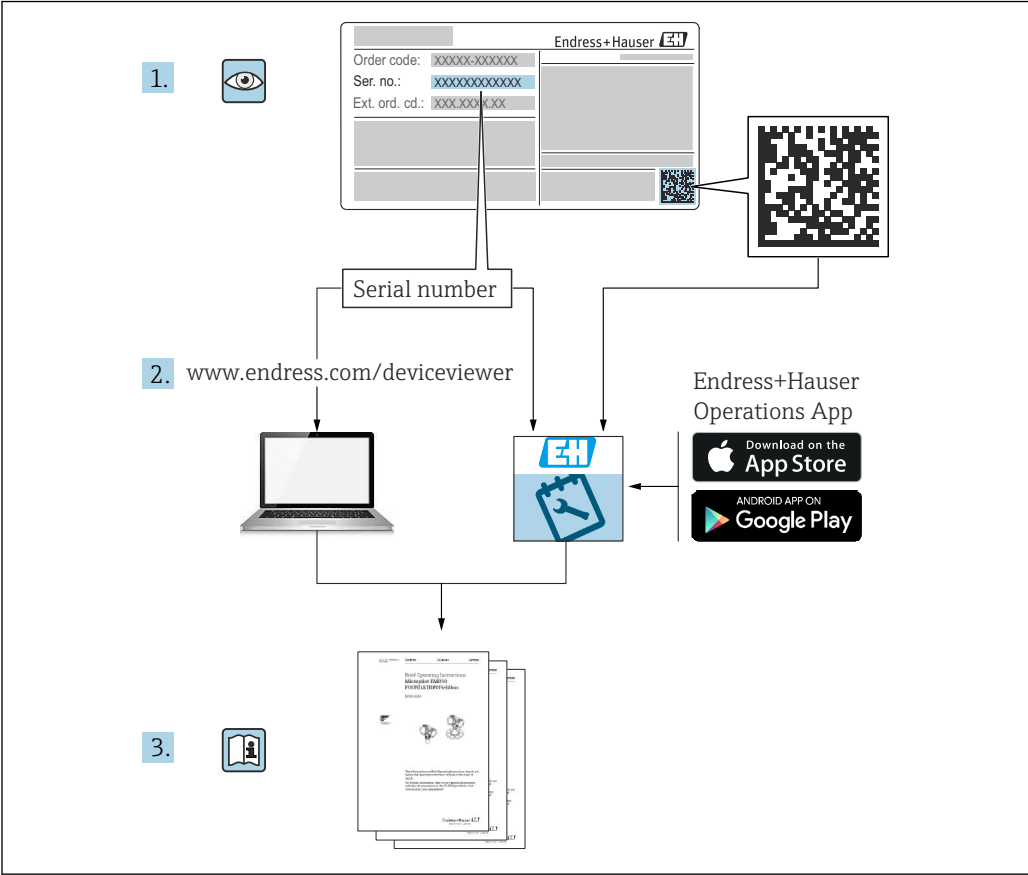


Functional Safety Manual

Tankside Monitor NRF81

Tankside monitor with 4 to 20 mA current output and switch output





A0023555

Table of contents


1	Declaration of Conformity	4	6.2	Installation	22
1.1	Other safety-related characteristic values	6	6.3	Commissioning	22
1.2	Useful lifetime of electrical components	6	6.4	Operation	22
2	About this document	7	6.5	Maintenance	22
2.1	Document function	7	6.6	Repair	23
2.2	Using this document	7	6.7	Modification	23
2.2.1	Information on the document structure	7	7	Appendix	24
2.3	Symbols used	7	7.1	Structure of the measuring system	24
2.3.1	Safety symbols	7	7.1.1	System components	24
2.3.2	Symbols for certain types of information and graphics	7	7.1.2	Description of use as a safety instrumented system	24
2.4	Supplementary device documentation	9	7.2	Proof testing	25
3	Permitted devices types	10	7.3	Notes on the redundant configuration of multiple sensors	25
3.1	SIL label on the nameplate	11	7.4	Further information	26
4	Safety function	11			
4.1	Definition of the safety function	11			
4.2	Safety-related signal	11			
4.3	Restrictions for use in safety-related applications	12			
4.3.1	Dangerous undetected failures in this scenario	13			
5	Use in safety instrumented systems	14			
5.1	Device behavior during operation	14			
5.1.1	Device behavior when switched on	14			
5.1.2	Device behavior in safety function demand mode	14			
5.1.3	Device behavior in the event of alarms and warnings	14			
5.1.4	Alarm and warning messages	14			
5.1.5	Device behavior when switched on	14			
5.1.6	Device behavior in safety function demand mode	14			
5.1.7	Device behavior in the event of alarms and warnings	15			
5.1.8	Alarm and warning messages	15			
5.2	Device configuration for safety-related applications	15			
5.2.1	Calibration of the measuring point	15			
5.2.2	Configuration method	16			
5.3	Proof testing	19			
5.3.1	Test sequence A (Feed in real currents)	20			
6	Life cycle	22			
6.1	Requirements for personnel	22			

1 Declaration of Conformity

SIL_00323_03.24

Endress+Hauser

People for Process Automation



Declaration of Conformity

Functional Safety according to IEC 61508

Based on NE 130 Form B.1

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

being the manufacturer, declares that the product

Tank Side Monitor NRF8x

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 conformity is exclusively valid for the listed products and accessories in delivery status.

