developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL2
ISO 13849
PLd

Ⓔx II 3G Ex ec IIC T4 Gc
Ⓔx II 3D Ex tc IIIB T125°C Dc

RoHS II COMPLIANT


# Safety manual

## DE90

Differential pressure transmitter

09015230 • SHB_EN_DE90 • Rev. ST4-B • 06/20

# Masthead

**Manufacturer:**

**FISCHER Mess- und Regeltechnik GmbH**

Bielefelderstr. 37a
D-32107 Bad Salzuflen

Telephone: +49 5222 974 0
Telefax: +49 5222 7170

eMail: info@fischermesstechnik.de
web: www.fischermesstechnik.de

**Technical editorial team:**

Documentation representative: T. Malischewski
Technical editor: R. Kleemann



## Version history

| | |
|---|---|
| Rev. ST4-A 03/20 | Version 1 (first edition) |
| Rev. ST4-B 06/20 | Version 2 (Change cover picture, DIN EN IEC 60079-7) |

# Table of contents

# 1 Scope and standards

**WARNING! This Safety Manual should only be used in conjunction with the operating instructions of the respective unit. Pay attention to the safety instructions in the operating instructions.**

This documentation contains information and safety instructions required for the use of the differential pressure transmitter DE90 in safety-related systems.

It is designed for persons that mount, configure and commission the device, and also for project developers and operators.

This safety manual applies for all models of the differential pressure transmitter DE90 of the series PRO-LINE® with the following restrictions.

- Firmware from version 1.12.
- Models with a Modbus interface are not allowed.
- Both channels may not be used for the same safety function.
- The safety coefficients were determined based on FMEAs. These apply under the condition that the output signals are monitored and analysed by a downstream control system.

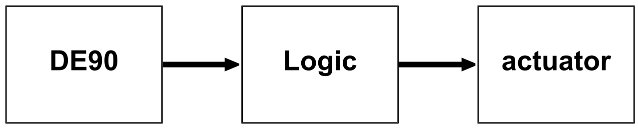



*Fig. 1:* Processing chain

The following norms are referenced for the calculations.

| | |
|---|---|
| Functional security | **IEC 61508: 2010**<br>Functional safety of safety-related electrical/ electronic/programmable electronic systems |
| Safety of Machinery | **EN ISO 13849-1:2015**<br>Safety of machinery - Safety-related parts of control systems - Part 1: General design principles |
| Part failure rate | **SN 29500: 2010**<br>Failure rates (Siemens) |

# 2 Description of the Device and Field of Application

## 2.1 Safety function

The differential pressure transmitter transfers the input signal (pressure) into a standardised analogue output signal. Also, it can be used to monitor the limit value (overstepping or undercutting) using the switch outputs.

### 2.1.1 Parameterization

**Analogue outputs**

Depending on the version, the device has one or two analog outputs. Devices without analog output do not need to be parameterized. The outputs can be designed as current or voltage outputs. Both outputs must be parameterized as follows:

| Analog output 1 | Parameter | Value |
|---|---|---|
| | An.output 1 assignmt | channel 1 |
| | Limit C1 | Off |

| Analog output 2 | Parameter | Value |
|---|---|---|
| | An.output 1 assignmt | channel 2 |
| | Limit C2 | Off |

| Signal limits (Channel, Channel 2) | Parameter | Value |
|---|---|---|
| Current output | Limit I min. | 0 mA |
| | Limit I max. | 21.5 mA |
| | I error signal | 0 mA or 21.5 mA |
| Voltage output | Limit U min. | 0 V |
| | Limit U max. | 10.5 V |
| | U error signal | 0 V or 10.5 V |

**Switching outputs**

The device has two or four switching outputs depending on the version. Two switching outputs each must be connected in inverting fashion. Both switching outputs switch at the same limit value (SP1=SP2) or (SP3=SP4) and must be parameterised as follows.

| Switching output 1 | Value | Switching output 2 | Value |
|---|---|---|---|
| SP1 Assignment | channel 1 | SP2 assignment | channel 1 |
| SP1 on | $P_{SP}$ | SP2 on | $P_{SP}$ |
| SP1 off | $P_{SP}$ | SP2 off | $P_{SP}$ |
| SP1 delay on | 0 s | SP2 delay on | 0 s |
| SP1 delay off | 0 s | SP2 delay off | 0 s |
| SP1 Function | Normally open | SP2 function | Normally closed |

| Switching output 3 | Value | Switching output 4 | Value |
|---|---|---|---|
| SP3 assignment | channel 2 | SP4 assignment | channel 2 |
| SP3 on | $P_{SP}$ | SP4 on | $P_{SP}$ |
| SP3 off | $P_{SP}$ | SP4 off | $P_{SP}$ |
| SP3 delay on | 0 s | SP4 delay on | 0 s |
| SP3 delay off | 0 s | SP4 delay off | 0 s |
| SP3 function | normally open | SP4 function | normally close |

$P_{SP}$: Programmed switching point (pressure value)

### 2.1.2 Model with current output

The following signal is allowed for the current output:

- 4 … 20 mA

#### Definition of a safe state

| **Single channel structure (HFT=0)** | |
|---|---|
| 0 ... 20 mA | Not allowed |
| 4 … 20 mA | $(4\ mA - \Delta I) \leq I_{out} \leq (20\ mA + \Delta I)$ |

| **Two-channel structure (HFT=1)** | |
|---|---|
| **Unit 1** | |
| 0 … 20 mA | Not allowed |
| 4 … 20 mA | $(4\ mA - \Delta I) \leq I_{out1} \leq (20\ mA + \Delta I)$ |
| **Unit 2** | |
| 0 ... 20 mA | Not allowed |
| 4 … 20 mA | $(4\ mA - \Delta I) \leq I_{out2} \leq (20\ mA + \Delta I)$ |

| | |
|---|---|
| Condition | $\lvert I_{out1} - I_{out2} \rvert < 2\ \Delta I$ |

The following applies to the evaluation by the safety control:

All values that meet the specified conditions can be considered correct. All other values must be considered as dangerous.

#### Calculation of the measurement uncertainty

The uncertainty of measurement (ΔI) is calculated from the data sheet data and the operating temperature (ϑ) using the following formula:

| | | |
|---|---|---|
| $e_{max}$ | [%] | *: Maximum measuring deviation* |
| $TK_{Zero}$ | [%/10K] | *: Maximum temperature coefficient at zero point* |
| $TK_{Span}$ | [%/10K] | *: Maximum temperature coefficient of the span* |

$$\Delta I = \Delta I_{max} = 16\ [mA] \cdot \left[ e_{max} + (\lvert \vartheta - 20\ [°C] \rvert) \cdot (TK_{Zero} + TK_{Span}) \right]$$

### 2.1.3 Model with voltage output

Two signals are permitted for the voltage output:

- 2 … 10 V
- 1 … 5 V

The voltage output is set to 0 ... 10 V in the factory. However, this signal cannot be used for the safety function and must be parameterized to one of the permissible signals.

#### Definition of the safe state

| **Single channel structure (HFT=0)** | | | |
|---|---|---|---|
| 0 … 10 V | Not allowed | | |
| | | **$U_{min}$** | **$U_{max}$** |
| 2 … 10 V | $(U_{min} - \Delta U) \le U_{out} \le (U_{max} + \Delta U)$ | 2 V | 10 V |
| 1 … 5 V | | 1 V | 5 V |

| **Two-channel structure (HFT=1)** | | | |
|---|---|---|---|
| 0 … 10 V | Not allowed | | |
| | | **$U_{min}$** | **$U_{max}$** |
| 2 … 10 V | Gerät 1: $(U_{min} - \Delta U) \le U_{out1} \le (U_{max} + \Delta U)$ | 2 V | 10 V |
| 1 … 5 V | Gerät 2: $(U_{min} - \Delta U) \le U_{out2} \le (U_{max} + \Delta U)$ | 1 V | 5 V |
| Condition | $\lvert U_{out1} - U_{out2} \rvert < 2\,\Delta U$ | | |

The following applies to the evaluation by the safety control:

All values that meet the specified conditions can be considered correct. All other values must be considered as dangerous.

