Disconnects

For local isolation of electrical devices, switches can be placed just prior to the device that needs to be isolated and locked out. The Bulletin 194E Load Switches are an example of a product that are capable of both isolation and lockout. Figure 116 shows an example of the Bulletin 194E.

Figure 116: Load switch with isolation and locking capability

Trapped Key Systems

Trapped key systems are another method for implementing a lockout system. Many trapped key systems start with an energy isolating device. When the switch is turned off by the “primary” key, the electrical energy to the machine is removed from all the ungrounded supply conductors simultaneously. The primary key can then be removed and taken to a location where machine access is needed. Figure 117 shows an example of the most basic system, an isolating switch and a gate access lock. Various components can be added to accommodate more complex lockout arrangements.

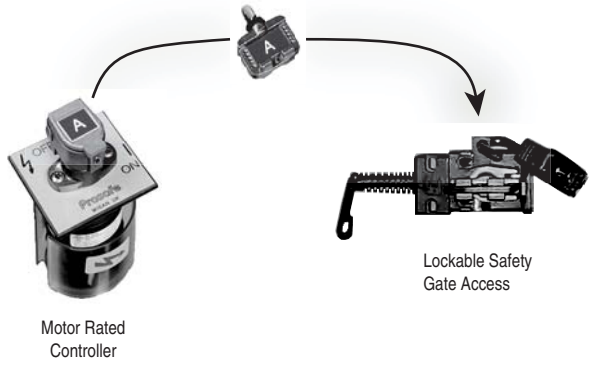


Figure 117: Trapped key isolation and lockable devices

Alternative Measures to Lockout

Lockout and tagout must be used during servicing or maintenance of the machines. Machine interventions during normal production operations are covered by safeguarding. The difference between servicing/maintenance and normal production operations is not always clear.

Some minor adjustments and servicing tasks, which take place during normal production operations, do not necessarily require the machine to be locked out. Examples include loading and unloading materials, minor tool changes and adjustments, servicing lubrication levels, and removing waste material. These tasks must be routine, repetitive, and integral to the use of the equipment for production, and the work is performed using alternative measures, like safeguarding, which provide effective protection. Safeguarding includes devices like interlocked guards, light curtains, and safety mats. Used with appropriate safety rated logic and output devices, operators can safety access the machine danger zones during normal production tasks and minor servicing.

Introduction to Safety-Related Control Systems

What is a safety-related control system (SRCS)? It is that part of the control system of a machine that prevents a hazardous condition from occurring. It can be a separate dedicated system or it may be integrated with the normal machine control system.

Its complexity will vary from a simple system, such as a guard door interlock switch and emergency stop switch connected in series to the control coil of power contactor, to a compound system comprising both simple and complex devices communicating through software and hardware.

Safety-related control systems are designed to perform safety functions. The SRCS must continue to operate correctly under all foreseeable conditions. So what is a safety function; how do we design a system to achieve this; and when we have done that, how do we show it?

Safety Function

A safety function is implemented by the safety-related parts of the machine control system to achieve or maintain the equipment under control in a safe state with respect to a specific hazard. A failure of the safety function can result in an immediate increase of the risks of using the equipment; that is, a hazardous condition.

A machine must have at least one “hazard,” otherwise, it is not a machine. A “hazardous condition” is when a person is exposed to a hazard. A hazardous condition does not imply that the person is harmed. The exposed person may be able to acknowledge the hazard and avoid injury. The exposed person may not be able to recognize the hazard, or the hazard may be initiated by unexpected startup. The main task of the safety system designer is to prevent hazardous conditions and to prevent unexpected startup.

The safety function can often be described with multi-part requirements. For example, the safety function initiated by an interlocking guard has three parts:

1. The hazard protected by the guard cannot operate until the guard is closed;
2. Opening the guard will cause the hazard to stop if operational at the time of the opening; and
3. The closure of the guard does not restart the hazard protected by the guard.

When stating the safety function for a specific application, the word “hazard” must be changed to the specific hazard. The hazard must not be confused with the results of the hazard. Crushing, cutting, and burning are results of a hazard. An example of a hazard is a motor, ram, knife, torch, pump, laser, robot, end-effector, solenoid, valve, other type of actuator, or a mechanical hazard involving gravity.

In discussing safety systems, the phrase “at or before a demand is placed on the safety function” is used. What is a demand on the safety function? Examples of demands placed on the safety function are the opening of an interlocked guard, the breaking of a light curtain, the stepping onto a safety mat, or the pressing of an e-stop. An operator is demanding that the hazard either stop or remain de-energized if it is already stopped.

The safety-related parts of the machine control system execute the safety function. The safety function is not executed by a single device, for example, just by the guard. The interlock on the guard sends a command to a logic device, which in turn, disables an actuator. The safety function starts with the command and ends with the implementation.

The safety system must be designed with a level of integrity that is commensurate with the risks of the machine. Higher risks require higher integrity levels to ensure the performance of the safety function. Machine safety systems can be classified into levels of performance of their ability to ensure the performance of their safety function or, in other words, their functional safety integrity level.

Introduction to Functional Safety of Control Systems

IMPORTANT The standards and requirements considered in this section are relatively new. Work is still being conducted by the drafting groups on some aspects especially with regard to clarification and combining some of these standards. Therefore it is possible that there will be some changes to some of the detail given in these pages. For the latest information please refer to the Rockwell Automation safety systems and components website at http://www.ab.com/safety and the Rockwell Automation Safety Solutions website at http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx.

What is Functional Safety?

Functional safety is the part of the overall safety that depends on the correct functioning of the process or equipment in response to its inputs. IEC TR 61508-0 provides the following example to help clarify the meaning of functional safety. “For example, an over-temperature protection device, using a thermal sensor in the windings of an electric motor to de-energize the motor before they can overheat, is an instance of functional safety. But providing specialized insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).” As another example, compare hard guarding to an interlocked guard. The hard guarding is not considered “functional safety” although it may protect against access to the same hazard as an interlocked door. The interlocked door is an instance of functional safety. When the guard is opened, the interlock serves as an “input” to a system that achieves a safe state. Similarly, personal protective equipment (PPE) is used as a protective measure to help increase safety of personnel. PPE is not considered functional safety.

Functional safety was a term introduced in IEC 61508:1998. Since then, the term has sometimes been associated with only programmable safety systems. This is a misconception. Functional safety covers a broad range of devices that are used to create safety systems. Devices like interlocks, light curtains, safety relays, safety PLCs, safety contactors, and safety drives are interconnected to form a safety system, which performs a specific safety-related function. This is functional safety. Therefore the functional safety of an electrical control system is highly relevant to the control of hazards arising from moving parts of machinery.

Two types of requirements are necessary to achieve functional safety:

- The safety function
- The safety integrity

Risk assessment plays a key role in developing the functional safety requirements. Task and hazard analysis leads to the function requirements for safety (i.e. the safety function). The risk quantification yields the safety integrity requirements (i.e. the safety integrity or performance level).

Four of the most significant control system functional safety standards for machinery are:

1. IEC/EN 61508 “Functional safety of electrical, electronic and programmable electronic control systems”

   This standard contains the requirements and provisions that are applicable to the design of complex electronic and programmable systems and subsystems. The standard is generic so it can be applicable to all industrial sectors.
2. IEC/EN 62061 “Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems”

   This standard is the machinery specific implementation of IEC/EN 61508. It provides requirements that are applicable to the system level design of all types of machinery safety-related electrical control systems and also for the design of non-complex subsystems or devices. It requires that complex or programmable subsystems should satisfy IEC/EN 61508.
3. EN ISO 13849-1 “Safety of machinery — Safety-related parts of control systems”

   This standard is intended to provide a direct transition path from the categories of the previous EN 954-1.
4. IEC 61511 “Functional safety — Safety instrumented systems for the process industry sector”

   This standard is the process sector specific implementation of IEC/EN 61508.

The functional safety standards represent a significant step beyond the familiar existing requirements such as Control Reliable and the Categories system of the previous ISO 13849-1:1999 (EN 954-1:1996).

Note: Recent to the time of publication of this text, CEN (European Committee for Standardization) announced that the final date for presumption of conformity of EN 954-1 will be extended to the end of 2011 to facilitate transition to the later standards. This replaces the original date of December 29, 2009.

For the latest information on the use and status of EN 954-1 visit: http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx. In the meantime, it is advised that the extension of the transition period is used to move over to the use of the later standards (EN ISO 13849-1 or IEC/EN 62061) in a timely manner.

Categories will not disappear completely; they are also used in current EN ISO 13849-1 which uses the functional safety concept and has introduced new terminology and requirements. It has significant additions and differences to the old EN 954-1 (ISO 13849-1:1999). In this section we will refer to the current version as EN ISO 13849-1. (EN ISO 13849-1:2008 has the same text as ISO 13849-1:2006).

IEC/EN 62061 and EN ISO 13849-1:2008

IEC/EN 62061 and EN ISO 13849-1 both cover safety-related electrical control systems. It is intended that they will eventually be combined into one standard with common terminology. Both standards produce the same results but use different methods. They are intended to provide users with an option to choose the one most suitable for their situation. A user can choose to use either standard and they are both harmonized under the European Machinery Directive.

The outputs of both standards are comparable levels of safety performance or integrity. The methodologies of each standard have differences that are appropriate for their intended users.

The methodology in IEC/EN 62061 is intended to allow for complex safety functionality which may be implemented by previously unconventional system architectures. The methodology of EN ISO 13849-1 is intended to provide a more direct and less complicated route for more conventional safety functionality implemented by conventional system architectures.

An important distinction between these two standards is the applicability to various technologies. IEC/EN 62061 is limited to electrical systems. EN ISO 13849-1 can be applied to pneumatic, hydraulic, mechanical as well as electrical systems.

Figure 118 provides a simplified flow chart to help the safety system designer determine which of these two standards to use.

Joint Technical Report on IEC/EN 62061 and EN ISO 13849-1

A joint report has been prepared within IEC and ISO to help users of both standards.

It explains the relationship between the two standards and explains how the equivalence can be drawn between PL (Performance level) of EN ISO 13849-1 and SIL (Safety Integrity Level) of IEC.EN 62061 both at system and subsystem level.

In order to show that both standards give equivalent results the report shows an example safety system calculated according to the methodologies of both standards.

The report also clarifies a number of issues that have been subject to different interpretations. Perhaps one of the most significant issues is the aspect of fault exclusion.

In general, where PLe is required for a safety function to be implemented by a safety-related control system it is not normal to rely upon fault exclusions alone to achieve this level of performance. This is dependent upon the technology used and the intended operating environment. Therefore it is essential that the designer takes additional care on the use of fault exclusions as the PL requirement increases.

In general the use of fault exclusions is not applicable to the mechanical aspects of electromechanical position switches and manually operated switches (e.g. an emergency stop device) in order to achieve PLe in the design of a safety-related control system. Those fault exclusions that can be applied to specific mechanical fault conditions (e.g. wear/corrosion, fracture) are described in Table A.4 of ISO 13849-2.

For example, a door interlocking system that has to achieve PLe will need to incorporate a minimum fault tolerance of 1 (e.g. two conventional mechanical position switches) in order to achieve this level of performance since it is not normally justifiable to exclude faults, such as, broken switch actuators. However, it may be acceptable to exclude faults, such as short circuit of wiring within a control panel designed in accordance with relevant standards.

SIL and IEC/EN 62061

IEC/EN 62061 describes both the amount of risk to be reduced and the ability of a control system to reduce that risk in terms of SIL (Safety Integrity Level). There are three SILs used in the machinery sector, SIL 1 is the lowest and SIL 3 is the highest.

Because the term SIL is applied in the same manner in other industrial sectors such as petro-chemicals, power generation and railways, IEC/EN 62061 is very useful when machinery is used within those sectors.

Risks of greater magnitude can occur in other sectors such as the process industry and for that reason IEC 61508 and the process sector specific standard IEC 61511 include SIL 4.

A SIL applies to a safety function. The subsystems that make up the system that implements the safety function must have an appropriate SIL capability. This is sometimes referred to as the SIL Claim Limit (SIL CL).

A full and detailed study of IEC/EN 62061 is required before it can be correctly applied. Some of the most commonly applicable requirements of the standard are summarized later in this text.

System Level Design
Conduct a task analysis and risk assessment to identify any hazards.
Decide which hazards will be addressed by a safety related control system.

Decide on which of the two alternative standards to use.

Are there complex safety functions or will the system require complex programmable electronics to a high level of intergrity?

If the answer to either question is yes, use

IEC62061:2005

Can the system be designed simply using the designated architectures of Categoies B, 1, 2, 3 or 4, or will the system include technologies other than electrical?
If the answer to either question is yes, use

EN/ISO13849-1:2006

Determine the functionality required for the safety function, for example:

Position Sensing → Logic Solving → Output Actuation

Note: This should take account of all tasks required at the machine and it is very important to also give full consideration to production and maintenance requirements when deciding on the safety function concept.

Use the risk assessment process to determine the required safety integrity level, SIL, for each safety function, for example SIL2

Use the risk assessment process to determine the required performance level, PL_r, for each safety function, for example, PL_d

Using the requirements for system design determine what subsystem components are required to implement the Function Blocks. Each subsystem must be suitable for the required SIL. For each subsystem, choose a combination of Safe Failure Fraction (SFF), fault tolerance, PFHd to achieve the required SIL Claim Limit.

For example for SIL2, the following is possible:

Sensing subsystem → Logic subsystem → Output subsytem

where each subsystem has
Fault Tolerance: 1, SFF: 80%, PFH_D: 1×10^{-7}

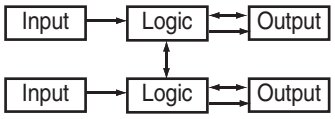
The combined PFH_D of all three subsystems is 3×10^{-7} and therefore meets the target PFH_D of 1×10^{-6} for the safety function.

The following information is required for each subsystem: PFH_D, fault tolerance, SFF.

The following is required for each system: measures against systematic failure.

Using the risk assessment charts or tables, determine which combination of architecture, diagnostic coverage and mean time to failure will achieved the required performance level.

For example, for PLd the following is possible



Designated architecture: Category 3
Diagnostic Coverage: Medium (95%)
$MTTF_d$ for each channel: 15yrs

The following information is required for each component:
$MTTF_d$

The following information is required for each system: designated architecture, diagnostic coverage, and measures against common cause and systematic failures.

Figure 118: System Design Flow Diagram

PL and EN ISO 13849-1

EN ISO 13849-1 does not use the term SIL; instead it uses the term PL (Performance Level). In many respects PL can be related to SIL. There are five performance levels, PLa is the lowest and PLe is the highest.

Comparison of PL and SIL

Table 8 shows the relationship (in terms of probability of dangerous failure between PL and SIL when applied to typical circuit structures.

PL (Performance Level)	PFH_D (Probability of Dangerous Failure per Hour)	SIL
a	$\geq 10^{-5}$ to $<10^{-4}$	None
b	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
c	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $<10^{-6}$	2
e	$\geq 10^{-8}$ to $<10^{-7}$	3

Table 8: Approximate correspondence between PL and SIL

IMPORTANT Table 8 is for general guidance and must NOT be used for conversion purposes. The full requirements of the standards must be taken into account.

System Design According to EN ISO 13849 and SISTEMA

A full and detailed study of EN ISO 13849-1 is required before it can be correctly applied. The following is a brief overview:

This standard provides requirements for the design and integration of safety-related parts of control systems, including some software aspects. The standard applies to a safety-related system but can also be applied to the component parts of the system.

SISTEMA Software PL Calculation Tool

SISTEMA is a software tool for the implementation of EN ISO 13849-1. Its use will greatly simplify the implementation of the standard.

SISTEMA stands for "Safety Integrity Software Tool for the Evaluation of Machine Applications" It was developed by the BGIA in Germany and is free for use. It requires the input of various types of functional safety data as described later in this section.

The Data can be input manually or automatically by using a Manufacturer's SISTEMA Data Library.

The Rockwell Automation SISTEMA Data Library is available for download, together with a link to the SISTEMA download site, at: http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx.

Overview of EN ISO 13849-1

This standard has wide applicability, as it applies to all technologies, including electrical, hydraulic, pneumatic and mechanical. Although ISO 13849-1 is applicable to complex systems, it also refers the reader to IEC 62061 and IEC 61508 for complex software embedded systems.

Let's have look at what are the basic differences between the old EN 954-1 and the new EN ISO 13849-1. The outputs of the old standard were Categories [B, 1, 2, 3 or 4]. The outputs of the new standard are Performance Levels [PL a, b, c, d or e]. The Category concept is retained but there are additional requirements to be satisfied before a PL can be claimed for a system.

