Safety Application Note ISO 13849

# CCF Measures

Safety Subfunctions Pneumatics


**Our effort – your advantage**

Our effort for the preparation of these documents

and your saved time 24 h

Free of charge for you.

100399

Title ..........Safety Subfunctions Pneumatics - CCF Measures
Version ..........1.10
Document number .......... 100399
Original ..........German
Author ..........Festo
Date ..........2026-08-17

## Legal Notice

In the following, the "Festo SE & Co. KG" is designated as "Festo".
This document is not binding. This document 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, 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 validation for your specific application and to ensure compliance with all requirements yourself, in particular the Machinery Directive 2006/42/EC (to be applied until 20 Jan. 2027) or the Machinery Regulation (EU) 2023/1230 (to be applied from 20 Jan. 2027). As the user, you are solely responsible for your specific use case and for the proper operation of the products described in this context.
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/EC (to be applied until 20 Jan. 2027) or the Machinery Regulation (EU) 2023/1230 (to be applied from 20 Jan. 2027) 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 recommendations on how measures against Common Cause Failures (CCF) according to ISO 13849-1, Annex F, can be implemented for pneumatics and their electrical actuation.

## 1.2 General notes

- The circuits shown are principle diagrams that, for reasons of clarity and scope, cannot be complete. They are recommendations and do not exclude other possibilities.
- Whether the recommendations contained here are suitable for a specific application must be verified by the user and confirmed in their technical documentation.

## 1.3 Definitions

- Failure due to common cause (Common Cause Failure, CCF)
  A failure that is the result of one or more events that cause simultaneous failures of two or more separate channels in a multi-channel system and lead to a failure of a safety function. [according to IEC 61508-4, 3.6.10]
  **Notes**
    - Failures due to common cause should not be confused with similar-type failures, since similar-type failures can have different causes. [according to ISO 12100, 3.36, note]
- Similar-type failures
  Failures of units that are characterized by the same mode of occurrence. [according to ISO 12100, 3.36]

## 1.4 Notes

- Some measures against common cause failures correspond to certain basic and well-tried safety principles from ISO 13849-2. In these cases, reference is made to those safety principles.

# 2 Common-cause failures

## 2.1 Basics

For safety circuits at or above Category 2, failures due to common cause must always be assessed. This is necessary because certain failure causes can lead to the failure of both channels of a safety circuit and thus disable a safety function. As a result, the required single-fault tolerance is no longer ensured.
The approach chosen by ISO 13849-1 uses the beta-factor (β) model from IEC 61508-6 and has been practically simplified for application in machinery and system engineering. This β-factor model allows an estimate of the proportion of dangerous failures in channels 1 and 2 that result from a given cause and that can also occur in the other channel.

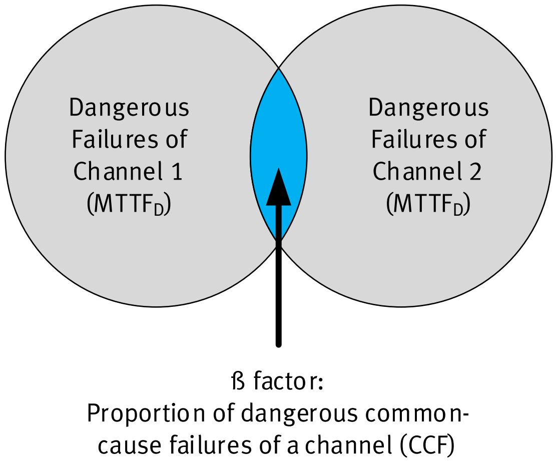



Figure 1 Relationship between channel failures and the β-factor for common-cause failures

Based on this figure, there are three ways to reduce the probability of common-cause failures:

1. Reduce the number of random hardware failures and systematic failures. This decreases the areas of the circles and therefore the size of the overlap.
2. Increase the independence, i.e., separation and diversity, of the channels. This reduces the overlap of the circles while their sizes remain the same.
3. Detect non-simultaneous failures resulting from a common-cause fault while only one channel is affected, i.e., apply diagnostic tests.

To determine the β-factor for a particular safety circuit more precisely, detailed FMEAs for the components and their circuitry in each channel for the intended application are required. This is very time-consuming, so ISO 13849-1 defines a checklist of eight key measures to enable estimation of the β-factor.
ISO 13849-1, Annex F, proposes a qualitative process for assessing the impact of common cause failures (CCF) for each subsystem. It provides measures and their contributions to reducing common-cause failures. The specified measures must be fully implemented to claim the associated score. If implemented only partially, the score is zero.
Recommendations for implementing each measure are given in the following sections.

