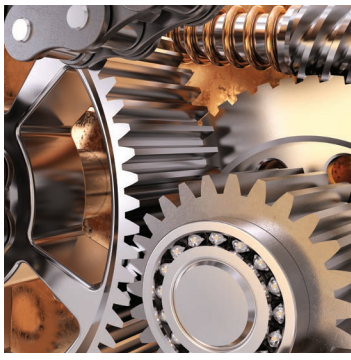
A Comprehensive Guide to Machine Safety

VAL-SIF-148



Parker

ENGINEERING YOUR SUCCESS.

A Comprehensive Guide to Machine Safety

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Introduction

Parker Hannifin takes great pride in safety; both in the workplace and on the machine. This “Comprehensive Guide to Machine Safety” is designed to help implement safe standards under current regulations.

Industry 4.0 has brought a rapid evolution of machine technology and enhancements for smart devices and data management. As a result, engineers face increasing pressure to implement the safest and newest technologies to ensure the safety of people and machinery.

Our goal is to guide the engineer on how to best eliminate accidents with the latest technology and safe machinery design principles.

We care at Parker because one accident is one to many.

Machine – 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.

Disclaimer:

This document gives only an overview of the process for meeting the essential requirements of the Machinery Directive. The manufacturer of the machinery always remains ultimately responsible for the safety and compliance of the product.

Why Parker?

Parker has over 100 years of expertise in the field of industrial automation while designing pneumatics with some of the industry’s best engineer’s on staff worldwide. As specialists in the area of development for factory automation, Parker consistently brings the newest technologies to market.

Rapid advances in machine technology in the area of factory automation has created an increased emphasis on smarter controls and a greater integration of smart devices and safety componentry. Advanced pneumatic components have now become an integral part of safety controls for implementing preventative technical measures required to make machinery safe including clamping, blocking, exhausting and holding equipment in place.

Parker offers the global expertise to solve your greatest challenges and the corporation has invested heavily in safety rated components designed to meet the most dangerous applications and performance levels. We offer the people, knowledge, breadth of line and compassion for ensuring that optimum safety is achieved for your people and machine.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

About the Machinery Directive

The goal of the Machinery Directive is to protect people, animals, property and the environment from accidents caused from all types of machinery. Overall, the Machinery Directive (MD) harmonizes the requirements for the European Union (EU) and European Norms (EN) also known as standards, and is the vehicle used to show compliance with these harmonized requirements.

Based on the Machinery Directive, the standards EN 13849-1 (Safety of Machinery) and EN 13849-2 (Validation) build the procedure to assess the safety of machinery and safety-related parts of control systems (SRP/CS). The new standards of 2006/42/EC replace the standards previously used under 98/37/EC which now better define several areas including safety components, partly completed machinery and other specific machinery topics.

The Machinery Directive originated in 1985 with the first standards published in 1989. The standards have evolved over the years to harmonize the European Union and became applicable law(s) for safe machine design throughout Europe. In 2008, the Machinery Directive became law, and has undergone several revisions to harmonize with other safety legislation including the likes of OSHA and ANSI in North America to name a few.

While the Machinery Directive is European, it raises the standard globally for machine builders and integrators by offering the most comprehensive set of guidelines to ensure safety and conformity.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

What is a Safety Component?

The Machinery Directive clearly distinguishes safety devices from standard pneumatic components used in a safety circuit. The term safety component does not imply the reliability or safety level of the component. Those products offered as safety rated must undergo stringent requirements for certification, testing and approval to be compliant as safety rated componentry.

The Machinery Directive also does not prescribe the use of safety rated componentry. It only describes the conformity assessment procedures to market a product as safety rated. These conformity procedures include:

- A guarantee that the product will perform a safety function
- The product be marketed separately as a safety product
- The product will bear the CE mark

And as such;

- A safety component is evaluated by its manufacturer for its safety function.

  (Examples of safety components include but are not limited to a light curtain, safety door switch, safety exhaust valve, emergency stop device or other safety integral specific component).
- A safety related part of a control system (SRP/CS) is developed by the manufacturer of a machine and its evaluation for safe function is part of the machinery design. This can be a standard fluid power component used to provide a safe function.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Safety Legislation

Globally, legal requirements exist to ensure the safe operation of machinery. In most counties these legal requirements include conducting a risk assessment to analyze the risk and assess the necessary steps to reduce the risk.

Risk – Combination of the possibility of harm occurring and the severity of injury possibly caused by that harm.

This guide largely follows the laws outlined in the European Machinery Directive EU 2006/42/EC and in particular the standards of EN ISO 13849-1 (Safety of Machinery) and EN ISO 13849-2 (Validation). The primary objective of these standards is:

- to provide guidelines as to basic health and safety requirements with respect to machinery design
- to act as a guide in best practices for evaluating the risk on a machine
- for determining the most suitable means of risk reduction through various measures. (Design measures, technical measures or instructive measures).

Presumption of conformity is assumed when the guidelines of the Machinery Directive are complied with. This includes both the legal security of operators and manufacturers. The Machinery Directive is a consolidation of Harmonized Standards to guide the machine builder in best practices. These best practices include conducting risk assessments and maintaining a detailed technical file on the machinery design which highlights all aspects of life cycle from construction to disposal and which must account for the safe installation, commissioning, operation, unintended use, limits of the machine and safe disposal.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Safety Standards

Machinery can be divided into three basic safety standards. Type A standards define basic safety requirements. Type B standards are safety group standards and can be sorted as B generic safety standards, B1 specific safety standards for (clearance, temperature and noise) and B2 protective devices and guards (e-stops, light curtains). Type C standards and machine-specific technical standards which contain detailed safety requirements for specific machine types such as presses.

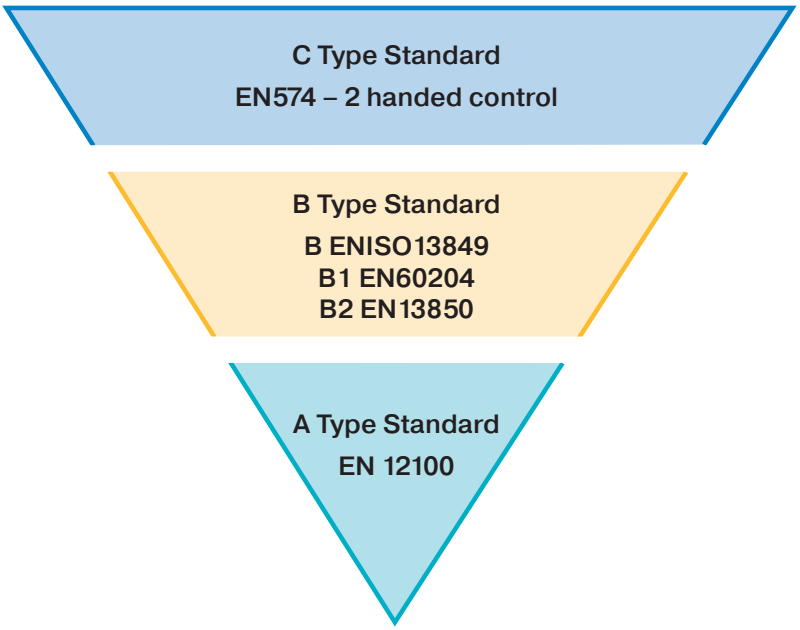
Type C Type C standards (machine safety standards) contain detailed safety requirements for a specific machine or machinery types

Type B Type B standards are (generic safety standards) which deal with one or more safety aspect or protective device for a series of machines

Type B1 Type B1 standards that cover specific safety aspects such as safety clearance, temperatures and noise.

