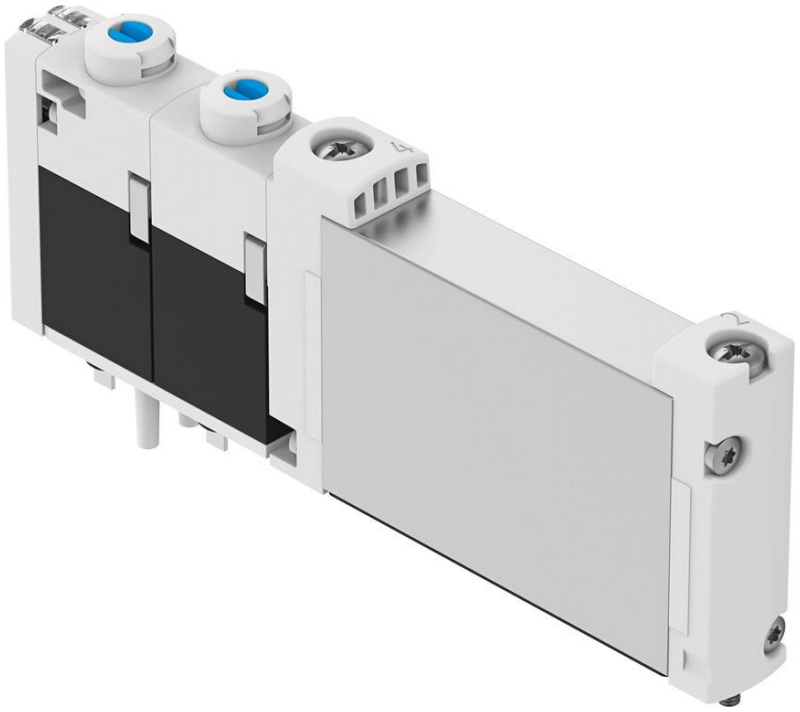
Safety Application Note ISO 13849

FESTO

Circuit
Safety-Subfunctions Pneumatic
Features of directional control valves

100396



Our effort – your advantage

Our effort for the preparation of these documents
and your saved time 16 h
Free of charge for you.

Title ..... Safety Subfunctions Pneumatics
Version 1.10
Document number 100396
Original ..... German
Author ..... Festo
Last date of saving 2023-11-17

Legal Notice

In the following, the “Festo SE & Co. KG“ is designated as “Festo”.

This document is not binding. This documents outlines a possible solution for a sample application and makes no claim of completeness, especially with regard to configuration and equipment, as well as any eventualities for your actual application. This document is not a customised solution, it merely offers assistance with typical task assignments.
The values stated in this document are partly assumptions and assessments which do not replace a detailed examination based on ISO 13849 part 1 and 2, IEC 61508, IEC 62061 and/or IEC 61511.
The actual characteristic values that can be obtained (especially PL, PFH_D, category, DC, $MTTF_D$, CCF, SIL, HFT, PFH, PFD) depend on the components used, as well as their conditions of use in the actual application.
This document does not relieve you of the obligation to carry out a risk assessment and a validation of the specific application and to ensure the adherence to all specifications, especially the EC Machinery Directive 2006/42/EG. As the user, you are responsible for your specific application and for the correct operation of the described products.
Festo does not accept any liability for damages arising from the use of any incorrect or incomplete information contained in this documentation or any information missing therefrom. This equally applies to defects resulting from improper handling of devices and modules. In addition, all liability, with the exception of intent or gross negligence on the part of Festo, for damages arising due to non-adherence of the specifications of the EC Machinery Directive 2006/42/EG is also rejected.
The information in this document is in no way intended as a substitute for the operating instructions of the respective manufacturers or the design and testing of the application by the user. The operating instructions for products from Festo can be found at www.festo.com. Users of this document must themselves verify that all the functions described herein also work correctly in the application. Even after examining this document and using the specifications contained herein, users are nevertheless solely responsible for their own application.
Otherwise, all stipulations concerning liability included in the terms and conditions of delivery, payment and use of software from Festo, which can be found at www.festo.com and can be supplied on request, apply.
This document is only suitable for persons with sufficient expertise for machine safety based on ISO 12100, ISO 13849, IEC 61508, IEC 62061 and IEC 61511. In addition, the following qualifications are required in the project team:

- Specialist in pneumatics
- Specialist in electrical engineering
- Specialist for the programming of control systems and safety switching devices

Copyright Notice

Table of Contents

1 General

1.1 Objectives of this Document

- This document provides additional guidance for some features of electrically operated directional control valves that should be taken into account when implementing functional safety.

1.2 General Notes

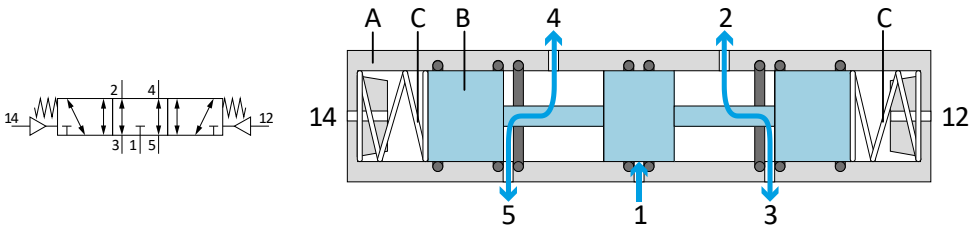
- The technical characteristics of electrically operated directional control valves must always be observed in accordance with the data sheet, product reliability data sheet, general operating conditions and any available operating instructions. The information in these documents has priority over the information in this Application Note.
- The circuits given are principle circuits which cannot be complete for reasons of clarity and comprehensiveness. They are recommendations that do not exclude other possibilities.

2 Electrically actuated directional control valves

A *directional control valve* is used to change, open or close volume flow paths of compressed air in a pneumatic system. The valves differ in terms of the design of their control element, the number of switching positions and flow paths, and the type of actuation (manual, mechanical, pneumatic or electric).
Electrically operated directional control valves usually consist of a main stage, e.g. 2.1 Piston spool valve (pneumatically operated) and a pilot valve, e.g. 2.3 Electrically, directly operated poppet valve.

2.1 Piston spool valve (pneumatically actuated)

If the feature “piston spool” is specified, the main stage of the valve has a piston spool in the valve housing which releases or blocks the flow paths.



Legend	
A	valve housing
B	piston spool
C	mechanical spring for reset
1, 2, 3, 4, 5	ports volume flow paths
12, 14	control ports

Figure 1 Valve with piston spool (symbol and intersection)

A valve with a piston spool releases or blocks the ports according to the position of the piston spool. In the normal position shown in figure 1, port 1 is blocked and the flow paths 2-3 and 4-5 are released. If pressure is applied to port 12, the piston slide is moved to the left stop. Port 3 is then blocked and flow paths 1-2 and 4-5 are opened. If, on the other hand, pressure is applied to port 14, the piston slide is moved to the right stop and port 5 is blocked and flow paths 1-4 and 2-3 are opened. If there is no more pressure at the control ports 12, 14, the piston slide moves back to its normal position in the middle.

Advantages with piston spool valves

- Large flow rates are possible;
- Vacuum operation of the flow paths of the main ports 1, 2, 3, 4, 5;
- Pressure balanced and therefore generally suitable for reverse operation;

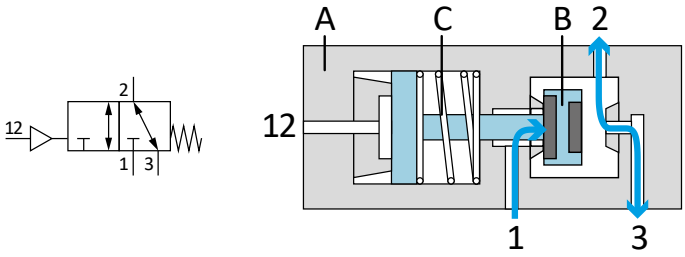
Disadvantages

- Longer travel due to the use of several pistons;
- Control edges run over the sealing points;
- Demanding tribology[1] leads to greater leakage over the service life as with poppet valves;
- After longer downtimes, there is at least a longer switching time due to adhesion effects. This effect can be stronger with poppet valves than with piston valves.

[1] Tribology is the science and technology of interacting surfaces in relative motion. It deals with the scientific description of friction, lubrication and wear.

2.2 Poppet valve (pneumatically actuated)

In a poppet valve, the control element is a plug, ball or disc. This control element blocks the flow paths through the valve by closing or opening orifices.



Legend	
A	valve housing
B	plunger with sealing disc
C	mechanical spring for reset
1, 2, 3	ports volume flow paths
12	control port

Figure 2 Poppet valve (symbol and intersection)

A valve with a seat releases or blocks the ports according to the position of the control element. In the normal position shown in figure 2, port 1 is blocked and the flow path 2-3 is released. If pressure is applied to port 12, the plunger with sealing disc is moved to the right stop. Port 3 is then blocked and flow path 1-2 is released. If there is no more pressure at port 12, the seat moves back to the normal position.

Advantages of poppet valves under nominal operating conditions are

- Very low leakage over the service life;
- Normally longer life and more reliable than piston valves;
- Less susceptible to contamination.
- It is driven onto the sealing and not run over.
- Closing by load-pressure
- Usually with negative overlap

Disadvantages of poppet valves

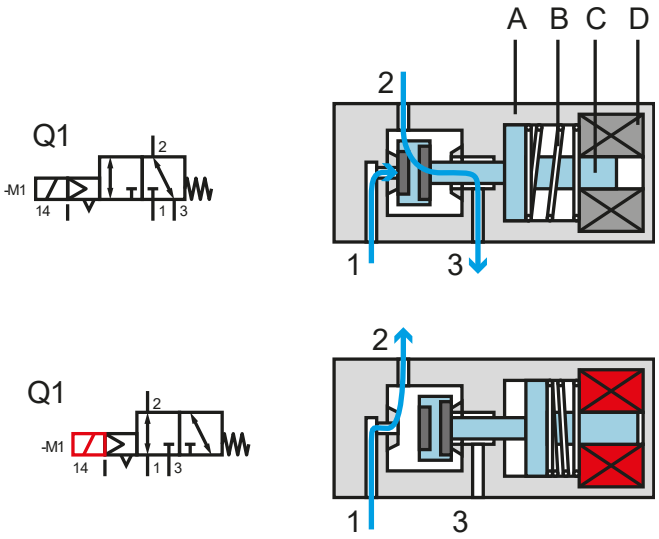
- Size to flow ratio is worse than piston spool.
- The working pressure has to be held by the spring, so it has to be much stronger than with a piston spool;
- Reverse or vacuum operation is not possible with 5/2-way valves.

Advantage or disadvantage depends on the application

- In the case of negative overlap, there is an overflow between the ducts during the switching process. This can be an advantage with a venting function (when stuck in an intermediate position, the venting function is always executed with a vented port 1).
  In a stop function, where trapped compressed air is required to stop, this is a disadvantage, because in the event of a fault, exhausting is always performed).

2.3 Electrically, directly actuated poppet valve

An electrically, directly actuated seat valve is actuated by a magnetic field generated by an electric current.



Legend

A	valve housing
B	disc with seals
C	mechanical return spring
D	armature
E	valve solenoid
1, 2, 3	Ports volume flow paths

Figure 3 Electrically, directly actuated poppet valve

A poppet valve releases or blocks the ports according to the position of the control element. In Figure 3, the intersection drawing shows the valve at normal position with port 1 blocked and flow path 2-3 open. If the valve solenoid is actuated with an electrical signal, the valve switches to the switching position and the disc moves to the right stop. Then the port 3 is blocked and the volume flow path 1-2 is opened. If the valve solenoid is no longer activated with an electrical signal, the valve returns to the normal position.

2.4 Electrically actuated directional control valve with pilot control

In the case of electrically actuated directional control valves with pilot valves, the pneumatically actuated main stage is controlled by one or two electrically actuated seat valves.

