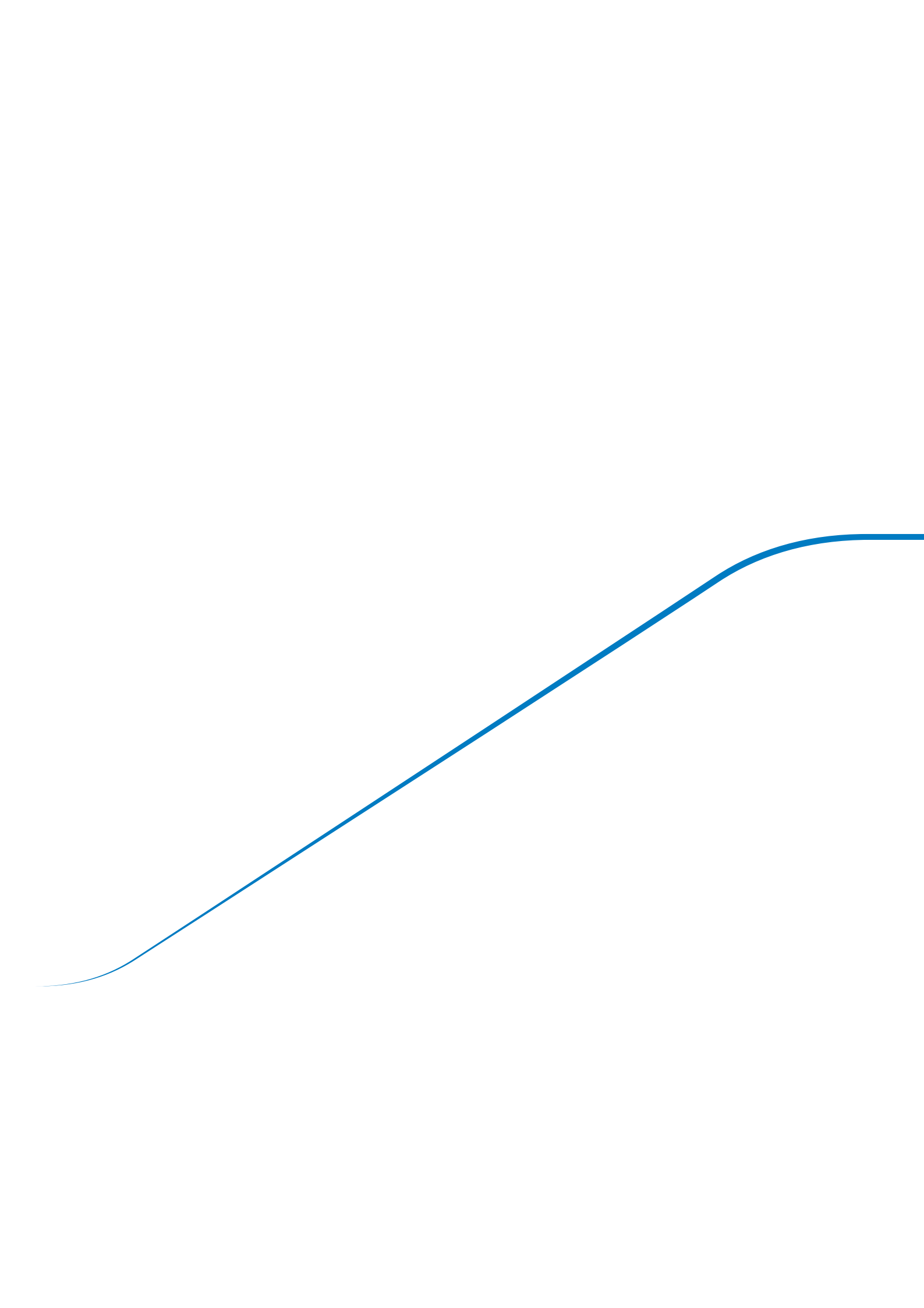




Expertise – Passion – Automation



**Safety in focus**







## On the safe side with SMC

**Trust us for safety.** SMC is a powerful and reliable partner for factory automation, offering a wide range of pneumatic solutions. We support our customers to achieve and maintain the required levels of functional safety when using our products.

We offer safety products compliant with the Machinery Directive to provide the necessary levels of risk reduction to provide a safe working environment for the operating personnel.

Achieving the required level of functional safety is a detailed task that can only be undertaken by qualified engineers. Our global network is there to support this work by providing the information needed for the best solution.

### The focus is on making machines safer

#### Index

On the safe side with SMC .....	p. 3	Components for machine safety .....	p. 18
SMC for first class state-of-the-art safety .....	p. 4	Symbols .....	p. 19
Our guide to your safe machine design .....	p. 5	Practical examples .....	p. 20
5 steps to safety .....	p. 6	Standards references .....	p. 34
FAQ in safety engineering .....	p. 14	SMC products .....	p. 36
Safety over Fieldbus with PROFIsafe .....	p. 16	Global engineering network .....	p. 40
Use of sensors in pneumatics .....	p. 17	Safety standard ISO 13849-1 .....	p. 42

# SMC for first class state of the art safe

**Stand up to the toughest requirements.** At SMC, top priority is given to the development of the highest quality, innovative products that have excellent performance.

Due to the continuous progress being made in production and mechanical engineering, safety is becoming increasingly important. With the introduction of the Machinery Directive 2006/42/EC, machinery manufacturers across the world have to comply with new requirements and harmonised standards in the design and development of their machines when delivering products to Europe.

We have many engineers located around the world in our Technical Centres in Japan, the United States, Europe and China. Quick, clear and detailed responses to customer requests are communicated through our sales group, and our engineers are constantly on the alert for new trends that lead to new world class products and solutions.





# Our guide to your safe machine design

**Safety concepts driven by expertise.** In addition to hazard analysis and risk assessment, a concept for a safe control system is required.

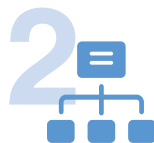
**ISO 13849-1 deals with safety-related components and their design guidelines for control systems.**

## The way to optimal safety – Key question



### Guidelines & standards research

- Which potential hazards can occur with my machine and how do I evaluate them?
- Can this be considered a safety function? Can the failure of this function be hazardous to personnel?
- Is my protective equipment dependent on a control system?



### Definition of safety chain

- Which safety functions are suitable for the respective hazards?
- Which performance level does my risk assessment indicate?
- Are design measures enough to minimise the hazard?
- What options do I have for achieving the required performance level?
- Which components belong to the safety function?



### Safety related key figures

- How often will the safety function be required?
- Does the safety system's service life correspond to that required by the standard?
- To what extent must I be able to detect a safety function's failure?



### Technical implementation

- How do I design a standardised circuit?
- Does a circuit have to be evaluated by an external assessor?
- What documents do I need for CE conformity?
- In what form must the documentation exist?
- How long must the documentation be retained for?



### Validation

- Was the required performance level actually achieved?
- Have I completed the activity based on latest state of the art?
- Were all safety principles properly implemented?
- Have I analysed all the possible misuses that could be expected?
- Does my quality assurance system comply with the requirements in the standard?

On the following pages, find out more about the relationship between the key considerations and the requirements in terms of the Machinery Directive and ISO 13849. SMC is happy to support you as your competent partner!

## 5 steps to safety

With the following 5 steps, we will take you through the entire process from risk assessment to safety function



**1** Risk  
assessment

**2** Risk  
reduction

**3** The control  
system as a  
component of  
risk reduction

**4** Specification of  
the machine's  
safety  
functions

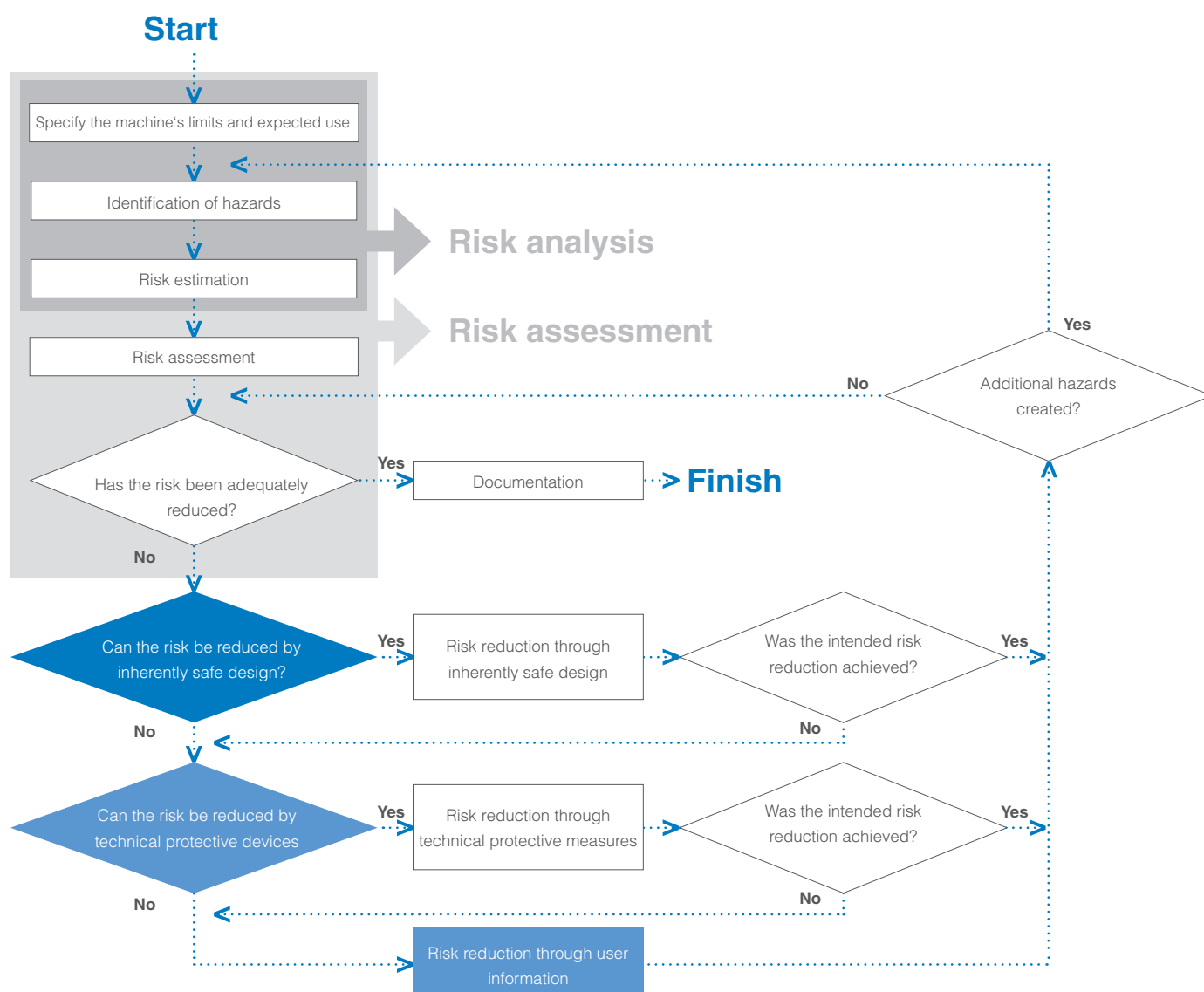
**5** Determination  
of the achieved  
performance  
level PL



# 1 Risk assessment

**Comprehensive safety engineering** begins with the concept and design for the system. Potential hazards and risks are analysed as per ISO 12100. If elimination is not possible, then risk reduction is required. This involves evaluating all of the operating states of the system: automatic mode, maintenance mode, cleaning, etc.

