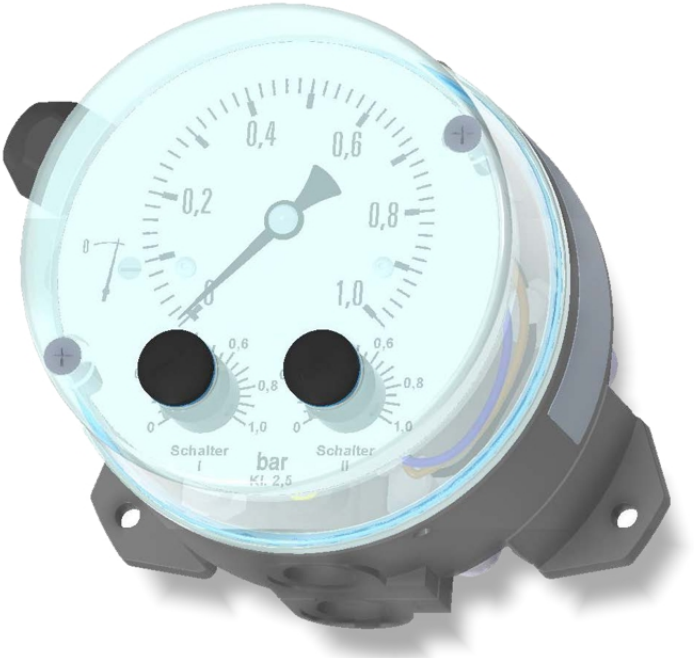
developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL



Safety manual

DS11

Differential pressure measuring and switching device

09015243 • SHB_EN_DS11 • Rev. ST4-D • 09/25

Table of Contents

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.

The safety manual applies to all versions of the differential pressure measuring and switching device DS11.

The DS11 was tested by TÜV NORD CERT GmbH, Prüflabor Produktsicherheit according to the following standard and a certificate with the number 44 7999 13759902 was issued.

IEC 61508: 2010
Functional safety of safety related electrical / electronic / programmable electronic systems

Parts 1 to 7

2 Device description and field of application

2.1 Design and mode of operation

A sturdy non-sensitive diaphragm measuring unit that is suitable for measuring differential pressure, and over and under-pressure is used as a measuring system. The unit uses the same measuring principle for all three measuring applications.

In the rest position, the spring forces on both sides of the membrane are balanced out. Due to the pressure or under-pressure to be measured, a single-sided force is created on the membrane which shifts the membrane system against the measurement range springs up to compensation of the spring forces. In case of overload, the membrane supports against the metallic support surfaces.

A centrally positioned tappet transfers the movement of the membrane system on the motion train and operating elements of the micro-switches.

2.2 Function diagram

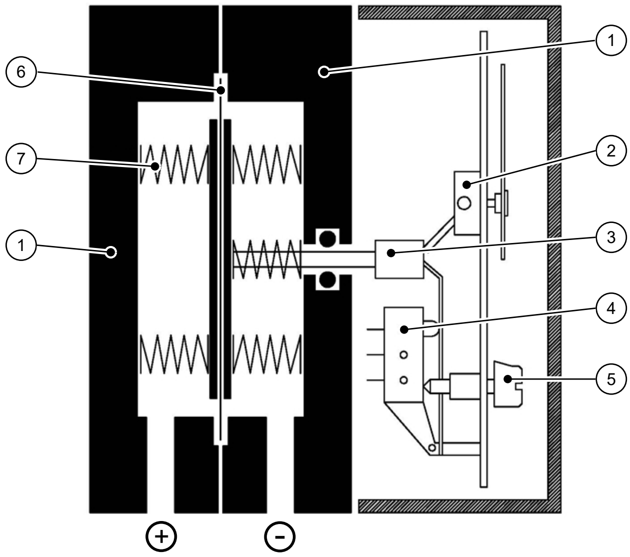


Fig. 1: Function diagram

1	Pressure chamber	**2**	Motion train
3	Tappet	**4**	Micro-switch
5	Switch point setting	**6**	Measuring diaphragm
7	Measuring springs		

2.3 Safe state

The safe function of the contact pressure gauge is the function of the two switching contacts and the display within the tolerance range specified in the data sheet.

