Principles, Standards and Implementation

Regulations

Regulations . . . 1-2
EU Directives and Legislation . . . 1-2
The Machinery Directive . . . 1-2
Essential Health and Safety Requirements . . . 1-2
Conformity Assessment . . . 1-3
Technical File . . . 1-3
Conformity Assessment for Annex IV Machines . . . 1-3
Notified Bodies . . . 1-4
EC Type Examination . . . 1-4
EC Declaration of Conformity Procedure . . . 1-4
EC Declaration of Incorporation . . . 1-4
The Use of Work Equipment Directive . . . 1-5
Regulations 1 to 10 . . . 1-5
Regulations 11 to 24 . . . 1-6
US Regulations . . . 1-6
Occupational Safety and Health Administration . . . 1-6
Canada Regulations . . . 1-8

Standards

Standards . . . 1-8
ISO (International Organization for Standardization) . . . 1-8
IEC (International Electrotechnical Commission) . . . 1-8
EN Harmonized European Standards . . . 1-9
ISO and EN Standards (Type A) . . . 1-9
ISO and EN Standards (Type B) . . . 1-9
ISO and EN Standards (Type C) . . . 1-10
IEC and EN Standards . . . 1-10
US Standards . . . 1-11
ANSI Standards . . . 1-11
National Fire Protection Association . . . 1-11
Association for Manufacturing Technology . . . 1-12
Packaging Machinery Manufacturer's Institute . . . 1-12
American Society of Safety Engineers . . . 1-13
Society of Plastics Industry . . . 1-13
Canada Standards . . . 1-13
Australia Standards . . . 1-13

Safety Strategy

Safety Strategy . . . 1-15
Risk Assessment . . . 1-15
Machine Limit Determination . . . 1-16
Task and Hazard Identification . . . 1-16
Risk Estimation . . . 1-16
Risk Reduction . . . 1-18
Hierarchy of Measures for Risk Reduction . . . 1-19
Inherently Safe Design . . . 1-19
Protective Systems and Measures . . . 1-19
Evaluation . . . 1-20
Training, Personal Protective Equipment . . . 1-20
Standards . . . 1-20

Protective Measures and Complementary Equipment

Protective Measures and Complementary Equipment . . . 1-22
Preventing Access . . . 1-22
Detection Devices . . . 1-22
Operator Interface Devices . . . 1-38
Logic Devices . . . 1-40
Safety Networks . . . 1-47
Output Devices . . . 1-48
Connection Systems . . . 1-50

Safety Distance Calculation

Safety Distance Calculation . . . 1-50
Formula . . . 1-50
Directions of Approach . . . 1-50
Speed Constant . . . 1-50
Stopping Time . . . 1-50
Depth Penetration Factor . . . 1-51
Reach Through Applications . . . 1-51
Single or Multiple Beams . . . 1-51
Distance Calculations . . . 1-51
Angled Approaches . . . 1-52
Safety Mats . . . 1-52
Examples . . . 1-52

Prevention of Unexpected Power-Up

Prevention of Unexpected Power-Up . . . 1-53
Lockout/Tagout . . . 1-53
Safety Isolation Systems . . . 1-53
Load Disconnects . . . 1-53
Trapped Key Systems . . . 1-54
Alternative Measures to Lockout . . . 1-54

Structure of Safety Related Control Systems

Structure of Safety Related Control Systems . . . 1-54
Safety Function . . . 1-54
Categories of Control Systems . . . 1-55
Category B . . . 1-55
Interlock Switch . . . 1-56
Programmable Logic Controller . . . 1-57
Contactor . . . 1-57
Wiring . . . 1-57
Start and Stop Switches . . . 1-57
Category 1 . . . 1-57
Category 2 . . . 1-58
Category 3 . . . 1-59
Undetected Faults . . . 1-59
Pulse Testing Fault Detection . . . 1-62
Category 4 . . . 1-62
Component and System Ratings . . . 1-64
Fault Considerations and Exclusions . . . 1-64
Systems Achieving Category 1 Stops . . . 1-64
US Safety Control System Requirements . . . 1-65
Robot Standards: US and Canada . . . 1-65

Functional Safety of Control Systems

Functional Safety of Control Systems . . . 1-66
What Is Functional Safety? . . . 1-66
IEC/EN 62061 and ISO/EN 13849-1:2006 . . . 1-67
SIL and IEC/EN 62061 . . . 1-67
PL and ISO/EN 13849-1:2006 . . . 1-67
Comparison of PL and SIL . . . 1-67

System Design According to IEC/EN 62061

System Design According to IEC/EN 62061 . . . 1-69
Subsystem Design: IEC/EN 62061 . . . 1-69
Transition Methodology for Categories . . . 1-71
IEC/EN 62061 Terminology Overview . . . 1-72
Architectural Constraints . . . 1-72
B10 and B10d . . . 1-72
Common Cause Failure (CCF) . . . 1-72
Diagnostic Coverage (DC) . . . 1-72
Management of Functional Safety . . . 1-72
Probability of Dangerous Failure (PFHD) . . . 1-72
Proof Test Interval . . . 1-73
Safe Failure Fraction (SFF) . . . 1-73
Systematic Failure . . . 1-73

System Design According to ISO/EN 13849-1:2006

System Design According to ISO/EN 13849-1:2006 . . . 1-73
Safety System Architectures (Structures) . . . 1-73
Mission Time . . . 1-74
Mean-Time-to-Dangerous Failure (MTTFd) . . . 1-74
Diagnostic Coverage (DC) . . . 1-74
Common-Cause Failure (CCF) . . . 1-74
Systematic Failure . . . 1-74
Performance Level (PL) . . . 1-75
Subsystem Design and Combinations . . . 1-75
Validation . . . 1-76
Machine Commissioning . . . 1-76
Fault Exclusion . . . 1-76

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 with relevance to industrial safety. 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 Low Voltage Directive—The ATEX Directive.

The Machinery Directive

This Directive (98/37/EC) covers the supply of new machinery and other equipment including safety components. It is an offense to supply machinery unless it complies with the Directive. This means it must satisfy wide ranging EHSR's contained in Annex I of the Directive, a conformity assessment must be carried out, a "Declaration of Conformity" must be given and the CE marking must be affixed (see Figure 1).

The key provisions of the Directive came into full force for machinery on January 1, 1995 and for Safety Components on January 1, 1997. A two year transition period was allowed whereby either existing national regulations could be used or the new Directive regime could be followed. It is the responsibility of the manufacturer, importer or end supplier of the equipment to ensure the equipment supplied is in conformity with the Directive.

A new version of the Machinery Directive was published as 2006/42/EC in 2006. The new Directive will not replace the provisions of the existing Directive until the end of 2009. In the interim the existing Machinery Directive applies in full. The following text deals with the existing Directive 98/37/EC but there will be very little change in terms of the essential requirements for most types of machinery in the new Directive.

Figure 1: CE Marking Affixed to Machine

Essential Health & Safety Requirements

The Directive gives a list of Essential Health & Safety Requirements (referred to as EHSRs) to which machinery must comply where relevant (Figure 2). The purpose of this list is to ensure 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.

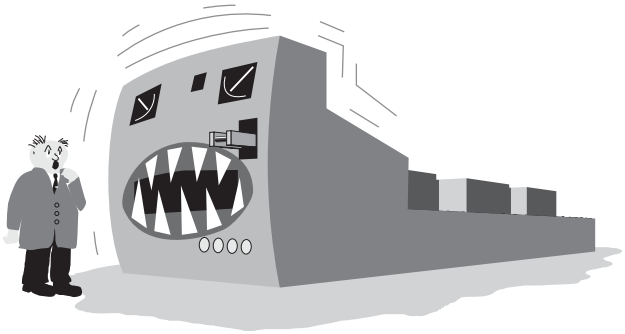


Figure 2: Machine Must Meet EHSRs

The Directive also provides a hierarchy of measures for eliminating the risk:

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

Where this is not possible; (2) Additional Protection Devices, 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 which 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 have one or more emergency stop devices fitted. Consideration must be given to complex installations where processes upstream or downstream can effect 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.

Conformity Assessment

The designer or other responsible body must be able to show evidence that proves conformity with the EHSRs. This file should include all relevant information such as test results, drawings, specifications, etc., as shown below.

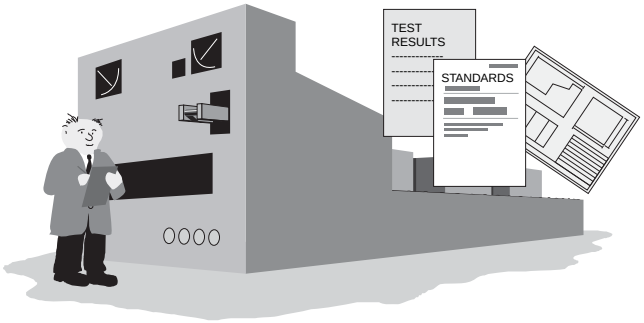


Figure 3: Document Assessment Results

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 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 all potential machine hazards are addressed. Similarly, it is the responsibility of the machine manufacturer to ensure all EHSRs are satisfied, even those that are not addressed by harmonized EN Standards.

Technical File

The person responsible for a declaration of conformity must ensure the following documentation will be available (Figure 4) on the premises for inspection purposes.

A technical file including:

1. Overall drawings of the equipment including control circuit drawings.
2. Detailed drawings, calculation notes, etc. required for checking the conformity of the machinery with the EHSRs.
3. A list of:

- The EHSRs relevant to the equipment.
- Applicable Harmonized European Standards.
- Other applicable standards.
- Technical design specifications.

4. A description of methods adopted to eliminate hazards presented by the machinery.
5. If desired, any technical report or certificate obtained from an approved body (test house) or laboratory.
6. If conformity is declared with a Harmonized European Standard, any technical report giving test results for it.
7. A copy of the instructions for the machinery.

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. Failure to make it available in response to a substantiated request by an enforcement authority may constitute grounds for doubting the conformity.

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.

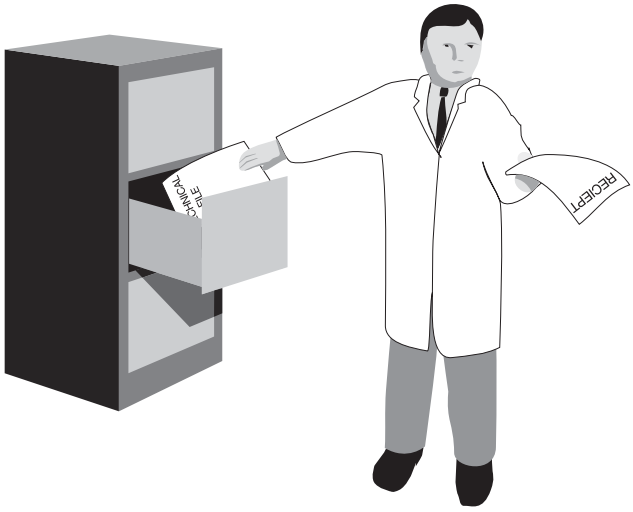


Figure 4: Technical File Must Be Available

Conformity Assessment for Annex IV Machines

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 light curtains and two-hand control units.

Figure 5: Conformity Assessments

For Annex IV machines in conformity with Harmonized European Standards there are three procedures to choose from:

1. Send the technical file to a notified body that will acknowledge receipt of the file and keep it.

   Note: With this option there is no assessment of the file. It may be used as a reference at a later date in the event of a problem or a claim of noncompliance.
2. Send the technical file to a notified body who will verify the Harmonized Standards have been correctly applied and will issue a certificate of adequacy for the file.
3. Submit an example of the machinery (Figure 6) to a notified body (test house) for EC type examination. If it passes, the machine will be given an EC type examination certificate.

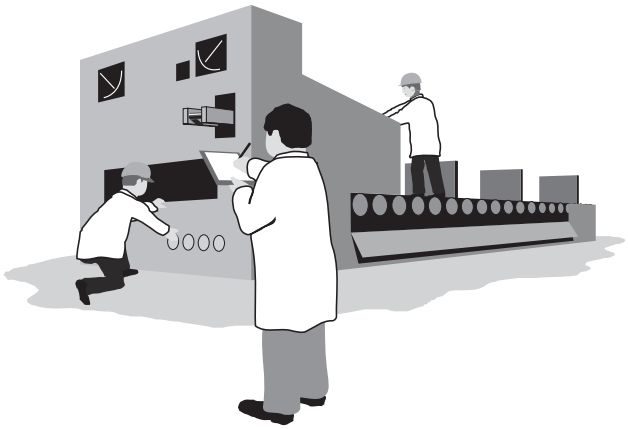


Figure 6: Notified Body Examinations

For Annex IV machines not in conformity with a standard or where no relevant Harmonized European Standard exists, an example of the machinery must be submitted to a notified body (test facility) for EC type examination.

Notified Bodies

A network of notified bodies who communicate with each other and work to common criteria exists throughout the EEA and certain other countries. Notified Bodies are appointed by governments (not by industry) and details of organizations with notified body status can be obtained from: *http://europa.eu.int/comm/enterprise/newapproach/legislation/nb/en 98-37-ec.pdf*.

EC Type Examination

For an EC type examination the notified body will require a technical file and access to the machine to be examined. They will check that the machine is manufactured in accordance with its technical file and that it satisfies the applicable EHSRs. If the examination is successful an EC type examination certificate will be issued. A body that refuses to issue a certificate must inform the other notified bodies.

CE

Figure 7: CE Mark

EC Declaration of Conformity Procedure

The responsible person must draw up an EC Declaration of Conformity and affix the CE mark (see Figure 7) to all machines supplied. The machines should also be supplied with the EC Declaration of Conformity (see Figure 8).

Note: Safety components should have an EC Declaration of Conformity but not a CE mark with respect to the Machinery Directive (although they may be CE marked to indicate conformity to other directives such as the EMC and/or Low Voltage Directives).

The CE mark indicates the machine conforms to all applicable European Directives and 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 EHSRs for all applicable directives and is, in fact, safe. It is also an offense to apply any mark that may be confused with the CE mark.

EC Declaration of Incorporation

Where the equipment is supplied for assembly with other items to form a complete machine at a later date, the responsible person may issue a DECLARATION OF INCORPORATION with it (instead of a declaration of conformity). 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.

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

Figure 9 provides a flow diagram to help explain the process for meeting the machinery directive.

Maykit Wright Ltd.
Declaration of Conformity

In respect of the following Directives:

European Machinery Directive 98/37/EC. (Any other Directives relevant to the machine e.g., the EMC Directive should also be included here.)

Company:

Maykit Wright Ltd.
Main Street
Anytown Industrial Estate
Anytown, England AB1 2DC
Tel: 00034 000890. Fax: 00034

Machine: Meat Packaging Machine.
Type: Vacustarwrap 7D
Serial Number: 00516

Conforming to standards: *(All relevant Harmonized European Standards used and, where appropriate, any national standards and specifications.)*

If the machine is covered by Annex IV it would be necessary at this point to include one of the following:

– The name and address of the Approved Body and the number of the Type Examination Certificate, or

– The name and address of the Approved Body which has drawn up a Certificate of Adequacy for the technical file, or

– The name and address of the Approved Body to which the technical file has been forwarded.

This is to declare that the above machine conforms with the relevant Essential Health and Safety Requirements of the European Machinery Directive 98/37/EC.

G. V. Wright

G.V. Wright, Managing Director
Issued 17th January 2003

Figure 8: Example of a DoC for a Machine That Is Self-Certified

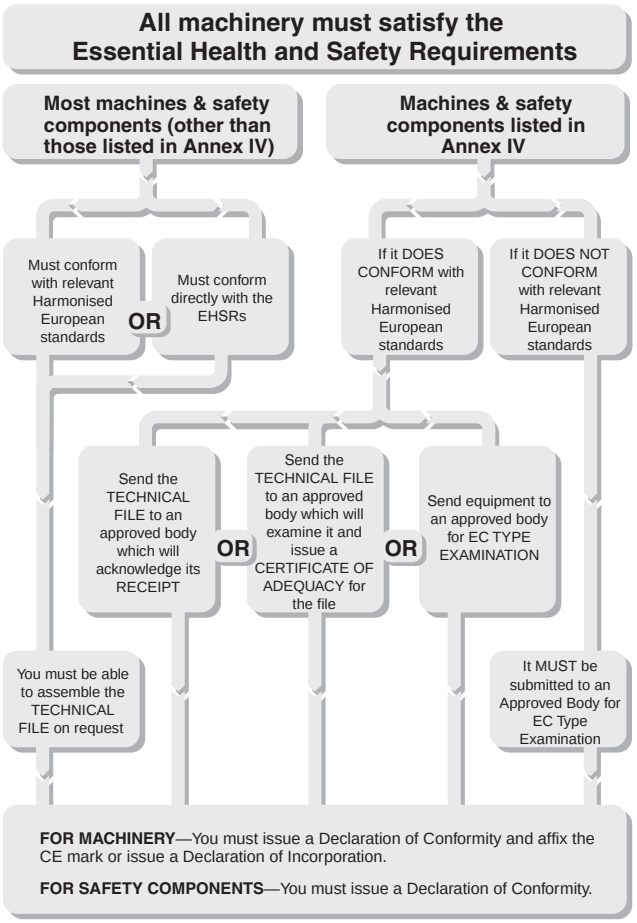


Figure 9: Overview of Procedures for the Machinery Directive

The Use of Work Equipment Directive

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

It is easier to understand the meaning of the requirements of the Use of Work Equipment Directive by looking at the example of its implementation into national legislation. We will look at its 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.

Regulations 1 to 10

These regulations 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 EEA) 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 EEA provided for the first time in the workplace must immediately satisfy regulations 11 to 24.

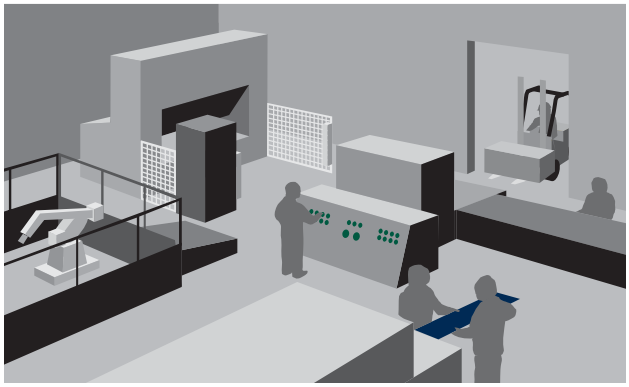


Figure 10: Directive Covers Use of Equipment

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).

Regulation 5 "Suitability of work equipment" lies at the heart of the directive and highlights the employer's responsibility to carry out a proper process of risk assessment.

Regulation 6 "Maintenance" requires machinery to 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.

Regulations 11 to 24

These regulations cover specific hazards and protective arrangements on machines.

They were not fully implemented until January 1, 1997 for existing unmodified machines in use before January 1, 1993. They applied immediately to other equipment. However, if the equipment conforms to relevant product directives, e.g., The Machinery Directive, they will automatically comply with the corresponding requirements of regulations 11 to 24 as they are similar in nature to the EHSRs of that Directive.

Of particular interest is Regulation 11, which gives a hierarchy of protection measures. These are:

1. Fixed enclosing guards.
2. Other guards or protection devices.
3. Protection appliances (jigs, holders, push sticks, etc.).
4. The provision of information, instruction, supervision and training.

These measures should be applied from the top as far as practical and usually a combination of two or more will be required.

US Regulations

This section introduces some of the industrial machine guarding safety regulations in the US. This is only a starting point; readers must further investigate the requirements for their specific applications and take measures to ensure 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 US 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, and 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 the Machinery Directive, which requires suppliers to place machines on the market that are free from hazards. In the US, 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 OSHA website at www.osha.gov. Unlike most standards, which are voluntary, OSHA standards are the law.

Some of the important parts of OSHA, 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	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.

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 energizing 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 energizing, 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 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.

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 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 July 2006, the following companies are nationally recognized test labs:

Applied Research Laboratories, Inc. (ARL)
Canadian Standards Association (CSA)
Communication Certification Laboratory, Inc. (CCL)
Curtis-Straus LLC (CSL)
Electrical Reliability Services, Inc. (ERS)
Entela, Inc. (ENT)
FM Global Technologies LLC (FM)
Intertek Testing Services NA, Inc. (ITSNA)
MET Laboratories, Inc. (MET)
NSF International (NSF)
National Technical Systems, Inc. (NTS)
SGS US 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 Regulations 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, safely, and cleanly. The standards also make trade between countries easier.

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.

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 two 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.

The solar system can be used to model the relationship of the machinery directive to the European standards. The planets represent the standards, which revolve around the sun, which represents the machinery directive. The inner orbits are the "A" and "B" standards. The outer orbits represent the "C" standards.

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://europa.eu.int/comm/enterprise/mechan_equipment/machinery/index.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.

ISO 14121 (EN 1050)

Principles for risk assessment.

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

ISO and EN Standards (Type B)

ISO 11161 (will also be EN 11161)

Safety of Integrated Manufacturing Systems—Basic Requirements.

This standard should be published in its revised form in 2007. This revised version has been significantly updated making it very useful for contemporary integrated machinery.

ISO 13849 (EN 954)

Safety related parts of control systems—Pt 1: General principles for design. Pt 2: Validation

This standard outlines requirements for safety critical parts of machine control systems and describes 5 categories of performance "B, 1, 2, 3 and 4." It is important to gather a working knowledge of this document as its categories are accepted as the common "language" for describing the performance of safety related control systems.

ISO 13849-1:2006

This standard underwent revision, and was published in late 2006. It is published both as an EN and ISO version with the same number: 13849-1. At the time of the printing of this catalog, it is expected that the current version of EN 954-1: 1996 will remain applicable probably until the end of 2009 for the European Community. The 2006 revision represents a significant change. It will introduce some aspects not considered in the current version. The term "PL" (Performance Level) is used to describe the level of integrity of a system or a subsystem.

The revised standard will be an alternative to EN/IEC 62061 (see later). It is intended to provide a more direct and simple methodology but at the expense of some constraints and restrictions. Either the revised ISO/EN 13849-1 or IEC/EN 62061 can be applied to most machinery electrical safety related systems and the user should choose whichever one is best suited to their needs.

ISO/EN 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.

ISO 13852 (EN 294)

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

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

ISO 13853 (EN 811)

Safety distances to prevent danger zones being reached by the 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)

Isolation and energy dissipation—Prevention of unexpected start-up.

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

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 type's pf machinery. For example:

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. In the U.S., this is equivalent to NFPA 79.

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 the revised version of ISO/EN 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 are 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/EN 62061

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

This standard is one of the new generation 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 the existing EN 954-1 and is intended to be useful for the increasingly complex safety functionality required for current and future machinery For less complex safety functionality the revised version of ISO/EN 13849-1 may be easier to implement. The use of these standards requires the availability of data such as PFHd (probability of dangerous failure per hour) or MTTFd (mean time to dangerous failure). The derivation of this data will be considered later in this section.

IEC/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.

Draft IEC 61800-5-2

Functional safety of power drive systems.

This standard will deal 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, non profit, 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

U.S. 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

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 11.

1. **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.
2. **RISK REDUCTION** is then performed if necessary and safety measures are selected based on the information derived from the risk assessment stage.

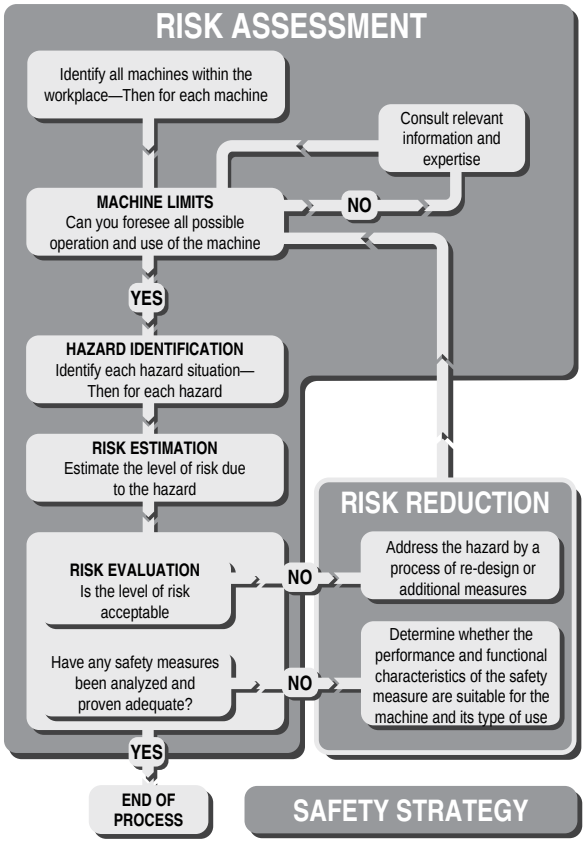


Figure 11: Safety Strategy

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” contains the most globally applied guidance.

Whichever 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 it may not be suitable for some applications. At the time of publication of this catalog, ISO TR (Technical Report) 14121-2 “Risk assessment – Practical guidance and examples of methods” is being prepared. Hopefully this document will be available in late 2007 and it will provide much needed practical guidance.