The requirements can be listed in basic form as follows:

- The architecture of the system. Essentially this captures what we have become used to as the Categories
- Reliability data is required for the constituent parts of the system
- The Diagnostic Coverage [DC] of the system is required. This effectively represents the amount of fault monitoring in the system
- Protection against common cause failure
- Protection against systematic faults
- Where relevant, specific requirements for software

Later we will take a closer look at these factors but before we do it will be useful to consider the basic intent and principle of the whole standard. It is clear at this stage that there are new things to learn but the detail will make more sense once we have understood what it is trying to achieve and why.

First of all why do we need the new standard? It is obvious that the technology used in machine safety systems has progressed and changed considerably over the last ten years. Until relatively recently safety systems have depended on "simple" equipment with very foreseeable and predictable failure modes. More recently we have seen an increasing use of more complex electronic and programmable devices in safety systems. This has given us advantages in terms of cost, flexibility and compatibility but it has also meant that the pre-existing standards are no longer adequate. In order to know whether a safety system is good enough we need to know more about it. This is why the new standard asks for more information. As safety systems start to use a more "black box" approach we start to rely more heavily on their conformity to standards. Therefore those standards need to be capable of properly interrogating the technology. In order to fulfill this they must speak to the basic factors of reliability, fault detection, architectural and systematic integrity. This is the intent of EN ISO 13849-1.

In order to plot a logical course through the standard, two fundamentally different user types must be considered: the designer of safety-related subsystems and the designers of safety-related systems. In general the subsystem designer [typically a safety component manufacturer] will be subjected to a higher level of complexity. They will need to provide the required data in order that the system designer can ensure that the subsystem is of adequate integrity for the system. This will usually require some testing, analysis and calculation. The results will be expressed in the form of the data required by the standard.

The system designer [typically a machine designer or integrator] will use the subsystem data to perform some relatively straightforward calculations to determine the overall Performance Level [PL] of the system.

PLr is used to denote what performance level is required by the safety function. In order to determine the PLr the standard provides a risk graph into which the application factors of severity of injury, frequency of exposure and possibility of avoidance are input.

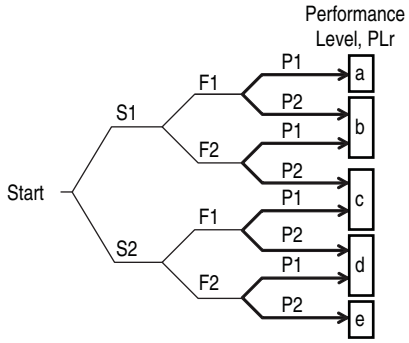


Figure 119: Risk Graph from Annex A of EN ISO 13849-1

The output is the PLr. Users of the old EN 954-1 will be familiar with this approach but take note that the S1 line now subdivides whereas the old risk graph did not. Note that this means a possible reconsideration of the integrity of safety measures required at lower risk levels.

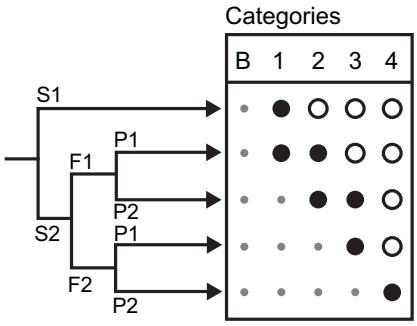


Figure 120: Risk Graph from Annex B of EN 945-1

There is one very important part yet to be covered however. We now know from the standard how good the system needs to be and also how to determine how good it is but we don't know what it needs to do. We need to decide what the safety function is. Clearly the safety function must be appropriate to the task so how do we ensure this? How does the standard help us?

It is important to realize that the functionality required can only be determined by considering the characteristics prevailing at the actual application. This can be regarded as the safety concept design stage. It cannot be completely covered by the standard because the standard does not know about all the characteristics of a specific application. This also often applies to the machine builder who produces the machine but does not necessarily know the exact conditions under which it will be used.

The standard does provide some help by listing out many of the commonly used safety functions (e.g. safety-related stop function initiated by safeguard, muting function, start/restart function) and giving some normally associated requirements. Other standards such as EN ISO 12100: Basic design principles and EN ISO 14121: Risk assessment, are highly recommended for use at this stage. Also there is a large range of machine specific standards that will provide solutions for specific machines. Within the European EN standards they are termed C type standards, some of them have exact equivalents in ISO standards.

So we can now see that the safety concept design stage is dependant on the type of machine and also on the characteristics of the application and environment in which it is used. The machine builder must anticipate these factors in order to be able to design the safety concept. The intended [i.e. anticipated] conditions of use should be given in the user manual. The user of the machine needs to check that they match the actual usage conditions.

So now we have a description of the safety functionality. From annex A of the standard we also have the required performance level [PLr] for the safety-related parts of the control system [SRP/CS] that will be used to implement this functionality. We now need to design the system and make sure that it complies with the PLr.

One of the significant factors in the decision on which standard to use [EN ISO 13849-1 or EN/IEC 62061] is the complexity of the safety function. In most cases, for machinery, the safety function will be relatively simple and EN ISO 13849-1 will be the most suitable route. Reliability data, diagnostic coverage [DC], the system architecture [Category], common cause failure and, where relevant, requirements for software are used to assess the PL.

This is a simplified description meant only to give an overview. It is important to understand that all the provisions given in the body of the standard must be applied. However, help is at hand. The SISTEMA software tool is available to help with the documentation and calculation aspects. It also produces a technical file.

At time of going to print of this publication SISTEMA is available in German and English. Other languages will be released in the near future. BGIA, the developer of SISTEMA, is a well-respected research and testing institution based in Germany. It is particularly involved in solving scientific and technical problems relating to safety in the context of statutory accident insurance and prevention in Germany. It works in cooperation with occupational health and safety agencies from over 20 countries. Experts from the BGIA, along with their BG colleagues had significant participation in the drafting of both EN ISO 13849-1 and IEC/EN 62061.

The “library” of Rockwell Automation safety component data for SISTEMA is available at:
http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx.

Whichever way the calculation of the PL is done it is important to start of from the right foundation. We need to view our system in the same way as the standard so let's start with that.

System Structure

Any system can be split into basic system components or “subsystems.” Each subsystem has its own discrete function. Most systems can be split into three basic functions; input, logic solving and actuation [some simple systems may not have logic solving]. The component groups that implement these functions are the subsystems.

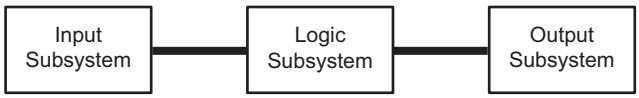


Figure 121

A simple single channel electrical system example is given in Figure 122. It comprises only input and output subsystems.

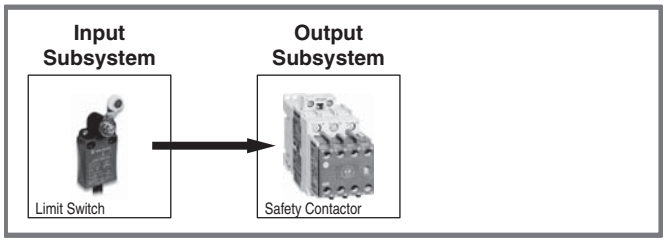


Figure 122: Interlock Switch and Contactor

In Figure 123 the system is a little more complex because some logic is also required. The safety controller itself will be fault tolerant (e.g. dual channel) internally but the overall system is still limited to single channel status because of the single limit switch and single contactor.

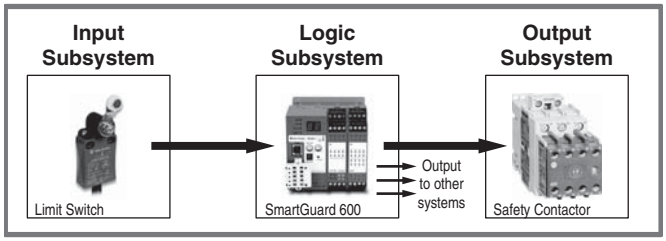


Figure 123: Interlock Switch, Safety Controller and Safety Contactor

If we take the basic architecture of Figure 123, there are also some other things to consider. First how many “channels” does the system have? A single channel system will fail if one of its subsystems fails. A two channel [also called redundant] system would need to have two failures, one in each channel before the system fails. Because it has two channels it can tolerate a single fault and still keep working. Figure 124 shows a two channel system.

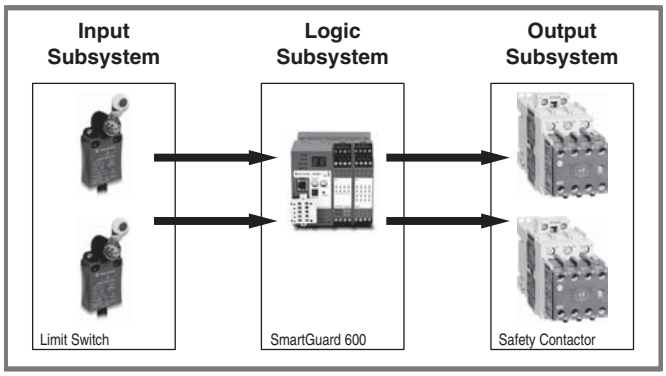


Figure 124: Dual Channel with Interlock Switch, Safety Controller and Safety Contactors

Clearly the system shown in Figure 124 is less likely to fail than the one shown in Figure 123 but we can make it even more reliable [in terms of its safety function] if we include diagnostic measures for fault detection. Of course, having detected the fault we also need to react to it and put the system into a safe state. Figure 125 shows the inclusion of diagnostic measures achieved through monitoring techniques.

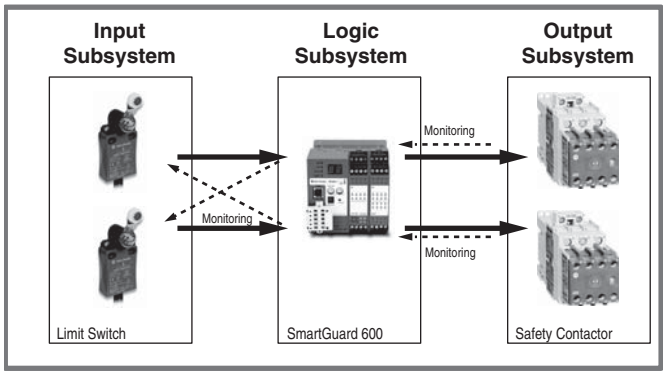


Figure 125: Dual Channel System with Interlock Switch, Safety Controller and Safety Contactors—Diagnostics Shown by Dashed Arrows

It is usually [but not always] the case that the system comprises two channels in all its subsystems as shown in Figure 125. Therefore we can see that, in this case each subsystem has two "sub channels." The standard describes these as “blocks.” A two channel subsystem will have two blocks and a single channel subsystem will have one block. It is possible that some systems will comprise a combination of dual channel and single channel blocks.

If we want to investigate the system in more depth we need to look at the components parts of the blocks. The SISTEMA tool uses the term “elements” for these component parts. Figure 126 shows our system using the SISTEMA terminology.

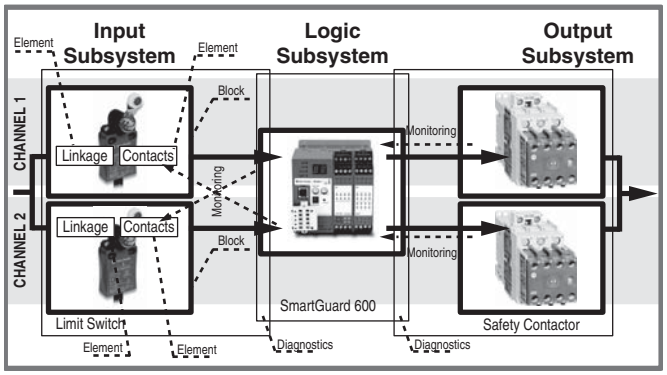


Figure 126: Dual Channel System Shown Subdivided into Subsystems, Blocks and Elements

The limit switches subsystem is shown subdivided down to its element level. The output contactor subsystem is subdivided down to its block level and the logic subsystem is not subdivided at all. The monitoring function for both the limit switches and the contactors is performed at the logic controller. Therefore the boxes representing the limit switch and contactor subsystems have a small overlap with the logic subsystem box.

This principle of system subdivision can be recognized in the methodology given in EN ISO 13849-1 and in the basic system structure principle for the SISTEMA tool. However, it is important to note that there are some subtle differences. The standard is not restrictive in its methodology but for the simplified method for estimating the PL the usual first step is to break the system structure into channels and the blocks within each channel. With SISTEMA the system is first divided into subsystems. The standard does not explicitly describe a subsystem concept but its use as given in SISTEMA provides a more understandable and intuitive approach. Of course there is no effect on the final calculation. SISTEMA and the standard both use the same principles and formulae. It is interesting to note that the subsystem approach is also used in EN/IEC 62061.

The system we have been using as an example is just one of the five basic types of system architectures that the standard designates. Anyone familiar with the Categories system will recognize our example as representative of either Category 3 or 4.

The standard uses the original EN 954-1 Categories as its five basic types of designated system architectures. It calls them Designated Architecture Categories. The requirements for the Categories are almost [but not quite] identical to those given in EN 954-1. The Designated Architecture Categories are represented by the following figures. It is important to note that they can be applied either to a complete system or a subsystem. The diagrams should not be taken purely as a physical structure. They are intended more as a graphical representation of conceptual requirements.

A more detailed look at the practical implementation of categories is dealt with in a later chapter.

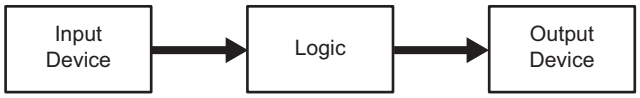


Figure 127: Designated Architecture Category B

Designated Architecture Category B must use basic safety principles [see annex of EN ISO 13849-2]. The system or subsystem can fail in the event of a single fault. See EN ISO 13849-1 for full requirements.

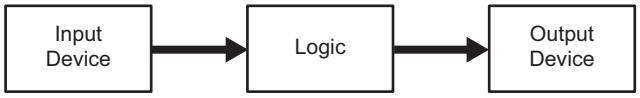


Figure 128: Designated Architecture Category 1

Designated Architecture Category 1 has the same structure as Category B and can still fail in the event of a single fault. But because it must also use well tried safety principles [see annex of EN ISO 13849-2] this is less likely than for Category B. See EN ISO 13849-1 for full requirements.

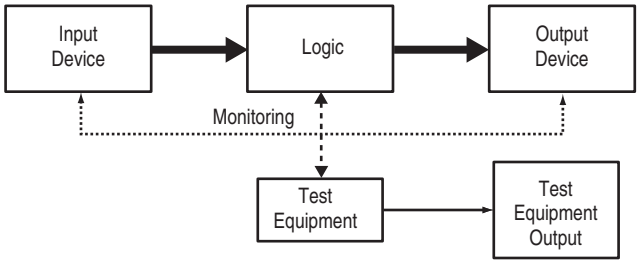


Figure 129: Designated Architecture Category 2

Designated Architecture Category 2 must use basic safety principles [see annex of EN ISO 13849-2]. There must also be diagnostic monitoring via a functional test of the system or subsystem. The test must occur at start up and then periodically with a frequency that equates to at least one hundred tests to every demand on the safety function. Note that this test rate is an additional requirement to that given in the old EN 954-1. The system or subsystem can still fail if a single fault occurs between the functional tests but this is usually less likely than for Category 1. See EN ISO 13849-1 for full requirements.

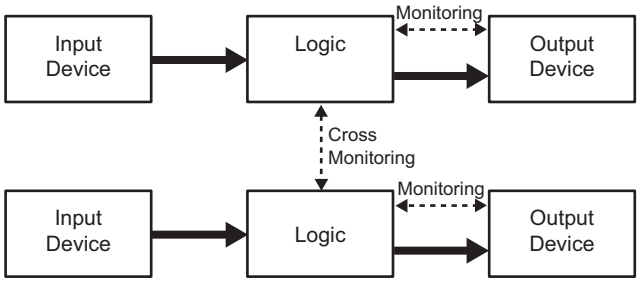


Figure 130: Designated Architecture Category 3

Designated Architecture Category 3 must use basic safety principles [see annex of EN ISO 13849-2]. There is also a requirement that the system/subsystem must not fail in the event of a single fault. This means that the system needs to have single fault tolerance with regard to its safety function. The most common way of achieving this requirement is to employ a dual channel architecture as shown in Figure 130. In addition a single fault shall be detected, wherever practicable. This requirement is the same as the original requirement for Category 3 from EN 954-1. In that context the meaning of the phrase “wherever practicable” proved somewhat problematic. It meant that Category 3 could cover everything from a system with redundancy but no fault detection [often descriptively and appropriately termed “stupid redundancy”] to a redundant system where all single faults are detected. This issue is addressed in EN ISO 13849-1 by the requirement to estimate the quality of the Diagnostic Coverage [DC]. By reference to Annex K or Table 9. We can see that the greater the reliability [MTTFd] of the system, the less the DC we need. However, DC needs to be at least 60% for Category 3 Architecture.

