A COMPREHENSIVE GUIDE TO MACHINE SAFETY

Parker

CONTENTS

A COMPREHENSIVE GUIDE TO MACHINE SAFETY

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 5.0 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.

What is a machine?

An assembly fitted with or intended to be fittedwith 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 machinery legislation. 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 pneumatic product development, Parker consistently brings the newest technologies to market.

Rapid advances in machine technology have 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.

ABOUT MACHINE SAFETY

The goal of machine safety is to protect people, animals, property and the environment from accidents caused from all types of machinery.

New legislation, EU2023/1230 effective January 2027 repeals the machinery directive 2006/42/EC and its early predecessor 98/37/EC.

This new legislation builds on the previous safety framework but adds additional requirements to further improve safety levels, set clear rules in relation to the framework, to update for new and emerging technologies and to fix inconsistencies that existed.

The factory floor and in plant machinery have seen considerable change since digitization and networking occurred. The digital transformation rapidly evolved into another revolution of emerging technologies.

The emergence of artificial intelligence, autonomous machinery and robotics. These rapid changes for a new smart factory created new related issues for industrial security, a review of standards and a restructuring of factory floors. One of the needs was an increase in cybersecurity resilience.

These fundamental shifts marked the necessity for updated legislation to harmonize the essential health and safety requirements for machinery in the European Union and to continually promote the free movement of machinery within the single market.

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

Parker Hannifin is a global corporation so careful consideration is paid to both the global standards (which we consider the most comprehensive) as well as regional standards.

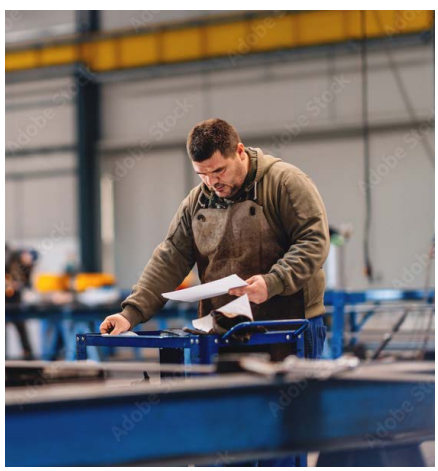
These are important considerations as we develop new products for our customers across a diverse and global landscape.

What is a Safety Component?

Safety standards clearly distinguish 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.

While safety standards do not prescribe the use of safety rated componentry, they do describe the conformity assessment procedures to market a product as safety rated.



- 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 for Europe and appropriate third-party verification. (Additional requirements for marks may be required for other countries such as electrical certification marks for North America.)

And as such,

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

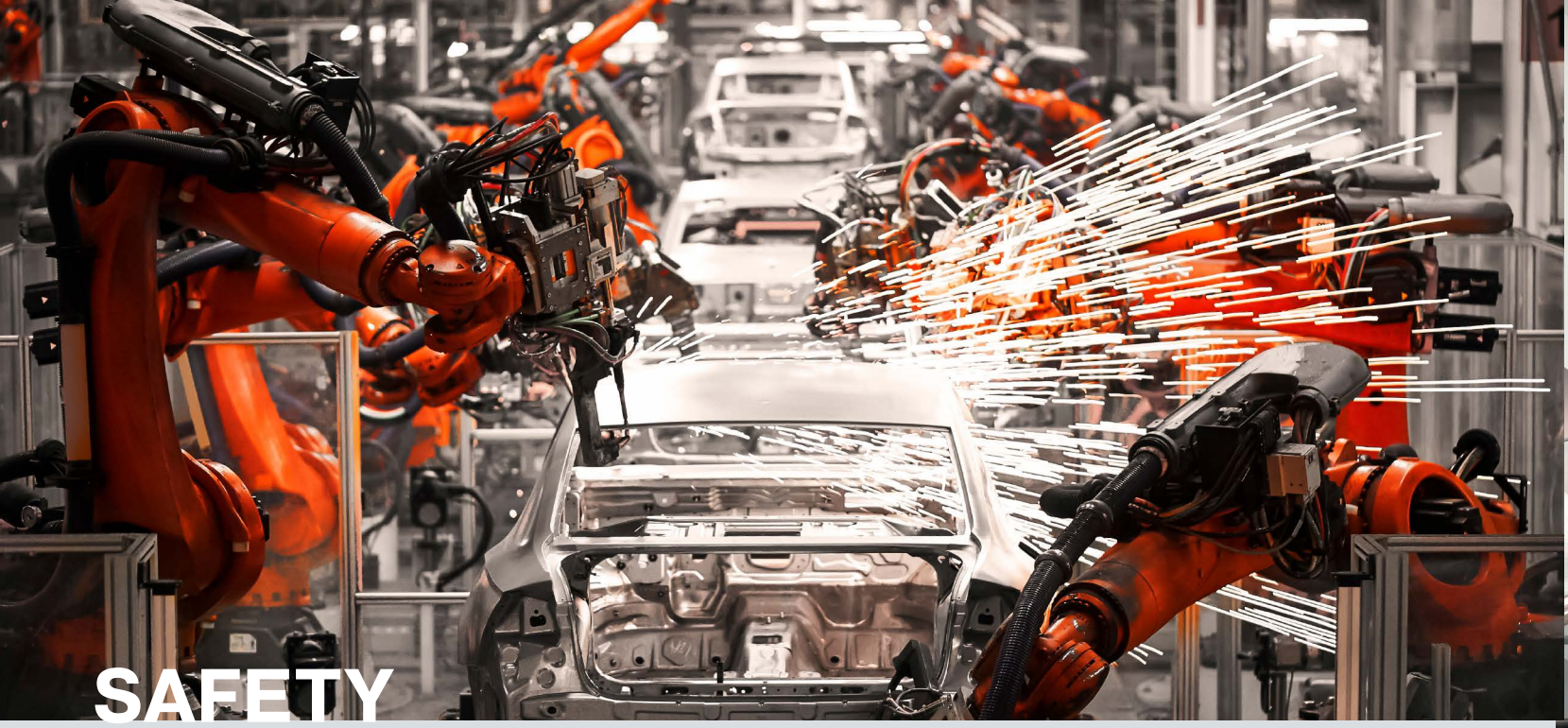
Examples of safety components include but are not limited to a light curtain, safety door switch, safety exhaust valve, emergency stop device, or other safety integral specific components).

- A safety related part of a control system (SRP/CS) is developed by the manufacturer of a machine and its evaluation for safety function is part of the machinery design.

This can be a standard fluid power component used to provide a safe function. Parker offers standard components, components suitable for use as an SRP/CS and safety rated components.

Products suitable for use as an SRP/CS are standard products that are well tried and tested and have available endurance life data. New recommendations in EU2023/1230 suggest manufacturers supply rated endurance life data so that machine builders can determine the integrity of the component for their given PL. **Parkers VDMA data library can be found online at DGUV:**

www.dguv.de/ifa/



SAFETY

Safety Legislation

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

This guide largely follows the laws outlined in EU Machinery Regulation 2023/1230 and Safety of Machinery standard ISO 13849.

The points to the right outline some of the key changes enacted by the new regulation.

It is not an inclusive list.

As of Jan 2027, the **Machinery Directive regulations will cease to apply**, and non-compliant machinery will be required to be rebuilt to comply which could potential be a laborious process.

Further, several hundred standards will require revision to adopt the requirements of the new legislation.

The structure of articles, appendices, and Annexes has shifted from the editorial layout perspective.

Higher risk machinery is now divided into two categories namely self-learning mechanisms as well as traditional machinery types.

New obligations for manufacturers are outlined in Article 10 with respect to recalling machinery that does not meet the new regulatory requirements.

Digital instructions are now permissible with requirements for how to access, store and retrieve the digital documentation. This is relevant to both the operating instructions as well as the declaration of conformity documents.

Protection of software corruption is outlined in Annex III requiring both the management of device access as well as providing protection against accidental and deliberate modification. These changes enhance the security in respect to the cyber resilience act and radio equipment directives.

Self-evolving machinery requirements and risk assessment procedures as well as self-learning software requirements (section 2.8)

Safety-related software such as function blocks for programmable controllers are created, they must be CE marked and carry a declaration of conformity.

Machinery must be designed to allow users the ability to test the safety functions.

Autonomous machinery must have a supervisory function that can be identified and operated remotely. In the case of an autonomous machine, it must be possible for an operator to start, stop or bring the machine to a safe state – without having to go directly to the machine and therefore into a potentially dangerous area.

HOW CAN PARKER HELP YOU?

Standards, Legal Requirements, Training, & Product Solutions

Standards & Legal Requirements

Parker offers expertise regarding the interpretation and application of legal requirements for machinery safety for both new machine design and support with selecting the applicable standards for retrofit of existing machinery.

Training

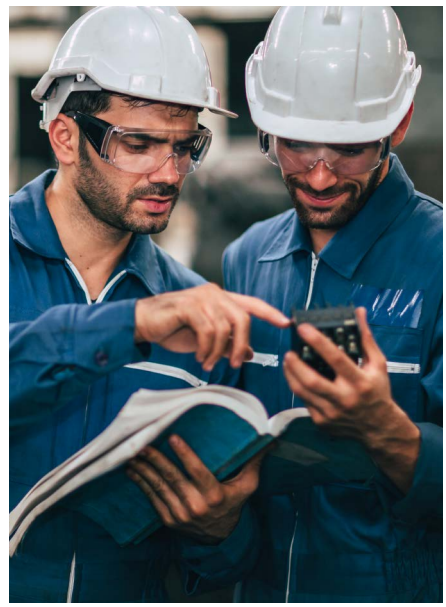
Parker offers training on the application of product solutions for pneumatic machinery safety, the process of risk assessment, and the application of safe machine design with pneumatics.

Product Solutions

Parker offers a range of products that are suitable for use as a safety related part of a control system or that are functional safety certified.

SAFETY STANDARDS

An Overview of Safety Standard Types and Classification Details



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.