The following information is intended to explain and illustrate the risk estimation section of the existing standard ISO 14121 "Principles for Risk Assessment."

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.

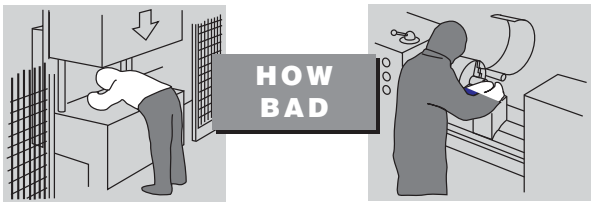
Make use of any data and expertise available to you. You are dealing with all stages of machine life, so to avoid too much complexity base your decisions on the worst case for each factor.

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 12. 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 12: 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**
- **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 is assigned a points value shown in Figure 13.

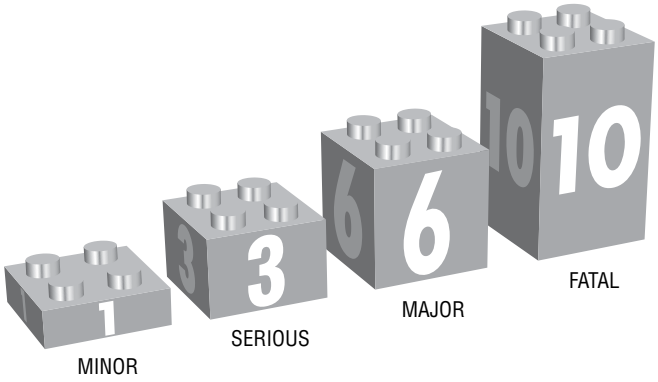


Figure 13: Points Assigned to Severity

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 14).

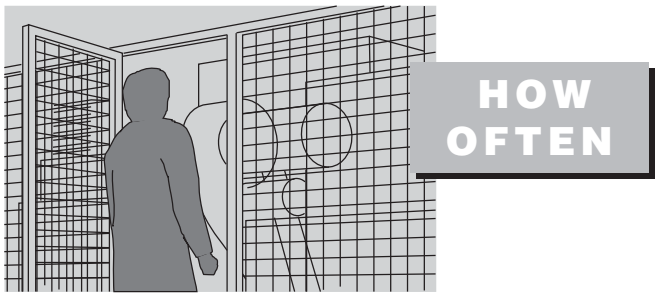


Figure 14: Frequency of Exposure

The frequency of exposure to hazard can be classified as:

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

Each description is assigned a points value shown in Figure 15.

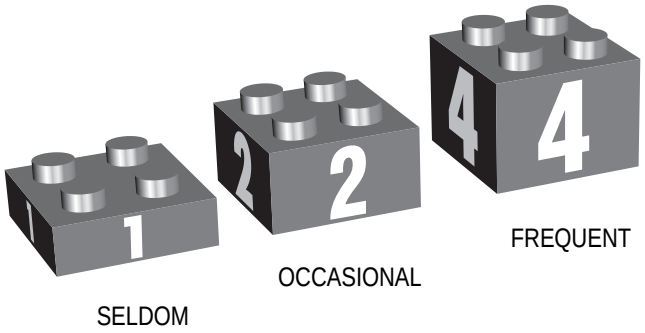
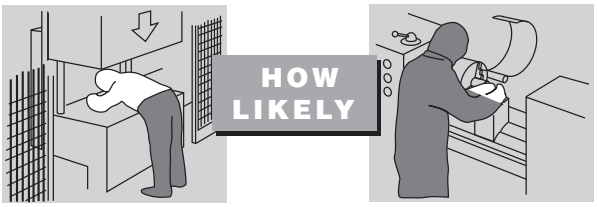


Figure 15: Points Assigned to Frequency of Exposure

3. Probability of injury

You should assume that the operator is exposed to the hazardous motion or process (Figure 16).



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 16: 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 is assigned a points value shown in Figure 17.

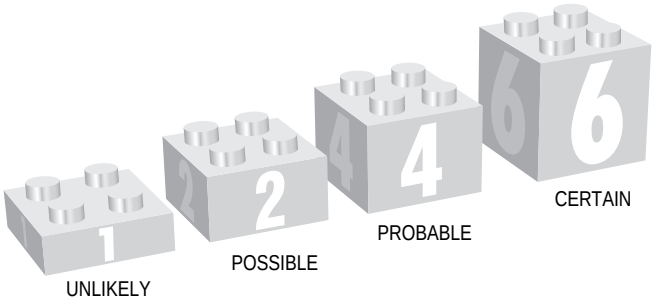


Figure 17: Points Assigned to Probability of Injury

All headings are assigned a value and they are now added together to give an initial estimate. Figure 18 shows the sum of the three components adds up to a value of 13. But we must consider a few more factors.

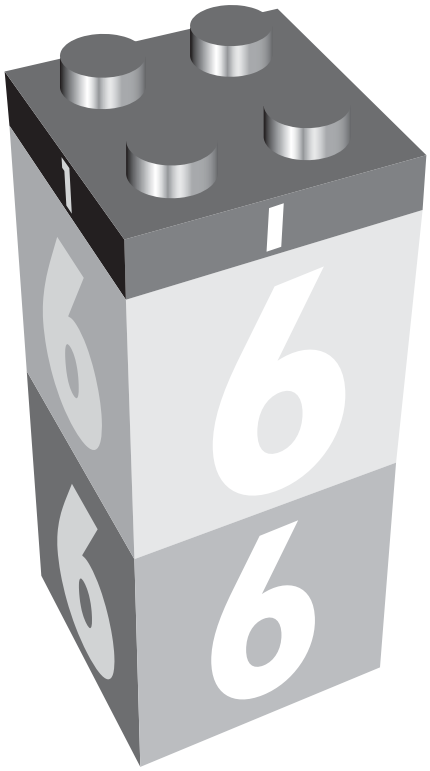


Figure 18: Initial Estimate

(**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., 1 year) between accesses. (There may be progressive and undetected failures particularly in monitoring systems.)	Add point's 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 19.

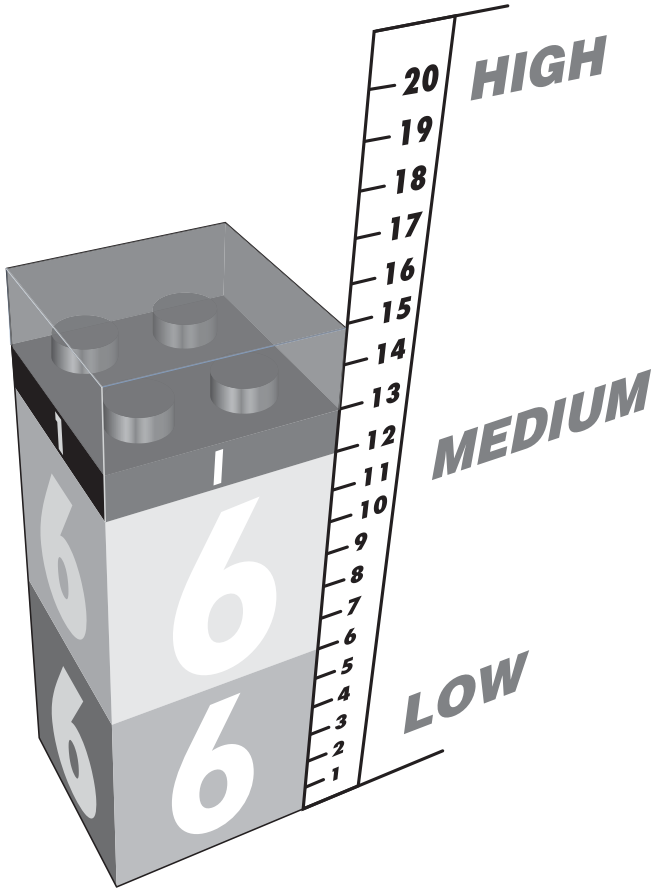


Figure 19: Final Value with Adjustments

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 20 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.

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 20: Risk Assessment Matrix

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.

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 keeping 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. The pre-revision version of the standard ISO 13849-1 outlines various categories for safety related parts of control systems and provides a risk graph in its Annex B. This is a very simplistic approach, but it can provide useful guidance determining some of the requirements for a protective system.

The revised version of ISO 13849-1 and IEC 62061 both provide useful methods and guidance on how to specify a safety related control system that is providing a protective measure or safety function.

ISO 13849-1:2006 provides an enhanced risk graph in its Annex A. This graph is shown in Figure 21.

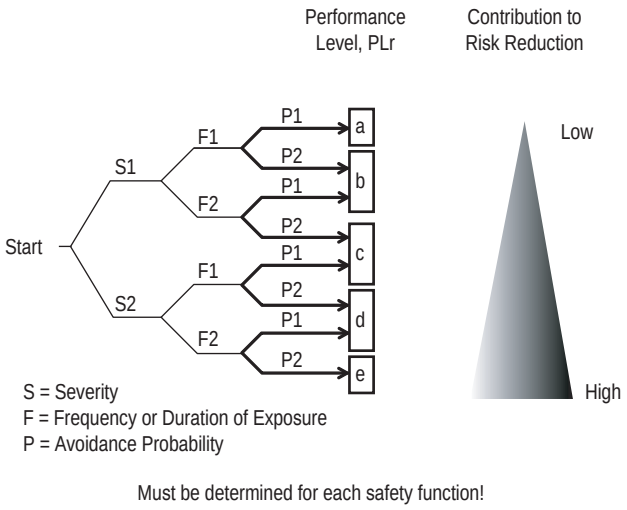


Figure 21: Risk Graph for Determining the Required Performance Level for a Safety Function—from ISO 13849-1:2006

IEC 62061 also provides a method in its Annex A, it takes the form shown in Figure 22.

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 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.

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

ISO 14121 (EN 1050): Principles for risk assessment.

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

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. Safeguards are defined as methods that either prevent access to a hazard or detect access to a hazard. Safeguards include devices like fixed guards, interlocked guards, light curtains, safety mats, two-hand controls and enabling switches.

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 23. 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.

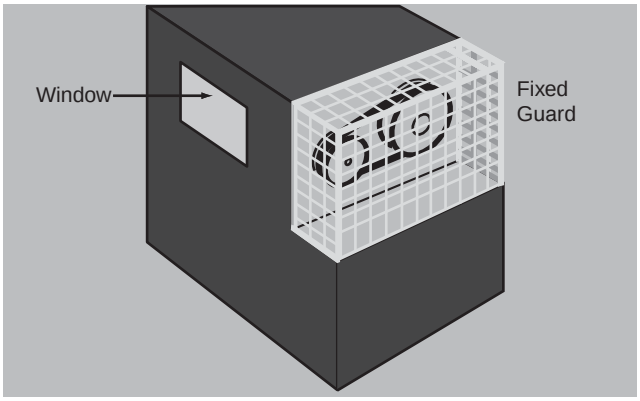


Figure 23: Fixed Guards

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

Safeguarding is 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 24 shows the block diagram of a simple safety system.

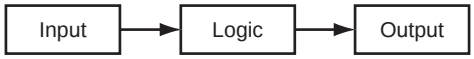


Figure 24: Simple Safety System Block Diagram

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.

- Switch off or disable power when a person enters the hazard area.
- 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.

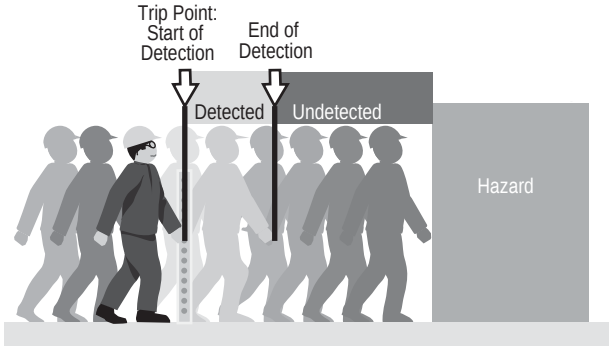


Figure 25: Full Body Access

Figure 25 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.

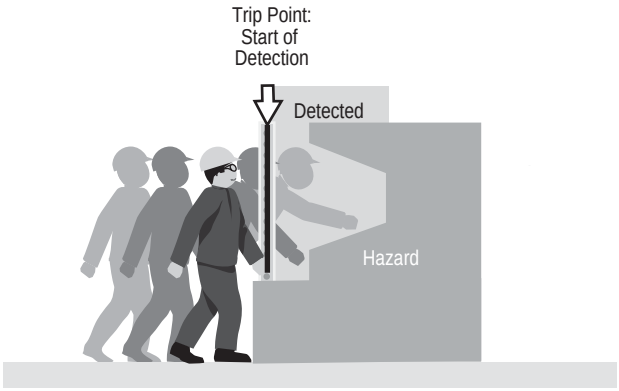


Figure 26: Partial Body Access

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 26, 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 include safety light curtains, single beam safety barriers, safety area scanners, safety mats and safety edges.

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. 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 27.

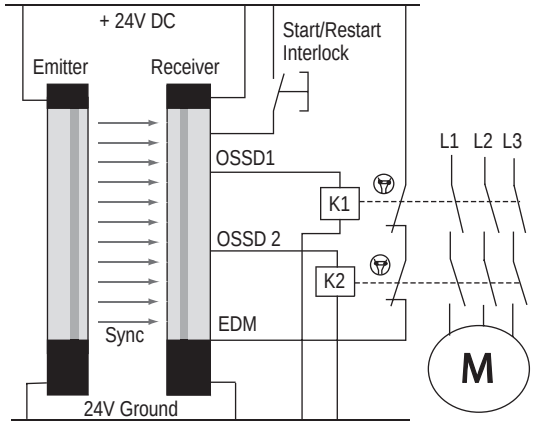


Figure 27: Basic Light Curtain Safety System

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 crossfault (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.

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 28. 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.

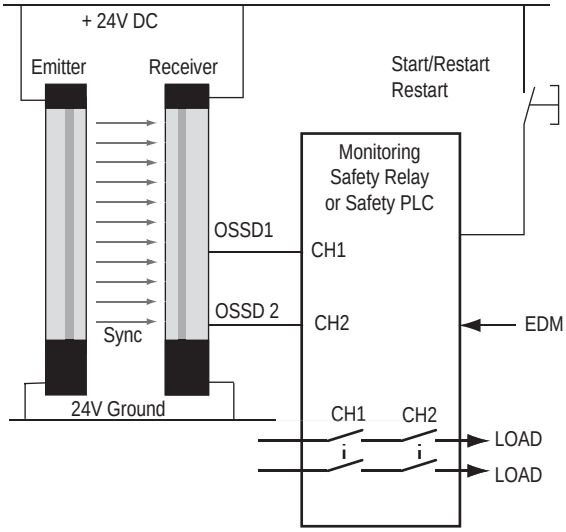


Figure 28: Light Curtain Interfacing with MSR or Safety PLC

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 29 shows an example of a vertical application.

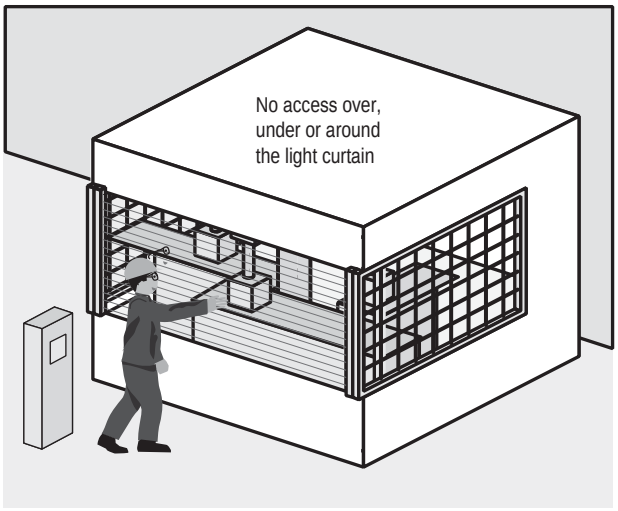


Figure 29: Vertical Application

Cascading

Cascading is a technique of connecting one set of light curtains directly to another set of light curtains like that shown in Figure 30. 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.

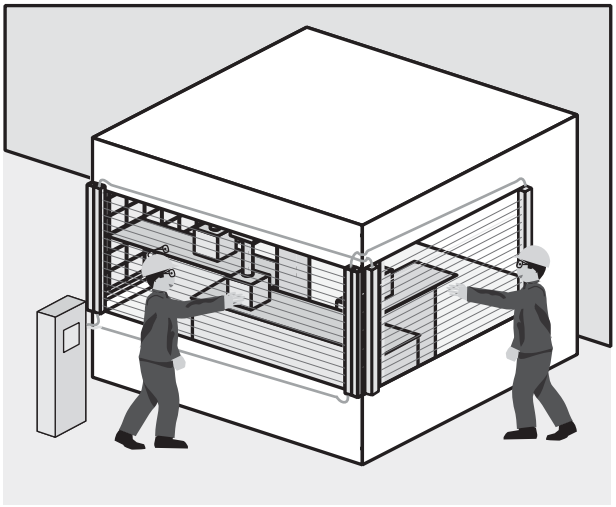


Figure 30: Cascaded Light Curtains

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.

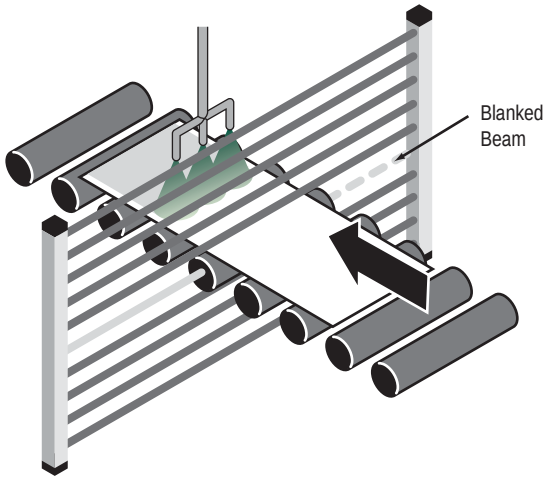


Figure 31: LIght Curtain Is Blanked Where Conveyor Is Fixed

Figure 31 shows an example where the object is stationary. Mounting hardware, a 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 workpiece, a stop signal is sent to the machine.

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 32, 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.

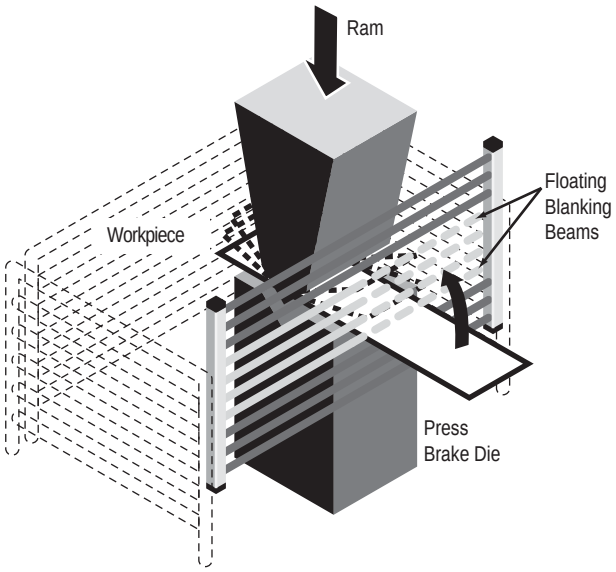


Figure 32: Floating Blanking

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 Safety Distance Calculation).

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 33. In either alternative, the light curtains must be located a safe distance away from the hazard.

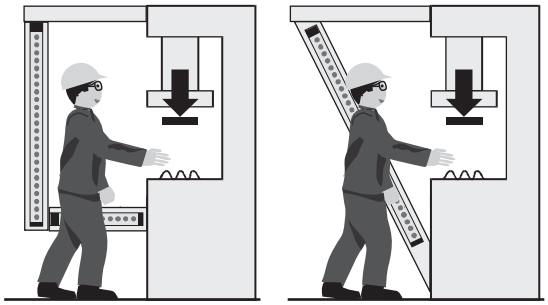


Figure 33: Alternative Solutions for Space between Light Curtain and Hazard

For longer safety distances or for area detection, light curtains can be mounted horizontally, as shown in Figure 34. 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.

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 35. 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.

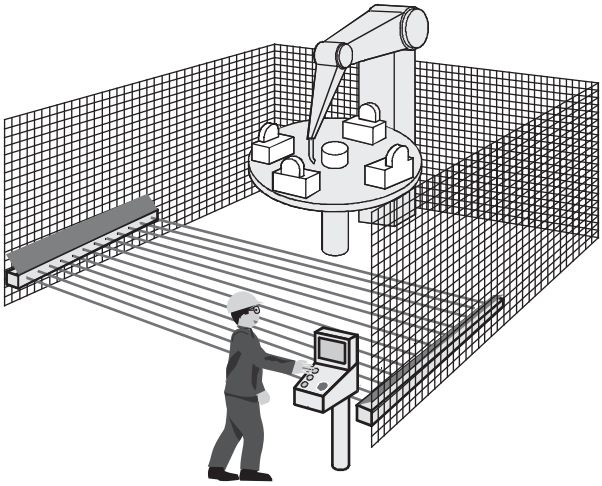


Figure 34: Horizontal Application of a Light Curtain

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.

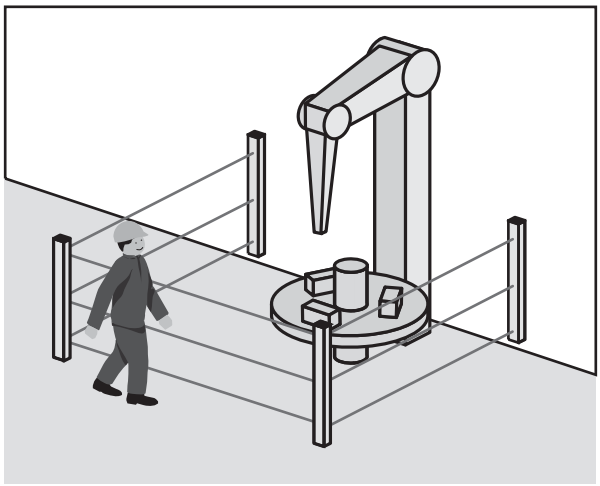


Figure 35: Mirrors Create Perimeter

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 discusses beam placement and spacing to achieve adequate protective fields. Figure 35 shows an example of a single-beam application. Breakage of the beam is used to stop the hazardous machine motion.

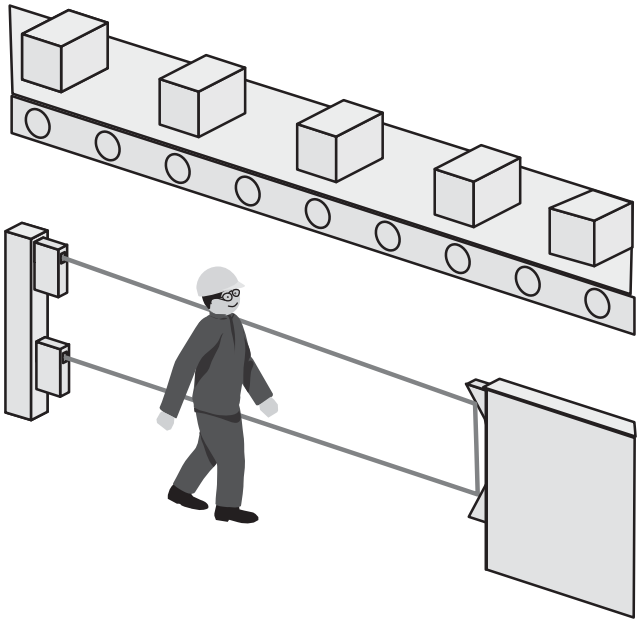


Figure 36: Single Beam Devices for Low Risk Applications

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 34. Objects entering or inside the safety zone cause the laser scanner to issue a stop command; the OSSD outputs turn off.

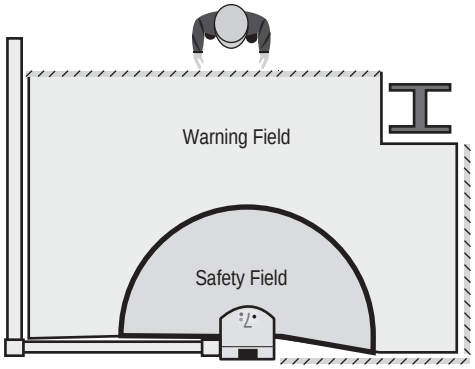


Figure 37: Warning Field Configured Around Structural Objects

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 37 shows an example of the warning field configured to ignore structural objects.

Developments in laser scanner technology allow a single scanner to cover multiple zones. In Figure 38, the laser scanner allows operator access to one side (shown as Case 1) while the robot is busy on the other side (Case 2).