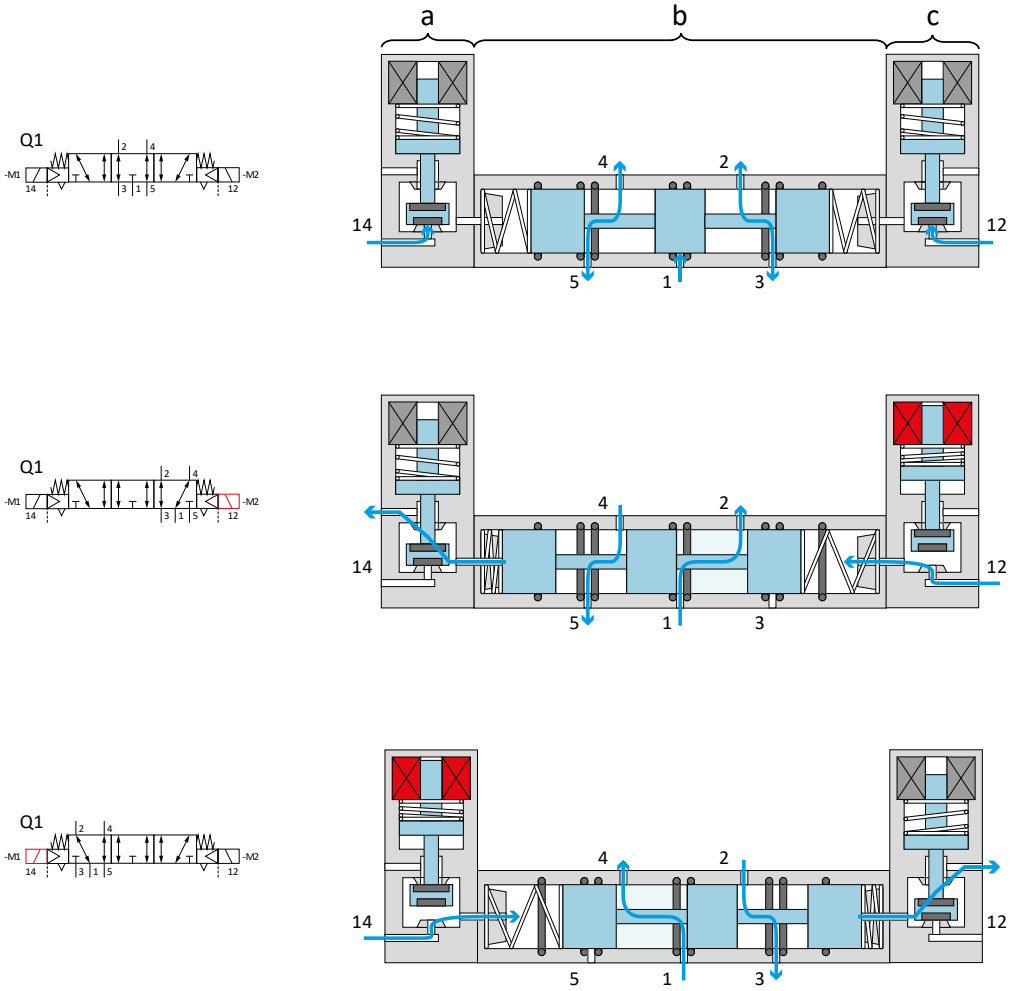


Figure 4 Electrically operated directional control valve with pilot valves

Legend

a	Pilot valve 14 (electrically actuated poppet valve)
b	Main stage (pneumatically actuated piston spool valve)
c	Pilot valve 12 (electrically actuated seat valve)
1, 2, 3, 4, 5	Main stage flow path connections
12, 14	Pilot valve air supply connections

A 5/3-way valve consists of three individual valves: a pneumatically actuated main stage and two electrically actuated pilot valves. If none of the electrically operated pilot valves is actuated, they are in normal position and the pilot air supply for controlling the main stage is not applied. The main stage blocks port 1 and the volume flow paths 2-3 and 4-5 are open. If the pilot valve 12 is actuated with an electrical signal, the pilot valve 12 moves to the switching position and switches the pilot air 12 to the main stage and the main stage moves to the one switching position and releases the volume flow paths 1-2 and 4-5. If the pilot valve 12 is not actuated and the pilot valve 14 is actuated with an electrical signal, the pilot valve 14 goes into the switching position and switches the control air 14 to the main stage and this moves into the other switching position and releases the volume flow paths 1-4 and 2-3.

Important notes

- If both pilot valves are actuated at the same time, the switching position of the main stage is usually not defined.
- In an FMEA, the pilot valves and the main stage must be evaluated separately (see also footnote ISO 13849-2, Table B.4).

3 Manual Override

A manual override is a manually operated device on a valve that allows the main stage of the valve to be moved to a switching position. If valves with manual override are used in a machine, machine manufacturers and operators must observe the requirements of the Machinery Directive 2006/42/EC and its harmonised standards. requirements of the Machinery Directive 2006/42/EC and its harmonised standards.

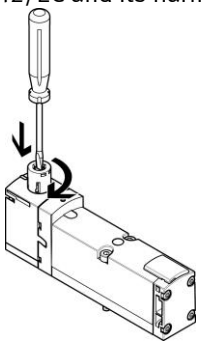


Figure 5 Operation of a manual override

The standard ISO 4414 specifies the state of the technology regarding electrically actuated valves in pneumatics. It specifies the following with regard to manual override.

> 5.4.3.4.2.4 Manual override
> If it is necessary to operate an electrically operated valve for **safety** [see 1.] or **other reasons** [see 2.] when electrical control is not available, then it should be fitted with manual override facilities. These shall be designed or selected so that they **cannot be operated inadvertently** [see 3.], and they shall reset **when manual control is removed** [see 4.] unless otherwise specified.

1. **Safety reasons** can be:
   - Dissipation of stored energy (ISO 14118)
   - Escape and rescuing trapped persons (ISO 12100, 6.3.5.3).
2. **Other reasons** are for example:
   - For instructed persons (if provided for the machine in question): Elimination of malfunction, setting up, teaching, process changeover, maintenance (ISO 12100, 6.2.11.9, 6.2.11.10).
   - For skilled personnel: Maintenance work and troubleshooting (EN ISO 12100, 6.2.11.9, 6.2.11.10)
3. **Unintentional operation** can be prevented by:
   - Concealed mounting, only accessible through the use of a tool

Figure 6 Valve terminal in housing

Example shows a valve terminal in a housing that can only be accessed by loosening several screws (the cover has been removed in the picture).

- Mounting in an area that is not accessible to operators, e.g. underneath a table, on the machine, in each case outside the operator's reach.
- Mounting in a control cabinet

Figure 7 Valve terminal in control cabinet

The control cabinet must be opened with a key accessible only to authorised personnel.

- Manual override to be operated by tool only

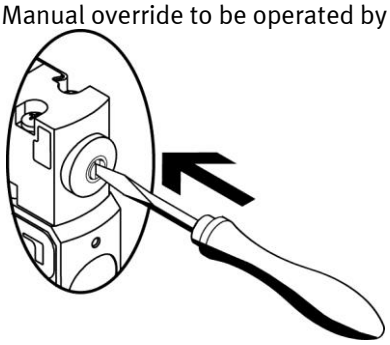


Figure 8 Manual override with tool

Manual override can only be operated with a tool that is not required and available for the intended use of the machine in automatic mode, otherwise other solutions must be selected.

- Cover of the manual override(s)

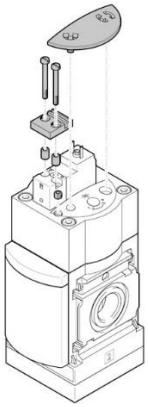


Figure 9 Manual override with cover

For certain valves, additional covers are available that cover the manual override. These additional covers can only be loosened with tools or are destroyed so that manipulations become visible.

- Control measures
  Detection of actuation by control measures in the automatic operating mode.
  Example circuit: The safety requirement (S2) only acts on the valves (Q20, Q21), i.e. the application is not disconnected from the compressed air supply and exhausted.
  If the limit switches on the cylinder (B20, B21) detect an actuation of the manual override of valve Q20, the application is disconnected from the compressed air supply and exhausted via the valve (Q22).
  A restart is only possible after acknowledgement with button (S1).

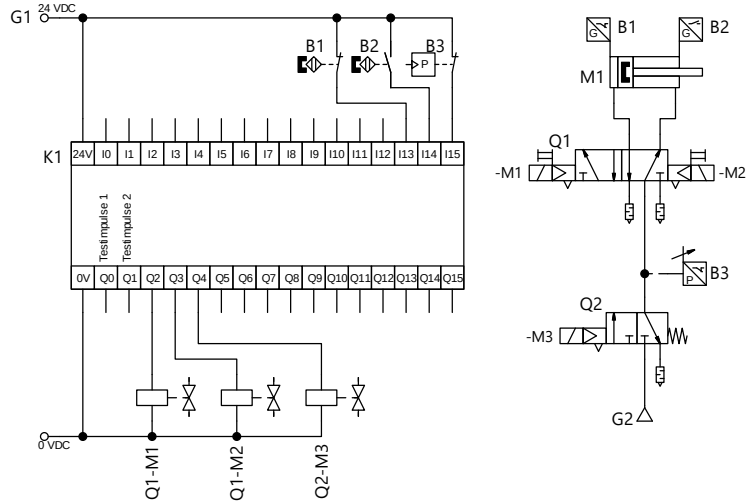


Figure 10 Use of control measures

4. Manual override, non-detenting or detenting
   It is recommended that the manual override for safety-related valves be of the non-detenting type. If the manual override is detenting, the manual override may not be reset and a safety function may no longer function. This is an impermissible way to manipulate safety functions.

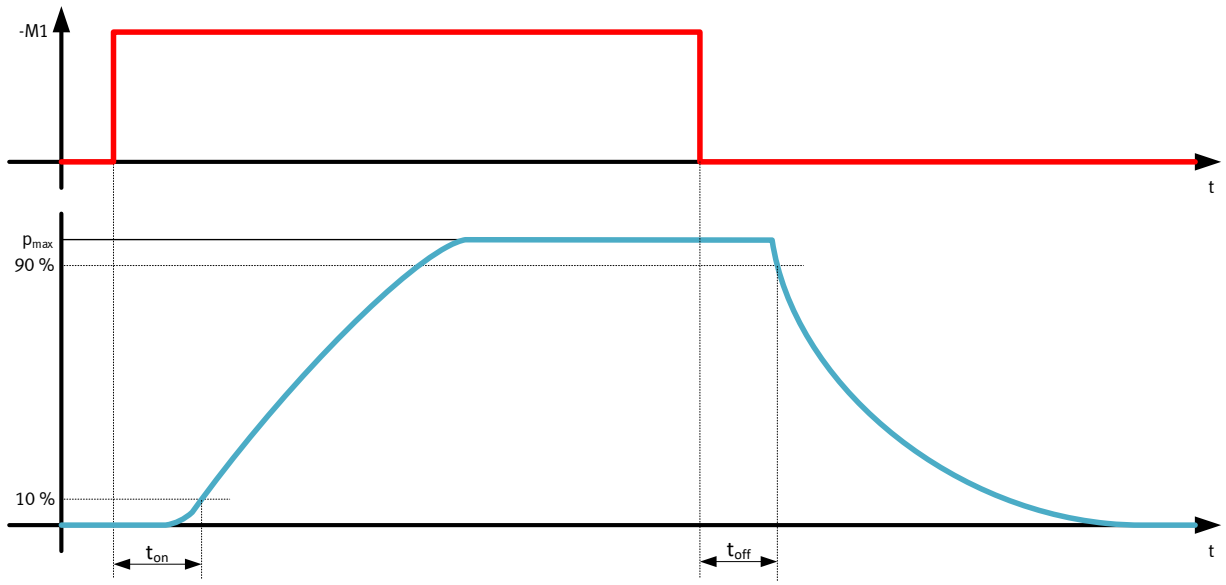
   However, a detenting manual override makes sense for on-off valves, as maintenance personnel need pressure in the pneumatic system when troubleshooting. If the resetting of this manual override is forgotten, this can usually be detected with simple pressure monitoring before the switch-on valve is actuated by a safety switching device.
   Note
   - Detenting manual overrides on the MS-SV series on-off valves are automatically reset when the on-off valves are actuated electrically for the first time.

Further notes

- Manual override in automatic mode
  The use of the manual override in automatic mode or for regular use is excluded. Due to the small actuating surface and actuating forces, these actuating elements of the manual override do not meet the requirements for frequent actuation.
- Of course, the reasonably foreseeable misuse of the manual override must be taken into account, i.e. the incentives for manipulation must be reduced to a sufficient degree (EN ISO 12100, 5.5.3.6 [3]; DGUV-Information 22 [5]). A possible misuse is the use of the manual override in automatic mode or the use by unauthorised personnel. For a sufficient reduction, the possibilities listed under “3 Unintentional operation can be prevented by:” can be used.

4 Switching times

At Festo, the switching time of a valve is always determined on the basis of ISO 12238. This standard specifies that when the control signal changes from 0 VDC to 24 VDC up to 10% of the supply pressure is evaluated as “switching time on” or when the control signal changes from 24 VDC to 0 VDC up to 90% of the supply pressure is evaluated as “switching time off”.