The Three Safety Standard Types:

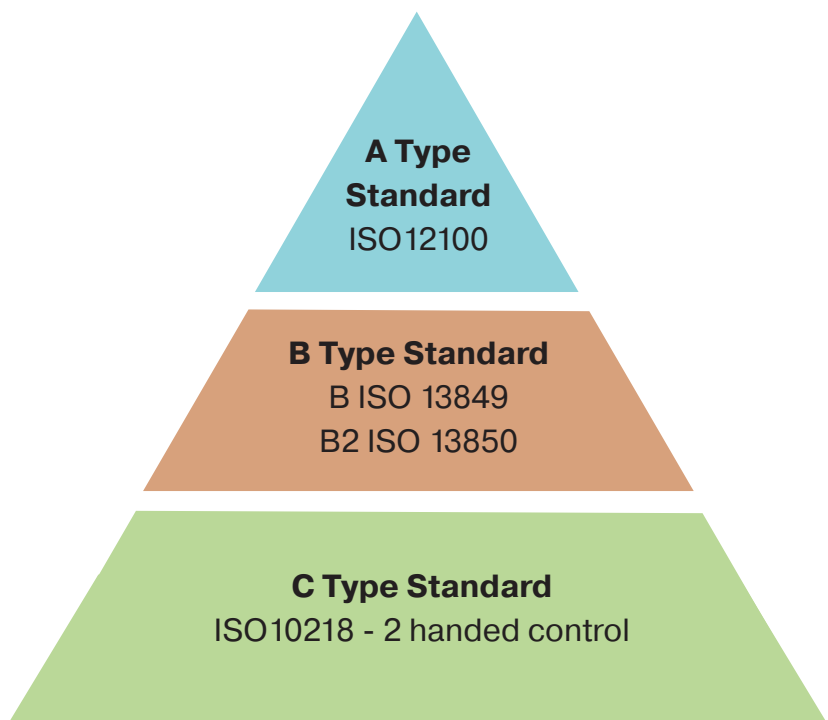
Type A standards define basic safety requirements.

Type B standards are safety group standards and can be sorted as B generic safety standards:

Type B1 specific safety standards for (clearance, temperature and noise), and

Type B2, protective devices and guards (e-stops, light curtains).

Type C standards and machine-specific technical standards contain detailed safety requirements for specific machine types such as presses.



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 for robots). **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.**

THE TECHNICAL FILE

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

Technical File Outline:

- ☐ 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

ASSESSING & MANAGING RISK

Risk Assessment

Risk: The combination of the **possibility of harm** occurring and the **severity of injury possibly** caused by that harm, based on **frequency of exposure to the hazard.**

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.

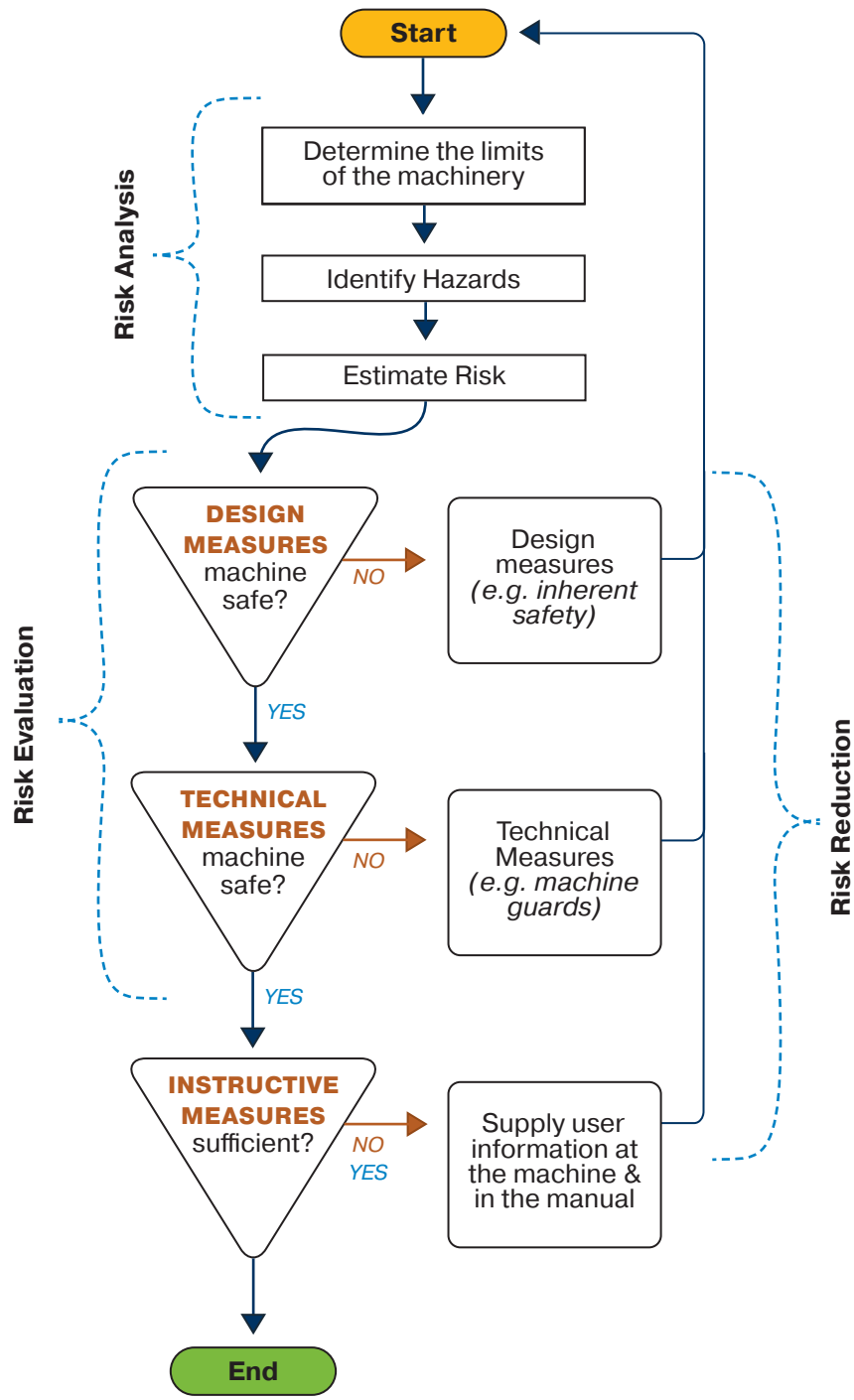
Risk assessment is a series of logical steps to enable the analysis and evaluation of the risks associated with a full or partial area of a piece of machinery and to take action if necessary to ensure risk reduction.

Risk Assessment Process:

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 or ANSI B11.0.



Risk Analysis

Determine the Limits of a Machine

The first step in conducting a risk assessment is the risk analysis.

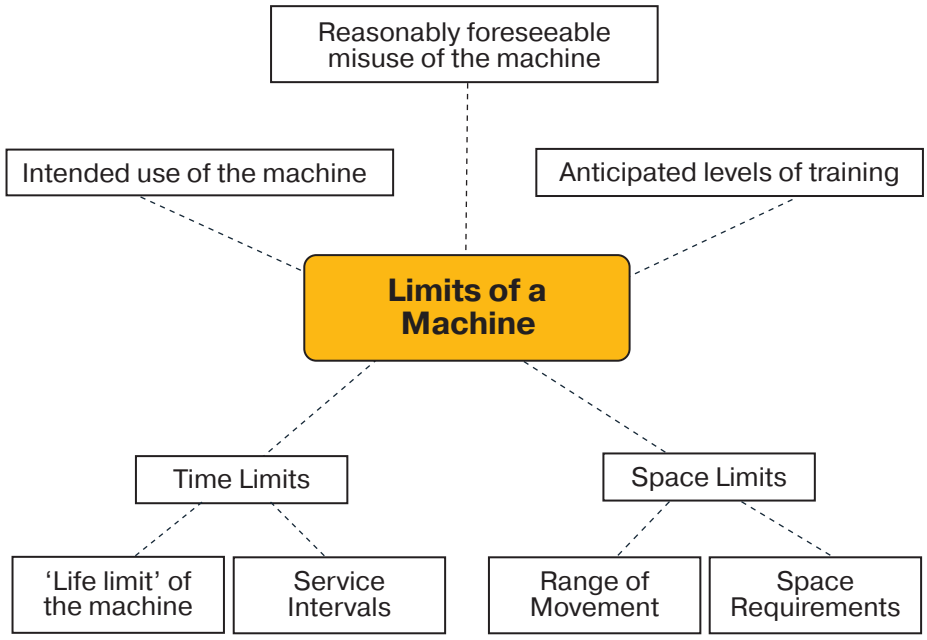
The risk analysis begins with determining the limits of the machinery.

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.*

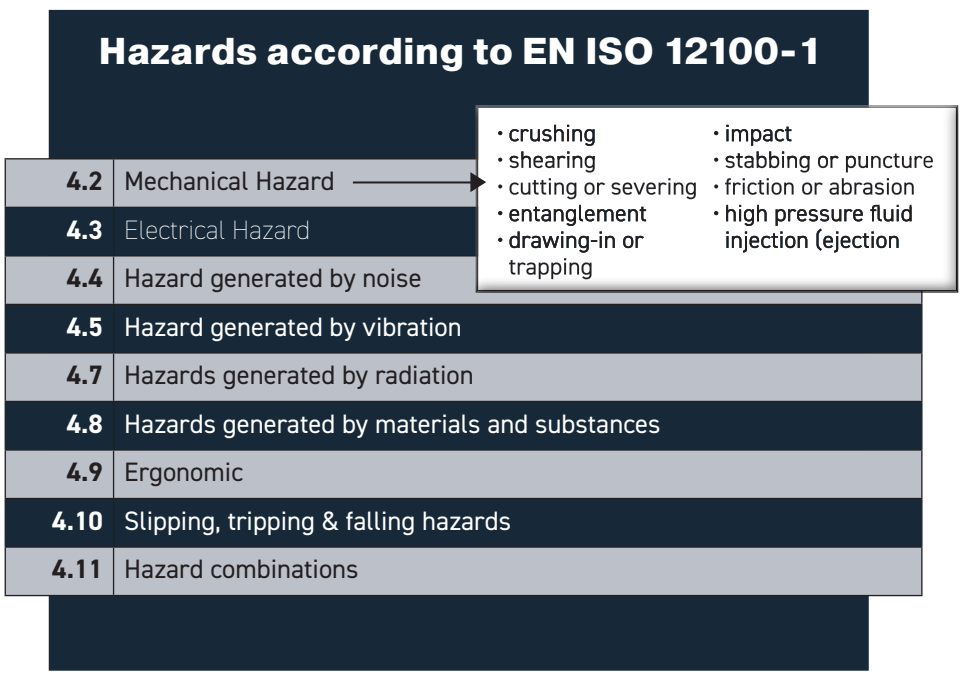
Identify Hazards

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.



Estimate Risk by 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 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**.

