

# Machinery Directive Overview

ISO 13849-1

Catalogue PDE2650TCUK May 2014

aerospace  
climate control  
electromechanical  
filtration  
fluid & gas handling  
hydraulics  
**pneumatics**  
process control  
sealing & shielding



ENGINEERING YOUR SUCCESS.

[www.comoso.com](http://www.comoso.com)

<b>1.</b>	<b>About this document</b> .....	3
<b>2.</b>	<b>Theory and background</b> .....	4
2.1.	Why must machinery meet these requirements? .....	4
2.2.	Safety and functional safety .....	5
<b>3.</b>	<b>Machinery Directive</b> .....	6
<b>4.</b>	<b>How do the new safety standards differ from EN954-1</b> .....	7
4.1.	BS EN ISO 13849-1: Safety related parts of control systems, Part 1: general principles for design .....	8
4.2.	BS EN 62061: "Functional safety of safety-related electrical, electronic and programmable electronic control systems". .	9
<b>5.</b>	<b>New Approach</b> .....	10
<b>6.</b>	<b>European Harmonised Standards</b> .....	11
6.1.	Hierarchy of the European harmonised standards system .....	11
<b>7.</b>	<b>Changes in the new Machinery Directive</b> .....	12
7.1.	Changes in how conformity is evaluated for dangerous machines listed in the Machinery Directive Annex IV. ....	12
7.2.	Changes in the Essential Health and Safety Requirements that are presented in the Machinery Directive's Annex I. ....	12
7.3.	Changes in proving the safety of different products. ....	12
7.4.	Introduction of the term 'Partly completed machinery'. ....	12
7.4.1.	Partially completed pneumatic machinery .....	13
7.4.2.	Pneumatic components .....	13
7.5.	Changes to the Low Voltage Directive. ....	13
7.7.	Changes in the hazard analysis. ....	13
7.8.	Changes in production control. ....	13
<b>8.</b>	<b>Categories of EN ISO 13849-1</b> .....	14
<b>9.</b>	<b>Step Method of Risk Reduction</b> .....	16
9.1.	Step 1: The limits (ISO 14121-1 paragraph 5) .....	16
9.2.	Step 2: Hazard identification .....	16
9.3.	Step 3: Risk estimation .....	16
9.4.	Step 4: Risk evaluation .....	18
9.5.	Step 5 – Risk Reduction - (ISO 12100-2 clause 4) .....	20
9.6.	Step 6 – Protective device risk reduction - (ISO 12100-2 clause 5) .....	20
9.7.	Step 7 – Information to the user .....	20
<b>10.</b>	<b>Calculations</b> .....	21
<b>11.</b>	<b>Validation tools for pneumatic systems</b> .....	23
<b>12.</b>	<b>Abbreviation Glossary</b> .....	24

## Table of figures

<b>Figure 1</b>	Transition period from old to new standards .....	10
<b>Figure 2</b>	Hierarchy of European Standards .....	11
<b>Figure 3</b>	Risk reduction process .....	15
<b>Figure 4</b>	Risk Elimination .....	17
<b>Figure 5</b>	Relationship between PL and SIL .....	18
<b>Figure 6</b>	Risk evaluation process .....	19

**This brochure is to be used only by machine builders with technical understanding and with reference to the complete Machine Directives. It is to be used only as a reference to assist in understanding the Machine Directives. If there is a conflict or question, the User should follow their own interpretation of the Machine Directives or seek expert advice to resolve the conflict or question. Under no circumstance should a User rely on this document alone to attempt to comply with the Machine Directives. If the User is analyzing legal risk or legal implications of the Machine Directives, then a lawyer must be consulted.**



**FAILURE OR IMPROPER SELECTION OR IMPROPER USE OF THE PRODUCTS AND/OR SYSTEMS DESCRIBED HEREIN OR RELATED ITEMS CAN CAUSE DEATH, PERSONAL INJURY AND PROPERTY DAMAGE.**

This document and other information from Parker Hannifin Corporation, its subsidiaries and authorized distributors provide product and/or system options for further investigation by users having technical expertise. It is important that you analyze all aspects of your application and review the information concerning the product or system in the current product catalog. Due to the variety of operating conditions and applications for these products or systems, the user, through its own analysis and testing, is solely responsible for making the final selection of the products and systems and assuring that all performance, safety and warning requirements of the application are met. The products described herein, including without limitation, product features, specifications, designs, availability and pricing, are subject to change by Parker Hannifin Corporation and its subsidiaries at any time without notice.

## SALE CONDITIONS

The items described in this document are available for sale by Parker Hannifin Corporation, its subsidiaries or its authorized distributors. Any sale contract entered into by Parker will be governed by the provisions stated in Parker's standard terms and conditions of sale (copy available upon request).

# 1. About this document

This document provides an overview of the Machinery Directive and the associated standards that must be taken into account when designing a machine incorporating pneumatic components, to ensure operational safety.

The aim of the document is to explain, in general terms, the principles of risk assessments and reliability determination, to meet the requirements of the Machinery Directive. Document EN 13849-1 will be referenced throughout and comparisons will be drawn with IEC 62061, the standard for '*Functional safety of safety-related electrical, electronic and programmable electronic control systems*'.

## This document introduces:

- The idea behind functional safety and how to comply with the Machinery Directive; it also presents the changes in the new Machinery Directive and explains the hierarchy of the European harmonised standards system.
- The way in which the new Machinery Directive and related standards are replacing the old standards. It also introduces the two standard systems and lists a number of safety relevant standards and safety functions.
- An overview of the seven steps that assist in the risk assessment process, to meet the essential requirements of the Machinery Directive.

### **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.***



## 2. Theory and background



Health and safety is taken as an inherent right for citizens throughout the European Union (EU). As such, it is enshrined in legislation at both a national and international level, with implementation of appropriate protocols being governed by a host of guidelines and directives.

For example, the design, manufacture and operation of machinery is covered by what are known as Essential Health and Safety Requirements (EHSR). Compliance with these requirements is essential before a machine or product can be brought to market or put into use within the EU.

Similarly, the new Machinery Directive 2006/42/EC (formerly 98/37/EC), now encapsulates EHSR, harmonising the health and safety requirements applicable to machinery across the EU, without adversely affecting free market conditions.

This effectively creates an environment where machinery can be produced, sold and used anywhere in Europe, with the assurance that it complies with a consistent and high standard of safety. In addition, the same standards are recognised in many regions outside Europe, thereby facilitating machinery trade and shipments around the world.

### 2.1. Why must machinery meet these requirements?



By complying with the Directive, a machine builder can design and manufacture systems that conform to an internationally recognised set of safety standards, thereby giving their customers the reassurance that each machine will be safe when in use. Equally, by demonstrating compliance, manufacturers are offered a degree of protection from litigation in the event of an accident arising through machine failure or misuse.

In the past, the safety-related elements of machine control systems have been designed in accordance with a separate standard: EN 954-1 (safety-related parts of control systems, part 1: general design principles).

This organised safety related factors into four categories: B, 1, 2, 3 and 4. Each of these was based on a qualitative approach for hazard identification and mitigation. However, the standard did not fully cover factors such as the use of electronic controls, testing intervals, life cycles, and the probability of failure of components.

Concerns about this approach subsequently led to the introduction of ISO 13849-1 2006 as a quantitative approach to risk assessment and safety validation, specifically addressing the programmable electronic safety devices that are being increasingly used in modern machines.

ISO 13849-1 2006 is now integral to the Machinery Directive.

## 2.2. Safety and functional safety

Meeting safety standards is now expected throughout the industry, with certified subsystems such as two handed controls becoming essential. In general terms, safety systems are now implemented through carefully defined processes, often using certified subsystems as building blocks to create complete devices that meet specific safety levels. As a result, machine safety is one of the most rapidly growing areas of importance in industrial automation.

In the context of the Machinery Directive, the goal is to protect people and the environment from accidents caused from all types of machinery.