Legend

-M1 Control signal valve solenoid

p_{max} Supply pressure of the test assembly

t_{on} Switching time on

t_{off} Switching time off

Figure 11 Switching times

Important notes

- The data in the data sheet are typical values of individual valves when the valve is new.
- For many valves, these switching times will increase over the service life. If switching time monitoring is provided for valves as a diagnostic measure by monitoring the piston spool, this behaviour must be taken into account. We recommend using a safety factor of 2...5.
- Test conditions for the switching time: 6 bar ±0.3 bar, environmental and medium temperature 23°C ±5°C. [according to FN 952012:2018-07]
- The switching times depend on the pilot and operation pressure supply of the valve.

5 Diagnostic measures

The functional safety standards prescribe diagnostic measures for detecting possible faults. The following options are available for directional control valves:

1. switching time monitoring with piston spool monitoring
2. switching time monitoring with pressure switch monitoring
3. positioning time monitoring with limit switches on the actuator

Important note

- These diagnostic measures are not suitable for every safety sub-function and achieve different levels of diagnostic coverage. The suitable diagnostic measures are specified in the application notes with the definitions of the safety sub-functions and how they can be used in categories 2, 3 and 4 can be found in the application notes with the circuits.

5.1 Switching time monitoring with piston spool monitoring

5.1.1 Monitoring function of valves with piston spool monitoring

Valves with monitoring of the piston spool, the built-in limit switch should monitor the normal position of the main stage of the valve. The switch is closed when the main stage is in normal position. The switch is opened before the volume flow paths of the normal position change during the switching process. If the valve is in the switching position, the switch remains open. If the valve switches back to the normal position, the switch is only closed when the volume flow paths of the normal position no longer change.

5.1.2 Example circuit for diagnostics with piston spool monitoring

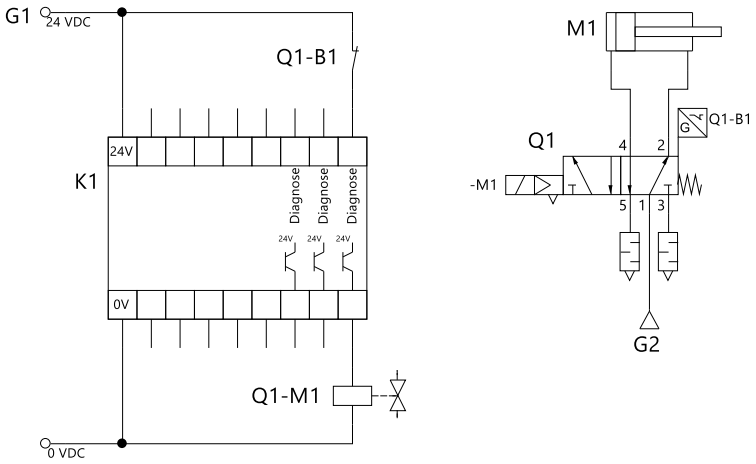
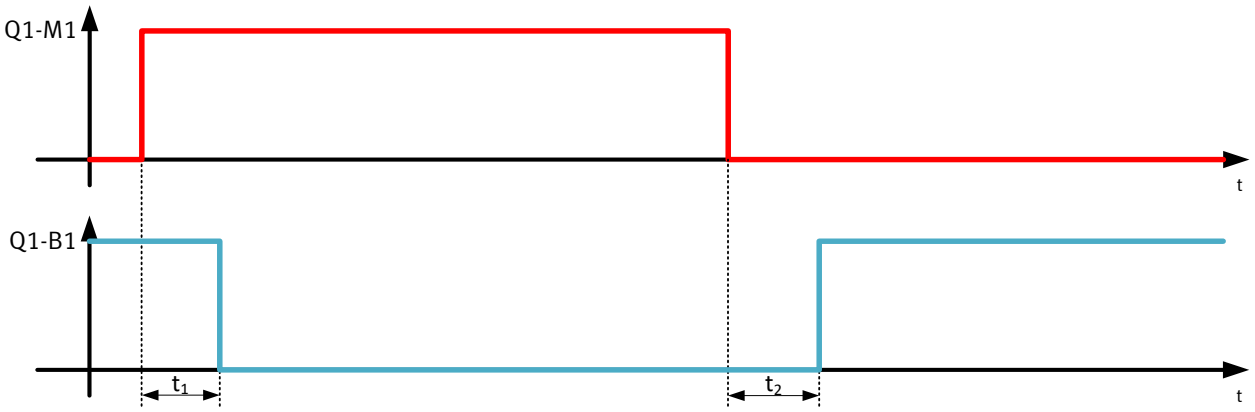


Figure 12 Diagnosis with piston spool monitoring



Legend

-M1 Control signal valve solenoid

-B1 Signal limit switch monitoring piston spool

t_1 Time delay from actuation valve coil to signal change limit switch

t_2 Time delay from deactivation of control valve coil to signal change limit switch

Figure 13 Time behaviour

Function of the circuit

- If the safety switching device K1 actuates the valve solenoid Q1-M1, the valve Q1 switches from the normal position to the switching position.
- If the piston spool moves out of the normal position, the output of the limit switch Q1-B1 is opened.
- The time delay from the activation of the valve solenoid to the opening of the output of the limit switch is the time that is monitored by the safety switching device to check the partial function switching in the switching position of the valve.
- If the safety switching device K1 no longer controls the valve solenoid Q1-M1, the valve Q1 switches from the switching position to the normal position.
- When the piston slide reaches the normal position, the output of the limit switch Q1-B1 is closed.
- The time delay from the switching off of the valve solenoid to the closing of the output of the limit switch is the time that is monitored by the safety switching device in order to check the partial function of switching in the normal position of the valve.

Monitoring times

The time for monitoring the switching process must be configured in the safety switching device. If only a maximum switching time is configured, the switching time specifications of the data sheet can be used as an evaluation basis. Over the service life of many valves, the switching time usually increases, so that a safety factor of 2...3 should be used for this setting.

There are safety switching devices in which a maximum and minimum switching time can be configured. The minimum switching time is the time from the control signal at which no signal change of the output of the limit switch Q1-B1 may occur. This minimum switching time should be set to a value that is 50 % of the switching time of the data sheet.

Note

- This value for the minimum switching time should be clearly below the typical switching time of the data sheet in order to achieve sufficient protection against false triggering by this diagnostic measure.

5.2 Switching time monitoring with pressure switch

5.2.1 Monitoring function of valves with pressure switch on output

The pressure switch is used to monitor the limit value at the output, which indicates that the safe state has been exceeded. Normally, the pressureless state of the output is monitored with a pressure switch with a limit value of ≤0.5 bar (recommendation, to be evaluated depending on the application).

5.2.2 Example circuit for diagnosis with pressure switch query

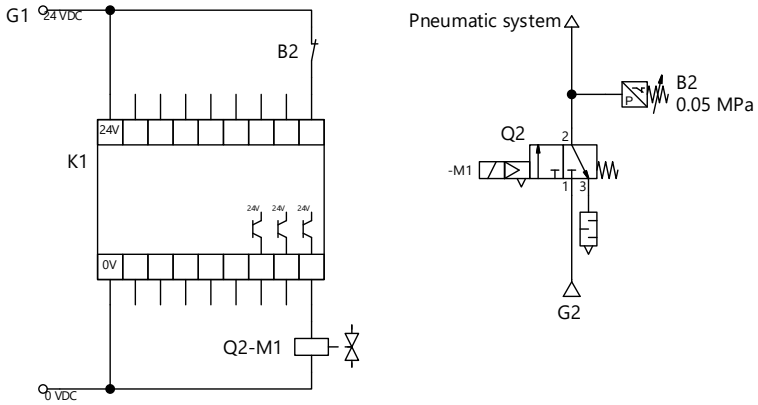
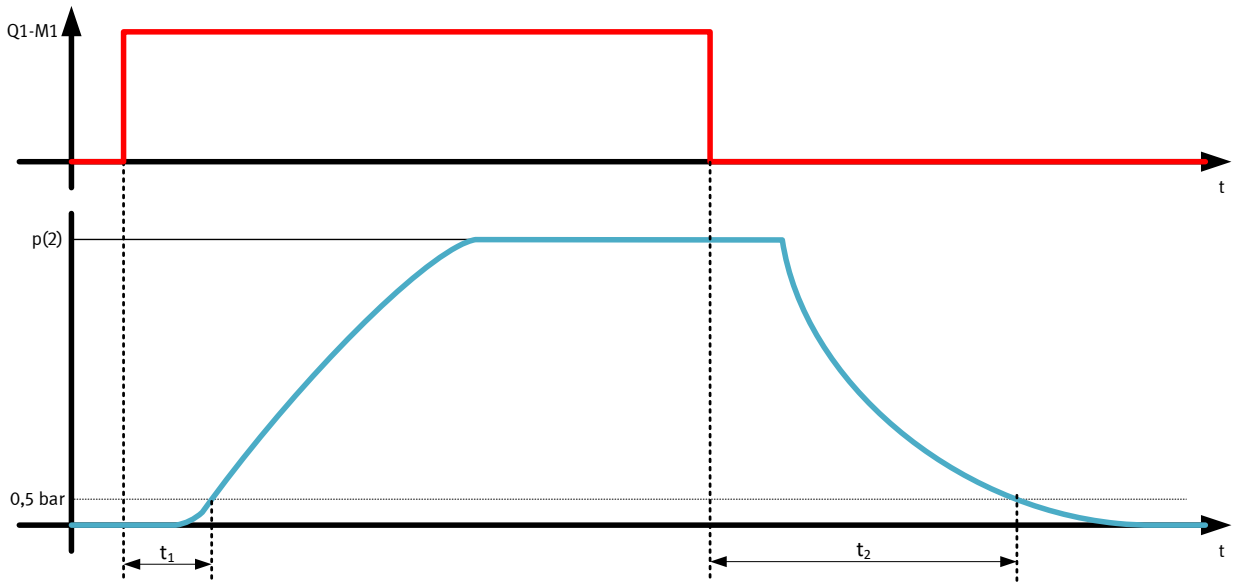


Figure 14 Diagnosis with pressure switch monitoring



Legend
-M1 Control signal valve solenoid
p(2) Pressure at port 2 of valve Q2
t_1 Time delay from activation of valve coil to signal change of pressure switch
t_2 Time delay from deactivation of control valve coil to signal change of pressure switch

Figure 15 Switching times

Function of the circuit

- If the safety switching device K1 activates the valve solenoid Q2-M1, the valve Q2 switches from the normal position to the switching position.
- This opens the volume flow path from 1-2 and closes port 3, so that the pressure at port 2 of the valve rises. If the set limit value of the pressure switch is exceeded, the output of pressure switch B2 opens.
- The time delay from the activation of the valve solenoid to the opening of the output of the pressure switch is the time that is monitored by the safety switching device to check the subfunction switching in the switching position of the valve.
- If the safety switching device K1 no longer controls the valve solenoid Q2-M1, the valve Q2 switches from the switching position to the normal position.
- When the piston slide reaches the normal position, the volume flow path 2-3 is opened and port 1 is closed so that the pressure is discharged at port 2 of the valve. If the pressure falls below the set limit value of the pressure switch, the output of pressure switch B2 closes.
- The time delay from the switching off of the valve solenoid to the closing of the output of the pressure switch is the time that is monitored by the safety switching device in order to check the subfunction switching in normal position of the valve.

Monitoring times

In the safety switching device, the time for monitoring the switching process must be configured. When monitoring with a pressure switch, these times depend on the application. Since low pressure is monitored when switching from the normal position to the switching position, this switch-on time can be in the order of size of the switching time of the valve. Over the service life of many valves, the switching time usually increases, so that a safety factor of 2...5 should be used for this setting.
Since when switching from the switching position to the normal position, the downstream pneumatic system or drive must first be depressurised before the pressure switch closes the contact again, this time must always be determined in relation to the application.

5.3 Example circuit for diagnosis with limit switch drive

5.3.1 Monitoring function

With the limit switches on the drive, positioning time monitoring of the drive is implemented by the safety switching device. Each time a valve solenoid is activated, the corresponding limit switch is expected to close its output after the expected positioning time.

