Safety in focus

Machinery Directive and ISO 13849 in practice
On the safe side with SMC

We think in optimal systems.

Safety creates trust. As a powerful and reliable partner in matters of automation technology, we have made it our task to accompany you competently and reliably during your system's entire life cycle – and to also ask, answer, and professionally resolve all queries relevant to safety in the process.

From the individually constructed machine to highly complex systems, we don’t just satisfy all demands for flexibility and productivity, but also trouble-free user and operating safety.

In order to guarantee this in your company too, we offer innovative and customized safety solutions and CE-conformant safety components. Achieving the highest possible risk minimization and protecting the people on the machines are the main focuses here.

Because the success of the whole lies in the details, we also rely on personal commitment in safety engineering. Talk with our certified safety experts about your queries and wishes concerning the safety of your system.

Please see our website: www.smc.at/safety
What may we do for you?

To first-class, state-of-the-art safety with the professionals from SMC.

To detect potential risks, to think preventively and act with foresight is the foundation of every CE-conformant system. Standards-compliant and effective system safety is one of our specialties as the world’s leading automation expert.

With interdisciplinary expertise, we guide you through the risk assessment, with questions about relevant directives and standards, as well as with all analyzes and measures for the applicable safety regulations. Based on this data, we support you during the definition of the safety chain and its implementation according to ISO 13849. We provide all of the necessary parameters for the success of this process and offer professional support during calculation of the standardized safety function.

The technical implementation – from the drafting of the schematics to the complete installation-capable, CE-conformant solution – is in the best hands with us. We likewise support you during testing and analysis of your safety system according to ISO 13849-2. Moreover we train your employees in order to anchor safety-related expertise in your company.

Important information can be found on following pages:

- Your guidelines for safety engineering  ➤ page 08
- Safety engineering FAQ  ➤ page 20
- Practical examples  ➤ page 29

Optimal safety creates confidence. SMC offers consulting and realization concerning safety matters.

“Optimal safety creates confidence. SMC offers consulting and realization concerning safety matters.”
From defining the safety chain to technical implementation and training – SMC is your reliable partner with safety-related expertise.


Your guidelines for safety engineering.

The professional marketing of machinery and safety-related applications in the European economic area assumes knowledge of sound legal principles and already begins with the design and construction of your system. Trust in our expertise and our knowledge about the requirements of the Machinery Directive for successful CE certification.

In addition to hazard analysis and risk assessment, we also stay fully focused on the conceptual design of safety control systems. ISO 13849 concerns itself with safety-related parts and their design guidelines for control systems. It often makes for lack of clarity with terms such as Performance Level, B10d, or degree of diagnostic coverage.

The overview below is intended to establish the connection between the central considerations and requirements for market introduction with regard to the Machinery Directive and ISO 13849. It also points out where and how SMC can thereby support you.

Together with your company’s technicians, we answer the essential safety questions and find solutions with substance.
We know the way to optimal safety. Accompany us.

1. DIRECTIVES AND STANDARDS RESEARCH
2. DEFINITION OF THE SAFETY CHAIN
3. SAFETY-RELEVANT INDICATORS
4. TECHNICAL IMPLEMENTATION
5. VALIDATION
6. TRAINING COURSES

Your key questions:

- Which potential hazards can occur in my machine and how can I assess them?
- Is a safety function involved? Does a failure of this function lead to the endangerment of persons?
- Do my protective devices depend on a control system?
- Should SMC provide an installation-ready solution (e.g. in the form of a control cabinet)?

Your key questions:

- What Performance Level emerges from my risk assessment?
- Do constructive measures suffice to minimize the hazard?
- Which safety functions are appropriate for the respective hazard situation?
- Which components belong to the safety function?
- Which options do I have to achieve the required Performance Level?

- How often can the safety function expect to be actuated?
- Does the safety chain’s service life correspond with that required by the standard?
- To what extent must I be able to detect a safety function’s failure?

- How do I design a standardized circuit?
- Must a circuit be evaluated by external assessors?
- What do I need for complete CE-conformant documentation?
- In which form must the documentation exist?
- How long must the documentation be available?

- Was the required Performance Level actually achieved?
- Have I worked according to the latest state of technology?
- Were all safety principles properly implemented?
- Have I analyzed all of the misuses that could be expected?
- Which errors can I preclude?
- Does my quality assurance satisfy the requirements of the standard?