Functional safety systems do this by lowering the probability of undesired events, so that errors or accidents are minimised when operating machinery. Safety standards define safety as 'freedom from unacceptable risk', with the definition of acceptable or unacceptable being defined by the society or environment within which a machine is used. Machine builders should always use the most stringent and acceptability criteria for all market areas, regardless of regional differences, and should apply them consistently.

The most effective method of eliminating risk is to ensure that safety is a key design criteria from the outset. In many instances, of course, the very nature of machine operation carries an inherent risk that cannot be removed; in such cases, introducing systems such as safety interlocks and static guarding becomes an essential requirement.

Functional machine safety typically involves the development of systems that safely monitor and, when necessary, take control of the machine processes to ensure safe operation. This will involve the detection of processes that are beginning to move into a potentially dangerous condition, with appropriate automatic actions being implemented either to return operation to a safe state, or to ensure that a specific action, such as controlled emergency shutdown, takes place.



As safety systems are not normally part of standard machine operation, it must be noted that any failure in the safety system will immediately increase the risks related to machine operation.



## 3. Machinery Directive



The Machinery Directive is one of the earlier directives to emanate from the EU's long running programme, a New Approach to Technical Harmonisation and Standardisation. A key part of this has been to regulate machinery in the European Union through the use of CE Marking.

The Machinery Directive was first introduced in 1989 and was subsequently amended twice before being consolidated in 1998 to document 98/37/EC. This has since been revised again and is now in force as the new Machinery Directive 2006/42/EC

The latest version does not radically change earlier directives, but does set out to improve and clarify many of the key concepts, with the aim of improving their practical application. As such, there are significant differences that affect suppliers, importers and manufacturers of machinery in the EU and the wider European Economic Area.

The latest version of the Machinery Directive defines a machine as:

*“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”.*

A critical point to note is that it is the manufacturer which is responsible for verifying that a particular product falls within the scope of the Machinery Directive.

The letters ‘CE’ on a machine essentially become the manufacturer’s proof that the machine meets the essential health and safety requirements of the Machinery Directive, together with other relevant compliance documents such as the Low Voltage Directive, EMC Directive and Pressure Directive.

The ESHRs for machinery take into account the potential dangers to system operators and other persons using or affected by the machine, and essentially cover:

- materials used in the construction
- lighting
- controls
- stability
- fire
- noise
- vibration
- radiation
- emission of dust, gasses etc.
- maintenance and documentation.

A company that complies with the appropriate Harmonised European Standards (often called Euro Norms or ENs) such as the Machinery Directive is normally recognised as also meeting the appropriate ESHRs.

Before a product is made available to the market the following must happen:

- The manufacturer must compile a Technical Construction File, which is a document that demonstrates that the product complies with the directive
- The manufacturer or the authorised representative must draw up a Declaration of Conformity, or for partially completed equipment, a Declaration of Incorporation.
- The manufacturer or the authorised representative must affix the CE mark.

## 4. How do the new safety standards differ from EN954-1

EN 954-1 has now been superseded by EN 13849-1 (safety of machines; safety-related parts of control systems, part 1: general design principles) and EN 62061 (safety of machines; functional safety of electrical, electronic and programmable electronic control systems).

A significant revision in these new standards is the approach that is taken to the assessment of safety-related control systems, especially with regard to modern electronic control circuits.

In essence, the new standard builds on the existing categories within EN 954-1, adding a new procedure for risk assessment. This is called a Performance Level (PL) and is associated with a given safety function, with definitions for diagnostic capabilities and common cause failures.

This ensures that safety is not just focussed on component reliability, but instead introduces common sense safety principles such as redundancy, diversity, and fail-safe behaviour.

PL's are based on the original B, 1, 2, 3 and 4 safety categories and are described by the following parameters:

- Category (structural requirement),
- Mean time to dangerous failure ( $MTTF_d$ ),
- Diagnostic coverage (DC),
- Common cause failure (CCF).

With EN ISO 13849-1 and EN 62061 the performance of each safety function is specified as either:

- PL (Performance Level,  $PL_a - PL_e$ ) in the case of EN ISO 13849-1
- SIL (Safety Integrity Level, SIL 1 - 3) in the case of EN 62061



## 4.1. BS EN ISO 13849-1: Safety related parts of control systems, Part 1: general principles for design

This standard may be applied to safety related parts of control systems (SRP/CS) and all types of machinery, regardless of the type of technology and energy used; for example, electrical, hydraulic, pneumatic, or mechanical. EN ISO 13849-1 also lists special requirements for SRP/CS with programmable electronic systems.

EN ISO 13849-1 examines complete safety functions, including all the components involved in their design. EN ISO 13849-1 goes beyond the qualitative approach of EN 954-1 to include a quantitative assessment of the safety functions. A performance level (PL) is used for this, building upon the categories.

### Components and devices require the following safety parameters:

- Category (structural requirement)
- PL (a – e): Performance level
- $MTTF_d$ : Mean time to dangerous failure
- $B10_d$ : Number of cycles by which 10% of a random sample of wearing components have failed dangerously
- DC: Diagnostic coverage
- CCF: Common cause failure



The standard describes how to calculate the performance level (PL) for safety related parts of control systems, based on designated architectures. EN ISO 13849-1 refers any deviations to IEC 61508. Where several safety related parts are

combined into one overall system, the standard describes how to calculate the PL that can be achieved.

For additional guidelines on validation EN ISO 13849-1 refers to Part 2, which was published at

the end of 2003. This part provides information on fault considerations, maintenance, and technical documentation and usage guidelines.



## 4.2. BS EN 62061: “Functional safety of safety-related electrical, electronic and programmable electronic control systems”.

This standard defines requirements and gives recommendations for the design, integration and validation of safety related electrical, electronic and programmable electronic control systems (SRECS) for machinery. It does not define requirements for the performance of non-electrical (e.g. hydraulic or pneumatic) safety related control elements for machinery.

BS EN 62061 has a sector specific standard under IEC 61508, and uses quantitative and qualitative criteria for assessing the safety related control functions. It describes the implementation of safety related electrical and electronic control systems on machinery and examines the overall lifecycle from the concept phase through to decommissioning. The performance level is described through a safety integrity level (SIL).

The safety functions identified from risk analyses are divided into safety sub-functions; these sub-functions are then assigned to actual devices, called sub-systems and sub-system elements; these cover both hardware and software.

A safety related control system typically is made up of several sub-systems. The safety related characteristics of these subsystems are described through parameters (SIL claim limit and PFHD).

### Safety-related parameters for subsystems:

- SILCL: SIL claim limit
- PFHD: Probability of dangerous failure per hour
- T1: Lifetime

These subsystems may, in turn, be made up of various interconnected sub-system elements with parameters to calculate the corresponding PFHD value of each sub-system.



### Internal parameters to be established during design and construction for a sub-system or a system comprised of sub-system elements:

- T2: Diagnostic test interval
- $\beta$ : Susceptibility to common cause failure
- DC: Diagnostic coverage
- PFHD: The PFHD value of the safety-related control system is calculated by adding the individual PFHD values of each sub-system.

