FESTO

Guideline for functional safety

Pneumatic and electric solutions

Festo – your partner for safety engineering

Your partner for safety engineering

For you, safety engineering is one of the most important requirements in factory automation or in the process industry.
That is why we offer products and solutions that are the perfect prerequisite to enable you to implement safety engineering as easily and cost-efficiently as possible.

Contents

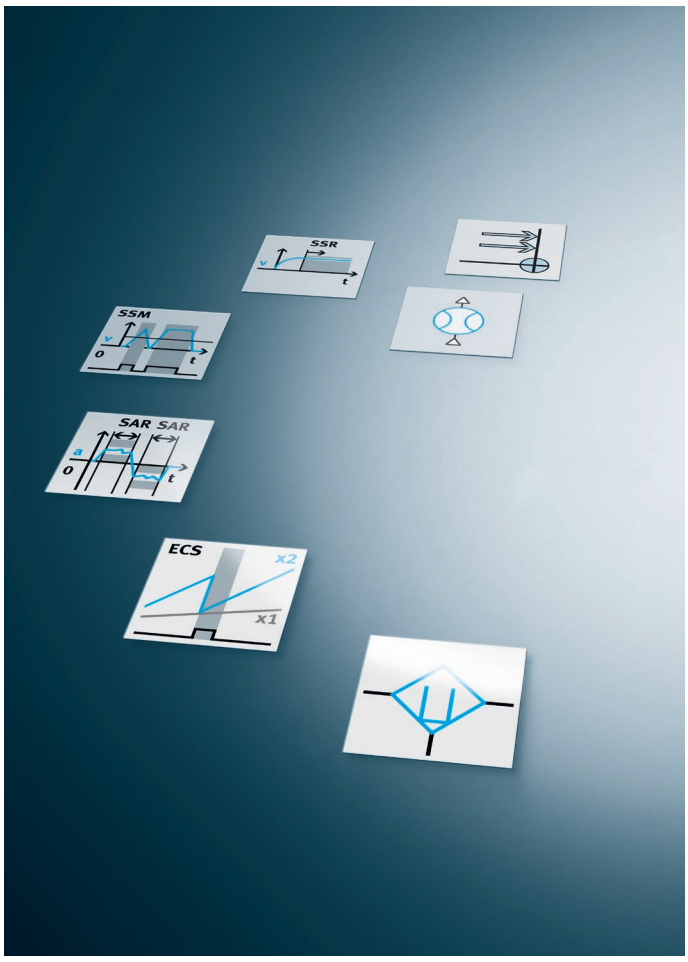
Your partner for safety

Quality has many aspects at Festo, one of which is working safely with machines. The result: our safety-related automation technology. It ensures that optimum safety is achieved in the workplace.

This brochure is intended as a guide and as a product overview.
It covers the core questions about safety-related pneumatics and electrical engineering:

- Why use safety-related pneumatic and electric components?
- How can I identify the risk posed by a machine or interlinked machine to the operator or user?
- Which standards and directives apply?
- What protective measures are based on these?
- What are the most common protective measures?

If you require more information, our specialists worldwide will be happy to help.



Reduce risk – think preventively

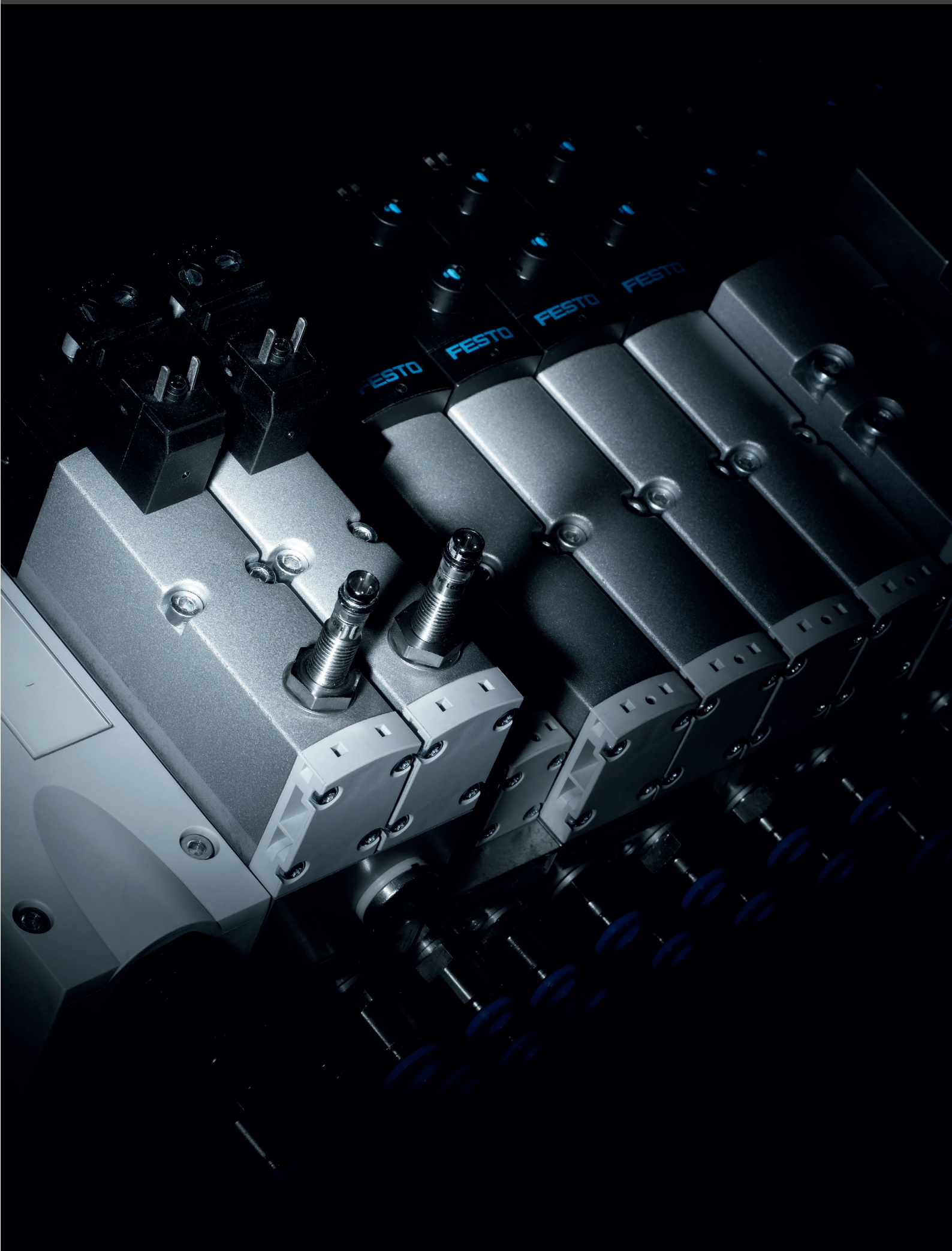
Machines have to be designed in a way that protects people, animals, property and the environment from harm. The objective is to prevent damage of any type. Using safety-related pneumatic and electric components from Festo provides you with the security that safety measures are implemented in compliance with the EC Machinery Directive.

This could, for example, be the reliable prevention of collisions or unexpected start-ups after an emergency stop. At the same time, using safety-related products also minimises the risk of liability claims.
The EC Machinery Directive 2006/42/EC prescribes a risk assessment for machines. This has helped to develop and define safety objectives.
These objectives are achieved using different passive protective measures and safety functions.

Safety-related solutions in the form of
- Components
- Circuits
- Engineering

make it easy to achieve your safety objectives.
Reliable operation of machines should be possible in all operating modes and stages of their service life.

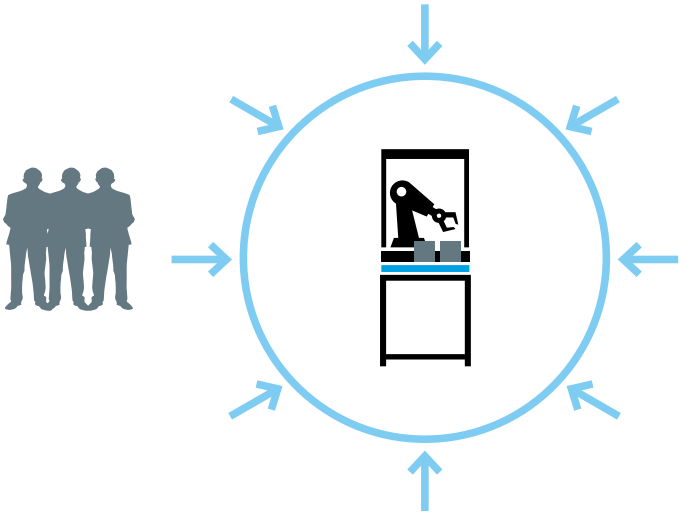
Safety-related solutions from Festo provide you with suggestions for
- Commissioning
- Automatic/manual operation
- Setting up
- Emergency functions
- Prevention of unexpected start-up
- Servicing/maintenance


FESTO
FESTO
FESTO
FESTO

Two sides: Security and Safety

There are two sides to safety engineering. On the one hand, it should provide protection for people and the environment against the hazards of machines and sytems. On the other hand, it should protect machines and systems against external threats, e.g. hackers.

Security

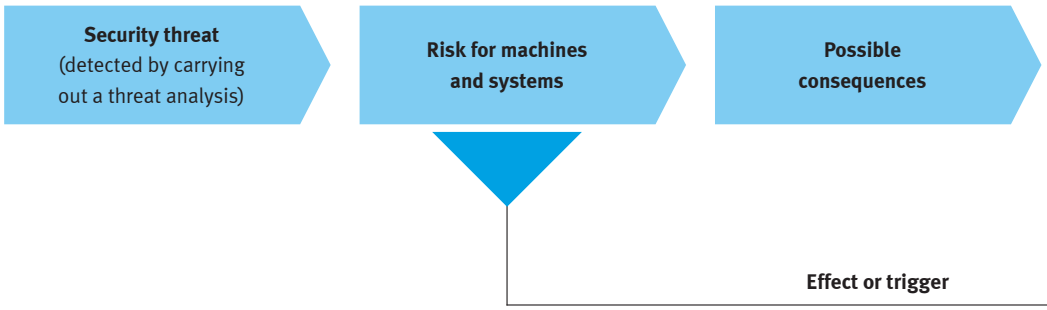


Protection of machines and systems

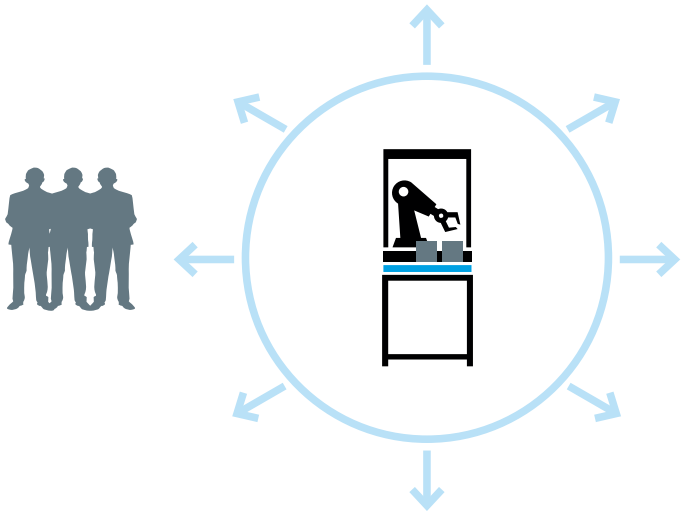
Machines and systems should be protected against external threats. These threats can include unauthorised access, viruses, trojans, etc.

Objectives:
- **Confidentiality**: No access to systems or data without authorisation.
- **Integrity:** Systems or data cannot be changed without authorisation.
- **Availability:** Authorised access to systems or data may not be obstructed.

These objectives lead to measures that form the basis for the protection of data, personal rights and knowledge. They are also a prerequisite for safety.



Safety (machines and system safety)



Protection of people and the environment

A machine or system may not pose any hazard to people and the environment.

Objectives:
- **Machine safety:** Protection against hazards posed by a machine or a system (protective measures, functional safety).
- **Occupational safety:** Protection against hazards associated with the use of a machine or system.

These objectives lead to measures that form the basis for the prevention of injury and health hazards.

In these guidelines, we will give an overview of products and solutions for machine safety in factory automation and in the process industry.

Failure or malfunction in a safety-related circuit → **Risk** → **Incorporation in the risk assessment**

Our added value in factory automation

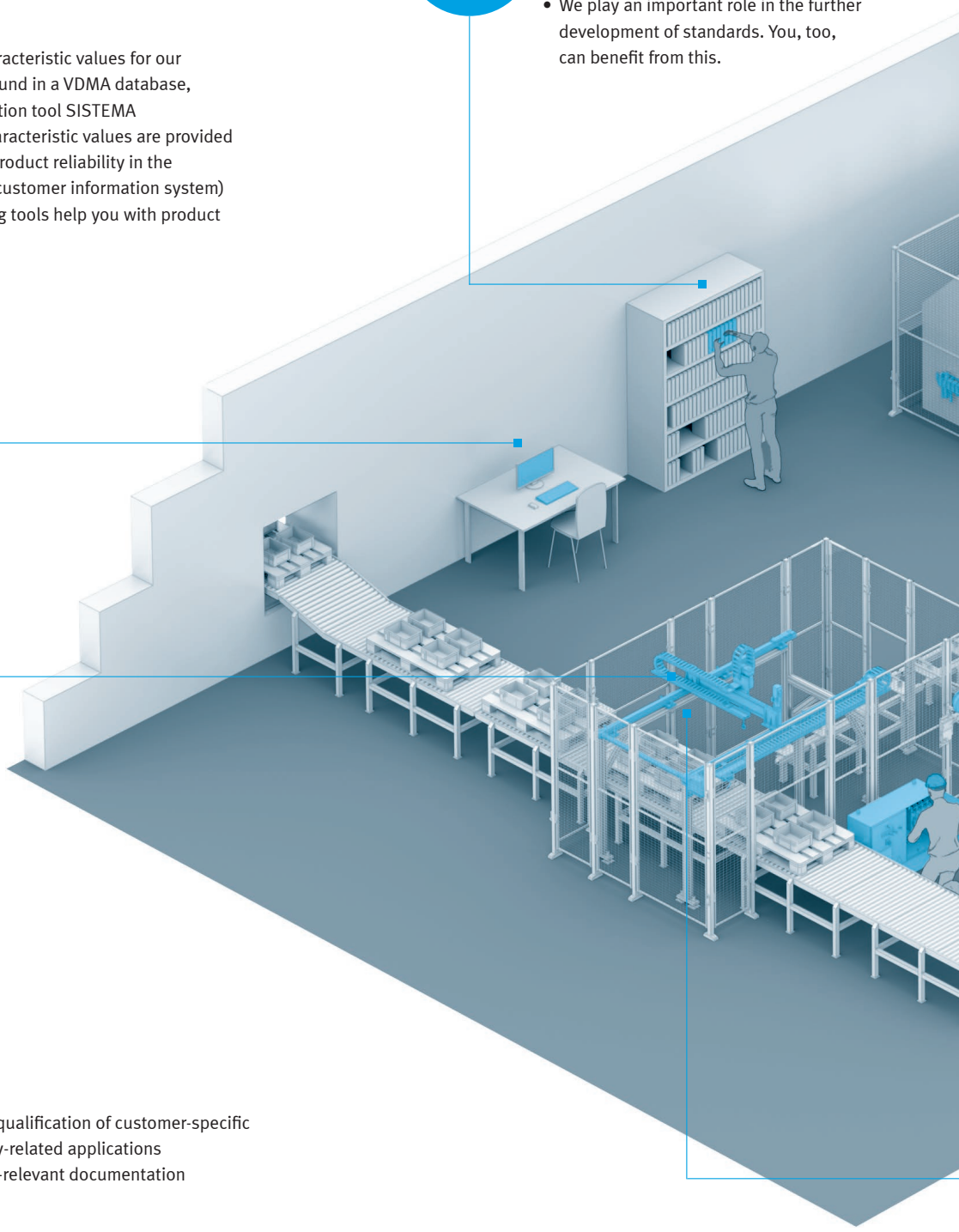
In factory automation, we support you with the implementation of functional safety in pneumatic and electric automation technology.

Standards and directives

- Our products are developed, tested and certified in accordance with the relevant standards
- Technical reports help you to implement the safety functions in accordance with the standards
- We play an important role in the further development of standards. You, too, can benefit from this.

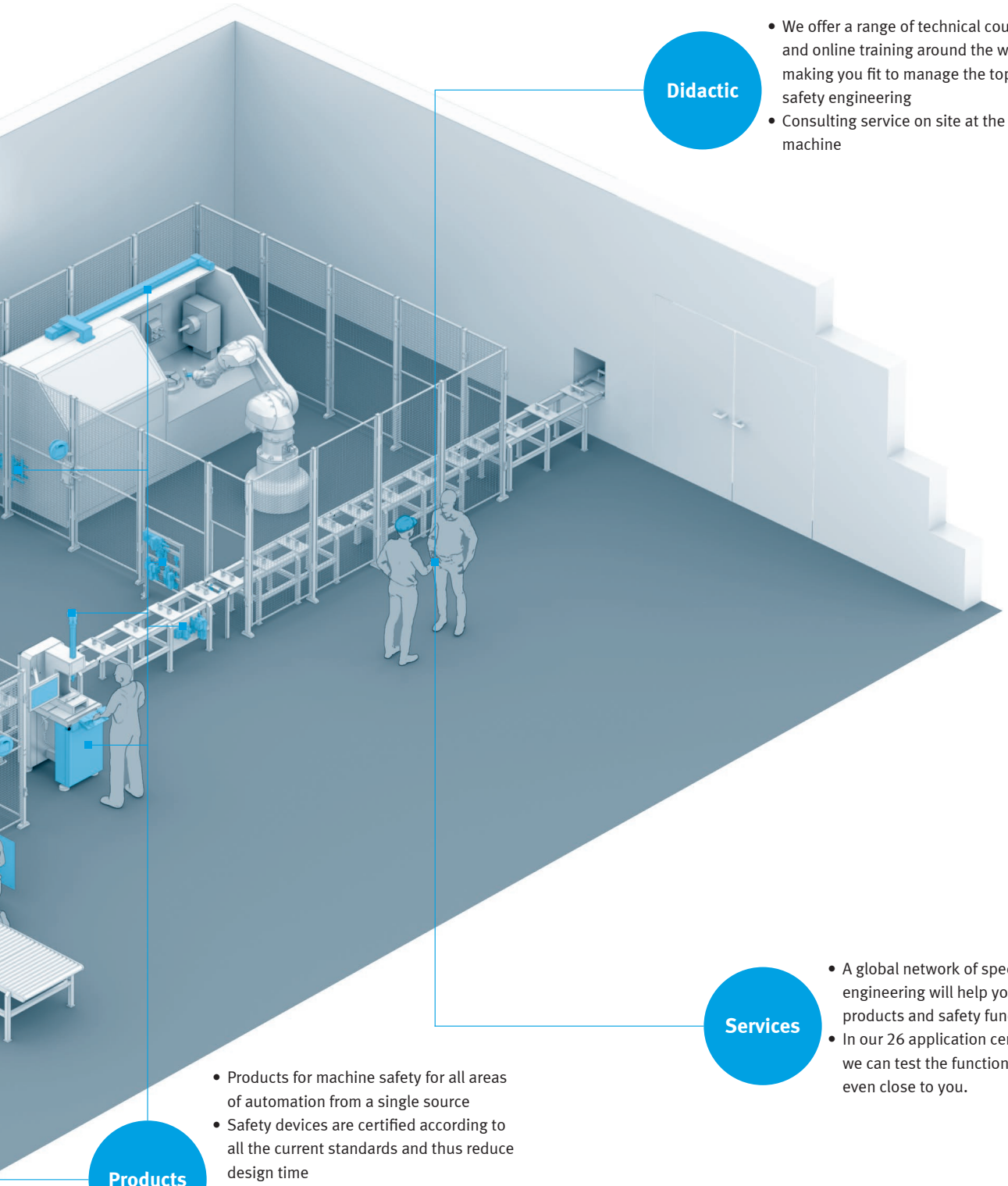
Tools

- Safety-related characteristic values for our products can be found in a VDMA database, e.g. for the calculation tool SISTEMA
- All the relevant characteristic values are provided in the data sheet product reliability in the catalogue (digital customer information system)
- Software and sizing tools help you with product selection



Customer-specific system solutions

- Development and qualification of customer-specific solutions for safety-related applications
- Provision of safety-relevant documentation



Didactic

- We offer a range of technical courses and online training around the world – making you fit to manage the topic of safety engineering
- Consulting service on site at the machine

Services

- A global network of specialists in safety engineering will help you to select the right products and safety functions
- In our 26 application centres worldwide, we can test the functions for your application – even close to you.

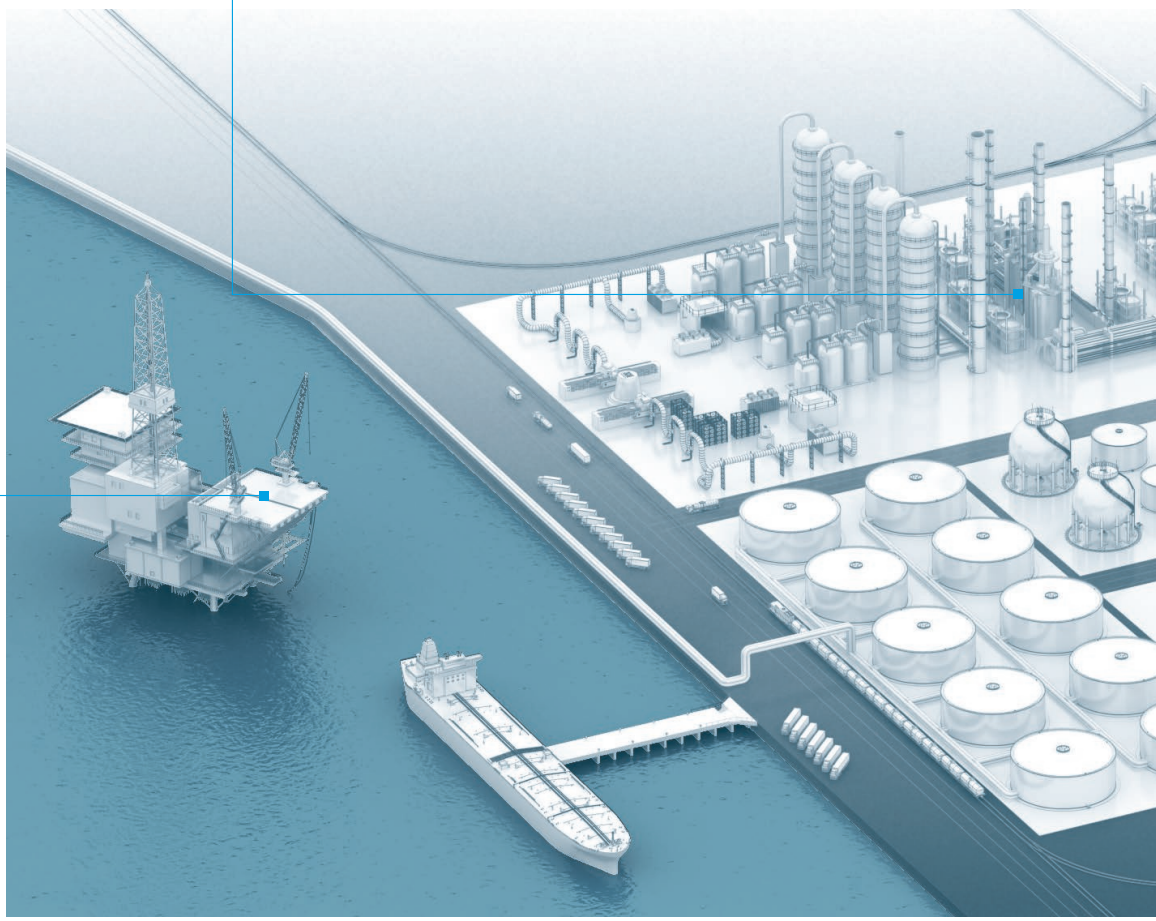
Products

- Products for machine safety for all areas of automation from a single source
- Safety devices are certified according to all the current standards and thus reduce design time
- All characteristic values for standard products are also available online
- Quick and easy calculation of the risk reduction

Our added value in the process industry

Customer-specific system solutions

- Development and qualification of customer-specific solutions for safety-related applications
- Provision of safety-relevant documentation



Certifica-tions

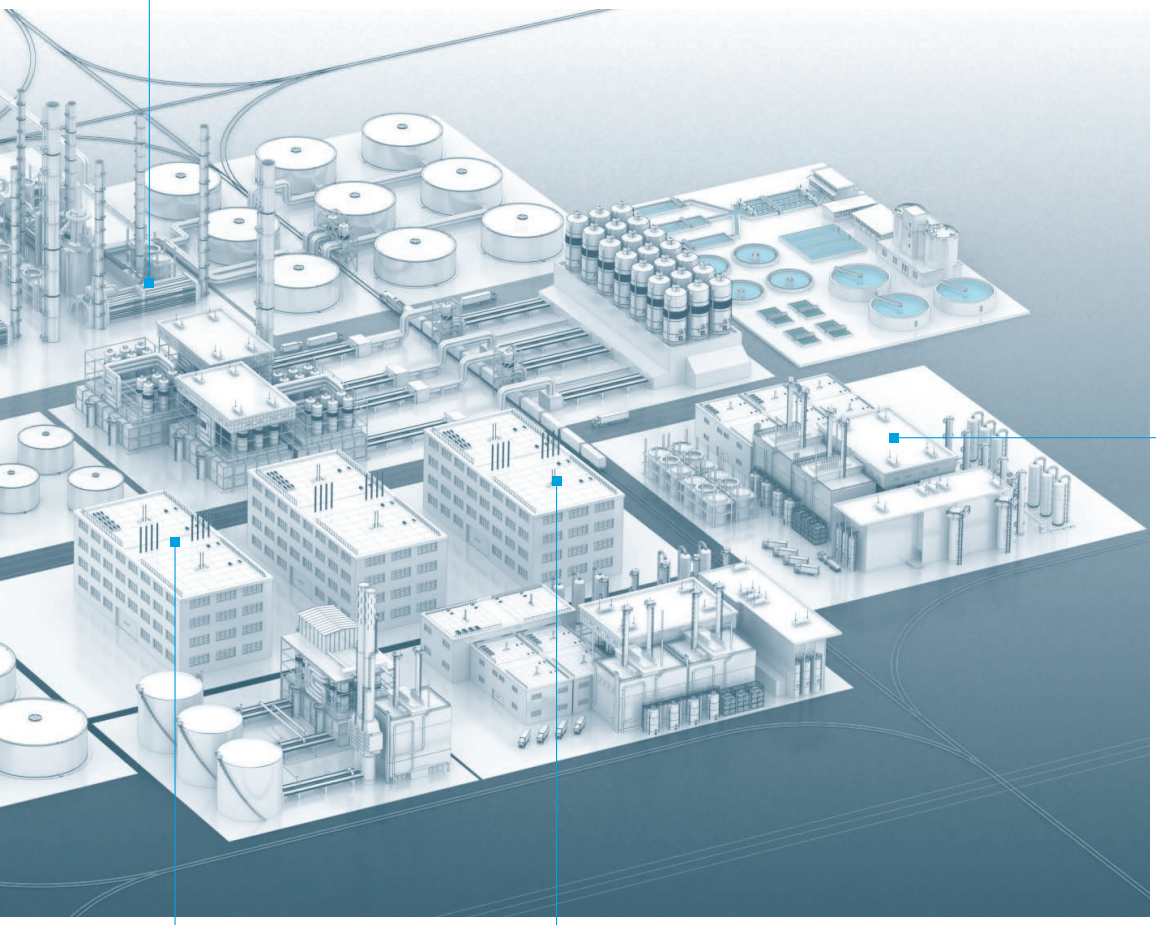
- SIL certificates from notified bodies
- SIL manufacturer's declaration available for numerous products and systems

Services

- A global network of specialists in safety engineering will help you to select the right products for safety-related circuits

Products

- Type tests in accordance with NE 95 for SIL-certified products
- Proven-in-use products for safety-related applications in the low-demand and high-demand area
- All safety-related product data are available online for a quick and easy calculation of the risk reduction



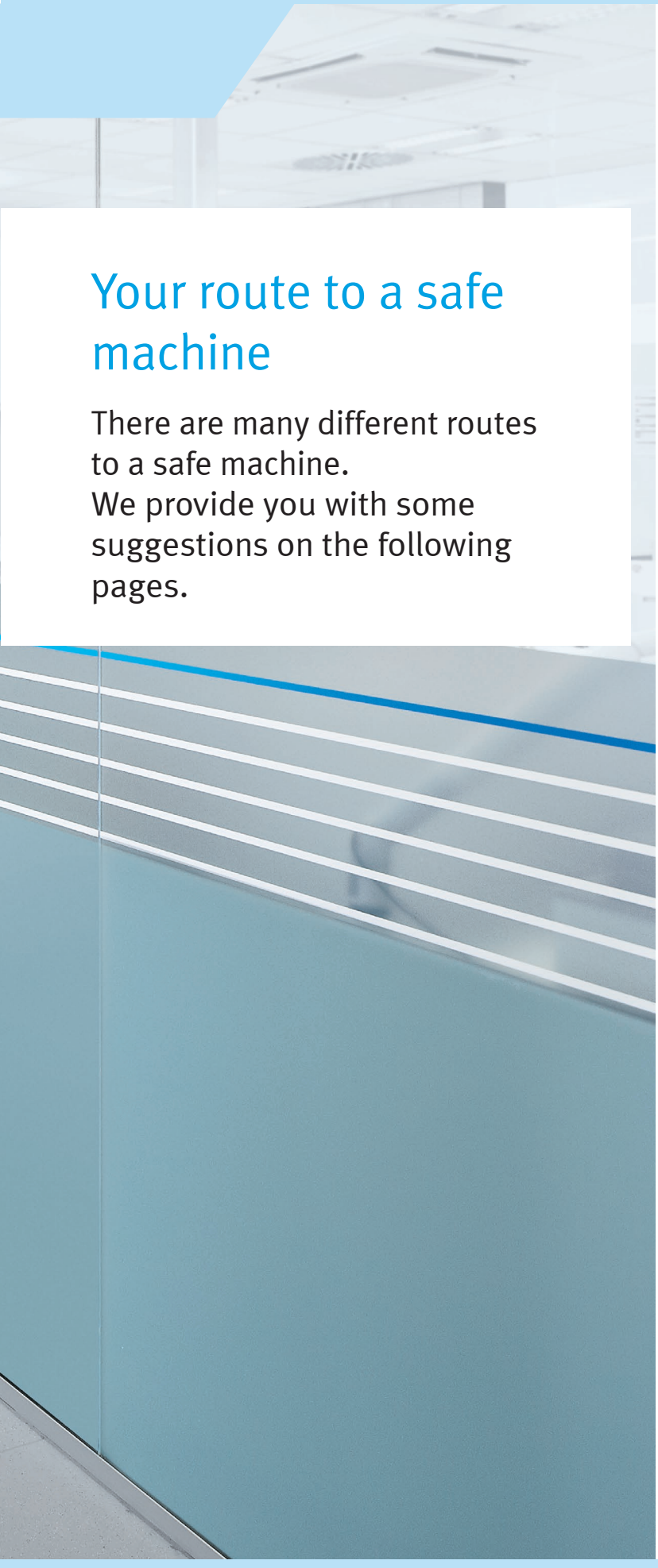
Didactic

- We offer a range of technical courses and online training around the world – making you fit to manage the topic of safety engineering

Standards and Directives

- We play an important role in the further development of standards – you, too, can benefit from this
- Our products are developed, tested and qualified in accordance with safety-related standards and recognised standards (e.g. NAMUR recommendations) for the process industry

01 Your route to a safe machine – factory automation



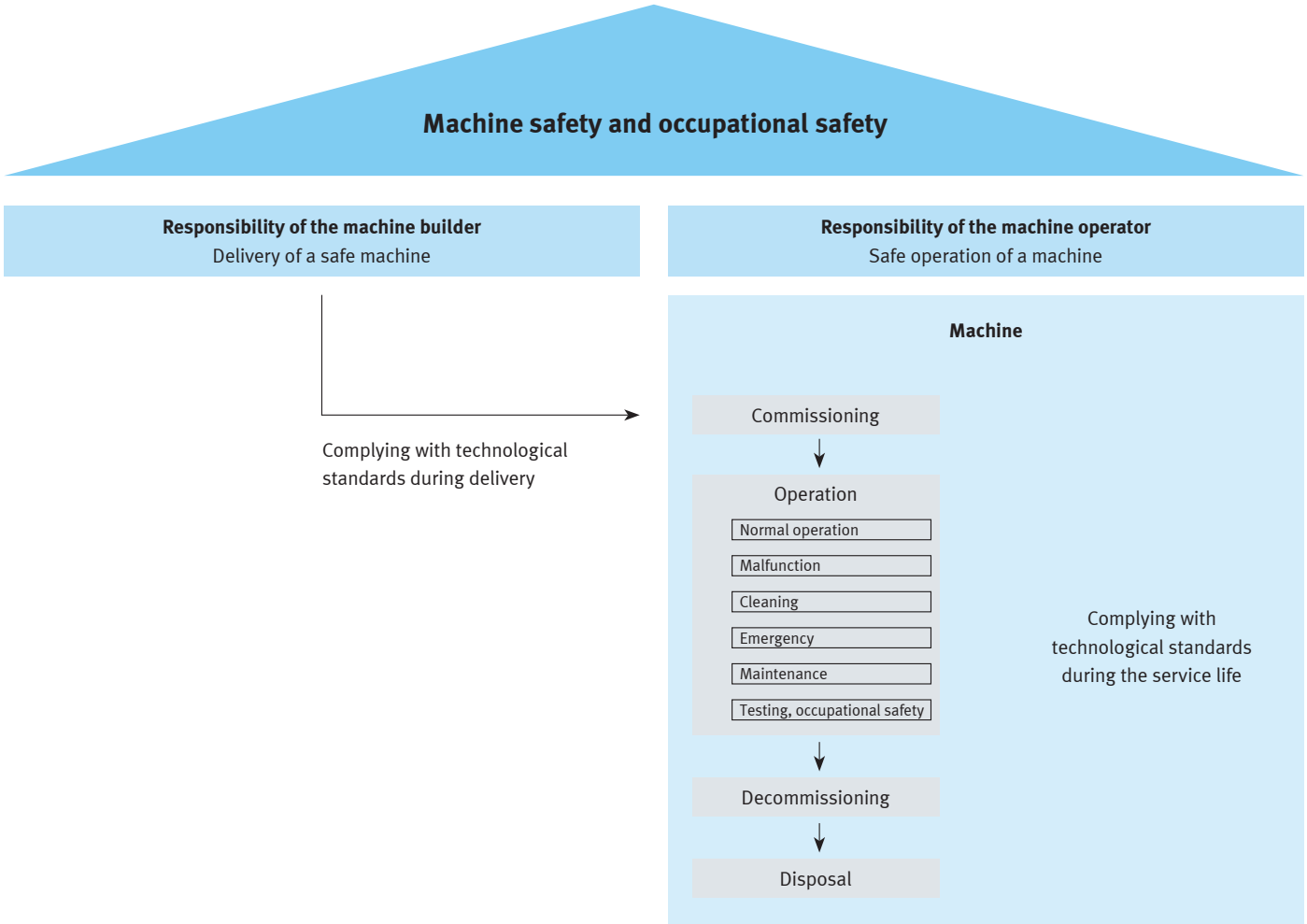
Your route to a safe machine

There are many different routes to a safe machine.
We provide you with some suggestions on the following pages.

Contents

Responsibility for machine safety and occupational safety

In the European Union, responsibility for machine safety is shared between the machine builder and the machine operator.
The machine builder is obliged to comply with technological standards for the required protective measures at the time of delivery of the machine. The legal conditions that need to be observed depend on the type of machine, application, the processed products, etc. At the very minimum, the machine builder generally needs to take into account the national laws on the implementation of the EC Machinery Directive 2006/42/ EC.
The machine operator must ensure that the requirements in terms of the occupational safety are complied with. The manufacturer is responsible for Complying with the technological standards of operation for the remainder of the service life. The legal framework conditions for a machine operator are specified by the national implementation of the Safety at Work Framework Directive 89/391/EEC. Specific directives such as the Work Equipment Directive 2009/104/EC are also relevant. The European guidelines provide the minimum requirements, and these can be strengthened by national regulations.



Outside the European Union, responsibility usually lies with just the machine operator. The contract can be designed so that it is the machine operator's obligation to employ corresponding safety engineering measures for the machine.

Basic standards for the implementation of machine safety

Research into the legal regulations and standards to be applied is crucial for the implementation of machine safety and a central component of each risk assessment. Festo Didactic offers training on carrying out risk assessments, see page 120.
How the requirements of guidelines can be implemented is specified in harmonised standards that can be applied on a voluntary basis.
The list with harmonised standards can be accessed via the “homepage” for the EC Machinery Directive 2006/42/EC:
→ European Commission
These standards do not fundamentally constitute the law and their application is thus voluntary. However, they define the latest technological state of the art for machine safety that must be complied with as a minimum.

