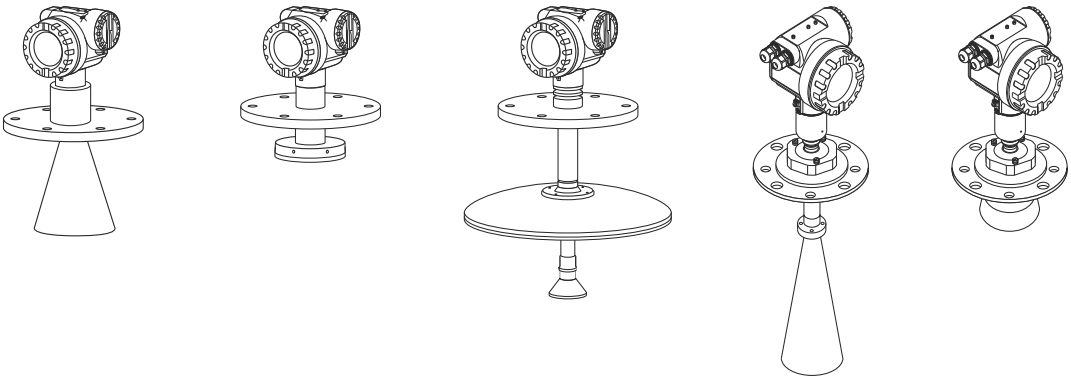
Functional Safety Manual
Micropilot S
FMR530/532/533, FMR540

Level-Radar with 4 to 20 mA output signal



Application

Operating minimum (e.g. dry run protection), maximum (e.g. overfill protection) and range monitoring of powdery to granular bulk solids and all types of liquids in systems to satisfy particular safety systems requirements as per IEC 61508 Edition 2.0.

The measuring device fulfils the requirements concerning

- Functional safety as per IEC 61508 Edition 2.0
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per EN 61326 and NAMUR recommendation NE 21
- Electrical safety as per IEC/EN 61010-1

Your benefits

- Used for level monitoring (MIN, MAX, Range)
  - SIL 1 for low and high requirement rates
  - SIL 2 for low requirement rate
- Permanent self-monitoring
- Continuous measurement
- Non-contact measurement: measurement is virtually independent of product properties
- Easy commissioning

Endress+Hauser

People for Process Automation

Table of contents

SIL Declaration of Conformity

SIL_00258_01.18

Endress+Hauser
People for Process Automation

SIL Declaration of Conformity

Functional Safety according to IEC 61508
Based on NE130 Form B.1

Endress+Hauser SE+Co. KG, Hauptstraße 1, 79689 Maulburg

being the manufacturer, declares that the product stated below

Micropilot S FMR530/532/533, FMR540

is suitable for the use in safety-instrumented systems according to IEC 61508. The instructions of the corresponding functional safety manual must be followed.

This declaration of compliance is exclusively valid for the customer listed in the cover letter of the respective Endress+Hauser sales center and for the listed products and accessories in delivery status.

Maulburg, 13-July-2018
Endress+Hauser SE+Co. KG

i. V.
Manfred Hammer
Dept. Manager Technology
Quality Management / FSM
Research & Development

i. V.
Thorsten Springmann
Dept. Manager Continuous
Level Measurement
Research & Development

1/2

SIL_08006a_de

SIL_00258_01.18

Endress+Hauser
People for Process Automation

General			
Device designation and permissible types	FMR530/532/533		
	FMR540		
Safety-related output signal	4...20 mA		
Fault current	≤ 3.6 mA ; ≥ 21 mA		
Process variable/function	Level measurement		
Safety function(s)	Min ; Max ; Range		
Device type acc. to IEC 61508-2	☐ Typ A	☒ Typ B	
Operating mode	☒ Low Demand Mode	☒ High Demand Mode	☐ Continuous Mode
Valid Hardware-Version	As of manufacturer date after June 30, 2018		
Valid Software-Version	As of version FMR530/532/533: V03.00.0074 and FMR540: V01.02.1332		
Safety manual	SD00345F		
Type of evalutation (check only one box)	☐	Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	☒	Evaluation of "Proven-in-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 w/o software	
Evaluation through – report no.	Endress+Hauser SE+Co. KG / report no. 713_ASSESS_SIL-ZertVerl-FMR5xx		
Test documents	Development documents	Test reports	Data sheets