Maulburg, January 4, 2024

Endress+Hauser SE+Co. KG

i. V.

E-SIGNED by Thomas Lützel

on 09 January 2024 06:43:01 GMT

Thomas Lützel

Dept. Man. R&D Inventory Management Systems

Research & Development

i. V.

E-SIGNED by Manfred Hammer

on 09 January 2024 06:32:12 GMT

Manfred Hammer

Dept. Man. R&D Quality Management/FSM

Research & Development

A0044234

SIL_00323_03.24

Endress+Hauser 
People for Process Automation

General			
Device designation and permissible types ¹⁾	Tank Side Monitor NRF8x ** * * ** * * * * * + [LA]		
	x = 1		
Safety-related output signal	4...20 mA / relay contact		
Fault signal	≤ 3.6 mA / ≥ 21 mA / open contact		
Process variable/function	Current measurement		
Safety function(s)	MIN / MAX / RANGE		
Device type acc. to IEC 61508-2	<input type="checkbox"/> Type A		<input checked="" type="checkbox"/> Type B
Operating mode	<input checked="" type="checkbox"/> Low Demand Mode	<input checked="" type="checkbox"/> High Demand Mode	
Valid hardware version	Manufacturing date after Nov. 28, 2016		
Valid software version	01.yy.zz (yy: any number, zz: any number)		
Safety manual	FY01104G		
Type of evaluation (check only <u>one</u> box)	<input checked="" type="checkbox"/>	Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	<input type="checkbox"/>	Evaluation of "proven in use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3	
	<input type="checkbox"/>	Evaluation of HW/SW field data to verify „prior use" acc. to IEC 61511	
	<input type="checkbox"/>	Evaluation by FMEDA acc. to IEC 61508-2 for devices w/o software	
Evaluation through – report/certificate no.	TÜV Rheinland 968/FSP 1809		
Test documents	Development documents	Test reports	Data sheets
SIL – Integrity			
Systematic safety integrity		<input type="checkbox"/> SC 2	<input checked="" type="checkbox"/> SC 3
Hardware safety integrity	Single channel use (HFT = 0)	<input checked="" type="checkbox"/> SIL 2 capable	<input type="checkbox"/> SIL 3 capable
	Multi channel use (HFT ≥ 1)	<input type="checkbox"/> SIL 2 capable	<input checked="" type="checkbox"/> SIL 3 capable
FMEDA			
Safety function	MIN	MAX	RANGE
$\lambda_{DU}^{2),3)}$	157 FIT	157 FIT	157 FIT
$\lambda_{DD}^{2),3)}$	4990 FIT	4990 FIT	4990 FIT
$\lambda_S^{2),3)}$	2255 FIT	2255 FIT	2255 FIT
SFF	98%	98%	98%
PFD _{avg} (T ₁ = 1 year) ³⁾ (single channel architecture)	$7.27 \cdot 10^{-4}$	$7.27 \cdot 10^{-4}$	$7.27 \cdot 10^{-4}$
PFH	$1.57 \cdot 10^{-7}$ 1/h	$1.57 \cdot 10^{-7}$ 1/h	$1.57 \cdot 10^{-7}$ 1/h
PTC ⁴⁾ A	99%	99%	99%
Diagnostic test interval ⁵⁾	≤ 60 min	≤ 60 min	≤ 60 min
Fault reaction time ⁶⁾	≤ 1 min	≤ 1 min	≤ 1 min
Comments			
–			
Declaration			
<input checked="" type="checkbox"/>	Our internal company quality management system ensures information on safety-related systematic faults which become evident in the future		

¹⁾ Valid order codes and order code exclusions are maintained in the E+H ordering system

²⁾ FIT = Failure In Time, number of failures per 10⁹ h

³⁾ 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

⁴⁾ PTC = Proof Test Coverage

⁵⁾ All diagnostic functions are performed at least once within the diagnostic test interval

⁶⁾ Maximum time between error recognition and error response

1.1 Other safety-related characteristic values

Characteristic value as per IEC 61508	Value
MTBF ¹⁾	36 years
System reaction time as per DIN EN 61508-2	In "Expert mode": User configurable

- 1) As per Siemens SN29500. This value takes into account failure modes relevant to the function of the electronic components.

1.2 Useful lifetime of electrical components

The established failure rates of electrical components apply within the useful lifetime as per IEC 61508-2:2010 section 7.4.9.5 note 3. In accordance with DIN EN 61508-2:2011 section 7.4.9.5 national footnote N3, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.

