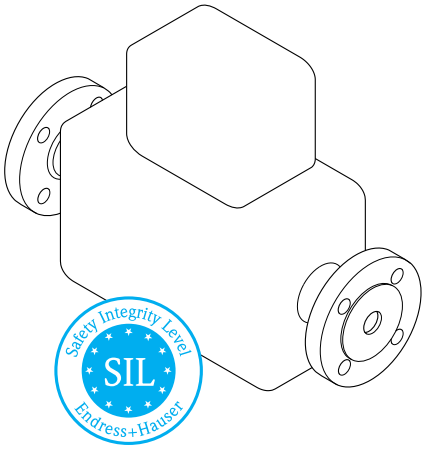
Special Documentation
Proline Promag 300

Functional Safety Manual



Electromagnetic flowmeter

Application

Monitoring of maximum and/or minimum flow in systems which are required to comply with the particular safety circuit requirements of IEC 61508.

The measuring device fulfills the requirements concerning:
- Functional safety as per IEC 61508
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per IEC 61326-3-2 and NAMUR recommendation NE 21
- Electrical safety as per IEC 61010-1

Your benefits

- Use for volume flow monitoring up to SIL 2 (single-channel architecture) or SIL 3 (multi-channel architecture with homogeneous redundancy) - independently assessed and certified by TÜV in accordance with IEC 61508
- Measurement is virtually independent of the process properties
- Permanent self-monitoring
- Easy installation and commissioning
- Integrated proof-testing
- Heartbeat verification for the documentation of diagnostic checks in accordance with IEC 61511

Endress+Hauser
People for Process Automation

Table of contents

Manufacturer's Declaration

Products Solutions Services

HE_61508_Promag_300_500_de_en.docx

Herstellererklärung - Manufacturer Declaration Funktionale Sicherheit / Functional Safety (IEC 61508)

Endress+Hauser Flowtec AG, Kägenstrasse 7, 4153 Reinach

erklärt als Hersteller, dass die Durchflussmessgeräte aus der Serie
declares as a manufacturer, that the flow meters of the product line

Proline Promag 300 (5a3B)
Proline Promag 500 (5a5B)

a = H, P, W

in sicherheitsrelevanten Anwendungen SIL 2 (HFT=0) bzw. SIL 3 (HFT=1) nach IEC 61508:2010 eingesetzt werden können.
are suitable for use in safety relevant applications up to SIL 2 (HFT=0) resp. SIL 3 (HFT=1) acc. IEC 61508:2010.

Für einen Einsatz in sicherheitsrelevanten Anwendungen entsprechend IEC 61508 sind die Angaben des Handbuches zur Funktionalen Sicherheit zu beachten. Die Installation muß konform zu diesem Handbuch ausgeführt werden und die Sicherheitshinweise sind zu beachten.
For safety relevant applications according to IEC 61508, we refer to our hand-book named functional safety. The installation has to be conform to our descriptions in our handbook in consideration of our safety instructions.

Die Kenngrößen für die Verwendung des Produktes in sicherheitsrelevanten Anwendungen können dem Handbuch zur Funktionalen Sicherheit entnommen werden.
The characteristics for use of these products in safety relevant applications can be found in the functional safety manual.

Reinach, 14. Juli 2016

Endress+Hauser Flowtec AG

Dr. B.-J. Schäfer
Managing Director

i.V.
M. Karolzak
Project Manager Functional Safety

Endress+Hauser
People for Process Automation

A0031601-EN

Safety-related characteristic values

General			
Device designation and permitted versions	5H3B (Promag H 300) 5P3B (Promag P 300)		
	Order code for "Output; input 1": ▪ Option **BA** "4-20mA HART" ▪ Option **BB** "4-20mA + Wireless HART" ▪ Option **CA** "4-20mA HART Ex-i" ▪ Option **CB** "4-20mA Ex-i + Wireless HART" Order code for "Output; input 2": All options Order code for "Output; input 3": All options Order code for "Additional approval": Option **LA** "SIL"		
Safety-related output signal	4 to 20 mA (output; input 1)		
Error current	≤ 3.6 mA or ≥ 21 mA		
Assessed measured variable/function	Volume flow monitoring		
Safety function(s)	Min., Max., Range		
Device type according to IEC 61508-2	☐ Type A ☑ Type B		
Operating mode	☑ Low Demand Mode ☑ High Demand Mode ☐ Continuous Mode [1]		
Valid hardware version (main electronics)	From delivery date August 2, 2016		
Valid firmware version	01.00.zz and higher (HART; from delivery date August 2, 2016)		
Safety manual	SD01740D		
Type of assessment (only 1 version can be selected)	☑Complete HW/SW assessment in the context of development including FMEDA and change process according to 61508-2, 3		
	☐ Assessment of evidence for proven-in-use HW/SW including FMEDA and change process according to 61508-2, 3		
	☐ Analysis of HW/SW field data for evidence of "prior use" according to IEC 61511		
	☐ Assessment by FMEDA according to IEC 61508-2 for devices without software		
Assessment by (including Report No. + FMEDA data source)	TÜV Rheinland Industrie Service GmbH – Certificate No. 968/FSP 1306.00/16		
Test documents	Development documents, test reports, data sheets		
SIL integrity			
Systematic safety integrity		☐ SIL 2 capable	☑ SIL 3 capable
Hardware safety integrity	Single-channel service (HFT = 0)	☑ SIL 2 capable	☐ SIL 3 capable
	Multi-channel service (HFT ≥ 1)	☐ SIL 2 capable	☑ SIL 3 capable
FMEDA			
Safety function(s)	Min., Max., Range		
	Option **BA, BB**	Option **CA, CB**	
λ_{DU} [2]	132 FIT	128 FIT	
λ_{DD} [2]	1647 FIT	1627 FIT	
λ_{SU} [2]	1528 FIT	1724 FIT	
λ_{SD} [2]	1240 FIT	1226 FIT	
SFF - Safe Failure Fraction	97 %		
PFD_{avg} for T_1 = 1 year [3] (single-channel architecture)	$5.8 \cdot 10^{-4}$	$5.6 \cdot 10^{-4}$	

PFD_{avg} for T_1 = 4 years [3] (single-channel architecture)	$2.3 \cdot 10^{-3}$	
PFH	$6.6 \cdot 10^{-8}$	$6.4 \cdot 10^{-8}$
PTC [4]	Up to 98 %	
$MTBF_{tot}$ [5]	69 years	58 years
Diagnostic test interval [6]	30 min	
Fault response time [7]	30 s	
Process safety time [8]	50 h	
Recommended test interval T_1	4 years	
$MTTF_d$ [9]	64 years	65 years
Note		
The measuring device has been developed for use in "Low Demand" and "High Demand" mode.		
Explanation		
☑Our in-house quality management system saves information on safety-related systematic errors that will become known in the future.		

1) No continuous operation in accordance with IEC 61508: 2011 (Section 3.5.16).
2) FIT = Failure In Time, number of failures per 10^9 h.
3) Valid for averaged ambient temperatures up to 40 °C (104 °F) in accordance with general standard for SIL devices.
4) PTC = Proof Test Coverage (diagnostic coverage achieved by device failure detection during manual proof testing).
5) This value takes into account all failure types of the electronic components as per Siemens SN29500.
6) All diagnostic functions are carried out at least once during this time.
7) Maximum time between fault detection and fault response.
8) The process safety time amounts to the diagnostic test interval * 100 (calculation as per IEC 61508).
9) $MTTF_d$ as per ISO 13849/IEC 62061 also includes soft errors (sporadic bit errors in data memories).