SIL - Integrity			
Systematic safety integrity		☐ SIL 2 capable	☐ SIL 3 capable
Hardware safety integrity	Single channel use (HFT = 0)	☒ SIL 1 capable	Low Demand Mode High Demand Mode
		☒ SIL 2 capable	Low Demand Mode
	Multi channel use (HFT ≥ 1)	☐ SIL 2 capable	☐ SIL 3 capable

FMEDA		
	FMR530/532/533	FMR540
Safety function	Min ; Max ; Range	Min ; Max ; Range
λ_{DU} *1), 2)	374 FIT	318 FIT
λ_{DD} *1), (2)	663 FIT	1215 FIT
λ_{SU} *1), (2)	335 FIT	19 FIT
λ_{SD} *1), (2)	313 FIT	0 FIT
SFF - Safe Failure Fraction	77,81 %	79,49 %
PFDavg *2) (T = 1 year) (single channel architecture)	1.64×10^{-3}	1.40×10^{-3}
PFDavg *2) (T = 2 years) (single channel architecture)	3.28×10^{-3}	2.80×10^{-3}
PTC *3)	98 %	98 %
λ_{total} *1), (2)	1908 FIT	2285 FIT
DC – Diagnostic Coverage	63 %	75 %
Diagnostic test interval	30 min	30 min
Fault reaction time	30 s	30 s

Comments
/

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

*1) FIT = Failure In Time, Number of failures per 10^9 h
*2) Valid for average ambient temperature up to +40 °C (+104 °F)
For continuous operation at ambient temperature close to +60 °C (+140 °F), a factor of 2.1 should be applied
*3) PTC = Proof Test Coverage

2/2

SIL_08006a_de

Introduction

General information on functional safety (SIL) is available at: www.de.endress.com/SIL (German) or www.endress.com/SIL (English) and in Competence Brochure CP01008Z/11/EN "Functional Safety in the Process Industry - Risk Reduction with Safety Instrumented Systems".

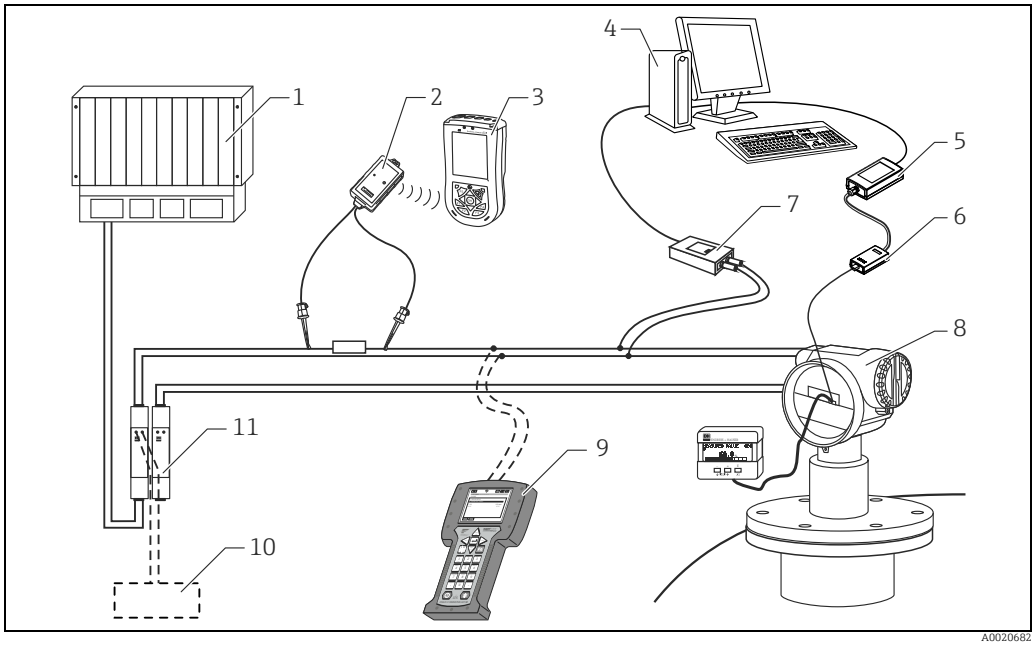
Other safety-related characteristic values