Table 1 Quantification of measures against CCF (according to ISO 13849-1, Annex F)

| No. | Measures against common cause failures (CCF) | Score |
|---|---|---|
| 1 | Separation / segregation | 15 |
| 2 | Diversity | 20 |
| 3 | Design / application / experience | – |
| | 3.1 protection against over-voltage, over-pressure, over-current, over-temperature | 15 |
| | 3.2 Components used are well-tried | 5 |
| 4 | Assessment / analysis | 5 |
| 5 | Training | 5 |
| 6 | Environmental | – |
| | 6.1 for electrical / electronic systems: prevention of electromagnetic interferences<br>For fluidic systems: prevention of contamination of the fluids | 25 |
| | 6.2 Other influences | 10 |
| | **Total** | |

**Evaluation of the result**

| Total score | Measures to prevent common-cause failures |
|---|---|
| 65 or better | Requirements reached |
| Smaller then 65 | Procedure failed ➔ Selection of additional measures necessary |

# 3 Separation / segregation

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 1 separation / segregation | Physical separation between the signal paths of redundant channels, e.g.:<br>1. Separation of wiring (e.g., multicore cables with appropriate insulation between conductors) ➔ 3.1;<br>2. Separation of piping (e.g., preventing damage to a hydraulic line from excessive pressure released by an adjacent line) ➔ 3.2;<br>3. Detection of shorts and open circuits in cables by dynamic testing ➔ 3.3.1 and 3.3.2;<br>4. Separate shielding of the signal path for each channel ➔ Table 2, row 4;<br>5. … (applies to printed circuit boards)<br>6. … (applies to printed circuit boards) |

The target of these measures is to make a failure of both channels of a safety function due to short circuits and crosstalk unlikely. The basis for implementing the separation/isolation measures is compliance with the installation guidelines of the following standards:

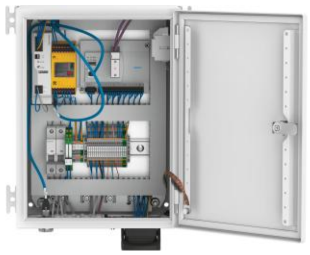
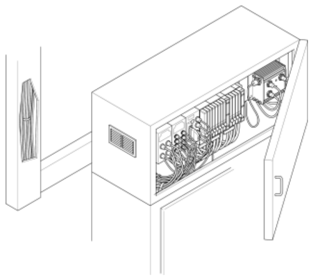
- IEC 60204-1 for the electrical installation of the machine,
- ISO 4414 for pneumatics in a machine.

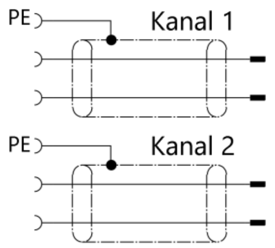
If these installation guidelines have been observed, this measure may already be satisfied. However, it must still be verified and documented separately.

## 3.1 Item 1: Separation of wiring

Wiring separation can be implemented in various ways:

Table 2 Measures for wiring separation

| | | |
|---|---|---|
| 1. |  | The conductors of the redundant channels are routed within an electrical enclosure according to IEC 60204-1, e.g., a control cabinet. Individual wires may then be used for both signals and can run in parallel. However, separate routing of these wires through the cabinet is recommended.<br>If IEC 60204-1 is fully complied with for the cabinet, it may be possible to define a fault exclusion to short and cross circuits within the cabinet. |
| 2. |  | Conductors of the redundant channels are routed fixed in place and protected against external damage. Protection against external damage must be appropriate to the environmental conditions and can be provided by a cable duct or conduit.<br>If IEC 60204-1 is fully complied with for the control cabinet and the electrical installation, it may be possible to define a fault exclusion to short and cross circuits in the installation. |
| 3. |  | The conductors of the redundant channels are routed in separate sheathed cables.<br>A sheathed cable provides individual insulation for each conductor plus a second layer of insulation provided by the outer sheath. |

| | | |
|---|---|---|
| 4. |  | The conductors of the redundant channels are individually protected by an earthed (grounded) shield.<br>If, for example, mechanical damage occurs, any resulting electrical connections are shorted to the shield and protective conductor. |

### 3.2 Item 2: Separation of piping

- Separation of piping or hose runs can be applied in pneumatics, but in most cases it is not relevant.
- If two pneumatic hoses are damaged at the same location, the compressed air will more likely be released to the surroundings, because the flow resistance to the environment is significantly lower. A noteworthy pressure exchange between two pneumatic hoses caused by a damage is considered technically unlikely.

### 3.3 Item 3: Detection of shorts and open circuits in cables by dynamic testing

A dynamic test is a monitored and systematic use of software, with or without operating the hardware, to verify the required behavior and detect faults (according to IEC 61508-4, 3.8.15).
Shorts and crosstalk can be detected by test pulses from safety semiconductor outputs; open circuits are detectable by a complete switching cycle (requesting and acknowledging a safety function or a safety subfunction).
The following diagnostic implementation options are available:

- Diagnosis by test pulses
- Diagnosis by a complete switching cycle of inputs and outputs

#### 3.3.1 Dynamic testing by test pulses

Implementation of dynamic testing to detect shorts and open circuits depends on the technology used.

1. Use of safety semiconductor outputs with short and cross circuit detection
   Safety single- and dual-pole semiconductor outputs typically use test pulses to verify correct output function. These test pulses can also be used to detect short and cross circuits on the connected lines. In principle there are two possibilities:
   - Safety single-pole semiconductor outputs with switching of 24 VDC
     Safety semiconductor outputs that switch only the 24 VDC supply typically use test pulses that can be used for short- and crosstalk detection.
     Additional measures may be required to detect shorts to 0 VDC. As a rule, based on IEC 60204-1, exclusions for shorts and crosstalk inside the control cabinet and for wiring outside the cabinet are assessed.