A selection of the important standards and technical specifications is provided in the following table:

Type A standard	ISO 12100	Risk assessment and risk reduction
	ANSI B 11.0	General Requirements and Risk Assessment (USA)
Type B standards	ISO 13849	Safety-related parts of control systems
	ANSI B 11.26	General Principles for the Design of Safety Control Systems Using ISO 13849-1 (USA)
	ISO 4414	Rules and requirements for pneumatic systems
	EN 60204-1	Electrical equipment for machines
	NFPA 70	National Electric Code (NEC) (USA)
	NFPA 79	Electrical Standard of Industrial Machinery (USA)
	ISO 14118	Unexpected start-up
	CFR 1910.147	Control of Hazardous Energy (Lockout/Tagout) (USA)
	ISO 14119	Interlocking devices with safety guards
	ISO 14120	Guards
	ISO 13850	Emergency stop function
	ISO 13855	Arrangement of protective devices
	ISO 13857	Safety distances
	EN 349	Minimum gaps to avoid crushing of body parts
	ISO 10218	Industrial robots
	ANSI / RIA R15.06	Industrial robots (USA)
Type C standards	ISO 16090-1	Machining centres, milling machines, transfer machines
	ANSI B11.23	Safety Requirements for Machining Centers, Milling, Drilling and Boring Machines
	EN 13736	Pneumatic presses
	ANSI B11.2	Safety Requirements for Hydraulic and Pneumatic Power Presses
	ISO 23125	Turning machines
	EN 1010	Printing and paper converting machines
	EN 422	Blow moulding machines
	EN 848	Woodworking machines
	ISO 11161	Integrated manufacturing systems
	ANSI B 11.20	Integrated Manufacturing Systems (USA)
Other standards	ISO 5598	Fluid power systems and components – Vocabulary
	ISO 1219	Fluid power systems and components – Graphical symbols and circuit diagrams
	EN 81346-2	Classification of objects and codes of classes
	EN 82079-1	Preparation of instructions for use
	EN 61508	Functional safety of safety-related electrical, electronic and programmable electronic systems
	EN 61511	Safety instrumented systems for the process industry
	EN 62061	Functional safety of safety-related electrical, electronic and programmable electronic control systems
	EN 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional safety
Technical specifications	ISO/TR 14121-2	Risk assessment – Practical guidance and examples of methods
	ISO/TR 23849	Guidelines on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machines
	ISO/TR 20218-1	Robots – end effectors
	VDMA 24584	Safety functions of regulated and unregulated systems
	ISO/TS 15066	Collaborating robots
	ZVEI CB24I	Position paper classification 24-V interfaces with testing

Global safety engineering conditions

There are legal requirements around the world to ensure that machines can be safely built and operated. Almost all regulations stipulate a risk assessment to be able to identify risks. These can be used to determine and implement measures aimed at minimising risk.

Training and Consulting by Festo Didactic

Festo solutions

Laws

e.g. EC Machinery Directive 2006/42/EG

Objectives: safe machines and protection of personnel

Risk assessment and risk reduction (ISO 12100)

Risk analysis ➔ Risk assessment (PL r, SIL CL) ➔ Risk reduction
- ➔ Design measures (inherently safe design)
- ➔ Safeguarding and additional protective measures
  - ➔ Passive protective measures, e.g. protective guard, safety door
  - ➔ Active protective measures, e.g. safe stop function
- ➔ Protective measures via user information

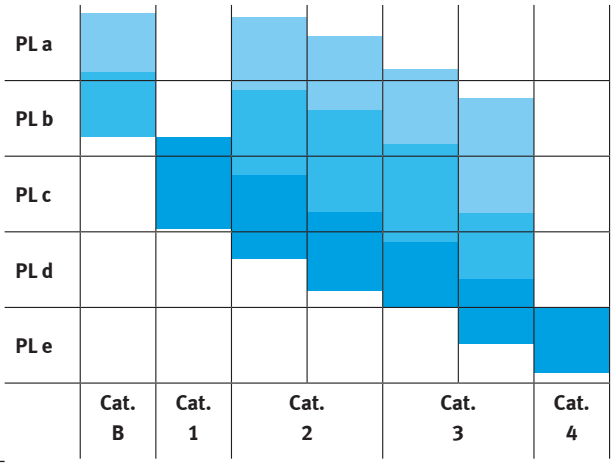
Objectives: standardised processes + “check lists” + adequate risk reduction

Safety function

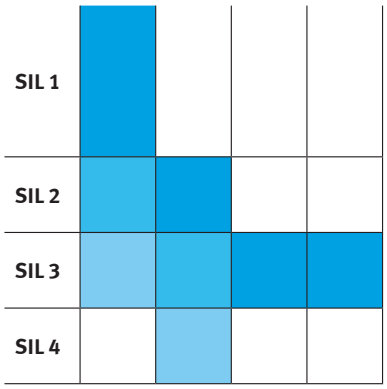
Input — Logic — Output

Objective: Standards-compliant implementation of active protective measures

Standards for machine safety: ISO 13849-1, IEC 62061



Standards for system safety: IEC 61511



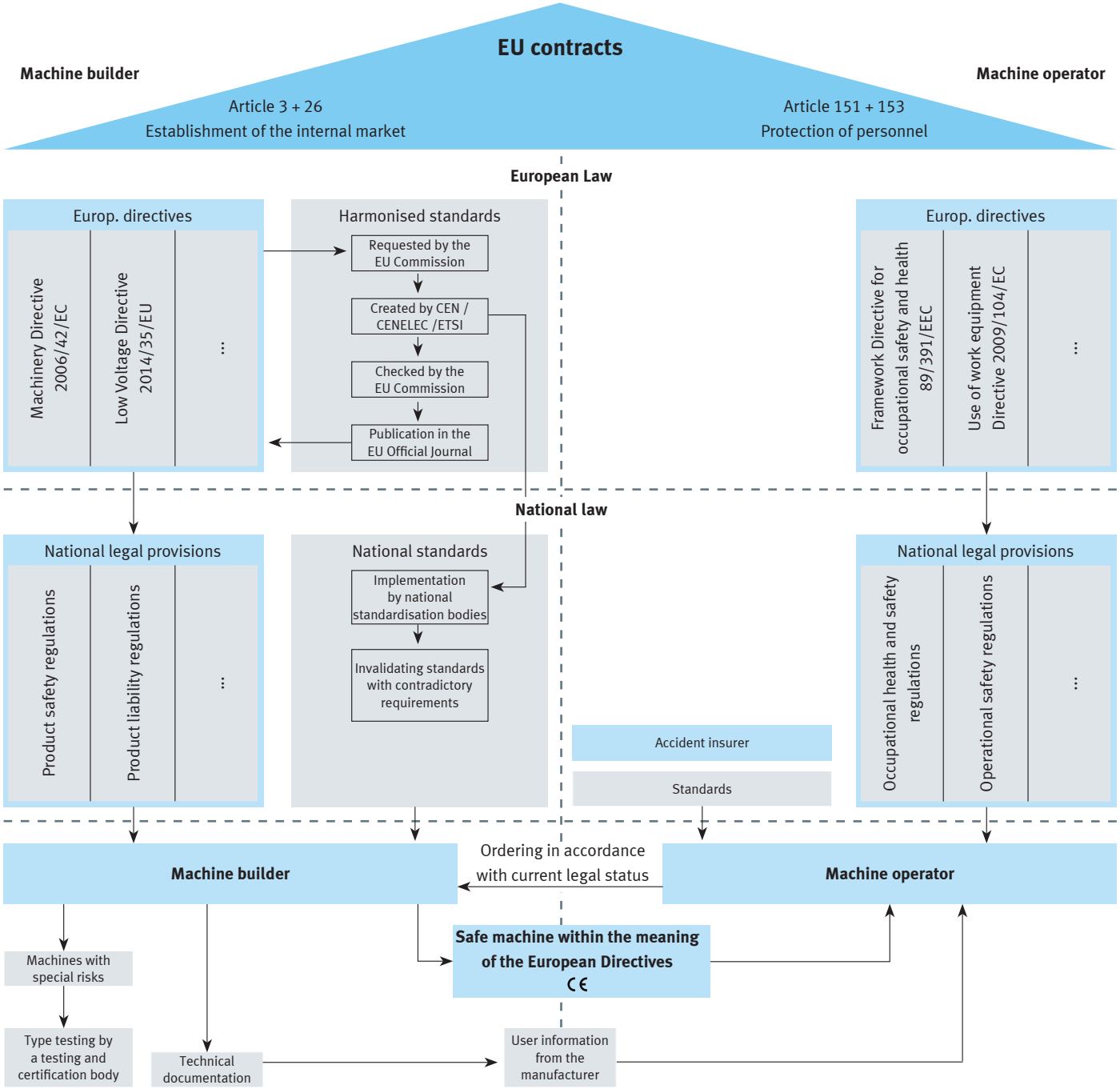
Objective: proof of adequate risk reduction through active protective measures

Evaluation:

PL ≥ PL r | **SIL ≥ SIL CL**

Safety engineering conditions in machine building for the EU

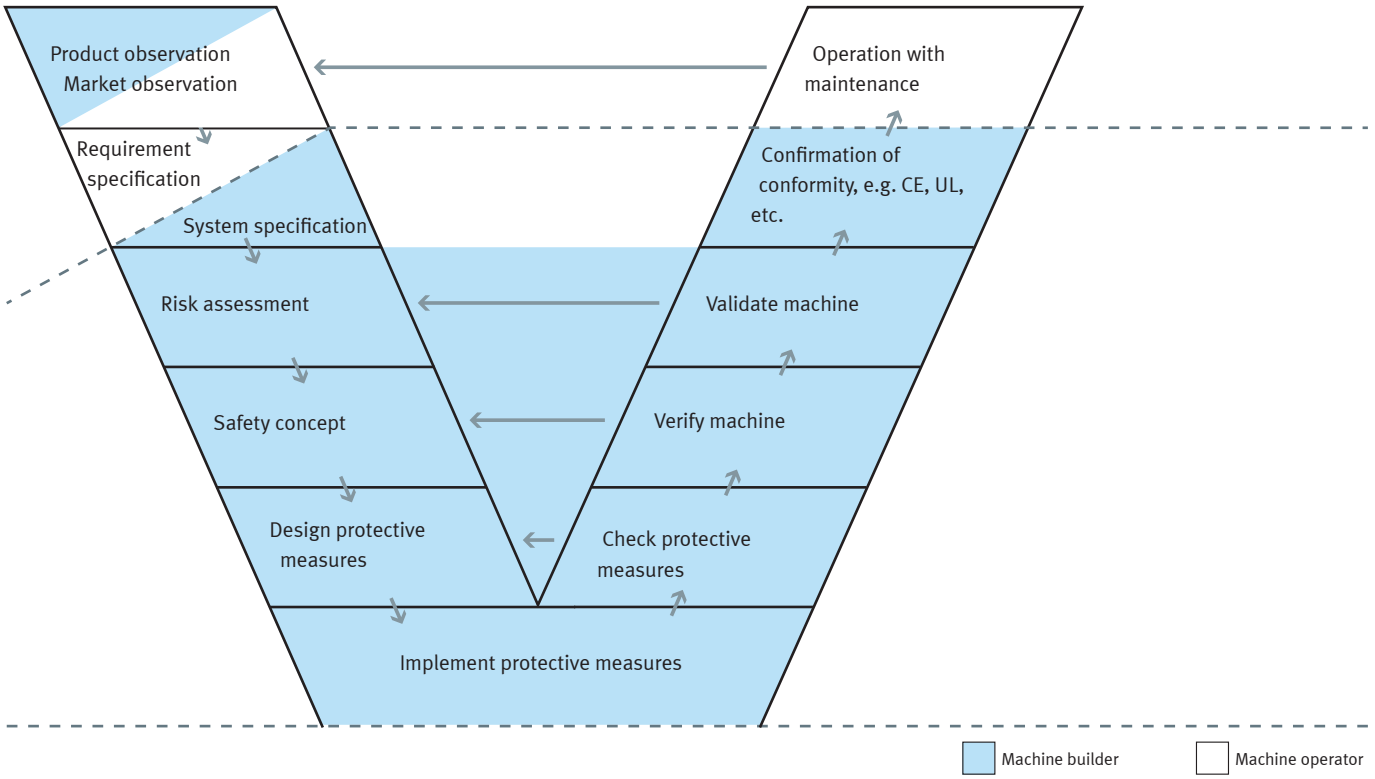
At the same time as the single European market was developed, the regulations and standards for machine construction in the manufacturing industry were harmonised.



It is always a challenge to determine which regulations and standards are applicable for a certain machine. The machine builders and machine operators must apply the valid laws, standards and regulations. The European Union publishes its guidelines in most languages spoken in the European Union and these must correspond with national legislation. For many European guidelines, there are also standard lists that specify how these guidelines can be implemented. The Internet sites of the European Union are therefore a good starting point for research.

Your route: V model for the development of a safe machine

Numerous regulations, standards and technical specifications have resulted in various steps that must be taken into account in compliance assessment procedures for a safe machine. The V model can help machine builders to put in place a quality-assured process.

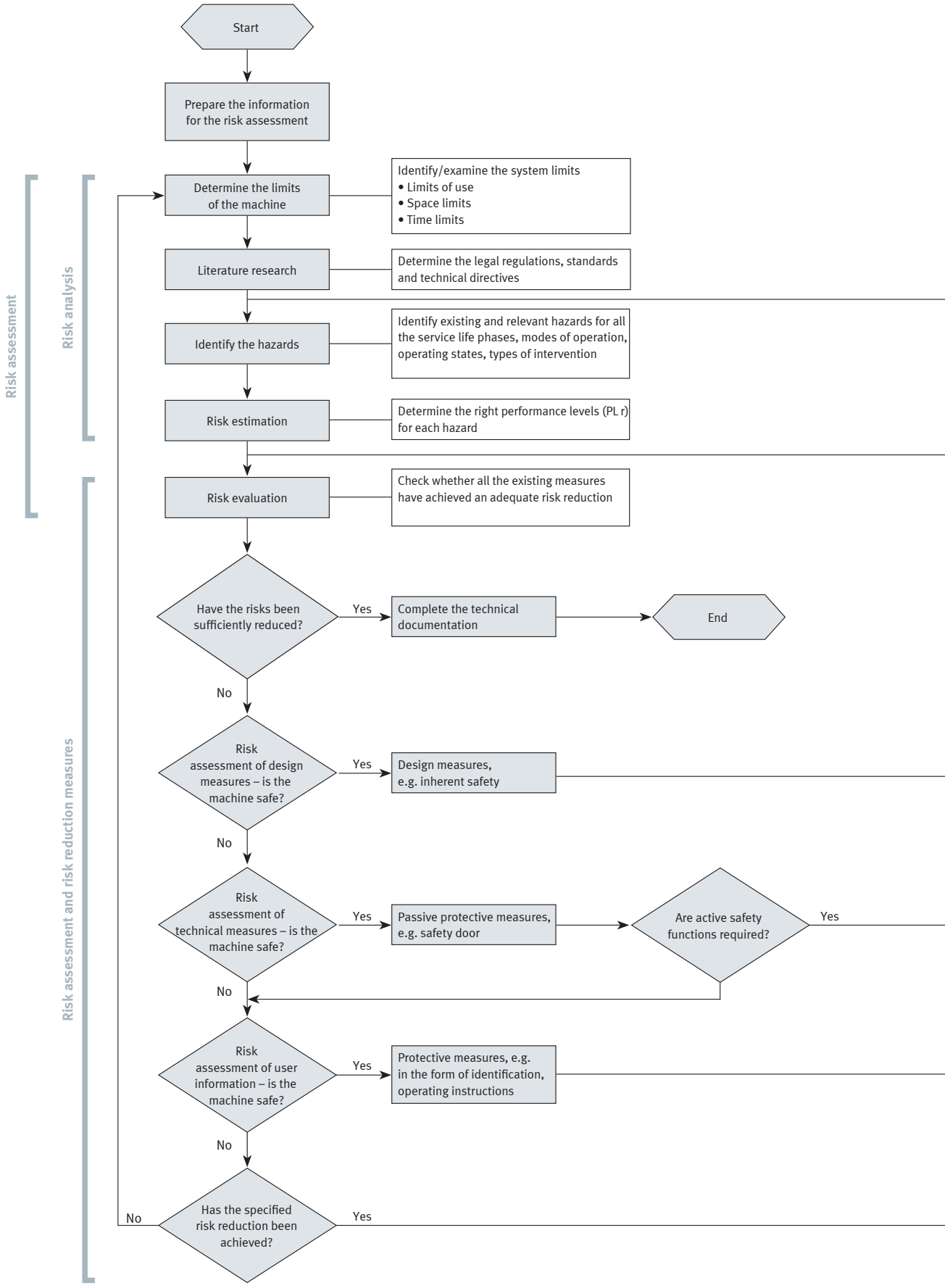


The first step is the technical specification and the requirements that need to be continuously extended. This is then followed by the implementation, which is checked against the specifications in ascending order. This creates the typical V model in which the individual development phases are compared to the respective test phases.

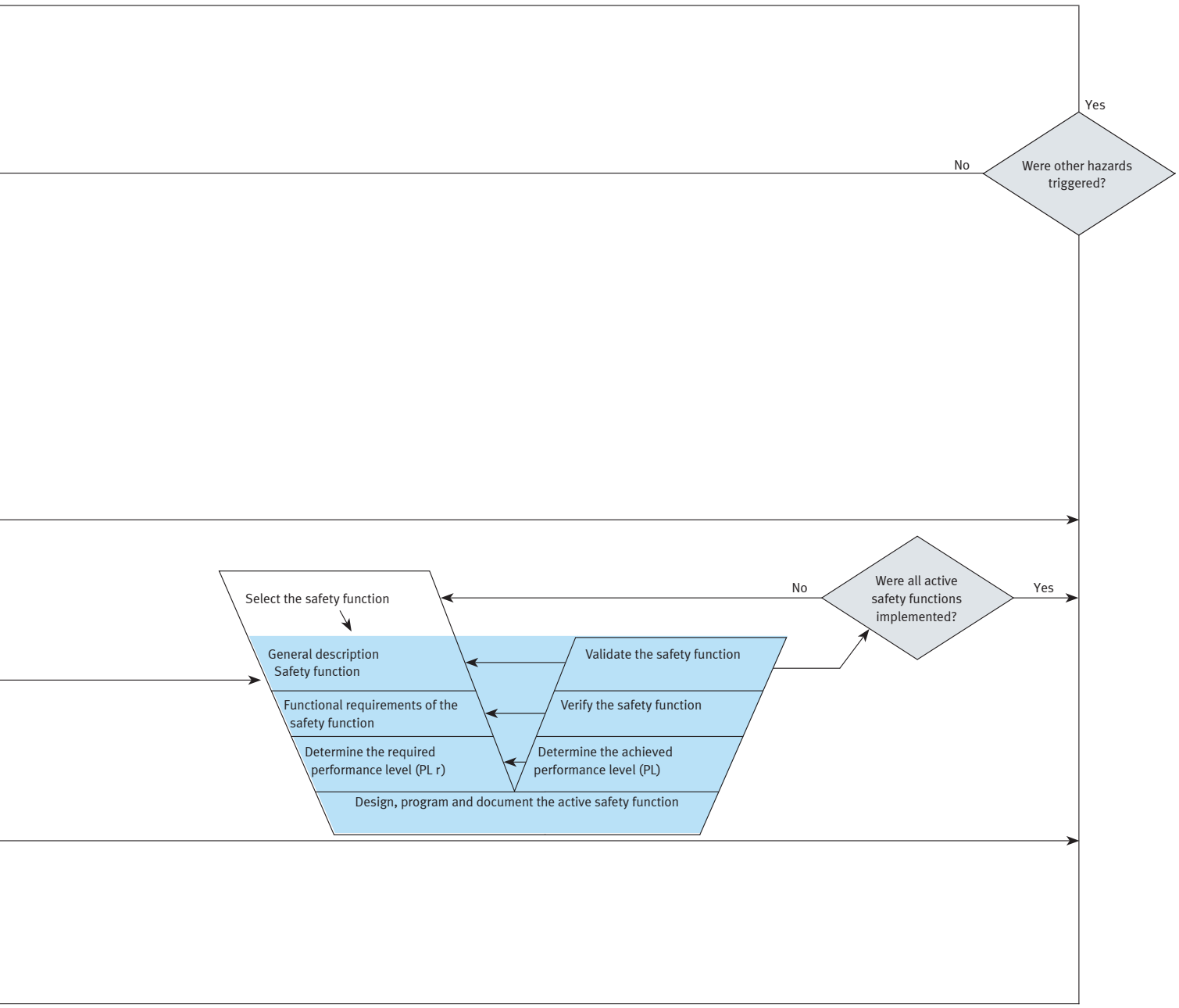

FESTO
Edit

Risk assessment and risk reduction

A well proven method throughout the world for determining the requirements for machine safety is carrying out a risk assessment, stipulating protective measures in accordance with ISO 12100 and implementing functional safety in accordance with ISO 13849 (for USA: ANSI B 11.0 and ANSI B11.26).
In the risk analysis, all the required information is first compiled, the basic hazards are identified and their risk potential estimated. On the basis of this risk estimation, a decision is taken on whether protective measures are required for each hazard.

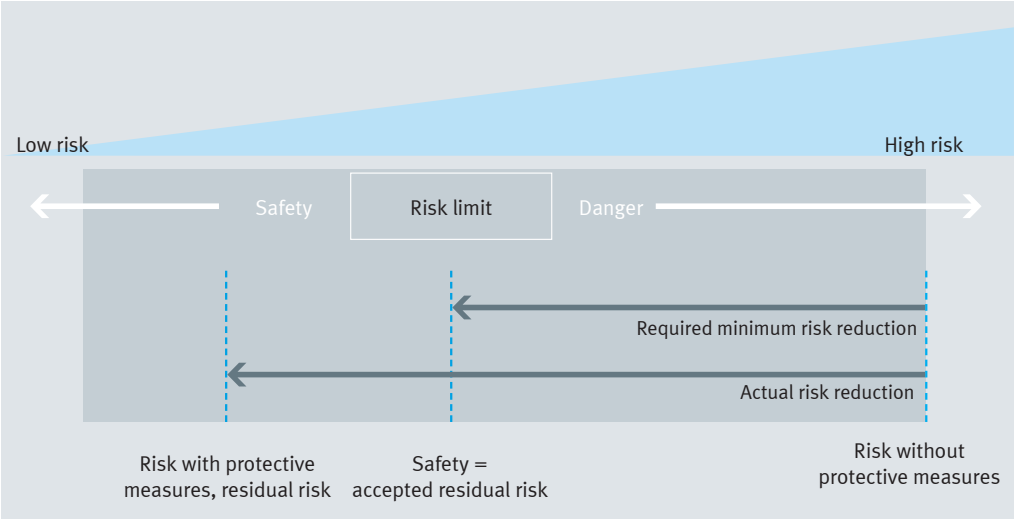


The protective measures are implemented in a three-phase process. First, a risk must be eliminated or reduced via design measures. If this is not possible, safeguarding measures can be taken. It if is also not possible to take safeguarding measures, a risk reduction can only take place through the user information. If the subsequent risk assessment leads to the conclusion that all risks have been sufficient reduced, the risk assessment can be completed.



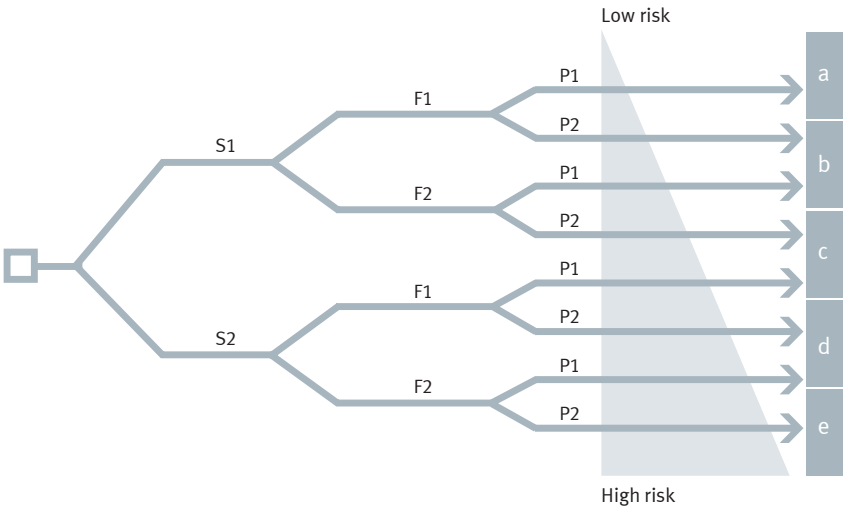
Risk and risk estimation – PL r

Risks are the result of hazards and relate to the severity of possible damage and the probability of the damage occurring.



Risk relative to the observed hazard = **Severity** of the possible damage • **Probability** of the damage occurring

There are numerous tools for estimating a risk. These include a risk matrix, a risk graph, numerical assessments, etc.
ISO 13849-1 recommends the use of a risk graph that specifies the risk potential as the required performance level (PL r).

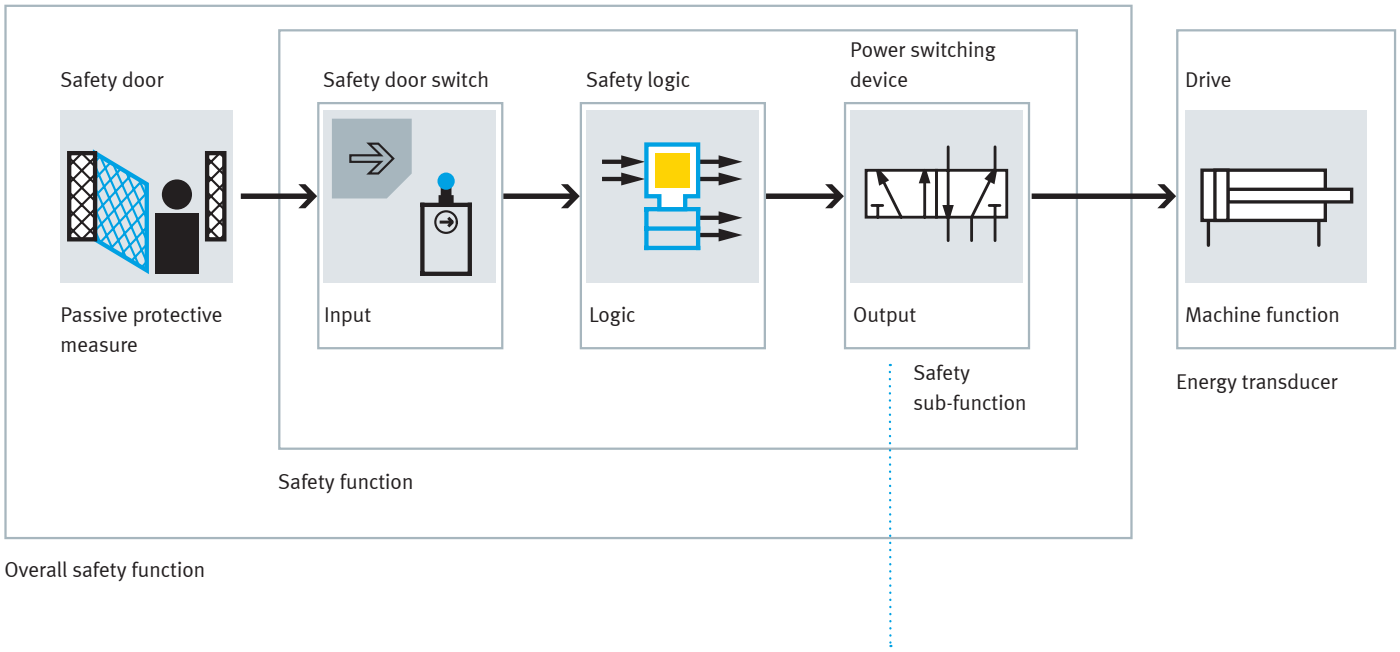


Risk parameter		Possible assessments
S	**Severity of injury**	
S1	Slight (generally reversible injury)	Injuries that require nothing more than first aid or do not lead to more than two days of absence from work.
S2	Serious (usually irreversible injury or death)	Injuries that require treatment by a doctor or lead to more than two days of absence from work.
F	**Frequency and/or duration of the exposure to hazard**	
F1	Seldom to less often and/or the time of exposure to hazard is short	No more than twice per shift (8 working hours) and shorter than 15 minutes in total per shift
F2	Frequent to continuous and/or the duration of the of exposure to hazard is long	More than twice per shift (8 working hours) or longer than 15 minutes in total per shift
P	**Possibility of avoiding the hazard or limiting the damage**	
P1	Possible under certain conditions	In certain cases, the hazard can be reduced.
P2	Scarcely possible	Hazard cannot be avoided.

Overall safety function

The overall safety function is a protective measure for risk reduction that can be used to reach or maintain a safe machine state. It takes specific risk events or situations into account.

An example is the separation of the operator from the hazard zone. To allow the operator access, the hazardous drive movement is stopped and the drive is then maintained The overall safety function thus consists of, as a minimum, a passive protective measure, the sensor (input), the logic (safety relay unit) and the valve combination (output).



Important: the safety sub-function
Safety sub-functions are part of a safety function.
A safety sub-function is performed by a component or a group of components of this safety function.

Typical example:
The disconnection from the power supply by a power switching device such as valve, motor controller or contactor (relay).

Overview of safety sub-functions

Normal operation


Safety door switch


Light curtain


Two-hand control

Special operation, e.g. collaborating operation


Laser scanner


Camera system

Set-up and service operation

Mode selector switch


Enabling button


Safety shut-off mat

Emergency operation


Emergency stop device

Monitoring functions

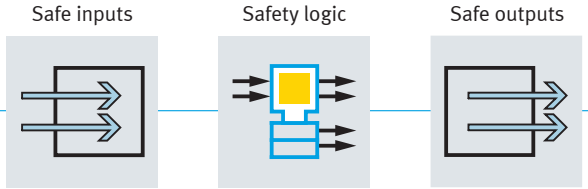

Limit switch

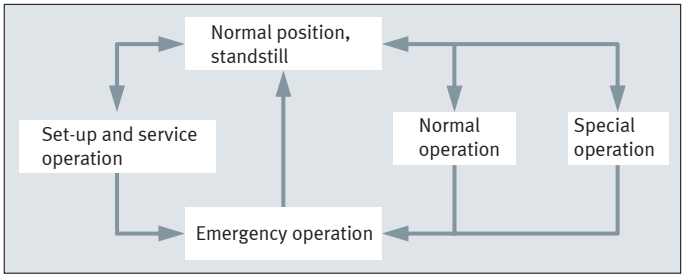

Measuring system


Pressure switch


Switching position monitoring


Position monitoring





Output

Output

Pneumatic drive technology
in accordance with VDMA standard sheet 24584

Safety sub-functions that affect systems


SDE –
Safe de-energization


SEZ – Safe energization


PUS (LOTO) – Prevention
of unexpected start-up,
lockout-tagout

Safety sub-functions that affect drives


STO – Safe torque off


PUS – Prevention of
unexpected start-up


SS1 – Safe stop 1


SSC – Safe stopping
and closing


SOS –
Safe operating stop


SS2 – Safe stop 2


SDI – Safe direction


SSB – Safe stopping and
blocking (in mechanics)


SB – Safe blocking (not
part of the VDMA 24584)


SBC – Safe brake control

Monitoring safety sub-functions


SLS –
Safely limited speed


SLT – Safely limited
torque (force)


SET – Safe equilibrium
of torque

Electric drive technology
in accordance with ISO 61800-5-2

Safety sub-functions that affect drives

STO – Safe torque off

SS1 – Safe stop 1

SOS –
Safe operating stop

SS2 – Safe stop 2

SDI – Safe direction


SSB – Safe stopping
and blocking (not part
of ISO 61800-5-2)

SBC – Safe brake control

Monitoring safety sub-functions

SLS –
Safely limited speed

SLT – Safely limited
torque

Safety sub-functions in drive technology

Pneumatics

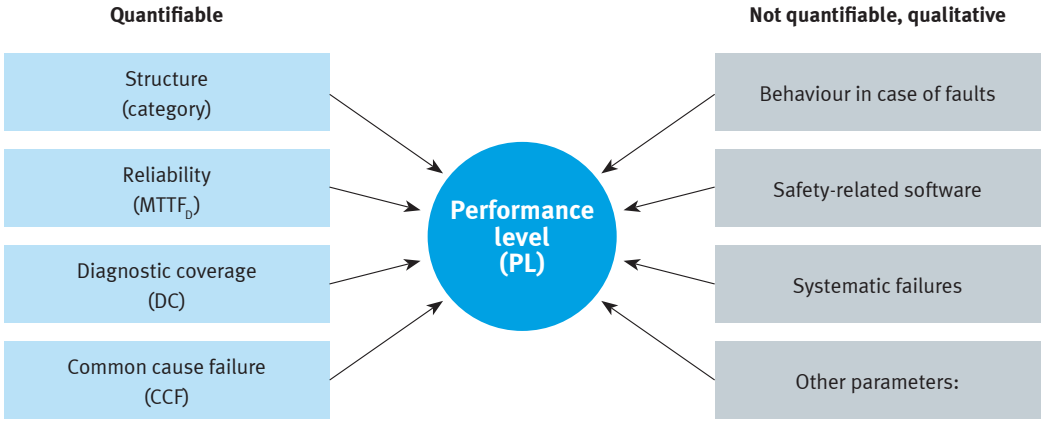
Safety sub-functions (active) that affect systems	**STO** **Safe torque off** **(Safe torque off)** The power supply to the pneumatic drive is separated. The chambers of the pneumatic drive are exhausted so that no force (torque) can be generated that could lead to a dangerous movement.	**SS1** **Safe stop 1** The volumetric flow rates into and out of the two chambers of the pneumatic drive are reduced or blocked. This slows down the movement of the drive and brings it to a stop. If the standstill is reached in accordance with the defined tolerance window, the pressure in the chambers of the pneumatic drive is reduced so that no force (torque) is generated that could lead to a dangerous movement.	**SOS** **Safe operating stop** **(Safe operating stop)** The SOS function prevents the drive from deviating from the stopping position by more than a specific amount. The compressed air supply is maintained to enable the drive to withstand the effect of external forces (e.g. variable load) without further measures (e.g. mechanical holding brakes).
	SS2 **Safe stop 2** The volumetric flow rates into and out of the two chambers of the pneumatic drive are reduced or blocked, thus slowing down the movement of the drive and bringing it to a stop. If the standstill is reached in accordance with the defined tolerance window, the pressure in the chambers of the pneumatic drive is maintained so that the existing pressure can be used to maintain the standstill.	**SSC** **Safe stopping and closing** The supply of energy to or dissipation of energy from at least one chamber of the pneumatic drive is closed, and the stored energy is used to achieve the stop.	**SLS** **Safely limited speed** The SLS function prevents the pneumatic drive from exceeding the permissible speed.
	SSB **Safe stopping and blocking** The pneumatic drive is brought to a standstill. The free movement of the output component is blocked. Blocking can be done by positive locking or friction locking.	**SB** **Safe blocking** **(not part of the VDMA 24584)** The free movement of the output component is blocked. Blocking can be done by positive locking or friction locking.	**SSx** **Safe stopping** **(not part of the VDMA 24584)** The movement of the drive is brought to a standstill. The SSx function is a higher-level safety sub-function and is generally implemented via various safety sub-functions with a stop character.
	SLT **Safely limited torque (force)** The SLT function prevents the pneumatic drive from exceeding the permissible torque (force).	**SET** **Safe equilibrium of torque** The SET function prevents the pneumatic drive from deviating from the torque (force) equilibrium by more than a specific amount.	**PUS** **Prevention of unexpected start-up** The PUS function prevents the start position of the valve from changing and leading to an unexpected start-up of a machine function.
Safety sub-functions (active) that affect systems	**SBC** **Safe brake control** The SBC function provides a safe output signal for controlling an external brake or clamping unit.	**SDE** **Safe de-energization** The SDE function enables the downstream pneumatic system to be safely separated and de-energised.	**SEZ** **Safe energization** The SEZ function permits safe energisation using a defined force/time function (soft-start function).

Electric systems

Safety sub-functions that affect systems	**STO** **Safe torque off**  A force-generating energy supply to the electric drive is prevented. This function also prevents an unexpected start-up in electric drives.	**SS1** **Safe stop 1**  The electric drive is brought to a standstill within specific limits (delay, time, etc.) and the safety sub-function STO is subsequently executed.	**SOS** **Safe operating stop**  The SOS function prevents the drive from deviating from the stopping position by more than a specific amount. The energy is supplied to the electric drive so that it can withstand the effect of external forces.
	SS2 **Safe stop 2**  The electric drive is brought to a standstill within specific limits (delay, time, etc.) and the safety sub-function SOS is subsequently executed.	**SDI** **Safe direction**  The SDI function prevents the drive from moving in the incorrect direction.	**SSB** **Safe stopping and blocking**  The pneumatic drive is brought to a standstill. The free movement of the output component is blocked. Blocking can be done by positive locking or friction locking.
Safety sub-functions that affect systems	**SBC** **Safe brake control**  The SBC function provides a safe output signal for controlling an external brake or clamping unit.		
Monitoring safety sub-functions	**SLS** **Safely limited speed**  The SLS function prevents the electric drive from exceeding the permissible speed.	**SLT** **Safely limited torque**  The SLT function prevents the electric drive from exceeding the permissible force (torque).	

