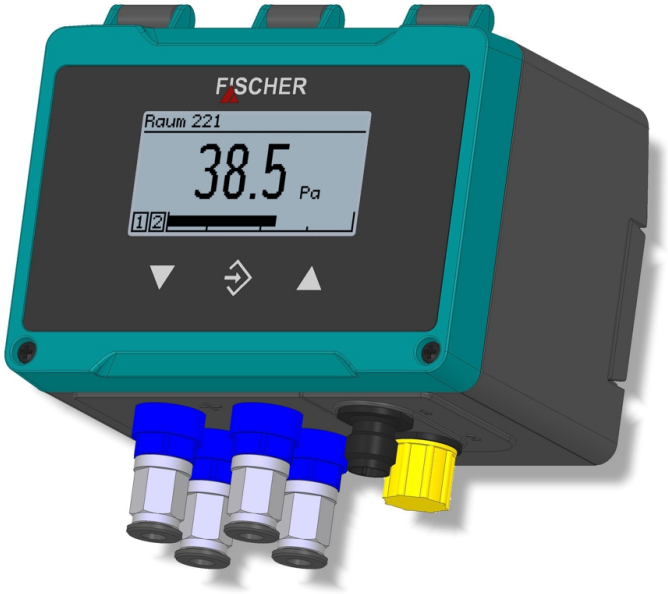
developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL
ISO 13849
PLd

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

RoHS III COMPLIANT



Safety manual

DE91

Differential pressure transmitter
PRO-LINE ®

for low pressure measurements

50043 • SHB_EN_DE91 • Rev. ST4-A • 05/26

Imprint

Manufacturer: **FISCHER Mess- und Regeltechnik GmbH**

Bielefelderstr. 37a
D-32107 Bad Salzuflen

Telephone: +49 5222 974 0

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

Technical editorial team: Technical editor: R. Kleemann

Version history

Rev. ST4-A 05/26	Version 1 (First edition)

Table of contents

1 Scope and standards

WARNING! This Safety Manual should only be used in conjunction with the operating instructions of the respective device. 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 DE91in safety-related systems.

It is designed for persons who 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 DE91 of the series PRO-LINE® with the following restrictions.

- Firmware version 1.45 or later.
- Versions with a Modbus or IO-Link interface are not permitted.
- In the case of two-channel devices, both channels must not be used for the same safety function, and both channels must only be fitted with ceramic pressure sensors.
- 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.

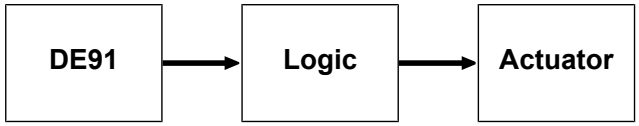


Fig. 1: Processing chain

The following norms are referenced for the calculations.

Functional security	**IEC 61508: 2010** Functional safety of safety-related electrical/ electronic/programmable electronic systems
Safety of Machinery	**EN ISO 13849-1:2023** Safety of machinery - Safety-related parts of control systems - Part 1: General design principles
Part failure rate	**SN 29500: 2010** 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 model, the device has one or two analogue outputs. Devices without an analogue output do not need to be configured. The outputs can be configured as current or voltage outputs. Both outputs must be configured as follows:

Analogue output 1	Parameter	Value
	An.output 1 assignment	Channel 1
	Limit C1	Off
Analogue output 2	Parameter	Value
	An.output 2 assignment	Channel 2
	Limit C2	Off
Signal limits	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

Switch outputs

Depending on the model, the device has two or four switch outputs. Two switch outputs each must be switched in an inverting manner. Both switch outputs switch at the same setpoint (SP1=SP2) or (SP3=SP4) and must be configured as follows.

Switch output 1	Value	Switch 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

Switch output 3	Value	Switch 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 closed

P_{SP}: Programmed switch 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*

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

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	$(U_{min} - \Delta U) \leq U_{out} \leq (U_{max} + \Delta U)$	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: $(U_{min} - \Delta U) \leq U_{out1} \leq (U_{max} + \Delta U)$	2 V	10 V
1 … 5 V	Gerät 2: $(U_{min} - \Delta U) \leq U_{out2} \leq (U_{max} + \Delta U)$	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.

There are two ways to complete the configuration.[1]

- Using the unit's keyboard
- Remote configuration using the transmitter PC interface

Please also note the guidelines in the section Configuration [▶ 5].

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 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 see the information in the operating instructions.

3.3.4 Assembly and installation

Please also observe the assembly instructions in the operating instructions.

NOTICE! Please note that the signals must be analysed and monitored with the downstream safety control system (SRP/CS). In case of a deviation, the safe state needs to be adopted.

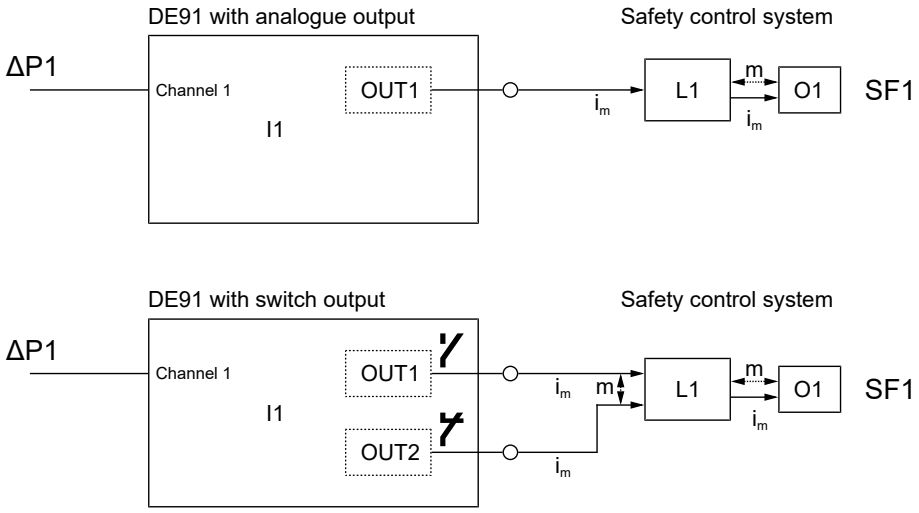
The following key applies to the wiring diagrams below:

Legend

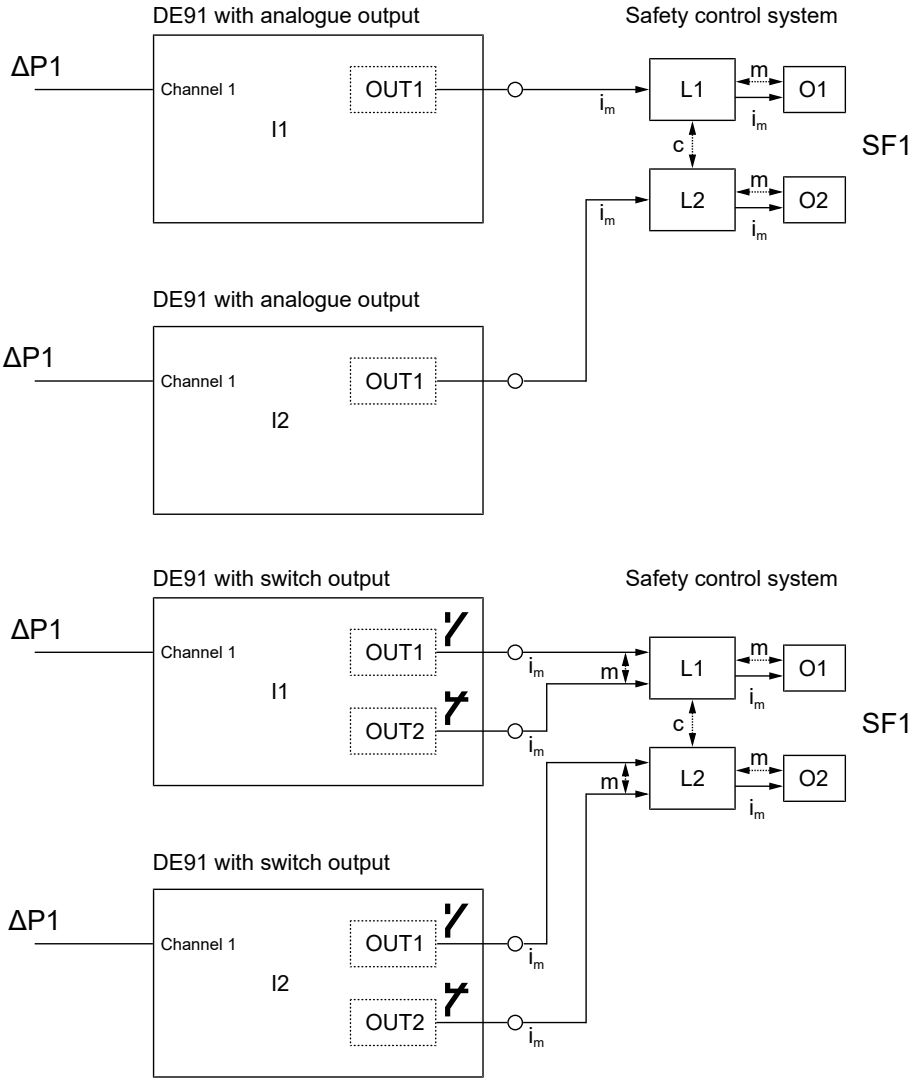
i_m	connecting equipment
c	Cross check
I1, I2	Differential pressure transmitter (DE91)
L1...L4	Logic
m	Monitoring
O1...O4	Output units
OUT1...OUT4	Output (DE91)
SF1, SF2	Safety function 1, Safety function 2