5.3.2 Example circuit for diagnostics with limit switch drive

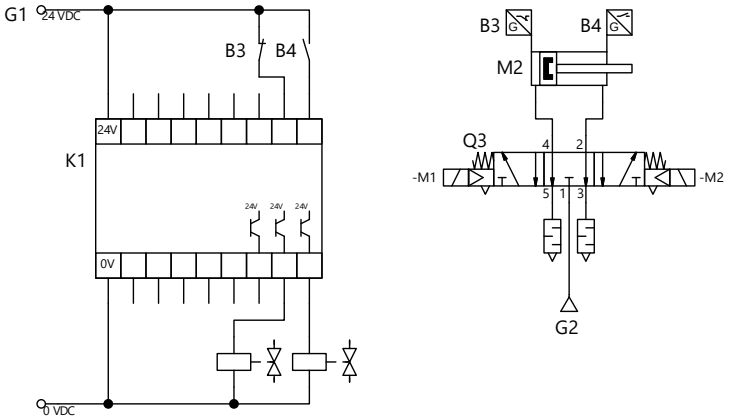
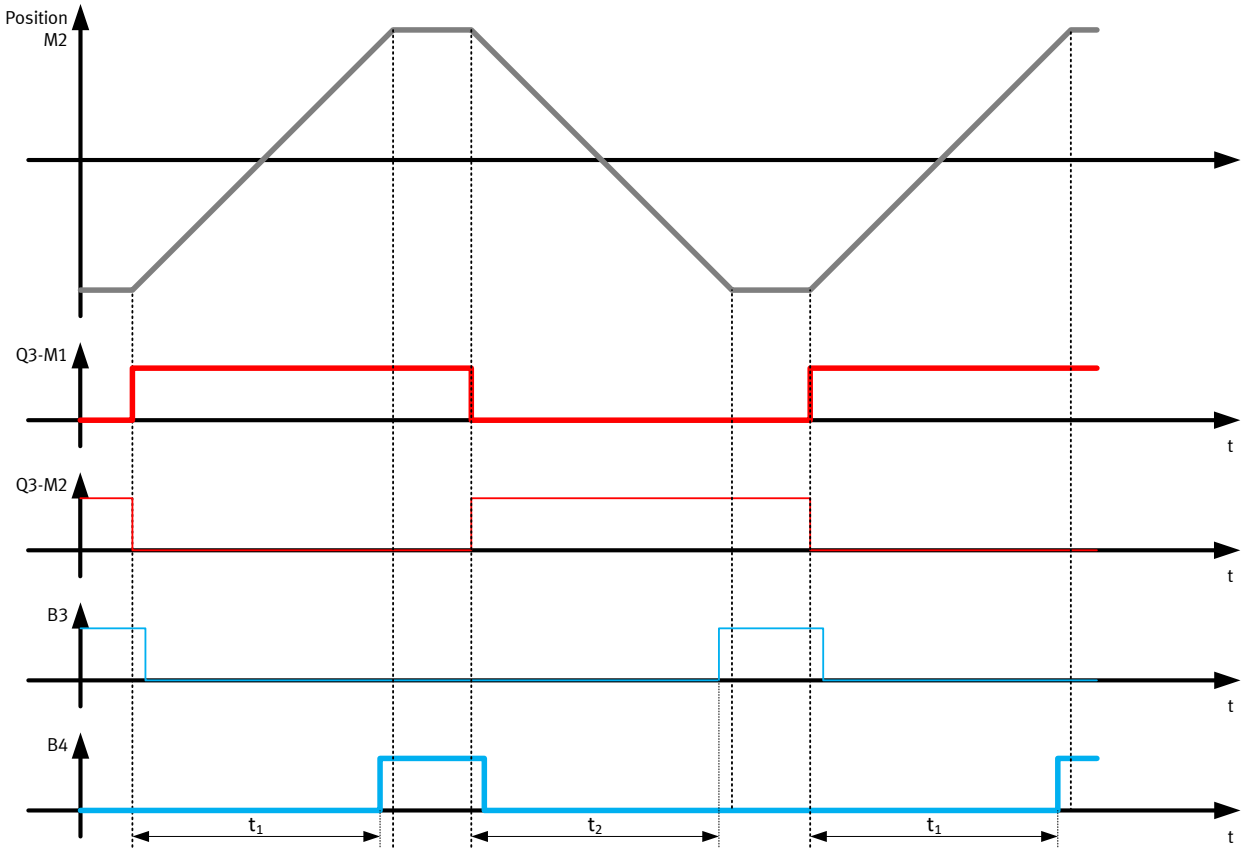


Figure 16 Diagnosis with limit switches on the drive



Legend

Position M1	Position of pneumatic drive M1
Q3-M1	Control signal valve solenoid -M1 of the valve Q3
Q3-M2	Control signal valve solenoid -M2 of valve Q3
B3	Output signal limit switch B3
B4	Output signal of limit switch B4
t_1	Time delay from activation of valve coil Q3-M1 to signal change of limit switch B4
t_2	Time delay from activation of valve coil Q3-M2 to signal change of limit switch B3

Figure 17 Switching times

Function of the circuit

- If the safety switching device K1 activates the valve solenoid Q3-M1, the valve Q3 switches from the normal position to the corresponding switching position.
- This opens the volume flow paths of 1-4 and 2-3 and closes port 5, so that the left chamber of the pneumatic drive is pressurised and the right chamber is exhausted. This extends the pneumatic drive.
- The safety switching device monitors the time from the actuation of the valve solenoid Q3-M1 until the pneumatic drive leaves the retracted position, i.e. limit switch B3 is no longer actuated. In addition, the safety switching device monitors the time from the actuation of the valve solenoid Q3-M1 until the extended position of the pneumatic drive is reached, i.e. limit switch B4 is actuated (monitoring of the positioning time).
- If the safety switching device K1 no longer activates the valve solenoid Q3-M1, but instead activates the valve solenoid Q3-M2, the valve Q3 switches to the other switching position.
- This opens the volume flow paths of 1-2 and 4-5 and closes port 3, so that the right-hand chamber of the pneumatic drive is pressurised and the left-hand chamber is exhausted. This retracts the pneumatic drive.
- The safety switching device monitors the time from the actuation of the valve solenoid Q3-M2 until the pneumatic drive leaves the extended positions, i.e. the limit switch B4 is no longer actuated. In addition, the safety switching device monitors the time from the actuation of valve solenoid Q3-M2 until the retracted position of the pneumatic drive is reached, i.e. limit switch B3 is actuated (monitoring of the positioning time).
- If the two valve solenoids Q3-M1, Q3-M2 are no longer actuated, valve Q3 switches to the normal position. If no forces act on the piston, the last position of the pneumatic drive is maintained.

Monitoring times

The time for monitoring the positioning process must be configured in the safety switching device. When monitoring with limit switches, these times must always be determined in relation to the application.

Note

It should be noted that the switching time of the valve is usually very short compared to the positioning time of the pneumatic drive. It can happen that a malfunction of the valve is only detected after the monitored positioning time has elapsed. This should not lead to any danger in the application.

5.3.3 Checking the safety sub-functions and diagnostics in the maintenance cycle of the machine

In the context of occupational health and safety, the safety functions of a machine must be checked regularly. The reason for this is that the diagnostic measures cannot normally detect all possible faults. Therefore, the characteristics of the safety-relevant parameters should be recorded and documented with external measuring devices before or during commissioning. The aim is to uncover faults that cannot be detected with the existing diagnostic measures.

In the case of directional control valves, these are at least the control signals, movement characteristics, signals from the sensors, pressures at the valve outputs, leakage.

6 Longer Downtimes and Dynamization of Valves

For machines with pneumatic or electropneumatic valves that are not switched on or off for weeks or months, the switch-on and switch-off time of the valves is extended.

6.1 Causes and Their Effects

If the moving parts of the valve remain stationary in a switching position (switched off or on) for a longer period of time, a temporary change in the tribological[2] system may occur. This change in the switching behaviour of the valve appears as a noticeable increase in the switching time (or the switching pressure) during the first switching operations.

Possible causes for the change in switching behaviour are, for example, the stick-slip effect, greater adhesion of the slightly dried lubricants, the settling behaviour of the seals, etc.

These are normal causes common to all moving components. They cannot be completely avoided, they can only be reduced by avoiding the negative influences.

Negative influences on the switching behaviour after a standstill can have the following influencing factors (not complete list, in the limit range within the specified technical data of the product):

- Low control pressure
- Oily air
- Extremely low or extremely high ambient temperatures
- Extremely low or extremely high media temperatures
- Low and high relative humidity
- Environments with high exposure to dust and dirt

If such influencing factors are present, the function of the valve should be checked. In practice, the easiest way to do this is to run the machine through several empty cycles after switching it on, possibly at a slightly higher control pressure (without exceeding the maximum permissible pressure). As a rule, the expected switching behaviour will be restored after several switching operations.

In addition, the effects of the above-mentioned effects can be reduced if the operating conditions in the application are as close as possible to the nominal operating conditions:

- Control pressure 6 bar,
- ambient temperature 23°C,
- compressed air temperature 23°C,
- compressed air quality according to the data sheet of the valve,
- dew point of compressed air ‹7°C,
- unlubricated air.

6.2 Recommended switching frequency

We recommend that all valves should be switched at least once a week. They should be switched once to all switching and normal positions (complete switching cycle).
Exceptions to this are all valves that are suitable for low-demand mode according to IEC 61508 or where the operating instructions specify forced dynamization.

6.3 Recommendations for Adapting the Switching Frequency

If the switching frequency of standard valves in factory automation falls below once a week in safety-related applications, e.g. during storage / transport of a machine, company holidays or normal operation, the switching behaviour of the valve should be checked before use, e.g. by a function test when the machine is switched on. In safety-related applications according to EN ISO 13849-1, this function test can be carried out by a manual safety request, e.g. opening the safety door or actuating the emergency stop switch.

It may be necessary to adjust the recommendation of actuation once a month or week to the observed behaviour of the machine.

- If there is a negative change, the actuation frequency should be increased. However, it should be considered that with many valves, friction increases over the service life is one of the main causes of failure (in addition to leakage, functional failure, increase in switching pressure) according to ISO 19973-2.
- However, it may also be shown that the actuation frequency can be extended to a longer period. It must be considered here that factory automation valves are designed for regular actuation.

---

[2] Tribology is the science and technology of interacting surfaces in relative motion. It deals with the scientific description of friction, lubrication and wear.

In the case of safety components, however, the specifications of the operating instructions for the switching frequency must always be observed. An extension is not permissible.

6.4 Dynamization of Safety-related Valves

According to EN ISO 13849, direct or indirect monitoring is necessary for safety-related valves[3] from category 2 in order to achieve the required level of diagnostic coverage. This monitoring requires dynamization in order to be able to detect static failures[4] by means of a dynamic test[5]. The possible static failures are listed in EN ISO 13849-2 in table B.3, e.g. with the faults “Change in switching times” and “Non-switching ... or incomplete switching ...”.

For safety-related applications according to category 1, the recommendations should be observed. From category 2, the switching frequency is determined by the test cycle of the safety switching device used or the testing is carried out automatically with each safety-related switching.

[3] For certified safety components, a minimum switching frequency is usually specified in the operating instructions.

[4] Static failures are all failures that can occur when the valve is not actuated and are only detected by switching the valve (a dynamic test).

[5] For valves, a dynamic test can be a function test in which the valve is moved from the current switching state to another switching state and the function is checked via direct monitoring (spool position monitoring) or indirect monitoring (e.g. pressure sensor, limit switch on the cylinder). Further possibilities are mentioned in ISO 13849-1.

7 Duty Cycle

The duty cycle [according to VDE 0580, 3.6.1.1] is the time between switching the control signal on and off. Three operating modes can be distinguished for valve solenoids

1. continuous operation (S1) [acc. to VDE 0580, 3.10.1]
   In continuous operation, the duty cycle is long enough to reach the steady-state temperature.
2. short-time duty (S2) [according to VDE 0580, 3.10.2]
   In short-time duty, the duty cycle is so short that the steady-state temperature is not reached and the switching pause is so long that the valve solenoid cools down to a temperature that deviates less than 2 K from the ambient temperature.
3. intermittent duty (S3) [according to VDE 0580, 3.10.3]
   In intermittent operation, the duty cycle and the pause alternate in regular sequence, whereby the pauses are so short that the valve solenoid does not cool down to the ambient temperature.

The duty cycle is a characteristic value that is important for the design of the insulation for the coil of the valve solenoid. Usually, the steady-state temperatures are reached in 10 to 30 minutes. The duty cycle of electrically operated valves or solenoid coils are specified in the data sheet.

Important notes

The duty cycle is **inadmissibly** associated with the operating modes according to IEC 61508, 3.5.16.

The operating mode according to IEC 61508 describes the type of use of a safety function.