SMC offers solutions:

- We support you during the risk assessment as well as with questions about various directives and about Performance Level.
- We help you to find the appropriate safety functions corresponding to the hazard and to implement them under ISO 13849 and the current safety regulations.
- We gladly provide all of the necessary parameters for SMC components. Furthermore, SMC offers expert support when calculating the safety function pursuant to ISO 13849-1.
- We support you comprehensively in the drafting of circuit schematics and concepts – from the simple circuit to complete, installation-ready CE-conformant solutions.
- We support you during the testing and analysis of your safety system according to ISO 13849-2.
- SMC offers targeted, customized training courses and advanced education on the subject of safe control with emphasis on pneumatics and electrical equipment.

- What duty of information do I have towards the machine’s user?
- Does a need exist in my team for further education and training in the area of machine safety and pneumatics?
5 steps for safety

Without worries from the risk assessment to the optimal safety function from SMC.

Understanding processes and their dynamics, knowing all of a system’s features and properties, and guaranteeing optimal performance make our technicians your safety experts. We accompany you from construction design to initial start-up and create a basis for legal security with safety inspections.

We guide you through the entire process from risk assessment to safety function with the five steps below.

1. Risk assessment
2. Risk reduction
3. The control system as a contribution to risk reduction
4. Determination of the achieved Performance Level
5. Determining the machine’s safety functions
For us holistic safety engineering begins as early as the design and construction of the system. Possible risks and failure scenarios are analyzed and assessed according to ISO 12100 and eliminated based on the results. The need for risk reduction is derived if elimination is not possible. Thereby all of the system’s operating states are to be assessed: automatic mode, maintenance mode, cleaning, and so forth.

Risk assessment

**Step 1**

**Risk reduction**

Federal law provides for three further risk-reduction measures if completely eliminating all potential risks is not possible in step 1. The order is to be strictly observed here.

We support you competently in all three areas, delivering individual solutions from individual safety applications to complete installation-ready solutions.
ISO 12100 requires for the design of protective devices if constructive solutions do not suffice to adequately reduce the risk. The configuration of control system’s safety-related parts for such protective devices is dealt with in the ISO 13849 standard, which is usable both for pneumatic and hydraulic, mechanical, and electrical safety functions.

Here the task of the required Performance Levels is a qualitative consideration of the safety function, which is determined by a risk assessment within ISO 13849 (see graph on next page).

According to ISO 13849, every irreversible injury (this also includes scars) is a serious one in the sense of the standard. In a remark, the standard gives the non-normative instruction that F2 should be selected when interventions occur more frequently than once per hour, otherwise F1 (please see graph on the next page).

Hazards such as actuators, pinch points, and so forth are always evaluated during formulation of the risk graphs without safety systems such as protective fence, light grid, or the like, because the safety systems are initially derived from the Performance Level. All of the machine’s operating states are to be assessed for this: automatic mode, maintenance mode, set-up mode, cleaning, and much more. Special attention should be paid to maintenance mode, because in this case people are working directly in the machine’s danger area.

### 5 steps for safety

**Step 3**

**The control system as a contribution to risk reduction**

ISO 13849-1

<table>
<thead>
<tr>
<th>S: SEVERITY OF INJURY</th>
<th>P: FREQUENCY AND/OR EXPOSURE TO HAZARD</th>
<th>P: POSSIBILITY OF AVOIDING HAZARD OR LIMITING HARM</th>
<th>SIZE OF RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1: Slight injury</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2: Serious injury</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P1: Possible under specific conditions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P2: Impossible</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Remark**

According to ISO 13849, every irreversible injury (this also includes scars) is a serious one in the sense of the standard. In a remark, the standard gives the non-normative instruction that F2 should be selected when interventions occur more frequently than once per hour, otherwise F1 (please see graph on the next page). Hazards such as actuators, pinch points, and so forth are always evaluated during formulation of the risk graphs without safety systems such as protective fence, light grid, or the like, because the safety systems are initially derived from the Performance Level. All of the machine’s operating states are to be assessed for this: automatic mode, maintenance mode, set-up mode, cleaning, and much more. Special attention should be paid to maintenance mode, because in this case people are working directly in the machine’s danger area.
### Determining the machine’s safety functions

The details of the safety function are now elaborated. This ranges from the definition of the actual safety function – such as safe stop, safe venting, protection against unexpected start-up, or the like – through the creation of block diagrams of safety-related parts, to the definition of necessary responses in case of fault.