3.3.4.1 Devices with one channel

3.3.4.1.1 Architecture 1oo1 (HFT=0)

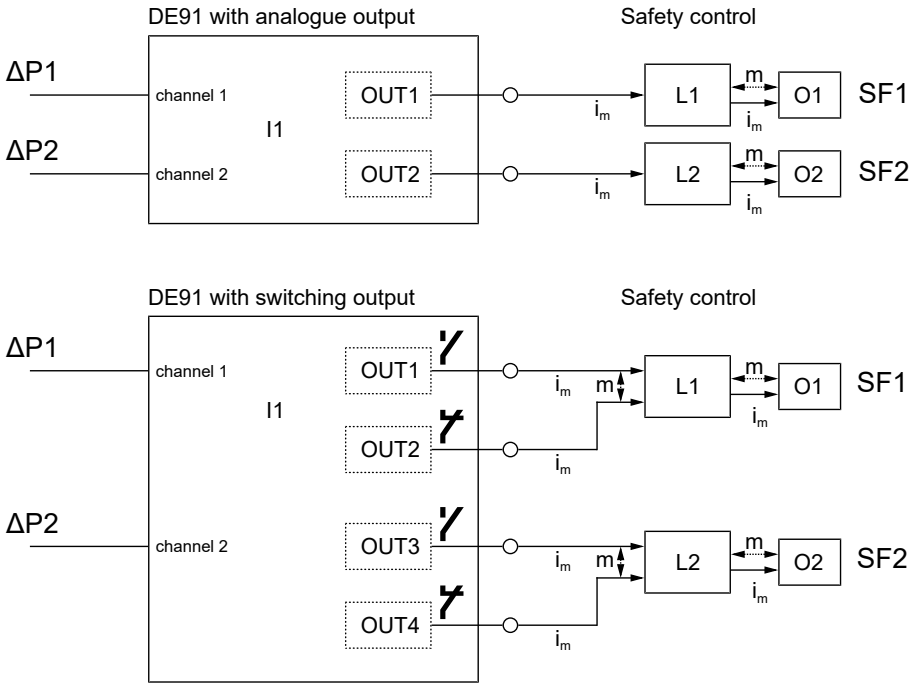


3.3.4.1.2 Architektur 1oo2 (HFT=1)

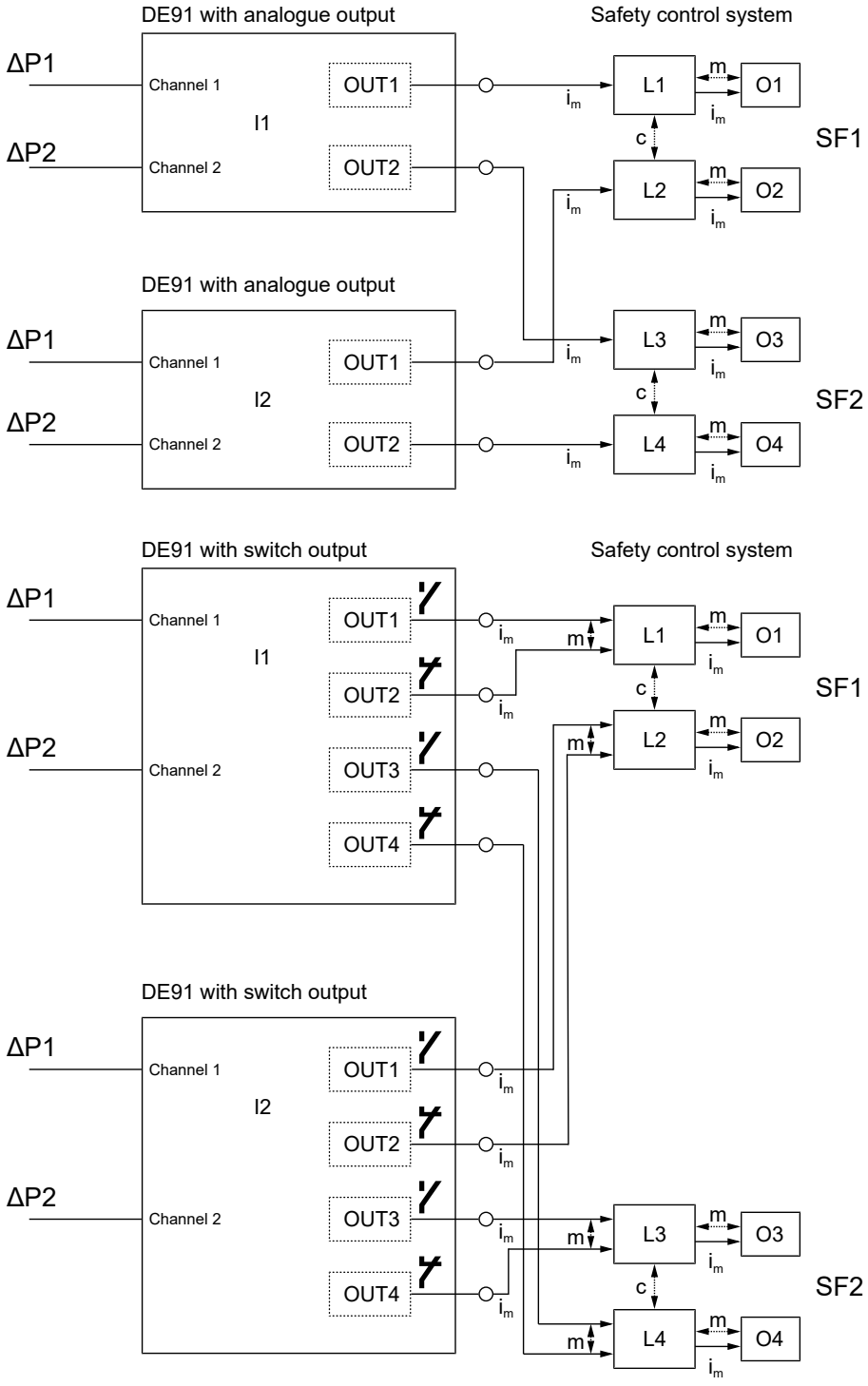


3.3.4.2 Devices with two channels

3.3.4.2.1 Architecture 1oo1 (HFT=0)



3.3.4.2.2 Architecture 1oo2 (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 assembly instructions in the operating instructions.

NOTICE! Please note that the signals must be analysed and monitored with the downstream safety control system (SRP/CS). In case of a deviation, the safe state needs to be adopted.