## Carrying out the risk assessment as per ISO 12100 in a simplified version

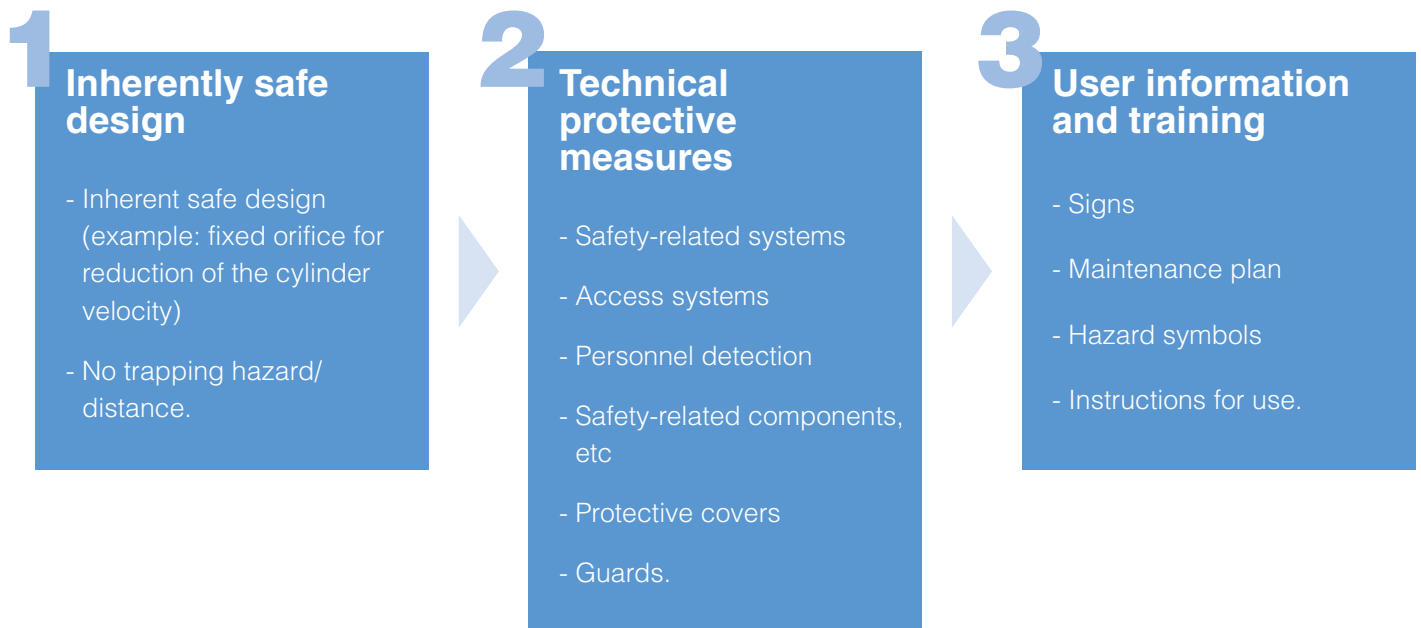


# 2

## Risk reduction

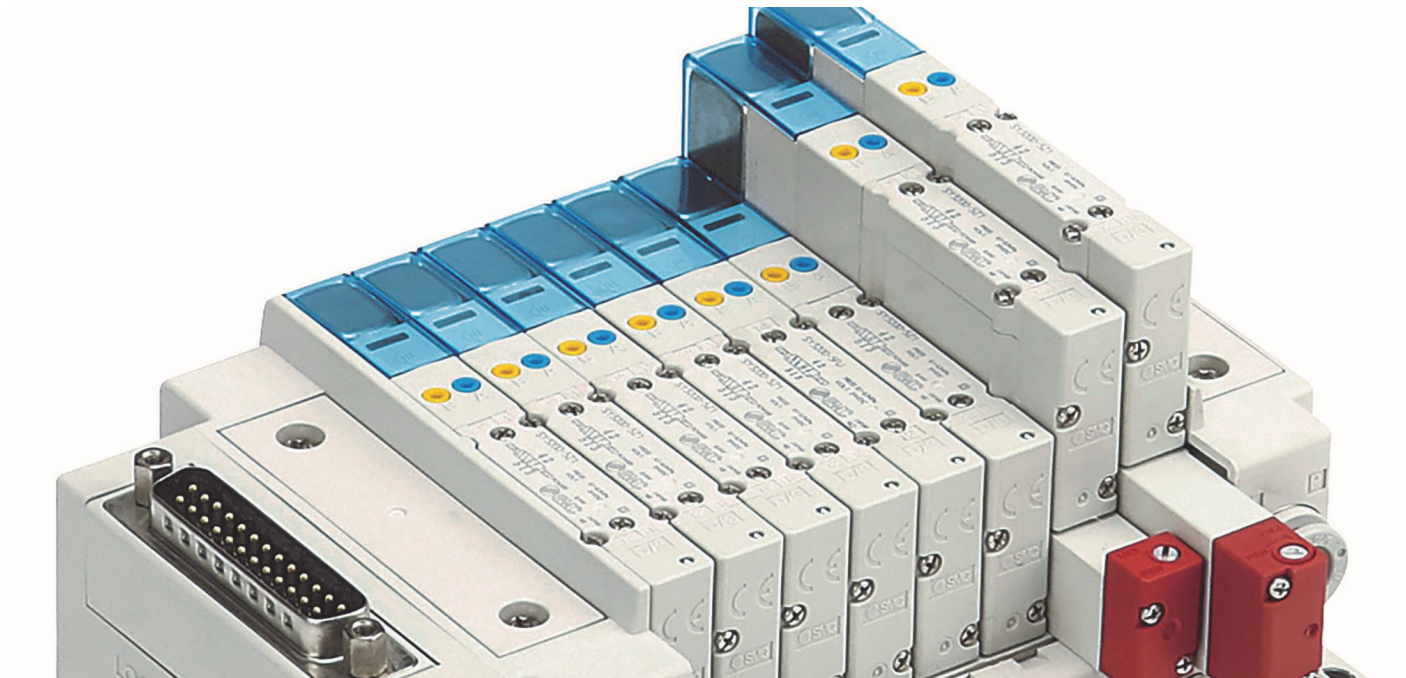
If not all potential risks could be completely eliminated in step 1, ISO 12100 requires three further measures for risk reduction. In this case, the sequence must be strictly observed.

### Measures for risk reduction





### 3 The control system as a component of risk reduction



If **design-related solutions** are insufficient for mini-mising the risk adequately, ISO 12100 requires the application of protective devices.

The performance requirements of the safety-related components of a control system for this type of protective equipment is included in ISO 13849, which is applicable to pneumatic as well as mechanical, hydraulic and electronic control systems.

In steps 4 and 5, there is a description of how to determine the required performance level  $PL_r$  which serves as a guideline for the achieved performance level,  $PL$ .

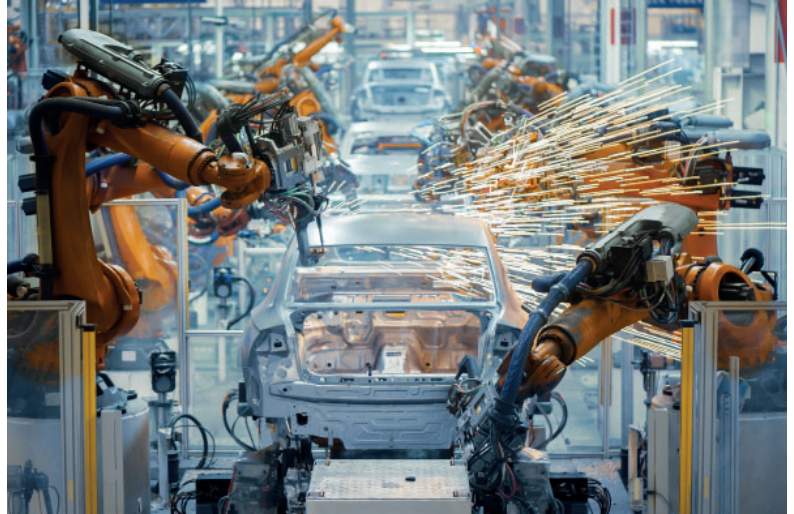
# 4

## Specification of the machine's safety functions

### The control system as a component of risk reduction

**Now the safety functions** need to be specified. This includes the defining of the actual safety functions – such as safe positioning, safe venting, prevention of unexpected start-up or similar – and creating block diagrams for the safety-related components, as well as specifying the required reactions in the event of a fault.

A performance level requirement  $PL_r$  is determined for each safety function using the risk-graphs.



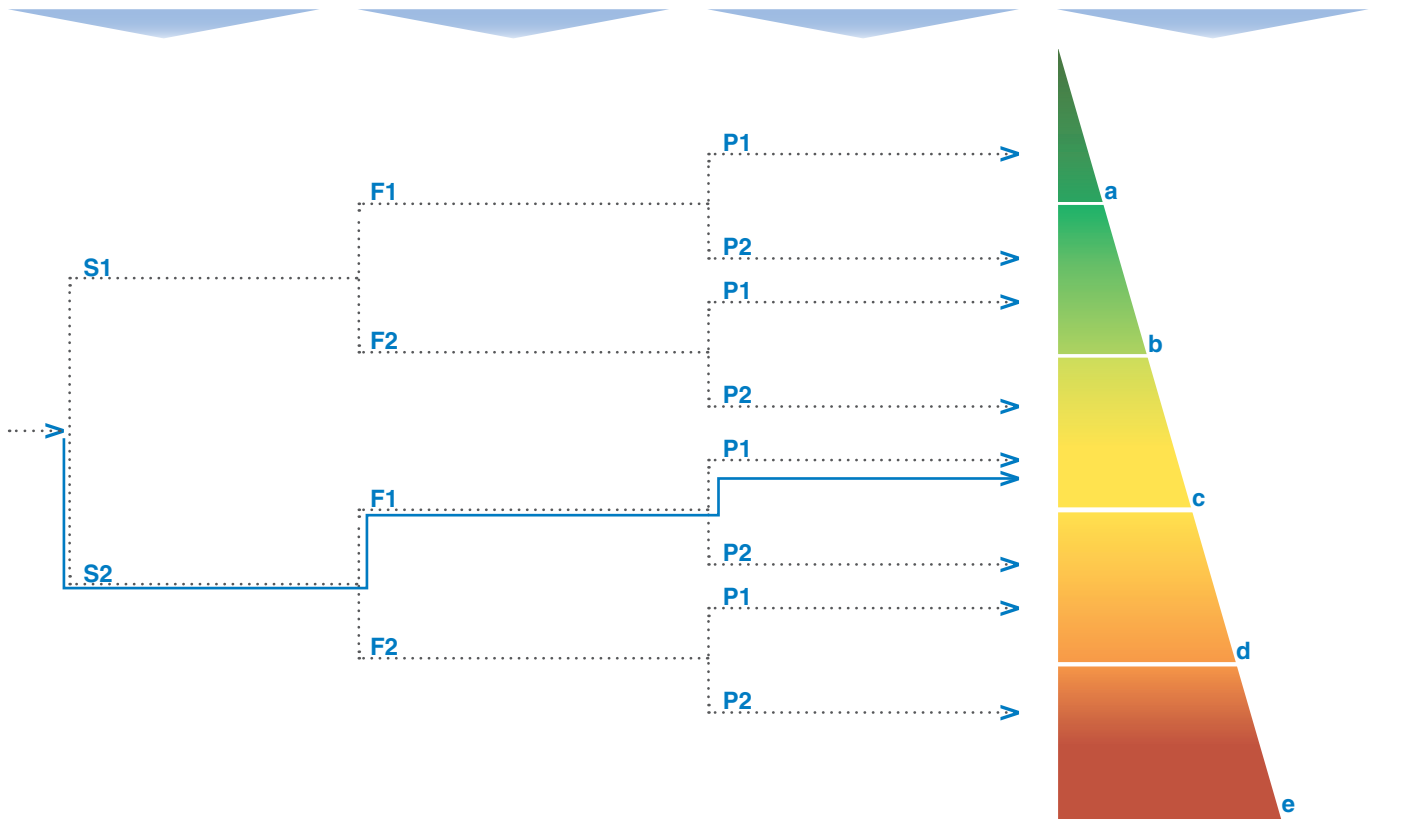
### ISO 13849-1 – Risk graph – to define the required Performance Level

**S:** Severity of injury

**F:** Frequency and exposure to hazard

**P:** Possibility of avoiding hazard

Level of risk



**S1:** Minor injury (commonly a reversible injury)

**S2:** Death or severe injury (commonly an irreversible injury)

**F1:** Seldom to occasionally

**F2:** Frequently to continuously

**P1:** Possible under certain circumstances

**P2:** Nearly impossible

**PL<sub>r</sub>**



## 5 The control system as a component of risk reduction

**For the evaluation** of the safety related system, the performance level PL is determined based on the following:

- Structure (category)
- $MTTF_D$  (Mean Time to Failure dangerous): Mean time to dangerous failure
- $DC_{avg}$  (Diagnostic coverage average) - Average diagnostic coverage level
- CCF (Common cause failure): faults with a common cause
- Response of safety functions under fault conditions
- Safety-related software
- Systematic failures
- The capability to execute safety functions under foreseeable environmental conditions

The process marked with blue arrows on the following double page will assist you with determining the performance level. Based on the four basic parameters (category,  $MTTF_D$ , DC and CCF) it should be determined that the actual performance level, PL, corresponds to no less than the required performance level  $PL_r$  from the risk graph (on page 10).

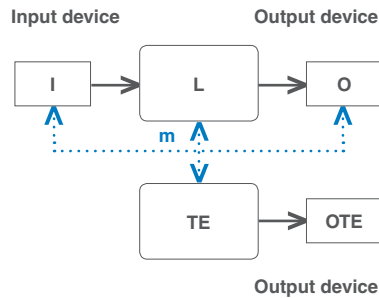
### Applicable for category B and category 1



I: Input device (e. g. sensor)  
 L: Logic unit (e.g., PLC)  
 O: Output device (e.g., valve, relays)

MTTF<sub>D</sub> category 1 is higher than category B, therefore the probability of a safety function failure is lower. Nonetheless, a fault can lead to a loss of a safety function.

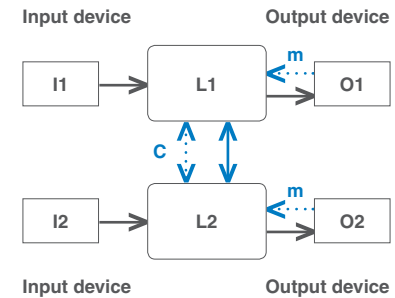
### Applicable for category 2



m: Monitoring  
 TE: Test equipment  
 OTE: Test equipment output

In category 2, a fault can lead to the loss of a safety function between checks and the loss of the safety function is detected by the check.

### Applicable for category 3 and category 4



m: Monitoring  
 C: Cross monitoring  
 ..... cat. 3: Periodic testing  
 — cat. 4: Testing prior to every command for a safety function

In category 3, a single fault does not lead to the loss of the safety function

In category 4, a single fault is detected at or before the next demand on the safety function. If that is not possible then an accumulation of faults shall not lead to a loss of the safety function.