Useful lifetime of electric components

The established failure rates of electrical components apply for a useful lifetime of 12 years as per IEC 61508-2: 2010, Section 7.4.9.5, Note 3.

The device's year of manufacture is coded in the first character of the serial number (→ table below).

Example: serial number L5ABBF02000 → year of manufacture 2016

ASCII character	Meaning	ASCII character	Meaning	ASCII character	Meaning
D	2010	K	2015	R	2020
E	2011	L	2016	S	2021
F	2012	M	2017	T	2022
H	2013	N	2018	V	2023
J	2014	P	2019	W	2024

Document information

Document function

The document is part of the Operating Instructions and serves as a reference for application-specific parameters and notes.

- General information about functional safety: **SIL**
- General information about SIL is available:
  In the Download Area of the Endress+Hauser Internet site: www.de.endress.com/SIL

Using this document

Information on the document structure

For the arrangement of the parameters as per the **Operation** menu, **Setup** menu, **Diagnostics** menu, along with a short description, see the Operating Instructions for the device

For information about the operating philosophy, see the "Operating philosophy" chapter in the device's Operating Instructions

Symbols used

Safety symbols

Symbol	Meaning
DANGER	**DANGER!** This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.
WARNING	**WARNING!** This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.
CAUTION	**CAUTION!** This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.
NOTICE	**NOTE!** This symbol contains information on procedures and other facts which do not result in personal injury.

Symbols for certain types of information

Symbol	Meaning
	Tip Indicates additional information.
	Reference to documentation
	Reference to page
	Reference to graphic
▶	Notice or individual step to be observed
1., 2., 3...	Series of steps
	Result of a step
	Operation via local display
	Operation via operating tool
	Write-protected parameter

Symbols in graphics

Symbol	Meaning
1, 2, 3 ...	Item numbers
A, B, C, ...	Views
A-A, B-B, C-C, ...	Sections

Supplementary device documentation

For an overview of the scope of the associated Technical Documentation, refer to the following:
- The *W@M Device Viewer* : Enter the serial number from the nameplate (www.endress.com/deviceviewer)
- The *Endress+Hauser Operations App*: Enter the serial number from the nameplate or scan the 2-D matrix code (QR code) on the nameplate.

Standard documentation

Operating Instructions

Measuring device	Documentation code
Promag H 300	BA01392D
Promag P 300	BA01393D

Description of Device Parameters

Measuring device	Documentation code
Promag 300	GP01051D

Technical Information

Measuring device	Documentation code
Promag H 300	TI01223D
Promag P 300	TI01224D

Supplementary device-dependent documentation

Safety Instructions

Contents	Documentation code
ATEX/IECEx Ex d/Ex de	XA01414D
ATEX/IECEx Ex ec	XA01514D
cCSAus XP	XA01515D
cCSAus Ex d/ Ex de	XA01516D
cCSAus Ex nA	XA01517D
INMETRO Ex d/Ex de	XA01518D
INMETRO Ex ec	XA01519D
NEPSI Ex d/Ex de	XA01520D
NEPSI Ex nA	XA01521D

Remote display and operating module DKX001

Contents	Documentation code
ATEX/IECEx Ex i	XA01494D
ATEX/IECEx Ex ec	XA01498D
cCSAus IS	XA01499D
cCSAus Ex nA	XA01513D
INMETRO Ex i	XA01500D
INMETRO Ex ec	XA01501D
NEPSI Ex i	XA01502D
NEPSI Ex nA	XA01503D

Special Documentation

Contents	Documentation code
Information on the Pressure Equipment Directive	SD01614D
Functional Safety Manual	SD01740D
Remote display and operating module DKX001	SD01763D

Installation Instructions

Contents	Documentation code
Installation Instructions for spare part sets	For an overview of the accessories available for order, see the Operating Instructions for the device

Permitted device types

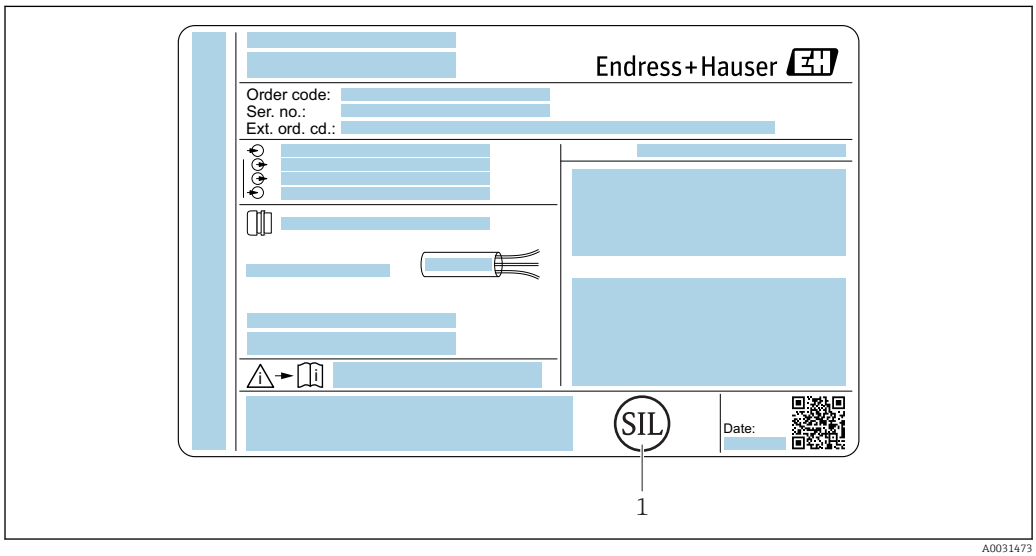
The details pertaining to functional safety in this manual relate to the device versions listed below and are valid as of the specified software and hardware versions. Unless otherwise specified, all subsequent versions can also be used for safety functions. A modification process according to IEC 61508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

Feature	Designation	Option selected
–	Order code	5H3B (Promag H 300) 5P3B (Promag P 300)
000	Nominal diameter	All
010	Approval; transmitter + sensor	All
015	Power supply	All
020	Output; input 1 [1)]	▪ Option **BA** "4-20mA HART" ▪ Option **BB** "4-20mA + Wireless HART" ▪ Option **CA** "4-20mA HART Ex-i" ▪ Option **CB** "4-20mA Ex-i + Wireless HART"
021	Output; input 2	All
022	Output; input 3	All
030	Display; Operation	All
040	Housing	All
050	Electrical connection	All
060	Lining	All

Feature	Designation	Option selected
070	Process connection	All
075	Electrodes	All
080	Calibration flow	All
480	Device model	All
500	Display operating language	All
520	Sensor option	All
530	Customer-specific configuration	All
540	Application Package	All
550 [2)]	Suitability for custody transfer measurement	All
570	Service	All
580	Test, certificate	All
590	Additional approval	LA (= SIL) [3)]
610	Accessory mounted	All
620	Accessory enclosed	All
850	Firmware version	Firmware with SIL capability, e.g. 01.00.zz (HART)
895	Marking	All

1) In devices with several outputs, only current output 1 (terminals 26 and 27) is suitable for safety functions. The other outputs can, if necessary, be connected for non-safety-oriented purposes.
2) Only for devices with approval for custody transfer
3) Additional selection of further approvals is possible.