2 About this document

2.1 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

2.2 Using this document

2.2.1 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

2.3 Symbols used

2.3.1 Safety symbols



This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.



This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.



This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.



This symbol contains information on procedures and other facts which do not result in personal injury.

2.3.2 Symbols for certain types of information and graphics



Tip
Indicates additional information



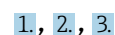
Reference to documentation



Reference to graphic



Notice or individual step to be observed



Series of steps



Result of a step

1, 2, 3, ...
Item numbers
A, B, C, ...
Views

2.4 Supplementary device documentation

Documentation	Comment
Technical Information: TI01251G/00	The documentation is available on the Internet: → www.endress.com
Operating Instructions BA01465G/00	The documentation is available on the Internet: → www.endress.com
Brief Operating Instructions: KA01209G/00	<ul style="list-style-type: none"> ■ The document is provided with the device. ■ The documentation is available on the Internet: → www.endress.com
Safety instructions depending on the selected option "Approval".	Additional safety instructions (XA, ZE) are supplied with certified device version. Please refer to the nameplate for the relevant safety instructions.



This supplementary Safety Manual applies in addition to the Operating Instructions, Technical Information and ATEX Safety Instructions. Other applicable device documentation must be observed during installation, commissioning and operation. The requirements specific to the protection function are described in this safety manual.

3 Permitted devices 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 functions. A modification process according to IEC 61508 is applied for any device modifications.

Valid device versions for safety-related use:

Order code	Designation	Option
010	Approval	All
020	Connector type	All
030	Power supply; display	All
040	Primary output	See next table
050	Secondary I/O analog	See next table
060	Secondary I/O digital Ex d/XP	See next table
070	Housing	All except Y9
090	Electrical connection	All
150	Accuracy, approval for custody transfer	All
500	Operating languages; display	All
540	Application package	All
570	Service	All
580	Test; certificate	All
590	Additional approval	LA ¹⁾ SIL
610	Accessory mounted	All
620	Accessory enclosed	All
850	Firmware version	If no version is selected here, the latest SW with SIL capability is supplied. Alternatively, the following SW version can be selected: 01.yy.zz
895	Identification	All

1) An additional selection of other versions is possible.

Order code	040	050	060
Option	E1	A1 or B1	*
	H1	A1 or B1	*
	E1	*	A1, A2, A3, B2 or B3
	H1	*	A1, A2, A3, B2 or B3
	*	A2	*
	*	B2	*
	*	C2	*
	*	A1	A1, A2, A3, B2 or B3
	*	B1	A1, A2, A3, B2 or B3

* All options are possible. (This selection does not affect SIL capability.)

- Valid firmware version: as of 01.02.zz (→ nameplate of the device)
- Valid hardware version (electronics): as of date of production 23.11.2016 (→ nameplate of the device)

3.1 SIL label on the nameplate



SIL certified devices are marked with the following symbol on the nameplate:

4 Safety function

4.1 Definition of the safety function

The device's safety function is:

- Current input monitoring
- The safety function comprises the measurement of the current of a connected device.

4.2 Safety-related signal

Digital

The device's safety-related signal is the closed relay contact of the digital output. All safety measures refer to this signal exclusively.

The analog input current (safety function) is correctly converted to a digital output value. The relay contact is closed within the range of validity, and is open outside this range.

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:

- Exceeding and/or undershooting a predefined point level.
- The occurrence of a fault, e.g. contact open (interruption of the signal line).



In the event of an error, it must be ensured that the equipment under control achieves or maintains a safe state.

Analog

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

The device can also communicate via HART for information purposes and contains all the 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:

- Exceeding and/or undershooting a predefined point level.
- The occurrence of a fault, e.g. failure current (≤ 3.6 mA, ≥ 21.0 mA, interruption or short-circuit of the signal line).