Type B2 Type B2 standards cover protective devices such as two-hand circuits and guards

Type A Type A standards define the (basic safety standards) gives basic concepts, terminology and design principles that can be applied to machinery.



Type C Machinery:

Type C machine safety standards provide detailed safety guidelines for a particular machine or group of machines (e.g. ISO 10218-1:2011). When a type C standard deviates from one or more technical revisions (ANSI/ISO 12100), type A or type B standard, the type C standard takes precedence.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

The Technical File

A technical file must be maintained outlining the construction of the machine in order to comply with the requirements of Machinery Directive. Here is a list of items that should be included in a technical file:

- ☐ A general description of the machine
- ☐ The drawing of the machine and drawings of the control circuits
- ☐ Descriptions and explanations necessary for understanding the machines operation
- ☐ Full detailed drawings
- ☐ All calculation notes, test results, certificates required to check the conformity of the machinery to ensure compliance to EHSR's
- ☐ Documentation on risk assessment showing procedures were followed
  - ☐ A list of EHSR's which apply to machinery
  - ☐ Full description of protective measures implemented to eliminate the hazards identified
  - ☐ Any indication of residual risk associated with the design
- ☐ A list of the standards and technical specs used
- ☐ A technical report showing the results of tests carried out by either the manufacturer or third party
- ☐ A copy of the machines instructions, operating manuals and user guides
- ☐ Guides referencing the preventative maintenance and care of the machine for wearing parts
- ☐ The declaration of incorporation for included partly completed machinery and the relevant assembly instructions
- ☐ Copies of the EC declarations of conformity for products incorporated into the machinery

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Risk Assessment

Risk – Combination of the possibility of harm occurring and the severity of injury possibly caused by that harm.

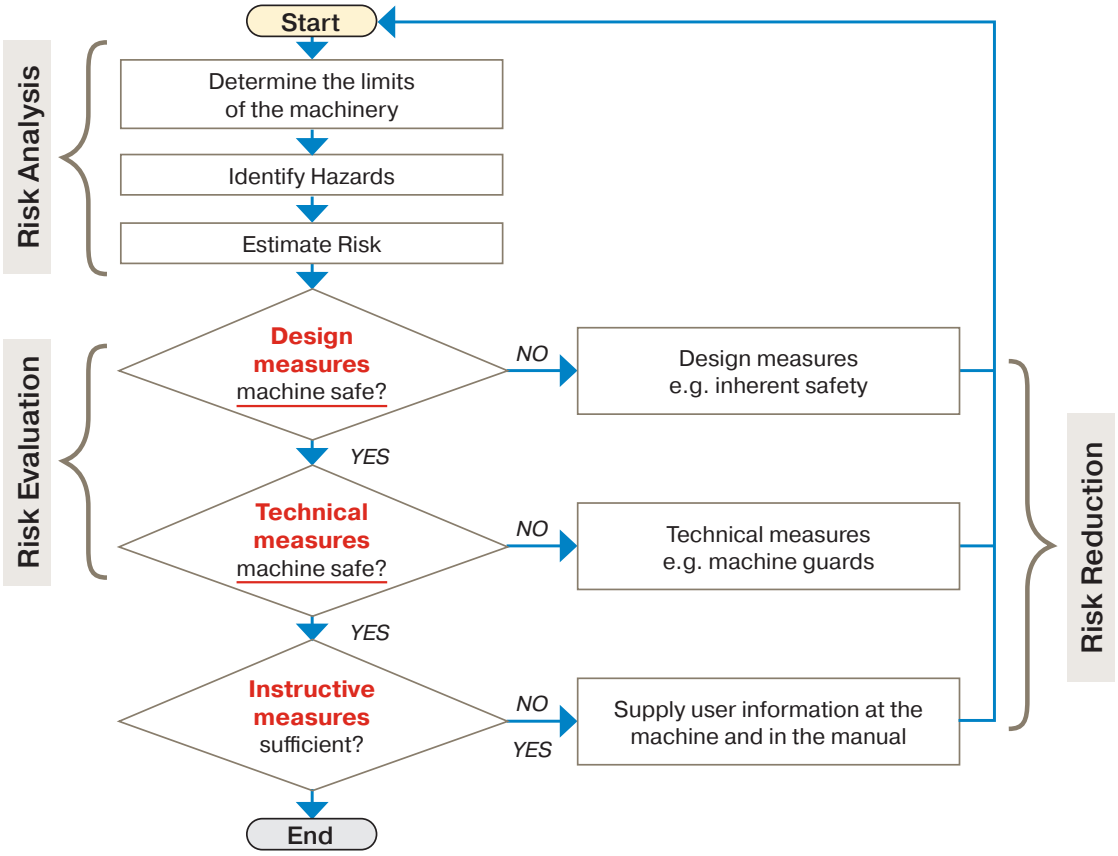
Hazards turn into risks and it is assumed a hazard on a machine will eventually lead to harm. Designing a safe machine is about eliminating the risks by eliminating or safeguarding any hazards identified by a risk assessment. The process of designing a safe machine and reducing risks is to think preventatively regarding many aspects of the design to minimize or eliminate the hazards.

Risk assessment is a series of logical steps to enable the analysis and evaluation of the risks associated with a full or partial area of a piece of machinery and to take action if necessary to ensure risk reduction.

The overall process comprises three steps as shown

1. Risk Analysis
2. Risk Evaluation
3. Risk Reduction

The risk assessment process is further defined by ISO 12100.



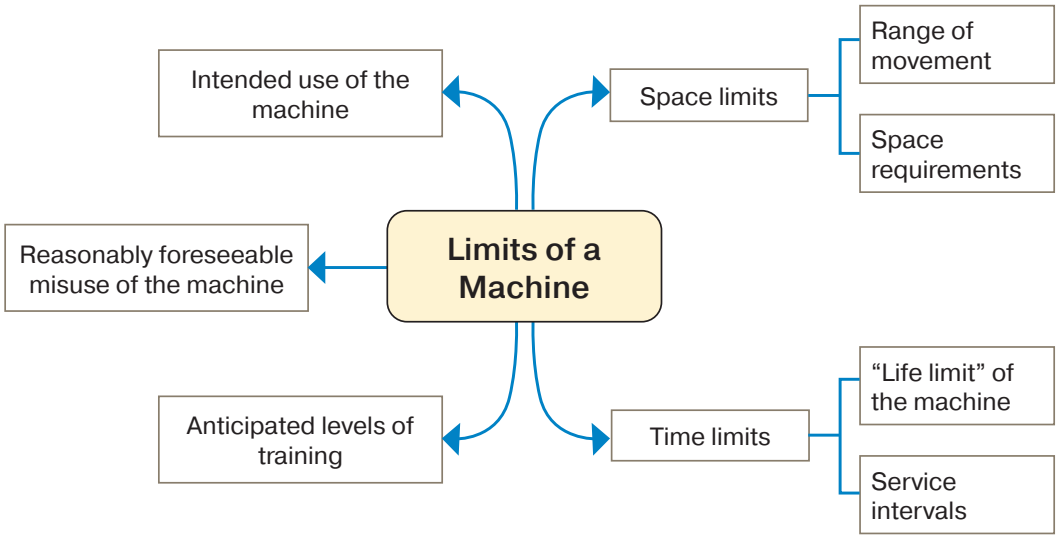
Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Risk Analysis (Determine the Limits of a Machine)

The first step in conduction a risk assessment is the risk analysis. The risk analysis begins with determining the limits of the machinery. Take into account all stages of the machines life cycle including the related people involved, the environment and products used.