Feature	Category				
	B	1	2	3	4
Design according to relevant standards, withstand the expected operating conditions	X	X	X	X	X
Basic safety principles	X	X	X	X	X
Well-tries safety principles		X	X	X	X
Well-tries components		X			
Mean Time to Dangerous Failure MTTF <sub>D</sub>	Low to medium	High	Low to high		High
Fault detection (Checks)			X	X	X
Single-fault tolerance				X	X
Consideration of fault accumulation					X
Average diagnostic coverage – DC <sub>avg</sub>	None		Low to medium		High
Measures against CCF			X	X	X
Mainly characterised by	Component selection		Structure		



1	Structure of hardware	Category	Structure of the safety function (configuration of I, L, O). The category is comprised of I (input), L (logic) and O (output).		5 levels	B 1 2 3 4	
2	Lifetime of components	MTTF <sub>D</sub>	<b>1 single component</b> 1. MTTFD-value provided by the manufacturer 2. MTTFD determination by ISO 13849-1, Annex C  If the B <sub>10D</sub> -value is known, the following formula is applied: $MTTF_D = \frac{B_{10D}}{0.1 \times n_{op}}$ *The machine manufacturer must determine the n <sub>op</sub> value (How many times the part operates in one year)	<b>2 Complete system</b>  $MTTF_D = \frac{1}{\sum_{i=1}^n \frac{1}{MTTF_{Di}}}$	3 levels	Low	3 years or more, less than 10 years
		B <sub>10D</sub>				Medium	10 years or more, less than 30 years
		n <sub>op</sub> *				High	30 years or more, no less than 100 years
3	Monitoring the system	DC <sub>avg</sub>	<b>1 single component</b> Determination of DC by ISO 13849-1, Annex E  Determination of DC via FMEA	<b>2 Complete system</b>  $DC_{avg} = \frac{\sum_{i=1}^n \frac{DC_i}{MTTF_{Di}}}{\sum_{i=1}^n \frac{1}{MTTF_{Di}}}$	4 levels	None	Less than 60 %
		DC				Low	60 % or more, less than 90 %
		MTTF <sub>D</sub>				Medium	90 % or more, less than 99 %
						High	99 % or more
4	System stability	CCF	The aim is to achieve no less than 65 points referring to the scoring checklist in ISO 13849-1, Annex F (starting with category 2)		2 levels	No	Less than 65 points
						Yes	65 points or more

	Category						
PL	B	1	2		3		4
a	MTTF <sub>D</sub> Low		MTTF <sub>D</sub> Low		MTTF <sub>D</sub> Low		
b	Medium	MTTF <sub>D</sub>	MTTF <sub>D</sub> Medium		MTTF <sub>D</sub> Medium		
c		High	High		High		
d							MTTF <sub>D</sub>
e							High
DC <sub>avg</sub> =	Without	Without	Low	Medium	low	Medium	High
CCF=	Irrelevant		65 points or more				

SMC will provide you with the necessary safety-related data for calculations.



## 1 Is it an operational function, or a safety function?

An operational function is a function that is necessary for the machine or equipment to fulfill its intended purpose. The failure of an operational function does not result in a loss of safety function.

A safety function is one that the failure and/or malfunction of which endangers the safety of persons, but it is not necessary in order for the machine to function.

## 2 Do pneumatic components require a safety-related assessment?

Yes, for example pneumatic actuators such as cylinders can also cause serious injuries, they are also to be evaluated as per ISO 12100, and if needed, safe-guarded by design or control-related measures. Pneumatic or electro-pneumatic controls must be evaluated and implemented as per ISO 13849-1 and -2.

## 3 What does “prevention of unexpected start-up” mean?

The safety function “prevention of unexpected start-up” means that the safety-related system controls the start-up sequence in such a way as no hazardous unexpected movements occur. After an energy outage (compressed air supply, compressor failure or a hose rupture) and a new start-up, the machine may not start automatically without receiving a separate start command.

## 4 Can bi-stable valves be used in safety functions?

The list of safety-principles contained in ISO 13849-2 contains the following point: “Safe Position”, which must be met by safety-related products and systems. Safe position’ means that a moving element of a component (eg. spool of valve) is mechanically retained in a fixed position. Friction only is not mechanical retention. Normally double solenoid valves with rubber seal are held in the last position only by friction; that’s why this principle is not satisfied. According to safety principles, mechanical retention is required for Category 1 or higher.

Bi-stable valves are permitted if they have a detent (mechanical lock) in the final position. Metal-sealed valves and some special rubber-sealed valves made by SMC have this type of detent and therefore can be used in safety-related control systems. In addition, it should be determined on an application basis whether unexpected and/or dangerous movements can occur as the result of a power loss or on machine start-up.

## 5 Is a valve, for which both the supply voltage and separately the pilot air is interrupted, considered to be a two-channel solution?

No, a two-channel solution must at least be “fail-safe”, which means that a single failure in the safety chain (such as failure to activate a valve) cannot result in the loss of the safety functions. This does not apply to a cylinder control valve, because a failure in the spool of the main valve (e.g. contamination that blocks the spool) can lead to the failure of the entire system.

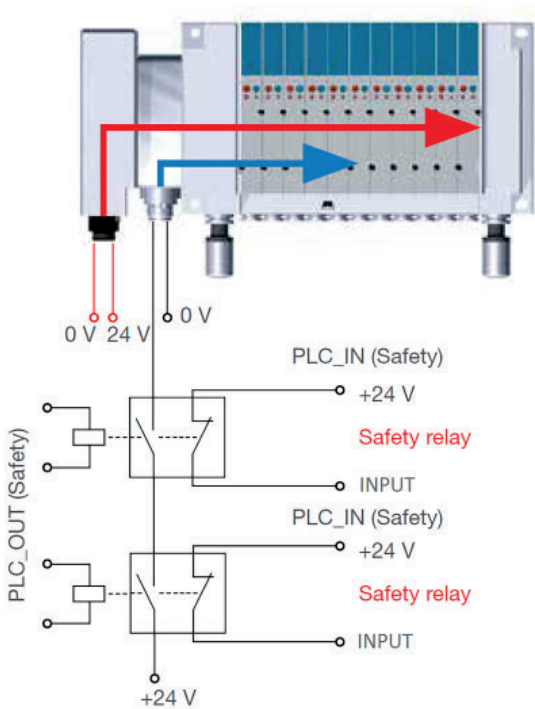
## 6 Is it possible to safely electrically isolate the supply to valves that are manifold mounted?

**There are a number of possible solutions:**

- Electrically isolate the power supply to a level of security that is appropriate to the required PL. e.g. EX245, EX250, EX260, EX600.
- In the case that a safe zone and unsafe zone is required in the manifold then EX9-PE1-X15/X22/X23 are available.
- Fieldbus system using PROFIsafe protocol is also available e.g. EX245-FPS#-X35. This range of products provides electrical isolation of the valves in up to three independent zones to Cat4/PL e acc to EN ISO 13849-1, SIL CL3 acc to IEC62061/IEC61508.

## 7 Do products used as safety related parts of a control system (SRP/CS) need to be tested or certified by an organization independent of the manufacturer?

No, ISO 13849-2 states that a third-party test is not required providing the validation process is carried out by persons independent of the design of the SRP/CS.



## 8 A safety-related PLC is very expensive. Can I also carry out my safety functions purely pneumatically?

In principle, it can be said that the safety functions which have electro-pneumatic actuation can also be carried out purely pneumatically. The cost-effectiveness of your own safety PLC depends on the complexity of the desired safety functions and the related operating functions. Special attention is given to the sensor technology required in ISO 13849 for fulfilling the diagnostic coverage level for category 2 and above. To realize this solely with pneumatics would generally be much more expensive.

## 9 Where can I find the safety-related data of SMC components?

SMC will gladly provide you with all safety-related data, such as B10 and MTTF. In addition, SMC has a SISTEMA library available. SISTEMA is a program for the calculation of your safety functions, which is provided free of charge by the German Institute for Occupational Safety and Health (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, IFA). Contact your local sales office for more information about the SISTEMA library.

## 10 What does a pneumatic LoTo (Lockout-Tagout) look like?

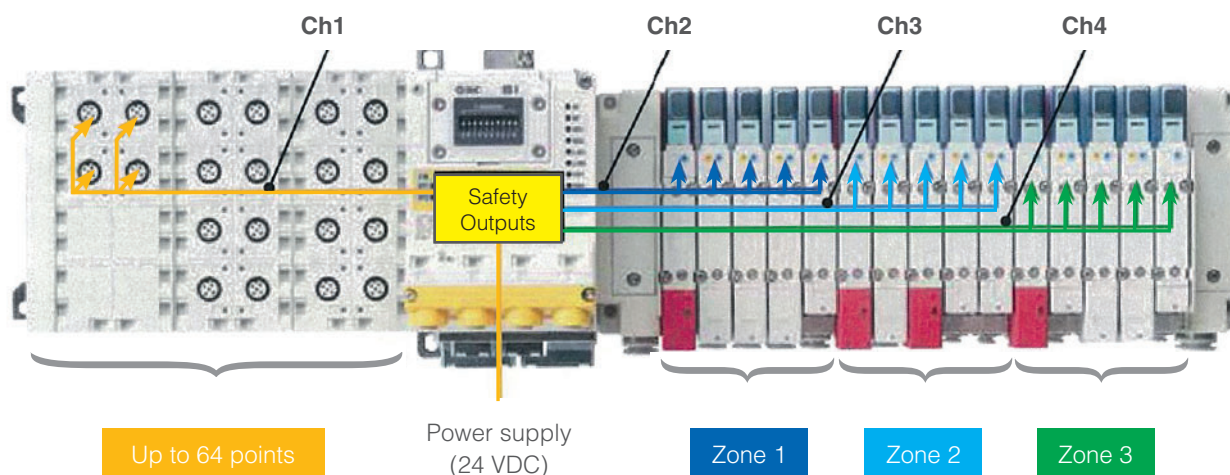
LoTo's (Lockout-Tagouts) are devices which lock the control elements of a system – such as switches, stopcocks, ball valves, etc. – into a specific position. They are used as prevention of unauthorised access or unexpected start-up, for example during a maintenance procedure. If configuration or maintenance procedures are carried out in a depressurised state, it is possible to lock an SMC pressure relief 3 port valve with locking holes (VHS) in the vented position.





# Safety over Fieldbus

SMC has a solution for Safety over Fieldbus with the EX245-FPS#-X35, which is a fully certified PROFIsafe product for use in safety applications up to PL e acc. to EN ISO 13849-1 and SIL 3 acc. to IEC 62061/IEC 61508.

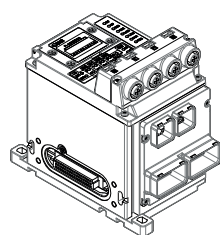


## Safe outputs - 4 power zones

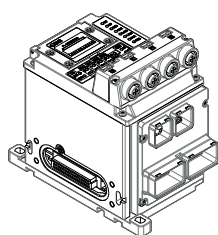
- 3 zones for valve output (8 points for valve output per zone)
- 1 zone for output module
- Built-in wiring for each power zone, no separate wiring needed.

## Safe inputs: 4 input connectors

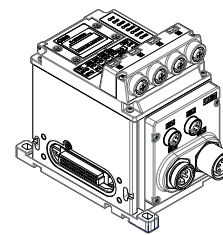
- Single channel: 8 points (SIL2/PLc)
- Dual channel: 4 points (SIL3/PLe)
- 2 channels of power supply.



**EX245-FPS1-X35**  
Use with fibre optic cable



**EX245-FPS2-X35**  
Use with copper cable



**EX245-FPS3-X35**  
Use with copper cable

## Connectors – Available with a variety of power connector & media interfaces

- Copper or fibre optic communications
- Push/pull or circular power & communications connectors.

## General

- Comprehensive system of diagnostics and error reporting
- Same mechanical footprint as existing EX245 PROFINET product series
- Compatible with EX245 I/O modules and applicable valve manifolds.

# Use of sensors in pneumatics

**Sensors can be used to determine the state of a system** with regard to pneumatic pressure or position of valve spools to provide diagnostic feedback as required for category 2 or above.

The supervisory controller (safety PLC) can determine if a digital or analogue sensor signal changes as expected within a specific time period.

For example, the final position switch of the respective cylinder must transmit a change signal within a pre-defined time period after a valve has been actuated.

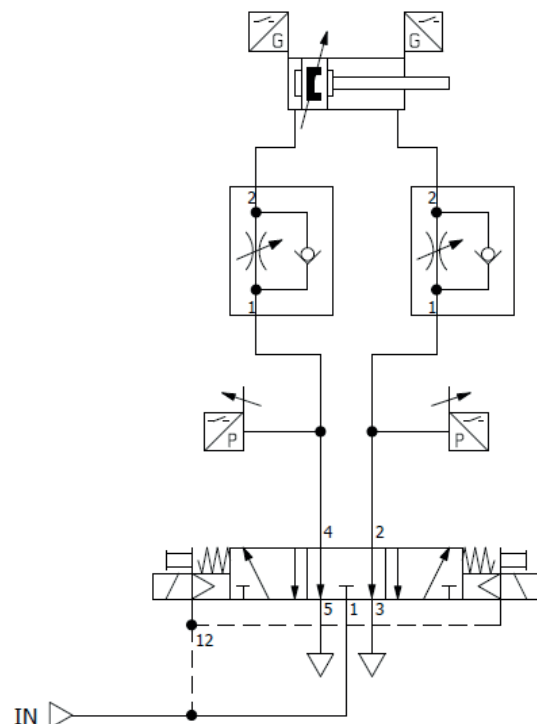
## Example

### Sensors:

- Position switch
- Pressure switch
- Detection of valve position with pressure switch.

### Detectable error from the list in ISO 13849-2:

- Change of switching times
- Non-switching or incomplete switch
- Spontaneous change of the initial switching position (without input signal).

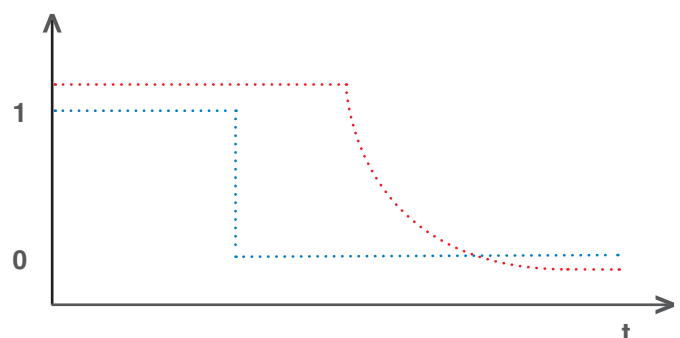


Detailed product information can be found in the respective instruction manuals. In addition to the listed information, the observance of legal references found on page 39 is mandatory.