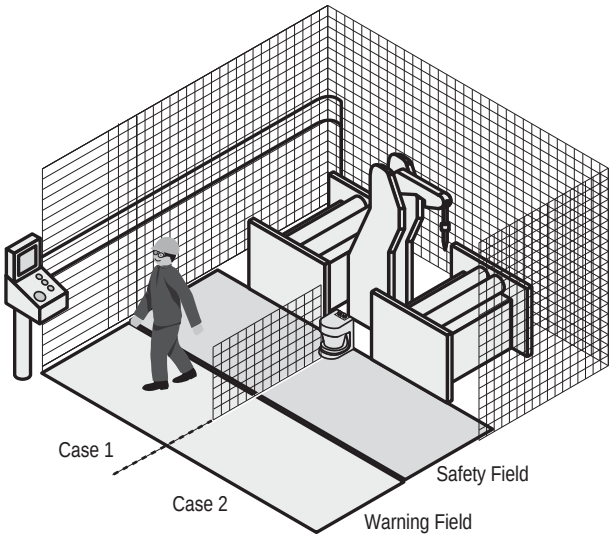


Figure 38: Multi-zone Application of Laser Scanner

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.

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 nonhazardous 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 nonsafety rated. The types, number and location of muting sensors must be selected to meet the safety requirements determined by the risk assessment.

Figure 39 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.

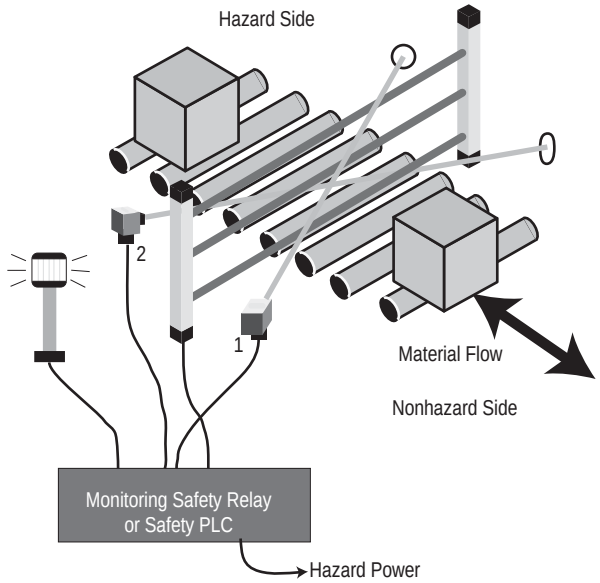


Figure 39: Conveyor 2 Sensor Muting

Another commonly applied approach is to use four sensors, as shown in Figure 40. Two sensors are mounted on the hazard side and two on the nonhazard 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.

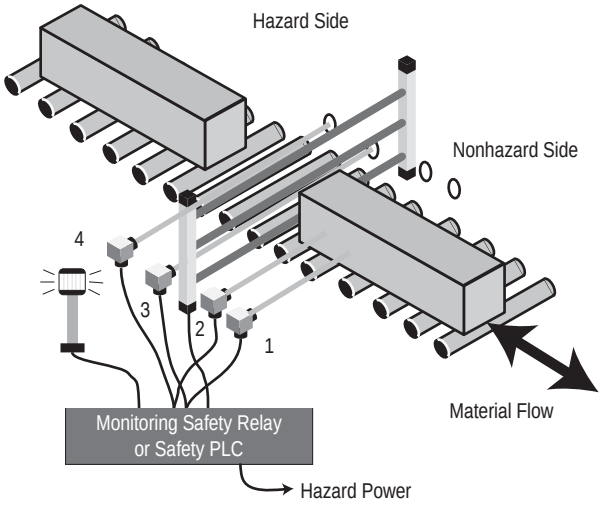


Figure 40: Conveyor 4 Sensor Muting

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 41 shows an example of this application.

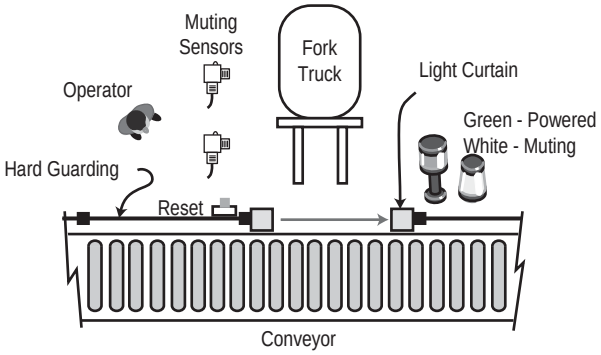


Figure 41: Fork Truck 2 Sensor Muting

Access to robot cells is also accomplished by muting. As shown in Figure 42, limit switches, located on the base of the robot, indicate the position of the robot. The safeguarding devices (light curtains and safety mats) are muted when the robot is not in a hazardous position.

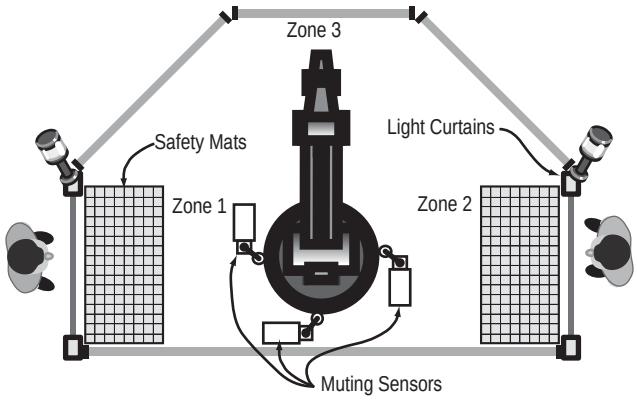


Figure 42: Muting of a Robot Cell

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 workpiece, 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 43 to 45 is an auto initiation double break mode (after initial start-up sequence).

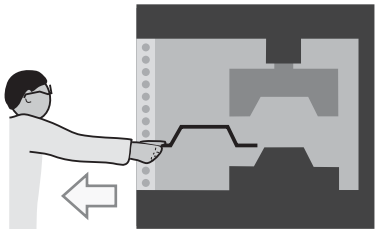


Figure 43: Step 1 of Double Break PSDI

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.

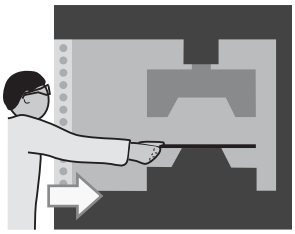


Figure 44: Step 2 of Double Break PSDI

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.

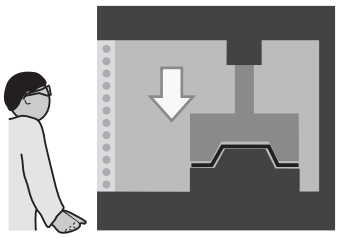


Figure 45: Step 3 of Double Break PSDI

Pressure Sensitive Safety Mats

These devices are used to provide guarding of a floor area around a machine, as shown in Figure 47. 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.

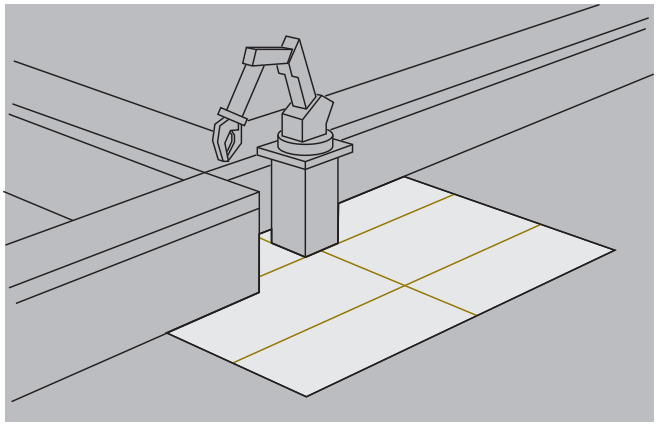


Figure 46: Safety Mats Surrounding a Robot

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 47. The plates are separated by spacers. The metal plates and spacers are encapsulated in a nonconductive material with its surface designed to prevent slipping.

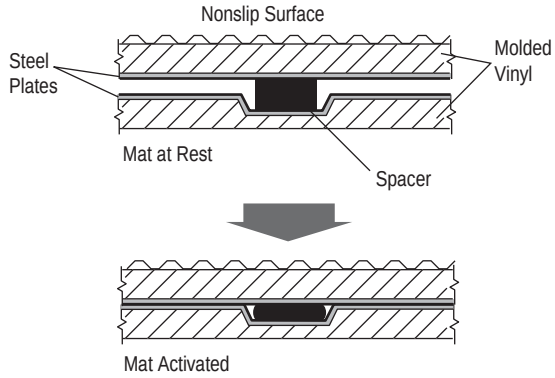


Figure 47: Typical Safety Mat Construction

To ensure 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 2 or 4 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 48 shows an example of how multiple four-wire mats are connected in series to ensure the safety mats are available for use.

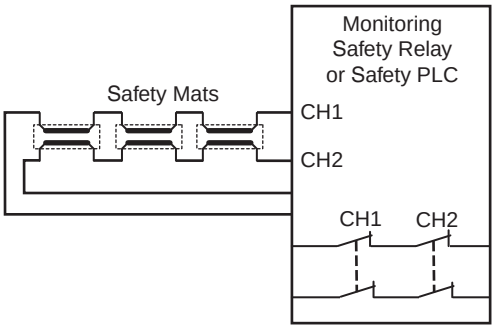


Figure 48: Safety Mat Interfacing

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 49.

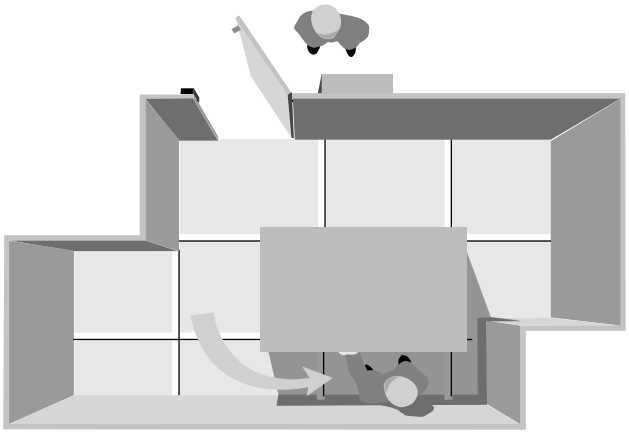


Figure 49: Safety Mat Detects Operator Behind Equipment

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

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 50.

Figure 50: Edge on Machine Table and Powered Door

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.

The Allen-Bradley Guardmaster Safedge uses conductive rubber, with two wires running the length of edge (Figure 51). At the end of the edge, a terminating resistor is used to complete the circuit. Depressing the rubber reduces the circuit resistance.

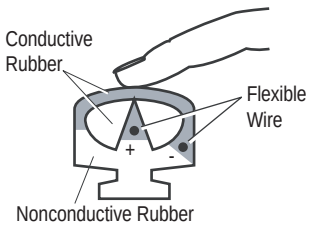


Figure 51: Conductive Rubber Safety Edge

Since a change in resistance must be detected, the monitoring safety relay must be designed to detect this change. An example wiring of this 2-wire design with a terminating resistor is shown in Figure 52. One advantage of the conductive rubber technology is that it provides active corners.

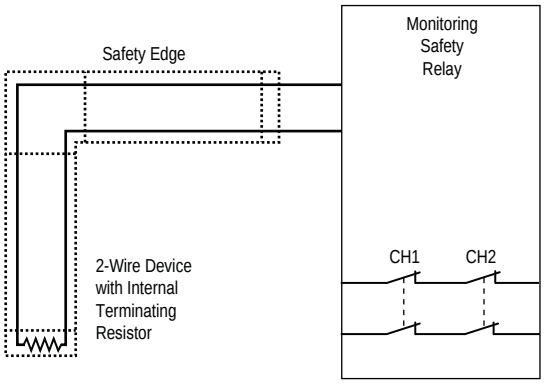


Figure 52: Conductive Rubber Safety Edge Circuit

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 (openable) 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 53.

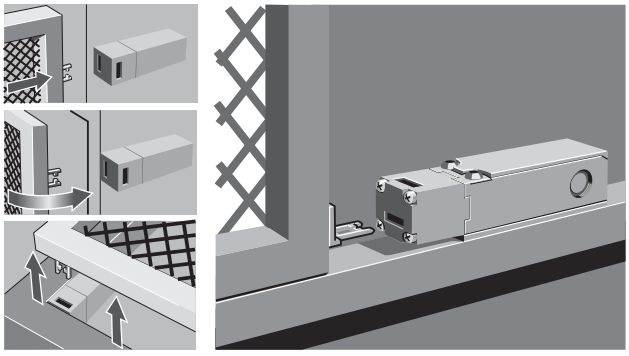


Figure 53: Tongues Interlocks on Sliding, Hinge or Removable Guards

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).

This is accomplished by making the actuator a special shape, as shown in Figure 54. 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 54, have a spring that prevents the tongue from fully entering and operating the interlock switch unless it is correctly fixed to the guard.

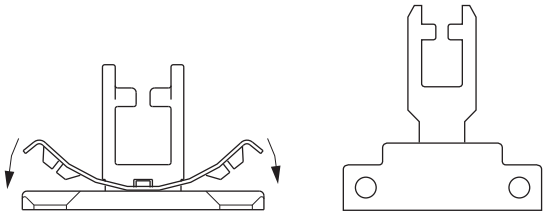


Figure 54: Tongue Shaped Actuators with Dimensional Features to Help Prevent Defeatability

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.

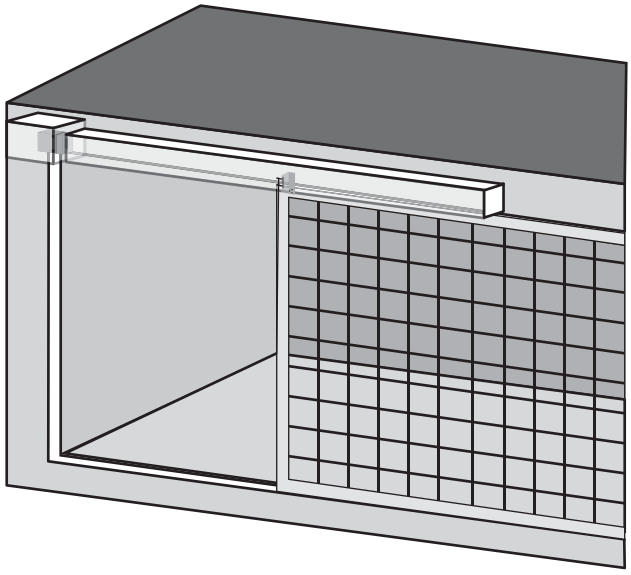


Figure 55: Switch and Actuator Hidden

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 55 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.

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 tests that can be used to verify Direct Opening Action. Products that meet the requirements of Direct Opening Action display the symbol shown in Figure 56 on their enclosure.

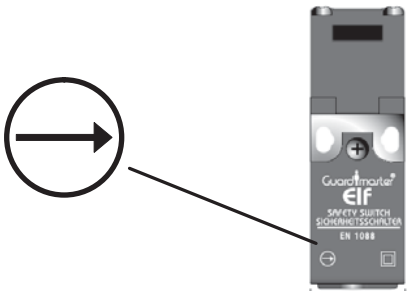


Figure 56: Symbol of Direct Opening Action

Figure 57 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.

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 nonsafety 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.

One advantage of using two normally closed contacts with interlocks is reduction in the wiring when multiple gates must be monitored. Figure 58 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.

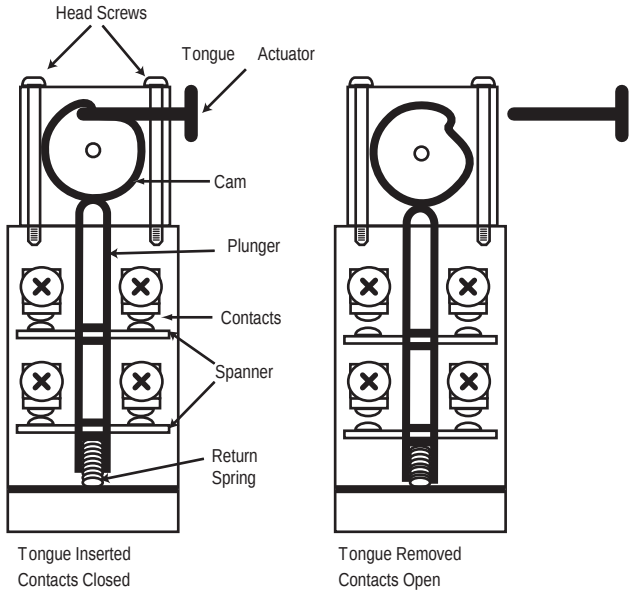


Figure 57: Double-Break with Direct Opening Action

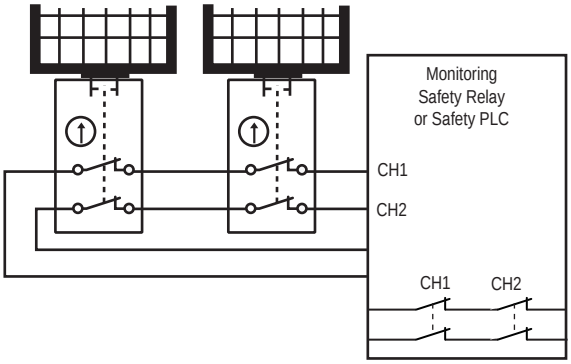


Figure 58: Daisy Chain of Multiple 2 N.C. Interlocks

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 59 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.

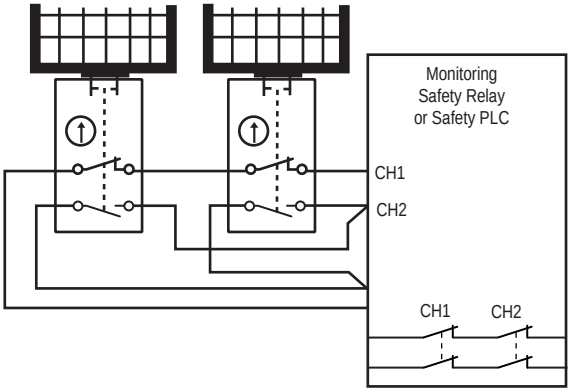


Figure 59: Multiple Interlocks with N.C. and N.O. Contacts

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 failures 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 60 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.

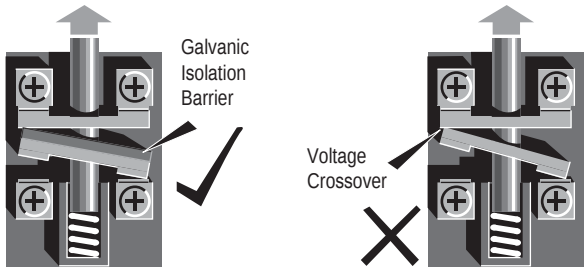


Figure 60: Galvanic Isolation of Contacts

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 61).

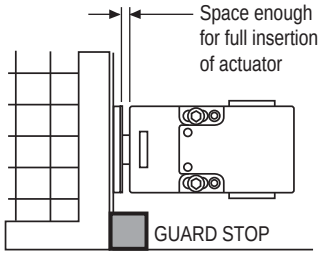


Figure 61: Mechanical Stops

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 62.

Figure 62: Metal Interface with Flexible Actuator

Contact operation affects performance of the switch in the safety/control system and must be taken into account by the machine designer. This performance is only important when both the normally closed contacts are used by the safety system and the normally open auxiliary contacts are used to indicate guard status to the PLC.

Contact operation is either slow-acting or snap-acting. In slow-acting operation, two types exist. Break before make (BBM) describes the operation where the normally closed contacts open before the normally open contacts close. Make before break (MBB) describes the operation where the normally closed contacts open after the normally open contacts close.

Due to wear, damage, or other changes to the guarding over time, pressure may be applied to the door forcing it open slightly. If the door moves between the point where the change-over occurs, the safety system and machine control system will get conflicting messages, as shown in Figure 63.

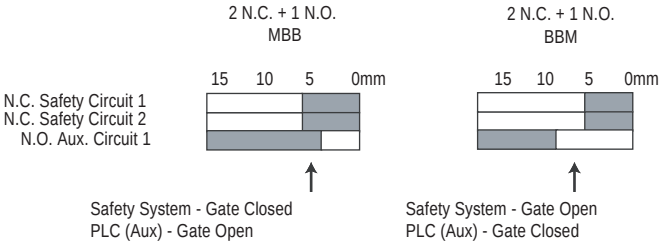


Figure 63: MBB and BBM Contacts—Conflicting Messages

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 noncontact 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 workpiece 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.

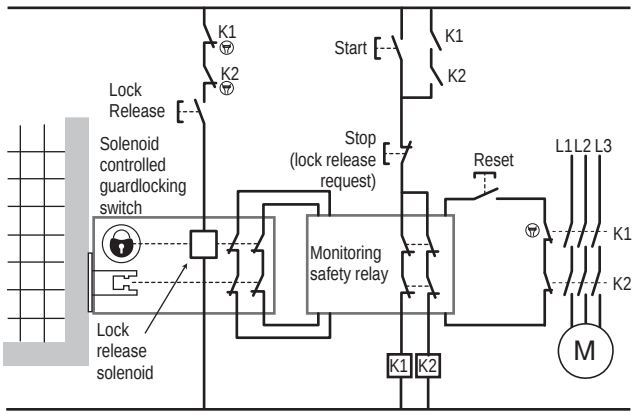


Figure 64: Simplified Basic Solenoid Guard Locking Switch Scheme

Figure 64 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 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.

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 65. 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.

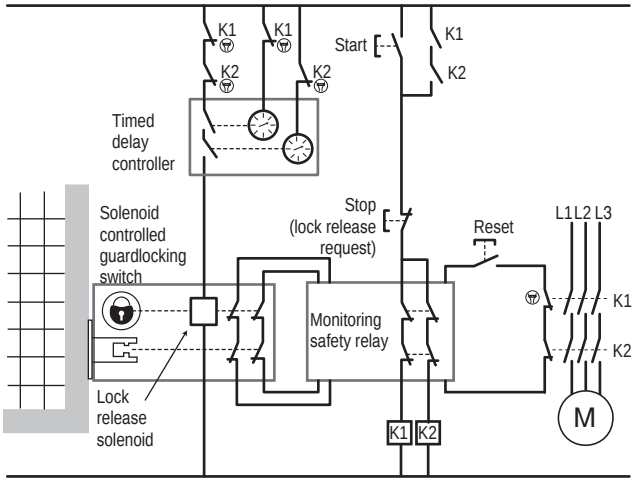


Figure 65: Simplified Timed Delay Controlled Solenoid Guard Locking Switch Scheme

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 66.

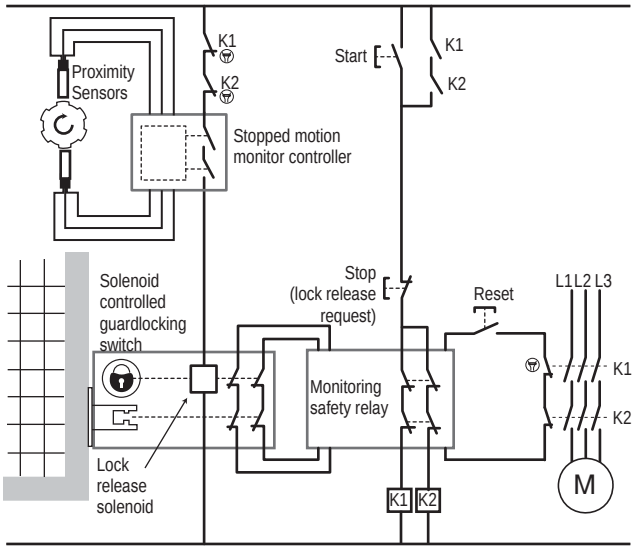


Figure 66: Simplified Stopped Motion Controlled Solenoid Guard Locking Switch Scheme

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 85 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 the Safety PLC is often a more suitable solution than individual relays and control units.

Construction

Popular 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 67.

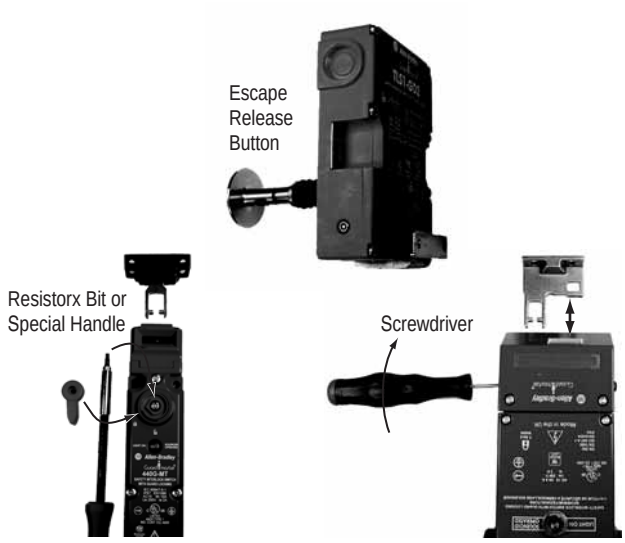


Figure 67: Escape Methods for Guard Locking

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 required may be reasonably low. Depending on where the guard locking switch is installed, operating leverage may suggest higher holding forces. Motorized doors may require higher holding forces.