Characteristic as per IEC 61508	value
System reaction time as per DIN EN 61298-2	≤ 5 s

Structure of the measuring system

System components

The measuring system's devices are displayed in the following diagram (example).



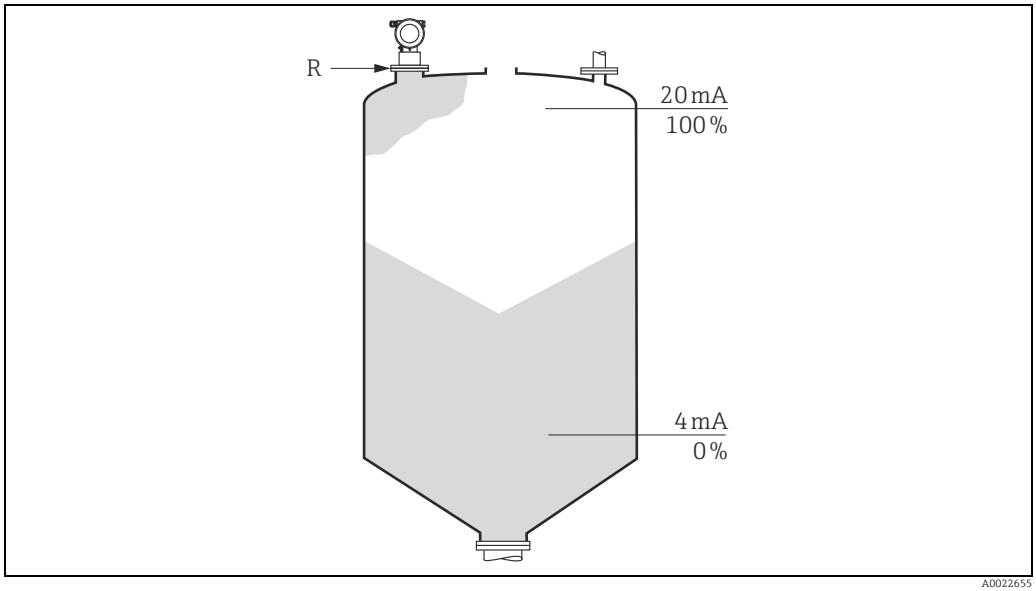
1 PLC (programmable logic controller)
2 VIATOR Bluetooth modem with connecting cable
3 Field Xpert
4 Computer with operating tool (e.g. FieldCare)
5 Commubox FXA291
6 ToF adapter FXA291
7 Commubox FXA195 (USB)
8 Micropilot with display module
9 Field Communicator 475
10 FXA195 or Field Communicator 475
11 Transmitter power supply unit RN221N (with communication resistor)

An analog signal (4 to 20 mA) in proportion to the level is generated in the transmitter. This is sent to a downstream logic unit (e.g. PLC, limit signal transmitter, etc.) where it is monitored to determine whether it is below or above a specified limit value. For fault monitoring, the logic unit must recognize both HI-alarms (≥ 21.0 mA) and LO-alarms (≤ 3.6 mA).

Description of use as a protective system

The Micropilot S is a "downward-looking" measuring system that functions according to the ToF method (ToF = Time of Flight). The distance from the reference point (process connection of the measuring device) to the product surface is measured. Radar impulses are emitted by an antenna, reflected off the product surface and received again by the radar system.

Typical measuring arrangement:



R Flange: Reference point of measurement

Correct installation is a prerequisite for safe operation of the device.

