developing solutions

IEC 61508
SIL

RoHS III COMPLIANT

Safety manual

DS21

Differential pressure measuring and switching device

09005985 • SHB_EN_DS21 • Rev. ST4-E • 04/21

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 models of the differential pressure measuring and switching device DS21.

The DS21 was tested by TÜV NORD CERT GmbH in its test laboratory for product safety in line with the following norm, 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 Description of the Device and Field of Application

2.1 Design and mode of operation

The measuring principle of the DS21 is based on two pressure chambers separated by a membrane that are operated at different pressures. On both sides of the membrane there are measuring springs whose spring forces are equalised when in the idle position. Due to the pressure that is to be measured or the differential pressure, force is exerted on one side of the membrane and this moves the membrane system against the measuring range springs until the spring forces are compensated. 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

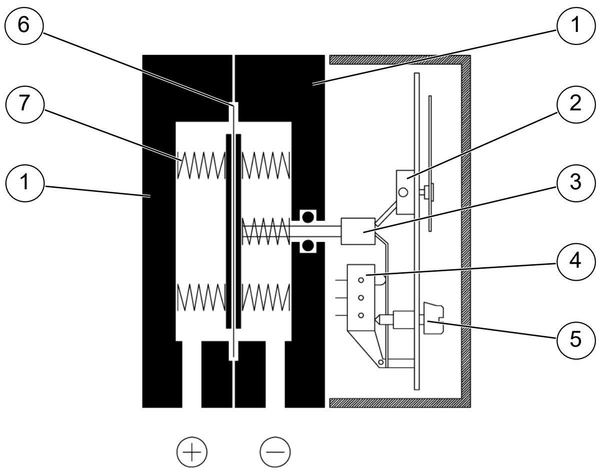

Fig. 1: DS21 Function diagram [Standard]

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 differential pressure measuring and switching device is the responsibility of the two switching contacts and the display within the tolerance range stated in the data sheet.

3 Notes on Planning

3.1 Intended use

The DS21 has been tested by TÜV NORD CERT GmbH on the basis of 'proven component' in accordance with EN61508 Part 2 Sections 7.4.7.6 to 7.4.7.9. The devices can be used in SIL2 applications with suitable testing (proof test).

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 DS21 has a service life of 15 years and is limited to maximum 250 000 switching cycles.

3.6 Assembly and installation

Pay attention to the assembly instructions in the operating instructions.

The safety indicators were determined on the basis of FMEAs. These apply under the condition that the output signals are monitored and evaluated by a downstream 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 legend applies to the connection 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)

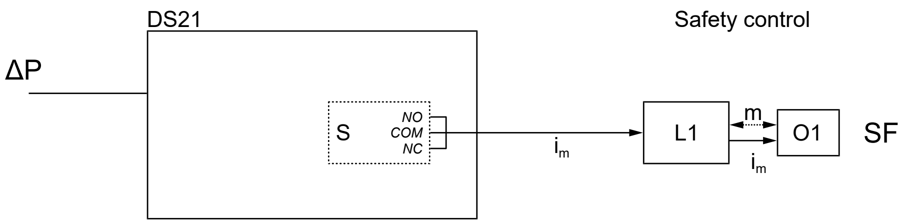

Fig. 2: Architecture 1oo1

3.6.2 Architecture 1oo2 (HFT=1)

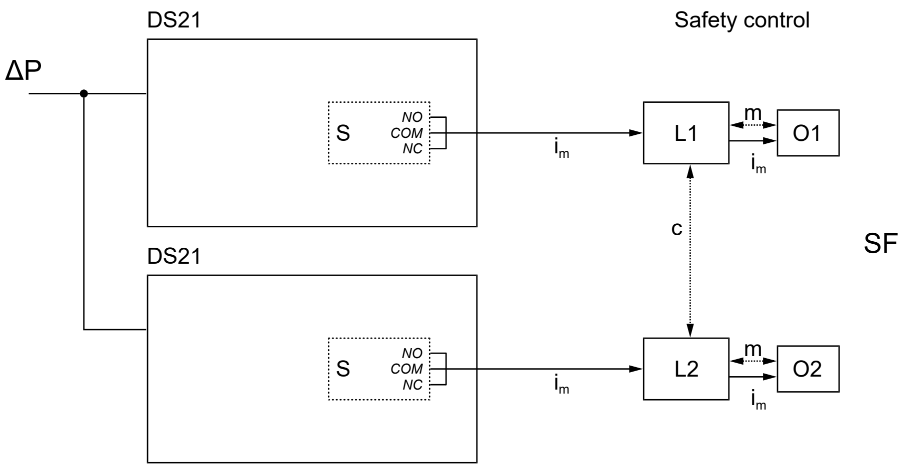

Fig. 3: Architecture 1oo2

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

Acc. to DIN 837 it is permitted to slightly tap the device to 'set' the display value.

The following functions must be tested for the DS21:

1. Checking the switch points in a depressurized state
2. Checking the switch points by changing the operational pressure.

The function test should be carried out with the safety system (SIS), if this is possible. Otherwise, the DE21 needs to be removed and wired with a pressure calibrator. If the stated limits are exceeded, the affected device may not be used again and needs to be replaced with a new device.