The limits of the machinery will guide you in the necessary course of action required. Consider the space required by the machine for example. Will you have room for machine guarding if necessary? You must include not only the machines intended use in your considerations but also reasonably foreseeable misuse of the machine to account for safety in all regards.

Reasonable foreseeable misuse – Use of a machine for purposes other than intended in the operating instructions.

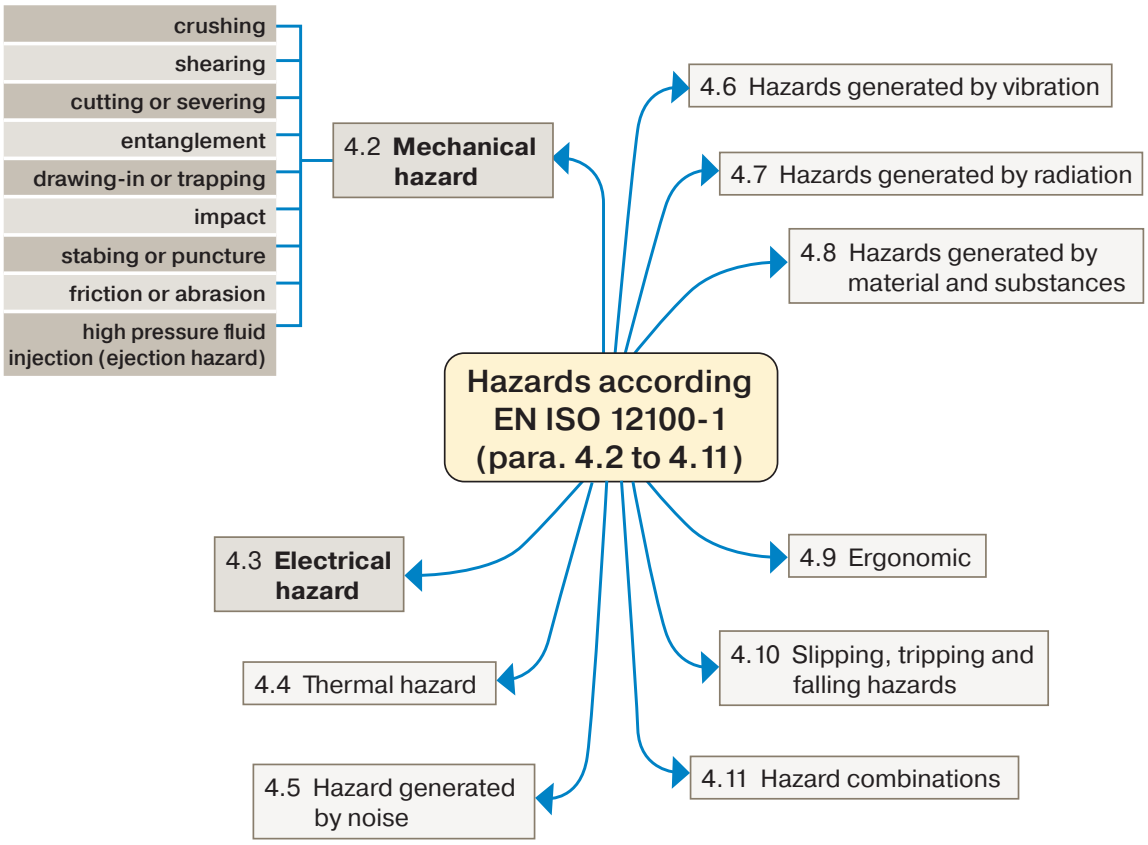


Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Risk Analysis (Identify Hazards)

Hazards on a machine create risk of injury. Identifying hazards through risk assessment allows the machine designer an opportunity to take corrective action early in the design process and prevent potential harm from occurring.

Consider the transport, assembly, installation, commissioning, use and disposal of the machine and potential hazards that may be present for each of these areas. Is the area prone to environmental conditions such as excessive heat, power fluctuations or seismic activity? If so you may want to consider additional bracing, surge suppression, vibration resistance, cooling options etc.



The analysis of hazards is an important step in the risk assessment process because only when hazards have been identified can steps be taken to eliminate the risks.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Risk Analysis (Estimate Risk)

Determining Performance Level Required (PLr)

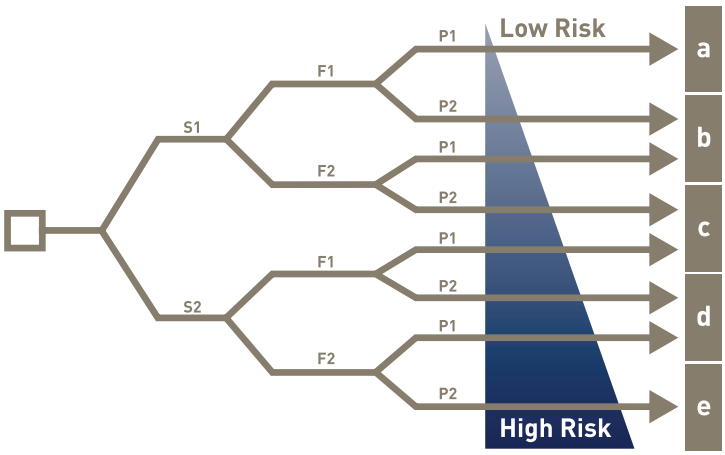
Several different methods of calculating inherent risk are available. The required performance level (PLr) based on a risk assessment are now commonly used to determine the safety level required for the controls system, for the application of machinery.

The level of each hazardous situation is classified into five performance levels from level a to e. With PL a, the control functions contribution to risk reduction is low, while at PL e it is high due to greater inherent risk.

The risk graph can be used as a guideline to determine the required performance level PLr for safe function based on a series of observations including the severity of injury, frequency of exposure to the hazard and possibility of avoiding the hazard. Together these questions will guide you to a determination about the performance level required to ensure a safe machine.

The final PL obtained on the machine must always be equal to or greater than the PLr from your assessment to ensure safety but PL cannot be determined until other considerations are included.

Understanding Risk Assessment



DIN EN ISO 13849 -1

(S) Severity of injury
- S1 Slight (normally reversible injury)
- S2 Serious (normally irreversible injury, or death)

(F) Frequency and / or duration of exposure to hazard
- F1 Seldom to less often and / or brief
- F2 Frequent to continuous and / or long

(P) Possibility of avoiding the hazard
- P1 Possibility of avoiding the hazard
- P2 Scarcely ever possible

Note:

Unfortunately, a clear boundary for selection between F1 and F2 does not exist. In the standard it is recommended that in cases where operator interventions occur more frequently than once per hour, F2 should be selected, otherwise F1 would prevail. This instruction is suitable for most situations which exist.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Risk Evaluation

Should you conclude that risks exist on a machine as identified in the risk analysis portion of a risk assessment, it is incumbent on the machine designer to determine how to best eliminate the risk and implement the changes for risk reduction. It is often helpful to break a larger machine into workable sections (known as zones or modules) such as the cutting zone, feeding zone etc., prior to conducting a risk evaluation. Then each zone and each hazard can be addressed efficiently.

