

# MACHINERY SAFEBOOK 5

 **Allen-Bradley**

 **Guardmaster**<sup>®</sup>



## **Safety related control systems for machinery**

Principles, standards and implementation  
*(Revision 5 of the Safebook series)*

LISTEN.  
THINK.  
SOLVE.<sup>SM</sup>

**Rockwell**  
**Automation**

# Safety related control systems for machinery

## Content

<b>Chapter 1</b>	<b>Regulations</b> EU Directives and Legislation, The Machinery Directive, The Use of Work Equipment Directive, U.S. Regulations, Occupational Safety and Health Administration, Canadian Regulations	<b>2</b>
<b>Chapter 2</b>	<b>Standards</b> ISO (International Organisation for Standardisation), IEC (International Electrotechnical Commission), EN Harmonised European Standards, U.S. Standards, OSHA Standards, ANSI Standards, Canadian Standards, Australian Standards	<b>18</b>
<b>Chapter 3</b>	<b>Safety Strategy</b> Risk Assessment, Machine Limit Determination, Task and Hazard Identification, Risk Estimation and Risk Reduction, Inherently safe design, Protective systems and measures, Evaluation, Training, personal protective equipment, Standards	<b>22</b>
<b>Chapter 4</b>	<b>Implementation of Protective Measures</b> Prevention of Unexpected Start-Up, Lockout / Tagout, Safety Isolation Systems, Preventing Access, Fixed Enclosing Guards, Detecting Access and Safety Technologies and Systems	<b>34</b>
<b>Chapter 5</b>	<b>Safety Distance Calculation</b> Formulas, guidance and application of safety solutions utilising safety distance calculations for safe control of potentially hazardous moving parts.	<b>56</b>
<b>Chapter 6</b>	<b>Safety Related Control Systems &amp; Functional Safety</b> Introduction, What is Functional Safety? IEC/EN 62061 and (EN) ISO 13849-1:2008, SIL and IEC/EN 62061, PL and (EN) ISO 13849-1:2008, Comparison of PL and SIL	<b>60</b>
<b>Chapter 7</b>	<b>System Design According to (EN) ISO 13849</b> SISTEMA, Safety System Architectures (Structures), Mission Time, Mean Time to Dangerous Failure (MTTF <sub>D</sub> ), Diagnostic Coverage (DC), Common Cause Failure (CCF), Systematic Failure, Performance Level (PL), Subsystem Design and Combinations, Validation, Machine Commissioning, Fault Exclusion	<b>66</b>
<b>Chapter 8</b>	<b>System Design According to IEC/EN 62061</b> Subsystem Design - IEC/EN 62061, Affect of the Proof Test Interval, Affect of Common Cause Failure Analysis, Transition methodology for Categories, Architectural Constraints, B10 and B10d, Common Cause Failure (CCF), Diagnostic Coverage (DC), Hardware Fault Tolerance, Management of Functional Safety, Probability of Dangerous Failure (PFH <sub>D</sub> ), Proof Test Interval, Safe Failure Fraction (SFF), Systematic Failure	<b>87</b>
<b>Chapter 9</b>	<b>Safety-Related Control Systems, Additional Considerations</b> Overview, Categories of Control Systems, Undetected Faults, Component and System Ratings, Fault Considerations, Fault Exclusions, Stop Categories According to IEC/EN 60204-1 and NFPA 79, U.S. Safety Control System Requirements, Robot Standards: U.S. and Canada	<b>98</b>
<b>Chapter 10</b>	<b>Application Examples</b> Application example of how you could use SISTEMA Performance Level Calculator tool with Rockwell Automation SISTEMA product library.	<b>110</b>
<b>Chapter 11</b>	<b>Products, tools and services</b> Products, technologies, tools and services available from Rockwell Automation.	<b>138</b>



## Chapter 1: Regulations

### EU Directives and Legislation

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

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

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

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

#### 1 The Machinery Directive

#### 2 The Use of Work Equipment by Workers at Work Directive

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

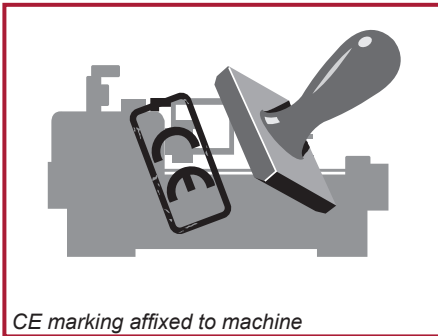
This section deals with aspects of both directives and it is strongly recommended that anyone concerned with the design, supply, purchase or use of industrial equipment within or into the EEA and also certain other European countries should familiarize themselves with their requirements. Most suppliers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

There are other European Directives that may have relevance to machinery. Most of them are fairly specialized in their application and are therefore left outside the scope of this section but it is important to note that, where relevant, their requirements must also be met. Examples are: The EMC Directive 2014/30/EC and the ATEX Directive 2014/34/EU.

## The Machinery Directive

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

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



*CE marking affixed to machine*

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

assessment for the determination of which EHSRs are applicable and there are changes made to the conformity assessment procedures for Annex IV equipment. Detailed information and guidance on the definition and all other aspects of the Machinery Directive can be found at the official EU website:

[http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index\\_en.htm](http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm)

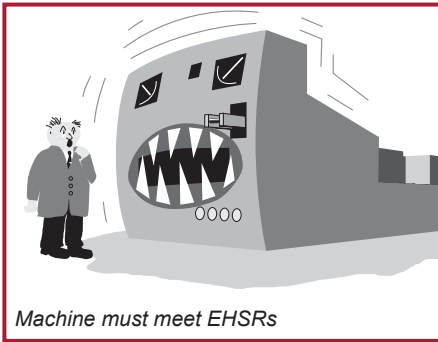
The key provisions of the original Directive (98/37/EC) came into force for machinery on January 1, 1995 and for Safety Components on January 1, 1997.

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

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



## Essential Health & Safety Requirements



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

Annex 1. A risk assessment must be carried out to determine which EHSRs are applicable to the equipment under consideration.

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

**(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 what is appropriate.

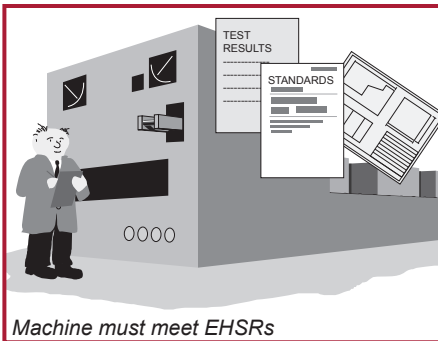
Suitable materials should be used for construction and operation. Adequate lighting and handling facilities should be provided. Controls and control systems must be safe and reliable. Machines must not be capable of starting up unexpectedly and should have one or more emergency stop devices fitted. Consideration must be given to complex installations where processes upstream or downstream can affect the safety of a machine. Failure of a power supply or control circuit must not lead to a dangerous situation. Machines must be stable and capable of withstanding foreseeable stresses. They must have no exposed edges or surfaces likely to cause injury.

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

Electrical and other energy supply hazards including stored energy, 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.



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 EHSR's. (Many recent standards listed in the OJ include a cross-reference identifying the EHSR's that are covered by the standard). Therefore, where equipment complies with such current harmonized European standards, the

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

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



### Technical File

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

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

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

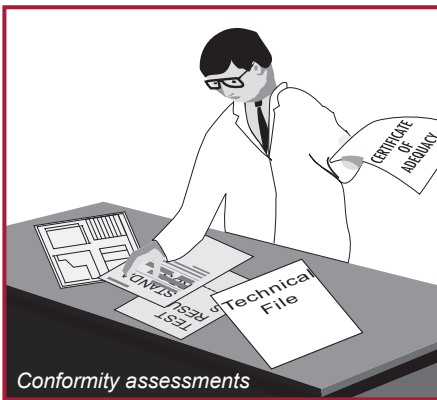
1. Overall drawings of the equipment including control circuit drawings.
2. Detailed drawings, calculation notes, etc. required for checking the conformity of the machinery with the EHSRs.
3. Risk assessment documentation, including a list of the essential health and safety requirements which apply to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

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

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

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

## Conformity Assessment 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 moulding machines, underground equipment, vehicle servicing lifts, etc.

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

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

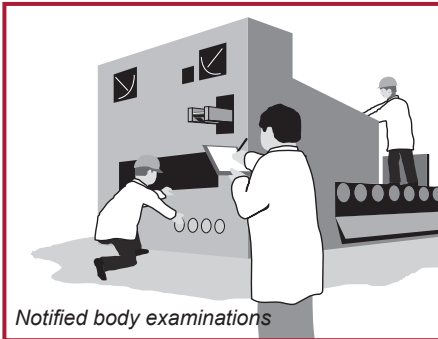
1. EC Type Examination. A Technical File must be prepared and an example of the machine must be submitted to a notified body (test house) for EC type examination. If it passes, the machine will be given an EC type examination certificate. The validity of the certificate must be reviewed every five years with the Notified Body.





## Safety related control systems for machinery

2. Full Quality Assurance. A Technical File must be prepared and the manufacturer must operate an approved quality system for design, manufacture, final inspection and testing. The quality system must ensure conformity of the machinery with the provisions of this Directive. The quality system must be periodically audited by a Notified Body.



Notified body examinations

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

### Notified Bodies

A network of notified bodies that communicate with each other and work to common criteria exists throughout the EU. Notified bodies are appointed by governments (not by industry) and details of organizations with notified body status can be obtained from:

<http://ec.europa.eu/growth/tools-databases/nando/>

### EC Declaration of Conformity Procedure



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

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

The EC Declaration of Conformity must contain the following information:

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

## EC Declaration of Incorporation for Partly Completed Machinery

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

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



The Declaration of Incorporation must contain the following information:

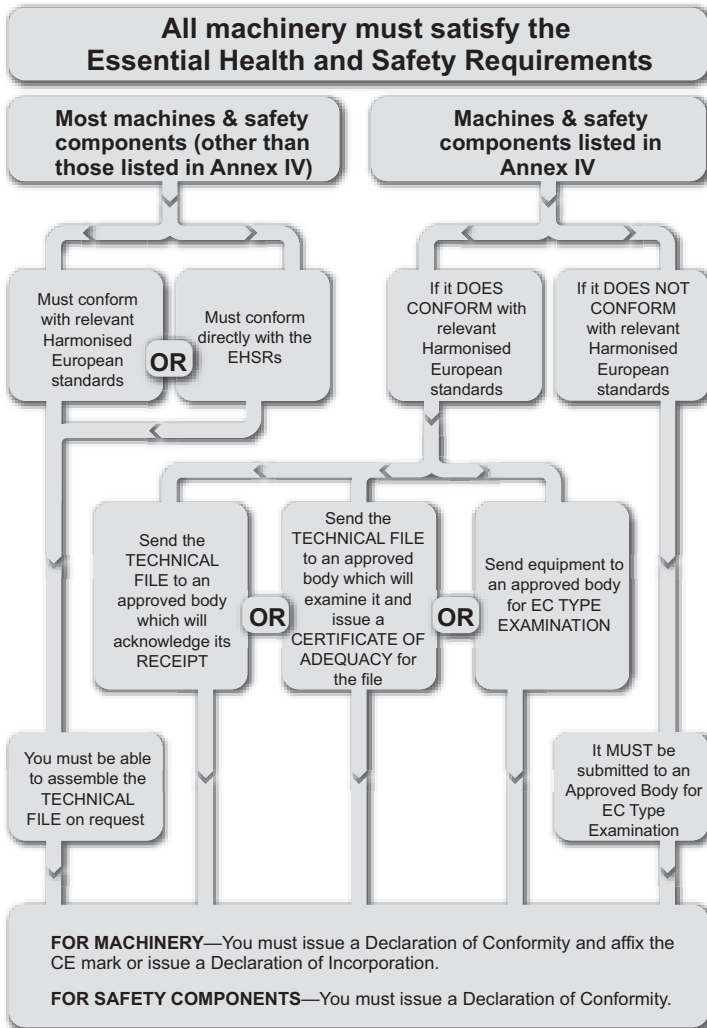
- Business name and full address of the manufacturer of the partly completed machinery and, where appropriate, the authorized representative;
- Name and address of the person authorized to compile the relevant technical documentation, who must be established in the Community (in the case of a manufacturer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

### **Machinery Supplied from Outside the EU - Authorized Representatives**

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

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

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



Whereas the Machinery Directive is aimed at suppliers, this Directive (2009/104/EC) is aimed at users of machinery. It covers all industrial sectors and it places general duties on employers together with minimum requirements for the safety of work equipment. All EU countries are enacting their own forms of legislation to implement this Directive.



## Safety related control systems for machinery

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

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

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

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

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

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

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

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

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

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

Detailed information on the Use of Work Equipment Directive can be found at the official EU website:

<https://osha.europa.eu/en/legislation/directives/3>

## U.S. Regulations

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

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

1. Corporations, which use established requirements as well as establish their own internal requirements;
2. The Occupational Safety and Health Administration (OSHA);
3. Industrial organizations like the National Fire Protection Association (NFPA), the Robotics Industries Association (RIA), and the Association of Manufacturing Technology (AMT), ANSI which publishes a list of recognized consensus standards; 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 1971 by an Act of the U.S. Congress. The purpose of this act is to provide safe and healthful working conditions and to preserve human resources. The act authorizes the Secretary of Labor to set mandatory occupational safety and health standards applicable to businesses affecting interstate commerce. This Act shall apply with respect to employment performed in a workplace in a State, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, American Samoa, Guam, the Trust Territory of the Pacific Islands, Wake Island, Outer Continental Shelf Lands defined in the Outer Continental Shelf Lands Act, Johnston Island, and the Canal Zone.

Article 5 of the Act sets the basic requirements. Each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical



## Safety related control systems for machinery

harm to his employees; and shall comply with occupational safety and health standards promulgated under this Act.

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

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

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

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

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

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

Some OSHA standards reference voluntary standards. The legal effect of incorporation by reference is that the material is treated as if it were published in full in the Federal Register. When a national consensus standard is incorporated by reference in one of the subparts, that standard has the ‘force of law’.

For example, NFPA 70, a voluntary standard known as the US National Electric Code, is referenced in Subpart S. This makes the requirements in the NFPA70 standard mandatory.

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

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

Minor tool changes and adjustments, and other minor servicing activities, which take place during normal production operations, are covered by ANSI Z244 “Alternative Measures” if they are routine, repetitive, and integral to the use of the equipment for production, provided that the work is performed using alternative measures which provide effective protection. This is directly supported by OSHA in the “OSHA Minor Servicing Exception”. 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.” This can be covered during the Risk Assessment.

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 1971, it adopted many existing ANSI standards. For example B11.1 for mechanical power presses was adopted as 1910.217.

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





## Safety related control systems for machinery

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, labelled, 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 testing laboratory (NRTL) which makes periodic inspection of the production of such equipment, and (b) states such equipment meets nationally recognized standards or has been tested and found safe for use in a specified manner.

As of August 2009, the following companies are recognized by OSHA as NRTLs:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

The Authority Having Jurisdiction (AHJ) has the final say on what is required. For example some states like NY, CA and IL have additional requirements.

Some states have adopted their own local OSHAs and may have additional requirements to the US/Federal OSHA requirements. 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
- Wilful: up to \$70,000 per violation
- Violations resulting in death: further penalties
- Failure to abate: \$7000/day

## Canadian 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.



## Chapter 2: Standards

This section covers some of the typical international and national standards that are relevant to machinery safety. It is not intended to form an exhaustive list but rather to give an insight on what machinery safety issues are the subject of standardization. This section should be read in conjunction with the Regulation section.

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

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

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

### ISO (International Organization for Standardization)

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

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

For more information, visit the ISO website: [www.iso.org](http://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](http://www.iec.ch)

## EN Harmonized European Standards

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

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

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

**Type B. STANDARDS:** Subdivided into 2 groups.

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

Type B2 STANDARDS: Cover safety components and protective devices.

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

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

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

For a complete list of EN Machinery Safety standards go to:

<http://ec.europa.eu/growth/single-market/european-standards/>



## U.S. 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.

### 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.

These standards are categorized as either application standards or construction standards. Application standards define how to apply 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. 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.

## **Canadian 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.

## **Australian Standards**

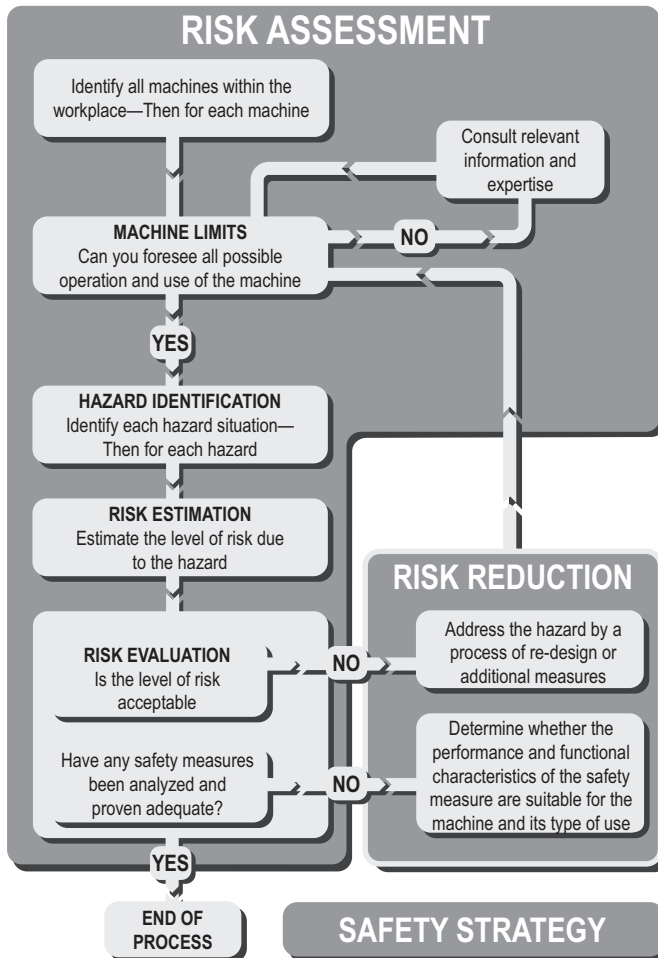
Most of these standards are closely aligned with the equivalent ISO/IEC/EN standards  
Standards Australia Limited  
286 Sussex Street, Sydney, NSW 2001  
Phone: +61 2 8206 6000  
Email: [mail@standards.org.au](mailto:mail@standards.org.au) - Website: [www.standards.org.au](http://www.standards.org.au)



## Chapter 3: 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 below.



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

**RISK REDUCTION** is then performed if necessary and safety measures are selected based on the information derived from the risk assessment stage. The manner in which this is done is the basis of the SAFETY STRATEGY for the machine.

Following this a systematic approach ensures 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 is also possible that individual safe machines may be combined together in a manner that could be unsafe.

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. (EN) ISO 12100 Safety of machinery — General principles for design — Risk assessment and risk reduction contains the most globally applied guidance. An ISO Technical Report: ISO/TR 14121-2 is also available. It gives practical guidance and examples of methods for risk assessment.

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 analysing 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 types of hazardous situations 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 describe 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.



ISO TR 14121-2 “Risk assessment – Practical guidance and examples of methods” shows different methods for quantification of risk. There are differences in the terminology and scoring systems but all the methods relate to the principles given in (EN) ISO 12100. The following text outlines the basic risk quantification principles and is intended to provide help regardless of which methodology is used. It generally follows the parameters given at the Hybrid Tool at clause 6.5 of ISO TR 14121-2.

The following factors are taken into account:

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

The probability of occurrence includes at least two factors:

- FREQUENCY OF EXPOSURE.
- PROBABILITY OF INJURY.

The probability factor itself is often split into other factors such as:

- PROBABILITY OF OCCURRENCE.
- POSSIBILITY OF AVOIDANCE.

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.

At this stage 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.

### **Severity of potential injury**

For this consideration we are presuming that the accident or incident has occurred. Careful study of the hazard will reveal what is the most severe injury possible.

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 according to the factors given in the chosen methodology.

For example as follows:

- Death, losing an eye or arm
- Permanent effect, e.g. losing fingers.
- Reversible effect and requires medical attention
- Reversible effect and requires first aid

### **Frequency of exposure**

Frequency of exposure answers the question of how often is the operator or the maintenance person exposed to the hazard. The frequency of exposure to hazard can be classified according to the factors given in the chosen methodology.

For example as follows:

- Greater than once per hour
- Between once per hour and once per day
- Between once per day and once per two weeks
- Between once per two weeks and once per year
- Lower than once per year

### **Probability of injury**

You should assume that the operator is exposed to the hazardous motion or process. The probability of occurrence of a hazardous event can be classified according to the factors given in the chosen methodology. By considering the characteristics of the machine, expected human behaviours and other factors the probability of occurrence can be classified.

For example as follows:

- Negligible
- Rare
- Possible
- Likely
- Very High

### **Possibility of avoidance**

By considering how people will interact with the machine and other characteristics such as speed of motion start-up, the possibility of avoiding injury can be classified according to the factors given in the chosen methodology.

For example as follows:

- Likely
- Possible
- Impossible



After all the headings have been addressed the results are entered into the graph or table of whichever risk quantification is being used. This produces some form of quantified estimate of the risks at the various hazards at a machine. This information can then be used to decide which risks need to be reduced in order to achieve an acceptable level of safety.

### **Risk Reduction**

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

#### **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 safeguarding and complementary protective measures in relation to risks that cannot be eliminated by design.
3. Provision of information for safe use including warning signs and signals. Also information of any residual risks and whether any particular training or personal protection equipment is required.

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.

#### **Elimination of risk (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 measures and systems**

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 unauthorised removal or bypassing.

One of the most involved and complete interactions between people and machinery is during maintenance, troubleshooting and repair. For routine and minor interventions it may be possible to use safety related system based protective measures (see later description) to ensure safety. But across all regulations it is absolutely clear that, for any type of intervention such as significant maintenance, repair, disassembly or work on power circuits, there should be both the provision and use of equipment that ensures the isolation and dissipation of energy (sometimes including gravitational force) at the machine. In this way the risk of unexpected start-up and exposure to energy sources can be eliminated. This is covered in many different regulations and standards. For example, see the previous text under “U S Regulations” that describes the “Lockout/Tagout” regulations and standard. European and ISO standard EN 1037 and ISO 14118 standards “Prevention of unexpected start-up” also give requirements. In terms of electrical technology IEC/EN 60204-1 and NFPA 79 also give guidance and requirements. Of course it is imperative that a proper working system that ensures all the correct procedures are followed.