Permitted device types

The details pertaining to functional safety in this manual relate to the device versions listed below and are valid as of the specified software and hardware version. Unless otherwise specified, all subsequent versions can also be used for safety instrumented systems.
A modification process according to IEC 61508 is applied for device changes.

Valid device versions for safety-related use:

Micropilot S FMR530, FMR540

Feature	Designation	Option model
010	Approval	all
020	Antenna; Seal	all
030	Process Connection	all
040	Output; Operation	all
050	Housing	all
060	Cable Entry	all
070	Weight + Measure Approval	all
080	Additional Option	all

Valid software version: FMR530: as of 01.00, FMR540: as of 01.01
Valid hardware version (electronics): as of delivery date June 2011

Micropilot S FMR532, FMR533

Featuer	Designation	Option model
010	Approval	all
020	Antenna	all
030	Process Connection	all
040	Output; Operation	all
050	Housing	all
060	Cable Entry	all
070	Weight + Measure Approval	all
080	Additional Option	all

Valid software version: FMR53x: as of 01.00
Valid hardware version (electronics): as of delivery date June 2011

Supplementary device documentation

Documentation	Contents	Comment
Technical Information ▪ TI00344F/00/EN (FMR530) ▪ TI01122F/00/EN (FMR532) ▪ TI01123F/00/EN (FMR533) ▪ TI00412F/00/EN (FMR540)	– Technical data – Instructions on accessories	The documentation is available on the Internet. → www.endress.com
Operating Instructions (HART) ▪ BA00206F/00/EN (FMR530) ▪ BA00208F/00/EN (FMR532) ▪ BA00209F/00/EN (FMR533) ▪ BA00326F/00/EN (FMR540)	– Identification – Installation – Wiring – Operation – Commissioning – Maintenance – Accessories – Troubleshooting – Technical data – Appendix	– The documentation is supplied with the device in pdf format on a CD. – The documentation is also available on the Internet. → www.endress.com
Operating Instructions (Device Functions) ▪ BA00217F/00/EN (FMR53x) ▪ BA00341F/00/EN (FMR540)	– Instructions on use – Micropilot S function menu – Function groups ... – ... – Envelope curve – Troubleshooting – Function menu index	– The documentation is supplied with the device in pdf format on a CD. – The documentation is available on the Internet. → www.endress.com
Safety instructions depending on the selected version "Approval"	Safety, installation and operating instructions for devices, which are suitable for use in potentially explosive atmospheres or as overfill protection (WHG, German Water Resources Act).	Additional safety instructions (XA, XB, XC, ZE, ZD) are supplied with certified device versions. Please refer to the nameplate for the relevant safety instructions.

Description of the safety requirements and boundary conditions

Safety function

The mandatory settings and safety function data emanate from the descriptions from → 9.
The measuring system's reaction time is ≤ 5 s.

MTTR is set at 8 hours.

Safety-related signal:

The Micropilot S's safety-related signal is the 4 to 20 mA analog output signal.
All safety measures refer to this signal exclusively.

The Micropilot S additionally communicates effectively via HART and contains all HART features with additional device information.

The safety-related output signal is fed to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter where it is monitored for the following:
- Overshooting and/or undershooting a specified level limit.
- The occurrence of a fault, e.g. error current (≤ 3.6 mA, ≥ 21.0 mA, interruption or short-circuit of the signal line).

Restrictions for use in safety-related applications

The measuring system must be used correctly for the specific application, taking into account the medium properties and ambient conditions. Carefully follow instructions pertaining to critical process situations and installation conditions from the Operating Instructions.
The specifications from the Operating Instructions ("Supplementary device documentation", → 7) must not be exceeded.

The following restriction also applies to safety-related use:
- The accuracy of the 4 to 20 mA safety-related output signal is ± 2%.

Dangerous undetected failures in this scenario:

An incorrect output signal that deviates from the real measured value by more than 2%, but is still in the range of 4 to 20 mA, is considered a dangerous, undetected failure.

