developing solutions

FISCHER
MESS- UND REGELTECHNIK

SIL 1
IEC 61508
SIL 2
IEC 61511

RoHS II
COMPLIANT

Safety manual

DE46

Digital differential pressure transmitter
with colour-change LCD

09005975 • SHB_EN_DE46 • Rev. ST4-A • 08/17

Table of contents

1 Functional security (IEC 61508 / IEC 61511) 3
1.1 Scope and standards 3
1.2 Description of the Device and Field of Application 3
1.3 Notes on Planning 4
1.4 Repeat tests 5
1.5 Safety-relevant variables 7
2 Attachments 10
2.1 Glossary 10
2.2 Failure rates 12
2.3 Unit types 12
2.4 Pictogram explanation 13
2.5 Address 13

1 Functional security (IEC 61508 / IEC 61511)

1.1 Scope and standards

NOTICE

Safety instructions

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 Safety Manual applies for the differential pressure transmitter of the series DE46 with the analogue outputs 4…20 mA in 3-conductor circuit. This corresponds to the following product number keys.

- DE46######PN###
- DE46######FN###

The DE46 underwent a function test by an independent institute (Risknowlogy®) to check its functional safety. The safety-specific coefficients were determined using a part analysis (FMEDA) and the following calculations. The results were recorded in the FMEDA Report 930.607.1/2017-07-20.

The transducers have been developed and tested in line with the following standards.

Functional safety (unit-specific/manufacturer)	**IEC 61508: 2010** Functional safety of safety-related electrical/ electronic/programmable electronic systems
Functional security (system-specific/user)	**IEC 61511: 2016** Functional safety - safety systems for the process industry
Part failure rate	**SN 29000: 2013** Failure rates (Siemens)

1.2 Description of the Device and Field of Application

1.2.1 Safety function

The differential pressure transmitter sends the input signal (pressure) to a standardised analogue 4…20 mA output signal. There is one measuring channel available.

⚠ WARNING

Other unit functions

Some models have other functions such as switch outputs or signal outputs (0…20 mA, 0…10 V) that can be activated through configuration. These functions are not part of the safety function and therefore may not be used for safety-relevant purposes.

1.2.2 Definition of a safe state

Output signal I_{out}	Safe state	Comment
4…20 mA	3.92 mA ≤ I_{out} ≤ 20.08 mA	Impressed current

1.2.3 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 unit configuration is protected by a password before delivery. This password is handed over on delivery and must be changed by the operator during commissioning. There is more information about the password in the operating instruction of the respective unit.

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

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

The following transmission errors are possible during remote configuration. Therefore, it is essential to verify all parameters and the safety function on the unit after transfer.

1.3 Notes on Planning

1.3.1 Intended use

The unit underwent a function test by an independent institute (Risknowlogy®) to check its functional safety in compliance with IEC 61508 and IEC 61511. The results were recorded in the FMEDA Report 930.607.1/2017-07-20.

- **IEC 61508**
  The unit is suitable for use in safety circuits with an SIL 1 classification.
- **IEC 61511**
  The unit is suitable for use in safety circuits with an SIL 2 classification (prior use).

1.3.2 Operating 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 variable is the PFD value.

1.3.3 Equipment type

This is a Type B unit (complex operating equipment).

1.3.4 Inspection intervals

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

The following table shows the average probability of a malfunction in case of demand depending on the inspection interval and the system architecture.

		Inspection interval (T_1)			
Architecture		**1 year**	**2 years**	**5 years**	**10 years**
1oo1	**PFD_{avg}**	8.7×10^{-4}	1.74×10^{-3}	4.35×10^{-3}	8.7×10^{-3}
1oo2	**PFD_{avg}**	4.4×10^{-5}	9.05×10^{-5}	2.4×10^{-4}	5.2×10^{-4}

1.3.5 Lifetime

The lifetime starting from the production date is 10 years.

[(1)] Please see the information in the operating instructions.

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.

1.3.6 Assembly and installation

Pay attention to the assembly instructions in the operating instructions.

1.4 Repeat tests

1.4.1 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.

1.4.2 Function test

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

The following function test must be carried out on the safety component DE46.

1. Check the function of the input values within the measuring range.
2. Check the error signal for input values outside the measuring range.
3. Check that the error signal is recognised correctly by the overriding safety control system.

The test pressure should be generated independently with the safety system (SIS), if this is possible. In this case steps could 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 DE46 needs to be removed and wired to a pressure calibrator, ammeter and a settable power supply as follows.