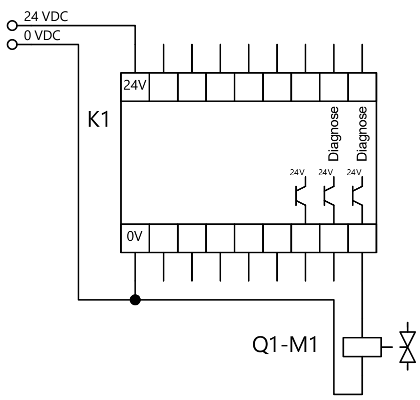
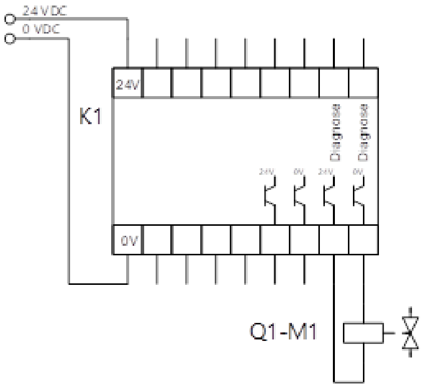



Figure 2 Safe single-pole semiconductor output

○ Safety 2-pole semiconductor outputs with switching of 24 VDC and 0 VDC




Safety semiconductor outputs that switch both 24 VDC and 0 VDC usually use test pulses that can be used for short- and crosstalk detection.
Shorts and crosstalk in the wiring are detected and the safety switching device typically disables all outputs.

Figure 3 Safe 2-pole semiconductor output

It is common to use both negative and positive test pulses.

- Negative test pulses
  Safety semiconductor outputs use negative test pulses (low test pulse, off-test, dark test) to check the output's ability to switch off. These test pulses also serve to detect shorts and crosstalk.

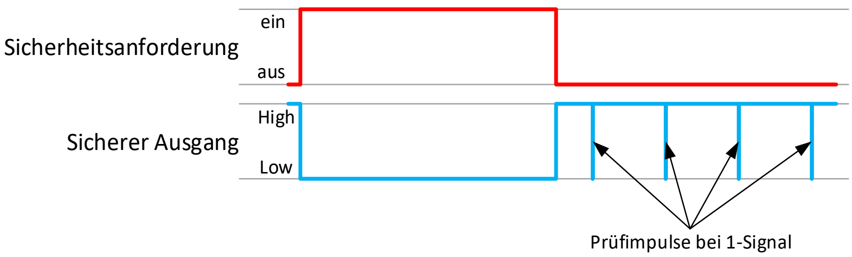



Figure 4 Test pulses at 1 signal

The duration of the test pulses must always be shorter than the time specified by the characteristic "max. negative test pulse at 1 signal" for the valve in the product reliability datasheet.

- Positive test pulses
  Positive test pulses (high test pulse, on-test, light test) are used by safety switching devices to check the output's ability to switch on. These test pulses also serve to detect shorts and crosstalk.

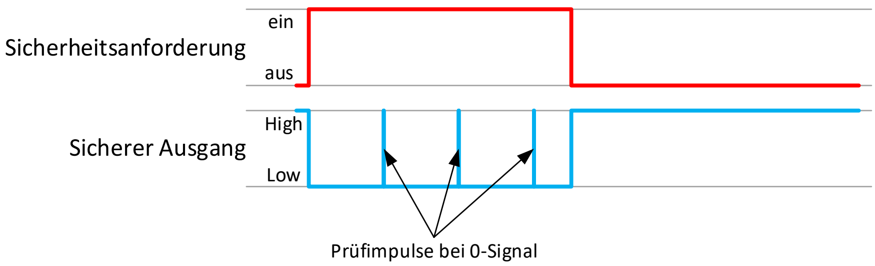



Figure 5 Test pulses at 0 signal

The duration of the test pulses must always be shorter than the time specified by the characteristic "max. positive test pulse at 0 signal" for the valve in the product reliability datasheet.

**Important notes on test pulses**

- Test pulses shall not cause any valve or pilot valve to operate; see also document ➚ 100396 Notes on characteristics of directional valves, section “15 Test pulses”.
- Valve manifolds typically include reverse-polarity protection diodes and EMC filters. These can filter out the test pulses, so short- and crosstalk detection in the manifold is not guaranteed. Detection of shorts and crosstalk is usually performed via diagnostic measures of the pneumatic circuit or, if present and enabled, via integrated diagnostics of the valve manifold.
- Some valve manifolds can detect shorts and crosstalk within the manifold using the test pulses from the safety outputs. This information, if applicable, is provided in the “F-SY Machine Safety – Declaration” certificate; see the valve manifold’s online page under Certificates.

### 3.3.2 Dynamic test by a valve switching cycle

**Important note**

- If open circuits and shorts are to be detected by a valve switching cycle, a complete switching operation of the valve or a full movement of the pneumatic drive is required. This must not create any hazard.

If test pulses cannot be used (e.g., with fast-acting valves), or are not available (e.g., with electromechanical switching contacts of the safety switching device), a full switching cycle (energizing and de-energizing each valve solenoid) can also detect open circuits, short and cross circuits in the electrical lines. The prerequisite is that the pneumatic circuit includes a suitable diagnostic measure capable of detecting every intended and unintended switching of the valve. Possible diagnostic measures for valves are described in Application Note ➚ 100396 Notes on characteristics of directional valves, section “5 Diagnostic measures”.