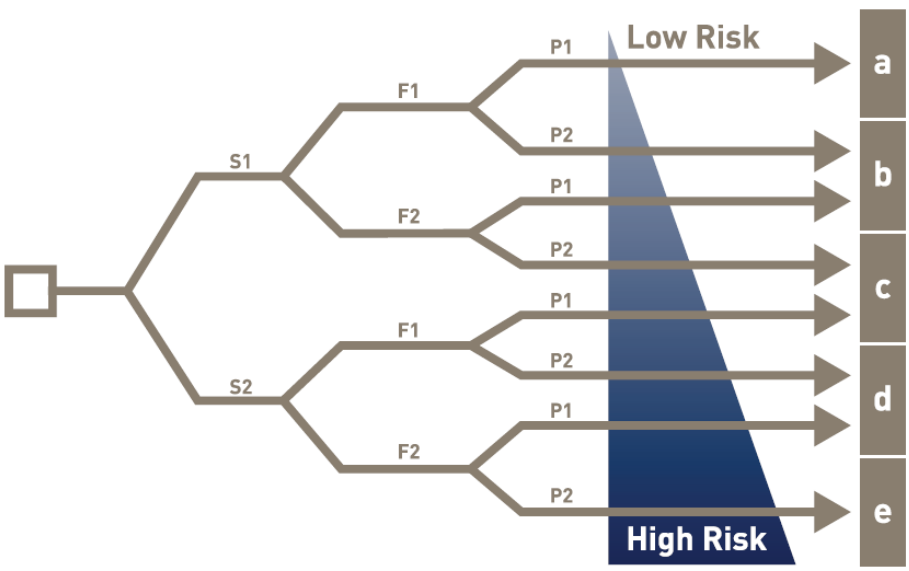
With PL a, the control functions contribution to risk reduction is low, while at PL e it is high due to greater inherent risk.

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



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.*

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.

Machinery should be risk assessed assuming no protective measures or barriers are in place.

Then, risk mitigation measures can be shown in the risk assessment. This ensurers potential hazards are not overlooked.

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.

Risk Mitigation Measures

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, the 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 ISO 13849 and 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.

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.

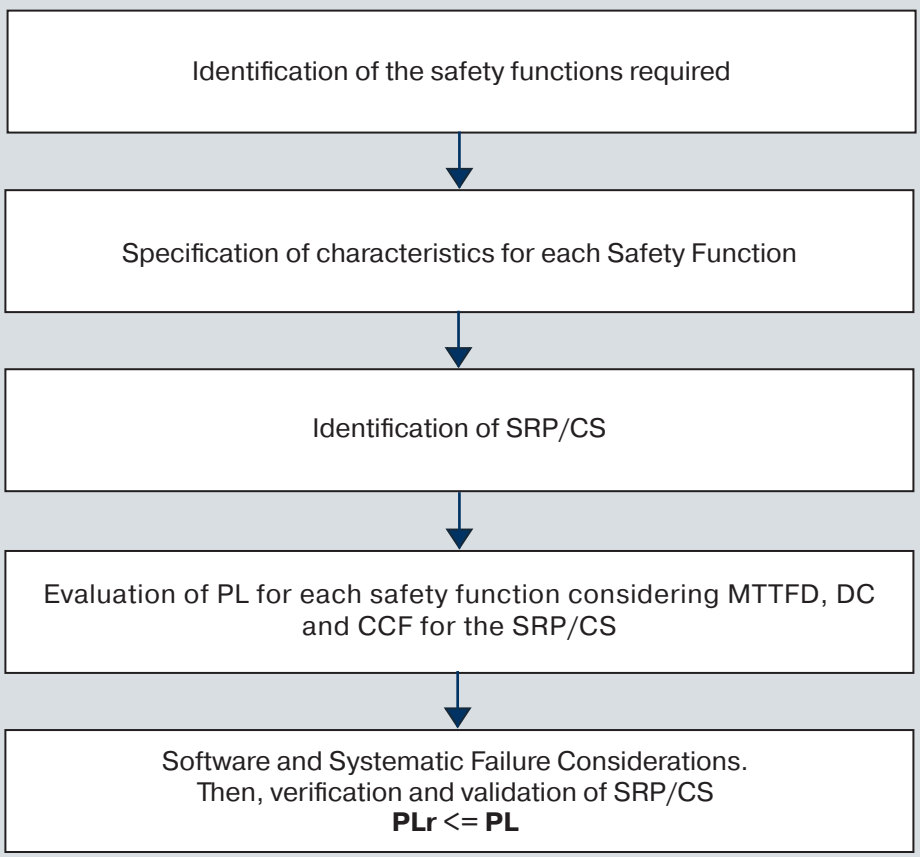
Risk Reduction

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, PLd, however, it is not uncommon to have different safety levels instituted in different zones of the machine where hazards may vary in severity.



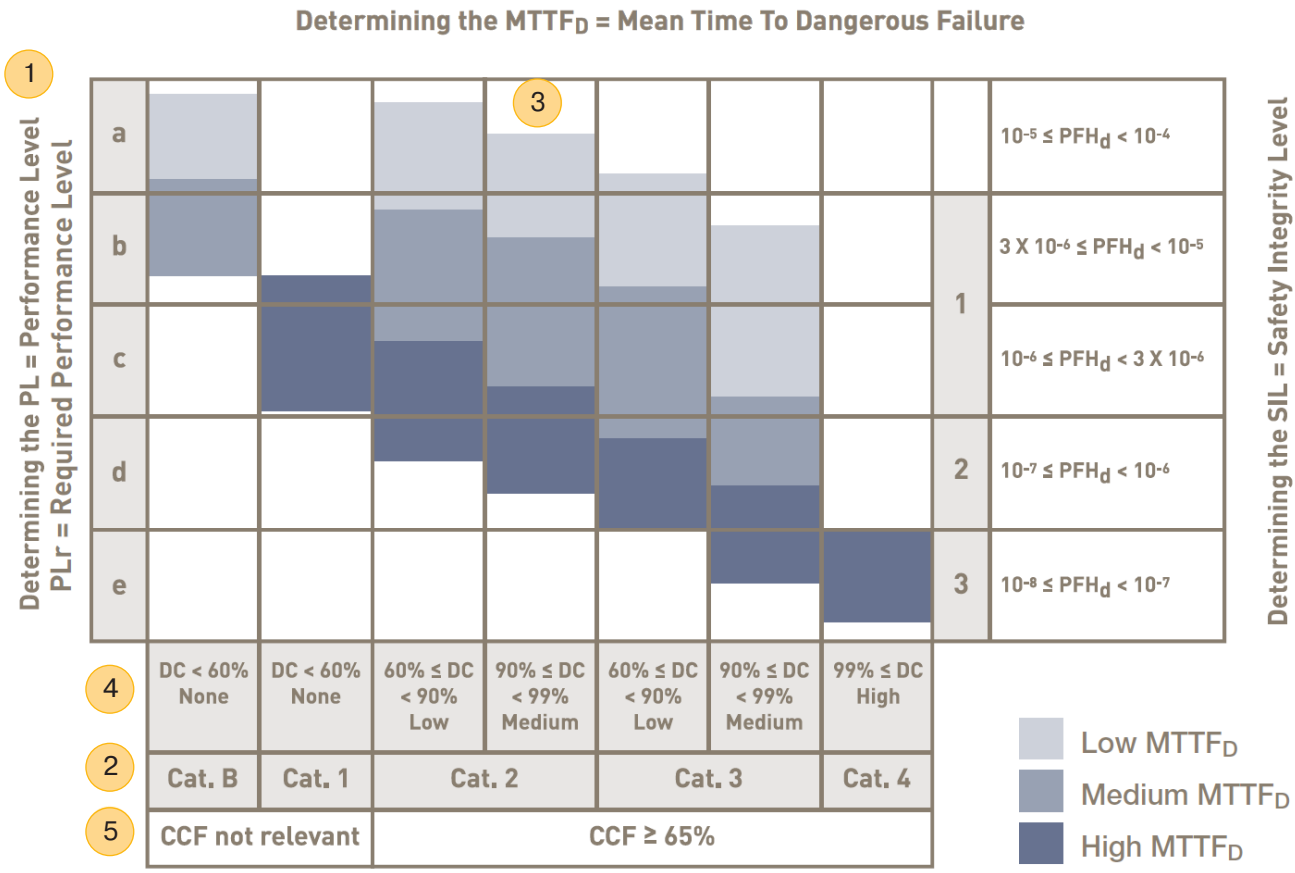
Determining Performance Level (PL)

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.

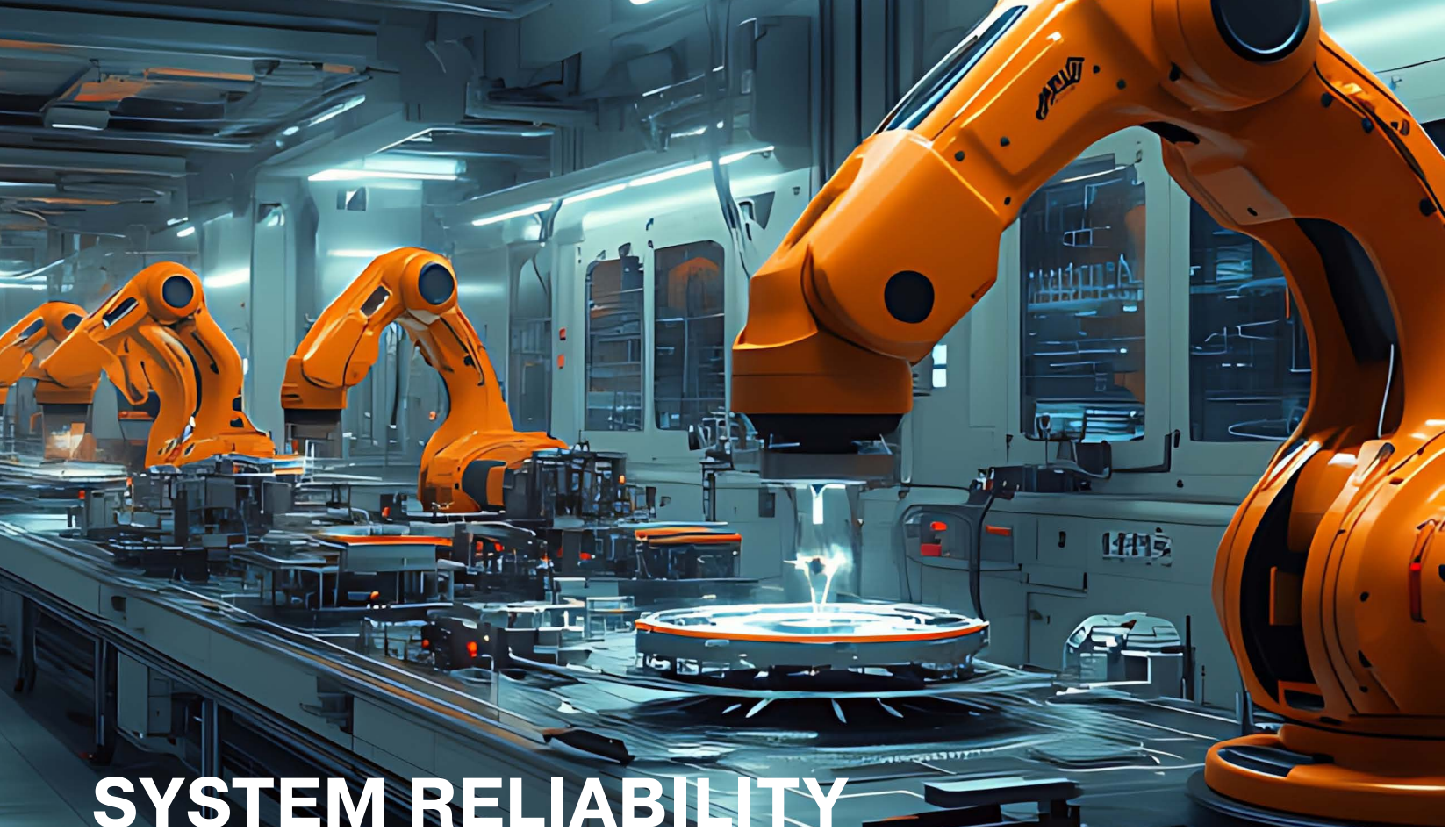
(2) This safety category will be based on a measure of diagnostic capabilities for the control system (DC), (4) the mean time to dangerous failure ($MTTF_D$), (3) and common cause failure (CCF) (5) which will define the safety levels of a given safety function.