## Diagram 1

### Sensors:

- Blue Line: Valve switching output
- Red Line: Pressure at a pressure switch
- The control system must output a fault if the pressure does not drop within a predefined time after switching the valve



# Components for machine safety

## Definitions and characteristics



**As per the Machinery Directive 2006/42/EC, article 2c,** a safety component is a component

- which serves to fulfil a safety function,
- which is independently placed on the market,
- the failure and/or malfunction of which endangers the safety of persons, and
- which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.

### Note

The safety component is evaluated **by the component manufacturer** in terms of safety and will be CE marked under the Machinery Directive. This eliminates the need for an additional validation process to be carried out by the safety system designer as per ISO 13849-2.

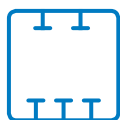
For safety-related control, standard components as well as safety components can be installed as decided by the safety system designer. However, this must be evaluated during the course of the system analysis.



# Symbols

## Safety functions and emergency stop

### Pneumatic safety functions



Safe stopping and closing



Safely reduced pressure



Safe venting



Two-hand control



Safe direction



Prevention of unexpected start-up



Safe direction



Emergency stop (extended safety function)

### The emergency stop function

Every machine must be equipped with an **emergency shutdown function**. It provides the opportunity to place the machine in a safe state in a hazardous situation.

# Practical examples

page 22

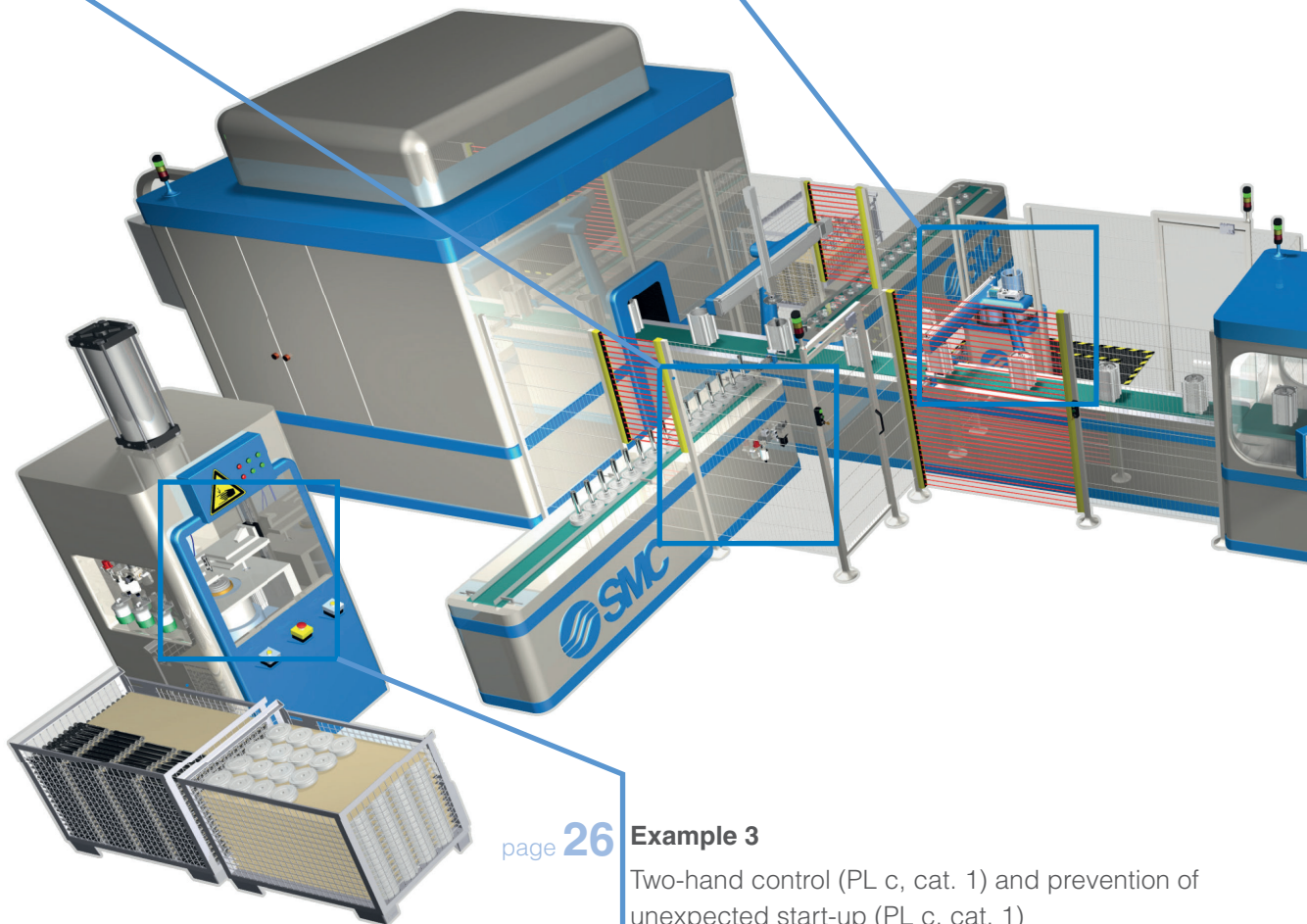
## Example 1

Safe venting (PL e, cat. 4) and prevention of unexpected start-up (PL e, cat. 4)

page 24

## Example 2

Safe stopping and closing (PL d, cat. 3) and prevention of unexpected start-up (PL e, cat. 3)



page 26

## Example 3

Two-hand control (PL c, cat. 1) and prevention of unexpected start-up (PL c, cat. 1)

**Based on our sample system,** there are six practical examples described, which show not only the basic considerations, but also tips on implementation.

Please note that the listed standard references are not intended to be complete, and serve solely as a guide. The listed performance level is only applicable to the shown structure. Lifetime parameters, diagnostic coverage level and supplementary sub-systems (input and logic units) must be evaluated by a suitably qualified engineer responsible for the safety of the machine.

### Note

To support the design of your safety functions, you will find common practical examples on the following pages.

page **28**

#### **Example 4**

Safe stopping and closing (PL d, cat. 3)  
and prevention of unexpected start-up (PL d, cat. 3)

page **32**

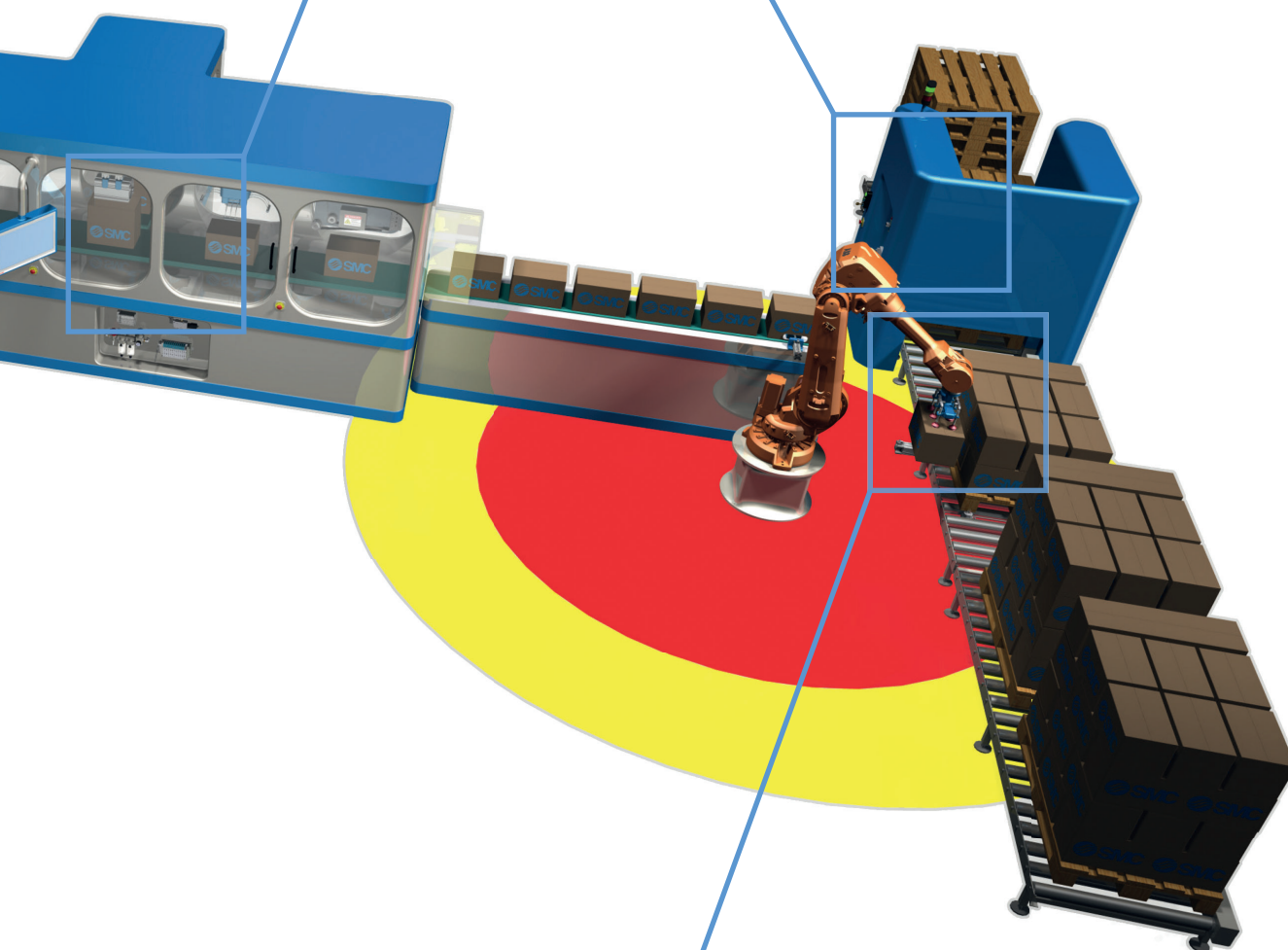
#### **Example 6**

Safely reduced pressure (PL b, cat. B)

page **30**

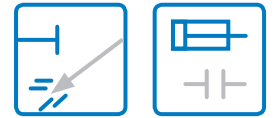
#### **Example 5**

Safe venting (PL c, cat. 1) and prevention of  
unexpected start-up (PL c, cat. 1)



## Example 1

### Safe venting (PL e, cat. 4) and prevention of unexpected start-up (PL e, cat. 4)



#### Initial situation

The opening of the protective door must cause the pneumatic system to be vented. In so doing, no unexpected machine start-up may occur within the hazardous area during maintenance procedures.

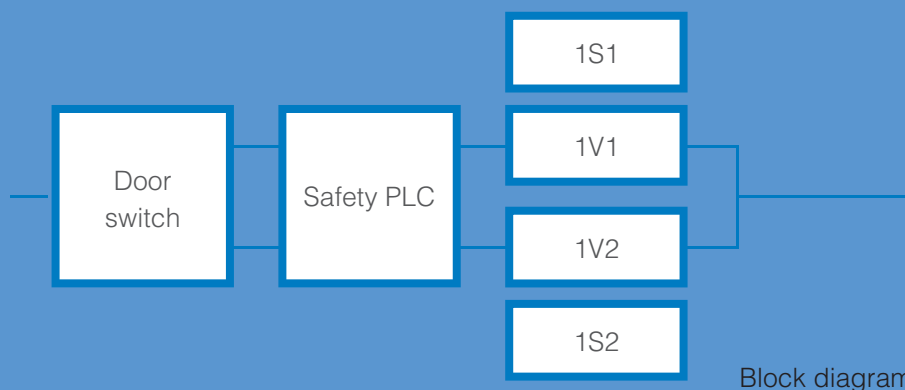
#### Information regarding implementation

- The **valve's venting capacity** must be designed so that immediately upon entering into the hazardous area, no further dangerous movement can occur within the area.
- **Downstream to the residual pressure relief valve**, no assemblies may inhibit or delay safe venting (e.g., by defective downstream components).
- Regular **checks of the performance of the system** must be carried out to confirm correct venting capability.
- The safety component does not require validation as per ISO 13849-2, because it has already been validated by the component manufacturer during the course of the CE conformity process.

Safety components





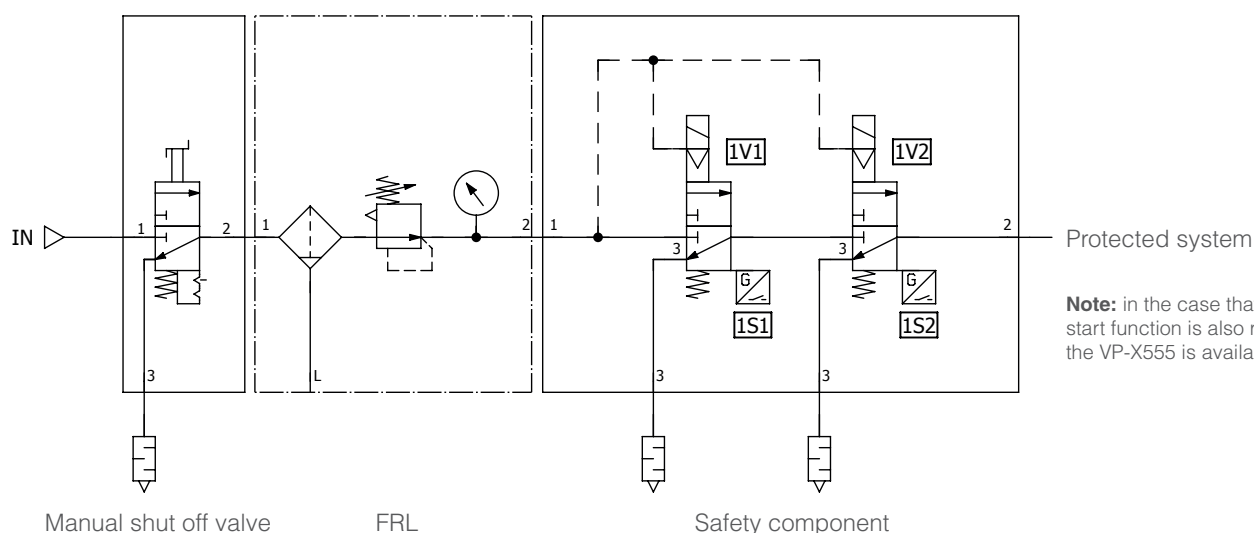


### Circuit description

The desired "safe venting" safety function as well as the prevention of unexpected start-up are implemented by the safety component (1V1 and 1V2) in this example.