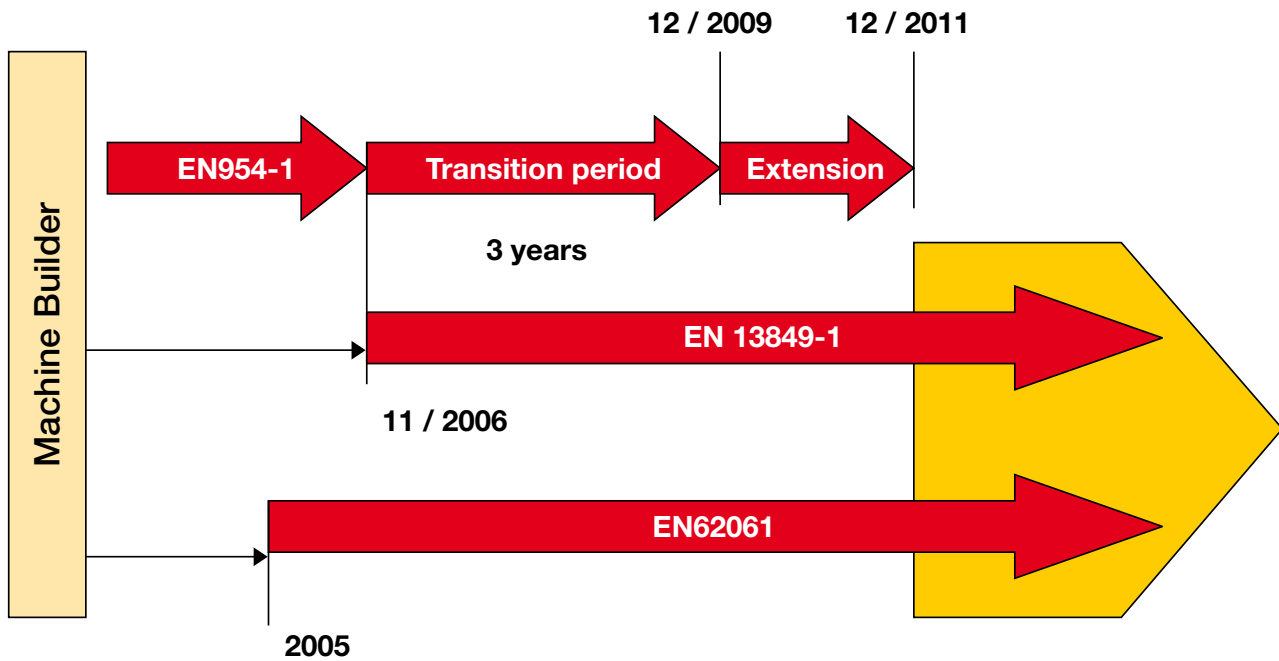
### Safety related parameters for subsystem elements (devices):

- Failure rate; for wearing elements described via the B10 value
- SFF: Safe failure fraction; for electro-mechanical devices the failure rate is indicated by the manufacturer as a B10 value, based on the number of cycles. The time-based failure rate and lifetime must be determined through the switching frequency for the respective application.

## 5. New Approach

The initial plan was that the standard EN 954-1 became obsolete on November 30, 2009, being replaced by standards EN ISO 13849-1 and EN 62061. A three-year transition period

was to begin in November 2006 and during this period EN 954-1 could be used in parallel with the new standards EN ISO 13849-1 and EN62061.



**Figure 1 Transition period from old to new standards**

There has now been official confirmation of an extended transition period for EN 954-1. The European Committee for Standardisation (CEN) has confirmed that the EN 954-1 presumption of conformity to the Machinery Directive has been prolonged for two years, until 31 December 2011.

The reason for this change is simply that many manufacturers are still unprepared for the move to the new standards EN ISO 13849-1 and EN62061.

Replacing the EN 954-1 standard with EN ISO 13849-1 and EN 62061 (which is applicable only to electrical control systems), is a move towards a probabilistic or reliability approach in safety related systems, away from the older category determination methodology.

The new standards take account of the probability of failure for the entire safety function, not only of its components. Unlike EN 954-1, these new standards allow the use of programmable safety systems,

based on the category concept of EN 954-1, and with the addition of concepts such as life-cycle thinking, quantification of component reliability and test quality, and common cause failure analysis.

## 6. European Harmonised Standards

### 6.1. Hierarchy of the European harmonised standards system

A European Harmonised Standard is a standard that supports one or more European Directives as a practical method of guaranteeing a high level of protection to EU workers and citizens, as determined by the essential requirements (EHSRs) of the Directives.

Although the use of standards is not mandatory, many European Directives make direct reference to them, effectively making their application obligatory. There is always a presumption of conformity with the directives if a machine is built to the appropriate Harmonised Standards.

European Standards (or Euro Norms) are identified by the letters “EN” and may be prefixed by the standards authorities in member states when adopted. In the United Kingdom, for example, this prefix is BS (British Standards). Standards such as EN 62061 (BS EN 62061 in the UK) are typical of the nomenclature.

The communalisation of standards is taking place throughout the world and the European Union is working with international standard authorities, such as ISO (the International Organisation for Standardisation) and the IEC, (the International Electrotechnical Commission), to adopt a global approach.

#### Standards for the safety of machinery in Europe fall into 3 basic categories:-

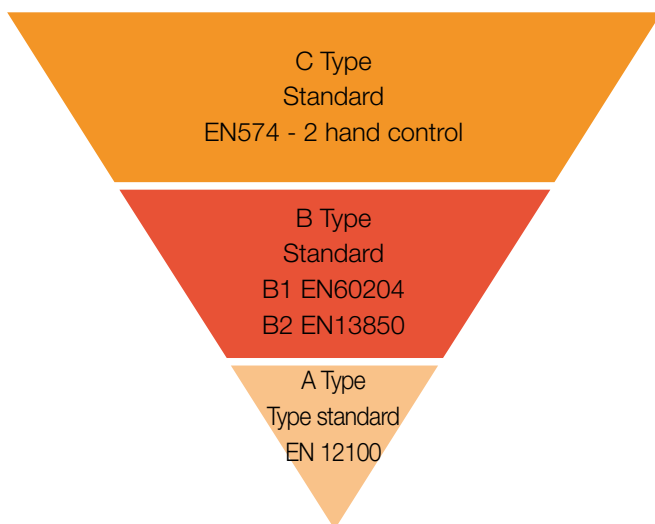


Figure 2 Hierarchy of European Standards

#### **Type C standards:**

Machinery safety standards for specific types of machines or industrial applications.

#### **Type B standards:**

Grouping more specific safety standards that may be applied across a range of machines and industries.

B standards are further subdivided:

**B1** standards detail the overriding safety aspects.

**B2** standards cover the actual safety devices.

#### **Type A standards:**

Fundamental safety standards, giving basic principles for design and general aspects for all machinery.

## 7. Changes in the new Machinery Directive

The new Directive will be applied to machines launched after the transition period, but machine builders and designers are advised to adopt the standards as soon as practical.

The aim of the new Directive is to reinforce the old Machinery Directive on the free circulation and safety of machinery and to improve its application.

There have been no dramatic changes between the old and the new, revised Directive.

Highlights of the changes in the new Machinery Directive are as follows:

### 7.1. Changes in how conformity is evaluated for dangerous machines listed in the Machinery Directive Annex IV.

The new directive still lists categories of machinery to which special procedures must be applied (Annex IV) but, significantly, the necessity to involve a Notified Body has been removed if the machinery is manufactured in accordance with harmonised standards; a manufacturer can therefore carry out self-certification. The manufacturer must, however, have a quality assurance procedure that has been implemented according to the requirements presented in the Machinery Directive's Annex X.

Where a Notified Body has been involved there is a new requirement for a review of the EC type-examination certificate every five years.

### 7.2. Changes in the Essential Health and Safety Requirements that are presented in the Machinery Directive's Annex I.

The manufacturer must now carry out a risk assessment on the EHSR. The revised Essential Health & Safety Requirements (EHSRs) now effectively includes the essential requirements of the LVD within the EHSRs.

There are significant additions and changes to the EHSRs that will affect machine design including requirements for guarding and control systems. The supplementary EHSRs have also been subject to change.

### 7.3. Changes in proving the safety of different products.

The same machine regulations will apply to machinery, exchangeable equipment, safety components etc. The products must include CE conformity assessment, declaration of conformity and the requisite user information.