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 ISO 13849 standards mandate 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.



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



SYSTEM RELIABILITY

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 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 pneumatic B10 values are available from our website:

https://discover.parker.com/PDN_B10-Datasheets

Mean Time to Dangerous Failure ($MTTF_D$)

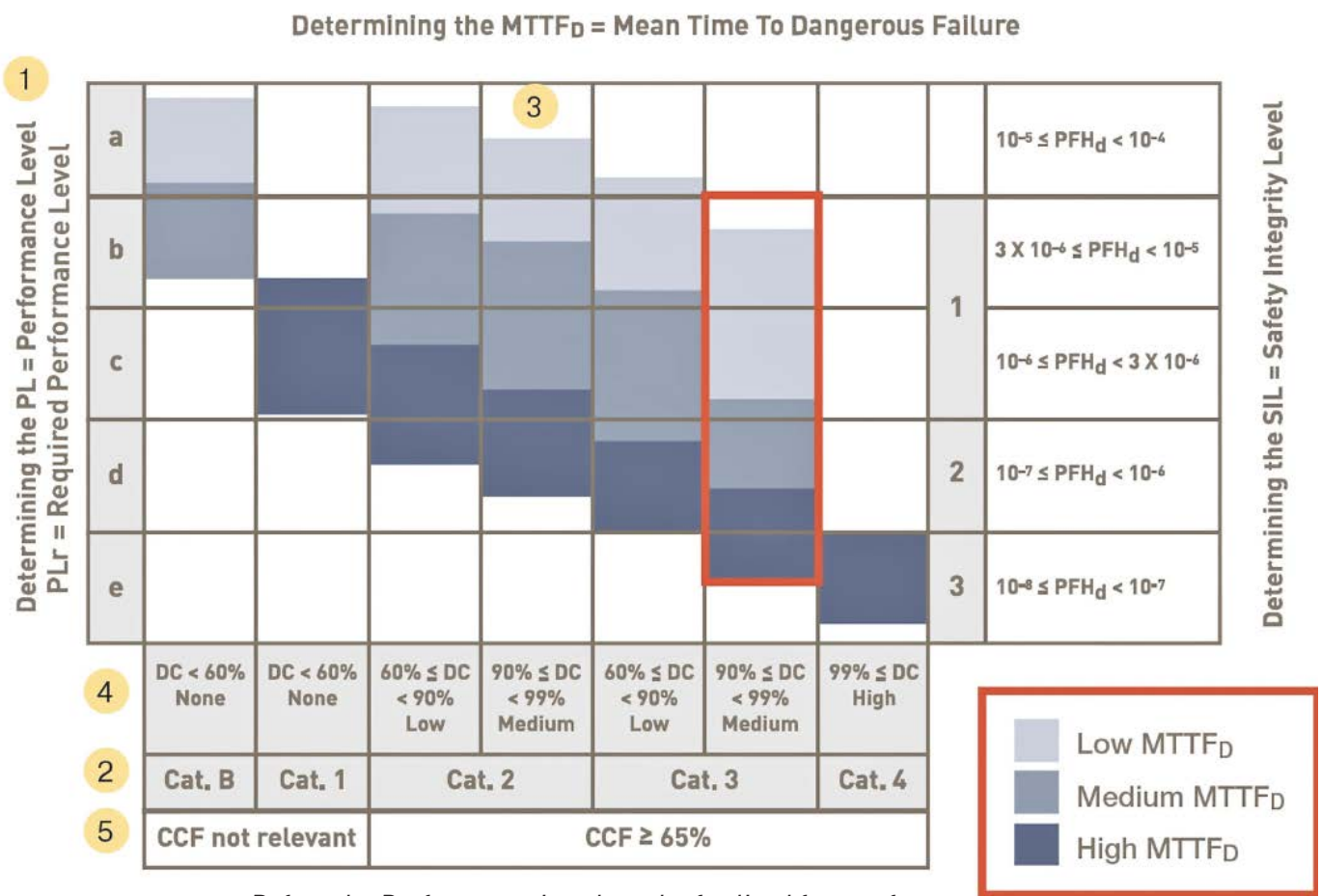
The reliability of a system has to be quantified as part of achieving a desired performance level (PL). Reliability is expressed as the Mean Time to Dangerous Failure ($MTTF_D$).

$MTTF_D$ 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 ISO 13849-1 there are three types of $MTTF_D$; low, medium and high.

Reliability:	$MTTF_D$:
None	DC < 60%
Low	60% < DC < 90%
Medium	90% < DC < 99%
High	99% < DC



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

Reliability of the system $MTTF_D$ is critical in system design to achieving the correct category and performance level. Refer to ISO 13849-1, annex K for more information.

Calculations:

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

$$MTTF_D = \frac{B10_D}{0.1 \times N_{op}}$$

To calculate the number of annual operations for the mechanical element:

$$N_{op} = \frac{D_{op} \times H_{op} \times 3600 s/h}{Tcycle}$$

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	seconds per cycle
$B10_D$	60,000,000	M (million) cycles
N_{op} =	2.16×10^6	cycles/year
$T10_D$ =	27.7	years
$MTTF_D$ =	277	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.

$$N_{op} = \frac{200\,days/year \times 15h/day \times 3600\,s/h}{5s/cycle}$$

$$T10_D = \frac{60 \times 10^6\,cycles}{2.16 \times 10^6\,cycles/year}$$

$$MTTF_D = \frac{27.7\,years}{0.1} = 277\,years$$

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 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:

$$DCavg = \frac{\frac{DC1}{MTTF_D 1} + \frac{DC2}{MTTF_D 2} + \frac{DC3}{MTTF_D 3} \quad (con't...)}{\frac{1}{MTTF_D 1} + \frac{1}{MTTF_D 2} + \frac{1}{MTTF_D 3} \quad (con't...)}$$

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

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

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

ARCHITECTURE

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 in machine safety.

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 = Input devices

L = Logic controllers

O = Outputs

^{i}m = means of interconnecting these components.

Controls Architecture | Single Channel

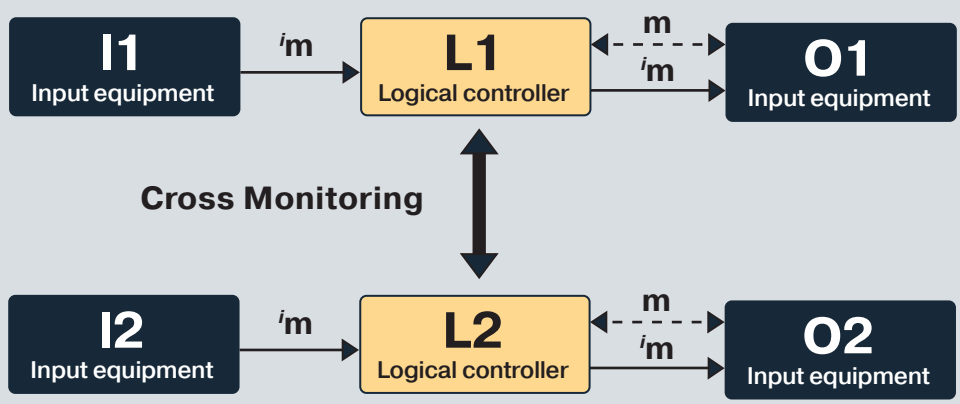
Single channel systems have a **single input device with a single interconnect means** to a logic controller which then connects to a single output device via a single interconnect.

A failure along this architecture will lead to the loss of the safety function.

Controls Architecture | Two Channel (Redundant)

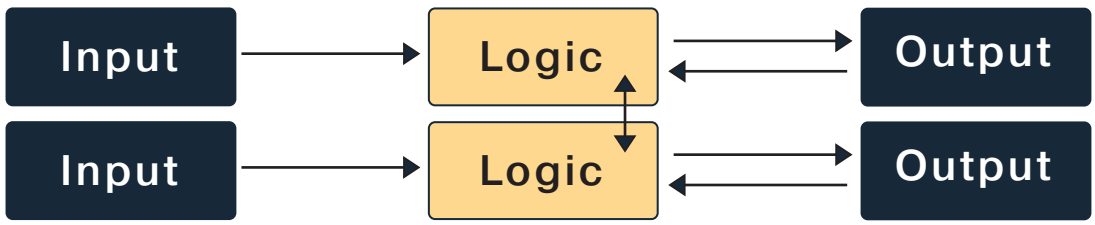
Input devices have a r**edundant interconnect means** to a **logical controller with redundant interconnect means to an output device.** The redundancy is referred to as **two channel architecture.**