#### Calculation of the measurement uncertainty

The uncertainty of measurement (ΔU) is calculated from the data sheet information and the operating temperature (ϑ) using the following formula:

| | | |
|---|---|---|
| $e_{max}$ | [%] | *: Maximum measuring deviation* |
| $TK_{Zero}$ | [%/10K] | *: Maximum temperature coefficient at zero point* |
| $TK_{Span}$ | [%/10K] | *: Maximum temperature coefficient of the span* |
| $U_{max}$ | [V] | *: Maximum signal value of the analog output* |
| $U_{min}$ | [V] | *: Minimum signal value of the analog output* |

$$\Delta U = \Delta U_{max} = (U_{max} - U_{min}) \cdot \left[ e_{max} + (|\vartheta - 20\,[°C]|) \cdot (TK_{Zero} + TK_{Span}) \right]$$

### 2.1.4 Model with switch output

**Definition of the safe state**

The operator has to decide whether, from the point of view of the installation, an undercut or an overcut is considered safe. The states of the switching outputs can be assumed to be correct as long as they differ from one another.

| **Single channel structure (HFT=0)** | | |
|---|---|---|
| **Two switching outputs** | Undercut | Exceed |
| | SP1 = 0 and SP2 = 1 | SP1 = 1 and SP2 = 0 |
| **Four switching outputs** | | |
| | SP1 = 0 and SP2 = 1 | SP1 = 1 and SP2 = 0 |
| | SP3 = 0 and SP4 = 1 | SP3 = 1 and SP4 = 0 |

| **Two-channel structure (HFT=1)** | | |
|---|---|---|
| **Unit 1** | Undercut | Exceed |
| **Two switching outputs** | SP1 = 0 and SP2 = 1 | SP1 = 1 and SP2 = 0 |
| **Four switching outputs** | SP1 = 0 and SP2 = 1 | SP1 = 1 and SP2 = 0 |
| | SP3 = 0 and SP4 = 1 | SP3 = 1 and SP4 = 0 |

| **Device 2** | Undercut | Exceed |
|---|---|---|
| **Two switching outputs** | SP1 = 0 and SP2 = 1 | SP1 = 1 and SP2 = 0 |
| **Four switching outputs** | SP1 = 0 and SP2 = 1 | SP1 = 1 and SP2 = 0 |
| | SP3 = 0 and SP4 = 1 | SP3 = 1 and SP4 = 0 |

*1: low impedance (through-switched) switching output*

*0: high-impedance (blocked) switching output*

# 3 Notes on Planning

## 3.1 Intended use

The device can be used as part of a safety function to monitor differential pressure.

In the corresponding version, the device can be used in areas at risk of explosion Zone 2 and 22.

## 3.2 Parameters

**⚠ WARNING**

**Parameter change**

The device is configured in the factory before delivery. Only the operator of the system or personnel he names and briefs may carry out the configuration work.

The set default limits for the output signal may not be changed.

The parameterization can be changed in two ways.[1]

- By keyboard input on the device
- By remote parameterization via transmitter PC interface

Please also note the specifications in the section Parameterization [▸ 9].

## 3.3 Functional security (IEC 61508)

### 3.3.1 Operation mode

The unit is used with a low demand rate operating mode. The demand rate is less than once a year and no more than twice the frequency of the repeat test. The associated reference variable is the PFD value.

### 3.3.2 Inspection intervals

A Proof Test must be carried out after commissioning and then, at the latest, after the end of the defined test interval.

The tables in the section Safety performance indicators [▸ 21] state the mean probability of a malfunction in the requirement case depending on the test interval and the system architecture.

### 3.3.3 Lifetime

The lifetime starting from the production date is 10 years.

If the lifetime is exceeded, the error rates can gradually increase due to wear and aging, and the calculated PFD values can no longer be used. In worst cases, this leads to a loss of the SIL classification.

[1] Please observe the information in the operating instructions.

### 3.3.4 Assembly and installation

Please also observe the installation instructions in the operating manual.

**NOTICE! Beachten Sie, dass die Auswertung und Überwachung der Signale durch die nachgeschaltete Sicherheitssteuerung (SRP/CS) erfolgen muss. Bei einer Abweichung muss der sichere Zustand eingenommen werden.**

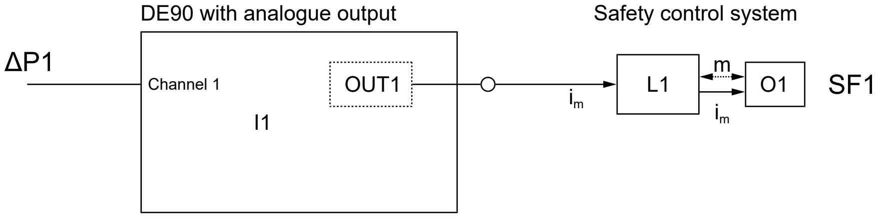
The following legend applies to the following connection diagrams:

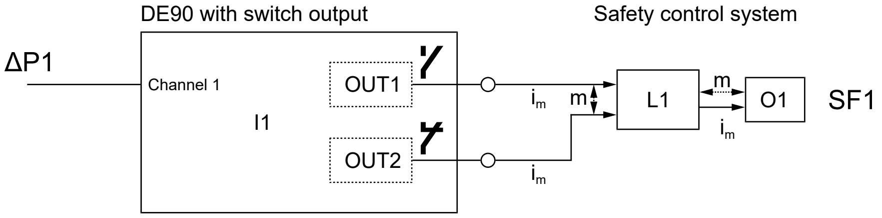
**Legend**

| | |
|---|---|
| $i_m$ | connecting equipment |
| c | Cross check |
| I1, I2 | Differential pressure transmitter (DE90) |
| L1...L4 | Logic |
| m | Monitoring |
| O1...O4 | Output units |
| OUT1...OUT4 | Output (DE90) |
| SF1, SF2 | Safety function 1, Safety function 2 |