### Determination of the achieved Performance Level, PL

To evaluate the selected safety chain, the Performance Level is determined with the help of the following values:

- **Structure (category)**
- **MTTFd (Mean Time to Failure dangerous):** mean time to dangerous failure
- **DC (Diagnostic Coverage):** degree of diagnostic coverage
- **CCF (Common Cause Failure):** faults with a common cause
- **Safety function behavior under fault conditions**
- **Safety-related software**
- **Systematic failures**
- **Ability to execute the safety function under foreseeable environmental conditions**

#### Please note

The subsequent documentation associated with the applicable directives plays a supporting role in meeting the burden of proof in all five steps and must be available in an arbitrary form for ten years.

The sequence marked with blue arrows on the subsequent double page gives advice in identifying the Performance Level. Based on the four main values (category, MTTFd, DC, and CCF) it shall be ensured that the actual Performance Level at least matches with the required Performance Level of the risk graph (see page 15).
**5 steps for safety**

### 1. Structure of hardware

#### Category

- Category **B**
- **Category 2**
- **Category 3 and Category 4**

#### Outline of requirements

- **B**
  - Safety-related parts of control systems should achieve their functions, and should withstand expected stress.
- **Category B**
  - Use of well tried safety components.
- **Category B**
  - Safety function(s) shall be checked at appropriate intervals.
- **Category B**
  - A single fault does not lead to the loss of safety function.
- **Category B**
  - A single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to the loss of safety function.

### 2. Life of components

- **MTTFd**
- **MTTFd** of each channel
- **DCavg**
- **CCF**

#### Configuration applicable to Category B and Category 1

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>L</td>
</tr>
</tbody>
</table>

#### Configuration applicable to Category 2

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>L</td>
</tr>
</tbody>
</table>

#### Configuration applicable to Category 3 and Category 4

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>L1</td>
</tr>
</tbody>
</table>

### 3. Reliability of system

- **MTTFd**
- **DCavg**
- **CCF**

#### Configuration applicable to Category B

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>L</td>
</tr>
</tbody>
</table>

### 4. Certainty of design

- **CCF**

#### Configuration applicable to Category 2

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>L</td>
</tr>
</tbody>
</table>

### 5. Configuration applicable to Category 3 and Category 4

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>L1</td>
</tr>
</tbody>
</table>

### Safety in focus

**Category B**

- Use of well tried safety components.

**Category 2**

- Safety function(s) shall be checked at appropriate intervals.

**Category 3 and Category 4**

- A single fault does not lead to the loss of safety function.

**Category B**

- A single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to the loss of safety function.

### Architecture or safety control system (configuration of L, O). The category is composed of I (input equipment), L (logical operation equipment) and O (output equipment).

### Levels

- **High**
  - MTTFd: 30 years or more, less than 100 years
- **Medium**
  - MTTFd: 10 years or more, less than 30 years
- **Low**
  - MTTFd: 3 years or more, less than 10 years

### MTTFd of each channel

- **Low**
  - a - a b b c -
- **Medium**
  - b - b c c d -
- **High**
  - - c c d d d e

### DCavg

- **None**
- **Low**
- **Medium**
- **High**

### CCF

- **None**
- **Low**
- **Medium**
- **High**

### The designer of the machine needs to ascertain Nop (how many times that part operates in one year).
3. What is implied by ‘Protection against unexpected start-up’? Must I deal with this?

In principle, protection against restart is to be considered with every safety function. This is regarded as one of the basic safety principles of ISO 13849-2. In pneumatics protection against restart means the following: after an energy failure (compressed air supply, compressor breaks down, or hose rupture) and subsequent recovery, the machine must not start up automatically without a separate start command. The detection of a primary-side pressure drop, which must lead to a system interlock, is often sufficient. (In this regard note the example on page 42.)

4. May bistable valves be installed in safety functions?

In the ‘ISO 13849-2’ list of proven safety principles, there is the point ‘secured position’, which safety-oriented products and systems must fulfill. This term means, that the moving element of a component (the spool valve) is held mechanically in one of the possible positions. Friction alone is not sufficient. However a bistable valve is only held in one position by friction and therefore does not fulfill this proven principle.

According to a statement from the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), bistable valves are permitted if they feature a detent (mechanical lock) at the end positions. Steel-slider valves from SMC have such a lock and therefore can be used in safety-related control systems.

These principles are to be fulfilled from Performance Level ‘b’ upward.

According to a statement from the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), bistable valves are permitted if they feature a detent (mechanical lock) at the end positions. Steel-slider valves from SMC have such a lock and therefore can be used in safety-related control systems. For this the ISO 13849-2’s fundamental, proven safety principles must be observed, in particular the following: application of the principle of energy separation (closed-circuit principle).