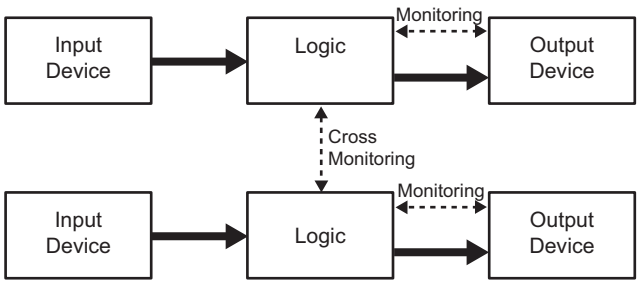


Figure 131: Designated Architecture Category 4

Designated Architecture Category 4 must use basic safety principles [see annex of EN ISO 13849-2]. It has a similar requirements diagram to Category 3 but it demands greater monitoring i.e. higher Diagnostic Coverage. This is shown by the heavier dotted lines representing the monitoring functions. In essence the difference between Categories 3 and 4 is that for Category 3 most faults must be detected but for Category 4 all faults must be detected. The DC needs to be at least 99%. Even an accumulation of faults must not cause a dangerous failure.

Reliability Data

EN ISO 13849-1 uses quantitative reliability data as part of the calculation of the PL achieved by the safety-related parts of a control system. This is a significant departure from EN 954-1. The first question this raises is "where do we get this data from?" It is possible to use data from recognized reliability handbooks but the standard makes it clear that the preferred source is the manufacturer. To this end, Rockwell Automation is making the relevant information available in the form of a data library for SISTEMA. In due course it will also publish the data in other forms. Before we go any further we should consider what types of data are required and also gain an understanding of how it is produced.

The ultimate type of data required as part of the PL determination in the standard [and SISTEMA] is the PFH [the probability of dangerous failure per hour]. This is the same data as represented by the PFHd abbreviation used in IEC/EN 62061.

PL	Average Probability of Dangerous Failure per Hour (1/h)	SIL
a	$\geq 10^{-5}$ to $<10^{-4}$	No correspondence
b	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
c	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $<10^{-6}$	2
e	$\geq 10^{-8}$ to $<10^{-7}$	3

Table 9

Table 9 shows the relationship between PFH and PL and SIL. For some subsystems the PFH may be available from the manufacturer. This makes life easier for the calculation. The manufacturer will usually have to perform some relatively complex calculation and/or testing on their subsystem in order to provide it. In the event that it is not available, EN ISO13849-1 gives us an alternative simplified approach based on the average MTTFd [mean time to a dangerous failure] of a single channel. The PL [and therefore the PFH] of a system or subsystem can then be calculated using the methodology and formulae in the standard. It can be done even more conveniently using SISTEMA.

NOTE: It is important to understand that, for a dual channel system (with or without diagnostics), it is not correct to use $1/PFH_D$ to determine the MTTFd that is required by EN ISO 13849-1. The standard calls for the MTTFd of a single channel. This is a very different value to the MTTFd of the combination of both channels of a two channel subsystem. If the PFH_D of a two channel subsystem is known, it can simply be entered directly in to SISTEMA.

MTTFd of a Single Channel

This represents the average mean time before the occurrence of a failure that could lead to the failure of the safety function. It is expressed in years. It is an average value of the MTTFd's of the "blocks" of a single channel and can be applied to either a system or a subsystem. The standard gives the following formula which is used to calculate the average of all the MTTFd's of each element used in a single channel or subsystem.

At this stage the value of SISTEMA becomes apparent. Users are spared time consuming consultation of tables and calculation of formulae since these tasks are performed by the software. The final results can be printed out in the form of a multiple page report.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$

Formula D1 from EN ISO 13849-1

In most dual channel systems both channel are identical therefore the result of the formula represents either channel.

If the system/subsystem channels are different the standard provides a formula to cater for this.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right]$$

Formula 1 from EN ISO 13849-1

This, in effect, averages the two averages. In the cause of simplification it is also allowable to just use the worst case channel value.

The standard groups the MTTFd into three ranges as follows:

Denotation of MTTFd of each channel	Range of MTTFd of each channel
Low	3 years <= $MTTF_d$ < 10 years
Medium	10 years <= $MTTF_d$ < 30 years
High	30 years <= $MTTF_d$ < 100 years

Table 10: Levels of $MTTF_d$

Note that EN ISO 13849-1 limits the usable $MTTF_d$ of a single channel of a subsystem to a maximum of 100 years even though the actual values derived may be much higher.

As we will see later, the achieved range of MTTFd average is then combined with the designated architecture Category and the diagnostic coverage [DC] to provide a preliminary PL rating. The term preliminary is used here because other requirements including systematic integrity and measures against common cause failure still have to be met where relevant.

Methods of Data Determination

We now need to delve one stage deeper into how a manufacturer determines the data either in the form of PFH_D or $MTTF_d$. An understanding of this is essential when dealing with manufacturers data.

Data can be grouped into two basic types: 1) mechanistic (electro-mechanical, mechanical, pneumatic and hydraulic) and 2) electronic (solid state).

There is a fundamental difference between the common failure mechanisms of these three technology types. In basic form it can be summarized as follows:

Mechanistic Technology: Failure is proportional to both the inherent reliability and the usage rate. The greater the usage rate, the more likely that one of the component parts may be degraded and fail. Note that this is not the only failure cause, but unless we limit the operation time/cycles it will be the predominant one. It is self evident that a contactor that has switching cycle of once per ten seconds will operate reliably for a far shorter time than an identical contactor that operates one per day. Physical technology devices generally comprise components that are individually designed for their specific use. The components are shaped, molded, cast, machined etc. They are combined with linkages, springs, magnets, electrical windings etc to form a mechanism. Because the component parts do not, in general, have any history of use in other applications, we cannot find any pre-existing reliability data for them. The estimation of the PFH_D or $MTTF_d$ for the mechanism is normally based on testing. Both EN/IEC 62061 and EN ISO 13849-1 advocate a test process known as B10d Testing.

In the B10d test a number of device samples [usually at least ten] are tested under suitably representative conditions. The mean number of operating cycles achieved before 10% of the samples fail to the dangerous condition is known as the B10d value.

In practice it is often the case that all of the samples will fail to a safe state but in that case the standard states that the B10d[dangerous] value can be taken as twice the B10[safe] value.

Electronic Technology: There are no physical wear related moving parts. Given an operating environment commensurate with the specified electrical and temperature [etc] characteristics, the predominant failure of an electronic circuit is proportional to the inherent reliability of its constituent components [or lack off it]. There are many reasons for individual component failure; imperfection introduced during manufacture, excessive power surges, mechanical connection problems etc. In general, faults in electronic components are difficult to predict by analysis and they appear to be random in nature. Therefore testing of an electronic device in test laboratory conditions will not necessarily reveal typical long term failure patterns.

In order to determine the reliability of electronic devices it is usual to use analysis and calculation. We can find good data for the individual components in reliability data handbooks. We can use analysis to determine which component failure modes are dangerous. It is acceptable and usual to average out the component failure modes as 50% safe and 50% dangerous. This normally results in relatively conservative data.

IEC 61508 provides formulae that can be used to calculate the overall probability of dangerous failure [PFH or PFD] of the device i.e. the subsystem. The formulae are quite complex and take into account [where applicable] component reliability, potential for common cause failure [beta factor], diagnostic coverage [DC], functional test interval and proof test interval. The good news is that this complex calculation will normally be done by the device manufacturer. Both EN/IEC 62061 and EN ISO 13849-1 accept a subsystem calculated in this way to IEC 61508. The resulting PFH_D can be used directly into either Annex K of EN ISO 13849-1 or the SISTEMA calculation tool.

Software: Failures of software are inherently systematic in nature. Any failures are caused by the way it is conceived, written or compiled. Therefore all failures are caused by the system under which it is produced, not by its use. Therefore in order to control the failures we must control that system. Both IEC 61508 and EN ISO 13849-1 provide requirements and methodologies for this. We do not need to go into detail here other than to say they use the classic V model.

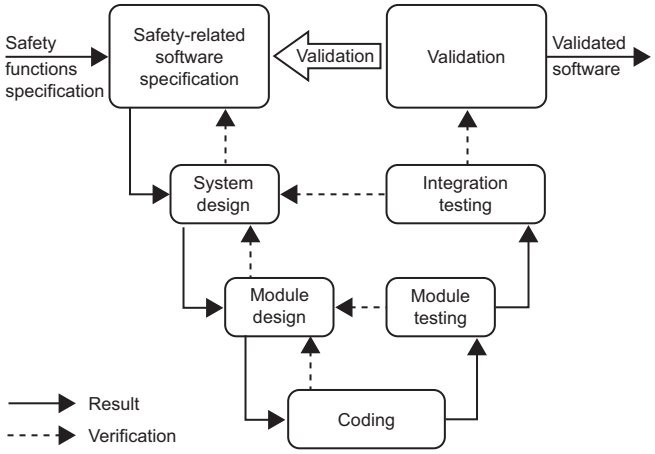


Figure 132: V Model for Software Development

Embedded software is an issue for the designer of the device. The usual approach is to develop embedded software in accordance with the formal methods explained in IEC 61508 part 3. When it comes to application code, the software that a user interfaces with, most programmable safety devices are provided with "certified" function blocks or routines. This simplifies the validation task for application code but it must be remembered that the completed application program still needs to be validated. The way the blocks are linked and parameterized must be proved correct and valid for the intended task. EN ISO 13849-1 and IEC/EN 62061 Both provide guidelines for this process.

Diagnostic Coverage

We have already touched on this subject when we considered the Designated Architecture Categories 2, 3 and 4. Those Categories require some form of diagnostic testing to check whether the safety function is still working. The term "diagnostic coverage" [usually abbreviated to DC] is used to characterise the effectiveness of this testing. It is important to realize that DC is not based just on the number of components that can fail dangerously. It takes account of the total dangerous failure rate. The symbol λ (lambda) is used for "failure rate." DC expresses the relationship of the rates of occurrence of the two following types of dangerous failure:

- Dangerous detected failure [λdd] i.e. Those failures would cause, or could lead to, a loss of the safety function, but which are detected. After detection, a fault reaction function causes the device or system to go to a safe state.
- Dangerous failure [λd] i.e. All those failures that could potentially cause, or lead to, a loss of the safety function. This includes both the failures that are detected and those that are not. Of course the failures that are that are truly dangerous are the dangerous undetected ones [termed λdu].

DC is expressed by the formula;

DC = λdd/λd expressed as a percentage.

This meaning of the term DC is common to EN ISO 13849-1 and EN/IEC 62061. However the way that it is derived differs. The latter standard proposes the use of calculation based on failure mode analysis but EN ISO 13849-1 provides a simplified method in the form of look-up tables. Various typical diagnostic techniques are listed together with the DC percentage that their use is deemed to achieve. In some cases rational judgment is still required, for example in some techniques the achieved DC is proportional to how often the test is performed. It is sometimes argued that this approach is too vague. However the estimation of DC can depend on many different variables and whichever technique is used the result can usually only truly be described as approximate. It is also important to understand that the tables in EN ISO 13849-1 are based on extensive research conducted by the BGIA into the results achieved by known actual diagnostic techniques used in real applications. In the interest of simplification the standard divides DC into four basic ranges :

<60% = none

60% to <90% = low

90% to <99% = medium

99%+ = high

This approach of dealing with ranges instead of individual percentage values can also be considered to be more realistic in terms of achievable accuracy. The SISTEMA tool uses the same look-up tables as the standard. As the use of complex electronics increases in safety-related devices DC becomes a more important factor. It is likely that future work on the standards will look further into clarification of this issue. In the meantime the use of engineering judgment and common sense should be sufficient to lead to the correct choice of DC range.

Common-Cause Failure

In most dual channel [i.e. single fault tolerant] systems or subsystems the diagnostic principle is based on the premise that there will not be dangerous failures of both channels at the same time. The term “at the same time” is more accurately expressed as “within the diagnostic test interval.” If the diagnostic test interval is reasonably short [e.g. less than eight hours] it is a reasonable assumption that two separate and unrelated faults are highly unlikely to occur within that time. However the standard makes it clear that we need to think carefully about whether the fault possibilities really are separate and unrelated. For example, if a fault in one component can foreseeably lead to failures of other components then the resulting totality of faults are deemed to be a single failure.

It is also possible that an event that causes one component to fail may also cause the failure of other components. This is termed “common cause failure” (CCF). The degree of propensity for CCF is normally described as the beta [ß] factor. It is very important that subsystem and system designers are aware of the possibilities of CCF. There are many different types of CCF and, correspondingly, many different ways of avoiding it. EN ISO 13849-1 plots a rational course between the extremes of complexity and over simplification. In common with EN/IEC 62061 it adopts an approach that is essentially qualitative. It provides a list of measures known to be effective in avoiding CCF.

Table 11 shows a summary of the scoring process.

No.	Measure Against CCF	Score
1	Separation/Segregation	15
2	Diversity	20
3	Design/Application/ Experience	20
4	Assessment/Analysis	5
5	Competence/Training	5
6	Environmental	35

Table 11: Scoring for Common-Cause Failure

A sufficient number of these measures must be implemented in the design of a system or subsystem. It could be claimed, with some justification, that the use of this list alone may not be adequate to prevent all possibility of CCF. However, if the intent of the list is properly considered it becomes clear that the spirit of its requirement is to make the designer analyse the possibilities for CCF and to implement appropriate avoidance measures based on the type of technology and the characteristics of the intended application. Use of the list enforces consideration of some of the most fundamental and effective techniques such as diversity of failure modes and design competencies. The BGIA SISTEMA tool also requires the implementation of the standard's CCF look up tables and makes them available in a convenient form.

Mission Time

Mission time represents the maximum period of time for which a subsystem (or system) can be used. After this time, it must be replaced. Mission time must be declared by the manufacturer of the components. Mission time will usually be the same as the “proof test interval” or “lifetime” (whichever is the smaller) as used in IEC/EN62061. The safety system designer must then consider the mission time of the components to determine the mission time of each safety function. For mechanistic components the T10d value gives this usable lifetime value in terms of the number of operations. The T10d value is derived as part of the B10d calculation.

Systematic Faults

We have already discussed quantified safety reliability data in the form of MTTFd and the probability of dangerous failure. However, this is not the whole story. When we referred to those terms we were really thinking about failures that appear to be random in nature. Indeed IEC/EN 62061 specifically refers to the abbreviation of PFH_D as the probability of random hardware failure. But there are some types of failures collectively known as “systematic failure” that can be attributed to errors committed in the design or manufacturing process. The classic example of this is an error in software code. The standard provides measures in Annex G to avoid these errors [and therefore the failures]. These measures include provisions such as the use of suitable materials and manufacturing techniques, reviews, analysis and computer simulation. There are also foreseeable events and characteristics that can occur in the operating environment that could cause failure unless their effect is controlled. Annex G also provides measures for this. For example it is easily foreseeable that there may be occasional losses of power. Therefore the de-energization of components must result in a safe state for the system. These measures may seem to be just common sense, and indeed they are, but they are nevertheless essential. All the rest of the requirements of the standard will be meaningless unless due consideration is given to the control and avoidance of systematic failure. This will also sometimes require the same types of measures used for the control of random hardware failure [in order to achieve the required PFH_D] such as automatic diagnostic test and redundant hardware.

Fault Exclusion

One of the primary analysis tools for safety systems is failure analysis. The designer and user must understand how the safety system performs in the presence of faults. Many techniques are available to perform the analysis. Examples include Fault Tree Analysis; Failure Modes, Effects and Criticality Analysis; Event Tree Analysis; and Load-Strength reviews.

During the analysis, certain faults may be uncovered that cannot be detected with automatic diagnostic testing without undue economic costs. Further, the probability that these faults might occur may be made extremely small, by using mitigating design, construction and test methods. Under these conditions, the faults may be excluded from further consideration. Fault exclusion is the ruling out of the occurrence of a failure because the probability of that specific failure of the SRCS is negligible.