3 Notes on Planning

3.1 Intended use

The DS11 has been tested by TÜV NORD CERT GmbH on the basis of 'operationally proven components' in accordance with EN61508 Part 2 Section 7.4.7.6 to 7.4.7.9. The devices can be used with a suitable test (proof test) in SIL2 applications.

NOTICE

SIL2 is achieved with one contact.

3.2 Operating mode

High Demand Mode

3.3 Equipment type

The device is Type A (simple operating equipment).

3.4 Inspection intervals

Conduct a proof test after commissioning and then after 1 year at the latest.

3.5 Lifetime

The DS11 has a service life of 15 years with a maximum limit of 250,000 switching cycles.

3.6 Assembly and installation

Pay attention to the assembly instructions in the operating instructions.

The safety parameters were determined using a Failure Mode and Effects Analysis (FMEA). They apply under the condition that the output signals monitored and evaluated by a safety control system.

NOTICE

SIL2 application

SIL2 is already achieved by using one changeover contact. The second contact can be used for another function.

The following key applies to the architecture diagrams:

Key

i_m	Connecting devices
c	Cross comparison
S	Changeover contact
L1, L2	Logic
m	Monitoring
O1, O2	Output units
SF	Safety function

3.6.1 Architecture 1oo1 (HFT=0)

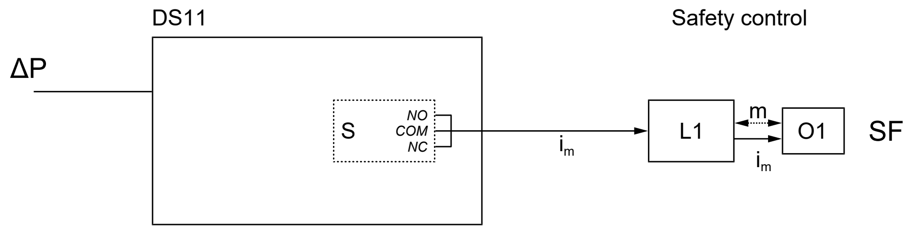


Fig. 2: Architecture 1oo1

3.6.2 Architecture 1oo2 (HFT=1)

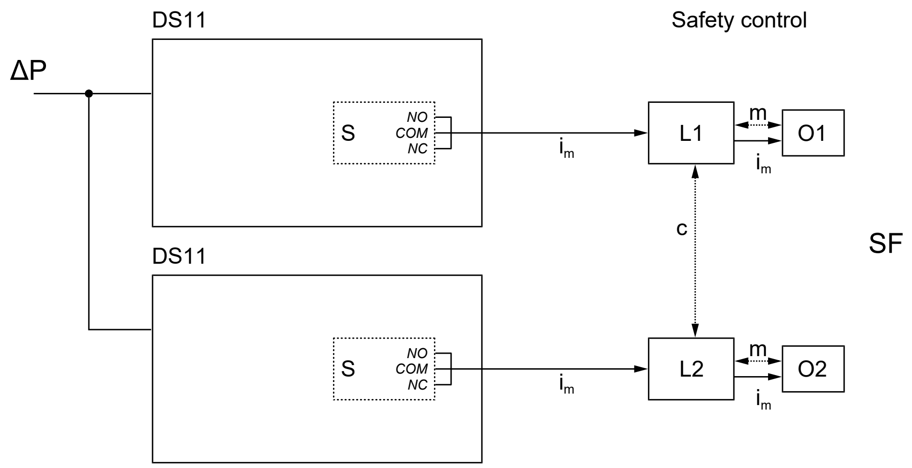


Fig. 3: Architecture 1oo2

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

NOTICE

Display value

According to DIN 837, light tapping on the device is permitted for 'setting' the display value.

The following functions must be checked for the DS11:

1. Testing of the switching points in depressurized condition
2. Testing the switching points by changing the operating pressure.