SIL label on the nameplate



1 SIL logo

Safety function

Definition of the safety function

The measuring device's permitted safety functions are:
- Monitoring of a maximum or minimum volume flow for liquid media
- Monitoring of a volume flow range for liquid media

Safety-related output signal

The measuring device's safety-related signal is the 4–20 mA analog output signal (output; input 1). All safety measures refer to this signal exclusively.

In devices with several outputs, only current output 1 (terminals 26 and 27) is suitable for safety functions. The other outputs can, if necessary, be connected for non-safety-oriented purposes.

The safety-related output signal is fed to a downstream automation system where it is monitored for the following:
- Overshooting and/or undershooting of a specified limit value for the volume flow
- The occurrence of a fault: e.g. error current (≤ 3.6 mA, ≥ 21 mA), interruption or short-circuit of the signal line

Restrictions for use in safety-related applications

Do not exceed the specifications indicated in the device documentation: → 🖹 8.

Dangerous undetected failures in this scenario

An incorrect output signal that deviates from the value specified in the Operating Instructions but is still in the range of 4 to 20 mA, is considered a dangerous, undetected failure.

Detailed information concerning measured errors:

For detailed information on the maximum measured error, see the Operating Instructions for the device → 🖹 8

Suitability of the measuring device

1. Carefully select the nominal diameter of the measuring device in accordance with the application's expected flow rates.
   ↳ The maximum flow rate during operation must not exceed the specified maximum value for the sensor.
   For detailed information on selecting the nominal diameter, see the Technical Information for the device → 🖹 8
2. In SIL mode: ensure that the measuring tube is filled.
   ↳ Empty pipe detection is switched to the **Off** option in the SIL mode.

NOTICE

Use the measuring device according to the specifications.
- ▶ Pay attention to the medium properties and the environmental conditions.
- ▶ Carefully follow instructions pertaining to critical process situations and installation conditions.

Detailed information on:
- Installation
- Electrical connection
- Medium properties
- Environment
- Process

Operating Instructions and Technical Information for the device → 🖹 8

⚠ CAUTION

For liquids that readily boil or in the case of suction lines:
- ▶ Ensure that the vapor pressure is not undershot and that the liquid does not start to boil.
- ▶ Please ensure that there is never any outgassing of the gases naturally contained in many liquids. Sufficiently high system pressure prevents the occurrence of these effects.
- ▶ In order to guarantee correct measurement, ensure that no cavitation occurs.
- ▶ Avoid applications that cause buildup, corrosion or abrasion.

Detailed information on the suitability of the measuring device for safety-related operation is available from your Endress+Hauser sales center.

Information on measured errors

When the measured value is transmitted via the 4–20 mA current output, the measuring device's relative measured error is made up of the contribution of the digitally determined measured value and the accuracy of the analog current output. These contributions, which are listed in the device documentation, apply under reference operating conditions and can depend on the sensor version

ordered. If process or ambient conditions are different, there are additional contributions, e.g. temperature or pressure, which are also listed.

For detailed information on calculating the measured error, see the Technical Information for the device → 8

Guidelines for minimal measured errors:

- Limit value monitoring: Depending on the process dynamics, the current value of the unfiltered 4–20 mA output signal can temporarily exceed the specified tolerance range.
  The device can optionally provide damping of the current output via a parameter that only affects the measured value output.
  - Device-internal diagnostics or the outputting of an error current (≤ 3.6 mA, ≥ 21 mA) are not affected by this damping.

Power supply to the 4–20 mA current output

Overvoltages at the 4–20 mA current output (passive, output; input 1) - caused by a fault in the supply unit for example - can result in a leak current in the device's input protection circuit. This may lead to falsification of the output signal by more than the specified error or the minimum error current (3.6 mA) can no longer be set due to the leak current.

- Use a 4–20 mA power supply unit with either voltage limitation or voltage monitoring.

NOTICE

The safety-related connection values depend on the Ex approval.

- Pay attention to the safety-related connection values.

For detailed information on the connection values, see the "Safety Instructions" documentation → 8

HART communication

The measuring device also communicates via HART or WirelessHART in the SIL mode. This comprises all the HART features with additional device information.

NOTICE

The measuring device's safety-related signal is the 4–20 mA analog output signal (output; input 1).

All safety measures refer to this signal exclusively.

- Please note the following: → 11.

NOTICE

When the SIL locking code is entered, the device parameters that affect the safety-related output signal are locked and write-protected. It is still possible to read the parameters.

When SIL locking is enabled, restrictions apply on all communication options, such as the service interface (CDI-RJ45), HART protocol and WirelessHART protocol, local display and WLAN.

- Deactivation of the SIL mode → 19.

Use in protective systems

Device behavior during operation

Device behavior during power-up

Once switched on, the device runs through a start-up phase. The current output is set to error current during this time. This current is ≤ 3.6 mA in the initial seconds of this start-up phase.

No communication with the device is possible via the interfaces during the start-up phase. After the start-up phase the device switches to the normal mode (measuring operation).

Behavior of device during operation

The device outputs a current value which corresponds to the measured value to be monitored. This value must be monitored and processed further in an attached automation system.

Device behavior in safety function demand mode

Depending on the setting of the **Failure mode** parameter, the current is as follows in demand mode:
- For **Min.** option: ≤ 3.6 mA
- For **Max.** option: ≥ 21 mA

Device behavior in event of alarms and warnings

The output current on alarm can be set to a value ≤ 3.6 mA or ≥ 21 mA.

In some cases (e.g. a cable open circuit or faults in the current output itself, where it is not possible to set the error current ≥ 21 mA) output currents of ≤ 3.6 mA occur irrespective of the configured error current.

In some other cases (e.g. short circuit of cabling), output currents of ≥ 21 mA occur irrespective of the configured error current.

For alarm monitoring, the downstream automation system must be able to recognize both maximum alarms (≥ 21 mA) and minimum alarms (≤ 3.6 mA).

Alarm and warning messages

The alarm and warning messages output on the device display or in the operating tool in the form of diagnostic events and the associated event text are additional information.

For detailed information on diagnostic events, see the Operating Instructions for the device → 8

NOTICE

When SIL mode is activated, additional diagnostics are activated.
If a diagnostic event occurs and the locked SIL mode is deactivated, the error message remains while the error persists, even if the diagnostic event is no longer active in the unlocked state.
- In this case, the device must be disconnected briefly from the power supply .
- When the device is then restarted, a self-check is carried out, and the diagnostics event is reset where applicable.

Parameter configuration for safety-related applications

Calibration of the measuring point

The measuring point is calibrated via the operating interfaces. A wizard guides you systematically through all the submenus and parameters that have to be set for configuring the measuring device.

For detailed information on operation options, see the Operating Instructions for the device → 8

For detailed information on the configuration of the measuring device, see the Operating Instructions for the device and the "Description of Device Parameters" documentation → 8

To activate the SIL mode, the device must run through a confirmation sequence. While running through this sequence, critical parameters are either set automatically by the device to standard values or transferred to the local display/operating tool to enable verification of the setting. On completion of parameter configuration, the SIL mode of the device must be enabled with a SIL locking code.

Availability of the SIL mode function

NOTICE

The SIL confirmation sequence is only visible on the local display and in the operating tools for devices with the order code for "Additional approval", option LA "SIL".
- For this reason, the SIL mode can also only be activated on these measuring devices.
- If the **LA** "SIL" option was ordered for the flowmeter ex works, this function is available when the measuring device is delivered to the customer. Access is via the operating interfaces of the measuring device.
- If the order option cannot be accessed in the measuring device, the function cannot be retrofitted during the life cycle of the device. If you have any questions please contact your Endress+Hauser service or sales organization.