Performance level – which parameters are used to determine this?

The performance level (PL) specifies the capability of safety circuits to execute a safety function under foreseeable conditions. It is specified as a discrete level from PL a to PL e. A performance level is only determined for complete safety circuits or for safety devices.



The **structure** of a safety circuit is determined by the arrangement of the components and the diagnostics. These structures are divided into categories B to 4, which determines the classification of the safety circuits in terms of their resistance against faults and their behaviour when a fault occurs. See page 32.

The **reliability** of the components used in the safety circuits is taken into account by the $MTTF_D$ value. The $MTTF_D$ value specifies the mean expected value up to a dangerous failure of a channel of the safety circuits.
Components affected by wear are assigned a B_{10} value that can be converted into an $MTTF_D$ value for a concrete application with the help of the actuation rate. Information on determining the $MTTF_D$ from the B_{10} can be found on page 34.

The **diagnostic coverage (DC)** is a measure of the effectiveness of the diagnostics. It specifies the proportion of identifiable and unidentifiable dangerous failures. The higher the risk, the higher the effectiveness of these diagnostics. See page 38.

Common cause failures (CCF) are failures of different components due to a single event with the failures not being interdependent. These failures are not the result of different causes. See page 40.

For category 2 safety circuits, the **behaviour in the event of faults** must be determined with a failure mode and effects analysis (FMEA) or fault tree analysis (FTA). Depending on the application and the selected components, additional measures may be needed to meet the requirements of ISO 13849.

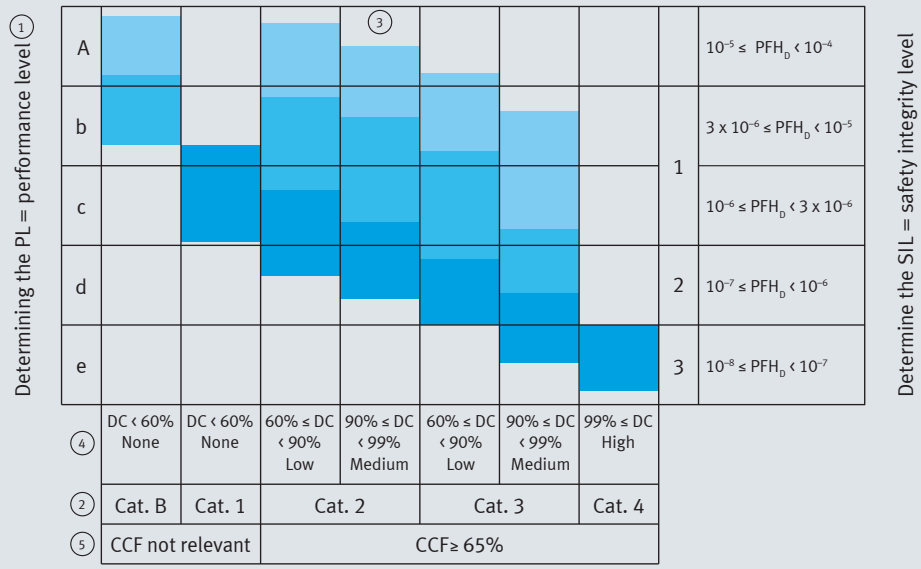
The product lifecycle of **safety-related user software** must take into account the prevention of faults. The primary objective is readable, understandable, testable, maintainable, and preferably fault-free user software. This is supported accordingly by the software for programmable or configurable safety relay units.

Systematic failures are failures that can be traced back to a specific cause and can only be eliminated by changing the design, manufacturing process, operating behaviour and documentation.

Other parameters concern the ambient conditions, requirement rate, substances affecting the materials, etc.

Your route to performance level

The figure shows the simplified procedure for determining the performance level (PL) of a safety function.
The PL is a function of categories B to 4, the diagnostic coverage (DC) “none to high”, various $MTTF_D$ areas and the common cause failure (CCF).
The PL can be assigned to a specific safety integrity level (SIL) level.
However, it is not possible to infer the PL from the SIL.



1. Risk graph: which performance level is required? PL r from a to e.
2. How is the control chain or safety function structured? Category B to category 4.
3. Reliability of the components in the control chain: determining the $MTTF_D$ for the entire safety circuit, from the sensor and the safety relay unit to the power switching device.
4. Degree of diagnostic coverage: Which dangerous faults are detected?
5. Common cause failure (CCF): measures for avoiding CCF

Evaluation	$MTTF_d$
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ < 100 years

Source: ISO 13849-1 Chapter 4.5

Control architectures – Categories

Basic safety principles must be fulfilled
(ISO 13849-1 Pt. 6.2.3/ISO 13849-2 Tab. A 1/B.1/ C.1/ D.1)

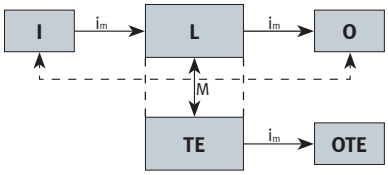
Suitable dimensioning for external influences
(ISO 13849-1 Pt. 6.2.3)

Well-tried safety principles must be fulfilled
(ISO 13849-2 6.2.4, 6.2.5, 6.2.6, 6.2.7; ISO 13849-2 Tab. A.2/B.2/ C.2/ D.2)

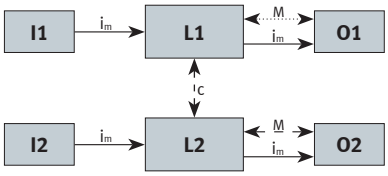
1 channel **0 fault safety** (ISO 13849-1 Pt. 6.2.3)	**1 channel** **Well-tried components** (ISO 13849-1 Pt. 6.2.4; ISO 13849-2 Tab. A.3/D.3) **0 fault safety** (ISO 13849-1 Pt. 6.2.4)		**1 channel** Requirement rate ≤1/100 of the test rate or test immediately on request of the safety function or requirement rate ≤1/25 of the rate if PFH_D * 1.1 is used (ISO 13849-1, 4.5.4, 6.2.5 and comment in Table K.1) **0 fault safety between the test phases**	**2 channels** (ISO 13849-1 Pt. 6.2.6) Some, but not all faults are detected before or during the next request of safety function **1 fault safety** An accumulation of undetected faults may result in the loss of the safety function	**2 channels** (ISO 13849-1 Pt. 6.2.7) Every fault must be detected before or during the next request of safety function **≥ 1 fault safety**
Category B	Compliance with basic and well-tried safety principles. Compliance with appropriate standards	Proven-in-use components. Already used in similar applications (refer to ISO 13849-2 B.4)			
	Category 1		**Category 2**	**Category 3**	**Category 4**

Category B or 1

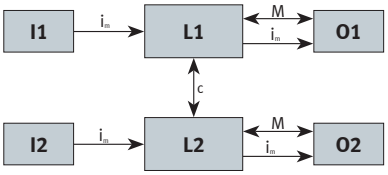
Category 2



Category 3

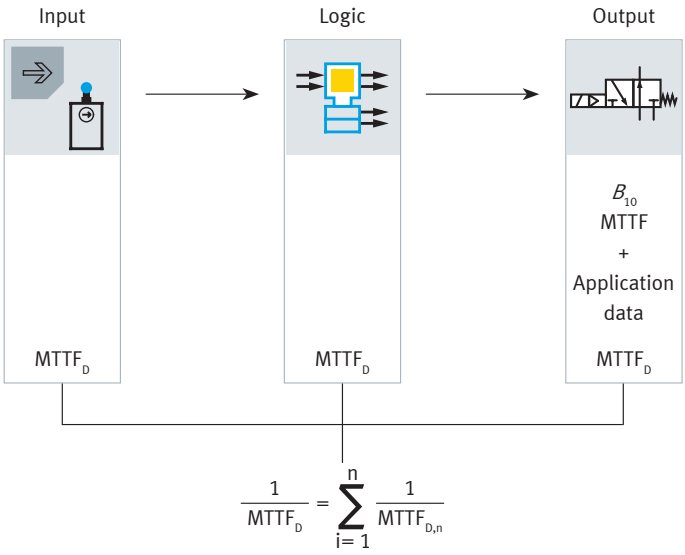


Category 4



Determining the $MTTF_D$ value for a channel

The mean time to dangerous failure, dangerous, $MTTF_D$ is the reliability characteristic value that must be determined for every channel of a safety function. Typical implementation of a safety function consists of a combination of input, logic, output and their connections. For each of these blocks, the component manufacturer should at least specify the reliability information (PFH, MTTF or B_{10}). If this information is not available, the characteristic values of good engineering practice can be found in ISO 13849-1, Table C.1.



Definitions for the characteristic values B_{10} and MTTF:

MTTF is an acronym for mean time to failure. The MTTF value is the expected value of the mean time to failure in accordance with ISO 13849-1, 3.1.25. The MTTF value is calculated on the basis of tables, e.g. in accordance with SN 29000, or calculated using e.g. the B_{10} values and their parameters of use.

The B_{10} value is the expected value until 10% of the components have failed.
The B_{10} value for pneumatic components is determined by endurance testing in accordance with the ISO 19973 series of standards.

Statistical procedures are used to determine both of these characteristic values in order to be able to estimate how long it will take for a large percentage of the evaluated products to fail. In practice, this value can be used to estimate the failure probability, the time until the first repair, the replacement intervals etc.

For safety-related parts of control systems, e.g. in accordance with ISO 13849-1, the reliability until the first dangerous failure has to be estimated. This estimate is based on $MTTF_D$ or B_{10D} values. The suffix "D" stands for dangerous. This means that these characteristic values indicate the mean expected value until a dangerous failure occurs. If the dangerous proportion of the B_{10} value cannot be explicitly specified – 50% of the B_{10} value can be assumed as dangerous in accordance with ISO 13849-1 C.4.2. The following therefore applies: $B_{10D} = 2 \times B_{10}$.

The $MTTF_D$ value is the expected value of mean time until a dangerous failure occurs with a probability of 63%
[as per ISO 13849-1, 3.1.25]

The B_{10D} value specifies the number of cycles until a dangerous failure occurs for 10% of the components (for pneumatic and electromechanical components) [as per ISO 13849-1, Table1]

From B_{10} and MTTF value to B_{10D} and $MTTF_D$ value

On the one hand, a detailed FMEA is necessary in order to determine $MTTF_D$ and B_{10D} values and, on other, those failures that might be dangerous for a given application have to be determined. Especially the second point can only be evaluated for an application with a specific safety function and if it is known how this function is implemented.

This is not possible for standard products because there is no indication as to which safety functions will be implemented. This is why ISO 13849-1 offers a simplified option for estimating $MTTF_D$ or the B_{10D} values based on the MTTF or B_{10} values:

In line with ISO 13849-1, Table C.1 comment 1 and C.4.2, the B_{10D} of pneumatic and electromechanical components can be estimated as two times B_{10}, i.e. it's assumed that 50% of all failures can be dangerous insofar as not otherwise specified.

The same can be assumed when estimating the $MTTF_D$ of electronic components in accordance with ISO 13849-1, section C.5.1, paragraph 3: " ... 50% of all dangerous failures, which means that the $MTTF_D$ for components is twice the specified MTTF value."

Depending on the application, greater factors are also possible in practice.

Determining the $MTTF_D$ from the B_{10D}
The $MTTF_D$ value is application-dependent and describes the mean period to a dangerous failure of a system part.

Where:

Formula for determining the $MTTF_D$ value for a mechanical or pneumatic component in a channel

$$MTTF_D = \frac{B_{10D}}{0.1 \bullet n_{op}}$$

B_{10D} [cycles] = mean number of cycles, up to 10% of the components fail dangerously
$B_{10D} = 2 \times B_{10}$ (ISO 13849-1)

Mean number of annual actuations n_{op} for the mechanical or pneumatic component

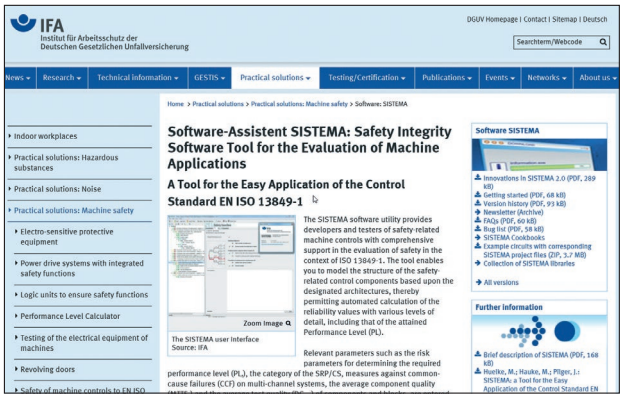
$$n_{op} = \frac{d_{op} \bullet h_{op} \bullet 3600s/h}{t_{cycle}}$$

h_{op} [h/d]: operating hours/day
d_{op} [d/anno]: operating hours/ year
t_{cycle} [s]: cycle time

Further reading
- ISO 13849-1 – Safety-related parts of control systems – Part 1: General principles for design
- ISO 13849-2 – Safety-related control parts of the systems – Part 2: Validation
- IEC 60050-191 – Dependability and quality of service
- ANSI B 11.0 General Requirements and Risk Assessment (USA)
- ANSI B 11.26 General Principles for the Design of Safety Control Systems Using ISO 13849-1 (USA)
- We determine our reliability characteristic values in accordance with international standards. Further information can be found in the
  → Brochure Product Service Life at Festo

→ Brochures can be found on the Festo homepage in the Support/Downloads area

Calculating and providing libraries



SISTEMA software from the Institute for Occupational Health and Safety [Institut für Arbeitsschutz (IFA)]

The SISTEMA software (Safety Integrity Software Tool for the Evaluation of Machine Applications) is a tool that can be used for part of the validation of safety circuits. With SISTEMA, you can evaluate whether certain safety circuits can achieve the required performance level (PL). This Windows tool maps the structure of the safety circuits on the basis of the designated architectures and calculates reliability values at various levels of detail, including the performance level (PL) reached.

The software is available as a free download via the following link:
→ https://www.dguv.de/webcode.jsp?query=e34183

Libraries with characteristic values

To simplify the use of SISTEMA, libraries from the component manufacturers can be used. These libraries contain the characteristic values needed for an evaluation so that these simply have to be entered in a SISTEMA project. We therefore offer libraries in accordance with VDMA 66413 in XML format.

These libraries can be found on our homepage at
→ https://www.festo.com/cms/en-gb_gb/15822.htm

Data sheet product reliability

As part of the validation, a check must be carried out to determine whether the required performance level (PL) can be achieved with the components used in the implemented safety circuits. This must be done with the current data from the component manufacturer. Festo has created data sheets for product reliability for this purpose, which will be provided online via the digital customer information system.

How to access the data sheets for product reliability from the Festo homepage:
1. Select the required product in the online product catalogue
2. Click on “data sheet” on the right-hand side
3. In the data sheet, click on “Data sheet product reliability” in the top right

The required and up-to-date characteristic values for evaluating and validating safety circuits are made available in the compact data sheet product reliability. These values include characteristic reliability values such B_{10} or MTTF and evaluation of a tried-and-tested component in accordance with ISO 13849. Additional information on the product and the use of that information is documented in footnotes, which make interpretation easier.

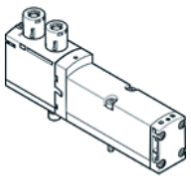
The option to obtain information allows you to directly access the central data for your product.

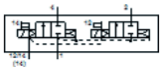
Note: The data sheet product reliability is only available online in the digital customer information system.

Example of a data sheet product reliability: ➔ VSVA-B-T22C-AZTR-A1-1T1L

solenoid valve
VSVA-B-T22C-AZTR-A1-1T1L
Part number: 8033032

FESTO





General operating conditions
Datasheet product reliability
➔ Support Portal

Datasheet product reliability

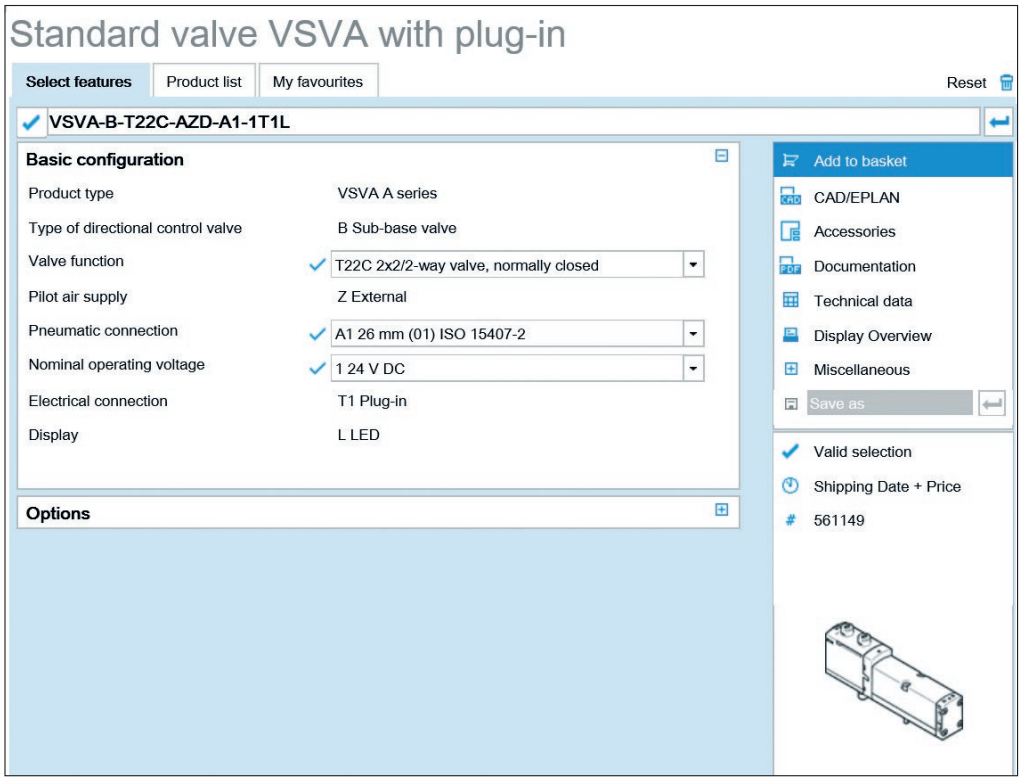
The information in this "Product reliability data sheet" is based on products being used as intended. This includes complying with all specifications in data sheets, catalogues, user documentation and the general operating conditions. The user alone is responsible for determining whether a product is suitable for a particular application.

Feature	Value
Relevant basic safety principles[1)]	Yes
Relevant well-tried safety principles[2)]	Yes
Well-tried component[3)]	Yes
Service-life value B_{10}[4)]	110 MioCyc
Vibration resistance	Transport application test with severity level 2 in accordance with FN942017-4 and EN 60068-2-6
Shock resistance	Shock test with severity level 2 in accordance with FN 942017-5 and EN 60068-2-27
Max. positive test pulse with 0 signal	1.500 µs
Max. negative test pulse with 1 signal	1.200 µs

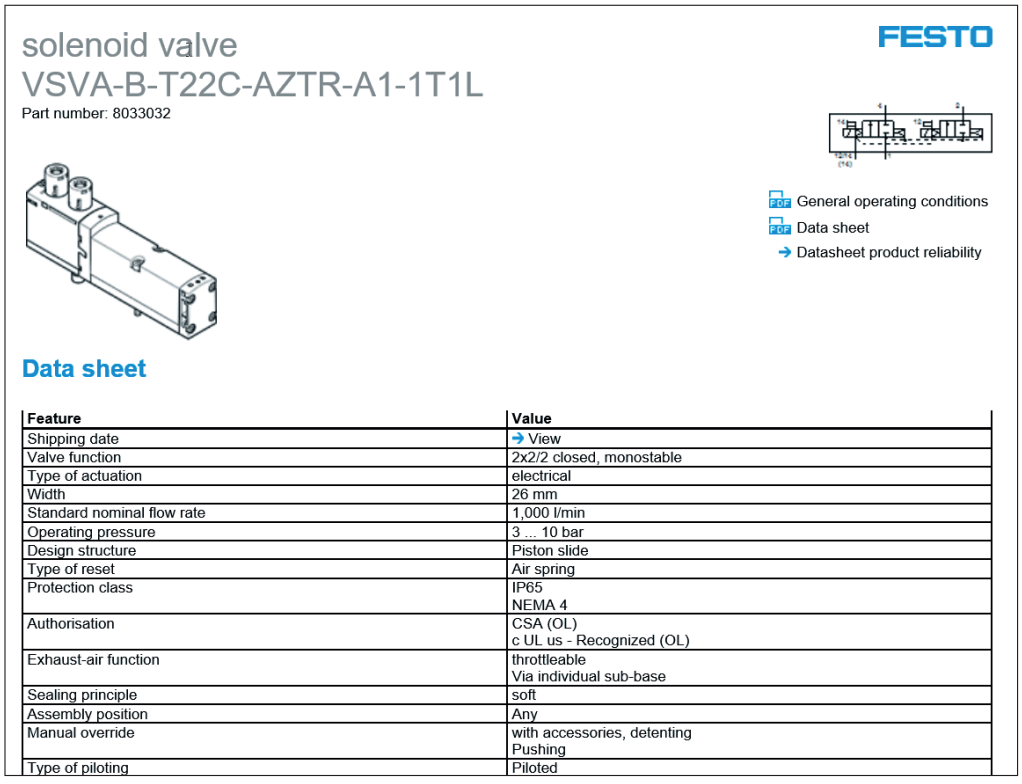
[1)] The product-relevant basic safety principles are fulfilled according to the ISO 13849-2.
[2)] The product-relevant well-tried safety principles are fulfilled according to the ISO 13849-2.
[3)] The product is a well-tried product for a safety-related application according to ISO 13849-1. The relevant basic and well-

➔ Data sheet product reliability

Where to find the data sheet product reliability



→ Electronic catalogue



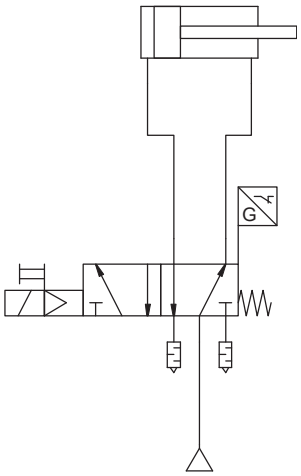
Feature	Value
Shipping date	→ View
Valve function	2x2/2 closed, monostable
Type of actuation	electrical
Width	26 mm
Standard nominal flow rate	1,000 l/min
Operating pressure	3 ... 10 bar
Design structure	Piston slide
Type of reset	Air spring
Protection class	IP65 NEMA 4
Authorisation	CSA (OL) c UL us - Recognized (OL)
Exhaust-air function	throttleable Via individual sub-base
Sealing principle	soft
Assembly position	Any
Manual override	with accessories, detenting Pushing
Type of piloting	Piloted

→ Datasheet

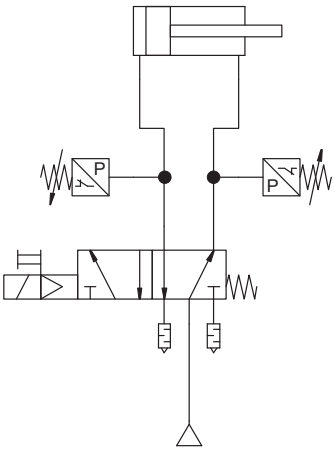
Diagnostic coverage in pneumatics – DC

The diagnostics of a safety sub-function must be able to monitor the safe state of the power switching component. If the safe state of the power switching element is exited, the signal changes from logic 1 to logic 0. If the safe state is resumed, the signal changes from logic 0 to logic 1.

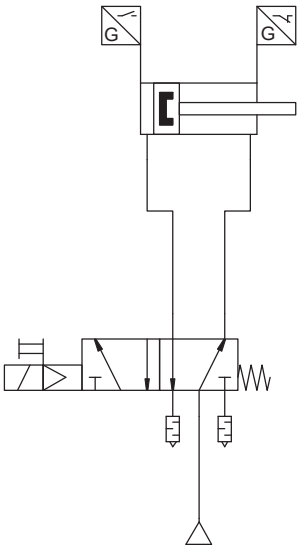
For power switching components with a specific normal position, e.g. via spring, the safe state is always the normal position. The safety sub-function is then executed in the normal position. For components with no specific normal position, e.g. double solenoid valves, the possible safe state is the maintaining of the current switching position.



Direct monitoring of the directional control valve



Indirect monitoring of the directional control valve



Indirect monitoring of the directional control valve (if the limit switches are evaluated directly by the safety relay unit)
Fault detection by the process (if the limit switches are evaluated using a control system)

Note: Only the most important options for diagnostics are shown here. Other sensors may also be suitable, e.g. flow sensors, displacement sensors, filling level sensors, etc.

How test pulses affect solenoid valves

The electronic outputs of the safety controller and safety relay units use test pulses for diagnostic purposes. Test pulses help to detect cross circuits or check the function of the outputs relative to their switch-off capability. Depending on the manufacturer, these test pulses have varying pulse widths of up to several milliseconds. For example, a controller manufacturer deactivates their outputs for a period of several milliseconds in the event of an ON signal. In the event of an OFF signal, the outputs are switched on for up to 4 ms to check whether they can be deactivated safely if a safety function is requested.

How does a solenoid valve react to these test pulses?
If a solenoid valve is connected to a failsafe output, the test pulses can cause the LED on the solenoid valve to flicker at the same speed as the pulses and a clicking can be heard in the solenoid valve. That clearly shows that these test pulses have an effect on the solenoid valve. Many modern solenoid valves consist of a magnetic system that uses an armature to actuate a pilot valve. This in turn actuates the working valve, which then actuates the drive. Even if the switching times for activation or deactivation, which are listed in the technical data, are far higher than the duration of the test pulses, the armature reacts much earlier. In some solenoid valves, this even happens with negative test pulses (blackout times) of just 0.1 ms.

Does this result in accidental deactivation of a solenoid valve in the event of an ON signal and a negative test pulse?
The reaction in the magnetic system generally indicates a reduction of the holding force for the armature. In turn, this means that unfavourable vibration-shock conditions could result in an unplanned activation of the pilot valve, and thus of the working valve.

Does this result in accidental activation of a solenoid valve in the event of an OFF signal and a positive test pulse?
Although these positive test pulses of several milliseconds cause the LED on the solenoid valve to flicker at the same speed as the test pulses, it is extremely rare for it to cause the solenoid valve to switch. In some solenoid valves, the armature begins to move after just 0.4 ms. When the machine is exposed to unfavourable vibration-shock conditions, this reaction could result in an unplanned activation of the pilot valve, and thus of the working valve. In turn, this means that unfavourable vibration-shock conditions at the machine could result in an unplanned activation of the pilot valve, and thus of the working valve.

Summary
At Festo, limit values are determined under “worst case” conditions, i.e. when pressure or voltage is reduced and the valve is deactivated. As the pressure and output voltage values approach the upper limits, the sensitivity of the solenoid valves decreases. The behaviour is reversed in the event of activation. In practice, the maximum positive and maximum negative test pulses must be determined. This information can be found in the data sheet product reliability. These limit values must be compared with the relevant test pulses of the safe outputs used for actuation. The minimal movements caused by the test pulses could result in the deterioration of the magnetic system. This, in turn, can adversely affect the service life of the solenoid valve.

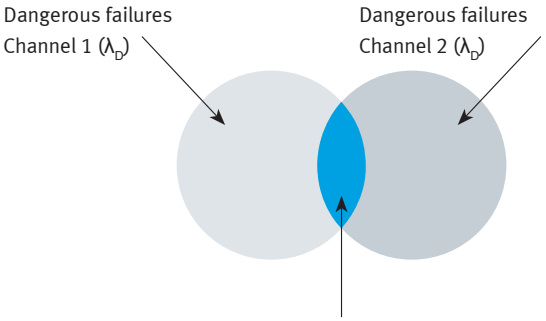
What are the alternatives for safe operation of solenoid valves?
You should always make sure that the requirements of the performance level to be achieved (with DC, $MTTF_D$, ...) are met.
Likewise, the data specified in the data sheet and in the operating instructions must be complied with.

- Use the safe output module CPX-FVDA-P2 from Festo or the safe interfaces VABA-S6-1-X2-Fx-CB on the VTSA-F-CB and you can be certain that valves from Festo will not be negatively affected
- If possible, switch off the test pulses
- Actuate the solenoid valve via a non-pulsed output of a standard PLC. For example, connect a normally open contact of a safety shutdown relay between the solenoid valve and the output, which guarantees the safety function when needed

Where can I find the maximum permissible pulse length of a solenoid valve?
During the design phase of a safety-related part of a control system, always contact the manufacturer of the solenoid valve, and ask for the maximum pulse widths of the test pulses. At Festo, you can find the information on the max. positive and negative test pulses in the data sheet product reliability.

Common cause failure – CCF

With safety circuits from category 2 onwards, common cause failures must always be analysed. This is necessary as certain causes of fault scan lead to failure of both channels, thereby disabling the safety function. The required single fault protection can thus no longer be guaranteed.
The selected approach of ISO 13849-1 uses the beta factor model of the IEC 61508-6 and has simplified it for use in machinery and system building.
This beta factor model enables the proportion of dangerous failures in a channel to be estimated following the cause of the error, when dangerous failures also appear in the second channel.



β factor:
Proportion of dangerous failures
with a common cause of a channel

The selected approach of ISO 13849-1 uses a point system with a list of measures sorted by the various causes. This list of measures is based on the experience of specialists and only covers the most important points. When using the list, it must be taken into account that in certain conditions of use some measures may be missing for certain machines.
How does Festo with the easy implementation of the measures to protect against common cause failures?

No.	Measure to prevent CCF	Solutions and comments from Festo
1	**Separation / Segregation** Physical separation of signal paths	
	• Separation the wiring	Valve cables with M8 plugs are sheathed cables. This means that twice the insulation is used, resulting in adequately isolated wiring.
	• Detection of short circuits and open circuits in cables by dynamic tests	In pneumatics, short circuits are not possible in pneumatic tubing that are not interconnected, which means they can be excluded.
		The safe output modules CPX-FVDA-P2 use an innovative solution to detect short circuits that does not require test pulses. ➔ Page 92
2	**Diversity**	
	• Different technologies	With a safe holding function, one channel has a holding brake or clamping unit and the other channel has piloted check valves.
		For vacuum generators on vacuum spiders, when one suction cup fails, a vacuum efficiency valve ISV-... can help to prevent the failure of the other suction cups.
	• Different valve designs	Depending on the safety sub-function selected, a channel can be realised using one valve on a valve terminal. The second channel is realised by an electric on/off valve of the service unit.
		Different valve technologies are used. Piston slides and poppet valves, soft-sealing and hard-sealing valves
	• Components with different loads	One valve is switched without operating pressure or flow rate and a second valve switches the operating pressure or the flow rate.
		One valve is switched at every machine cycle, the other valve only on request of the safety function.
	• Various switching frequencies	One (working) valve is switched at every machine cycle, the other valve only on request of the safety function.

3	**Design/application/experience**	
3.1	Protection against overvoltage, over-pressure, over-current, over-temperature, etc.	Over-pressure can be easily controlled with a pressure regulator that is set to a value below the maximum permitted operating pressure for pneumatic components in a machine. ➔ Page 68 Over-current in the servo motors is effectively limited to a I^2t limit in the motor controllers. ➔ Page 100
3.2	Use of well-tried components	Almost all valves from Festo are tested and classified according to ISO 13849-1. This and other information can be found in the data sheet product reliability. ➔ Page 36
4	**Assessment/analysis**	
	For each component of safety-related parts of a control system, a failure mode and effects analysis was carried out and their results taken into account in order to prevent common cause faults in the design.	To analyse the types of failures, the list of faults and fault exclusions from ISO 13849-2 Appendix A to D can be used.
5	**Competency/training**	
	Training of designers to understand the causes and consequences of common cause failures.	Festo Didactic offers training for the implementation of ISO 13849 in your machines ➔ Page 115
6	**Environment**	
6.1	Electric/electronic systems, preventing contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with the relevant standards (e.g. IEC 61326-3-1).	Products with electronic modules comply with the EMC Directive and the user information contains all the required measures to protect against EMC malfunctions.
	Pneumatic systems: filtering the pressure medium, preventing contamination, drainage of compressed air.	In service units, filters are easy to integrate. Important: a compressed air quality of [7:4:4] is sufficient for most pneumatic products from Festo. ➔ page 90
6.2	Other factors: Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity as specified in the relevant standards.	The possible use of our products for safety-related applications is described in the relevant product data sheet. This specifies the permissible conditions of use including for temperature, shock, vibration, etc. so that you can easily assess these influences. Any violation of the limits described in the data sheet must be excluded during usage. Important: our testing processes are carried out in accordance with international standards so that our values can be compared. Other possible influences can include: • Water and bacteria around polyurethane tubing • Solvents in printing ink • Burn-off when labelling using a laser • Pressure drops in valves or voltage drops in electronic modules • Stress on cylinders by deflection

Definition of a Safety Device

What is a safety device according to Article 2 c) 2006/42/EG ?

- It guarantees a safety function
- It is placed on the market separately
- Its failure and/or malfunction would endanger the safety of people
- Is not required for correct functioning of the machine or system or can be replaced by standard components for the correct functioning of the machine

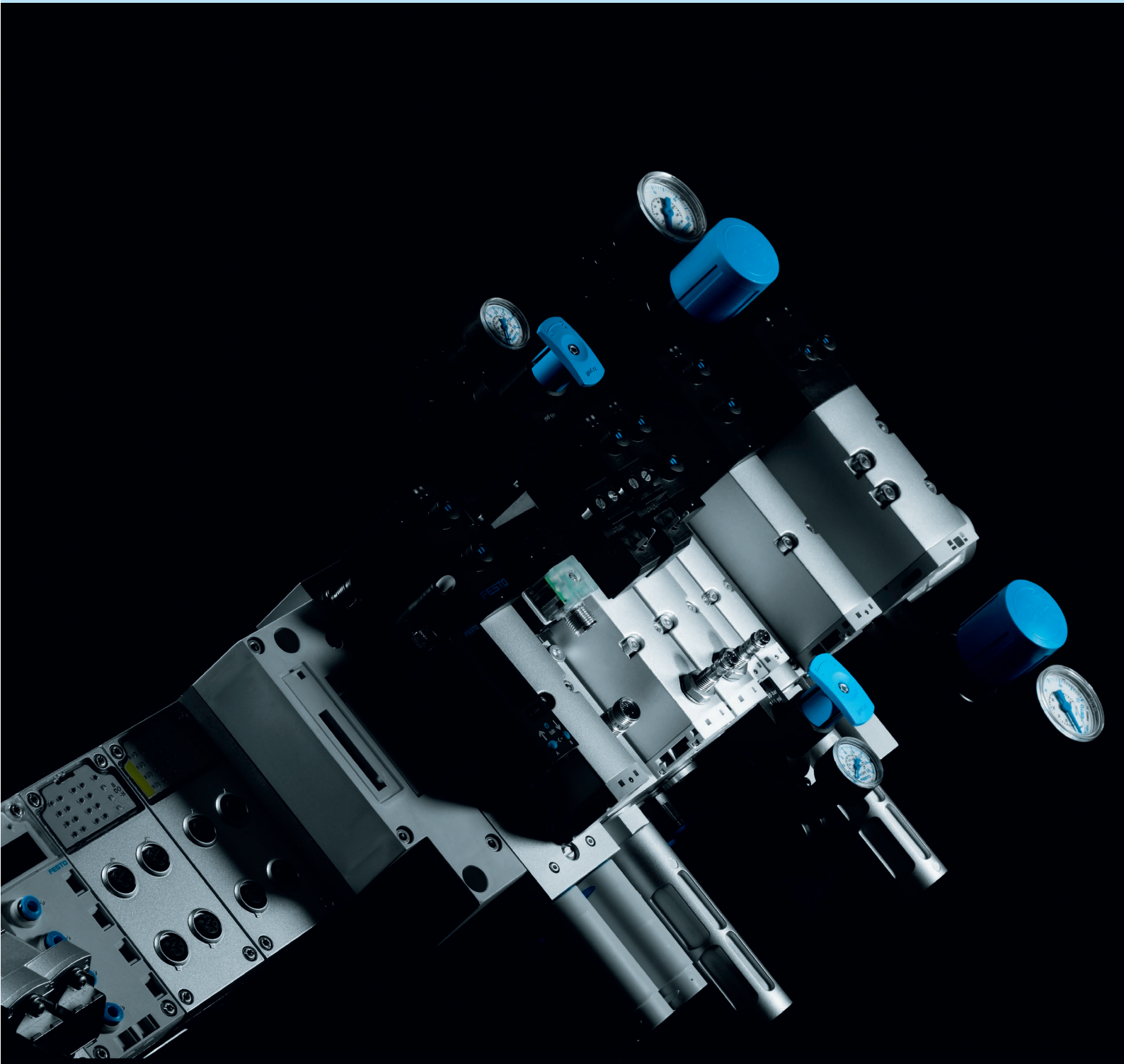
The EC Machinery Directive 2006 / 42 / EC defines whether a component is a safety device or not. It depends on how it is placed on the market. The term safety device generally does not indicate the safety level or reliability of a device. The EC Machinery Directive does not prescribe the use of safety devices. It only describes the conformity assessment procedure for components that correspond to the definition for safety devices. Manufacturers of safety devices must comply with the conformity assessment procedures in order to market the safety devices in the EEA. The user can use either safety devices or standard components that are suitable for use in safety-related applications.