- Operating mode with low demand (low-demand mode)
  The safety function is only executed on demand in order to transfer the dangerous machine function into a defined safe state. The frequency of the request is not more than once a year.
- Operating mode with high demand (high-demand mode)
  The safety function is only executed on demand in order to transfer the dangerous machine function into a defined safe state. The frequency of the request is more than once a year.
- Operating mode with continuous demand (continuous mode)
  The safety function maintains the hazardous machine function in a safe state as part of normal operation.

These parameters are necessary to determine the reliability of the execution of a safety function.

Attention
For all operating modes, with the exception of high-demand mode, valves are only suitable for this operating mode if the operating mode, e.g. low-demand mode, is explicitly confirmed in the Product Reliability Data Sheet. Otherwise, the valves must be dynamized, i.e. the valves must be switched regularly. Background information and possible measures for this are given in section “6 Longer Downtimes and Dynamization of Valves”.

Attention
The duty cycle does not indicate whether the valve is suitable for low, high or continuous mode according to IEC 61508-4.

8 Safety Principles

The **safety principles** of ISO 13849-2 are design features to be observed for mechanical, pneumatic and electrical systems in order to ensure sufficient reliability of a safety circuit and to control systematic faults.
The **basic safety principles** correspond to good engineering practice for mechanical, pneumatic and electrical systems in all functional circuits in a machine or plant. Based on ISO 13849, these functional circuits can also be assigned a performance level a or b and then become safety circuits.
The **well-tried safety principles** are further design features to increase the reliability of safety circuits from PL c compared to functional circuits.
Important
The safety principles listed in ISO 13849-2 refer to systems. Within the limits of a component, assembly or part in such a system, all of these safety principles can never apply.

8.1 Relevant basic safety principles for valves

Within the limits of directional control valves, the following basic safety principles may be relevant. Compliance with the relevant basic safety principles is confirmed across the board in the Product Reliability Data Sheet of the valve. As a rule, the following safety principles are assessed:
Mechanical System

- Use of suitable materials and adequate manufacturing
- Correct dimensioning and shaping
- Proper selection, combination, arrangements, assembly and installation of components/system
- Use of de-energization principle
  The principle of energy separation (or closed circuit principle) requires that when the electrical and/or pneumatic control signals, e.g. 12, 14, or the working pressure, e.g. from 1, is interrupted and exhausted, the main stage assumes its safe state. For monostable valves this can be the normal position or for bistable valves the last switching position.
  Within the limits of the valve, it is only evaluated whether a safe state is possible. Since the evaluation of this safe state is only possible with a known safe state of the application, the user must always additionally evaluate the application-related aspects.
- Proper fastening
- Protection against unexpected start-up
  Within the limits of the safety principles, “protection against unexpected start-up” is usually implemented by “application of the principle of energy separation” or “safe position”.
- Simplification
- Proper lubrication
- Proper prevention of the ingress of fluids and dust

Pneumatic System

- Use of suitable materials and adequate manufacturing
- Correct dimensioning and shaping
- Proper selection, combination, arrangement, assembly and installation of components/system
- Use of de-energization principle
  See information in the section “Mechanical system”
- Proper fastening
- Protection against unexpected start-up
  See information in the section “Mechanical system”
- Simplification

Electrical System

- Use of suitable materials and adequate manufacturing
- Correct dimensioning and shaping
- Proper selection, combination, arrangements, assembly and installation of components/system
- Use of de-energization
  See information in the section “Mechanical system”
- Transient suppression
  Only applicable for electrically operated valves. This safety principle is observed for valves with holding current reduction. If another measure is integrated to limit the voltage pulse when the valve solenoid is switched off (free-wheeling diode, varistor, RC element), this is specified in the technical characteristics of the valve. If this information is missing, additional measures must be taken by the user, see also the "General conditions of use, section spark suppression".
- Protection against unexpected startup
  See information in the section “Mechanical system”

8.2 Relevant well-tried safety principles for valves

Within the limits of directional control valves, the following well-tried safety principles may be relevant. Compliance with the relevant well-tried safety principles is confirmed across the board in the Product Reliability Data Sheet of the valve. As a rule, the following safety principles are assessed:

Mechanical System

- Use of carefully selected materials and manufacturing
- Use of components with oriented failure mode
- Overdimensioning/safety factor
- Safe position
  Only applicable for valves with mechanical or pneumatic spring or for valves with a detent.
  Note: For bistable valves without a detent, the manufacturer's fault exclusion “automatic change of the main stage without input signal” may be a higher-quality alternative to this safety principle.
- Increased OFF force
  Only applicable for valves with mechanical or pneumatic spring or for valves with a detent.
- Careful selection, combination, arrangement, assembly and installation of components/system related to the application
- Careful selection of fastening related to the application
- Use of well-tried spring
  Only applicable for valves with mechanical or pneumatic spring or for valves with a detent.

Pneumatic System

- Overdimensioning/safety factor
- Safe position
  See information in the section “Mechanical system”
- Increased OFF force
  See information in the section “Mechanical system”
- Valve closed by load pressure
  Only applicable if explicitly listed in the “design characteristics” of the data sheet or data sheet product reliability.
- Use of well-tried spring
  If the valve is classified as “well-tried according to ISO 13849-1" in its product reliability data sheet, the springs it contains are also well-tried.
- Sufficient positive overlapping
  If “positive overlap” is specified in the characteristics, this characteristic is present by design. Only if a fault exclusion “failure of positive overlap” is specified, the requirement “sufficient” is fulfilled.
- sufficiently negative overlapping (safety principle added by Festo).
  If “negative overlap” is specified in the characteristics, this characteristic is present in the design. Only if a fault exclusion “failure of negative overlap” is specified, the requirement “sufficient” is fulfilled.

Electrical System

- Separation distance
- Overdimensioning

9 Well-tried component

The confirmation that a valve is a “well-tried component according to ISO 13849-1” is the result of the component manufacturer's evaluation of whether this valve is suitable for use in safety circuits and achieves sufficient reliability for this purpose.

Important

This confirmation must always be checked by the user whether the valve can also be classified as “well-tried” for his particular application.

The classification “well-tried component” for a specific application must first be denied by the user if

- Characteristics of the valve cannot be maintained, e.g. pressure peaks, too high or too low temperatures;
- Substances affecting the material in the environment of the valve, e.g. solvents that can attack seals and plastics;
- Heavy contamination by dust and other substances that can penetrate pneumatic components and cause malfunctions, e.g. fine dust particles.
- etc.

In these examples, additional measures can make the classification “well-tried component” possible again, but these must always be evaluated in relation to the application.

Example:

Well-tried component[1)]	yes

[1)] The product is a well-tried product for a safety-related application according to ISO 13849-1. The relevant basic and well-tried safety principles according ISO 13849-2 for this product are fulfilled. The suitability of the product for a precise application must be verified and confirmed by the user.

Additional notes

In order for Festo to classify a newly developed product as “well-tried according to ISO 13849-1”, the following points must be met

- Development process is adhered to
- Development confirms the basic and well-tried safety principles on the basis of checklists.
- Technical characteristics of the product have been tested and approved by trials.
- Lifetime tests have been carried out, B_{10} value determined and evaluated by experts
- Well-tried is confirmed by
    - Reliability determined by FMEDA, i.e. proof of well-tried based on failure rates from databases and evaluated by experts.
    - confirmed by evaluation of market returns (only for products that have been on the market for a long time).
    - Basic and well-tried safety principles AND proof of technical characteristics through testing.

“Well-tried component” refers to well-tried components for safety-related applications according to ISO 13849-1.

Attention

It cannot be deduced from this that valves meet the requirements for proven-in-use elements according to IEC 61508-2, 7.4.10.

At Festo, this is confirmed via the product reliability data sheet.

10 Service life rating B10

The reliability of valves is indicated by the service life rating B_{10}. This is a value usually determined statistically by tests, which indicates the number of cycles until 10 % of the tested valves have failed.

The life expectancy value is determined on the basis of the standards

- ISO 19973-1:2015-08 - Pneumatics - Evaluation of reliability of components by testing - Part 1: General methods
- ISO 19973-2:2015-09 - Pneumatics - Evaluation of reliability of components by testing - Part 2: Valves

The service life values determined on the basis of ISO 19973 always refer to the standard conditions:

Test pressure	6.3 bar ± 0.3 bar
Ambient temperature	23°C ±10°C
Medium temperature	23°C ±10°C
Filter	5 µm
Dew point	+7°C
Additional lubrication	none

If the operating conditions in a particular application differ from this, the user should evaluate whether an adjustment of the B_{10} value is necessary. The possible influences due to pressure, temperature, substances affecting the material, actuation, etc. are so varied that no generally applicable specifications can be made by Festo.

Example:

Service-life value B_{10}[2)]	10 Mio cycles

[2)] The ascertainment of characteristic service life values is generally based on the ISO 19973 "Pneumatic fluid power – Assessment of component reliability by testing".

10.1 Estimation of B_{10D} values

ISO 13849-1, Annex E, gives B_{10D} values for various components as good engineering practice. The application of these values can lead to considerable deviations for various pneumatic components, e.g. for on-off valves. Therefore, if B_{10} values are missing, always check with the manufacturer.

The B_{10} value can be used to estimate a B_{10D} value using the formula below.

$$B_{10D} = \frac{1}{RDF} \cdot B_{10} = \frac{1}{0{,}5} \cdot 10.000.000 = 20.000.000$$

The abbreviation RDF stands for “ratio of dangerous failures”. For pneumatic and electromechanical components, an RDF of 50% can be assumed according to ISO 13849-1, Table C.1, Note 1, unless otherwise specified.

Notes

- There are components for which an RDF of 50% must not be assumed, e.g. locking units and holding brakes. For these products, most possible failures will result in a dangerous failure, so an RDF of 100% should be assumed.
- Festo provides the B_{10} values for the evaluation of circuits as a VDMA library ↗ Link.

11 Design characteristics Mechanical Spring Reset

The ISO 13849-2 standard states in table A.5 that various fault exclusions are possible for pressure-coil springs if well-tried springs and carefully selected types of fastening are used. If these fault exclusions can be assumed, a spring force is always present and there is the possibility of achieving high reliability with single-channel circuits.

First of all, it must be established what the standard DIN EN ISO 13849-2 understands by pressure-coil springs. Table A.2 under "Use of well-tried spring" gives the following information:

Well-tried compression coil springs may also be designed, by

- use of carefully selected materials, manufacturing methods (e.g. pre-setting and cycling before use) and treatments (e.g. rolling and shot-peening),
- sufficient guidance of the spring,
- clearance between the turns less than the wire diameter when unloaded, and
- sufficient force after a fracture(s) is maintained (i.e. a fracture(s) will not lead to a dangerous condition).

ISO 13849-2 means a pressure-coil spring as shown in the picture on the left. Under no circumstances should this be confused with the spring on the right, which is usually also a pressure-coil spring, but not in the sense of the fault exclusion in ISO 13849-2.

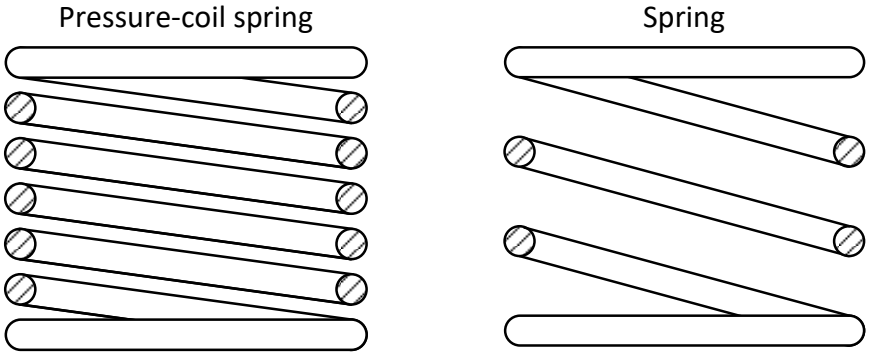


Figure 18 Pressure-coil spring and springs

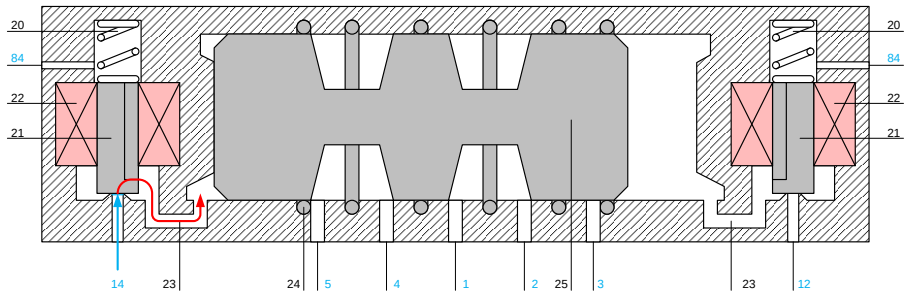
The essential feature is that the coil distance with unloaded spring is smaller than the wire diameter. This means that any wire breakage that may occur generally only leads to a minimal reduction in the spring force. With this justification, the basis for this exclusion of faults becomes understandable.