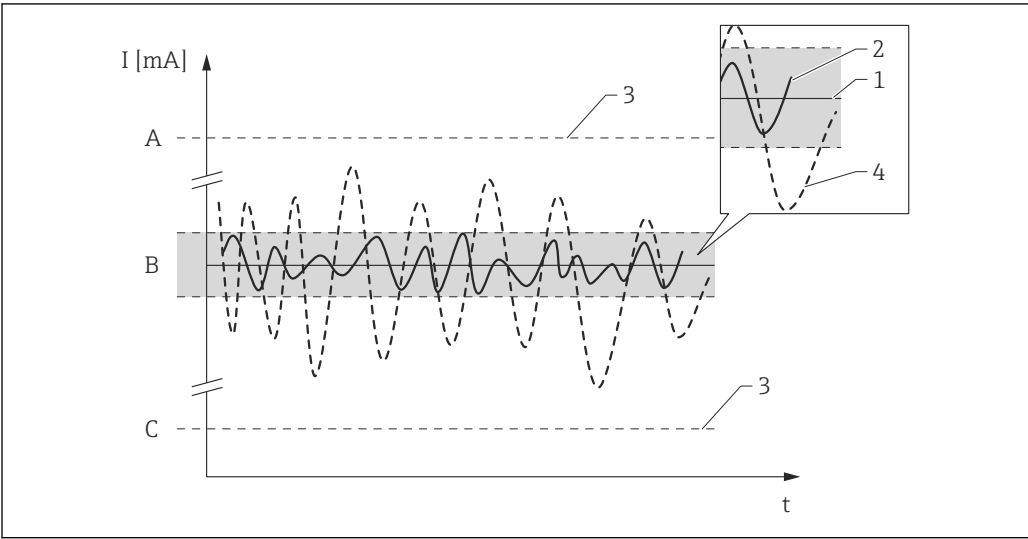


In the event of an error, it must be ensured that the equipment under control achieves or maintains a safe state.

4.3 Restrictions for use in safety-related applications

- Information on the safety-related signal, (→ 11).
 - The specifications from the Operating Instructions must not be exceeded, (→ 9).
 - The following restriction also applies for safety-related use:
 - Strong, pulse-like EMC interference on the line can cause transient (<1 s) deviations ≥ ±2 % in the output signal. For this reason, filtering with a time constant of ≥1 s should be performed in the downstream logic unit.
 - The error range is device-specific and is defined according to FMEDA (Failure Modes, Effects and Diagnostic Analysis) on delivery from the factory. It includes all influential factors described in the Technical Information (e.g. non-linearity, non-repeatability, hysteresis, zero drift, temperature drift, EMC influences).
- The safety-related errors are classified into different categories according to IEC/EN 61508 (see the following table). The table shows the implications for the safety-related analog output signal and for measuring uncertainty.

Safety-related error	Explanation	Implications for the safety-related output signal	Impact on measuring uncertainty (Position, see figure → 12)
No device error	Safe: No error	None	1 Is within the specification (see TI, BA, ...)
λ_{SD}	Safe detected: Safe failure which can be detected	Causes the output signal to signal the failsafe mode (see, → 14)	3 No implications
λ_{SU}	Safe undetected: Safe failure which cannot be detected	Is within the defined error range	2 May be outside specifications
λ_{DD}	Dangerous detected: Dangerous failure which can be detected (Diagnostic within the device)	Causes the output signal to signal the failsafe mode (see, → 14)	3 No implications
λ_{DU}	Dangerous undetected: Dangerous failure which cannot be detected	May be outside the defined error range	4 May be outside the defined error range



A0025264

- A HI alarm ≥21 mA
- B Error range ±2 %
- C LO alarm ≤3.6 mA

4.3.1 Dangerous undetected failures in this scenario

A dangerous, undetected failure is considered to be an incorrect output signal that deviates from the real value by more than 2 %, wherein the output signal is still in the range of 4 to 20 mA or the relay contact remains closed.

5 Use in safety instrumented systems

5.1 Device behavior during operation

Digital

5.1.1 Device behavior when switched on

Once switched on, the device runs through a diagnostic phase of approx. 30 seconds. The relay contact is open during this time. During the diagnostic phase, communication via the service interface (CDI) or via protocols (HART, V1, Modbus, WM550) is not possible.

5.1.2 Device behavior in safety function demand mode

The device displays a digital output value which corresponds to the limit value to be monitored. The relay contact is closed within the range of validity, and is open outside this range. This must be monitored and processed accordingly by a connected logic unit.

5.1.3 Device behavior in the event of alarms and warnings

The relay contact is always open in the event of alarms and warnings. This must be monitored and processed accordingly by a connected logic unit.

5.1.4 Alarm and warning messages

Additional information is provided by the alarm and warning messages in the form of error codes and associated plain text messages.

The following table shows the correlation between the error code and the relay contact output:

Error code ¹⁾	Relay contact (message type)	Note
Fxxx	Open	xxx = three-digit number
Mxxx	corresponding to measuring mode	xxx = three-digit number
Cxxx	corresponding to measuring mode	xxx = three-digit number
Sxxx	corresponding to measuring mode	xxx = three-digit number

1) The error codes are listed in the Operating Instructions.

Analog

5.1.5 Device behavior when switched on

Once switched on, the device runs through a diagnostic phase of approx. 30 seconds. The current output is set to failure current ≤ 3.6 mA during this time.

During the diagnostic phase, communication via the service interface (CDI) or via protocols (HART, V1, Modbus, WM550) is not possible.

5.1.6 Device behavior in safety function demand mode

The device outputs a current value corresponding to the limit value to be monitored. This value must be monitored and processed further in a connected logic unit.

5.1.7 Device behavior in the event of alarms and warnings

The output current in the event of an alarm can be set 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 failure current ≥ 21.0 mA cannot be set, output currents of ≤ 3.6 mA occur irrespective of the configured failure current.

In some other cases (e.g. cabling short circuit), output currents of ≥ 21.0 mA occur irrespective of the configured failure current.

For alarm monitoring, the downstream logic unit must be able to recognize failure currents of the upper signal on alarm level (≥ 21.0 mA) and of the lower signal on alarm level (≤ 3.6 mA).

