Safety Manual

DPT-20

GB

Two-wire 4 … 20 mA/HART
With SIL qualification

Part of your business

Contents

Editing status: 2020-10-20

1 Document language

DE	Das vorliegende *Safety Manual* für Funktionale Sicherheit ist verfügbar in den Sprachen Deutsch, Englisch, Französisch und Russisch.
EN	The current *Safety Manual* for Functional Safety is available in German, English, French and Russian language.
FR	Le présent *Safety Manual* de sécurité fonctionnelle est disponible dans les langues suivantes: allemand, anglais, français et russe.
RU	Данное руководство по функциональной безопасности *Safety Manual* имеется на немецком, английском, французском и русском языках.

2 Scope

2.1 Instrument version

This safety manual applies to differential pressure transmitters

DPT-20

DPT-20 with diaphragm seal DSS1 or DSS2 [1)]

Electronics types:

- Two-wire 4 … 20 mA/HART with SIL qualification
- Two-wire 4 … 20 mA/HART with SIL qualification and supplementary electronics "Additional current output 4 … 20 mA"

Valid versions:

- from HW Ver 1.0.0
- from SW Ver 1.2.2

2.2 Application area

The differential pressure transmitter can be used in a safety-related system according to IEC 61508 in the modes *low demand mode* or *high demand mode* for the measurement of the following process variables:

- Differential pressure measurement
- Hydrostatic level
- Flow measurement
- Density measurement
- Interface measurement

Due to the systematic capability SC3 this is possible up to:

- SIL2 in single-channel architecture
- SIL3 in multiple channel architecture

The following interface can be used to output the measured value:

- Current output: 4 … 20 mA

SIL The following interfaces are only permitted for parameter adjustment and for informative use:

- HART
- Display and adjustment module (also via Bluetooth)
- USB Communicator (auch via Bluetooth)
- Current output II [2)]

2.3 SIL conformity

The SIL confirmity was judged and certified independently by *TÜV Rheinland* according to IEC 61508:2010 (Ed.2) (verification documents see " *Supplement*").

[1)] DSS1 = Diaphragm Seal Single side, DSS2 = Diaphragm Seal Both sides

[2)] Only with instrument version with supplementary electronics "Additional current output 4 … 20 mA".

SIL The certificate is valid for the entire service life of all instruments that were sold before the certificate expired!

3 Planning

3.1 Safety function

Safety function

The transmitter generates on its current output a signal between 3.8 mA and 20.5 mA corresponding to the process variable. This analogue signal is fed to a connected processing system to monitor the following conditions:

- Exceeding a defined limit value of the process variable
- Falling below a defined limit value of the process variable
- Monitoring of a defined range of the process variable

Safety tolerance

For the design of the safety function, the following aspects must be taken into account with regard to the tolerances:

- Due to undetected failures in the range between 3.8 mA and 20.5 mA, an incorrect output signal can be generated which deviates from the real measured value by up to 4 %
- Due to the special application conditions, increased measurement deviations can be caused (see Technical data in the operating instructions)

3.2 Safe state

Safe state

The safe state of the current output depends on the safety function and the characteristics set on the sensor.

Characteristics	Monitoring upper limit value	Monitoring lower limit value
4 … 20 mA	Output current ≥ Switching point	Output current ≤ Switching point
20 … 4 mA	Output current ≤ Switching point	Output current ≥ Switching point

Fault signals in case of malfunction

Possible fault currents:

- ≤ 3.6 mA ("fail low")
- > 21 mA ("fail high")

3.3 Prerequisites for operation

Instructions and restrictions

- The measuring system should be used appropriately taking pressure, temperature, density and chemical properties of the medium into account. The application-specific limits must be observed.
- The specifications according to the operating instructions manual, particularly the current load on the output circuits, must be kept within the specified limits
- Existing communication interfaces (e. g. HART, USB) are not used for transmission of the safety-relevant measured value
- The instructions in chapter "*Safety-related characteristics*", paragraph "*Supplementary information*" must be noted
- All parts of the measuring chain must correspond to the planned "*Safety Integrity Level (SIL)*"

4 Safety-related characteristics

4.1 Characteristics acc. to IEC 61508

General information

Parameter	Value
Safety Integrity Level	SIL2 in single-channel architecture SIL3 in multiple channel architecture [3]
Hardware fault tolerance	HFT = 0
Instrument type	Type B
Mode	Low demand mode, High demand mode
SFF	> 90 %
MTBF [4]	0.31 x 10^6 h (35 years)
Diagnostic test interval [5]	< 30 min