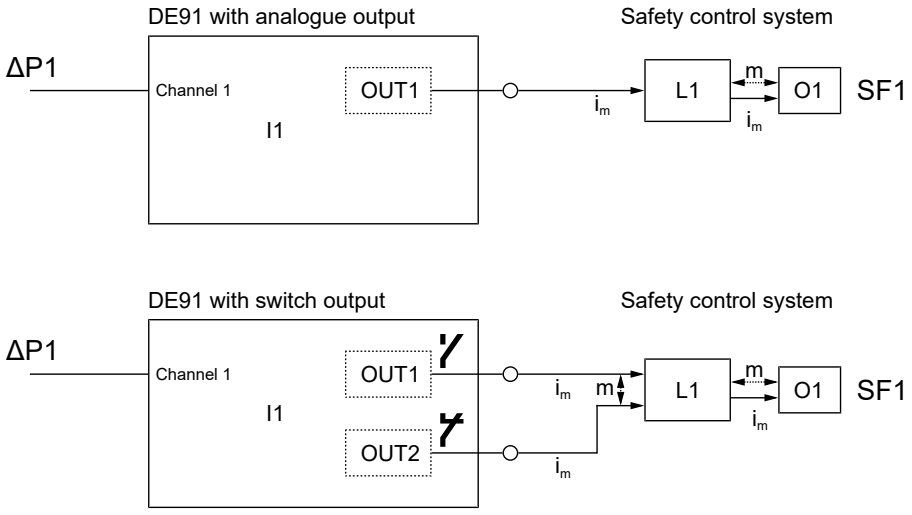
The following key applies to the wiring diagrams below:

Legend

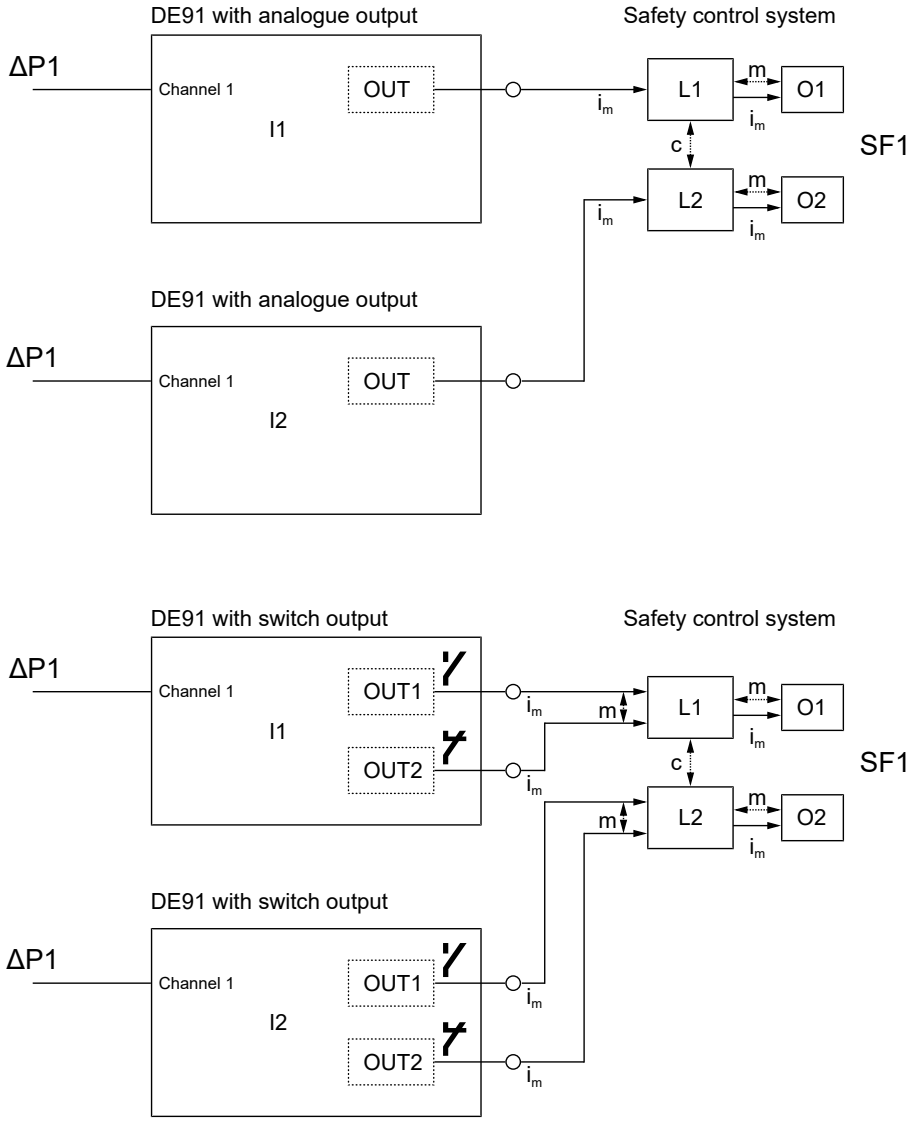
i_m	connecting equipment
c	Cross check
I1, I2	Differential pressure transmitter (DE91)
L1...L4	Logic
m	Monitoring
O1...O4	Output units
OUT1...OUT4	Output (DE91)
SF1, SF2	Safety function 1, Safety function 2