ISO13849-1:2006 allows fault exclusion based on the technical improbability of occurrence, generally accepted technical experience and the technical requirements related to the application. ISO13849-2:2003 provides examples and justifications for excluding certain faults for electrical, pneumatic, hydraulic and mechanical systems. Fault exclusions must be declared with detailed justifications provided in the technical documentation.

It is not always possible to evaluate Safety-related Control System without assuming that certain faults can be excluded. For detailed information on fault exclusions, see ISO 13849-2.

As the level of risk gets higher, the justification for fault exclusion gets more stringent. In general, where PLe is required for a safety function to be implemented by a safety-related control system it is not normal to rely upon fault exclusions alone to achieve this level of performance. This is dependent upon the technology used and the intended operating environment. Therefore it is essential the designer takes additional care on the use of fault exclusions as that PL requirement increases.

For example, a door interlocking system that has to achieve PLe will need to incorporate a minimum fault tolerance of 1 (e.g. two conventional mechanical position switches) in order to achieve this level of performance since it is not normally justifiable to exclude faults, such as, broken switch actuators. However, it may be acceptable to exclude faults, such as short circuits in wiring within a control panel designed in accordance with relevant standards.

Performance Level (PL)

The performance level is a discrete level that specifies the ability of the safety-related parts of the control system to perform a safety function.

In order to assess the PL achieved by an implementation of any of the five designated architectures, the following data is required for the system (or subsystem):

- $MTTF_d$ (mean-time-to-dangerous failure of each channel)
- DC (diagnostic coverage)
- Architecture (the category)

Table 12 shows the PL achieved by various combinations. Refer to Annex K of the standard for more precise determination.

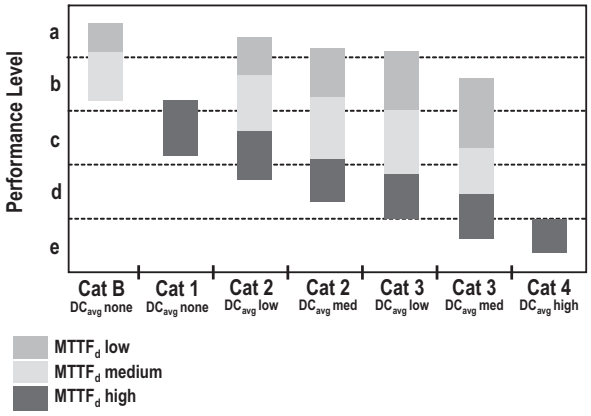


Figure 133: Graphical Determination of PL

Table 12 shows the PL achieved by various combinations. Refer to Annex K of the standard for more precise determination. For example, an application uses the Category 3 designated architecture. If the DC is between 60% and 90%, and if the MTTFd of each channel is between 10 and 30 years, then according to Figure 133, PL_d is achieved.

Other factors must also be realized to satisfy the required PL. These requirements include the provisions already discussed such as for common cause failures, systematic failure, and mission time.

If the PFH_D of the system or subsystem is known, Table 12 (Annex K of the standard) can be used to derive the PL.

System Design According to EN ISO 13849 and SISTEMA

$MTTF_d$ for each channel	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)															
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL		
Years	DC_{avg} = none		DC_{avg} = none		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = low		DC_{avg} = medium		DC_{avg} = high			
3	$3,80 \times 10^{-5}$	a			$2,58 \times 10^{-5}$	a	$1,99 \times 10^{-5}$	A	$1,26 \times 10^{-5}$	a	$6,09 \times 10^{-6}$	b				
3,3	$3,46 \times 10^{-5}$	a			$2,33 \times 10^{-5}$	a	$1,79 \times 10^{-5}$	A	$1,13 \times 10^{-5}$	a	$5,41 \times 10^{-6}$	b				
3,6	$3,17 \times 10^{-5}$	a			$2,13 \times 10^{-5}$	a	$1,62 \times 10^{-5}$	a	$1,03 \times 10^{-5}$	a	$4,86 \times 10^{-6}$	b				
3,9	$2,93 \times 10^{-5}$	a			$1,95 \times 10^{-5}$	a	$1,48 \times 10^{-5}$	a	$9,37 \times 10^{-6}$	b	$4,40 \times 10^{-6}$	b				
4,3	$2,65 \times 10^{-5}$	a			$1,76 \times 10^{-5}$	a	$1,33 \times 10^{-5}$	a	$8,39 \times 10^{-6}$	b	$3,89 \times 10^{-6}$	b				
4,7	$2,43 \times 10^{-5}$	a			$1,60 \times 10^{-5}$	a	$1,20 \times 10^{-5}$	a	$7,58 \times 10^{-6}$	b	$3,48 \times 10^{-6}$	b				
5,1	$2,24 \times 10^{-5}$	a			$1,47 \times 10^{-5}$	a	$1,10 \times 10^{-5}$	a	$6,91 \times 10^{-6}$	b	$3,15 \times 10^{-6}$	b				
5,6	$2,04 \times 10^{-5}$	a			$1,33 \times 10^{-5}$	a	$9,87 \times 10^{-6}$	b	$6,21 \times 10^{-6}$	b	$2,80 \times 10^{-6}$	c				
6,2	$1,84 \times 10^{-5}$	a			$1,19 \times 10^{-5}$	a	$8,80 \times 10^{-6}$	b	$5,53 \times 10^{-6}$	b	$2,47 \times 10^{-6}$	c				
6,8	$1,68 \times 10^{-5}$	a			$1,08 \times 10^{-5}$	a	$7,93 \times 10^{-6}$	b	$4,98 \times 10^{-6}$	b	$2,20 \times 10^{-6}$	c				
7,5	$1,52 \times 10^{-5}$	a			$9,75 \times 10^{-6}$	b	$7,10 \times 10^{-6}$	b	$4,45 \times 10^{-6}$	b	$1,95 \times 10^{-6}$	c				
8,2	$1,39 \times 10^{-5}$	a			$8,87 \times 10^{-6}$	b	$6,43 \times 10^{-6}$	b	$4,02 \times 10^{-6}$	b	$1,74 \times 10^{-6}$	c				
9,1	$1,25 \times 10^{-5}$	a			$7,94 \times 10^{-6}$	b	$5,71 \times 10^{-6}$	b	$3,57 \times 10^{-6}$	b	$1,53 \times 10^{-6}$	c				
10	$1,14 \times 10^{-5}$	a			$7,18 \times 10^{-6}$	b	$5,14 \times 10^{-6}$	b	$3,21 \times 10^{-6}$	b	$1,36 \times 10^{-6}$	c				
11	$1,04 \times 10^{-5}$	a			$6,44 \times 10^{-6}$	b	$4,53 \times 10^{-6}$	b	$2,81 \times 10^{-6}$	c	$1,18 \times 10^{-6}$	c				
12	$9,51 \times 10^{-6}$	b			$5,84 \times 10^{-6}$	b	$4,04 \times 10^{-6}$	b	$2,49 \times 10^{-6}$	c	$1,04 \times 10^{-6}$	c				
13	$8,78 \times 10^{-6}$	b			$5,33 \times 10^{-6}$	b	$3,64 \times 10^{-6}$	b	$2,23 \times 10^{-6}$	c	$9,21 \times 10^{-7}$	d				
15	$7,61 \times 10^{-6}$	b			$4,53 \times 10^{-6}$	b	$3,01 \times 10^{-6}$	b	$1,82 \times 10^{-6}$	c	$7,44 \times 10^{-7}$	d				
16	$7,31 \times 10^{-6}$	b			$4,21 \times 10^{-6}$	b	$2,77 \times 10^{-6}$	c	$1,67 \times 10^{-6}$	c	$6,76 \times 10^{-7}$	d				
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c	$5,67 \times 10^{-7}$	d				
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c	$4,85 \times 10^{-7}$	d				
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c	$4,21 \times 10^{-7}$	d				
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d	$3,70 \times 10^{-7}$	d				
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d	$3,10 \times 10^{-7}$	d				
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d	$2,65 \times 10^{-7}$	d	$9,54 \times 10^{-8}$	e		
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d	$2,30 \times 10^{-7}$	d	$8,57 \times 10^{-8}$	e		
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d	$2,01 \times 10^{-7}$	d	$7,77 \times 10^{-8}$	e		
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d	$4,53 \times 10^{-7}$	d	$1,78 \times 10^{-7}$	d	$7,11 \times 10^{-8}$	e		
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d	$3,87 \times 10^{-7}$	d	$1,54 \times 10^{-7}$	d	$6,37 \times 10^{-8}$	e		
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$	c	$6,49 \times 10^{-7}$	d	$3,35 \times 10^{-7}$	d	$1,34 \times 10^{-7}$	d	$5,76 \times 10^{-8}$	e		
51			$2,24 \times 10^{-6}$	c	$1,13 \times 10^{-6}$	c	$5,80 \times 10^{-7}$	d	$2,93 \times 10^{-7}$	d	$1,19 \times 10^{-7}$	d	$5,26 \times 10^{-8}$	e		
56			$2,04 \times 10^{-6}$	c	$1,02 \times 10^{-6}$	c	$5,10 \times 10^{-7}$	d	$2,52 \times 10^{-7}$	d	$1,03 \times 10^{-7}$	d	$4,73 \times 10^{-8}$	e		
62			$1,84 \times 10^{-6}$	c	$9,06 \times 10^{-7}$	d	$4,43 \times 10^{-7}$	d	$2,13 \times 10^{-7}$	d	$8,84 \times 10^{-8}$	e	$4,22 \times 10^{-8}$	e		
68			$1,68 \times 10^{-6}$	c	$8,17 \times 10^{-7}$	d	$3,90 \times 10^{-7}$	d	$1,84 \times 10^{-7}$	d	$7,68 \times 10^{-8}$	e	$3,80 \times 10^{-8}$	e		
75			$1,52 \times 10^{-6}$	c	$7,31 \times 10^{-7}$	d	$3,40 \times 10^{-7}$	d	$1,57 \times 10^{-7}$	d	$6,62 \times 10^{-8}$	e	$3,41 \times 10^{-8}$	e		
82			$1,39 \times 10^{-6}$	c	$6,61 \times 10^{-7}$	d	$3,01 \times 10^{-7}$	d	$1,35 \times 10^{-7}$	d	$5,79 \times 10^{-8}$	e	$3,08 \times 10^{-8}$	e		
91			$1,25 \times 10^{-6}$	c	$5,88 \times 10^{-7}$	d	$2,61 \times 10^{-7}$	d	$1,14 \times 10^{-7}$	d	$4,94 \times 10^{-8}$	e	$2,74 \times 10^{-8}$	e		
100			$1,14 \times 10^{-6}$	c	$5,28 \times 10^{-7}$	d	$2,29 \times 10^{-7}$	d	$1,01 \times 10^{-7}$	d	$4,29 \times 10^{-8}$	e	$2,47 \times 10^{-8}$	e		

Table 12: Precise $MTTF_d$ to Determine PL

Source of Table 12 is Table K.1 of ISO/EN 13849-1:2006

Subsystem Design and Combinations

If the PLs of all the subsystem are known, they can be combined simply into a system using Table 13. The rational behind this table is clear. First, that the system can only be as good as its weakest link (subsystem). Second, the more subsystems there are, the greater the possibility for failure.

PL_{low}	N_{low}	PL
a	>3	Not allowed
	=<3	a
b	>2	a
	=<2	b
c	>2	b
	=<2	c
d	>3	c
	=<3	d
e	>3	d
	·3	e

Table 13: PL calculation for series combined subsystems

In the system shown in Figure 135, the lowest Performance Levels are at Subsystems 1 and 2. Both are PLb. Therefore, using Table 13, we can read across b (in the PLlow column), through 2 (in the Nlow column) and find the achieved system PL as b (in the PL column). If all three subsystems were PLb the achieved PL would be PLa.

Note: The application of this table is not mandatory. The use of Annex K of the standard (or SISTEMA) is the preferred method. This table is only intended to provide a very simple approach for small systems.

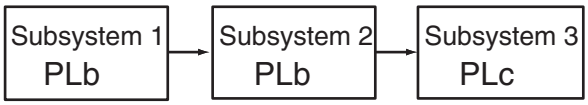


Figure 134: Combination of series subsystems as a PLb system

Validation

Validation plays an important role throughout the safety system development and commissioning process. ISO/EN 13849-2:2003 sets the requirements for validation. It calls for a validation plan and discusses validation by testing and analysis techniques such as Fault Tree Analysis and Failure Modes, Effects and Criticality Analysis. Most of these requirements will apply to the manufacturer of the subsystem rather than the subsystem user.

Machine Commissioning

At the system or machine commissioning stage, validation of the safety functions must be carried out in all operating modes and should cover all normal and foreseeable abnormal conditions. Combinations of inputs and sequences of operation must also be taken into consideration. This procedure is important because it is always necessary to check that the system is suitable for actual operational and environmental characteristics. Some of those characteristics may be different from the ones anticipated at the design stage.

System Design According to IEC/EN 62061

IEC/EN 62061, "Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems," is the machinery specific implementation of IEC/EN 61508. It provides requirements that are applicable to the system level design of all types of machinery safety-related electrical control systems and also for the design of non-complex subsystems or devices.

The risk assessment results in a risk reduction strategy which in turn, identifies the need for safety-related control functions. These functions must be documented and must include:

- Functional requirements specification
- Safety integrity requirements specification

The functional requirements include details like frequency of operation, required response time, operating modes, duty cycles, operating environment, and fault reaction functions. The safety integrity requirements are expressed in levels called safety integrity levels (SIL). Depending on the complexity of the system, some or all of the elements in Table 14 must be considered to determine whether the system design meets the required SIL.

Element for SIL Consideration	Symbol
Probability of Dangerous Failure per Hour	PFH_D
Hardware Fault Tolerance	No Symbol
Safe Failure Fraction	SFF
Proof Test Interval	T_1
Diagnostic Test Interval	T_2
Susceptibility to Common Cause Failures	ß
Diagnostic Coverage	DC

Table 14: Elements for SIL Consideration

Subsystems

The term "subsystem" has a special meaning in IEC/EN 62061. It is the first level subdivision of a system into parts which, if they fail, would cause a failure of the safety function. Therefore if two redundant switches are used in a system neither individual switch is a subsystem. The subsystem would comprise both switches and any associated fault diagnostic function.

Probability of Dangerous Failure per Hour (PFH_D)

IEC/EN 62061 uses the same basic methods as discussed in the section on EN ISO 13849-1 to determine failure rates at the component level. The same provisions and methods apply for "mechanistic" and electronic components. In IEC/EN 62061 there is no consideration of MTTFd in years. The failure rate per hour (λ) is either calculated directly or obtained or derived from the B10 value by the following formula:

$\lambda = 0.1 \times C/B10$ (where C = the number of operating cycles per hour)

There is a significant difference between the standards in the methodology for determining the total PFH_D for a subsystem or system. An analysis of the components must be undertaken to determine the probability of failure of the subsystems. Simplified formulae are provided for the calculation of common subsystem architectures (described later in text). Where these formulae are not appropriate it will be necessary to use more complex calculation methods such as Markov models. The Probability of Dangerous Failure (PFH_D) of each subsystem are then added together to determine the total PFH_D for the system. Table 15 (Table 3 of the standard) can then be used to determine which Safety Integrity Level (SIL) is appropriate to that range of PFH_D.

$\lambda_{DssB} = (1\text{-}ß)2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

The formulae for this architecture take into account the parallel arrangement of the subsystem elements and add the following two elements from Table 14:

ß (Beta) is the susceptibility to common cause failures.

SIL (Safety Integrity Level)	PFH_D (Probability of Dangerous Failure per Hour)
3	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-6} \ldots < 10^{-5}$

Table 15: Probabilities of Dangerous Failure for SILs

The PFH_D data for a subsystem will usually be provided by the manufacturer. Data for Rockwell Automation safety components and systems is available in a number of forms including: http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx

This website will be periodically updated as more data for other Rockwell Automation components and systems will become available over time.

IEC/EN 62061 also makes it clear that reliability data handbooks can be used if and where applicable.

For low complexity electromechanical devices, the failure mechanism is usually linked to the number and frequency of operations rather than just time. Therefore for these components the data will derived from some form of testing (e.g. B10 testing as described in the chapter on EN ISO 13849-1). Application based information such as the anticipated number of operations per year is then required in order to convert the B10d or similar data to PFH_D.

NOTE: In general the following is true (taking into account a factor to change years to hours):

$PFH_D = 1/MTTFd$

However, it is important to understand that, for a dual channel system (with or without diagnostics), it is not correct to use 1/ PFH_D to determine the MTTFd that is required by EN ISO 13849-1. That standard calls for the MTTFd of a single channel. This is a very different value to the MTTFd of the combination of both channels of a two channel subsystem.