DPT-20

Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{H}	λ_{L}	λ_{AD}
0 FIT	0 FIT	2412 FIT	47 FIT	9 FIT	59 FIT	34 FIT

PFD_{AVG}	0.041 x 10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.059 x 10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.115 x 10^{-2}	(T1 = 5 years)
PFH	0.047 x 10^{-6} 1/h	

Proof Test Coverag (PTC)

Test type [6]	Remaining failure rate of dangerous undetected failures	PTC
Test 1	24 FIT	49 %
Test 2	2 FIT	96 %

DPT-20 with diaphragm seal DSS1 (unilateral)

Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{H}	λ_{L}	λ_{AD}
0 FIT	0 FIT	2412 FIT	115 FIT	9 FIT	59 FIT	34 FIT

PFD_{AVG}	0.098 x 10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.143 x 10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.278 x 10^{-2}	(T1 = 5 years)
PFH	0.115 x 10^{-6} 1/h	

[3] Homogeneous redundancy possible, because systematic capability SC3.
[4] Including errors outside the safety function.
[5] Time during which all internal diagnoses are carried out at least once.
[6] See section "Proof test".

Proof Test Coverag (PTC)

Test type [7]	Remaining failure rate of dangerous undetected failures	PTC
Test 1	92 FIT	20 %
Test 2	2 FIT	98 %

DPT-20 with diaphragm seal DSS2 (bilateral)

Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{H}	λ_{L}	λ_{AD}
0 FIT	0 FIT	2412 FIT	183 FIT	9 FIT	59 FIT	34 FIT

PFD_{AVG}	0.154×10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.226×10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.442×10^{-2}	(T1 = 5 years)
PFH	0.183×10^{-6} 1/h	

Proof Test Coverag (PTC)

Test type [8]	Remaining failure rate of dangerous undetected failures	PTC
Test 1	160 FIT	12 %
Test 2	2 FIT	99 %

4.2 Characteristics acc. to ISO 13849-1

The transmitter has been manufactured and verified using principles that demonstrate its suitability and reliability for safety-related applications. It can therefore be considered a " *proven component*" according to DIN EN ISO 13849-1.

Derived from the safety-related characteristics, the following figures result according to ISO 13849-1 machine safety): [9]

DPT-20

Parameter	Value
$MTTF_d$	45 years
DC	98 %
Performance Level	4.67×10^{-8} 1/h

DPT-20 with diaphragm seal DSS1 (unilateral)

Parameter	Value
$MTTF_d$	43 years
DC	96 %
Performance Level	1.15×10^{-7} 1/h

[7] See section "Proof test".
[8] See section "Proof test".
[9] ISO 13849-1 was not part of the certification of the instrument.

DPT-20 with diaphragm seal DSS2 (bilateral)

Parameter	Value
$MTTF_d$	42 years
DC	93 %
Performance Level	1.83 x 10^{-7} 1/h

4.3 Supplementary information

Determination of the failure rates

The failure rates of the instruments were determined by an FMEDA according to IEC 61508. The calculations are based on failure rates of the components according to **SN 29500**:

All figures refer to an average ambient temperature of 40 °C (104 °F) during the operating time. For higher temperatures, the values should be corrected:

- Continuous application temperature > 50 °C (122 °F) by factor 1.3
- Continuous application temperature > 60 °C (140 °F) by factor 2.5

Similar factors apply if frequent temperature fluctations are expected.

Assumptions of the FMEDA

- The failure rates are constant. Take note of the useful service life of the components according to IEC 61508-2.
- Multiple failures are not taken into account
- Wear on mechanical parts is not taken into account
- Failure rates of external power supplies are not taken into account
- The environmental conditions correspond to an average industrial environment

Calculation of PFD_{AVG}

The values for PFD_{AVG} specified above were calculated as follows for a 1oo1 architecture:

$$PFD_{AVG} = \frac{PTC \times \lambda_{DU} \times T1}{2} + \lambda_{DD} \times MTTR + \frac{(1 - PTC) \times \lambda_{DU} \times LT}{2}$$

Parameters used:

- T1 = Proof Test Interval
- PTC = 90 %
- LT = 10 years
- MTTR = 8 h

Boundary conditions relating to the configuration of the processing unit

A connected control and processing unit must have the following properties:

- The failure signals of the measuring system are judged according to the idle current principle
- " *fail low*" and " *fail high*" signals are interpreted as a failure, whereupon the safe state must be taken on

If this is not the case, the respective percentages of the failure rates must be assigned to the dangerous failures and the values stated in chapter *Safety-related characteristics*“ redetermined!