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 68. 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.

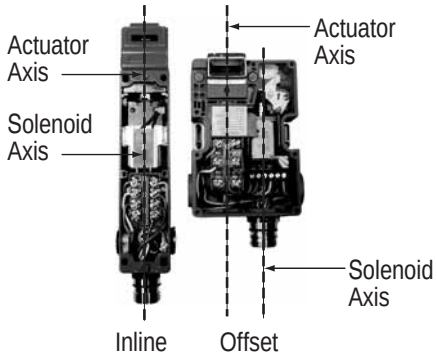


Figure 68: Inline and Offset Solenoid

The inline arrangement does not always 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 69.

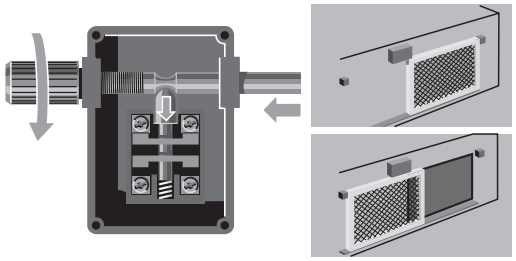


Figure 69: Sliding Bolt Interlock

Non-contact Interlock Switches

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 noncontact interlock switch. The contacts are connected with an internal non-resettable 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 70. This is prevented by the nonresettable overcurrent protection device. There is a large margin of safety between the rating of this device and the reed contacts. Because it is nonresettable, the switch should be protected by a suitably rated external fuse. The Allen-Bradley Guardmaster Ferrogard interlocks use this technique.

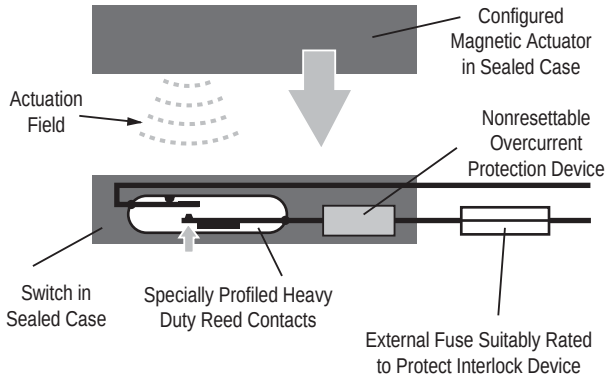


Figure 70: Simple Magnetic Operated Noncontact Interlock

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 71.

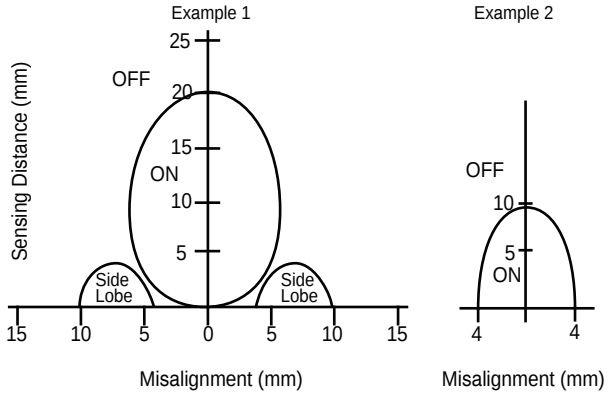


Figure 71: Non-Contact Operating Curve

Another important consideration for applying non-contact switches is the direction of approach of the actuator, as shown in Figure 72. The coding techniques determine which approaches are acceptable.

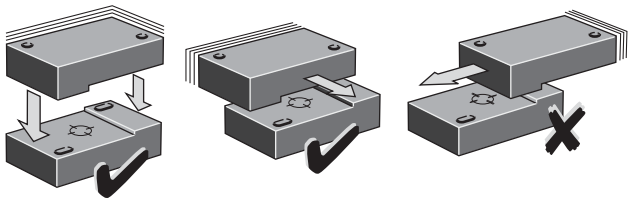


Figure 72: Approach of Actuator Affects Performance

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 73. They should also be installed where they are not subjected to extraneous interference by magnetic/electric fields.

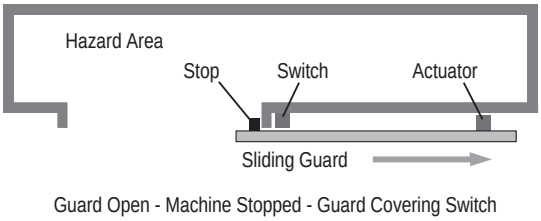


Figure 73: Sliding Guard Protects Access to Sensor

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 is 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 4.52. The opening of the guard is transmitted via a positive mode operating mechanism to the control circuit contacts.

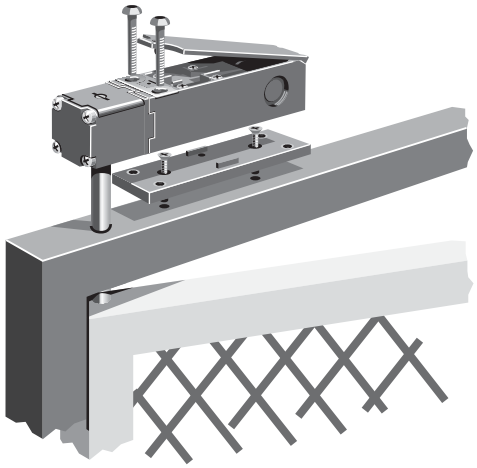


Figure 74: Hinge Switch Installation

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 during selection 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 75). 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.

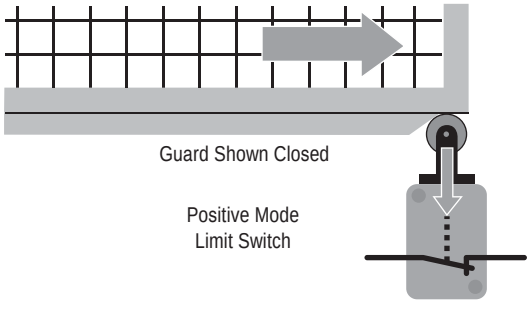


Figure 75: Positive Mode Limit Switch

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 76. One operates in positive mode (direct action to open contact), and one operates in negative mode (spring return).

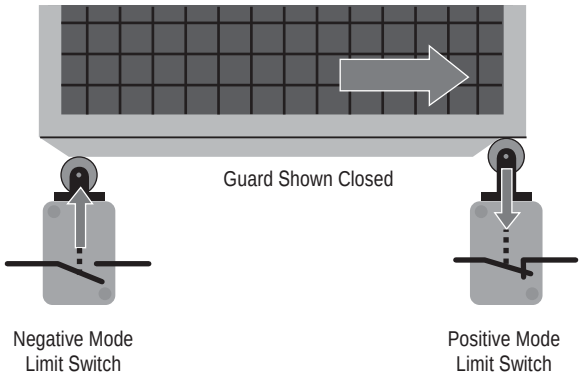


Figure 76: Diverse Redundant Position Switches

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.

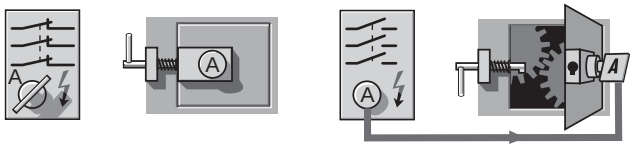


Figure 77: Power Interlocking with Trapped Key System

The most practical method of power interlocking is a trapped key system (see Figure 77). 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.

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 78, 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.

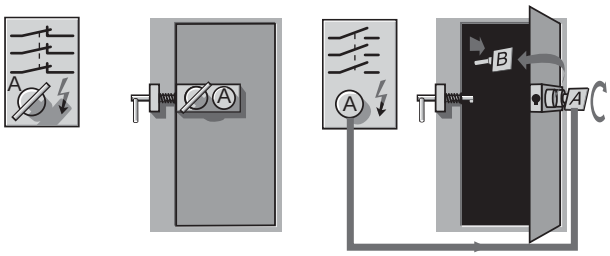


Figure 78: Full Body Access—Operator Takes "B" Key

In another example shown in Figure 79, Key "A" is rotated and removed 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.

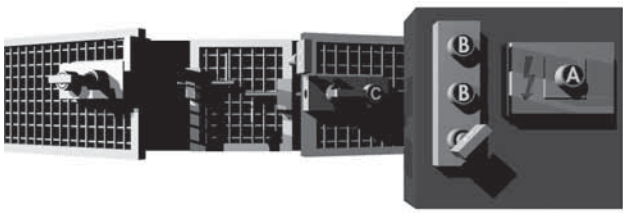


Figure 79: Multiple Doors Are Accessible

Figures 80 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.

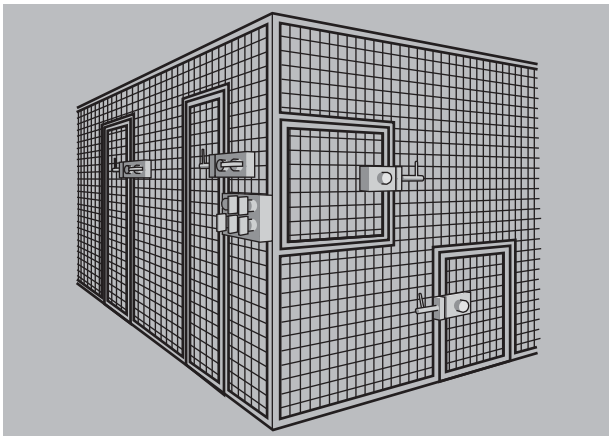


Figure 80: Defined Sequence of Events

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 IEC 61508, can be used in the e-stop circuit.

Emergency Stop Devices

Wherever there is a danger of an operator being exposed to a hazardous condition 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/EN 13850, IEC 60947-5-5, NFPA 79 and IEC 60204-1, AS 4024.1, Z 432-04.

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 81). They must be strategically placed in sufficient quantity around the machine to ensure there is always one in reach at a hazard point.

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.

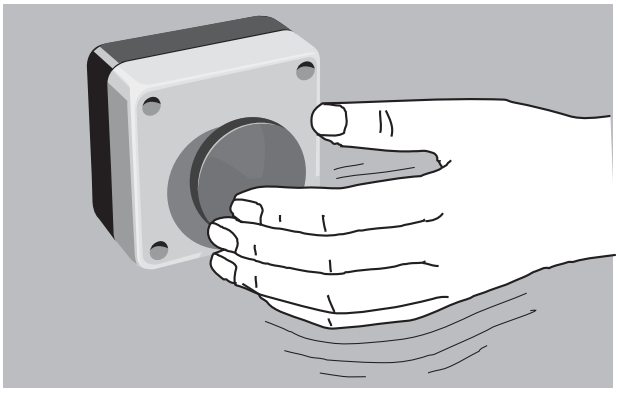


Figure 81: E-Stop Push Button—Red Colored Mushroom Head on a Yellow Background

One of the latest technologies to be applied to e-stops is a self-monitoring technique. An additional contact is added to the back of the 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 82 shows the self-monitoring contact connected in series with one of the direct opening safety contacts.

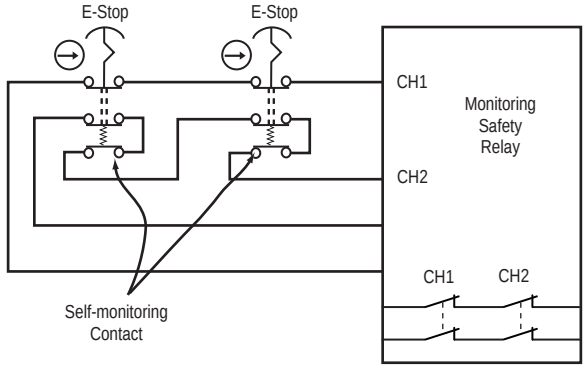


Figure 82: Self-Monitoring Contacts on E-Stop

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 83) 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.

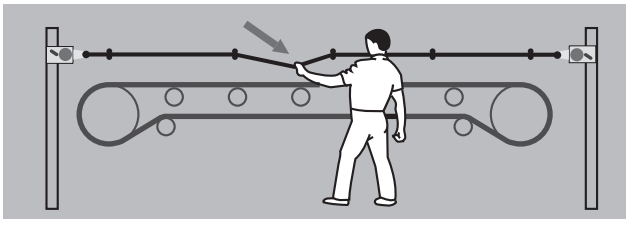


Figure 83: Cable Pull Switches

The cable pull switches must detect both a pull on the cable as well as when the cable goes slack. Slack detection ensures a severed cable is detected.

Cable distance effects 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 a single action by the operator initiates a stop command.

The required cable pull force should not exceed 200 N (45 lbs) 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 method of preventing access while a machine is in a dangerous condition. Two controls must be operated concurrently (within 0.5s of each other) to start the machine. This ensures 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 2 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 84.

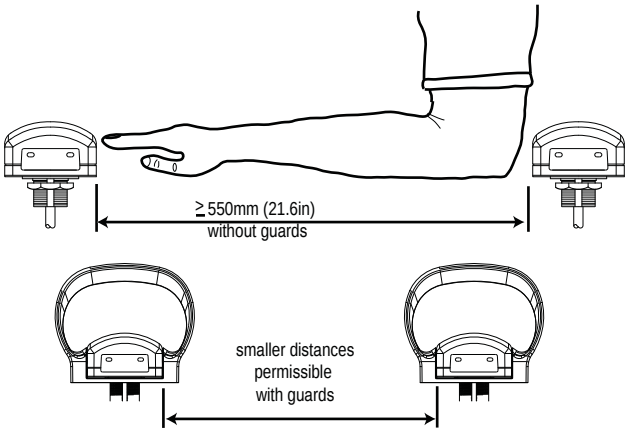


Figure 84: Separation of Two hand Controls

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 may 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- 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 85.

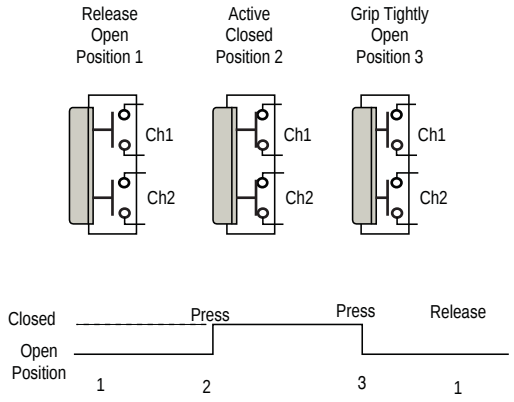


Figure 85: Enabling Switch Operation

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.

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 to indicate 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 crossfault detection for the dual channel arrangement.

Non-Contacts Interlocks and E-Stops

- Mechanical contacts, may be 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 crossfault detection. The MSR must be able to ignore the devices’ crossfault 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 four-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 in 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 0.5 sec. timing and sequencing logic.

MSRs must be designed specifically to interface with each of these types of devices, as they have different electrical characteristics. Some MSRs can connect to a few different types of inputs, but once the device is chosen, the MSR can only interface with that device. The system designer must select an MSR that is compatible with the input device.

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. When the input impedance is greater than 500 ohms, it will not switch on its outputs. Care must be taken by the user to ensure the input impedance remains below the maximum specification. The length, size, and type of wire used effects input impedance. Table 4 shows typical resistance of annealed copper wire at 25°C.

ISO Cross Section mm^2	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

Number of Input Devices

The risk assessment process should be used to help determine how many inputs devices should be connected to an MSR unit 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 rarely used. A program should therefore 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 functional test, and the time between functional tests is called the functional 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. 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 crossfaults, must be detected by the safety system. This is accomplished by the sensing device or the MSR.

Microprocessor-based devices (e.g., MSRs, light curtains, laser scanners, and the advanced non-contact sensors) detect these shorts in a variety of ways. One common way of detecting crossfaults is by using diverse pulse testing shown in Figure 86. 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.

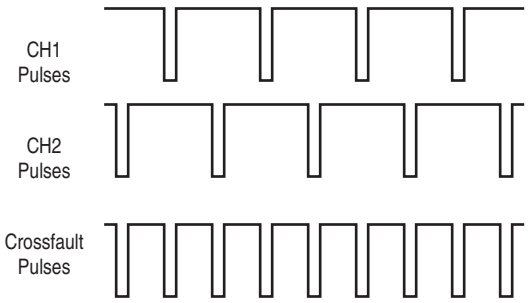


Figure 86: Pulse Testing to Detect Crossfaults

Electromechanically-based MSRs employ a different diversity technique: one pull-up input and one pull-down input. This is shown in Figure 87. A short from Channel 1 to Channel 2 will make the over-current protection device active and the safety system will shut down.

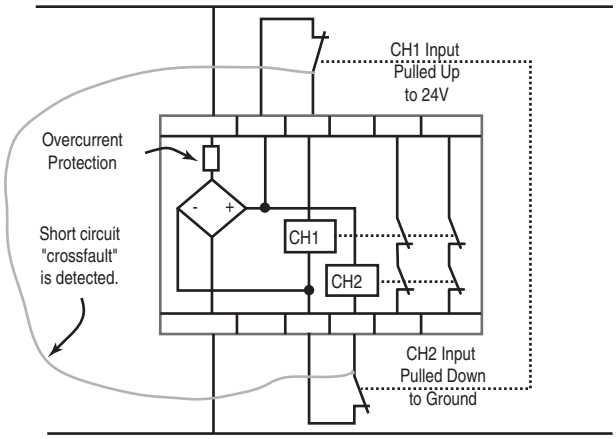


Figure 87: Diverse Inputs Detect Crossfaults

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 two 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 88 shows the symbols used for immediate and delayed contacts.

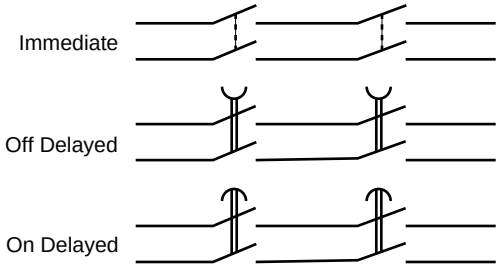


Figure 88: Symbols for Contact Types

MSRs also have auxiliary outputs. Generally these are considered normally closed and are used to signal the machine control system that the safety system is off. Figure 89 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.

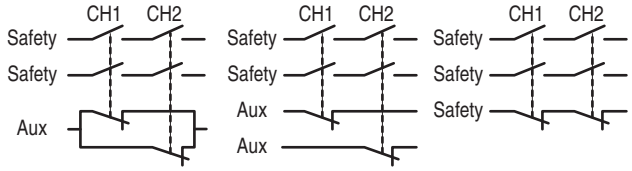


Figure 89: NC Contact Usage

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 90. An interlocked guard door is used as an example here but the requirements apply to other protection devices and emergency stop systems.

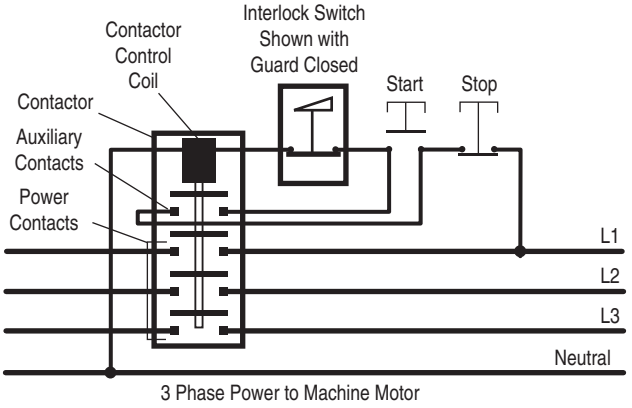


Figure 90: Simple Machine Start Stop Interlock Circuit

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 switch the normal start button to ON, 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 that operate as described above (or have a system that 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 closing and opening of a circuit after the gate is closed or the E-stop is reset. Figure 91 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 power switching contactors are connected in series with a momentary pushbutton. After the guard has been opened and closed again, the safety relay will not allow the machine to be restarted until after the reset button has been pressed and released. When this is done, the safety relay verifies (e.g., monitors) both contactors are off and that both interlock circuits (and therefore the guards) are closed. If these verifications are successful, the machine can then be restarted from the normal controls.

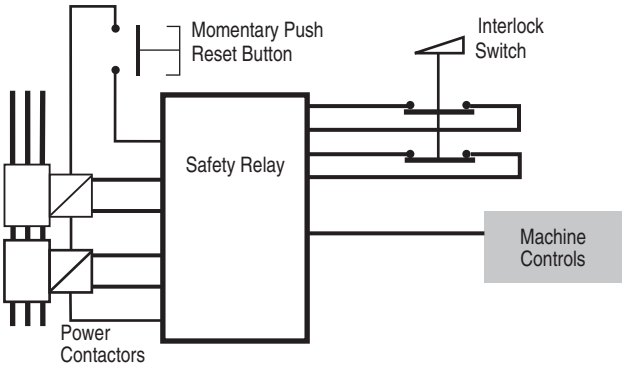


Figure 91: Monitored Manual Reset

The reset switch should be located in a place that provides a good view of the hazard so that the operator can check 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 shorted or jammed reset switch will not be detected.

Alternatively, the reset line can be jumpered, allowing an automatic reset. The user must then provide another mechanism for preventing machine startup 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 startup 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/her 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 92, come in various platforms to accommodate the scalability, functional, and integration requirements of the more complex safety systems.

Figure 92: Safety PLC Platforms

Hardware

Redundancy of CPUs, memory, I/O circuits, and internal diagnostics are enhancements that safety PLCs have that are not required in a standard PLC. A Safety PLC spends significantly more time performing internal diagnostics on memory, communications, and I/O. These additional operations are necessary to reach the required safety certification. The additional redundancy and diagnostics are taken care of in the operating system of the controller, making it transparent to the programmer, so that the safety PLC program functions much like a standard PLC program.

The microprocessors controlling these devices perform extensive internal diagnostics to ensure the performance of the safety function. Figure 93 provides an example block diagram of a safety PLC. Although microprocessor-based controllers differ slightly from one family to another, similar principles are applied to achieve a safety rating.

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 of the two microprocessors can perform the safety function, and extensive diagnostics are performed to ensure that both microprocessors are operating in sync.

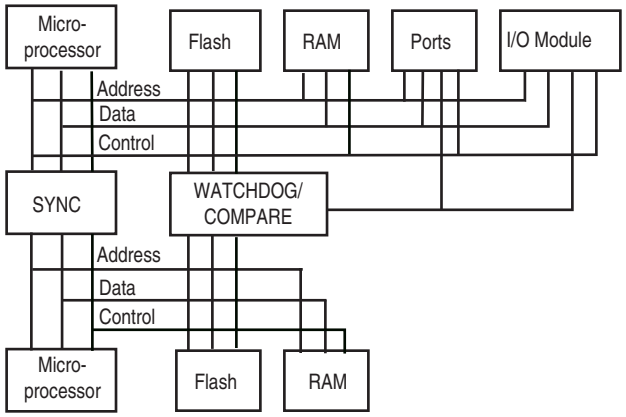


Figure 93: 1oo2D Architecture

Also, each input circuit is internally tested many times each second to make sure that it is operating correctly. Figure 94 shows a block diagram of an input. The E-Stop might only be hit once a month; but when it is, the circuit has been continuously tested so that the E-Stop will be sensed correctly internal to the safety PLC.

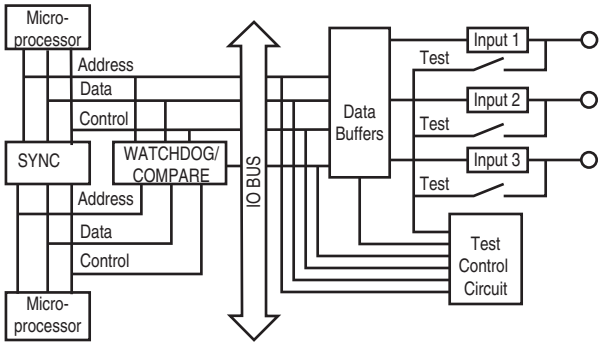


Figure 94: Block Diagram of a Safety Input Module

Safety PLC outputs are electromechanically or safety-rated solid-state outputs. Figure 95 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 they can turn the output off. If any one of the three circuits fail, the output is turned off by the other two, and the fault is reported by the internal monitoring circuit.

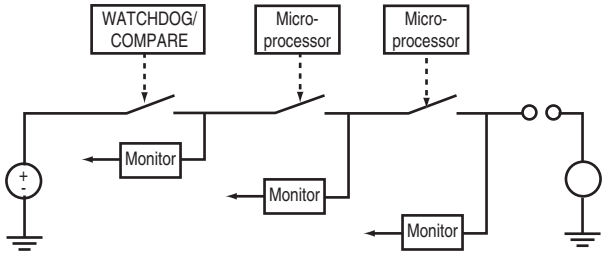


Figure 95: Safety Output Module Block Diagram

When using safety devices with mechanical contacts (E-stops, gate switches, etc), the user can apply pulse test signals to detect crossfaults. To avoid using expensive safety outputs, many safety PLCs provide specific pulsing outputs that can be connected to mechanical contact devices. A wiring example is shown in Figure 96. In this example, outputs O1, O2, O3, and O4 are each pulsing at a different rate. The safety PLC expects to see these different pulse rates reflected at the inputs. If identical pulse rates are detected, a crossfault has occurred and appropriate action is taken in the safety PLC.