The safe state is achieved by releasing energy. This means that the most recent switching position before the release must be the safe state. Moreover it must be checked in the specific case of application, whether energy failure and recovery can lead to unexpected and/or additional hazardous movements.
5. Does a valve in which both the supply voltage and the pilot air can be interrupted separately represent a two-channel solution?

A two-channel solution must be at least ‘one fault safe’, meaning that one single fault in the safety chain (e.g. a valve not switching) must not lead to the loss of the safety function. That is not the case with the pilot-controlled valve because a fault in the main valve’s spool (e.g., a chip that blocks the spool valve) leads to the failure of the entire system. Only a fault exclusion according to ISO 13849-2 for failures on the main valve can confirm this system as suitable. However fault exclusions should be used with caution.

6. Is there a correlation between SIL (Safety Integrity Level) and PL (Performance Level)?

Yes. Both systems are linked by the probability of failure and can be converted accordingly. SIL can generally only be calculated for complete systems. An individual product cannot have a SIL.

7. Which principles are to be observed when designing (pneumatically driven) isolating guards?

EN 953 for isolating guards is to be fulfilled. Quote from standard 953:2009, point 5.2.5.2: ‘Force-actuated moveable guards must not cause any injuries (e.g. due to closing pressure, force, speed, sharp edges). If an isolating guard is fitted with a non-isolating protective device which automatically causes the isolating guard to re-open as soon as a person or object comes into contact with the isolating guard, the force for preventing closure of the isolating guard must not be more than 150 N. The kinetic energy of the isolating guard must not be more than 10 J. If no such protective device is attached, these values must be reduced to 75 N and 4 J respectively.’

8. Can I implement my safety function using serial transmission?

If you do not install a secure bus device (master, valve cluster, etc.), a maximum Performance Level, PL, of ‘b’ is achievable. If a higher PL is required, it is possible to use a standard bus protocol (Profibus, CAN, EtherCAT, and many others) as long as the safety function is excluded from it.

The voltage supply module EX9-PE1-X15 provides a fault exclusion for electrical cross-circuit to enable a 2-channel electrical switch-off of the valve sections.

9. A safety PLC is very expensive. Can I also design my safety function purely pneumatically?

In principle it is possible to say that safety functions that can be implemented electro-pneumatically can also be designed purely pneumatically. In this case the cost-effectiveness of purchasing one’s own safety PLC depends on the complexity of the desired safety functions and the operating functions required for this. Special attention is on the sensors required by ISO 13849 to fulfill the degree of diagnostic coverage from category 2 upward. Realizing this purely pneumatically represents considerable extra expense in the conceptual design of the circuit, component quantity, and the costs resulting from that. The acquisition of a safety PLC compared with a purely pneumatic version of the safety function therefore often represents the more cost-effective solution.

10. Where can I get the necessary safety-relevant key figures of the SMC components?

SMC will gladly provide you via email with all of the safety-relevant key figures, such as B10 and MTTF. Furthermore SMC offers a Sistema library available online at www.smc.at/safety.

Sistema is a program for calculating your safety functions. It is provided free of charge by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA).

11. What does a pneumatic maintenance backup (lockout/tag out) look like?

Maintenance safeguards (lockout/tag out, LOTO) are technical facilities that lock control elements of a technical system, in other words switches, shut-off or ball valve, and so forth, in a particular position. They are used to protect against unauthorized access or unintentional activation, for instance during a maintenance procedure.

It is possible to lock the pressure relief 3-port valve from SMC (VHS series) if setting or maintenance operation can occur in the depressurized state.

5 safety rules:
The general safety rules are defined in the ‘Regulation on the protection of workers against hazards arising from electrical current’ (e.g. Electrical Protection Regulation 2012 – ESV 2012 in Austria) defined in § 12 as follows:
1. Unlocking
2. Safeguarding against reactivation
3. Confirming absence of voltage on all poles
4. Earthing and shorting
5. Covering or closing off adjacent live parts

These rules should be applied analogously to the pneumatics to the extent possible.
Expectations in pneumatics

Pneumatic systems and electrical sensors.

In the optimal interplay of pneumatic components and electronic sensors, we guarantee the safety of complete control systems. The sensors are essential for the degree of diagnostic coverage from category 2 upward.

Based on the plausibility check it is evaluated, whether a digital or analogue signal from a sensor changes as expected within a time period.

Consequently, for example, the limit switch of the associated cylinder must output a signal change within a predefined time window after a valve is switched.
Safety components acc. machinery directive

Definitions and characteristics.