The required diagnostic coverage level is also fulfilled (by 1S1 and 1S2). It must be ensured that any

downstream valves can be vented even in the event of a power outage or malfunction. For example, a 3-position valve with a closed centre position may not be used.



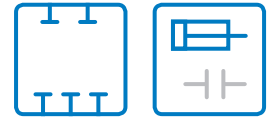
Detailed product information can be found in the respective instruction manuals. In addition to the listed information, the observance of legal references found on page 39 is mandatory.

### SMC products (also see page 36~39)

<p><b>Pressure relief 3 port valve with locking holes</b> Item: <b>VHS</b></p>	<p><b>Residual pressure release valve with detection of de-energised position</b> Item: <b>VG342-X87</b></p>	<p><b>Residual pressure release valve with detection of de-energised position</b> Item: <b>VP-X555</b></p>	<p><b>Residual pressure release valve with detection of de-energised position</b> Item: <b>VP-X538/VP-X585</b></p>

## Example 2

Safe stopping and closing (PL d, cat. 3) and prevention of unexpected start-up (PL d, cat. 3)

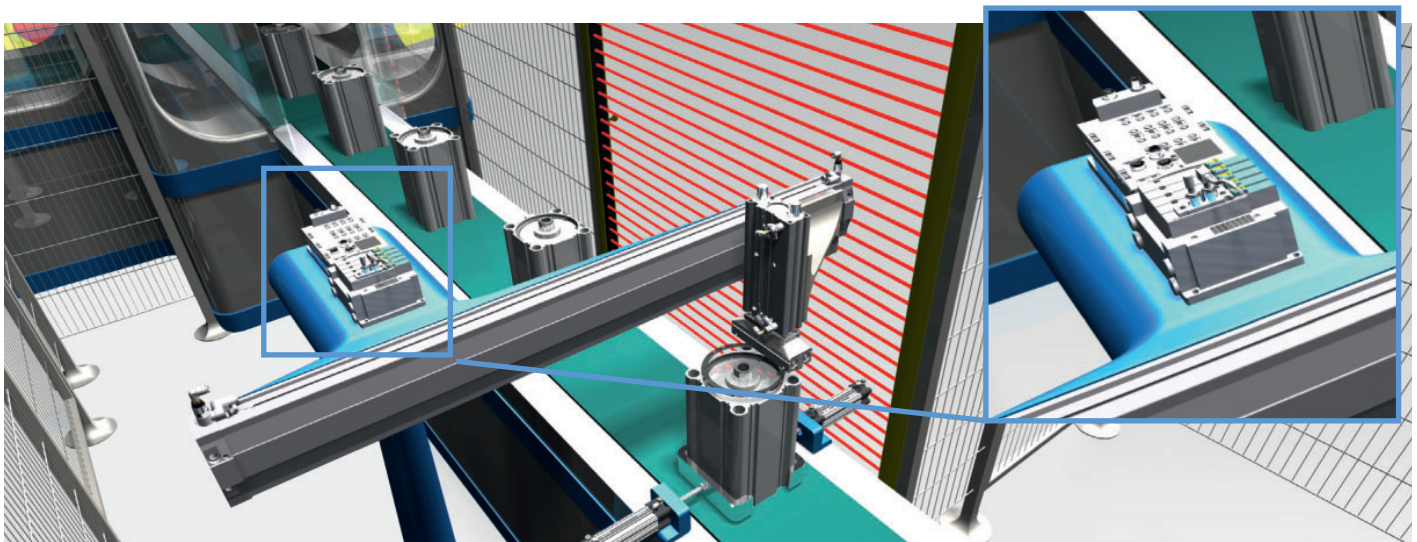


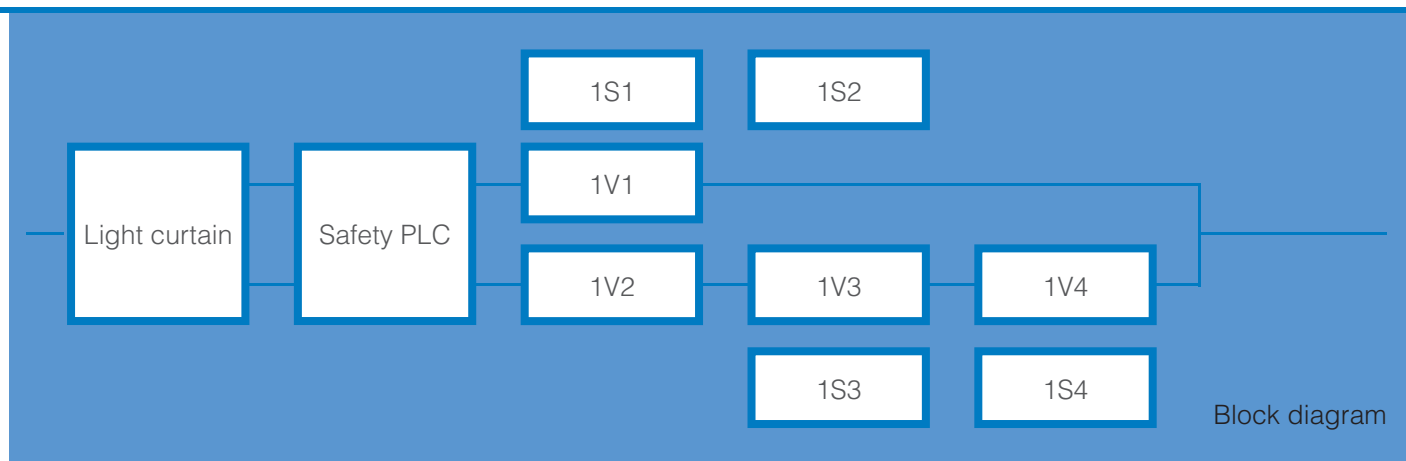
### Initial situation

For the removal of components from the conveyor belt, the downstream drives should stop safely due to the interruption of the light curtain. When carrying out work in the hazardous area it must not be possible for the machine to unexpectedly start up.

### Information regarding implementation

- The **Sensors** must be installed to be tamper-proof and require a special tool or access code to make any adjustments. The **distance between the light barrier** and the hazardous area must be large enough that the safety system can stop the dangerous actuator in a timely manner, before the operating personnel enters into the hazardous area.
- The **de-energising of the safety-related valves** shall not be carried out via the standard serial communication – a safety protocol such as PROFIsafe or another safety technique should be used. Refer to FAQ number 6.
- Particularly with **the vertical installation of actuators**, which are subject to heavy loads, pilot operated check valves should be mounted directly into the cylinder.
- Pilot check valve with state detection can be directly monitored to avoid the usual need to add a regular non-cyclic test routine which requires process time and implementation costs.
- For the pneumatic safety function "Safe stopping and closing", the **cylinder overrun must always be** considered due to air compression.

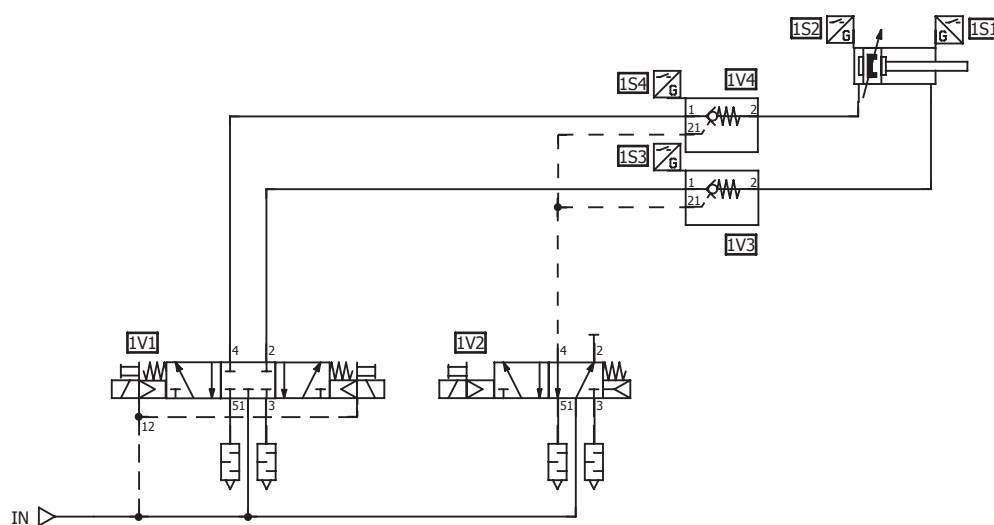




## Circuit description

The first channel of the safety function consists of a 3-position valve (1V1). As shown in the block diagram, the 3-position valve 1V1 needs the sensors 1S1 and 1S2, in order to achieve the required diagnostic coverage level. The second channel consists of a 2-position valve (1V2) and pilot operated check valves with state detection (1V3 and 1V4). In this example, the sensors

(1S3 and 1S4) monitor the functions of the second circuit with components 1V3 and 1V4. Prevention of unexpected start-up, cat. 3, is realized by the 3-position valve with a closed centre position and the pilot operated check valve with state detection. The sensors 1S3 and 1S4 are detecting faults of the whole channel including 1V2.



In the case of valve 1V2, the spool is returned to the OFF position on pressure loss by a mechanical spring. Detailed product information can be found in the respective instruction manuals. In addition to the listed information, the observance of legal references found on page 39 is mandatory.

## SMC products (also see page 36~39)

<p><b>Solenoid valve</b> Item: <b>SY3000/5000/7000</b></p>	<p><b>Solenoid valve</b> Item: <b>SY-X350</b></p>	<p><b>Pilot check valve with state detection</b> Item: <b>XT34-303</b></p>	<p><b>Auto switch</b> Item: <b>D-M9</b></p>

## Example 3

Two-hand control (PL c, cat. 1) and prevention of unexpected start-up (PL c, cat. 1)



### Initial situation

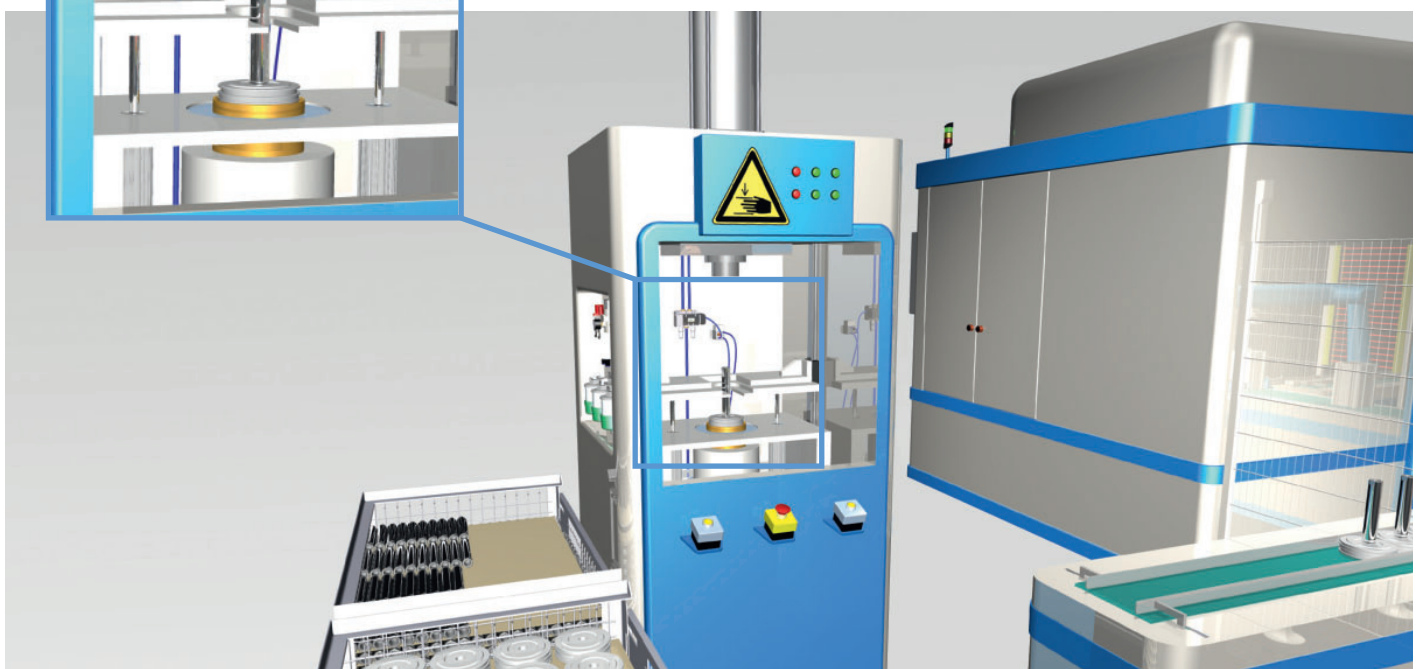
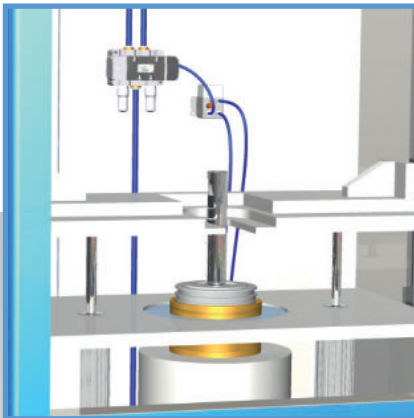
Crimping between the cylinder piston and the piston rod is realized by means of a purely pneumatic press with two-hand control. When the button is released, the press cylinder will move to the upper final position.