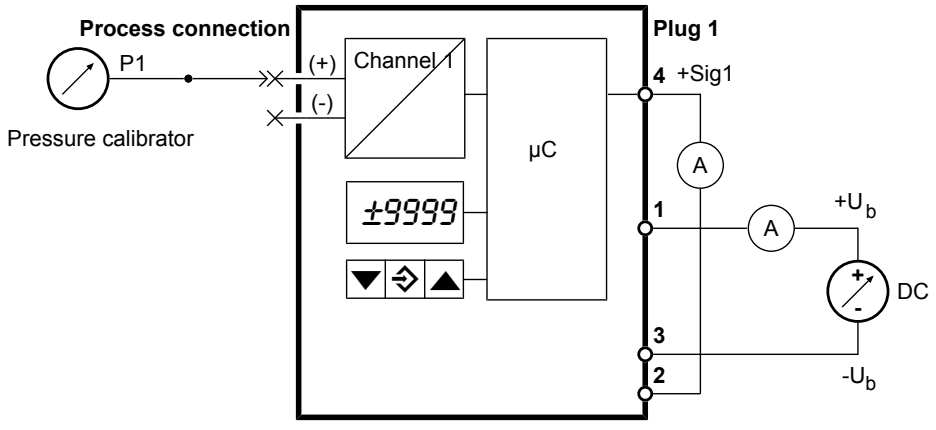

Fig. 1: Function test

Test equipment list

Test equipment	Usage	resolution
Pressure calibrator (±1 bar)	Input signal	0.1% of final value
Multimeter	Absorbed current	1 mA

Test equipment	Usage	resolution
Multimeter	Output signal	1 µA
Power supply	Can be set between 12 ... 32 V DC	0.1V

Input values within the measuring range

1. Set an operating voltage of 24V ± 0.1V.
2. Use the pressure calibrator to set an input signal that corresponds to the start of the measuring range.
3. Check the output signal. The output must deliver a signal of 4 mA ±0.08 mA.
4. Use the pressure calibrator to set an input signal that corresponds to the end of the measuring range.
5. Check the output signal. The output must deliver a signal of 20 mA ±0.08 mA.
6. Check the absorbed current The absorbed current may not exceed a value of 145 mA.

Input values outside the measuring range

1. Use the pressure calibrator to set an input signal that lies well below the start of the measuring range.
2. Check the output signal. The output must deliver a signal of less than 3.92 mA.
3. Use the pressure calibrator to set an input signal that lies well above the start of the measuring range.
4. Check the output signal. The output must deliver a signal in excess of 20.08 mA.

Check the error signal in the SIS

1. Wire the DE46 to the overriding safety controls system.
2. Use the pressure calibrator to set an input signal that lies well below the start of the measuring range so that an error signal is generated.
3. Check that the error signal is recognised correctly by the safety control system.

This marks the end of the function test. If the unit does not pass the function test, please send it to our repair department.

1.4.3 Repair work

Only the manufacturer may repair units.

All defective or faulty devices should be sent directly to our repair department. Please coordinate all shipments with our sales department.

⚠ WARNING

Process media residues

Process media residues in and on dismantled devices can be a hazard to people, animals and the environment. Take adequate preventive measures. If required, the devices must be cleaned thoroughly.

Return the device in the original packaging or a suitable transport container.

1.5 Safety-relevant variables

1.5.1 Safety coefficients

Percentage of non-dangerous faults	**SFF**	63 %
Equipment type		Type B

Failure rates		FIT
Non-dangerous faults	λ_s	195
Detectable safe faults	λ_{sd}	0
Non-detectable safe faults	λ_{su}	195
Dangerous faults	λ_d	334
Detectable dangerous faults	λ_{dd}	136
Non-detectable dangerous faults	λ_{du}	198

Safety integrity level according to IEC 61508

	SIL 1	SIL 2
Required units	1	2
System architecture:	1oo1	1oo2
Hardware Failure Tolerance HFT:	0	1

Safety integrity level according to IEC 61511

	SIL 2
Required units	1
System architecture:	1oo1
Hardware Failure Tolerance HFT:	0

Inspection intervals

		Inspection interval (T_1)			
Architecture		**1 year**	**2 years**	**5 years**	**10 years**
1oo1	**PFD_{avg}**	8.7×10^{-4}	1.74×10^{-3}	4.35×10^{-3}	8.7×10^{-3}
1oo2	**PFD_{avg}**	4.4×10^{-5}	9.05×10^{-5}	2.4×10^{-4}	5.2×10^{-4}

1.5.2 Safety integrity level (SIL)

The following table shows the probability of a dangerous failure of the safety function depending on the SIL level and the operating mode.

Low Demand Mode

SIL	PFD	Max. 1 dangerous failure per
SIL4	$\geq 10^{-5}$ to $< 10^{-4}$	10000 demands
SIL3	$\geq 10^{-4}$ to $< 10^{-3}$	1000 demands
SIL2	$\geq 10^{-3}$ to $< 10^{-2}$	100 demands
SIL1	$\geq 10^{-2}$ to $< 10^{-1}$	10 demands

High Demand Mode

SIL	PFH	Max. 1 dangerous failure per
SIL4	$\geq 10^{-9}$ to $< 10^{-8}$	100,000,000 demands
SIL3	$\geq 10^{-8}$ to $< 10^{-7}$	10,000,000 demands
SIL2	$\geq 10^{-7}$ to $< 10^{-6}$	1,000,000 demands
SIL1	$\geq 10^{-6}$ to $< 10^{-5}$	100,000 demands

The SIL Level for the entire safety system (SIS) is the sum of the PFD values for the individual components. The following picture is that of a system of this kind comprising a sensor, safety control system and an actuator.

