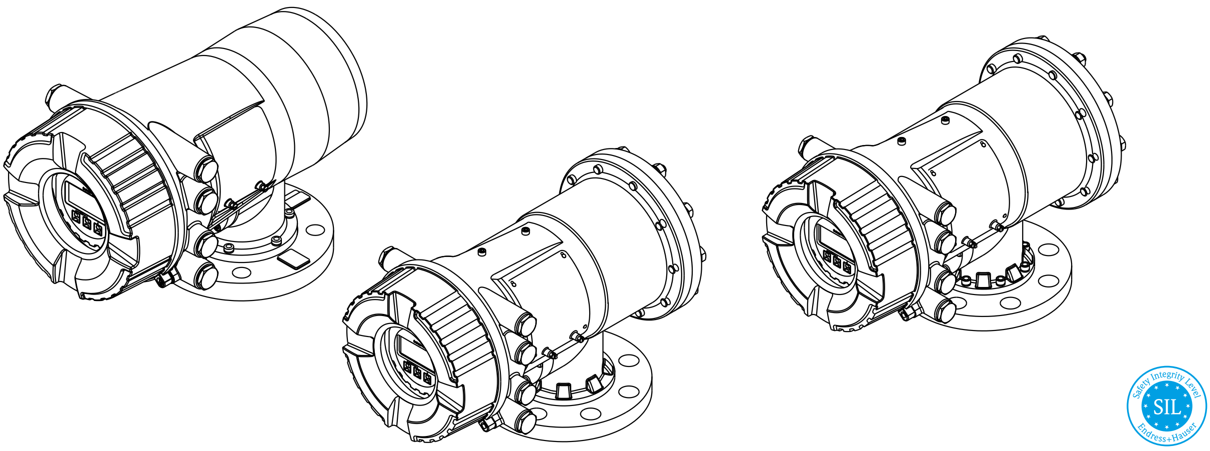
SD01920G/00/EN/04.20
71501458
2020-10-07

Special Documentation
Proservo NMS80/81/83

Functional Safety Manual



Intelligent tank gauge for high-precision measurement of the level of liquids with a 4 to 20 mA output signal and switch output

Endress+Hauser
People for Process Automation

Table of contents

Declaration of Conformity

SIL_00326_02.20

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

Proservo NMS80/81/83

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, 31-July-2020
Endress+Hauser SE+Co. KG

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

A0044238

SIL_00326_02.20

Endress+Hauser
People for Process Automation

General

Device designation and permissible types	Level servo, Proservo NMS8x - ************+LA		
	x = 0,1,3		
Safety-related output signal a) b)	a) 4...20 mA	b) relay contact	
Fault signal a) b)	a) ≤ 3.6 mA ; ≥ 21 mA	b) open contact	
Process variable/function	Level measurement, Current in measurement		
Safety function(s)	MIN, MAX, Range		
Device type acc. to IEC 61508-2	☐ Type A	☒ Type B	
Operating mode	☒ Low Demand Mode	☒ High Demand Mode	☐ Continuous Mode
Valid hardware version	As of manufacturing date after Nov.28,2016		
Valid software version	As of 01.02.zz (zz: any double number)		
Safety manual	SD01920G		
Type of evaluation (check only one box)	☒	Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	☐	Evaluation of "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 IEC 61508-2 for devices w/o software	
Evaluation through – report/certificate no.	TÜV Rheinland Industrie Service GmbH-report no. 968/FSP 1687.00/18		
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 2 capable	☐ SIL 3 capable
	Multi channel use (HFT 1)	☐ SIL 2 capable	☒ SIL 3 capable

FMEDA

Safety function	MIN	MAX	Range
λ_{DU} 1),2)	196 FIT	196 FIT	196 FIT
λ_{DD} 1),2)	6095 FIT	6095 FIT	6095 FIT
λ_{SU} 1),2)	2529 FIT	2529 FIT	2529 FIT
λ_{SD} 1),2)	23 FIT	23 FIT	23 FIT
SFF	97 %	97 %	97 %
PFD_{avg} (T_1 = 1 year) 2) (single channel architecture)	9.06×10^{-4}	9.06×10^{-4}	9.06×10^{-4}
PFD_{avg} (T_1 = 2 years) 2) (single channel architecture)	1.76×10^{-3}	1.76×10^{-3}	1.76×10^{-3}
PFH	1.96×10^{-7} 1/h	1.96×10^{-7} 1/h	1.96×10^{-7} 1/h
PTC 3)	Depending on the proof test, see safety manual	Depending on the proof test, see safety manual	Depending on the proof test, see safety manual
λ_{total} 1,2)	8842 FIT	8842 FIT	8842 FIT
Diagnostic test interval 4)	60 min	60 min	60 min
Fault reaction time 5)	1 min	1 min	1 min

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
4) All diagnostic functions are performed at least once within the diagnostic test interval
5) Maximum time between error recognition and error response

A0044239

Other safety-related characteristic values

Characteristics as per IEC 61508	Value
MTBF [1]	29 Jahre
System reaction time as per DIN EN 61508-2	In "Expert mode": User configurable

1) According to Siemens SN29500. This value takes into account failure types relevant to the function of the electronic components.