3.4.4.1 Devices with one channel

3.4.4.1.1 Category 1

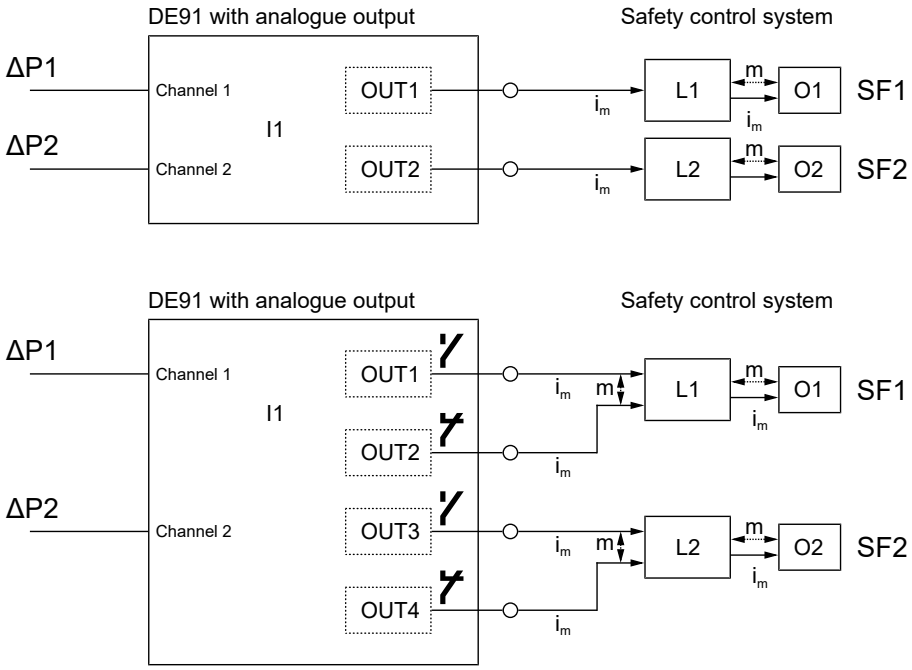


3.4.4.1.2 Category 3

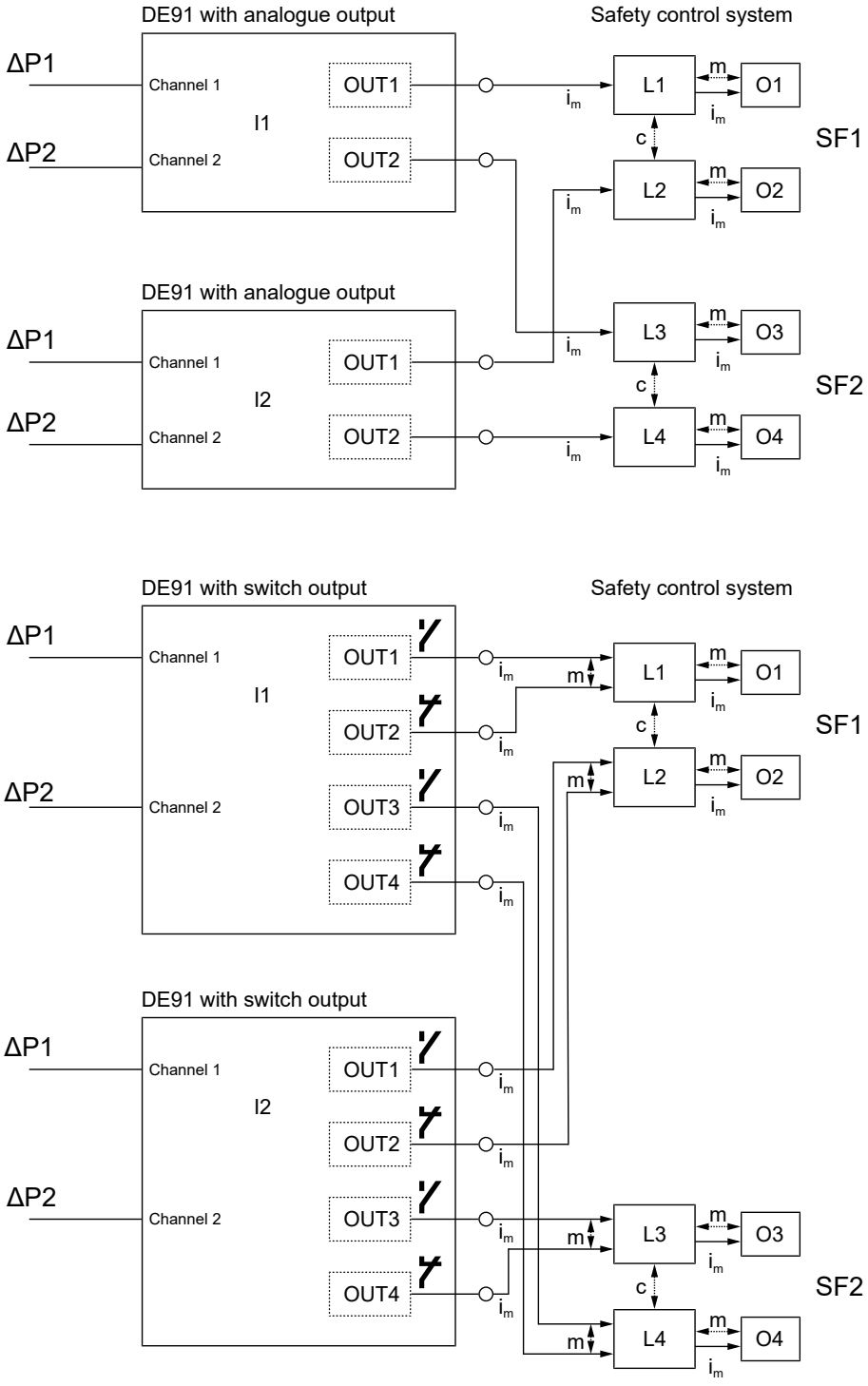


3.4.4.2 Devices with two channels

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 level of the EMC Directive 2014/30/EU.

The operator is responsible for defining the proof test procedure for the entire safety system.

The following functional test must be carried out on the safety-related component DE91.

1. Check the function of the input values within the measuring range.
2. Check the switch points

The test pressure should be generated independently with the safety system (SIS), if this is possible. In this case steps can be taken at the same time to check whether the signals from the overriding safety control system are processed correctly and forwarded via the actuator.

Otherwise, the DE91 must be removed and wired as follows. Please note that some models do not have an analogue output.