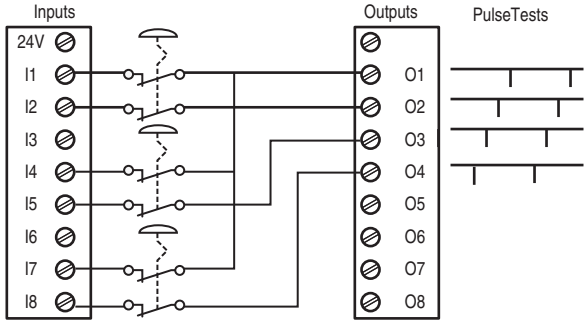


Figure 96: Pulse Testing of 2 N.C. Mechanical Inputs

Software

A safety PLC is programmed much like a standard PLC. All the additional diagnostics and error checking mentioned earlier are performed by the operating system. The programmer is not aware this 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 97 operates very much like an MSR127. Though the logic behind each of these instructions is complex, the safety program looks relatively simple because the programmer simply connects these blocks together. These instructions, along with other logic, math, data manipulation, etc. instructions are certified by a third party to ensure their operation is consistent with the applicable standards.

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.

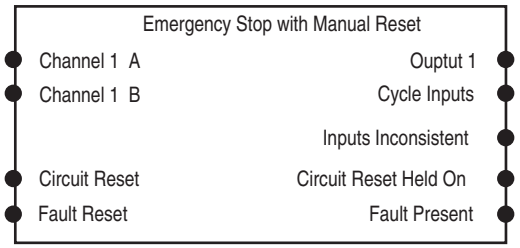


Figure 97: E-Stop Function Block

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 an example 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

A safety PLC generates 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 MSRs. Unlike wiring to specific terminals on MSRs, 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. Each feature improves productivity, reduces the time it takes to troubleshoot problems, and reduces training costs due to commonality.

Figure 98 shows an example of the integration of control and safety. The standard nonsafety related control functions reside in the main task. The safety related functions reside in the safety task.

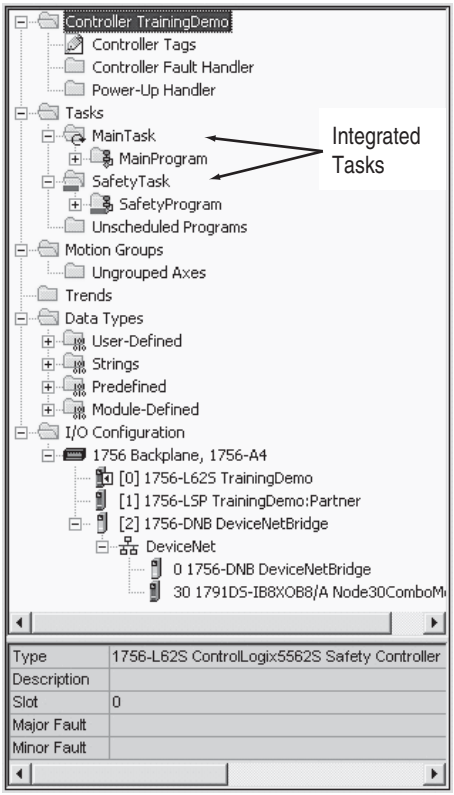


Figure 98: Integrated Safety and Nonsafety Tasks

All standard and safety-related functions are isolated from each other. Figure 99 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 (HMIs), personal computers (PCs), or other controllers.

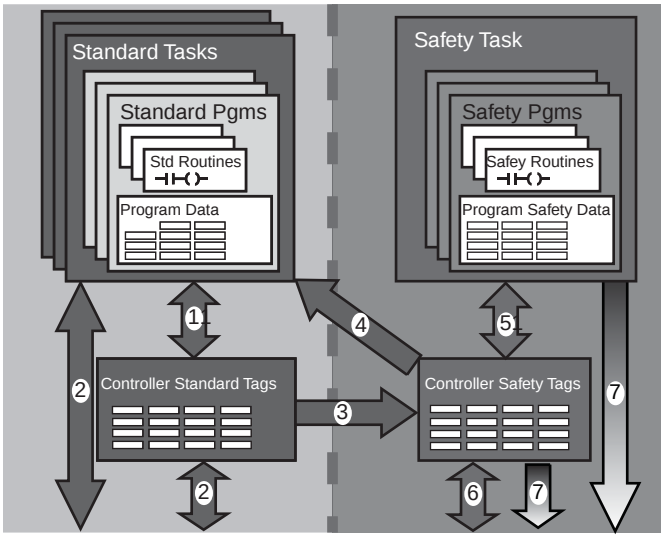


Figure 99: Standard and Safety Task Interaction

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 to 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, either 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 ability to improve flexibility, increase diagnostics, increase distance, reduce installation and wiring costs, 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 referred to as a safety state (safe 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), which increased 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 100 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 safety data to 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 announce 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.

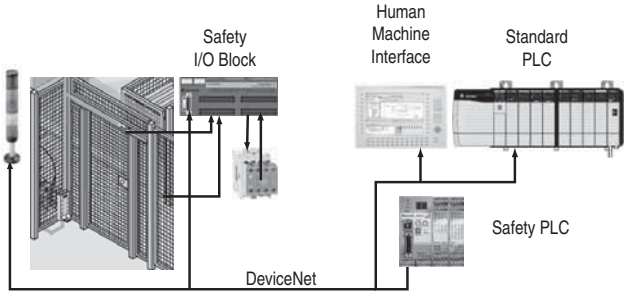


Figure 100: Example of a Simple Distributed Safety Network

For larger manufacturing systems, where safety information and control must be shared, Ethernet/IP can also be used. Figure 101 shows an example of communications between two safety controllers while DeviceNet is used for local distribution of I/O within a smaller subsystem.

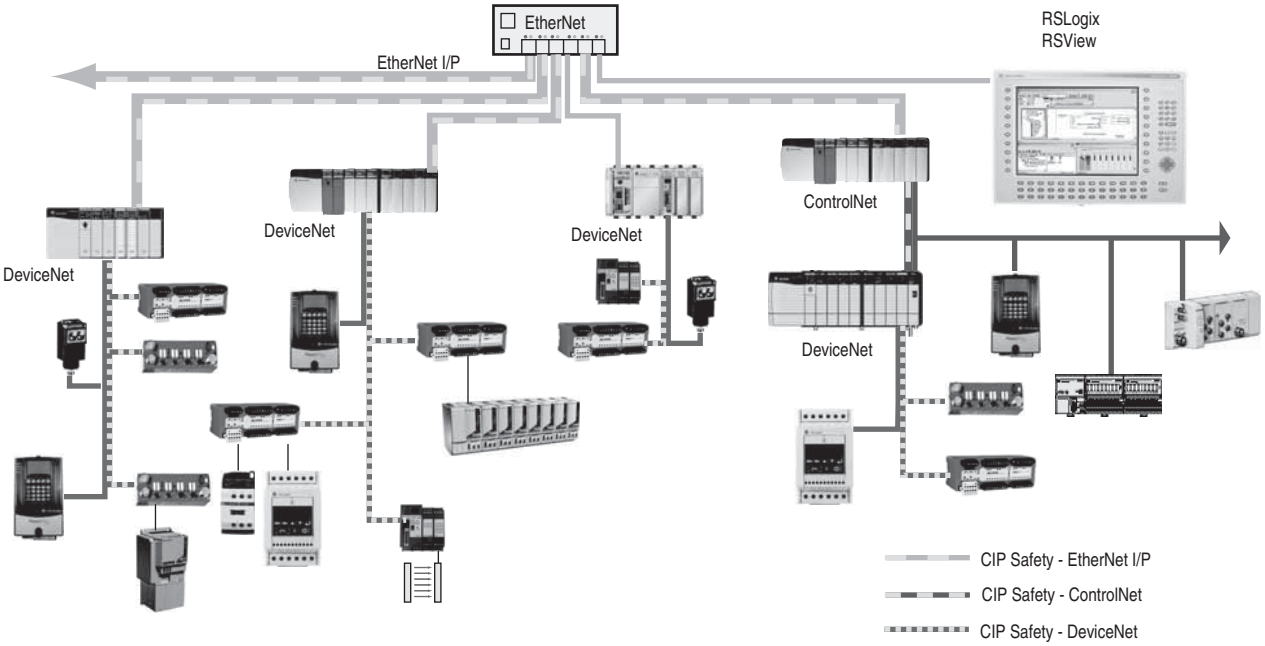


Figure 101: Example of a Complex Distributed Safety Network

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 normally-open contacts can not 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 0.5mm. 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 102 is applied to the product.

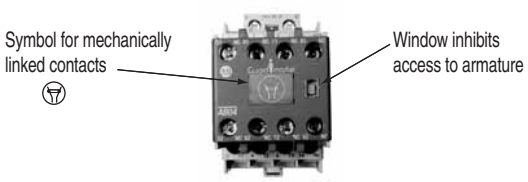


Figure 102: Mechanically Linked Contact Symbol

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.

On larger contactors, an adder deck is insufficient to accurately reflect the status of the wider spanner. In this case, mirrored contacts, shown in Figure 103, are located on either side of the contactor.

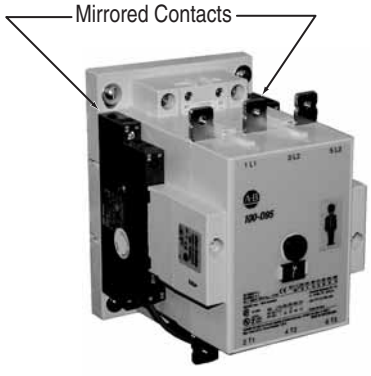


Figure 103: Mirrored Normally Closed Contacts

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 dropout time is not effected. For DC powered coils, the dropout time is increased. The increase is dependent on the type of suppression selected.

Control relays and contactors are designed to switch large current loads, 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 lower current.

Overload Protection

Overload protection for motors is required by electrical standards and local building codes. Diagnostics provided by the overload protection device enhances equipment and operator safety. Technologies available today can detect fault conditions such as an overload, phase loss, ground fault, stall, jam, under-load, current imbalance, and over-temperature. Detecting and communicating abnormal conditions prior to tripping helps improve production up time and helps protect operator and maintenance personnel from hazardous conditions.

Figure 104 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 required for each motor.

Figure 104: 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. It is a hardware signal that removes the input signal to the gate control circuitry. The second channel is a positive guided relay that removes 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 105.

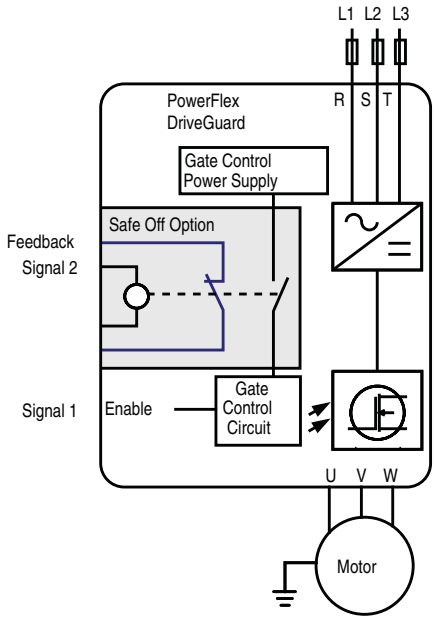


Figure 105: Drive Safety Signals

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

The servo achieves a result similar to the AC drives. Figure 106 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.

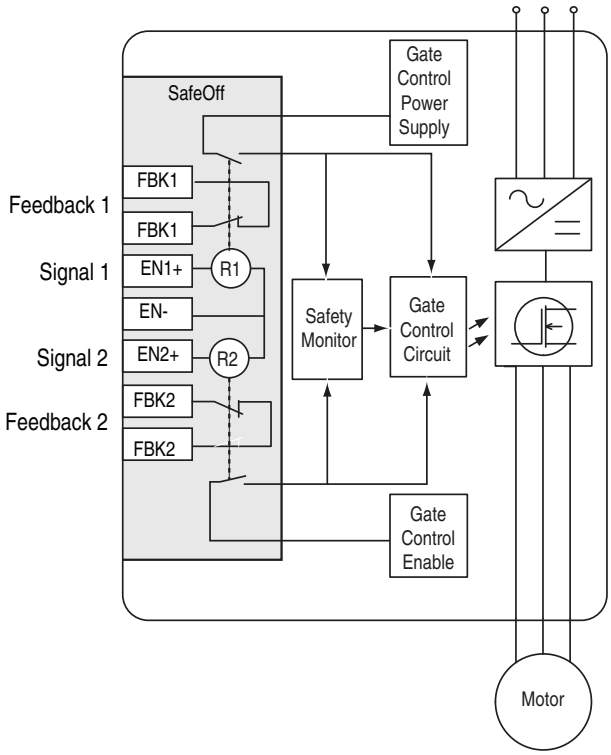


Figure 106: Kinetix Drive Safety Signals

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 107 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.

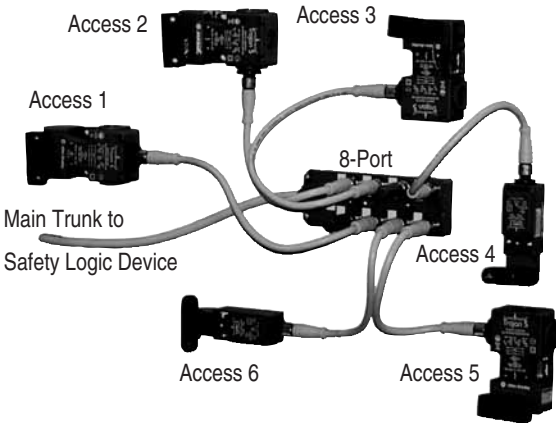


Figure 107: Safety Distribution Block

When a diverse set of devices is required, an ArmorBlock Guard I/O box can be used. Figure 108 shows an 8-port and 4-port block with an IP 67 rating which can be mounted on the machine without an enclosure. The inputs can be configured by software to accommodate various types of devices.

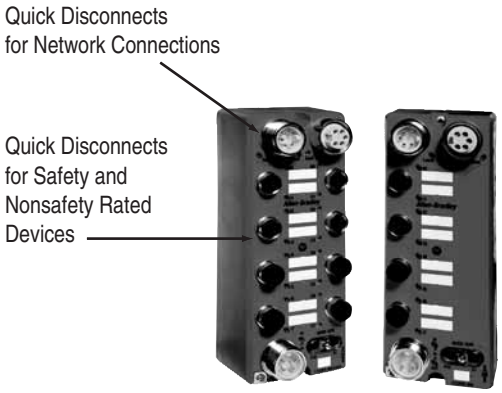


Figure 108: ArmorBlock Guard I/O

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

US CAN: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

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 curtain or area scanner is used, the approach to the detection device must be considered. The three approach considerations are:

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./sec.) 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./sec.) to 2500 mm/sec. (100 in./sec.). 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 least desirable stopping time of the machine/equipment. Tc is the least desirable 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 Factor 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 109 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.

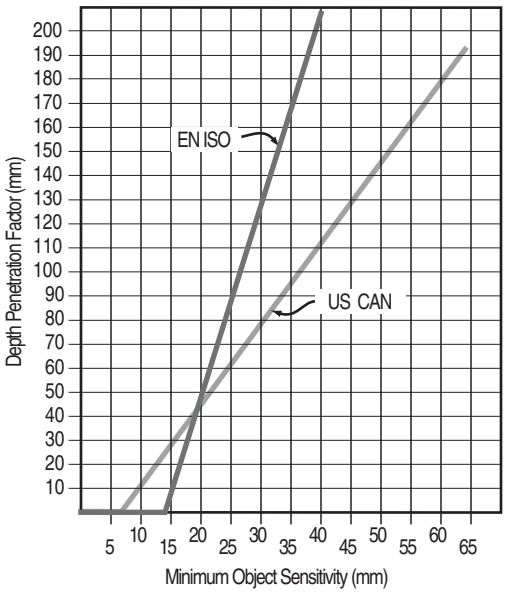


Figure 109: Depth Penetration vs. Object Sensitivity

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 110 summarizes the differences. The ISO EN value is 850 mm where the US CAN value is 900 mm. The standards also differ in the object sensitivity. Where the ISO EN standard allows for 40…70mm, the US CAN standard allows up to 600 mm.

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. This value 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.

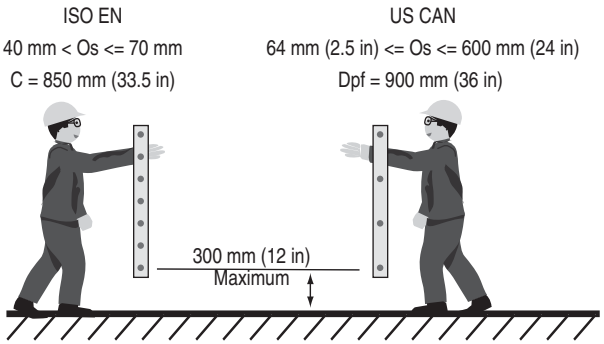


Figure 110: Depth Penetration Factors for Reach-Through Applications

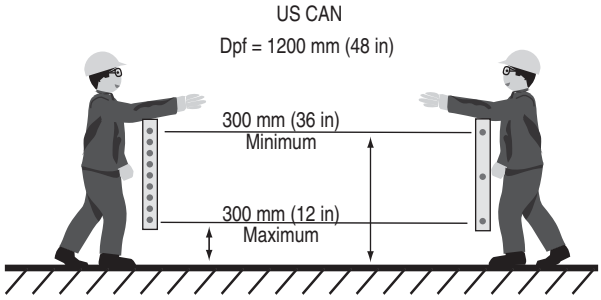


Figure 111: Depth Penetration Factors for Reach-Over Applications

Single or Multiple Beams

Single- or multiple-separate beams are further defined by the ISO EN standards. Table 7 shows the practical heights of multiple beams. 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 considered.

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 US CAN are close, but differences do exist. For the normal approach to vertical light curtains where the object sensitivity is a maximum of 40 mm, 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 S can be is 100 mm. When the distance is greater than 500 mm, the value of K can be reduced to 1600. When using K=1600, the minimum value of S is 500 mm.

The US 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 112 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.

Safety Distance Calculation

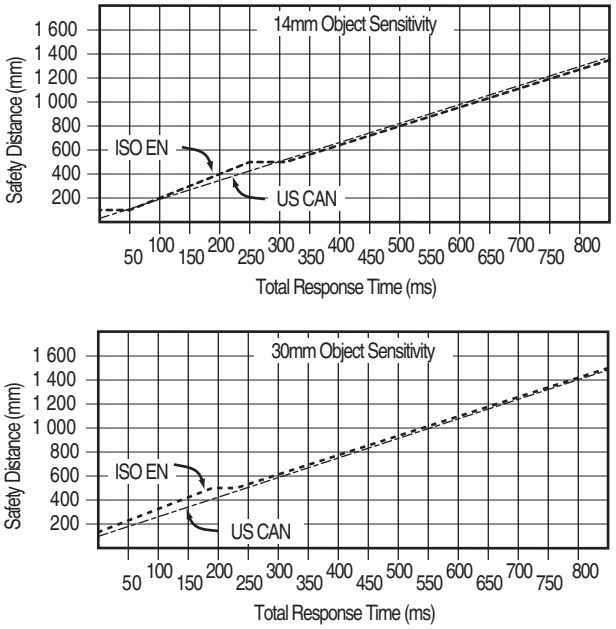


Figure 112: Safety Distance Comparisons

Angled Approaches

Most light curtains and scanners are mounted vertically (normal approach) or horizontally (parallel approach). These mounting configurations are not considered angled if they are within +/-5° of the intended design. When the angle exceeds +/-5°, potential risks (e.g., shortest distance) must be considered. 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 shown in Figure 113.

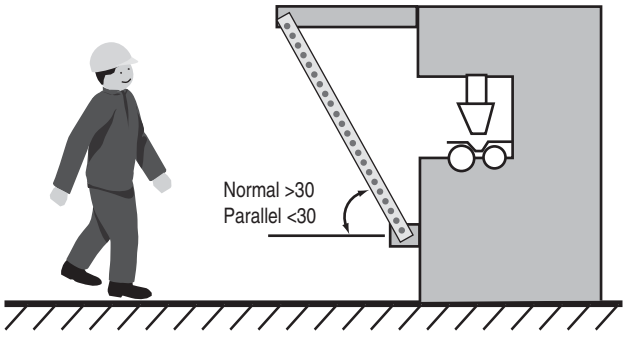


Figure 113: Angular Approach to the Detection Field

Safety Mats

With safety mats, the safety distance must take into account the pace and stride of the operator, assuming the operator is walking and the safety mats are installed on the floor. The operator's first step on the mat is a depth penetration factor of 1200 mm (48 in.) as shown in Figure 114.

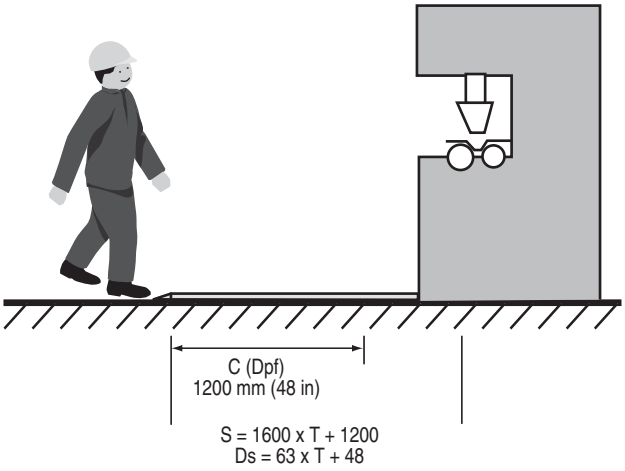


Figure 114: Safety Mat Mounted on Floor

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 115).

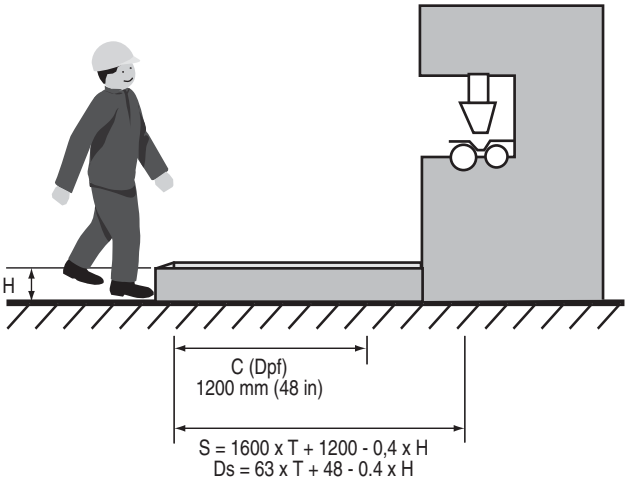


Figure 115: Step Up to Safety Mat Mounted on a Platform

Examples

Example: An operator uses a normal approach to a 14 mm light curtain, which is connected to an MSR 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 0. 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
Ds = 63 x (0.17 + 0.13 + 0) + 1
Ds = 63 x (0.3) + 1
Ds = 18.9 + 1
Ds = 19.9 in (505 mm)

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18.9 in)

Therefore, the minimum safe distance the safety light curtain must be mounted from the hazard is 20 inch or 508 mm, 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: ISO14118, EN1037, ISO12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05, AS 4024.1603, NFPA70[NEC] 430.109(a)(7). These standards have a common theme: the primary method of preventing unexpected power up is to remove the energy from the system and lock the system in the off state. The purpose is to safely allow people to enter a danger zone of a machine.

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 lock to the energy isolating devices. Each lock must be identifiable to its owner.

In the US, 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 116 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.