Useful lifetime of electric 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.

Certificate

Certificate

No.: 968/FSP 1687.00/18

Product tested	Tank Gauging Proservo	**Certificate holder**	Endress+Hauser SE + Co. KG Hauptstraße 1 79689 Maulburg Germany

Type designation NMS8x [x = 0,1,3]

Codes and standards IEC 61508 Parts 1-7:2010

Intended application The devices comply with the requirements of Hardware Safety Integrity SIL 2 and Systematic Capability SC 3 acc. to IEC 61508 and can be used in applications up to SIL 2 (HFT=0) resp. SIL 3 (HFT=1) for following safety functions:
- Safe detection of a level (min, max, range) within the measuring range, accuracy of ±2%;
- Safe current in measurement (min, max, range) within the measuring range, accuracy of ±1%;
with safe analogue and/or digital outputs.

Specific requirements The instructions of the associated Operating Manual and Safety Manual shall be considered.

Valid until 2023-07-05

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1687.00/18 dated 2018-07-05.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2018-07-05

Certification Body Safety & Security for Automation & Grid

Dr.-Ing. Thorsten Gantevoort

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

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

TÜVRheinland®
Precisely Right.

A0037374

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

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
A0011193	**Tip** Indicates additional information.
	Reference to documentation
	Reference to page
	Reference to graphic
1., 2., 3....	Series of steps

Symbols in graphics

Symbol	Meaning
1, 2, 3,...	Item numbers
1., 2., 3....	Series of steps
A, B, C, ...	Views

Supplementary device documentation

Documentation	Comment
Technical Information: ▪ TI01248G/00 (NMS80) ▪ TI01249G/00 (NMS81) ▪ TI01250G/00 (NMS83)	The documentation is available on the Internet: → www.endress.com
Operating Instructions ▪ BA01456G/00 (NMS80) ▪ BA01459G/00 (NMS81) ▪ BA01462G/00 (NMS83)	The documentation is available on the Internet: → www.endress.com
Brief Operating Instructions: ▪ KA01200G/00 (NMS80) ▪ KA01203G/00 (NMS81) ▪ KA01206G/00 (NMS83)	▪ 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. The supplementary device documentation must be observed during installation, commissioning and operation. The requirements specific to the protection function are described in this Safety Manual.

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 functions. A modification process according to IEC 61508 is applied for device changes.

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
080	Process pressure	All
090	Electrical connection	All
110	Measuring range; wire; diameter	All except Y
120	Displacer material; type	All except Y
130	Process seal	All
140	Process 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 SIL-enabled SW is supplied. Alternatively, the following SW version may be selected: 01.02.zz or 01.03.zz
895	Marking	All

1) An additional selection of further versions is possible.

Order code	040	050	060
Option	E1	*	*
	H1	*	*
	*	A1	*
	*	A2	*
	*	B1	*
	*	B2	*
	*	C2	*
	*	*	A1
	*	*	A2

Order code	040	050	060
	*	*	A3
	*	*	B2
	*	*	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)

SIL label on the nameplate

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

Safety function

Definition of the safety function

The device's safety functions are:

Safety function 1 (level measurement)
- Maximum point level monitoring (overfill protection)
- Minimum point level monitoring (dry run protection)
- Level range monitoring

The safety functions comprise the measurement of the level of a liquid.

Safety function 2 (current input measurement)
Current input monitoring

The safety function comprises the measurement of the current of a connected device.

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 level value (safety function 1: level measurement) or the analog input current (safety function 2: current input measurement) are 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:
- Exceed and/or undershoot a specific level limit.
- The occurrence of a fault, e.g. contact open (interruption of the signal line).

In case of fault 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.