## 4 Diversity

The following recommendations are included in ISO 13849-1, Annex F:

| | |
|---|---|
| 2 Diversity | Considerations for diversity include, for example:<br>1. Different technologies/designs or physical principles are used, e.g.:<br>o the first channel is electronic or programmable electronic and the second channel is electromechanical, hard-wired;<br>o different initiation of the safety function for each channel (e.g., position, pressure, temperature);<br>o valves in the first channel with rubber seals and valves in the second channel with metal seals;<br>o two position switches are used to detect the opening of a movable guard (safety door): the first is actuated when the guard is opened and uses a normally closed contact with direct opening action in accordance with IEC 60947-5-1:2020 Annex K; the second is actuated when the guard is closed and uses a normally open contact.<br>2. Sensor elements use different measurement principles (e.g., digital and analog) or physical principles (e.g., distance, pressure or temperature).<br>3. Different components, e.g., from different manufacturers (no relabeling).<br>4. Different loading conditions, e.g., the first contact/valve switches without load, the second contact/valve switches under load. |

The standard mixes different solution approaches for inputs, logic and outputs. Here, diversity requirements for inputs and outputs are listed separately.

1. Diversity for sensors (inputs)
   Electronic – electromechanical pressure switches
   One channel is implemented with an electronic (programmable) pressure sensor and the other channel with an electromechanical pressure switch.


Pressure sensor SDE5-D10-C-Q4E-P-M8 (542889)

Pressure switch PEV-1/4-B (10773)

Pressure sensor SDE5-D10-C-Q4E-P-M8 (542889) Pressure switch PEV-1/4-B (10773)

For electronic sensors, diversity of the embedded software used must also be assessed. The embedded software is not accessible to the user, so the requirements of ISO 13849-1, 7.3.1 cannot be fulfilled. Therefore, the alternative procedure for inaccessible embedded software must be used (see also section → 12.2.1). This means:

- For a subsystem with Category 2, the PL is limited to PL c.
- For a subsystem with Category 3, the PL is limited to PL d.
- Both channels must use different technologies or physical principles from each other.
- The manufacturer confirms for two different electronic sensors that their embedded software is diverse (no shared subprograms are used).

For the following electronic sensors the embedded software is diverse. This is confirmed in the FAQ document FAQ-200138 (available on request).


SPAU-P10R-W-G18FD-L-PNLK-PNVBA-M8U (8001231)

SPBA-P2R-G18-2P-M12-0,25X (8000210)

2. Diversity for valves (outputs)
   Diversity of valves can be implemented by different measures:
   - First channel uses a spool valve, second channel uses a seated valve.
   - First channel uses a valve on a valve manifold, second channel uses a valve in the maintenance unit.
   - First channel is a working valve with frequent actuation, second channel is a switching valve for operating pressure that is actuated infrequently.

   **Notes**

   - For valves, diversity-based redundancy (different valve types) is often not used; typically identical valves are used for redundancy. Reasons include:
     - Categories 3 and 4 already provide high fault tolerance through two-channel architecture and strong fault detection via diagnostics.
     - ISO 13849-1 requires measures against CCF but does not mandate diversity. Other measures – such as physical separation, different power supplies and organizational measures – can also be acceptable.
   - The decision to use diversity depends on the risk assessment, the required PL and technical feasibility. In many cases, diversity is not economically or technically sensible, especially where other CCF measures are sufficiently effective.

# 5 Protection against overvoltage, overpressure, overcurrent, overtemperature, etc.

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 3.1 Protection from or control of, for example, overvoltage, overpressure, overcurrent, overtemperature | Protection from or control of, for example, overvoltage, overpressure, overcurrent, overtemperature, etc.<br>1. The inputs and outputs of the SRP/CS and the logic power supply are protected against potential overvoltages and/or overcurrents (see also IEC 60204-1);<br>NOTE Parts of the SRP/CS are able to withstand potential overvoltage and/or overcurrent levels, or they are protected against them. The possible maximum overvoltage level of a SMPS (switch-mode power supply) depends on the standard applied (for example, the maximum voltage limit under a fault condition).<br>It is important to consider the possible maximum overvoltage level according to the standard applied to the SMPS as well as other operating conditions (for example, overvoltage category, operating temperature).<br>2. The measure against overpressure can be a single-channel system if the primary pressure in the fault case can never rise above the operating pressure multiplied by 1.5. ISO 4414 defines a requirement for protection against unintended pressure (for example, a pressure relief valve). |

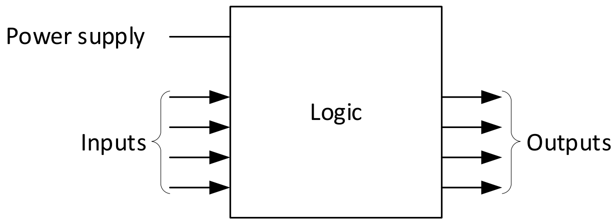



Figure 6 Overvoltage/overcurrent protection required for power supply, inputs, and outputs

## 5.1 Protection against transient overvoltage

Item 1 refers to the standard IEC 60204-1. Section 7.9 of IEC 60204-1 describes protection against transient overvoltage.
For protection against transient overvoltages caused by lightning or switching operations, the use of SPDs and various standards is referenced. The Application Note ➚ 100565 Electromagnetic Immunity (EMI) for safety-related circuitry according to ISO 13849, section “3.1 Overvoltage protection” describes which surge protective devices (SPDs) should be used and where.