What is the difference between a safety device and a safety-related part of a controller (SRP/CS)?

- A safety device is evaluated by its manufacturer for its safety function. The manufacturer also provides characteristic values for a safety device: performance level (PL), safety integrity level (SIL), average probability of a dangerous failure per hour (PFH_D), category (cat.), diagnostic coverage (DC), common cause failures (CCF), etc.
- The manufacturer provides characteristic values for a standard component that is suitable for safety-related applications: B_{10} values, tried-and-tested component, compliance with basic and proven safety principles, fault exclusions if required

Examples of safety devices

- Light curtain
- Safety door switch
- Emergency stop command device
- Safety relay
- Soft start/quick exhaust valve MSx-SV-...
- Control block VOFA-...
- Control block for two-hand start ZSB-...
- Input module CPX-F8DE-N
- Output module CPX-FVDA-P2
- Safety module CAMC-G-...
- And many more



02 Your route to a safe system – process industry

Your route to a safe system

Your objective is to reduce the hazards created by these systems for people, the environment and property to the lowest practical level. Our solutions for the process industry can make a significant contribution here.

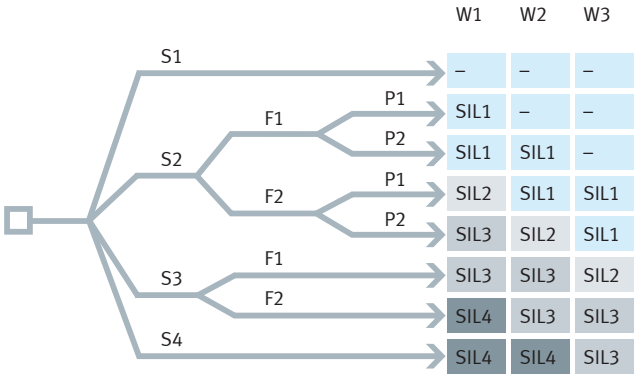
Contents

SIL – Safety integrity level

Safety devices in process industry systems are required to reduce the hazards created by these systems for people, the environment and property down to the lowest practicable level.
Depending on the potential hazards, a safety integrity level (SIL1 to SIL4) is assigned to a particular system.
SIL1 represents the lowest risk and SIL4 the highest acceptable risk with catastrophic consequences.

As a general principle, the more hazardous the system, the more reliably its safety devices must operate in case of an emergency. Once a SIL level has been assigned to a system, specific installation principles must be observed, e.g. redundant design. This enables the risk to be reduced to the greatest possible extent in the event of a malfunction.

SIL (Safety Integrity Level)



Four discrete levels (SIL1 to SIL4). The higher the SIL of a safety-related system, the lower the probability of the system not being able to execute the necessary safety functions.

S Severity of the harm
- S1 Slight injury to a person
- S2 Serious injury to several persons or death of a person
- S3 Deaths of several persons
- S4 Catastrophic consequences with multiple deaths

F Frequency and exposure time
- F1 Seldom to relatively frequent
- F2 Frequent to continuous

P Avoiding/reduction of harm
- P1 Possible under certain conditions
- P2 Hardly possible

W Probability of occurrence
- W1 Relatively high
- W2 Low
- W3 Very low

SIL in concrete terms

The standards:
The basic standard for functional safety is IEC 61508, entitled “Functional Safety of electrical/electronic/programmable electronic safety-related systems”. IEC 61511, entitled “Functional safety – safety instrumented systems for the process industry sector” applies to process automation.

SIL certified according IEC 61508

IEC 61508 describes the method for assessing risks using a risk graph and the measures required to design suitable safety functions, ranging from sensors and logic circuits to actuators.
A safety circuit, or SIS – safety integrated system – normally consists of the following components:

- Sensors, e.g. Pressure, temperature, filling level gauge
- Evaluation and output unit, e.g. safety PLC
- Automated process valve comprising solenoid valve, actuator and process valve

IEC 61511 describes the specific implementation of IEC 61508 for the process industry. The focus here is on applications with a low demand mode. In process plants, this represents most safety functions.

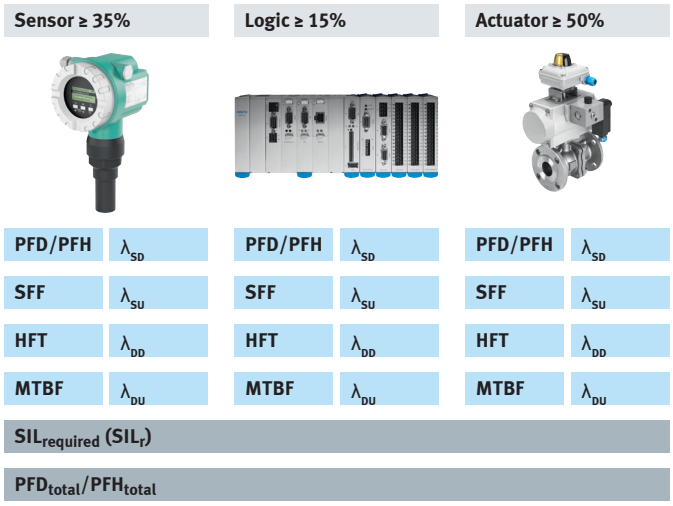
Important to know
The requirement for the probability of failure to IEC 61508 always refers to a complete protective device and not to individual components. A component, in and of itself, can therefore not have a SIL level, only a complete safety instrumented system (SIS) can.

Relevant characteristic values for calculating SIL

- **PFD (probability of failure on demand):**
  Probability that a safety function will fail in low demand mode (demand rate/year ≤ 1) Low Demand
- **PFH (probability of failure per hour):**
  Probability that a safety function will fail during continuous use (demand rate/year › 1) High Demand
- **SFF (safe failure fraction):**
  Proportion of safe failures out of the total number of failures
- **HFT (hardware failure tolerance):**
  The ability to continue to execute the required function in the event of faults and deviations
  HFT0: A single failure could lead to the loss of the safety function, e.g. 1oo1 circuits
  HFT1: At least two failures must occur simultaneously to cause a loss of safety, e.g. 1oo2 circuits
  HFT2: At least three failures must occur simultaneously to cause a loss of safety, e.g. 1oo3 circuits
- **λ (Failure rates):**
  λ_S: Total failure rate for safe failures
  λ_{SD}: Failure rate for safe, identifiable failures
  λ_{SU}: Failure rate for safe, unidentifiable failures
  λ_D: Total failure rate for dangerous failures
  λ_{DD}: Failure rate for dangerous, identifiable failures
  λ_{DU}: Failure rate for dangerous, unidentifiable failures
- **MTBF (mean time between failures):**
  Mean time between two successive failures
- **Device type A:**
  Device for which the failure behaviour of all components and the failure characteristics are adequately determined, e.g. through operational reliability.
- **Device type B:**
  Device for which the failure behaviour of at least one component and the behaviour in the event of a failure are not adequately determined.

SIL in concrete terms

Typical distribution of the PFD/PFH between the sub-systems of a safety function in single-channel systems



What does SIL mean for operators?

A company that erects and operates a system which represents a potential hazard for employees, local residents or the environment must minimise the risk presented by the process under fault conditions.

To achieve this, both IEC 61508 and IEC 61511 essentially require the following steps to be carried out:

1. Risk definition and assessment
according to detailed failure probabilities for everything from sensors to controllers and actuators for the entire service life of the components.

2. Definition and implementation of measures
to minimise residual risk.

3. Use of suitable devices
(evaluated or certified)

4. Recurring test
to ensure compliance with safety functions.

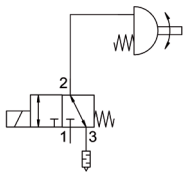
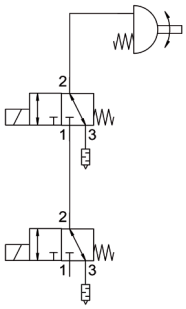
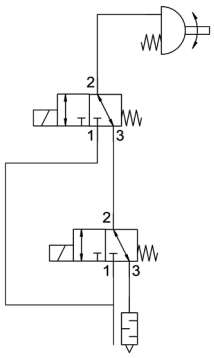
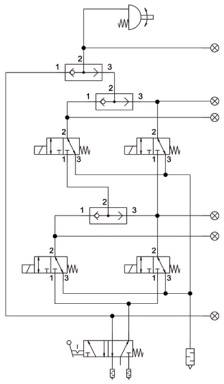
Target: SIL ≥ SIL_r

SIL level	High demand mode [1/h]	Max. acceptable failure of the safety system	Device type A, Safe failure fraction (SFF) ‹ 60%	Device type A, SFF 60…90%	Device type A, SFF 90…99%	Device type A, SFF › 99%	Device type B, SFF ‹ 60%	Device type B, SFF 60…90%	Device type B, SFF 90…99%	Device type B, SFF › 99%	Low demand mode	Max. acceptable failure of the safety system
	$10^{-5} \le PFH < 10^{-4}$	One risk of failure every 10,000 hours										
1	$3x10^{-6} \le PFH < 10^{-5}$	One risk of failure every 1,250 days	HFT 0				HFT 1	HFT 0			$10^{-2} \le PFD < 10^{-1}$	Once every 10 years
	$10^{-6} \le PFH < 3x10^{-6}$	One risk of failure every 115.74 years										
2	$10^{-7} \le PFH < 10^{-6}$	One risk of failure every 115.74 years	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \le PFD < 10^{-2}$	Once every 100 years
3	$10^{-8} \le PFH < 10^{-7}$	One risk of failure every 1,157.41 years	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \le PFD < 10^{-3}$	Once every 1,000 years
4	$10^{-9} \le PFH < 10^{-8}$	One risk of failure every 11,574.1 years		HFT 2	HFT 1	HFT 1			HFT 2	HFT 1	$10^{-5} \le PFD < 10^{-4}$	Once every 10,000 years
					HFT 2	HFT 2				HFT 2		

Redundant system conditions for safety-related applications

Process safety and reliability are always at the forefront when using redundant systems. Current safety circuits in process engineering are 1oo2 (One out of Two), 2oo2 (Two out of Two) and 2oo3 (Two out of Three). These are used in the production and processing of high-value and hazardous substances such as crude oil, natural gas, chemicals etc.

The functions in the circuit diagram

1oo1 (One out of One)	1oo2 (One out of Two)	2oo2 (Two out of Two)	2oo3 (Two out of Three)
			
A single failure can lead to a loss of safety.	**Safety** If a fault is detected in a valve, the entire system is exhausted. This leads to a loss of safety and the system moves to a safe position.	**Increased uptime** Only when both valves fail is the correct function no longer ensured and this leads to a loss of safety.	**Safety and reliability** At least three failures must occur simultaneously to cause a loss of safety.

To provide redundancy in the event that a valve fails, the above-mentioned systems are installed in safety- or process-critical systems.
Their compact design reduces the cost of the piping and simultaneously the potential for leaks in a system.
This saves costs when mounting and operating the system.

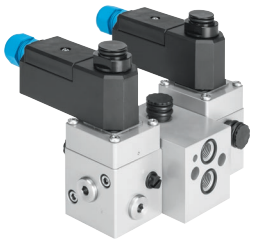
Redundant system conditions for safety-related applications

Most widely used redundant systems at field level

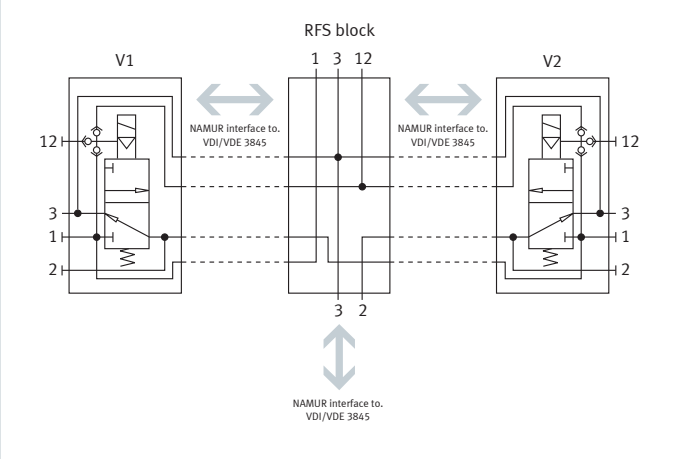
Safety (1oo2)
With enhanced safety (1oo2), two valves are connected in series. Both valves are energised during operation. Should a valve or a solenoid fail during operation, the entire system is exhausted in order to protect it from subsequent damage. Media conveyor lines frequently require this higher level of safety.

Increased uptime (2oo2)
With increased uptime (2oo2), two valves are connected in parallel. Both valves are energised during operation. Should a valve or a solenoid fail during operation, the system remains active and the entire system continues to work. For example, cooling circuits require this increased uptime.

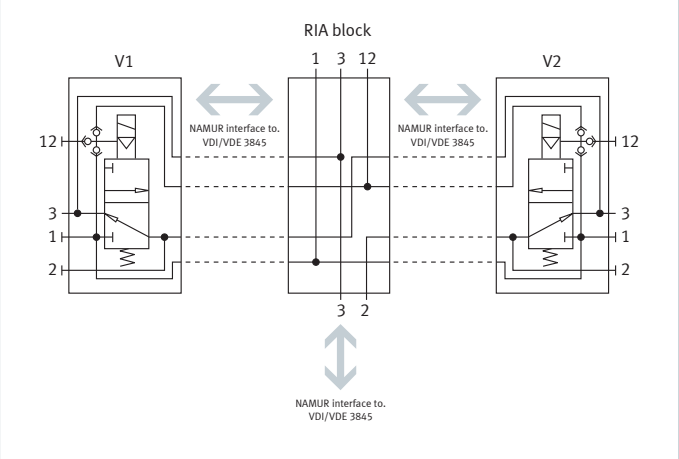
Redundant NAMUR block (1oo2 & 2oo2)



- The NAMUR block enables the installation of two solenoid valves VOFC or VOFD. The NAMUR interfaces make redundancy easy to implement. The advantages: low warehousing costs and easy replacement of solenoid valves.
- Both solenoid valves are redundantly interconnected and provide a redundant function for automated process valves. The blocks are available in fail-safe function (1oo2) or with increased uptime (2oo2)
- The NAMUR block can be mounted directly on quarter turn actuators using the standardised interface. Separate installation with suitable piping is also possible.
- With 1oo2 and using the additional auxiliary power terminal, the NAMUR block can also be used with piloted solenoid valves on actuators that have a positioner for fail-safe functions.
- High flexibility due to the available types of ignition protection and global certification of the solenoid coils.
- Available with G and NPT connections.



Redundant fail safe – 1oo2



Redundant increased uptime – 2oo2

	Redundancy block			Suitable basic valve		
Solution	**Type**	**Pneumatic connection**	**Part no.**	**Type**	**Pneumatic connection**	**Part no.**
1oo2*	VABS-S7-RB-B-G14-V14-A	G1/4, NAMUR	3580505	VOFC-LT-M32C-M-FG14-F19	G1/4, NAMUR	4514738
				VOFC-LT-M32C-M-FG14-F19A (intrinsically safe)	G1/4, NAMUR	4514739
	VABS-S7-RB-B-N14-V14-A	1/4NPT, NAMUR	4727331	VOFC-L-M32C-M-FN14-F19	1/4NPT, NAMUR	3344863
				VOFC-L-M32C-M-FN14-F19A (intrinsically safe)	1/4NPT, NAMUR	3344863
2oo2*	VABS-S7-RB-B-G14-V14-A-2oo2-CS	G1/4, NAMUR extended	–	VOFC-LT-M32C-M-FG14-F19	G1/4, NAMUR	4514738
				VOFC-LT-M32C-M-FG14-F19A (intrinsically safe)	G1/4, NAMUR	4514739

* Other (connection) variants / combinations on request.

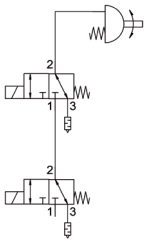
Suitable solenoids VACC-...
→ See catalogue (VOFC)

Redundant INLINE valves (1oo2 & 2oo2)

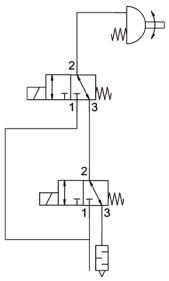
With these compact systems, Festo is drawing on the tried-and-tested technology (proof-in-use) of the valves VOFD and is combining this in one housing. Thanks to the Ematal coating, these valves meet the highest safety standards in process engineering and can withstand the toughest of ambient conditions. Available types of ignition protection:
Ex me, Ex d.

- Simple replacement of individual valve installations.
- The valve's redundant circuit ensures a redundant fail-safe function (1oo2) or provides increased uptime (2oo2) for automated process valves.
- High flexibility due to the available types of ignition protection and global certification of the solenoid coils.
- Compact and robust housing for installations in harsh ambient conditions.
- Available with G and NPT connections.

1oo2 (One out of Two)



2oo2 (Two out of Two)

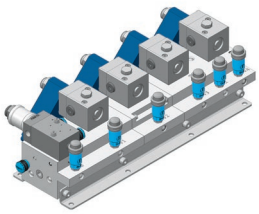


Redundant in-line valves			
Solution	**Type**	**Pneumatic connection**	**Part no.**
1oo2*	VOFD-L50T-M32-MN-N14N12-F10-RC-A1oo2-CS	1/4NPT	11917129
2oo2*	VOFD-L50T-M32-MN-N14N12-F10-RC-A2oo2-CS	1/4NPT	11917129

* Other (connection) variants / combinations on request.

Suitable solenoids VACC-...
→ See catalogue (VOFD)

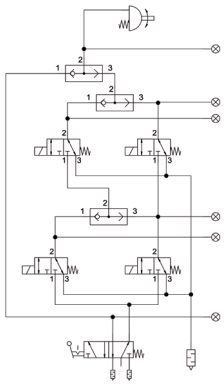
Safety and reliability inline/ Namur (2oo3)



There is a combination that provides maximum safety and availability at the same time. This so-called 2oo3 system combines both technologies and meets the highest demands of a system. The block is an inline variant and is integrated in your system. The built-in standard valves are mounted on the block via the NAMUR interface. This opens up the opportunity for diversity in the design. It also means that individual valves can be easily replaced. In addition, with the 2oo3 system the functions of the four valves can be bypassed. This bypass can be unlocked with a key so that maintenance can be carried out during operation.

The mechanical pressure indicators or pressure gauges, mounted directly on the valve block, always give a reliable and swift indication if a valve is pressurised. In addition, the mechanical displays can be replaced with electronic pressure sensors in order to reflect the status in the control system.

2oo3 (Two out of Three)



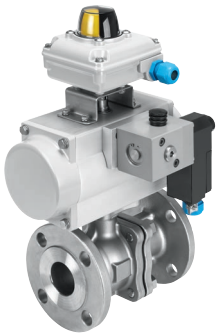
Inline redundancy block with NAMUR valves			
Solution	**Type**	**Pneumatic connection**	**Part no.**
2oo3*	VOFC-L-M32/52-CS	G1/4	11917129

* Other (connection) variants / combinations on request.

Suitable solenoids VACC-...
→ See catalogue (VOFC)

Solutions for safety-related applications

1. Actuator units from Festo – ready to install



Complete actuator units, whether single- or double-acting, save you time and money. We will build your ready-to-install and tested actuator unit in accordance with your requirements – including for safety-related systems. To do this, we use automated process valves based on certified components with a corresponding SIL manufacturer's declaration.

- Fully assembled to your specifications
- Costs and time saving
- Ready to install
- SIL or ATEX assessment of the actuator units with the corresponding manufacturer's declaration possible
- Designs for low temperatures

2. Panel and control cabinet solutions for safety-related applications

Piped pneumatic control systems
Festo offers a broad spectrum of pneumatic control systems. Our offer encompasses all stages of the value chain, from initial planning and engineering up to assembly, testing and delivery of the ready-to-install panel.

Control cabinets for the process industry
Control cabinet solutions tailored to your specifications and requirements protect the components used against environmental factors, fluids and foreign matter. You decide whether tubing or piped connections are more suitable for your purpose.

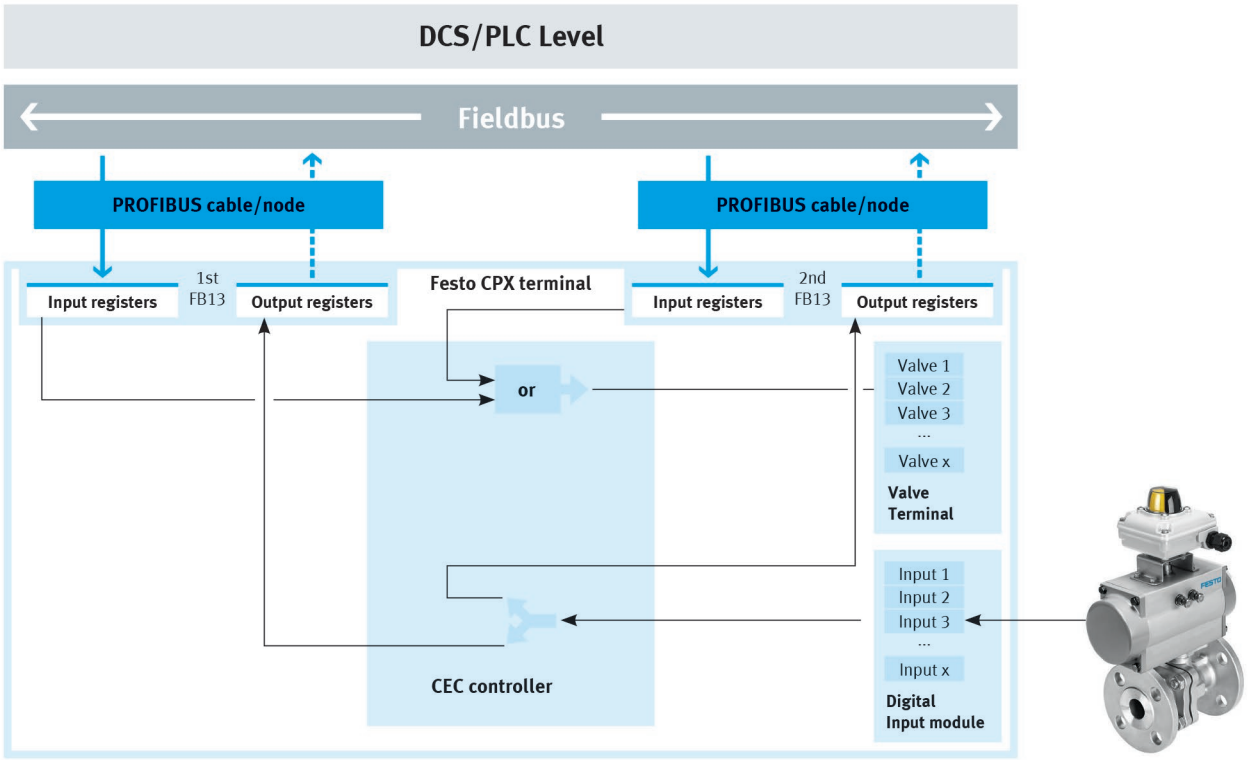
Regardless of whether you are using pneumatic, electric or electro-pneumatic components:
you will receive a control cabinet that is completely in line with your requirements.
On request, we can subject the entire cabinet to a SIL assessment.
For explosion protection, we also manufacture control cabinets in a 2GD or 3GD design with international approvals and in accordance with the U.S. NEC standard.

3. Current solutions for batch processes

3.1 PROFIBUS redundancy

Festo uses a redundant PROFIBUS solution to increase the safety between the control system (DCS) and remote I/O. If a PROFIBUS cable is removed or the PROFIBUS node is faulty, the second PROFIBUS cable/node takes over. This reliably sends and receives the control system protocols.

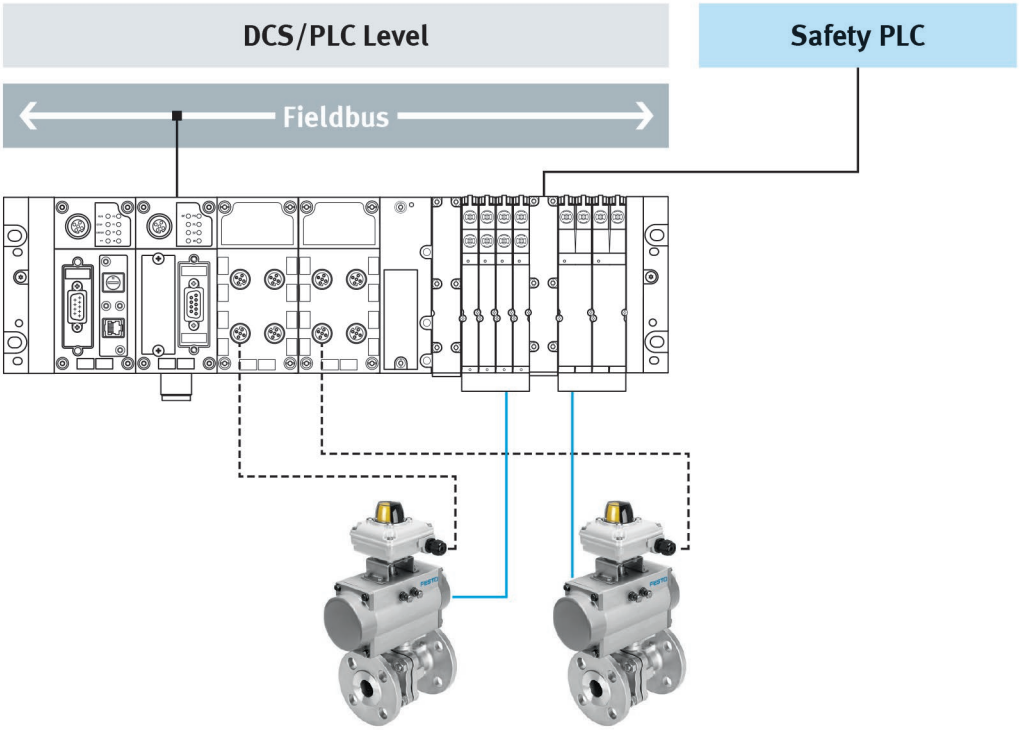
Additional benefit:
you can access the remote I/O directly on site via a controller with Ethernet interface and parameterise or implement additional processes. The tried-and-tested technology of the CPX-P, with its input modules for connecting NAMUR sensors, reliably takes over the tasks of the control level. The modular terminal CPX together with the SIL2-rated valve terminal MPA is a compact alternative.



Solutions for safety-related applications

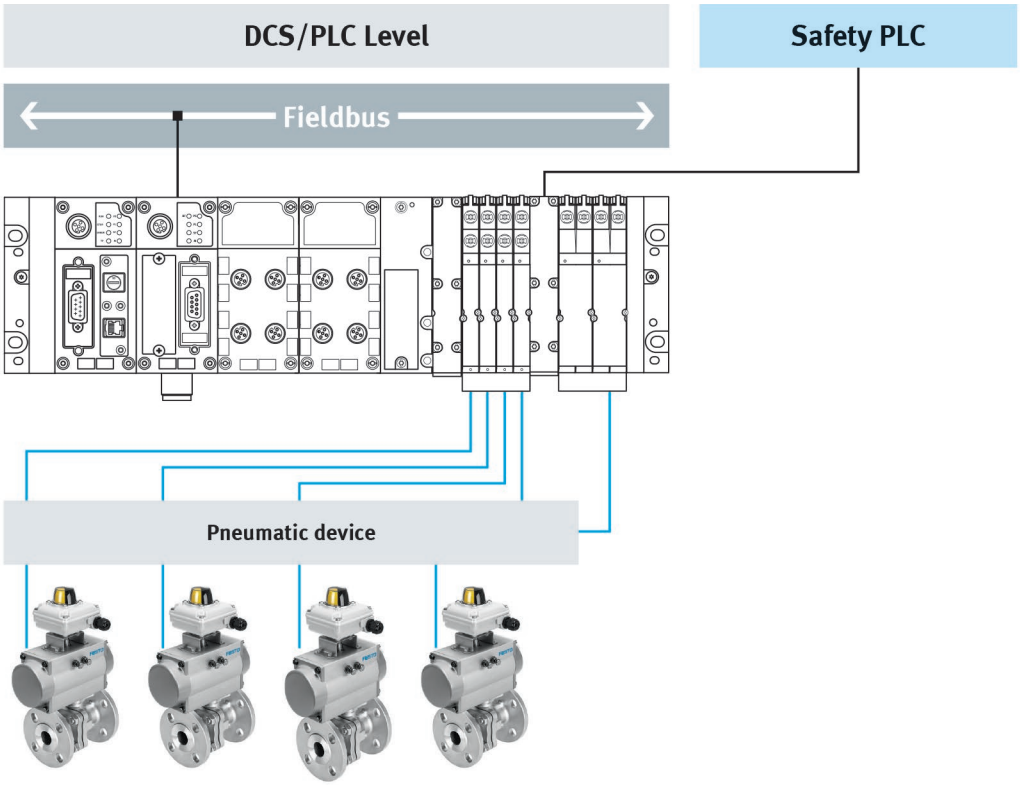
3.2.1 CPX / MPA with safety PLC
Valve terminal with integrated safety shutdown to control separate actuators.

In the operating mode, the valve terminal is activated via a fieldbus and controls actuators in the process. In addition, the valve terminal has a separate supply from the safety PLC, which actuates the valves on the valve terminal for the safety shutdown. The actuators for the operating mode and the actuators for the safety shutdown are connected in series. This solution is suitable for SIL 2 circuits. To increase the safety level, there is also an option of interconnecting the valves redundantly.



3.2.2 CPX / MPA with safety PLC
Valve terminal with integrated safety shutdown to control actuators in operating and safety mode.

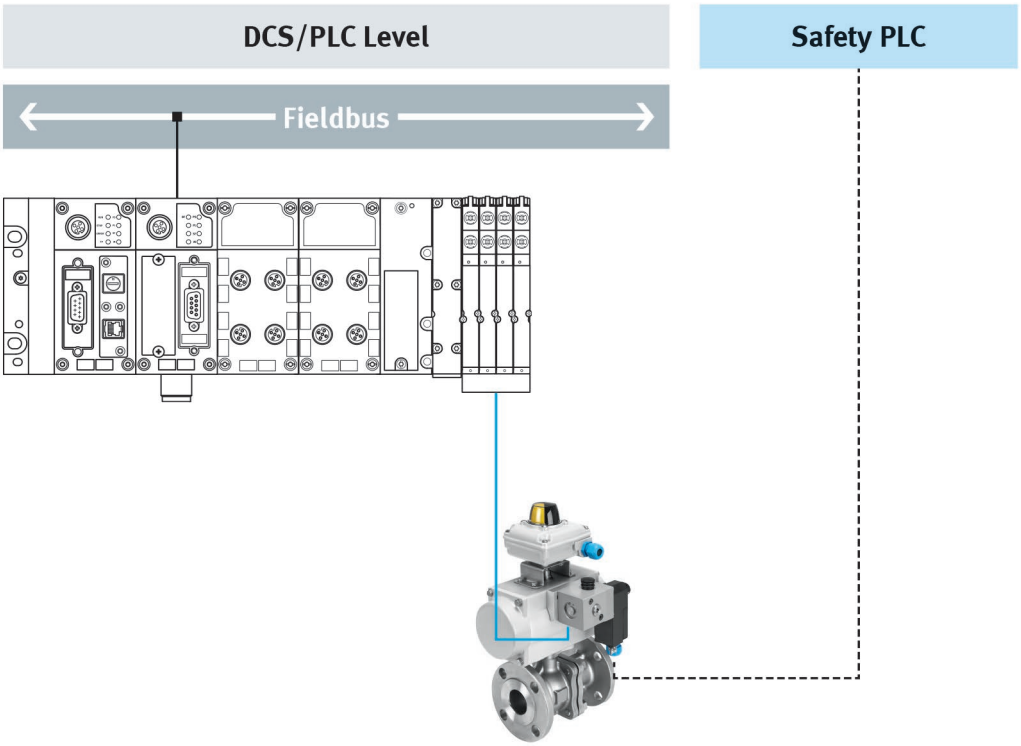
In operating mode, the valve terminal is actuated via a fieldbus and switches actuators in the process. In addition, the valve terminal has a separate supply from the safety PLC, which actuates the valves on the valve terminal for the safety shutdown. It also controls the same actuators in order to shut down the process safely. This solution is suitable for SIL 2 circuits. To increase the safety level, there is an option to switch the valves redundantly.



3.3 VOFC/D as a safety valve

Valve terminal plus single valve for safety shut-off

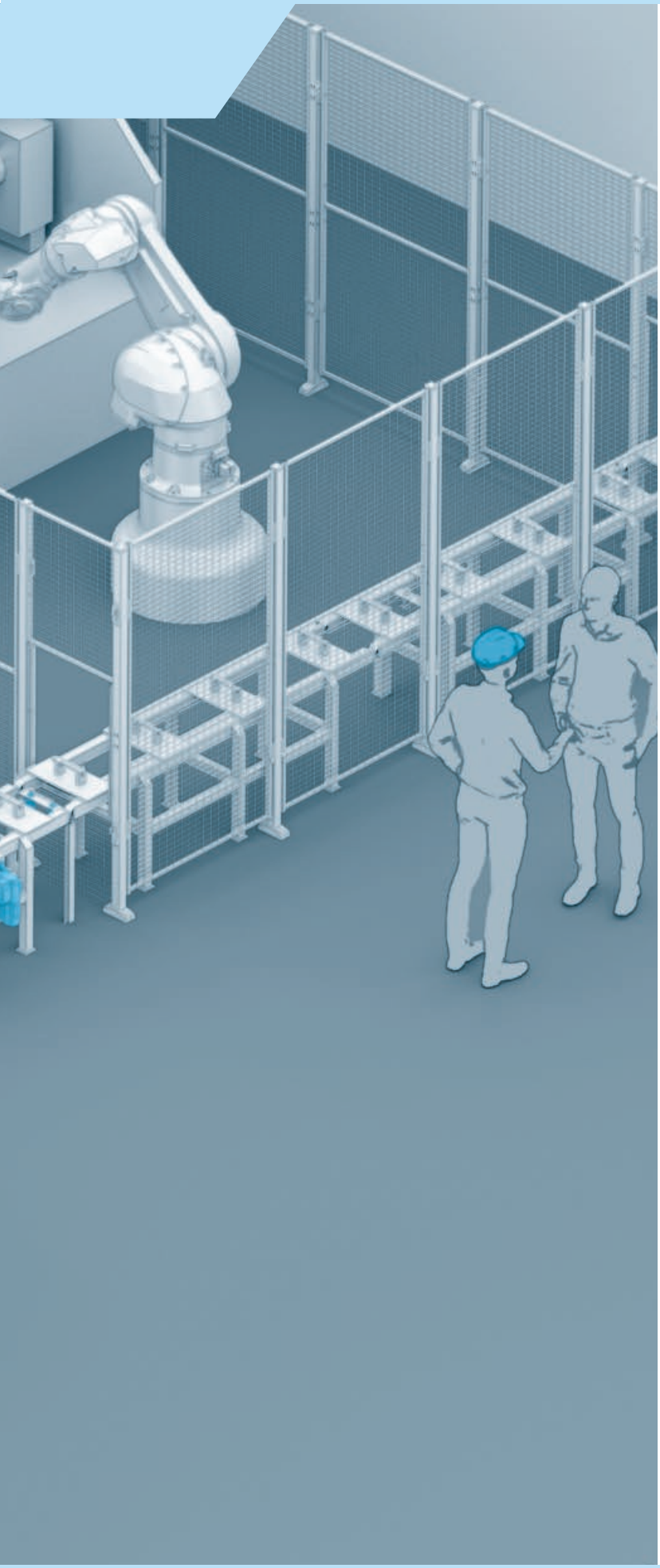
The operating mode is activated via the fieldbus and the valve terminal, and is used to control actuators in the field. The certified individual valve mounted on the same actuator is directly actuated by the safety PLC and, if required, switches off safely.
These valves can be used in safety-related circuits up to SIL3 level.