The following section describes some typical implementations.

### **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, and AS 4024.1603. These standards have a common theme: the primary method of preventing unexpected power up is to remove the energy from the system and to lock the system in the off state. The purpose is to allow people to safely enter a machine’s hazard zones.

### **Lockout / Tagout**

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

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



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

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

### **Safety Isolation Systems**

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

### **Load Disconnects**

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

### **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. Various components can be added to accommodate more complex lockout arrangements.

### **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 measures such as guard door interlocking systems. The difference between servicing/maintenance and normal production operations is not always clear.

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

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 we need to have some way of relating the extent of the protective measures to the level of risk obtained at the risk estimation stage.

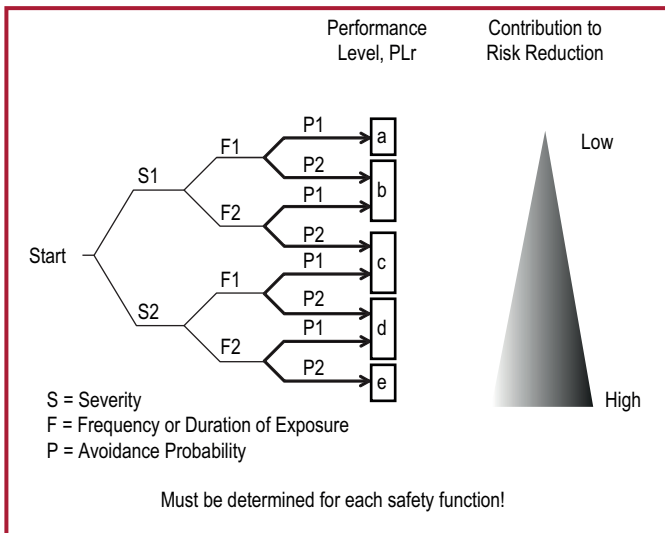
Whichever type of protective device is chosen it must be remembered that a “safety related system” may contain many elements including the protective device, wiring, power switching device and sometimes parts of the machine’s operational control system. All these elements of the system (including guards,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





# Safety related control systems for machinery

(EN) ISO 13849-1:2015 provides an enhanced risk graph in its Annex A.



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

**Risk assessment and safety measures**

Document No.: \_\_\_\_\_  
Part of: \_\_\_\_\_

Product: \_\_\_\_\_  
 Issued by: \_\_\_\_\_  
 Date: \_\_\_\_\_

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

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

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

Comments


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

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

### **Evaluation**

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

### **Training, personal protective equipment etc.**

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

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



## Chapter 4: Implementation of protective measures

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. Safety control system protective measures in conjunction with guarding either prevent access to a hazard or prevent dangerous motion at a hazard when access is available. Typical examples of safety control system protective measures are discussed later and include interlocked guards, light curtains, safety mats, two-hand controls and enabling switches.

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

### Preventing Access with 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. 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. Care must be taken in the selection of the material used, as chemical interactions with cutting fluids, ultra-violet rays and simple aging could cause the window materials to degrade over time.

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

### Detecting Access

Protective measures can be used to detect access to a hazard. When detection is selected as the method of risk reduction, the designer must understand that a complete safety system must be used; the safeguarding device, by itself, does not provide necessary risk reduction. This safety system generally consists of three blocks: 1) an input device that senses the access to the hazard, 2) a logic device that process the signals from the sensing device, checks the status of the safety system and turns on or off output devices, and 3) an output device that controls the actuator (for example, a motor).

## Implementation of Protective Measures

### 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.

- Environmental factors that might impact the detector reliability
- Frequency of access,
- Stopping time of hazard,
- Importance of completing the machine cycle, and
- Containment of projectiles, fluids, mists, vapours, 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 until the machine has had time to reach a complete stop or when stopping the machine in the middle of the cycle is undesirable.

Presence sensing devices, like light curtains, mats and laser 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 likely to be removed or by-passed.

### Presence Sensing Devices

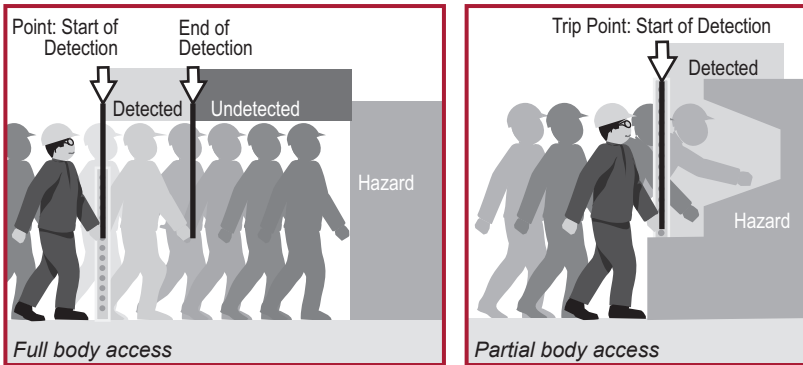
IEC 62046 gives useful guidance on the application of presence sensing devices. Its use is recommended. When deciding how to protect a zone or area it is important to have a clear understanding of exactly what safety functions are required. In general there will be at least two functions.

- 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 safety 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.



## Safety related control systems for machinery



The picture 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.

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, the same types of devices perform tripping and presence sensing. The only difference being the type of application.

Presence sensing devices are used to detect the presence of people. The family of devices includes safety light curtains, single beam safety barriers, safety laser scanners and safety mats. For all presence sensing devices the size of the detection zone and the positioning of the device must take the required safety distance into account.

### 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 can allow for greater productivity. 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.

### 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

## Implementation of Protective Measures

scanner. By taking the measured distance and the location of the object, the laser scanner determines the exact position of the object.

### Pressure Sensitive Safety Mats

These devices are used to provide guarding of a floor area around a machine. 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. Pressure sensitive mats are often used within an enclosed area containing several machines, flexible manufacturing systems or robotics cells. When cell access is required (for setting or robot "teaching," for example), they prevent dangerous motion if the operator strays from the safe area. It is important to prevent any movement of the mat(s) by correct and secure fixing.

### 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.

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.

Light curtains, scanners, floor mats and sensitive edges are also 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 or when there is a possibility of part ejection, movable (operable) guards are often 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



## Safety related control systems for machinery

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. (EN) ISO 14119 provides useful guidance on the selection of all types of guard interlocking devices. Its use is recommended.

There is a wide variety of safety switch options including:

- **Tongue Interlock Switches** - these devices require a tongue-shaped actuator to be inserted and removed from the switch for operation
- **Hinge Interlock Switches** - these devices are placed on the hinge-pin of a guard door and utilize the opening action of the guard to actuate.
- **Guardlocking Switches** - In some applications, locking the guard closed or delaying the opening of the guard is required. Devices suitable for this requirement are called guardlocking 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.
- **Non-contact Interlock Switches** - these devices require no physical contact to actuate with some versions incorporating a coding function for increased resistance to tampering.
- **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. It is generally used on sliding guards.
- **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.

### 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.

## Implementation of Protective Measures

NOTE: these categories are different to the categories from ISO 13849-1. See standards NFPA79 and IEC/EN 60204-1 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 (brakes), not requiring power, may also be 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. This type of stop may result in a faster and more controlled stop from which a restart can be quicker. NOTE: The 2016 Edition of IEC/EN 60204-1 will expand the types of Category 1 stop.

**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. Wherever there is a danger of an operator getting into trouble on a machine there must be a facility for fast access to an emergency stop device. The emergency stop device must be continuously operable and readily available. Operator panels should contain at least one emergency stop device. Additional emergency stop devices may be used at other locations as needed. Emergency Stop devices come in various forms. Push buttons and cable pull switches are examples of the more popular type devices





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

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. They rely on human interaction.

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

### **Emergency Stop Push Buttons**

When a push button is used as an emergency stop device, it must be mushroom shaped, red coloured and with a yellow background. When the emergency 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 restart the machine.

One of the latest technologies to be applied to emergency stops is a self-monitoring technique. An additional contact is added to the back estop 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.

### **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 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.

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

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

## Implementation of Protective Measures

pull force should not exceed 200N (45lbs) or a distance of 400mm (15.75in) at a position centred between two eye bolts. It is important to follow the manufacturer's instructions to achieve proper operational performance.

### Two-Hand Controls

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

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. The table below shows the relationship of the types to the categories of safety performance.

Requirements	Types				
	I	II	III		
			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 of requirements from ISO 13851*

The physical design spacing should prevent improper operation (e.g., by hand and elbow). This can be accomplished by distance or shields. The machine should not go from one cycle to another without the releasing and pressing of both buttons. This provides “anti-repeat” and 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 are sometimes part of a permissive strategy to allow an operator to enter a hazard area with the hazard motor running at safe speed and only while the operator is holding the enabling device in the actuated position. Enabling devices use either two-position or three position types of switches. Two position types are off when the actuator is not operated, and are on when the actuator is operated. Three position switches are off when not actuated (position 1), on when held in the centre 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.

Enabling devices must be used in conjunction with other safety related functions. A typical example is placing the motion in a controlled safe slow mode. When using an enabling device, a signal must indicate that the enabling device is active.

### **Logic Devices**

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

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

### **Monitoring Safety Relays (MSR)**

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.

## Implementation of Protective Measures

Positive guided relays are designed to prevent the normally closed and normally open contacts from being closed simultaneously. Some monitoring safety relays have 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 connected to its outputs. If okay, the MSR awaits a reset signal to energize its outputs. Therefore a correctly selected and configured MSR can provide system fault detection by checking its connected input and output devices. It can also provide a start/restart interlock.

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

### Types of Inputs to Monitoring Safety Relays (MSR)

Different types of safeguarding devices provide different types of inputs to a monitoring safety relay so it is important to check for compatibility. The following is a brief summary of the types inputs that can be expected and the required cross-fault detection characteristics.

**Electromechanical Interlocks, some Non-Contact Interlocks and Emergency Stops:** Mechanical contacts, single channel with one normally closed contact or dual channel, both normally closed. The MSR must be able to accept single or dual channel and provide cross-fault detection for the dual channel arrangement.

**Some Non-Contacts Interlocks and Emergency Stops:** Mechanical contacts, dual channel, one normally open and one normally closed contact. The MSR must be able to process diverse inputs.

**Devices with solid state outputs:** Light curtains, laser scanners and some non-contact guard interlocks have two sourcing outputs and perform their own cross-fault detection. The MSR must be able to ignore the devices cross-fault detection method.

**Pressure Sensitive Mats:** Mats create a short circuit between two channels. The MSR must be specifically designed or configurable for this application.

**Pressure Sensitive Edges:** Some edges are designed like 4-wire mats. Some are two wire devices that create a change in resistance. The MSR must be able to detect a short circuit or the change resistance.



**Motor motion sensing:** Measures the back EMF of a motor during rundown. The MSR must be able to tolerate high voltages as well as detect low voltages as the motor spins down.

**Stopped Motion:** The MSR must detect pulse streams from diverse, redundant sensors.

**Two-hand Control:** The MSR must detect normally open and normally closed diverse inputs as well as provide 0.5s timing and sequencing logic.

Monitoring safety relays must be specifically designed or configurable to interface with each of these types of devices, as they have different electrical characteristics. Some MSRs are completely configurable into different types. 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 designer must select or configure 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 that the input impedance remains below the maximum specification. The length, size and type of wire used affects input impedance.

### Number of Input Devices

The risk assessment process should be used to help determine how many input devices should be connected to a monitoring safety relay unit MSR and how often the input devices should be checked. To assure that emergency 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 emergency stops. Since emergency stops are typically used only for emergencies, they are likely to be rarely used. Therefore a program should be established to exercise the emergency stops and confirm their effectiveness on a scheduled basis. Exercising the safety system in this way is called performing a functional test. A third example might be access doors for machine

## Implementation of Protective Measures

adjustments, which like emergency stops might be rarely used. Here again a program should be established to exercise the checking function on a scheduled basis.

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

### Input Cross-fault Detection

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

Microprocessor based monitoring safety relays, like light curtains, laser scanners and advanced non-contact sensors detect these shorts in a variety of ways. One common way of detecting cross-faults is by using pulse testing. The signals input to the MSR 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.

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

### Outputs

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

Most MSRs have at least 2 immediately operating safety outputs. MSR safety outputs are characterized as normally-open. These are safety rated due to the redundancy and internal checking. A second type of output is delayed outputs. Delayed-off 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. MSRs also have auxiliary outputs. Generally these are considered normally closed.

### 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, 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.

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

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

**Thermal Current, I<sub>th</sub>:** 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 U<sub>e</sub> and Current I<sub>e</sub>:** 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 typically rated at 125VAC, 250VAC and 24VDC.

**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 7200VA 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 720 VA because the steady state current of the electromagnetic load is 6A, which is the rated operational current.

Example 2: An N150, DC-13 rating indicates that the contacts can make a 275VA circuit. At 125V AC, the contacts can make a 2.2 amp circuit. DC electromagnetic

## Implementation of Protective Measures

loads do not have an inrush current like AC electromagnetic loads. The breaking of the circuit is also 275VA because the steady state current of the electromagnetic load is 2.2 amp, which is the rated operational current.

### Machine Re-start

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.

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

The requirement for normal interlocking situations is made clear in ISO 12100 (extract):

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

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

### Reset Functions

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

#### Monitored Manual Reset

A monitored manual reset requires a change of state of the reset circuit after the gate is closed or the emergency stop is reset. The mechanically linked normally closed auxiliary contacts of the power switching contactors are connected in series with a momentary push button. After the guard has been opened and closed again, the safety relay will not allow the machine to be restarted until there is a change of





state at the reset button. This is in compliance with the intent of the requirements for additional manual reset as given in (EN) ISO 13849-1. i.e., the reset function ensures that both contactors are OFF and that both interlock circuits (and therefore the guards) are closed and also (because a change of state is required) that the reset actuator has not been bypassed or blocked (tied down) in any way. If these checks are successful the machine can then be restarted from the normal controls. (EN) ISO 13849-1 cites the change of state from energized to de-energized ('falling edge').

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

### **Auto/ Manual Reset**

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

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

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

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

### **Control Guards**

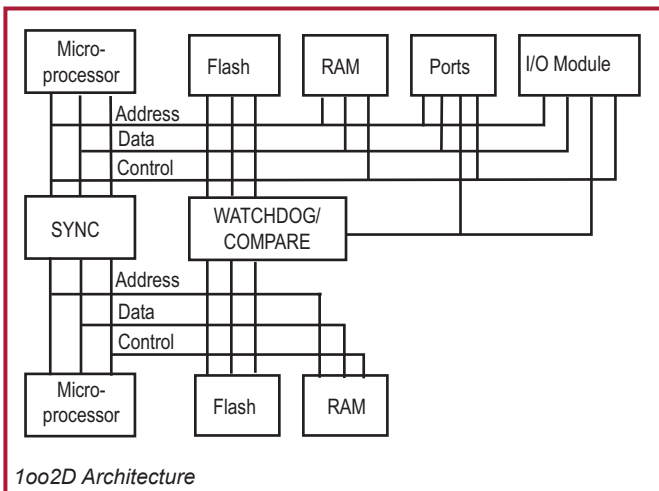
A control guard stops a machine when the guard is opened and directly starts it again when the guard is closed. The use of control guards is only allowed under certain stringent conditions because any unexpected start-up or failure to stop would be extremely dangerous. The interlocking system must have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

## Implementation of Protective Measures

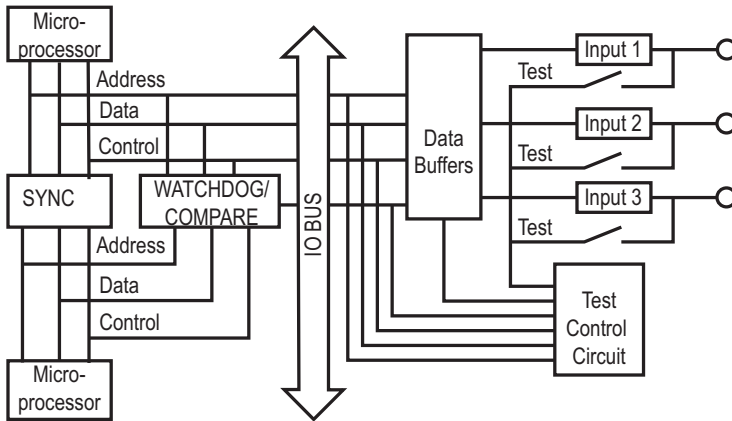
### Safety Programmable Logic Controls

The need for flexible and scalable 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 come in various platforms to accommodate the scalability, functional and integration requirements of the more complex safety systems.

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



Also, each input circuit is internally tested many times each second to make sure that it is operating correctly. You may only hit the emergency stop once a month; but when you do, the internal circuit has been continuously tested.



*Safety input module block diagram*

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

When using safety devices with mechanical contacts (emergency stops, gate switches, etc), the user can apply pulse test signals to detect cross-faults.

## Software

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

Function blocks are the predominant methods for programming safety functions. In addition to Function Blocks and Ladder Logic, safety plc's also provide certified safety application instructions. Certified safety instructions provide application specific behaviour.

## Implementation of Protective Measures

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.

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

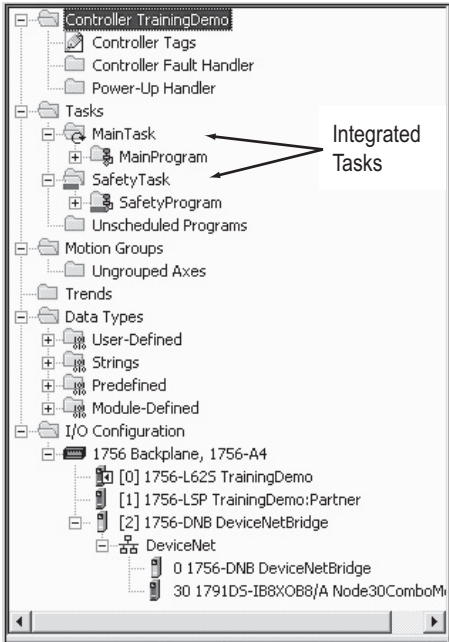
Wiring is simplified with programmable logic systems as compared to monitoring safety relays. Unlike wiring to specific terminals on monitoring safety relays, input devices are connected to any safety input terminals and output devices are connected to any safety output terminals. The terminals are then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

### Integrated Safety Controllers

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

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

All standard and safety related functions are isolated from each other. For example, safety tags can be directly read by the standard logic. Safety tags can be exchanged between GuardLogix controllers over EtherNet/IP, ControlNet or DeviceNet. Safety tag data can be directly read by external devices, Human Machine Interfaces (HMI), personal computers (PC) or other controllers.



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/IP.
7. Safety tag data, program or controller scoped, can be read by external devices, HMI's, PC's, other controllers, etc. Note, once this data is utilized outside of the safety task, it is considered standard data, not safety data.

## Implementation of Protective Measures

### Safety Networks

Plant floor communication networks have traditionally provided manufacturers the capability to improve flexibility, increase diagnostics, increase distance, reduce installation & wiring cost, ease maintainability and generally improve the productivity of their manufacturing operations. These same motivations have also driven 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 for both safety and standard IO communications, 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 are designed to detect transmission errors and initiate an appropriate fault reaction function. Communication errors that are detected include: message insertion, message loss, message corruption, message delay, message repeat, and incorrect message sequence.

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

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

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



## Output Devices

### Safety Control Relays and Safety Contactors

Control Relays and Contactors are used to remove electrical power from the actuator. Special features are added to control relays and contactors to enable their use for safety.

Mechanically linked auxiliary contacts are used to feed back the status of the control relays and contactors to a monitoring logic device. The use of mechanically linked contacts helps ensure the safety function. To meet the requirements of mechanically linked contacts, the normally closed and the normally open contacts cannot be in the closed state at the same time. IEC 60947-4-1 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.

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

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

Control relays and contactors are designed to switch large loads, anywhere from 0.5A to over 100A. 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 24VDC. The safety control relays and safety contactors use gold plated bifurcated contacts to reliably switch this small current.

## Implementation of Protective Measures

### Overload Protection

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

### 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. The redundant channels are monitored by either external or integral logic depending on the type of drive. 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 in a manner similar to the AC drives using redundant safety signals are used to achieve the safety function “safe torque-off”.

### 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. With an IP67 rating, these types of boxes can be mounted on the machine at remote locations. When a diverse set of devices is required, an ArmorBlock Guard I/O box can be used. The inputs can be configured by software to accommodate various types of devices.





## Chapter 5: 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. In this chapter, these standards are grouped as follows:

**ISO EN: (EN ISO 13855)**

**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:  $D_s = K \times (T_s + T_c + T_r + T_{bm}) + D_{pf}$

Where:  $D_s$  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 light curtains or an area scanner is used, the angle of approach to the detection device must be taken into consideration. Three types of approaches are considered:

Normal - an approach perpendicular to the detection plane

Horizontal - an approach parallel to the detection plane

Angled - an angled approach to the detection zone.

## Safety Distance Calculation

### 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 1600mm/sec (63in/s) hand speed of an operator while the body is stationary. The circumstances of the actual application must be taken into account. As a general guideline, the approach speed will vary from 1600mm/s (63in/s) to 2500mm/sec (100in/s). The appropriate speed constant must be determined by the risk assessment.

### Stopping Time

T is the overall stopping time of the system. The total time, in seconds, starts from the initiation of the stop signal to the cessation of the hazard. This time can be broken down to its incremental parts (Ts, Tc, Tr and Tbm) for easier analysis. Ts is the worst case stopping time of the machine/equipment. Tc is the worst case 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 Factors

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

$Dpf = 3.4 \times (\text{Object Sensitivity} - 6.875\text{mm})$ , but not less than zero.

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

$C = 8 \times (\text{Object Sensitivity} - 14 \text{ mm})$ , but not less than 0

These two formulas have a cross over point at 19.3mm. For object sensitivity less than 19mm, 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 19.3mm, 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.