Architectural Constraints

The essential characteristic of IEC/EN 62061 is that the safety system is divided into subsystems. The hardware safety integrity level that can be claimed for a subsystem is limited not only by the PFH_D but also by the hardware fault tolerance and the safe failure fraction of the subsystems. Hardware fault tolerance is ability of the system to execute its function in the presence of faults. A fault tolerance of zero means that the function is not performed when a single fault occurs. A fault tolerance of one allows the subsystem to perform its function in the presence of a single fault. Safe Failure Fraction is the portion of the overall failure rate that does not result in a dangerous failure. The combination of these two elements is known as the architectural constraint and its output is the SIL Claim Limit (SIL CL) Table 16 shows the relationship of the architectural constraints to the SILCL. A subsystem (and therefore its system) must satisfy both the PFH_D requirements and the Architectural Constraints together with the other relevant provisions of the standard.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance		
	0	1	2
<60%	Not allowed unless specific exceptions apply	SIL1	SIL2
60%…<90%	SIL1	SIL2	SIL3
90%…<99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

Table 16: Architectural Constraints on SIL

For example, a subsystem architecture that possesses single fault tolerance and has a safe failure fraction of 75% is limited to no higher than a SIL2 rating, regardless of the probability of dangerous failure.

When combining subsystems, the SIL achieved by the SRCS is constrained to be less than or equal to the lowest SIL CL of any of the subsystems involved in the safety-related control function.

System Realization

To compute the probability of dangerous failure, each safety function must be broken down into function blocks, which are then realized as subsystems. A system design implementation of a typical safety function would include a sensing device connected to a logic device connected to an actuator. This creates a series arrangement of subsystems. As we have already seen, if we can determine the probability of dangerous failure for each subsystem and know its SIL CL, then the system probability of failure is easily calculated by adding the probability of failures of the subsystems. This concept is shown in Figure 136.

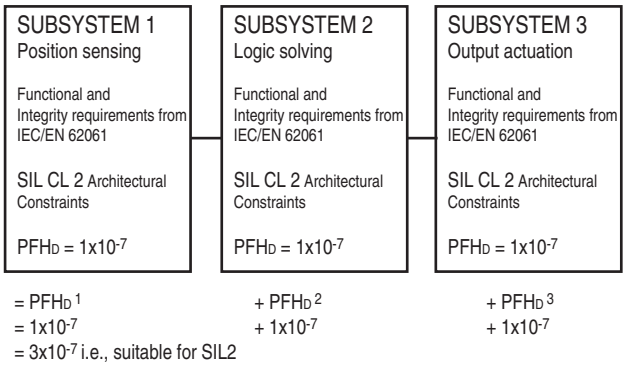


Figure 135: Example combination of subsystems

If, for example, we want to achieve SIL 2, each subsystem must have a SIL CL of at least SIL 2, and the sum of the PFH_D for the system must not exceed the limit allowed in Table 15.

Subsystem Design: IEC/EN 62061

If a system designer uses components ready “packaged” into subsystems according to IEC/EN 62061 life becomes much easier because the specific requirements for the design of subsystems do not apply. These requirements will, in general, be covered by the device (subsystem) manufacturer and are much more complex than those required for system level design.

IEC/EN 62061 requires that complex subsystems such as safety PLCs comply with IEC 61508 or other appropriate standards. This means that, for devices using complex electronic or programmable components, the full rigor of IEC 61508 applies. This can be a very rigorous and involved process. For example, the evaluation of the PFH_D achieved by a complex subsystem can be a very complicated process using techniques such as Markov modeling, reliability block diagrams or fault tree analysis.

IEC/EN 62061 does give requirements for the design of lower complexity subsystems. Typically this would include relatively simple electrical components such as interlock switches and electromechanical safety monitoring relays. The requirements are not as involved as those in IEC 61508 but can still be quite complicated.

IEC/EN 62061 supplies four subsystem logical architectures with accompanying formulae that can be used to evaluate the PFH_D achieved by a low complexity subsystem. These architectures are purely logical representations and should not be thought of as physical architectures. The four subsystem logical architectures with accompanying formulae are shown in Figures 136 through 139.

For a basic subsystem architecture shown in Figure 136, the probabilities of dangerous failures are simply added together.

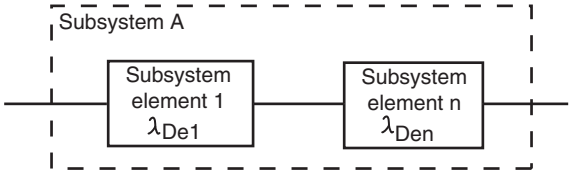


Figure 136: Subsystem logical architecture A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$

$PFH_{DssA} = \lambda_{DssA} \times 1h$

λ, (Lambda) is used to designate the failure rate. The units of the failure rate are failures per hour. λD is the dangerous failure rate. λDssA, is the dangerous failure rate of subsystem A. It is the sum of the failure rates of the individual elements, e1, e2, e3, up to and including en. The probability of dangerous failure is multiplied by 1 hour to create the probability of failure within one hour.

Figure 137 shows a single fault tolerant system without a diagnostic function. When the architecture includes single fault tolerance, the potential for common cause failure exists and must be considered. The derivation of the common cause failure is briefly described later in this section.

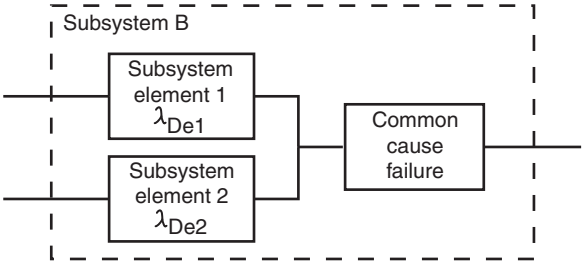


Figure 137: Subsystem logical architecture B

$\lambda_{DssB} = (1-ß)2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

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

The formulae for this architecture take into account the parallel arrangement of the subsystem elements and add the following two elements from Table 14:

ß (Beta) is the susceptibility to common cause failures.

T1 is the proof test interval or lifetime, whichever is smaller. The proof test is designed to detect faults and degradation of the safety subsystem so that the subsystem can be restored to a perfect operating condition. In practical terms this usually means replacement (like the equivalent term “mission time” in EN ISO 13849-1).

Figure 139 shows the functional representation of a zero fault tolerant system with a diagnostic function. Diagnostic coverage is used to decrease the probability of dangerous hardware failures. The diagnostic tests are performed automatically. The definition of diagnostic coverage is the same as given in EN ISO 13849-1 i.e. the ratio of the rate of detected dangerous failures compared to the rate of all dangerous failures.

These formulae include the diagnostic coverage, DC, for each of the subsystem elements. The failure rates of each of the subsystems are reduced by the diagnostic coverage of each subsystem.

The fourth example of a subsystem architecture is shown in Figure 139. This subsystem is single fault tolerant and includes a diagnostic function. The potential for common cause failure must also be considered with single fault tolerant systems.

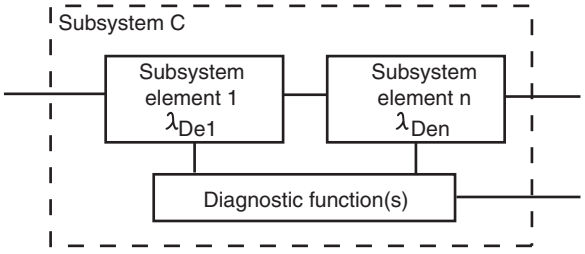


Figure 138: Subsystem logical architecture C

Figure 138 shows the functional representation of a zero fault tolerant system with a diagnostic function. Diagnostic coverage is used to decrease the probability of dangerous hardware failures. The diagnostic tests are performed automatically. The definition of diagnostic coverage is the same as given in EN ISO 13849-1 i.e. the ratio of the rate of detected dangerous failures compared to the rate of all dangerous failures.

These formulae include the diagnostic coverage, DC, for each of the subsystem elements. The failure rates of each of the subsystems are reduced by the diagnostic coverage of each subsystem.

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

$PFH_{DssC} = \lambda_{DssC} \times 1h$

The fourth example of a subsystem architecture is shown in Figure 139 This subsystem is single fault tolerant and includes a diagnostic function. The potential for common cause failure must also be considered with single fault tolerant systems.

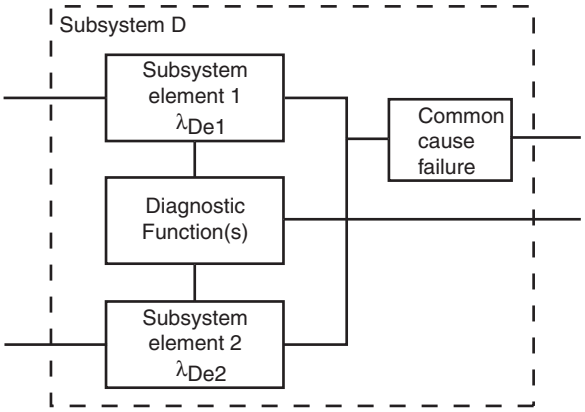


Figure 139: Subsystem logical architecture D

If the subsystem elements are different in each channel, the following formula is used:

$\lambda_{DssD} = (1 - \beta)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2 / 2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1 / 2 \} + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

If the subsystem elements are the same in each channel the following formula is used:

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

$PFH_{DssD} = \lambda_{DssD} \times 1h$

Notice that both formulae use one additional parameter, **T2** the diagnostic test interval. This is just a periodic check of the function. It is a less comprehensive test than the Proof Test.

As an example, assume the following values for the example where the subsystem elements are different:

β = 0.05
$\lambda_{De} = 1 \times 10^{-6}$ failures/hour
T1 = 87600 hours (10 years)
T2 = 2 hours
DC = 90%

PFH_{DssD} = 5.791E-08 dangerous failures per hour. This would be within the range required for SIL 3.

Affect of the Proof Test Interval

IEC/EN 62061 states that a Proof Test Interval (PTI) of 20 years is preferred (but not mandatory) Let us look at the affect the proof test interval has on the system. If we re-calculate the formula with T1 at 20 years it gives the result PFH_{DssD} = 6.581E-08. It is still within the range required for SIL 3. The designer must keep in mind that this subsystem must be combined with other subsystems to calculate the overall dangerous failure rate.

Affect of Common Cause Failure Analysis

Let's look at the affect the common cause failures have on the system. Suppose we take additional measures and our β (Beta) value improves to 1% (0,01), while the proof test interval remains at 20 years. The dangerous failure rate improves to 2.71E-08 which means that the subsystem is now more suitable for use in a SIL 3 system.

Common Cause Failure (CCF)

Common cause failure is when multiple faults resulting from a single cause produce a dangerous failure. Information on CCF will generally only be required by the subsystem designer, usually the manufacturer. It is used as part of the formulae given for estimation of the PFH_D of a subsystem. It will not usually be required at the system design level.

Annex F of IEC/EN62061 provides a simple approach for the estimation of CCF. Table 17 shows a summary of the scoring process.

No.	Measure Against CCF	Score
1	Separation/Segregation	25
2	Diversity	38
3	Design/Application/Experience	2
4	Assessment/Analysis	18
5	Competence/Training	4
6	Environmental	18

Table 17: Scoring for Measures Against Common Cause Failure

Points are awarded for employing specific measures against CCF. The score is added up to determine the common cause failure factor, which is shown in Table 18. The beta factor is used in the subsystem simplified architecture formulae to influence the failure rate as has already been shown.

Overall Score	Common Cause failure factor (ß)
<35	10% (0,1)
35…65	5% (0,05)
65…85	2% (0,02)
85…100	1% (0.01)

Table 18: Beta Factor for Common Cause Failure

Diagnostic Coverage (DC)

Automatic diagnostic tests are employed to decrease the probability of dangerous hardware failures. Being able to detect all dangerous hardware failures would be ideal, but in practice the maximum value is set at 99% (this can also be expressed as 0.99)

Diagnostic coverage is the ratio of the probability of detected dangerous failures to the probability all the dangerous failures.

Probability of Detected dangerous failures, λ_{DD}

$$DC = \frac{\text{Probability of Detected dangerous failures, } \lambda_{DD}}{\text{Probability of Total dangerous failures, } \lambda_{Dtotal}}$$

Hardware Fault Tolerance

Hardware fault tolerance represents the number of faults that can be sustained by a subsystem before it causes a dangerous failure. For example, a hardware fault tolerance of one means that two faults could cause a loss of the safety-related control function but one fault would not.

Management of Functional Safety

The standard gives requirements for the proper control of planning, project management and technical activities that are necessary for the achievement of a safety-related electrical control system.

Proof Test Interval

The proof test interval represents the time after which a subsystem must be either totally checked or replaced to ensure that it is in an "as new" condition. In practice, in the machinery sector, this is achieved by replacement. So the proof test interval is usually the same as lifetime. EN ISO 13849-1 refers to this as Mission Time.

A proof test is a check that can detect faults and degradation in a SRCS so that the SRCS can be restored as close as practical to an "as new" condition. The proof test must detect 100% of all dangerous failures. Separate channels must be tested separately.

In contrast to diagnostic functional tests, which are automatic, proof tests are usually performed manually and off line. Diagnostic functional testing is usually performed often (typically over a few hours) as compared to proof testing which is done infrequently (typically over many years). For example, the circuits going to an interlock switch on a guard can be functionally tested automatically for short and open circuit conditions with diagnostic (e.g., pulse) testing.

The proof test interval must be declared by the manufacturer. Sometimes the manufacturer will provide a range of different proof test intervals.

Safe Failure Fraction (SFF)

The safe failure fraction is similar to diagnostic coverage (DC) but also takes account of any inherent tendency to fail towards a safe state. For example, when a fuse blows, there is a failure but it is highly probable that the failure will be to an open circuit which, in most cases, would be a "safe" failure. SFF is (the sum of the rate of "safe" failures plus the rate of detected dangerous failures) divided by (the sum of the rate of "safe" failures plus the rate of detected and undetected dangerous failures). It is important to realize that the only types of failures to be considered are those which could have some affect on the safety function.

Most low complexity mechanical devices such as E-stop buttons and interlock switches will (on their own) have a relatively low SFF. Most electronic devices for safety have designed in redundancy and monitoring therefore an SFF of greater than 90% is common although this is usually completely due to the Diagnostic Coverage capability.

The SFF value will normally be supplied by the manufacturer.

The Safe Failure Fraction (SFF) can be calculated using the following equation:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_D)$$

where

λ_S = the rate of safe failure,
$\Sigma\lambda_S + \Sigma\lambda_D$ = the overall failure rate,
λ_{DD} = the rate of detected dangerous failure
λ_D = the rate of dangerous failure.

Systematic Failure

The standard has requirements for the control and avoidance of systematic failure. Systematic failures differ from random hardware failures which are failures occurring at a random time, typically resulting from degradation of parts of hardware. Typical types of possible systematic failure are software design errors, hardware design errors, requirement specification errors and other operational procedures. Examples of steps necessary to avoid systematic failure include:

- Proper selection, combination, arrangements, assembly, and installation of components,
- Use of good engineering practice,
- Follow manufacturer's specifications and installation instructions,
- Ensuring compatibility between components,
- Withstanding environmental conditions,
- Use of suitable materials.

Safety-Related Control System Structure Considerations

Overview

This chapter looks at general structural considerations and principles that should be taken into account when designing a safety related control system to any standard. It uses much of language of the Categories from the outgoing EN 954-1 because the Categories primarily address the structure of control systems.

Note: Recent to the time of publication of this text, CEN (European Committee for Standardisation) announced that the final date for presumption of conformity of EN 954-1 will be extended to the end of 2011 to facilitate transition to the later standards. This replaces the original date of December 29, 2009.

For the latest information on the use and status of EN 954-1 visit: *http://discover.rockwellautomation.com/EN_Safety_Solutions.aspx*. In the meantime it is advised that the extension of the transition period is used to move over to the use of the later standards (EN ISO 13849-1 or IEC/EN 62061) in a timely manner.

Categories of Control Systems

The "Categories" of control systems originated in the outgoing EN 954-1:1996 (ISO13849-1:1999). However they are still often used to describe safety control systems and they remain an integral part of EN ISO13849-1 as discussed in "Introduction to Functional Safety of Control Systems" section.

There are five categories describing the fault reaction performance of a safety related control system. See Table 19 for a summary of these categories. The following notes apply to the table.

Note 1: Category B in itself has no special measures for safety but it forms the base for the other categories.

Note 2: Multiple faults caused by a common cause or as inevitable consequences of the first fault shall be counted as a single fault.

Note 3: The fault review may be limited to two faults in combination if it can be justified but complex circuits (e.g. microprocessor circuits) may require more faults in combination to be considered.