03 From requirements to implementation

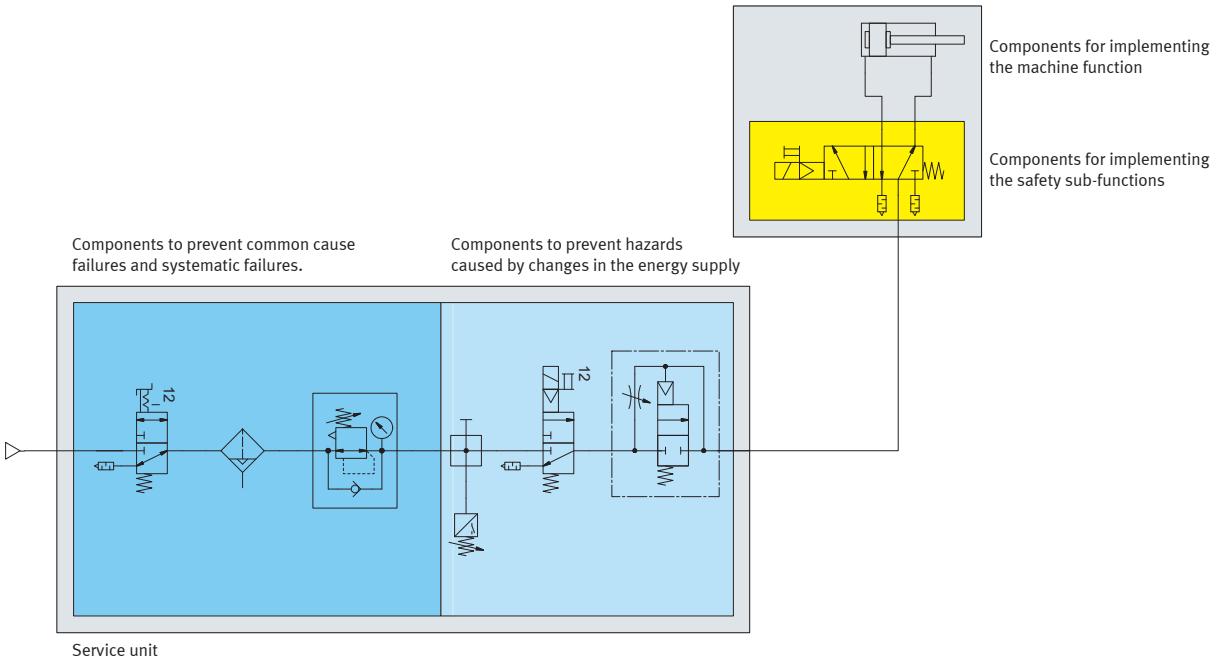
Your route to a safe machine

Application examples to help you create safe solutions using basic pneumatic and electrical circuits.



Contents

Systematic circuit design for safety sub-functions



The following points show a tried-and-tested method for designing pneumatic circuits with integrated safety sub-functions and their targeted selection and sizing.

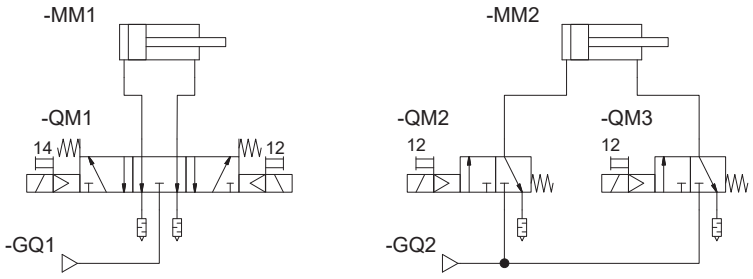
1. **Select the components for the actual machine function**
   Determine which components are suitable for designing the required machine function, e.g. to move or clamp a workpiece.
2. **Select the components for implementing the safety sub-functions**
   When developing the safety concept, the safety sub-function that is needed for the machine is stipulated along with the safety requirements they need to fulfil. The components required for the implementation need to be selected and sized so that the existing requirements can be met.
3. **Select components to prevent hazards caused by changes in the energy supply**
   When the compressed air supply to a system is switched on, sudden pressurisation can present a hazard.
   This hazard can be reduced using a soft-start valve.
   If, on the other hand, the operating pressure falls below the minimum operating pressure needed for the components used, this can result in unexpected behaviour.
   This is prevented by a pressure monitoring function, which induces a safe state (de-energised state) when the permissible limit values are not observed.
4. **Select components for measures against common cause failures and against systematic failures**
   ISO 4414 for pneumatic safety, in addition to ISO 13849, stipulates certain measures. These measures include, for example, the use of a filter for maintaining the compressed air quality, an overpressure valve or pressure regulating valve for maintaining the permissible pressure range and a manual on/off valve to be able to manually disconnect the compressed air supply and exhaust the machine.
   The requirements from ISO 4414 with respect to a service unit are described on Page 72, the requirements with respect to common cause failures on Page 40.

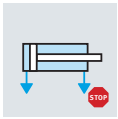
Further reading
- ISO 13849-1 – Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
- ISO 13849-2 – Safety of machinery – Safety-related parts of control systems – Part 2: Validation
- ISO 4414 – Fluid engineering – General rules and safety requirements for pneumatic systems and their components
- ISO 14118 – Machine safety – Prevention of unexpected start-up
- ANSI B 11.26 – General Principles for the Design of Safety Control Systems Using ISO 13849-1 (USA)
- CFR 1910.147 – Control of Hazardous Energy (Lockout/Tagout) (USA)

→ Application notes can be found on the Festo homepage in the Support/Downloads area.

The circuits shown here are basic circuits as per VDMA 24584 and show a suitable structure for category 1.
To achieve this structure, the requirements of the category must be complied with.

STO – Safe torque off





STO

Component	Designation
QM1	5/3-way valve (mid-position exhausted)
QM2, QM3	3/2-way valve (NC)

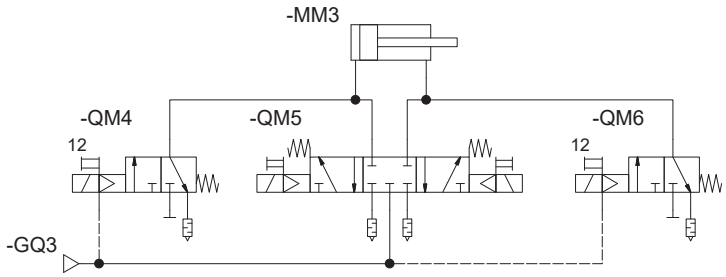
Safe state

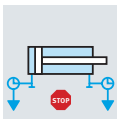
- The pneumatic drive is exhausted and de-energised.

Application note

→ 100225

SS1 – Safe stop 1





SS1

Component	Designation
QM5	5/3-way valve (mid-position closed)
QM4, QM6	3/2-way valve (NC)

Safe state

- The pneumatic drive is exhausted and de-energised.

Comments

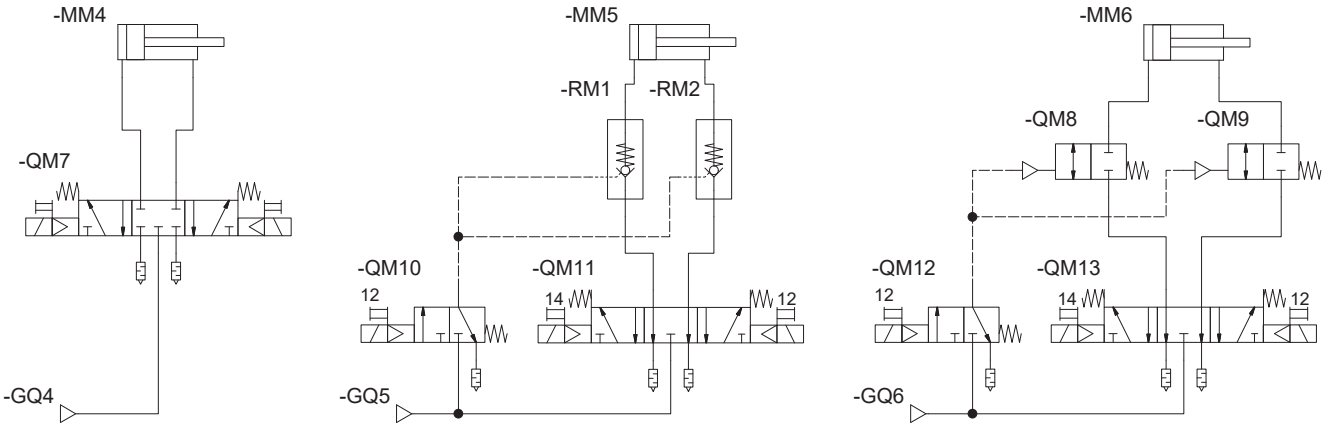
- With this circuit, the safety sub-function SS1-t (safe stop 1 time controlled) can be implemented in accordance with VDMA 24584. This means that the STO function follows the drive delay after a certain period of time has elapsed. This means that, after switching from QM5, a specified period of time must elapse before QM4 and QM6 are switched to the normal position.

Application note

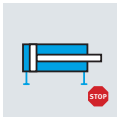
→ 100226

Basic circuits for safety sub-functions

SSC – Safe stopping and closing



Component	Designation
QM7	5/3-way valve (mid-position closed)
RM1, RM2	Piloted check valve
QM8, QM9	2/2-way valve (NC)
QM10, QM12	3/2-way valve (NC)



SSC

Safe state

- Compressed air is locked in the pneumatic drive to maintain the last position occupied.

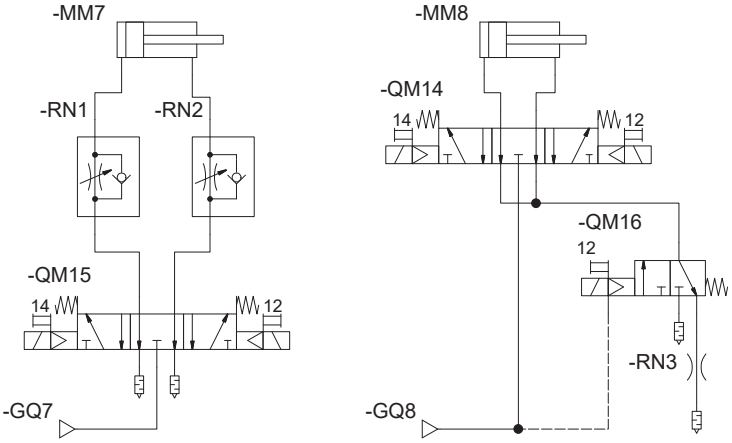
Comments

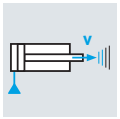
- Leakages can lead to a slower movement of the drive after longer idle periods.

Application note

→ 100231

SLS – safely limited speed





SLS

Component	Designation
RN1, RN2	One-way flow control valve on the pneumatic drive
QM16	3/2-way valve (NC)
RN3	Flow control valve

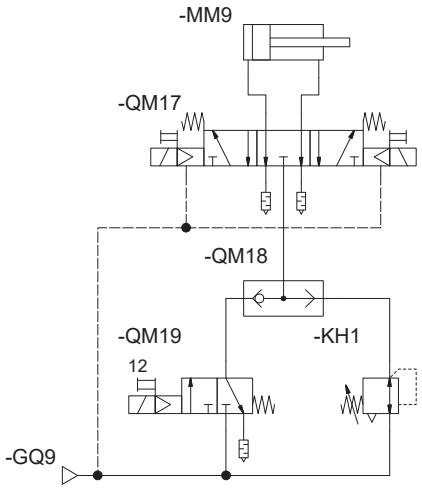
Safe state

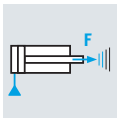
- The pneumatic drive cannot exceed a certain speed.

Application note

→ 100232

SLT – safely limited torque





SLT

Component	Designation
KH1	Pressure regulator

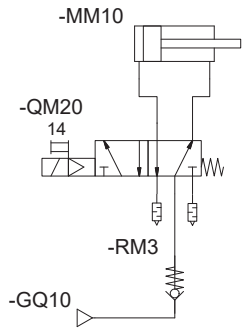
Safe state

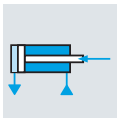
- By limiting the pressure, the pneumatic drive cannot exceed the set force.

Application note

→ 100233

SDI – safe direction





SDI

Component	Designation
QM20	5/2-way valve

Safe state

- It prevents the drive from moving in the wrong direction.

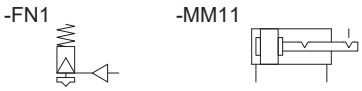
Comments

- The check valve RM3 can, in the event of a pressure drop, prevent a movement in the wrong direction as a result of external forces.

Application note

→ 100235

SB – safe blocking; not part of VDMA 24584



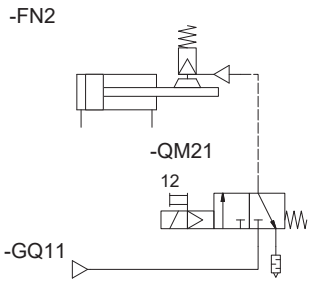

SB

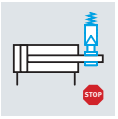
Component	Designation
FN1	Clamping unit
MM11	Drive with end-position locking

Safe state

- The pneumatic drive is blocked so it cannot move freely.

SSB – Safe stopping and blocking



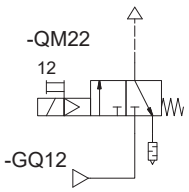

SSB

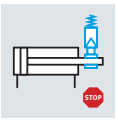
Component	Designation
FN2	Clamping unit with SSB characteristics

Safe state

- The pneumatic drive is stopped and its free movement is blocked.

SBC – safe brake control




SBC

Component	Designation
QM22	3/2-way valve (NC)

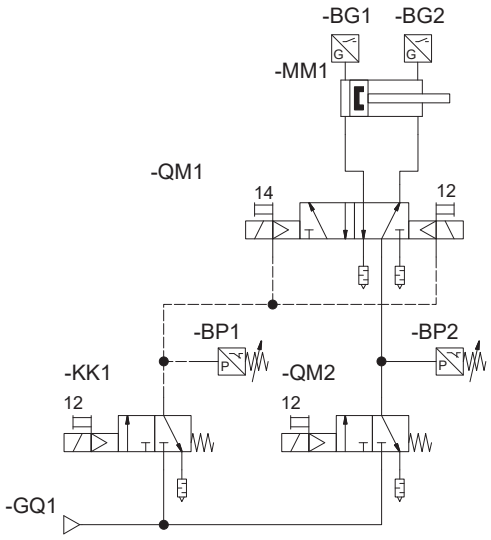
Safe state

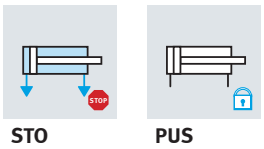
- The control input of the brake is depressurised.

Comments

- The safety sub-functions SB and SSB are mechanical safety sub-functions and are usually combined with safety sub-function SBC.

Sample circuit of clamping device for workpieces





Component	Designation
BG1, BG2	Limit switch, cylinder
BP1, BP2	Pressure switch
MM1	Pneumatic drive
QM1	5/2-way valve, double solenoid
QM2	3/2-way valve, single solenoid
KK1	3/2-way valve, single solenoid

Safe state, e.g. for safety requirements with light curtain, for the safety sub-function PUS (working air present), category 3, up to PL e
The valves QM1 and KK1 are switched-off safety related.
The pneumatic drive MM1 is in a monitored end position. One chamber of the pneumatic drive is pressurised. QM1 cannot switch and trigger a movement from MM1.

Safe state, e.g. for safety requirements with emergency stop or safety door switch, for the safety sub-function PUS (working air exhausted), category 3, up to PL e
The valves QM1 and QM2 are switched-off safety related.
The pneumatic drive is in a monitored end position. The pneumatic drive is exhausted and de-energised. The valves cannot switch and trigger a movement.

Safe state, e.g. for safety requirements via the emergency stop function, for the safety sub-function STO, category 1, up to PL c
The valve QM2 is switched-off safety related.
The pneumatic drive is exhausted and de-energised.

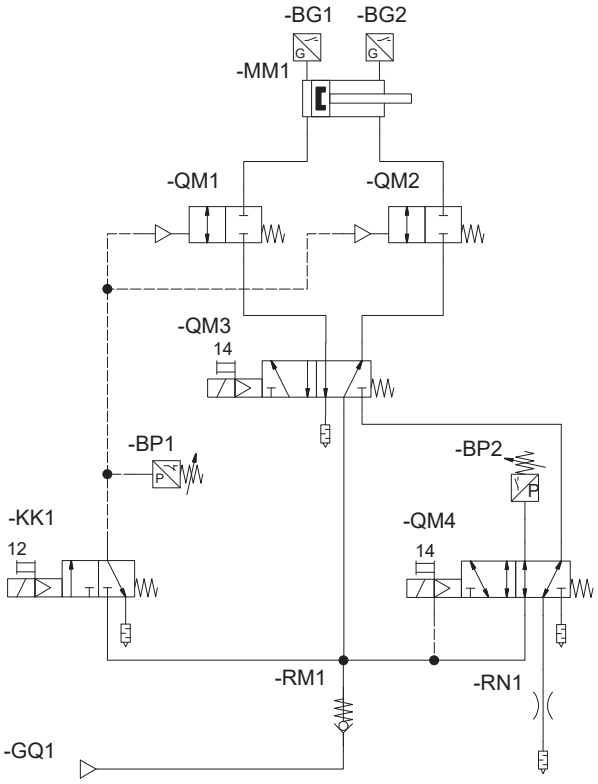
Implementation of the safety sub-functions
- Safe torque off (STO), category 1, up to PL c
- Prevention of unexpected start-up (PUS) with existing working air, category 3, up to PL e
- Prevention of unexpected start-up (PUS) with exhausted working air, category 3, up to PL e

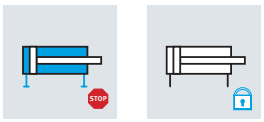
Comments
- Exhausting the working air from QM2 reduces the clamping force of MM1.
- The valve QM1 must have a fault exclusion for “spontaneous change of the initial switching position without an input signal”.

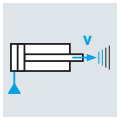
Information on the fault exclusion “spontaneous change of the initial switching position of the main stage without an input signal” can be found in the Support/Downloads area on the Festo homepage under Technical Report
→TR-300003 and
→TR-300004

→ Application notes can be found on the Festo homepage in the Support/Downloads area.

Sample circuit with limited speed and stopping of the movement







Component	Designation
BG1, BG2	Limit switch, cylinder
BP1, BP2	Pressure switch
MM1	Pneumatic drive
QM3, QM4	5/2-way valve, single solenoid
QM1, QM2	2/2-way valve, single solenoid
KK1	3/2-way valve, single solenoid
RM1	Check valve
RN1	Flow control valve

Safe state

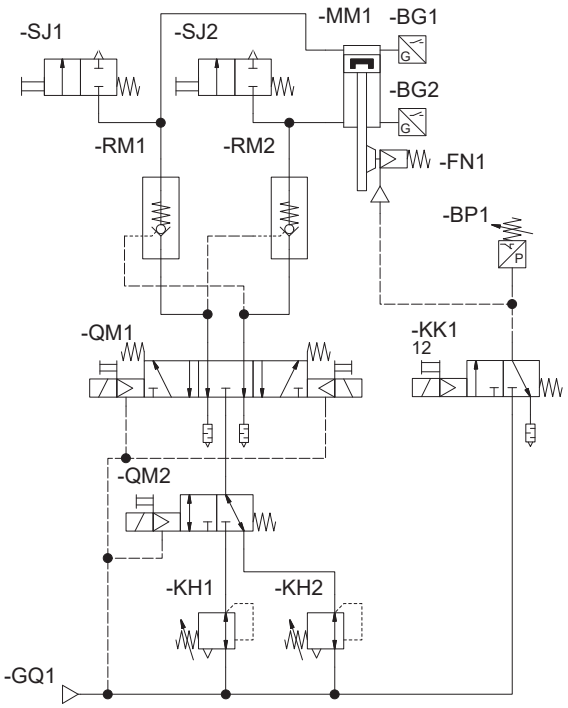
- The compressed air is locked in the pneumatic drive so it maintains the position last occupied (SSC).
- A hazardous movement can be avoided.
- The pneumatic drive cannot exceed a certain speed (SLS).

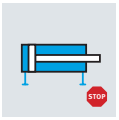
Implementation of the safety sub-functions

- Safe stopping and closing (SSC), up to category 1, PL c
- Prevention of unexpected start-up (PUS), up to category 3, PL e
- Safely limited speed (SLS), up to category 2, PL d

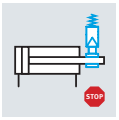
→ Application notes can be found on the Festo homepage in the Support/Downloads area.

Sample circuit for a vertical axis with limited force and stopping of the movement



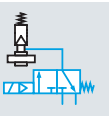


SSC



SSB

PUS



SBC

Component	Designation
BG1, BG2	Limit switch, cylinder
BP1	Pressure switch
MM1	Pneumatic drive
QM1	5/3-way valve, mid-position exhausted, single solenoid
RM1, RM2	Piloted check valve
QM2	3/2-way valve, single solenoid
KK1	3/2-way valve, single solenoid
KH1, KH2	Pressure regulating valve with sufficient secondary exhausting
SJ1, SJ2	2/2-way valve, single solenoid
FN1	Clamping unit with emergency stop characteristics

Safe state

- By limiting the pressure (SLT), the pneumatic drive cannot exceed the set force.
- Compressed air is locked in the pneumatic drive to maintain the last position occupied (SSC).

Implementation of the safety sub-functions

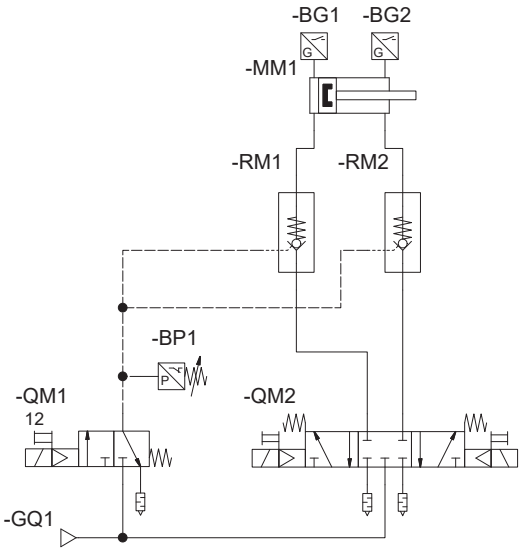
- Safely limited torque (force) (SLT), up to category 1, PL c
- Safe stopping (SSx), up to category 3, PL d
  - Safe stopping and closing (SSC), up to category 1, PL c
  - Safe stopping and blocking (SSB), up to category 1, PL c
- Prevention of unexpected start-up (PUS), up to category 3, PL e
- Safe brake control (SBC), up to category 1, PL c

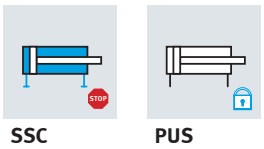
Comments

Long idle periods or leakages can lead to exhausting of the piston chambers. Please bear this mind when taking the safety sub-function PUS into account and when opening the brake.

→ Application notes can be found on the Festo homepage in the Support/Downloads area.

Sample circuit for stopping the movement with SSC





Component	Designation
BG1, BG2	Limit switch, cylinder
BP1	Pressure switch
MM1	Pneumatic drive
QM2	5/3-way valve, mid-position closed Single solenoid
RM1, RM2	Piloted check valve
QM1	3/2-way valve, single solenoid

Safe state

- Compressed air is locked in the pneumatic drive to maintain the last position occupied (SSC).
- A hazardous movement is avoided.

Implementation of the safety sub-functions:

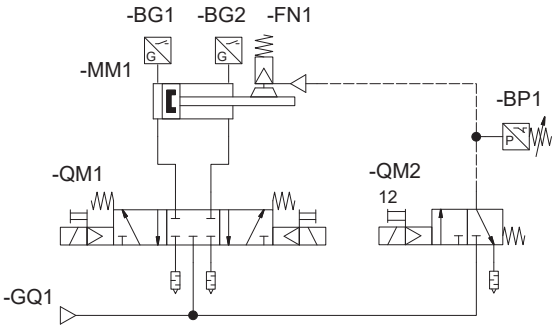
- Safe stopping and closing (SSC), up to category 3, PL d
- Prevention of unexpected start-up (PUS), up to category 3, PL e

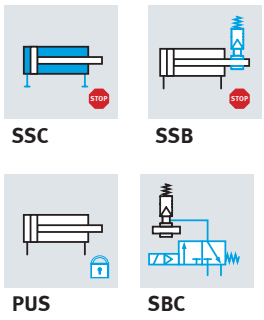
Comments

- Always check whether each channel in multi-channel solutions fulfils the safety sub-function.
- The diagnostics must be performed via a test routine.
- The drive is stopped using compressed air. This means there is still energy stored as compressed air in the system. Additional measures must be taken to be able to exhaust the drive chambers.
- If trapped compressed air can result in a hazard, further measures are required.
- Please note that the technical values of the components are complied with during braking via dynamic energy (e.g. via resulting pressure peaks).
- In the event of a fault of the 5/3-way valve (QM2), compressed air can flow through the check valves (RM1, RM2) until the forces are balanced. That can lead to an increased overtravel time of the drive.
- After the drive stops, it can move depending on the leakage of individual components. This can result in the drive chambers being exhausted. Please also bear this in mind for the unexpected restart and when opening the brake.

→ Application notes can be found on the Festo homepage in the Support/Downloads area.

Sample circuit for stopping the movement with SSC and SSB





Component	Designation
BG1, BG2	Limit switch, cylinder
BP1	Pressure switch
MM1	Pneumatic drive
QM1	5/3-way valve, mid-position closed, single solenoid
QM2	3/2-way valve, single solenoid
FN1	Clamping unit with SSB characteristics

Safe state

- The compressed air is locked in the pneumatic drive so it maintains the last occupied position (SSC).
- The pneumatic drive is stopped and its free movement is blocked (SSB).
- A hazardous movement is avoided.
- The control input of the brake is depressurised (SBC).

Implementation of the safety sub-functions:

- Safe stopping (SSx), up to category 3, PL d
  - Safe stopping and closing (SSC), up to category 1, PL c
  - Safe stopping and blocking (SSB), up to category 1, PL c
- Prevention of unexpected start-up (PUS), up to category 3, PL e
- Safe brake control (SBC), up to category 1, PL c

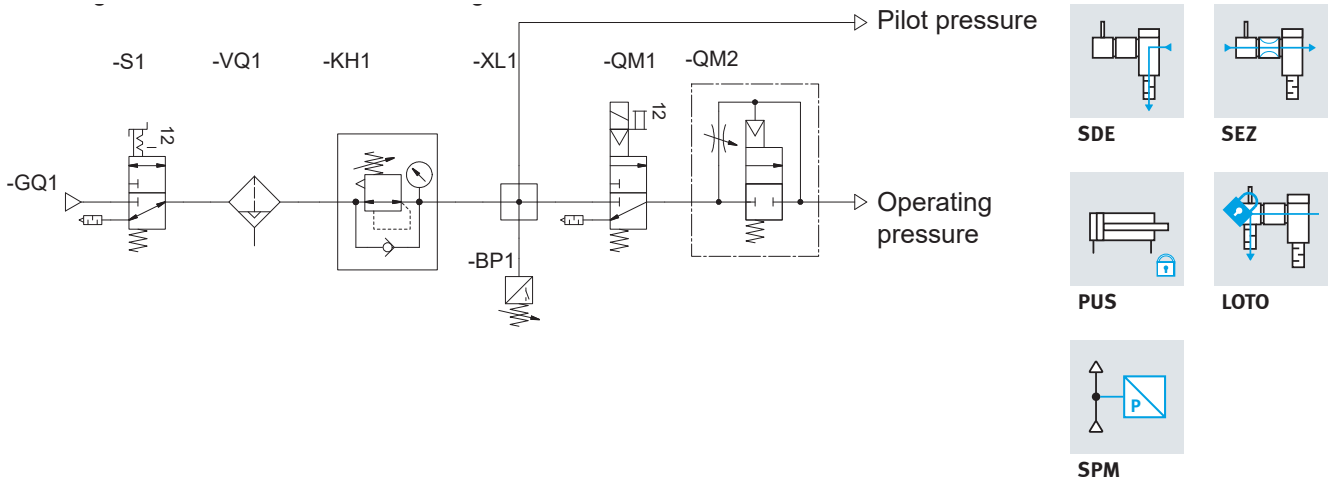
Comments

- Always check whether each channel in multi-channel solutions fulfils the safety function.
- The diagnostics must be performed via a test routine.
- After the drive stops, the drive chambers can exhaust depending on the leakage of the individual components. Please also bear this in mind for the unexpected start-up.

→ Application notes can be found on the Festo homepage in the Support/Downloads area.

Service unit for safety circuits

Every machine or system with pneumatic drive technology needs a service unit.
With the following service unit, requirements for machine safety and functional safety can be implemented.



Component	Designation
S1	On/off valve, manual
VQ1	Filter with water separator, automatic
KH1	Pressure regulator with pressure gauge
XL1	Branching module
BP1	Pressure switch
QM1	On/off valve
QM2	Soft-start valve
	Silencer

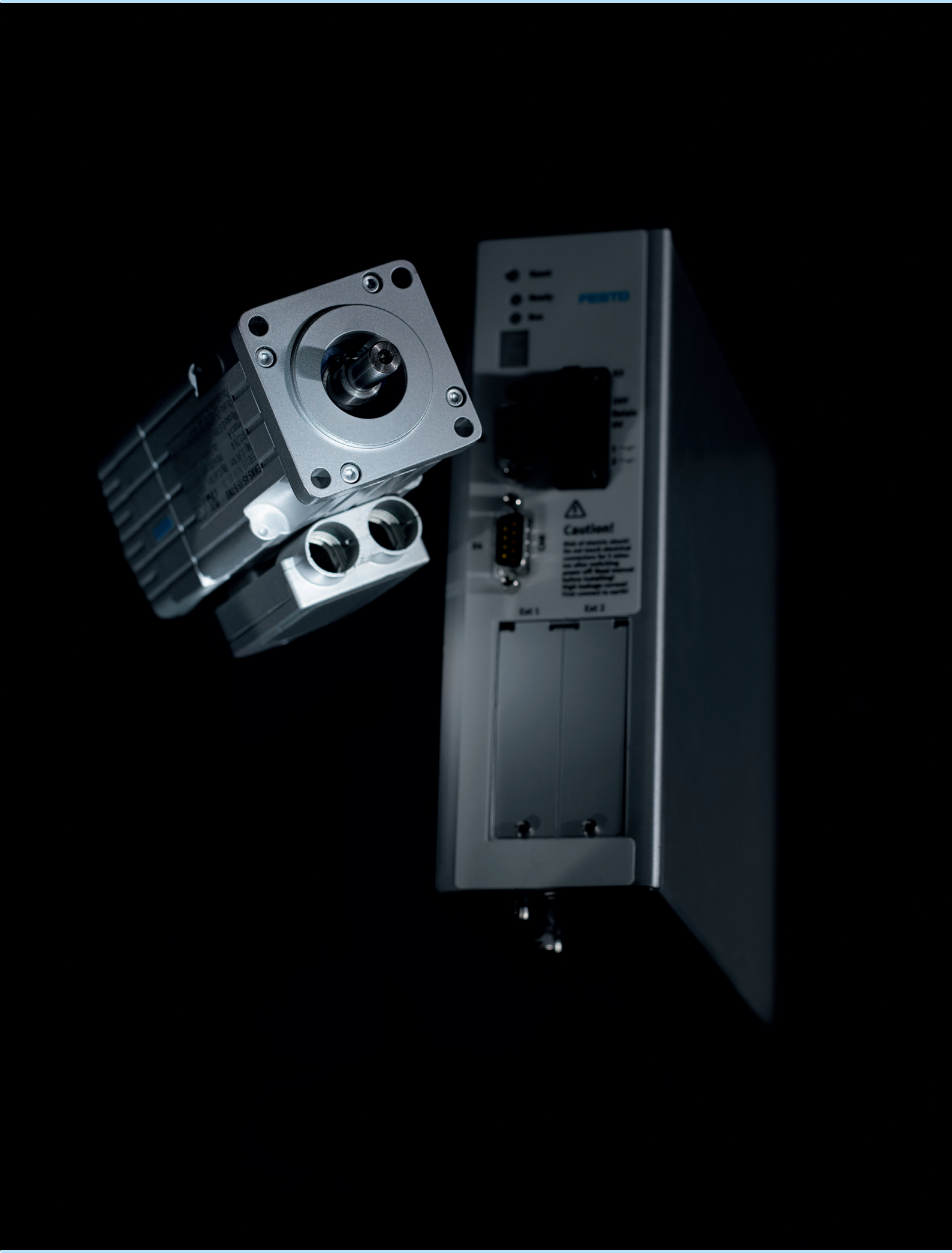
Safe state
- The part of the pneumatic system directly downstream of the on/off valve (QM1) is separated from the compressed air supply and exhausted.
- For a planned system pressurisation, the working air needs a controlled pressure rise.

Implementation of the safety sub-functions in accordance with VDMA 24584
- Safe de-energization (SDE), category 1, up to PL c
- Safe energization (SEZ), category 1, up to PL c
- Prevention of unexpected start-up (PUS), category 1, up to PL c
- Safe pressure monitor (SPM), category 1, up to PL c

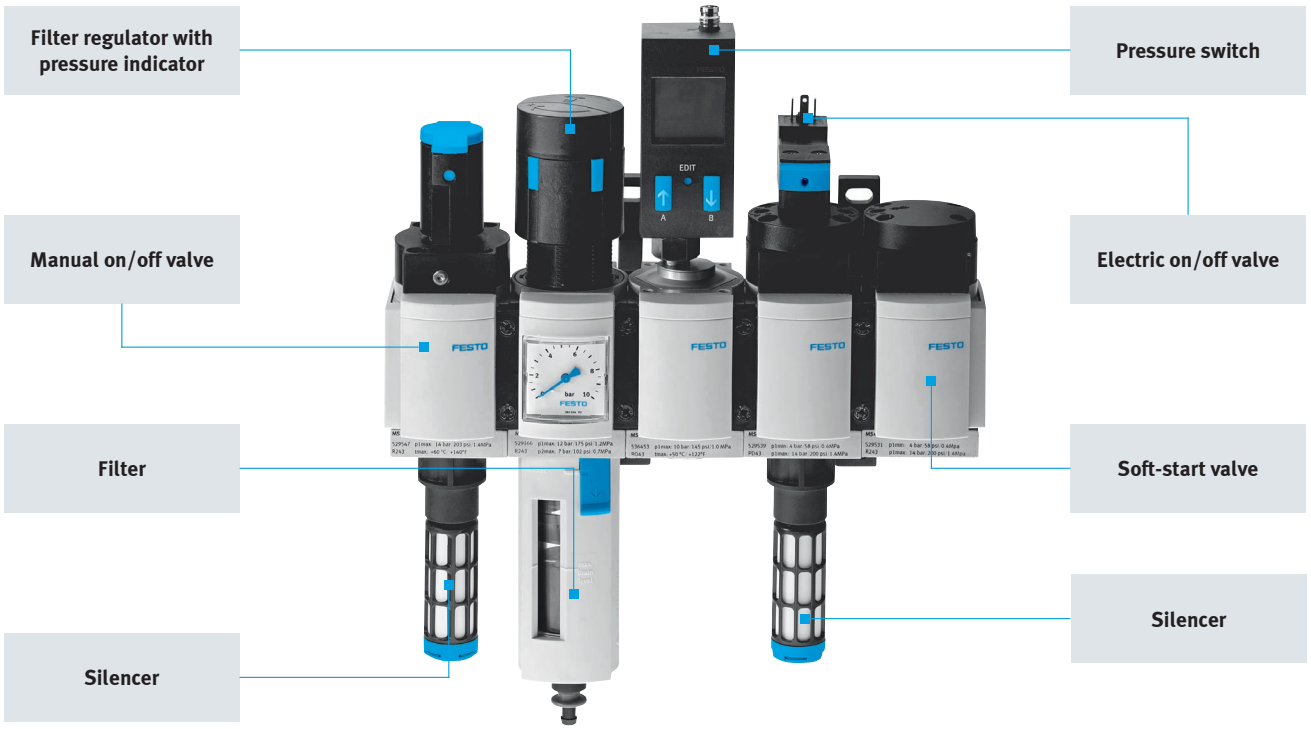
Implementation of measures for pneumatic safety in accordance with ISO 4414
- Safe disconnection and exhausting of the compressed air supply
- Protection in the event the compressed air fails or is switched off and then restored
- Checking the disconnection and exhausting
- Filtering hazardous substances
- Protection against overpressure and underpressure
- Protection against uncontrolled movements of drives
- Protection against noise levels that are too high

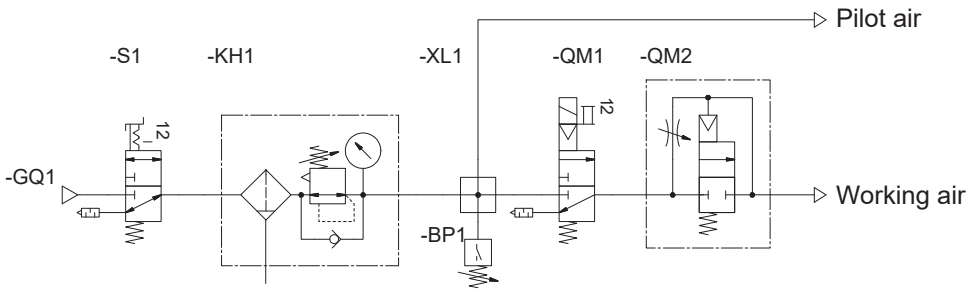
Implementation of measures for functional safety in a machine in accordance with ISO 13849
- Measures to control and prevent systematic failures
- Measures against common cause failures (CCF)
- Fundamental and proven safety principles

→ Application notes can be found on the Festo homepage in the Support/Downloads area.