Useful lifetime of electrical components:

The established failure rates of electrical components apply within the useful lifetime as per IEC 61508-2 Abschnitt 7.4.9.5 note 3.

In accordance with DIN EN 61508-2, Note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.

Behavior of device during operation and in case of error

Behavior of device during power-up

The safe 4 to 20 mA output signal is available after 17 s after the device is switched on or when the voltage returns.

Device response in the event of alarms or warnings

Error current

In the event of an alarm, the output current can be configured to a value of ≤ 3.6 mA or ≥ 21.0 mA.

In some cases (e.g. failure of power supply, a cable open circuit and faults in the current output itself, where the error current cannot be set), output currents ≤ 3.6 mA (FMR53x) or ≥ 21.0 mA (FMR540) irrespective of the configured error current can occur.

For alarm monitoring, the logic unit must therefore be able to recognize both HI-alarms (≥ 21.0 mA) and LO-alarms (≤ 3.6 mA).

Alarm and warning messages

Additional information is available in the form of fault codes on the alarm and warning messages output.

Installation

Installation, wiring and commissioning

Installation, wiring and commissioning of the device is described in the accompanying Operating Instructions ("Supplementary device documentation", → 7).

Orientation

The permitted orientations of the device are described in the Operating Instructions.

Operation

Calibration of the measuring point

Calibration of the measuring point is described in the Operating Instructions.

The method of device configuration

Altered settings (display/FieldCare) in the "extended calibr." function group (Pos. 05) such as "offset" or "fixed current" (Pos. 063) in the "output" function group have an effect on the output signal.
This must be taken into account when calculating the response height (see relevant Operating Instructions).
We recommend that you check that the behavior of the current signal matches the expected behavior by means of level simulation (correctness of configuration).

Configuration schemata/basic calibration

FieldCare / Display - plain text display	Display VU331 Position
Tank shape	002
↓	
Medium conditions	003
↓	
Process conditions	004
↓	
Empty calibration E	005
↓	
Full calibration F	006
↓	
Pipe diameter (for bypass / stilling well)	007
↓	
Mapping	See Operating Instructions
↓	
Further settings: function group 05	See Operating Instructions
↓	
Overfill protection WHG	018
↓	
On-site locking: 3 keys on the VU331 display	Yes

The parameters are safety-oriented with the "WHG" setting in 018 (→ information in the following table).
As an alternative to activating the "WHG" setting, it is also possible to make the safety-oriented setting manually. In doing so, please observe the information in the table below.

The parameters in *italics* are located on the service level, which can be opened with the code "300".

FMR53x

FieldCare / Display - plain text display	Value/parameter	Display VU331	Comment
Safety settings			
Output on ALARM	Max. 110%, 22 mA	010	Parameter **must** be configured in this way
Output echo loss	ALARM	012	Parameter **must** be configured in this way
Delay time	1 s	014	→ Note 1
In safety distance SD	self holding	016	→ Note 3
Filtering/averaging/delay			
MAM filter length	5	*0D11*	→ Note 2
MAM filter border	1	*0D12*	→ Note 2
Output damping	0	058	→ Note 2
Echo detection			
FEF edge (nur bei MIN)	0	*0D56*	Parameter **must** be configured in this way
FAC adder	6 dB	*0D35*	Parameter **must** be configured in this way
Tank bottom detection	OFF	*0D61*	Parameter **must** be configured in this way
First echo factor	unchanged, but if previously smaller than 30, than: 0D53	*0D51*	→ Note 3
FEF threshold	0	*0D52*	→ Note 3
FEF at near distance	30 dB	*0D53*	→ Note 3
FEF distance near	500 mm	*0D54*	→ Note 3
FEF distance far	3000 mm	*0D55*	Parameter **must** be configured in this way
Max. filling speed	0 mm/s (factory setting)	*0D15*	Parameter **must** be configured in this way
Max. drain speed	0 mm/s (factory setting)	*0D16*	Parameter **must** be configured in this way
Other			
Hysterese width	0 mm (factory setting)	*0D14*	Parameter **must** be configured in this way
Communication address	0	060	Parameter **must** be configured in this way
Current output mode	**"Standard"** if previously **"Fixed current"**	063	Parameter **must** be configured in this way
Simulation	Sim. / OFF	065	Parameter **must** be configured in this way