Test switching

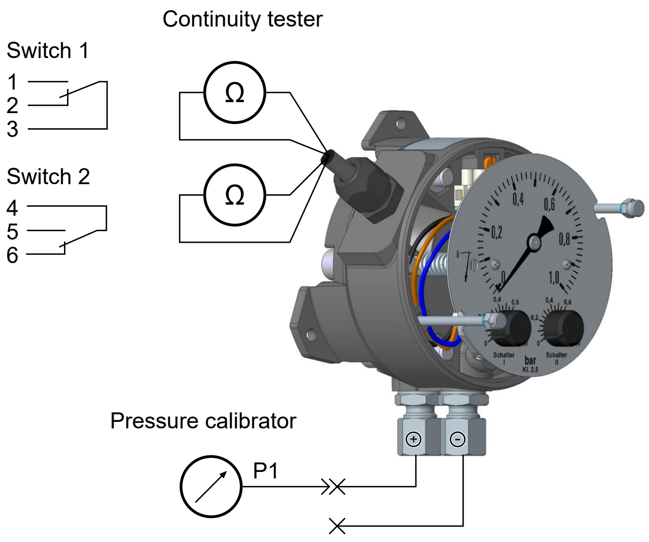

Fig. 4: Function test

Test sequence

- (Depending on the model) open the unit either by removing the hood or the bayonet ring of the front disk.
- Checking in a depressurized state
  - Turn the switch 1 toward the zero-point until the micro-switch is activated. Check the state of the switching output with a continuity tester.
  - Turn the switch 2 toward the zero-point until the micro-switch is activated. Check the state of the switching output with a continuity tester.
- Check the measuring accuracy (± 2.5% of the end range value)
  - Use the pressure calibrator to set a differential pressure that corresponds to the start of the measuring range. Check the display value.
  - Use the pressure calibrator to set a differential pressure that corresponds to the end of the measuring range. Check the display value.
  - Use the pressure calibrator to set a differential pressure that corresponds to the middle of the measuring range. Check the display value.
- Checking by changing the operational pressure
  - Set the switch points using the switches 1 and 2.
  - Now increase the differential pressure with the pressure calibrator until the first switch point has been reached, and then check the state of the switch output with a continuity tester. Note the pressure value at which the first switch activates.
  - Now increase the differential pressure with the pressure calibrator until the second switch point has been reached, and then check the state of the switch output with a continuity tester. Note the pressure value at which the second switch activates.
  - Now reduce the differential pressure and establish the pressure values at which the switches drop. Note the values and determine the hysteresis of the switching points. This may not undercut the limit value of 2.5% of the measuring range end value.
- Close the unit.

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	**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.

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

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

Fig. 5: Calculation of the PFD value

6 Attachments

6.1 SIL certificate

TÜV NORD

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**
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**

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.
This certifies the result of the examination of the product sample submitted by the manufacturer. A general statement concerning the quality of the products from the series manufacture cannot be derived there from.

Registrier-Nr. / *Registered No.* 44 799 13759902
Prüfbericht Nr. / *Test Report No.* 3526 2583
Aktenzeichen / *File reference* 8003015248

Gültigkeit / Validity
von / *from* 2020-03-18
bis / *until* 2025-03-17

F. Hegenfeld

Zertifizierungsstelle der
TÜV NORD CERT GmbH

Essen, 2020-03-18

TÜV NORD CERT GmbH Langemarckstraße 20 45141 Essen www.tuev-nord-cert.de technology@tuev-nord.de

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

Fig. 6: SIL_4479913759902

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

Allgemeine Angaben *General Information*	**Siehe auch Seite 1 des Zertifikats** *See also page 1 of the certificate*
Produktbeschreibung: *Product description:*	**Differenzdruck Mess- und Schaltgerät /** *Differental Presure Switch* **DS11, DS13, DS21** **Kontaktmanometer** / Contact Pressure Gauge MS11
Technische Daten: *Technical data:*	**Sicherheitsparameter /** *Safety Parameter* SFF = 70 % PFH = 3,3 10^{-11} 1/h HFT = 0 Typ-A-Teilkomponente / *Type*

Die Geräte können mit einer geeigneten Testung in SIL2 Anwendungen eingesetzt werden.
The components can be used with an appropriate testing in SIL2 applications.

Zertifizierungsstelle der
TÜV NORD CERT GmbH

Essen, 2020-03-18

TÜV NORD CERT GmbH Langemarckstraße 20 45141 Essen www.tuev-nord-cert.de technology@tuev-nord.de

Fig. 7: SIL_4479913759902

6.2 Glossary

Fig. (↓A Z)	Definition
β	**Common Cause Factor** 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** 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. $DC = \frac{\sum \text{dangerous detected failure}}{\sum \text{dangerous failure}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
FIT	**Failure in Time** Failure rate with respect to the time interval 10^9 hours. $1\ \text{FIT} = 1 \times 10^{-9}\ \frac{1}{h}$
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 annually.
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 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:

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**

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.

6.3 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.

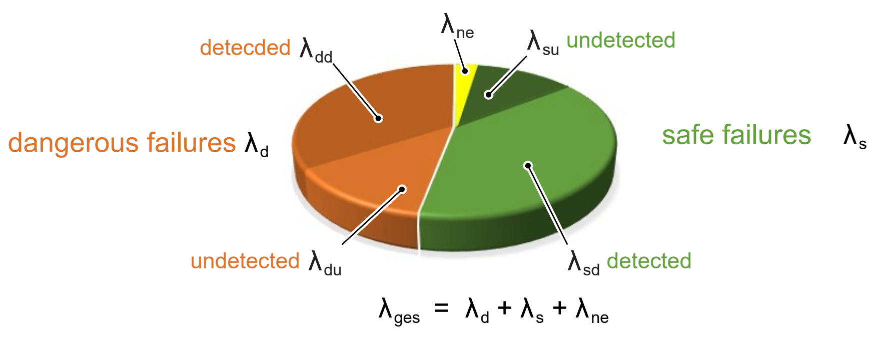

Fig. 8: Failure rates

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.

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