FESTO
Caution!

Service unit for pneumatic and functional safety





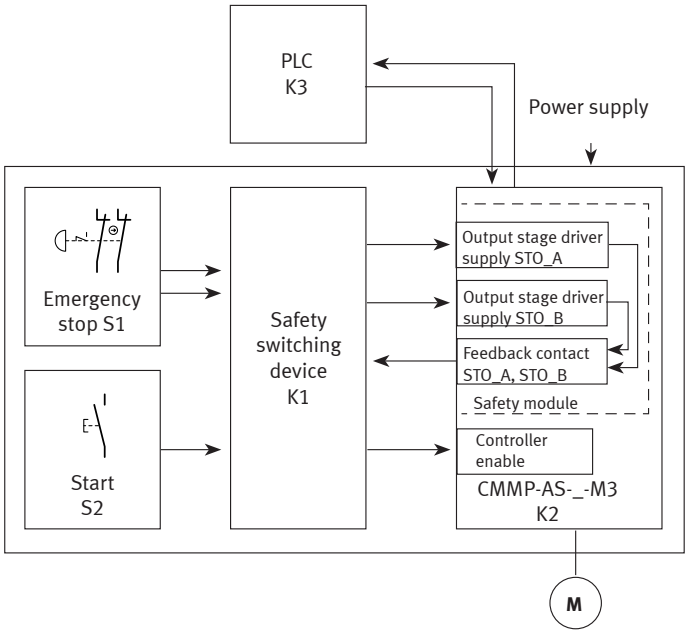
A service unit fulfils various safety-related requirements for pneumatic systems as well as functional safety. These include, for example, measures against systematic failures, measures against common cause failures, basic and well-tried safety principles and measures against unexpected start-up. The specified components can be suitable for implementing the requirements.

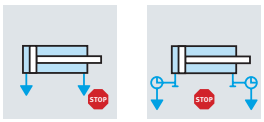
Components of the service unit	General requirements [1, 4]	Measures to control and prevent systematic failures [1]	Measures against common cause failures (CCF) [2]	Basic safety principles [3]	Proven safety principles [3]
Manual on/off valve [4,5]	Disconnecting and exhausting the compressed air supply, lockout and tagout	Applying energy shut-off	Using tried-and-tested components	Applying the energy shut-off principle, protection against unexpected start-up	
Filter	Harmful solid, fluid and gaseous substances are filtered from the air.	Compliance with the necessary operating conditions	Filtering, preventing contamination, draining compressed air	Appropriate measures to prevent the contamination of the fluid	Suitable prevention of fluid contamination
Pressure regulator	Protection against overpressure	Measures to manage the effects of overpressure	Using well-tried components, protection against overpressure	Pressure limitation	Suitable range for the operating conditions
Pressure indicator	Pressure measurement, checking the energy shut-off and discharge				
Pressure switch	Protection against hazards caused by the compressed air being switched off, disconnected or failing and the supply being switched back on (together with electric on/off valve)	Failure detection via automatic tests, measures to manage the effects of overpressure and underpressure	Using well-tried components	Protection against unexpected start-up (together with automatic on/off valve)	Suitable range for the operating conditions (together with the electric on/off valve)
Electric on/off valve	Protection against hazards caused by the compressed air being switched off, disconnected or failing and the supply being switched back on (together with electric on/off valve), Protection against unexpected start-up		Using well-tried components, Diversity when using 2-channel safety sub-functions Use of well-tried components	Applying the energy shut-off principle Protection against unexpected start-up	
Soft-start valve	Reducing the hazards caused by uncontrolled movements of drives		Using well-tried components		
Silencer [6]	Measure against noise levels that are too high				

Further reading

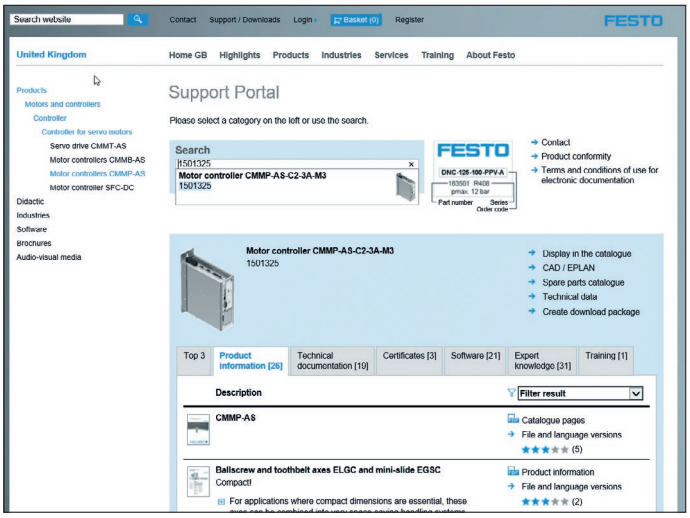
- [1] ISO 4414 – Fluid engineering – General rules and safety requirements for pneumatic systems and their components
- [2] ISO 13849-1 – Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
- [3] ISO 13849-2 – Safety of machinery – Safety-related parts of control systems – Part 2: Validation
- [4] ISO 14118 – Machine safety – Prevention of unexpected start-up
- [5] OSHA 1910.147 The control of hazardous energy (lockout/tagout)
- [6] ISO 11688-2 – Acoustics – Recommended practice for the design of low-noise machinery and equipment — Part 2: Introduction to the physics of low-noise design

Application examples





Part no.	Type
1501325	CMMP-AS-C2-3A-M3
1501326	CMMP-AS-C5-3A-M3
1501327	CMMP-AS-C5-11A-P3-M3
1501328	CMMP-AS-C10-11A-P3-M3
561406	CMMD-AS-C8-3A
550041	CMMP-AS-C2-3A
550042	CMMP-AS-C5-3A
551023	CMMP-AS-C5-11A-P3
551024	CMMP-AS-C10-11A-P3
1366842	CMMP-AS-C20-11A-P3
572986	CMMS-AS-C4-3A-G2
572211	CMMS-ST-C8-7-G2
1512316	CMMO-ST-C5-1-DIOP
1512317	CMMO-ST-C5-1-DION
5111189	CMMT-AS-...-11A-P3-...
5111184	CMMT-AS-...-3A-...
5340819	CMMT-AS-C2-3A-EC-S1
5340814	CMMT-AS-C2-3A-PN-S1
5340820	CMMT-AS-C4-3A-EC-S1
5340815	CMMT-AS-C4-3A-PN-S1



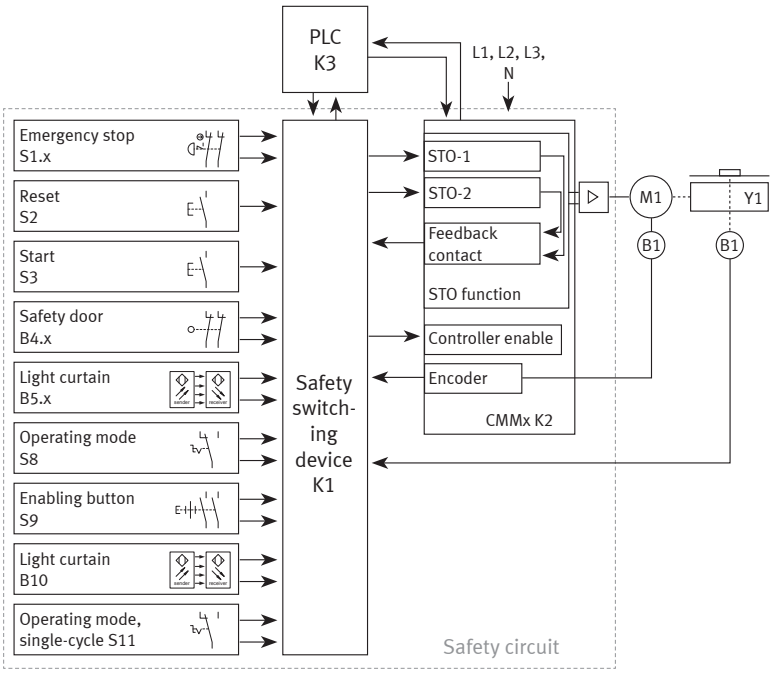
See the technical data of the individual products for detailed information.

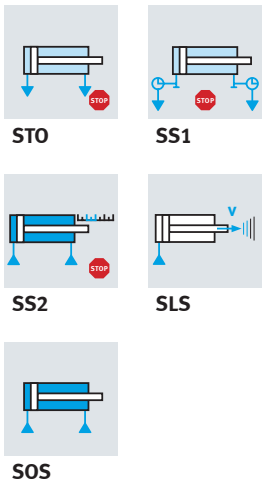
CMMx motor controller / servo drive

- The application examples show the circuitry of the CMMx motor controller for safety switching devices.
- The application examples show how the safety sub-functions safe torque off (STO) or safe stop 1 (SS1) can be implemented.
- As well as the description, circuit diagram and parts list, it also includes an evaluation of the described safety sub-functions with SISTEMA.

→ Application notes can be found on the Festo homepage in the Support/Downloads area.

No more programming – just parameterisation



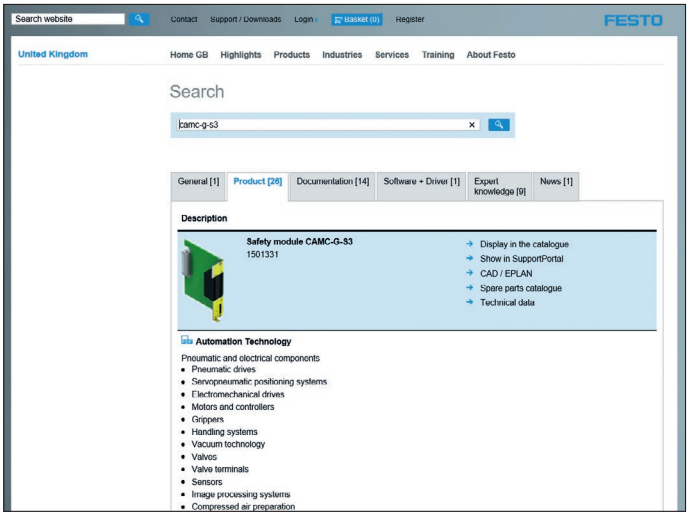


Comments

The programming examples cover the usual configurations of the safety module CAMC-G-S3.

- Emergency stop switch trips the safety sub-function STO in drives
- Emergency stop switch trips the safety sub-function SS1 in drives
- Emergency stop switch and safety doors trip the safety sub-function SS1 in drives, operating mode automatic and manual
- Emergency stop switch and safety doors trip the safety sub-function SS1 in drives, operating mode automatic and manual (with enabling button and safely limited speed (SLS))
- Emergency stop switch, safety doors and light curtain trip the safety sub-function SS1 in drives, operating mode automatic and manual (with enabling button and safely limited speed (SLS))
- Two-hand control trips the safety sub-function SS1 in drives
- Emergency stop switch and two-hand control trip the safety sub-function SS1 in drives
- Emergency stop switch, safety doors and two-hand control trip the safety sub-function SS1 in drives
- Emergency stop switch, safety doors and two-hand control trip the safety sub-function SS1 in drives, operating mode automatic and manual (with enabling button and safely limited speed (SLS))
- Emergency stop switch, safety doors and light curtains trip the safety sub-function SS1 in drives, operating mode automatic and manual (with enabling button and safely limited speed (SLS)), a light curtain in single-cycle operation (intervention leads to SS2, with automatic start)

The application programs in these programming examples reduce the complexity of a programmable safety system to straightforward configuration and wiring, as with a simple safety relay.



→ Application notes can be found on the Festo homepage in the Support/Downloads area.

04 Your safety implementation with our products

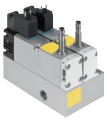
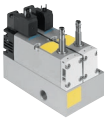
Your route to a safe machine and system

There are many different safety functions that are needed to ensure a machine in your application is safe.
We will show you how you can achieve this using our products.

Contents

Safety sub-functions in pneumatic drive technology

Safety sub-functions that affect systems

Application	Up to PL e			Up to PL d
SDE Safe de-energization	 → MS6-SV-1/2-E-...	 → VOFA-L26-T32C-...	 → MS6-SV-1/2-D-...	
SEZ Safe energization				
PUS Prevention of unexpected start-up	 → MS6-SV-1/2-E-...	 → VOFA-L26-T32C-...	Clamping devices for workpieces	 → MS6-SV-1/2-D-...
SBC Safe brake control				

Your safety implementation with our products

04

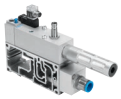
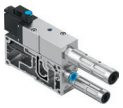
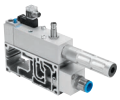
Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in pneumatic drive technology

Up to PL c						
						
→ MSx-SV-...-C	→ VABF-S6-1-P5A4-...-G12-1T5-PA	→ VABF-S6-1-P5A4-G12-4-1-P	→ MSx-EE-..., MSx-EE-...-S-CS	→ HEE-D-..., HEE-D-...-SA	→ VABP-...	Service unit for safety circuits
						
→ MS6-SV-1/2-E-...	→ MS6-SV-1/2-D-...	→ MSx-DL-...	→ HEL-D-...	→ VABF-S6-1-P5A4-...-G12-1T5-PA	→ VABF-S6-1-P5A4-G12-4-1-P	Service unit for safety circuits
						
→ MS6-SV-1/2-C-...	Service unit for safety circuits					
						
Well-tried standard valves (e.g. monostable 3/2 NC with exhausting from 2 to 3)	Vertical axis with limited force and stopping of the movement	Stopping the movement with SSC and SSB				

Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

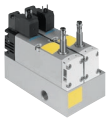
Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in pneumatic drive technology

Safety sub-functions that affect drives

Application	Up to PL e			Up to PL d
STO Safe torque off	 → VOFA-L26-T32C-...			
SSB Safe stopping and blocking				
SB Safe blocking (not part of VDMA)				
SSC Safe stopping and closing		Stopping the movement with SSC	Limited speed and stopping of the movement	
SET Safe equilibrium of torque				
PUS Prevention of unexpected start-up	 → VABA-S6-1-X2-Fx + → VSVA-BTM32CS-...-A2-... + → VABV-S4-...-CB-2T3	 → CPX-FVDA-P2 + → VSVA-B-M52-MZD-xx-1T1L-APP + → VABF-S4-1-S	• Clamping device for workpieces • Vertical axis • Stopping the movement with SSC • Stopping the movement with SSC and SSB • Limited speed and stopping the movement	

Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in pneumatic drive technology

Up to PL c						
						
Well-tried standard valves (e.g. monostable 3/2 NC with exhausting from 2 to 3	→ VABP-...	Clamping device for workpieces				
						
→ DACS / → DFLx	Vertical axis with limited force and stopping of the movement	Stopping the movement with SSC and SSB				
						
→ KP-... / → KPE-...	→ DSBC-...-C-...	→ DDPC-...-CT	→ ADN-...-KP-...	→ DSNU-...-KP	→ DGC-...-1H...-PN	→ DGSL-...-C-...
			 			
→ VFOF-LE-BAH-... → VBNF-LBA-...	→ HGL-... HGL-...-CS	VL-2-1/4-SA	→ VABP-...	Limited speed and stopping of the movement	Vertical axis with limited force and stopping of the movement	Stopping the movement with SSC and SSB
	 					
→ MSx-LR-...	→ VABP-...					
						
Standard bistable valves (technical report → TR-300004)						

Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in pneumatic drive technology

Application		Up to PL e			Up to PL d
Safety sub-functions that affect drives	**SLS** Safely limited speed				Limited speed and stopping the movement
	SLT Safely limited torque (force)				
	SDI Safe direction	→ VOFA-L26-T52-...			
	THC Two-hand control				
Monitoring safety sub-functions	**SCA** Safe cam	2 piece: → SME/→ SMT			
	SVP Safe valve position				
	SPM Safe pressure monitor				

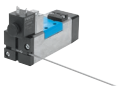
Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in pneumatic drive technology

Up to PL c						
						
→ GRLA-..., → GRLO-..., → GRLZ-..., → GRO-...	GRLA-xxx-B-SA (with tamper protection)	→ VFOF-LE-...	→ VFOF-LE-BAH-...			
						
→ MSx-LR-...	LR-D-MINI-ZD-V24-SA	Vertical axis with limited force and stopping of the movement				
						
Standard valves (e.g. single solenoid 5/2 valve)	→ VABP-...	→ VBNF-LBA-...	→ H-...			
						
→ ZSB-1/8-B						
						
→ SME/→ SMT + → SAMH-S-N8	Service unit for safety circuits					
						
MDH-5/2-...-SA						
						
→ SPBA-P2R-G18-...						

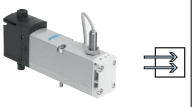
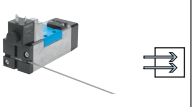
Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in pneumatic drive technology

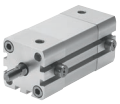
Application	Possible			
Protection against tampering	 GRLA-...-B-SA	 → LRPS-... → LRS-...	 → HE-...-LO	 → MSx-LR-...-AS
	 MSx-EMx-...-SA	 → SAMH-S-N8-...	 Cover caps e.g. VAMC-S6-CS	 → MSx-SV-C-MK
Lockout-tagout (LOTO) Reliable disconnection of the energy source	 → HE-...-LO	 → MSx-EM-...	 MSx-EMx-...-SA	 Service unit for safety circuits
For protecting against unintentional pressure	 → MSx-LR-...	 → LRPS-..., → LRS-...		
Creating zones	 → VTSA	 → MPA		
Valves with negative overlap (selection from the relevant product series)	 → VMPA1-..., → VSVA-..., ...	 → VUVS-LTxx-..., → VUWS-LTxx-..., ...	 → MHAx-..., → MHEx-..., → MHPx-..., ...	 → VSNC-FTx-...
Valves with switching position monitoring	 → VSVA-B-M52-...-APx → VSVA-B-M52-...-ANx	 MDH-5/2-...-SA		

Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Application		Possible			
Additional functions	**Releasing trapped persons**				
		→ HAB-...	→ VFOF-LE-BAH-... → VBNF-LBA-...		
	End-position locking				
		→ DSBC-...-E1-...	→ ADN-...-ELx-...	→ DGSL-...-E3-...	
	Safety coupling				
		→ NPHS-D6-P-...	→ NPHS-D6-M-...		
	Safe inputs				
		→ CPX-F8DE-P			
	Safe outputs				
		→ CPX-FVDA-P2			

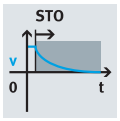
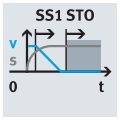
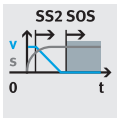
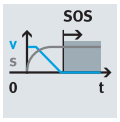
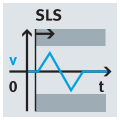
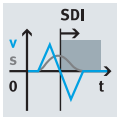
Safety device in accordance with the EC Machinery Directive certified by an independent testing institute

Application note

To control the components shown with a safe output with PL e, the CPX-FVDA-P2 can be used, for example

To record the signals from the components shown with a safe input up to PL e, the CPX-F8DE-P can be used, for example

Safety sub-functions in electric drive technology

Application	Up to PL e			
 **STO** Safe torque off				
		→ CMMT-AS	→ CMMP-AS with → CAMC-G-S3	→ CMMP-AS with → CAMC-G-S1
 **SS1** Safe stop 1				
	→ CMCA	→ CMMT-AS[1]	→ CMMP-AS with → CAMC-G-S3	→ CMMP-AS with → CAMC-G-S1[1]
 **SS2** Safe stop 2				
		→ CMMP-AS with → CAMC-G-S3 → EMME-AS-... → EGC-...-M...		
 **SOS** Safe operating stop				
		→ CMMP-AS with → CAMC-G-S3 → EMME-AS-... → EGC-...-M...		
 **SLS** Safely limited speed				
		→ CMMP-AS with → CAMC-G-S3 → EMME-AS-... → EGC-...-M...		
 **SDI** Safe direction				
		→ CMMP-AS with → CAMC-G-S3 → EMME-AS-... → EGC-...-M...		

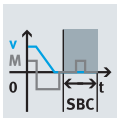
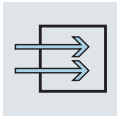
[1] With external safety switching device

Safety sub-functions in electric drive technology

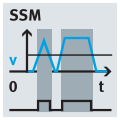
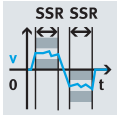
Up to PL e		Up to PL d			Up to PL c	
						
→ CMMO-ST	→ CMXH	→ CMMS-ST	→ EMCA-EC			
						
→ CMMO-ST[1]	→ CMXH[1]	→ CMMS-ST[1]	→ EMCA-EC[1]			
						
			→ CMMP-AS with → CAMC-G-S3 with → EMME-AS...-..X			
						
			→ CMMP-AS with → CAMC-G-S3 with → EMME-AS...-..X			
						
			→ CMMP-AS with → CAMC-G-S3 with → EMME-AS...-..X			
						
			→ CMMP-AS with → CAMC-G-S3 with → EMME-AS...-..X			

Safety sub-functions in electric drive technology

Safety sub-functions that affect systems

Application	Up to PL e			
 **SBC** Safe brake control				
	→ CMMP-AS with → CAMC-G-S3	→ CMMT-AS		
 Safe inputs				
	→ CPX-F8DE-P			
 Safe outputs				
	→ CPX-FVDA-P2			
 Clamping unit				

Monitoring safety sub-functions

Application	Up to PL e			
 **SSM** Safe speed monitor				
		→ CMMP-AS with → CAMC-G-S3 → EMME-AS-... → EGC-...-M...		
 **SSR** Safe speed range				
		→ CMMP-AS with → CAMC-G-S3 → EMME-AS-... → EGC-...-M...		

[2] Only with additional measures

Up to PL e		Up to PL d			Up to PL c	
						
		→ CMMP-AS with → CAMC-G-S1				
						
		→ EGC with 2-channel clamping unit[2]				→ EGC with 1-channel clamping unit

Up to PL e		Up to PL d			Up to PL c	
						
			→ CMMP-AS with → CAMC-G-S3 with → EMME-AS...-..X			
						
			→ CMMP-AS with → CAMC-G-S3 with → EMME-AS...-..X			

Safety sub-functions in the pneumatic process industry

		Redundant interconnection[1]					
		Low demand			High demand		
	Certificate issuing authority	Up to SIL 1	Up to SIL 2	Up to SIL 3	Up to SIL 1	Up to SIL 2	Up to SIL 3
Pilot valve VOFC 	TÜV			•			•
Pilot valve VOFD 	TÜV			•			•
Quarter turn actuator DFPD 	TÜV			•			•
Pilot valve VSNC 	Festo			•			•
Linear actuator DLP 	Festo			•			•
Valve terminal MPA 	Festo						•
Valve terminal VTSA 	Festo						•
Valve terminal CPV 	Festo						•
Sensor box SRBC 	Festo			•			•
Sensor box SRBE 	Festo			•			•
Sensor box SRBG 	Festo			•			•

[1] Redundant arrangement of two or more simple devices (in accordance with IEC 61508) to implement a hardware fault tolerance of >0 in a safety-related system.

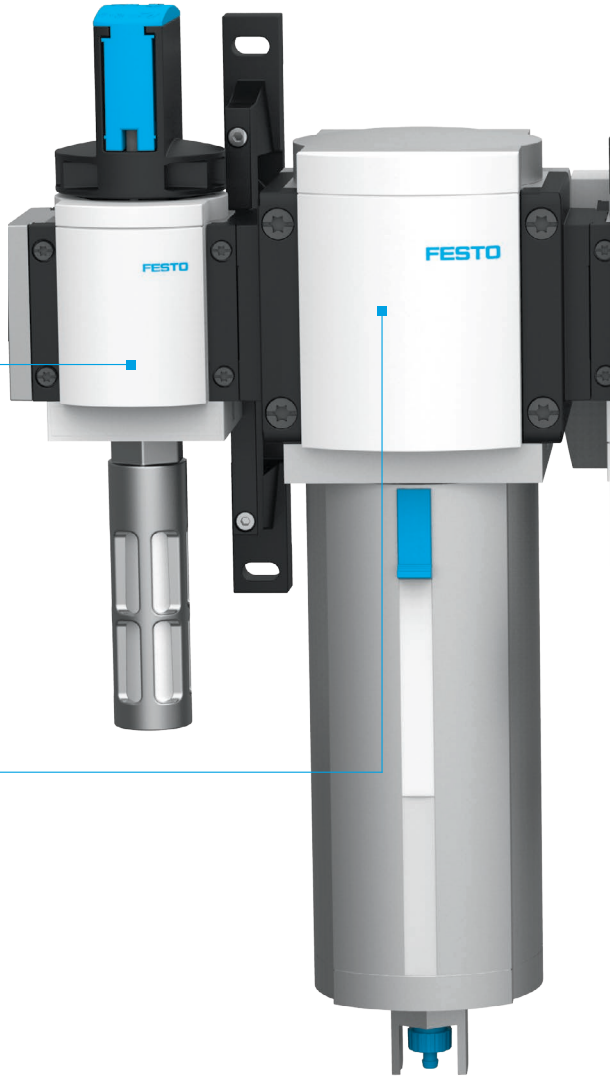
Single-channel interconnection					
Low demand			High demand		
Up to SIL 1	Up to SIL 2	Up to SIL 3	Up to SIL 1	Up to SIL 2	Up to SIL 3
	•			•	
	•			•	
	•			•	
	•			•	
	•			•	
				•	
				•	
				•	
	•			•	
	•			•	
	•			•	

Safety@Festo with MS

The MS series offers a wide range of highly functional components and various services for compressed air preparation. These components and services will help you on your route to a safe machine. Your application will determine which solution you should choose, from individual components and ready-to-install combinations to integrated safety engineering with certified safety devices. All the relevant functions of compressed air preparation are represented.

The benefits of a safety-relevant application:
- All relevant functions are available in various sizes to suit your application
- Integrated sensors and safety functions, also with the MS-SV:
  Fast and reliable exhausting of systems up to PL e
  (certified to ISO 13849-1) with integrated soft-start function

The image shows the most important functions for functional safety and their effect on safety functions:



Manual on/off valve (MS-EM1)

Application:
Manually disconnecting and exhausting the compressed air supply

Note:
LOTO applications (lockout-tagout), protection against unexpected start-up (PUS)

Compressed air filter with water/oil separating function (MS-LF)

Application:
Removing particles, oil and water from the compressed air

Note:
Measures against common cause failure (CCF) by filtering the pressure medium, preventing contamination and draining compressed air

Pressure regulation (MSE6-C2M / MS-LR)

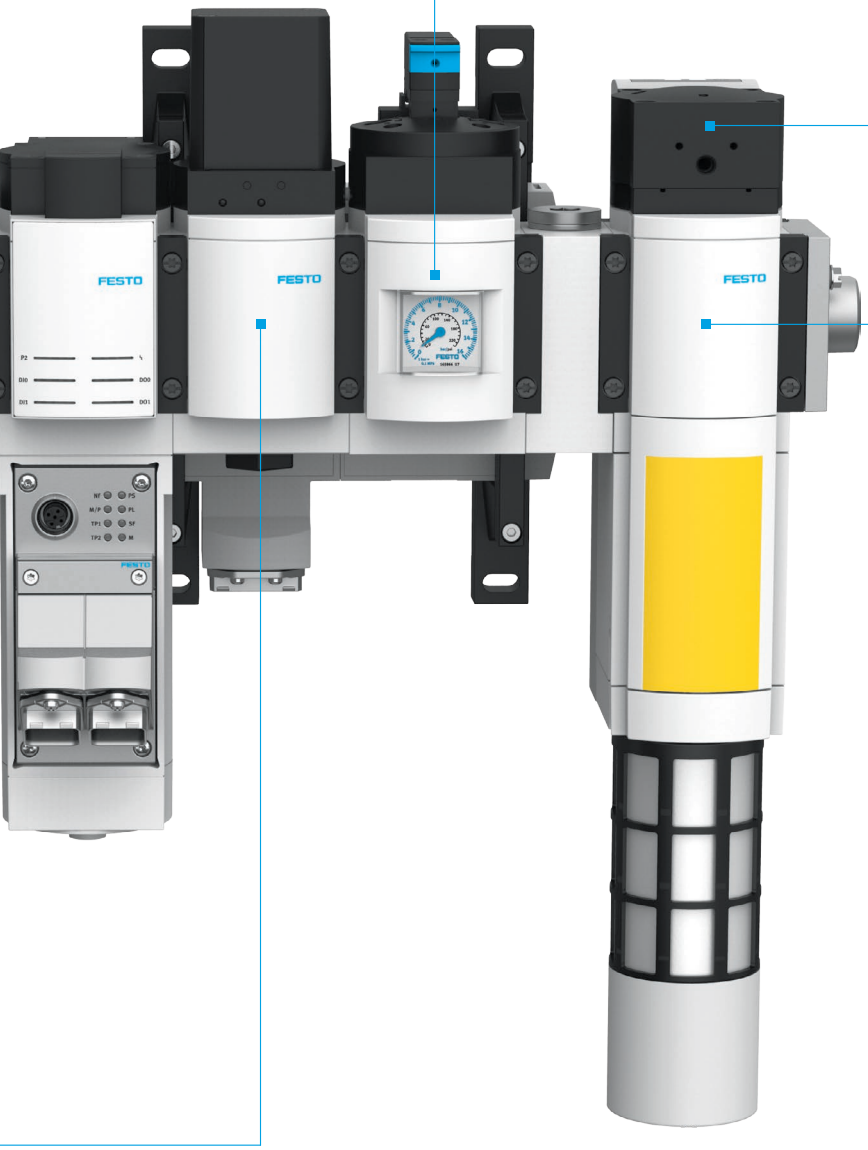
Application:
Regulating specified operating pressure

Note:
Measures against common cause failure (CCF), protection against overpressure and protection against tampering with a lockable rotary knob or electronic adjustment

Pressure measurement / flow rate measurement / pressure indicator
(MSE6-C2M / SPAU / SFAM)

Application:
Monitoring and detecting critical limit violations

Note:
Preventing systematic faults by detecting error states, checking the pressure is disconnected



Safe venting of the system (MS6-SV-E)

Application:
Quick exhausting of the system and de-energising it to the safe state

Note:
Certified safety device for safe de-energization (SDE) and protection against unexpected start-up (PUS) category 4, PL e

MS6-SV-D

Like MS6-SV-E, but in category 3, PL d.
Ideal for manufacturers of series-produced machines with high safety requirements up to PL e.
In contrast to the MS6-SV-E, appropriate programming is required on the safety PLC.

MS6-SV-C
Like MS6-SV-E, but in category 1, PL c.

Ideal for applications with medium safety requirements up to PL c.
The single-channel design ensures safe, fast exhausting – and is very cost-effective as well.

Pressurisation (soft-start) (MS6-SV)

Application:
Controlled gradual pressurisation

Note:
The gradual pressurisation protects unexpected sudden movements in the start-up phase and preserves the mechanical components.

Safety@Festo with the valve terminal CPX/VTSA-F

The valve terminal CPX/VTSA-F offers the following functions that could help with machine safety issues:

- Pilot air switching valve for exhausting duct 14, with integrated proximity sensor or external pressure switch
- Soft-start valve for exhausting duct 1, with integrated proximity sensor or external pressure switch
- Valves with switching position sensing of the normal position
- Integration of the VOFA control block for implementing the safe direction (SDI)
- Combination with safe input and output modules on the CPX
- Internal switch-off of the power supply to the valves with the CPX-PROFIsafe module
- Any pressure zones (including disconnection of duct 14) and compressed air supply possible

Soft-start/quick exhaust valve (VABF-S6-1-P5A4-G12-4-1-P)

Application:
The pressure for the pressure zone used is gradually built up to bring the valves and drives into a specific state.
The pressure zone is exhausted in line with the requirement of the safety sub-function SDE, and the drives are thus switched to unpowered depending on the valve type. This also prevents an unexpected start-up.

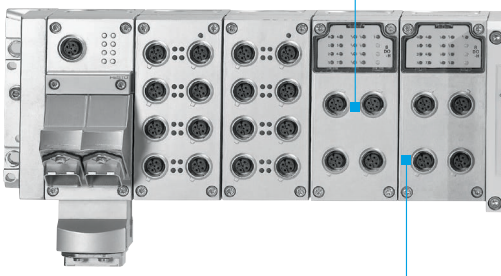
Note:
Suitable for
- Safe energization (SEZ)
- Safe de-energization (SDE)
- Prevention of unexpected start-up (PUS)

In single-channel architectures up to PL c

Safe inputs (CPX-F8DE-P)

Application:
4 safe inputs for integrating sensors with OSSD signal or potential-free contact. Easy configuration of operating modes.

Note:
Reliable detection and evaluation of input statuses up to category 4, PL e / SIL 3



Safe outputs (CPX-FVDA-P2)

Application:
Safe switch-off of the supply voltage to the valves. There are also 2 safe external outputs that are ideal for safely connecting external devices such as valves or other valve terminals. With this module, valves that are located on and connected to the valve terminal are not negatively affected by the test pulses. This prevents a reduction of the service life and prevents the test pulses from causing the valves to switch.

Note:
Safe switch-off category 3, PL e / SIL 3

Pilot air switching valve (VSVA-B-M52-MZD-xx-1T1L-APP)

Application:
If the pilot air switching valve is switched to the normal position (switched off) – here with the help of the safe electrical zone – the piloted double solenoid valves remain in the switching position occupied while the piloted single solenoid valves are switched to the normal position and remain there.

Note:
In combination with the safe electrical zone (CPX-FVDA-P2), the application is suitable for preventing an unexpected start-up (PUS) up to PL e. For use in an electrical zone that is not safe, the application is suitable for preventing an unexpected an unexpected start-up (PUS) up to PL c.

5/2 valves double solenoid (VSVA-B-B52-...)

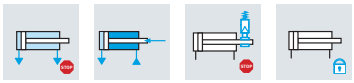
Application:
The double solenoid valves remain in the switching position last occupied when switched off. However, when the connected drive is supplied with working air and is pressurised, a workpiece can be clamped or the position can be maintained.

Note:
Without electrical control, suitable for[1]:
- Prevention of unexpected start-up (PUS)

If the switching position last occupied is the safe position, other safety sub-functions can be implemented.

[1]Depending on the valve type and pneumatic drive, one or more safety sub-functions can be achieved in single-channel architectures up to PL c and in two-channel architectures with additional components up to PL e. The requirements to achieve the performance levels in accordance with ISO 13849 must be fulfilled.

5/2 and 3/2 valves, single solenoid
(VSVA-B-M52-..., VSVA-B-T32x-...)

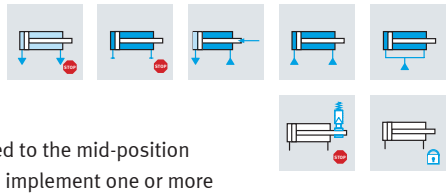


Application:
If the valves are switched to the normal position (switched off), they can then implement one or more safety sub-functions.

Note:
Without electrical control, suitable for[1]:
- Safe torque off (STO)
- Safe direction (SDI)
- Safe brake control (SBC)
- Prevention of unexpected start-up (PUS)

Without working air for normally open valves, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)

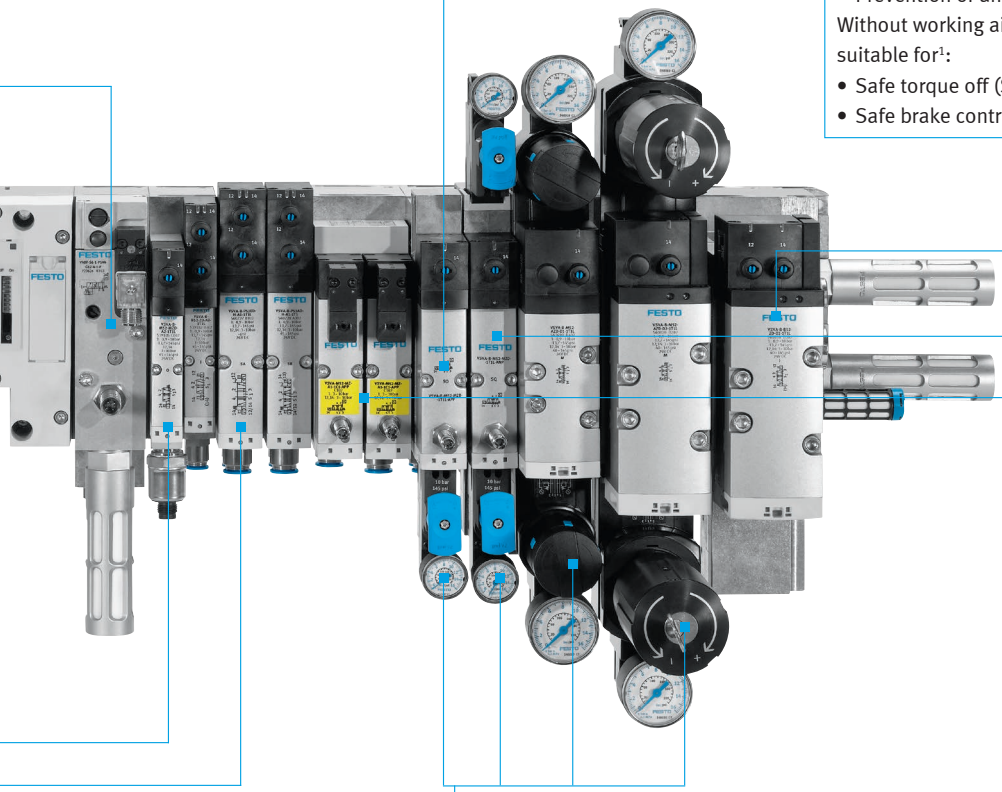
5/3 valves, single solenoid
(VSVA-B-P53C/E/U-...)