## 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. The ISO EN value is 850mm where the US CAN value is 900mm. The standards also differ in the object sensitivity.

## Reach-Over Applications

Both standards agree that the minimum height of the lowest beam should be 300mm, but differ with respect to the minimum height of the highest beam. The ISO EN states 900mm, whereas the US CAN states 1200mm. The value for the highest beam seems to be moot. When considering this to be a reach-through application, the height of the highest beam will have to be much higher to accommodate an operator in a standing position. If the operator can reach over the detection plane, then the reach over criteria applies.

## Single or Multiple Beams

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

# Beams	Height above the floor - mm (in)	C - mm (in)
1	750 (29.5)	1200 (47.2)
2	400 (5.7), 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)

## 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 40mm, the ISO EN approach requires two steps. First, calculate S using 2000 for the speed constant.

$$S = 2000 \times T + 8 \times (d - 14)$$

The minimum distance that S can be is 100mm.

## Safety Distance Calculation

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

The US CAN approach uses a one step approach:  $D_s = 1600 \times T * D_{pf}$

This leads to differences greater than 5% between the standards, when the response time is less than 560ms.

### Angled Approaches

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

### Safety Mats

With safety mats, the safety distance must take into account the operators pace and stride. Assuming the operator is walking and the safety mats are mounted on the floor. The operator's first step onto the mat is a depth penetration factor of 1200mm or 48 in. 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. It is important to fix the mat(s) securely to prevent any movement.

### Example

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

$$D_{pf} = 3.4 (14 - 6.875) = 1 \text{ in (24.2mm)} \quad C = 8 (14-14) = 0$$

$$\begin{aligned} D_s &= K \times (T_s + T_c + T_r + T_{bm}) + D_{pf} & S &= K \times T + C \\ D_s &= 63 \times (0.17 + 0.13 + 0) + 1 & S &= 1600 \times (0,3) + 0 \\ D_s &= 63 \times (0.3) + 1 & S &= 480 \text{mm (18.9in)} \\ D_s &= 18.9 + 1 \\ D_s &= 19.9 \text{ in (505mm)} \end{aligned}$$

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



## Chapter 6: Safety Related Control Systems

### Introduction

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

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

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

### Safety Function

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

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

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

1. The 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.

## Safety Related Control Systems & Functional Safety

When stating the safety function for a specific application, the word “hazard” must be changed to the specific hazard. The source of 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 source is a motor, ram, knife, torch, pump, laser, robot, end-effector, solenoid, valve, other type of actuator, or a mechanical hazard involving gravity.

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

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

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

### Functional Safety of Control Systems

#### What is Functional Safety?

Functional safety is the part of the overall safety requirement and that depends on the correct functioning of the process or equipment in response to its inputs. IEC TR 61508-0 provides the following example to help clarify the meaning of functional safety. “For example, an over-temperature protection device, using a thermal sensor in the windings of an electric motor to de-energize the motor before they can overheat, is an instance of functional safety. But providing specialized insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).”

As another example, compare hard guarding to an interlocked guard. The hard guarding is not considered “functional safety” although it may protect against access to the same hazard as an interlocked door. The interlocked door is an instance of functional safety. When the guard is opened, the interlock serves as an “input” to a system that achieves a safe state. Similarly, personal protective equipment (PPE)



is used as a protective measure to help increase safety of personnel. PPE is not considered functional safety.

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

Therefore the functional safety of an electrical control system is highly relevant to the control of hazards arising from moving parts of machinery.

Two types of requirements are necessary to achieve functional safety:

- The safety function and
- The safety integrity.

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

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

1. IEC/EN 61508 “Functional safety of 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”

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

## Safety Related Control Systems & Functional Safety

3. (EN) ISO 13849-1 “Safety of machinery - Safety related parts of control systems”

This standard is intended to provide a direct transition path from the categories of the previous EN 954-1.

4. IEC 61511 “Functional safety - Safety instrumented systems for the process industry sector”

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

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

Categories have not disappeared completely; they are still used in the current (EN) ISO 13849-1.

### **IEC/EN 62061 and (EN) ISO 13849-1**

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

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

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

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

### **Joint Technical Report on IEC/EN 62061 and (EN) ISO 13849-1**

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





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

In order to show that both standards give equivalent results the report shows an example safety system calculated according to the methodologies of both standards. The report also clarifies a number of issues that have been subject to different interpretations. Perhaps one of the most significant issues is the aspect of fault exclusion.

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

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

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

### **SIL and IEC/EN 62061**

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

Because the term SIL is applied in the same manner in other industrial sectors such as petro-chemicals, power generation and railways, IEC/EN 62061 is very useful when machinery is used within those sectors. Risks of greater magnitude can occur in other sectors such as the process industry and for that reason IEC 61508 and the process sector specific standard IEC 61511 include SIL 4.

## Safety Related Control Systems & Functional Safety

A SIL applies to a safety function. The subsystems that make up the system that implements the safety function must have an appropriate SIL capability. This is sometimes referred to as the SIL Claim Limit (SIL CL). A full and detailed study of IEC/EN 62061 is required before it can be correctly applied.

### PL and (EN) ISO 13849-1

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

### Comparison of PL and SIL

This table shows the approximate relationship between PL and SIL when applied to typical circuit structures.

PL (Performance Level)	PFH <sub>D</sub> (Probability of dangerous failure per hour)	SIL (Safety Integrity Level)
a	$\geq 10^{-5}$ to $< 10^{-4}$	None
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$	1
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $< 10^{-6}$	2
e	$\geq 10^{-8}$ to $< 10^{-7}$	3

*Approximate correspondence between PL and SIL*

**IMPORTANT:** The table shown above is for general guidance and must NOT be used for conversion purposes. The full requirements of the standards must be referenced. The tables in Annex K provide more detailed information.



## Chapter 7: System design according to (EN) ISO 13849

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

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

### SISTEMA Software PL Calculation Tool

SISTEMA is a software tool for the implementation of (EN) ISO 13849-1. Its use will greatly simplify the quantification and calculation aspects of the implementation of the standard.

SISTEMA stands for “Safety Integrity Software Tool for the Evaluation of Machine Applications” and is regularly reviewed and updated by IFA. It requires the input of various types of functional safety data as described later in this section. The data can be input manually or automatically by using a manufacturer’s SISTEMA Data Library.

The Rockwell Automation SISTEMA Data Library is available for download, together with a link to the SISTEMA download site, at: [www.rockwellautomation.com](http://www.rockwellautomation.com), under *Solutions & Services > Safety Solutions*.

### Overview of (EN) ISO 13849-1

The following general overview is intended to provide an overview of the basic provisions of (EN) ISO 13849-1. It also includes some mention of its revision published early in 2106. It is essential that the standard itself is studied in full detail. This standard has wide applicability, as it applies to all technologies, including electrical, hydraulic, pneumatic and mechanical. Although ISO 13849-1 is applicable to complex systems, it also refers the reader to IEC 61508 for complex software embedded components.

The outputs of ISO 13849-1 are Performance Levels [PL a, b, c, d or e]. The original Category concept is retained but there are additional requirements to be satisfied before a PL can be claimed for a system.

The requirements can be listed in basic form as follows:

- The architecture of the system. Essentially this captures what we have become used to as Categories

## System Design According to (EN) ISO 13849

- Reliability data is required for the constituent parts of the system
- The Diagnostic Coverage [DC] of the system is required. This represents the effectiveness of fault monitoring in the system
- Protection against common cause failure
- Protection against systematic faults
- Where relevant, specific requirements for software

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

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

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

The system designer [typically a machine designer or integrator] will use the subsystem data to perform some relatively straightforward calculations as part of the determination of the overall performance level [PL] achieved by the system.



### Determination of the safety function

We need to decide what the safety function is. Clearly the safety function must be appropriate to the required task. How does the standard help us?

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

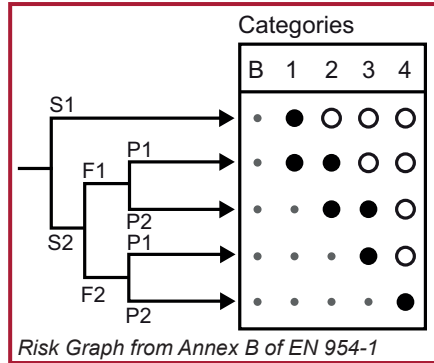
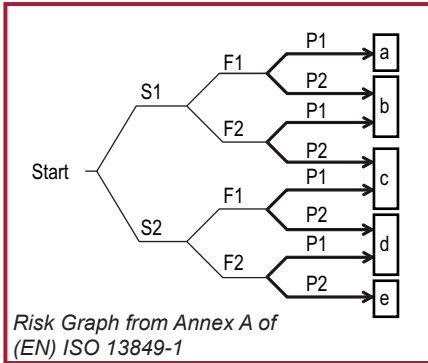
The standard does provide some help by listing out many of the commonly used safety functions (e.g. safety-related stop function initiated by safeguard, muting function, start/restart function) and providing some normally associated requirements. Study of (EN) ISO 12100: "Basic design principles and Risk assessment" is recommended for use at this stage. ISO TR 22100-2 provides useful guidance on the relationship between the machine risk assessment process from ISO 12100 and the PL allocation process of (EN) ISO 13849-1. There is a large range of machine specific standards that will provide safety function requirements for specific machines. Within the European EN standards they are termed C type standards, some of them have exact equivalents in ISO standards. ISO TR 22100-1 provides further information on the relationship between ISO 12100 and C standards.

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

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

The output is the PLr. Users of the old EN 954-1 will be familiar with this approach but take note that within (EN) ISO 13849-1 the S1 line now subdivides whereas the old risk graph did not. The 2015 version provides the possibility for decreasing the PLr by one level in some circumstances depending on the foreseeable probability of occurrence.

## System Design According to (EN) ISO 13849



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

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

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

SISTEMA is available in a range of languages including German and English. IFA, the developer of SISTEMA, is a well-respected research and testing institution based in Germany. It is particularly involved in solving scientific and technical problems relating to safety in the context of statutory accident insurance and prevention in Germany. It works in cooperation with occupational health and safety agencies from over 20 countries.

Experts from the IFA, along with their BG colleagues had significant participation in the drafting of both (EN) ISO 13849-1 and IEC/EN 62061.

The “library” of Rockwell Automation safety component data for use with SISTEMA is available at: [www.rockwellautomation.com](http://www.rockwellautomation.com), under Solutions & Services > Safety Solutions.

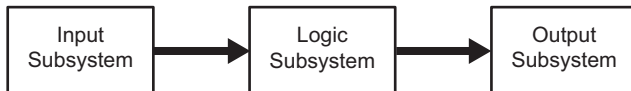


## Safety related control systems for machinery

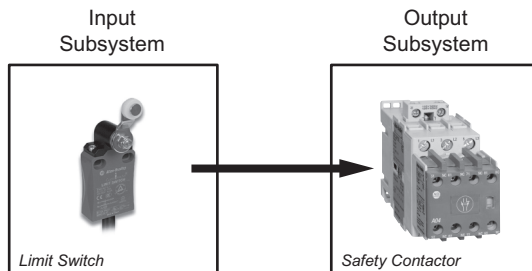
Whichever way the calculation of the PL is done it is important to start from the right foundation. We need to view our system in the same way as the standard so let's start with that.

### System Structure

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



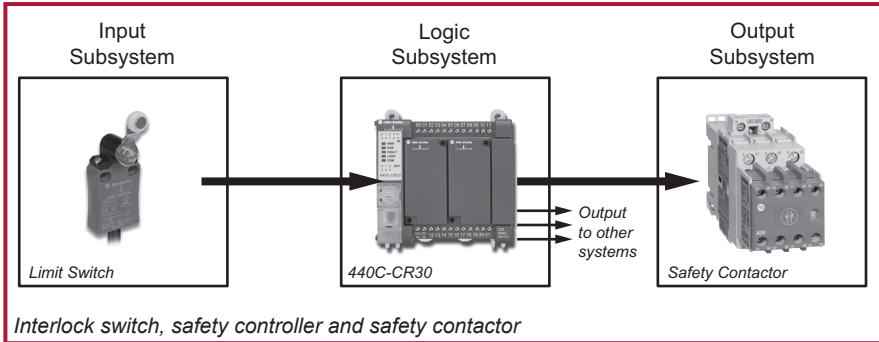
The component groups that implement these functions are the subsystems.



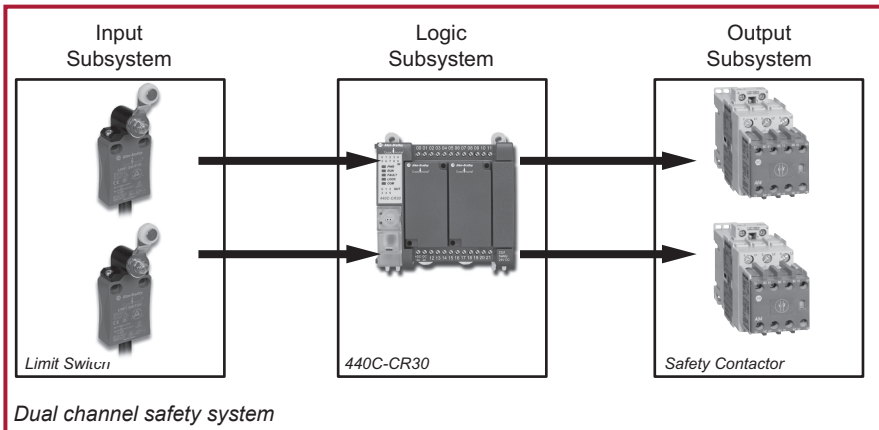
*Interlock switch and safety contactor*

A simple single channel electrical system example is shown above. It comprises only input and output subsystems.

## System Design According to (EN) ISO 13849



The system shown above is a little more complex because some logic is also required. The safety controller itself will be fault tolerant (e.g. dual channel) internally but the overall system is still limited to single channel status because of the single limit switch and single contactor subsystems. A single channel system will fail if one of its single channel subsystems fails; it is not “fault tolerant”.

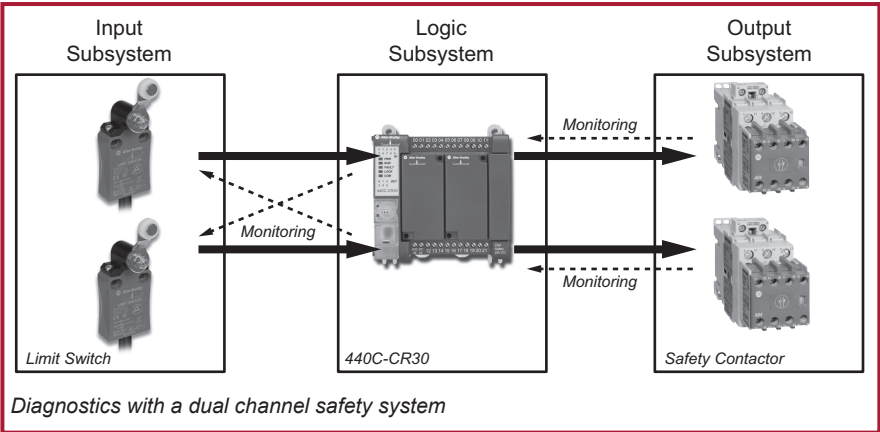


A dual channel [also called redundant or “fault-tolerant”] system shown above. Each subsystem has two channels and can tolerate a single fault and still provide the safety function. This safety function would need to have two failures, one in each channel before the subsystem, and therefore the system, fails. Clearly a dual channel system is less likely to fail to a dangerous condition than a single channel system. But we can make it even more reliable [in terms of its safety function] if we include diagnostic measures for fault detection. Of course, having detected the fault we also need to react to it and put the system into a safe state. The following diagram shows the inclusion of diagnostic measures achieved by monitoring techniques.





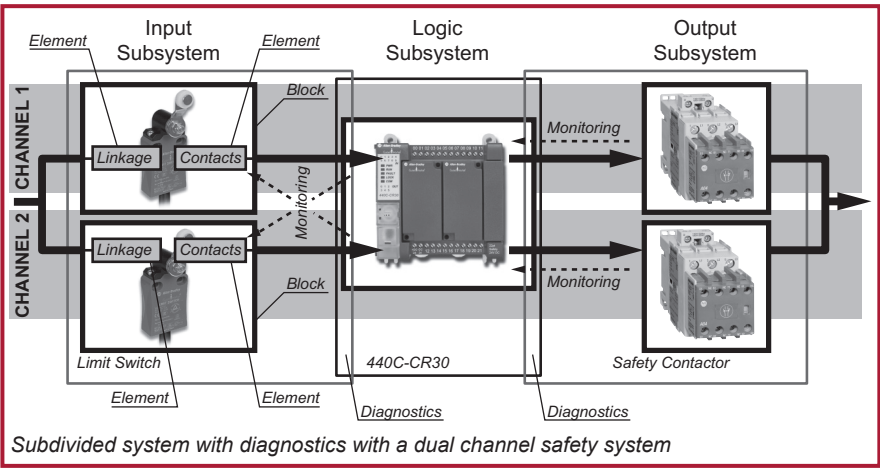
# Safety related control systems for machinery



*Diagnostics with a dual channel safety system*

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

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



*Subdivided system with diagnostics with a dual channel safety system*

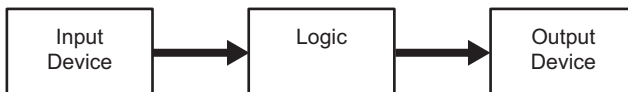
## System Design According to (EN) ISO 13849

The limit switches subsystem is shown subdivided down to its element level. The output contactor subsystem is subdivided down to its block level. The logic subsystem is not subdivided because it is already qualified and validated by the manufacturer to a given PL. The monitoring function for both the limit switches and the contactors is performed by the logic controller. Therefore the boxes representing the limit switch and contactor subsystems have a small overlap with the logic subsystem box.

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

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

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

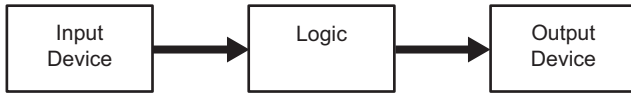


*Designated Architecture Category B*

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

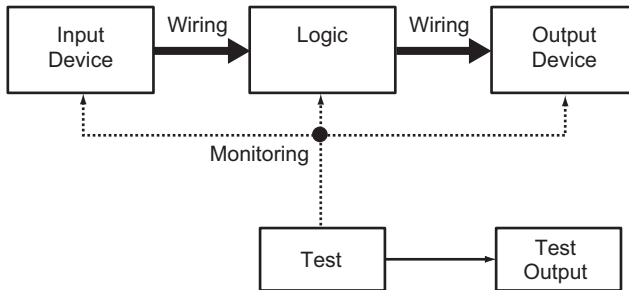


## Safety related control systems for machinery



*Designated Architecture Category 1*

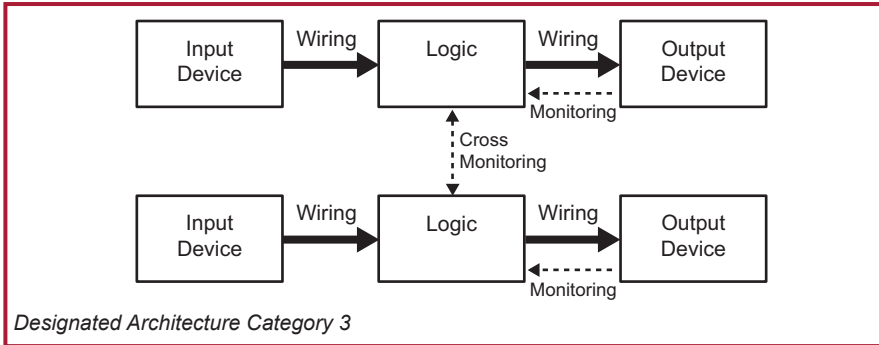
Designated Architecture Category 1 has the same structure as Category B and can still fail in the event of a single fault. But because it must also use well tried safety principles [see annex of (EN) ISO 13849-2] this is less likely than for Category B. See (EN) ISO 13849-1 for full requirements.



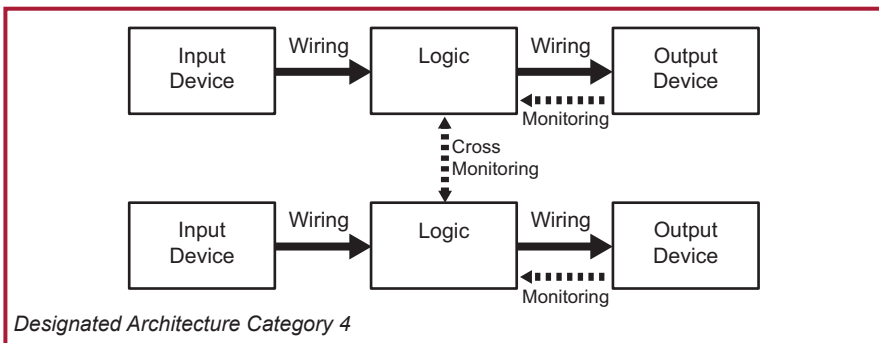
*Designated Architecture Category 2*

Designated Architecture Category 2 must use basic safety principles [see annex of (EN) ISO 13849-2]. There must also be diagnostic monitoring via a functional test of the system or subsystem. This must occur at start up and then periodically with a frequency that equates to at least one hundred tests to every demand on the safety function. The 2015 amendment allows for an alternative requirement for the safety function to go to safe state before process safety time.. The system or subsystem can still fail if a single fault occurs between the functional tests but this is usually less likely than for Category 1. Note that for Category 2 used for PLd there must be two signal output devices because, in the event of a fault detection, the test output must initiate a safe state. See (EN) ISO 13849-1 for full requirements.

## System Design According to (EN) ISO 13849



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



Designated Architecture Category 4 must use basic safety principles [see annexes of (EN) ISO 13849-2]. It has a similar requirements diagram to Category 3 but it



demands greater monitoring i.e. higher Diagnostic Coverage. This is shown by the heavier dotted lines representing the monitoring functions. In essence the difference between Categories 3 and 4 is that for Category 3 most faults must be detected but for Category 4 all single dangerous faults and dangerous combinations of faults must be detected. In practice this is usually achieved by having a high level of diagnostics to ensure that all relevant faults are detected before any accumulation is possible. The DC needs to be at least 99%.