Category 1 is aimed at the prevention of faults. It is achieved through the use of suitable design principles, components and materials. Simplicity of principle and design together with stable and predictable material characteristics are the keys to this category.

Categories 2, 3 and 4 require that if faults cannot be prevented they must be detected and appropriate action taken.

Redundancy, diversity and monitoring are the keys to these categories. Redundancy is the duplication of the same technique. Diversity is using two different techniques. Monitoring is the checking the status of devices and then taking appropriate action based on results of the status. The usual, but not only, method of monitoring is to duplicate the safety critical functions and compare operation.

Summary of Requirements	System Behavior
Category B (see Note 1) Safety related parts of machine control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be applied.	When a fault occurs, it can lead to a loss of the safety function.
CATEGORY 1 The requirements of category B apply together with the use of well tried safety components and safety principles.	As described for category B but with higher safety related reliability of the safety related function. (The higher the reliability, the less the likelihood of a fault).
CATEGORY 2 The requirements of category B and the use of well tried safety principles apply. The safety function(s) shall be checked at machine start-up and periodically by the machine control system. If a fault is detected a safe state shall be initiated or if this is not possible a warning shall be given. EN ISO 13849-1 assumes that the test rate is at least 100 times more frequent that the demand rate. EN ISO 13849-1 assumes that the MTTFd of the external test equipment is larger than half of the MTTFd of the functional equipment being tested.	The loss of safety function is detected by the check. The occurrence of a fault can lead to the loss of safety function between the checking intervals.
CATEGORY 3 (see Notes 2 & 3) The requirements of category B and the use of well tried safety principles apply. The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function. Where practicable, a single fault shall be detected.	When the single fault occurs the safety function is always performed. Some but not all faults will be detected. An accumulation of undetected faults can lead to the loss of safety function.
Category 4 (see Notes 2 & 3) The requirements of category B and the use of well tried safety principles apply. The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function. The single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to a loss of safety function.	When the faults occur, the safety function is always performed. The faults will be detected in time to prevent the loss of safety functions.

Table 19: Categories of Safety Performance

Category B

Category B provides the basic requirements of any control system; whether it is a safety related control system or non-safety related. A control system must work in its expected environment. The concept of reliability provides a foundation for control systems, as reliability is defined as the probability that a device will perform its intended function for a specified interval under expected conditions.

Category B requires the application of basic safety principles. ISO 13849-2 tells us the basic safety principles for electrical, pneumatic, hydraulic and mechanical systems. The electrical principles are summarized as follows:

- Proper selection, combination, arrangements, assembly and installation (i.e., per manufacturer's instructions)
- Compatibility of components with voltages and currents
- Withstand environmental conditions
- Use of de-energization principle
- Transient suppression
- Reduction of response time
- Protection against unexpected start-up
- Secure fixing of input devices (e.g. mounting of interlocks)
- Protection of control circuit (per NFPA79 & IEC60204-1)
- Correct protective bonding

The designer must select, install, and assemble according to the manufacturer's instructions. These devices must work within the expected voltage and current ratings. The expected environmental conditions, like electromagnetic compatibility, vibration, shock, contamination, washdown, must also be considered. The de-energization principle is used. Transient protection is installed across the contactor coils. The motor is protected against overloads. The wiring and grounding meets the appropriate electrical standards.

Category 1

Category 1 requires the system to meet the terms of Category B and, in addition, to use well-tried components. EN ISO 13849-2 gives information about well tried components for mechanical, hydraulic, pneumatic and electrical systems. Annex D addresses electrical components.

Components are considered to be well-tried if they have been successfully used in many similar applications. Newly designed safety components are considered to be well-tried if they are designed and verified in compliance to appropriate standards. Table 20 lists some electrical components and their respective standards.

Well-Tried Component	Standard
Switch with positive mode actuation (direct opening action)	IEC 60947-5-1
Emergency stop device	ISO 13850, IEC60947-5-5
Fuse	IEC 60269-1
Circuit Breaker	IEC 60947-2
Contactors	IIEC 60947-4-1, IEC 60947-5-1
Mechanically linked contacts	IEC 60947-5-1
Auxiliary contactor (e. g. contactor, control relay, positive guided relays)	EN 50205 IEC 60204–1, IEC 60947–5–1
Transformer	IEC 60742
Cable	IEC 60204-1
Interlocks	ISO 14119
Temperature Switch	IEC 60947-5-1
Pressure Switch	IEC 60947-5-1 + pneumatic or hydraulic requirements
Control and protective switching device or equipment (CPS)	IEC 60947-6-2
Programmable Logic Controller	IEC 61508

Table 20: Standards for Well-Tried Components

Applying well-tried components to our Category B system, the limit switch would be replaced by a direct opening action tongue switch and the contactor would be over-dimensioned to further protect against welded contacts.

Figure 140 shows the changes to the simple Category B system to achieve Category 1. The interlock and the contactor play the key roles in removing energy from the actuator, when access to the hazard is needed. The tongue interlock meets the requirements of IEC 60947-5-1 for direct opening action contacts, which is shown by the symbol of the arrow within the circle. With the well-tried components, the probability of energy being removed is higher for Category 1 than it is for Category B. The use of well-tried components is intended to prevent a loss of the safety function. Even with these improvements, a single fault can still lead to the loss of the safety function.

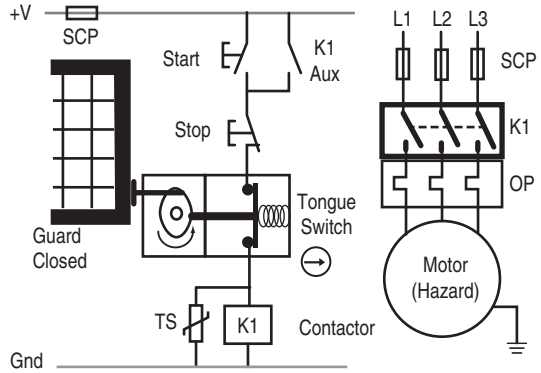


Figure 140: Category 1 of Simple Safety System

Categories B and 1 are prevention based. The design is intended to prevent a hazardous situation. When prevention by itself does not provide enough reduction in the risk, fault detection must be used. Categories 2, 3 and 4 are fault detection based, with increasingly stringent requirements to achieve higher levels of risk reduction.

Category 2

In addition to meeting the requirements of Category B and using well tried safety principles, the safety system must undergo testing to meet Category 2. The tests must be designed to detect faults within the safety related parts of the control system. If faults are not detected, the machine is allowed to run. If faults are detected, the test must initiate a command to bring the machine to a safe state.

Figure 141 shows a block diagram of a Category 2 system. The equipment performing the test can be an integral part of the safety system or a separate piece of equipment.

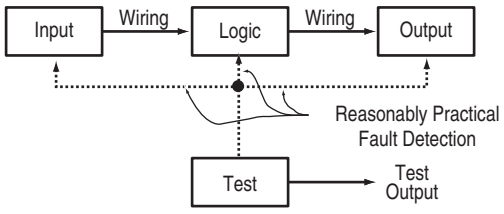


Figure 141: Category 2 Block Diagram

The testing must be performed:

- When the machine is initially powered,
- Prior to the initiation of a hazard, and
- Periodically if deemed necessary by the risk assessment.

Note: EN ISO 138491-1 assumes a test to safety function demand ration of 100:1. The example given here would not meet that requirement.

The words “whenever possible” and “reasonably practicable” indicate that not all faults are detectable. Since this is a single channel system (i.e., one wire connects input to logic to output), a single fault may lead to the loss of the safety function. In some cases, Category 2 cannot be fully applied to a safety system, because not all of the components can be checked.

Figure 140 shows the simple Category 1 system enhanced to meet Category 2. A monitoring safety relay (MSR) performs the testing. Upon power-up, the MSR checks its internal components. If no faults are detected, the MSR checks the tongue switch by monitoring the cycling of its contacts. If no faults are detected and the guard is closed, the MSR then checks the output device: the mechanically linked contacts of the contactor. If no faults are detected and the contactor is off, the MSR will energize its internal output and connect the coil of K1 to the Stop button. At this point, the non safety rated parts of the machine control system, the Start/Stop/Interlock circuit, can turn the machine on and off.

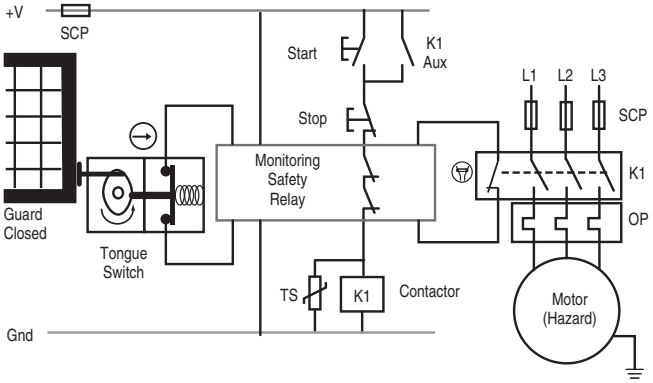


Figure 142: Category 2 Safety System

Opening the guard turns the outputs of the MSR off. When the guard is re-closed, the MSR repeats the safety system checks. If no faults are discovered, the MSR turn on is internal output. The MSR allows this circuit to meet Category 2 by performing tests on the input device, the logic device (itself) and the output device. The test is performed on initial power-up and before initiation of the hazard.

With its inherent logic capabilities, a Safety PLC (PLC safety-rated to IEC 61508) based safety system can be designed to meet category 2.

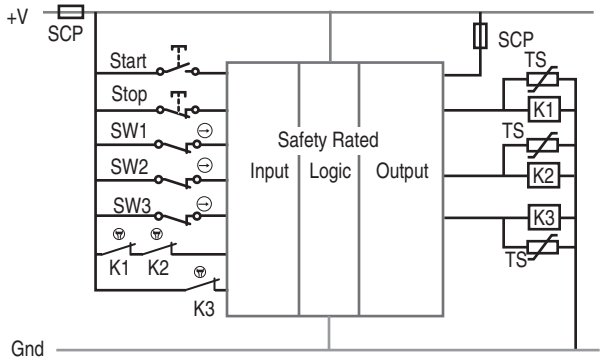


Figure 143: Complex Category 2 Safety System

Safety-Related Control System Structure Considerations

Figure 143 shows an example of a complex system using a safety rated PLC. A safety rated PLC meets the requirements of well-tried as it is designed to an appropriate standard. The mechanically linked contacts of the contactors are fed into the Input of the PLC for testing purposes. These contacts may be connected in series to one input terminal or to individual input terminals, depending on the program logic.

Although well-tried safety components are used, a single fault occurring between the checks can lead to the loss of the safety function. Therefore, Category 2 systems are used in lower risk applications. When higher levels of fault tolerance are needed, the safety system must meet Categories 3 or 4.

Category 3

In addition to meeting the requirements of Category B and well-tried safety principles, Category 3 requires successful performance of the safety function in the presence of a single fault. The fault must be detected at or before the next demand on the safety function, whenever reasonably practicable.

Here again we have the phrase “whenever reasonably practicable.” This covers those faults that may not be detected. As long as the undetectable fault does not lead to the loss of the safety function, the safety function can meet category 3. Consequently, an accumulation of undetected faults can lead to the loss of the safety function.

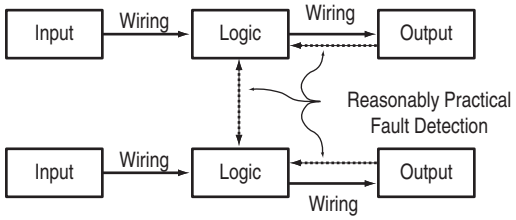


Figure 144: Category 3 Block Diagram

Figure 144 shows a block diagram to explain the principles of a Category 3 system. Redundancy combined with reasonably practicable cross monitoring and output monitoring are used to ensure the performance of the safety function

Figure 145 shows an example of a Category 3 system. A redundant set of contacts are added to the tongue interlock switch. Internally, the monitoring safety relay (MSR) contains redundant circuits that cross monitor each other. A redundant set of contactors remove power from the motor. The contactors are monitored by the MSR through the “reasonably practicable” mechanically linked contacts.

Fault detection must be considered for each part of the safety system, as well as the connections (i.e., the system). What are the failure modes of a dual channel tongue switch? What are the failure modes of the MSR? What are the failure modes of the contactors K1 and K2? What are the failure modes of the wiring?

The tongue interlock switch is designed with direct opening contacts. Therefore we know that opening the guard is designed to open a welded contact. This resolves one failure mode. Do other failure modes exist?

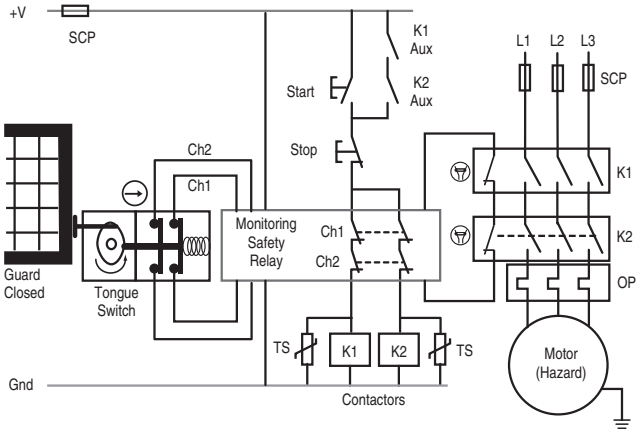


Figure 145: Category 3 System

The direct opening action switch is usually designed with a spring operate return. If the head is removed or broken off, the safety contacts spring back to the closed (safe) state. Many interlock switches are designed with removable heads to accommodate installation requirements of various applications. The head can be removed and rotated between two to four positions.

A failure could occur where the head mounting screws are not torqued properly. With this condition, the expected vibration of the machine may cause the head mounting screws to back out. The operating head, under spring pressure, removes the pressure from the safety contacts, and the safety contacts close. Subsequently, opening the guard does not open the safety contacts, and a failure to danger occurs.

Similarly, the operating mechanism within the switch must be reviewed. What is the probability that a failure of a single component will lead to the loss of the safety function? A common practice is to use tongue interlocks with dual contacts in Category 3 circuits. This usage must be based on excluding the single failure of the switch to open the safety contacts. This is considered “fault exclusion” and is discussed later in this chapter.

A monitoring safety relay (MSR) is often evaluated by a third party and assigned a category level (and/or a PL and SIL CL). The MSR often includes dual channel capability, cross channel monitoring, external device monitoring and short circuit protection. No specific standards are written to provide guidance on the design or usage of monitoring safety relays. MSRs are evaluated for their ability to perform the safety function per EN ISO 13849-1 or the outgoing EN 954-1. The rating of the MSR must be the same or higher than the required rating of the system in which it is used.

Two contactors help to ensure that the safety function is fulfilled by the output devices. With overload and short-circuit protection, the probability of the contactor failing with welded contacts is small but not impossible. A contactor can also fail due with its power switching contacts staying closed due to a stuck armature. If one contactor fails to a dangerous state, the second contactor will remove power from the hazard. The MSR will detect the faulted contactor upon the next machine cycle. When the gate is closed and the start button pressed, the mechanically linked contacts of the faulted contactor will remain open and the MSR will not be able to close its safety contacts, thereby, revealing the fault.

Undetected Faults

With a Category 3 system structure there may be some faults that cannot be detected but they must not, by themselves, lead to the loss of the safety function.

Where faults can be detected we need to know if, under some circumstances, they could be either masked or unintentionally cleared by the operation other devices within the system structure.

Figure 146 shows a widely used approach for connecting multiple devices to a monitoring safety relay. Each device contains two normally closed direct opening action contacts. These devices can be a mix of interlocks or e-stop buttons. This approach saves wiring costs as the input devices are daisy-chained. Assume a short circuit fault occurs across one of the contacts at Sw2 as shown. Can this fault be detected?

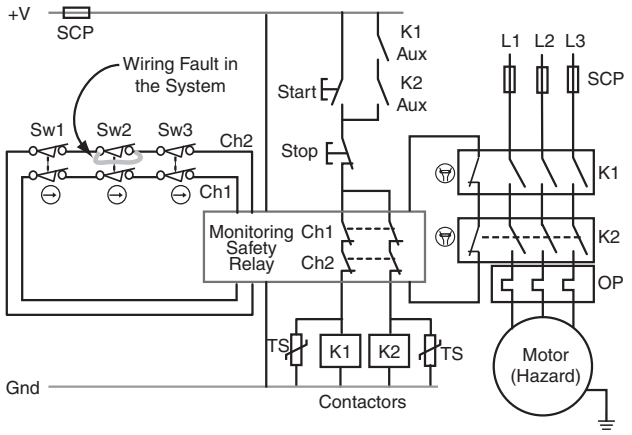


Figure 146: Series Connection of Inputs Devices

If switch Sw1 (or Sw3) is opened, both Ch1 and Ch2 are open circuit and the MSR removes power from the hazard. If Sw3 is then opened and then closed again the fault across its contacts will not be detected because there is no change of status at the MSR: both Ch1 and Ch2 remain open. If Sw1 (or Sw3) is then closed, the hazard can be restarted by pressing the start button. Under these circumstances the fault did not cause a loss of the safety function but it was not detected, it remains in the system and a subsequent fault (a short circuit across the second contact of Sw2) could lead to the loss of the safety function.