Application:
If the valves are switched to the mid-position (switched off), they can implement one or more safety sub-functions

Note:
Without electrical control, suitable for[1]:
- Safe torque off (STO)
- Safe stopping and closing (SSC)
- Safe direction (SDI)
- Safe operating stop (SOS)
- Safe equilibrium of torque (SET)
- Safe brake control (SBC)
- Prevention of unexpected start-up (PUS)

Without working air for mid-position exhausted/pressurised valves, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)



Valves with switching position monitoring
(VSVA-B-M52-...-APx/ANx)

Application:
By sensing the switching position, the normal position is monitored, thus enabling a high diagnostic coverage.

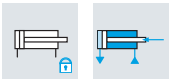
Note:
Diagnostic coverage of 99% to ISO 13849-1 can be achieved.

Vertical stacking
(VABF-Sx-...)

Application:
Other functional units can be added to the valve by using vertical stacking plates. This means that pressure regulation, pressure blocking and flow rate throttling can be combined with the valve function.

Advantage for safety application[1]:
- Safely limited speed (SLS)
- Safely limited torque (force) (SLT)
- Safe operating stop (SOS)
- Safe equilibrium of torque (SET)
- Lockout-tagout (LOTO), only with vertical shut-off valve VABF-S4-..-L1D2-C

Control block with safety function (VOFA-LS-T52-...)



Application:
To implement a safe reversing movement of a drive or a system part with a high degree of reliability. This is particularly interesting for press applications.

Note:
- Reversing a movement category 4, up to PL e
- Protection against tampering, prevention of unexpected start-up category 4, up to PL e

Safety@Festo with the valve terminal CPX/VTSA-F-CB

The valve terminal CPX/VTSA-F-CB is expanding the VTSA series to include the following additional machine safety functions:

- Flexible shutdown of up to 3 voltage zones in the CPX interfaces, either internally with PROFIsafe or externally by 3x M12 (via safe outputs)
- Pilot air switching valve for exhausting duct 14, with integrated pressure sensor as well as integrated activation and feedback
- Soft-start valve for exhausting the duct, with integrated pressure sensor, activation and feedback
- Combination with safe input and output modules on the CPX (depending on configuration)
- Serial communication in the pneumatic part (similar to MPA-S)
- With max. 4 voltage zones for load voltage of the valves in the pneumatic part
- Any pressure zones (including disconnection of duct 14) and compressed air supply possible

Soft-start/quick exhaust valve
(VABF-S6-1-P5A4-...-1T5-PA)

Application:
The pressure for the pressure zone is gradually built up to bring the valves and drives into a specific state. The pressure zone is exhausted in line with the requirement of the safety sub-function SDE, and the drives are thus switched to unpowered depending on the valve type. This also prevents an unexpected start-up.

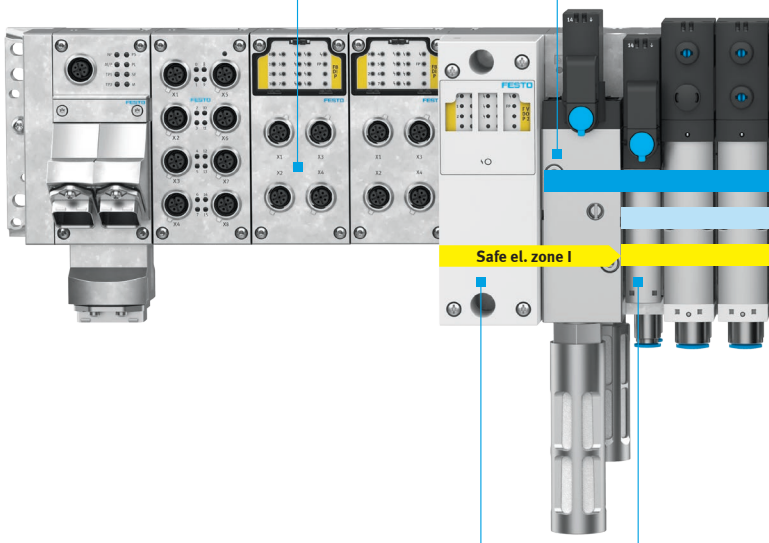
Note:
Suitable for
- Safe energization (SEZ)
- Safe de-energization (SDE)
- Protection against unexpected start-up (PUS)

In single-channel architectures up to PL c

Safe inputs (CPX-F8DE-P)

Application:
4 safe inputs for integrating sensors with OSSD signal or potential-free contact. Easy configuration of operating modes.

Note:
Reliable detection and evaluation of input statuses up to category 4, PL e / SIL 3



Interface with 3 safe electrical zones
(VABA-S6-1-X2-F1-CB)

Application:
Implementing an individual safety concept by creating safe electrical zones on the valve terminal for partially switching off the valves or activating a soft-start/quick exhaust valve. Safe switch-off of up to three valve terminal zones.

Note:
Safe switch-off category 3, PL e / SIL 3

VABA-S6-1-X2-F2-CB
Interface with 2 safe electrical zones and a safe external output
Ideal for the safe connection of an external device such as, for example, a valve or another valve terminal. In addition, 2 safe internal electrical zones can be implemented.

VABA-S6-1-X2-3V-CB
Interface via external safety controller to implement 3 safe electrical zones
Commercially available safety controllers can be used to realise 3 internal zones. Using your existing control architectures, you can thus safely control zones on the valve terminal.

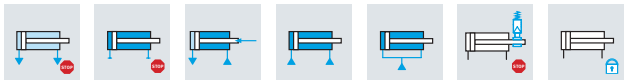
Pilot air switching valve (VSVA-BT-M32CS-...-A2-...)

Application:
If the pilot air switching valve is switched to the normal position (switched off), the piloted double solenoid valves remain in the switching position occupied while the piloted single solenoid valves are switched to the normal position and remain there.

Note:
In combination with the safe electrical zone (CPX-FVDA-P2), the application is suitable for preventing an unexpected start-up (PUS) up to PL e. For use in an electrical zone that is not safe, the application is suitable for preventing an unexpected an unexpected start-up (PUS) up to PL c.

[1]Depending on the valve type and pneumatic drive, one or more safety sub-functions can be achieved in single-channel architectures up to PL c and in two-channel architectures with additional components up to PL e. The requirements to achieve the performance levels in accordance with ISO 13849 must be fulfilled.

5/3 valves, single solenoid (VSVA-B-P53C/E/U-...)

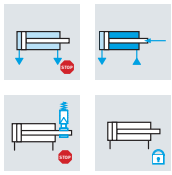


Application:
If the valves are switched to the normal position (switched off), they can then implement one or more safety sub-functions.

Note:
Without electrical control, suitable for[1]:
- Safe torque off (STO)
- Safe stopping and closing (SSC)
- Safe direction (SDI)
- Safe operating stop (SOS)
- Safe equilibrium of torque (SET)
- Safe brake control (SBC)
- Prevention of unexpected start-up (PUS)

Without working air for mid-position exhausted/pressurised valves, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)

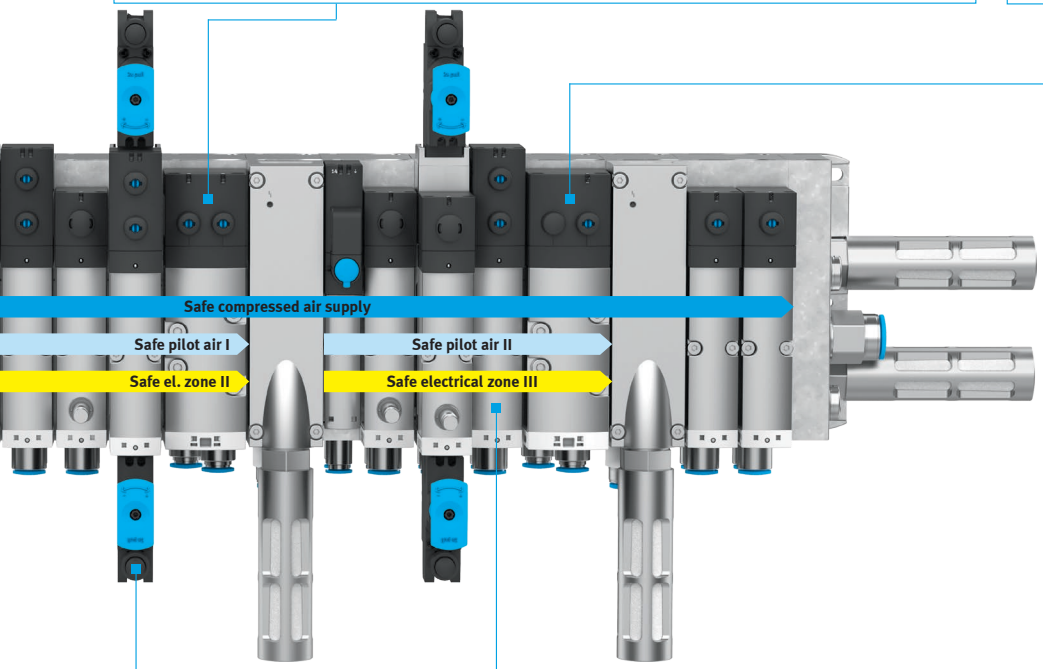
5/2 and 3/2 valves, single solenoid (VSVA-B-M52-..., VSVA-B-T32x-...)



Application:
If the valves are switched to the normal position (switched off), they can then implement one or more safety sub-functions.

Note:
Without electrical control, suitable for[1]:
- Safe torque off (STO)
- Safe direction (SDI)
- Safe brake control (SBC)
- Prevention of unexpected start-up (PUS)

Without working air for normally open valves, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)



Vertical stacking (VABF-Sx-...)

Application:
Other functional units can be added to the valve by using vertical stacking plates. This means that pressure regulation, pressure blocking and flow rate throttling can be combined with the valve function.

Advantage for safety application[1]:
- Safely limited speed (SLS)
- Safely limited torque (force) (SLT)
- Safe operating stop (SOS)
- Safe equilibrium of torque (SET)
- Lockout-tagout (LOTO), only with vertical shut-off valve VABF-S4-..-L1D2-C

5/2 valves double solenoid (VSVA-B-B52-...)

Application:
The double solenoid valves remain in the switching position last occupied when switched off. However, when the connected drive is supplied with working air and is pressurised, a workpiece can be clamped or the position can be maintained.

Note:
Without electrical control, suitable for[1]:
- Protection against unexpected start-up (PUS)

If the switching position last occupied is the safe position, other safety sub-functions can be implemented.

Safety@Festo with the valve terminal MPA-S

MPA-S is a modular valve system with sub-base valves and has the following characteristics in terms of machine safety:

- Any pressure zones and compressed air supply are possible
- Flexible switch-off of the power supply to internal valves with the CPX-PROFIsafe module
- Limitation of the drive speed with fixed flow restrictor

5/2 valves, double solenoid
(VMPAx-M1H-J-..., VMPAx-M1H-F-...)

Application:
The double solenoid valves remain in the switching position last occupied when switched off. However, when the connected drive is supplied with working air and is pressurised, a workpiece can be clamped or the position can be maintained.

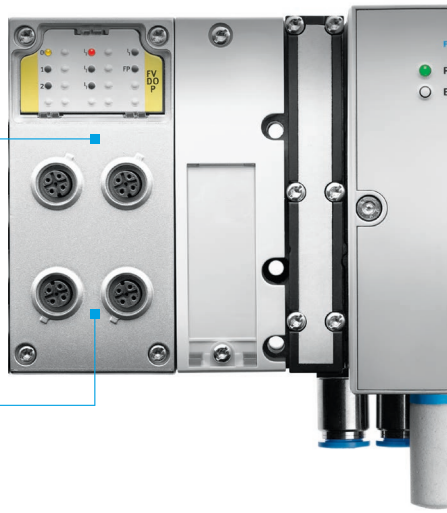
Note:
Without electrical control, suitable for[1]:
- Protection against unexpected start-up (PUS)

If the switching position last occupied is the safe position, other safety sub-functions can be implemented.

Safe inputs (CPX-F8DE-P)

Application:
4 safe inputs for integrating sensors with OSSD signal or potential-free contact. Easy configuration of operating modes.

Note:
Reliable detection and evaluation of input statuses up to category 4, PL e / SIL 3



Safe outputs (CPX-FVDA-P2)

Application:
Safe switch-off of the supply voltage to the valves. There are also 2 safe external outputs that are ideal for safely connecting external devices such as valves or other valve terminals.
With this module, valves that are located on and connected to the valve terminal are not negatively affected by the test pulses. This prevents a reduction of the service life and prevents the test pulses from causing the valves to switch.

Note:
Safe switch-off category 3, PL e / SIL 3

5/2 and 3/2 valves, single solenoid
(VMPAx-M1H-M/MS /K/KS/N/NS/ H/HS/X/W...)

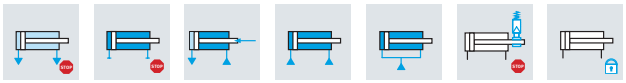
Application:
If the valves are switched to the normal position (switched off), they can then implement one or more safety sub-functions.

Note:
Without electrical control, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)
- Prevention of unexpected start-up (PUS)

Without working air for normally open valves, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)

[1]Depending on the valve type and pneumatic drive, one or more safety sub-functions can be achieved in single-channel architectures up to PL c and in two-channel architectures with additional components up to PL e. The requirements to achieve the performance levels in accordance with ISO 13849 must be fulfilled.

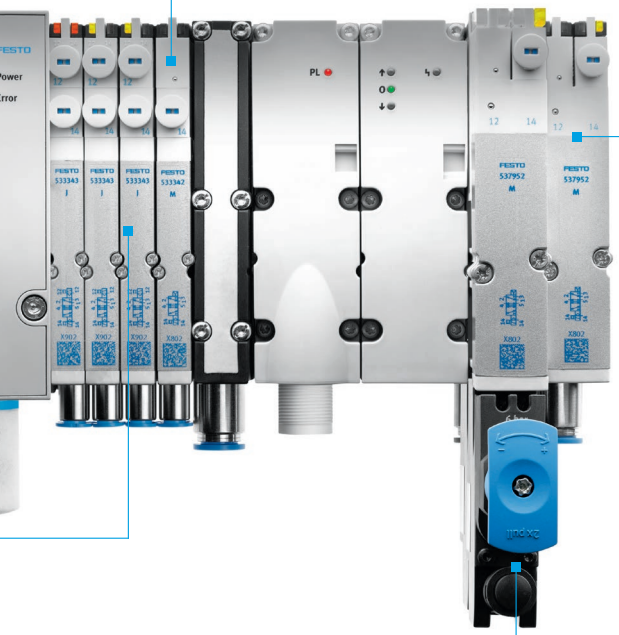
5/3 valves, single solenoid
(VMPAx-M1H-G/B/E...)



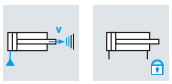
Application:
If the valves are switched to the normal position (switched off), they can then implement one or more safety sub-functions.

Note:
Without electrical control, suitable for[1]:
- Safe torque off (STO)
- Safe stopping and closing (SSC)
- Safe direction (SDI)
- Safe operating stop (SOS)
- Safe equilibrium of torque (SET)
- Safe brake control (SBC)
- Prevention of unexpected start-up (PUS)

Without working air for valves with mid-position exhausted/pressurised, suitable for[1]:
- Safe torque off (STO)
- Safe brake control (SBC)



Fixed flow restrictors
(VMPAx-B8/HS)



Application:
The exhaust air flow rate can be regulated using a fixed flow restrictor in order to limit the drive speed.

Note:
Depending on the evaluation, a safely limited speed (SLS) can be achieved.

Vertical stacking
(VMPAx-B8/HS)

Application:
Other functional units can be added to the valve by using vertical stacking plates. This means that pressure regulation, pressure blocking and flow rate throttling can be combined with the valve function.

Advantage for safety applications[1]:
- Safely limited torque (force) (SLT)
- Safe operating stop (SOS)
- Safe equilibrium of torque (SET)
- Lockout-tagout (LOTO), only with vertical pressure shut-off plate VMPA..-HS

Safety@Festo with CMMT

Safe brake control (SBC)

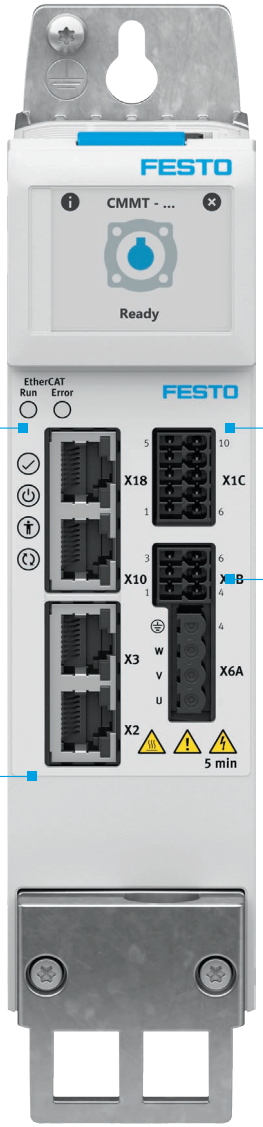
Application:
Safe control of the motor brake and/or clamping unit of the axis

Note:
Safe brake control (SBC), up to category 3, PL e / SIL 3 / SILCL 3

Safe stop 1 (SS1)

Application:
Initiating a brake ramp using an external controller with subsequent torque release within an externally definable time

Note:
Control of the CMMP within a defined time period with safe torque off (STO) category 4, PL e / SIL 3 / SILCL 3



Safe brake test (SBT)

Application:
The brakes can be tested with external programming and should be carried out at regular intervals

Note:
Diagnostics of the brake function using an external controller

Safe torque off (STO)

Application:
Safely releasing the torque of a drive and switching the system to the safe state

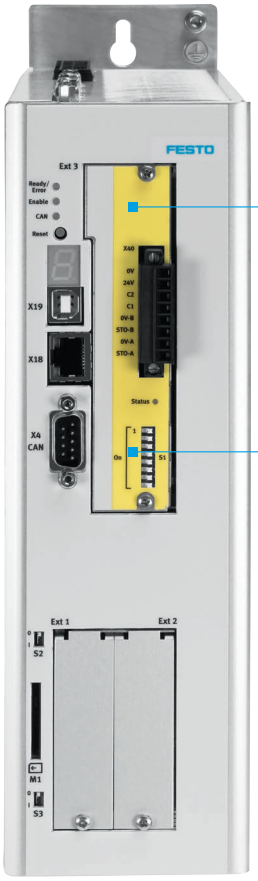
Note:
Safe torque off (STO) category 4, PL e / SIL 3 / SILCL 3

Standard safety

Safe torque off (STO)

Application:
Safely releasing the torque of a drive and switching the system to the safe state

Note:
Safe torque off (STO) category 4, PL e / SIL 3



Safe stop 1 (SS1)

Application:
Initiating a brake ramp with subsequent torque release within an externally definable time

Note:
Safe torque off (STO) category 4, PL e / SIL 3

Advanced safety

Safe speed range (SSR)

Application:
Only permits a speed within a specific range

Note:
Safe speed range (SSR) up to category 4, PL e / SIL 3

Safe brake test (SBT)

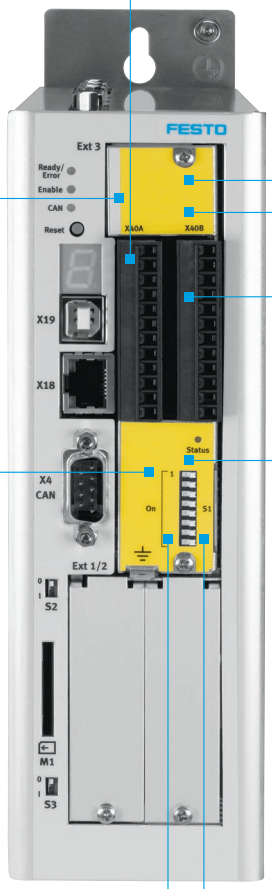
Application:
The brakes can be tested with external programming and should be carried out at regular intervals

Note:
Validation of the safe brake activation with an external safety controller

Safe stop 2 (SS2)

Application:
Initiating a brake ramp with subsequent safe and energised holding of the end position

Note:
Safe stop 2 (SS2) up to category 4, PL e / SIL 3



Safe brake control (SBC)

Application:
Safe activation of the motor brake and/or clamping unit of the axis.

Note:
Safe brake control (SBC) up to category 4, PL e / SIL 3

Safe operating stop (SOS)

Application:
Safely holding a position

Note:
Safe operating stop (SOS) / up to category 4, PL e/ SIL 3

Safely limited speed (SLS)

Application:
Keeps the speed within a specific range

Note:
Safely limited speed (SLS) up to category 4, PL e / SIL 3

Safe speed monitor (SSM)

Application:
Emits a safe signal when the specified speed range is not observed.

Note:
Safe speed monitor (SSM) up to category 4, PL e / SIL 3

Ready-to-install solutions for your safety-related systems

On the basis of your requirements, we will put together complete, ready-to-install solutions for use in safety circuits.
We will provide you with a description and documentation of the solution, e.g. a process valve unit, in line with IEC 61508 and IEC 61511-1.
This will save costly assembly and calculation work and you will receive tested complete solutions from a single source.

Sensor box SRBC

For the electronic and visual position indication of automated process valves in safety-related systems up to SIL2 for low-demand and high-demand applications.

- Housing protection IP67/NEMA 4/4X
- Type of ignition protection: Ex i
- Explosion protection to ATEX: II 2G c X / II 2D c X
- cCSAus: ordinary location
- Operating conditions: indoors/outdoors

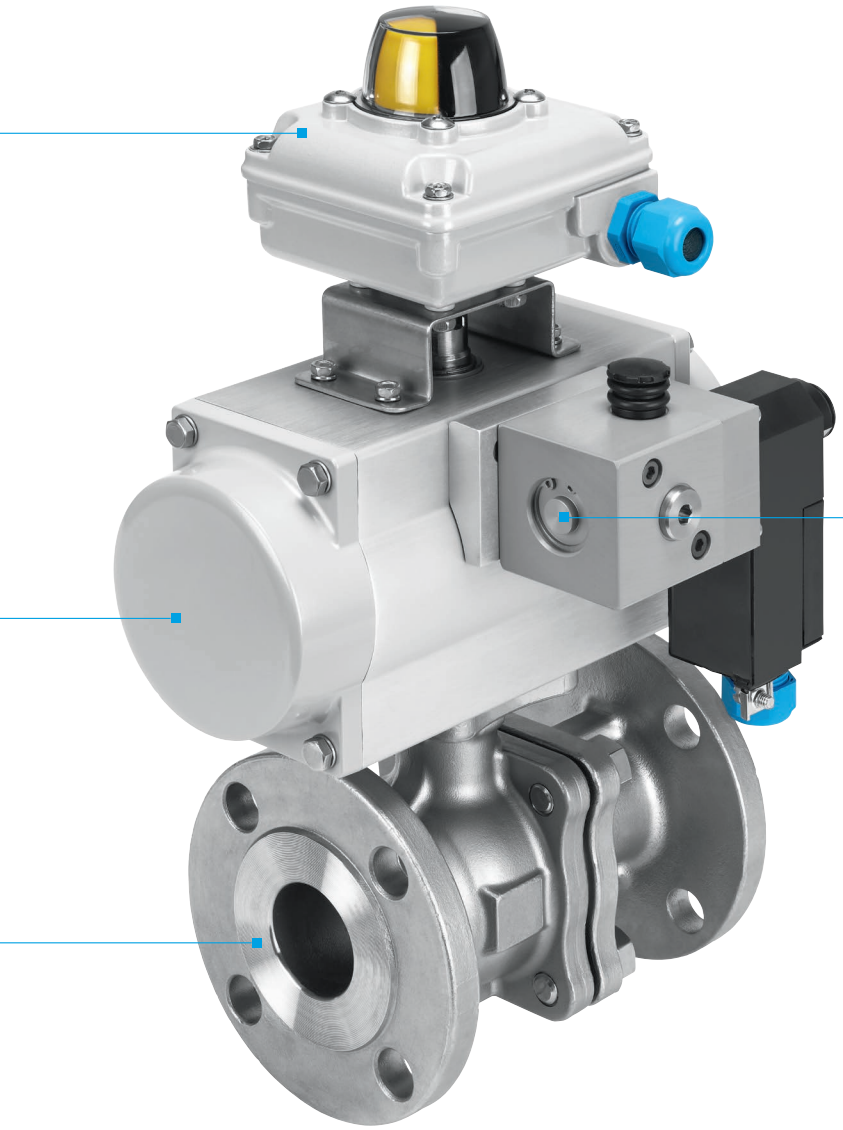
Quarter turn actuator DFPD

Double- and single-acting for activating process valves in safety-related systems up to SIL3 in a redundant design or to SIL2 in single-channel design in low demand and high demand applications.

- Temperature range: –50 ... + 150 °C
- Explosion protection to ATEX: II 2G c T4 X / II 2 D c 125 °C X
- Rotation angle up to 180°
- Surface finish: stainless steel shaft, housing with epoxy coating

Process valve based on your requirements

Selecting the right process valve can vary depending on the application.
You will be provided with several process valves or we will integrate the process valves into the system in line with your specifications. The valve must be SIL-certified and the values needed for the SIL calculation must be available.



Pilot valves VOFC

For safety-related systems up to SIL3 in redundant circuits or up to SIL2 in single-channel circuits for low demand, high demand and ESD (Emergency Shut Down) applications.

- Design principle: pilot operated
- Explosion protection to IEC Ex: EPL Gb/ EPL Db
- Explosion protection to ATEX: II 2 G / II 2 D
- Types of ignition protection for solenoid coils: Ex i, Ex me, AEx-m
- IP65 housing protection
- Surface finish: aluminium (Ematal coated) – stainless steel
- Operating conditions: indoors/outdoors

We will provide you with a ready-to-install unit, tailored to your requirements and including a declaration that confirms the suitability for use in safety-related systems in line with IEC 61508

FESTO

Declaration

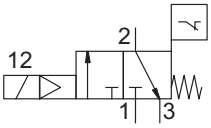
Supplement to the product catalogue with special solutions for safety-related applications

On the following pages you will find additions to to our standard product catalogue for safety-related applications.
If you have any questions about additions or modifications to our products, please do not hesitate to contact us. We will be happy to help.

On/off valve, MS series, with piston position monitoring

Function
Solenoid actuated on/off valve for pressurising and exhausting pneumatic systems
Contactless switching position sensing for SMT-8M-A

Circuit symbol



Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	Switching position sensing
Ducts	1
Safety device in accordance with EC MD 2006/42/EC	No

Part no.	Type
8028347	MS4-EE-1/4-10V24-S-CS
8028348	MS4-EE-1/4-V24-S-CS
1627966	MS6-EE-1/2-10V24-S-SA
2649234	MS6-EE-1/2-V24-S-SA

All specified values are maximum values that can be achieved by operating the component correctly.

On/off valve HEE with switching position monitoring

Technical data

Voltage
24 V DC

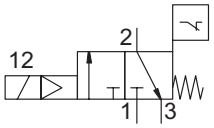
Operating pressure
2.5 ... 16 bar

Temperature range
-10 ... +60 °C

Function

For sensing the piston position of the on/off valve, standard sensors with reed contacts can be used for the T-slot: type SME-8M, SMT-8M, SME-8, SMT-8

Circuit symbol



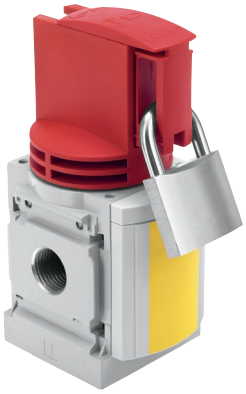
Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	Switching position sensing
Ducts	1
Safety device in accordance with EC MD 2006/42/EC	No

Part no.	Type
533537	HEE-D-MIDI-...-SA207225
548535	HEE-D-MAXI-...-SA217173

All specified values are maximum values that can be achieved by operating the component correctly.

Supplement to the product catalogue with special solutions for safety-related applications

Manual on/off valve MS with red rotary knob



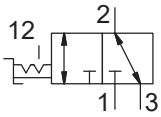
Technical data

Temperature range
-10 ... 60 °C

Function

The purpose of the manual on/off valve is to pressurise and exhaust pneumatic systems. When the valve is closed, the rotary knob can be secured with a padlock. This function can be used to implement the Lockout-tagout (LOTO) principle.

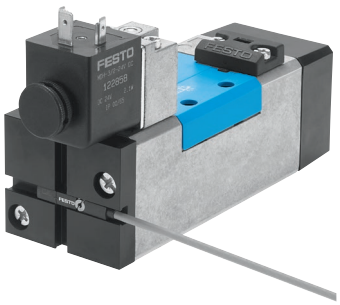
Circuit symbol



Part no.	Type
571429	MS6-EM1-1/2-R-SA-241043C
1542176	MS9-EM-G-VS-R-SA-244130A
571521	MS12-EM-G-GR-SA-242625A

All specified values are maximum values that can be achieved by operating the component correctly.

Valve MDH with switching position monitoring



Technical data

Voltage
24 V DC

Pressure
3 ... 10 bar

Temperature range
-10 ... +50 °C

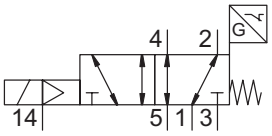
Flow rate
1200 ... 4500 l/min

Function

- The position of the piston spool is monitored directly
- Monitors position, not pressure
- Suitable for circuits with a higher diagnostic coverage
- Suitable for higher category circuits to ISO 13849-1
- Standard sensors with reed contacts can be used for a T-slot: Type SME-8M, SME-8
- Contactless switching output or via reed contacts

Please note: sensors must be ordered separately

Circuit symbol



Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	Switching position sensing
Ducts	1
Safety device in accordance with EC MD 2006/42/EC	No

Order code

Part no.	Type
185994	MDH-5/2-D1-FR-S-C-A-SA27102
188005	MDH-5/2-D2-FR-S-C-A-SA23711
188006	MDH-5/2-D3-FR-S-C-A-SA23712

All specified values are maximum values that can be achieved by operating the component correctly.

Supplement to the product catalogue with special solutions for safety-related applications

Dual-pressure regulator

Technical data

Output pressure P2
0.5 ... 7 bar

Supply pressure P1
1.5 ... 10 bar

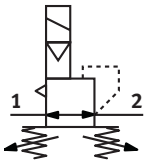
Flow rate
up to 1300 l/min

Temperature range
-10 ... +60 °C

Function

Diaphragm pressure regulator with two secondary exhausts for setting 2 different initial pressures in one device. Switching between the two values is done electrically.

Circuit symbol



	
Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	
CCF	
Ducts	1
Safety device in accordance with EC MD 2006/42/EC	No

Part no.	Type
550588	LR-D-MINI-ZD-V24-SA
567841	LR-D-MINI-ZD-V24-UK-SA

All specified values are maximum values that can be achieved by operating the component correctly.

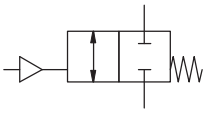
Stop valve

Technical data

Operating pressure
0 ... 10 bar

Temperature range
-20 ... 80 °C

Circuit symbol



Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	
CCF	
Ducts	1
Safety device in accordance with EC MD 2006/42/EC	No

Part no.	Type
25025	VL-2-1/4-SA

All specified values are maximum values that can be achieved by operating the component correctly.

Supplement to the product catalogue with special solutions for safety-related applications

Piloted check valve HGL, red anodised

Image in grey scales

Technical data

Operating pressure
0.5 ... 10 bar

Pilot pressure
2 ... 10 bar

Temperature range
-10 ... 60 °C

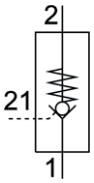
Description

This specially designated valve complies with the following requirement in DIN EN 12100:
6.2.10 pneumatic and hydraulic hazards
... all components that remain pressurised after the machine has been disconnected from the power supply must have clearly identifiable discharge mechanisms and a warning label referring to the need to relieve the pressure relief for these parts before setup or maintenance work can be carried out on the machine. ....
This is not a safety device

Function

The piloted check valve is suitable for brief positioning and braking functions in pneumatic drives.

Circuit symbol



	
Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	
CCF	
Ducts	1
Safety device in accordance with EC MD 2006/42/EC	No

Part no.	Type
4516340	HGL-1/2-B-CS
4516338	HGL-3/8-B-CS
4516324	HGL-1/4-B-CS
4512517	HGL-1/8-1/8-B-CS

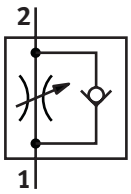
All specified values are maximum values that can be achieved by operating the component correctly.

Tamper-proof one-way flow control valve GRLA

Function

- Setting a specified flow rate
- Secured with a spring pin against unauthorised adjustment of the flow rate

Circuit symbol



Cat.	Can be used in systems of a higher category with additional measures
PL	
DC	
CCF	
Ducts	1
Safety component in accordance with EC MD 2006/42/EG	No

Part no.	Type
539717	GRLA-M5-B-SA
539661	GRLA-1/8-B-SA
539662	GRLA-1/4-B-SA
539715	GRLA-3/8-B-SA
539716	GRLA-1/2-B-SA
539714	GRLA-3/4-B-SA

All specified values are maximum values that can be achieved by operating the component correctly.

What must be taken into account when using Festo products?

The limit values specified in the technical data and any specific safety instructions must be adhered to by the user in order to comply with the intended use.

When using pneumatic components, ensure that they are operated using correctly prepared compressed air without aggressive media and that they comply with environmental specifications (e.g. climate). These can be found in the catalogue data sheet and in the general conditions of use.

The relevant national regulations, directives and applicable standards as well as occupational health and safety laws must always be adhered to when using Festo products in safety-related applications.

Unauthorised conversions or modifications to products and systems from Festo constitute a safety risk and are thus not permitted. Festo does not accept any liability for the resulting damages.

You should contact Festo if one of the following applies to your application:
- The ambient conditions and conditions of use or the operating medium differ from the specified technical data.
- The product is to perform a safety function.
- A risk or safety analysis is required.

All technical data is correct at the time of going to print.

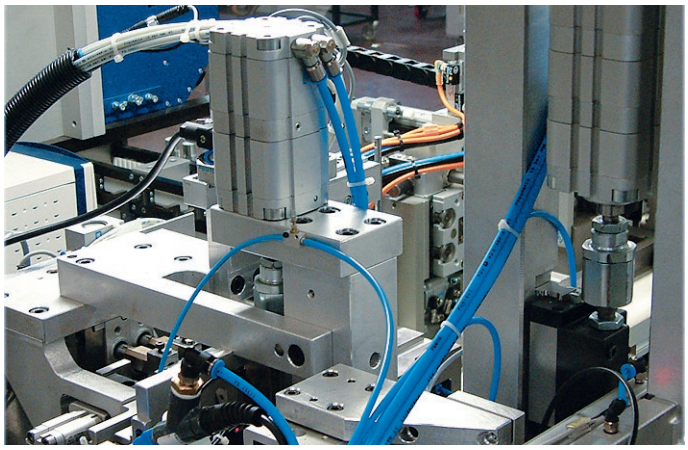
05 Your competency with our training

Competency in safety engineering

Competencies in safety engineering from Festo Training and Consulting expand your knowledge, enable innovation and ensure safety when planning and implementing your solutions. You will also benefit from the experience of the trainers and other course participants and you will be given ample food for thought.
The range of courses is a result of our efforts to address the current issues and to comply with legal regulations, while simultaneously focusing on market developments. Against this background, we have also developed our training and further training packages for safety engineering.

Contents

Safety-related pneumatics – practical course



Safety in machine building covers a range of technologies.
Everyone is familiar with the function of safe electrics, but how do safe pneumatics work in combination with electrics?
This practical course with many two-channel circuits provides an opportunity to understand this interaction. Programmable and non-programmable safety relay units are used.

Content
- Control system categories in accordance with ISO 13849-1
- Stop categories in accordance with EN 60204-1
- Diagnostic options in pneumatics and electropneumatics
- Failure characteristics of safety-related circuits
- Electronic and contact-based safety relay units
- Interaction in the safety chain
- Safety circuits
  - Switching to unpowered, braking, stopping, reversing
  - Unexpected start-up
  - Pressurisation and start-up of a machine
  - Function and testing of holding and service brakes
- Two-hand control devices
- External pilot exhaust air and double pilot valves
- Slowing-down path for light barriers
- Finding and eliminating faults

Requirements
Basics of pneumatic and electropneumatics as per our course

Course objectives
After this course, participants will be able to build and commission various two-channel electropneumatic circuits and eliminate faults. They will understand the cross-technology interaction of pneumatics and electrics as well as the meaning and function of diagnostics in pneumatic circuits.