### 7.4. Introduction of the term 'Partly completed machinery'.

The term partly completed machinery refers to an assembly that is almost a full system but that cannot in itself perform a specific application or function. Partly completed machinery is intended to be incorporated into, or assembled with, other machinery or partly completed machinery:

- o It consists of several parts, at least one of which is moving
- o It is fitted with or intended to be fitted with a drive system
- o It cannot by itself perform a specific application
- o It is to be incorporated into part completed or complete machinery.

Additional to the manufacturer's declaration, the manufacturer must also supply a declaration of incorporation; this defines the particular requirements of the directive that apply to the

part or incomplete machine, and which comply with the directive. Product documentation must also include installation instructions.

**Example: -**

**7.4.1. Partially completed pneumatic machinery** is an arrangement of several modules or components with frame, actuators and power control valves that are not ready to be used; e.g. feeder units and rotary tables intended to be incorporated into or assembled into, or assembled with other machinery, or partly completed machinery to build a production line.

**7.4.2. Pneumatic components** that are assembled into a control system are excluded from the scope of the Machinery Directive, i.e.: Combination of solenoid valves, valve islands, filter regulators, lubricators, pressure switches, all connected with fittings.

**7.5. Changes to the Low Voltage Directive.**

The scope of the Low Voltage Directive (2006/95/EC) now identifies electrical and electronic product types instead of a specified risk. There is also now a clearer differentiation between the Machinery Directive and the Low Voltage Directive.



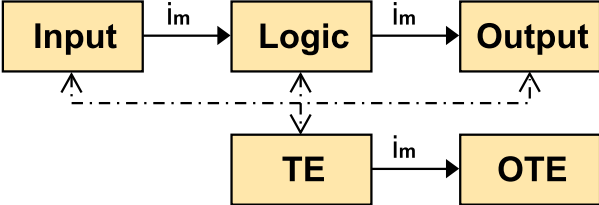
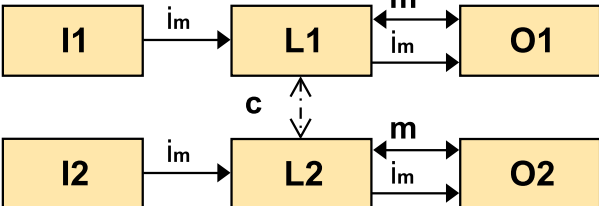
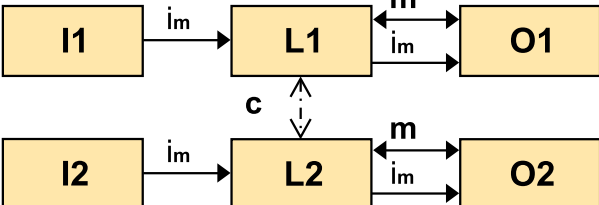
**7.7. Changes in the hazard analysis.**

The hazard analysis is replaced by mandatory risk assessment and risk evaluation.

**7.8. Changes in production control.**

Series machines now have internal production controls, specified in the Machinery Directive Annex VIII.

# 8. Categories of EN ISO 13849-1

Category	Summary	Schematic
<b>Category B</b>	When a fault occurs it can lead to the loss of the safety function	 <pre> graph LR     Input[Input] -- im --&gt; Logic[Logic]     Logic -- im --&gt; Output[Output]             </pre>
<b>Category 1</b>	When a fault occurs it can lead to the loss of the safety function, but the MTTFd of each channel in Category 1 is higher than in Category B. Consequently the loss of the safety function is less likely.	 <pre> graph LR     Input[Input] -- im --&gt; Logic[Logic]     Logic -- im --&gt; Output[Output]             </pre>
<b>Category 2</b>	Category 2 system behaviour allows that: the occurrence of a fault can lead to the loss of the safety function between the checks; the loss of the safety function is detected by the check.	 <pre> graph LR     Input[Input] -- im --&gt; Logic[Logic]     Logic -- im --&gt; Output[Output]     TE[TE] -- im --&gt; OTE[OTE]     Logic -.-&gt; OTE             </pre>
<b>Category 3</b>	SRP/CS to Category 3 shall be designed so that a single fault in any of these safety related parts does not lead to the loss of the safety function. Whenever reasonably possible the single fault shall be detected at or before the next demand upon the safety function.	 <pre> graph LR     I1[I1] -- im --&gt; L1[L1]     L1 -- im --&gt; O1[O1]     O1 -- m --&gt; L1     I2[I2] -- im --&gt; L2[L2]     L2 -- im --&gt; O2[O2]     O2 -- m --&gt; L2     L1 &lt;--&gt;  c  L2             </pre>
<b>Category 4</b>	SRP/CS to Category 4 shall be designed so that a single fault in any of these safety related parts does not lead to the loss of the safety function, and the single fault is detected on or before the next demand upon the safety functions, e.g. immediately, at switch on, at end of a machine operation cycle. If this detection is not possible an accumulation of undetected faults shall not lead to the loss of the safety function.	 <pre> graph LR     I1[I1] -- im --&gt; L1[L1]     L1 -- im --&gt; O1[O1]     O1 -- m --&gt; L1     I2[I2] -- im --&gt; L2[L2]     L2 -- im --&gt; O2[O2]     O2 -- m --&gt; L2     L1 &lt;--&gt;  c  L2             </pre>

**Key**

$i_m$	Interconnecting means	$c$	Cross monitoring
I	Input	$m$	Monitoring
L, L1, L2	Logic	TE	Test equipment
O, O1, O2	Output	OTE	Output of TE