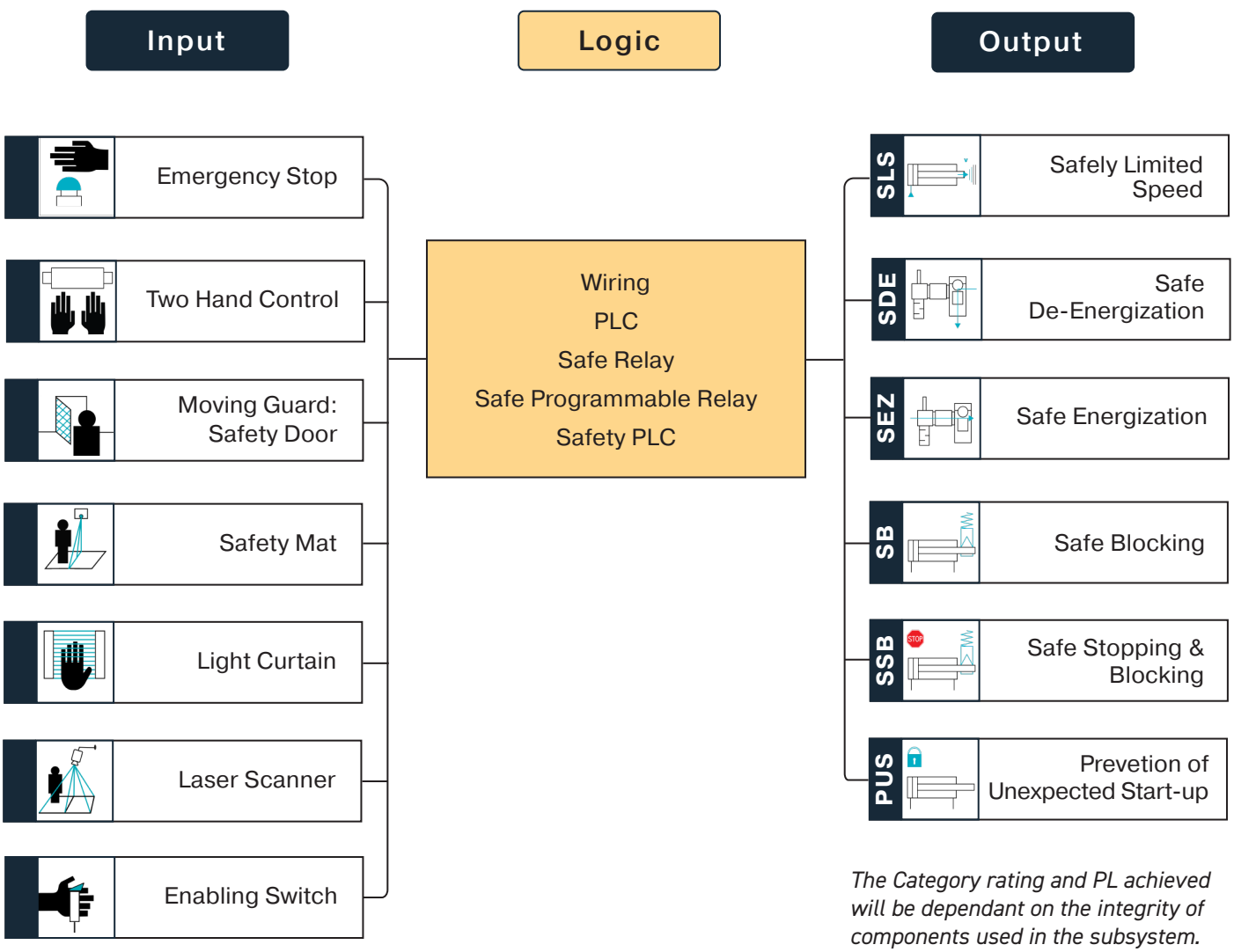
In addition to redundancy in design, **two channel systems require a robust means of logical controller** capable of monitoring between the logic device and the output equipment and also the ability to monitor internally to ensure proper function.



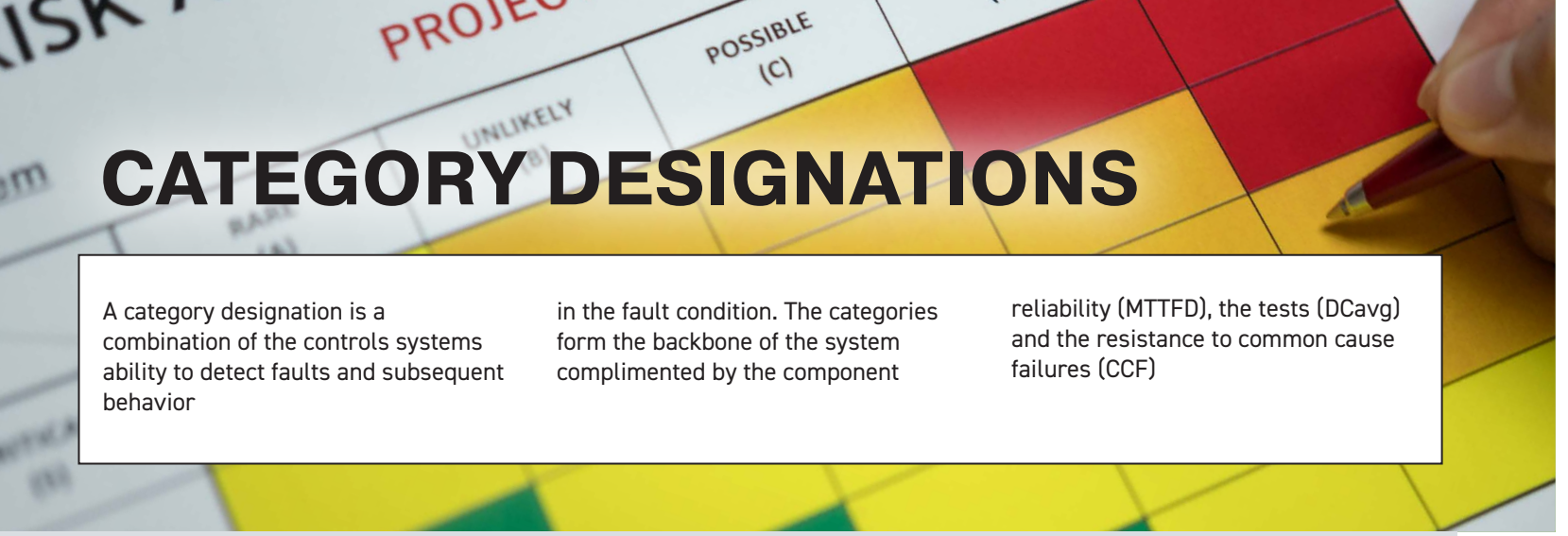
Machine Architecture

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.



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 (MTTFD), the tests (DCavg) and the resistance to common cause failures (CCF)

Category B

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, DCavg = none

Maximum PL = b

CCF, not relevant

I	Input Device
L	Logic
O	Output Device
^{i}m	Interconnecting Means

Category 1

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, DCavg = none

Maximum PL = c

CCF, not relevant

I	Input Device
L	Logic
O	Output Device
^{i}m	Interconnecting Means

Category 2

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 startup, 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.

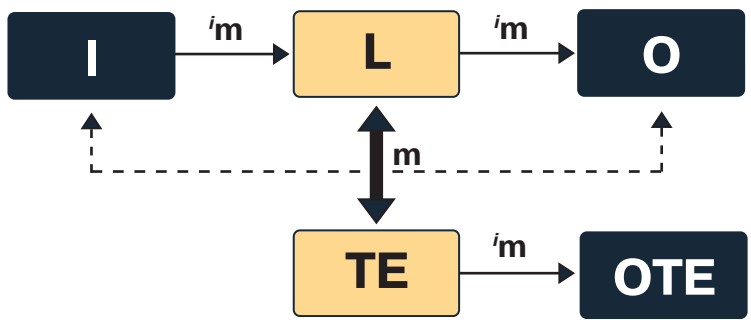
Component $MTTF_D$, low to high

Diagnostic Coverage, DCavg = low

Maximum PL = d

CCF, applicable

I	Input Device
L	Logic
O	Output Device
^{i}m	Interconnecting Means
TE	Test Equipment
OTE	Output of TE
m	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.

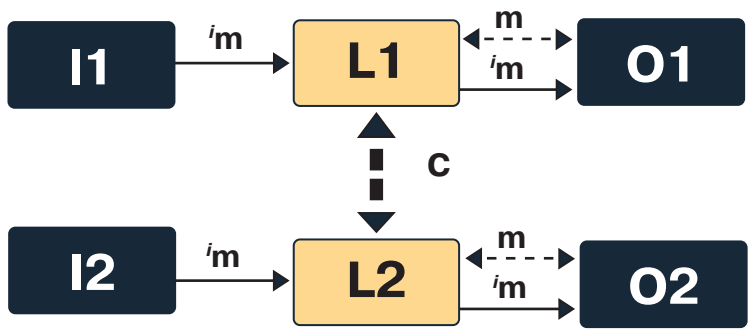
Component $MTTF_D$, low to high

Diagnostic Coverage, DCavg = low to medium

Maximum PL = e

CCF, applicable

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 4** shall be designed and constructed following relevant standards using well-tried safety principles.

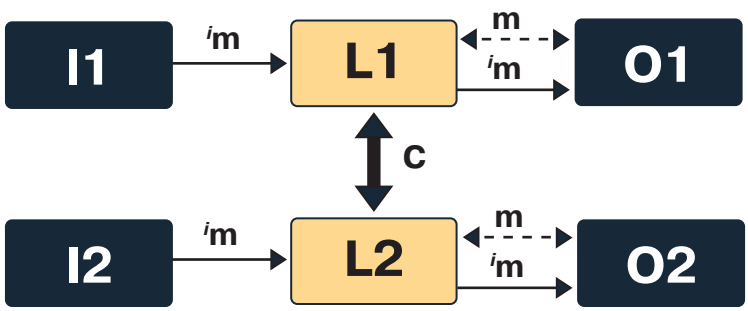
Component MTTFD, high

Diagnostic Coverage, DCavg = high

Maximum PL = e

CCF, applicable

I1, I2	Input Device
L1, L2	Logic
O1, O2	Output Device
^{i}m	Interconnecting Means
m	Monitoring
c	Cross Monitoring



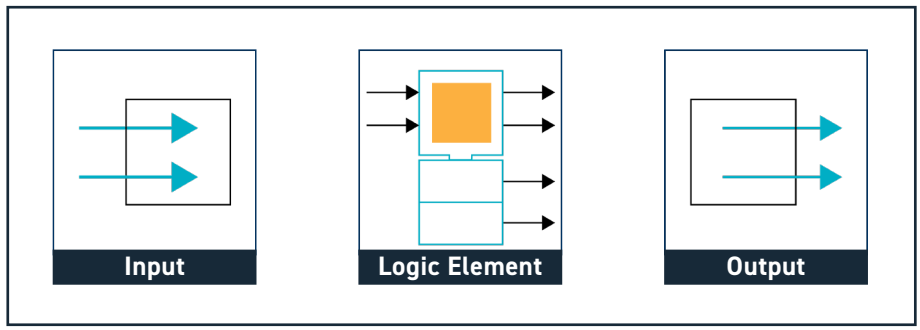
SAFE FUNCTIONS

Safe Functions

Ideally machine designers should **design out risk during risk assessment.** This task is not always possible due to the type of hazard, restrictions of the machine such as space, cost containment or simply the fact that it's an existing piece of equipment being retrofit.

When risk cannot be designed out machine designers turn to technical measures to ensure safety. The technical measures are usually the combination of an input device, logic controller and output device **(known as the safety chain)**.

SAFETY CHAIN



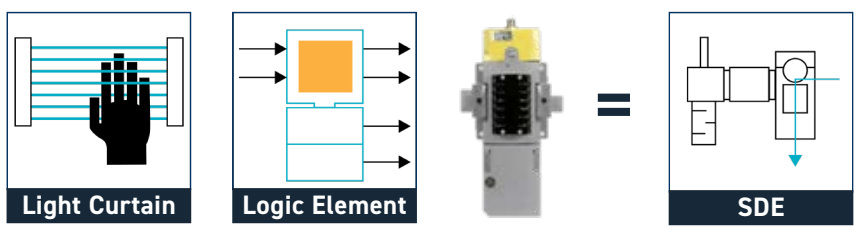
SRP/CS

These devices are known as the **safety related parts of the control system**, or **SRP/CS** for short. The combination of technical measures implemented result in a safe function.