### Reliability Data

(EN) ISO 13849-1 uses quantitative reliability data as part of the calculation of the PL achieved by the safety related parts of a control system. The first question this raises is “where do we get this data from?” It is possible to use data from recognised reliability handbooks but the standard makes it clear that the preferred source is the manufacturer. To this end, Rockwell Automation has made the relevant information available in the form of a data library for SISTEMA.

Before we go any further we should consider what types of data are required and also gain an understanding of how it is produced.

The ultimate type of data required as part of the PL determination in the standard [and SISTEMA] is the PFH [the probability of dangerous failure per hour]. This is the same data as used in IEC 61508 and represented by the  $PFH_D$  abbreviation used in IEC/EN 62061.

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

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

## System Design According to (EN) ISO 13849

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

### MTTF<sub>D</sub> of a Single Channel

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

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

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

Formula D1 from (EN) ISO 13849-1

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

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

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

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



The standard groups the  $MTTF_D$  into three ranges as follows:-

Denotation of $MTTF_D$ of each channel	Range of $MTTF_D$ of each channel
Low	3 years $\leq$ $MTTF_D$ < 10 years
Medium	10 years $\leq$ $MTTF_D$ < 30 years
High	30 years $\leq$ $MTTF_D$ < 100 years

### Levels of $MTTF_D$

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

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

### Methods of Data Determination

We now need to delve one stage deeper into how a manufacturer determines the data either in the form of  $PFH_D$  or  $MTTF_D$ . An understanding of this is essential when dealing with manufacturers data. Components can be grouped into three basic types:

- Mechanistic (Electro-mechanical, mechanical, pneumatic, hydraulic etc)
- Electronic (i.e. solid state)
- Software

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

### Mechanistic Technology:

Failure is proportional to both the inherent reliability and the usage rate. The greater the usage rate, the more likely that one of the component parts may be degraded and fail. Note that this is not the only failure cause, but unless we limit the operation time/cycles it will be the predominant one. It is self evident that a contactor that has switching cycle of once per ten seconds will operate reliably for a far shorter time than an identical contactor that operates one per day.

## System Design According to (EN) ISO 13849

Physical technology devices generally comprise components that are individually designed for their specific use. The components are shaped, moulded, cast, machined etc. They are combined with linkages, springs, magnets, electrical windings etc to form a mechanism. Because the component parts do not, in general, have any history of use in other applications, we cannot find any pre-existing reliability data for them. The estimation of the  $PFH_D$  or  $MTTF_D$  for the mechanism is normally based on testing. Both EN/IEC 62061 and (EN) ISO 13849-1 advocate a test process known as  $B10_D$  Testing.

In the  $B10_D$  test a number of device samples [usually at least ten] are tested under suitably representative conditions. The mean number of operating cycles achieved before 10% of the samples fail to the dangerous condition is known as the  $B10d$  value. In practice it is often the case that all of the samples will fail to a safe state but in that case the standard states that the  $B10d$  [dangerous] value can be taken as twice the  $B10$  value.

### Electronic Technology:

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

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

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

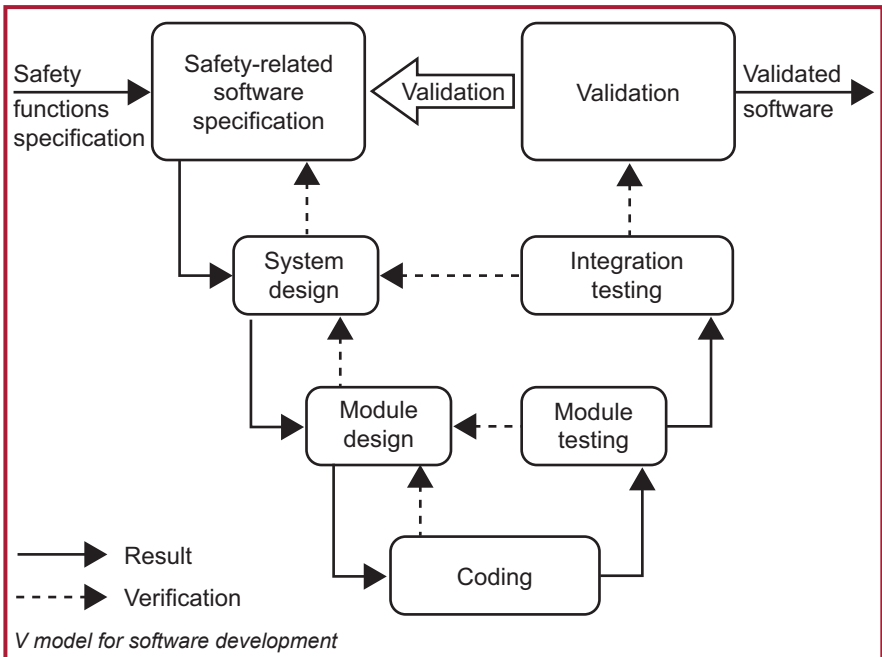




## Safety related control systems for machinery

### Software:

Failures of software are inherently systematic in nature. Failures are caused by the way it is conceived, written or compiled. Therefore all failures are caused by the system under which it is produced, not by its use. Therefore in order to control the failures we must control that system. Both IEC 61508 and (EN) ISO 13849-1 provide requirements and methodologies for this. We do not need to go into detail here other than to say they use the classic V model. Embedded software is an issue for the designer of the device. The usual approach is to develop embedded software in accordance with the formal methods laid out in IEC 61508 part 3. When it comes to application code, the software that a user interfaces with, most programmable safety devices are provided with “certified” function blocks or routines. This simplifies the validation task for application code but it must be remembered that the completed application program still needs to be validated. The way the blocks are linked and parameterised must be proved correct and valid for the intended task. (EN) ISO 13849-1 and IEC/EN 62061 both provide guidelines for this process.



## System Design According to (EN) ISO 13849

### Diagnostic Coverage

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

**Dangerous detected failure [ $\lambda_{dd}$ ]** i.e. Those failures that would cause, or could lead to, a loss of the safety function, but which are detected. After detection, a fault reaction function causes the device or system to go to safe state.

**Dangerous failure [ $\lambda_d$ ]** i.e. All those failures that could potentially cause, or lead to, a loss of the safety function. This includes both the failures that are detected and those that are not. Of course the failures that are truly dangerous are the dangerous undetected ones [termed  $\lambda_{du}$ ]

DC is expressed by the formula;

DC =  $\lambda_{dd}/\lambda_d$  expressed as a percentage.

This meaning of the term DC is common to (EN) ISO 13849-1 and EN/IEC 62061. However the way that it is derived differs. The latter standard proposes the use of calculation based on failure mode analysis but also allows the use of the simplified method in the form of look-up tables as provided in (EN) ISO 13849-1. Various typical diagnostic techniques are listed together with the DC percentage that their use is deemed to achieve. In some cases rational judgment is still required, for example in some techniques the achieved DC is proportional to how often the test is performed. It is sometimes argued that this approach is too vague. However the estimation of DC can depend on many different variables and whichever technique is used the result can usually only truly be described as approximate.

It is also important to understand that the tables in (EN) ISO 13849-1 are based on extensive research conducted by the IFA into the results achieved by known, actual diagnostic techniques used in real applications. In the interest of simplification the standard divides DC into four basic ranges.

<60% = none  
 60% to <90% = low  
 90% to <99% = medium  
 ≥99% = high



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

### Common Cause Failure

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

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

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

*Scoring for Common Cause Failure*

## System Design According to (EN) ISO 13849

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

### Systematic Faults

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

### Fault Exclusion

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



During the analysis, certain faults may be uncovered that cannot be detected with automatic diagnostic testing without undue economic costs. Further, the probability that these faults might occur may be made extremely small because of 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.

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

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

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

### Performance Level (PL)

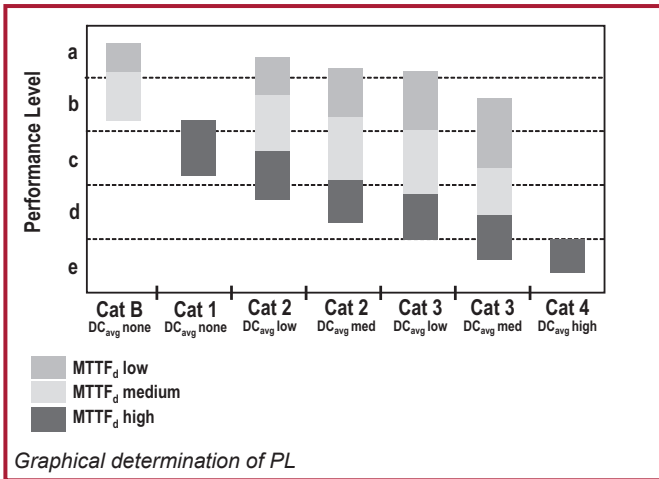
The performance level is a discrete level that specifies the ability of the safety-related parts of the control system to perform a safety function.

In order to assess the PL achieved by an implementation of any of the five designated architectures, the following data is required for the system (or subsystem):

- $MTTF_D$  (mean time to dangerous failure of each channel)
- DC (diagnostic coverage).
- Architecture (the category)

The following diagram shows a graphical method for determining the PL from the combination of these factors. The table at Annex K shows the tabular results of different Markov models that created the basis of this diagram. Refer to the table when more precise determination is needed.

## System Design According to (EN) ISO 13849



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, the tables at Annex K can be used to derive the PL.

### Subsystem Design and Combinations

Subsystems that conform to a PL can be combined into a system using the table as shown.

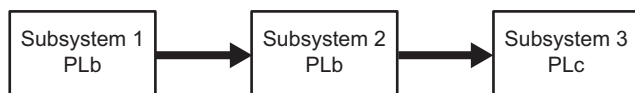
PL <sub>low</sub>	N <sub>low</sub>	PL
a	>3	not allowed
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

*PL calculation for series combined subsystems*



The use of this table from the standard is not mandatory, it is just intended to provide a very simple and a worst case alternative method if the PFHd values are not known. The system PL can be calculated by other methods including SISTEMA. The rationale behind the table is clear. First, that the system can only be as good as its weakest subsystem. Second, the more subsystems there are, the greater the possibility for failure.

In the system shown in the following diagram, the lowest Performance Levels are at Subsystems 1 and 2. Both are PLb. Therefore, using this table, we can read across b (in the PL<sub>low</sub> column), through 2 (in the N<sub>low</sub> 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.



*Combination of series subsystems as a PLb system*

### Validation

Validation of safety functions includes and goes beyond the verification of the achieved performance levels. The intent is to validate that the implemented safety function does in fact support the overall safety requirements for the machinery. Validation plays an important role throughout the safety system development and commissioning process. ISO/EN 13849-2:2012 sets the requirements for validation. It calls for a validation plan and discusses validation by testing and analysis techniques such as Fault Tree Analysis and Failure Modes, Effects and Criticality Analysis. Most of these requirements will apply to the manufacturer of the subsystem rather than the subsystem user.

### Machine Commissioning

At the system or machine commissioning stage, validation of the safety functions must be carried out in all operating modes and should cover all normal and foreseeable abnormal conditions. Combinations of inputs and sequences of operation must also be taken into consideration. This procedure is important because it is always necessary to check that the system is suitable for actual operational and environmental characteristics. Some of those characteristics may be different from the ones anticipated at the design stage.

# System Design According to IEC/EN 62061

## Chapter 8: 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 a:

- 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 the table below 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	HFT
Safe Failure Fraction	SFF
Proof Test Interval	$T_1$
Diagnostic Test Interval	$T_2$
Susceptibility to Common Cause Failures	$\beta$
Diagnostic Coverage	DC

### *Elements for SIL Consideration*

### **Subsystems**

The term “subsystem” has a special meaning in IEC/EN 62061. It is the first level subdivision of a system into parts which, if they fail, would cause a failure of the safety function. Therefore if two redundant switches are used in a system neither individual switch is a subsystem. The subsystem would comprise both switches and any associated fault diagnostic function.





### Probability of Dangerous Failure per Hour ( $PFH_D$ )

IEC/EN 62061 uses the same basic methods as discussed in the section on (EN) ISO 13849-1 to determine failure rates at the component level. The same provisions and methods apply for “mechanistic” and electronic components. In IEC/EN 62061 there is no consideration of  $MTTF_D$  in years. The failure rate per hour ( $\lambda$ ) is either calculated directly or obtained or derived from the B10 value by the following formula:

$$\lambda = 0.1 \times C/B10 \text{ (where } C = \text{the number of operating cycles per hour)}$$

There is a significant difference between the standards in the methodology for determining the total  $PFH_D$  for a subsystem or system. An analysis of the components must be undertaken to determine the probability of failure of the subsystems. Simplified formulae are provided for the calculation of common subsystem architectures (described later in text). Where these formulae are not appropriate it will be necessary to use more complex calculation methods such as Markov models. The Probability of Dangerous Failure ( $PFH_D$ ) of each subsystem are then added together to determine the total  $PFH_D$  for the system. Table 3 of the standard can then be used to determine which Safety Integrity Level (SIL) is appropriate to that range of  $PFH_D$ .

SIL (Safety Integrity Level)	$PFH_D$ (Probability of dangerous failure per hour)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

#### *Probabilities of Dangerous Failure for SILs*

The  $PFH_D$  data for a subsystem will usually be provided by the manufacturer. Data for Rockwell Automation safety components and systems is available at:

[www.rockwellautomation.com](http://www.rockwellautomation.com), under Solutions & Services > Safety Solutions

IEC/EN 62061 also makes it clear that reliability data handbooks can be used if and where applicable.

For low complexity electromechanical devices, the failure mechanism is usually linked to the number and frequency of operations rather than just time. Therefore for these components the data will derived from some form of testing (e.g. B10 testing as described in the chapter on (EN) ISO 13849-1). Application based information such as the anticipated number of operations per year is then required in order to convert the B10d or similar data to  $PFH_D$ .

## System Design According to IEC/EN 62061

NOTE: In general the following is true (taking into account a factor to change years to hours):

$$PFH_D = 1/MTTF_D$$

However, it is important to understand that, for a dual channel system (with or without diagnostics), it is not correct to use  $1/PFH_D$  to determine the  $MTTF_D$  that is required by (EN) ISO 13849-1. That standard calls for the  $MTTF_D$  of a single channel. This is a very different value to the  $MTTF_D$  of the combination of both channels of a two channel subsystem including the effect of diagnostic coverage.

### Architectural Constraints

The essential characteristic of IEC/EN 62061 is that the safety system is divided into subsystems. The hardware safety integrity level that can be claimed for a subsystem is limited not only by the  $PFH_D$  but also by the hardware fault tolerance and the safe failure fraction of the subsystems. Hardware fault tolerance is the ability of the system to execute its function in the presence of faults. A fault tolerance of zero means that the function is not performed when a single fault occurs. A fault tolerance of one allows the subsystem to perform its function in the presence of a single fault. Safe Failure Fraction is the portion of the overall failure rate that does not result in a dangerous failure. The combination of these two elements is known as the architectural constraint and its output is the SIL Claim Limit (SIL CL). The following table shows the relationship of the architectural constraints to the SILCL. A subsystem (and therefore its system) must satisfy both the  $PFH_D$  requirements and the Architectural Constraints together with the other relevant provisions of the standard.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance		
	0	1	2
<60%	Not allowed unless specific exceptions apply	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - < 99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

#### Architectural Constraints on SIL

For example, a subsystem architecture that possesses single fault tolerance and has a safe failure fraction of 75% is limited to no higher than a SIL2 rating, regardless of the probability of dangerous failure. When combining subsystems, the



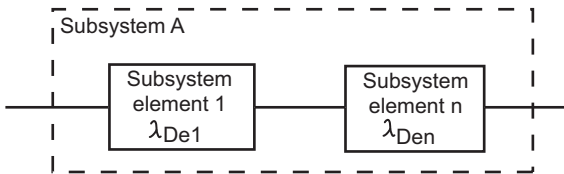
## System Design According to IEC/EN 62061

the evaluation of the  $PFH_D$  achieved by a complex subsystem can be a very complicated process using techniques such as Markov modelling, reliability block diagrams or fault tree analysis.

IEC/EN 62061 does give requirements for the design of lower complexity subsystems. Typically this would include relatively simple electrical components such as interlock switches and electromechanical safety monitoring relays. The requirements are not as involved as those in IEC 61508 but can still be quite complicated.

IEC/EN 62061 supplies four subsystem logical architectures with accompanying formulae that can be used to evaluate the  $PFH_D$  achieved by a low complexity subsystem. These architectures are purely logical representations and should not be thought of as physical architectures. The four subsystem logical architectures with accompanying formulae are shown in the following four diagrams.

For a basic subsystem architecture shown below, the probabilities of dangerous failures are simply added together.



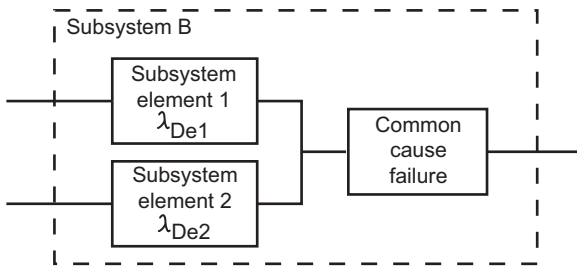
*Subsystem logical architecture A*

$$\lambda_{DssA} = \lambda_{De1} + \dots + \lambda_{Den}$$

$$PFHD_{ssA} = \lambda_{DssA}$$

$\lambda$  Lambda is used to designate the failure rate. The units of the failure rate are failures per hour.  $\lambda_D$ , Lambda sub D is the dangerous failure rate.  $\lambda_{DssA}$ , Lambda sub DssA is the dangerous failure rate of subsystem  $\lambda$ . Lambda sub 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 the probability of failure within one hour.

The next diagram 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.



*Subsystem logical architecture B*

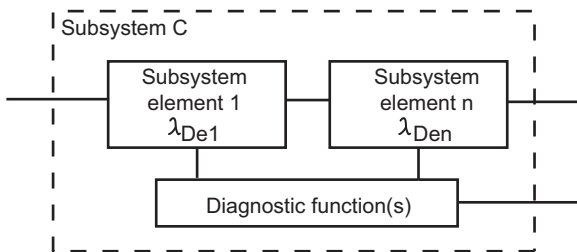
$$D_{ssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T1 + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$
$$PFHD_{ssB} = \lambda_{DssB}$$

The formulae for this architecture takes into account the parallel arrangement of the subsystem elements and adds the following two elements from the previous table 'Elements for SIL Consideration'.

$\beta$  - 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. In practical terms this usually means replacement (like the equivalent term "mission time" in (EN) ISO 13849-1).

The next diagram shows the functional representation of a zero fault tolerant system with a diagnostic function. Diagnostic coverage is used to decrease the probability of dangerous hardware failures. The diagnostic tests are performed automatically. The definition of diagnostic coverage is the same as given in (EN) ISO 13849-1 i.e. the ratio of the rate of detected dangerous failures compared to the rate of all dangerous failures.



*Subsystem logical architecture C*

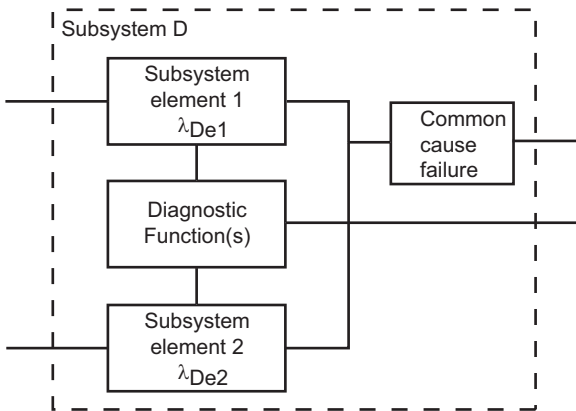
## System Design According to IEC/EN 62061

$$\lambda_{DssC} = \lambda_{De1} (1-DC1) + \dots + \lambda_{Den} (1-DCn)$$

$$PFHD_{ssC} = \lambda_{DssC}$$

These formulae include the diagnostic coverage, DC, for each of the subsystem elements. The failure rates of each of the subsystems are reduced by the diagnostic coverage of each subsystem.

The fourth example of a subsystem architecture is shown next. 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.



### Subsystem logical architecture D

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

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De1} \times \lambda_{De2} \times (DC1 + DC2)] \times T2 / 2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC1 - DC2)] \times T1 / 2 \} + \beta \times (\lambda_{De1} + \lambda_{De2}) / 2$$

$$PFHD_{ssD} = \lambda_{DssD}$$

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

$$\lambda_{DssD} = (1 - \beta)^2 \{ [\lambda_{De}^2 \times 2 \times DC] \times T2 / 2 + [\lambda_{De}^2 \times (1-DC)] \times T1 \} + \beta \times \lambda_{De}$$

$$PFHD_{ssD} = \lambda_{DssD}$$

Notice that both formulas use one additional parameter, T2 the diagnostic interval. This is just a periodic check of the function. It is a less comprehensive test than the Proof Test.



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

$$\beta = 0.05$$

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

$$T1 = 87600 \text{ hours (10 years)}$$

$$T2 = 2 \text{ hours}$$

$$DC = 90\%$$

**PFHD<sub>ssD</sub>** = 5.790E-8 dangerous failures per hour. This would be within the range required for SIL3

### Effect of the Proof Test Interval

IEC/EN 62061 states that a Proof Test Interval (PTI) of 20 years is preferred (but not mandatory) Let us look at the effect the proof test interval has on the system. If we re- calculate the formula with T1 at 20 years it gives the result PFHD<sub>ssD</sub> = 6.58E-8. It is still within the range required for SIL 3. The designer must keep in mind that this subsystem must be combined with other subsystems to calculate the overall dangerous failure rate.

### Effect of Common Cause Failure Analysis

Let's look at the effect the common cause failures have on the system. Suppose we take additional measures and our  $\beta$  (Beta) value improves to 1% (0,01), while the proof test interval remains at 20 years. The dangerous failure rate improves to 2.71E-8 which means that the subsystem is now more suitable for use in a SIL 3 system.

### Common Cause Failure (CCF)

Common cause failure is when multiple faults resulting from a single cause produce a dangerous failure. Information on CCF will generally only be required by the subsystem designer, usually the manufacturer. It is used as part of the formulae given for estimation of the  $PFH_D$  of a subsystem. It will not usually be required at the system design level.