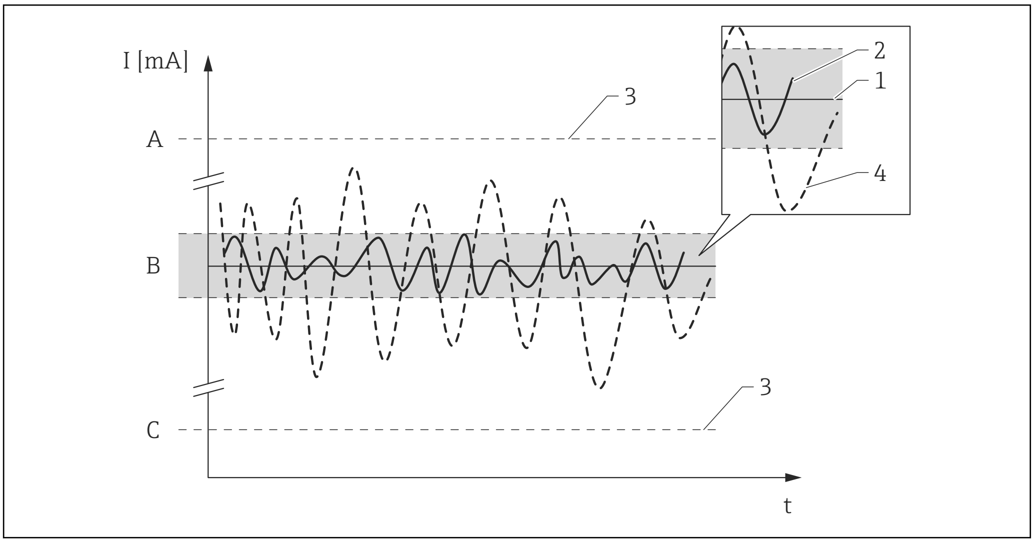
The safety-related output signal is fed to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter where it is monitored for the following:
- Exceed and/or undershoot a specific level limit.
- The occurrence of a fault, e.g. failure current (≤3.6 mA, ≥21.0 mA), interruption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

In case of fault it must be ensured that the equipment under control achieves or maintains a safe state.

Restrictions for use in safety-related applications

- The measuring system must be used correctly for the specific application, taken into account the medium properties and ambient conditions. Carefully follow instructions pertaining to critical process situations and installation conditions from the Operating Instructions. The application-specific limits must be observed.
- Information on the safety-related signal, (→ 🖹 10).
- The specifications from the Operating Instructions must not be exceeded, (→ 🖹 8).
- The following restrictions also applies to 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. It includes all influential factors described in the Technical Information (e.g. non-linearity, non-repeatability, hysteresis, zero drift, temperature drift, EMC influences).
    According to IEC / EN 61508 the safety related failures are classified into different categories, 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	Implications for the measuring uncertainty (Position, see figure. → 🖹 11)
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, → 🖹 13)	3 No implications
λ_{SU}	Safe undetected: Safe failure which cannot be detected	Is within the defined error range	2 May be beyond the specification
λ_{DD}	Dangerous detected: Dangerous failure which can be detected (Diagnostic within the device)	Causes the output signal to signal the failsafe mode (see, → 🖹 13)	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



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

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.

Use in safety instrumented systems

Device behavior during operation

Digital

Device behavior during power-up

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, no communication is possible via the service interface (CDI) or via protocols (HART, V1, Modbus).

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.

Device behavior in 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.

Alarm and warning messages

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

Device behavior during power-up

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, no communication is possible via the service interface (CDI) or via protocols (HART, V1, Modbus).

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.

Device behavior in event of alarms and warnings

The output current on alarm can be set to a value ≤3.6 mA or ≥21.0 mA.

In some cases e.g. failure of power supply, cable open circuit and faults in the current output itself, where the failure current ≥21.0 mA cannot be output, output currents ≤3.6 mA occur irrespective of the failure current defined.

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 level for signal on alarm (≥21.0 mA) and of the lower level for signal on alarm (≤3.6 mA).

Alarm and warning messages

Additional information is provided by the alarm and warning messages in the form of error codes and associated clear 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	Simulation failure mode

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

Parameter configuration for safety-related applications

It is recommended to carried out factory reset before setting the parameters.

Navigate to: Setup → Advanced setup → Administration

Device reset = **To factory defaults**

This resets all parameters to defined values.

Calibration of the measuring point - safety function 1 (level measurement)

The calibration of the measuring point is described in the Operating Instructions (→ 📄 8).

Specify which type of configuration a) or b) should be used. Both configurations can apply in parallel or in combination with safety function 2 (current input measurement).

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

Level value (source) (1)

Make sure that the application is configured correctly.

Navigate to: Setup

Setting
- **Level source** = **Level**
- **Empty** and**Tank reference height** must be set correctly.
- **High stop level** and**Low stop level** must be set correctly.