Safe function is the **overall protective measure for risk reduction in machine design.** Various safe functions exist and can be used together in one safety circuit. For example, PUS and SEZ work will together to ensure prevention of unexpected start-up and safe energization.

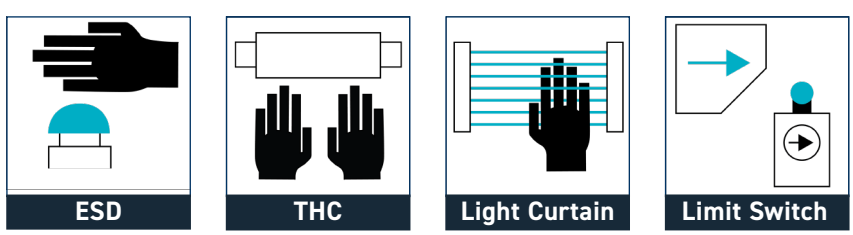
Inputs initiate a signal to the logic controller to perform a task. A two-hand control will initiate an input command that allows the machine to start. While an input signal from a light curtain will tell the machine to perform the output command such as exhausting air. The output device could be a safety exhaust valve, and the safe function achieved is safe de-energization

SAFE FUNCTION EXAMPLE



Safe de-energization

COMMON INPUT DEVICES

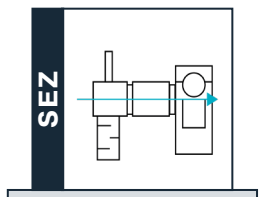


Emergency stop device

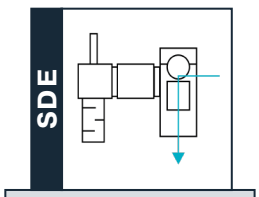
Two hand control

SAFETY SUB-FUNCTIONS

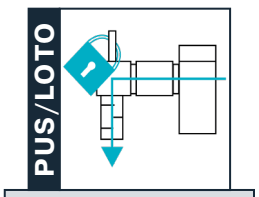
Start-up



Safe energization

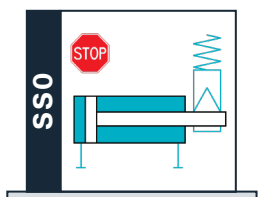


Safe de-energization

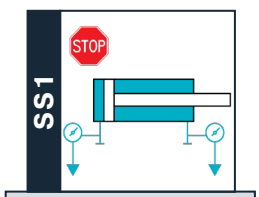


Prevention of unexpected start-up / lockout-tagout

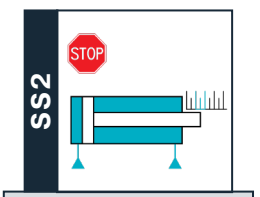
Stopping



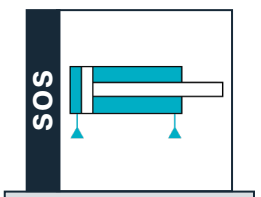
Safe stop (uncontrolled)



Safe stop (deceleration)

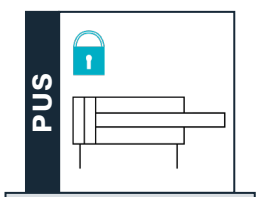


Safe stop (controlled with power)

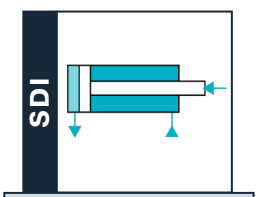


Safe operating stop

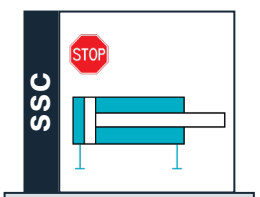
Actuators



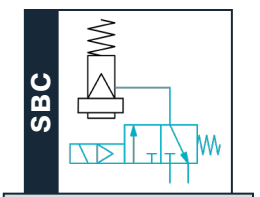
Prevention of unexpected start-up



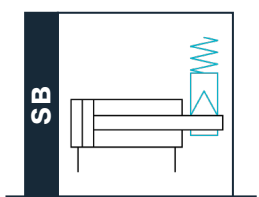
Safe direction



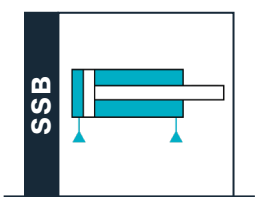
Safe stopping & closing



Safe brake control

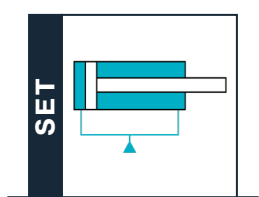


Safe blocking

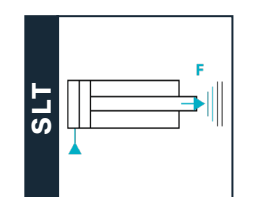


Safe stopping & blocking

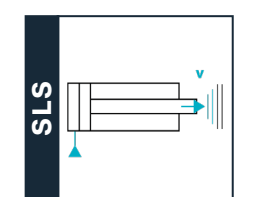
Monitoring Systems



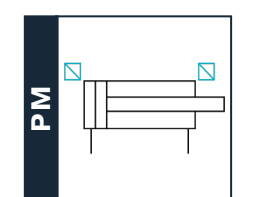
Safe equilibrium of torque



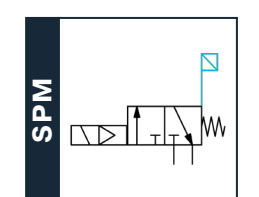
Safely limited torque (force)



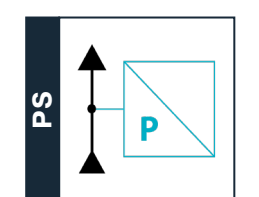
Safely limited speed



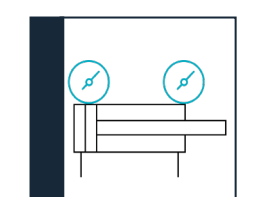
Position monitoring



Switch position monitoring



Pressure Switch

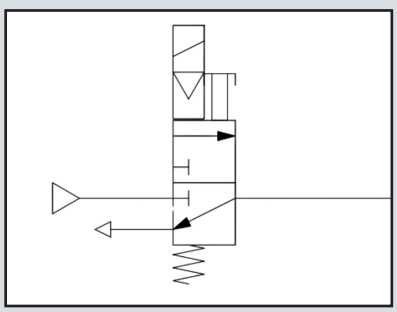

Pressure Monitoring

DESIGNING CIRCUITS WITH PNEUMATIC VALVES

The ability to monitor the safe state of the power switching component is essential in ensuring the safe function is met when incorporating pneumatic valves into system design.

These can be performed with an array of devices capable of providing diagnostic coverage feedback. (including but not limited to, limit switches, pressure sensors, flow sensors, level detection devices...)

Valve Selection:



Mechanical switching components with a specific normal position (such as spring return) **should have the safe state as the normal position.**

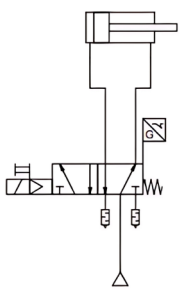
This can be blocked or open, depending on the safe function the designer hopes to achieve. The safety sub-function is then actuated in the normal position.

Spring assisted, single solenoid valves are often selected for safety circuits for **known return position.**

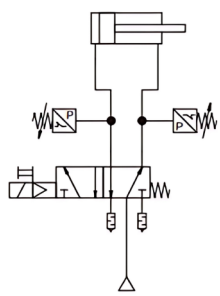
When using valves with no specific normal position (such as double solenoid valves), the possible safe state is the maintaining of the current switching position.

MONITORING

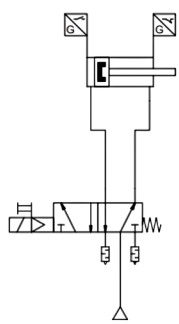
Direct monitoring can be done via the use of external pressure sensors, directly on the directional control valve.



Indirect monitoring can be accomplished indirectly to the directional control valve.



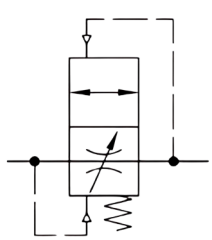
Indirect monitoring with switches monitored by the logic control system. Typically used for Cat 3 or Cat 4 applications where a high degree of diagnostic coverage is required for fault detection.



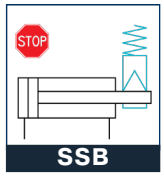
SOFT START

Soft-start functions provide a **controlled increase of downstream pressure** to prevent a rapid pressurization of a system.

Most often these are preset to a full flow set point (ie; 50% of working pressure) or come adjustable on a device.

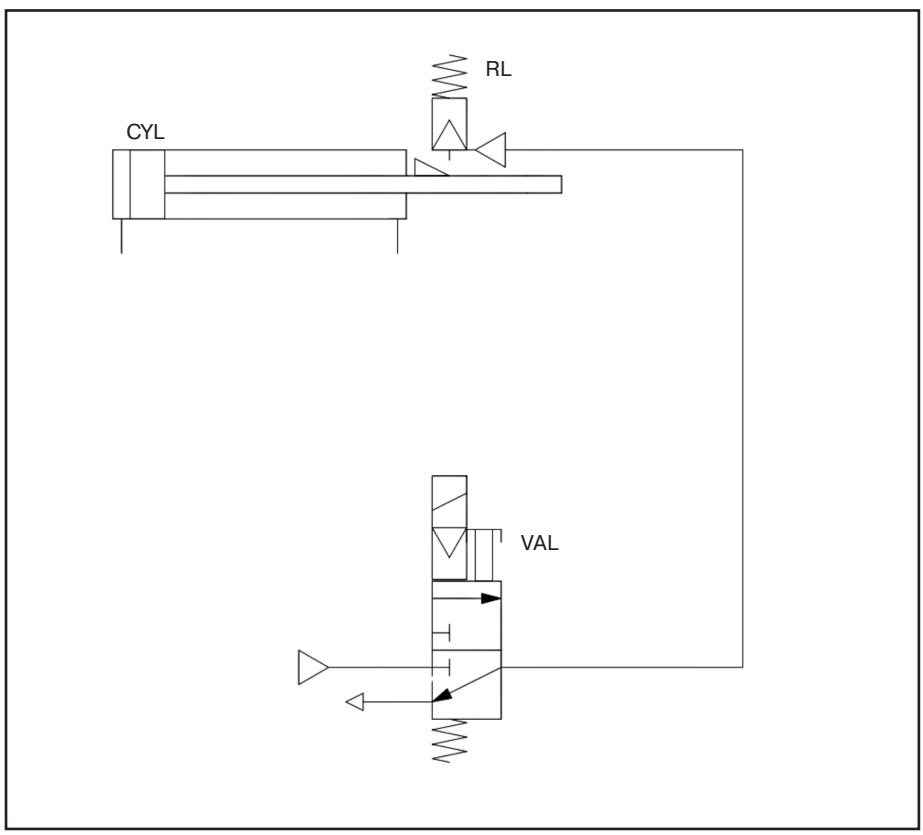


SAFE STOPPING & BLOCKING



Safe stopping & blocking (SSB) is achieved when a pneumatic drive is stopped in a safe way and the free movability of the piston & rod assembly is blocked.