Design Measures

The best solution is always to design out these hazards whenever possible. Designing out the hazards eliminates liability and the potential for injury.

Technical Measures

If designing out the risk is not possible due to limits of the machine your next step is to implement technical measures. Technical measures involve active components that work within the SRP/CS to prevent harm from occurring. These can be safety components or non-safety rated components as defined in EN ISO 13849 and EN ISO 12100 that will achieve safe operation of the machine. Commonly used technical measures include two-handed controls, light curtains, machine guards, safety mats or other protective devices.

Instructive Measures

The worst case scenario is to provide instructive measures through information of the potential harm within the user's operation manual and to label the machine to warn of inherent danger. This option is only allowed when design or technical measures are not possible.

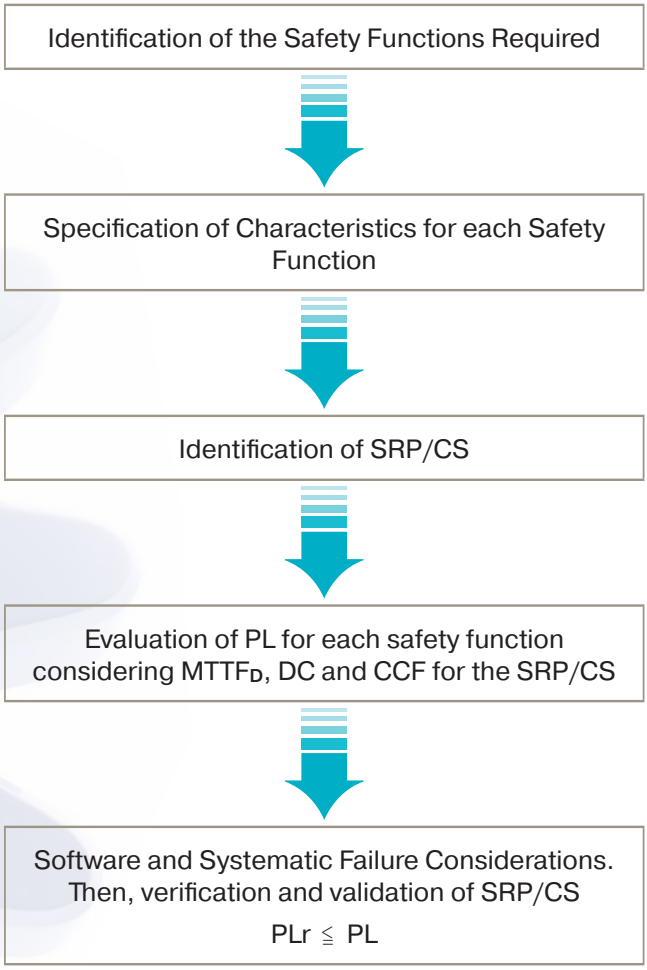
In the process of risk assessment, risk evaluation is followed whenever necessary, by risk reduction. Iteration of this process is necessary to eliminate hazards and to adequately reduce risks by the implementation of protective measures where designing out the hazard is not possible. Review the risk assessment process again and ensure your changes do not create additional potential risks in other areas of the design. It may be necessary to repeat this process many times to ensure full safety is met.

Remember, it is assumed that, when present on machinery, a hazard will sooner or later lead to harm if no protective measure(s) have been implemented.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Risk Reduction

Each risk evaluated will require the use of design measures, technical measures or instructive measures. When technical measures are utilized careful documentation of these safety functions should be added to the technical file for future review if needed.



Each safety function is evaluated independently and the suitable PL determined once the control system is reviewed. A machine is often built to a specific safety level such as Cat 3, PL d, however; it is not uncommon to have different safety levels instituted in different zones of the machine where hazards may vary in severity.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

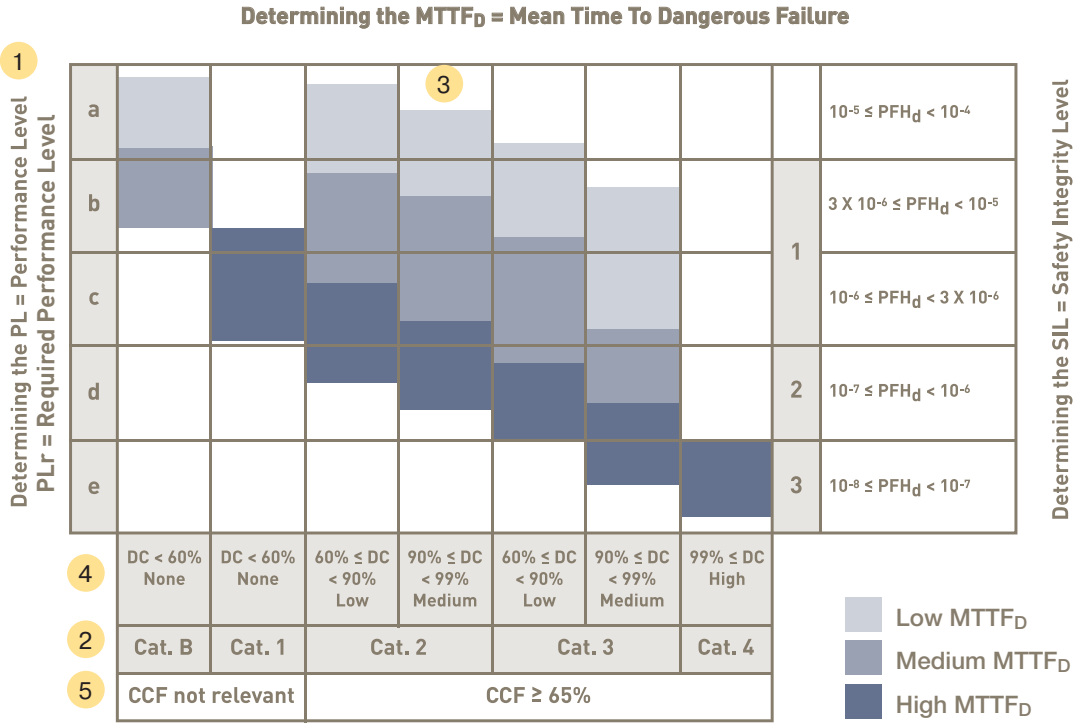
Determining Performance Level (PL)

After the PLr is established, and the risk assessment completed, the performance level (PL) (1) will need to be determined based on the safety categories B, 1, 2, 3 and 4. (2) This safety category will be based on a measure of diagnostic capabilities for the control system (DC), (4) the mean time to dangerous failure ($MTTF_D$), (3) and common cause failure (CCF) (5) which will define the safety levels of a given safety function.

These variables work together to ensure that safety is not just focused on component reliability, but instead introduces common sense safety principles such as redundancy, diversity and fail-safe behavior of the safety related control parts. When determining the performance level, the greater the risk, the higher the requirements of the control system.

The EN 13849 standards dictates that the machine is safe when the Performance level (PL) of the safety control circuit is equal to or greater than the required performance level PLr of the application.

$PLr \leq PL$



Before the Performance Level can be finalized for a safety function B10, $MTTF_D$, DC and CCF must be considered.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

System Reliability, for B10 and $B10_D$ Values

When looking at the reliability of a system it is necessary to obtain the reliability information of the components used within that system from the manufacturer. The B10 value of a product defines a statistical probability of failure and should be obtained from the manufacturer for any component subject to wear that will be used in a safety related circuit. This value does not apply to stationary items with no wear parts such as fittings, tubes, mounting hardware or other such items.