Navigate to: Setup → Gauge command

Setting
Gauge command = **Level**

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** = **Tank level**
- **0 % value** must be set correctly.
- **100 % value** must be set correctly.
- **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 → Alarm X

Setting
- **Alarm mode** = **On**
- **Alarm value source** =**Tank level** (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.

Calibration of the measuring point - safety function 2 (current input measurement)

The calibration of the measuring point is described in the Operating Instructions (→ 🗎 8).

Specify which type of configuration c) or d) should be used. Both configurations can apply in parallel or in combination with safety function 1 (level measurement).

c) Analog input (source) (1) -> safety-related signal: analog output (2)
d) 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 → 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.

Configuration method

When using the devices in process control safety systems, the device configuration must comply with 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. This means that the device can be adapted to difficult applications. However, the settings must be checked by directly approaching the level in the tank or by applying a comparable method.

A tank with liquid can be used for example as a method for checking in the case of MAX monitoring.

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

It is only in the case of SIL devices (ordering feature 590 "Additional Approval", option LA "SIL") that the SIL commissioning sequence is 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 (→ 34):

1. Carry out configuration, see also → 14.
   The configuration procedure and the meaning of the individual parameters are described in the Operating Instructions (→ 8). Comply with the parameter settings in the following table (→ 18) .
2. Start the commissioning check and ensure that the distance between the level and reference position is at least 500 mm (19.7 in).
   Navigate to: Diagnostics → Device check → Commissioning check
   Commissioning check = **Start** (for more information, see Operating Instructions → 8).
   A commissioning check is carried out. The device's sensor calibration is checked and any installation errors are detected.
3. Set Proservo to the "Level" gauge command.
   Navigate to: Operation → Gauge command
   Gauge command = **Level**
   Proservo returns to level mode. Depending on the tank height and the previous position of the displacer, wait for a sufficient period of time until the displacer reaches the level surface.
4. Start the SIL confirmation sequence.
   Navigate to: Setup → Advanced setup → SIL/WHG confirmation
   SIL/WHG confirmation = **Set write protection** and enter the relevant locking code (SIL: 7452).
   Press "Next" to confirm.
5. Press "Next" to confirm **Commissioning** = **Expert mode**.
   The device checks the parameter settings in accordance with the following table (→ 18) and forces the switching of parameters if necessary.
   SIL preparation = **Finished** is shown when the check is finished. The commissioning sequence can be continued. Press "Next" to confirm.

6. Carry out function test.
For MIN and MAX monitoring, at least one level/current input value above (MAX monitoring) or below (MIN monitoring) the switch point must be approached.
For range monitoring, 5 level values/current input values which cover the entire measuring range should be approached. In doing so, check that the safety-related signal (current output/relay contact) responds correctly in each case.

   If it is not possible to approach the required level values, perform a test in accordance with test sequence C → 25 prior to locking. However, this does not detect all possible errors (e.g. insufficient adjustment). For this reason, we recommend that the measured values be tested and documented in accordance with test sequence A → 21 at the point in time when the required point levels/levels are reached. In accordance with IEC 61508-1:2010, Section 7.14, this test is included in the "Overall safety validation" and is the responsibility of the operator.

7. Confirm that the function test has been successful.
Confirm function test = **Yes**.

8. **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 "✓".

9. 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
Setup	Upper density
Setup	Process condition
Setup	High stop level
Setup	Low stop level
Setup	Empty
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
Operation → Gauge command → Gauge command	Level
Setup → Advanced setup → Input/output → Digital input mapping → Digital input source 1	None
Setup → Advanced setup → Input/output → Digital input mapping → Digital input source 2	None
Setup → Advanced setup → Input/output → Digital Xy-z → Contact type	Normally closed
Setup → Advanced setup → Input/output → Digital Xy-z → Output simulation	Disable
Setup → Advanced setup → Application → Tank calculation → HyTD → HyTD mode	No
Setup → Advanced setup → Application → Tank calculation → CTSh → CTSh mode	No
Setup → Advanced setup → Application → Alarm → Alarm X → Error value	All alarms
Setup → Advanced setup → Application → Alarm → Alarm X → Alarm mode	On
Setup → Advanced setup → Safety settings → Output out of range	Alarm
Diagnostics → Simulation → Simulation distance on	Off
Diagnostics → Simulation → Current output 1 simulation	Off
Expert → Input/output → Digital Xy-z → Error on event	Any error
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 → Analog I/O → Feedback threshold	1 s

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 in order to change the configuration for proof tests as per test sequence A → 21, test sequence B → 23or test sequence C → 27.

⚠ 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**.
   ↳ The "End of sequence" message indicates that the device was successfully unlocked.

Proof testing

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

The values and graphics in the "Additional safety-related characteristics" section can be used for this purpose (→ 🗎 5). 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.