The springs in pneumatic valves and pneumatic actuators do not fulfil this essential characteristic. The springs commonly used in pneumatics are cylindrical or conical coil springs whose coil distance is considerably greater than the wire diameter. A fault exclusion according to ISO 13849-2, Table A.5, is therefore not applicable for pneumatic valves and pneumatic actuators.

Notes

- Table A.2 also lists the specifications for "well-tried springs". These specifications are not applicable to pressure-coil springs for which fault exclusions according to Table A.5 are to be assumed.
- The use of a fault exclusion spring fracture in pilot operated pneumatic valves is extremely questionable. All pilot valves known to us in pneumatics are poppet valves. If a spring breaks there, the spring force is considerably reduced and the force exerted by the applied control pressure will open the pilot valve and switch the main stage of the valve. This allows a dangerous movement of a connected pneumatic actuator.

The figure below shows a diagram of a bistable 5/2 directional control valve. If the spring of the left pilot valve (20) breaks, the pilot pressure at port 14 opens the pilot valve and the spool piston of the main stage is moved to the other switching position. A connected pneumatic actuator will move to the opposite end position.



Legend

1, 2, 3, 4, 5	Main ports
12, 14	Control ports
20	Springs of the pilot valves
21	Pilot valve armature
22	Coil, unpowered
23	Control signal for operation of the main stage
24	Seals, soft sealing
25	Main stage spool valve
84	Exhaust of the control signal of the main stage

Figure 19 5/2 directional control valve, bistable

12 Design characteristics type of reset with pneumatic spring

12.1 Summary

- An pneumatic spring is to be considered at least equivalent to a mechanical spring, if the pressure supply for the pneumatic spring is ensured.
- The predominant failure modes of mechanical springs are random (probabilistic failures). Air springs are more likely to fail due to systematic failures, which are evaluated with an FMEA.
- If the compressed air supply to the pneumatic spring is interrupted and exhausted together with the operation pressure or control pressure, there is a residual risk when restarting until the pneumatic spring acts from a pressure of approx. 1 bar.

12.2 Explanations

For the use of pneumatic springs in valves, the requirements of ISO 13849 must be determined and compared with the characteristics of pneumatic springs. The requirements are described in the following safety principles:

- Safe position
- Use of well-tried springs
- Safe switching position
- Increased OFF force

Requirement 1: safe position

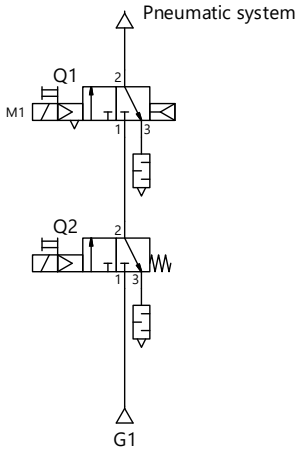
The standard ISO 13849-2 specifies the following requirements in table B.2:

> "The moving part of the component is held in one of the possible positions by mechanical means (friction only is not enough). Force is needed to change the position."

Here it is first necessary to define the term "mechanical". According „Physik für Ingenieure (Physics for Engineers)" from Ekbert Hering, "mechanics is the part of physics that deals with the composition and equilibrium of forces acting on a body at rest (statics), with processes of motion (kinematics) and with forces as the cause of motion (dynamics)." In the context of functional safety, this means that the normal position must be maintained with an existing force.

Fulfilment of the requirements of a safe position thus depends on the application of force by an air spring to the piston slide. The force generated by the air spring depends on the operating states of the compressed air supply.

- **Pneumatic spring with supply from port 1 (working pressure)**
  For valves with internal supply of the pneumatic spring from port 1 (working pressure), the following behaviour usually results when the compressed air supply is un-interrupted and exhausted with valve Q2:
  Valve Q1 is actuated and in the switching position: If port 1 is slowly exhausted, the subsequent pneumatic system is exhausted. If the minimum control pressure is significantly undershot, the air spring usually has a greater force effect than the control air through the pilot valve, so that the piston spool of the main stage is switched to normal position.
  If port 1 is exhausted very quickly, the subsequent pneumatic system and the control pressure in the valve are exhausted so quickly that the main stage of valve Q1 can get stuck in the switching position or an intermediate position. In this case, the safe position is not ensured. In most applications is an exhausting not shorter than the switching time of the valve. To check this, we recommend a short test with a pressure sensor at port 2 of valve Q1.
  Valve Q2 is switched on, valve Q1 is switched on, pressure is present at connection 2. Valve Q2 is switched off, valve Q1 is switched off. If Q2 is now switched on and there is no indication of pressure at port 2 of valve Q1, a safe position is also given here.
  Note
  The main stage of the valve shifts due to vibrations and shocks. If it is then switched on via a soft start valve, pressure can build up at port 2 until the air spring takes effect. It is therefore important to ensure that the characteristic values for vibration and shock are not exceeded.



If the worst case is considered, i.e. the valve is in the switching position when the compressed air is switched on at port 1, the pneumatic spring starts to act at a pressure of approx. 1 bar (depending on design) and switches the valve to the normal position. This can lead to a pressure build-up at port 2, which is normally in the order of magnitude of the switching time of the valve. Depending on the size of the valve, hoses and drives, it must be assessed whether a movement can occur. For standard drives, the minimum required operating pressure is 1...2 bar, so that in almost all applications no dangerous movement is likely to occur.

Possible measure for compliance with the safety principle “safe position”:

In case of single valves or the two valves Q1, Q2 are in different voltage zones: The valves are to be switched with a time delay, i.e. during the switch-on process, valve Q2 must always be actuated first so that a working pressure is present at port 1 of valve Q2 and then valve Q1 may be actuated. When switching off, valve Q1 should always be switched off first so that the valve is switched to the normal position by the pneumatic spring before valve Q2 is switched off. In this way, the safety principle of “safe position” can be maintained.

For valve terminals with load voltage switch-off and the two valves Q1, Q2 are in the same voltage zone: It must be checked whether, in the worst case (see above), a movement of an drive or other hazard can occur. Depending on the application, it must be evaluated which measures can be used to sufficiently reduce the risk that may exist.

- **Pneumatic spring with supply from port 12/14 (pilot air pressure)**

  If the valve has a pneumatic spring supplied from one of the ports 12 or 14, the working pressure at port 1 can be interrupted and exhausted and the air spring remains functional.

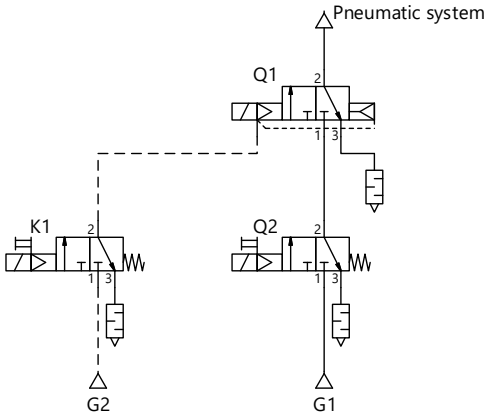
  Valve Q1 is activated and in the switching position: When port 12 is slowly exhausted, the pilot air for the pilot valve and the air spring is exhausted. If the minimum control pressure is significantly undershot, the air spring usually has a greater force effect than the control air through the pilot valve, so that the piston spool of the main stage is switched to normal position.

  If the port 12 is exhausted very quickly, the pilot air is exhausted so quickly that the main stage of valve Q1 can get stuck in the switched position or an intermediate position. In this case, the safe position is not ensured.

  Possible measure for compliance with the safety principle “safe position”:

  In case of single valves or the two valves Q1, Q2 are in different voltage zones: The valves must be switched with a time delay, i.e. the electrical control of valve Q1 must first be switched off so that this valve switches to the normal position before the pilot air supply is interrupted and exhausted with valve K1.

  For valve terminals with load voltage switch-off and the two valves K1, Q2 are in the same voltage zone: It must be checked whether, in the worst case (see above), a movement of an drive or other hazard can occur. Depending on the application, it must be evaluated which measures can be used to sufficiently reduce the risk that may exist.



Requirement 2: Use of well-tried springs

According to ISO 13849-2, table A.2, a well-tried spring requires:

- "Use of carefully selected materials, manufacturing processes (e.g. pre-setting and cycling before use) and treatments (e.g. rolling and shot-peening);"
  With an air spring, the carefully selected materials correspond to the prepared compressed air. The minimum required compressed air quality is specified in the data sheet of the valve under "Operating medium" and can be ensured by a suitable service unit.
  The carefully selected manufacturing process is the tribological system of the valves. The proof is the lifetime characteristic value B_{10} determined by service life tests. This is given in the product reliability data sheet.
- Adequate guidance of the spring
  With an air spring, the piston slide is properly guided, and the air column cannot break out through the guide tube.
- Sufficient safety factor for fatigue loading (i.e. high probability of no breakage).
  Fatigue strength is given with air, as no deformation or breakage can occur due to elastic or inelastic stresses. Breakage can be equated with leakage in the case of an air spring. If leakage occurs, it is compensated for by the compressed air supply.

The behaviour described here is an advantage over a mechanical component. If mechanical springs are designed well-tried, e.g. according to EN 13906-1 [4], it cannot be assumed that the mechanical spring will not break. A spring breakage can lead to the normal position no longer being assumed and the dangerous switching position of the valve being maintained.

An air spring can thus be considered at least equivalent to a well-tried mechanical spring.

Requirement 3: Safe switching position

The safe switching position of a valve is defined in ISO 4414, 5.4.6.9:

> Any actuator required to maintain its position or to adopt a specific position for safety in the event of a control system failure shall be controlled by a valve that is held in or switched back to the safe position (e.g. by spring tension or comparable physical principle).
>
> Note: To leave the safe position, pressure or force is necessary; see ISO 13849-2, table B.2

That the air spring is at least equivalent to a mechanical spring is fulfilled by the proof of requirement 2 (see above). This means that the safe switching position (normal position) is assumed as long as the minimum operating pressure is not fallen below.

Requirement 4: Increased OFF force

The increased OFF force requires according to ISO 13849-2 [2], table B.2:

> "One solution can be that the area ratio for moving a valve spool to the safe position (OFF position) is significantly larger than for moving the spool to ON position (a safety factor)."

The increased OFF force, i.e. that the safe normal position is left, is ensured by the application of the pneumatic spring, as the additional force of the pneumatic spring must be overcome.

Recommended measures

- In order to ensure the minimum operating pressure for valves with air springs, this should be monitored. This can be considered as part of the well-tried safety principle of "appropriate range of working conditions" [3, table B.2]. This pressure monitoring can be implemented with a pressure switch with normally open contact, whose pressure setting is switched on to a value above the minimum pressure of the valves with air spring. If the pressure drops below this switching point during operation, the compressed air supply to the pneumatic system is switched off with the electrical switch-on valve of the maintenance unit.

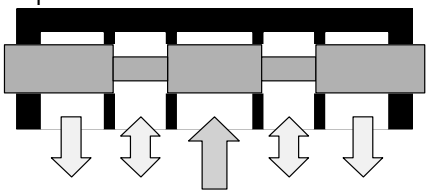
- With most pneumatic drives, a higher minimum pressure is required for movement than for activation of the pneumatic spring. If this is the case, no dangerous movement can be generated under the usual operating conditions. For this purpose, the technical data of the pneumatic drive and the valve used must be compared.
- If a nozzle is supplied by the valve, a volume flow may escape at the nozzle. However, this depends on the specific conditions in the application and must therefore always be evaluated in relation to the application.
- If the above measures cannot be implemented or evaluated, the pneumatic system should only be pressurised with activated protective measures, e.g. closed safety doors.
- To consider: If high vibration/shock values occur when the valve is switched off, the main stage can shift. This can result in a short build-up of pressure at 2 when switching on with a pressure build-up valve.

13 Overlap

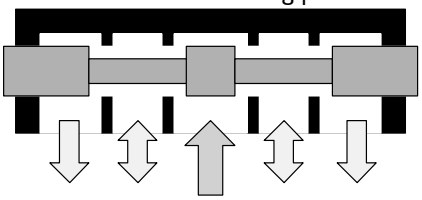
13.1 Piston spool valves

In piston spool valves, overlap refers to the distance in the longitudinal direction between the fixed and movable control edges.