If Sw2 alone was opened and closed, with no operation of the other switches, Ch1 opens and Ch2 remains closed. The MSR de-energizes the hazard because Ch1 opened. When Sw2 closes, the motor cannot be started when the Start button is pressed, because Ch2 did not open. The fault is detected. However if for any reason, Sw1 (or Sw3) is then opened and closed, both Ch1 and Ch2 will be open then closed circuit. This sequence simulates the clearing of the fault and will result in unintentional reset at the MSR.

This raises the question of what DC could be claimed for the individual switches within this structure when using EN ISO 13849-1 or IEC 62061. At the time of publication of this text there is no specific definitive guidance on this but it is usual and reasonable to assume a DC of 60% under the condition that the switches are individually tested at suitable periods to reveal faults. If it is foreseeable that one (or more) of the switches will never be individually tested then it can be argued that its DC should be described as zero. At the time of publication of this text EN ISO 13849-2 is undergoing revision. When it is published it may provide more guidance on this issue.

The series connection of mechanical contacts is limited to Category 3 as it may lead to the loss of the safety function due to an accumulation of faults. In practical terms, the reduction of the DC (and therefore SFF) would limit the maximum achievable PL and SIL to PLd and SIL2.

It is interesting to note that these characteristics of a Category 3 structure have always required consideration but they are brought into sharp focus by the newer functional safety standards.

Figure 147 shows a category 3 circuit using a safety rated variable frequency drive. Recent developments in drive technology coupled with the updating of EN/IEC 60204-1 and NFPA79 standards allow safety rated drives to be used in e-stop circuits without the need for an electro-mechanical disconnect of the actuator (e.g., the motor).

Pressing the E-Stop opens the outputs of the MSR. This sends a stop signal to the drive, removes the enable signal and opens the gate control power. The drive executes a Category 0 Stop—immediate removal of power to the motor. This function is termed “Safe Torque Off.” The drive achieves category 3 because it has redundant signals to remove power to the motor: the enable and a positive guided relay. The positive guided relay provides reasonably practicable feedback to the actuator. The drive itself is analyzed to determine that a single fault does not lead to the loss of the safety function.

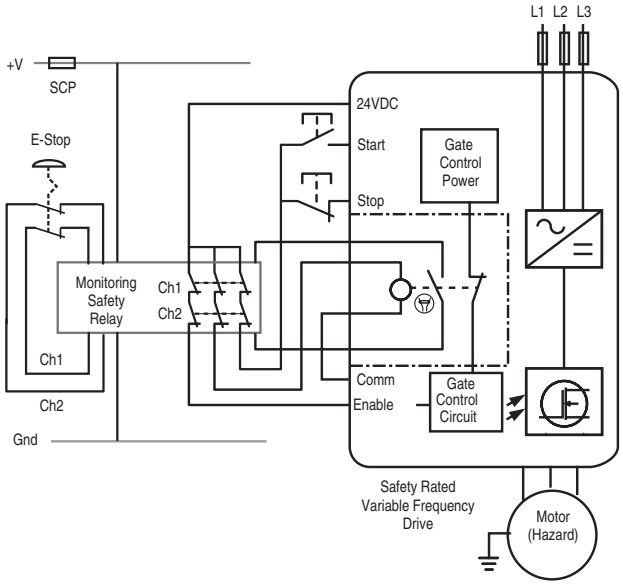


Figure 147: Safety Rated Drives with E-stop Rated to Category 3

Figure 148 shows an example of a wiring fault, a short circuit, from the MSR Channel 2 safety output to the coil of Contactor K1. All components are operating properly. This wiring fault can occur prior to machine commissioning or at some later date during maintenance or enhancements. Can this fault be detected?

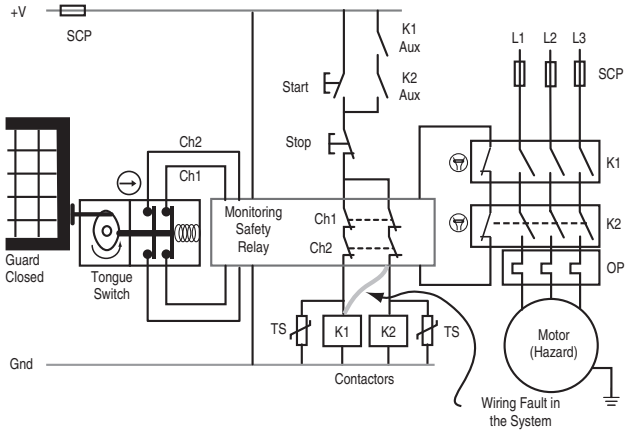


Figure 148: Example 1 of Wiring Fault

This fault cannot be detected by the safety system as shown. Fortunately it does not, on its own, lead to the loss of the safety function. This fault, as well as the fault from Ch1 to K2, must be detected during commissioning or checks following maintenance work. The list of possible fault exclusions given in EN ISO 13849-2 Annex D Table D4 clarifies that these types of faults can be excluded if the equipment is contained within an electrical enclosure and both the enclosure and wiring comply with the requirements of IEC/EN 60204-1. The Joint Technical report on EN ISO 13849-1 and IEC 62061 also clarifies that this fault exclusion can be considered up to and including PLe and SIL3. It can also be used at Category 4.

Figure 149 shows another wiring fault example. This fault occurs from the mechanically linked contact of K2 to the monitoring input of the MSR. Can this fault be detected?

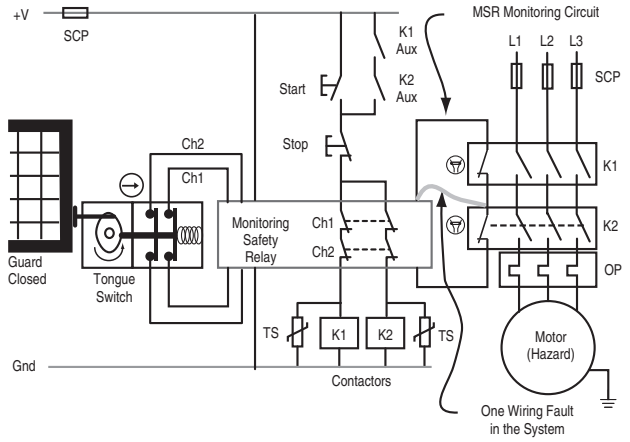


Figure 149 Monitored Manual Reset to Detect Fault

This fault cannot be detected by the safety system, as shown. The MSR monitoring circuit is a series circuit that must be closed prior to startup. As long as the circuit is closed, the MSR believes all monitored devices are in the off state and ready to go. In this example, a welded or stuck K1 contactor will not be detected; it will be masked by the short circuit fault. With two contactors, the safety function is performed by K2, if K1 is indeed faulted. An MSR with monitored manual reset could be substituted for the MSR with automatic reset to detect this type of fault. This type of MSR requires a change of state in terms of a rising or falling signal edge as discussed in the next example and also in the "Protective Measures and Complimentary Equipment" section.

Figure 150 shows the same situation as 149, except the monitoring circuit of the MSR has changed function from automatic to monitored manual. This is accomplished in the MSR by wiring changes or model changes. The monitored manual reset can detect this type of fault because the monitoring circuit must be open at the time that the guard is closed. After closing the guard, the reset button must be pressed. In many (but not all) relays, the MSR outputs energize when the reset button is released. This requirement for a change of state means that the relay cannot be "fooled" into reset by a permanent blocking down of the reset button or unintentionally reset by a short circuit fault.

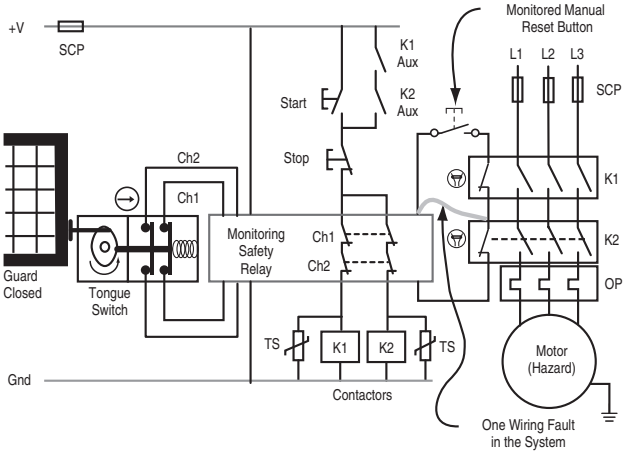


Figure 150: Monitored Manual Reset to Detect Fault

Figure 151 shows a cross channel input fault. A fault occurs from Channel 1 to Channel 2 at the input of the MSR. With eight connections for the two channels, there are numerous potential ways to create the cross channel fault. Can this fault be detected?

Detection of this fault is dependent upon the type of MSR. Microprocessor based MSRs use pulse testing fault detection techniques (see later explanation) and some MSRs utilize diverse inputs. One input is pulled up to +V, and the second input is pulled down to ground. In either case this wiring short will be detected immediately, and the safety input of the MSR will turn off, removing energy from the hazard.

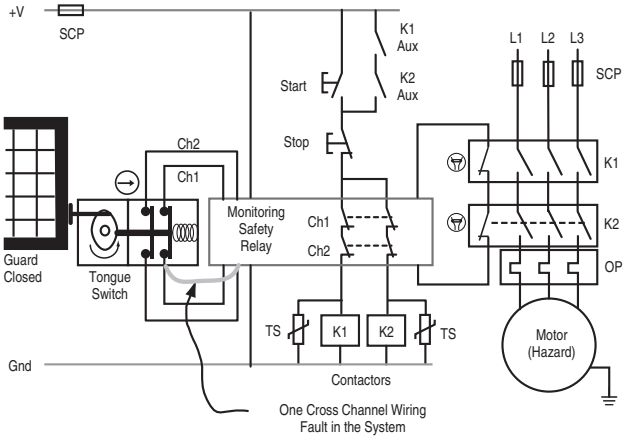


Figure 151: Cross Channel Input Fault

Pulse Testing Fault Detection

Safety circuits are designed to be carrying current when the safety system is active and the hazard is protected. Pulse testing is a technique where the circuit current drops to zero for a very short duration. The duration is too short for the safety circuit to respond and turn the hazard off, but is long enough for a microprocessor based system to detect. The pulses on the channels are offset from each other. If a cross fault short circuit occurs, the microprocessor detects the pulses on both channels and initiates a command to turn the hazard off.

Figure 152 illustrates this principle. This technique also detects shorts to the +V supply. Microprocessor based safety monitoring relays and safety PLC based systems use the pulse testing technique.

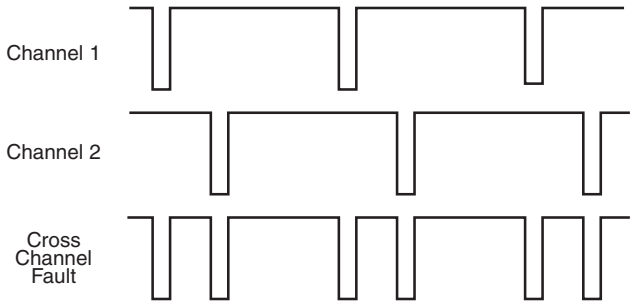


Figure 152: Cross Channel Fault with Pulse Testing

Figure 153 shows an arrangement where two outputs of the PLC are configured for pulse testing. Alternating pulses are connected to each channel operated by mechanical switches. This approach detects cross channel faults as well as faults to power and ground. This pulse testing is required by Category 3 because it is reasonably practicable to detect cross channel faults in this manner.

The faults described above are only a subset of all the faults that must be considered. Short circuits to +V, to Ground, shorts to other circuits, and open circuit conditions must be evaluated. In addition, the component ratings and performance must be considered.

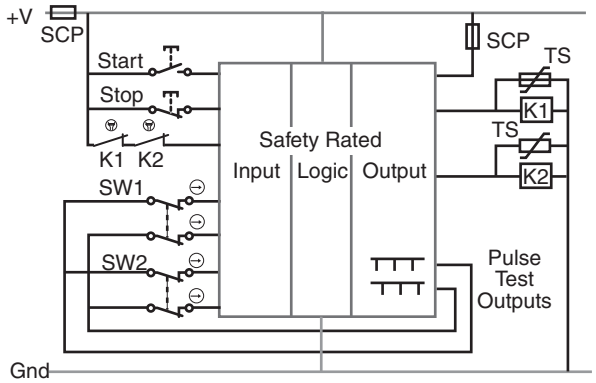


Figure 153: Safety PLC using Pulse Testing for Fault Detection

Figure 154 shows a variation of a Safety PLC arrangement. In some cases, connecting a non-safety rated device to a safety system is needed and beneficial. If the outputs are sourcing type, they can be connected directly to the input of the safety PLC. If they are dual channel, they can be considered to meet Category 3 reasonable requirements.

Another consideration for Safety PLC modules is the number of inputs. Occasionally, one or two additional inputs may be needed, but panel space does not allow for an additional block. In this case, input devices may be connected in series (e.g., SW1 and SW2) and still meet the requirements of Category 3. The tradeoff is the loss of information as to which switch is actuated, unless an additional contact is used and connected to the machine control system.

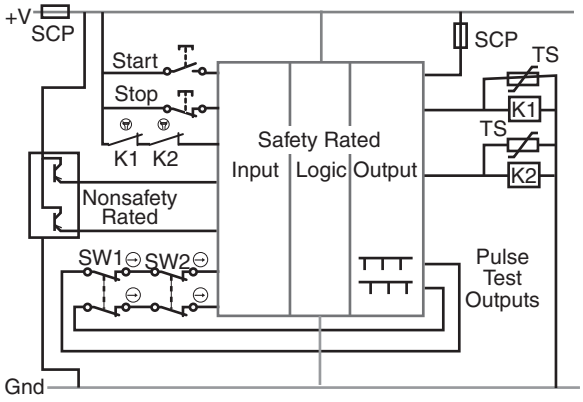


Figure 154: Complex Inputs Meeting Category 3 with a Safety PLC

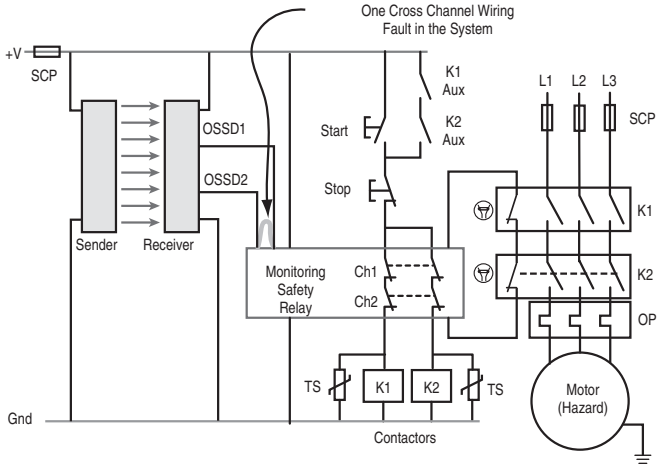


Figure 155: Cross Channel Wiring Fault with Light Curtains

Figure 155 shows an example safety system with light curtains (solid state OSSD outputs).

In this example, the wiring fault is detected by the pulse testing at the light curtain. The detection of the fault is immediate, and the light curtain turns off its output.

Category 4

Like Category 3, Category 4 requires the safety system to meet Category B, use safety principles and perform the safety function in the presence of a single fault. Unlike Category 3 where an accumulation of faults can lead to the loss of the safety function, Category 4 requires performance of the safety function in the presence of an accumulation of faults. In practice the consideration of two accumulated faults may be sufficient, although 3 faults may be necessary for some designs due to complexity.

Figure 156 shows the block diagram for Category 4. Monitoring of both output devices and cross monitoring is essentially required, not just when reasonably practicable. This helps differentiate Category 4 from Category 3.