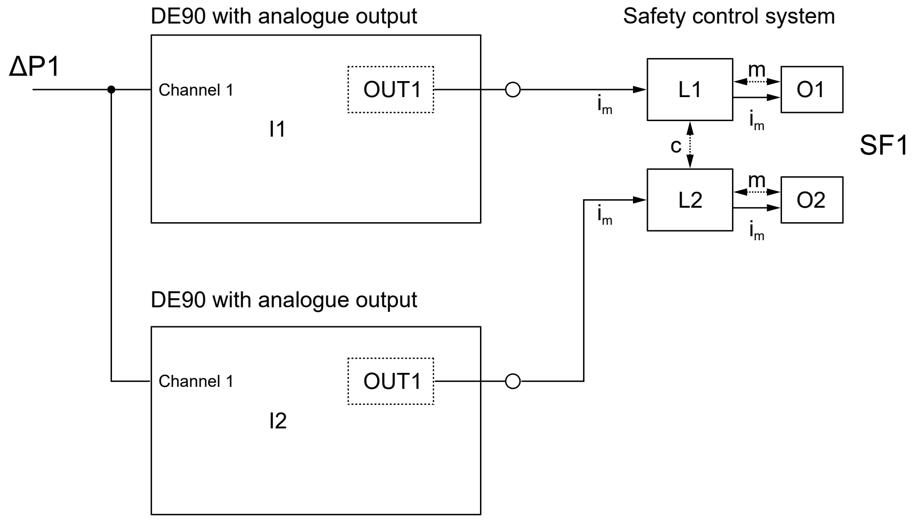
#### 3.3.4.1 Devices with one channel

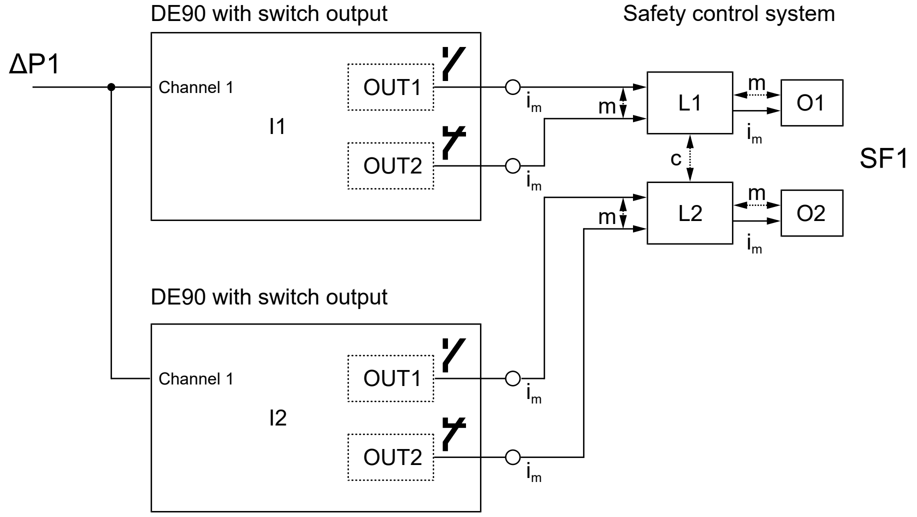
##### 3.3.4.1.1 Architecture 1oo1 (HFT=0)



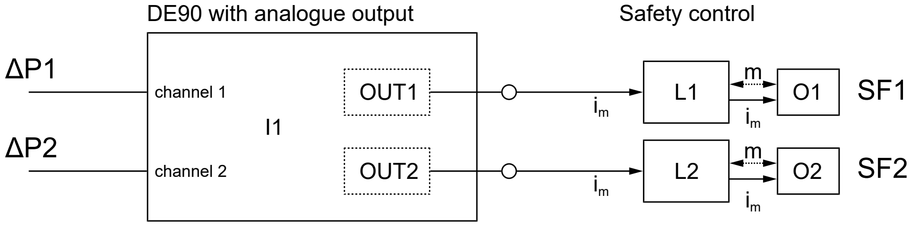
### 3.3.4.1.2 Architektur 1oo2 (HFT=1)

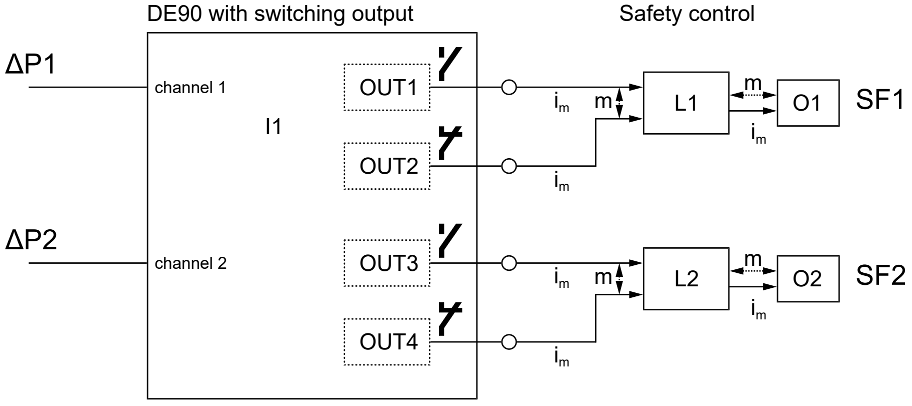


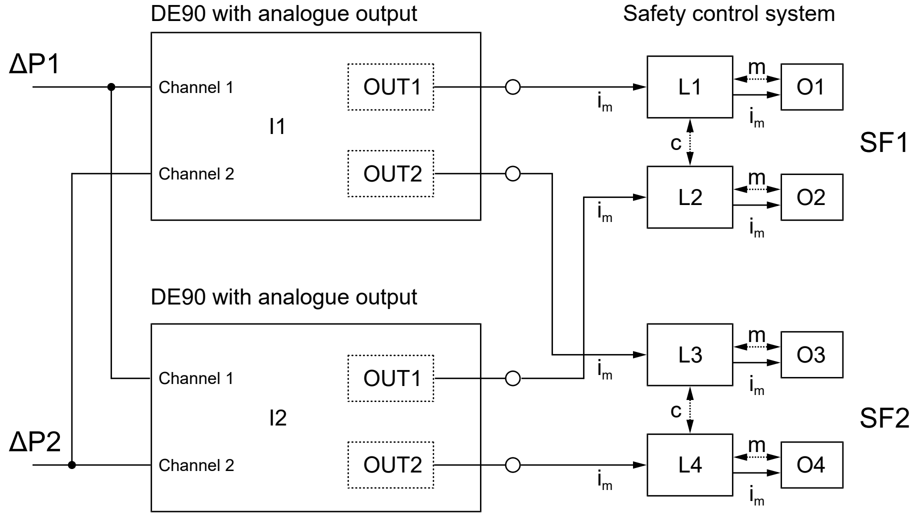
### 3.3.4.2 Devices with two channels

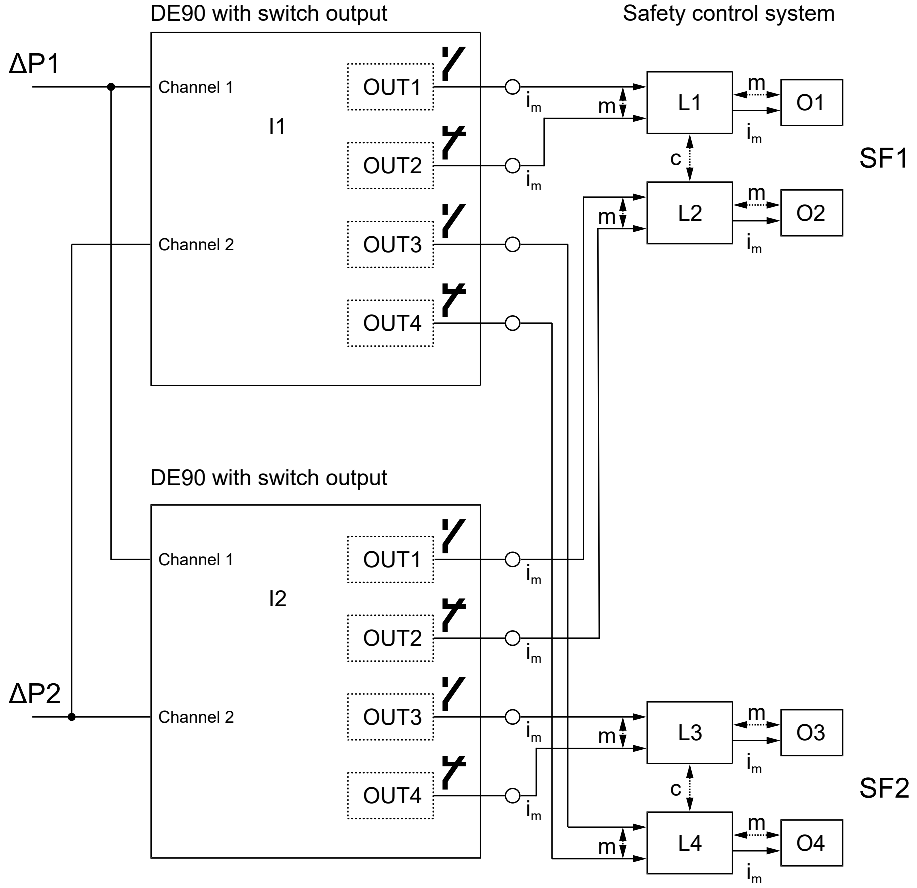
#### 3.3.4.2.1 Architecture 1oo1 (HFT=0)



### 3.3.4.2.2 Architecture 1002 (HFT=1)



## 3.4 Performance Level (EN ISO 13849-1)

### 3.4.1 Operation mode

The unit is used with a high demand rate operating mode. Maximum one requirement per year allowed.