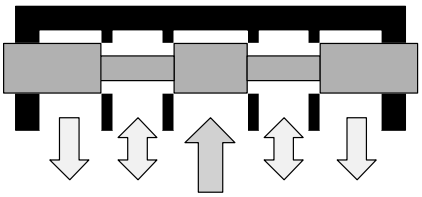
- With a **positive overlap**, the volume flow paths of the switching positions of the valve are blocked during the switching process. One flow path is blocked before the other flow path is opened.



- In the case of a **negative overlap**, the volume flow path of one switching position remains at least partially open until the volume flow path of the other switching position is at least partially opened.



- In the case of an **undefined overlap**, the type of overlap cannot be clearly determined due to manufacturing tolerances.



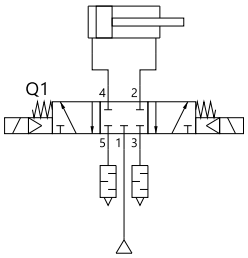
When using piston spool valves in functional safety, the fault behaviour of the valves must also be considered. ISO 13849-2, Table B.3, lists the following fault:

> Not complete switching (stuck in any intermediate position).

For this fault, the overlap has a significant influence on the fault effects and their possible use:

- Fault effects and application of valves with positive overlap
  If a valve with positive overlap gets stuck in the closed intermediate position, the volume flow paths through the valve are closed. This has the consequence
  - Compressed air can be trapped in the downstream pneumatic system or a downstream pneumatic drive;
  - The supply of compressed air is interrupted;
  - Exhausting of the downstream pneumatic system or pneumatic drive is not possible;

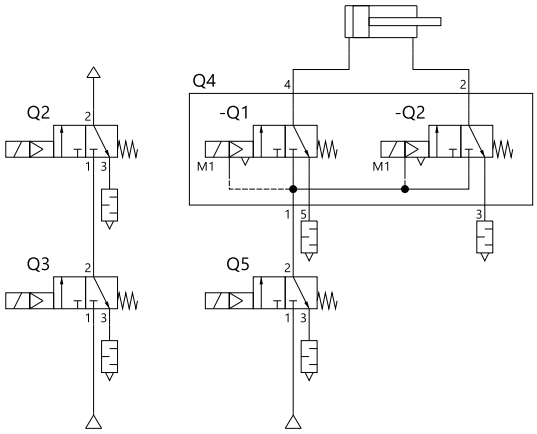
  Application: This is a desirable feature for valves that are to enclose compressed air in a subsequent pneumatic drive.



Example
The safety sub-function “safe stop and shut-off (SSC)” is to be implemented. In this case, it is recommended to use a valve with the feature “positive overlap”. In this way, the well-tried safety principle “sufficiently large positive overlap in spool valves” according to ISO 13849-2, Table B.2, can also be implemented.

- Failure effects and application of valves with negative overlap
  If a valve with negative overlap gets stuck in an intermediate position, at least one volume flow path remains open. This results in
  - Compressed air will be exhausted via port 3 (or 5);
  - The supply of compressed air is not interrupted.
  - If port 1 of the working valve (in the examples Q2 and Q4) is exhausted, exhausting is ensured through ports 3 (or 5) or 1

  Application: This is a requirement to be complied with for valves that are to ensure exhausting of the downstream pneumatic system or drive when port 1 is exhausted.



Example 1:
If a 2-channel exhaust is to be ensured by connecting two 3/2-way valves in series, if the working valve Q2 has a negative overlap. If both valves Q2 and Q3 are no longer actuated, they switch to normal position. In the case of the failure “not fully switched”, exhausting can be ensured via port 3 or via port 1 of valve Q2, provided it has a negative overlap.

- Effects of faults and use of valves with zero overlap or indefinite overlap
  If a valve with zero overlap or indefinite overlap gets stuck in an intermediate position, it is not predetermined whether the volume flow paths are open or closed. This has the consequence
  - It is not known whether compressed air is included or exhausted in the subsequent pneumatic system.
  - It is not known whether the compressed air supply is interrupted;

  In applications where pressure, speed, flow, etc. are to be controlled, this is a desired feature of the working valve. It is recommended to implement safety sub-functions through external valves.

13.2 Poppet valves

Negative overlap on poppet valves

Most poppet valves have a negative overlap due to their design. However, there are also poppet valves with zero or undefined overlap. For this reason, it is always necessary to check whether the feature “negative overlap” is specified for seat valves.

14 Vibration and shock resistance

Valves are exposed to vibrations and shocks during their service life. Care must be taken to ensure that these values are not exceeded during storage, transport, assembly, use and maintenance.
Vibration and shock resistance is tested at Festo on the basis of the following standards:

- DIN EN 60068-2-6:2008-10 - Environmental testing - Part 2-6: Tests - Test Fc: Vibration (sinusoidal) (IEC 60068-2-6:2007); German version EN 60068-2-6:2008
- DIN EN 60068-2-27:2010-02 - Environmental testing - Part 2-27: Tests - Test Ea and guidance: Shock (IEC 60068-2-27:2008); German version EN 60068-2-27:2009

14.1 Vibration resistance

The data on vibration resistance are divided into two ranges.
In the low frequency range, the vibration displacement s is constant, so that the acceleration a increases with increasing frequency. In the case of severity level 1, the specifications f=10..58 Hz with a vibration displacement of 3.5 mm are common at Festo.
In the medium frequency range, the acceleration a is constant, so that the vibration displacement s becomes smaller as the frequency increases. For severity level 1, the specifications 58...150 Hz with an acceleration of 20 m/s^2 are common.

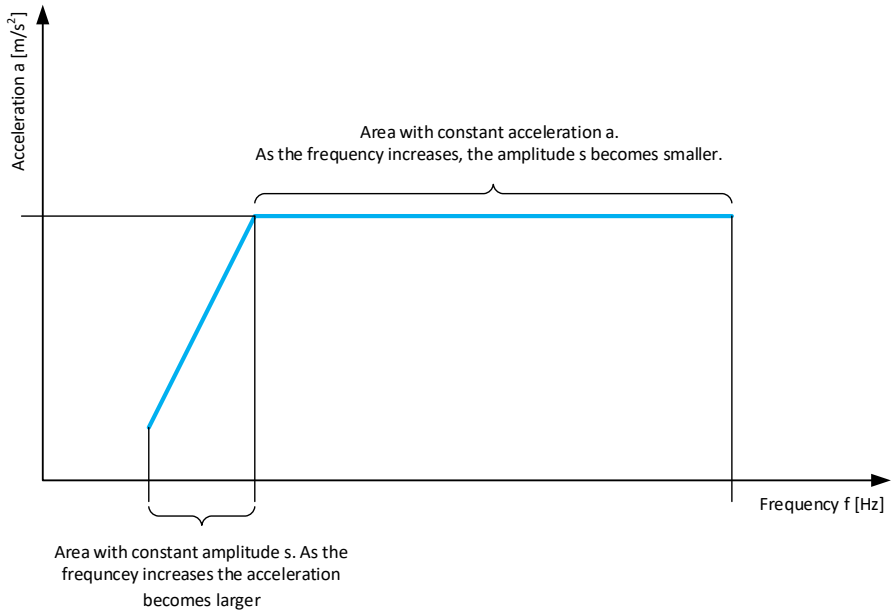


Figure 20 Frequency ranges and acceleration for testing vibration resistance

14.2 Shock resistance

The specifications for shock resistance define a sinusoidal shock with a specific peak acceleration a for a specific shock duration t. The test object is subjected to this shock five times at intervals of 0.5 to 1 second. During the test, a test object is subjected to this shock five times at intervals of 0.5 to 1 s. The test object is then subjected to the shock five times.

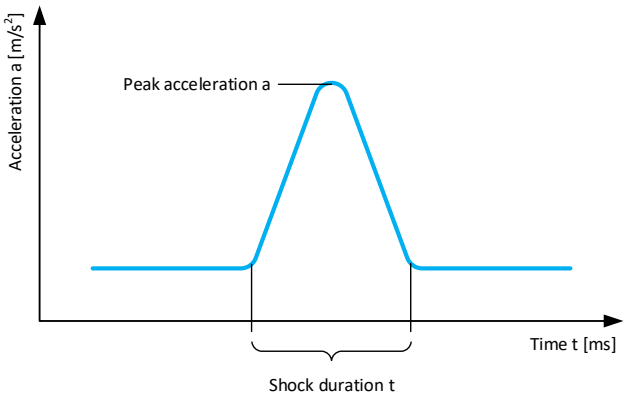


Figure 21 Sinusoidal shocks for testing shock resistance

14.3 Severity levels

At Festo, the following severity levels for vibration and impact resistance are common. These specifications have been verified by tests.

Test	Description	Vibrations			Shocks	
		f [Hz]	s [mm]	a [m/s²]	a [m/s²]	t [ms]
Transport test		2...9 10...150	3.5 -	- 10		
Degree of severity 1	Equipment intended for machines with low vibration level (e.g. in laboratories, freestanding control cabinets)	10...58 58...150	0.15 -	- 20	150	11
Degree of severity 2	Equipment (e.g. valve terminals) intended for direct mounting on machines with a medium vibration level (e.g. automatic assembly machines, handling and conveyor systems)	10...60 60...150	0.35 -	- 50	300	11
Degree of severity 3	Equipment (e.g. sensors and sensor brackets) intended for direct mounting on machines with a high vibration level (e.g. handling systems for presses)	10...61 61...2000	1 -	- 150	100	11

ATTENTION

If the specified vibration and shock resistance for directional control valves is exceeded, failures and damages may occur.

If the characteristic values are exceeded, the spool of the main stage of the valve or the armature in the pilot valve may move. However, damage is also possible, e.g. electrical and electronic components in the valve can become detached and lead to a failure.

15 Test Pulses

15.1 Max. negative test pulse with 1 signal

The safe electronic outputs of safety switching devices use negative test pulses (low test pulses, switch-off test, dark test) to test its switch-off function. These test pulses are also used for short-circuit and cross-circuit detection.

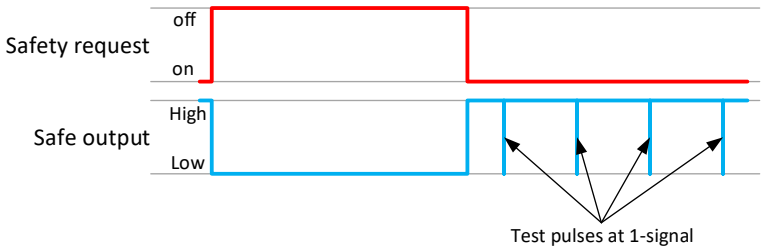


Figure 22 Negative test pulses at 1-signal

Safety switching devices use test pulses when safe outputs are switched on (unless deactivated). The time for the characteristic “max. negative test pulse for 1 signal” specifies for valves how long these test pulses may be without the valve or pilot valve switching.

Example:

Max. negative test pulse with 1 signal	900 µs

If the negative test pulses are longer than 900 µs, the pilot valve or valve may switch.

Attention

If the valve switches during the test pulses, this is to be evaluated as normal switching and the service life of the valve is significantly reduced. The premature failure of the executed safety sub-function is to be expected.

The maximum allowable negative test pulse is specified in the Product Reliability data sheet.

15.2 Max. positive test pulse with 0 signal

The safe electronic outputs of safety switching devices use positive test pulses (high test pulses, light test) to test its switch-on function. These test pulses are also used to detect interruptions, short circuits and cross circuits.

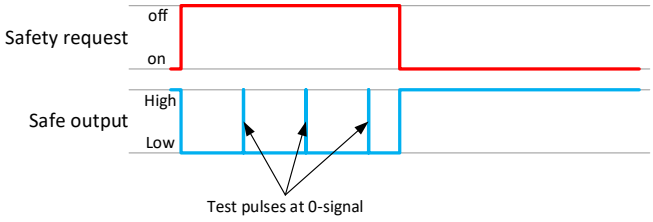


Figure 23 Test pulses at 0-signal

There are some safety switching devices that use test pulses when the safe outputs are switched off (unless disabled). The duration of the test pulses must always be shorter than the time for the characteristic “max. positive test pulse with 0 signal” of the valve in the product reliability data sheet.

Example:

Max. positive test pulse with 0 signal	900 µs

If the positive test pulses are longer than 900 µs, the pilot valve or valve may switch.

Attention

If the valve switches during the test pulses, this is to be evaluated as normal switching and the service life of the valve is significantly reduced. The premature failure of the executed safety sub-function is to be expected.