Ways to check function availability in the measuring device:
Using the serial number:
W@M Device viewer [1] → Order code for *"Additional approval"*, option LA *"SIL"*

1) www.endress.com/deviceviewer

Detailed information concerning the SIL label:
- Permitted device types → 9
- SIL label on the transmitter nameplate → 10

Overview of the SIL mode

The SIL mode enables the following steps:

1. Makes sure that the preconditions are met.
   ↳ The measuring device checks whether the user has correctly configured a predefined set of parameters for the safety function.
   If the result is positive, the device continues with the activation of the SIL mode.
   If the result is negative, the sequence is not permitted or is aborted, and the device does not continue with the activation of the SIL mode.
2. Automatically switches a predefined set of parameters to the default values specified by the manufacturer.
   ↳ This parameter set ensures that the flowmeter works in the safety mode.
3. Guides the user through the preconfigured parameters for checking.
   ↳ This ensures that the user actively checks all the important pre-settings.
4. Activates write protection for all the relevant parameters in the SIL mode.

All this ensures that the parameter settings that are required for the safety function are configured correctly. (These settings cannot be circumvented either deliberately or by accident.)

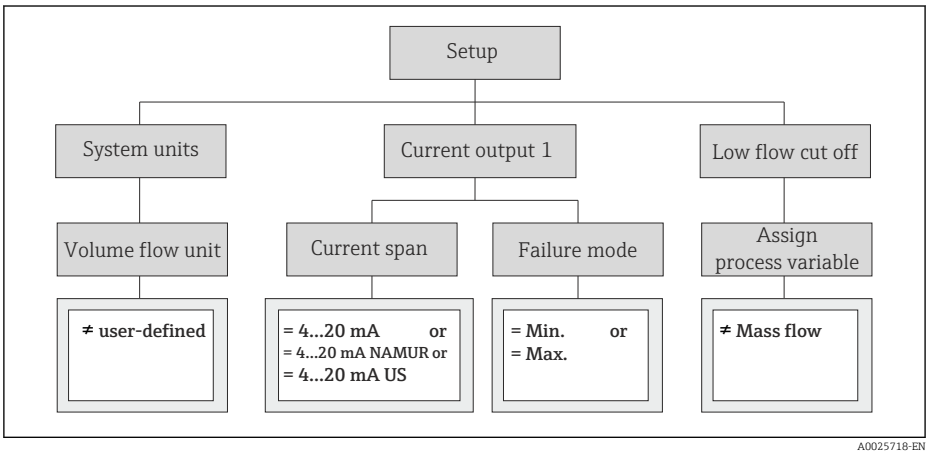
Locking a SIL device

When locking a SIL device, all safety-related parameter settings are shown to the operator individually and must be confirmed explicitly. Parameter settings not permitted in the locked SIL mode are reset to their default values where necessary. A SIL locking code is then entered to lock the device software to ensure that parameters cannot be changed. Non-safety-related parameters remain unchanged.

NOTICE

Once the SIL device has been locked, the process-related parameters are write protected, and thereby locked, for security reasons.
It is still possible to read the parameters. When SIL locking is enabled, restrictions apply on all communication options, such as the service interface, HART protocol and WirelessHART protocol, local display and WLAN.
► Follow the specified locking sequence.

1. Check preconditions.
   ↳



2. In the **Setup** menu → **Advanced setup** submenu, select the **SIL confirmation** wizard.
3. Select **Set write protection** parameter.
4. Enter the SIL locking code **7452**.
   ↳ The device first checks the preconditions listed under item 1.

NOTICE

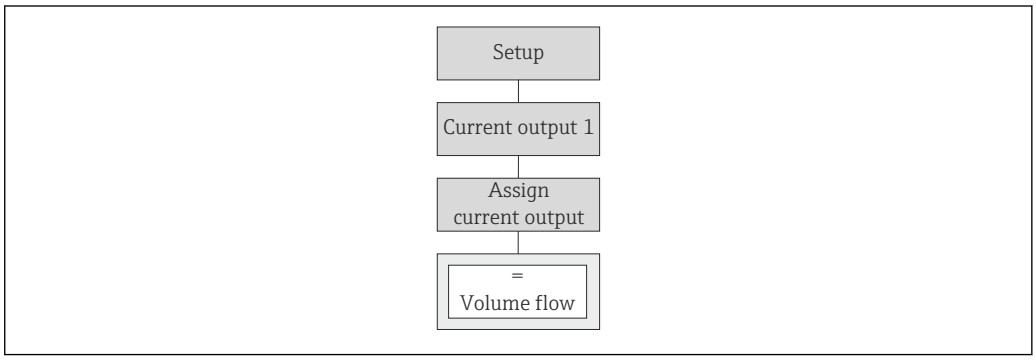
If these preconditions are not met, the message "SIL preparation = failed" appears on the display along with the parameter that failed to meet the preconditions under 1.
The SIL confirmation sequence is not continued.
- ▶ Check preconditions.

If the conditions are met, the message "SIL preparation = finished" appears on the display.

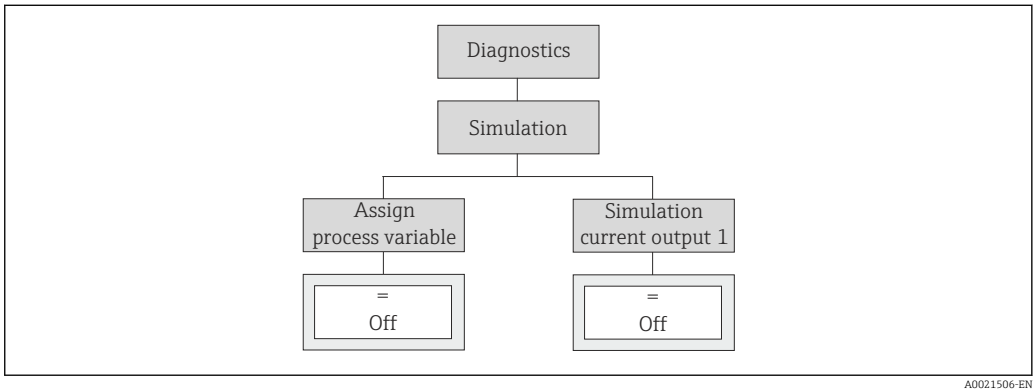
Once the preconditions have been met, the device automatically switches the following parameters to safety-oriented settings:

NOTICE

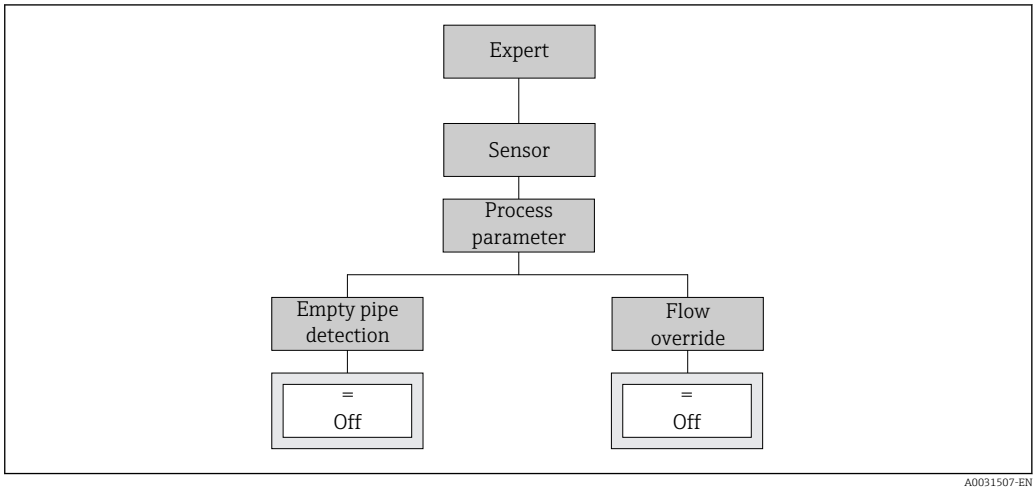
If the measuring device has been configured for the "mass flow" measured variable, the Assign current output in the SIL confirmation sequence is automatically switched to Volume flow.
The 4 mA value and 20 mA value are reset to the factory setting.
- ▶ Cancel the SIL confirmation sequence.
- ▶ Check the settings of the current output and change them if necessary.



A0025650-EN

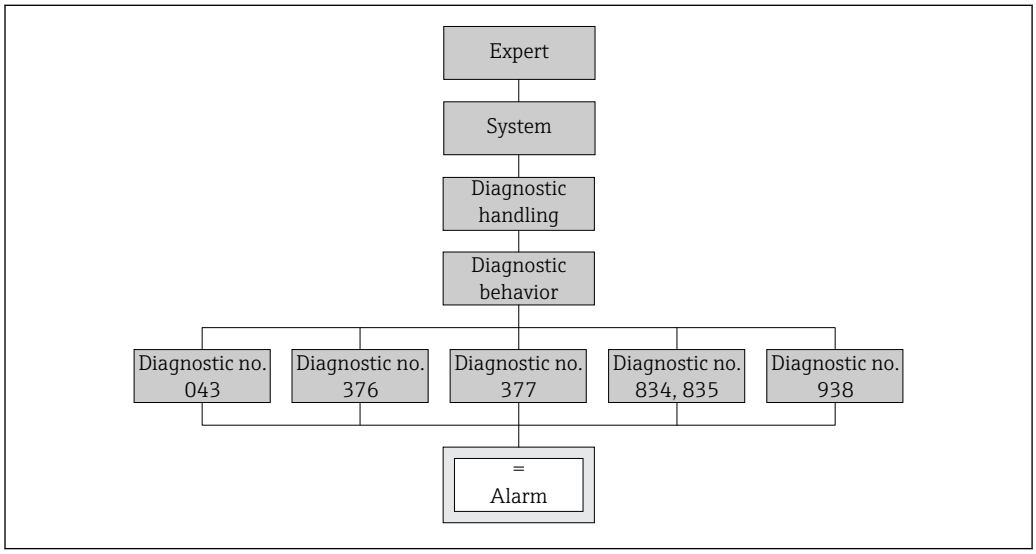


A0021506-EN

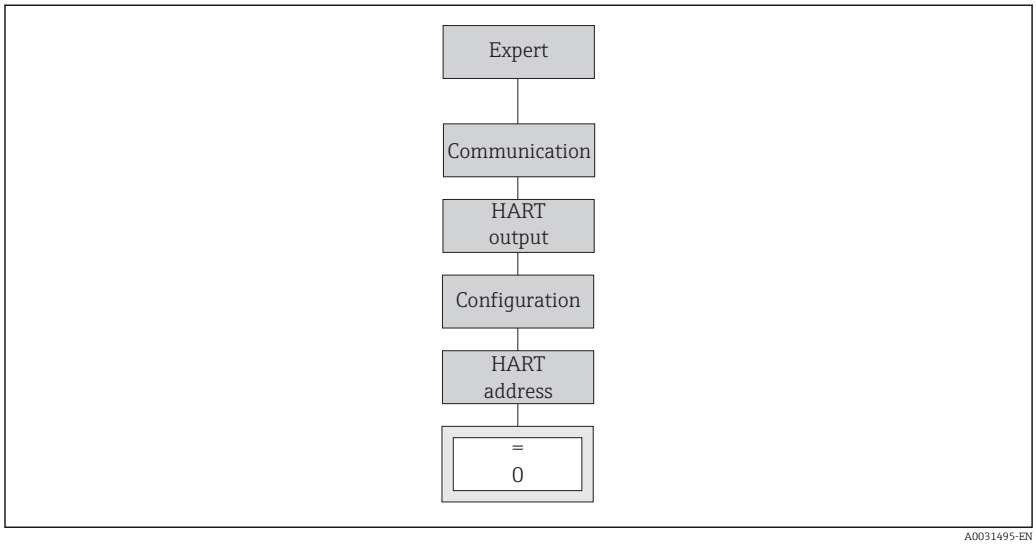


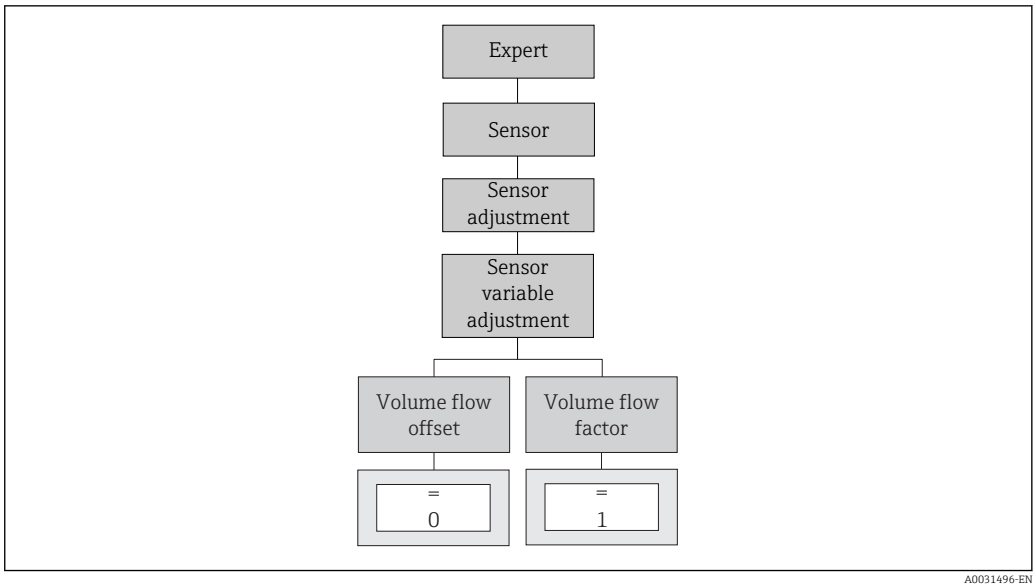
A0031507-EN

The diagnostic behavior is set in such a way that the measuring device is set to the safe state when an error occurs. This means that the diagnostic messages listed in the graphic are set to alarm and the current output adopts the configured failsafe mode → 🖹 12.