FMR540

FieldCare / Display - plain text display	Value/parameter	Display VU331	Comment
Safety settings			
Output on ALARM	Max. 110%, 22 mA	010	Parameter **must** be configured in this way
Output echo loss	ALARM	012	Parameter **must** be configured in this way
Delay time	1 s	014	→ Note 1
In safety distance SD	self holding	016	→ Note 3
Filtering/averaging/delay			
Envelope statistics up	2	*0D23*	→ Note 2
Envelope statistics down	2	*0D24*	→ Note 2
MAM filter length	5	*0D11*	→ Note 2
MAM filter border	1	*0D12*	→ Note 2
Output damping	0	058	→ Note 2
Echo detection			
FEF edge (nur bei MIN)	0	*0D56*	Parameter **must** be configured in this way
FAC mode	FMC rising	*0D99*	Parameter **must** be configured in this way
FAC adder	6 dB	*0D35*	Parameter **must** be configured in this way
Tank bottom detection	OFF	*0D61*	Parameter **must** be configured in this way
First echo factor	unchanged, but if previously smaller than 30, than: 0D53	*0D51*	→ Note 3
FEF threshold	0	*0D52*	→ Note 3
FEF at near distance	30 dB	*0D53*	→ Note 3
FEF distance near	500 mm	*0D54*	→ Note 3
FEF distance far	3000 mm	*0D55*	Parameter **must** be configured in this way
Max. filling speed	0 mm/s (factory setting)	*0D17*	Parameter **must** be configured in this way
Max. drain speed	0 mm/s (factory setting)	*0D18*	Parameter **must** be configured in this way
Other			
Detection window	OFF	*0A7*	Parameter **must** be configured in this way
Hysterese width	0 mm (factory setting)	*0D16*	Parameter **must** be configured in this way
Communication address	0	060	Parameter **must** be configured in this way
Current output mode	**"Standard"** if previously **"Fixed current"**	063	Parameter **must** be configured in this way
Simulation	Sim. / OFF	065	Parameter **must** be configured in this way

1. This parameter determines the reaction time of the device in the event of echo loss; a setting of less than 30 s is recommended.
2. This parameter determines the reaction time of the device; deviating settings are possible. In case of changes in **"process cond." (004)** it is automatically adjusted. The corresponding reaction time is indicated in the documentation BA.
3. This parameter can be selected differently, depending on the application.

A measuring condition (echo) which results in an ALARM in the "Safety distance SD" area can be reset or deleted by
– confirming the ALARM in Pos. 017 locally by means of the VU331 LCD display;
– confirming the alarm via the communication protocol (HART) (FieldCare: "ackn. alarm" under safety settings).

Locking

The device must be locked once the Micropilot S has been calibrated as per the Operating Instructions.

Type of locking	Code/action	Position/VU331 display
Hardware (recommended)	3 keys together "lock"	Locally via VU331 display (keys O and S and F)
	↓	
Software (mandatory)	WHG (german)	018

Unlocking

The device is unlocked by firstly removing the hardware lock by locally pressing all the three keys together via the VU331 LCD display and then by setting the "Overfill protection" parameter (Position 018) to "Standard" if necessary.

Type of unlocking	Code/action	Position/VU331 display
Hardware (if locked)	3 keys together "unlock"	Locally via VU331 display (keys O and S and F)
	↓	
Software	Standard	018

Maintenance

Please refer to the relevant Operating Instructions ("Supplementary device documentation", → 🖹 7) for instructions on maintenance and recalibration.
Alternative monitoring measures must be taken to ensure process safety during configuration, proof-testing and maintenance work on the device.

Proof-test

Proof-test

Check the operativeness and safety of safety functions at appropriate intervals!
The operator must determine the time intervals.