### 3.4.2 Inspection intervals

Conduct a proof test after commissioning and then after 5 years at the latest.

### 3.4.3 Lifetime

The lifetime starting from the production date is 20 years.

If the lifetime is exceeded, the error rates can gradually increase due to wear and aging.

### 3.4.4 Assembly and installation

Please also observe the installation instructions in the operating manual.

**NOTICE! Please note that the evaluation and monitoring of the signals must be carried out by the downstream safety controller (SRP/CS). If there is a deviation, the safe state must be assumed.**

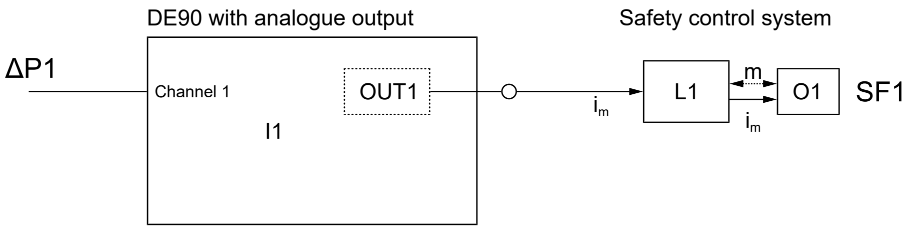
The following legend applies to the following connection diagrams:

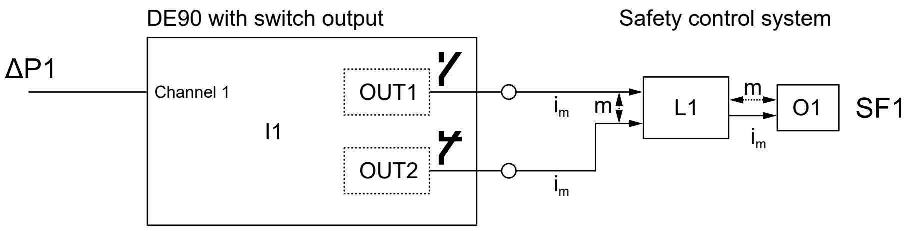
**Legend**

| | |
|---|---|
| $i_m$ | connecting equipment |
| c | Cross check |
| I1, I2 | Differential pressure transmitter (DE90) |
| L1...L4 | Logic |
| m | Monitoring |
| O1...O4 | Output units |
| OUT1...OUT4 | Output (DE90) |
| SF1, SF2 | Safety function 1, Safety function 2 |