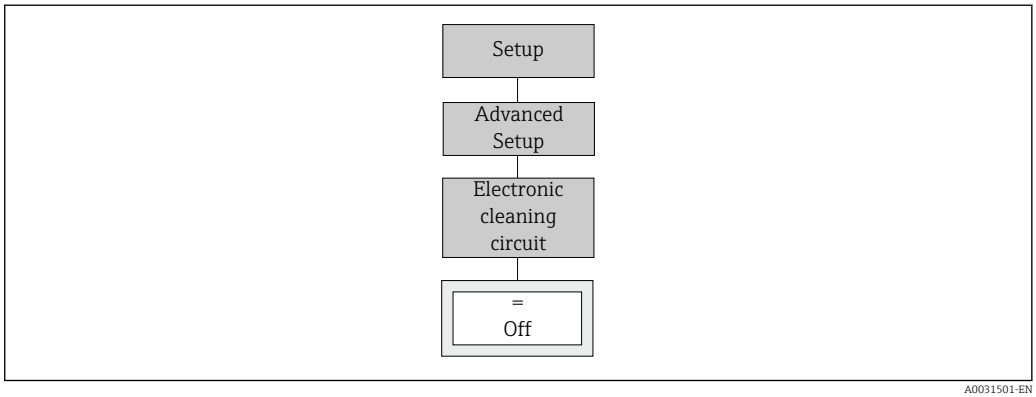


- Diagnostic message **043 Sensor short circuit**
- Diagnostic message **376 Sensor electronic (ISEM) faulty**
- Diagnostic message **377 Sensor electronic (ISEM) faulty**
- Diagnostic message **834 Process temperature too high**
- Diagnostic message **835 Process temperature too low**
- diagnostic message **938 EMC interference**

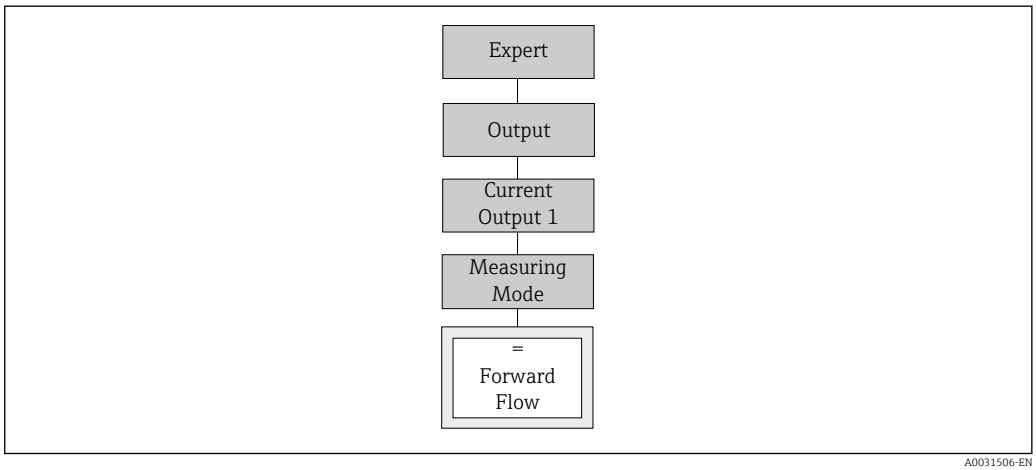




A0031496-EN



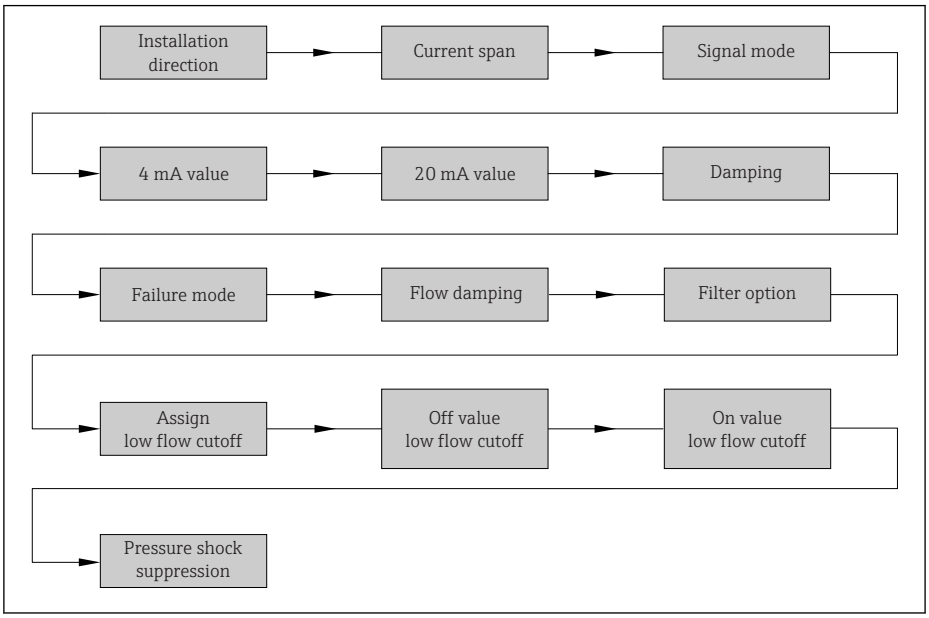
A0031501-EN



A0031506-EN

To check that values are displayed correctly, the following string appears on the device display or operating tool: **0123456789+-.**

5. The user must confirm that the values are displayed correctly.
   ↳ The device displays the current settings for the following parameters one after another for the user to confirm each of them:

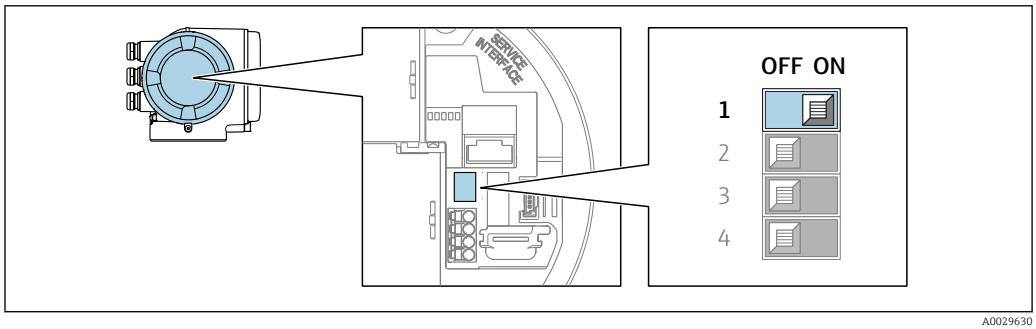


For detailed information on the parameters in the graphic, see the Operating Instructions for the device → 8

6. At the end of the verification, the SIL locking code **7452** must be entered in the **Set write protection** parameter again to confirm that all the parameter values have been defined correctly.
   ↳ If the SIL locking code has been entered correctly, the message **"End of sequence"** appears on the display.
7. Press the E key to confirm.

The SIL mode is now activated.

Recommendation:



1. Check the write protection switch (WP) in the connection compartment.
2. Set this switch to the **ON** position where necessary.
   ↳ Hardware write protection enabled.
3. Restart the device on completion of the SIL confirmation sequence.

NOTICE

If the SIL confirmation sequence is aborted before the "End of sequence" message is displayed, the SIL device is not locked. The safety-oriented parameter settings have been made but the SIL device has not been locked.

► Perform SIL device locking again.

Unlocking a SIL device

A device in the locked SIL mode is protected against unauthorized operation by means of a SIL locking code and, where applicable, by means of a user-specific release code and a hardware write protection switch. The device must be unlocked in order to change parameters, for proof-tests as well as to reset self-holding diagnostic messages.