$B10_D$ is in reference to dangerous machine failures only. It is determined that since half of machine failures may be dangerous that B10 x 2 = $B10_D$; or that twice the point of failure is defined as the point of dangerous failure within a machine.

B10 *the point at which 10% of a sample lot has failed (measured in switching cycles). The values are determined according to EN ISO 19973.*

$B10_D$ *the point at which 10% of a sample lot has failed dangerously. Note* $B10_D$ can be referenced as B10 x 2.*

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Mean Time to Dangerous Failure ($MTTF_D$)

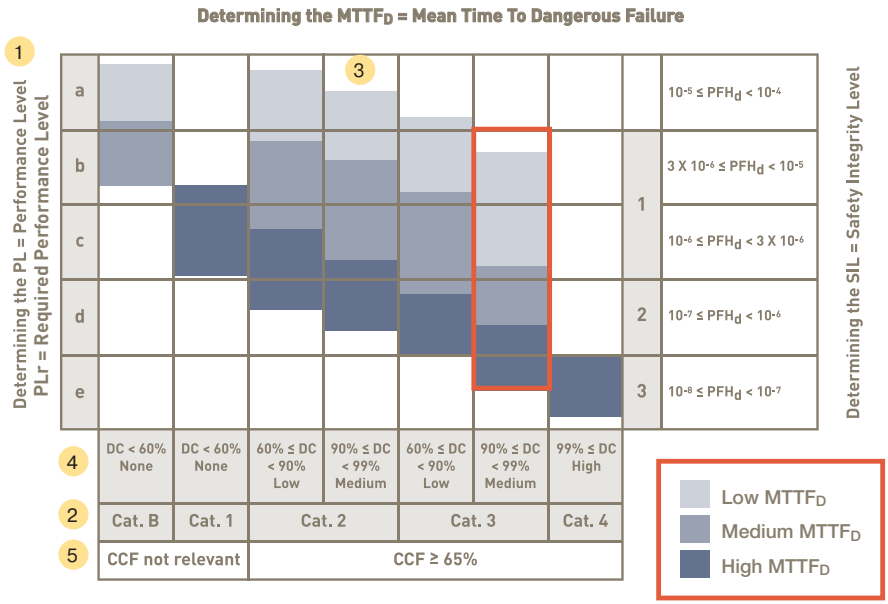
The reliability of a system has to be quantified as part of achieving a desired performance level (PL). Reliability is expressed as the Mean Time to Dangerous Failure ($MTTF_D$).

Reliability	$MTTF_D$
Low	3 years ⩽ $MTTF_D$ < 10 years
Medium	10 years ⩽ $MTTF_D$ < 30 years
High	30 years ⩽ $MTTF_D$ < 100 years

$MTTF_D$ is a statistical calculation which defines the mean time (usually expressed in years) until a dangerous failure occurs in a component.

While there are no guaranteed values when it comes to statistical calculations, the idea is to understand the probability of failure within a system. This will provide some insight into the reliability of the component used.

Based on the standard EN ISO 13849-1 there are three types of $MTTF_D$; low, medium and high.



Reliability of the system $MTTF_D$ is critical in system design to achieving the correct category and performance level. Refer to ENISO 1349-1, annex K for more information.

Before the Performance Level can be finalized for a safety function B10, $MTTF_D$, DC and CCF must be considered.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Calculations

Calculating the $MTTF_D$ for a mechanical component in a single channel SRP/CS

$$MTTF_D = \frac{B10_D}{0.1 \; x \; N_{op}}$$

To calculate the number of annual operations for the mechanical element

$$N_{op} = \frac{Dop \; x \; hop \; x \; 3600 s/h}{Tcycle}$$

N_{op} (actuations per year of the mechanical component

H_{op} (operating hours per day)

D_{op} (operating days per year)

T_{cycle} (cycle time)

The operation time of the component is limited to $T10_D$ (the mean time until 10% of components fail dangerously).

$$T10_D = \frac{B10_D}{N_{op}}$$

Example:

For a pneumatic valve, a manufacturer determines a mean value of 60 million cycles as $B10_D$. The valve is used for two shifts each day on 220 operation days a year. The mean time between the beginning of two successive switching of the valve is estimated as 5s. This yields the following values:

D_{op}	200	days per year
H_{op}	15	hours per day
T_{cycle}	5	sec per cycle
$B10_D$	60000000	million cycles
N_{op}	2.16×10^6	cycles/year
$T10_D$=	27.7	years
$MTTF_D$=	277	years

$$N_{op} = \frac{200 \; days / year \; x \; 15h / day \; x \; 3600 \; s / h}{5s / cycles}$$

$$T10_D = \frac{60 \; x \; 10^6 \; cycles}{2.16 \; x \; 10^6 \; cycles / year}$$

$$MTTF_D = \frac{27.7 \; years}{0.1} = 277 \text{ years}$$

Note – This will give a high $MTTF_D$ for the component. These assumptions are only valid for a restricted operation time of 27.7 years for the valve.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Diagnostic Coverage

Diagnostic coverage (DC) is the measure of a control systems ability to detect faults. It is the ratio of the rate of detected dangerous failures compared to the rate of all dangerous failures.

Diagnostic coverage (DC) is a requirement of a safety related control system. The degree of diagnostic coverage requirements will vary based on the performance level needed. When a dangerous failure does occur it is the monitoring quality of the control system which will detect the fault and bring the machine to a safe state. The diagnostic coverage is therefore a very important part of achieving the performance level requirements. The performance level includes the monitoring quality of the control system and until this is established the PL and category cannot be defined. The engineer must analyze the machines switching capability and processes to estimate the percentage of errors than can be discovered by these measures.

Diagnostic Coverage	DC Range
None	DC < 60%
Low	60% ⩽ DC < 90%
Medium	90% ⩽ DC < 99%
High	99% ⩽ DC

Simplified explanation of DC ranges from EN ISO 13849-1

The engineer must analyze the machines switching capability and processes to estimate the percentage of errors that can be discovered by these measures. Average diagnostic coverage can be calculated using this formula.

$$DCavg = \frac{\frac{DC1}{MTTF_D1} + \frac{DC2}{MTTF_D2} + \frac{DC3}{MTTF_D3} \ldots\ldots\ldots}{\frac{1}{MTTF_D1} + \frac{1}{MTTF_D2} + \frac{1}{MTTF_D3} \ldots}$$

$$\text{Where, DC1} = \frac{\Sigma\ (Recognized\ dangerous\ failures)}{\Sigma\ (Total\ dangerous\ failures)}$$

Machine design software commonly used today (such as SISTEMA) will provide these calculations based on components chosen.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Common Cause Failure

Common Cause Failure (CCF) is the failure in a component for one common reason or failures stemming from a common source.

Common cause failure can occur from one common source for example, contamination or excessive high heat. Measures must be implemented to combat these failures. It is interesting to note that component manufacturers cannot support or influence this area since it is mostly related too environmental issues or measures determined by machine design such as vibration and not normally relevant to one particular component.

Common cause failure analysis is best achieved using the point system allotted in Annex F of ISO 13849-1 where a number of mechanical and electronic elements are assigned point scores to help determine your total CCF.

A few measures against CCF include:

- Separate shielding for the signal path of each channel
- Different initiation of safety function for each channel
- Training to understand the causes and consequences of CCF
- Proper filtration to prevent failure from contamination

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Systems Architecture (Controls Wiring)

Safety on machine can be achieved in many ways.