5.1.8 Alarm and warning messages

Additional information is provided by the alarm and warning messages in the form of error codes and associated plain text messages.

The following table shows the correlation between the error code and the current output:

Error code ¹⁾	Current output (message type)	Note
Fxxx	≥ 21.0 mA or ≤ 3.6 mA	xxx = three-digit number
Mxxx	corresponding to measuring mode	xxx = three-digit number
Cxxx	corresponding to measuring mode	xxx = three-digit number
Sxxx	corresponding to measuring mode	xxx = three-digit number

1) The error codes are listed in the Operating Instructions.

Exceptions:

Error code ¹⁾	Current output (message type)	Note
C484	≥ 21.0 mA or ≤ 3.6 mA	Failure mode simulation

1) The error codes are listed in the Operating Instructions.

5.2 Device configuration for safety-related applications

It is recommended to carry out a factory reset before configuring the parameters.

Navigate to: Setup → Advanced setup → Administration

Device reset = To factory defaults

This resets all parameters to defined values.

5.2.1 Calibration of the measuring point

Calibration of the measuring point is described in the Operating Instructions (→  9).

Specify which type of configuration a) or b) should be used. Both configurations can be operated in parallel.

- a) Analog input (source) (1) -> safety-related signal: analog output (2)
- b) Analog input (source) (1) -> safety-related signal: digital output (3)

Analog input (source) (1)

Make sure that the correct source is configured (Analog I/O B1-3 or Analog I/O C1-3).

Navigate to: Setup → Advanced setup → Input/output → Analog I/O

Setting

- **Operating mode** = 4..20mA input or HART master+4..20mA input
- **Analog input 0% value** must be set correctly.
- **Analog input 100% value** must be set correctly.

Analog output (2)

Make sure that the correct output is configured (Analog I/O B1-3 or Analog I/O C1-3).

Navigate to: Setup → Advanced setup → Input/output → Analog I/O

Setting

- **Operating mode** = 4..20mA output or HART slave +4..20mA output
- **Analog input source** = AIO B1-3 value mA or AIO C1-3 value mA (depending on the source)
- **0 % value**
- **100 % value**
- **Used for SIL/WHG** = Enabled

Digital output (3)

First select an alarm block (Alarm 1, Alarm 2, Alarm 3 or Alarm 4) for the limit value settings.

Navigate to: Setup → Advanced setup → Application → Alarm 1 → Alarm X

Setting

- **Alarm mode** = On
- **Alarm value source** = AIO B1-3 value mA or AIO C1-3 value mA (depending on the source)
- **HH alarm value, H alarm value, L alarm value and LL alarm value** must be configured in line with the application such that the valid range is within the HH, H and L, LL limits.

Make sure that the correct output is configured (Digital A1-2, Digital A3-4, Digital B1-2, Digital B3-4, Digital C1-2, Digital C3-4, Digital D1-2, Digital D3-4).

Navigate to: Setup → Advanced setup → Input/output → Digital Xy-z

Setting

- **Operating mode** = Output passive
- **Digital input source** = selected alarm block (**Alarm 1 any, Alarm 2 any, Alarm 3 any or Alarm 4 any**)
- **Used for SIL/WHG** = Enabled must be set to use this digital output as a SIL output.

5.2.2 Configuration method

When the devices are used in safety instrumented systems, the device configuration must meet two requirements:


- **Confirmation concept:**
Proven, independent testing of safety-related parameters entered.
- **Locking concept:**
Locking of the device following parameter configuration (IEC 61511-1: 2016 Section 11.6.3).

To activate SIL mode, the device must run through an operating sequence, during which the device can be operated via the device display or any asset management tool (e.g., FieldCare) for which integration is available.


"Expert mode"



A larger number of safety-related parameters can be freely configured here.

A detailed description of the configuration steps is provided in the following section.

 Only in the case of SIL devices (order code 590 "Additional Approval", option LA "SIL") is the SIL commissioning sequence visible on the display and in external operating tools. For this reason, SIL locking can only be activated on these devices.


Locking in "Expert mode"

To commission the device, carry out and document the following steps in the order shown →  25:

1. Perform parameter configuration, see also →  14: The parameter configuration procedure as well as the meaning of the individual parameters are described in the Operating Instructions. The parameter settings in the following table must be observed →  18.
2. Start the SIL confirmation sequence.
Navigate to: Setup → Advanced setup → SIL/WHG confirmation
Set write protection = Enter the relevant locking code (SIL: 7452). Press "Next" to confirm.
3. Press "Next" to confirm **Commissioning = Expert mode**. The device checks the parameter settings in accordance with the following table and forces the switching of parameters if necessary.
When the check is finished, **SIL preparation = Finished** is shown. The commissioning sequence can be continued.
Press "Next" to confirm.
4. Perform function test: For MIN and MAX monitoring, at least one current input value above (MAX monitoring) or below (MIN monitoring) the switch point must be approached.
For range monitoring, 5 current input values should be approached which cover the entire measuring range. In doing so, check that the safety-related signal (current output/relay) responds correctly in each case.
5. Confirm that the function test has been successful:
Confirm function test = Yes.
6. **Set write protection** = Enter the locking code again (SIL: 7452). Check the locking status after performing SIL locking.
Navigate to: Setup → Advanced setup
Locking status = SIL locked must be confirmed by selecting "✓".
7. As an option, hardware locking can also be activated (via the dip switch marked "WP" on the main electronics).