NOTICE

Unlocking the device deactivates diagnostic functions, and the device may not be able to carry out its safety function in the unlocked SIL mode.

- Therefore, independent measures must be taken to ensure that there is no risk of danger while the SIL device is unlocked.

Unlocking procedure:

1. Check the write protection switch (WP) in the connection compartment.
2. Set this switch to the **OFF** position where necessary.
   - Hardware write protection disabled.
3. Enter the user-specific release code if necessary.
4. In the **Setup** menu → **Advanced setup** submenu, select the **Deactivate SIL** wizard.
5. Select **Reset write protection** parameter.
6. Enter the SIL locking code **7452**.
   - If the SIL locking code has been entered correctly, the message **"End of sequence"** appears on the display.
7. Press the E key to confirm.

The SIL mode is now deactivated.

Proof-testing

NOTICE

The safety function is not guaranteed during a proof test.

Nevertheless, process safety must be guaranteed during proof testing.

- The safety-related output signal 4 to 20 mA (output; input 1) may not be used for the protective system.
- Take alternative monitoring measures if necessary.

Proof testing the safety function of the entire system

1. Check the functional integrity of the safety function at appropriate intervals.
2. The operator specifies the testing interval and this must be taken into account when determining the probability of failure PFD_{avg} of the sensor system.
   - In the case of a single-channel system architecture, the average probability of failure (PFD_{avg}) of the sensor is derived from the proof-test interval T_i, the failure rate for dangerous undetected failures λ_{du}, the proof test coverage PTC and the assumed mission time by close approximation as follows:

$$PFD_{avg} \approx \lambda_{du} \times (PTC/2 \times T_i + (1 - PTC) / 2 \times MT)$$

A0023571

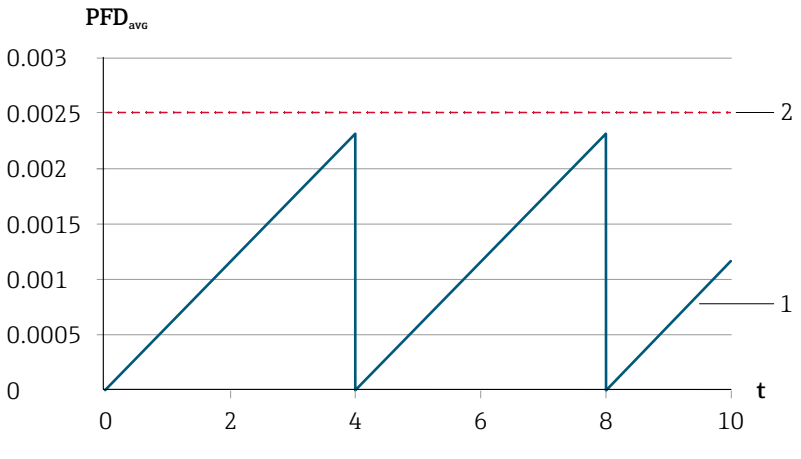
MT Mission time
PTC Proof test coverage
Ti Test interval

3. The operator also specifies the procedure for proof-testing.
   - **NOTE!**
     In accordance with IEC 61511, as an alternative to testing the safety function of the entire system an independent proof test of the subsystems, → 20 e.g. the sensor, is permitted.

Average probability of failure and useful lifetime

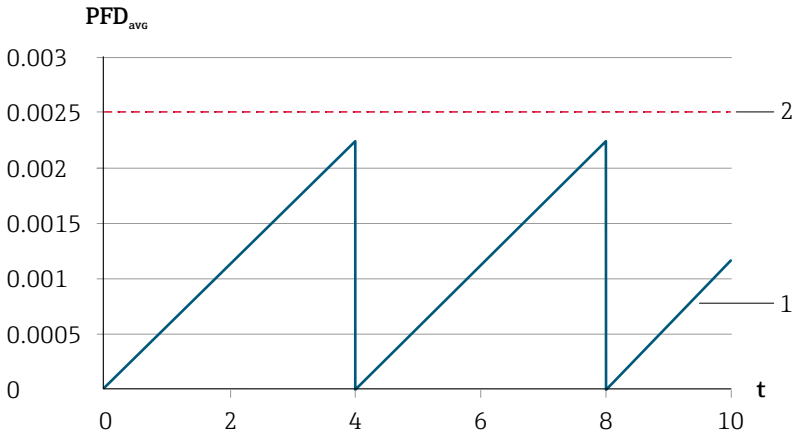
PFD_{avg} for a single-channel system:

SIL2 - 1oo1



A0031610

1 Option BA "4-20mA HART", option BB "4-20mA + Wireless HART"



A0031611

2 Option CA "4-20mA HART Ex-i", option CB "4-20mA Ex-i + Wireless HART"

t *Mission time in years*

1 *PFD_{avg} - Average probability of dangerous failure on demand*

2 *Limit value for average probability of failure*

1oo1 *Single-channel architecture*

Proof testing the sensor subsystem

If there are no operator-specific requirements for the proof test, the following alternative is available for testing the sensor subsystem [2)] depending on the measured variable "volume flow" used for the safety function.

Check of the measured value for liquid volume flow

I. Test sequence:

The measured values (3 to 5 measuring points) are checked with a secondary standard on an installed device (mobile calibration rig or calibrated reference device) or on a factory calibration rig following device removal.

The measured values of the secondary standard and the device under test (DUT) are compared using one of the following methods:

2) Under IEC 61508 the sensor is synonymous with the entire flowmeter.

a. Comparison by reading off the digital measured value

Compare the digital measured value of the secondary standard against the measured value display of the DUT at the logic subsystem (process control system or safety-related PLC).

b. Comparison of the measured value by measuring the current

1. Measure the current at the DUT using an external, traceably-calibrated ammeter.
   ↳ Note: measuring equipment requirements:
   - DC current measuring uncertainty ±0.2 %
   - DC current resolution 10 µA
2. Measure the current of the DUT at the logic subsystem (process control system or safety-related PLC).

II. Assessment of the results:

The amount of deviation between the measured flow rate and the set point must not exceed the measured error specified for the safety function.

- Follow the information in the section on "Restrictions for use in safety-related applications – information on measured errors" → 11.

Other recommendations

It is advisable to perform a visual inspection on site.

- As part of the visual inspection of the transmitter, ensure that all of the electronics compartment cover seals and cable entries are providing adequate sealing.

NOTICE

At least 98 % of dangerous, undetected failures are detected using these test sequences (PTC = 0.98). The influence of systematic errors on the safety function is not fully covered by the test. Systematic faults can be caused, for example, by medium properties, operating conditions, build-up or corrosion.

- 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 protective system.
- Take measures to reduce systematic errors.

Detailed information on:
- Orientation
- Medium properties
- Operating conditions

Operating Instructions for the device → 8

Heartbeat Technology

Heartbeat Technology continuously diagnoses whether failures have occurred. The scope of the diagnostics in the SIL mode corresponds to the SFF.

Heartbeat Technology also allows operators to create documented proof that diagnostic checks have been carried out and thereby supports the documentation of proof testing in accordance with IEC 61511-1, Section 16.3.3, "Documentation of proof testing and inspections".

NOTICE

The SIL mode needs to be disabled temporarily in order to perform heartbeat verification.

- On completion of the verification, the SIL mode must be enabled again .

The **Heartbeat Verification** application package is available as an order option and can be retrofitted on all measuring devices.