# 9. Step Method of Risk Reduction

## Strategy for Risk Assessment (source ISO 12100)

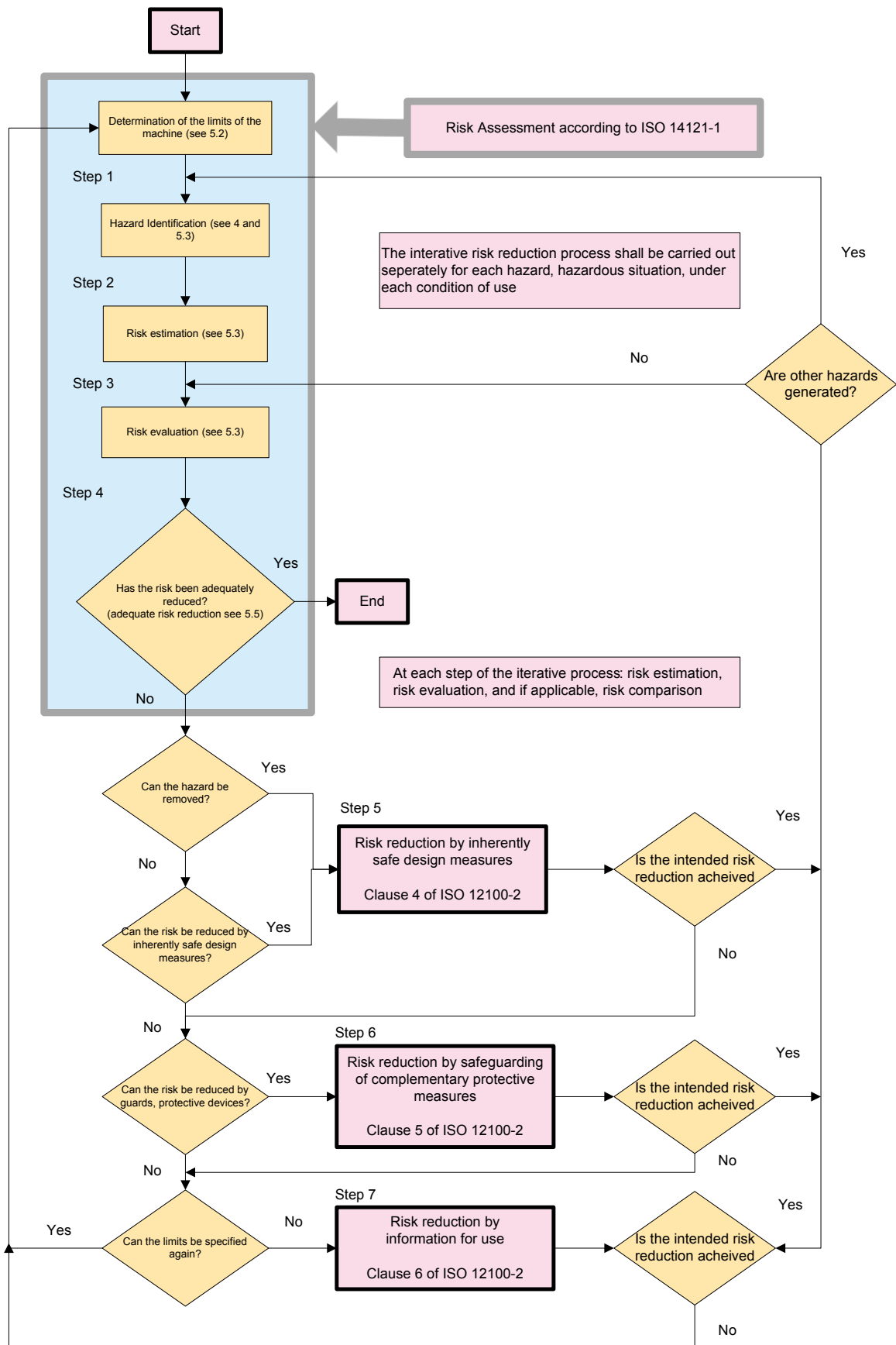


Figure 3 Risk reduction process

The Machinery Directive requires machinery to be safe; there is, however, no such thing as zero risk. The objective therefore has to be to achieve the lowest possible risk.

The process for fulfilling the EHSR of the Machinery Directive using harmonised standards can be divided into seven steps

(figure 3), which enable risk estimation to become an iterative process. This means it may be necessary to go through the process more than once. The risk must be estimated and the PL<sub>r</sub> (SIL) defined for each hazard on which the risk is to be reduced through control measures.

## **9.1. Step 1: The limits (ISO 14121-1 paragraph 5) of the machinery: -**

### **9.1.1. Use Limits**

- o Operating modes
- o Use of the machine – industrial, domestic etc.
- o Training, user ability
- o Exposure to hazard

### **9.1.2. Space limits**

- o Range of movement
- o User interaction
- o Space requirements for operation, maintenance
- o Power supply

### **9.1.3. Time Limits**

- o Machinery life
- o Component life
- o Service intervals

### **9.1.4. Other limits**

- o Environmental
- o Housekeeping
- o Processed material property.

**9.2. Step 2: Hazard identification:** The requirement is to assess and identify reasonably foreseeable hazards. The phases of a machine life cycle should be considered, such as transport, commissioning, use, decommissioning and disposal. The practical use of standard tools such as FMEA's, process mapping and fish bone analysis could be utilised.

**9.3. Step 3: Risk estimation: Having identified the hazard the impact should be assessed. Some of the aspects to be considered include:**

- Persons exposed
- Type, frequency and duration of exposure
- Relationship between exposure and effects
- Human factors
- Suitability of protective measure
- Possibility of overriding or circumventing protection methods
- Ability to maintain the protective measure.

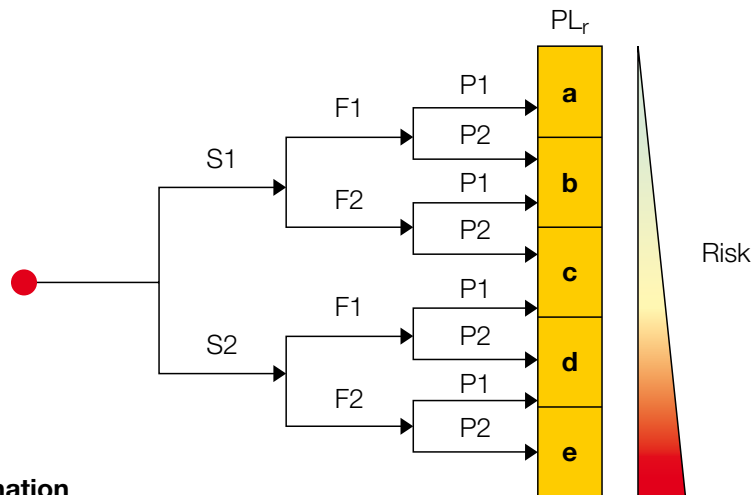


Determine the required performance level PL according to ISO 13849-1

The greater the risk, the higher the requirements of the control system.

The contribution of reliability and structure can vary depending on the technology used.

The level of each hazardous situation is classified in five stages, from a to e. With PL a the control function's contribution to risk reduction is low, while at PL e it is high. The risk graph can be used to determine the required performance level (PL<sub>r</sub>) for the safety function described above.



Source EN 13849-1

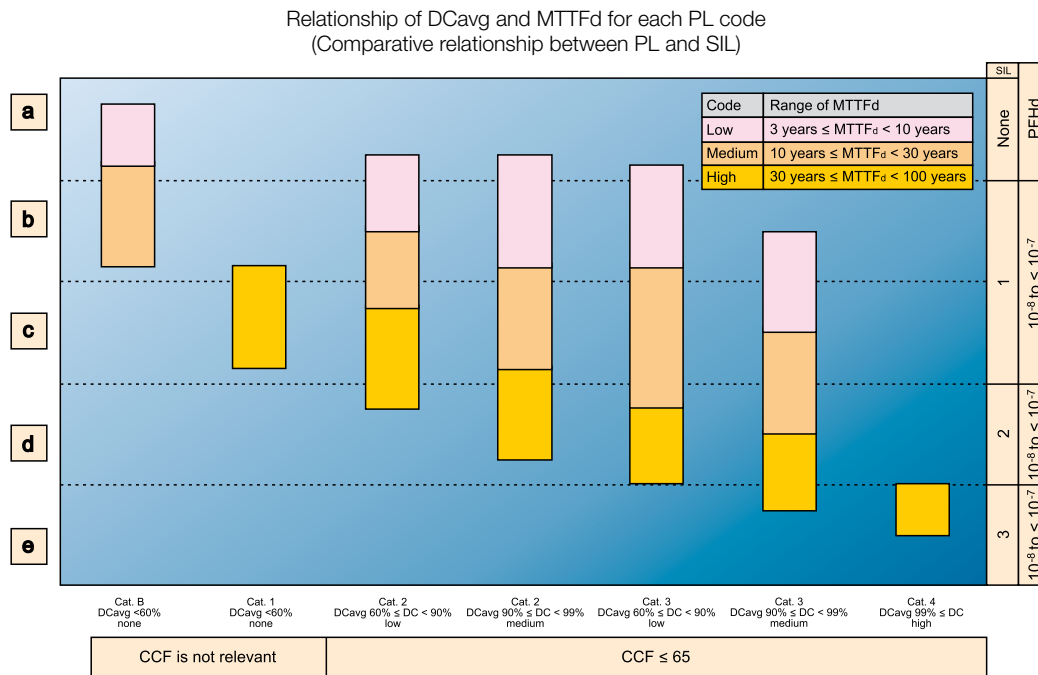
Figure 4 Risk Elimination

ISO 13849-1	IEC 62061		
	Se - severity of injury		Score
S1 slight (normally reversible injury)	Irreversible	death, losing an eye or arm	<b>4</b>
	Irreversible	broken limb(s), losing a finger(s)	<b>3</b>
	Reversible	requiring attention from a medical practitioner	<b>2</b>
	Reversible	requiring first aid	<b>1</b>
S2 serious (normally irreversible injury or death)			
	Fr - frequency and/or exposure to hazard		
F1 seldom-to-less-often and/or exposure time is short	≤ 1 h		<b>5</b>
	> 1 h to ≤ 1 day		<b>5</b>
	> 1 day to ≤ 2 weeks		<b>4</b>
	> 2 weeks to ≤ 1 year		<b>3</b>
	> 1 year		<b>2</b>
	Pr - possibility of avoiding hazard or limiting harm		
P1 P1 possible under specific conditions	Impossible		<b>5</b>
P2 P2 scarcely possible	Rarely		<b>3</b>
	Probable		<b>1</b>

Figure 4 illustrates how the methodology of ISO 13849-1 differs from IEC 62061.