### Note

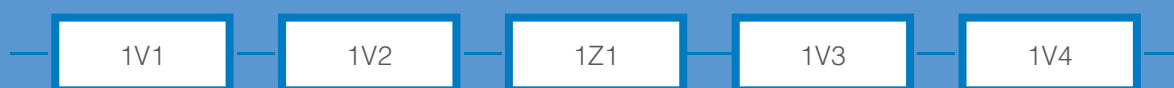
Countries may have specific regulations for industrial presses, these need to be complied with.

### Information regarding implementation

- When reversing the press tool, **the crushing hazard must be** evaluated. Actuating a safety function should not result in the generation of a new hazard. The appropriate response in the event of a failure should be included in the risk analysis.
- EN 574 must be observed with regard to the **distance between both actuation buttons**.
- The **safety component** (1Z1) does not require validation as per ISO 13849-2, because it has already been validated by the component manufacturer during the course of the CE conformity process.



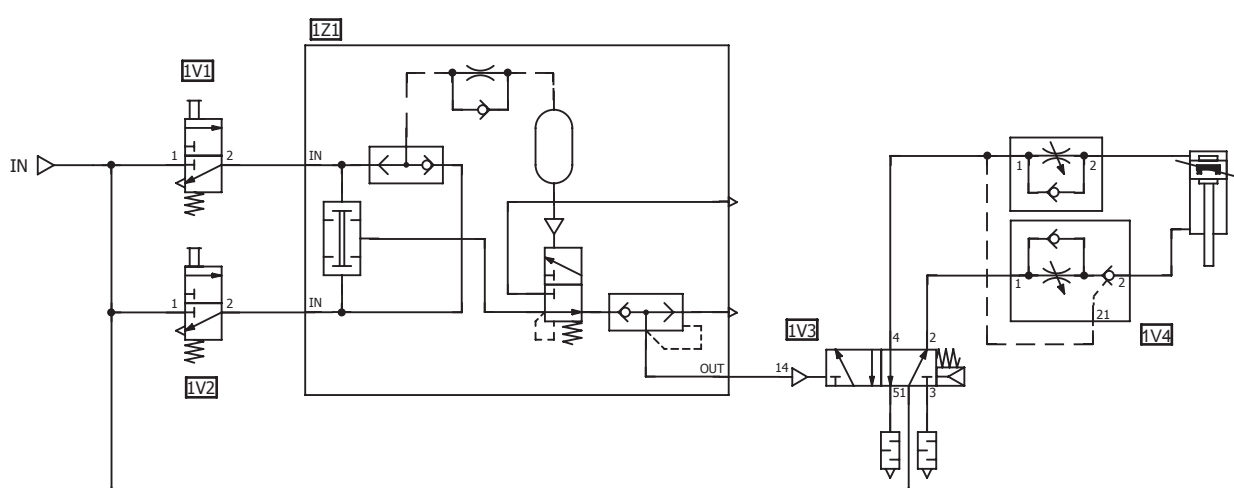




Block diagram

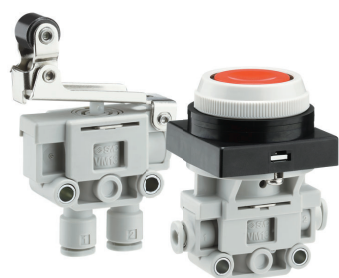
## Circuit description

By pushing both buttons within the required time, a pneumatic output signal on the two-hand control valve (1Z1) is generated. Automatic reverse is realized by means of a pneumatically controlled 2 position valve (1V3), which returns to home position after the pilot signal is removed.



In the case of valve 1V3, the spool is returned to the OFF position on pressure loss by a mechanical spring.

## SMC products (also see page 36~39)



**Manual valve**  
Item: VM



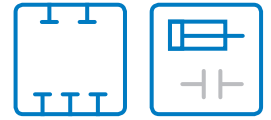
**Two-hand control valve**  
Item: VR51



**5 port air operated valve**

## Example 4

Safe stopping and closing (PL d, cat. 3) and  
prevention of unexpected start-up (PL d, cat. 3)



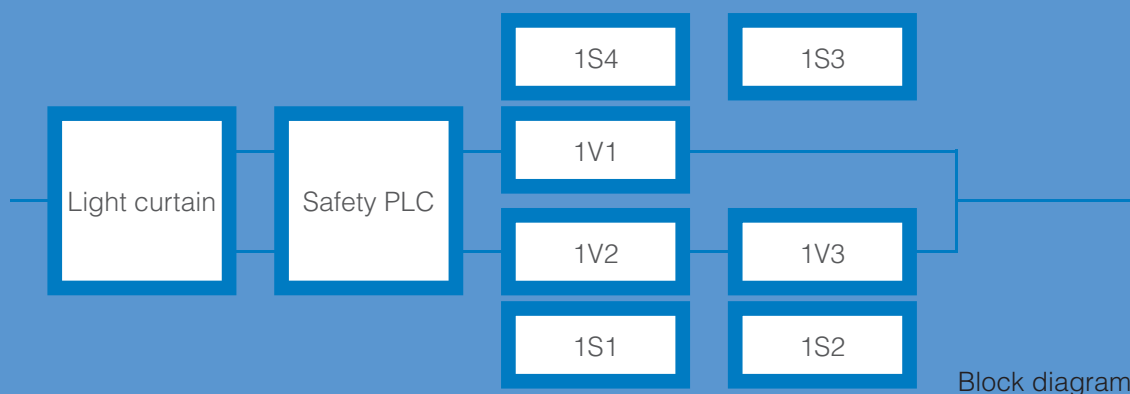
### Initial situation

It must not be possible to open the packaging machine's protective guarding, until all pneumatic drives are at a standstill.

### Information regarding implementation

- The **protective guard** remains closed by means of a dual-channel lock until the drive has come to a standstill.
- For the vertical installation of **actuators**, appropriate measures against possible hose breakage must be taken, e. g. using metal piping.



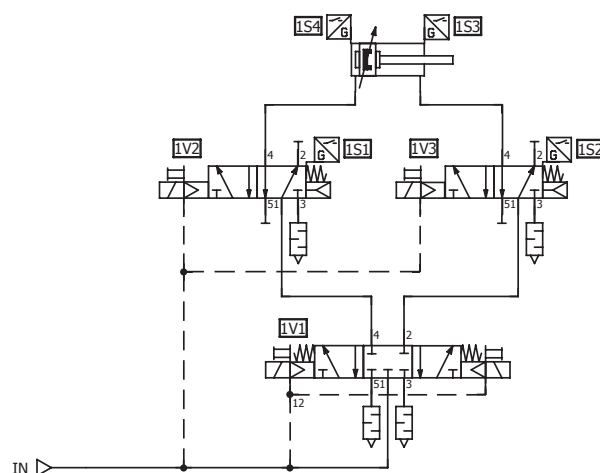


## Circuit description

As shown in the block diagram, the first channel, which is realized by means of the 3-position valve (1V1), needs the respective sensors (1S4 and 1S3) to achieve the required diagnosis coverage level.

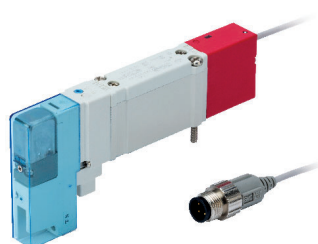
The second channel, consists of two valves (1V2 and 1V3), which are directly linked to the cylinder. In contrast to example 2, by using valves that can be monitored,

regular functional testing of the solenoid valves can be omitted. In this example, the spool detection integrated in the valves (1S1 and 1S2) monitors the functions of the second circuit. Safe stopping and closing and prevention of unexpected start-up in category 3 is realized by the 3-position valve with a closed centre position and the two solenoid valves with spool position detection.

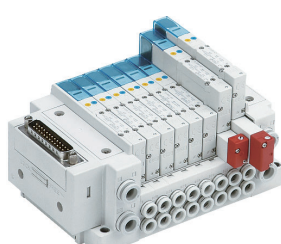


In the case of valve 1V2, and 1V3 the spool is returned to the OFF position on pressure loss by a mechanical spring.

## SMC products (also see page 36~39)



**Solenoid valve  
with indirect monitoring**  
Item: **SY-X30**



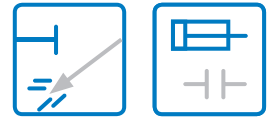
**Solenoid valve**  
Item: **SY**



**Digital pressure sensor**  
Item: **PS1000**

## Example 5

Safe venting (PL c, cat. 1) and prevention of unexpected start-up (PL c, cat. 1)

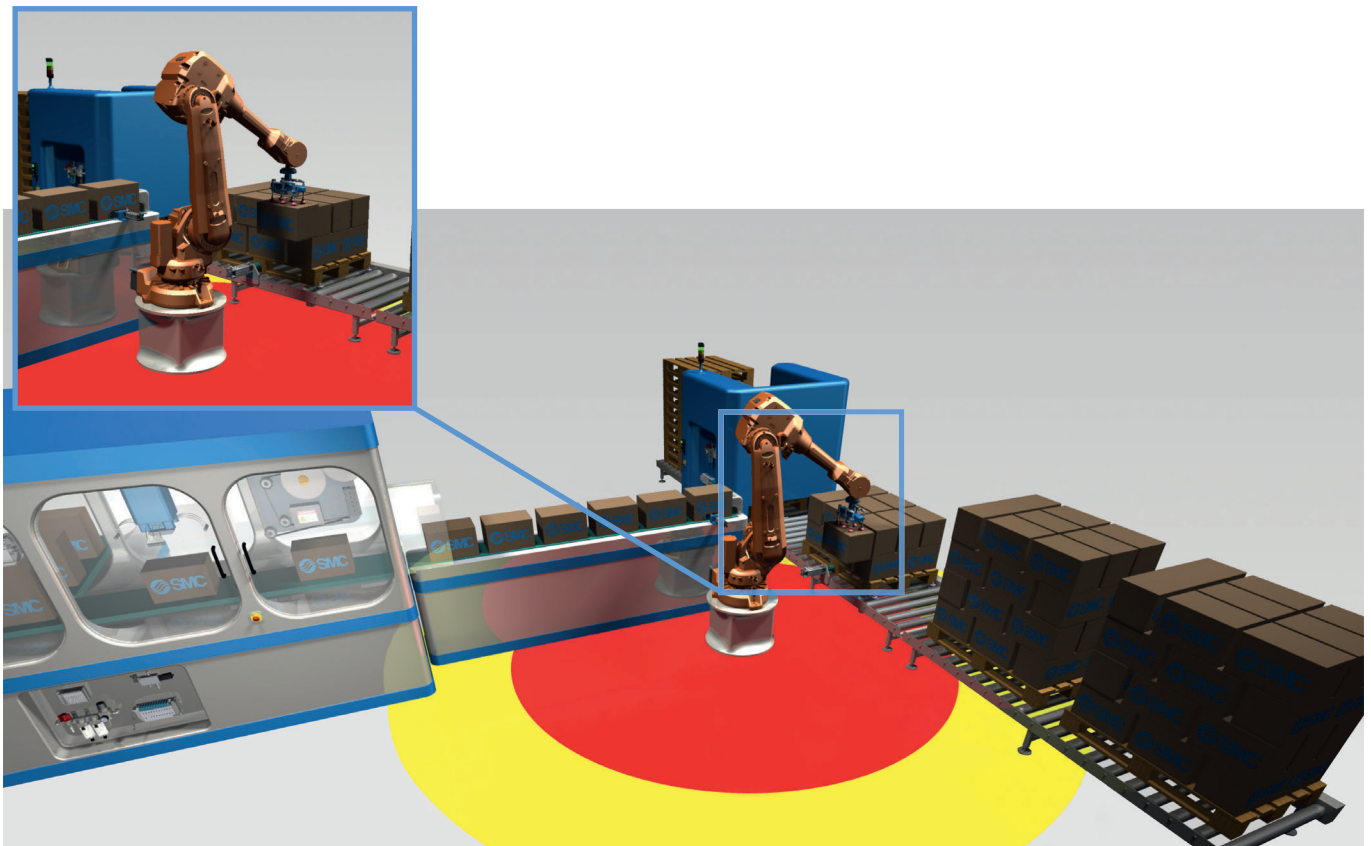


### Initial situation

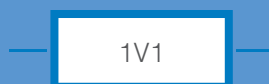
If the operator enters into the hazardous area marked in red, the robot should stop and the pneumatic system should vent safely. The hazardous area is monitored using a laser scanner. In this example the safety requirements for the robot must also be evaluated.

### Information regarding implementation

- The **valve's venting capacity** must be designed so that immediately upon entering into the hazardous area, no further dangerous movement can occur within the area.
- **Downstream to the residual pressure relief valve**, no assemblies may inhibit or delay safe venting.
- Regular **checks of the performance of the system** must be carried out to confirm correct venting capability.



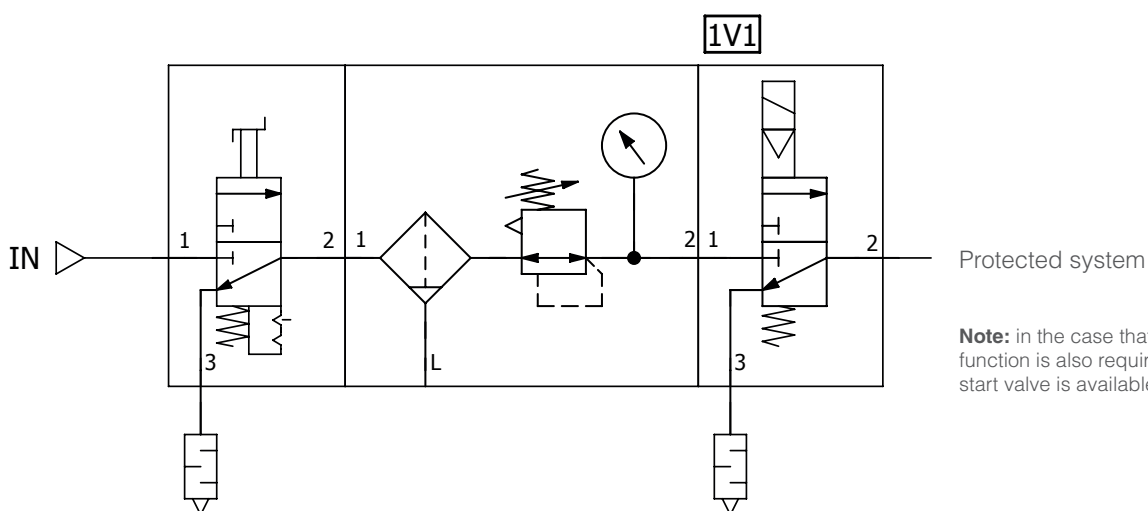




Block diagram

### Circuit description

The valve 1V1, vents the single channel system.  
Diagnostics are not required for category 1.