Annex F of IEC/EN62061 provides a simple approach for the estimation of CCF. The table below shows a summary of the scoring process

## System Design According to IEC/EN 62061

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

### Scoring for Measures Against Common Cause Failure

Points are awarded for employing specific measures against CCF. The score is added up to determine the common cause failure factor, which is shown in the following table. The beta factor is used in the subsystem models to “adjust” the failure rate.

Overall Score	Common Cause failure factor (R)
<35	10% (0,1)
35 - 65	5% (0,05)
65 - 85	2% (0,02)
85 - 100	1% (0,01)

### Beta Factor for Common Cause Failure

### Diagnostic Coverage (DC)

Automatic diagnostic tests are employed to decrease the probability of dangerous hardware failures. Being able to detect all dangerous hardware failures would be ideal, but in practice the maximum value is set at 99% (this can also be expressed as 0.99)

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

$$DC = \frac{\text{Probability of Detected dangerous failures, } \lambda_{DD}}{\text{Probability of Total dangerous failures, } \lambda_{Dtotal}}$$

The value of diagnostic coverage will lie between zero and 99%.





## 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.

## Proof Test Interval

The proof test interval represents the time after which a subsystem must be either totally checked or replaced to ensure that it is in an “as new” condition. In practice, in the machinery sector, this is achieved by replacement. So the proof test interval is usually the same as lifetime. (EN) ISO 13849-1 refers to this as Mission Time.

A proof test is a check that can detect faults and degradation in a SRCS so that the SRCS can be restored as close as practical to an “as new” condition”. The proof test must detect 100% of all dangerous faults including the diagnostic function (if any). 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. It is more usual to just replace the subsystem with a new one rather than actually perform a proof test.

## Safe Failure Fraction (SFF)

The safe failure fraction is similar to diagnostic coverage but also takes account of any inherent tendency to fail towards a safe state. For example, when a fuse blows, there is a failure but it is highly probable that the failure will be to an open circuit which, in most cases, would be a “safe” failure. SFF is (the sum of the rate of “safe” failures plus the rate of detected dangerous failures) divided by (the sum of the rate of “safe” failures plus the rate of detected and undetected dangerous failures). It is important to realize that the only types of failures to be considered are those which could have some effect on the safety function.

## System Design According to IEC/EN 62061

The SFF value will normally be stated by the manufacturer if it is relevant.

The Safe Failure Fraction (SFF) can be calculated using the following equation:

$$\text{SFF} = (\sum \lambda_s + (\sum \lambda_{DD})) / ((\sum \lambda_s + (\sum \lambda_D))$$

where

- $\sum \lambda_s$  = the rate of safe failure,
- $\sum \lambda_s + \sum \lambda_D$  = the rate of all failure,
- $\lambda_{DD}$  = the rate of detected dangerous failure
- $\lambda_D$  = the rate of all 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 some form of 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



## Chapter 9: Safety-Related Control Systems, Additional Considerations

### Overview

This chapter looks at general structural considerations and principles that should be taken into account when designing a safety related control system..

### Categories of Control Systems

The “Categories” of control systems originated in the former EN 954-1:1996 (ISO13849-1:1999). However they are still often used to describe the structure of safety control systems and they remain an integral part of (EN) ISO13849-1 as Designated Architectures. The description and requirements of the Categories are discussed earlier in this publication at “Overview of (EN) ISO 13849-1”. This section is intended to provide a simplified but practical guide on how to implement the Category structures.

### Category B

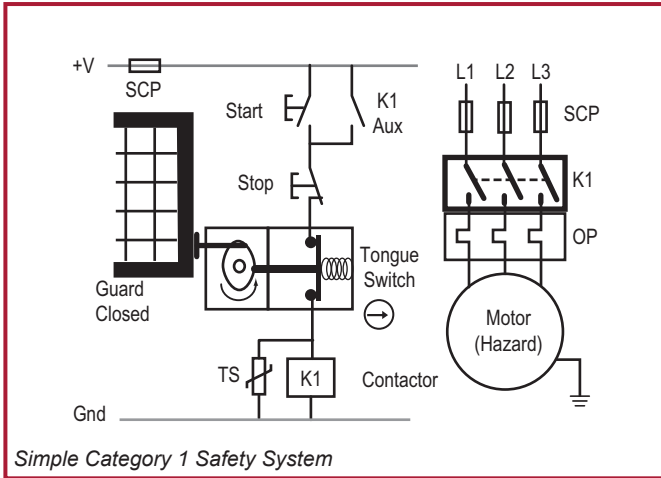
Category B should be regarded as the basic foundation upon which all the other Categories are built. It does not have any special provisions or structure for safety beyond the Basic Safety Principles as given in the Annexes A to D of (EN) ISO 13849-2. These represent general good practice in design and selection of materials.

### Category 1

Category 1 requires the use of Well Tried Components and Well Tried Safety Principles.

Shown here is a typical system intended to achieve Category 1. The interlock and the contactor play the key roles in removing energy from the motor, when access to the hazard is needed. The tongue interlock meets the requirements of IEC 60947-5-1 for direct opening action contacts, which is shown by the symbol of the arrow within the circle. With the well-tried components, the probability of energy being removed is higher for Category 1 than it would be for Category B. The use of well-tried components is intended to minimize the possibility of a loss of the safety function but note that a single fault can still lead to the loss of the safety function.

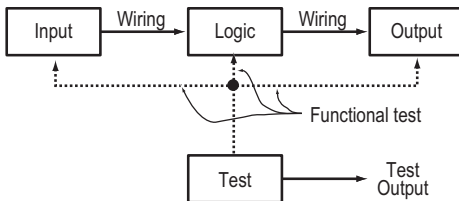
## Safety-Related Control Systems, Additional Considerations



Category 1 is intended to prevent failure by using simple design with components with high reliability. When this type of prevention by itself does not provide enough reduction of the risk, fault detection must be used. Categories 2, 3 and 4 are failure or 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 no faults are detected, the machine is allowed to run. If faults are detected a fault reaction function must ensure that the machine remains in a safe state.



The equipment performing the test can be an integral part of the safety system or a separate piece of equipment.



The testing must be performed:

- when the machine is initially powered,
- prior to the initiation of a hazard, and.
- periodically if deemed necessary by the risk assessment

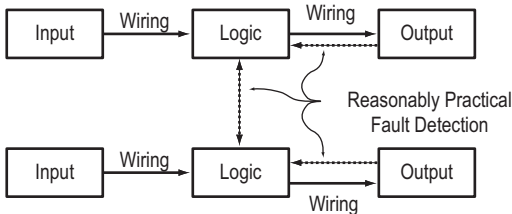
Note: (EN) ISO 138491-1 assumes a test to safety function demand ratio of 100:1 or a test at the demand of the safety function with the capability to detect a fault and stop the machine in a shorter time than it takes to reach the hazard.

In essence a safety system or subsystem must be exercised in order to test if its safety function is still working correctly. This means it can be difficult or impossible to implement with technologies that have mechanical characteristics. A Category 2 approach is usually more relevant to electronic technology. For PLd there must be a test output capable of initiating a safe state in the event of the detection of a fault.

### Category 3

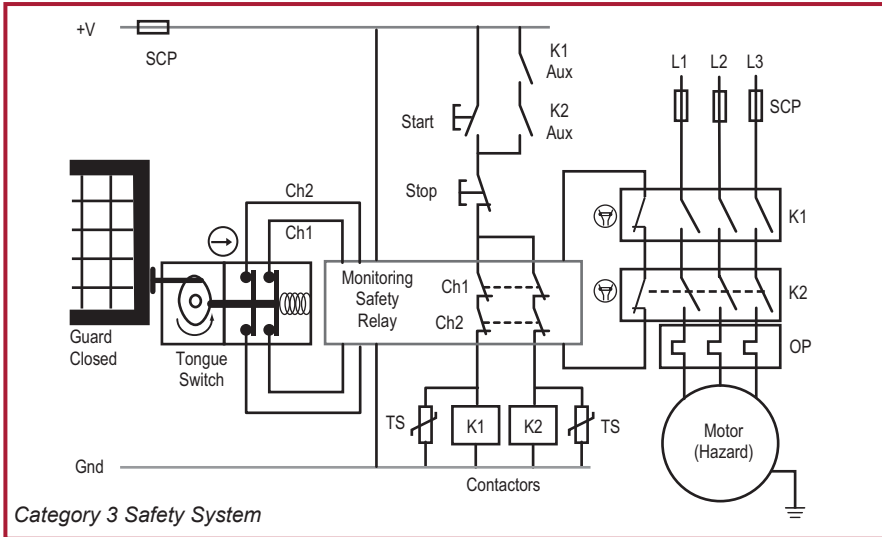
In addition to meeting the requirements of Category B and well-tried safety principles, Category 3 requires successful performance of the safety function in the presence of a single fault. The fault must be detected at or before the next demand on the safety function, whenever reasonably practicable.

Some faults, such as cross-faults, which do not cause an immediate loss of safety function may not be detected. This means that for Category 3 an accumulation of undetected faults can lead to the loss of the safety function.



Here is a block diagram to explain the principles of a Category 3 system. Redundancy combined with cross monitoring and output monitoring are used to ensure the performance of the safety function

## Safety-Related Control Systems, Additional Considerations



Shown here is an example of a Category 3 system. The tongue interlock switch has redundant sets of contacts. Internally, the monitoring safety relay (MSR) contains redundant circuits that cross monitor each other. A redundant set of contactors remove power from the motor. The contactors are monitored by the MSR via the mechanically linked contacts.

Fault detection must be considered for each part of the safety 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?

For Category 3 circuits it is common practice to use single tongue interlock switches with redundant electrical contact sets. This means that the possibility that a fault of a single component within the actuation linkage must be excluded. If this fault cannot be excluded it means that a single fault can cause the loss of the safety function. It is very important that any fault exclusion is fully justified.

The monitoring safety relay (MSR) provides fault diagnostics for the tongue interlock switch and for the contactors. The MSR can also facilitate other functionality such as a manual reset. In terms of their internal architecture monitoring safety relays are usually PLe or SIL3.

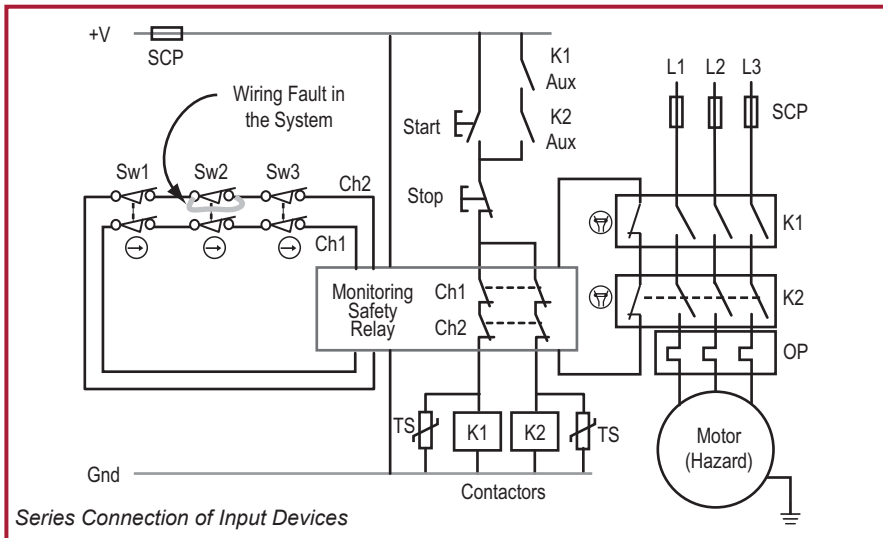
The two contactors should have overload and short-circuit protection. The probability of the contactor failing with welded contacts is small but not impossible. A contactor can



also fail due to its power switching contacts staying closed due to a stuck armature. If one contactor fails to a dangerous state, the second contactor will still continue to function and will remove power from the motor. The MSR will detect the faulted contactor upon the next machine cycle. When the gate is closed and the start button pressed, the mechanically linked contacts of the faulted contactor will remain open and the MSR will not be able to close its safety contacts, thereby, revealing the fault

## Undetected Faults

With a Category 3 system structure there may be some faults that cannot be detected but they must not, by themselves, lead to the loss of the safety function. Where faults can be detected we need to know if, under some circumstances, they could be either masked or unintentionally cleared by the operation of other devices within the system structure.



Shown here is a widely used approach for connecting multiple devices to a monitoring safety relay. Each device contains two normally closed direct opening action contacts. This approach saves wiring costs as the input devices are daisy-chained. Assume a short circuit fault occurs across one of the contacts at Sw2 as shown. Can this fault be detected?

If switch Sw1 (or Sw3) is opened, both Ch1 and Ch2 are open circuit and the MSR removes power from the hazard. If Sw3 is then opened and then closed again the fault across its contacts will not be detected because there is no change of status at the MSR: both Ch1 and Ch2 remain open. If Sw1 (or Sw3) is then closed, the

## Safety-Related Control Systems, Additional Considerations

hazard can be restarted by pressing the start button. Under these circumstances the fault did not cause a loss of the safety function but it was not detected, it remains in the system and a subsequent fault (a short circuit across the second contact of Sw2) could lead to the loss of the safety function.

If Sw2 alone was opened and closed, with no operation of the other switches, Ch1 opens and Ch2 remains closed. The MSR de-energizes the hazard because Ch1 opened. When Sw2 closes, the motor cannot be started when the Start button is pressed, because Ch2 did not open. The fault is detected. However if for any reason, Sw1 (or Sw3) is then opened and closed, both Ch1 and Ch2 will be open then closed circuit. This sequence simulates the clearing of the fault and will result in unintentional reset at the MSR.

This raises the question of what DC could be claimed for the individual switches within this structure when using (EN) ISO 13849-1 or IEC 62061? Up until the publication of ISO TR 24119 (November 2015: Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts) there was no specific definitive guidance on this but it was usual to assume a DC of 60% under the condition that the switches are individually tested at suitable periods to reveal faults. If it was foreseeable that one (or more) of the switches would never be individually tested then it could be argued that its DC should be described as zero. ISO TR 24119 provides detailed guidance for the determination of DC for guard interlocking devices using series connected volt-free contacts. The following Table provides a basic overview. It is essential to study the document in full in order to determine the actual maximum allowable DC for any particular architecture and application.

Number of frequently used movable guards <sup>1</sup>	Number of additional movable guards	Masking probability	Diagnostic Coverage	Maximum Achievable PL
0	2 to 4	Low	Medium	PL d
	5 to 30	Medium	Low	PL d
	>30	High	None	PL c
1	1	Low	Medium	PL d
	2 to 4	Medium	Low	PL d
	≥5	High	None	PL c
>1	--	High	None	PL c

<sup>1</sup> Switching frequency greater than once per hour



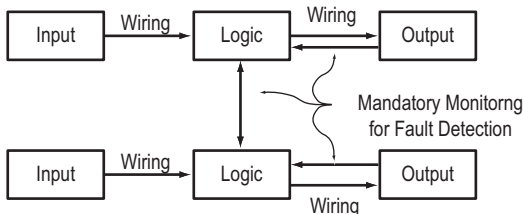


The series connection of electro-mechanical contacts is limited to a maximum of PLd and in some cases can be constrained to a maximum of PLc. Note that in any case, if it is foreseeable that fault masking will occur (e.g. multiple movable guards will be open at the same time as part of normal operation or service), then the DC is limited to none.

It is interesting to note that these characteristics of a Category 3 structure have always required consideration but they are brought into sharp focus by the functional safety standards.

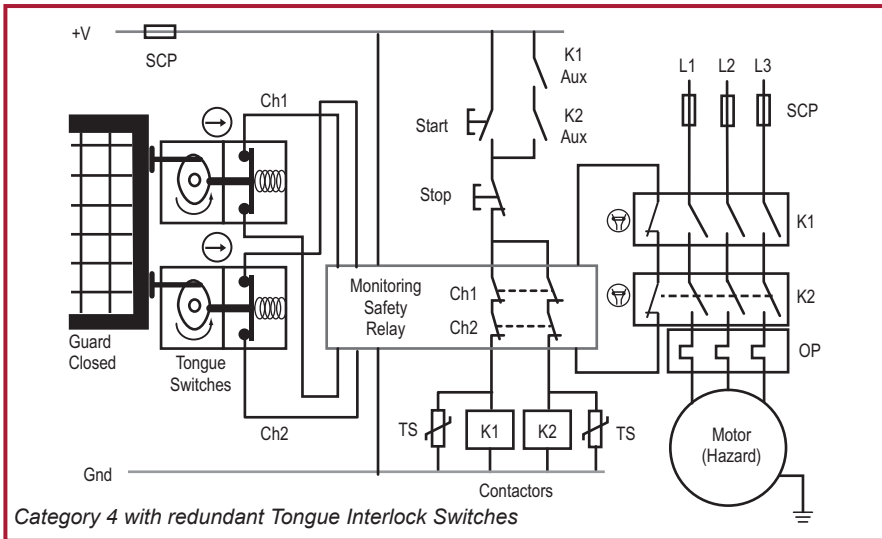
### Category 4

Like Category 3, Category 4 requires the safety system to meet Category B, use well tried safety principles and perform the safety function in the presence of a single fault. Unlike Category 3 where an accumulation of faults can lead to the loss of the safety function, Category 4 requires performance of the safety function in the presence of an accumulation of faults. In practice this is usually achieved by having a high level of diagnostics to ensure that all relevant faults are detected before any accumulation is possible. When considering a theoretical accumulation of faults, 2 faults may be sufficient, although 3 fault consideration may be necessary for some designs.

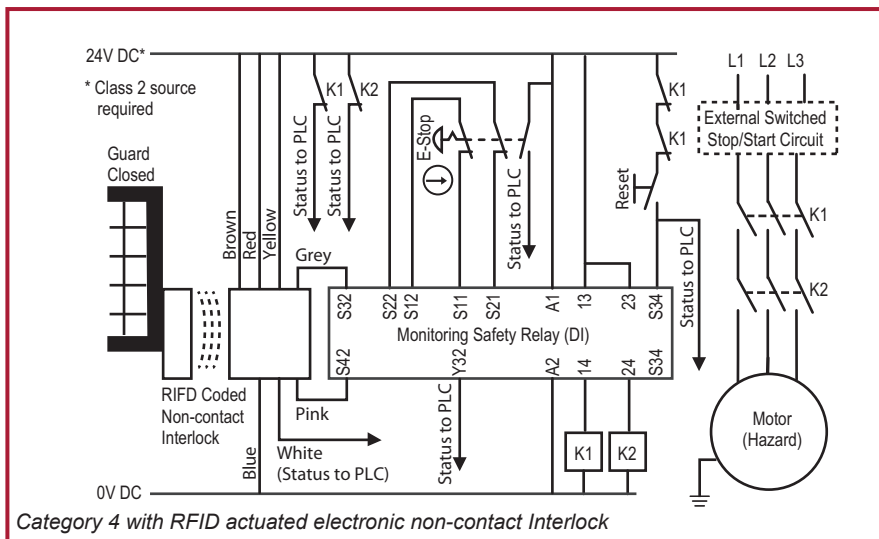


Shown here is the block diagram for Category 4. Monitoring of both output devices and cross monitoring is required. Category 4 has a higher diagnostic coverage than Category 3.

## Safety-Related Control Systems, Additional Considerations



Up until relatively recently, single tongue actuated interlock switches with two electrical channels have been considered for use in Category 4 circuits. In order to use a single tongue interlock in a dual channel circuit it is necessary to exclude the possible single fault failure points on the mechanical actuation tongue and switch linkage. However, the Joint Technical Report ISO TR 23849 has clarified that this type of fault exclusion should not be used in PLe or SIL 3 systems. If the safety system designer prefers using tongue style interlocks, then two separate switches can be used to meet Category 4.



Contemporary technology has a different approach to achieving a Category 4 architecture (and PLe / SIL 3). The use of complex electronics has enabled the cost effective integration of fault tolerance and a high level of diagnostic coverage into a single device. The interlocking device shown not only achieves Category 4, it also provides an extremely high level of resistance to tampering (overriding) by the use of RFID coding. It can also be connected in series with other similar devices with no lowering of Category or diagnostic coverage.

### PL (Performance Level) for Component and System Ratings

The Designated Architectures (Categories) of (EN) ISO 13849 can be used as part of safety component (device) PL ratings as well as system PL ratings. This generates some confusion that can be clarified by understanding the components and their capabilities. By studying the preceding examples we find that a component such as an interlock switch rated to Category 1 can be used on its own in a Category 1 system.

It can also form part of a Category 3 or 4 system if two of the components are used together with a diagnostic function provided by a monitoring safety relay

Some components such as monitoring safety relays and programmable safety controllers have their own internal diagnostics and they check themselves to ensure proper performance. Therefore they can be rated as safety components to meet Categories 2, 3 or 4 without any additional measures.

## Safety-Related Control Systems, Additional Considerations

### 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 is needed. ISO 13849-1 and ISO 13849-2 provide details on fault considerations and fault exclusions.

If a fault results in a failure of a subsequent component, the first fault and all the subsequent faults shall be considered a single 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 independent faults at the same time is considered to be highly unlikely and is not considered in this analysis.

### Fault Exclusions

(EN) ISO 13849-1 and IEC 62061 permit the use of fault exclusions when determining a safety system classification if it can be shown that the occurrence of the fault is extremely unlikely. It is important that where fault exclusions are used that they are properly justified and are valid for the intended lifetime of the safety system. The greater the level of risk protected by the safety system then the more stringent becomes the justification required for the fault exclusion. This has always caused some confusion about when certain types of fault exclusion can or cannot be used. As we have seen already in this chapter, recent standards and guidance documents have clarified some aspects of this issue.

In general, where PLe or SIL3 is specified for a safety function to be implemented by a safety system ISO TR 23849 explains that it is not normal to rely upon fault exclusions to achieve this level of performance. This is dependent upon the technology used and the intended operating environment. Therefore it is essential that the designer takes additional care on the use of fault exclusions as that the PLe or SIL increases. For example fault exclusion is not applicable to the mechanical aspects of electromechanical position switches and manually operated switches (e.g. an emergency stop device) in order to achieve a PLe or SIL3 system. Those fault exclusions that can be applied to specific mechanical fault conditions (e.g. wear/corrosion, fracture) are described in Table A.4 of ISO 13849-2. Therefore a guard interlocking system that has to achieve PLe or SIL3 will need to incorporate a minimum fault tolerance of 1 (e.g. two conventional mechanical position switches) in order to achieve this level of performance since it is not normally justifiable to exclude faults, such as, broken switch actuators. However, it may be acceptable to exclude faults, such as short circuit of wiring within a control panel designed in accordance with relevant standards.