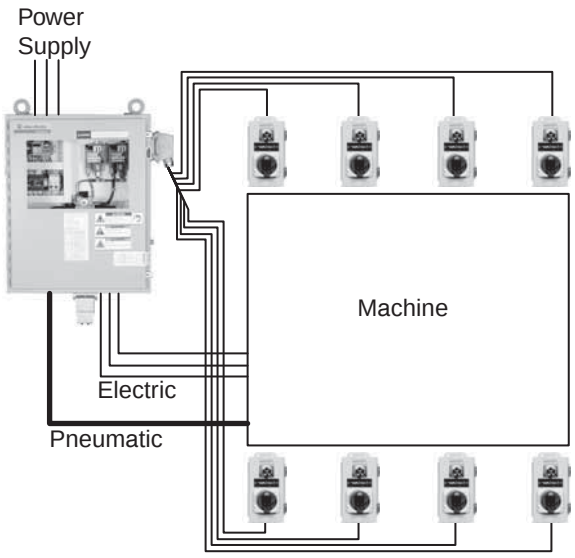


Figure 116: Layout of Safety Isolation System

Figure 117 shows the safety isolation system not only removes power from the machine, but also grounds the load side. The operator receives a monitored, visible signal at the remote station indicating the machine is in a safe state and the energy has been dissipated

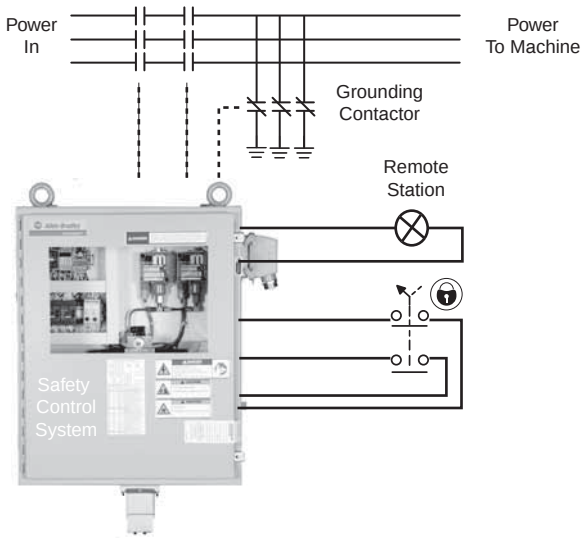


Figure 117: Machine side is grounded with signal to operator.

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 capable of both isolation and lockout. Figure 118 shows an example of Bulletin 194E.

Figure 118: 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 119 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.

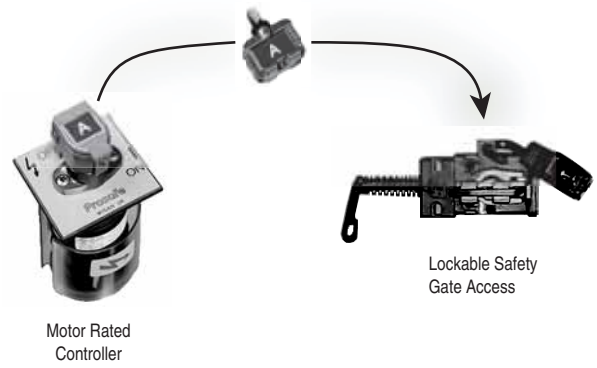


Figure 119: Trapped key isolation and lockable devices

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. The work is performed using alternative measures, like safeguarding, which provide effective protection. Safeguarding includes devices such as interlocked guards, light curtains, and safety mats. Used with appropriate safety rated logic and output devices, operators can safely access machine danger zones during normal production tasks and minor servicing.

Structure of Safety Related Control Systems

Overview

A safety related control system (SRCS) is the part of the machine control system 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 a power contactor, to a compound system comprising of 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.

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 using the equipment; that is, a hazardous condition.

A machine must usually have at least one hazard. A hazardous condition occurs when a person is exposed to a hazard. A hazardous condition does not imply 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 an unexpected startup. The main task of the safety system designer is to prevent hazardous conditions and unexpected startups.

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 hazards 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 interruption 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 categorized as to their design intent and ability to ensure the performance of the safety function.

Categories of Control Systems

The following discussion of categories is based on ISO 13849-1:1999, which is equivalent to EN 954-1:1996. In 2006, ISO 13849-1 was significantly revised to agree with IEC 62061 and IEC 61508, both of which can be used for highly complex safety systems. The 2006 version of ISO 13849-1 continues to utilize categories of safety performance; the categories are considered the structure or architecture of the SRCS. Additional information about the components and system design complement this structure to provide a performance level rating. The following category discussion applies to both the 1999 and 2006 revisions of ISO 13849-1.

The standard ISO 13849-1 safety-related parts of control systems, Part 1 General principles for design lays down a language of five categories for benchmarking and describing the performance of SRCSs. See Table 8 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.

So how do you decide which category you need? The risk assessment process should direct you to the proper category. In order to translate these requirements into a system design specification, there has to be an interpretation of the basic requirements.

It is a common misconception that Category 1 provides the least protection and Category 4 provides the most protection. This is not the reasoning behind the categories. They are intended as reference points that describe the functional performance of different methods of safety related control and the constituent parts.

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 key 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 key to these categories. Redundancy is the duplication of the same technique. Diversity is using two different techniques. Monitoring is checking the status of the devices and then taking appropriate action based on results of the status. The usual, but not the only method of monitoring is to duplicate the safety critical functions and compare operation.

Category B

Category B provides basic requirements of any control system; whether it is a safety related or non-safety related control system. 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.

Although we have a system that meets our reliability goals, we know the system will fail eventually. The safety system designer needs to know whether the system will fail to danger or whether it will fail to a safe state. The mantra is, “How does the system perform in the presence of faults?”

Starting with this concept, what principles should be followed to guide the system design? Cat 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:

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.	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 8: Categories of Safety Performance

- Proper selection, combination, arrangements, assembly and installation (i.e., per mfg'rs 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

Figure 120 shows an example of a Category B system. The guard is interlocked with a negative-mode (spring driven) limit switch. Short circuit and overload protection is provided to meet the electrical standard requirements for protection of the control circuit. Transient suppression is used to help prevent contact welding when the contactor coil is de-energized. The de-energization principle is used: the guard interlock turns the motor off. The components must be selected and installed to meet the foreseeable environment conditions and current/voltage requirements. Note that no special measures for safety are applied under Category B. Therefore, additional measures may be required.

Press the start button with the guard closed to energize the motor, which symbolizes the hazard. When the K1 contactor closes, an auxiliary contact maintains the circuit and the start button can be released. Press the stop button or open the guard to turn the motor off. Releasing the stop button or closing the guard does not cause the motor to restart.

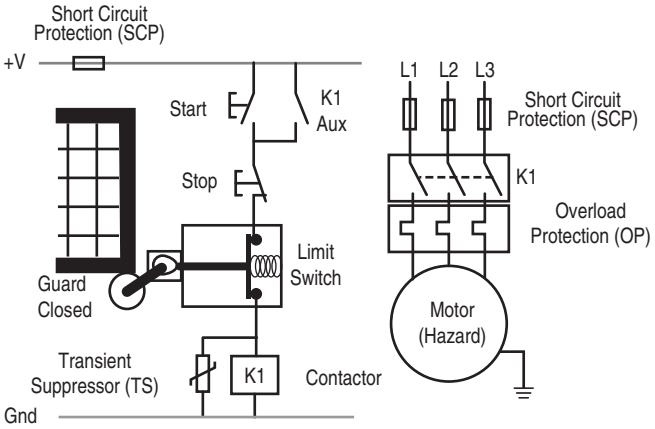


Figure 120: Simple Category B System

Figure 121 shows a complex system that meets Category B. Here, multiple sensing devices (limit switches) and push buttons are connected to the input module of a programmable logic controller (PLC). Multiple actuators are connected to the output module. A software-controlled logic module determines which outputs to turn on or off in response to the state of the sensing devices.

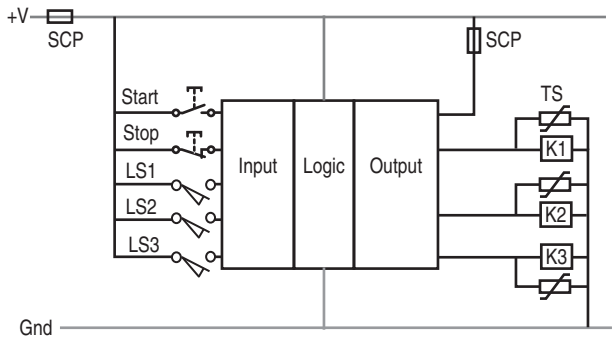


Figure 121: A Complex Category B System

How do we know these circuits meet Category B?

First, the designer must select, install, and assemble the devices according to the instructions provided by the manufacturer. These devices must work within the expected voltage and current ratings. The expected environmental conditions, like electromagnetic compatibility, vibration, shock, contamination, and 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. All wiring and grounding meets appropriate electrical standards.

The next step in the safety analysis is to separate the system into its major components and consider their modes of potential failure. Previously we looked at the system as three blocks. When considering safety system performance, the wiring must also be included in the analysis. Figure 122 shows the safety system block diagram.

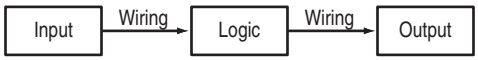


Figure 122: Safety System Block Diagram

In the Category B examples, the components are:

- Interlock (Limit) switch
- Programmable logic controller
- Contactor
- Wiring

Interlock Switch

The limit switch is a mechanical device. The task it performs is a simple one — open the contacts when the guard opens. Years ago, limit switches were used in this fashion. But their design has limitations that do not provide enhanced safety performance.

Electrical standards require short circuit protection devices (e.g., fuses or circuit breakers) for branch circuits. This protection may not be enough to prevent a welded contact in the limit switch. The contacts in the limit switch are designed to open by the force of a spring. Unfortunately, the spring force is not always strong enough to overcome the force of a welded contact.

A second consideration is the spring itself. Repeated flexing may eventually lead to breakage and the force exerted on the contacts may not be enough to open the circuit. Other internal faults in the operator head or the linkage may also result in the contacts remaining closed when the guard is opened. Another important consideration is defeatability. When the guard is open, the limit switch is easily defeated by pushing the lever into the actuated position and holding it in place with tape, wire, or simple tools.

Programmable Logic Controller

PLCs are the preferred control system for machines. The input devices, like limit switch interlocks, are connected to input modules. The output devices, like contactors, are connected to the output modules. The logic device assigns the input devices to the appropriate output devices under the desired logic conditions.

Although reliability of PLCs has dramatically improved since their introduction, they will eventually wear out and fail. The safety system designer needs to understand the potential mechanism failure and whether that failure will result in a dangerous condition. PLCs have two major categories of failure: hardware and software.

Hardware failures may occur internally in the input, logic, or output modules. These failures may cause the outputs to remain energized, even though a stop command is initiated. Software failures in the application program or in the firmware may also lead to the outputs remaining energized even though a stop command is initiated.

Contactor

Contactors energize a machine's actuators; motors, solenoids, heaters, and other types of actuators. The actuators use high currents, and some have inrush currents that can be 10 times greater than their steady state value. Contactors should always have their power contacts protected by overload and short-circuit protective devices to prevent welding. Even with this protection, a potential exists for the power switching contacts to remain closed. This may be due to welding or a stuck armature. When a fault of this nature occurs, the stop button becomes ineffective and the machine must be de-energized by the main disconnect switch.

Contactors should be regularly inspected to detect loose connections that can lead to overheating and distortion. The contactor must comply with relevant standards that cover the required characteristics and conditions of use. IEC60947-4-1 and IEC60947-5-1 describe detailed tests that contactors must meet for use in various applications.

Wiring

Although designing and installing to the appropriate electrical standard reduces the chances of wiring failures, wiring faults do occur. Wiring faults to consider include both short circuits as well as open circuits. Short-circuit analysis must include shorts to power, shorts to ground, and shorts to other circuits that may lead to a hazardous condition.

Start and Stop Switches

Consideration must be also given to the start and stop switches. If the start button fails shorted, the machine will unexpectedly restart when the stop button released or the guard is closed. Fortunately, the guard must be closed to start the motor. If the guard is closed, then access to the hazard should be protected. A broken stop button or short across its contacts will inhibit the stop command from being executed. Again, the guard is closed so access to the hazard should be protected.

The safety related parts of the control system must interface with the non-safety related parts. Since faults across the start and stop control devices should not lead to a loss of the safety function, these devices are not considered part of the safety system. This start/stop/holding circuit symbolizes the non-safety rated parts of the machine control circuitry and can be substituted with a PLC.

Category B provides the foundation for safety system design. Although proper design, selection, and installation provide a basis for a robust system, many potential single factors can lead to the loss of the safety system. By attending to these factors, the possibilities of failure (danger) can be further minimized. The use of Category B on its own is not suitable for most safety related applications.

Category 1

Category 1 requires the system to meet the terms of Category B and to use well-tried safety components. What exactly are safety components and how do we know whether they are well-tried? ISO 13849-2 helps answer those questions 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 9 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 9: 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 123 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 IEC60947-5-1 for direct opening action contacts, which is shown by symbol representation of an arrow within a 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.

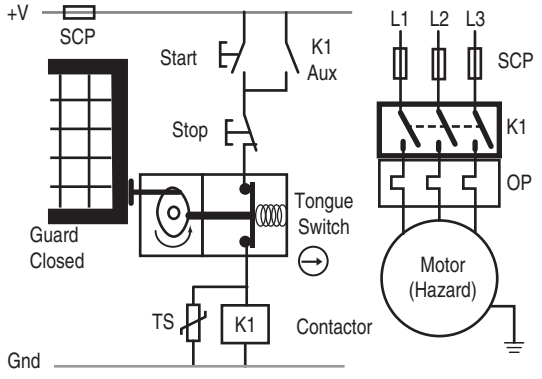


Figure 123: Category 1 of Simple Safety System

Can we apply these same principles to the PLC based Category B system to enhance the safety performance to Category 1?

Replacing all limit switches operating in negative mode with direct opening-action interlocks and over-dimensioning the contactors will improve the probability of performing the safety function. The PLC then becomes the focus of attention.

Has the PLC been used in similar applications? Is the logic program validated and stable or is it constantly modified for improvements and adjustments? Has firmware (software a user cannot modify) been revised recently? What is the history of hardware failures-to-danger in similar applications? Have steps been taken to eliminate or reduce these failures to acceptable levels?

In theory, it is possible that a PLC could be considered a well-tried component based on a proven in use construct. To adopt this approach for a device such as a PLC would be a significant undertaking involving an extremely high level of record keeping and analysis. In order to simplify the situation and avoid the arbitrary use of ordinary PLCs, ISO 13849-1:1999 states that on the level of single electronics alone, it is not normally possible to realize Category 1.

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. Whenever possible, the command must bring the machine to a safe state.

Figure 124 shows a block diagram of a Category 2 system. The test must provide reasonably practical detection of faults. The equipment performing the test can be an integral part of the safety system or a separate piece of equipment.

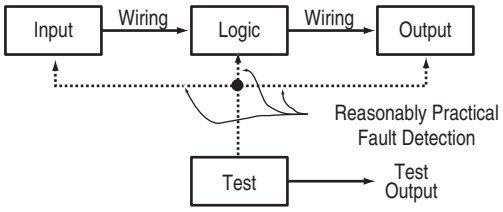


Figure 124: Category 2 Block Diagram

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.

The words *whenever possible* and *reasonably practical* 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 components can be checked.

Figure 125 shows the simple Category 1 system enhanced to meet Category 2. A monitoring safety relay (MSR) feature 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.

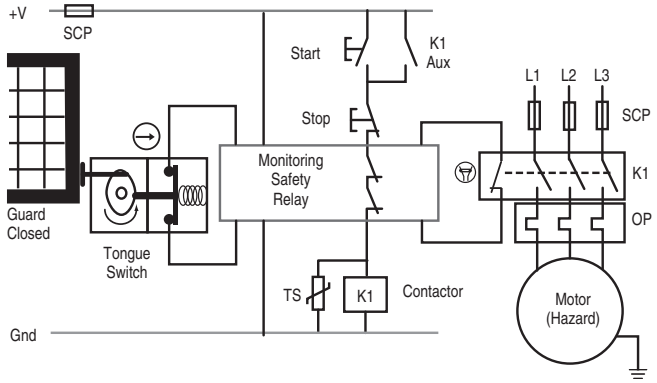


Figure 125: Category 2 Safety System

Opening the guard turns the outputs of the MSR off. When the guard is closed again, the MSR repeats the safety system checks. If no faults are discovered, the MSR turns on its 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 PLC-based safety system can be designed to meet Category 2. As stated in the Category 1 discussion above, the well-tried justification of the PLC (including its testing capabilities) becomes the challenge. For complex safety systems requiring a Category 2 rating, a PLC safety-rated to IEC 61508 should be substituted for the non-safety rated PLC.

Figure 126 shows an example of a complex system using a safety rated PLC. A safety rated PLC meets the requirements of well-tried as 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.

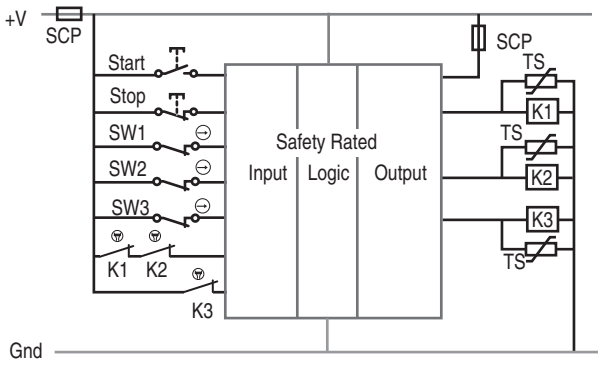


Figure 126: Complex Category 2 Safety System

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 required, 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 feasible.

Here again, we have the phrase *whenever feasible*. 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 127 explains the principles of a Category 3 system. Redundancy combined with feasible cross monitoring and output monitoring are used to ensure the performance of the safety function.

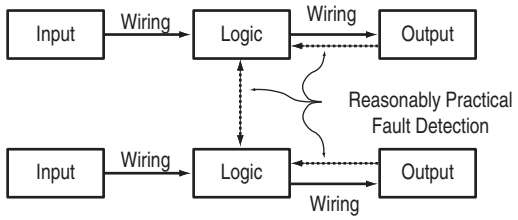


Figure 127: Category 3 Block Diagram

Figure 128 shows an example of a Category 3 system. A redundant set of contacts are added to the tongue interlock switch. Internally, the MSR contains redundant circuits that cross monitor each other. A redundant set of contactors removes power from the motor. The contactors are monitored by the MSR through the *feasible* mechanically linked contacts.

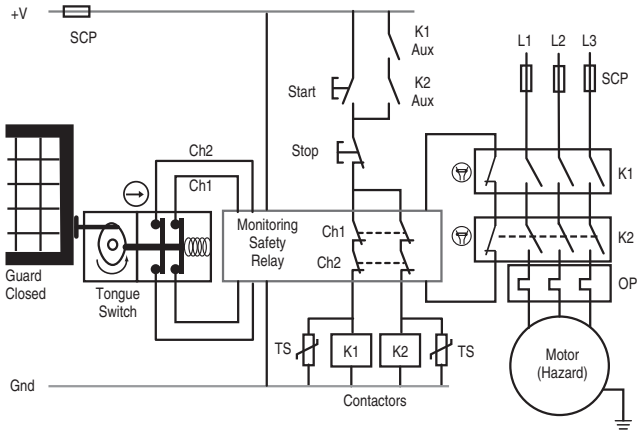


Figure 128: Category 3 System

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 opening the guard is designed to open a welded contact. This resolves one failure mode. Do other failure modes exist?

The direct opening action switch is usually designed with a spring operated 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? These questions will be answered in the near future as mean time to dangerous failure, diagnostic coverage, and safe failure fraction must be provided to meet the increasing knowledge required to assure the performance 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.

An electro-mechanical based monitoring safety relay is a low-complexity device that is often evaluated by a third party and assigned a category level. The MSR often includes dual channel capability, cross-channel monitoring, external-device monitoring, and short-circuit protection. No specific standard is written to provide guidance on the design or usage of MSRs. MSRs are evaluated for their ability to perform the safety function per ISO 13849-1 or its predecessor EN 954-1. To meet a system safety category rating, the MSR must be the same or have a higher rating.

Two contactors help ensure 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 with its power switching contacts 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

As stated earlier, some faults cannot be detected. These faults alone, do not lead to the loss of the safety function. When evaluating faults, a series of questions must be asked. The answer to the first question will lead to different follow-up questions:

Opening Question: Can the fault be detected?

If yes, then we need to know whether this detection is immediate or on the next demand. We also need to know if it can be masked (i.e., cleared) by other devices.

If no, did the fault lead to the loss off the safety function? Would a subsequent fault lead to the loss of the safety function?

Figure 129 shows a widely used approach for connecting multiple devices to an MSR. 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. Can this fault be detected?

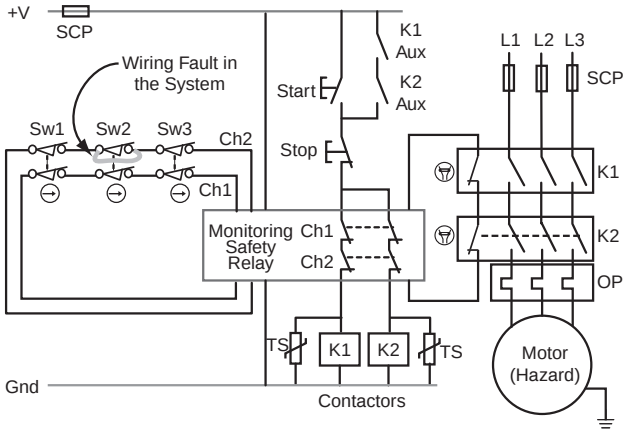


Figure 129: Series Connection of Inputs Devices

When switches Sw1 and Sw3 are opened, the MSR successfully removes power from the hazard. When Sw1 and Sw3 are closed the hazard can be restarted by pressing the start button. During these actions, the fault was not detected but did not lead to the loss of the safety function. What occurs when Sw2 is opened?

When Sw2 opens, 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. The weakness to this design is that switch Sw1 or Sw3 can be opened and closed and mask the fault. A subsequent fault (a short circuit across the second contact or Sw2) will lead to the loss of the safety function. 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.

Figure 130 shows a Category 3 circuit using a safety rated variable frequency drive. Recent developments in drive technology coupled with the updating of the electrical 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. 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 practical 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.

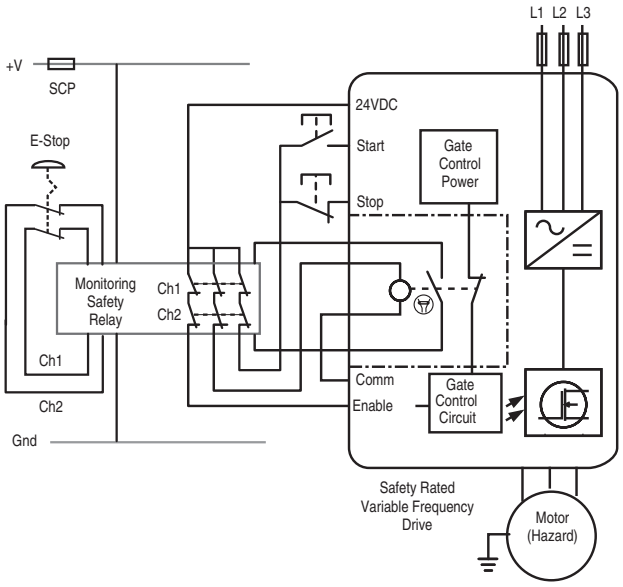


Figure 130: Safety Rated Drives with E-stop Rated to Category 3

Figure 131 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 enhancements or maintenance. Can this fault be detected?

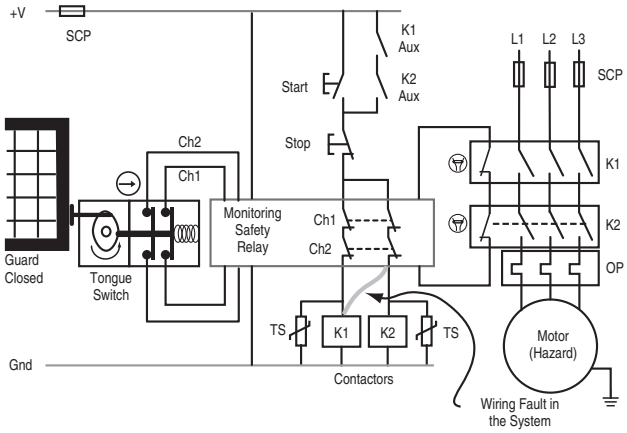


Figure 131: Example 1 of Wiring Fault

This fault cannot be detected by the safety system as shown. Fortunately, it does not lead to the loss of the safety function. This fault, as well as the fault from Ch1 to K2, must be detected during commissioning.

Figure 132 shows a second fault that leads to the loss of the safety function. This is a short from the output of the MSR to the start button. Upon power-up with the guard closed, these two faults go undetected. Pressing the start button initiates the hazard. Opening the guard does not cause the hazard to turn off.

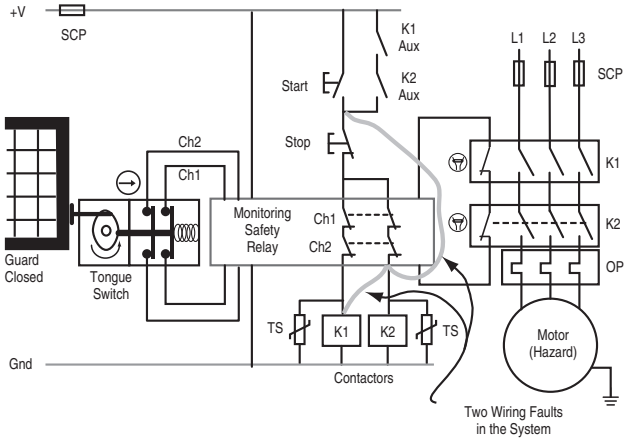


Figure 132: Two Faults Lead to Loss of Safety Function

Figure 133 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?