**Note:** in the case that a soft start function is also required the AV soft start valve is available.

Detailed product information can be found in the respective instruction manuals. In addition to the listed information, the observance of legal references found on page 39 is mandatory.

### SMC products (also see page 36~39)



**Pressure Relief 3 Port Valve with Locking Holes**  
Item: VHS



**Soft start-up valve**  
Item: AV-A



**Pilot poppet valve**  
Item: VP542Y

## Example 6

### Safely reduced pressure

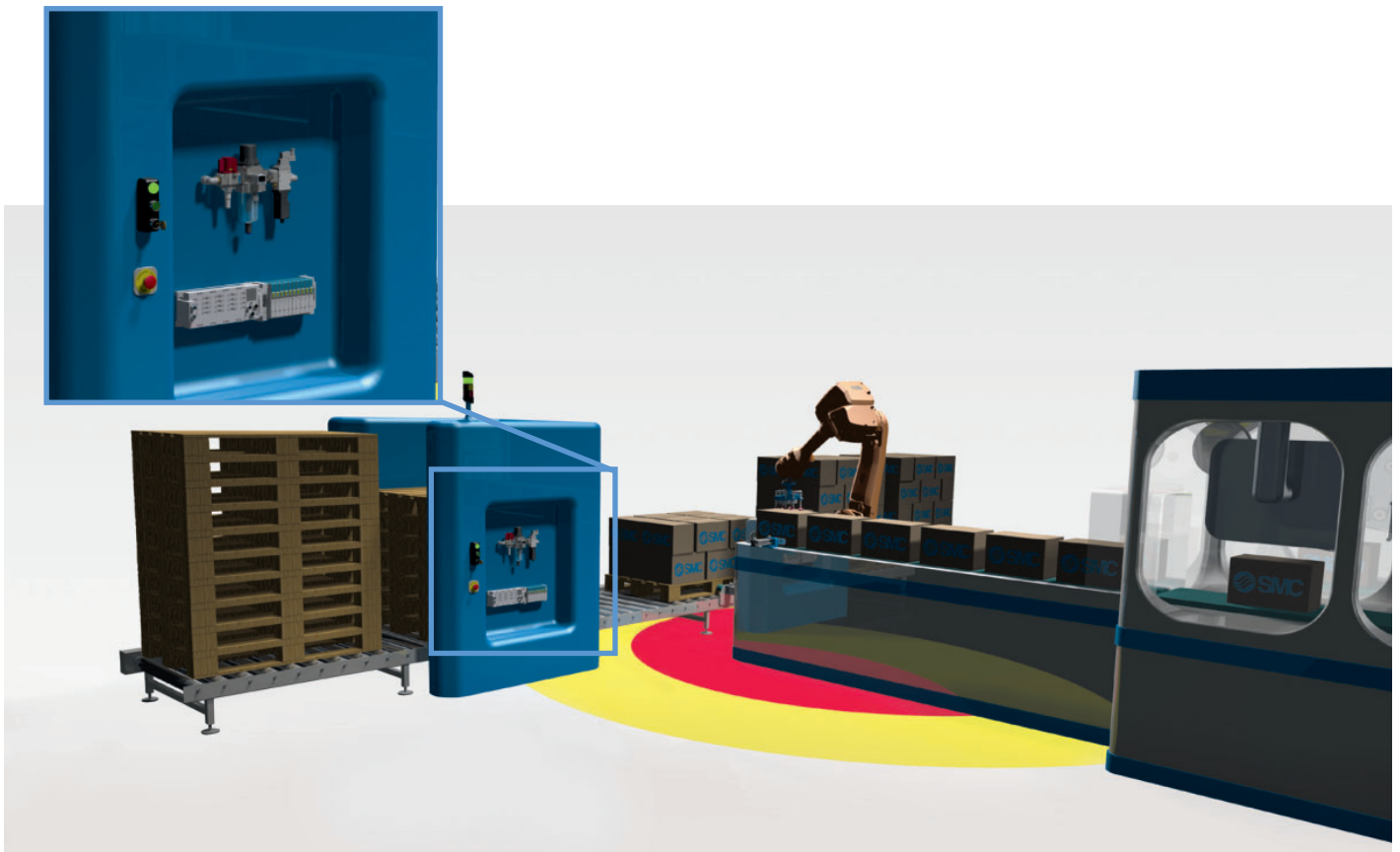


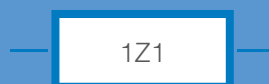
#### Initial situation

During normal operation if the operator enters the hazardous area monitored by the laser scanner then the robot movement is stopped. In the case of maintenance mode the additional hazard due to the pneumatic system needs to be evaluated.

#### Information regarding implementation

- In maintenance mode the pneumatic system pressure needs to be reduced to a safe level to reduce the crushing hazard of the actuator.
- In applications with large lateral forces the sizing is often based on resistance to lateral forces of the bearing of the cylinder. This can result in oversizing of the cylinder and increased risk due to the larger thrust force.

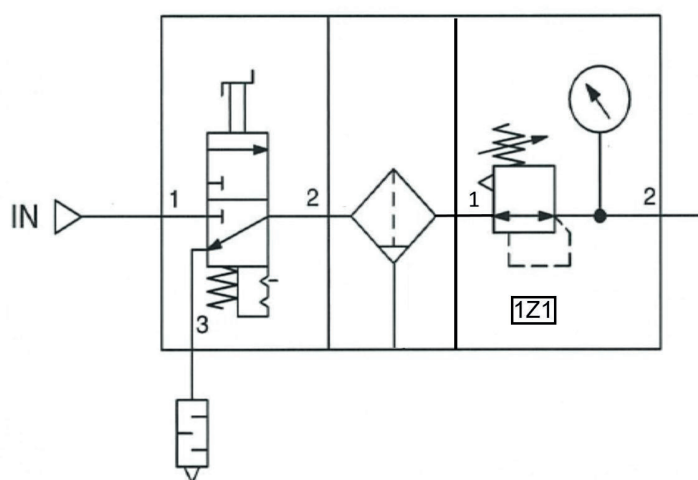




Block diagram





## Circuit description

The supply to the cylinder is switched (circuit not shown) to a secondary circuit with a tamper-proof regular installed (1Z1). Tamper-proof knob cover is required for the regulator.



Detailed product information can be found in the respective instruction manuals. In addition to the listed information, the observance of legal references found on page 39 is mandatory.

## SMC products (also see page 36~39)

			
<p><b>Knob Cover</b> Item: AR□□□P-580AS</p>	<p><b>Regulator</b> Item: AR-B</p>	<p><b>Precision Regulator</b> Item: IR</p>	<p><b>Pressure relief 3-port valve with locking holes</b> Item: VHS</p>

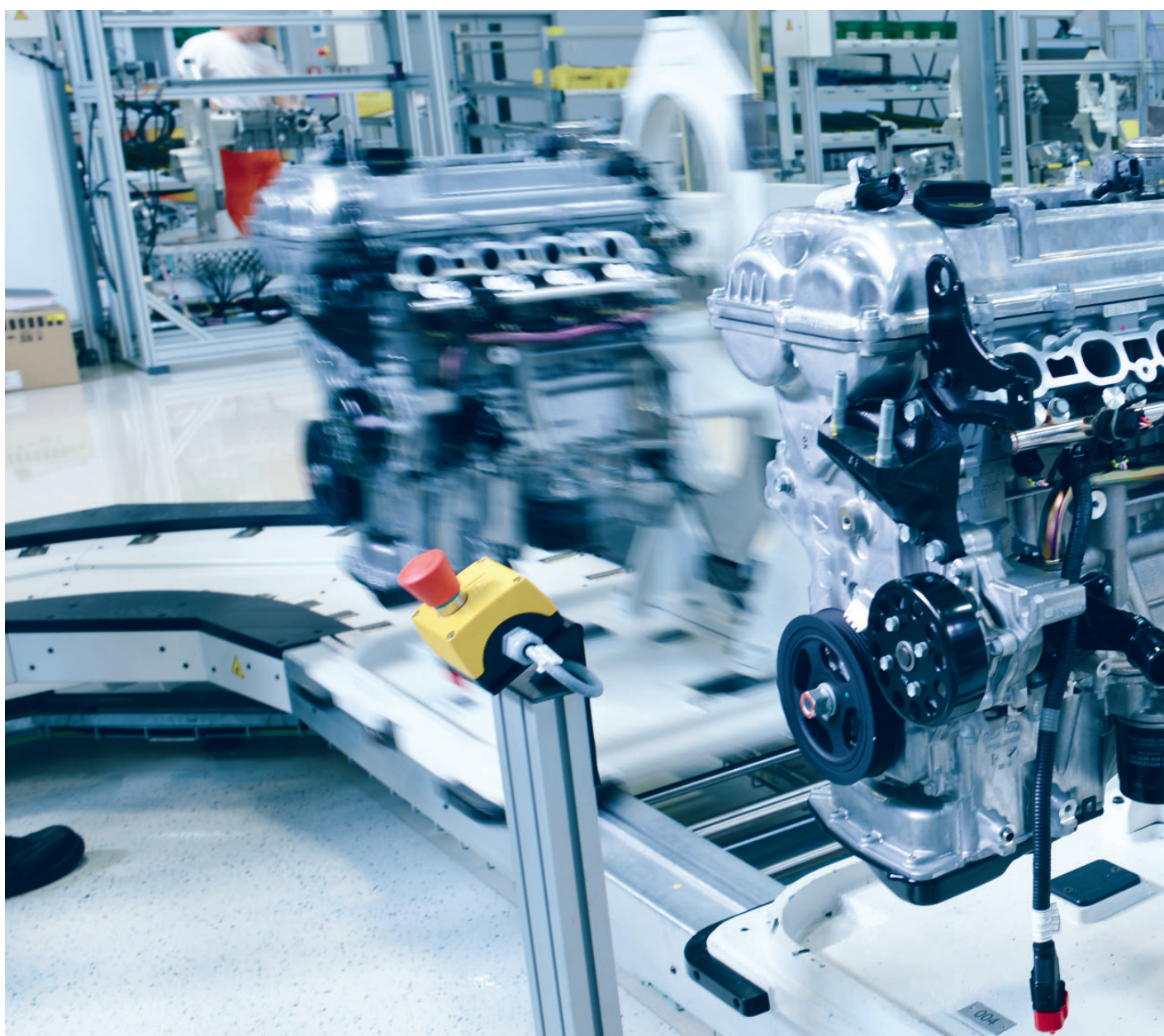
## Standards

<b>EN ISO 12100</b>	Safety of machinery - General principles for design - Risk assessment and risk reduction
<b>EN ISO 13849-1</b>	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
<b>EN ISO 13849-2</b>	Safety of machinery - Safety-related parts of control systems - Part 2: Validation
<b>EN ISO 13857</b>	Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs
<b>EN 1037</b>	Safety of machinery - Prevention of unexpected start-up
<b>EN ISO 4414</b>	Pneumatic fluid power - General rules and safety requirements for systems and their components
<b>EN 574</b>	Safety of machinery - Two-hand control devices - Functional aspects - Principles for design
<b>EN ISO 13850</b>	Safety of machinery - Emergency stop function - Principles for design
<b>ISO 1219-1</b>	Fluid power systems and components - Graphical symbols and circuit diagrams - Part 1: Graphical symbols
<b>EN ISO 13855</b>	Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body
<b>EN 60204-1</b>	Safety of machinery — Electrical equipment of machines — Part 1: General requirements

The list of standards is not intended to be exhaustive.

The machine manufacturer determines the applicable standards during the process of risk assessment for the machine.