## Stop Categories according to IEC/EN 60204-1 and NFPA 79

It is both unfortunate and confusing that the term “Category” in relation to safety related control systems has different meanings. So far we have discussed the categories that originated in EN 954-1. They are a classification of the performance of a safety system under fault conditions.

There is also a classification known as “Stop Categories” that originated in IEC/EN 60204-1 and NFPA 79. There are three Stop Categories.

**Stop Category 0** requires immediate removal of power to the actuators. This is sometimes considered as an uncontrolled stop because, in some circumstances, motion can take some time to cease because the motor may be free to coast to a stop.

**Stop Category 1** requires that power is retained to apply braking until the stop is achieved and then remove power to the actuator. Note: See IEC 60204-1 for information on Stop Categories 1a and 1b.

**Stop Category 2** is a controlled stop with power left available to the machine actuators. A normal production stop is considered a category 2 stop.

Note that only Stop Categories 0 or 1 can be used as emergency stops. The choice of which of the two Categories to use should be dictated by a risk assessment.

All the circuit examples shown so far in this chapter have used a Stop Category 0. A Stop Category 1 is achieved with a time-delayed output for the final removal of power. An interlocked guard with guardlocking often accompanies a Category 1 stop system. This keeps the guard locked in a closed position until the machine has reached a safe (i.e., stopped) state.

Stopping a machine without taking proper account of the programmable controller may affect restarting and could result in tool and machine damage. A standard (non safety) PLC alone cannot be relied on for a safety related stopping task; therefore, other approaches need to be considered. Two possible solutions for category 1 stopping are given below:

### 1. Safety Relay with Time Delayed Override Command

A safety relay with both immediate acting and delayed action outputs is used. The immediate acting outputs are connected to inputs at the programmable device (e.g., PLC or the drive “enable”) and the delayed acting outputs are connected to a main 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 a sufficient time has elapsed to allow this process,

## Safety-Related Control Systems, Additional Considerations

the delayed output on the safety relay switches and isolates the main contactor.

Note: Any calculations to determine the overall stopping time must take the safety relay output delay period into account. This is particularly important when using this factor to determine the positioning of devices in accordance with the safety distance calculation

### 2. Safety PLCs

The logic and timing functions required can be conveniently implemented by using a Safety PLC such as GuardLogix.

### U.S. Safety Control System Requirements

#### Control Reliable

The highest level of risk reduction in the U.S. and Canadian robot standards is achieved by safety related control systems meeting the requirements of Control Reliable. Control reliable safety related control systems are dual channel architectures with monitoring. The stopping function of the robot must not be prevented by any single component failure, including the monitoring function.

The monitoring shall generate a stop command upon detection of a fault. If a hazard remains after motion stops, a warning signal must be provided. The safety system must remain in a safe state until the fault is corrected. Preferably, the fault is detected at the time of the failure. If this cannot be achieved, then the failure must be detected at the next demand on the safety system. Common mode failures must be taken into consideration if a significant probability of such a failure can occur.

The Canadian requirements differ from the U.S. requirement by adding two additional requirements. First, the safety related control systems shall be independent of the normal program control systems. Second, the safety system must not be easily defeated or bypassed without detection.

#### Comments on Control Reliable

The most fundamental aspect of Control Reliable is single fault tolerance and monitoring (fault detection). 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 detected, (2) adding the word “component” raises questions about wiring, and (3) wiring is an integral part of the safety system. Wiring faults can result in the loss of a safety function.



The intent of Control Reliability is clearly the performance of the safety function in the presence of a fault. If the fault is detected, then the safety system must execute a safe action, provide notification of the fault, and prevent further operation of the machine until the fault is corrected. If the fault is not detected, then the safety function must still be performed upon demand.

### Chapter 10: Application Examples

#### Overview - Pre-engineered safety functions for machines

Machinery safety functions – be it an emergency stop, guarding, or presence sensing function – require multiple elements including a sensor or input device, a logic device, and an output device. Together, these elements provide a level of protection calculated by Performance Level as outlined in (EN) ISO 13849-1.

In this chapter we have selected one of many pre-engineered safety functions for machines that Rockwell Automation have developed. These safety function documents each provide guidance for a specific safety function based on functional requirement, equipment selection, and performance level requirement, including set-up and wiring, configuration, verification and validation plan, and calculation of performance level.

The pre-engineered safety functions are free and are available to download on the Rockwell Automation website.

*[www.rockwellautomation.com](http://www.rockwellautomation.com), under Solutions & Services > Safety Solutions.*

The following pre-engineered safety function is based on a door-monitoring interlock switch with a configurable safety relay. The products used are: SensaGuard RFID coded, non-contact safety interlock switch which is connected to a Guardmaster 440C-CR30 configurable safety relay. The output devices used are 100S-C safety contactors.

The safety rating achieved by this pre-engineered safety function is: CAT. 4, PLe to (EN) ISO 13849-1.

The publication number of the original document is: SAFETY-AT133C-EN-P

#### Functional Safety Description

Personnel are protected from the hazardous motion by a fixed barrier. Access to the hazardous area, when necessary, is through a swinging door. The door is monitored by a SensaGuard non-contact interlock, which is connected to inputs of the 440C-CR30 configurable safety relay. The 440C-CR30 relay controls two 100S-C safety contactors which, connected in a series, control power to the motor that drives the hazardous motion. Whenever this monitored door is opened, the safety system

## Application Examples

removes power to the motor. The motor and the hazardous motion it drives coast to a stop (Stop Category 0). The motor cannot be restarted while the monitored door is open. Once the door is closed, the motor can be restarted by pressing and releasing the Reset button to reset the 440C-CR30 relay and then initiating the external Start to restore the motor power that is controlled by the 100S-C contactors.

The SensaGuard switch monitors the status (open or closed) of the door. The SensaGuard switch also monitors its two OSSD outputs for faults. The 440C-CR30 relay monitors the inputs from the SensaGuard switch for faults, and it also monitors the status of the Reset and Feedback signals from the 100S-C contactors. The relay monitors its own outputs for faults as well. These outputs control the 100S-C contactors. The 440C-CR30 relay turns off its outputs and removes power to the motor when a fault is detected. It does not reset until that fault is corrected.

### Bill of Material

This application uses these products.

Catalog Number	Description	Quantity
440N-Z21S16B	SensaGuard switch, 18 mm plastic, 2 x PNP, 0.2A max., safety output, 10 m cable	1
800FP-R611	800F reset, round plastic (type 4/4X/13, IP66), blue, R , standard pack	1
2080-IQ4OB4	4-channel digital input/output combination module	1
1761-CBL-PM02	Cable; 440C-CR30 configurable safety relay to personal computer, printer cable	1
440C-CR30-22BBB	Guardmaster 440C-CR30 software configured safety relay, PLe SIL 3, 22 safety I/O, embedded serial port, USB programming port, 2 plug-in slots, 24.0V DC	1
100S-C23EJ23BC	MCS 100S-C safety contactor, 23A, 24V DC (with electric coil), bifurcated contact	2

### System Overview

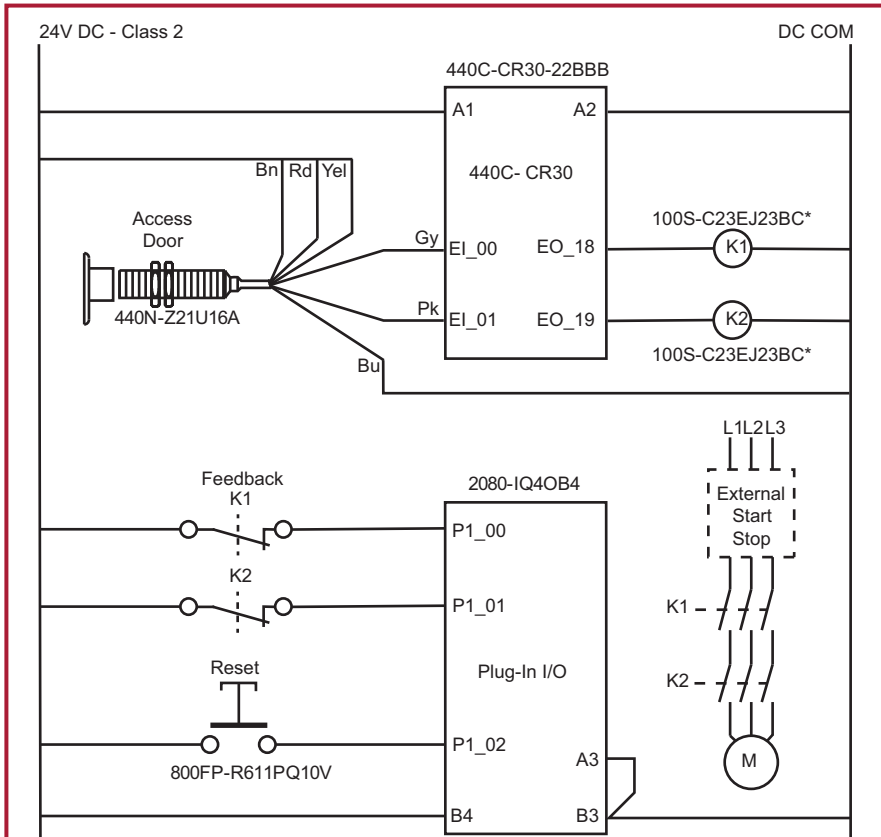
The SensaGuard interlock switch is used to confirm that the guarded door is in the safe, closed condition. Hazardous motion is ceased or prevented whenever this door is not closed. In addition to monitoring the state of the guarded door, the SensaGuard switch monitors its outputs for all fault conditions. The 440C-CR30 configurable safety relay also detects an open-wire fault, a single-channel fault, or a short to 0V at its SensaGuard switch inputs.





## Safety related control systems for machinery

The 440C-CR30 configurable safety relay monitors the pulse-tested outputs that drive the safety contactor coils for all fault conditions. The proper, safe state of the safety contactors, K1 and K2, is confirmed by the 440C-CR30 configurable safety relay that is monitoring the feedback signals at SMF2 at start-up.



*\*ISO 13849-2 requires transient suppression across the load as a Basic Safety Principal. The 'EJ' electronic coil provides suitable suppression.*

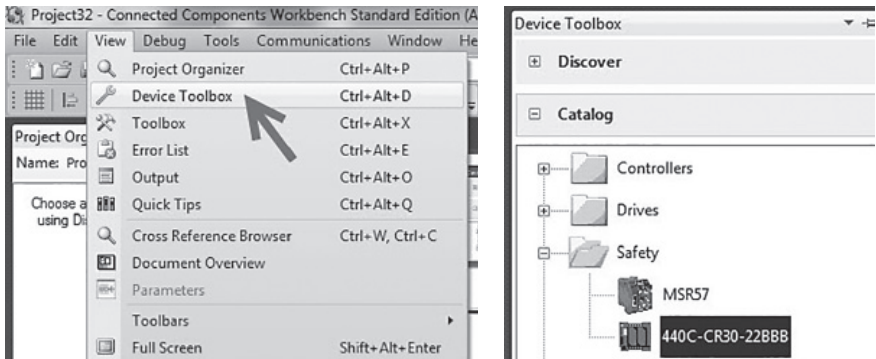
## Configuration

The 440C-CR30 relay is configured by using Connected Components Workbench™ software, release 6.01 or later. A detailed description of each step is beyond the scope of this document. Knowledge of the Connected Components Workbench software is assumed.

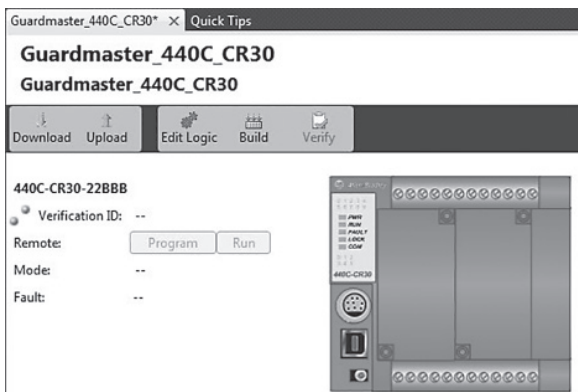
### Configure the 440C-CR30 Relay

Follow these steps to configure the Guardmaster 440C-CR30 relay in Connected Components Workbench software.

1. In Connected Components Workbench software, choose View and then Device Toolbox. When in Device Toolbox, select 440C-CR30-22BBB.

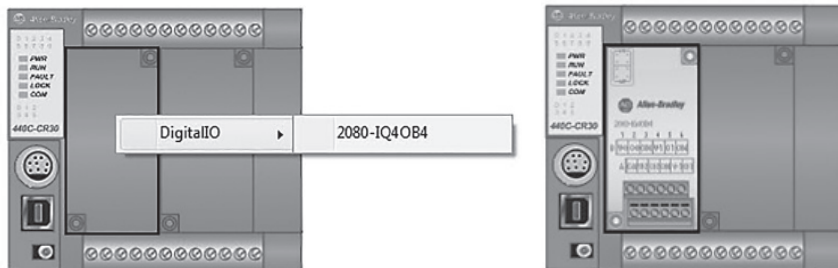


2. In the Project Organizer, double-click Guardmaster\_400C\_CR30 \*.



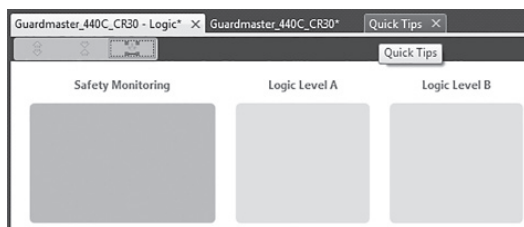
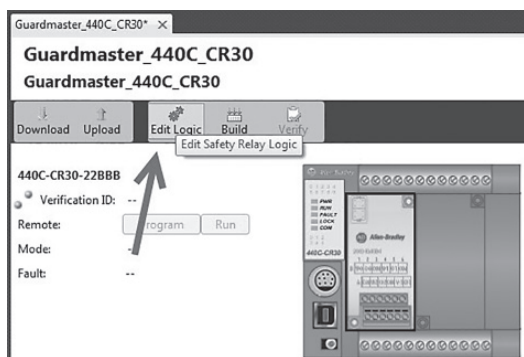


3. To add the plug-in I/O module called for in this circuit, right-click the left plug-in module space and choose the 2080-IQ4OB4 module.

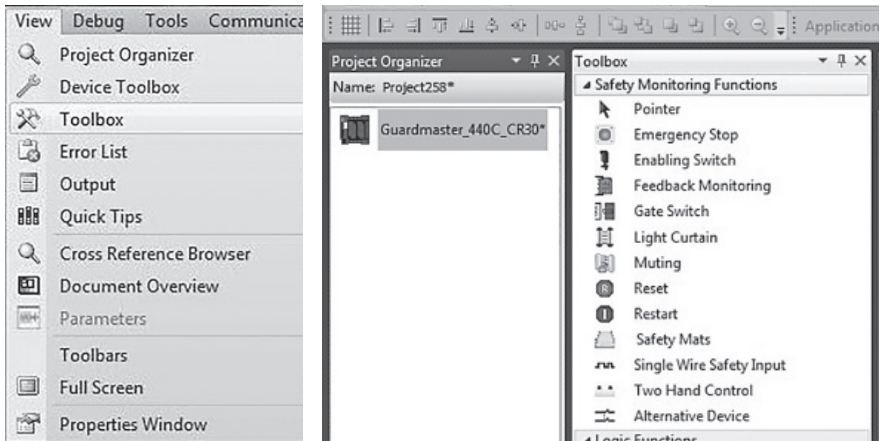


TIP: The I/O module is shown in standard gray, because it is not a safety I/O module. That is permissible in this application, because it is not used to connect safety signals. Inputs such as Feedback and Reset button are not considered strict, safety signals. Using the standard I/O for these non-safety signals can reserve the limited number of safety inputs and outputs for true safety signals.

4. Click the Edit Logic button to open the Connected Components Workbench workspace. A blank workspace appears.



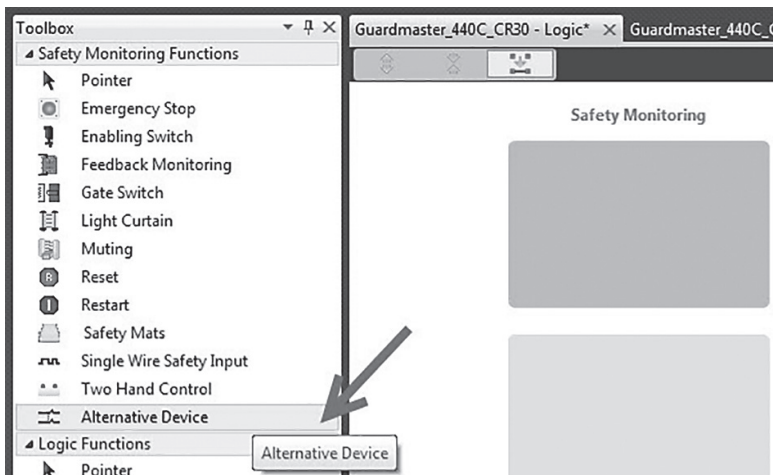
5. From the View pull-down menu, choose Toolbox. The Toolbox appears.



### Configure the Inputs

The Toolbox does not list a SensaGuard Safety Monitoring Function. Follow these steps to configure one.

1. Select Alternative Device. Drag it to the green block in the Safety Monitoring column and release it.

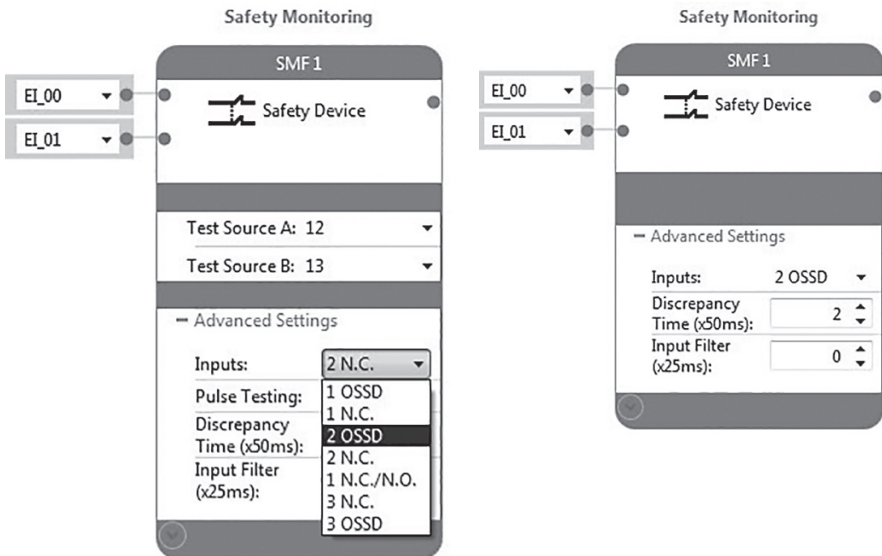




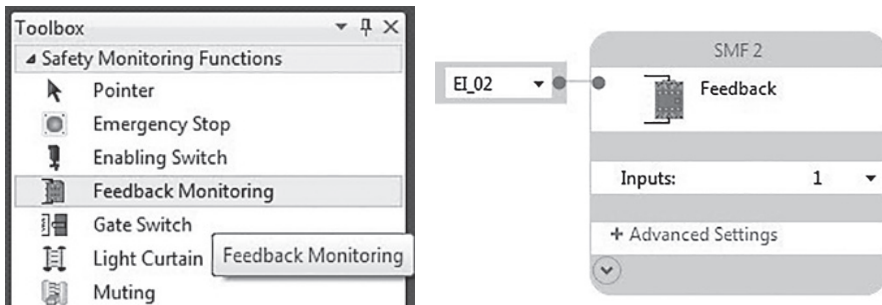
## Safety related control systems for machinery

Connected Components Workbench software automatically assigns the first two available inputs, EI\_00 and EI\_01, to the device. Leave those as assigned. Connected Components Workbench software automatically assigns the function name SMF 1 to this block. By default, the software assumes an electro-mechanical device and assigns Test Sources. The SensaGuard switch has two OSSD outputs and does not require Test Sources.

- To properly configure the block, open Advanced Settings and select 2 OSSD from the Inputs pull-down menu. The resulting block appears as shown.



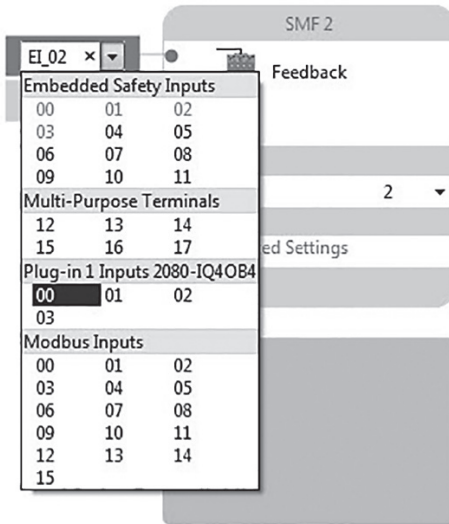
- Click, drag and release a Feedback Monitoring Safety Monitoring function to the Safety Monitoring block below the SensaGuard block in the workspace.



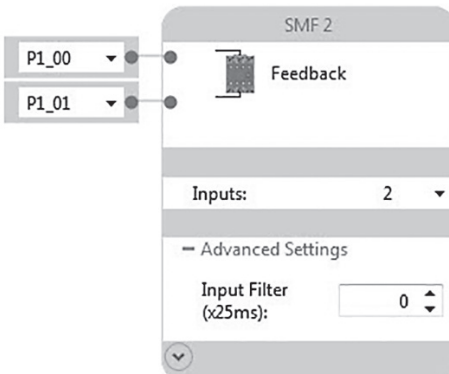
## Application Examples

Note that Connected Components Workbench software assigns this to input terminal EI\_02, the next available Safety Input terminal. The software assumes that this is a single input and automatically assigns the function name SMF 2 to this block.