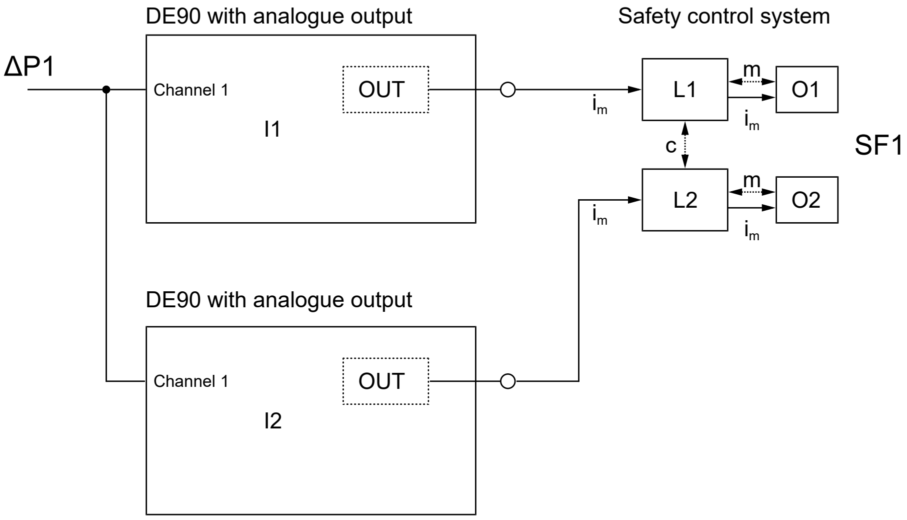
#### 3.4.4.1 Devices with one channel

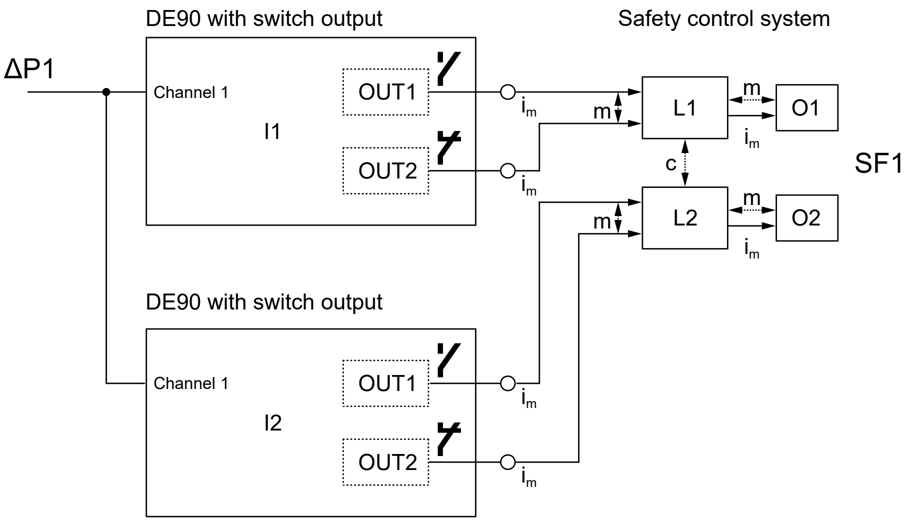
##### 3.4.4.1.1 Category 1



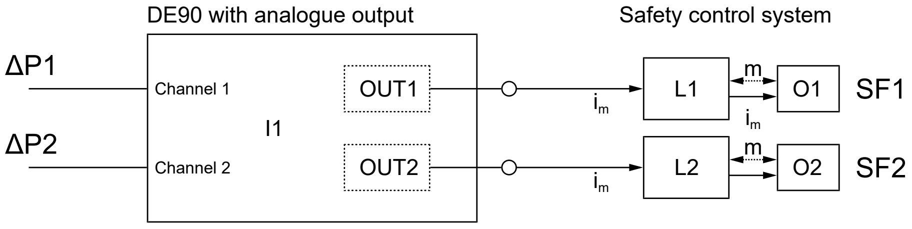
### 3.4.4.1.2 Category 3

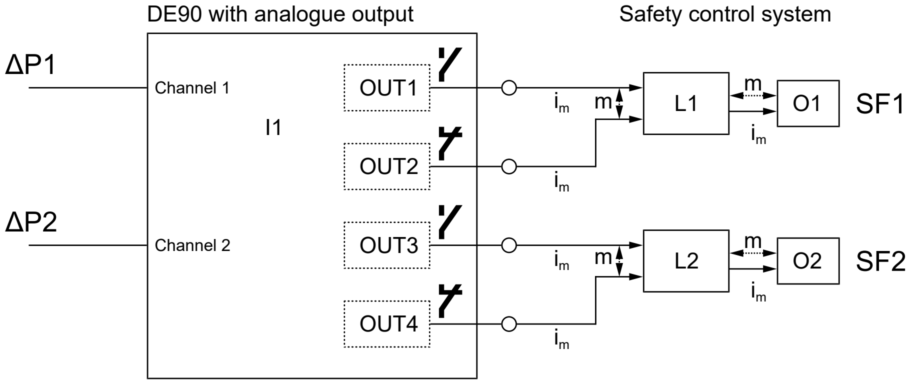


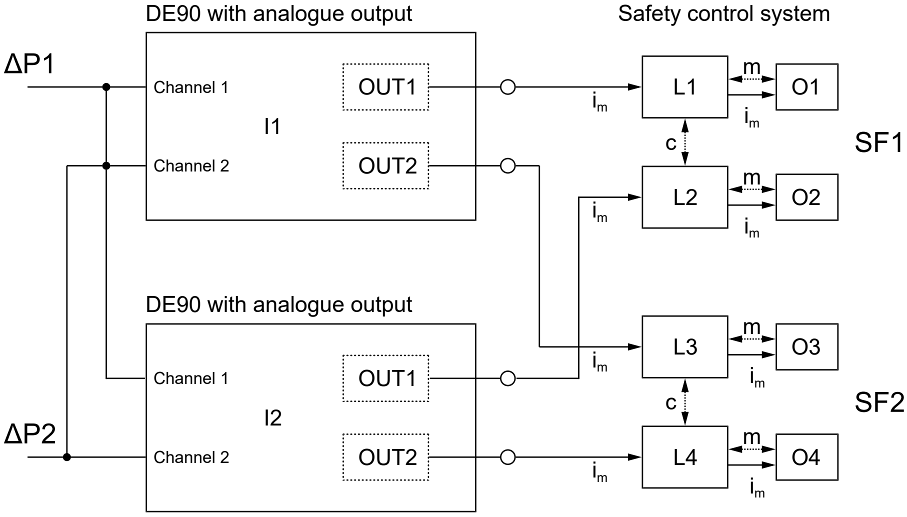
### 3.4.4.2 Devices with two channels

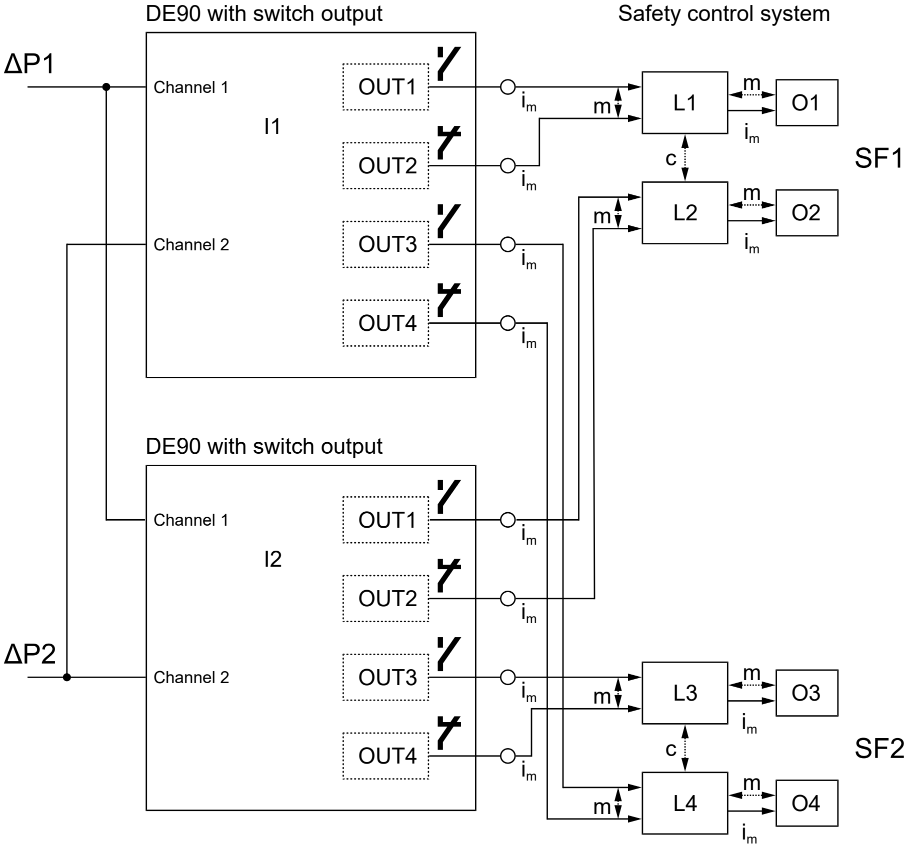
#### 3.4.4.2.1 Category 1



### 3.4.4.2.2 Category 3



# 4 Repeat tests

## 4.1 Maintenance

Proof tests are an integral part of the safety concept to detect dangerous failures. The proof test checks the following aspects of a safety-critical component:

- Functionality
- do the components satisfy the prevailing application conditions
- are the interfaces to other components OK

All critical parts need to be tested with the proof test. Spot checks are sufficient for parts that are not critical for safety.

## 4.2 Function test (proof test)

**NOTICE! The EMC and environmental conditions must correspond to the tested levels of the EMC Directive 2014/30/EU.**

The determination of the proof-test procedure for the entire safety engineering system is the responsibility of the operator.

The following functional test must be carried out for the DE90 safety component.

1. Checking the functionality for input values within the measuring range
2. Checking the switching points

If possible, the test pressure should be generated by the Safety Engineering System (SIS) itself. In this case, it can be checked at the same time whether the signals are correctly processed by the higher-level safety control system and forwarded via the actuator.

Otherwise the DE90 must be removed and connected as follows Please note that some versions do not have an analogue output.

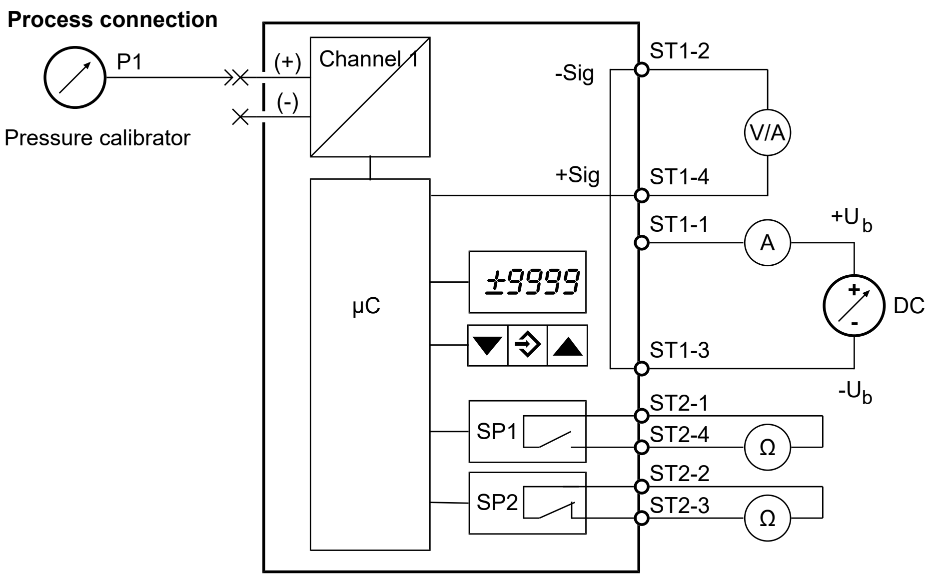



*Fig. 2:* Functional test

### 4.2.1 Analog output

- Set an operating voltage within the range of the permissible operating voltage.
- Check the power consumption. The power consumption must not exceed the value specified in the data sheet.
- The calculation of the measurement uncertainty ΔI or ΔU can be found in
  - Version with Current output [▸ 6] resp.
  - Ausführung mit Voltage output [▸ 7].