Proof-testing of the device can be performed as follows:
- Approaching the level (→ test sequence A).
- Removing the device and measuring a medium with comparable properties (→ test sequence B).

You must also check that all cover seals and cable entries are sealing correctly.

Process for proof-testing

Test sequence A

Preparation

1. Connect suitable measuring device (recommended accuracy better ±0.1 mA) to the current output.
2. Determine the safety setting (level limit or range monitoring).

Procedure for level limit monitoring

1. Approach the level directly below (MAX monitoring) or directly above (MIN monitoring) the level limit to be monitored.
2. Read the output current, record it and assess for accuracy.
3. Approach the level directly above (MAX monitoring) or directly below (MIN monitoring) the level limit to be monitored.

4. Read the output current, record it and assess for accuracy.
5. The test is deemed successful if the current in step 2 does not result in activation of the safety function but the current in step 4 does.

Procedure for range monitoring

1. Approach five levels within the range to be monitored.
2. Read the output current at each level value, record it and assess for accuracy.
3. The test is deemed successful if the current values in step 2 are within the required level of accuracy.

The proof-test is deemed to have failed if the expected current value deviates for a specific level by > ±2%.
For troubleshooting, → Operating Instructions ("Supplementary device documentation", → 7).
98% of dangerous, undetected failures are detected using this test.

Test sequence B

Preparation

1. Prepare the test tank with the medium (dielectric constant comparable to that of the medium to be measured). For installation instructions, → Operating Instructions ("Supplementary device documentation", → 7), Section 3.
2. Remove the device and mount it in the test tank.
3. Connect suitable measuring device (recommended accuracy better than ±0.1 mA) to the current output.
4. Perform interference echo mapping if the shape and size of the test tank is different.
5. Determine the safety setting (level limit monitoring).

Procedure for level limit monitoring or range monitoring
→ Test sequence A

- The proof-test is deemed to have failed if the expected current value deviates for a specific level by > ±2%. For troubleshooting, → Operating Instructions ("Supplementary device documentation", → 7).
  98% of dangerous, undetected failures are detected using this test.
- If an interference echo mapping was performed in the test tank, a valid interference echo mapping must be performed after the device is mounted in the original tank.
- If one of the test criteria from the test sequences described above is not fulfilled, the device may no longer be used as part of a safety instrumented system.
  The purpose of proof-testing is to detect random device failures. The impact of systematic faults on the safety function is not covered by this test and must be assessed separately. Systematic faults can be caused, for example, by process material properties, operating conditions, build-up or corrosion.

Repairs

Repairs

Repairs on the devices must always be carried out by Endress+Hauser.
Safety functions cannot be guaranteed if repairs are carried out by anybody else.

Exception:

The customer may replace the following components on condition that original replacement parts are used, the member of staff responsible has previously been trained by Endress+Hauser to carry out this task and the relevant repair instructions are observed:
- Sensor
- Electronic insert (HF module included)
- Terminal module

The replaced components must be sent to Endress+Hauser for the purpose of fault analysis.

Once the components have been replaced, a proof-test must be carried out as per test sequence A (→ 🖹 13) or test sequence B (→ 🖹 14).

In the event of failure of a SIL-labeled Endress+Hauser device, which has been operated in a protection function, the "Declaration of Contamination and Cleaning" with the corresponding note "Used as SIL device in protection system" must be enclosed when the defective device is returned.
Please refer to the Section "Return" in the Operating Instructions ("Supplementary device documentation", → 🖹 7).

Appendix

Commissioning or proof test protocol

System-specific data		
Company		
Measuring point / TAG no.		
System		
Device type / Order code		
Serial number of device		
Name		
Date		
Signature		
Device-specific commissioning parameters		
Empty calibration		
Full calibration		
Proof-test protocol		
Test stage	Set point	Actual value
1. Current value 1		
2. Current value 2		
3. If necessary current value 3		
4. If necessary current value 4		
5. If necessary current value 5		

www.addresses.endress.com

Endress+Hauser

People for Process Automation