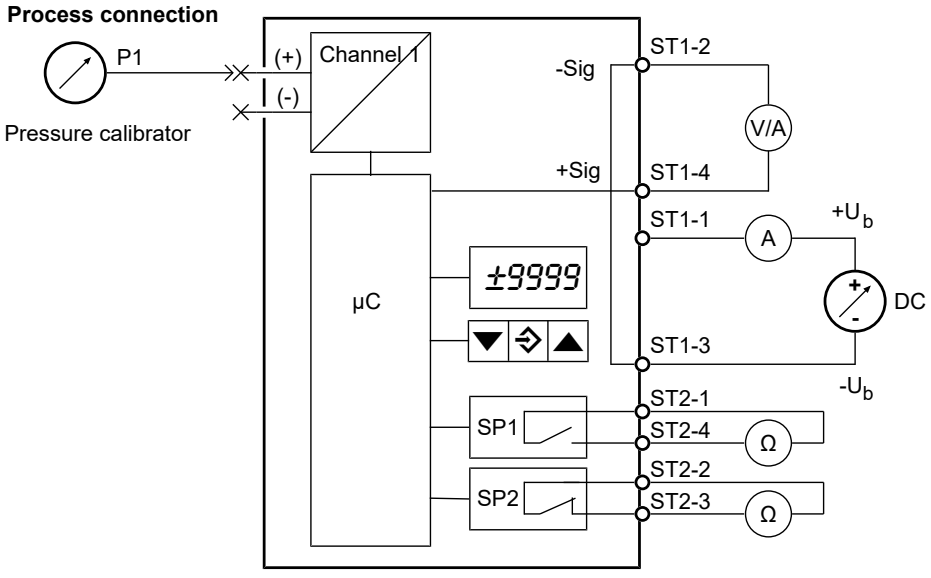


Fig. 2: Function test

4.2.1 Analog output

- Set the operating voltage within the permissible operating voltage range.
- 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 the section
  - Model with current output or
  - Model with voltage output.

Input values within the measuring range

1. Set an input signal with the pressure calibrator that corresponds to the start of the measuring range.
2. Test the output signal with a multimeter.
   - If a voltage signal is used, the value must lie within U_{min} ± ΔU.
   - If the current signal is to be used, the value must lie within 4mA ± ΔI.
3. Set an input signal with the pressure calibrator that corresponds to the end of the measuring range.
4. Test the output signal with a multimeter.
   - If a voltage signal is used, the value must lie within Umax ± ΔU.
   - If the current signal is to be used, the value must lie within 20mA + ΔI.
5. Repeat this step for every measuring channel.

Input values outside the measuring range

1. Set an input signal with the pressure calibrator that lies well below the start of the measuring range.
2. Test the output signal with a multimeter.
   - If a voltage signal is used, the value must lie below Umin - ΔU.
   - If the current signal is to be used, the value must lie below 4mA - ΔI.
3. Set an input signal with the pressure calibrator that lies well above the end of the measuring range.
4. Test the output signal with a multimeter.
   - If a voltage signal is used, the value must lie above Umax + ΔU.
   - If the current signal is to be used, the value must lie within 20mA + ΔI.
5. Repeat this step for every measuring channel.

Check the error signal in the SIS

1. Connect the analogue output of the DE91 electrically to the overriding safety control system.
2. Set an input signal with the pressure calibrator that lies well below the start of the measuring range, so that an error signal is generated.
3. Check whether the incorrect signal is recognised by the safety control system.

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.

Check behaviour of the adjusted switching point.

P_{SP} is the parameterized switching point
ΔMB_{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 specifications do not apply to devices with Modbus or IO-Link. In the case of 2-channel devices, both channels must be fitted with ceramic pressure sensors (Type A).

5.1 Model with analogue output

Safety coefficients		
λ_s	1039.427 Fit	Safe failure rate
λ_d	1108.319 Fit	Dangerous failure rate
λ_{dd}	686.263 Fit	Dangerous detected failure rate
λ_{du}	422.056 Fit	Dangerous undetected failure rate

SIL (IEC 61508)

Dev. type	Type B	Complex device
Operating mode	Low Demand	Requirement max. 1/year

1oo1 architecture

HFT	0	Hardware failure tolerance
SFF	80.35%	Safe failure fraction

The probability of a malfunction in a requirement case (PFD) depends on the test interval.

Inspection intervals	1 year	2 years	5 years	10 years
PFD	$1.86 \cdot 10^{-3}$	$3.71 \cdot 10^{-3}$	$9.25 \cdot 10^{-3}$	$1.85 \cdot 10^{-2}$
IEC 61508	SIL1	SIL1	SIL1	SIL1

1oo2 architecture

β	10%	Probability that the same error occurs at the same time in both channels.
β_d	5%	Probability of the same dangerous fault occurring at the same time in both channels.
MRT	8 hours	Mean repair time
MTTR	8 hours	Mean time to repair
HFT	1	Hardware fault tolerance
SFF	80.35%	Safe failure fraction

The probability of a malfunction in a requirement case (PFD) depends on the test interval.

Inspection intervals	1 year	2 years	5 years	10 years
PFD	$1.89 \cdot 10^{-4}$	$3.86 \cdot 10^{-4}$	$1.02 \cdot 10^{-3}$	$2.24 \cdot 10^{-3}$
IEC 61508	SIL2	SIL2	SIL2	SIL2

PL (DIN EN ISO 13849)

Dev. type	Type B	Complex device	
Operating mode	High Demand	Requirement max. 1/year	
$MTTF_d$	103.0 years	high	Mean time to the dangerous failure
DC	61.92 %	low	Diagnostic coverage factor

Achievable performance level	PL
Category 1	c
Category 3	d

5.2 Model with switch output

Safety coefficients		
λ_s	707.761 Fit	Safe failure rate
λ_d	1348.499 Fit	Dangerous failure rate
λ_{dd}	1034.503 Fit	Dangerous detected failure rate
λ_{du}	313.996 Fit	Dangerous undetected failure rate

SIL (IEC 61508)

Dev. type	Type B	Complex device
Operating mode	Low Demand	Requirement max. 1/year

1oo1 architecture

HFT	0	Hardware failure tolerance
SFF	84.73 %	Safe failure fraction

The probability of a malfunction in a requirement case (PFD) depends on the test interval.