Further parameter settings


The following parameters affect the safety function. However, they may be freely configured in accordance with the application:

 It is recommended to note down the configured values!

Parameter	Parameter name
Current input measurement: Setup → Advanced setup → Input/output → Analog I/O	0 % value
	100 % value

The following parameters affect the safety function and are not freely configurable in Expert mode. Instead, they are automatically set by the device to the safety-related values mentioned at the start of SIL confirmation:

Parameter	Preset value
Setup → Advanced setup → Input/output → Digital A1-2 → Contact type	Normally closed
Setup → Advanced setup → Application → Alarm 1 → Alarm X → Error value	All alarms
Setup → Advanced setup → Application → Alarm 1 → Alarm X → Alarm mode	On
Diagnostics → Simulation → Current output 2 simulation	Off
Expert → Input/output → Analog I/O → Error on event	Any error
Expert → Input/output → Analog I/O → Output out of range	Alarm
Expert → Input/output → Digital A1-2 → Error on event	Any error
Expert → Input/output → Digital A1-2 → Output simulation	Disable

 Those parameters which are not mentioned do not affect the safety function and can be configured to any meaningful values. The visibility of the parameters mentioned in the operating menu depends in part on the user role, the SW options ordered and on the configuration of other parameters.

Unlocking a SIL device

When SIL locking is active on a device, the device is protected against unauthorized operation by means of a locking code and, as an additional option, by means of a hardware write protection switch. The device must be unlocked to change parameter configuration.

CAUTION

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

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

To unlock, proceed as follows:

1. Check the position of the hardware write protection switch (dip switch marked "WP" on the main electronics), and set this switch to "OFF".
2. Select the sequence "Setup → Advanced setup → Deactivate SIL/WHG" and enter the corresponding unlocking code (SIL: 7452) for the **Reset write protection** parameter.
 - ↳ The "End of sequence" message indicates that the device was successfully unlocked.

5.3 Proof testing

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

The values and graphics in the "Additional safety-related characteristics" section can be used for this purpose → 6. The test must be carried out in such a way that it verifies the correct operation of the safety instrumented system in interaction with all of the components.

i In a single-channel architecture, the PFD_{avg} value to be used depends on the proof test's diagnostic coverage (PTC = Proof Test Coverage) and the intended lifetime (LT = Lifetime), as specified in the following formula:

$$PFD_{avg} = \frac{1}{2} \cdot PTC \cdot \lambda_{DU} \cdot T_1 + \lambda_{DD} \cdot MTTR + \frac{1}{2} \cdot (1 - PTC) \cdot \lambda_{DU} \cdot LT$$

A0024244

The individual proof test coverages that can be used for calculation are specified for the proof tests described below. The proof test coverage depends on the test sequence.

A test sequence for the proof test must be carried out for the safety function used.

Safety function (current input measurement)		PTC
	Test sequence A – Feed-in real currents	99 %

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

⚠ CAUTION

Ensuring process safety

► During the proof test, alternative monitoring measures must be taken to ensure process safety.

i If one of the test criteria from the following test sequence 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 (λ_{du}). The impact of systematic failures on the safety function is not covered by this test and must be assessed separately. Systematic failures can be caused, for example, by substance properties, operating conditions, buildup or corrosion.

5.3.1 Test sequence A (Feed in real currents)

Preparation

1. Point level monitoring and range monitoring can also be performed when the SIL mode is active.
2. If the safety-related "Analog" signal is used, connect a suitable measuring device (recommended accuracy better than ± 0.1 mA) in the installed circuit.
3. If the safety-related "Digital" signal is used, connect a suitable measuring device (resistance tester/resistance measurement), (recommended accuracy better than ± 0.1 Ω) to the digital output.
4. Determine the safety setting (point level or range monitoring).

Procedure for point level monitoring (current)

1. Input a current directly below (MAX monitoring) or directly above (MIN monitoring) the current limit value to be monitored (e.g. by simulation on a connected device).
2. Read the output current (mA), record it and assess for accuracy.
3. Read the relay switch status (Ω), record it and assess for accuracy.
4. Enter a current directly above (MAX monitoring) or directly below (MIN monitoring) the current limit value to be monitored.
5. Read the output current (mA), record it and assess for accuracy.
6. Read the relay switch status (Ω), record it and assess for accuracy.

The test has been passed successfully if the current and the relay switch status trigger the safety function in steps 5 and 6 only, and not in steps 2 and 3.