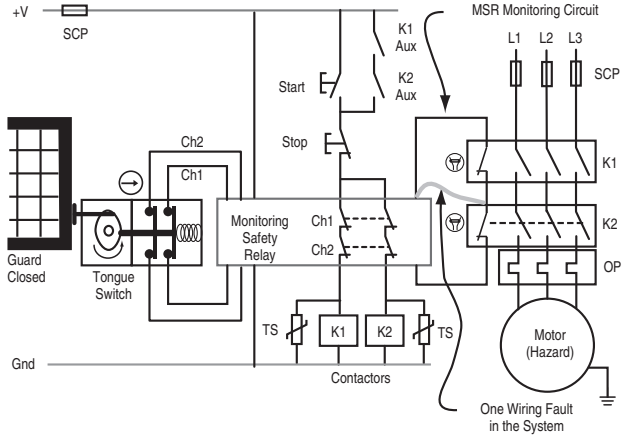


Figure 133: Monitoring Circuit Fault

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.

Figure 134 shows the same situation as shown in Figure 133, 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 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.

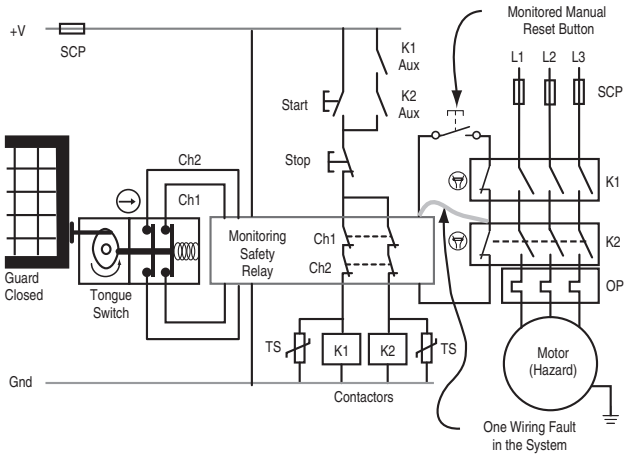


Figure 134: Monitored Manual Reset to Detect Fault

Figure 135 shows a cross-channel input fault. A fault occurs from Ch1 to Ch2 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 MSR. MSRs designed for two normally-closed contacts utilize diverse inputs. One input is pulled up to +V, and the second input is pulled down to ground. A wiring short will be detected immediately and the safety input of the MSR will turn off, removing energy from the hazard.

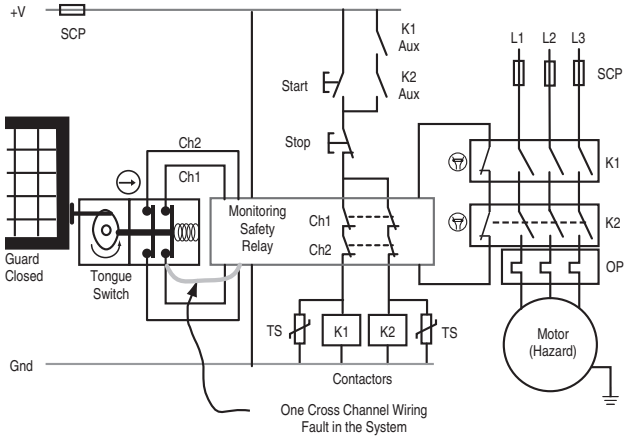


Figure 135: Cross Channel Input Fault

Some MSRs are designed to interface with input devices such as light curtains and laser scanners. These devices have solid state OSSD (Output Signal Switching Devices) with built-in cross-fault detection.

Figure 136 shows an example safety system with light curtains (OSSD outputs). Can the safety system detect this fault?

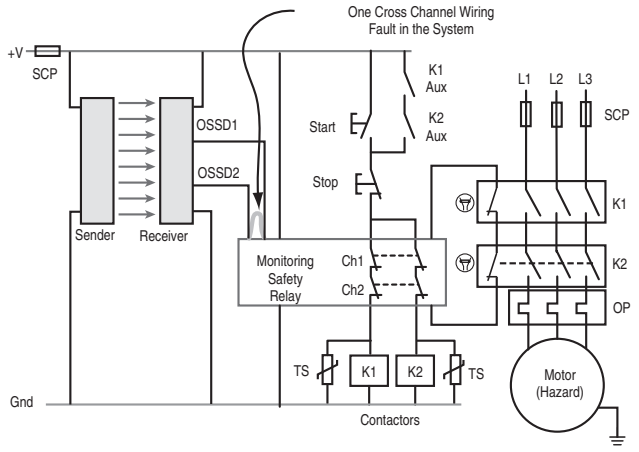


Figure 136: Cross Channel Wiring Fault with Light Curtains

The MSR cannot detect this fault, because both inputs are pulled up to +V. In this example, the wiring fault is detected by the light curtain. Some light curtains use a fault detection technique called pulse testing. With these light curtains, the detection of the fault is immediate and the light curtain turns off its output. In others, the detection is made when the light curtain is cleared. When the light curtain attempts to energize its output, the fault is detected and the output remains off. In either case, the hazard remains off in the presence of the fault.

Pulse Testing Fault Detection

Safety circuits are designed to carry 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 crossfault short circuit occurs, the microprocessor detects the pulses on both channels and initiates a command to turn the hazard off.

Figure 137 illustrates this principle. This technique also detects shorts to the +V supply.

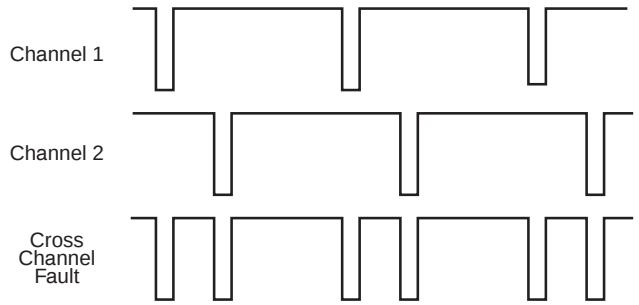


Figure 137: Cross Channel Fault with Pulse Testing

Microprocessor-based safety monitoring relays and safety PLC-based systems use the pulse testing technique as their inputs are not diverse; they are designed to interface with pull-up devices.

Figure 138 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 practical to detect cross-channel faults in this manner

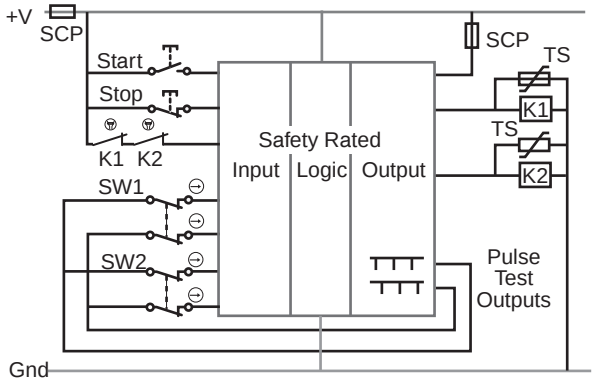


Figure 138: Safety PLC using Pulse Testing for Fault Detection

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 139 shows a variation of a Safety PLC arrangement. In some cases, connecting a non-safety rated device to a safety system is necessary 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 the reasonable requirements of Category 3.

Another consideration for Safety PLC modules is the number of inputs. Occasionally, one or two additional inputs may be required, 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 trade off is the loss of information as to which switch is actuated, unless an additional contact is used and connected to the machine control system.

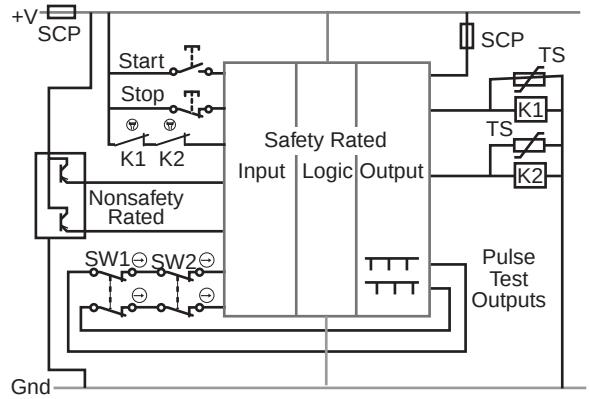


Figure 139: Complex Inputs Meeting Category 3 with a Safety PLC

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. When considering an accumulation of faults, two faults may be sufficient, although three faults may be necessary for some designs.

Figure 140 shows the block diagram for Category 4. Monitoring both output devices and cross monitoring is essentially required, not just when reasonably practicable. This helps differentiate Category 4 from Category 3.

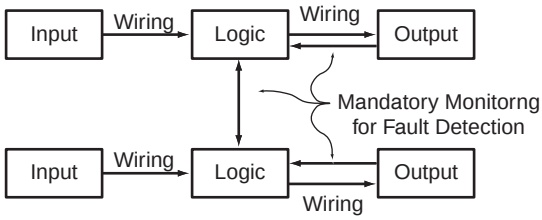


Figure 140: Category 4 Block Diagram

Figure 141 shows an example Category 4 circuit using fault exclusion on the tongue interlock. Fault exclusion eliminates consideration of the failure of the tongue interlock contacts to open. Fault exclusion must be technically justified and documented. Actuator speed, actuator alignment, mechanical stops, and secured operating head must be considered in the justification.

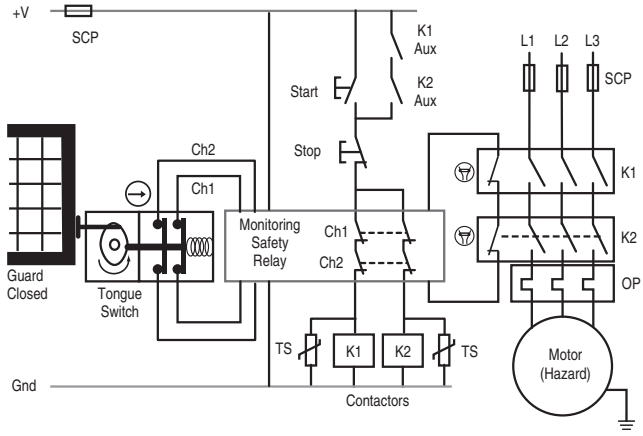


Figure 141: Category 4 with Fault Exclusion on the Tongue Interlock

If the safety system designer prefers using tongue style interlocks, but is not comfortable using fault exclusion on the interlocks, then two tongue interlocks can be used to meet Category 4. Figure 142 shows an example with two tongue interlock switches with direct opening-action contacts to reduce the likelihood of losing the safety function if the operating head were to come loose or break off. The MSR must be rated to meet Category 4 and both output contactors, using mechanically linked contacts, must be monitored.

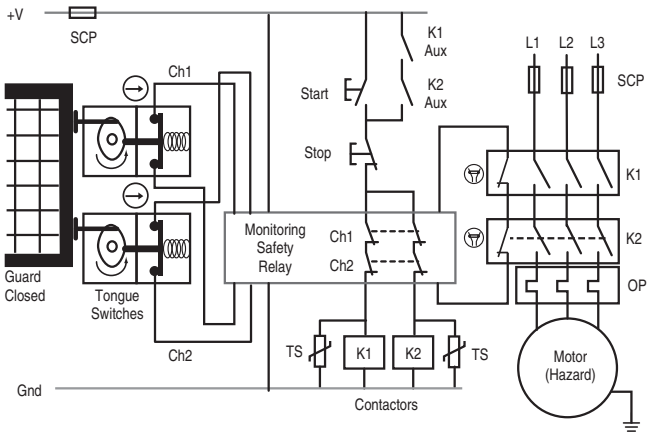


Figure 142: Category 4 with Redundant Tongue Interlocks

Diversity can be applied to further reduce the probability of loss of the safety function due to common mode or common cause failures, one of the tongue interlock switches can be converted to negative mode. One switch operating in negative mode is acceptable, provided a second switch with direct-opening action contacts is used. Figure 143 shows an example of this diverse approach. With this approach, the MSR must be designed to accept normally-open and normally-closed inputs.

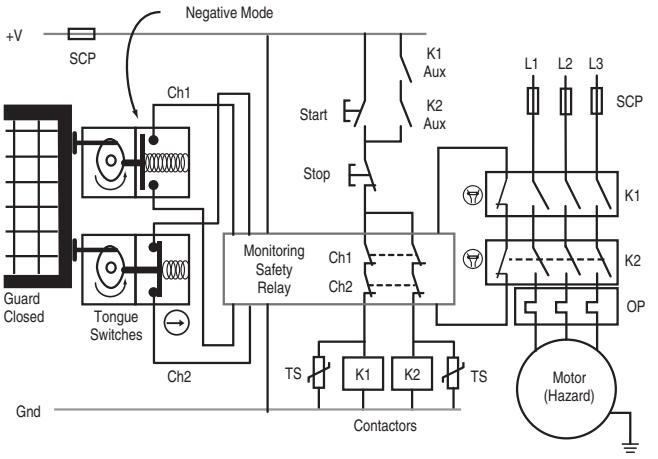


Figure 143: Category 4 with Diverse Redundant Tongue Interlocks

Figure 144 shows an approach using a non-contact interlock. With the diversity of one normally-open and one normally-closed contact, a single non-contact interlock connected to an MSR meets the requirements of Category 4.

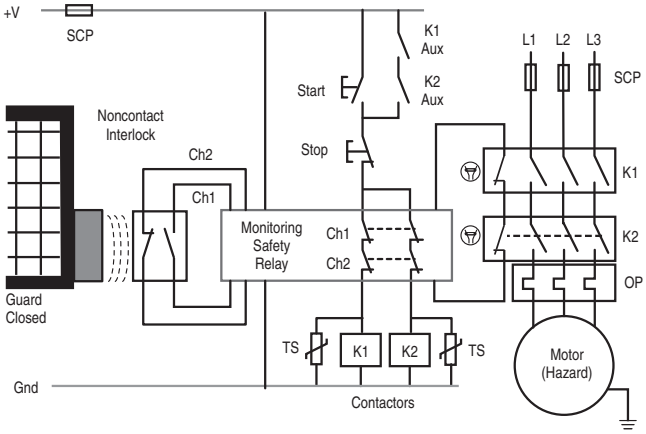


Figure 144: Noncontact Interlock Category 4 System

Figure 145 shows a modular MSR with one 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 this modular approach, the safety relay is microprocessor based and utilizes pulse checking to detect crossfaults.

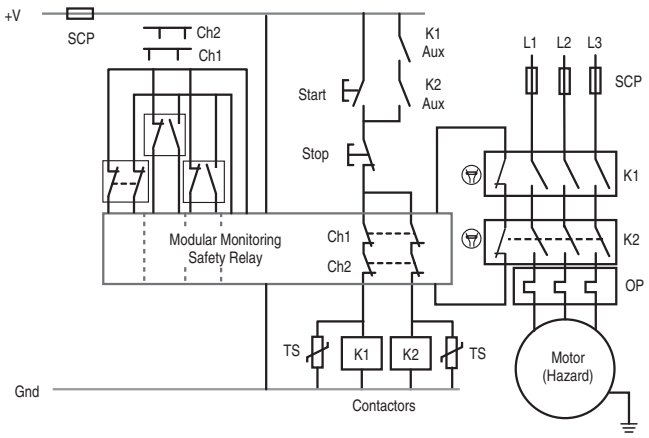


Figure 145: Modular Safety Relay Category 4 System

Component and System Ratings

ISO13849-1 requires component ratings as well as system ratings. This generates some confusion that can be clarified by understanding the components and their capabilities. What we find is that a **component** rated to Category 1 can be used in a **system** rated Category 2, 3, or 4 depending on the system architecture.

Categories B and 1 are described as prevention based, whereas categories 2, 3, and 4 are described as detection based. These categories are applied on a component basis as well as a system basis. The typical safety system consists of a safety interlock switch, a safety relay, and a safety contactor. The interlock and the contactor are rated as Category 1 devices because they are only prevention based. They utilize safety principles but do not perform any detection or self-checking. These devices can be used in redundancy in Category 3 and 4 systems provided the logic device performs the detection.

Logic devices are not only prevention based, but also detection based. Internally, they check themselves to ensure proper performance. Therefore, MSRs and programmable safety controllers are rated to meet Categories 2, 3, or 4.

Fault Considerations and Exclusions

Safety analysis requires extensive analysis of faults and a thorough understanding of the performance of the safety system in the presence of faults. ISO13849-1 and ISO13849-2 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. Between demands placed on the safety system, the basic assumption is that only one fault occurs.

When components and systems are designed to appropriate standards, the occurrence of the fault may be excluded. For example, the failure of normally-closed contacts to open can be excluded if the switch is built to IEC 60947-5-1 Annex K. ISO 13849-2 provides a list of fault exclusions.

Systems Achieving Category 1 Stops

All the above examples show Category 0 stops (immediate removal of power to the actuators). A Category 1 stop (apply braking until the stop is achieved and then remove power to the actuator) is achieved with a time-delayed output. 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 (stopped) state.

Stopping a machine without properly considering 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.

Three possible solutions are:

1. Safety PLCs

Utilizing a PLC with a safety integrity level high enough for safety related use. In practice this would be achieved by using a safety PLC such as GuardLogix for both safety and non-safety control.

2. Safety Relay with Time Delayed Override Command

Figure 146 shows a system with a high-integrity level of hard wiring that allows a correctly sequenced shut-down to protect the machine and program.

A safety relay with immediate and delayed outputs is used (MSR138DP). The immediate acting outputs are connected to inputs at the programmable device (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 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 consider the safety relay output delay period. This is particularly important when using this factor to determine the positioning of devices in accordance with the safety distance calculation.

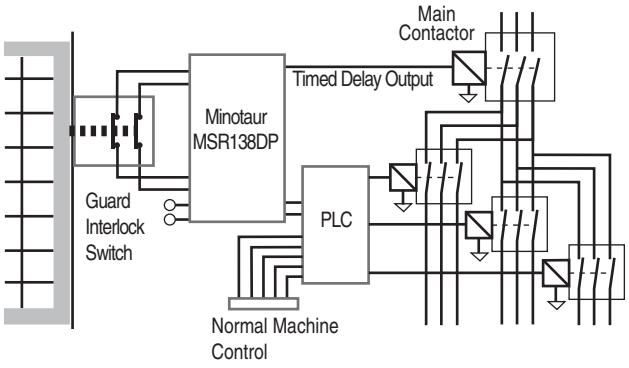


Figure 146: Delayed Outputs for Orderly Shutdown

3. Programmable System Controlled Guard Locking Devices

Figure 147 provides the high integrity level of hard wiring combined with the ability to give a correctly sequenced shut down, but it is only applicable where the hazard is protected by a guard.

In order to allow opening of the guard door, the interlock switch solenoid lock must receive a release signal from the PLC. This signal will only be provided after a stop command sequence has been completed, to decrease the risk of tool damage or program loss. When the solenoid is energized, the door can be opened causing the control circuit contacts on the interlock switch to isolate the machine contactor.

In order to overcome machine run-down or spurious release signals, it may be necessary to use a timed-delay unit (MSR178DP) or stopped-motion detector (CU2) in conjunction with the PLC.

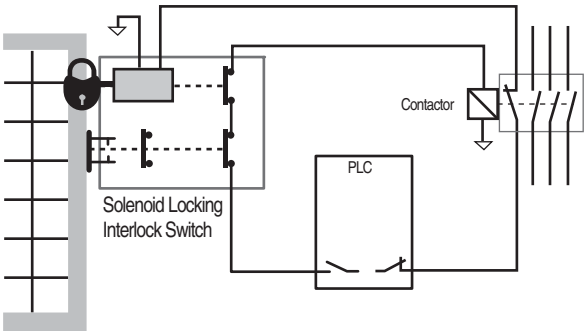


Figure 147: PLC Implementation of Orderly Shutdown

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

ANSI B11.TR3 safeguards providing the lowest degree of risk reduction include: electrical, electronic, hydraulic and pneumatic devices, and associated control systems using a single-channel configuration. Implicit in these requirements is the requirement to use safety rated devices. This is closely aligned with Category 1 of ISO13849-1.

Low/Intermediate Risk Reduction

ANSI B11.TR3 safeguards providing low/intermediate risk reduction include control systems having redundancy that may be manually checked to confirm the performance of the safety system. Looking at the 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

ANSI B11.TR3 safeguards providing high/intermediate risk reduction 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 safeguard providing the highest risk reduction include control systems having redundancy with continuous self-checking. Self checking must confirm 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 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 placed 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 or 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.

Simple

At this lowest level, simple, safety control systems must be designed and constructed with accepted single-channel circuitry. These systems may also 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 acceptable. What is an acceptable 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 and safety controllers) are allowed providing these devices are safety rated. This rating provides that any single safety-related component or firmware failure does not lead to the loss of the safety function. When a 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 US, 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 US 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 a 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 considered if a significant probability of such a failure can occur.

Canadian requirements differ from US requirements 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 be considered regarding faults: (1) not all faults are detectable; (2) adding the word *component* raises questions about wiring; and (3) wiring is an integral part of the safety system and wiring faults can result in the loss of a safety function.

The intent of Control Reliable 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.

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 of these standards, especially with regard to clarification and combining some of the standards. Therefore, it is likely some of the information presented in the following pages may change in 2007/8. For the latest information, please refer to the Rockwell Automation safety systems and components website at: http://www.ab.com/safety.

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. The IEC website 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-energise 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 is 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.

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

1. IEC/EN 61508 "Functional safety of safety related 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 is not restricted to the machinery sector.

2. IEC/EN 62061"Safety of machinery - Functional safety of safety related electrical, electronic and programmable electronic control systems"

It 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. ISO/EN 13849-1:2006 "Safety of machinery – Safety related parts of control systems"

Intended to provide a functional safety transition path from the use of Categories.

The functional safety standards represent a significant step beyond the familiar existing requirements such as Control Reliable and the Categories system of ISO 13849-1:1999 (EN 954-1:1996). Categories are not disappearing yet, the original standard will remain valid in the European Community until 2010 to provide a period for transition to its new revised version. This new version of ISO/EN 13849-1 uses the functional safety concept and has introduced new terminology and requirements. In this section we will refer to the new version as ISO/EN 13849-1:2006.

Interest in the functional safety standards will grow because they are the future and they facilitate more flexibility and the use of new technology for machinery safety.

IEC/EN 62061 and ISO/EN 13849-1:2006

IEC/EN 62061 and ISO/EN 13849-1:2006 both cover safety related electrical control systems. It is intended that they will eventually be combined as two parts of 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.

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.

One restriction for ISO/EN 13849-1:2006 is given in Table 1of the Introduction. When complex and programmable technology is used, the maximum PL to be considered is PLd.

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 ISO 13849-1:2006 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. ISO/EN 13849-1 can be applied to pneumatic, hydraulic, mechanical, and electrical systems.

The following overviews reveal the underlying similarities in values and rational between the standards. It must be understood that these are brief overviews only. Both standards cover much more than shown here and it is important to take account of the full texts of both standards.

Figure 148 provides a simplified flow chart to help the safety system designer determine which of these two standards to use. Each path shares common processes: safety functions and risk assessment. The system design information (e.g., PFH, MTTF, DC, SFF) differs as the path diverges to one standard or the other.

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.

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).

PL and ISO/EN 13849-1:2006

ISO/EN 13849-1:2006 will not use the term SIL; instead it will use 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 10 shows the approximate relationship between PL and SIL when applied to typical circuit structures achieved by low complexity electro-mechanical technology.

PL (Performance Level)	PFH_D (Probability of Dangerous Failure per Hour)	SIL
a	≥10–5 to <10–4	None
b	≥3 x 10–6 to <10–5	1
c	≥10–6 to <3 x 10–6	1
d	≥10–7 to <10–6	2
e	≥10–8 to <10–7	3

Table 10: Approximate correspondence between PL and SIL

IMPORTANT: Table 10 is for general guidance and must NOT be used for conversion purposes. The full requirements of the standards must be taken into account.