According to the Machinery Directive, a safety component is a component
› that serves to guarantee a safety function,
› that is brought into circulation separately,
› the failure or malfunction of which endangers
  the safety of persons, and
› that is not required for the machine to function
  or be replaced by the usual components for the
  machine’s function.

Please note
The manufacturer of the component
conducts a safety-related evaluation of
the safety component. Revalidation by the
machine manufacturer according to
ISO 13849-2 is thus no longer required.

In a safety-oriented control system, besides in-
stallation-ready safety components, standard
components can also be installed. However
these must be assessed in the framework of
the system analysis.

Symbols

Safety functions and emergency stop.

Pneumatic safety functions

Safe Stop
Reducing Pressure
Safe Venting
Two-Hand Control
Safe Running-in
Protection against Unexpected Start-up
Safe Moving-out
Emergency Stop (extended safety function)

Remark concerning emergency stop:
Every machine must have its own emergency stop safety function. However this cannot replace any
primary safety function that works automatically. It merely offers the possibility to bring the machine
to a safe position in a hazardous situation.
Example 1
Safe venting (PL c, cat. 4) and protection against unexpected start-up (PL c, cat. 4)

Example 2
Safe stop (PL d, cat. 3) and protection against unexpected start-up (PL d, cat. 3)

Example 3
Two-hand control (PL c, cat. 1) and protection against unexpected start-up (PL c, cat. 1)

Example 4
Reducing pressure (PL c, cat. 1) and protection against unexpected start-up (PL c, cat. 1)

Example 5
Safe venting (PL c, cat. 1) and protection against unexpected start-up (PL c, cat. 1)

Example 6
Safe venting (PL c, cat. 1) and protection against unexpected start-up (PL c, cat. 1)

Example 7
Reducing pressure (PL d, cat. 3) and protection against unexpected start-up (PL d, cat. 3)
Initial situation
Opening the protective screen door should vent the pneumatic system. Thereby no unexpected start-up of the machine may occur during maintenance work in the danger area.

Instructions for implementation
- The valve’s safe deaeration capacity must be designed so that no further hazardous movements can occur in the danger area at the time of entry.
- After the safe deaeration valve, no assembly may endanger or delay safe venting (e.g. due to defective downstream components).
- Regular inspection of the silencer guarantees timely safe deaeration. The safety component does not need to be validated according to ISO 13849-2, because this has already been carried out by the component manufacturer in the framework of CE conformity.

Circuit description
In this example the required safety function ‘safe deaeration’ as well as the protection against unexpected start-up are realized by the safety component. The required degree of coverage is also fulfilled as a result (via 1S1.1 and 1S1.2). Thereby it must be ensured, that valves installed on the secondary side (2V1 and 3V1) also permit safe deaeration during a power failure or malfunction. Therefore, for example, no 5/3-way valve with blocked middle position may be used.
**Initial situation**

When bad parts are removed from the conveyor belt, interruption of the light curtain should safely stop the drives situated behind it. The machine must not start up unexpectedly during work in the danger area within the light curtain. The pneumatic valves as well as the diagnostics by means of pressure switch should be installed on a valve cluster.

**Instructions for implementation**

- The sensors are to be installed tamper-proof so that adjustment can only be accomplished with a special tool. The distance of the light grid from the place of danger should be selected large enough that the safety chain can stop the hazardous actuator in time, before operating personnel enter the danger zone.

- Shutdown of the safety-relevant valves does not take place over the standard serial transmission. That would be too unsafe. Instead it is carried out via an independently controlled module within the valve cluster (for details see ‘Frequently asked questions’ on page 22).

- Especially when installing actuators in a vertical position with high loads, the pilot-controlled throttle check valves are to be screwed directly into the cylinder.

- Since the unlockable throttle check valves currently feature no position monitoring, regular inspection of their function must be conducted.

- For the pneumatic safety function ‘safe stop’, the overtravel of the cylinder due to the compression of compressed air must be observed at all times.

**Circuit description**

The first channel of the safety function consists of the 5/3-way valve (2V1). As can be seen in the block diagram, the 5/3-way valve 2V1 requires the sensors 2S1 and 2S2 to achieve the required degree of diagnostic coverage. The second channel consists of the 5/2-way valve (2V2) and the pilot-controlled throttle check valves (2V3 and 2V4). In this example the installed pressure sensor (2S3) monitors the functions of the second circuit with the components (2V2, 2V3, and 2V4). The protection against unexpected start-up cat. 3 is realized by the 5/3-way valve with blocked middle position and the pilot-controlled throttle check valves.