Inspection intervals	1 year	2 years	5 years	10 years
PFD	$1.39 \cdot 10^{-3}$	$2.76 \cdot 10^{-3}$	$6.89 \cdot 10^{-3}$	$1.38 \cdot 10^{-2}$
IEC 61508	SIL1	SIL1	SIL1	SIL1

1oo2 architecture

β	10%	Probability that the same error occurs at the same time in both channels.
β_d	5%	Probability of the same dangerous fault occurring at the same time in both channels.
MRT	8 hours	Mean repair time
MTTR	8 hours	Mean time to repair
HFT	1	Hardware fault tolerance
SFF	84.73 %	Safe failure fraction

The probability of a malfunction in a requirement case (PFD) depends on the test interval.

Inspection intervals	1 year	2 years	5 years	10 years
PFD	$1.40 \cdot 10^{-4}$	$2.85 \cdot 10^{-4}$	$7.44\ 10^{-4}$	$1.60 \cdot 10^{-3}$
IEC61508	SIL2	SIL2	SIL2	SIL2

PL (DIN EN ISO 13849)

Dev. type	Type B	Complex device	
Operating mode	High Demand	Requirement max. 1/year	
$MTTF_d$	84.65 years	high	Mean time to the dangerous failure
DC	76.72 %	low	Diagnostic coverage factor

Achievable performance level	PL
Category 1	c
Category 3	d

6 Attachments

6.1 Manufacturer's declarations SIL/PL

FISCHER MESS- UND REGELTECHNIK

(Translation)

Manufacturer's declaration

The manufacturer

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

Tel.+49 5222 974-0
www.fischermesstechnik.de

hereby declares for the units of the series described below:

Product designation **Differential pressure transmitter**

Type designation **DE91 with analog output**

The device can be used in safety-related systems. According to IEC 61508 or ISO 13849, the correct operation of the safety function must be verified. The required key figures, safety instructions, mounting and maintenance instructions can be found in the safety manual.

λ_s	*1039.427 FIT*
λ_d	*1108.319 FIT*
λ_{dd}	*686.263 FIT*
λ_{du}	*422.056 FIT*

SIL (IEC 61508)			**PL (ISO 13849)**	
Architecture	*1oo1*	*1oo2*	*MTTFd*	*103.0 years*
HFT	*0*	*1*	*DC*	*61.92 %*
SIL	*SIL 1*	*SIL2*	*Achievable performance level*	
SFF	*80.35 %*	*80.35 %*	*Category 1*	*c*
PFD (T1=1 year)	$1.86 * 10^{-3}$	$1.89 * 10^{-4}$	*Category 3*	*d*
PFD (T1=2 years)	$3.71 * 10^{-3}$	$3.86 * 10^{-4}$		
PFD (T1=5 years)	$9.25 * 10^{-3}$	$1.02 * 10^{-3}$		
PFD (T1=10 years)	$1.85 * 10^{-2}$	$2.24 * 10^{-3}$		

Bad Salzuflen
22 July 2026

T. Malischewski
Managing Director

50045 • HE_EN_DE91_SIL-PL_Analog • Rev. ST4-B • 06/26

1 / 1

Fig. 3: HE_DE_DE91_SIL-PL_Analog

FISCHER MESS- UND REGELTECHNIK

(Translation)

Manufacturer's Declaration

The manufacturer

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

Tel.+49 5222 974-0
www.fischermesstechnik.de

hereby declares for the units of the series described below:

Product designation **Differential pressure transmitter**

Type designation **DE91 with switch output**

The device can be used in safety-related systems. According to IEC 61508 or ISO 13849, the correct operation of the safety function must be verified. The required key figures, safety instructions, mounting and maintenance instructions can be found in the safety manual.

λ_s	*707.761 FIT*
λ_d	*1348.499 FIT*
λ_{dd}	*1034.503 FIT*
λ_{du}	*313.996 FIT*

SIL (IEC 61508)			**PL (ISO 13849)**	
Architecture	*1oo1*	*1oo2*	*MTTFd*	*84.65 years*
HFT	*0*	*1*	*DC*	*76.72 %*
SIL	*SIL 1*	*SIL2*	*Achievable performance level*	
SFF	*84,73 %*	*84.73 %*	*Category 1*	*c*
PFD (T1=1 year)	$1.39 * 10^{-3}$	$1.40 * 10^{-4}$	*Category 3*	*d*
PFD (T1=2 years)	$2.76 * 10^{-3}$	$2.85 * 10^{-4}$		
PFD (T1=5 years)	$6.89 * 10^{-3}$	$7.44 * 10^{-4}$		
PFD (T1=10 years)	$1.38 * 10^{-2}$	$1.60 * 10^{-3}$		