#### Input values within the measuring range

1. Use the pressure calibrator to set an input signal that corresponds to the beginning of the measuring range.
2. Check the output signal using a multimeter.
   - When using a voltage signal, the value must be within $U_{min}$ ± ΔU.
   - If the current signal is used, the value must be within 4mA ± ΔI.
3. Use the pressure calibrator to set an input signal that corresponds to the end of the measuring range.
4. Check the output signal using a multimeter.
   - When using a voltage signal, the value must be within Umax ± ΔU.
   - If the current signal is used, the value must be within 20mA ± ΔI.
5. Repeat these steps for each measuring channel.

#### Input values outside the measuring range

1. Use the pressure calibrator to set an input signal that is well below the beginning of the measuring range.
2. Check the output signal using a multimeter.
   - When using a voltage signal, the value must be below Umin - ΔU.
   - If the current signal is used, the value must be below 4mA - ΔI.
3. Use the pressure calibrator to set an input signal that is well above the end of the measuring range.
4. Check the output signal using a multimeter.
   - When using a voltage signal, the value must be above Umax + ΔU.
   - If the current signal is used, the value must be within 20mA + ΔI.
5. Repeat these steps for each measuring channel.

#### Checking the error signal in the SIS

1. Connect the analogue output of the DE90 electrically to the higher level safety controller.
2. Use the pressure calibrator to set an input signal that is well below the start of the measuring range so that an error signal is generated.
3. Check whether the faulty signal is detected by the safety controller.

### 4.2.2 Switch output

- Set an operating voltage within the range of the permissible operating voltage.
- Check the power consumption. The power consumption must not exceed the value specified in the data sheet.
- When evaluating the switching states, it must be noted whether the defined switching points are monitored if they are exceeded or not. The correct switching states can be found in the section Device description/Model with switch output [▶ 8].

**Check behaviour of the adjusted switching point.**

$P_{SP}$ is the parameterized switching point
$\Delta MB_{max}$ corresponds to the (basic) measuring deviation according to the data sheet.

1. Use the pressure calibrator to set the input signal to $P < P_{SP} - \Delta MB_{max}$ . Check the states of the switching outputs. The contacts must not switch (initial state).
2. Use the pressure calibrator to set the input signal to $P > P_{SP} - \Delta MB_{max}$ (passing the switching point). Check the states of the switching outputs. The contacts must now have switched.
3. Use the pressure calibrator to set the input signal to $P < P_{SP} - \Delta MB_{max}$ . Check the states of the switching outputs. The contacts must now have switched back to their original state.

**Checking the error signal in the SIS**

1. Connect the two switching outputs of the device electrically to the higher-level safety controller.
2. Use the pressure calibrator to set an input signal that is clearly below the set switching point. Check the states of the switching outputs. The contacts must not switch (output state). Check whether the change in state of the device is detected by the safety controller.
3. Now change the input signal during operation so that it is clearly above the set switching point (passing the switching point). Check the states of the switching outputs. The contacts must now have switched. Check whether the change of state of the device is detected by the safety controller.
4. Use the pressure calibrator to set an input signal that is clearly below the set switching point. Check the states of the switching outputs. The contacts must now have switched back to their original state. Check whether the change in state of the device is detected by the safety controller.

### 4.2.3 Assessment

If the device does not pass one of the stated steps, the function test is failed and the device must be replaced immediately.

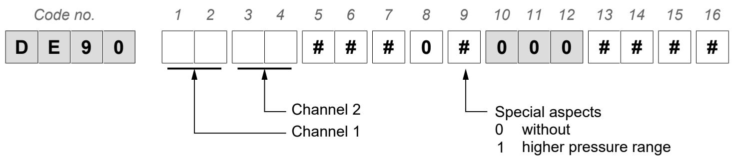
# 5 Safety-relevant variables

**NOTICE! The safety performance indicators do not apply for devices with a Modbus.**

The safety-related performance indicators depend on the sensors used (Type A or Type B) for the respective pressure range. For this reason, the performance indicators are sorted according to sensor type and pressure range. The performance indicators apply per channel.

## 5.1 Sensor type A

The following safety performance indicators apply for the following device models:




| Measuring range | Special aspects = 0 | Measuring range | Special aspects = 1 |
|---|---|---|---|
| **51** | 0 … 1 mbar | **52** | 0 … 4 mbar |
| **A4** | -1 … +1 mbar | **53** | 0 … 6 mbar |
| **D1** | 0 … 25 Pa | **54** | 0 … 10 mbar |
| **D2** | 0 … 40 Pa | **A6** | -2.5 … +2.5 mbar |
| **D3** | 0 … 60 Pa | **A7** | -4 … +4 mbar |
| **D4** | 0 … 100 Pa | **A8** | -6 … +6 mbar |
| **L5** | -25 … +25 Pa | **A9** | -10 … +10 mbar |
| **R6** | -40 … +40 Pa | **D7** | 0 … 400 Pa |
| **2L** | -60 … +60 Pa | **D8** | 0 … 600 Pa |
| **L7** | -100 … +100 Pa | **N1** | 0 … 1 kPa |
| **L0** | -20 … + 80 Pa | **L6** | -250 … +250 Pa |
| | | **R1** | -400 … +400 Pa |
| | | **R2** | -600 … +600 Pa |
| | | **S8** | -1 … +1 kPa |

### 5.1.1 Model with analogue output

| Safety coefficients | | |
|---|---|---|
| $\lambda_s$ | 142.3 Fit | Safe failure rate |
| $\lambda_d$ | 2046.6 Fit | Dangerous failure rate |
| $\lambda_{dd}$ | 1291.8 Fit | Dangerous detected failure rate |
| $\lambda_{du}$ | 754.8 Fit | Dangerous undetected failure rate |

**SIL (EN 61508)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | Low Demand | Requirement max. 1/year |

#### 1oo1 architecture

| | | |
|---|---|---|
| HFT | 0 | Hardware fault tolerance |
| SFF | 65.5 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $3.3 \cdot 10^{-3}$ | $6.6 \cdot 10^{-3}$ | $1.7 \cdot 10^{-2}$ | $3.3 \cdot 10^{-2}$ |
| SIL | SIL1 | SIL1 | SIL1 | SIL1 |

#### 1oo2 architecture

| | | |
|---|---|---|
| $\beta$ | 10% | Probability that the same error occurs at the same time in both channels. |
| $\beta_d$ | 5% | Probability that the same dangerous error occurs at the same time in both channels. |
| MRT | 8 h | Mean repair time |
| MTTR | 8 h | Mean time to repair |
| HFT | 1 | Hardware fault tolerance |
| SFF | 65.5 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $3.5 \cdot 10^{-4}$ | $7.1 \cdot 10^{-4}$ | $2.0 \cdot 10^{-3}$ | $4.6 \cdot 10^{-3}$ |
| SIL | SIL2 | SIL2 | SIL2 | SIL2 |