**SMC products** (see page 46)

- **Solenoid valve**
  - article: SY

- **Pilot check valve**
  - article: ASP

- **Pressure switch**
  - article: ISE30A
Initial situation

The crimping between the cylinder piston and piston rod is realized by means of a purely pneumatic press with two-hand tripping. Thereby the press cylinder should travel back to the upper end position when the button is released.

Instructions for implementation

- The danger of crushing is to be evaluated when the press tool is reversed. Executing a safety function must not generate any new hazard point. The appropriate behavior in the event of a fault should emerge from the risk analysis.
- EN 574 is to be observed with regard to the distances of the two release buttons and their execution.
- The safety component (1Z1) need not be validated according to ISO 13849-2, because this has already been carried out by the component manufacturer in the framework of CE conformity.

Circuit description

Timely pressing of both buttons generates a pneumatic output signal of the two-hand safety valve (1Z1). Automatic reversing is realized via the pneumatically activated 5/2-way valve (1V3), which returns to the home position after the signal drop.

SMC products (see page 46)

- two-hand control valve article: VR51
- pilot operated spool valve article: VSA7-6
- optical indicator article: VR31
Safety in focus

Initial situation

All of the pneumatic drives should be safely brought to a standstill by opening the packaging machine’s protective enclosure. The protective enclosure is thereby monitored using a two-channel reed switch.

Instructions for implementation

- The distance of the safety door from the hazard point should be selected large enough, so that the safety chain can stop the hazardous actuator in time before operating personnel enter the danger zone.
- Especially when installing actuators in a vertical position with high loads, the pilot-controlled throttle check valves are to be screwed directly into the cylinder.
- For the pneumatic safety function ‘safe stop’, the overtravel of the cylinder due to the compression of compressed air must be observed at all times.
- The safety components (2V2 and 2V3) do not need to be validated according to ISO 13849-2, because this has already been carried out by the component manufacturer in the framework of CE conformity.

Circuit description

As can be seen in the block diagram, the first channel, which is realized with the 5/3-way valve (2V1), requires the respective sensors (2S1 and 2S2) in order to achieve the required degree of diagnostic coverage.

The second channel consists of two safety components (2V2 and 2V3), which are connected directly to the cylinder. In contrast to example 2, regular functional testing of the unlockable throttle check valves is dispensed with by using the queryable safety valves. The slider query (2S3 and 2S4) integrated in the safety components monitors the function of the second circuit in this example. The protection against unexpected start-up in category 3 is realized by the 5/3-way valve with blocked middle position and the two safety components.

SMC products (see page 46)

- safety component acc. to ISO 13849-1
  article: VP42-X036
- solenoid valve
  article: SY
- residual pressure release valve
  article: KE

SMC products (see page 46)
Initial situation

The robot should stop safely and the pneumatic system should deaerate safely when the operator steps on the danger area marked red. A laser scanner monitors the danger area. In this example the robot is not part of the safety-related consideration.

Instructions for implementation

- The valve’s venting capacity must be designed so that no further hazardous movements occur in the danger area at the time of entry.
- After the venting valve, no assembly may endanger or delay safe venting (e.g. due to defective downstream components).
- Regular inspection of the silencer guarantees timely venting.
- The safety component does not need to be validated according to ISO 13849-2, because this has already been carried out by the component manufacturer in the framework of CE conformity.

Circuit description

The safety component, valve (1V1), vents the system through one channel. A degree of diagnostic coverage is not required for category 1.

Safety functions in practice - Example 5

Initial situation

The robot should stop safely and the pneumatic system should deaerate safely when the operator steps on the danger area marked red. A laser scanner monitors the danger area. In this example the robot is not part of the safety-related consideration.

Instructions for implementation

- The valve’s venting capacity must be designed so that no further hazardous movements occur in the danger area at the time of entry.
- After the venting valve, no assembly may endanger or delay safe venting (e.g. due to defective downstream components).
- Regular inspection of the silencer guarantees timely venting.
- The safety component does not need to be validated according to ISO 13849-2, because this has already been carried out by the component manufacturer in the framework of CE conformity.

Circuit description

The safety component, valve (1V1), vents the system through one channel. A degree of diagnostic coverage is not required for category 1.

SMC products (see page 46)

- safety component acc. to ISO 13849-1
  - article: VP 42-X036
- soft start-up valve
  - article: AV (A)
- solenoid valve
  - article: VT
Reducing pressure (PL c, cat. 1) and protection against unexpected start-up (PL c, cat. 1)

Initial situation

The robot should reduce the speed, and the pneumatic system should reduce the pressure, when the operator steps on the danger area marked yellow. A laser scanner monitors the danger area. In this example the robot is not part of the safety-related consideration.