- Because the circuit requires two inputs, one from each contactor, change the number of inputs to 2, one for the N.C. contact from each 100S contactor.



- Assign the inputs to Plug-In terminals PI\_00 and PI\_01. This avoids unnecessarily using Safety Inputs for feedback signals.





## Safety related control systems for machinery

- Click, drag and release a Reset safety monitoring function to the Safety Monitoring block below the Feedback Monitoring block in the workspace.

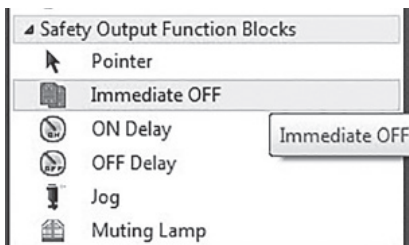


Connected Components Workbench software automatically assigns the function name SMF 3 to this block. Re-assign the Reset Input to Plug-In terminal PI\_02.

### Configure the Outputs

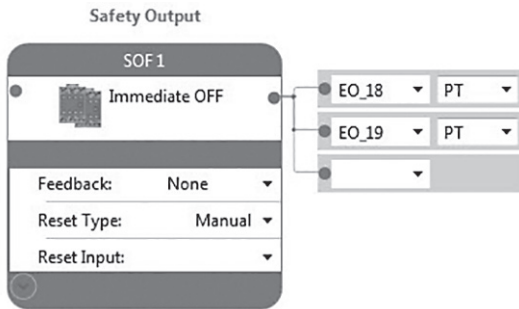
Follow these steps to configure the outputs.

- Click and drag Immediate OFF from the Safety Output Function Blocks section of the Toolbox.



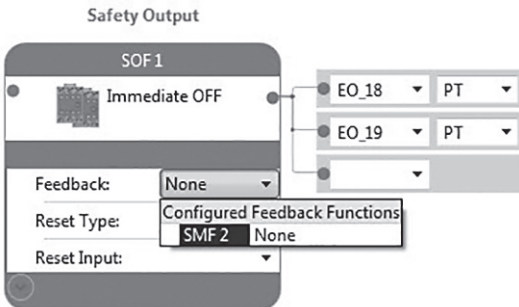
## Application Examples

- Release it on the top block of the Safety Output column in the workspace.

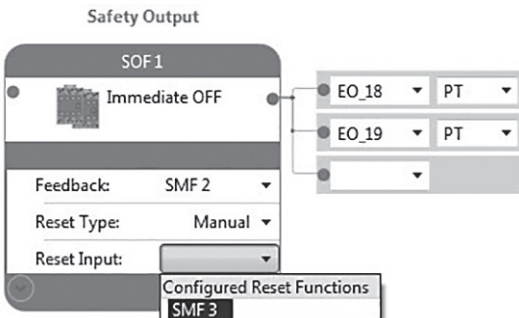


Connected Components Workbench software automatically assigns output terminals EO\_18 and EO\_19. Pulse Testing is the default for these terminals. The default Reset Type is Manual. Leave these settings at their defaults.

- Choose SMF 2 from the Feedback pull-down menu.



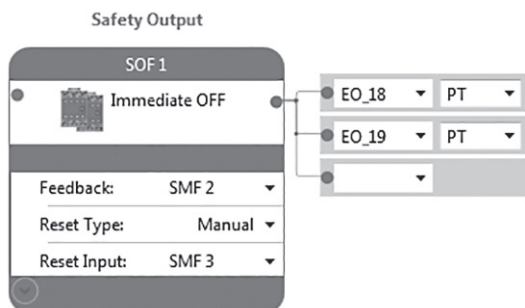
- Choose SMF 3 from the Reset Input pull-down menu.







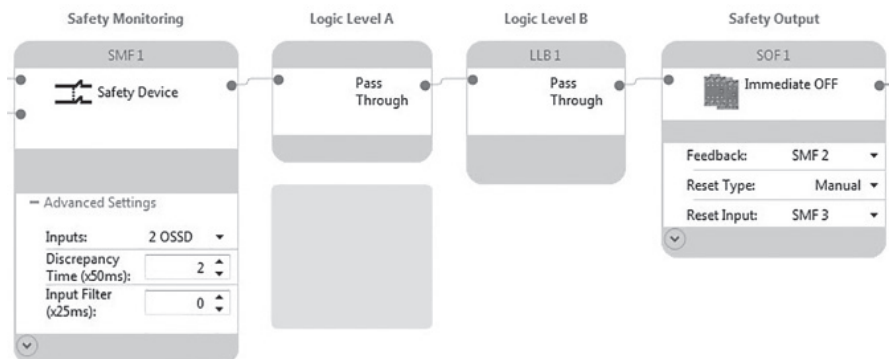
The safety output configuration is complete.



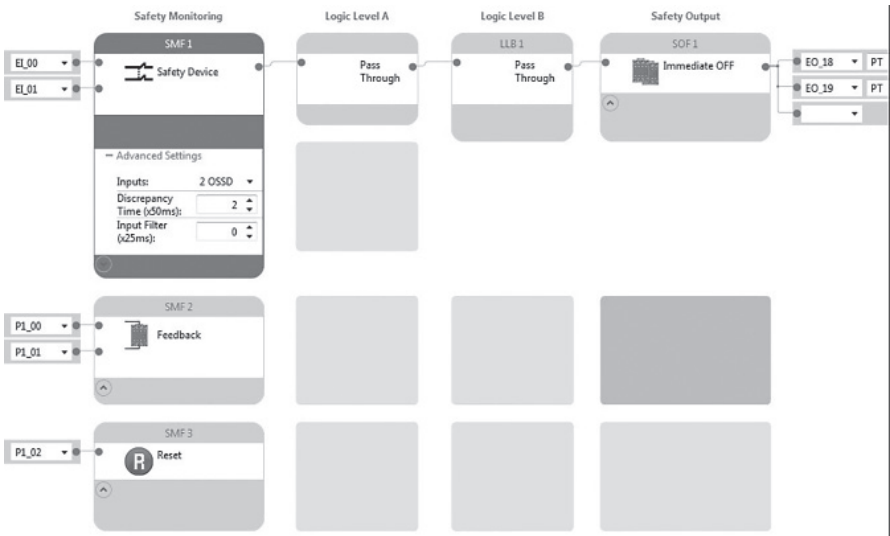
## Configure the Logic

The Logic section determines how the safety outputs respond to the safety monitoring inputs. In this case, the safety output follows the safety monitoring input directly.

1. Click the blue dot on the right side of the SensaGuard Safety Monitoring input block. It turns gray.
2. Click the blue dot on the left side of the Safety Output block to connect the logic.

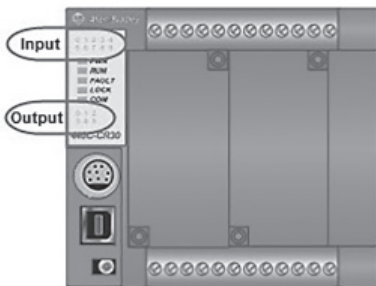


The completed logic looks like this.



### Configure the Status Indicators

The 440C-CR30 configurable safety relay provides ten user-configurable input status indicator LEDs and six user-configurable output status indicator LEDs. In many cases, they can be very helpful in installing, commissioning, monitoring and troubleshooting a 440C-CR30 configurable safety relay system. They do not affect the operation of the system in any way, and it is not necessary to configure them, but they are easy to configure and it is a recommended practice to use them.





1. Click Guardmaster\_440C\_CR30\*.



2. Select LED Configuration.

440C-CR30-22BBB

Verification ID: --

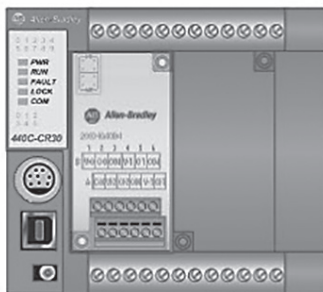
Remote:

Program

Run

Mode: --

Fault: --



LED	Type Filter	Value
0	Not Used	Not Used
1	Not Used	Not Used
2	Not Used	Not Used
3	Not Used	Not Used
4	Not Used	Not Used

3. For the Type Filter, choose Terminal Status for LED 0.

LED	Type Filter	Value
0	Terminal Status	Not Used
1	Safety Monitoring Function Status	Not Used
2	Safety Output Function Status	Not Used
3	Not Used	Not Used
4	Not Used	Not Used
5	Not Used	Not Used

## Application Examples

- For LED 0, choose Terminal 00 from the Value pull-down menu. The Status Indicator LED 0 is now configured to show the status of terminal 00.

LED	Type Filter	Value
0	Terminal Status	Terminal 00
1	Not Used	Terminal 00
2	Not Used	Terminal 01
3	Not Used	Terminal 02
4	Not Used	Terminal 03
5	Not Used	Terminal 04

- Assign the next four Input LEDs (1...4) in the same manner. The input status indicator LEDs are now configured.

LED	Type Filter	Value
0	Terminal Status	Terminal 00
1	Terminal Status	Terminal 01
2	Safety Monitoring Function Status	SMF 1
3	Safety Monitoring Function Status	SMF 2
4	Safety Monitoring Function Status	SMF 3
5	Not Used	Not Used

SensaGuard OSSD 1 Status  
SensaGuard OSSD 2 Status  
SensaGuard Status  
Feedback Status  
Reset Status

- Assign the three output LEDs as follows.

LED	Type Filter	Value
0	Terminal Status	Terminal 18
1	Terminal Status	Terminal 19
2	Safety Output Function Status	SOF 1
3	Not Used	Not Used
4	Not Used	Not Used

Output Channel 1 Status  
Output Channel 2 Status  
Safety Output Status

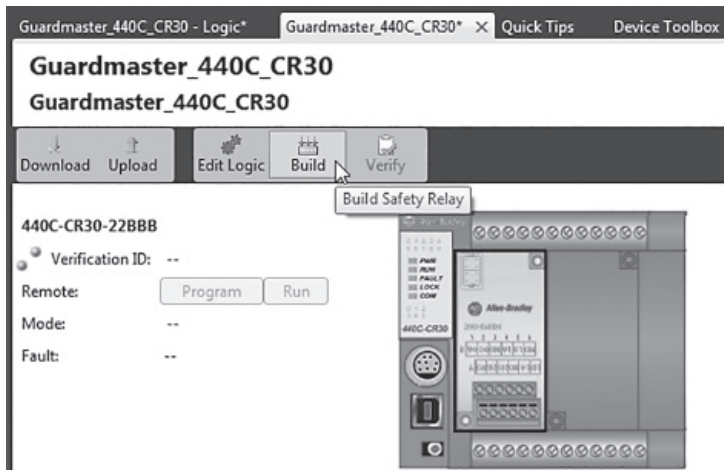
### Confirm the Validity of the Build

Follow these steps to confirm the validity of the logic by using the Build feature in Connected Components Workbench software.

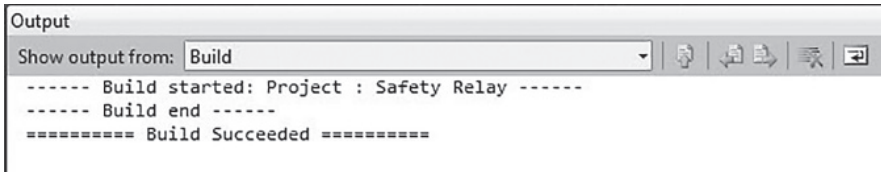
- Click Guardmaster\_440C\_CR30 in the bar above the workspace.



2. Click Build.



A Build Succeeded message confirms that the configuration is valid.



If an error or omission is discovered during a build, a message is displayed which details the error so that it may be corrected. After you correct the error, you need to perform the build again.

### Save and Download the Project

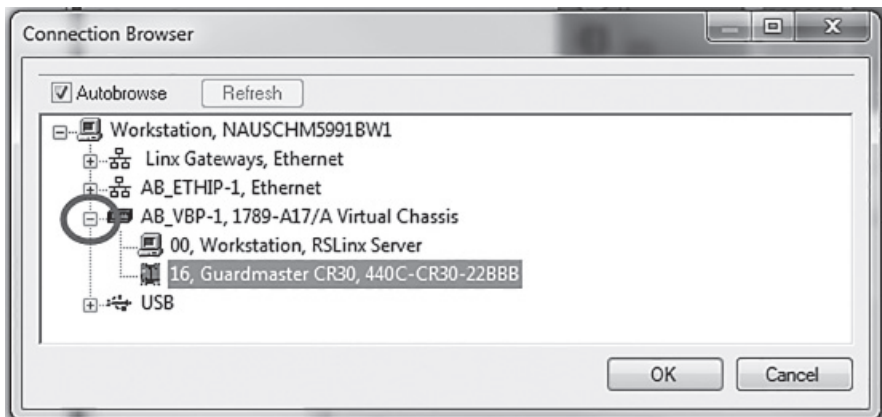
Follow these steps to save and download the project.

1. From the File menu, choose Save as to save the project.
2. In the Project Organizer window, double click Guardmaster\_440C\_CR30 to open the workspace.
3. Power up the 440C-CR30 safety relay.
4. Connect the USB cable to the 440C-CR30 relay.

5. Click Download.

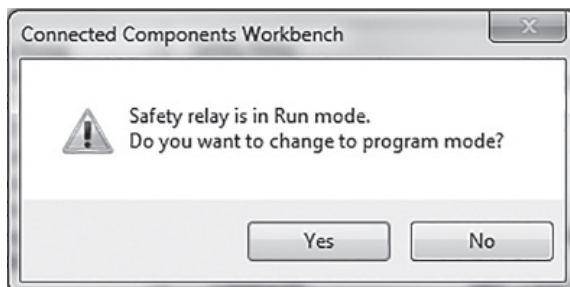


6. In the Connection Browser, expand the AB\_VBP-1 Virtual Chassis and select the Guardmaster 440C-CR30-22BBB. Click OK.

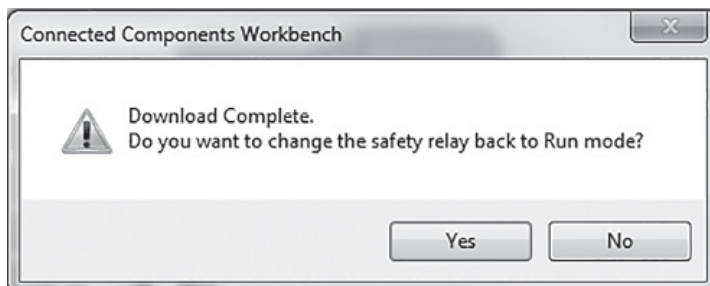




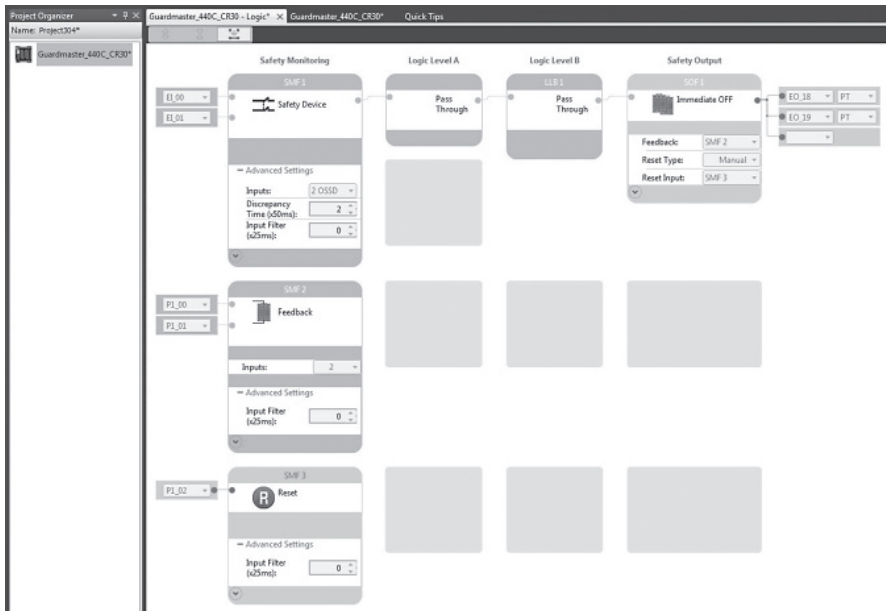
7. Click Yes to change from Run to Program mode.



8. When the download is complete, click Yes to change from Program to Run mode.



9. Click Edit Logic to see the online diagnostics.



Green indicates that a block is True or that an input or output terminal is ON. Flashing green indicates that a Safety Output Function is ready to be Reset. The online diagnostics mode of the 440C-CR30 relay can be very helpful during the verification process.

10. Review the information in Calculation of the Performance Level and Verification and Validation Plan before proceeding with Verification of the Configuration

### Calculation of the Performance Level

When properly implemented, this safety-related stop function can achieve a safety rating of Category 4, Performance Level e (CAT. 4, PL<sub>e</sub>), according to ISO 13849-1: 2008, as calculated by using the SISTEMA software PL calculation tool. The minimum Performance Level required (PL<sub>r</sub>) from the risk assessment for this safety function is PL<sub>d</sub>.





**Project** IFA

Documentation Safety functions

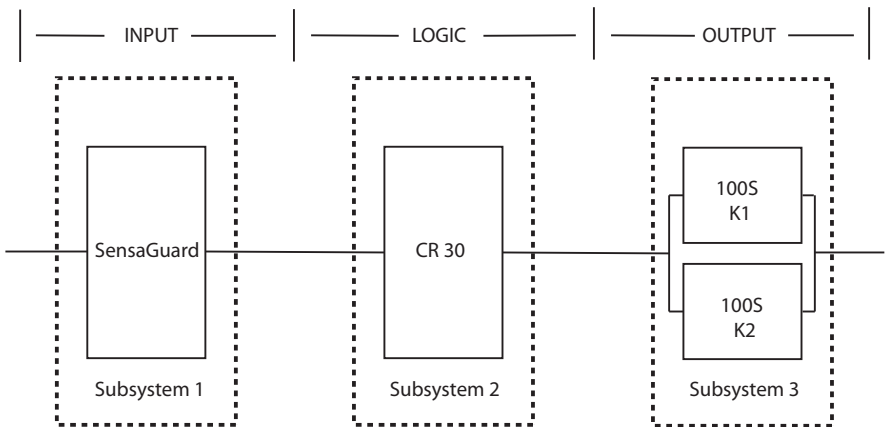
Status	Type	Name	Type	PLr	PL
▼	SF	SensaGuard	Safety-related stop function initiated by safeguard	d	e

**Safety function** IFA

Documentation PLr PL Subsystems

Status	Type	Name	PL	PFH [1/h]	CCF score	DCavg [%]	MTTFd [a]	Category	Requirements of the category
▼	SB	Interlock Switch: SensaGuard	e	1.12E-9	not relevant	not relevant	not relevant	4	fulfilled
▼	SB	CR 30	e	SE-B	not relevant	not relevant	not relevant	4	fulfilled
▼	SB	100S Contactors	e	2.47E-8	65 (fulfilled)	99 (High)	100 (High)	4	fulfilled

This safety-related stop initiated by a safeguard safety function can be modelled as follows:



Because these are electro-mechanical devices, the safety contactors data includes the following :

- Mean Time to Failure, dangerous (MTTF<sub>D</sub>)
- Diagnostic Coverage (DCavg )
- Common Cause Failure (CCF)

Electro-mechanical devices' functional safety evaluations include the following:

- How frequently they are operated
- Whether they are effectively monitored for faults
- Whether they are properly specified and installed

SISTEMA calculates the MTTFd by using B10d data provided for the contactors, along with the estimated frequency of use, entered during the creation of the SISTEMA project.

The DCavg (99%) for the contactors is selected from the Output Device table of ISO 13849-1 Annex E, Direct Monitoring.

The CCF value is generated by using the scoring process outlined in Annex F of ISO 13849-1. The complete CCF scoring process must be performed when actually implementing an application. A minimum score of 65 must be achieved.

### Verification and Validation Plan

Verification and validation play important roles in the avoidance of faults throughout the safety system design and development process. ISO 13849-2 sets the requirements for verification and validation. The standard calls for a documented plan to confirm that all of the safety functional requirements have been met.

Verification is an analysis of the resulting safety control system. The Performance Level (PL) of the safety control system is calculated to confirm that the system meets the required Performance Level (PLr) specified. The SISTEMA software is typically used to perform the calculations and assist with satisfying the requirements of ISO 13849-1.

Validation is a functional test of the safety control system to demonstrate that the system meets the specified requirements of the safety function. The safety control system is tested to confirm that all of the safety-related outputs respond appropriately to their corresponding safety-related inputs. The functional test includes normal operating conditions in addition to potential fault injection of failure modes. A checklist is typically used to document the validation of the safety control system.

Prior to validating the system, confirm that the Guardmaster 440C-CR30 configurable safety relay has been wired and configured in accordance with the installation instructions.



## Verification and Validation Checklist

General Machinery Information	
Description	
Machine Name/Model Number	
Machine Serial Number	
Customer Name	
Test Date	
Tester Names	
Schematic Drawing Number	
Input Devices	440N-Z21S16B
Configurable Safety Relay	440C-CR30-22BBB
Variable Frequency Drive	
Safety Contactor	100S-C23EJ23BC

Safety Wiring and Relay Configuration			
Test Step	Verification	Pass/Fail	Changes/Modifications
1	Confirm that all components' specifications are suitable for the application. Refer to Basic Safety Principles and Well-tried Safety Principles from ISO 13849-2.		
2	Visually inspect the safety relay circuit to confirm that it is wired as documented in the schematics.		
3	Confirm that the configuration in the 440C-CR30 configurable safety relay is the correct, intended configuration.		