Multiple channel architecture

Due to the systematic capability SC3, this instrument can also be used in multiple channel systems up to SIL3, also with a homogeneously redundant configuration.

The safety-related characteristics must be calculated especially for the selected structure of the measuring chain using the stated failure rates. In doing this, a suitable Common Cause Factor (CCF) must be considered (see IEC 61508-6, appendix D).

5 Setup

5.1 General information

Mounting and installation

Take note of the mounting and installation instructions in the operating instructions manual.

Setup must be carried out under process conditions.

5.2 Instrument parameter adjustment

Tools

The following adjustment units are permitted for parameterization of the safety function:

- Display and adjustment module
- The DTM suitable for DPT-20 in conjunction with an adjustment software according to the FDT/DTM standard, e. g. PACTware
- The device description EDD suitable for DPT-20

The parameter adjustment is described in the operating instructions manual.

SIL Wireless connection is also possible with existing Bluetooth function.

SIL The documentation of the device settings is only possible with the full version of the DTM Collection.

Safety-relevant parameters

For protection against unwanted or unauthorzed adjustment, the set parameters must be protected against unauthorized access. For this reason, the instrument is shipped in locked condition. The PIN in delivery status is "0000".

The default values of the parameters are listed in the operating instructions. When shipped with customer-specific parameter settings, the instrument is accompanied by a list of the values differing from the default values.

Safe parameterization

To avoid or detect possible errors during parameter adjustment for unsafe operating environments, a verification procedure is used that allows the safety-relevant parameters to be checked.

Parameter adjustment proceeds according to the following steps:

- Unlock adjustment
- Change parameters
- Lock adjustment and verify modified parameters

The exact process is described in the operating instructions.

SIL Wireless connection is also possible with existing Bluetooth function.

SIL The instrument is shipped in locked condition!

SIL For verification, all modified, safety-relevant and non safety-relevant parameters are shown.

The verification texts are displayed either in German or, when any other menu language is used, in English.

Unsafe device status

Warning:
When adjustment is unlocked, the safety function must be considered as unreliable. This applies until the parameters are verified and the adjustment is locked again. If the parameter adjustment process is not carried out completely, the device statuses described in the operating instructions must be taken into consideration.

If necessary, you must take other measures to maintain the safety function.

Instrument reset

Warning:
In case a reset to " *Delivery status*" or " *Basic setting*" is carried out, all safety-relevant parameters must be checked or set anew.

6 Diagnostics and servicing

6.1 Behaviour in case of failure

Internal diagnosis

The instrument permanently monitored by an internal diagnostic system. If a malfunction is detected, a fault signal will be output on the safety-relevant output (see section " *Safe status*").

The diagnosis interval is specified in chapter " *Safety-related characteristics*".

Error messages in case of malfunction

A fault message coded according to the type of fault is output. The fault messages are listed in the operating instructions.

SIL

If failures are detected, the entire measuring system must be shut down and the process held in a safe state by other measures.

The manufacturer must be informed of the occurrence of a dangerous undetected failure (incl. fault description).

6.2 Repair

Electronics exchange

The procedure is described in the operating instructions manual. Note the instructions for parameter adjustment and setup.

Software update

The procedure is described in the operating instructions manual. Note the instructions for parameter adjustment and setup.

7 Proof test

7.1 General information

Objective

To identify possible dangerous, undetected failures, the safety function must be checked by a proof test at adequate intervals. It is the user's responsibility to choose the type of testing. The time intervals are determined by the selected PFD_{AVG} (see chapter " *Safety-related characteristics*").

For documentation of these tests, the test protocol in the appendix can be used.

If one of the tests proves negative, the entire measuring system must be switched out of service and the process held in a safe state by means of other measures.

In a multiple channel architecture this applies separately to each channel.

Preparation

- Determine safety function (mode, switching points)
- If necessary, remove the instruments from the safety chain and maintain the safety function by other means
- Provide an approved adjustment unit

Unsafe device status

Warning:
During the function test, the safety function must be treated as unreliable. Take into account that the function test influences downstream connected devices.

If necessary, you must take other measures to maintain the safety function.

After the function test, the status specified for the safety function must be restored.