The architecture of a control system is largely defined as either a single channel or two channel design.

Single channel offers no redundancy and can result in the loss of the safety function. For this reason, single channel systems are reserved for low risk applications where probability of failure is low and resultant injury is negligible.

Two channel systems however; provide a redundancy and are typically monitored to ensure that a failure does not result in the loss of the safety function. Control systems are largely made up of input devices that send signals to logic devices to activate output devices.

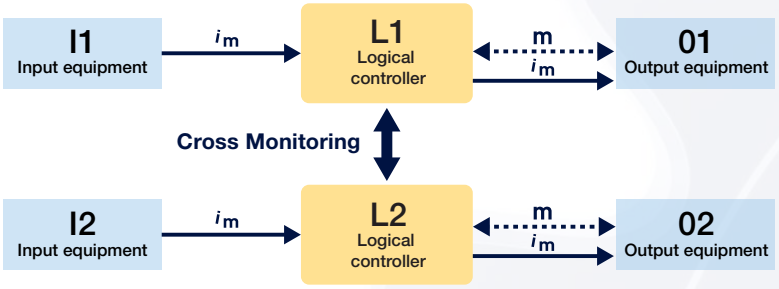
I represents input devices, L represents logic controllers and O represents outputs while *i*m shows a means of interconnecting these components.

Controls Architecture - Single Channel

Single channel systems have a single input device with a single interconnect means to a logic controller which then connects to a single output device via a single interconnect. A failure along this architecture will lead to the loss of the safety function.

Controls Architecture – Two Channel (Redundant)

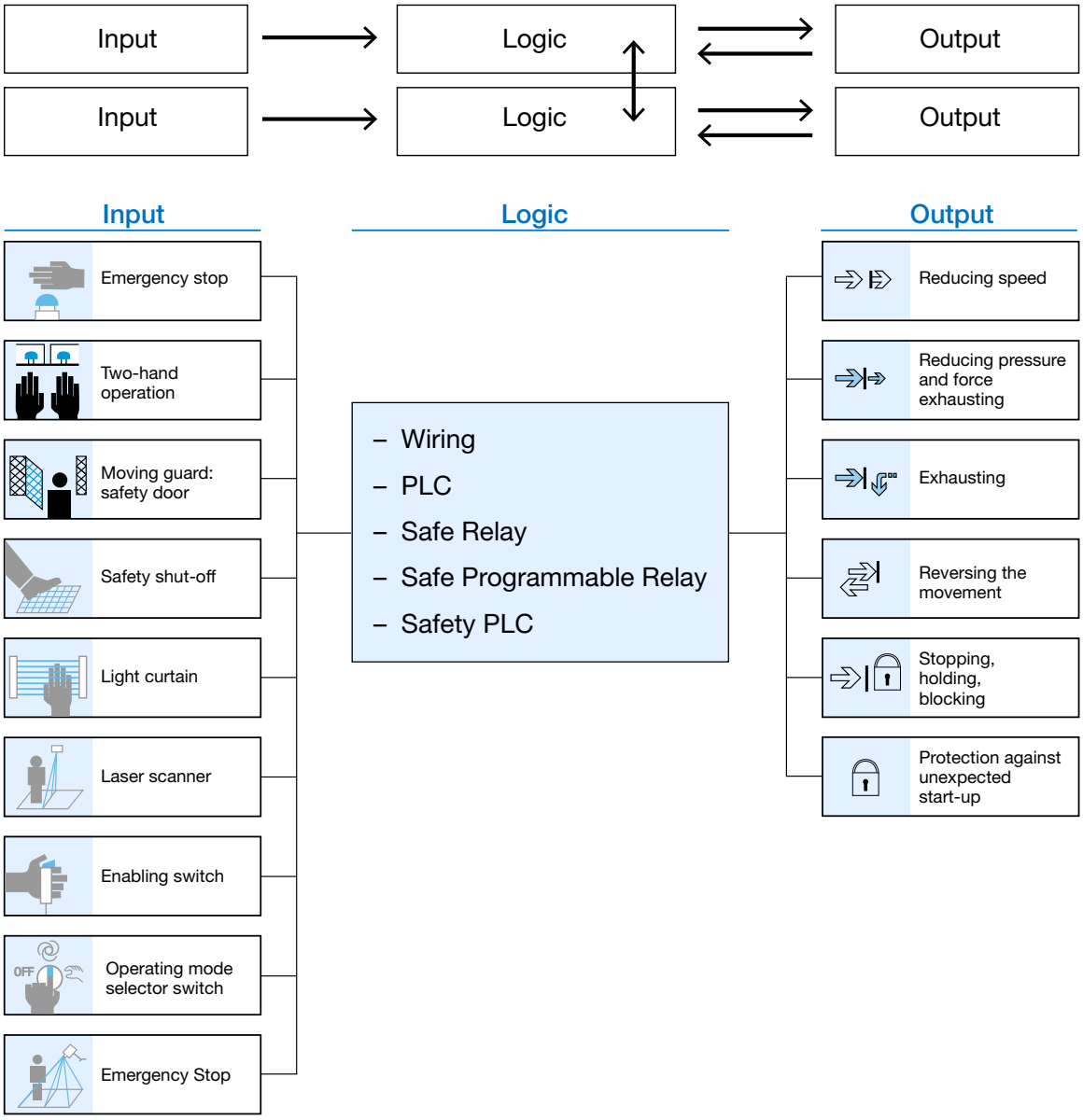
Input devices have a redundant interconnect means to a logical controller with redundant interconnect means to an output device. The redundancy is referred to as two channel architecture. In addition to redundancy in design, two channel systems require a robust means of logical controller capable of monitoring between the logic device and the output equipment and also the ability to monitor internally to ensure proper function.



Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Machine Architecture

Safety on machine can be achieved in many ways. Control systems are largely made up of input devices that send signals to logic devices to activate output devices. A simplified methodology is I, L, O or input, logic, output to explain the relationship between components used to achieve a safe machine.



The Category rating and PL achieved will be dependant on the integrity of components used in the subsystem.

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Category Designations

A category designation is a combination of the controls systems ability to detect faults and subsequent behavior in the fault condition. The categories form the backbone of the system complimented by the component reliability ($MTTF_D$), the tests (DCavg) and the resistance to common cause failures (CCF)

Category B

I	Input device
L	Logic
O	Output device
i_m	Interconnecting means

In **Category B** when a fault occurs it can lead to the loss of the safety function.

Single-channel architecture offers no redundancy, and the loss of the safety function is likely if the architecture is faulted or damaged in any way.

Category B shall be designed, constructed, selected, assembled and combined in accordance with the relevant standards using basic safety principles.

Component $MTTF_D$, low to medium

Diagnostic Coverage, DC_{avg} = none

Maximum PL = b

CCF, not relevant

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Category 1

I	Input device
L	Logic
O	Output device
i_m	Interconnecting means

In **Category 1** when a fault occurs it can lead to the loss of the safety function.

Single-channel architecture offers no redundancy, and the loss of the safety function is likely if the architecture is faulted or damaged in any way.
Note: The higher $MTTF_D$ in Category 1 makes the loss of the safety function less likely than in Category B.

Category 1 shall be designed and constructed following relevant standards and using both well-tried components and well-tried safety principles.