Instructions for implementation

- Pressure in the maintenance unit should be reduced to a safe level as long as the application permits, so that no further risk of crushing emanates from the actuator.

- Applications, where lateral forces occur, very often focus on a cylinder’s guiding properties and lead to over-dimensioning of the cylinder. The consequence is an increased safety risk due to greater thrust.

Circuit description

The installed filter regulator (1Z1) reduces the pressure. The pressure relief valve vents critical system overpressure in the event of a fault. The pressure switch is optional, because it is not absolutely necessary for category 1.

SMC products (see page 46)

- Pressure switch article: IS10
- Pressure relief 3-port valve article: VHS
- Soft start-up valve article: AV(A)
Initial situation

Besides automatic mode, the maintenance mode can also be selected with the mode selector switch. In the handling stations’ maintenance mode, the actuators must be movable under pressure.

Pressure in the maintenance unit should be reduced to a safe level, so that no further risk of crushing emanates from the actuators, however setting and adjustment work can still be carried out. The system should vent if pressure reaches a critical level.

Instructions for implementation

- It must only be possible to select maintenance mode on the mode selector switch using a suitable key.
- Trained personnel must be familiarized with the residual risks existing in maintenance mode.

Circuit description

Although this circuit is designed according to category 3, safe pressure reduction is carried out over only one electro-pneumatic pressure regulator.

When the pressure in one of the two pressure switches exceeds the defined threshold value, the entire system vents via the safety valve (1V1).

The diagnostic is realized via the plunger inquiry integrated in the safety component.

Protection against unexpected start-up is fulfilled using the pressure switches (1S3 and 1S4), which are monitored by means of cross comparisons.
## Standard references

### Safety functions in practice

<table>
<thead>
<tr>
<th>STANDARDS</th>
<th>EXAMPLE 1</th>
<th>EXAMPLE 2</th>
<th>EXAMPLE 3</th>
<th>EXAMPLE 4</th>
<th>EXAMPLE 5</th>
<th>EXAMPLE 6</th>
<th>EXAMPLE 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 12100 General design principles for risk assessment and risk reduction</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 13849-1 Safety of machinery – Safety-related parts of control systems – Part 1: General design principles</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 13849-2 Safety of machinery – Safety-related parts of control systems – Part 2: Validation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 13857 Safety of machinery – Safety distances to prevent hazard zones from being reached by the upper and lower limbs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EN 1037 Safety of machinery – Prevention of unexpected start-up</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 4414 Pneumatic fluid power – General rules and safety requirements for systems and their components</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>EN 574 Safety of machinery – Two-hand control devices – Functional aspects – Principles for design</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 13850 Safety of machinery – Emergency stop – Principles for design</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 1219-1 Fluid power systems and components. Graphical symbols and control diagrams. Graphical symbols for conventional use and data-processing applications</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
SMC products

SAFETY COMPONENTS

Safety component according to ISO 13849-1
- Safety component
- Cat. 1
- Deaeration capacity up to 3700 NL/min

Safety component according to ISO 13849-1
- Safety component
- Cat. 4
- Deaeration capacity up to 2180 NL/min

Safety component according to ISO 13849-1
- Safety component
- Cat. 4
- Deaeration capacity up to 13000 NL/min

Two-hand control valve
- Safety component
- Cat. 1, Typ. 8A according to EN 574

DIRECTIONAL CONTROL VALVE

Solenoid valve
- Multiple valve options with residual pressure release
- Metal seal for 2-position double
- Also available as a single valve

Solenoid valve
- Multiple valve options
- Rubber seal

Solenoid valve
- 3-port valve, directly actuated

Soft start-up valve
- With manual override and adjustable venting-speed valve
- Also available: solely pneumatic

Pilot operated spool valve
- 5-port valve, pilot operated; size ISO 1 and ISO 2

Pilot operated spool valve
- 3-port valve, pilot operated
**Pressure Relief 3-Port Valve**
- Connectable to modular FRL units
- For lockout/tag out systems

**Pilot Check Valve**
- Thread: 1/8” bis 1/2”
- Direct mounting on the cylinder

**Pilot Check Valve with Residual Pressure Release**
- Thread: 1/8” bis 1/2”
- Direct mounting on the cylinder

**Residual Pressure Release Valve**
- Push-in dia 6-12mm or thread Rc 1/4” to Rc 3/8”

**Shuttle Valve**
- Logic valve AND / OR function

**Optical Indicator**
- Air operated; for pressure detection
- Thread: Rc 1/8”

**Sensors**

**Pressure Switch**
- Pressure and vacuum sensor
- Adjustable with digital display

**Pressure Switch**
- Adjustable, normally open reed contact
- Connectable to modular FRL units

**Autoswitch**
- Electronic
- For round groove

**Autoswitch**
- Mechanically (reed)
- For round groove
Safety in focus

CE-conformant with certainty

Complete solutions from SMC.