If possible, the functional test should be carried out with the Safety Engineering System (SIS). Otherwise, the DS11 must be removed and connected to a pressure calibrator. If the specified limit values are exceeded, the device concerned must not be put back into operation and must be replaced by a new device.

Test circuit

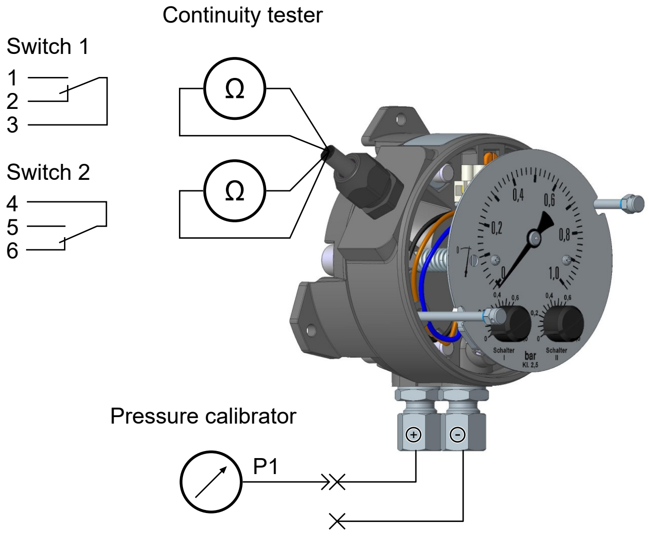


Fig. 4: Functional test

Test sequence

- Open the unit by removing either the hood or the bayonet ring of the front cover (depending on the model).
- Testing in unpressurized condition
  - Turn the switch 1 in direction zero until the micro switch switches. Check the state of the switching output with a continuity tester.
  - Turn the switch 2 in direction zero until the microswitch switches. Check the state of the switching output with a continuity tester.
- Testing of the measuring accuracy (±2.5% of the measuring range end value)
  - Set a differential pressure on the pressure calibrator that corresponds to the lower range value. Check the displayed value.
  - Set a differential pressure on the pressure calibrator that corresponds to the end of the measuring range. Check the displayed value.
  - Set a differential pressure on the pressure calibrator that corresponds to the middle of the measuring range. Check the displayed value.
- Test by changing the working pressure
  - Set the switching points with the switches 1 and 2.
  - Now increase the differential pressure with the pressure calibrator until the first switching point is reached and check the state of the switching output with a continuity tester. Note the pressure value at which the first switch switches.
  - Now increase the differential pressure with the pressure calibrator until the second switching point is reached and check the state of the switching output with a continuity tester. Note the pressure value at which the second switch switches.
  - Now reduce the differential pressure and determine the pressure values at which the switches drop out. Note the values and determine the hysteresis of the switching points. This must not exceed the limit value of 2.5% of the measuring range end value.
- Close the device.

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.

5 Safety-relevant variables

The units can be used in SIL2 applications with suitable testing. SIL2 is achieved with one contact.

Safe Failure Fraction	**SFF**	70 %
Probability of dangerous Failure per Hour	**PFH**	$3{,}3 * 10^{-11}$ 1/h
Hardware Fault Tolerance	**HFT**	0
Type of device		Type A subsystem
Test interval	$\mathbf{T_1}$	1 year

Use in Low Demand Mode

In accordance with the EN 61508 standard, the PFD value can be determined as follows. The calculated value applies to a single unit.

$$\lambda_{du} = PFH$$
$$T_1 = 1\ year = 365 * 24\ h$$

$$\begin{aligned} \text{PFD} &= \lambda_{du} * \frac{T_1}{2} \\ &= 33 * 10^{-11} \left[\frac{1}{h}\right] * \frac{365 * 24\ [\ h\ ]}{2} \\ &= 1{,}45 * 10^{-7} \end{aligned}$$

Fig. 5: Calculation of the PFD value

6 Attachments

6.1 SIL certificate

TÜVNORD

ZERTIFIKAT
CERTIFICATE

Hiermit wird bescheinigt, dass das unten beschriebene Produkt der Firma
This certifies that the product mentioned below from company

Fischer Mess- und Regeltechnik
Bielefelder Straße 37a
32107 Bad Salzuflen
Deutschland

die Anforderungen der folgenden Prüfunterlage(n) erfüllt.
fulfills the requirements of the following test regulations.