Component $MTTF_D$, high

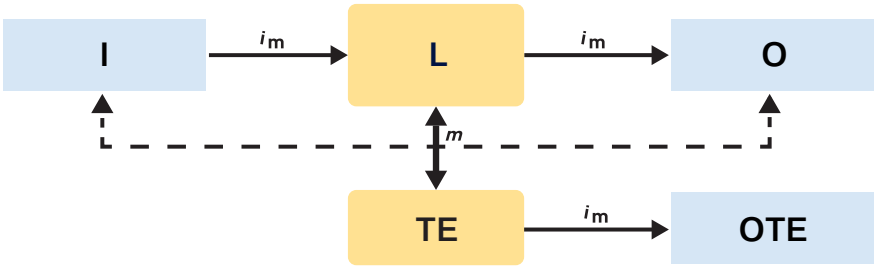
Diagnostic Coverage, DC_{avg} = none

Maximum PL = c

CCF, not relevant

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Category 2



I	Input device
L	Logic
O	Output device
i_m	Interconnecting means
TE	Test equipment
OTE	Output of te
m	Monitoring

Category 2 combines the requirements for category 1, plus the components are checked for faults affecting the safety function.

Faults are checked at regular intervals including start-up, prior to initiation of any hazardous situation or as the risk assessment deems necessary.

Single-channel architecture offers no redundancy, and the loss of the safety function is detected by the check. *The occurrence of a fault can lead to the loss of the safety function between checks.*

Category 2 shall be designed and constructed following relevant standards using well-tried safety principles.

Component $MTTF_D$, low to high

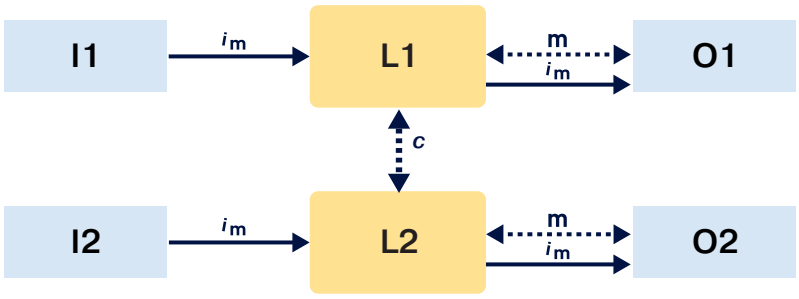
Diagnostic Coverage, DC_{avg} = low

Maximum PL = d

CCF, applicable

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Category 3



I1, I2	Input device
L1,L2	Logic
O1,O2	Output device
i_m	Interconnecting means
m	Monitoring
c	Cross monitoring

Category 3
Redundant, 2 channel architecture

Category 3 systems detect some faults but not all faults are detected. A single fault does not lead to the loss of the safety function however, multiple undetected faults, may lead to the loss of the safety function.

Whenever reasonably possible the single fault shall be detected at or before the next demand on the safety function.

Category 3 shall be designed and constructed following relevant standards using well-tried safety principles.

Component $MTTF_D$, low to high

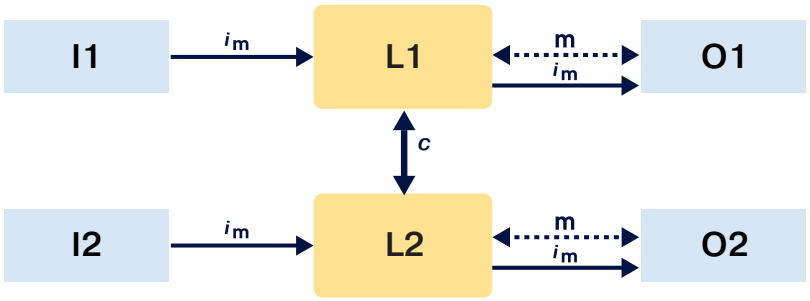
Diagnostic Coverage, DC_{avg} = low to medium

Maximum PL = d

CCF, applicable

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Category 4



I1, I2	Input device
L1,L2	Logic
O1,O2	Output device
i_m	Interconnecting means
m	Monitoring
c	Cross monitoring

Category 4
Redundant, 2 channel architecture

Category 4 architecture should be applied where the greatest inherent dangers exist. This architecture offers the highest possible safety coverage with monitoring, cross monitoring, redundancy and a 99%> DC diagnostic coverage for high fault detection.

Every fault must be detected before or during the next request. If single fault detection is not possible the accumulation of faults will not lead to the loss of the safety function.

To achieve the highest diagnostic coverage possible, safety-rated logic controllers should be utilized that meet the diagnostic coverage requirements.

Category 3 shall be designed and constructed following relevant standards using well-tried safety principles.

Component $MTTF_D$, high

Diagnostic Coverage, DC_{avg} = high

Maximum PL = e

CCF, applicable

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Sistema

Sistema is a free software. Its name stands for

“Safety Integrated Software Tool for the Evaluation of Machine Applications”.

Its purpose is to provide developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of EN ISO 13849-1.

Sistema is a Windows based software which enables users to model the structure of the safety-related control components based upon the architectures and permits automated calculation of the reliability values including that of the attained Performance Level (PL).

The link to download Sistema can be found at
www.dguv.de/bgia

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Facts, Answers, Questions

What if the performance level is not achieved?

Based on the calculations and process involved several options can be implemented to increase the performance level needed. Start by using components with a longer service life and B 10_D value. This will increase your $MTTF_D$. Adding redundancy will increase your performance level and by increasing your ability to monitor with the proper components you can increase the diagnostic coverage of your controls system. If possible you can also reduce the frequency of switching cycles (Nop).

What makes a product a safety component?

A product is deemed to be a safety component under the terms of the Machinery Directive when it is tested and verified to provide specific safe function for a given period of time at a given state. It must bear the CE mark for Europe and receive independent certification.

What is the difference between a safety component and a safety related part of a control system (SRP/CS)?

Any fluid power component can be used in the safety related part of a control system to provide safe function. A safety component is tested and verified to provide specific safe function for a given period of time at a given state.

Can I use the PLr as my PL?

The main difference is PL accounts for the ability to detect faults (diagnostic coverage), the quality and service life of the components ($MTTF_D$) and the ability of the components to withstand conditions on/in the machine (CCF). The PLr only looks at the risk and not at the control system. Therefore, PLr cannot be assumed to be the same as PL.

If I'm not in Europe am I required to comply with the Machinery Directive?

Yes, if you are shipping into the European market. You must comply fully with the Machinery Directive requirements. If you are not shipping into Europe, then you must follow the local laws and standards that you will find align closely to those of the EU.

Can I conduct my own risk assessment?

Risk assessment must be conducted by an individual either within your organization capable of evaluating a machine that has not been involved in the machinery design. If you do not have an individual like this on staff then third party services must be selected to perform this function.

What is partially completed machinery?