It should be noted that a SIL cannot be determined for a component, e.g. a valve.  
The risk is estimated through consideration of:

- the severity of the injury (Se),
- the frequency and duration of exposure to the hazard (Fr),
- the probability of occurrence of a hazardous event (Pr) and
- the probability of avoiding or limiting harm (Av).



**Figure 5 Relationship between PL and SIL**

### 9.4. Step 4: Risk evaluation

After the risk assessment has been carried out, there are two options, depending on the outcome of the assessment:

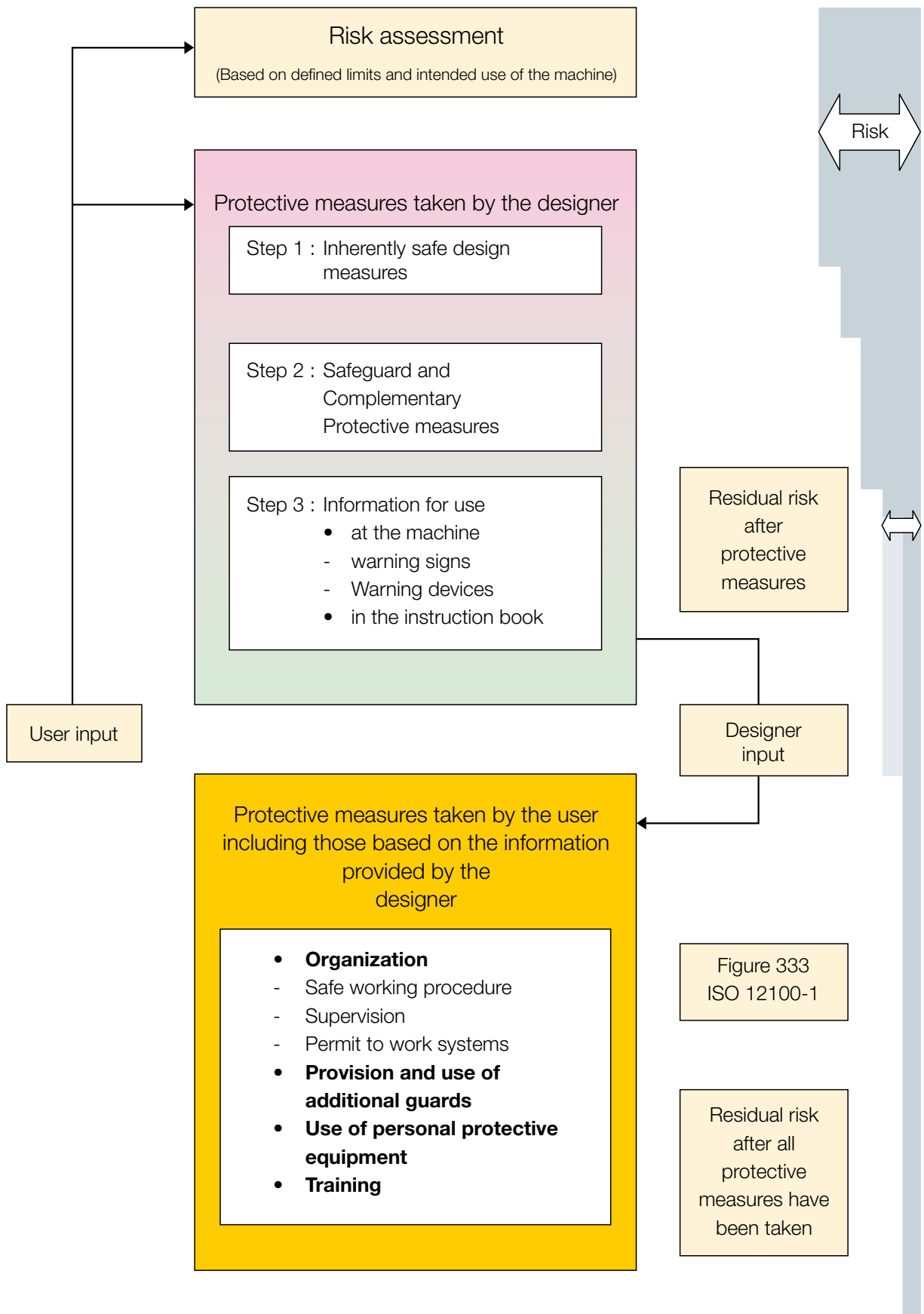
- If the assessment reached the conclusion that the safety measures used effectively negate the need for risk reduction, then the machine has reached the adequate level of safety required by the Machinery Directive.
- If the assessment process (step 1 to 4) reveals that the risk remains unacceptable, a procedure for risk minimisation is required. According to standard EN ISO 12100-1, risk reduction can be divided into a further 3 three steps (Step 5 to 7).

*Note:*

For a machine to be approved and CE marking affixed, the remaining risks must be documented in the appropriate operation and maintenance manuals. There will, however, always to be an element of residual risk.

The process is outlined in figure 6

**Figure 6 Risk evaluation process**



## 9.5. Step 5 – Risk Reduction - (ISO 12100-2 clause 4)

Is there a safer design or can the process be changed?

machinery can be compared to those of similar machinery or machine parts, provided the following criteria apply.

As part of the process of risk evaluation, the risks associated with machinery or parts of the

Adequate risk reduction is achieved when:

- all operating conditions and all intervention procedures have been considered
- the hazards have been eliminated or risks reduced to the lowest practicable level
- any new hazards introduced by the protective measures have been properly addressed
- users are sufficiently informed and warned about the residual risks
- protective measures are compatible with each other
- sufficient consideration has been given to the consequences that can arise from the use of a machine
- designed for professional or industrial use when it is used in a non-professional/ or non-industrial context
- the protective measures do not adversely effect the operator's working conditions or the usability of the machine.

## 9.6. Step 6 – Protective device risk reduction - (ISO 12100-2 clause 5)

The risk is considered to have been reduced by the application of safeguarding and complementary protective measures of a type that adequately reduces risk for the intended use and reasonably foreseeable misuse, and

which are appropriate for the application.

Can the risk be reduced with the provision and use of additional safeguards?

- Use of personal protective equipment (PPP).
- Use of guards
- Safety interlock
- Light guards etc.

## 9.7. Step 7 – Information to the user

Information for use shall not be a substitute for the correct application of inherently safe design measures or safeguarding or complementary protective measures.

User Information should be considered:

- on the machine
  - Warning signs, signals and warning devices
  - Operating instructions.
  - Training users.
  - Reading operating and safety instructions and acting accordingly.

## 10. Calculations

Calculation of  $MTTF_d$  for components from  $B_{10d}$

### References

$B_{10}$	Number of cycles, until 10% of the components fails
$B_{10d}$	Number of cycles, until 10% of the components fails dangerously (may use $B_{10d} = 2 B_{10}$ )
$n_{op}$	The mean number of annual operations
$MTTF_d$	Mean Time to Dangerous failure
$h_{op}$	Mean number of operations, hours per day

With  $B_{10d}$  and  $n_{op}$ , the mean number of annual operations,  $MTTF_d$  for components can be calculated as: -

$$MTTF_d = \frac{B_{10d}}{0.1 \times n_{10op}}$$

where

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s / h}{t_{cycles}}$$

with the following assumptions having been made on the application of the component:

$h_{op}$  is the mean operation, in hours per day;

$d_{op}$  is the mean operation, in days per year;

$t_{cycle}$  is the mean time between the beginning of two successive cycles of the component.