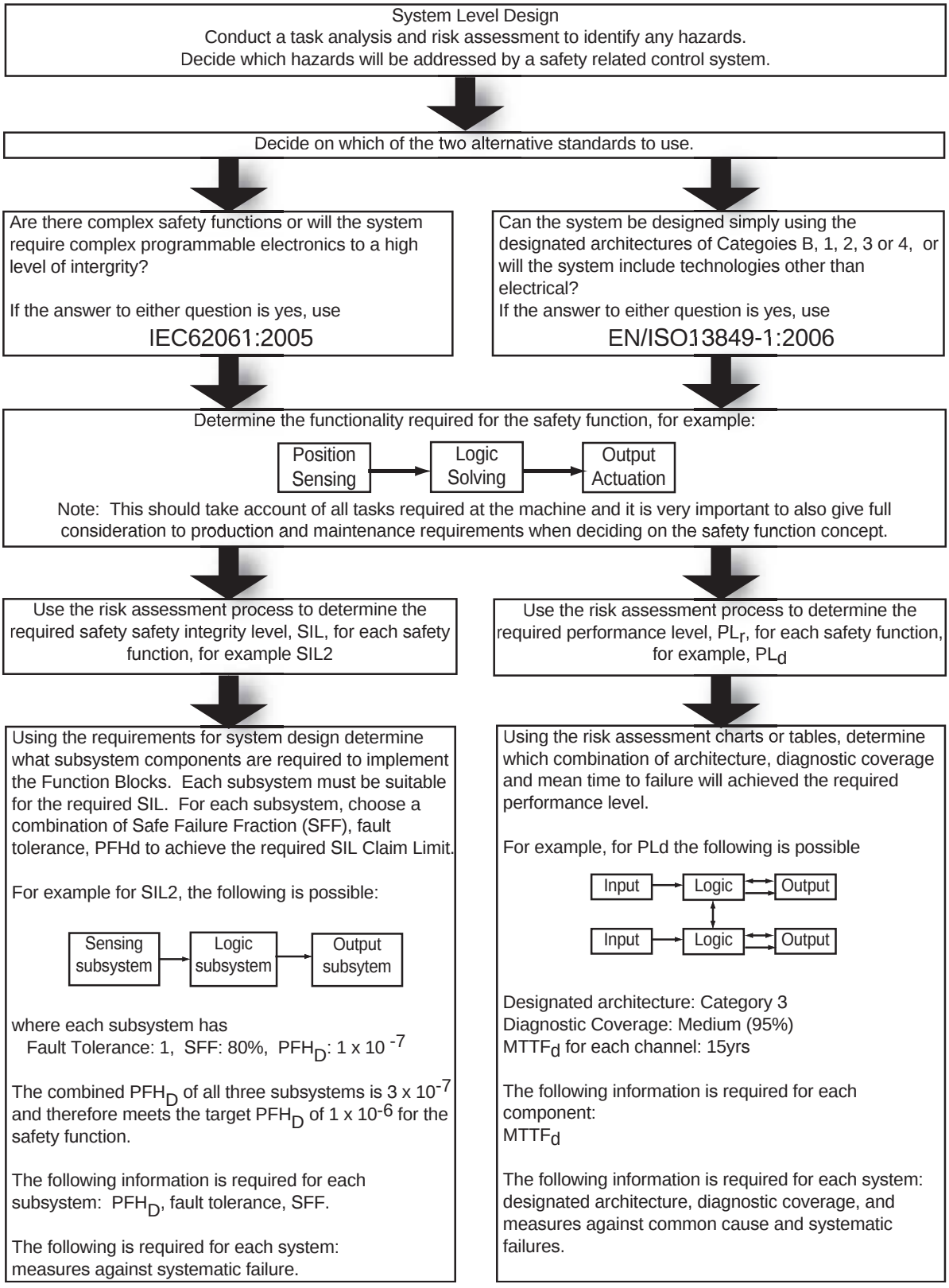


Figure 148: Simplified outline of system level design using IEC/EN 62061 or ISO/EN 13849-1:2006.

System Design According to IEC/EN 62061

IEC/EN 62061, "Safety of machinery - Functional safety of safety related 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 and a
- 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 11 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 11: Elements for SIL Consideration

For electronic systems, a significant contribution to failure is time, as compared to number of operations for electro-mechanical devices. Therefore the failure rate of electronic systems is considered on an hourly basis. An analysis of the components must be undertaken to determine their probability of failure. Safety systems are specifically interested in not just the probability of failure, but more importantly, the probability of failure to danger on an hourly basis, the PFH_D. Once this is known, Table 12 can be used to determine which SIL is achieved.

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 12: Probabilities of Dangerous Failure for SILs

The safety system is divided into subsystems. The hardware safety integrity level that can be claimed for a subsystem is limited 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 is designated as SILCL. Table 13 shows the relationship of the architectural constraints to the SILCL.

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 13: Architectural Constraints on SIL

For example, an 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.

To compute the probability of dangerous failure, each safety function must be broken down into function blocks, which are then realized as subsystems. The system design of many safety functions include a sensing device connected to a logic device connected to an actuator. This creates a series arrangement of subsystems. If we can determine the probability of dangerous failure for each subsystem and know its SILCL, then the system probability of failure is easily calculated by adding the probability of failures of the subsystems. This concept is shown in Figure 149.

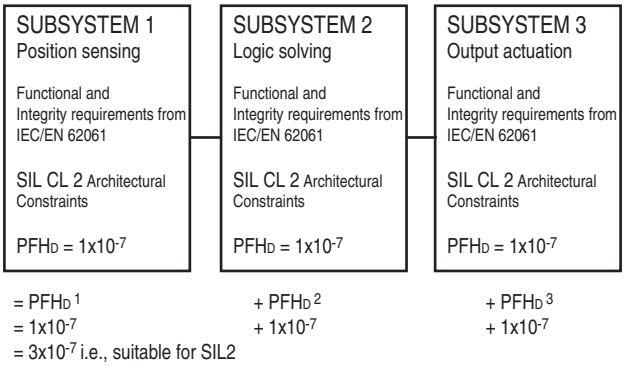


Figure 149: Example subsystem combination into system implementing a SIL 2 safety related electrical control function.

If, for example, we want to achieve SIL 2, each subsystem must have a SIL Claim Limit (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 12.

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 the associated fault diagnostic function (if any).

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. This means that, for devices using complex electronic or programmable components, the full rigor of IEC 61508 applies. This can be a very difficult 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 very 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 150 through 153.

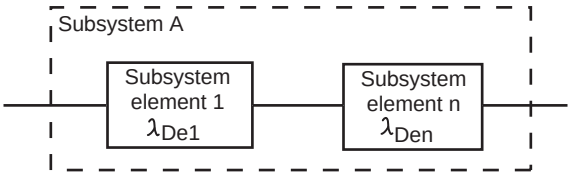


Figure 150: Subsystem logical architecture A

$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

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

For a basic subsystem architecture shown in Figure 150, the probability of dangerous failures are simply added together.

λ, Lambda is used to designate the failure rate. The units of the failure rate are failures per hour. λ_D, is the dangerous failure rate. λ_{DssA} is the dangerous failure rate of subsystem A. λ_{DssA} 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 a unitless probability of failure.

Figure 151 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 chapter.

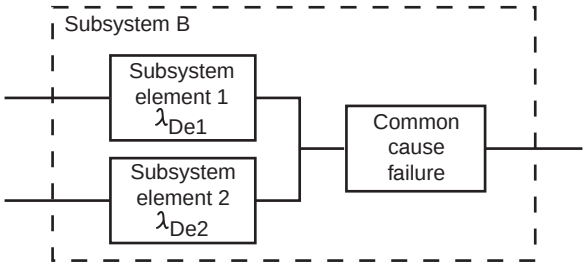


Figure 151: Subsystem logical architecture B

$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

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

The formulae for this architecture takes into account the parallel arrangement of the subsystem elements and adds the following two elements from Table 11:

ß – the susceptibility to common cause failures (Beta)

T1 – 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 an operating condition.

As an example, assume the following values:

ß = 0.10

λ_{De1} = 1 x 10 -6 failures/hour

λ_{De2} = 1 x 10 -6 failures/hour

T1 = 87600 hours (10 years)

The failure rate for the system is 1.70956E-07 failures per hour (SIL2).

Affect of the Proof Test Interval

Let's look at the affect the proof test interval has on the system. Assume the proof test interval was reduced to twice a year. This reduces T1 to 4380 hours, and the dangerous failure rate improves to 1.03548E-07 failures per hour. This is still only SIL2. If the proof test were reduced to a monthly interval (730 hours), the dangerous failure rate improves to 1.0059E-07 failures per hour. This is still only SIL2. Additional improvement in failure rate, proof test interval, or common cause failure is needed to achieve a SIL3 rating. In addition, 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 beta value improves to its best level of 1% (0,01), while the proof test interval remains at 10 years. The dangerous failure rate improves to 9.58568E-08. The system now meets SIL3.

Figure 152 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. Diagnostic coverage is the ratio of the rate of detected dangerous failures compared to the rate of all dangerous failures. The type or number of safe failures is not considered when calculating diagnostic coverage; it is only the percentage of detected dangerous failures.

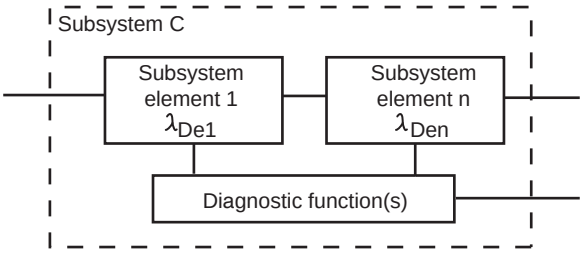


Figure 152: Subsystem logical architecture C

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

$PFH_{DssC} = \lambda_{DssC} \times 1h$

This formulae includes 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 153. 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.

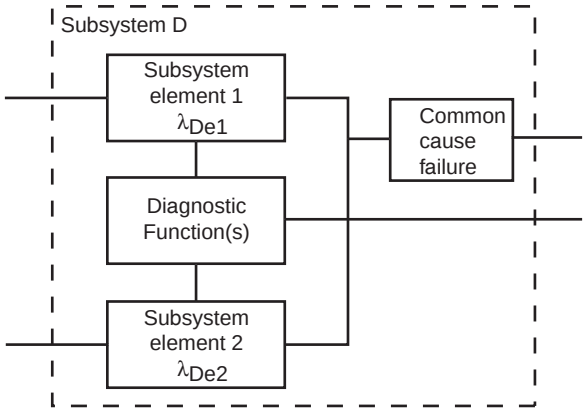


Figure 153: Subsystem logical architecture D

If the subsystem elements are the same, the following formulae is used:

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

$PFH_{DssD} = \lambda_{DssD} \times 1h$

If the subsystem elements are the different, the following formulae is used:

$\lambda_{DssD} = (1\text{-}ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 +$

$\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1/2 \} +$

$ß \times (\lambda_{De1} + \lambda_{De2}) / 2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

Notice that both formulas use one additional parameter, T2 the diagnostic interval.

As an example, assume the following values for the example where the subsystem elements are different:

$ß = 0.10$

$\lambda_{De1} = 1 \times 10^{-6}$ failures/hour

$\lambda_{De2} = 2 \times 10^{-6}$ failures/hour

$T_1 = 87600$ hours (10 years)

$T_2 = 876$ hours

$DC_1 = 0{,}8$

$DC_2 = 0{,}6$

$PFH_{DssD} = 2.36141E\text{-}07$ dangerous failures per hour

Transition Methodology for Categories

During the writing of IEC/EN 62061, it was realized that all the required data for systems and devices would take some considerable time to become fully available. Two tables were included to help with the existing subsystem designs that are based on the original Categories concept and have been proven in use to be effective. They provide equivalency for PFH_d and Architectural Constraints (Hardware Fault Tolerance). They facilitate a useful transition path to the functional safety standards. Tables 14 and 15 below are shown in a simpler form than what appears in the Standards. If they are studied, it becomes apparent that as the architectures of the Category systems can be converted to probability of failurer of danger that can be claimed for a subsystem.

Category	Hardware Fault Tolerance	Diagnostic Coverage	PFH_D (Can Be Claimed for the Subsystem)
1	0	0%	See IEC 62061
2	0	60…90%	$\geq 10^{-6}$
3	1	60…90%	$\geq 2 \times 10^{-7}$
4	>1	60…90%	$\geq 3 \times 10^{-8}$
	1	>90%	$\geq 3 \times 10^{-8}$

Table 14: Category based PFH_D claim

Also, for low complexity category based subsystems, Table 7 from IEC/EN 62061 is available. Table 14 is a simplified version of Table 7 from the standard. Use this table when a category-based subsystem becomes part of the SRCS that must meet IEC/EN 62061. For simplicity, the safety system designer can claim a PFH_D of 2×10^{-7} for a category 3 based system that has 60% diagnostic coverage. Alternatively, the safety system designer can perform a complete analysis to determine if a better PFH_D can be claimed.

Category	Hardware Fault Tolerance	SFF	Max. SIL Claim Limit According to Architectural Constraints
1	0	<60%	See IEC 62061
2	0	60…90%	SIL 1
3	1	< 60%	SIL 1
	1	60…90%	SIL 2
4	>1	60…90%	SIL 3
	1	>90%	SIL 3

Table 15: Category based architectural constraints

Table 15 can be used to determine the SIL Claim Limit of a category-based subsystem. The diagnostic coverage of the category-based system must be converted to safe failure fraction.

Knowing the PFH_D and SILCL of a category-based system, the safety system designer can apply these values into one of the subsystems shown in Figure 149. If the category-based system is the complete SRCS, then equivalent SIL and PFH_D are determined by Tables 14 and 15. The safety system designer must also satisfy the requirements for common cause failures, systematic failures and proof test interval. The scoring system for common cause failures is slightly different for each standard. The concepts for systematic safety integrity are similar in both standards; neither standard uses a scoring system. The proof test interval may be considered the same as the mission time, or a shorter interval may be chosen.

IEC/EN 62061 Terminology Overview

Architectural Constraints

The safety integrity level that can be claimed for a system or subsystem is limited by the architectural characteristics. The two primary characteristics are hardware fault tolerance and safe failure fraction. Secondary characteristics include common-cause faults and fault exclusion.

When combining subsystems, the SIL achieved by the SRCS is constrained to be less than or equal to the lowest SIL Claim Limit of any of the subsystems involved in the safety related control function.

B10 and $B10_d$

For electromechanical subsystems, the probability of failure should be estimated taking into account the number of operating cycles declared by the manufacturer, the load and the duty cycle. The probability of failure is expressed as the B10 value, which is the expected time at which 10% of the population will fail. B10d is the expected time at which 10% of the population will fail to danger.

Common Cause Failure (CCF)

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. The table below 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 16: Scoring Process Summary

Points are awarded for employing specific measures against CCF. The score is added up to determine the common cause failure factor. The beta factor is used in the subsystem models to "adjust" the failure rate.

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 17: Common-Cause Failure Factor

Diagnostic Coverage (DC)

Automatic diagnostic tests are employed to decrease the probability of dangerous hardware failures. Being able to detect 100% of the dangerous hardware failures would be ideal, but is often very difficult to accomplish.

Diagnostic coverage is the ratio of the detected dangerous failures to all the dangerous failures.

$$DC = \frac{\text{Rate of Detected Dangerous Failures, } \lambda_{DD}}{\text{Rate of Total Dangerous Failures, } \lambda_{Dtotal}}$$

The value of diagnostic coverage will lie between zero and one.

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 1 means that 2 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 control of management and technical activities that are necessary for the achievement of a safety related electrical control system.

Probability of Dangerous Failure (PFH_D)

Part of the requirements needed to achieve any given SIL capability for a system or subsystem is data on PFH_d (probability of a dangerous failure per hour) due to random hardware failure. Table 12 gives the probability ranges for each SIL.

This data will be provided by the manufacturer. Data for recent Rockwell Automation safety components and systems (e.g. GuardLogix, GuardPLC, SmartGuard, Kinetix with GuardMotion) is already available. Data for other Rockwell Automation safety components and systems will become available during 2007.

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 be derived from some form of lifetime testing; e.g. B10 testing. Application-based information such as the anticipated number or operations per year, is then required in order to convert the $B10_d$ or similar data to $MTTF_d$ (Mean-Time-To-Dangerous Failure). This, in turn, is then converted to PFH_d.

In general, the following can be assumed:

$PFH_d = 1/MTTF_d$

And for electromechanical devices:

$MTTF_d = B10_d/(0.1 \times \text{mean number of operations per year})$

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. ISO 13849-1:2006 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 tests, which are automatic, proof tests are usually performed manually and off line. Being automatic, diagnostic testing is performed often as compared to proof testing which is done infrequently. For example, the circuits going to an interlock switch on a guard can be 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. The appropriate proof-test interval is determined by reviewing the formulae for the selected architecture. In general, the shorter the proof-test interval, the lower the failure rate.

Safe Failure Fraction (SFF)

The Safe Failure Fraction is similar to Diagnostic Coverage (DC) but also takes account 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 an SFF of less than 60%. But most electronic devices, used for safety, have designed in redundancy and monitoring. Therefore, an SFF of greater than 90% is common. 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 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.

The standard provides additional and more detailed requirements needed to avoid systematic failures.

System Design According to ISO/EN 13849-1:2006

A full and detailed study of ISO/EN 13849-1:2006 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.

This standard also has wide applicability, as it applies to all technologies, including electrical, hydraulic, pneumatic, and mechanical. Although ISO13849-1 is applicable to complex systems, it refers the reader to IEC 62061 and IEC 61508 for complex software embedded systems.

With this standard the safety integrity of a system is classified into 5 PLs (Performance Levels). PLa is the lowest integrity and PLe is the highest integrity. They are evaluated taking the following factors into account:

STRUCTURE – given as designated architectures. These are directly related to the categories.

MTTFd – mean-time-to-dangerous failure

DC – diagnostic coverage

CCF – common cause failures

Behaviour under fault conditions

Software

Systematic failures

Environmental conditions

Safety System Architectures (Structures)

The standard provides a simplified categories-based procedure for estimating the PL. The intention behind this approach is to provide a recognizable transition path from the original Category based standard to the Performance Level based 2006 version. The standard gives five designated architectures as shown below. They correspond to the existing five Categories B, 1, 2, 3 and 4. These diagrams must be studied carefully in clause 6 of the standard where the requirements, differences, and assumptions are explained. The architecture diagrams for Categories B and 1 and also 3 and 4 may look the same, but the standard explains the detail differences in terms of their requirements including diagnostic coverage, etc. Figures 154 through 156 show block diagrams of the 5 category architectures.

It will also be helpful to study Structures of Safety Related Systems in this publication which discusses the Categories in detail with practical examples of their implementation.

System Design According to ISO/EN 13849-1:2006

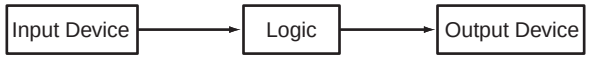


Figure 154: Designated architecture for Category B and 1

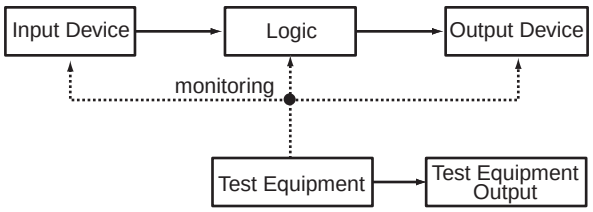


Figure 155: Designated architecture for Category 2

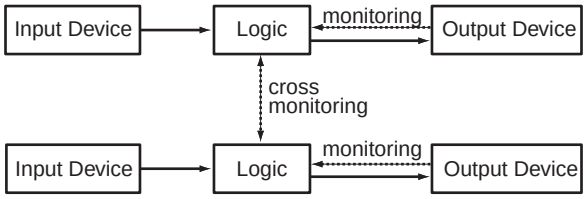


Figure 156: Designated architecture for Category 3 and 4

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* 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.

Mean-Time-to-Dangerous Failure ($MTTF_d$)

$MTTF_d$ (Mean-Time-to-Dangerous Failure) Is used directly in ISO 13849-1:2006 as part of estimating the PL. The standard offers three methods to determine the $MTTF_d$: 1) use Manufacturer's Data, 2) use Annexes C and D which provide component failure rates, or 3) use a default value of 10 years. Selecting the default value restricts the range to Medium as shown in Table 18.

Denotation of $MTTF_d$ of each Channel	Range of $MTTF_d$ 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 18: Levels of $MTTF_d$

When the safety system involves interfacing with IEC62061, the $MTTF_d$ number must be converted to PFH_D. This is done by using the following relationship:

$PFH_D = 1 / MTTF_d$

And, for electromechanical devices:

$MTTF_d = B10_d/(0.1 \times \text{mean number of operations per year})$.

The $MTTF_d$ and PFH_D will usually be derived from the same source of test or analysis data. 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 be derived from some form of lifetime testing e.g., B10 testing. Application based information such as the anticipated number or operations per year is then required in order to convert the $B10_d$ or similar data to $MTTF_d$.

Diagnostic Coverage (DC)

Diagnostic coverage (DC) represents the effectiveness of fault monitoring of a system or subsystem. DC is the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.

ISO/EN 13849-1:2006 and IEC 61508 provide tables that can be used in deriving the DC, and in some cases, the DC may be provided by manufacturers.

Common-Cause Failure (CCF)

Common-cause failures (CCF) occur when multiple faults resulting from a single cause produce a dangerous failure. These are failures of different items, resulting from a single event. The failures are not consequences of each other. Annex F of ISO/EN 13849-1:2006 provides a simplified qualitative method for determining the CCF. Table 19 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 19: Scoring for Common-Cause Failure

A score of at least 65 must be achieved to claim conformance to Categories 2, 3, and 4.

Systematic Failure

The standards have requirements for the control and avoidance of systematic failure. Typical types of possible systematic failure are software design errors, hardware design errors, and requirement specification errors.

Systematic failures differ from random hardware failures which are failures occurring at a random time, typically resulting from degradation of parts of hardware. Annex G of ISO/EN 13849-1:2006 describes measures for the control and avoidance of systematic failure.

Performance Level (PL)

When the design criteria are evaluated, the SRCS will be assigned a Performance Level. 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)

Figure 157 shows a graphical method for determining the PL from the combination of these factors. Table 21 shows the tabular results of different Markov models that created the basis of this Figure 157. Refer to the table when more precise determination is needed.

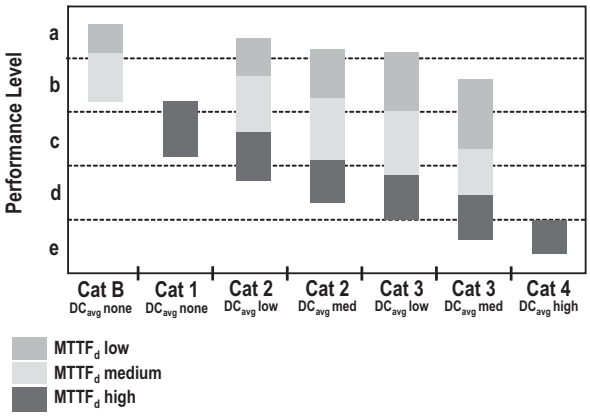


Figure 157: Graphical method to determine PL

The reader will notice there is some overlap at the PL division lines. If MTTF is only provided in categorical terms (as low, medium or high), use Figure 158 to determine the PL.

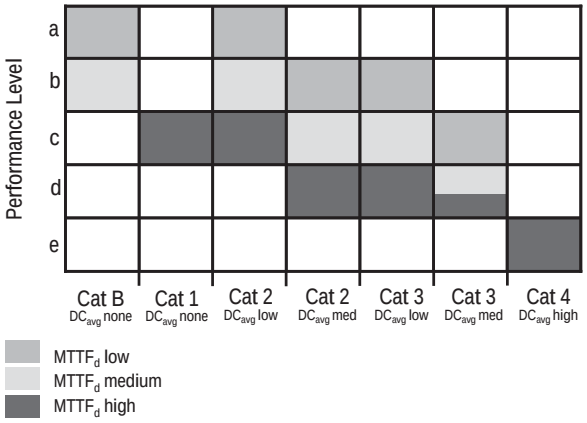


Figure 158: Simplified graphical method

For example, an application uses the Category 3 architecture. If the DC is between 60% and 90%, and if the $MTTF_d$ of each channel is between 10 and 30 years, then according to Figure 158, PLd is achieved.

Other factors must also be realized to satisfy the required PL. These requirements include the provisions for common cause failures, systematic failure, environmental conditions and mission time.

If the PFH_D of the system or subsystem is known, Table 20 (Annex K of the standard) can be used to derive the PL.

Subsystem Design and Combinations

Subsystems that conform to a PL can be combined into a system using Table 20. The rationale behind this table is clear. First, the system can only be as good as its weakest 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 20: PL calculation for series combined subsystems

In the system shown in Figure 159 the lowest Performance Levels are at Subsystems 1 and 2. Both are PLb. Therefore, using Table 20, 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.

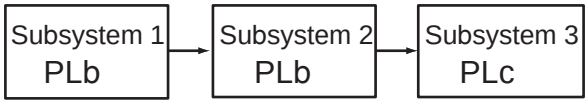


Figure 159: Combination of series subsystems as a PLb system

Validation

Validation plays an important role throughout the safety system development and commissioning process. ISO/EN 13849-2:2003 sets the requirements for validation for systems designed to the original ISO 13849-1 (EN 954-1). It is anticipated that this standard will be revised to bring it in line with EN ISO 13849-1:2006 of systems designed to ISO/EN 13849-1:2006. Validation in ISO 13849-2 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.

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.

Fault exclusion can lead to a very high PL. Appropriate measures to allow this fault exclusion must be applied during the complete mission time. It is not always possible to evaluate SRCS without assuming that certain faults can be excluded. For detailed information on fault exclusions, see ISO 13849-2.

$MTTF_d$ 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 21: Precise $MTTF_d$ to Determine PL

Notes