The maximum allowable positive test pulse is specified in the Product Reliability data sheet.

15.3 Alarm messages from safety PLCs for valve terminals

When valve terminals are used, the short-circuit and cross-circuit detection of the safe output modules of safety PLCs (here using the ET200-SP as an example) can result in various alarm messages.

1. Diagnostic message “Output short-circuited to L+” (fault code 261D)
2. Diagnostic message “Output short-circuited to ground” (fault code 262D)

These alarm messages may mean that operation is not possible.

Note

- The following information is based on the manual for ET 200 SP digital output module F-DQ 4x24VDC/2A PM HF [1].

15.3.1 Error description

A short-circuit (cross-circuit) is detected by the dark test within an indefinable time after a valve terminal is switched on.

In the device manual of the ET 200SP digital output module F-DQ 4x24VDC/2A PM HF, the following information is given for the diagnostic alarms “Output short-circuited with L+/M” (ET-200SP device manual, Table 6-6, page 39)

Table 1 Diagnostic messages ET-200SP

Diagnostic message	Fault code	Meaning	Remedy
Output short-circuited to L+	261_D	Short circuit to L+ can mean: • The output cable is short-circuited to L+. • The capacitive load is too high.	• Correct the process wiring. • Increase the test times (dark, light, switch-on tests).
Output short-circuited to ground	262_D	Short circuit to ground can mean: • The output cable is short-circuited to ground. • The output signal is short-circuited to ground. • There is a short circuit between two output channels. • The capacitive load is too high.	• Correct the process wiring. • Increase the test times (dark, light, switch-on tests).

15.3.2 Explanation

Section of the user manual, “B.1 Connecting capacitive loads”, indicates that loads with capacitances may result in the detection of a short circuit. The reason is that during the parameterized readback time the capacities are not sufficiently discharged.

The capacities included in the valve terminals are EMC measures (electromagnetic compatibility) and must be used on account of the harmonized standards for EMC guideline 2014/30/EU, for which reason they cannot be reduced.

If no valves are activated during the dark test, existing capacitance is not discharged quickly enough. Furthermore, different numbers of valves on the valve terminal can be switched during the dark test. This results in a dynamic load for the fail-safe output which can also affect the dark test.

15.3.3 Solution – Step 1: Increase Readback Time Dark Test

According to the recommendation included in the section entitled “Setting readback time dark test” (page 21), a higher value should be selected for maximum dark test readback time. If an excessively large value is selected, the valves of the connected valve terminal are switched off and on. As a rule, this switching off and on is audible as a “clattering” sound. These switching operations result in wear and must be taken into consideration when calculating the $MTTF_D$ value, resulting in massive restriction of the T_{10D} value and thus the service life of the valves as well.

As a first step towards a possible solution, you should try to increase “dark test readback time”. If maximum readback time for the dark test cannot be increased, the “Output short-circuited to L+” fault may occur sporadically again and again.

If the diagnostic message cannot be eliminated by increasing the “Darkness test readback time”, the wiring must be changed (see Solution - 2nd step) or the modules used must be changed (see Solution - 4th step).

Be sure to observe maximum permissible dark time for the installed valves. This information can be found in the product reliability data sheet for the valves where it’s designated “max. negative test pulse with 1 signal”.

15.3.4 Solution – Step 2: Switch Off of Every Valve Terminal Separately Via a Fail-safe Output

If a diagnostic message occurs directly after activating the fail-safe output, switch-on current may be too high. This might be the case if you switch off several valve terminals at the same time with a single fail-safe output. In this case, you should try to switch off each valve terminal separately via a fail-safe output. This solution may be possible if you can subsequently increase “dark test readback time”. However, we cannot guarantee whether this change is the solution due to the dynamic change in load described above.

Be sure to observe maximum permissible dark time for the installed valves. This information can be found in the product reliability data sheet for the valves where it’s designated “max. negative test pulse with 1 signal”.

15.3.5 Solution – Step 3: Increase Load Current with Resistor

The following procedure is described in appendix “B.1 Connecting capacitive loads”, in the section entitled “Remedy for detection a short circuit”:

1. Determine the load current and capacitance of the load.
2. Locate the operating point in the diagram above (comment: the figure contains characteristic curves for the switching of capacitive loads relative to configured dark and light test times).
3. If the operating point is above the curve, you must increase the load current until the new operating point is below the curve by connecting a resistor in parallel.

This solution may be possible if only individual valves are switched and short connecting cables are used. As a rule, however, it’s not possible to foresee how many valves will be switched on during the dark test. Consequently, this solution is unusable for most applications.

Be sure to observe maximum permissible dark time for the installed valves. This information can be found in the product reliability data sheet for the valves where it’s designated “max. negative test pulse with 1 signal”.

15.3.6 Solution – Step 4: Hardware Change

If you do not succeed in eliminating the diagnostic message with the two previous solution steps, the hardware must be changed. The following options are available to this end:

1. Use of distributed I/O system Siemens ET 200S.
2. Use of fail-safe power module Siemens F-PM-E 24 V DC / 8 A PPM (article no. 6ES7 136-6PA00-0BC0) instead of fail-safe digital output module Siemens F-DQ 4x24 V DC / 2 A PM high feature (article no. 6ES7 136-6DB00-0CA0).
3. **Use of a valve terminal with directly integrated PROFIsafe, i.e. with CPX and PROFIsafe shutoff module CPX-FVDA-P2 (part no. 1971599) from Festo.**

We are only certain that the required short-circuit and cross-circuit detection will function properly in the application when using a valve terminal with PROFIsafe shut-off module CPX-FVDA-P2.

16 Holding current reduction for valves

Many Festo valves have a holding current reduction. This reduction in holding current can lead to a valve no longer being able to be switched off in the case of certain safe outputs.

16.1 Functionality of holding current reduction

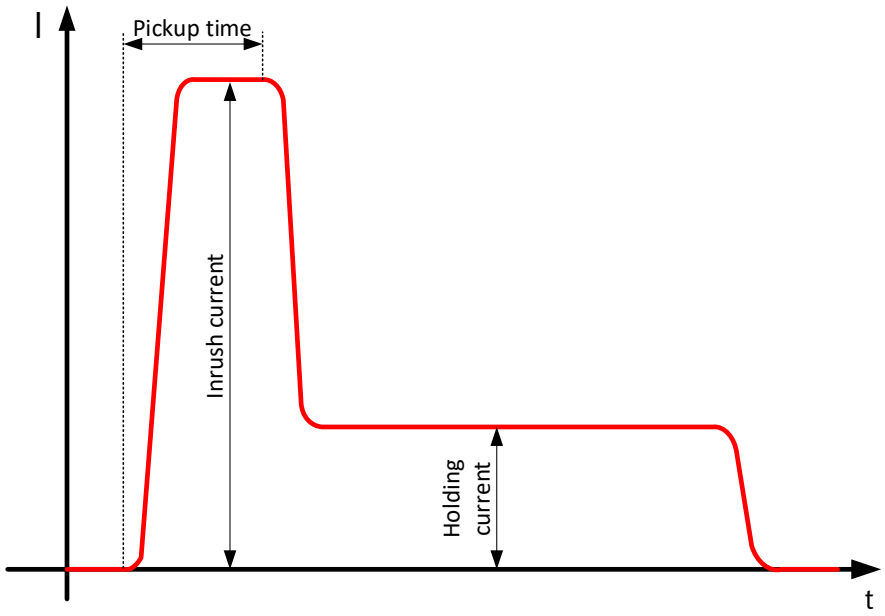


Figure 24 Funktionsweise Haltestromabsenkung

To control a valve solenoid, the coil is first energized with the rated current during holding current reduction. When a sufficiently strong magnetic field has built up in the coil, the plunger is moved from the normal position to the switching position. This movement of the plunger takes place during the attraction time of the valve solenoid.

To hold the plunger in the switching position, not so much energy is required, so that the current through the coil can be lowered to the holding current.

16.2 Behavior with certain safe outputs

There are safe outputs that allow current to flow through the load not only when switched on, but also when switched off. In the off state, a small current (up to 10 mA) is driven through the load at the safe output. This can be used for short circuit, cross circuit and open circuit detection.

The problem with some valves is that the holding current is less than the current that this type of safe output drives through the load. As a result, the valve cannot be turned off.

16.3 Possible solutions

We recommend the use of outputs which do not drive current through the load when switched off. If it is not possible to change the safe output, valves without holding current reduction must be used.

17 Used Literature

17.1 Cited documents from Festo

[1] General operating conditions, edition 2022/11
[2] FN 942012:2018-07 - Functional and Endurance Testing - Valves - Long-Term
[3] CPX Terminal Output Module CPX-FVDA-P2, Description (8022607 EN 1209NH [8022613]

17.2 Standards

[4] DIN ISO 12238:2005-12 – Pneumatic fluid power - Directional control valves - Measurement of shifting time (ISO 12238:2001)
[5] DIN EN ISO 4414:2011-04 – Pneumatic fluid power - General rules and safety requirements for systems and their components (ISO 4414:2010); German version EN ISO 4414:2010
[6] ISO 5598:2020-01 – Fluid power systems and components - Vocabulary
[7] DIN EN ISO 12100:2011-03 – Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010); German version EN ISO 12100:2010
[8] DIN EN ISO 14118:2018-07 – Safety of machinery - Prevention of unexpected start-up (ISO 14118:2017); German version EN ISO 14118:2018
[9] VDMA 24584:2022-06 – Safety functions of regulated and unregulated (fluid) mechanical systems; German Version
[10] DIN EN ISO 13849-1:2016-06 – Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2015); German version EN ISO 13849-1:2015
[11] DIN EN ISO 13849-2:2013-02 – Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2012); German version EN ISO 13849-2:2012
[12] ISO 19973-1:2015-08 - Pneumatic fluid power - Assessment of component reliability by testing - Part 1: General procedures
[13] DIN EN 61508-4:2011-02 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations (IEC 61508-4:2010); German version EN 61508-4:2010
[14] Fachbereich AKTUELL FBHM-022 Manipulation von Schutzeinrichtungen Verhindern, Erschweren, Erkennen, Ausgabe 2021.12, downloaded 13.09.2017 from https://publikationen.dguv.de/regelwerk/publikationen-nach-fachbereich/holz-und-metall/maschinen-robotik-und-fertigungsautomation/4435/fbhm-022-manipulation-von-schutzeinrichtungen-verhindern-erschweren-erkennen
[15] Manual of ET 200SP Digital output module F-DQ 4x24VDC/2A PM HF (6ES7136-6DB00-0CA0), edition 07/2013, A5E03858037-01

17.3 For the legal notice additionally

[16] Machinery Directive: Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
[17] DIN EN 61508:2011-02 - Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508:2010); German version EN 61508:2010
[18] DIN EN 61511:2019-02 - Functional safety - Safety instrumented systems for the process industry sector - (IEC 61511:2016); German version EN 61511:2017
[19] DIN EN IEC 62061:2023-02 - Safety of machinery - Functional safety of safety-related control systems (IEC 62061:2021); German version EN IEC 62061:2021

18 Information about the Document

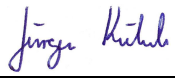
18.1 General Information

Project	100396
	20230322-001
	Circuit – safety subfunctions pneumatic Features of directional control valves

18.2 Revision History

Ver.	Date	Ed.	Chapter	Description of change/impact
1.10	2023-11-17	JKHL	All	Creation of the document

18.3 Approval/Release of the Document

Role	Signature
Release	 Digital signiert von Jürgen Kühnle DN: cn=Jürgen Kühnle gn=Jürgen Kühnle c=DE Germany l=DE Germany o=Festo SE & Co. KG ou=SC-OTP e=juergen.kuehnle@festo.com Grund: Freigabe dieses Dokuments Ort: Esslingen Datum: 2023-11-17 10:17+01:00

18.4 Period of Validity

Document is valid until 2028-11-17 or until one of the documents used or the required relevant base are changed.

Do you have any questions about this Application Note?

You are welcome to send us your questions via the contact form.

Are you looking for Safety Application Notes with solution examples for the most important safety sub-functions in pneumatics?

We regularly expand our collection of documents in the Support Portal.

Do you want to get a general overview of machine and system safety?

We have compiled information on machine and functional safety in our guide.

Download the guide.

Do you need further support?

We also offer services for machine safety

- Risk assessment
- Safety concept
- Circuit design
- Verification / validation

You can request a quotation via the contact form.

Do you need training or further education?

At Festo Didactic you will find training courses on machine safety, functional safety and CE marking.

Request a quote for training or workshop.