(e.g. switching of a valve) in seconds per cycle

The operation time of the component is limited to  $T_{10d}$ ,  
the mean time until 10 % of the components fail  
dangerously:

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

$B_{10d}$  the mean number of cycles till 10 % of the components fail dangerously, can be converted to  $T_{10d}$ , the mean time until 10 % of the components fail dangerously, by using  $n_{op}$ , the mean number of annual operations:

The reliability methods in this part of ISO 13849 assume that the failure of components is distributed exponentially over time:  $F(t) = 1 - \exp(-\lambda dt)$ . For pneumatic and electromechanical components, a weibull distribution is more likely.

But if the operation time of the components is limited to the mean time until 10 % of the components fail dangerously ( $T_{10d}$ ), then a constant dangerous failure rate ( $\lambda_d$ ) over this operation time can be estimated as

$$\lambda_d = \frac{0.1}{T_{10d}} = \frac{0.1 \times n_{op}}{B_{10d}} \quad (C5)$$

Equation (C.5) takes into account that with a constant failure rate, 10 % of the components in the

assumed application fail after  $T_{10d}$  [years], corresponding to  $B_{10d}$  [cycle]. To be exact:

$$F(T_{10d}) = 1 - \exp(-\lambda T_{10d}) = 10\% \quad \text{means} \quad \lambda_d = \frac{\ln(0.9)}{T_{10d}} = \frac{0.10536}{T_{10d}} = \frac{0.1}{T_{10d}}$$

With  $MTTF_d = 1/\lambda_d$  for exponential distributions, this yields

$$MTTF_d = \frac{T_{10d}}{0.1} = \frac{B_{10d}}{0.1 \times n_{op}}$$

### Example

For a pneumatic valve, a manufacturer determines a mean value of 60 million cycles as  $B_{10d}$ . 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 5 s. This yields the following values:

	input	
$d_{op}$	220	days per year
$h_{op}$	16	hours per day
$t_{cycle}$	5	sec per cycle
$B_{10d}$	60000000	million cycles
$n_{op} =$	2.53E+06	cycles/year
$T_{10d} =$	23.7	years
$MTTF_d =$	237	years

$$n_{op} = \frac{220 \text{ days / year} \times 16 \text{ h / day} \times 3600 \text{ s / h}}{5 \text{ s / cycles}}$$

$$T_{10d} = \frac{60 \times 10^6 \text{ cycles}}{2.53 \times 10^6 \text{ cycles / year}}$$

$$MTTF_d = \frac{23.7 \text{ years}}{0.1}$$

This will give a  $MTTF_d$  for the component "high" according to Table 5.

These assumptions are only valid for a restricted operation time of 23,7 years for the valve.

# 11. Validation tools for pneumatic systems

## Failure mode

### General

Fault lists and fault exclusions see EN ISO 13849-2, Annex B.5.

Following further information are given with regard to the use of the fault lists.

### Directional control valves

- Fault considered: Change of the switching time
  - Fault exclusion: No, for pilot operated valves, because there is no positive actuation
- Fault considered: No complete movement into the rest position
  - Fault exclusion: Yes, for direct operated valves; no, for pilot operated valves
  - Fault consequence at poppet valves: Connection of ports or non-functioning
  - Fault consequence at spool valves: Blocking of ports

### Non-return valves/quick-exhaust valves/shuttle valves etc.

- Fault considered: Change of the switching time
- Fault exclusion: Yes, due to the high closing speed change of switching time is not relevant  
NOTE For shut-off valves see directional control valves.

### Flow control valves (throttle valves - and one-way flow control valves)

- Fault considered: Change of the flow rate without change of setting of the adjustment device
  - Fault exclusion: No, for one-way flow control valves
  - Fault cause: Change of the leakage in the non-return system
  - Fault consequence: Increased flow rate

### Pressure valves (pressure relief valves, pressure regulators)

- Fault considered: Leakage of the pressure regulator
  - Fault exclusion: No
  - Fault cause: Too high leakage at the seat of the control element
  - Fault consequence: Pressure rise at the outlet
- Fault considered: In spite of shutoff of the supply pressure non-exhausting of the system by the pressure regulator
  - Fault exclusion: Yes, at presence of constructional conditions (e.g. sufficient area ratio or integrated non-return function)
  - Fault consequence: System remains under pressure

### Tube and hose assemblies

- Fault considered: Kinking of plastic tubes and hoses
  - Fault exclusion: Yes, if the bending radius falls not below the minimum bending radius
- Fault considered: Burst, pull out, break off of plastic tubes
  - Fault exclusion: Yes, at compliance with recommended service life
  - Fault consequence: pressure loss

### Cylinders

- Fault considered: Cushion failure
  - Fault consequence: Uncontrolled deceleration at the ends of stroke.
- Fault considered: loosening of rod connection
  - Fault consequence: Load becomes detached and out of control
- Fault considered: Loosening of the mountings
  - Fault consequence: Load becomes detached and out of control

## 12. Abbreviation Glossary

Abbreviation	Glossary	Comment
CE marking		A mandatory conformity mark on machinery and many other kinds of products placed on the single market in the European Economic Area (EEA). By affixing CE marking to the product, the manufacturer ensures that the product meets all of the essential requirements of the relevant European Directive(s).
CCF	Common Cause Failure	A situation where several subsystems fail due to a single event. All failures are caused by the event itself and are not consequences of each other. Score should be greater than equal to 65,
DC	Diagnostic Coverage	Diagnostic Coverage (DC) is the effectiveness of fault monitoring of a system or subsystem. It is the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.
EHSR	Essential Health and Safety Requirements	Requirements that machinery must meet in order to comply with the European Union Machinery Directive and obtain CE marking. These requirements are listed in the Machinery Directive's Annex I.
EN	Standards for Euro Norm	This prefix is used with harmonised standards
Harm	Physical injury or damage to health.	
Harmonized standard		A European standard that has been prepared under the mandate of the European Commission or the EFTA Secretariat with the purpose of supporting the essential requirements of a directive and is effectively mandatory under the EU law.
MTTFd	Mean Time To dangerous Failure	Expectation of the average time for a dangerous failure to occur. Average probability of dangerous failure taking place during one hour.
PFHd	Probability of dangerous Failure per Hour	PFHd is the value that is used for determining the SIL or PL value of a safety function.
PL	Performance Level	Levels (a, b, c, d, e) for specifying the capability of a safety system to perform a safety function under foreseeable conditions.
Risk		A combination of how possible it is for the harm to happen and how severe the harm would be.
Safety function		A function designed for adding safety to a machine whose failure can result in an immediate increase in risk(s).
SIL	Safety Integrity Level	Levels (1, 2, 3, 4) for specifying the capability of an electrical safety system to perform a safety function under foreseeable conditions. Only levels 1-3 are used in machinery.

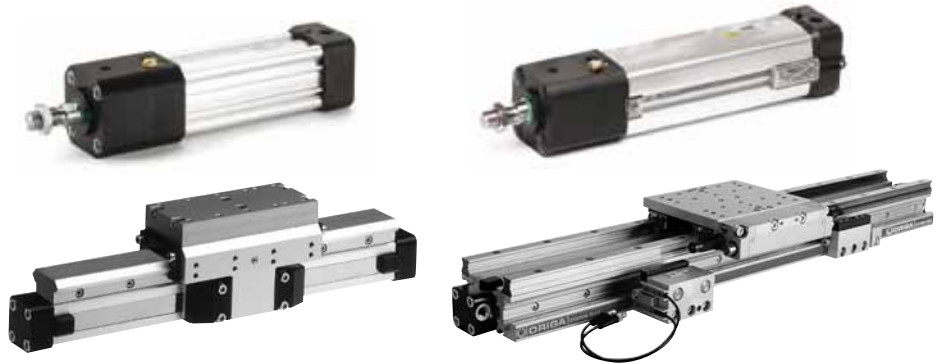
### References

**ABB**  
**Schneider**  
**CETOP**  
**VDMA**  
**BSI**  
**Europa**  
**BERR**



# Products offering safety functions

(ISO 4414 compliant)



## Actuators

Typical B10 values – 10 M cycles (3000Kms)

**5.2.2.4** Loss of pressure or pressure drop shall not expose persons to a hazard and should not damage the machinery.

### 5.2.3 Mechanical movements

Mechanical movements, whether intended or unintended (e.g. effects from acceleration, deceleration or lifting/holding of masses), shall not result in a situation hazardous to persons.