Please contact your Endress+Hauser service or sales organization to retrofit the device.

For detailed information on the verification of the measuring device with **Heartbeat Verification**,application package, refer to the Special Documentation for the device → 8

Life cycle

Requirements for the personnel

The personnel for installation, commissioning, diagnostics and maintenance must fulfill the following requirements:
- Trained, qualified specialists must have a relevant qualification for this specific function and task.
- Are authorized by the plant owner/operator.
- Are familiar with federal/national regulations.
- Before starting work, read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
- Follow instructions and comply with basic conditions.

The operating personnel must fulfill the following requirements:
- Are instructed and authorized according to the requirements of the task by the facility's owner-operator.
- Follow the instructions in this manual.

Installation

Installation and electrical connection

Detailed information on:
- Installation
- Electrical connection
- Medium properties
- Environment
- Process

Operating Instructions and Technical Information for the device → 8

Orientation

For detailed information on the orientation, see the Operating Instructions for the device → 8

Commissioning

For detailed information on commissioning, see the Operating Instructions for the device → 8

Operation

For detailed information on operation options, see the Operating Instructions for the device → 8

Maintenance

For detailed information on maintenance, see the Operating Instructions for the device → 8

Alternative monitoring measures must be taken to ensure process safety during configuration, proof-testing and maintenance work on the device.

Repairs

Repair means restoring functional integrity by replacing defective components. Components of the same type must be used for this purpose. It is recommended to document the repair. This includes specifying the device serial number, the repair date, the type of repair and the individual who performed the repair.

For detailed information on device returns, see the Operating Instructions for the device → 8

Replacing device components

The following components may be replaced by the customer's technical staff if genuine spare parts are used and the appropriate installation instructions are followed:
- Sensor
- Transmitter without a sensor
- Display module
- Power unit
- Main electronics module
- I/O-Module
- Terminals
- Connection compartment cover
- Electronics compartment cover

- Seal sets for electronics compartment cover
- Securing clamps for electronics compartment cover
- Cable glands

Installation Instructions: see the Download Area at www.endress.com.

The replaced component must be sent to Endress+Hauser for the purpose of fault analysis if the device has been operated in a protective system and a device error cannot be ruled out. In this case, always enclose the "Declaration of Hazardous Material and Decontamination" with the note "Used as SIL device in protection system" when returning the defective device. Please also refer to the "Return" section in the Operating Instructions ..

Modification

Modifications are changes to devices with SIL capability already delivered or installed.

- ▶ Modifications to devices with SIL capability are usually performed in the Endress+Hauser manufacturing center.
- ▶ Modifications to devices with SIL capability onsite at the user's plant are possible following approval by the Endress+Hauser manufacturing center. In this case, the modifications must be performed and documented by an Endress+Hauser service technician.
- ▶ Modifications to devices with SIL capability by the user are not permitted.

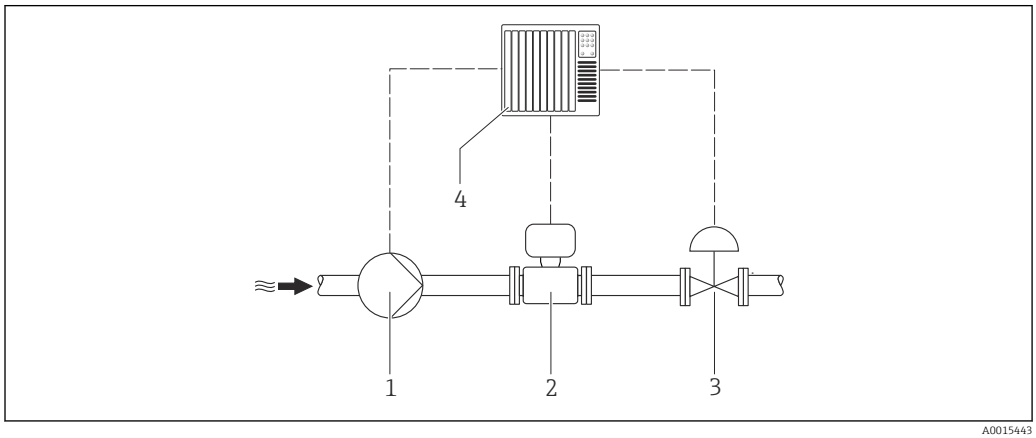
Decommissioning

For detailed information on decommissioning, see the Operating Instructions for the device → 8

Appendix

Structure of the measuring system

System components



3 System components

1 Pump
2 Measuring device
3 Valve
4 Automation system

An analog signal (4–20 mA) proportional to the volume flow is generated in the transmitter. This is sent to a downstream automation system where it is monitored to determine whether it falls below or exceeds a specified limit value. The safety function (volume flow monitoring) is implemented in this way.

Description of use of protective system

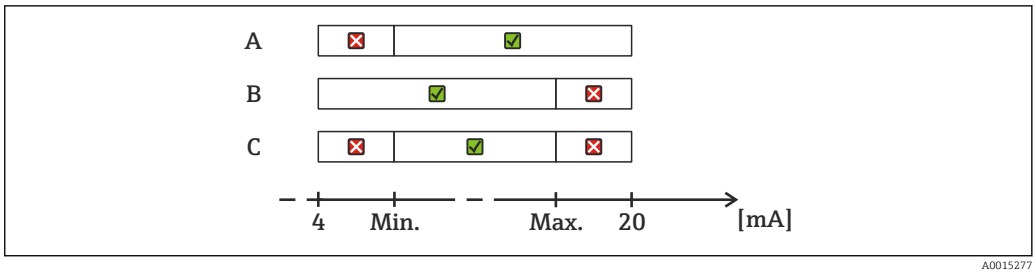
The measuring device can be used in protective systems to monitor the following (Min., Max. and range):
Volume flow

NOTICE

The device must be correctly mounted to guarantee safe operation.

- ▶ Observe the mounting instructions.

For detailed information on mounting, see the Operating Instructions for the device → 8



4 *Monitoring options in protective systems*

A Min. alarm
B Max. alarm
C Range monitoring

= *Safety function is triggered*

= *Permitted operating status*

Verification or calibration

The SIL mode must be disabled in order to verify the measuring point with Heartbeat Technology or calibrate the measuring point.

NOTICE

To use the device in a safety function again following a verification or calibration, the configuration of the measuring point must be checked and the SIL mode must be enabled again.

- ▶ Activation of the SIL mode → 14.

Notes on the redundant use of multiple sensors

This section provides additional information regarding the use of homogeneously redundant sensors e.g. 1oo2 or 2oo3 architectures.

The common cause factors β and β_D indicated below are minimum values for the device. These must be used when designing the sensor subsystem:

- Minimum value β for homogeneously redundant use: 2 %
- Minimum value β_D for homogeneously redundant use: 1 %

The device meets the requirements for SIL 3 in homogeneously redundant applications. When installing identical sensors, i.e. the same type and nominal diameter, the sensors must not be connected directly flange to flange but at different locations in the pipe. This is to prevent the sensors from affecting each other acoustically.

NOTICE

Note the following if a fault is detected in one of the redundantly operated devices during the proof test:

- ▶ Check the other devices to see if the same fault occurs there.

Version history

Version	changes	Valid as of firmware version
SD01740D/06/xx/01.16	First version	01.00.zz (HART; from delivery date August 2, 201)

www.addresses.endress.com

Endress+Hauser

People for Process Automation