Blocking can take place by means of positive locking or frictional locking. A common method of holding de-energized circuits is the use of a rod lock on a cylinder. This prevents the rod from drifting or unexpected movement during re-energization of the circuit. Pneumatic cylinders are often designed with 3/2 valves to hold the last position.



Trapped energy holding a load will move with leakage in the system.

A risk assessment is used to evaluate if a hazard is posed and what secondary means would be best to prevent movement.

Rod locks are also implemented as a secondary means of holding an energized cylinder rod in place when depletion of energy would create an unsafe state.

The preferred method of stopping the output device is static braking as dynamic braking (during motion) can cause excessive premature wear and damage to both the locking mechanism and the output device.

Parker pneumatics offer a safety certified solution for frictional locking of the 4MA cylinder rod assembly.

Product Examples:

4MAP (cylinder plus rod lock combination).

The cylinder and lock can be configured for Cat 1 to Cat 4 safety circuits using for safety switching tasks or static emergency holding.

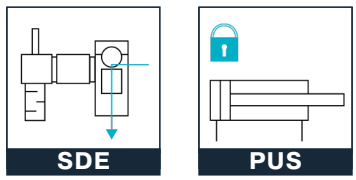
4MAP Cylinder & Rod Lock

P2LCZ Viking Valve

Component	Component Type
CYL	Cylinder
RL	Rod Lock
VAL	3 Way NC Valve

The circuits and procedure described are recommendations only and do not exclude other possibilities. For the complete safety function, other safety related control components must be added as subsystems such as input and logic devices. Devices used must meet the DC, CCF and rated endurance values required by the category the designer wishes to achieve. Manufacturer supplied B10d values help in the calculation of the MTTFd. The safe functions are defined by VDMA 24584.

SAFE DE-ENERGIZATION



This circuit allows safe exhaust (SDE) of the system via two exhausting valves (dual channel).

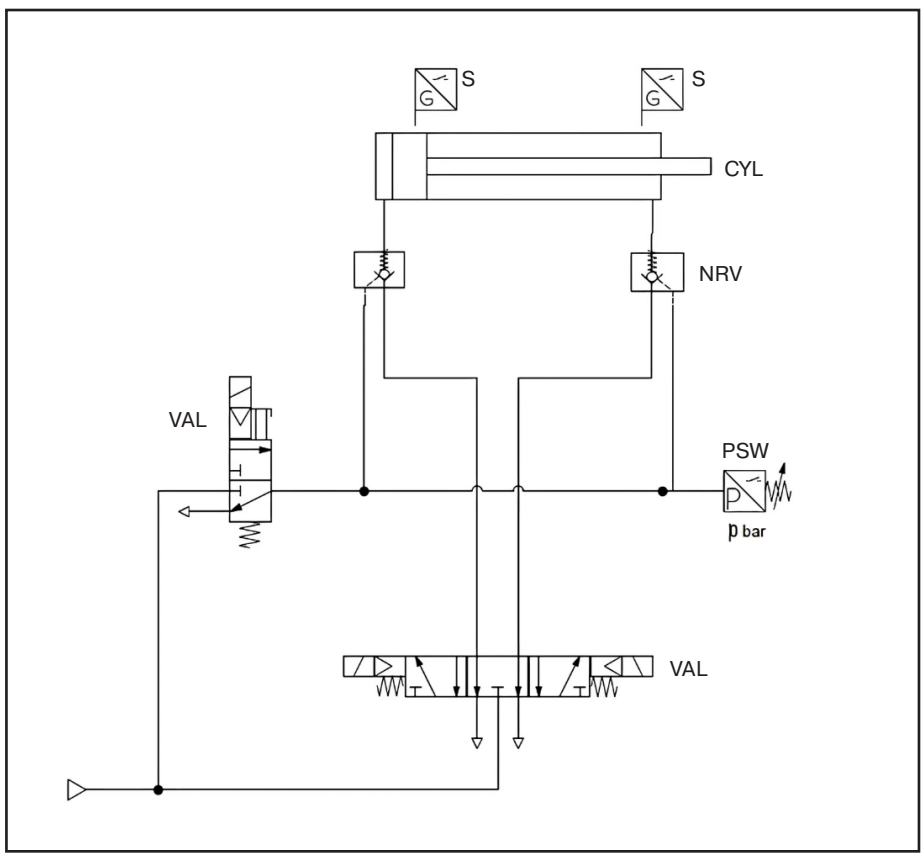
Cylinder function is only possible with the combined actuation of both valves. It is important to note that this system provides redundancy in the valves and the failure of one of the valves does not prevent exhaust of the system thereby jeopardizing safe function.

The safety-related switching position is achieved by removing the electrical signal.

In the event of a failure, the non-return valves must be engineered to assume an open state to safely exhaust the cylinder.

It is also important to consider the minimum opening pressure of the non-return valves to overcome spring forces.

The cylinder switching valve functions can be monitored by querying the cylinder position switches and the pressure switch.



Component	Component Type
CYL	Cylinder
S	Sensor
NRV	Non-Return Valve
PSW	Pressure Switch
VAL	Valve 1
VAL	Valve 2

Product Examples:

Pressure Sensor SCPSD

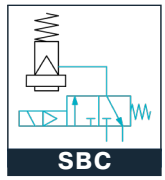
4MA Cylinder

Viking Lite

CPS Sensor

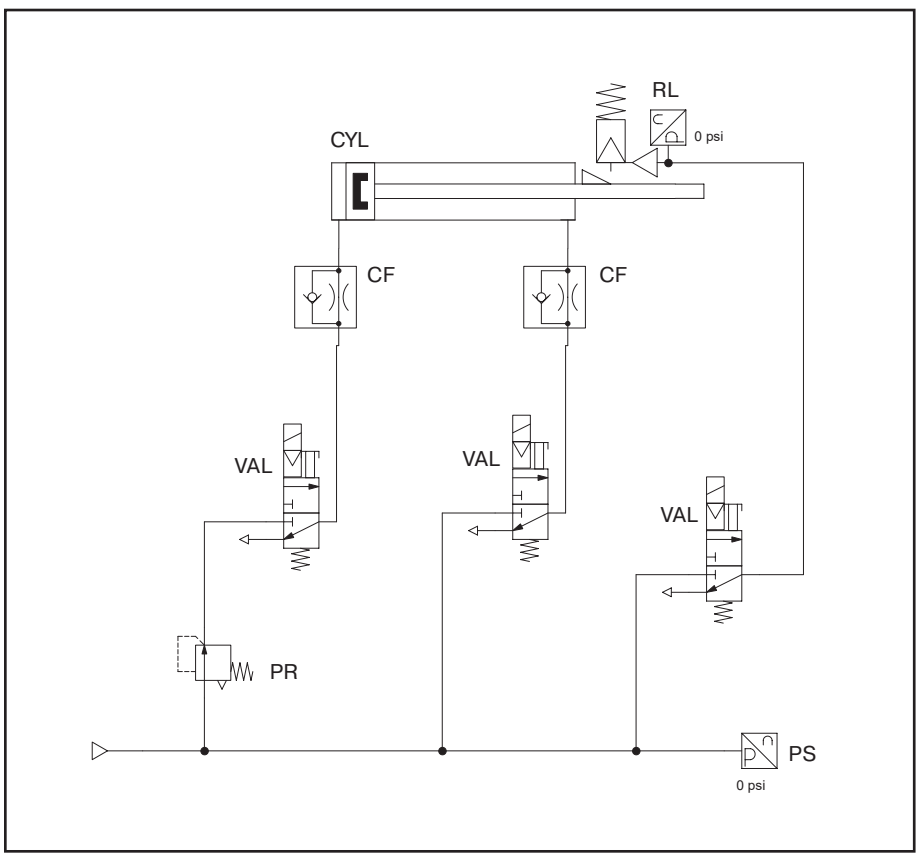
The circuits and procedure described are recommendations only and do not exclude other possibilities. For the complete safety function, other safety related control components must be added as subsystems such as input and logic devices. Devices used must meet the DC, CCF and rated endurance values required by the category the designer wishes to achieve. Manufacturer supplied B10d values help in the calculation of the MTTFd values. The safe functions are defined by VDMA 24584.

SAFE BRAKING CONTROL



The simple circuit for safe braking control allows a cylinder to be held in position via a locking device with valves normally closed in the starting position.

Redundancies in the circuit shown allow its suitable for up to Cat 3 pl d in accordance with ISO 13849-1 for the safe braking control (SBC) to prevent unexpected movement of machine. Safety sub-functions SB (safe blocking) and SSB (safe stopping and blocking) are mechanical safety sub-functions and are usually combined with safety sub-function SBC.



Safe pneumatic braking control relies on implementing safety measures in pneumatic systems, ensuring brakes can safely decelerate or hold loads, even in the event of a failure.

Proper control system design and validation should ensure that spring-applied safety brakes (normally engaged when de-energized) are released by sufficient pneumatic pressure, ensuring a fail-safe mechanism where the brakes engage automatically if pneumatic pressure is lost or drops significantly due to leakage.

Product Examples:

4MAP

Viking Extreme

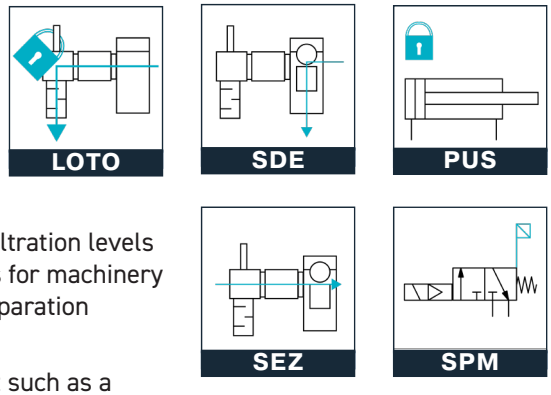
Pressure Regulator

Pressure Sensor SCPSD

Component	Component Type
VAL	Valve
CYL	Cylinder
CF	Check Valve Flow Control
PR	Pressure Regulator
PS	Pressure Sensor
RL	Rod Lock

The circuits and procedure described are recommendations only and do not exclude other possibilities. For the complete safety function, other safety related control components must be added as subsystems such as input and logic devices. Devices used must meet the DC, CCF and rated endurance values required by the category the designer wishes to achieve. Manufacturer supplied B10d values help in the calculation of the MTTFd values. The safe functions are defined by VDMA 24584 (exception SB).