Geprüft nach: *Tested in accordance with:*	**EN 61508:2010 Teile/Parts 1-7**
Zertifizierungsprogramm: *Certification program:*	**P14.1VA001**
Beschreibung des Produktes: (Details s. Anlage 1) *Description of product:* *(Details see Annex 1)*	**Differenzdruck Mess- und Schaltgerät** / *Differental Presure Switch* **Kontaktmanometer** / *Contact Pressure Gauge*
Typenbezeichnung: *Type Designation:*	**DS11, DS13 und DS21** **MS11**
Bemerkungen: *Remarks:*	**Die Geräte können mit einer geeigneten Testung in SIL2 Anwendungen eingesetzt werden.** *The components can be used with an appropriate testing in SIL2 applications.*

Dieses Zertifikat bescheinigt das Ergebnis der Prüfung an dem vorgestellten Prüfgegenstand. Eine allgemein gültige Aussage über die Qualität der Produkte aus der laufenden Fertigung kann hieraus nicht abgeleitet werden.

Registrier-Nr. / *Registered No.* 44 799 13759902
Prüfbericht Nr. / *Test Report No.* 35392078
Aktenzeichen / *File reference* 8003081893

Gültigkeit / Validity
von / *from* 2025-03-24
bis / *until* 2030-03-23

F. Hegenfeld
Zertifizierungsstelle der
TÜV NORD CERT GmbH

Essen, 2025-03-24

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de machinery@tuev-nord.de

Bitte beachten Sie auch die umseitigen Hinweise
Please also pay attention to the information stated overleaf

Fig. 6: 4479913759902_SIL_2030-03-23_page_1

TÜVNORD

ANLAGE
ANNEX

Anlage 1, Seite 1 von 1
Annex 1, page 1 of 1

zum Zertifikat Registrier-Nr. / *to Certificate Registration No.* 44 799 13759902

Produktbeschreibung: *Product description:*	**Differnzdruck Mess- und Schaltgerät /** *Differental Presure Switch* **Kontaktmonometer** / *Contact Pressure Gauge*
Typenbezeichnung: *Type designation:*	**DS11, DS13 und DS21** **MS11**
Technische Daten: *Technical data:*	**Sicherheitsparameter** / *Safety Parameter* SFF = 70% PFH = 3,3 10^{-11} 1/h HFT = 0 Typ-A-Teilkomponente / *Type*

F. Hegenfeld
Zertifizierungsstelle der
TÜV NORD CERT GmbH

Essen, 2025-03-24

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de machinery@tuev-nord.de

Fig. 7: 4479913759902_SIL_2030-03-23_page_2

6.2 Glossary

Fig. ($\downarrow^{A}_{Z}$)	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. $1\ \text{FIT} = 1 \times 10^{-9}\ \frac{1}{h}$
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.[1]
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.

[1] 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.

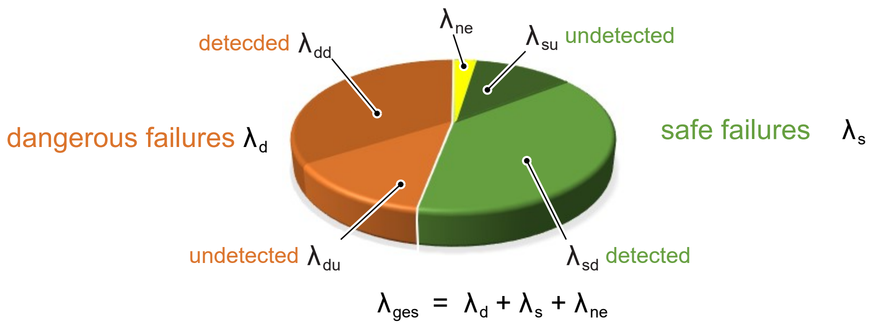


Fig. 8: Failure rates

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.

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