Normal Operation Verification - The safety system properly responds to all normal Start, Stop, Reset, Emergency Stop and SensaGuard switch inputs.			
Test Step	Verification	Pass/Fail	Changes/Modifications
1	Confirm that no one is in the guarded area.		
2	Confirm that the hazardous motion is stopped.		
3	Confirm that the door is closed.		
4	Apply power to the safety system.		
5	Confirm that the Terminal 00, Terminal 01, and SMF1 input status indicator LEDs of the 440C-CR30 safety relay are green. Confirm that all output status indicators are OFF. Confirm that the Power and Run status indicator LEDs are green. Monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
6	Press and release the Reset button on the 440C-CR30 safety relay. Confirm that the Terminal 18, Terminal 19, and SOF1 output status indicator LEDs are green. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		

# Application Examples

7	Confirm that the hazardous motion does not start on powerup.		
8	Press and release the drive Start button. Confirm that the hazardous motion begins and that the machine begins to operate.		
9	Press the external Stop button. The machine must stop in its normal, configured manner. The safety system must not respond.		
10	Press and release the external Start button. Confirm that the hazardous motion starts and the machine begins to operate.		
11	Open the guarded door. The safety system must trip. The hazardous motion must stop within less than 0.7 seconds. Monitor the status indicator LEDs for proper operation and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
12	Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 configurable safety relay must not respond. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software		
13	Close the guarded door. The machine must not start. The 440C-CR30 safety relay must not respond. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
14	Press and release the Reset button on the 440C-CR30 safety relay. The SOF 1 of the 440C-CR30 safety relay must energize. The hazardous motion must not start. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
15	Press and release the external Start button. Confirm that the motor starts and that the machine begins to operate.		

**Validation of Safe Response to Abnormal Operation - The safety system responds properly to all foreseeable faults with corresponding diagnostics.**

**SensaGuard and 440C-CR30 Configurable Safety Relay Tests**

Test Step	Verification	Pass/Fail	Changes/ Modifications
1	Keep the guarded door closed. While the hazardous motion continues to run, remove the SensaGuard OSSD1 wire to terminal E1_00 of the 440C-CR30 safety relay. The 440C-CR30 safety relay must trip immediately. The red Fault status indicator LED on the relay must blink. Monitor all status indicator LEDs for proper operation and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
2	Reconnect the wire to E1_00. The 440C-CR30 safety relay must not respond. Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 safety relay must not respond. Monitor all status indicator LEDs for proper operation and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
3	Open and close the guarded door. The red Fault status LED must be OFF. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		



## Safety related control systems for machinery

4	Press and release the Reset button on the 440C-CR30 safety relay. The SOF 1 output on the 440C-CR30 relay must energize. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
5	Press the external Start button. The machine must start to run. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software. This step is optional in the following SensaGuard validation tests (Steps 6 through 27).		
6	With the guarded door closed, connect OSSD 1 to 24V DC. After approximately 40 seconds, the SensaGuard switch trips. The 440C-CR30 safety relay trips. The red Fault status indicator LED on the 440C-CR30 safety relay must blink. The status indicator on the SensaGuard switch flashes red. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
7	Disconnect OSSD 1 from 24V DC. Neither the SensaGuard switch nor the 440C-CR30 safety relay respond. Press and release the Restart button on the 440C-CR30 safety relay. Neither the SensaGuard switch nor the 440C-CR30 safety relay respond. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
8	Cycle power to the SensaGuard switch. Approximately five seconds after power is restored to the SensaGuard switch, its status LED turns steady green. The blinking red Fault status indicator LED on the 440C-CR30 safety relay turns OFF. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
9	Press and release the Reset button on the 440C-CR30 safety relay. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
10	Connect OSSD 1 to DC COM. The 440C-CR30 safety relay trips immediately. The red Safe Stop stack light turns ON. The amber Gate 1 stack light turns ON. The red Fault status indicator LED on the 440C-CR30 safety relay must blink. The status indicator on the SensaGuard switch flashes red.		
11	Disconnect OSSD1 from DC COM. Neither the SensaGuard switch nor the 440C-CR30 safety relay respond. Press and release the Restart button on the 440C-CR30 safety relay. Neither the SensaGuard switch nor the 440C-CR30 safety relay respond.		
12	Cycle power to the SensaGuard switch. Approximately five seconds after power is restored to the SensaGuard switch, its status indicator LED lights steady green. The amber Gate 1 stack light turns OFF. The red Safe Off stack light remains ON. The blinking red Fault status indicator LED on the 440C-CR30 safety relay turns OFF.		
13	Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 safety relay's SOF 1 must energize the contactors. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
14 to 27	Repeat steps 1 through 13 using EI_01 in place of EI_00, and OSSD 2 in place of OSSD 1.		

## Application Examples

28	Connect OSSD 1 to OSSD 2 (terminal EI_00 to terminal EI_01). After approximately 50 seconds, the SensaGuard switch trips. The 440C-CR30 safety relay trips. The status indicator on the SensaGuard switch flashes red. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
29	Disconnect OSSD 1 from OSSD 2. Neither the SensaGuard switch nor the 440C-CR30 safety relay respond. Press and release the Restart button on the 440C-CR30 safety relay. Neither the SensaGuard switch nor the 440C-CR30 safety relay respond.		
30	Cycle power to the SensaGuard switch. Approximately five seconds after power is restored to the SensaGuard switch, its status LED turns steady green. The blinking red Fault status indicator LED on the 440C-CR30 safety relay turns OFF. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		
31	Press and release the Reset button on the 440C-CR30 safety relay. The red Safe Stop stack light must be OFF. The SOF1 output on the 440C-CR30 safety relay must energize the contactors. Monitor all status indicator LEDs for proper operation, and monitor the 440C-CR30 safety relay for proper status by using Connected Components Workbench software.		

**Validation of Safe Response to Abnormal Operation – The safety system responds properly to all foreseeable faults with corresponding diagnostics.**

**Contactors – 440C-CR30 Configurable Safety Relay Tests**

Test Step	Verification	Pass/Fail	Changes/Modifications
1	While the machine continues to run, break the connection between terminal EO_18 of the 440C-CR30 configurable safety relay and the A1 terminal of the K1 coil. The hazardous motion must coast to a stop.		
2	Press the external Stop button. Restore the connection. Press the external Start button to resume the hazardous motion.		
3	While the hazardous motion continues to run, connect the A1 terminal of the K1 coil to 24V DC. After approximately 18 seconds, the 440C-CR30 safety relay must trip. K2 must de-energize. The hazardous motion coasts to a stop. The red Fault status indicator LED on the 440C-CR30 safety relay is ON.		
4	Disconnect the A1 terminal of the K1 coil from 24V DC. Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 safety relay must not respond.		
5	Cycle power to the 440C-CR30 safety relay. It responds. The 440C-CR30 safety relay Fault status indicator LED is OFF.		
6	Press and release the Reset button on the 440C-CR30 safety relay. Press the external Start button. The hazardous motion must resume.		
7	While the machine continues to run, short the A1 terminal of the K1 coil to DC COM. The 440C-CR30 safety relay must trip. The red Fault status indicator LED on the 440C-CR30 safety relay is ON.		



## Safety related control systems for machinery

8	Disconnect the A1 terminal of the K1 coil from DC COM. Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 safety relay must not respond.		
9	Cycle power to the 440C-CR30 safety relay. The 440C-CR30 safety relay responds. The Fault status indicator LED on the 440C-CR30 safety relay is OFF.		
10	Press and release the Reset button on the 440C-CR30 safety relay. Press the external Start button. The hazardous motion resumes.		
11 to 21	Repeat steps 1 to 10 using EO_19 in place of EO_18, and K2 in place of K1.		
22	Connect the A1 terminal of K1 to the A1 terminal of K2. After approximately 18 seconds, the 440C-CR30 safety relay must trip. The hazardous motion coasts to a stop. The red Fault status indicator LED on the 440C-CR30 safety relay is ON.		
23	Disconnect the A1 terminal of K1 from the A1 terminal of K2. Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 safety relay must not respond.		
24	Cycle power to the 440C-CR30 safety relay. It responds. The Fault status indicator LED on the 440C-CR30 safety relay is OFF.		
25	Press and release the Reset button on the 440C-CR30 safety relay. Press the external Start button. The hazardous motion must resume.		

**Validation of Safe Response to Abnormal Operation – The safety system responds properly to all foreseeable faults with corresponding diagnostics.**

**Contactors Feedback – 440C-CR30 Configurable Safety Relay Tests**

Test Step	Verification	Pass/Fail	Changes/ Modifications
1	While the machine continues to run, remove the K1 feedback connection at terminal P1_00. The machine must continue to run.		
2	Open the guarded door. The safety system must trip. The hazardous motion must stop within less than 0.7 seconds. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 relay for proper status by using the Connected Components Workbench software.		
3	Close the guarded door. The machine must not start. The 440C-CR30 relay must not respond. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 relay for proper status by using the Connected Components Workbench software.		
4	Press and release the Reset button on the 440C-CR30 safety relay. The 440C-CR30 relay must not respond. Monitor the status indicator LEDs for proper operation, and monitor the 440C-CR30 relay for proper status by using Connected Components Workbench software.		
5	Replace the connection at P1_00. Cycle power to the 440C-CR30 relay. Press the Reset button on the 440C-CR30 relay. The 440C-CR30 relay outputs must energize. Press and release the external Start button. Confirm that the motor starts and that the machine begins to operate.		
6	Repeat steps 1 through 5 using the K2 feedback connection at terminal P1_01.		

## Verification of the Configuration

The system must verify the configuration of each individual application by using the Verify command. If the 440C-CR30 configuration safety relay is not verified, it will fault after 24 hours of operation.

**ATTENTION:** The verification process should be documented in the safety system's technical file.

Follow these steps to download and verify the configuration.

1. Make sure the 440C-CR30 relay is powered up and connected to your workstation via the USB cable.
2. Confirm that the upper right-hand corner of the Connected Components Workbench Project tab shows that the 440C-CR30 relay is connected. If it is not, click Connect to Device to establish the software connection.



3. Click Verify.







4. Answer all the questions and check each box, if completed. Click Generate.

Connected Components Workbench


- Have you followed installation instructions and precautions to conform to applicable safety standards?
- Have you verified that the electrical specifications of the sensor and inputs are compatible?
- Have you verified that the electrical specifications of the outputs and the actuators are compatible?
- Have you calculated the system's safety response time for each safety chain?
- Is the system response time in proper relation to the process tolerance time?
- Have probability (PFD/PFH/PLx) values been calculated according to the system's configuration?
- Have you performed all appropriate functional verification tests on the system?

Safety Verification ID:

**IMPORTANT:** All of the boxes must be marked in order to Generate the Verification ID.

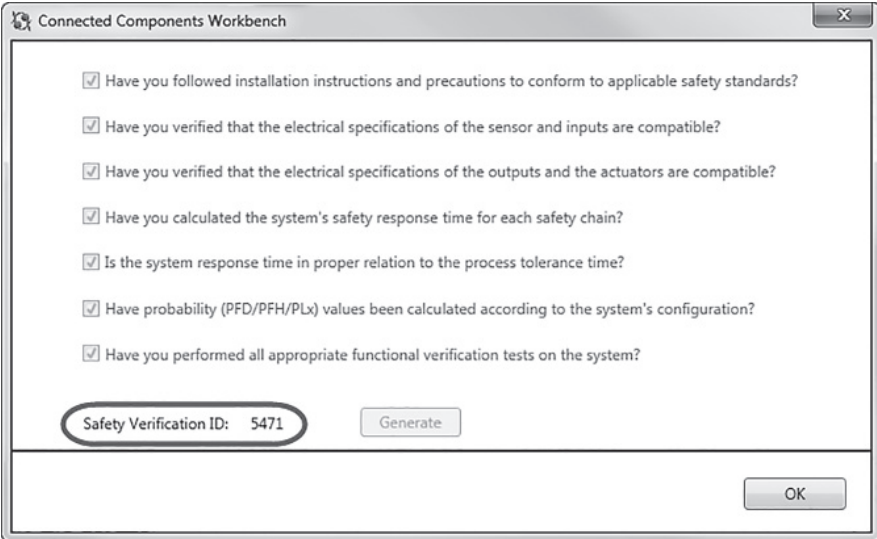
6. Click Yes to proceed with the verification.

Connected Components Workbench

 Performing a Safety Verify will change the safety relay to Program mode.  
Proceed with the Safety Verify?

7. Click Yes to change to Run mode.

8. Record the Safety Verification ID in the machine's documentation.



The screenshot shows a dialog box titled "Connected Components Workbench". It contains a list of seven safety verification questions, each with a checked checkbox:

- Have you followed installation instructions and precautions to conform to applicable safety standards?
- Have you verified that the electrical specifications of the sensor and inputs are compatible?
- Have you verified that the electrical specifications of the outputs and the actuators are compatible?
- Have you calculated the system's safety response time for each safety chain?
- Is the system response time in proper relation to the process tolerance time?
- Have probability (PFD/PFH/PLx) values been calculated according to the system's configuration?
- Have you performed all appropriate functional verification tests on the system?

Below the list, there is a "Generate" button and a field displaying "Safety Verification ID: 5471". The field is circled in red. At the bottom right, there is an "OK" button.

This process is the feedback to the 440C-CR30 relay that the system verification and functional tests have been completed. The unique verification ID can be used to check if changes have been made to a configuration file. Any change to the configuration removes the Safety Verification ID. Subsequent Verify actions generate a different verification ID. The Safety Verification ID is displayed in Connected Components Workbench software only when you are connected to the 440C-CR30 relay.



## Chapter 11: Products, Tools and Services

### Overview

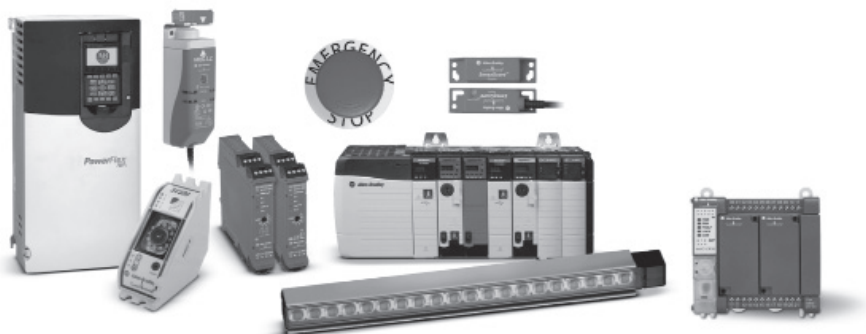
Rockwell Automation is a leading global provider of industrial power, control and information solutions, and has been supporting its customers across multiple industries, for well over 100 years. Part of its industrial automation portfolio is comprehensive machinery safety technologies, tools and services.

### Products and technologies for your applications

Rockwell Automation has the broadest portfolio of any machinery safety solutions supplier, and can provide all three parts of a safety system (input device, logic control and final power element).



### Products and technologies available include:-



## Safety input devices

- **Presence-sensing safety devices**

Presence Sensing Safety Devices detect the location of objects or personnel near hazardous areas. These include: safety light curtains, safety laser scanners, hand detection safety sensors, pressure sensitive mats and edges

- **Safety interlock switches**

Safety Switches are designed and built to global standards for high reliability, stability, and quality. Safety switches include limit and interlock switches and emergency stop switches.

- **Emergency stop & trip devices**

Emergency Stop Switches include a range of mushroom push-button devices with positively guided contacts. Enabling switches and cable pull switches offer the emergency function across an application or are tethered to allow the operator movement within the safety application.

- **Operator interface**

Operator interface devices allow the operator to interact with the application and offer additional dedicated safety functionality.

## Safety logic controllers

- **Safety relays (Single function or Configurable)**

Safety Relays check and monitor a safety system and either allow the machine to start or execute commands to stop the machine. Single-function safety relays are the most economical solution 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.

- **Integrated safety controllers**

Safety PLCs bring the benefits of traditional PLC systems to safety applications, replacing hard-wired relay systems that are normally required to bring automated processes to a safe state. Safety PLCs allow standard and safety-related programs to reside in a single controller chassis, providing flexibility in programming as well as a familiar and easy-to-use environment for programmers. Safety controller solutions provide open and integrated control that will help to ensure machine safety and protection of your assets.



## Safety related control systems for machinery

- **Safety I/O devices**

The Guard I/O™ Safety products provide all the advantages of traditional distributed I/O but are designed for safety systems. They reduce wiring costs and startup time for machines and cells and are available with a variety of features for both in-cabinet and on-machine applications.

### Safety actuators

- **Safety contactors and Starters**

ArmorStart® distributed motor controllers achieves Category 4 safety functionality while providing a safety solution integrated into your DeviceNet™ On-Machine™ safety installation. The IEC safety contactors and control relays help protect personnel from unintended machine starts and loss of the safety function.

- **PowerFlex® AC drives**

PowerFlex drives are available with safety features. The PowerFlex 525 AC drives include embedded Safe Torque-Off as a standard feature. Safe Torque-Off is an optional feature for the PowerFlex 40P, 70, 700H, 700S, and 750-Series AC drives, which also support Safe Speed Monitor functionality.

- **Kinetix® integrated motion**

Kinetix 300, 6000, 6200, 6500 and 7000 servo drives all feature built-in safety functionality. With Safe Torque-Off, a drive output is disabled to remove motor torque without removing power from the entire machine. Safe Speed Monitoring permits users to reduce and monitor the speed of the application to help an operator safely perform some types of work without completely stopping the machine.

### Connection systems/networks

- **‘Quick connect’ connection systems**

Guardmaster® Safety t-ports/splitters, distribution boxes, and shorting plugs are parts of a quick-disconnect system that is dedicated to machine safety.

- **GuardLink™**

GuardLink is a safety-based communications protocol utilising standard cabling in a ‘trunk and drop’ topology with ‘plug and play’ connections. It enables communication of safety devices for diagnostics and control such as remote reset and lock commands over a single cable. As many as 32 devices can be connected on a cable span of up to 1,000 metres. Allen-Bradley safety devices featuring GuardLink technology give you access to safety system information and enables this information to be accessed over EtherNet/IP. GuardLink can help simplify system configuration, reduce wiring and increase diagnostic information for maintenance and operation.

- **Safety over EtherNet/IP**

The EtherNet/IP™ network provides plant-wide network systems using open, industry-standard networking technologies. It offers real-time control and information in discrete, continuous process, batch, safety, drive, motion, and high availability applications. EtherNet/IP networks connect devices such as motor starters and sensors to controllers and HMI devices and on into the wider enterprise. It supports non-industrial and industrial communications on a single, common network infrastructure.

## Tools to help you

A wide range of tools that support compliance with safety standards, reduce the risk of injuries and improve productivity.

### **Safety Automation Builder**

Safety Automation Builder is a FREE software tool to help simplify machine safety design and validation, reducing time and costs. Integration with RASWin Risk Assessment Software provides users with consistent, reliable, documented management of the Functional Safety Lifecycle. Safety Automation Builder streamlines safety system design, helping improve compliance and reduce costs by guiding users through the development of safety systems including safety system layout, product selection, and safety analysis to help meet machinery safety Performance Level (PL) requirements as outlined by global standard (EN) ISO 13849-1.

### **RASWin**

RASWin software helps users manage the progression through the functional safety lifecycle, organizing information from each step of the process and machinery validation. RASWin links the steps of the safety lifecycle to avoid systematic failures, including safety function specifications, Performance Level requirements (PLr) assignment and PLr calculation, safety circuit validation, and documentation.

### **SISTEMA Performance Level Calculator**

The SISTEMA tool, developed by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), automates calculation of the attained Performance Level from the safety-related parts of a machine's control system to (EN) ISO 13849-1. Data for Rockwell Automation machinery safety products is available in the form of a library that can be used with the SISTEMA calculation tool. The combination of the two gives machinery and system designers comprehensive time-saving support in evaluating safety to (EN) ISO 13849-1. An export function from Safety Automation Builder allows the safety system design to be easily imported into SISTEMA in order to receive a third party verification of the required Performance Level.



### **Pre-engineered Safety Functions for machines**

Machinery safety functions require multiple elements including a sensor or input device, a logic device, and an output device. Together, these elements provide a level of protection calculated by performance level as outlined in (EN) ISO 13849-1 Rockwell Automation has developed many safety function documents, each providing guidance for a specific safety function based on functional requirement, equipment selection, and performance level requirement. They including set-up and wiring, configuration, verification and validation plan, and calculation of performance level.

### **Safety maturity Index tool**

The Safety Maturity Index™ is a comprehensive measurement of performance in safety culture, compliance processes and procedures, and capital investments in safety technologies. It helps companies understand their current level of performance and steps they can take to improve safety and profitability.

### **Services and experience to support you**

As the world's largest industrial safety provider, Rockwell Automation can help to reduce injuries and costs while improving productivity at every phase of the Safety Life Cycle.

Safety services are delivered by experienced staff who are safety qualified; many with TÜV Rheinland Machinery Safety certifications. Rockwell Automation employs people who are TÜV Functional Safety Experts, Engineers and Technicians to help customers with their holistic safety lifecycle.

The Safety Life Cycle is a clearly-defined process that helps to maximize productivity and improve safety by identifying the steps required to assess and mitigate machinery risks. The Safety Life Cycle can be seen and downloaded in this document.

Some of the services available are:

- **Safety Assessments**  
Services that help to evaluate plant risk and support well-informed decisions that help to improve employee and machine safety.
- **Design Services**  
Comprehensive circuit design, correct application of devices and design reviews to help improve overall safety.
- **Installation and Validation Services**  
Verification that systems are operating within defined parameters and standards.

- **Safety Training**  
Comprehensive training programmes delivered by industry-leading experts.
- **Customized Services**  
Covering client-specific applications, technologies, applications, platforms, and configurations.

### **Why choose Rockwell Automation**

Integrating safety with automation can offer productivity enhancing benefits in many stages of the manufacturing process, from equipment design and testing, installation and commissioning, through operation and maintenance and on to modification or decommissioning. All stages can be optimised through correctly applied safety solutions.

As the world leader in industrial automation and safety and as a technology innovator, Rockwell Automation is ideally placed to support your development of more efficient, safer and more productive manufacturing solutions.

With many years of automation and safety experience, application knowledge and applying leading edge guiding principles from safety standards such as ISO 12000, (EN) ISO 13849-1 and IEC 62061, Rockwell Automation can assist you with the selection, integration, training and support of machinery safety, process safety and electrical safety solutions.





**[www.rockwellautomation.com](http://www.rockwellautomation.com)**

---

**Power, Control and Information Solutions Headquarters**

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication: SAFE BK-RM002C-EN-P - November 2016  
Supersedes Publication: SAFE BK-RM002B-EN-P

© 2016 Rockwell Automation, Inc. All Rights Reserved.