SAFE PRESSURIZATION



Pneumatics require clean dry air and use air preparation to ensure proper filtration levels are met while proper pressure is directed through the circuit. Requirements for machinery safety and functional safety can be implemented when designing the air preparation system.

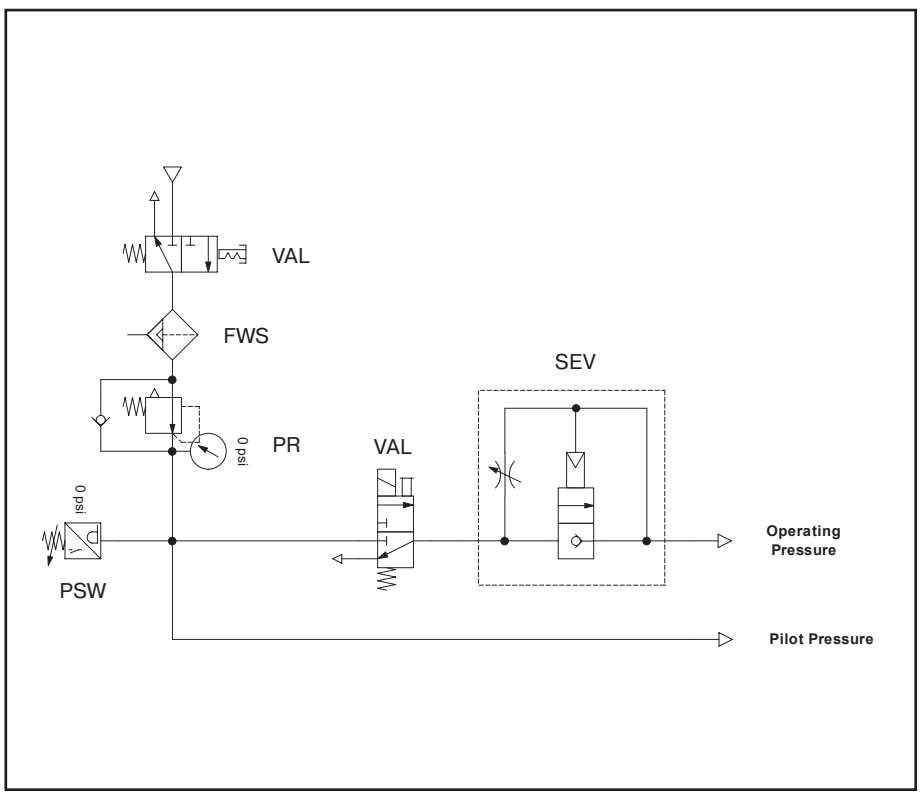
Safe energization is achieved by using a defined time function in the product such as a soft start device. Safe de-energization allows the downstream components to be safely de-energized and disconnected if necessary. Prevention of unexpected start up can be achieved by removing power when a controlled stop is triggered, or a fault is detected (via monitoring system).

Further, the prevention of unexcepted start-up (PUS) function prevents the control valve from functioning and leading to unexpected start-up of a machine.

Lock out tag out is offered on many devices via manual/mechanical intervention to ensure a start function is not enabled.

Pneumatic pressure sensors monitor the physical changes in pressure. Their pinpoint measurements are converted into electric signals, which are displayed as usable data for interpretation.

Monitoring these signals allows them to be controlled by electronic devices such as PLCs and tablets.



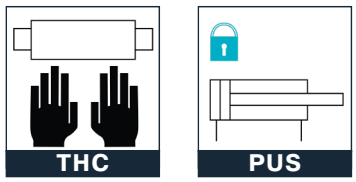
Component	Component Type
VAL	Valve
PSW	Pressure Switch
FWS	Filter with Water Seperator
PR	Pressure Regulator
SEV	Safety Exhaust Valve

Product Examples:

Filter *Regulator* *Filter/Regulator* *Safety Valve* *Pressure Sensor SCPSD*

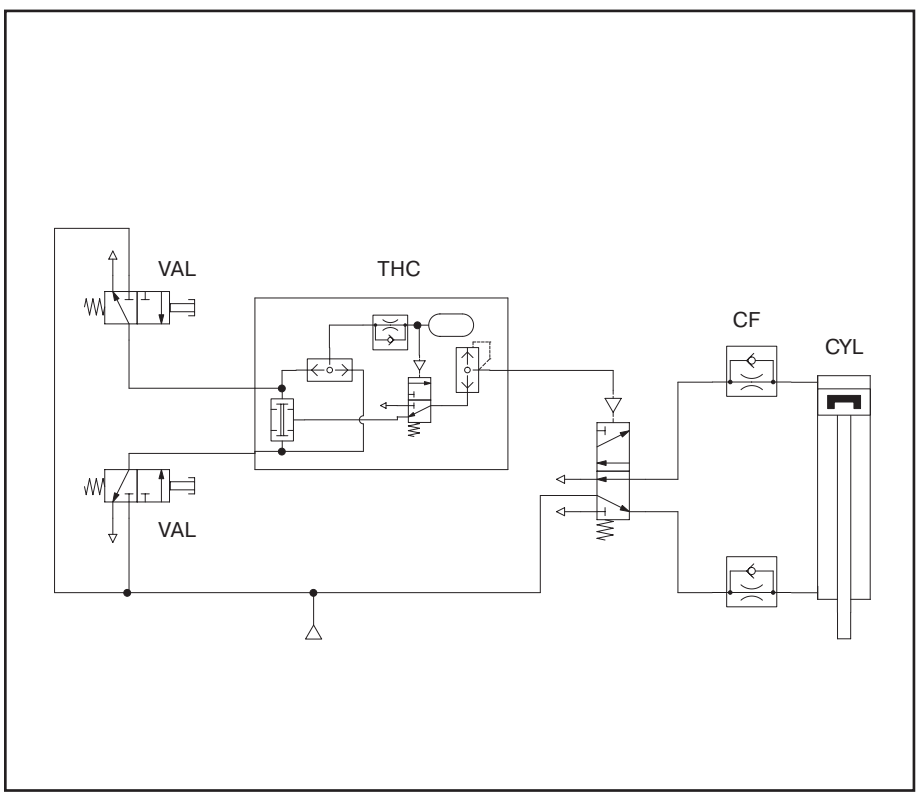
The circuits and procedure described are recommendations only and do not exclude other possibilities. For the complete safety function, other safety related control components must be added as subsystems such as input and logic devices. Devices used must meet the DC, CCF and rated endurance values required by the category the designer wishes to achieve. Manufacturer supplied B10d values help in the calculation of the MTTFd values. The safe functions are defined by VDMA 24584.

TWO-HAND OPERATION



Two hand operation (THC) ensures a worker is not present in the functional part of the machine during operation by requiring both hands to energize the circuit. PUS is prevention of unexpected start-up. The two hand control modules are used in applications that require the operator's hands to be occupied before a pneumatic signal is sent in an automation system.

The two hand control module provides a pneumatic output signal if both push buttons are simultaneously operated within 0.5 seconds or less of each other, and will remain only if both push buttons remain in the depressed condition. The output signal will not be sent in the event that the second push button is operated more than 0.5 seconds after the first push button.



There are several ways to achieve prevention of unexpected start-up (PUS) in machine design.

While two hand controls are an excellent operators control mechanism other solutions are also available such as safety valves.

Safety valves with redundancy are monitored and require a minimum operating pressure and redundant electrical signals before allowing a machine to fill with compressed air.

Product Examples:

Two Hand Control

Regulator

Safety Exhaust Valve

Viking Lite Valve

Component	Component Type
THC	Two Hand Control
CYL	Cylinder
VAL	Valve
CF	Check Valve Flow Control

The circuits and procedure described are recommendations only and do not exclude other possibilities. For the complete safety function, other safety related control components must be added as subsystems such as input and logic devices. Devices used must meet the DC, CCF and rated endurance values required by the category the designer wishes to achieve. Manufacturer supplied B10d values help in the calculation of the MTTFd values. The safe functions are defined by VDMA 24584.

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

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 B10D value. This will increase your MTTFD.

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 (MTTFD) 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?

Yes, if you are shipping into the European union must follow the legislation for the country in which the equipment will reside.

If you are not shipping into Europe, then you must follow the local laws and standards for the respective region.

You may find local laws and standards align closely to those of the EU and may be less stringent.

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.

GLOSSARY OF TERMS

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

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

B10d
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 taken to eliminate hazards

Diagnostic Coverage
The measure of a system's ability to detect failures or, Ratio of dangerous detected failures to the total number of dangerous failures expressed as a percentage.

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

Fault
Inability to perform a required function in a components normal state

FB
Function block

FIT
Failure in time

FIT
Fault injection testing

Fixed guard
A guard secured to provide protection that is not easily removed

Guard
A physical barrier installed to provide protection

HARA
Hazards analysis risk assessment

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

HFT
Hardware fault tolerance – ability of SRP/CS to continue to perform a required function in the presence of faults or failures.

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

im
Interconnecting means

Impeding device
A device that creates an obstruction (such as a rail or barrier)

Instruction measures
To identify and label the hazard

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 SRECS 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

Lambda (λ)
Rate of failures (failure rate), λS is the rate of safe failure, λD is the rate of dangerous failures.

Limiting device
Device that prevents a hazardous condition based on a machines operating variables

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 TM
Intended usage period after which the product has to be replaced

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

MTTFd
Mean time to dangerous failure

MTTR
Mean time to repair

nop
Number of operations (annually)

O, O1, O2
Output devices

OTE
Output on test equipment

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

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

Proof test
A form of stress test to demonstrate the fitness of a structure

Protective measures
A measure taken to provide protection from a hazard

RDF
Ratio of dangerous failures

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 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
Determining the severity of risk

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-related part of a control system
Part of a control system that responds to safety-related input signals and generates safety-related output signals

Sensitive protective equipment
Equipment capable of detecting persons or parts and able to generate a signal for the CS

SFF
Safe failure fraction

Significant hazard
A hazard requiring specific action to remedy it

SIL
Safety integrity level

SILCL
Maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity

SPE
Sensitive protective equipment

SRCF
Safety-related control function

SRECS
Safety-related electrical control system

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

Subsystem
A self-contained system within a larger system

Subsystem Element
An individual component from an SRP/CS

Systematic failure
Failure related to a certain cause in the design, manufacturing or other factors

T1
Proof test interval or lifetime, whichever is the smaller

T2
Diagnostic test interval

T10d
Mean time until 10% of components fail dangerously

TE
Test equipment

TM
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

Usability
The ease of understanding the function of a machine or its controls

ISO
International Standards Organization

Parker Hannifin Corporation
Pneumatic Division NA
8676 E. M89
Richland, MI USA
phone 269 629 5000
www.parker.com