## Safety components

<p><b>Residual pressure relief valve with direct monitoring</b></p> <ul style="list-style-type: none"> <li>- Safety valve as per 2006/42/EC</li> <li>- For max. cat. 2</li> </ul>	 <p>Item: <b>VP-X536</b></p>
<p><b>Residual pressure relief valve with direct monitoring</b></p> <ul style="list-style-type: none"> <li>- Safety valve as per 2006/42/EC</li> <li>- For max. cat. 4</li> <li>- Mountable with SMC FRL units</li> </ul>	 <p>Item: <b>VP-X538</b></p>
<p><b>Residual pressure relief valve with direct monitoring and soft start function.</b></p> <ul style="list-style-type: none"> <li>- Safety valve as per 2006/42/EC</li> <li>- For max. cat. 4</li> <li>- Mountable with SMC FRL units</li> <li>- Gradual pressure increase</li> </ul>	 <p>Item: <b>VP-X555 / VP-X585</b></p>
<p><b>Residual pressure relief valve with direct monitoring</b></p> <ul style="list-style-type: none"> <li>- Safety valve as per 2006/42/EC</li> <li>- For max. cat. 4</li> </ul>	 <p>Item: <b>VG342-X87</b></p>
<p><b>Two-hand control valve</b></p> <ul style="list-style-type: none"> <li>- Safety valve as per 2006/42/EC</li> <li>- Cat. 1 type IIIA as per EN 574</li> </ul>	 <p>Item: <b>VR51</b></p>










## Safety over fieldbus with PROFIsafe

<p><b>Safety over Fieldbus with PROFIsafe: EX245 PROFIsafe</b></p> <ul style="list-style-type: none"> <li>- Certified PROFIsafe product for use in safety applications up to PL e acc. to EN ISO 13849-1 and SIL 3 acc. to IEC 62061 / IEC 61508</li> </ul>	 <p>Item: <b>EX245-FPS#-X35</b></p>
---	--

## Recommended SMC products validated according to ISO 13849




<b>3/5 Port solenoid valve</b> SY Series	
<b>3/5 Port solenoid valve</b> SY Series	
<b>Solenoid valve</b> JSY Series	
<b>3 port 2-position directly actuated poppet valve</b> VT(0)307 Series	
<b>Pilot poppet valve</b> VP Series	
<b>Mechanical valve</b> VM100-A(-30, -32, -33) Series	
<b>Mechanical valve</b> VM200-A(-30, -32, -33) Series	
<b>Mechanical valve</b> VM1000 Series	
<b>Mechanical valve</b> VZM500(-08, -34, -36, -37) Series	
<b>Shuttle valve</b> VR12□0(F) Series	
<b>Shuttle valve</b> VR1211F Series	

# Recommended SMC products validated according to ISO 13849

<p><b>Shut off valve</b></p> <p>VHS Series</p>	
<p><b>Residual pressure release valve</b></p> <p>KE Series</p>	
<p><b>Pilot operated check valve with state detection</b></p> <p>XT34-303 Series</p>	
<p><b>Check valve with one touch fitting</b></p> <p>AKH Series</p>	
<p><b>Check valve with one touch fitting</b></p> <p>AKB Series</p>	
<p><b>Quick exhaust valve</b></p> <p>AQ Series</p>	
<p><b>Speed controller</b></p> <p>ASP Series</p>	
<p><b>Check valve</b></p> <p>XTO-2571/-1239/-1719 Series</p>	
<p><b>2 port valve</b></p> <p>VNB(20,30,40)-X700 Series</p>	



## Recommended SMC products validated according to ISO 13849

<b>Regulator</b> AR-A/-B Series	
<b>Soft start up valve</b> AV□□□□-A-X2004 Series	
<b>Precision regulator</b> IR1000-AV2000-A/3000-A Series	
<b>Vacuum regulator</b> IRV10(A)/20(A) Series	
<b>High purity chemical valve</b> LVA / LVC Series	

### Legal information

The circuit examples shown introduce sample applications for our products and assemblies, with which various pneumatic sub-systems for safety functions can be realised.

The circuits are merely examples for the listed safety functions, and do not represent a binding solution or application recommendation for a specific application. Even if a similar type of safety function is being assessed, it is not guaranteed that the existing risk can be adequately reduced by this example in a real application (see Chapter 5.5, EN ISO 12100). The machine manufacturer or control system integrator is solely responsible for testing independently each individual application, and if required, to make additions or changes to the circuits. In so doing, the machine manufacturer or control system integrator must independently examine and comply with all laws, guidelines, standards and product information pertaining to the design

and manufacture of the system and to observe them during implementation. The machine manufacturer or control system integrator bear sole responsibility for the suitability of the circuits for the installed components. SMC assumes no warranty or liability for an implemented solution designed by the machine manufacturer or control system integrator for their respective, specific application, or for the assumption of a sample circuit shown here for their specific application.

The circuits show only the pneumatic subsystem (control-component “actuator”). For the completeness of the safety functions, the machine manufacture or control system integrator must generally add additional safety-related subsystems (usually “sensor” and “logic” control components).

NOTE: The PL achieved by the sub-system is directly related to the overall MTTF and to the average number of cycles of the component. A greater number of cycles leads to a lower level of PL.

# Global engineering network

## Technical centres are located in the United States, Europe and China, as well as Japan

**Following the basic concept of developing products from the customer's standpoint, SMC dedicates a large staff to research and development.** This is undertaken to promote research on basic technology with future potential and to produce products that are adapted to the needs of the marketplace in a timely manner. To provide positive and speedy response to the problems presented by customers throughout the world, technical centres have been established in the United States, Europe and China, creating a powerful global engineering network with Japan as its nucleus. All of the technical centres share information and maintain close contact in order to quickly respond to requirements locally, and to offer the same high quality of technical service throughout the world.



### JTC (Japan Technical Center) Japan

**The Japan Technical Center oversees worldwide technical development.**

The JTC is the center of SMC research and development and produces new products for the global market based on our customers' current and future needs.





### **CTC (China Technical Center) China**

The CTC strengthens the system through product development and technical services to quickly respond to a wide range of needs and requirements in the Chinese market.



### **ETC (European Technical Centre) U.K.**

The ETC has been established to support the European subsidiaries by responding to technical questions, specifying and designing special products for customer needs, training their engineers to provide fast local product support and developing new technology products for modern factory automation.



### **UTC (US Technical Center) U.S.A.**

The UTC is enhancing engineering capabilities to quickly respond to customers' needs through product development and technical services offered in the North American market.



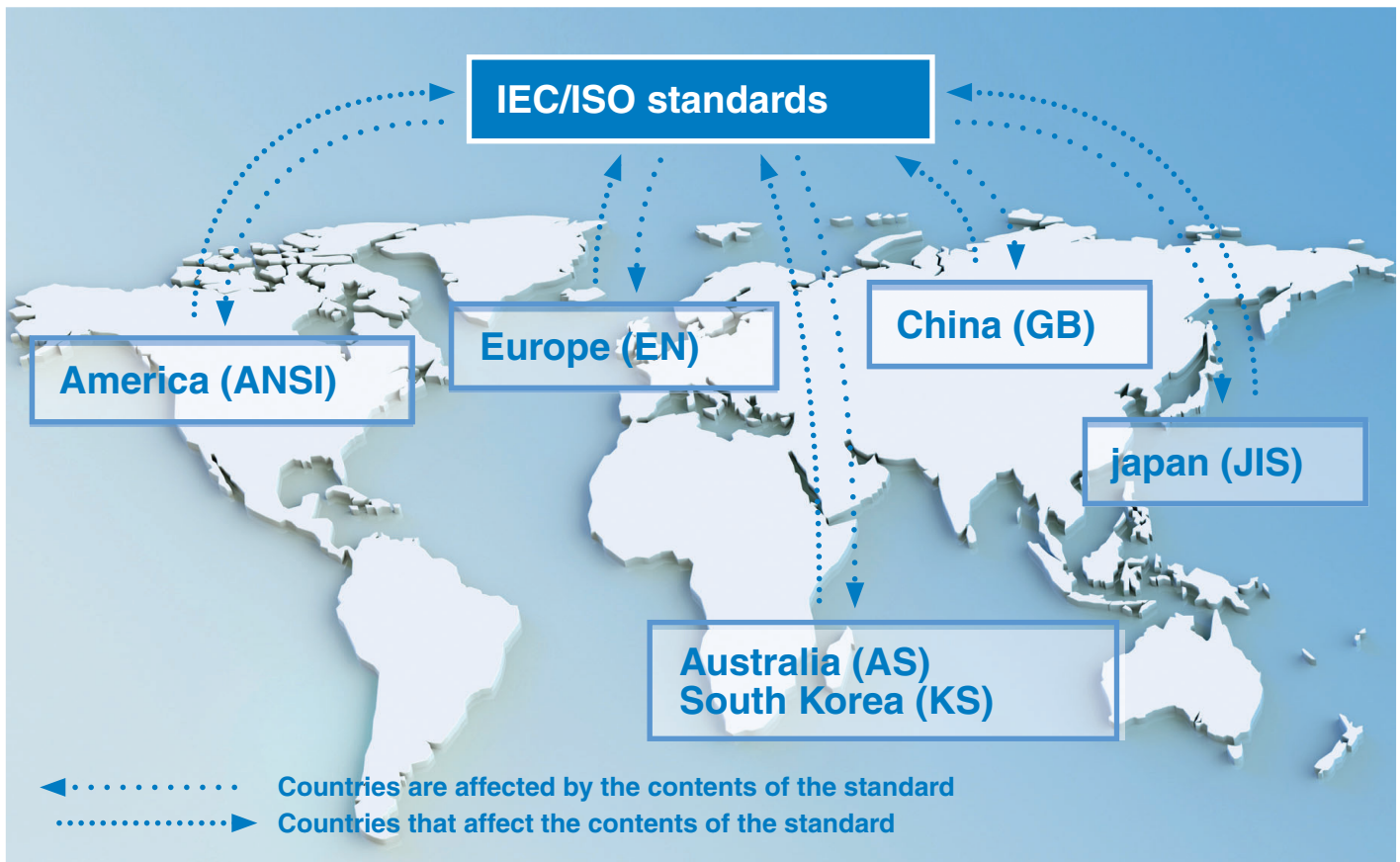
### **GTC (German Technical Center) Germany**

GTC develops products and provides technical services by quickly responding to customers' requirements with a focus on the German market.



# Safety standard ISO 13849-1

The globalization of the concept of machine safety by international standards is accelerating



## Conforming to international standards (IEC/ISO standards) is important.

Example: In Europe, the safety requirements of the Machinery Directive are mandatory and ISO 13849 can be used to ensure compliance. Equipment that does not conform to the directive cannot be distributed in the EU region. This safety concept is also being taken up globally.

## Globalization is accelerating

Member countries of the WTO/TBT agreement must confirm to international standards. The standards in each country are aligned internationally.

## Symbols and abbreviated terms

Symbol or abbreviation	Description
<b>a, b, c, d, e</b>	Denotation of performance levels
<b>B, 1, 2, 3, 4</b>	Denotation of categories
<b>B<sub>10</sub></b>	Number of cycles until 10 % of the components fail (for pneumatic and electromechanical components)
<b>B<sub>10D</sub></b>	Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components)
<b>Cat.</b>	Category
<b>CCF</b>	Common cause failure
<b>DC</b>	Diagnostic coverage
<b>DC<sub>avg</sub></b>	Average diagnostic coverage
<b>CE</b>	Conformité Européene (European Conformity)
<b>F, F1, F2</b>	Frequency and/or time of exposure to the hazard
<b>I/O</b>	Inputs/Outputs
<b>ISO</b>	International Standards Organization
<b>FMEA</b>	Failure modes and effects analysis
<b>MTTF</b>	Mean time to failure
<b>MTTF<sub>D</sub></b>	Mean time to dangerous failure
<b>n<sub>op</sub></b>	Number of annual operations
<b>P, P1, P2</b>	Possibility of avoiding the hazard
<b>PL</b>	Performance level
<b>PL<sub>r</sub></b>	Required performance level
<b>PLC</b>	Programmable logic controller
<b>S, S1, S2</b>	Severity of injury
<b>SIL</b>	Safety integrity level
<b>SRP/CS</b>	Safety-related part of a control system
<b>TE</b>	Test equipment
<b>T<sub>M</sub></b>	Mission Time
<b>T<sub>10D</sub></b>	Mean time until 10 % of the components fail dangerously





Expertise – Passion – Automation

## SMC Corporation

Akihabara UDX 15F, 4-14-1  
Sotokanda, Chiyoda-ku, Tokyo 101-0021, JAPAN  
Phone: 03-5207-8249  
Fax: 03-5298-5362

<b>Austria</b>	+43 (0)2262622800	www.smc.at	office@smc.at
<b>Belgium</b>	+32 (0)33551464	www.smc.be	info@smc.be
<b>Bulgaria</b>	+359 (0)2807670	www.smc.bg	office@smc.bg
<b>Croatia</b>	+385 (0)13707288	www.smc.hr	office@smc.hr
<b>Czech Republic</b>	+420 541424611	www.smc.cz	office@smc.cz
<b>Denmark</b>	+45 70252900	www.smc.dk.com	smc@smcdk.com
<b>Estonia</b>	+372 6510370	www.smc.pneumatics.ee	smc@smcpneumatics.ee
<b>Finland</b>	+358 207513513	www.smc.fi	smc@smc.fi
<b>France</b>	+33 (0)164761000	www.smc-france.fr	info@smc-france.fr
<b>Germany</b>	+49 (0)61034020	www.smc.de	info@smc.de
<b>Greece</b>	+30 210 2717265	www.smchellas.gr	sales@smchellas.gr
<b>Hungary</b>	+36 23513000	www.smc.hu	office@smc.hu
<b>Ireland</b>	+353 (0)14039000	www.smcautomation.ie	sales@smcautomation.ie
<b>Italy</b>	+39 03990691	www.smcitalia.it	mailbox@smcitalia.it
<b>Latvia</b>	+371 67817700	www.smc.lv	info@smc.lv

<b>Lithuania</b>	+370 5 2308118	www.smclt.lt	info@smclt.lt
<b>Netherlands</b>	+31 (0)205318888	www.smc.nl	info@smc.nl
<b>Norway</b>	+47 67129020	www.smc-norge.no	post@smc-norge.no
<b>Poland</b>	+48 222119600	www.smc.pl	office@smc.pl
<b>Portugal</b>	+351 214724500	www.smc.eu	apoiocliente@smc.smces.es
<b>Romania</b>	+40 213205111	www.smcromania.ro	smcromania@smcromania.ro
<b>Russia</b>	+7 8123036600	www.smc.eu	sales@smcru.com
<b>Slovakia</b>	+421 (0)413213212	www.smc.sk	office@smc.sk
<b>Slovenia</b>	+386 (0)73885412	www.smc.si	office@smc.si
<b>Spain</b>	+34 945184100	www.smc.eu	post@smc.smces.es
<b>Sweden</b>	+46 (0)86031200	www.smc.nu	smc@smc.nu
<b>Switzerland</b>	+41 (0)523963131	www.smc.ch	helpcenter@smc.ch
<b>Turkey</b>	+90 212 489 0 440	www.smc.pneumatik.com.tr	info@smcpneumatik.com.tr
<b>UK</b>	+44 (0)845 121 5122	www.smc.uk	sales@smc.uk