7.2 Test 1: Without checking the process variable

Conditions

- Instrument can remain in installed condition
- Output signal corresponds to the assigned process variable
- Device status in the menu Diagnosis: " *OK*"

Procedure

1. Carry out a re-start (separate the test item at least 10 seconds from mains voltage)
2. Simulate upper fault current > 21 mA and check current output (test line resistor)
3. Simulate lower fault current ≤ 3.6 mA and check current output (test quiescent currents)

Expected result

Step 1: Output signal corresponds to the assigned process variable and the device status in the menu Diagnosis is " *OK*"

Step 2: Output signal corresponds to > 21 mA

Step 3: Output signal corresponds to ≤ 3.6 mA

Proof Test Coverage

See *Safety-related characteristics*

7.3 Test 2: With check of the process variable

Conditions

- Instrument can remain in installed condition
- A reference pressure measurement is carried out on the high pressure side
- The low pressure side is ventilated to atmospheric pressure or pressurized with the static pressure corresponding to the application
- Output signal corresponds to the assigned process variable
- Device status in the menu Diagnosis: " *OK*"

Procedure

1. Carry out a re-start (separate the test item at least 10 seconds from mains voltage)
2. Simulate upper fault current > 21 mA and check current output (test line resistor)
3. Simulate lower fault current ≤ 3.6 mA and check current output (test quiescent currents)
4. Reference pressure measurement at 0 % - 50 % - 100 % of the adjusted measuring range in use (4 mA - 12 mA - 20 mA)
5. If necessary, sensor calibration through service log-in and subsequent reference pressure measurement as under point 4

Expected result

Step 1: Output signal corresponds to the assigned process variable and the device status in the menu Diagnosis is " *OK*"

Step 2: Output signal corresponds to > 21 mA

Step 3: Output signal corresponds to ≤ 3.6 mA

Step 4 and 5: Output signal corresponds to the reference pressure

Proof Test Coverage

See *Safety-related characteristics*

8 Appendix A: Test report

Identification	
Company/Tester	
Plant/Instrument TAG	
Meas. loop TAG	
Instrument type/Order code	
Instrument serial number	
Date, setup	
Date of the last proof test	

Test reason/Test scope	
	Setup without checking the process variable
	Setup with check of the process variable
	Proof test without checking the process variable
	Proof test with check of the process variable

Mode	
	Monitoring of an upper limit value
	Monitoring a lower limit value
	Range monitoring

Adjusted parameters of the safety function are documented	
	Yes
	No

Test result (if necessary)				
Test point	**Process variable [10)]**	**Expected measured value**	**Real value**	**Test result**
Value 1				
Value 2				
Value 3				
Value 4				
Value 5				

Confirmation	
Date:	Signature:

[10)] e.g.: limit level, level, interface, pressure, flow, density

9 Appendix B: Term definitions

Abbreviations

SIL	Safety Integrity Level (SIL1, SIL2, SIL3, SIL4)
SC	Systematic Capability (SC1, SC2, SC3, SC4)
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{AVG}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of a dangerous failure per hour (Ed.2)
FMEDA	Failure Mode, Effects and Diagnostics Analysis
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
λ_S	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_H	Rate for failure, who causes a high output current (> 21 mA)
λ_L	Rate for failure, who causes a low output current (≤ 3.6 mA)
λ_{AD}	Rate for diagnostic failure (detected)
λ_{AU}	Rate for diagnostic failure (undetected)
DC	Diagnostic Coverage
PTC	Proof Test Coverage (Diagnostic coverage for manual proof tests)
T1	Proof Test Interval
LT	Useful Life Time
MTBF	Mean Time Between Failure = MTTF + MTTR
MTTF	Mean Time To Failure
MTTR	IEC 61508, Ed1: Mean Time To Repair IEC 61508, Ed2: Mean Time To Restoration
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

10 Supplement C: SIL conformity

SIL Manufacturer declaration, NE130: Form B.1

Manufacturer	
WIKA Alexander Wiegand SE & Co. KG Alexander-Wiegand-Straße 30, 63911 Klingenberg, Germany	