### 5.2.8 Positive isolation from energy sources

↓ releasing or supporting mechanical loads when the system is depressurized;



### 5.2.8 Positive isolation from energy sources

Isolating the supply with a suitable shut-off device, which should be lockable, and shall be accessible without causing a hazard, or isolating

and dissipating pressure from the system with a suitable shut-off device(s) having a pressure-release feature, which it can be necessary to be able to lock;

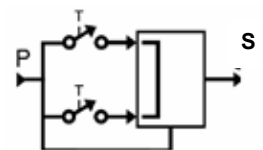
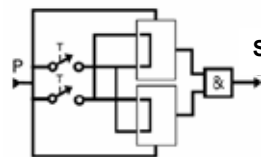
## Function fittings



### 5.2.3 Mechanical movements

Mechanical movements, whether intended or unintended (e.g. effects from acceleration, deceleration or lifting/ holding of masses), shall not result in a situation hazardous to persons.

## Safety Products



## 2 Hand Control

### 5.4.6.8 Two-hand controls

If two-hand controls are provided, they shall be designed and applied in accordance with ISO 13851.



### 5.4.5.8 Quick-action couplings

Quick-action (quick-release) couplings shall be selected and installed so that when they are being coupled or uncoupled,

- the coupling shall not couple or uncouple in a hazardous manner;
- compressed air or particles shall not be expelled in a hazardous manner;
- a controlled pressure-release system shall be provided where a hazard may exist.



### Soft Start and Dump Valve

#### 5.2.8 Positive isolation from energy sources

Precautions should be taken when the supply is reinstated after isolation or depressurization.

#### 5.2.11 Uncontrolled actuator movement

If rapid opening of the shut-off valve can produce uncontrolled movement of actuators, a soft-start/slow-start valve shall be incorporated



### Air Fuse

5.4.5.11.1 When failure of a hose assembly or plastic piping constitutes a whiplash hazard, it shall be restrained or shielded by suitable means. In addition, an air fuse for compressed air should be mounted.

# Parker Worldwide

## Europe, Middle East, Africa

**AE – United Arab Emirates,**  
Dubai

Tel: +971 4 8127100  
parker.me@parker.com

**AT – Austria,** Wiener Neustadt

Tel: +43 (0)2622 23501-0  
parker.austria@parker.com

**AT – Eastern Europe,** Wiener  
Neustadt

Tel: +43 (0)2622 23501 900  
parker.easteurope@parker.com

**AZ – Azerbaijan,** Baku

Tel: +994 50 2233 458  
parker.azerbaijan@parker.com

**BE/LU – Belgium,** Nivelles

Tel: +32 (0)67 280 900  
parker.belgium@parker.com

**BY – Belarus,** Minsk

Tel: +375 17 209 9399  
parker.belarus@parker.com

**CH – Switzerland,** Etoy

Tel: +41 (0)21 821 87 00  
parker.switzerland@parker.com

**CZ – Czech Republic,** Klecany

Tel: +420 284 083 111  
parker.czechrepublic@parker.com

**DE – Germany,** Kaarst

Tel: +49 (0)2131 4016 0  
parker.germany@parker.com

**DK – Denmark,** Ballerup

Tel: +45 43 56 04 00  
parker.denmark@parker.com

**ES – Spain,** Madrid

Tel: +34 902 330 001  
parker.spain@parker.com

**FI – Finland,** Vantaa

Tel: +358 (0)20 753 2500  
parker.finland@parker.com

**FR – France,** Contamine s/Arve

Tel: +33 (0)4 50 25 80 25  
parker.france@parker.com

**GR – Greece,** Athens

Tel: +30 210 933 6450  
parker.greece@parker.com

**HU – Hungary,** Budapest

Tel: +36 23 885 475  
parker.hungary@parker.com

**IE – Ireland,** Dublin

Tel: +353 (0)1 466 6370  
parker.ireland@parker.com

**IT – Italy,** Corsico (MI)

Tel: +39 02 45 19 21  
parker.italy@parker.com

**KZ – Kazakhstan,** Almaty

Tel: +7 7272 505 800  
parker.easteurope@parker.com

**NL – The Netherlands,** Oldenzaal

Tel: +31 (0)541 585 000  
parker.nl@parker.com

**NO – Norway,** Asker

Tel: +47 66 75 34 00  
parker.norway@parker.com

**PL – Poland,** Warsaw

Tel: +48 (0)22 573 24 00  
parker.poland@parker.com

**PT – Portugal,** Leca da Palmeira

Tel: +351 22 999 7360  
parker.portugal@parker.com

**RO – Romania,** Bucharest

Tel: +40 21 252 1382  
parker.romania@parker.com

**RU – Russia,** Moscow

Tel: +7 495 645-2156  
parker.russia@parker.com

**SE – Sweden,** Spånga

Tel: +46 (0)8 59 79 50 00  
parker.sweden@parker.com

**SK – Slovakia,** Banská Bystrica

Tel: +421 484 162 252  
parker.slovakia@parker.com

**SL – Slovenia,** Novo Mesto

Tel: +386 7 337 6650  
parker.slovenia@parker.com

**TR – Turkey,** Istanbul

Tel: +90 216 4997081  
parker.turkey@parker.com

**UA – Ukraine,** Kiev

Tel +380 44 494 2731  
parker.ukraine@parker.com

**UK – United Kingdom,** Warwick

Tel: +44 (0)1926 317 878  
parker.uk@parker.com

**ZA – South Africa,** Kempton Park

Tel: +27 (0)11 961 0700  
parker.southafrica@parker.com

## North America

**CA – Canada,** Milton, Ontario

Tel: +1 905 693 3000

**US – USA,** Cleveland

Tel: +1 216 896 3000

## Asia Pacific

**AU – Australia,** Castle Hill

Tel: +61 (0)2-9634 7777

**CN – China,** Shanghai

Tel: +86 21 2899 5000

**HK – Hong Kong**

Tel: +852 2428 8008

**IN – India,** Mumbai

Tel: +91 22 6513 7081-85

**JP – Japan,** Tokyo

Tel: +81 (0)3 6408 3901

**KR – South Korea,** Seoul

Tel: +82 2 559 0400

**MY – Malaysia,** Shah Alam

Tel: +60 3 7849 0800

**NZ – New Zealand,** Mt Wellington

Tel: +64 9 574 1744

**SG – Singapore**

Tel: +65 6887 6300

**TH – Thailand,** Bangkok

Tel: +662 186 7000-99

**TW – Taiwan,** Taipei

Tel: +886 2 2298 8987

## South America

**AR – Argentina,** Buenos Aires

Tel: +54 3327 44 4129

**BR – Brazil,** Sao Jose dos Campos

Tel: +55 800 727 5374

**CL – Chile,** Santiago

Tel: +56 2 623 1216

**MX – Mexico,** Apodaca

Tel: +52 81 8156 6000

European Product Information Centre

Free phone: 00 800 27 27 5374

(from AT, BE, CH, CZ, DE, DK, EE, ES, FI,  
FR, IE, IL, IS, IT, LU, MT, NL, NO, PL, PT, RU,  
SE, SK, UK, ZA)

**Parker Hannifin Ltd.**

Tachbrook Park Drive

Tachbrook Park,

Warwick, CV34 6TU

United Kingdom

Tel.: +44 (0) 1926 317 878

Fax: +44 (0) 1926 317 855

parker.uk@parker.com

www.parker.com