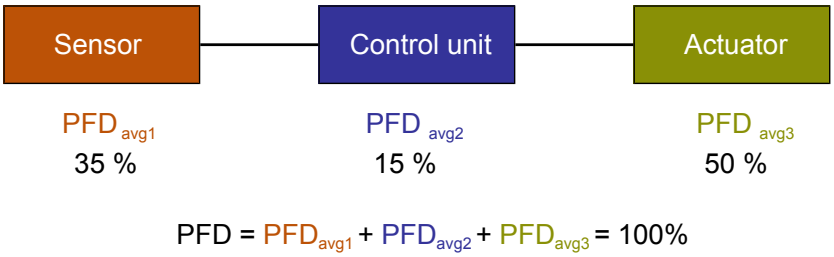

Fig. 2: PFD division

1.5.3 Architectural limitations (SFF, HFT)

The following table shows the maximum level of safety integrity that can be reached; this is the sum of SFF and HFT depending on the unit type of the components used. The SFF is calculated according to IEC 61508.

Type A – simple operating equipment

Safe Failure Fraction	HFT (Hardware Failure Tolerance)		
SFF	**0**	**1**	**2**
< 60 %	SIL 1	SIL 2	SIL 3
60 % … < 90 %	SIL 2	SIL 3	SIL 4
90 % to < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Type B – complex operating equipment

Safe Failure Fraction	HFT (Hardware Failure Tolerance)		
SFF	**0**	**1**	**2**
< 60 %	not allowed	SIL 1	SIL 2
60 % … < 90 %	SIL 1	SIL 2	SIL 3
90 % to < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

2 Attachments

2.1 Glossary

Fig. (↓A Z)	Definition
DC	**Diagnostic Coverage Factor** 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. $DC = \frac{\sum \text{erkannter gefährlicher Fehler}}{\sum \text{gesamter gefährlicher Fehler}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
FIT	**Failure in Time** Failure rate with respect to the time interval 10^9 hours. $1\ FIT = 1 \times 10^{-9} \frac{1}{h}$
FMEDA	**Failure Mode Effect and Diagnostic Analysis** Procedure to determine causes of failures and their impact on the system
HDM	**High Demand Mode** Operating mode with high or continuous demand on the safety function. The demand rate to the safety system is greater than once a year or greater than twice the frequency of the repeat test.
HFT	**Hardware Fault Tolerance** 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	**Low Demand Mode** The safety function will only be carried out on demand to bring the system into a defined safe state. The demand rate is less than once a year and less than twice the frequency of the repeat test.
MooN	**Architecture with M out of N channels** 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	**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**
	Average 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 the result of the rate of safe failures plus the diagnosed and/ore detected failures as a ratio to the total system failure rate.
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.

2.2 Failure rates

The error rates differ in principle as follows:

- Safe failures
- Dangerous failures

These failure types are then further divided into detectable and undetectable failures.

The safe failures, be they detectable or undetectable, do not impact on the safety function. In contracts, dangerous failures put the system into a dangerous state. The following diagram provides and overview.

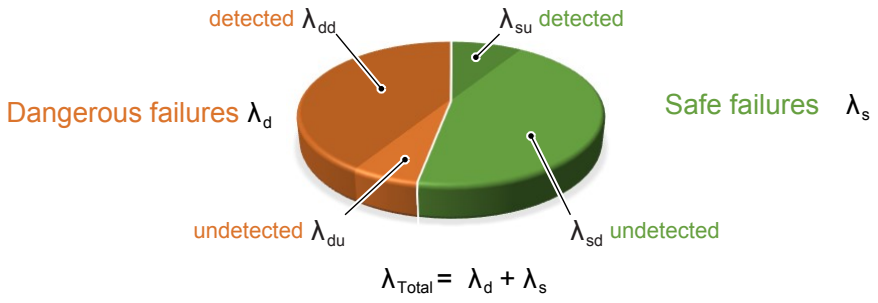

Fig. 3: Failure rates

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**

2.3 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.

2.4 Pictogram explanation

⚠ DANGER

Type and source of danger

This indicates a **direct** dangerous situation that could lead to death or **serious injury** (highest danger level).

a) Avoid danger by observing the valid safety regulations.

⚠ WARNING

Type and source of danger

This indicates a **potentially** dangerous situation that could lead to death or **serious injury** (medium danger level).

a) Avoid danger by observing the valid safety regulations.

⚠ CAUTION

Type and source of danger

This indicates a **potentially** dangerous situation that could lead to slight or serious injury, damage or **environmental pollution** (low danger level).

a) Avoid danger by observing the valid safety regulations.

NOTICE

Note / advice

This indicates useful information of advice for efficient and smooth operation.

2.5 Address

FISCHER Mess- und Regeltechnik GmbH
Bielefelder Str. 37a
D-32107 Bad Salzuflen
Tel. +49 5222-974-0
Fax. +49 5222-7170

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