Partially completed machinery refers to an assembly that is almost a full system but cannot in itself perform a specific application for function. It is intended to be incorporated into, or assembled with, other machinery or partially completed machinery. Partially completed machinery:

- Consists of several parts, at least one of which is moving
- Is fitting with or intended to be fitted with a drive system
- Cannot by itself perform a specific application
- Is to be incorporated into partially completed or completed machinery

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Glossary of Machine Safety Terms and Abbreviations

Term	Defined
a, b, c, d, e	Performance level designation
Adequate risk reduction	Action to prevent risk that is considered reasonable based on technology available
Adjustable guard	A guard which can be wholly or partially adjusted or moved
ANSI	American National Standards Institute
AOI	Add on instruction
AOPD	Active optoelectronic protective device (light curtain)
B,1,2,3,4	Category designation
B10	Number of switching cycles until failure occurs in 10% of the sample lot
$B10_D$	Number of switching cycles until dangerous failure occurs in 10% of the sample lot.
Cat.	Category (B, 1,2,3,4)
Category	Classification of SRP/CS parts by resistance to faults and reliability
CCF	Common cause failure
CEN	European committee for standardization
CENELEC	European committee for electrotechnical standardization
Common Cause Failure	Failure of different items resulting from a single event
Common mode failures	Failures of items by the same fault mode (can be from different causes)
Comparative emission value	Set of data used to compare two or more machines pollutants
Control system	The system that is used to manage components on a machine circuit
CS	Control system
Dangerous Failure	Failure that results in dangerous state or malfunction
DC	Diagnostic coverage
DCavg	Average diagnostic coverage
Design measures	Steps to provide protection
Diagnostic Coverage	Effectiveness to determining failures
Embedded Software	Software in a machine that usually cannot be altered by the user
Emergency operation	Actions and functions to end an emergency situation
Emergency situation	Hazardous situation needing urgent attention
Emergency stop	A function initiated by a single human action to prevent or stop a hazardous situation
Emission value	A number to quantify a machine generated pollutant (such as noise or vibration)
Enabling device	A device that is used in conjunction with a start control to allow a machine to function
Energy dissipation	Removal of stored energy from a machine
E-stop	Emergency stop
EU	European Union
F, F1, F2	Frequency of exposure to hazard
Failure	Termination of the ability of an item to perform a required function
Failure to danger	A malfunction that increases a risk

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Fault	Inability to perform a required function in a components normal state
FB	Function block
Fixed guard	A guard secured to provide protection that is not easily removed
Guard	A physical barrier installed to provide protection
Harm	Physical injury or damage to health
Hazard	Potential source of harm
Hazard Area	Zone where person can be exposed to a hazard
Hazardous event	An event that can cause harm
Hazardous situation	Where a person is exposed to at least one potential harm
Hold to run control device	A device which initiates and maintains machine function only when manually actuated
I, I1, I2	Input devices
I/O	Inputs / outputs
ICS	Industrial control system
i_m	Interconnecting means
Impeding device	A device that creates an obstruction (such as a rail or barrier)
Input	A command sent in
Instructive measure	To provide information where an unsafe condition exists
Intended use	Use of a machine as set out in the operating instructions
Interlocking device	A device that will prevent the operation of a machine if conditions are not met
Interlocking guard	A guard which works with the SRP/CS to provide protection based on the state of the machine
Interlocking guard with start function	A guard which allows a machine to start only when ideal conditions are obtained
ISO	International Standards Organization
Isolation	Disconnecting or separating
L, L1, L2	Logic devices such as a PLC
Limiting device	Device that prevents a hazardous condition based on a machines operating variables
Logic Controller	A hardware device that performs a function from inputs and outputs.
Machinery	Components joined together to perform and intended function
Maintainability	Ability of a component to be looked after to fulfil an intended function
Malfunction	Failure to provide an intended function
Manual reset	Function in the SRP/CS used to restore safety functions before restarting a machine
Mission Time	Time period of intended use of an SRP/CS
Monitoring	A function to ensure adequate protection is provided in the event of a failure
Movable guard	A guard which can be opened or moved without the use of tools
MTBF	Mean time between failures
MTTF	Mean time to failure
$MTTF_D$	Mean time to dangerous failure

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

MTTR	Mean time to repair
Muting	Temporary automatic suspension of safety function
n_{op}	Number of operations (annually)
O, O1, O2	Output devices
OTE	Output on test equipment
Output	A command sent out
P	Potential of avoiding the hazard
Performance level	Level used to specify the ability of safety-related parts of control systems to perform a safety function
PES	Programmable electric system
PFH	Probability of failure per hour
PFHd	Probability of dangerous failure per hour
PL	Performance level
PLC	Programmable logic controller
PLr	Performance level required in order to achieve the required risk reduction for each safety function
Programmable logic controller	A hardware device that allows user interface and performs a function from inputs and outputs with software
Protective measures	A measure taken to provide protection from a hazard
Reasonably foreseeable misuse	Use of a machine for purposes other than intended in the operating instructions
Relevant hazard	A hazard associated with a machine
Reliability	Ability of a component to perform a specific function without failing for a period of time
Residual	Remaining or left behind
Residual risk	Risk remaining after protective measures have been taken
Risk	Combination of hazards and potential for injury
Risk analysis	Determining risk based on hazards and machine limits
Risk assessment	Process of analysis and evaluation of risk
Risk estimation	Determining probability of an occurrence that could be harmful
Risk evaluation	Judgment of whether risk reduction was achieved
S, S1, S2	Severity of injury
Safeguarding	Actions or equipment to protect where design measures cannot adequately provide protection
Safety function	A function that can result in a potential risk if failure occurs
Safety instrumented function	Built in function on a machine to bring it to a safe state if predetermined conditions are not met
Safety integrity level	Level of risk reduction provided by a safety function
Safety-related part of a control system	Part of a control system that responds to safety-related input signals and generates safety-related output signals

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Sensitive protective equipment	Equipment capable of detecting persons or parts and able to generate a signal for the CS
SIF	Safety instrumented function
Significant hazard	A hazard requiring specific action to remedy it
SIL	Safety integrity level
SPE	Sensitive protective equipment
SRASW	Safety related application software
SRESW	Safety related embedded software
SRP	Safety-related part
SRP/CS	Safety related parts of a control system
SRS	Safety requirements specification
Start-up	A change in motion from rest to movement
Systematic failure	Failure related to a certain cause in the design, manufacturing or other factors
$T10_D$	Mean time until 10% of components fail dangerously
TE	Test equipment
Technical measure	Using safety components or mechanical measures to prevent risk
Test rate	Frequency of automated fault detection
T_M	Mission time
Two handed control device	A device requiring actuation with both hands to allow machine function
Unexpected start-up	A motion that creates a risk which was unintended
Unintended use	Use of a machine other than as prescribed
Usability	The ease of understanding the function of a machine or its controls

Information Resources

ANSI	American National Standards Institute	www.ansi.com
BGIA	Institute for Occupational Safety & Health of the German Social Accident Insurance	www.dguv.de
CEN	European Committee for Standardization	www.cen.eu
CSA	Canadian Standards Association	www.csagroup.org
DGUV	German Social Accident Insurance	www.dguv.de
ISO	International Standards Organization	www.iso.org
NFPA	National Fire Protection Association	www.nfpa.org
NFPA	National Fluid Power Association	www.nfpa.com
OSHA	Occupational Safety & Health Association	www.osha.gov
PARKER HANNIFIN	Manufacturer	www.parker.com
SISTEMA	Safety Integrated Software Tool for the Evaluation of Machine Applications	www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema
UL	Underwriters Laboratories	www.ul.com

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

Parker Hannifin Corporation
Pneumatic Division
Richland, Michigan
www.parker.com/pneumatics

VAL-SIF-148 05/2022

Parker Hannifin Corporation
Pneumatic Division
8676 E. M89
Richland, MI 49083 USA
Phone: 269 629 5000
Applications Engineering: E-mail: **pdn.technical@support.parker.com**
Customer Support: E-mail: **pdncustsvc@parker.com**
www.parker.com/pneumatics