## 5.2 Protection against continuous overvoltage

In addition, protection against continuously applied overvoltage is required. This can be achieved by using a PELV power supply. For this PELV power supply, information must be available on the maximum possible output voltage in a fault condition, e.g., 30 VDC for a 24 VDC nominal voltage.
Protection for voltages of 230 VAC or 400 VAC is usually provided by a main switch with overvoltage release.

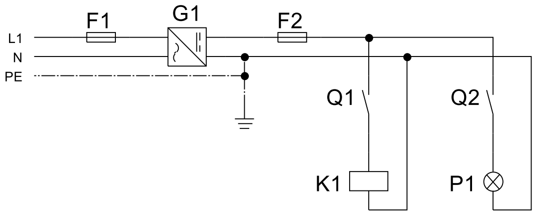
**Notes**

- A PELV power supply can also be suitable for transient overvoltage protection if it is designed for overvoltage category II.

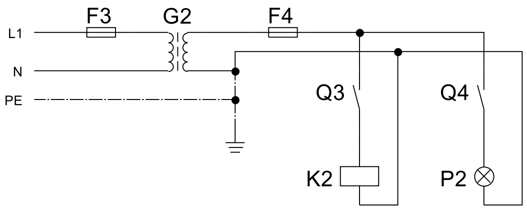
## 5.3 Overcurrent protection — logic power supply

Overcurrent protection for the logic power supply is described in the safety principle “Protection of the control circuit.” (Application Note ➚ 100619) Depending on the power supply used, appropriate fuses should be used in the primary and secondary circuits:

With PELV power supply




With control transformer




With SELV power supply

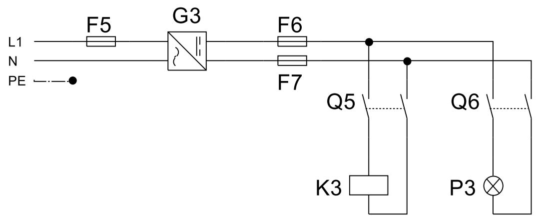



Figure 7 Protection of logic by fuses

## 5.4 Protection against transient overvoltage at inputs and outputs

- For inputs, transient overvoltage are normally not expected because no inductances are switched. If transient overvoltage are present, the EMC-compliant installation should generally be improved; see Application Note 100565.
- For outputs that switch valve coils, transient overvoltage occurs. Application Note ➚ 100568 provides a detailed description of the required measures.

## 5.5 Overcurrent protection inputs

For the logical states of controller inputs, IEC 61131-2 specifies the minimum and maximum permissible voltages and currents. Short circuits to 24 VDC or 0 VDC must therefore not cause damage to the input. Safety switching devices typically have two monitored outputs that supply test pulses to safety command devices, e.g., safety door switches, emergency stop, or to other sensors, e.g., limit switches, pressure switches. These outputs provide the test pulses for short-circuit and cross-circuit detection and are short-circuit tolerant, i.e., at least a current limitation is present.

**Notes**

- Line length must be considered because voltage drop along the line can cause a connected sensor or electronic device to receive insufficient voltage for proper operation.

## 5.6 Overcurrent protection outputs

For the logical states of controller outputs, IEC 61131-2 also specifies the minimum and maximum permissible voltages and currents. Outputs can be short-circuit tolerant, but this must be stated in the output documentation. Otherwise, overcurrent protection must be provided. The following safety principles can be applied:

- Safety principle “Protection of the control circuit” (see section 5.3, ➚ Application Note 100619).

### 5.7 Overpressure

The measures to be provided against overpressure are described in Application Note ➚ 100512 Service Units. The sections to be taken into account at a minimum are:

- Pressure relief valve F1
- 4.4 Pressure regulator K1
- 4.6 Pressure switch B1 (together with on/off valve Q1)

# 6 Use of well-tried components

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 3.2 Use of well-tried components | **F.3.3 Design / application / experience**<br>...<br>Only well-tried components are used. See ISO 13849-1, 6.1.11 and ISO 13849-2. |

To satisfy this CCF measure, use components that demonstrably have high reliability and are suitable for safety-related applications. Consider the following points:

1. Well-tried technology
    - Components must be classified by the manufacturer as “well-tried components according to ISO 13849-1.”
    - Components should have a proven track record in comparable applications over a long period.
    - Do not use new components without sufficient field data.
2. Documented reliability
    - Manufacturer data for $B_{10}$ or MTTF values.
    - Evidence from field data or safety assessments.
3. Standards compliance
    - Components should be tested to the relevant standards.
    - Safety functions must meet the requirements of ISO 13849-1.
4. Environmental conditions
    - The intended use must conform to the conditions specified by the component manufacturer (temperature, EMC, humidity, vibration, shock).
    - The technical specifications prescribed by the manufacturer must always be observed; otherwise, the component will lose its classification as “well-tried” in accordance with ISO 13849-1.
5. Supplier assessment
    - The manufacturer must demonstrate quality control.
    - Long-term availability and support are important.
6. Documentation
    - List of used well-tried components.
    - References to previous applications or manufacturer approvals.
    - Test reports or certificates archived.