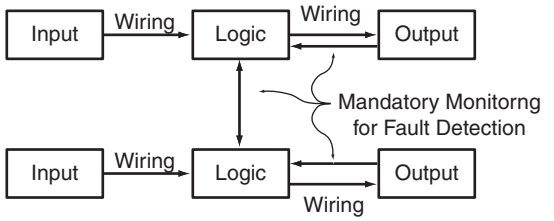


Figure 156: Category 4 Block Diagram

Figure 157 shows an example Category 4 circuit using a two channel non-contact interlock switch.

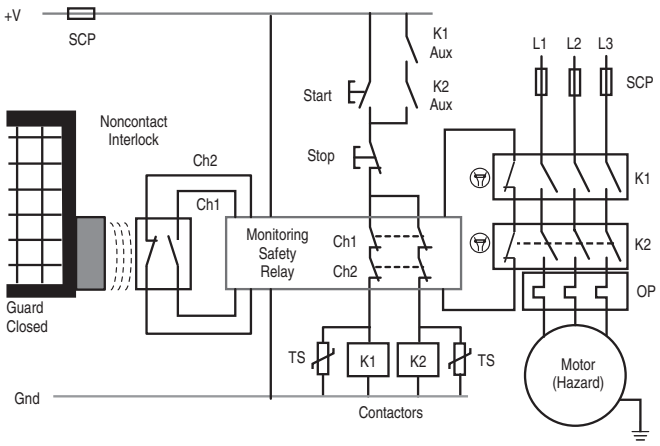


Figure 157: Non-contact Interlock Category 4 System

Up until relatively recently, tongue actuated interlock switches have sometimes been used for Category 4 circuits. In order to use a tongue interlock in a dual channel circuit it is necessary to exclude the possible single fault failure points on the mechanical actuation tongue and switch linkage. However, the Joint Technical Report on EN ISO 13849-1 and IEC 62061 has clarified that this type of fault exclusion should not be used in PLe or SIL 3 systems.

If the safety system designer prefers using tongue style interlocks, then two switches can be used to meet Category 4. Figure 158 shows an example with two tongue interlock switches with direct opening action contacts.

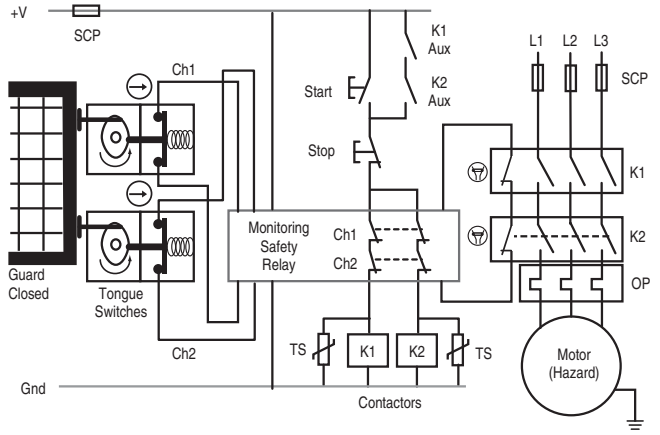


Figure 158: Category 4 with Redundant Tongue Interlocks

The Monitoring safety relay itself must be rated to meet Category 4, and both output contactors, using mechanically linked contacts, must be monitored.

Figure 159 shows a modular monitoring safety relay with one non-contact switch device connected to each input module. If the safety relay is rated for category 4, this arrangement of input devices meets Category 4. Notice that with the modular approach, the safety relay is microprocessor based and utilizes pulse checking to detect cross faults.

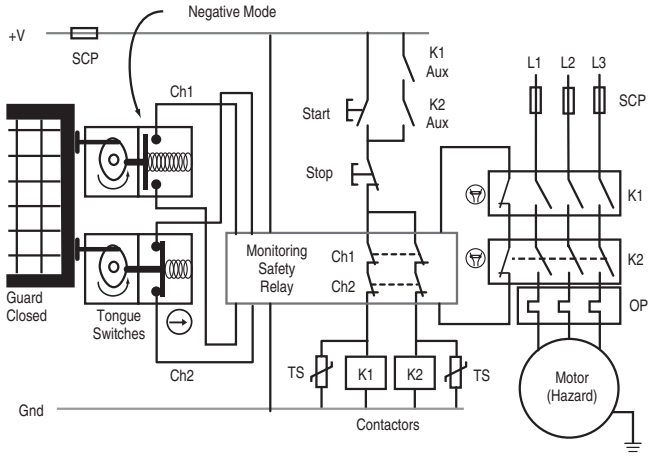


Figure 159: Modular Safety Relay Category 4 System

Component and System Ratings

Categories can be used as part of safety component (device) ratings as well as system ratings. This generates some confusion that can be clarified by understanding the components and their capabilities. By studying the preceding examples we find that a component such as an interlock switch rated to Category 1 can be used on its own in a Category 1 system, and it can be used in a Category 2 system if additional function monitoring is provided. It can also form part of a Category 3 or 4 system if two of the components are used together with a diagnostic function provided by a monitoring safety relay

Some components such as monitoring safety relays and programmable safety controllers have their own internal diagnostics and they check themselves to ensure proper performance. Therefore they can be rated as safety components to meet Categories 2, 3 or 4 without any additional measures.

Fault Considerations

Safety analysis requires extensive analysis of faults, and a thorough understanding of the performance of the safety system in the presence of faults is needed. ISO 13849-1 and ISO 13849-2 provide details on fault considerations and fault exclusions.

If a fault results in a failure of a subsequent component, the first fault and all the subsequent faults shall be considered one fault.

If two or more faults occur as a result of a single cause, the faults shall be considered a single fault. This is known as a common cause fault.

The occurrence of two or more faults at the same time is considered to be highly unlikely and is not considered in this analysis. There is a basic assumption is that only one fault will occur between demands placed on the safety function providing that the periods between the use of the function are not excessively long

Fault Exclusions

The outgoing EN 954-1, and the more recent EN ISO 13849-1 and IEC 62061 all permit the use of fault exclusions when determining a safety system classification if it can be shown that the occurrence of the fault is extremely unlikely. It is important that where fault exclusions are used that they are properly justified and are valid for the intended lifetime of the safety system. The greater the level of risk protected by the safety system then the more stringent becomes the justification required for the fault exclusion. This has always caused some confusion about when certain types of fault exclusion can or cannot be used. As we have seen already in this chapter, recent standards and guidance documents have clarified some aspects of this issue.

In general, where PLe or SIL3 is specified for a safety function to be implemented by a safety system it is not normal to rely upon fault exclusions alone to achieve this level of performance. This is dependent upon the technology used and the intended operating environment. Therefore it is essential that designer takes additional care on the use of fault exclusions as that PL or SIL increases. For example fault exclusion is not applicable to the mechanical aspects of electromechanical position switches and manually operated switches (e.g. an emergency stop device) in order to achieve a PLe or SIL3 system. Those fault exclusions that can be applied to specific mechanical fault conditions (e.g. wear/corrosion, fracture) are described in Table A.4 of ISO 13849-2. Therefore a guard interlocking system that has to achieve PLe or SIL3 will need to incorporate a minimum fault tolerance of 1 (e.g. two conventional mechanical position switches) in order to achieve this level of performance since it is not normally justifiable to exclude faults, such as, broken switch actuators. However, it may be acceptable to exclude faults, such as short circuit of wiring within a control panel designed in accordance with relevant standards.

Further information on the use of fault exclusions will be provided in the forthcoming revision of EN ISO 13849-2.

Stop Categories according to IEC/EN 60204-1 and NFPA 79

It is both unfortunate and confusing that the term “Category” in relation to safety related control systems has two different meanings. So far we have discussed the categories that originated in EN 954-1. They are a classification of the performance of a safety system under fault conditions.

There is also a classification known as “Stop Categories” that originated in IEC/EN 60204-1 and NFPA 79 There are three Stop Categories.

Stop Category 0 requires immediate removal of power to the actuators. This is sometimes considered as an uncontrolled stop because, in some circumstances, motion can take some time to cease because the motor may be free to coast to a stop.

Stop Category 1 requires that power is retained to apply braking until the stop is achieved and then remove power to the actuator.

Stop Category 2 allows that power need not be removed from the actuator.

Note that only Stop Categories 0 or 1 can be used as emergency stops. The choice of which of the two Categories to use should be dictated by a risk assessment.

All the circuit examples shown so far in this chapter have used a Stop Category 0. A Stop Category 1 is achieved with a time-delayed output for the final removal of power. An interlocked guard with guardlocking often accompanies a Category 1 stop system. This keeps the guard locked in a closed position until the machine has reached a safe (i.e., stopped) state.

Stopping a machine without taking proper account of the programmable controller may affect restarting and could result in severe tool and machine damage. A standard (non safety) PLC alone cannot be relied on for a safety related stopping task; therefore, other approaches need to be considered.

Two possible solutions are given below:

1. Safety Relay with Time Delayed Override Command

Figure 160 shows a hard wired system that has allows a correctly sequenced shut-down which protects the machine and program.

A safety relay with both immediate acting and delayed action outputs is used (e.g. MSR138DP). The immediate acting outputs are connected to inputs at the programmable device (e.g., PLC.) and the delayed acting outputs are connected to the contactor. When the guard interlock switch is actuated, the immediate outputs on the safety relay switch. This signals the programmable system to carry out a correctly sequenced stop. After short but sufficient time has elapsed to allow this process, the delayed output on the safety relay switches and isolates the main contactor.

Note: Any calculations to determine the overall stopping time must take the safety relay output delay period into account. This is particularly important when using this factor to determine the positioning of devices in accordance with the safety distance calculation.

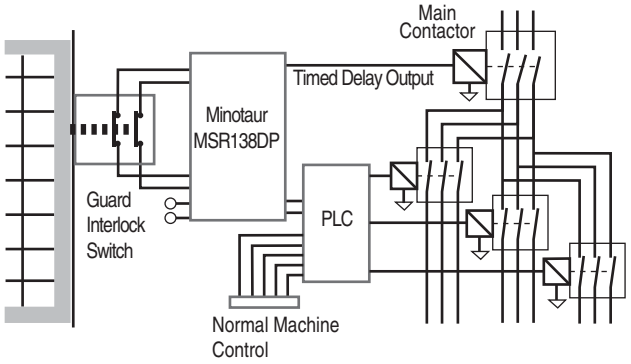


Figure 160: Delayed Outputs for Orderly Shutdown

2. Safety PLCs

The logic and timing functions required can be conveniently implemented by using a (safety) PLC with an appropriate safety integrity level. In practice this would be achieved by using a Safety PLC such as the SmartGuard or GuardLogix.

Safety-Related Control System Structure Considerations

U.S. Safety Control System Requirements

In the U.S., safety related control system requirements can be found in a number of different standards but two documents stand out: ANSI B11.TR3 and ANSI R15.06.

The technical report ANSI B11.TR3 sets out four levels characterized by the expected amount of risk reduction that each can provide: The requirements for each level follows.

Lowest

In ANSI B11.TR3, safeguards providing the lowest degree of risk reduction include electrical, electronic, hydraulic or pneumatic devices and associated control systems using a single-channel configuration. Implicit in the requirements is the requirement to use safety rated devices. This is closely aligned with Category 1 of ISO13849-1.

Low/Intermediate Risk Reduction

Safeguards, in ANSI B11.TR3 providing low/intermediate risk reduction include control systems having redundancy that may be manually checked to verify the performance of the safety system. Looking at the pure requirements, the system employs simple redundancy. Use of a checking function is not required. Without checking, one of the redundant safety components can fail, and the safety system would not realize it. This would result in a single channel system. This level of risk reduction aligns best with Category 2 when checking is used.

High/Intermediate Risk Reduction

Safeguards providing high/intermediate risk reduction in ANSI B11.TR3 include control systems having redundancy with self-checking upon startup to confirm the performance of the safety system. For machines that are started every day, the self-checking provides a significant improvement in the safety integrity over the purely redundant system. For machines running 24/7, the self-checking is a marginal improvement, at best. Employing periodic monitoring of the safety system aligns the requirements with Category 3.

Highest Degree of Risk Reduction

ANSI B11.TR3 provides a highest risk reduction by control systems having redundancy with continuous self-checking. The self checking must verify the performance of the safety system. The challenge to the safety system designer is to determine what is continuous. Many safety systems perform their checks at startup and when a demand is placed on the safety system.

Some components, on the other hand, perform continuous self-checking. Light curtains, for example, sequentially turn on and off their LEDs. If a fault occurs, the light curtain turns off its outputs, before a demand is place on the safety system, as it continuously checks itself. Microprocessor based relays and safety PLCs are other components that perform continuous self-checking.

The control system requirement for “continuous” self checking is not intended to limit the selection of components to light curtains and microprocessor based logic units. The checking should be performed at startup and after every demand on the safety system. This level of risk reduction is intended to align with Category 4 of ISO13849-1.

Robot Standards: U.S. and Canada

The robot standards in the U.S. (ANSI RIA R15.06) and Canada (CSA Z434-03) are quite similar. Both have four levels, which are similar to the categories of EN954-1:1996 and which are described below.

Simple

At this lowest level, simple safety control systems must be designed and constructed with accepted single channel circuitry, and these systems may be programmable.

In Canada, this level is further restricted for signaling and annunciation purposes only.

The challenge for the safety system designer is to determine what is “accepted”. What is an accepted single channel circuit? To whom is the system acceptable?

The simple category is most closely aligned with Category B of EN954-1:1996.

Single Channel

The next level is a single channel safety control system that:

- Is hardware based or is a safety rated software/firmware device
- Includes components that are safety rated; and
- Is used in accordance with manufacturers’ recommendations and
- Uses proven circuit designs.

An example of a proven circuit design is a single channel electromechanical positive break device that signals a stop in a de-energized state.

Being a single channel system, a single component failure can lead to the loss of the safety function.

The simple category most closely aligns with Category 1 of EN954-1:1996.

Safety Rated Software/Firmware Device

Although hardware based systems have been the preferred method providing safeguarding of robots, software/firmware devices are becoming a popular choice due to their ability to handle complex systems. Software/firmware devices (safety PLCs or safety controllers) are allowed provided these devices are safety rated. This rating requires that a single safety-related component or firmware failure does not lead to the loss of the safety function. When the fault is detected, subsequent automatic operation of the robot is prevented until the fault is cleared.

To achieve a safety rating, the software/firmware device must be tested to an approved standard by an approved lab. In the U.S., OSHA maintains a list of nationally recognized testing laboratories (NRTL). In Canada, the Standards Council of Canada (SCC) maintains a similar list.

Single Channel with Monitoring

Single channel safety control systems with monitoring must fulfill the requirements for single channel; be safety rated and utilize checking. The check of the safety function(s) must be performed at machine start-up, and periodically during operation. Automatic checking is preferred over manual checking.

The checking operation allows operation if no faults have been detected or generates a stop signal if a fault is detected. A warning must be provided if a hazard remains after cessation of motion. Of course, the check itself must not cause a hazardous situation. After detecting the fault, the robot must remain in a safe state until the fault is corrected.

Single Channel with Monitoring most closely aligns with Category 2 of EN954-1:1996.

Control Reliable

The highest level of risk reduction in the U.S. and Canadian robot standards is achieved by safety related control systems meeting the requirements of Control Reliable. Control reliable safety related control systems are dual channel architectures with monitoring. The stopping function of the robot must not be prevented by any single component failure, including the monitoring function.

The monitoring shall generate a stop command upon detection of a fault. If a hazard remains after motion stops, a warning signal must be provided. The safety system must remain in a safe state until the fault is corrected.

Preferably, the fault is detected at the time of the failure. If this cannot be achieved, then the failure must be detected at the next demand on the safety system.

Common mode failures must be taken into consideration if a significant probability of such a failure can occur.

The Canadian requirements differ from the U.S. requirement by adding two additional requirements. First, the safety related control systems shall be independent of the normal program control systems. Second, the safety system must not be easily defeated or bypassed without detection.

Control reliable systems align with Category 3 and 4 of EN 954-1:1996.

Comments on Control Reliable

The most fundamental aspect of Control Reliable is single fault tolerance. The requirements state how the safety system must respond in the presence of “a single fault,” “any single fault,” or “any single component failure.”

Three very important concepts must considered regarding faults: (1) not all faults are detected, (2) adding the word “component” raises questions about wiring, and (3) wiring is an integral part of the safety system. Wiring faults can result in the loss of a safety function.

The intent of Control Reliability is clearly the performance of the safety function in the presence of a fault. If the fault is detected, then the safety system must execute a safe action, provide notification of the fault, and prevent further operation of the machine until the fault is corrected. If the fault is not detected, then the safety function must still be performed upon demand.

Notes

Visit our website: www.ab.com/catalogs
Publication S117-CA001A-EN-P