**PL (DIN EN ISO 13849)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | High Demand | Requirement max. 1/year |

| | | | |
|---|---|---|---|
| $MTTF_d$ | 55.8 years | high | Mean time to dangerous failure |
| DC | 63.1 % | low | Diagnostic coverage factor |

| Achievable performance level | PL |
|---|---|
| Category 1 | c |
| Category 3 | d |

### 5.1.2 Model with switch output

| Safety coefficients | | |
|---|---|---|
| $\lambda_s$ | 177.2 Fit | Safe failure rate |
| $\lambda_d$ | 2402.9 Fit | Dangerous failure rate |
| $\lambda_{dd}$ | 1741.3 Fit | Dangerous detected failure rate |
| $\lambda_{du}$ | 661.7 Fit | Dangerous undetected failure rate |

**SIL (EN 61508)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | Low Demand | Requirement max. 1/year |

#### 1oo1 architecture

| | | |
|---|---|---|
| HFT | 0 | Hardware fault tolerance |
| SFF | 74.4 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $2.9 \cdot 10^{-3}$ | $5.8 \cdot 10^{-3}$ | $1.5 \cdot 10^{-2}$ | $2.9 \cdot 10^{-2}$ |
| SIL | SIL1 | SIL1 | SIL1 | SIL1 |

#### 1oo2 architecture

| | | |
|---|---|---|
| $\beta$ | 10% | Probability that the same error occurs at the same time in both channels. |
| $\beta_d$ | 5% | Probability that the same dangerous error occurs at the same time in both channels. |
| MRT | 8 h | Mean repair time |
| MTTR | 8 h | Mean time to repair |
| HFT | 1 | Hardware fault tolerance |
| SFF | 74.4 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $3.0 \cdot 10^{-4}$ | $6.2 \cdot 10^{-4}$ | $1.7 \cdot 10^{-3}$ | $3.9 \cdot 10^{-3}$ |
| SIL | SIL2 | SIL2 | SIL2 | SIL2 |

**PL (EN ISO 13849)**

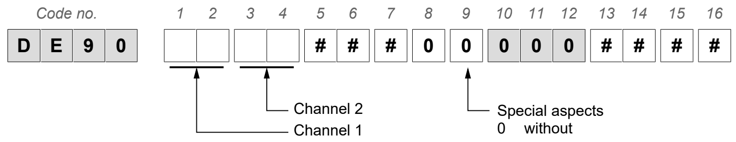
| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | High Demand | Requirement max. 1/year |

| | | | |
|---|---|---|---|
| $MTTF_d$ | 47.5 years | high | Mean time to dangerous failure |
| DC | 72.5 % | low | Diagnostic coverage factor |

| Achievable performance level | PL |
|---|---|
| Category 1 | c |
| Category 3 | d |

## 5.2 Sensor type B

The following safety performance indicators apply for the following device models:




| Measuring range | | Measuring range | |
|---|---|---|---|
| **52** | 0 … 4 mbar | **D7** | 0 … 400 Pa |
| **55** | 0 … 16 mbar | **N2** | 0 … 1.6 kPa |
| **56** | 0 … 25 mbar | **N3** | 0 … 2.5 kPa |
| **57** | 0 … 40 mbar | **N4** | 0 … 4 kPa |
| **58** | 0 … 60 mbar | **N5** | 0 … 6 kPa |
| **59** | 0 … 100 mbar | **E5** | 0 … 10 kPa |
| **60** | 0 … 160 mbar | **E6** | 0 … 16 kPa |
| **82** | 0 … 250 mbar | **E7** | 0 … 25 kPa |
| **A6** | -2.5 … +2.5 mbar | **R1** | -400 … +400 Pa |
| **A7** | -4 … +4 mbar | **L6** | -250 … +250 Pa |
| **B1** | -16 … +16 mbar | **L9** | -1.6 … +1.6 kPa |
| **C5** | -40 … +40 mbar | **M6** | -2.5 … +2.5 kPa |
| **B2** | -25 … +25 mbar | **M7** | -4 … +4 kPa |
| **B3** | -60 … +60 mbar | **M8** | -6 … +6 kPa |
| **B4** | -100 … +100 mbar | **R8** | -10 … +10 kPa |
| **R5** | -160 … +160 mbar | **R9** | -16 … +16 kPa |
| **B6** | -250 … +250 mbar | **T1** | -25 … +25 kPa |

### 5.2.1 Model with analogue output

| Safety coefficients | | |
|---|---|---|
| $\lambda_s$ | 142.3 Fit | Safe failure rate |
| $\lambda_d$ | 992.6 Fit | Dangerous failure rate |
| $\lambda_{dd}$ | 614.2 Fit | Dangerous detected failure rate |
| $\lambda_{du}$ | 378.3 Fit | Dangerous undetected failure rate |

**SIL (EN 61508)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | Low Demand | Requirement max. 1/year |

#### 1oo1 architecture

| | | |
|---|---|---|
| HFT | 0 | Hardware fault tolerance |
| SFF | 66.7 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $1.7 \cdot 10^{-3}$ | $3.3 \cdot 10^{-3}$ | $8.3 \cdot 10^{-3}$ | $1.7 \cdot 10^{-2}$ |
| SIL | SIL1 | SIL1 | SIL1 | SIL1 |

#### 1oo2 architecture

| | | |
|---|---|---|
| $\beta$ | 10% | Probability that the same error occurs at the same time in both channels. |
| $\beta_d$ | 5% | Probability that the same dangerous error occurs at the same time in both channels. |
| MRT | 8 h | Mean repair time |
| MTTR | 8 h | Mean time to repair |
| HFT | 1 | Hardware fault tolerance |
| SFF | 66.7 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $1.7 \cdot 10^{-4}$ | $3.5 \cdot 10^{-4}$ | $9.1 \cdot 10^{-4}$ | $2.0 \cdot 10^{-3}$ |
| SIL | SIL2 | SIL2 | SIL2 | SIL2 |

**PL (EN ISO 13849)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | High Demand | Requirement max. 1/year |

| | | | |
|---|---|---|---|
| $MTTF_d$ | 115 years | high | Mean time to dangerous failure |
| DC | 61.9 % | low | Diagnostic coverage factor |

| Achievable performance level | PL |
|---|---|
| Category 1 | c |
| Category 3 | d |

### 5.2.2 Model with switch output

| Safety coefficients | | |
|---|---|---|
| $\lambda_s$ | 177.2 Fit | Safe failure rate |
| $\lambda_d$ | 1348.9 Fit | Dangerous failure rate |
| $\lambda_{dd}$ | 1038.6 Fit | Dangerous detected failure rate |
| $\lambda_{du}$ | 310.3 Fit | Dangerous undetected failure rate |

**SIL (EN 61508)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | Low Demand | Requirement max. 1/year |

#### 1oo1 architecture

| | | |
|---|---|---|
| HFT | 0 | Hardware fault tolerance |
| SFF | 79.7 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $1.4 \cdot 10^{-3}$ | $2.7 \cdot 10^{-3}$ | $6.8 \cdot 10^{-3}$ | $1.4 \cdot 10^{-2}$ |
| SIL | SIL1 | SIL1 | SIL1 | SIL1 |

#### 1oo2 architecture

| | | |
|---|---|---|
| $\beta$ | 10% | Probability that the same error occurs at the same time in both channels. |
| $\beta_d$ | 5% | Probability that the same dangerous error occurs at the same time in both channels. |
| MRT | 8 h | Mean repair time |
| MTTR | 8 h | Mean time to repair |
| HFT | 1 | Hardware fault tolerance |
| SFF | 79.7 % | Safe failure fraction |