Well-tried components generally reduce the occurrence of faults, as well as the risk of simultaneous failures due to common causes. . The reasons include:

- Their weak points are known and can be addressed in the design,
- Under defined conditions well-tried components operate reliably,
- They are less susceptible to unknown failure mechanisms.

## 7 Assessment / analysis

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 4 Assessment / analysis | **F.3.4 Assessment / analysis**<br>For each part of the SRP/CS a failure-effects analysis or an FTA has been performed to identify possible causes of CCF, and the results were taken into account to avoid CCFs in the design. |

### 7.1 Objective of the measures

An analysis must be performed for every part of the safety circuit to identify possible causes of failures due to common cause (CCF). The analysis results must be evaluated and measures derived that sufficiently reduce the effects of these failures.

### 7.2 Required methods

Two standards are commonly used for performing these analyses and assessments:

- IEC 60812 — Analysis techniques for system dependability — Procedure for failure mode and effects analysis (FMEA)
  FMEA examines how individual component failures affect the overall system.
- IEC 61025 — Fault tree analysis (FTA)
  FTA is a top-down analysis intended to identify causes of critical failures.

### 7.3 Procedure

The following procedure has proven effective for the analysis:

1. Capture system structure
    - Create an architecture overview and safety-related block diagrams of the safety circuit.
    - Identify all interfaces, e.g., inputs and outputs.
    - Identify common resources, e.g., power supply, software modules.
2. Perform the analysis
    - FMEA: Document possible failure modes, causes and effects for each component. ISO 13849-2 contains failure lists for components.
    - FTA: Define critical events, e.g., loss of the safety function, as the top event and derive causes.
3. Assess CCF risks

   Examine analysis results for common causes, e.g.:

    - Same environmental influences such as temperature, EMI, humidity
    - Common power supply
    - Identical software or firmware
    - Human errors, e.g., repeated assembly mistakes
4. Derive measures

   From the assessment of the CCF risks, derive and implement measures that sufficiently reduce the effects. Examples include:

    - Physical separation of channels
    - Different technologies or manufacturers
    - Separate power supplies
    - Software diversity or independent development
5. Documentation

   Archive the produced documents for traceability. These should include:

    - Analysis reports (FMEA and FTA)

- Evidence that analysis and assessment results were incorporated into the design, e.g., design changes, additional protective measures

## 8 Training

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 5 Training | Designers have been trained (with documentation, e.g., training certificate) to understand the causes and effects of failures due to common cause. |

Measure F.3.5 “Training” in ISO 13849-1 requires that designers and developers be trained to understand the causes and effects of common cause failures (CCF). The standard does not prescribe a detailed training agenda, but the requirements and practical guidance suggest typical contents:

**Training agenda: “CCF avoidance according to ISO 13849-1”**
**Target audience:** designers, developers
**Objective:** Understand causes and effects of common cause failures (CCF) and apply the normative measures.

- **Module 1: Introduction to functional safety**
  - Overview of EN ISO 13849-1 and -2
  - Relation to the Machinery Regulation and risk assessment
  - Performance Level (PL), $MTTF_D$, DC, CCF — terms and meanings
- **Module 2: Common Cause Failures (CCF)**
  - Definition and typical causes
  - Practical examples
  - Effects on redundant systems and PL calculations
- **Module 3: Normative requirements and measures**
  - ISO 13849-1 Annex F: measures F.3.1 to F.3.7
  - Focus on F.3.5 Training
  - Other measures: physical separation, diversity, differing technologies
- **Module 4: Practical implementation**
  - Assessing CCF in SISTEMA
  - Documentation and evidence
  - Examples of correct and incorrect implementations
- **Module 5: Workshop & discussion**
  - Group exercise: analysis of an example project
  - Identification of CCF risks and countermeasures
  - Questions & answers

# 9 Environment for electrical / electronic systems

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 6.1 Preventing electromagnetic disturbances | For electrical/electronic systems, contamination and electromagnetic disturbances shall be prevented to protect against CCFs in accordance with the applicable standards (e.g., IEC 61326-3-1, IEC 61000-6-7:2014, IEC 61000-1-2:2016, IEC 61800-5-2).<br>NOTE 1 These EMI standards typically include more stringent requirements compared with the requirements used for standard components (e.g., PLCs for general-purpose applications). See IEC 61800-3 for further information. (according to ISO 13849-1, F.3.6.1)<br>...<br>For combined fluid and electrical systems both aspects should be considered. (according to ISO 13849-1, F.3.6.1) |

Electromagnetic disturbances can quickly cause faults in both channels of a safety circuit. Therefore, EMC standards for safety components and safety circuits impose higher requirements than for purely functional components and circuits. These elevated requirements make it difficult for many users to find a suitable interpretation of the requirements. ISO 13849-1:2023 includes a dedicated Annex L on electromagnetic immunity (EMI) that outlines the different options. The following application notes explain the basics and give recommendations on how failures caused by electromagnetic disturbances can be sufficiently reduced:

- Electromagnetic Immunity (EMI) for safety-related Circuits according to ISO 13849 Application Note ➚ 100565.
- Electromagnetic Immunity (EMI) - Interpretation of ISO 13849-1, Annex L, Application Note ➚ 100513.