General			
Device designation and permissible types	DPT-20		
	Two-wire 4…20mA/HART with SIL qualification Item-No: DPT-20-***-*****-S*-…		
Safety-related output signal	4…20 mA		
Fault current	≥ 21 mA; ≤ 3,6 mA		
Process variable / function	Differential pressure transmitter for process pressure or hydrostatic level measurement		
Safety function(s)	Generation of a measured value to monitor MIN / MAX / Range		
Device type acc. to IEC 61508-2	☐ Type A	☒ Type B	
Operating mode	☒ Low Demand Mode	☒ High Demand or Continuous Mode	
Valid Hardware-Version	≥ 1.0.0		
Valid Software-Version	≥ 1.2.2		
Safety manual	Document ID: 62276		
Type of evaluation (check only one box)	☒	Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	☐	Evaluation of “Prior use” performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3	
	☐	Evaluation of HW/SW field data to verify „prior use” acc. to IEC 61511	
	☐	Evaluation by FMEDA acc. to IEC61508-2 for devices without software	
Evaluation through (incl. certificate no.)	TÜV Rheinland Industry Service GmbH, Nr./No. 968/FSP 2124.00/20		
Test documents	Development documents	Test reports	Data sheets

Safety Integrity			
Systematic Capability (SC)		☐ SC2 for SIL2	☒ SC3 for SIL3
Hardware Safety Integrity	Single-channel use (HFT=0)	☒ SIL2 capable	☐ SIL3 capable
	Multi-channel use (HFT≥1)	☐ SIL2 capable	☒ SIL3 capable

FMEDA	Version		
	DPT-20	**with chemical seal CSS (one-sided)**	**with chemical seal CSB (both-sided)**
Safety function(s)	MIN / MAX / Range	MIN / MAX / Range	MIN / MAX / Range
λ_{DU} (FIT = Failure In Time / 109 h)	47 FIT	115 FIT	183 FIT
λ_{DD}	2514 FIT	2514 FIT	2514 FIT
λ_{SU}	0 FIT	0 FIT	0 FIT
λ_{SD}	0 FIT	0 FIT	0 FIT
SFF (Safe Failure Fraction)	> 90 %	> 90 %	> 90 %
PTC (Proof Test Coverage)	Test 1: 49% / Test 2: 96%	Test 1: 20% / Test 2: 98%	Test 1: 12% / Test 2: 99%
FMEDA data source	SN 29500		

Declaration	
☒	Our internal company quality management system ensures information on safety-related systematic faults which become evident in the future.

Certificate

Nr./No.: 968/FSP 2124.00/20

Prüfgegenstand **Product tested**	Differenzdrucktransmitter Differential pressure transmitter	**Zertifikats-inhaber** **Certificate holder**	WIKA Alexander Wiegand SE & Co. KG Alexander-Wiegand-Str. 30 63911 Klingenberg Germany
Typbezeichnung **Type designation**	DPT-20		
Prüfgrundlagen **Codes and standards**	IEC 61508 Parts 1-7:2010 IEC 61010-1:2010 + Corr.1:2011 + Corr.2:2013	EN 61326-3-2:2008	
Bestimmungsgemäße Verwendung **Intended application**	Der Differenzdrucktransmitter DPT-20 erfüllt die Anforderungen der genannten Prüfgrundlagen und kann in einem sicherheitsbezogenen System in einer HFT=0 Konfiguration bis SIL 2 gemäß der IEC 61508 und redundant (HFT=1) bis SIL 3 (Systematische Eignung SC 3) u.a. im Anwendungsbereich der IEC 61511-1 eingesetzt werden. The differential pressure transmitterDPT-20 complies with the requirements of the stated standards and can be used in a safety-related system in a HFT=0 configuration up to SIL 2 acc. to IEC 61508 and redundantly (HFT=1) up to SIL 3 (Systematic Capability SC 3) amongst others in the application area of IEC 61511-1.		
Besondere Bedingungen **Specific requirements**	Die zugehörigen Betriebsanleitungen und das Safety Manual sind zu beachten. The operating instructions and the safety manual shall be considered.		

Gültig bis / Valid until 2023-05-28

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 2124.00/20 vom 29.09.2020 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 2124.00/20 dated 2020-09-29.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit

Köln, 2020-09-29 — Certification Body Safety & Security for Automation & Grid — Dipl.-Ing. (FH) Wolf Rückwart

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-01

TÜVRheinland®
Precisely Right.

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

Printing date:

All statements concerning scope of delivery, application, practical use and operating conditions of the sensors and processing systems correspond to the information available at the time of printing.

WIKA Alexander Wiegand SE & Co. KG
Alexander-Wiegand-Straße 30
63911 Klingenberg
Germany
Phone (+49) 9372/132-0
Fax (+49) 9372 132-406
E-mail: info@wika.de
www.wika.de

62276-EN-201020