Procedure for range monitoring (current)

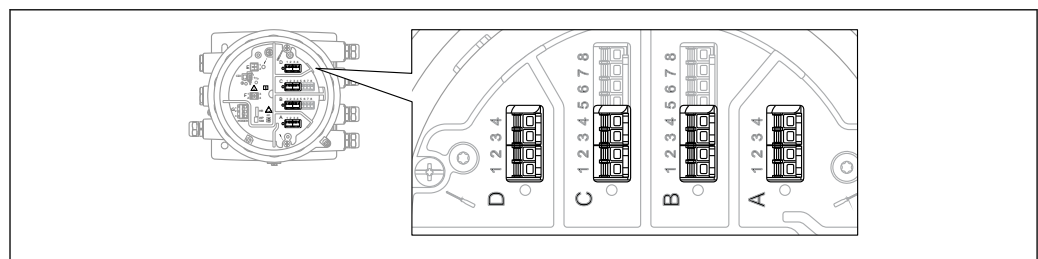
1. Input five current values within the range to be monitored (e.g. by simulation on a connected device).
2. For every current value, read the output current (mA) and the switch status of the relay (Ω), record them and assess for accuracy.

The test has been passed successfully if the current values and the switch status of the relay in step 2 are within the required accuracy limits.

Relay self-monitoring

Relay self-monitoring must only be performed if the "Digital" safety-related signal is used.

Example of terminal designation: If the Digital IO module used for the safety function is installed in slot D and contacts 3 and 4 are used, Digital D3-4 must be used instead of Digital Xy-z below.



A0033370

1. Deactivate SIL mode. Navigate to: Setup → Advanced setup → Deactivate SIL/WHG and enter the relevant unlocking code (SIL: 7452) for the **Reset write protection** parameter.

2. Perform the device self-check as follows. Navigate to: Setup → Advanced setup
3. Set: **Input/output = Digital Xy-z**
4. Check whether **Contact type = Normally closed** (SIL factory setting).
5. Set: **Output simulation = Simulating inactive.**
6. Check whether the contact is closed (resistance $< 1 \Omega$) between contacts Xy and Xz.
7. Set: **Output simulation = Fault 1.**
8. Check whether the contact is open (resistance $> 1 M\Omega$) between contacts Xy and Xz.
9. Set: **Output simulation = Simulating inactive.**
10. Check whether the contact is closed (resistance $< 1 \Omega$) between contacts Xy and Xz.
11. Set: **Output simulation = Fault 2.**
12. Check whether the contact is open (resistance $> 1 M\Omega$) between contacts Xy and Xz.
13. Set: **Output simulation = Simulating active.**
14. Check whether the contact is open (resistance $> 1 M\Omega$) between contacts Xy and Xz.
15. Set: **Output simulation = Disable.**
16. Reactivate SIL mode as per "Device configuration for safety-related applications"
→ 15, points 3, 4, 6, 7, 8 only. (All other requirements in this section have been implemented in the context of (initial) commissioning/configuration or in the context of this proof test.)

The test has been passed successfully if the relay resistance values in steps 6-15 are within the required level of accuracy.

End of test sequence A



- The device has failed the proof test if the expected current value/relay resistance values at a specific level deviate by $> \pm 2 \%$. For troubleshooting, refer to the Operating Instructions → 9. This test detects 99 % of dangerous, undetected failures (proof test coverage, PTC = 0.99).
- If the "Expert" menu group is selected, a prompt for the access code appears on the display. If an access code has been defined under Setup → Advanced setup → Administration → Define access code this code must be entered here. If no access code was defined, the prompt can be acknowledged by pressing the "E" key.

6 Life cycle

6.1 Requirements for personnel


The personnel for installation, commissioning, diagnostics, repair and maintenance must meet 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 beginning work, the specialist staff must have read and understood the instructions in the manuals and supplementary documentation as well as in the certificates (depending on the application)
- Follow instructions and comply with basic conditions


The operating personnel must meet 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


6.2 Installation

The installation of the device is described in the relevant Operating Instructions (→  9).

6.3 Commissioning

The commissioning of the device is described in the relevant Operating Instructions (→  9).

6.4 Operation

The operation of the device is described in the relevant Operating Instructions (→  9).

6.5 Maintenance

Please refer to the relevant Operating Instructions for information on maintenance and recalibration, (→  9).



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

6.6 Repair



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

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:

Component	Checking the device after repair
I/O module Mainboard Front plane assembly, labeled	<ul style="list-style-type: none"> Visual inspection to check whether all parts are present and properly mounted. Proof test, test sequence A
Cover, aluminum, sight glass Cover lock O-ring, housing	<ul style="list-style-type: none"> Visual inspection to check whether all parts are present and properly mounted. Check the measurement at an arbitrary level.
Electronic box, complete	<ul style="list-style-type: none"> Visual inspection to check whether all parts are present and properly mounted. Proof test, test sequence A
Housing filter	Visual inspection to check whether all parts are present and properly mounted
SD card with holder	Visual inspection to check whether all parts are present and properly mounted.
Display set Display holder, fixing ring	Visual inspection to check whether all parts are present and properly mounted.
Terminal set, push-in Terminal set, screw type	Visual inspection to check whether all parts are present and properly mounted.