## 10 Environment for fluid systems

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 6.1 Preventing ... contamination of the fluid | ...<br>For fluid systems, filtration of the pressure medium, prevention of ingress of contamination, and draining of compressed air shall be carried out in accordance with the component manufacturer's requirements for fluid cleanliness (see ISO 8573-1 for guidance).<br>For combined fluid and electrical systems both aspects should be considered. (after ISO 13849-1, F.3.6.1) |

For pneumatic systems, compressed air should be adequately filtered. A description of the required measures is given in Application Note ➚ 100512 Service Units.

Note the requirement "prevention of ingress of contamination." This requires measures during different life phases of a machine:

- Manufacture
    - The assembly area should be kept free of dust and particles that could enter openings of pneumatic components or the system.
    - Pneumatic components should be removed from the manufacturer's original packaging only shortly before assembly.
    - Openings of the pneumatic system should be closed with blind plugs or closed silencers.
- Storage and transport
    - If there are open, unsealed openings of the pneumatic system, these should be closed with blind plugs or closed silencers. If this is not possible, the machine or machine part should be wrapped dust-tight, e.g., stretch film or welded foil.
- Operation
    - For pneumatic systems note that exhaust openings can draw air from the surroundings into the pneumatic system, e.g., when a pneumatic drive is moved manually. Therefore, all exhaust openings should be fitted with a silencer or a filter element.
    - Silencers should exhaust into an area where dust, dirt and other particles cannot accumulate.
- - Maintenance
    - If a pneumatic system is opened for maintenance, first clean the machine or machine part so that no dirt can enter.
    - The assembly area should be kept free of dust and particles that could enter openings of pneumatic components or the system.
    - Pneumatic components should be removed from the manufacturer's original packaging only shortly before assembly.
    - Openings of the pneumatic system should be closed with blind plugs or closed silencers.
- - Dismantling
    - Before dismantling a machine, e.g., for transport, the machine should first be cleaned so that no dirt can enter.
    - Openings of the pneumatic system should be closed with blind plugs or closed silencers.

## 11 Environment — other influences

The following recommendations are contained in ISO 13849-1, Annex F:

| | |
|---|---|
| 6.2 Other influences | The safety circuit shall be immune to all relevant environmental influences such as temperature, shock, mechanical stress, vibration, and humidity as specified in the applicable standards, e.g., the IEC 60068 series, which take the stricter requirements for safety-related applications into account. (according to ISO 13849-1, F.3.6.2) |

This CCF measure aims to identify and assess all other environmental influences that could cause failure of both channels of a safety circuit.
It is explicitly stated that the safety circuit must withstand more stringent requirements than the machine's functional circuit. This can be achieved either by appropriate selection of components or by system-level measures.
The external influences listed include:

- Temperature
- Shock
- Mechanical stress
- Vibration
- Humidity

For each of these external influences, perform the following steps:

1. Determine the possible value ranges of the external influence at the location of each safety-circuit component, e.g., possible temperature range in the control cabinet: 15…40°C.
   The IEC 60068 series can be used here to define possible value ranges for external influences.
2. Specify which additional operating conditions the safety-circuit components should meet, e.g., component operating range 5…50°C.
3. Select components accordingly or verify that already selected components meet these requirements. If these requirements are not met, select other measures so that the safety-circuit components have higher resistance to these external influences, e.g., use forced cooling in the control cabinet.
4. Verify that these ratings are maintained during operation. If necessary, testing according to the IEC 60068 series can be performed.

**Notes**

- It shall be considered that the list of external influences may need to be extended for specific applications.
- For specific applications, this CCF measure can be implemented using the well-tried safety principle "reduced range of environmental parameters."

## 12 Additional measures against common-cause failures

Additional measures against common-cause failures may be required. One reason is that the systematic capabilities of a subsystem limit the possible risk reduction.

### 12.1 Systematic capabilities

Systematic capabilities refer to the ability of a safety-related system or subsystem to avoid or control systematic faults. These faults do not occur randomly but result from failures in the development process, for example:

- Failures in the specification, e.g., insufficient resolution of light curtains or sensors,
- Design failures, e.g., inadequate diagnostic measures,
- Software failures, e.g., use of embedded software not developed according to functional safety practices,
- Failures in change management, e.g., inadequate control during updates.

Therefore, for safety circuits, measures to prevent systematic faults are always required as part of implementing protections against common-cause failures:

- Structured development process, e.g., according to a V-model,
- Documentation and traceability,
- Verification and validation,
- Independence of testing/inspection activities,
- Qualified tools and methods, e.g., static code analysis, FMEA.

These measures are the commonly used organizational measures that form the basic preconditions for any development of safety-related systems.