Note
This training can also be tailored to your company and be carried out at the company's premises.

Duration
4 days

Dates and other information
www.festo-didactic.com

Machinery Directive 2006/42/EC – Building, acceptance-testing and operating machines

Legislation places the responsibility for machine/system safety on both the machine builder and the machine operator. The legal requirements of European guidelines are described in the Product Safety Act (ProdSG) and the new Industrial Safety Regulation (BetrSichV) dated 1 June 2015 and are implemented in national legislation.
What are the requirements of these laws and what kind of freedoms do they offer?
If all those concerned are aware of the terms, responsibilities and processes, this provides a good basis for cost savings.

Content
- European directives
- EC Machinery Directive – Operational safety regulation
- Responsibilities of machine suppliers, manufacturers and operators
- Performance specifications and technical specifications
- Participants
- Acceptance test criteria
- Limits of the machine
- Basic changes

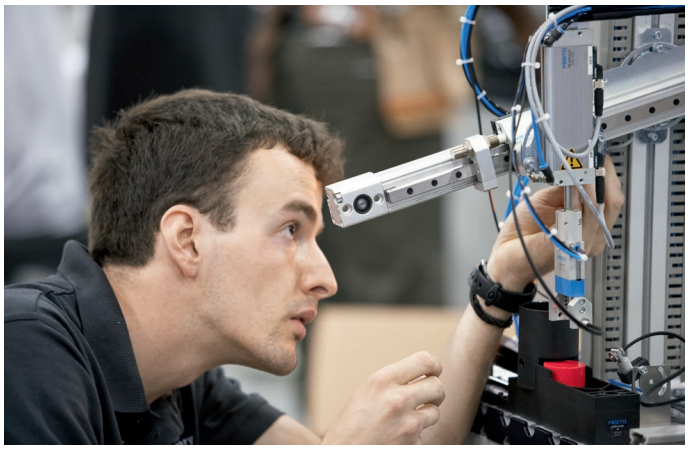
Course objectives
After this course, participants will understand the meaning of the EC Machinery Directive and the consequences of not complying with it. They will be aware of the responsibility of the manufacturers and operators as well as the protective measures required.

Note
This training can also be tailored to your company and be carried out at the company's premises.

Duration
1 day

Dates and other information
www.festo-didactic.com

Safety in pneumatics and electropneumatics for design engineers



Safe pneumatic and electropneumatic circuits can be easy if you know how they work. Switching off the power does not always solve everything; other functions offer many opportunities to make a machine safe and thus gain cycle time.
Carrying out diagnostics of pneumatic components enables safety circuits up to control category 4. Validation and fault analysis are also part and parcel of safety-related circuits.

Content
- Design and function of safety-related circuits in accordance with ISO 13849-1
- Identifying the safety categories of circuits
- Selecting spare parts
- Power failure and restore
- Reliable pressurising and exhausting
- Safe opening of brakes and clamps
- Basic and well-tried safety principles of pneumatics in accordance with ISO 13849-2
- Selected protective measures of safety-related pneumatics: stopping/ blocking, reversing, pneumatic stopping and two-hand control devices
- Fault analysis and exclusion according to ISO 13849-2
- Effect of tube length, diameter and fittings on the speed of cylinders
- Note on operating instructions and maintenance

Course objectives
After this course, participants will understand the connection between pneumatic and electric components, be able to evaluate the behaviour of pneumatic drives and will be able to design safety circuits up to control category 4.

Note
This training can also be tailored to your company and be carried out at the company's premises.

Duration
2 days

Dates and other information
www.festo-didactic.com

Calculating safety circuits in accordance with ISO 13849-1 with the SISTEMA software

It is one thing to determine the performance level in accordance with ISO 13849-1. Calculating this with the SISTEMA software, however, is another. Which components installed in the machine are part of my safety chain?
How do I get a complex machine into the software?
What does a multi-technology safety chain look like?
Are there ways to make my work easier?
These questions are answered during the course.

Content
- Risk assessment according to ISO 13849-1
- Changes to the old standards and the simplified procedure
- Terms used in the standard
  - Performance level (PL)
  - Probability of failure per hour (PFH)
  - Mean time to failure (MTTF)
  - Characteristic service life values (B_{10})
  - Diagnostic coverage (DC)
  - Common cause failure (CCF)
- Safety functions and control categories
- Determining the components in the safety chain
- Calculating with complex structures
- Calculating with safety components and fault exclusion
- Creating your own libraries
- Practical exercises with the software SISTEMA Version 2

Course objectives
This course will enable participants to specify the components in a safety circuit and calculate the performance level of this circuit using the SISTEMA software. They will be able to understand the qualitative aspect of ISO 13849-1.

Note
This training can also be tailored to your company and be carried out at the company's premises.

Duration
2 days

Dates and other information
www.festo-didactic.com

Risk assessment and safe mechanical design

Safe mechanical design provides the basis for machine safety. This is where the potential to build a safe and economically efficient machine is at its greatest.
What does the legislation stipulate and what kind of solutions are offered by these standards?
Of central importance is ISO 12100, which describes the procedure for risk reduction and formulates the requirements for technical systems.

Content

- Risk assessment and risk reduction in accordance with ISO 12100
  - Risk assessment
  - Identification of hazards
  - Risk estimation
  - Risk assessment
  - Risk reduction
  - Documentation on risk assessment and risk reduction
- Structure of the body of standards
- Standards on safe mechanical design
- Basic and well-tried safety principles of mechanics
- Prevention of shear, clamp and crushing hazards and other mechanical hazards
- Operating mode and design of work processes
- Selection of protective devices
- Prevention of tampering

Course objectives

After this course, participants will be able to carry out a risk assessment and risk reduction in accordance with ISO 12100. They will be familiar with all the relevant standards and have the knowledge needed for the safe mechanical design of a machine, and will be familiar with how to successfully implement this.

Note

This training can also be tailored to your company and be carried out at the company's premises.

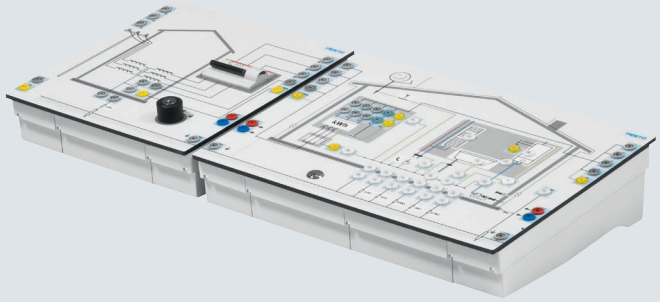
Duration

2 days

Dates and other information

www.festo-didactic.com

Equipment set TP 1110 – Electrical protective measures (for metalworking occupations)



Creating an awareness of hazards!

The aim of protective measures is to protect people and machines from harm.
Special rules must be followed when dealing with electrical energy, because electrical energy is recognisable only by its effects.
This training package provides an introduction to the topic of electrical protective measures. It explains where and why hazards arise even in a mechanic's range of activities and how they can be avoided. It uses numerous examples to illustrate the particular issues of hazards due to electrical energy and explains the necessary protective measures.

The exercises require the existing conditions to be examined and show the hazards resulting from a particular situation by using concrete measurements.
The subsequent analysis and interpretation of the measurement results clarify the relationships and justify the protective measures taken.

Content
- Mains supply
  - Mains systems (TN, TT, IT systems)
  - Protective measures in the different networks
- Domestic supply
  - Components of a domestic supply system
  - Additional designations in the TN system (TN-C, TN-S, TN-C-S)
  - Selection of the protective measure and protective devices
  - Measuring devices for protective devices
  - Initial tests acc. to DIN VDE 0100-610 and proof tests acc. to DIN VDE 0105 and BGV A3

Benefits
- Lockable error switches integrated in the housing facilitate realistic fault finding.
- No additional power supply required.
- For a practical explanation of the protective measures, measurements and tests are carried out using conventional test and measuring devices.
- The optionally available Systainer solution meets work, transport and storage requirements efficiently.

Workbook
The workbook contains project exercises that build on each other and include solutions, training notes, posters on safety and worksheets for trainees.

Available in DE, GB, FR, ES, CN

For information, please contact:
www.festo-didactic.com

Equipment set TP 1111 – Power supply systems and protective measures

Basic principles of electrical protective measures

Protecting people plays an important role when using electrical energy, as it is not visible and is recognisable only by its effects. Possible risks must therefore be minimised through suitable protective measures. Examples provide an introduction to the problems associated with electrical protective measures. The existing conditions are examined and the hazards resulting from a particular situation are shown using measurements. The subsequent analysis and interpretation of the measurement results indicate the relationships and identify measures.

Content

- Mains supply
  - Mains systems (TN, TT, IT systems)
  - Protective measures in the different networks
- Domestic supply
  - Components of a domestic supply system
  - Additional designations in the TN system (TN-C, TN-S, TN-C-S)
  - Selection of the protective measure and protective devices
  - Measuring devices for protective measures
  - Initial tests acc. to DIN VDE 0100-610 and proof tests acc. to DIN VDE 0105 and BGV A3
- Sub-distribution board
  - Using protective measures and measuring devices
  - Planning and executing initial and repeat tests
  - Analysing measurement results
  - Creating test reports
  - Identifying, describing and measuring dangers due to errors
  - Systematic troubleshooting
- Conducting customer meetings
  - for system transfer
  - for proof tests
  - for faults/malfunctions in the electrical system
  - following successful repair

Benefits

- Lockable error switches integrated in the housing facilitate realistic fault finding.
- No additional power supply required.
- For practical explanation of the protective measures, measurements and tests are carried out using conventional test and measuring devices.
- The optionally available Systainer solution meets work, transport and storage requirements efficiently.

Workbook

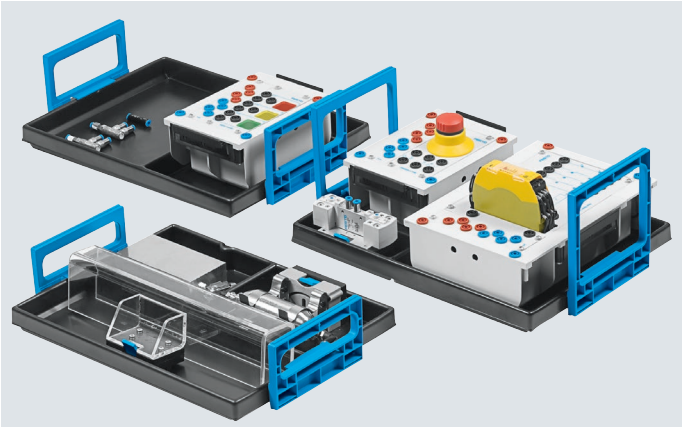
The workbook contains project exercises that build on each other and include solutions, training notes, posters on safety and worksheets for trainees.

Available in DE, GB, FR, ES, CN

For information, please contact:

www.festo-didactic.com

Equipment set TP 250 – Advanced level: safety in pneumatic systems



Risk reduction!

Just like good functionality and economic efficiency, safety is essential to the success of any product. Furthermore, new directives and laws require intelligent solutions and increase the level of training requirements. As a result, there is a wide range of different products, information and training for safety engineering. However, most of these focus on the control level. But as risks arise in the power section, it is important to develop the ability to reduce risk in that area.

Content

- Reducing pressure and force according to the work to be performed
- Reducing the speed and acceleration while observing the cycle time and the control for the specific load conditions
- Emergency stop and release: suitable measures for stopping and properly recommissioning a pneumatic drive
- Appropriate measures in the event power is cut and restored, as well as instructions on how to store and use auxiliary energy
- Appropriate measures the event power is cut and restored
- Getting to know the operating modes and signals for operating statuses
- Using sensors to detect malfunctions
- Increasing the performance level using a two-channel emergency stop
- Selecting and applying suitable protective measures

However, what does a “pneumatics specialist” entrusted with the commissioning, troubleshooting, set-up, maintenance and simple optimisation of a system need to know? And how can this knowledge be conveyed in a clear manner, with easy-to-follow steps?

TP 250!

TP 250 builds on the training content and components of TP 101 (Basic principles of pneumatics) and TP 201 (Basic principles of electropneumatics), focusing on the systematic optimisation of safety in pneumatic systems. The aim of the training package is to detect risks in pneumatic processes, to assess the risks for a simple “machine” and to learn what measures can be used to reduce risks and how to implement them properly.

Workbook

The workbook contains project exercises that build on each other and include solutions, training notes, posters on safety and work sheets for trainees.

Additional media

- Design and simulation using FluidSIM
- Measurement and control with FluidLab
- Pneumatics/electropneumatics workbook

Available in DE, GB, FR, ES, CN

For information, please contact:

www.festo-didactic.com

Equipment set – Basic principles of electrical engineering

Increasing safety using state-of-the-art electrical components!

Modern machines have high safety requirements. In addition to the classic two-hand operation and emergency stop circuits, light curtains and contactless systems are increasingly being used in machine building. To meet the requirements for installing and maintaining of such systems, an understanding of the individual components and their function is required.

Content

- Two-hand control
- Electromechanical position switch
- Contactless position switch
- Light curtain
- Enabling button
- Appropriate measures the event power is cut and restored
- Getting to know the operating modes and signals for operating statuses
- Using sensors to detect malfunctions
- Increasing the performance level using a two-channel emergency stop
- Selecting and applying suitable protective measures

To meet the requirements for installing and maintaining of such systems, an understanding of the individual components and their function is required.

For information, please contact:
www.festo-didactic.com

Appendix

Contents

List of abbreviations

Abbreviation	English denotation	Source
a, b, c, d, e (PL)	Denotation of performance levels	ISO 13849-1
a	annum (year)	
AOPD	Active optoelectronic protection device	ISO 12100, IEC 61496-1, IEC 62046
AOPDDR	Active optoelectronic protective devices responsive to diffuse reflection	IEC 61496-1, IEC 61496-3, IEC 62046
B, 1, 2, 3, 4	Denotation of categories	ISO 13849-1
B_{10}	Number of cycles until 10% of the components fail (for pneumatic and electromechanical components)	ISO 13849-1
B_{10D}	Number of cycles until 10% of the components fail dangerously (for pneumatic and electromechanical components)	ISO 13849-1
BPCS	Basic process control system	IEC 61511
CCF	Common cause failure	IEC 61508, IEC 62061, IEC 61511-1, ISO 13849-1
CE	EU Conformity Mark	Decree (EC) no. 765/2008
CEN	European Committee for Standardization	https://www.cen.eu/
CENELEC	European Committee for Electrotechnical Standardization	https://www.cenelec.eu/
DC	Diagnostic coverage	EN ISO 13849-1, IEC 62061, IEC 61508-2
DC_{avg}	Diagnostic coverage, average	ISO 13849-1
E	External risk reduction facilities	EN 61511-1
I/O	Input/output	
E/E/PE	Electrical/electronic/programmable electronic	IEC 61511, IEC 61508
E/E/PES	Electrical/electronic/programmable electronic system	IEC 61511, IEC 61508
EMC	Electromagnetic compatibility	EN 61000-6-.., EN 61000-6-7, EN 61326-3-1
F, F1, F2	Frequency and/or time of exposure to the hazard	ISO 13849-1
FB	Function block	ISO 13849-1
FMEA	Failure modes and effects analysis	ISO 13849-1, ISO 12100, EN 60812
FTA	Fault tree analysis	ISO 12100, EN 61025
Hazard	Potential source of injury or damage to health	EC Machinery Directive 2006/42/EC
Hazard zone	Any zone in and/or around machinery in which a person is subject to a risk to his health or safety	ISO 12100
Inherent safety	Protective measure that either eliminates hazards or reduces the risks associated with hazards by changing the design or operating characteristics of the machine without the use of guards or protective devices.	ISO 12100
Declaration of conformity	Process whereby the manufacturer or their authorised representative established in the Community declares that the machine placed on the market complies with all relevant essential health and safety requirements.	EC Machinery Directive 2006/42/EC
L, L1, L2	Logic	ISO 13849-1
Lambda (λ)	Failure rate	IEC 62061, IEC 61508, IEC 61511
MTBF	Mean time between failures	IEC 61508-4
MTTF/$MTTF_D$	Mean time to failure/ Mean time to dangerous failure	ISO 13849-1
MTTR	Mean time to repair	IEC 61508-4
Emergency off	Emergency switch-off	EN 60204-1-Appendix E
Emergency stop	Emergency stop	ISO 13850, EN 60204-1 Appendix E
NP	Non-programmable system	IEC 61511-1
O, O1, O2, OTE	Output device, e.g. valves, motor controllers, conductors	ISO 13849-1
OSSD	Output signal switching device, electronic safety switching output	EN 61496-1
P, P1, P2	Possibility of avoiding the hazard	EN ISO 13849-1
PFD	Probability of failure on demand	IEC 61508, IEC 61511
PFH	Probability of failure per hour	IEC 61508, IEC 62061, ISO 13849
PFH_D	Probability of dangerous failure per hour	IEC 62061, ISO 13849
PL (Performance Level)	Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions	ISO 13849-1
PL r (required performance level)	Required performance level (PL)	ISO 13849-1

List of abbreviations

Abbreviation	English denotation	Source
PLC	Programmable logic controller	IEC 61511, EN ISO 13849-1
Residual risk	Risk remaining after safety measures have been taken	ISO 12100
Risk	Combination of the severity of harm and the probability of its occurrence	ISO 12100
Risk analysis	Combination of the specification of the limits of the machine, hazard identification and risk estimation	ISO 12100
Risk assessment	Overall process comprising a risk analysis and a risk evaluation	ISO 12100
Risk estimation	Defining the likely severity of harm and the probability of its occurrence	ISO 12100
Risk evaluation	Judgement, on the basis of risk analysis, of whether the risk reduction objectives have been achieved	ISO 12100
S, S1, S2	Severity of injury	ISO 13849-1
Safety loop	A complete controlled safety loop with sensors, logic and final control element that can be implemented with a safety instrumented system (SIS). The SIS system switches off a process system or part of a system for safety reasons, but keeps the system running safely in the event of a device failure.	
Damage	Physical injury or damage to the health of people or damage to property or the environment	EN 61508-4, IEC 61511-1, ISO 13849-1
Protective measure	Measure that eliminates a hazard or reduces a risk	ISO 12100, EN 61511-1
SIF	Safety instrumented function	EN 61511-1
SIL	Safety integrity level	IEC 61508, IEC 61511, ISO 13849-1
SIS	Safety instrumented system	EN 61511-1
SRP/CS	Safety-related part of control systems	ISO 13849-1
SRS	Safety requirements specification	IEC 61511
TE	Test equipment	ISO 13849-1
Safeguarding	Protective measure using safeguards to protect persons from hazards which cannot reasonably be eliminated or from risks which cannot be sufficiently reduced by inherently safe design measures	ISO 12100
T_M	Mission time	ISO 13849-1
TÜV	Association for Technical Inspection	
VDMA	German Mechanical Engineering Industry Association (VDMA)	https://www.vdma.org/

Glossary

Human-machine interface

Mode selector switch, 2-stage


Light curtain

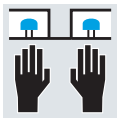

Stop button


Enabling button

Mode selector switch, 3-stage


Emergency stop


Jogging

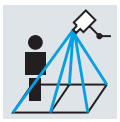

Two-hand control


Movable guard: safety door


Emergency stop


Safety shut-off mat


Two-hand control


Camera system


Acknowledgment

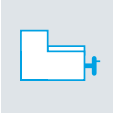

Restart


Laser scanner

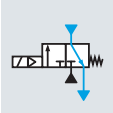

Start button

Pneumatics

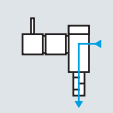
Safety sub-functions that affect systems



E-SF
Safety sub-functions that affect systems

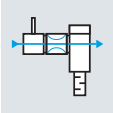


SDE
Safe de-energization (SDE)

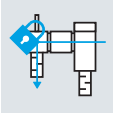


SDE
Safe de-energization (SDE)

SEZ
Safe energization



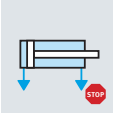
SEZ
Safe energization



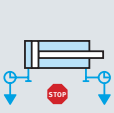
LOTO
Lock-out / tag-out (not part of VDMA 24584)

Safety sub-functions that affect drives

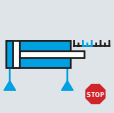
E-SF
Safety sub-function that affects drives



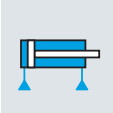
STO
Safe torque off



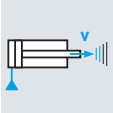
SS1
Safe stop 1



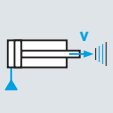
SS2
Safe stop 2



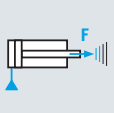
SOS
Safe operating stop



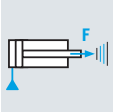
SLS
Safely limited speed



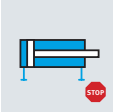
SSR
Safe speed range



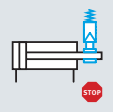
SLT
Safely limited torque (force)



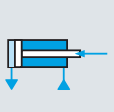
STR
Safe torque range



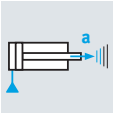
SSC
Safe stopping and closing



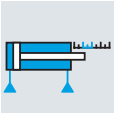
SSB
Safe stopping and blocking



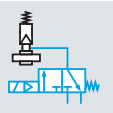
SDI
Safe direction



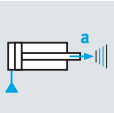
SLA
Safely limited acceleration



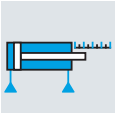
SLP
Safely limited position



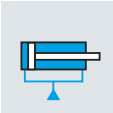
SBC
Safe brake control



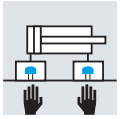
SAR
Safe acceleration range



SLI
Safely limited increment



SET
Safe equilibrium of torque

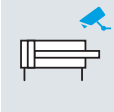


THC
Two-hand control

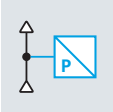
PUS
Prevention of unexpected start-up

SB
Safe blocking (not part of VDMA)

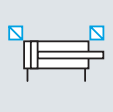
Monitoring safety sub-function



E-SF (1)
Monitoring safety sub-function

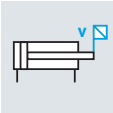


SPM
Safe pressure monitor

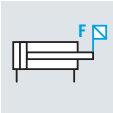


SCA
Safe cam

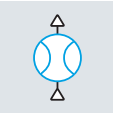
SBM
Safe brake monitor



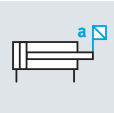
SSM
Safe speed monitor



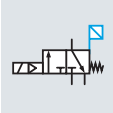
STM
Safe torque monitor



SVM
Safe volumetric flow monitoring



SAM
Safe acceleration monitor

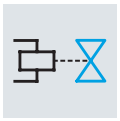


SVP
Safe valve position

Glossary

Pneumatics

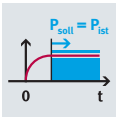
Components


Valve

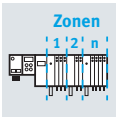

Service unit

Additional functions

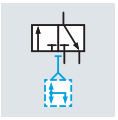

Protection against tampering

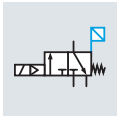


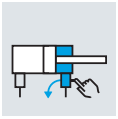
For protecting against unintentional pressure

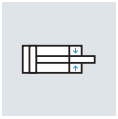


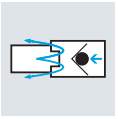
Creating zones

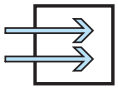

Valves with negative overlap

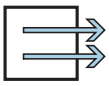

Valves with switching position monitoring


Releasing trapped persons


End-position locking

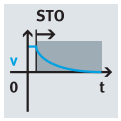

Safety coupling


Safe inputs

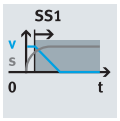

Safe outputs

Electric systems

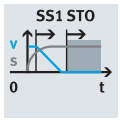
Safety sub-functions



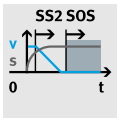
STO
Safe torque off



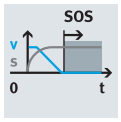
SS1
Safe stop 1



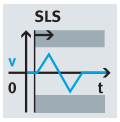
SS1-t
Safe stop 1 with
time control



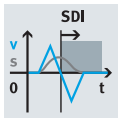
SS2
Safe stop 2



SOS
Safe operating
stop

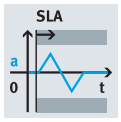


SLS
Safely limited
speed



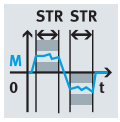
SDI
Safe direction

SLT
Safely limited
torque



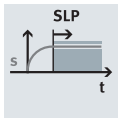
SLA
Safely limited
acceleration

SAR
Safe acceleration
range

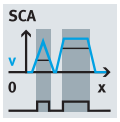


STR
Safe torque range

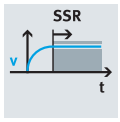
SLI
Safely limited
increment



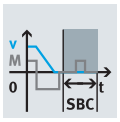
SLP
Safely limited
position



SCA
Safe cam

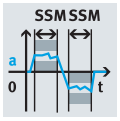


SSR
Safe speed range

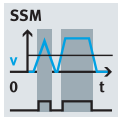


SBC
Safe brake control

SMT
Safe motor
temperature

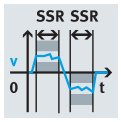


SSM
Safe speed monitor



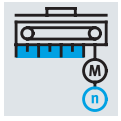
SSM
Safe speed monitor

SBT
Safe brake test

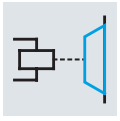


SSR
Safe speed range

Components

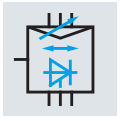


Measuring system

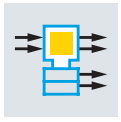


Brake

Contactor

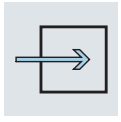


Motor controller

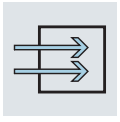


Safety logic

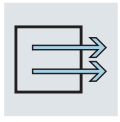
Logic, inputs and outputs



Input



Input redundant



Output redundant

Sales and service network – International

Argentina
Festo S.A.
Edison 2392
1640 Buenos Aires
P +54 810 555 33786
F +54 810 444 3127
ventas.ar@festo.com

Australia
Festo Pty. Ltd. Head Office
Browns Road 179-187
Noble Park
3174 Melbourne
P +61 397 9595-55
F +61 397 9597-87
info_au@festo.com

Austria
Festo Gesellschaft m.b.H.
Linzer Straße 227
1140 Vienna
P +43 1 910 75-100
F +43 1 910 75-250
info_at@festo.com

Belarus
IUP Festo
Masherov avenue 78
Office 201
220035 Minsk
P +375 17 204 85 58
F +375 17 204 85 59
info_by@festo.com

Belgium
Festo Belgium nv
Rue Colonel Bourg 101
1030 Bruxelles
P +32 2 702 32 11
F +32 2 702 32 09
info_be@festo.com

Brazil
Festo Brasil Ltda
Rua Guiseppe Crespi 76
Jd. Santa Emília
04183-080 São Paulo
P +55 11 5013 1600
F +55 11 5013 1801
linhadireta.br@festo.com

Bulgaria
Festo EOOD
Bul. Christopher Kolumb 9
1592 Sofia
P +359 2 960 07 12
F +359 2 960 07 13
festo_bg@festo.com

Canada
Festo Inc.
Explorer Drive 5300
L4W 5G4 Mississauga
P +1 905 614 4600
F +1 877 393 3786
info_ca@festo.com

Chile
Festo S.A.
Av. Américo Vespucio 760
9020000 Santiago de Chile
P +56 2 2690 2801
F +56 2 2690 2860
info.cl@festo.com

China
Festo (China) Ltd.
Yunqiao Road, 1156
Jinqiao Export Processing Zone
201206 Shanghai
P +86 21 60 81 51 00
F +86 21 58 54 03 00
info.cn@festo.com

Colombia
Festo S.A.S.
Autopista Medellín Km 6.3
Costado Sur
Tenjo, Cundinamarca
P +57 1 865 7788
F +57 1 865 7729
info_co@festo.com

Croatia
Festo d.o.o.
Nova Cesta 181 A
10000 Zagreb
P +385 1 619 1969
F +385 1 619 1818
info_hr@festo.com

Czech Republic
Festo, s.r.o.
Modřanská 543/76
14700 Prague
P +420 261 09 96 11
F +420 241 77 33 84
info_cz@festo.com

Denmark
Festo A/S
Islevdalvej 180
2610 Rødovre
P +45 70 21 10 90
F +45 70 21 10 99
sales_dk@festo.com

Estonia
Festo OY AB Eesti Filiaal
Karjavälja 10
12918 Tallinn
P +372 666 1560
F +372 666 15 6
info.ee@festo.com

Finland
Festo Oy
Mäkituvantie 9
01511 Vantaa
P +358 9 87 06 51
F +358 9 87 06 52 00
info.fi@festo.com

France
Festo E.U.R.L.
Rue du Clos Sainte-Catherine 8
ZA des Maisons Rouges
94360 Bry-sur-Marne
P +33 1 48 82 64 00
F +33 1 48 82 64 01
info_fr@festo.com

Germany
Festo Vertrieb GmbH & Co. KG
Festo Campus 1
73734 Esslingen
P +49 711 347-1111
F +49 711 347-2244

Greece
FESTO Ε.Π.Ε.
Tatoiou Ave. 92
14452 Athen
P +30 210 341 29 00
F +30 210 341 29 05
info_gr@festo.com

Hongkong
Festo Ltd
Castle Peak Road 497
6/F New Timely Factory Building
Kowloon
P +852 3904 20 91
F +852 2745 91 43
sales_hk@festo.com

Hungary
Festo Kft.
Csillaghegyi út 32-34
1037 Budapest
P +36 1 436 51 11
F +36 1 436 51 01
info_hu@festo.com

India
Festo India Private Limited
Bommasandra Indl. Area 237B
Bengaluru - Hosur Highway
560 099 Bengaluru
P +91 1800 425 0036
F +91 1800 121 0036
sales.in@festo.com

Indonesia
PT. Festo
Jl. Tekno V Blok A/1 Sektor 11
Kawasan Industri BSD
15314 Tangerang
P +62 21 27507900
F +62 21 27507998
info_id@festo.com

Iran
Festo Pneumatic S.K.
Special Karaj Road
6th street, 16th avenue, # 2
1389793761 Teheran
P +98 21 44 52 24 09
F +98 21 44 52 24 08
info@festo.ir

Ireland
Festo Limited
Sandyford Park Unit 5
D18VH99 Dublin
P +353 (0)1 295 49 55
info_ie@festo.com

Israel
Festo Pneumatic Israel Ltd.
Ha'atzma'ut Road 48
P.O. Box 1076
5630421 Yehud
P +972 3 632-2266
F +972 3 632- 2277
info_il@festo.com

Italy
Festo SpA
Via Enrico Fermi 36/38
20090 Assago
P +39 02 45 78 81
F +39 02 488 06 20
info_it@festo.com

Japan
Festo K.K.
Hayabuchi 1-26-10
Tsuzuki-ku
224-0025 Yokohama
P +81 45 593 56 10
F +81 45 593 56 78
info.jp@festo.com

Jordan
Festo DMCC
Zahar St. 13
11953 Amman
P +962-6-5563646
F +962-6-5563736
info_mena@festo.com

Korea
Festo Korea Co., Ltd.
Gasan Digital 1-ro 204
153-803 Seoul
P +82-1666 0202
saleskr@festo.com

Latvia
Festo SIA
Gunāra Astras 8b
1082 Riga
P +371 67 57 78 64
F +371 67 57 79 46
info_lv@festo.com

Lithuania
Festo, UAB
V. Krevės pr. 129
50312 Kaunas
P +370 37 3213 14
F +370 37 32 13 15
info_lt@festo.com

Malaysia
Festo Sdn. Berhad
Jalan Teknologi 14A
Taman Sains Selangor 1
47810 Petaling Jaya
P +60 3 6144 1122
F +60 3 6141 6122
info.my@festo.com

Mexico
Festo Pneumatic, S.A.
Av. Ceylán 3
Col. Tequesquináhuac
54020 Tlalnepantla
P +52 01 800 337 8669
F +52 01 800 337 8639
contacto@festo.com

Netherlands
Festo B.V.
Schieweg 62
2627 AN Delft
P +31 15 251 88 90
F +31 15 251 88 67
sales.nl@festo.com

New Zealand
Festo Ltd.
Fisher Crescent 20
Mt. Wellington
1062 Auckland
P +64 9 574 10 94
F +64 9 574 10 99
info_nz@festo.com

Nigeria
Festo Automation Ltd.
Badejo Kalesanwo Street 6
C. Woermann Building, Matori Industrial Estate
Lagos
P +234 2930812
F +234 2930813
enquiry.ng@festo.com

Norway
Festo AS
Ole Deviks vei 2
0666 Oslo
P +47 22 72 89 50
F +47 22 72 89 51
sales_no@festo.com

Peru
Festo S.R.L.
Av. Elmer Faucett 3350
01 Lima
P +51 1 219 69 60
F +51 1 219 69 71
ventas.pe@festo.com

Philippines
Festo Inc Head Office
West Service Road KM18
South Superhighway
1700 Paranaque City
P +63 (2) 77 66 888
F +63 2 82 34 220/21
info_ph@festo.com

Poland
Festo Sp. z o.o.
ul. Mszczonowska 7
05-090 Raszyn
P +48 22 711 41 00
F +48 22 711 41 02
info_pl@festo.com

Portugal
Festo – Automação, Unipessoal, Lda.
Rua Manuel Pinto De Azevedo 567
Apartado 8013
4109601 Porto
P +351 22 615 6150
F +351 22 615 6189
info.pt@festo.com

Romania
Festo S.R.L.
Strada Sfântul Constantin 17
010217 Bucharest
P +40 21 403 95 00
F +40 21 310 24 09
info_ro@festo.com

Russia
OOO Festo-RF
Michurinskiy prosp. 49
119607 Moscow
P +7 495 737 34 00
F +7 495 737 34 01
info.ru@festo.com

Singapore
Festo Pte. Ltd.
Kian Teck Way 6
628754 Singapore
P +65 62 64 01 52
F +65 62 61 10 26
info.sg@festo.com

Singapore
Festo Pte. Ltd.
Kian Teck Way 6
628754 Singapore
T +65 62 64 01 52
F +65 62 61 10 26
info.sg@festo.com

Slovakia
Festo spol. s r.o.
Gavlovičová ul. 1
83103 Bratislava
P +421 2 49 10 49 10
F +421 2 49 10 49 11
info_sk@festo.com

Slovenia
Festo d.o.o.
Blatnica 8
1236 Trzin
P +386 1 530 2100
F +386 1 530 2125
info_si@festo.com

South Africa
Festo (Pty) Ltd.
Electron Avenue, Isando 22-26
P.O. Box 255
1600 Johannesburg
P +27 11 971-5500
F +27 11 974-2157
sales.za@festo.com

Spain
Festo Automation, S.A.U.
Avinguda de la Granvia 159
Hospitalet de Llobregat
08908 Barcelona
P +34 901243660
F +34 902243660
info_es@festo.com

Sweden
Festo AB
Stillmansgatan 1
200 21 Malmö
P +46 40 38 38 00
F +46 40 38 38 10
sales_se@festo.com

Switzerland
Festo AG
Gass 10
5242 Lupfig
P +41 44 744 5544
F +41 44 744 5500
info.ch@festo.com

Taiwan
Festo Co., Ltd.
Gongba Road 9
Linkou 2nd Industrial Zone
24450 Linkou
P +886 2 26 01-92 81
F +886 2 26 01 92 86-7
info_tw@tw.festo.com

Thailand
Festo Ltd. Head Office
Kanchanapisek Road 200,202
Ramintra, Khannayao
10230 Bangkok
P +66 1800-019-051
F +66 1800-019-052
sales_th@festo.com

Turkey
Festo San. ve Tic. A.S.
Universite Cad. 45
Tuzla
34953 Istanbul
P +90 216 585 00 85
F +90 216 585 00 50
info_tr@festo.com

Ukraine
DP Festo
Borysohlibska 11
04070 Kiev
P +380 44 233 6451
F +380 44 463 7096
orders_ua@festo.com

United Arab Emirates
Festo DMCC
Swiss Tower, unit 505
Cluster Y, JLT
Dubai
P +962 6 5563646
F +962 6 5563736
info_mena@festo.com

United Kingdom
Festo Limited
Caswell Road 55
Applied Automation Centre
NN4 7PY Northampton
P +44 800 626 422
info.gb@festo.com

United States
Festo Corporation
Columbia Road 7777
45039 Mason
P +1 (513) 486-1050
customer.service.us@festo.com

Venezuela
Festo C.A.
Av. 23 esquina con calle 71
Nº 22-62, Edif. Festo, Sector Paraíso
Maracaibo
P +58 261 759 1120
F +58 261 759 1417
info_ve@festo.com

Vietnam
Festo Co Ltd
Vành Đai Đông (Nguyên Hoàng)
1515 – 1516
An Phu, District 2
Ho Chi Minh City
P +84 28 62 81 4453
F +84 28 62 81 4442
info_vn@festo.com

Guideline for functional safety

Pneumatic and electric solutions

135242 (EN)
Subject to change
2019/05

www.festo.com