Bad Salzuflen
22 July 2026

T. Malischewski
Managing Director

Fig. 4: HE_DE_DE91_SIL-PL_Schalt

6.2 Glossary

Fig. (A Z)	Definition
β	*(en)* **Common Cause Factor** *(de)* Beta-Faktor Proportionality factor between the CCF rate (failure due to a common cause) and the dangerous failure rate of the individual channel.
DC	*(en)* **Diagnostic Coverage Factor** *(de)* Diagnosedeckungsgrad The DC parameter shows the ratio of the number of detected dangerous failures (λ_{DD}) to the total number of dangerous failures (λ_D) an. $DC = \frac{\sum \text{Known dangerous error}}{\sum \text{Total dangerous error}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
FIT	*(en)* **Failure in Time** *(de)* Ausfälle pro Zeit Failure rate with respect to the time interval 10^9 hours. $1\ FIT = 1 \times 10^{-9} \frac{1}{h}$
FMEDA	*(en)* **Failure Mode Effect and Diagnostic Analysis** *(de)* Gefährdung und Risikoanalyse Procedure to determine causes of failures and their impact on the system.
HDM	*(en)* **High Demand Mode** *(de)* Betriebsart mit hoher Anforderungsstufe Operating mode with high or continuous demand on the safety function. The demand rate to the safety system is greater than once annually.
HFT	*(en)* **Hardware Fault Tolerance** *(de)* Hardware-Fehlertoleranz The hardware fault tolerance states how many dangerous failures are possible due to the architecture without endangering the execution of the safety function. • HFT = 0 The occurrence of a dangerous failure will lead to a failure of the safety function. • HFT = 1 Only the occurrence of two dangerous failures will lead to a failure of the safety function.

LDM	*(en)* **Low Demand Mode** *(de)* Betriebsart mit niedriger Anforderungsstufe 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	*(en)* **Architecture with M out of N channels** *(de)* Systemarchitektur mit M aus N Kanälen System architecture MooN with the variables M and N: Classification and description of safety-related systems with regard to redundancy and applied selection procedures. • N - is the total number of redundant channels of a safety-related architecture and/or safety circuit. • M - determines the number of channels that must operate correctly to carry out the safety function.
MTBF	*(en)* **Mean Time Between Failures** *(de)* Mittlere Brauchbarkeitsdauer Mean operating duration between two failures.
$MTTF_d$	*(en)* **Mean Time To Dangerous Failures** *(de)* Mittlere Zeit bis zum gefahrbringenden Ausfall Operating duration up to a dangerous fault.
MRT	*(en)* **Mean Repair Time** *(de)* Mittlere Reparaturdauer Mean time for the repair.
MTTR	*(en)* **Mean Time To Repair** *(de)* Mittlere Instandsetzungszeit Average time between the occurrence of a failure and restoration of the system.
PFD	*(en)* **Probability of Failure on Demand** *(de)* Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall Probability of a dangerous failure on demand of the safety function for an operating mode with a low demand rate.
PFH	*(en)* **Probability of a dangerous Failure per Hour** *(de)* Ausfallwahrscheinlichkeit pro Stunde für die Sicherheitsfunktion Frequency of a dangerous failure of the safety function for an operating mode with a high or continuous demand rate (high demand).

PFS	*(en)* **Probability of Failure Spurious** *(de)* Ausfallwahrscheinlichkeit aufgrund einer nicht beabsichtigten Prozessabschaltung 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.
SC	*(en)* **systematic capability** *(de)* systematische Eignung Measure of confidence (expressed on a scale of SC 1 to SC 4) that an item's systematic safety integrity meets the requirements of the stated SIL for the designated item safety function when the item is specified in accordance with the compliant item safety manual for the item instructions is applied.
SFF	*(en)* **Safe Failure Fraction** *(de)* Anteil der ungefährlichen Ausfälle Resulting from the rate of safe errors plus the diagnosed or detected errors in relation to the system's total failure rate.[(2)]
SIF	*(en)* **Safety Instrumented Function** *(de)* Sicherheitstechnische Funktion 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	*(en)* **Safety Integrity Level** *(de)* Sicherheits-Integritätslevel 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	*(en)* **Safety Instrumented System** *(de)* Sicherheitstechnisches-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	*(en)* **Proof Test Interval** *(de)* Prüfintervall 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.

[(2)] Due to the lack of diagnosis and negligible number of errors in mechanical components, the method can only be used to a limited extent for valves, drives and other mechanical components. It is therefore the responsibility of the end user to ensure an appropriate SFF through suitable diagnostic measures and intrinsically safe construction.

6.3 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.

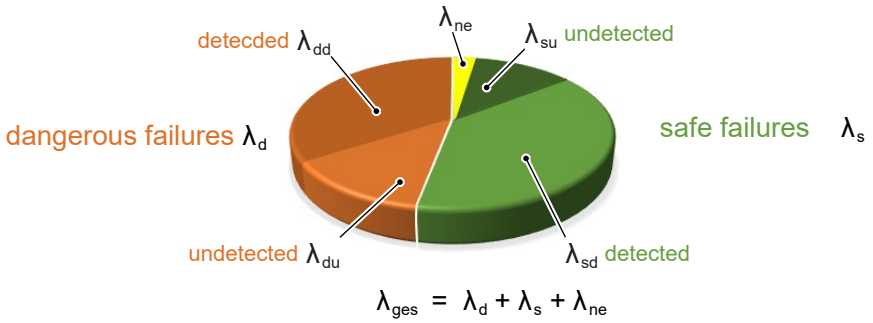


Fig. 5: Failure rates

λ_d	**Dangerous failure rate**
λ_{dd}	**Dangerous detected failure rate**
λ_{du}	**Dangerous undetected failure rate**
λ_s	**Safe failure rate**
λ_{sd}	**Safe detected failure rate**
λ_{su}	**Safe undetected failure rate**
λ_{ne}	**No effect failure rate**

6.4 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

Notes

Notes

FISCHER Mess- und Regeltechnik GmbH
Bielefelder Str. 37a
D-32107 Bad Salzuflen
Tel. +49 5222 974-0
www.fischermesstechnik.de
info@fischermesstechnik.de