### 12.2 Limitations due to limited systematic capabilities

Standards provide various statements about limitations resulting from limited systematic capabilities. These include:

- ISO 13849-1, section “7.3.2 Alternative procedures for non-accessible embedded software”

#### 12.2.1 Non-accessible embedded software (firmware)

When standard components with integrated embedded software (firmware) are used, that software may not have been developed according to a functional safety standard and therefore does not meet the systematic capability requirements for use in safety circuits. The standard permits the use of standard components with integrated embedded software (firmware) subject to the following limitations regarding category and Performance Level (ISO 13849-1, 7.3.2):

- Without further measures, a subsystem with category B, 2, or 3 that contains a standard component with integrated embedded software in one of the channels is limited to PL a or PL b.
- If diversity requirements are met by using different technologies/designs or physical principles, a safety circuit with category 2 is limited to PL c and a category 3 to PL d. This can be implemented, for example, with one channel using a pressure sensor with embedded software and the other channel using an electromechanical pressure switch without software.

## 12.3 Further information on implementing diversity

Standards also provide guidance for implementing diversity as a measure against common cause failures.

- ISO 14119 – Interlocking devices associated with guards that separate hazardous areas

### 12.3.1 Interlocking devices

ISO 14119 gives several examples of how diversity can be implemented for position switches.

- Combining a position switch with direct mechanical actuation and forced opening with a position switch with indirect mechanical actuation prevents common-cause failures (according to ISO 14119, 6.4), and diversity may be claimed for that subsystem (according to ISO 14119, 9.2.3, last paragraph).
- Monitoring a protective door with a mechanically actuated valve and with a position switch that interrupts the actuation of a second valve: by using different technologies (diversity of energy sources), a dangerous simultaneous failure of both channels is technically unlikely (according to ISO 14119, 9.2.4).

# 13 Used Literature

## 13.1 Cited Documents from Festo


[1] 100396 Notes on features of directional control valves
[2] 100512 Service Units
[3] 100513 Electromagnetic Interferences (EMI) – Interpretation ISO 13849-1, Annex L
[4] 100565 Electromagnetic Interferences (EMI) for safety-related circuits according to ISO 13849
[5] 100568 Transient Suppression
[6] 100619 Protection of the Control Circuit
[7] FAQ-200138 Diverse Software in Pressure Sensors


## 13.2 Standards


[8] 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
[9] ISO 5598:2020-01 – Fluid power systems and components - Vocabulary
[10] 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
[11] DIN EN ISO 13849-1:2023-12 – Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2023); German version EN ISO 13849-1:2023
[12] 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
[13] DIN EN ISO 14119: 2025-09 - Safety of machinery - Interlocking devices associated with guards - Principles for design and selection (ISO 14119:2024); German version EN ISO 14119:2025
[14] ISO 19973-1:2015-08 - Pneumatic fluid power - Assessment of component reliability by testing - Part 1: General procedures
[15] VDMA 24584:2022-06 – Safety functions of regulated and unregulated (fluid) mechanical systems; German Version
[16] DIN EN 60068-1:2015-09 - Environmental testing - Part 1: General and guidance (IEC 60068-1:2013); German version EN 60068-1:2014
[17] DIN EN 60204-1:2026-06 - Safety of machinery - Electrical equipment of machines - Part 1: General requirements (IEC 60204-1:2016, modified + AMD1:2021); German version EN 60204-1:2018 + A1:2025
[18] DIN EN 60721-1:1997-02 - Classification of environmental conditions - Part 1: Environmental parameters and their severities (IEC 60721-1:1990 + A1:1992 + A2:1995); German version EN 60721-1:1995 + A2:1995
[19] DIN EN 60812:2006-11 - Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (IEC 60812:2006); German version EN 60812:2006
[20] DIN EN 60947-5-1:2018-03 - Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices (IEC 60947-5-1:2016 + COR1:2016); German version EN 60947-5-1:2017
[21] DIN EN 61025:2007-08 - Fault tree analysis (FTA) (IEC 61025:2006); German version EN 61025:2007
[22] DIN EN 61131-2:2008-04 - Programmable controllers - Part 2: Equipment requirements and tests (IEC 61131-2:2007); German version EN 61131-2:2007
[23] DIN EN 61508:2011-02 - Functional safety of electrical/electronic/programmable electronic safety-related systems (IEC 61508:2010); German version EN 61508:2010
[24] 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
[25] DIN EN 61508-6:2011-02 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6:2010); German version EN 61508-6:2010
[26] DIN EN 61511-1:2019-02 - Functional safety - Safety instrumented systems for the process industry sector - (IEC 61511:2016); German version EN 61511-1:2017
[27] 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

### 13.3 Legal Regulations

[28] 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)

[29] Machinery Regulation: Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC

# 14 Information about the Document

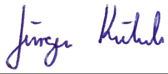
## 14.1 General Information

| **Document Number** | **100399** | |
|---|---|---|
| Title | CCF Measures – Safety Subfunctions Pneumatics | |

## 14.2 Revision History

| Ver. | Date | Ed. | Chapter | Description of Change/Impact |
|---|---|---|---|---|
| 1.10 | 2026-08-17 | JKHL | All | Creation of document |

## 14.3 Approval/Release of the Document

| Role | Signature |
|---|---|
| **Release** |  Digital signiert von Jürgen Kühnle<br>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<br>Grund: Freigabe dieses Dokuments<br>Ort: Esslingen<br>Datum: 2026-08-17 07:07+02:00 |

## 14.4 Period of Validity

Document is valid until 2031-08-11 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.