Installation Instructions: see the Downloads area on 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 safety instrumented 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 safety instrumented system" when returning the defective device. Please refer to the "Return" section in the Operating Instructions (→ 9).

6.7 Modification

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

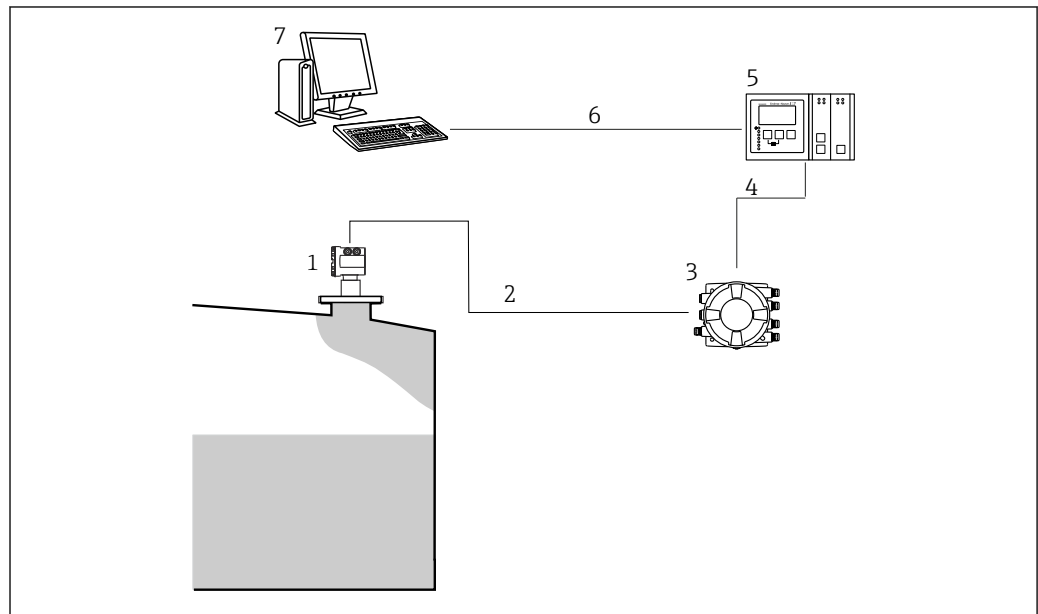
- Modifications to devices with SIL capability are usually performed in the Endress+Hauser manufacturing center.
- Modifications to devices with SIL capability onsite at the user's plant are possible following approval by the Endress+Hauser manufacturing center. In this case, the modifications must be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

7 Appendix

7.1 Structure of the measuring system

7.1.1 System components

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



A0033366

- 1 Level radar
- 2 4-20 mA HART
- 3 Tankside monitor
- 4 Fieldbus (e.g. Modbus, V1)
- 5 Tankvision Tank Scanner NXA820
- 6 Ethernet
- 7 Computer with Fieldcare

7.1.2 Description of use as a safety instrumented system

The tankside monitor is a field device for the integration of tank sensors into tank inventory systems. It enables access to all connected tank sensors. All measured and calculated values can be displayed at the on-site display. They can be transferred to an inventory control system via a field communication protocol.

The device can be used in this arrangement in safety instrumented systems for MIN safety, MAX safety and range monitoring.



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

7.2 Proof testing

System-specific data	
Company	
Measuring point/TAG no.	
Facility	
Device type/Order code	
Device serial number	
Name	
Date	
Access code (if individual to each device)	
Locking code used	SIL <input type="checkbox"/> 7452
Signature	

Device-specific commissioning parameters	
Tube diameter (liquid measurement; pipe/bypass)	
Empty calibration	
Full calibration	

Proof test protocol		
Test step	Target value	Actual value
1. Current value 1		
2. Current value 2		
3. Current value 3 (if necessary)		
4. Current value 4 (if necessary)		
5. Current value 5 (if necessary)		
Resistance value		

7.3 Notes on the redundant configuration 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 in the table below are minimum values for the device. These must be used when designing the sensor subsystem.

Minimum value β with homogeneous redundant use	5%
Minimum value β_D with homogeneous redundant use	2%

The device meets the requirements for SIL 3 in homogeneously redundant applications.

Please note the following when carrying out the proof test: If an error is detected in one of the redundantly operated devices, the other devices must be checked to see if the same error occurs.

7.4 Further information



General information on functional safety (SIL) is available at:

www.de.endress.com/SIL (Germany) or www.endress.com/SIL (English) and in the Competence Brochure CP01008Z/11 "Functional Safety in the Process Industry- Risk Reduction with Safety Instrumented Systems".



www.addresses.endress.com