SMC stands for top performance, forward-looking pioneering spirit and global market leadership. In matters of safety, beyond pure automation technology we rely on personal commitment and individual solutions that cover all legal, commercial, and operational aspects.

At our headquarters in Korneuburg (Austria) and with our network of experts, we offer:

- flexible, customer-oriented production;
- comprehensive storage for best product availability partially within 24 hours;
- a highly modern technology center in Austria with engineering, prototype construction, test laboratories, endurance test facilities, and training center; and
- quality assurance with ‘ISO 9001’ certification.

These first-class prerequisites make SMC a strong partner, that can develop and realize the safety components that you request according to the specifications of the Machinery Directive. The installation ready safety solutions that we provide are CE certified directly at the SMC site in Korneuburg. Upon delivery you receive a standardized operation manual and CE declaration.

Our services involving control cabinets liable to CE compliance range from comprehensive analysis through conceptual design, design and production, to documentation, validation and instruction directly on your premises. We thereby guarantee CE-conformity and first-class quality of all components and modules.

We have prepared a simple online form for you under www.smc.at/safety in order to evaluate whether your application involves a safety component liable to CE compliance.
SMC. Without doubt in the best hands.

Trust the global market leader.

A great vision demands perfection in detail, innovation demands creative passion, and quality demands genuine conviction. As global market leader in industrial automation with pneumatic and electrical systems, we are able to count numerous top international producers among our customers. As your reliable partner, we are also happy to make tomorrow’s technologies your mission-critical edge of today.

Rewarded innovative strength.

› In 2013, the renowned business magazine ‘Forbes’ distinguished SMC for the third time in a row by listing it among the ‘Top 100 of the world’s most innovative companies’. The ranking is based on commitment to research and development, rate of reinvestment, and the Group’s financial performance. This recognition is unique in the entire branch.

The highest quality is our motto.

› Where highest quality is involved, we make no compromises. Our quality standard doesn’t just apply to our products and services; it covers all areas of our company. Thanks to a perfectly coordinated infrastructure, the SMC service is efficient, comprehensive and 100% customer-oriented.

We open up new horizons.

› Some 2000 technicians and engineers work in the most modern research and development centers in Japan, China, the USA, and Europe, setting trends for the entire automation industry. The result is a comprehensive product portfolio characterized by diversity and the highest quality. SMC’s standard product range includes more than 11,000 product groups and offers a variety of variants numbering millions in the fields of air conditioning, valve technology, actuators, vacuum technology, and sensors as well as electrical control and drive technology. On average, we introduce 40 new products per year to the European market.

Moreover, the development of customized high-tech solutions (SMC Customized Solutions) as well as services and professional consulting to increase productivity (SMC Customized Services) are important elements of the range of competence.

Your personal experts. Always on site for you.

› With branches in 54 countries worldwide, 50 production sites, and more than 16,000 employees, we offer a comprehensive network and optimal solutions by the shortest route.

The Austrian headquarters in Korneuburg is also the headquarters for 14 Central and Eastern European countries at the same time. With a dense network of sales organizations and distribution offices, SMC is comprehensively present in the entire CEE. Customers are supported personally on site and benefit from an internationally consistent high standard of quality. Continuous process improvements, latest production technologies and local warehouses in those countries guarantee systems and products of the highest quality as well as short delivery times.

In SMC local productions, individual components, applications, and system solutions are produced. Our highly modern technology center with engineering, prototype construction, test laboratories, endurance-test facilities, and training center are also located at the site.

Allow yourself to be convinced and talk about your visions with our experts. Because whenever it involves setting new standards, we are your partner. We look forward to a promising collaboration.

Our CMSE® certified specialists.

Philipp Herdlicka
Engineering
T: +43 (0) 2262 62 280-1758
p.herdlicka@smc.at

DI(FH) Patrick Wotawa
Engineering
T: +43 (0) 2262 62 280-1777
p.wotawa@smc.at

Our CMSE® certified specialists.