The probability of a failure on demand (PFD) depends on the test interval.

| Proof-Test interval | 1 year | 2 years | 5 years | 10 years |
|---|---|---|---|---|
| PFD | $1.4 \cdot 10^{-4}$ | $2.8 \cdot 10^{-4}$ | $7.4 \cdot 10^{-4}$ | $1.6 \cdot 10^{-3}$ |
| SIL | SIL2 | SIL2 | SIL2 | SIL2 |

**PL (EN ISO 13849)**

| | | |
|---|---|---|
| Device type | Type B | Complex device |
| Operating mode | High Demand | Requirement max. 1/year |

| | | | |
|---|---|---|---|
| $MTTF_d$ | 84.6 years | high | Mean time to dangerous failure |
| DC | 77 % | low | Diagnostic coverage factor |

| Achievable performance level | PL |
|---|---|
| Category 1 | c |
| Category 3 | d |

# 6 Attachments

## 6.1 Glossary

| Fig. (↓A Z) | Definition |
|---|---|
| β | **Common Cause Factor**<br>Proportionality factor between the CCF rate (failure due to a common cause) and the dangerous failure rate of the individual channel. |
| DC | **Diagnostic Coverage Factor**<br>The DC parameter shows the ratio of the number of detected dangerous failures ($\lambda_{DD}$) to the total number of dangerous failures ($\lambda_D$) an.<br>$DC = \frac{\sum \text{dangerous detected failure}}{\sum \text{dangerous failure}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$ |
| FIT | **Failure in Time**<br>Failure rate with respect to the time interval $10^9$ hours.<br>$1\ FIT = 1 \times 10^{-9} \frac{1}{h}$ |
| FMEDA | **Failure Mode Effect and Diagnostic Analysis**<br>Procedure to determine causes of failures and their impact on the system |
| HDM | **High Demand Mode**<br>Operating mode with high or continuous demand on the safety function. The demand rate to the safety system is greater than once annually. |
| HFT | **Hardware Fault Tolerance**<br>The hardware fault tolerance states how many dangerous failures are possible due to the architecture without endangering the execution of the safety function.<br>• HFT = 0<br>The occurrence of a dangerous failure will lead to a failure of the safety function.<br>• HFT = 1<br>Only the occurrence of two dangerous failures will lead to a failure of the safety function. |
| LDM | **Low Demand Mode**<br>The safety function will only be carried out on demand to bring the system into a defined safe state. The frequency of requirements does not exceed one a year. |

| | | |
|---|---|---|
| **MooN** | **Architecture with M out of N channels** | System architecture MooN with the variables M and N:<br>Classification and description of safety-related systems with regard to redundancy and applied selection procedures.<br>• N - is the total number of redundant channels of a safety-related architecture and/or safety circuit.<br>• M - determines the number of channels that must operate correctly to carry out the safety function. |
| **MTBF** | **Mean Time Between Failures** | Mean operating duration between two failures. |
| **$MTTF_d$** | **Mean Time To Dangerous Failures** | Operating duration up to a dangerous fault. |
| **MRT** | **Mean Repair Time** | Mean time for the repair. |
| **MTTR** | **Mean Time To Repair** | Average time between the occurrence of a failure and restoration of the system. |
| **PFD** | **Probability of Failure on Demand** | Probability of a dangerous failure on demand of the safety function for an operating mode with a low demand rate. |
| **PFH** | **Probability of a dangerous Failure per Hour** | Frequency of a dangerous failure of the safety function for an operating mode with a high or continuous demand rate (high demand). |
| **PFS** | **Probability of Failure Spurious** | Frequency of failure due to a false alarm that leads to an unintentional process shutdown by the safety system. The smaller the value, the higher the system availability. |
| **SFF** | **Safe Failure Fraction** | This is determined by the rate of non-dangerous errors plus the diagnosed and/or recognised errors in ration to the overall failure rate of the system. |
| **SIF** | **Safety Instrumented Function** | The safety function (SIF) is a protective measure that is only activated in the event of an incident to prevent injuries, damage and pollution. |

| | | |
|---|---|---|
| **SIL** | **Safety Integrity Level** | One of four discrete levels to assess the requirements relating to the reliability of the safety functions in safety systems. SIL 4 is the highest and SIL 1 the lowest safety integrity level. Each level corresponds to a probability range for the failure of a safety function. |
| **SIS** | **Safety Instrumented System** | Safety system for performance of one or several safety functions. A system of this kind comprises at least a sensor, an overriding safety control system and an actuator. |
| **$T_1$** | **Proof Test Interval** | The safety system must always be in a state that guarantees the defined safety integrity. The proof test is carried out to confirm this. The test interval states the intervals in which a proof test needs to be carried out to guarantee the safety function. |

## 6.2 Failure rates

The error rates differ in principle as follows:

1. Safe failures
2. Dangerous failures
3. No effect failure

The first two types of errors are further divided into detectable and undetectable errors.

The failure without effect and the safe failures, whether detected or undetected, have no influence on the safety function. On the other hand, dangerous errors lead to a dangerous state of the system. The following diagram provides an overview.

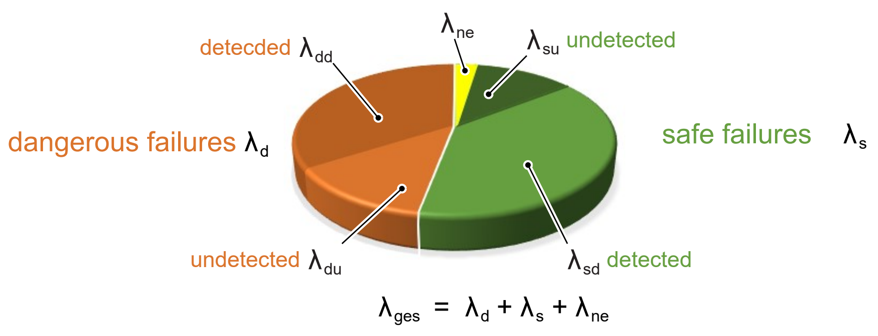



*Fig. 3:* Failure rates

| | |
|---|---|
| $\lambda_d$ | **Dangerous failure rate** |
| $\lambda_{dd}$ | **Dangerous detected failure rate** |
| $\lambda_{du}$ | **Dangerous undetected failure rate** |
| $\lambda_s$ | **Safe failure rate** |
| $\lambda_{sd}$ | **Safe detected failure rate** |
| $\lambda_{su}$ | **Safe undetected failure rate** |
| $\lambda_{ne}$ | **No effect failure rate** |

## 6.3 Unit types

**Type A** — **Simple operating equipment**

Type A units are 'simple' units for which the failure behaviour of all parts used and the behaviour under failure conditions is completely known.

This includes e.g. relays, resistors and transistors, however no complex electronic parts, e.g. microcontrollers.

**Type B** — **Complex operating equipment**

Type B units are 'complex' units for which the failure behaviour of all parts used and the behaviour under failure conditions is not completely known.

These units contain electronic parts such as microcontrollers, microprocessors or ASICs. In these parts and, in particular for software-controlled functions, it is difficult to fully determine all failures.

## Notes

FISCHER MESS- UND REGELTECHNIK

developing solutions

**FISCHER Mess- und Regeltechnik GmbH**
Bielefelder Str. 37a
D-32107 Bad Salzuflen

Tel. +49 5222 974-0
Fax +49 5222 7170
www.fischermesstechnik.de
info@fischermesstechnik.de