In a single-channel architecture, the PFD_{avg} value to be used depends on the diagnostic rate of coverage for the proof test (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 rates depend on the specific test sequence.

A test sequence for the proof test must be selected from the following table for every safety function used. If both safety functions are used, two test sequences must be performed for the proof test.

Safety function 1 (level measurement)		PTC
	Test sequence A – Approach the level	99%
	Test sequence B – Simulation of the level	91%
	Test sequence C – Simulation of the level and single-point verification of the level	97%
Safety function 2 (current input measurement)		
	Test sequence D – Feed in real currents	99%

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

⚠ CAUTION

To ensure process safety.

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

If one of the test criteria from the following test sequences 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 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.

Test sequence A (Approach the level)

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 "Digital" safety-related 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

1. Check safety function: Approach at least one level immediately above (MAX monitoring) or below (MIN monitoring) the point level to be monitored.
2. Check safety function: Read the output current (mA)/relay resistance value (Ω), record it and assess for accuracy.
3. If (as an option) the function of the measuring point is to be checked immediately in front of the switch point: Checks the function in front of MIN or MAX switch point: Approach level immediately below (MAX monitoring) or above (MIN monitoring) the point level to be monitored. Read the output current/relay resistance value, record it and assess for accuracy. This does not check the safety function of the device.

The test has been passed successfully if the current values/relay resistance values trigger or ensure the required function.

Procedure for range monitoring

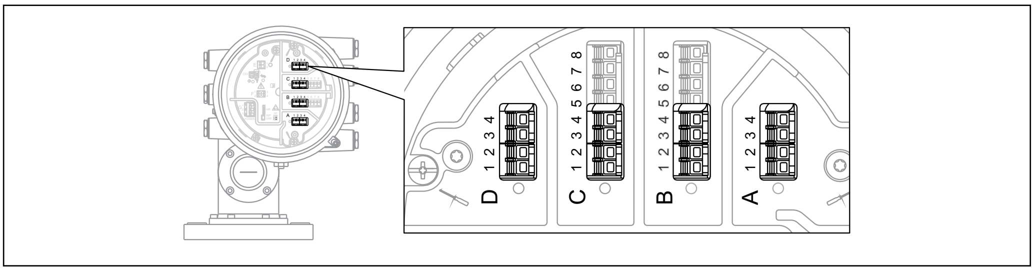
1. Approach five levels within the range to be monitored.
2. For every level value, read the output current (mA)/relay resistance value (Ω), record it and assess for accuracy.

The test has been passed successfully if the current values/relay resistance values in step 2 are within the required level of accuracy.

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.



A0032860

1. Deactivate SIL mode. Navigate to: Setup → Advanced setup → Deactivate SIL/WHG and enter the corresponding 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 Ω) between contacts Xy and Xz.
7. Set: **Output simulation** = **Fault 1**.

8. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
9. Set: **Output simulation** = **Simulating inactive**.
10. Check whether the contact is closed (resistance <1 Ω) between contacts Xy and Xz.
11. Set: **Output simulation** = **Fault 2**.
12. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
13. Set: **Output simulation** = **Simulating active**.
14. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
15. Set: **Output simulation** = **Disable**.
16. Reactivate SIL mode as per "Device configuration for safety-related applications" → 📄 14, only points 4, 5, 7, 8, 9. (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 value at a specific level deviates by > ±2 %. For troubleshooting, refer to the Operating Instructions (→ 📄 8). 99 % of dangerous, undetected failures are detected using this test (proof test coverage, PTC = 0.99).

Test sequence B (simulate the level)

Preparation

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

1. Navigate to: Expert → Sensor → Sensor diag
2. Set: **Start self check** = **Yes**. If the self check is successful, the following appears: **Result self check**= **Ok**.
   ↳ The self check has been passed.
3. Navigate to: Diagnostics → Simulation
4. Set: **Simulation distance on** = **On**. Simulate a level directly below (MAX monitoring) or directly above (MIN monitoring) the level limit to be monitored. To simulate the level, you must calculate the level to the distance (value entered) (level = empty - distance).
5. Read the output current (mA), record it and assess for accuracy.
6. Read the state of the relay contact (Ω), record it and assess for accuracy.
7. Simulate a level directly above (MAX monitoring) or directly below (MIN monitoring) the level limit.
8. Read the output current (mA), record it and assess for accuracy.
9. Read the state of the relay contact (Ω), record it and assess for accuracy.

The test has been passed successfully if the current values and the state of the relay contact trigger the safety function in step 7 only, and not in step 4.

Procedure for range monitoring

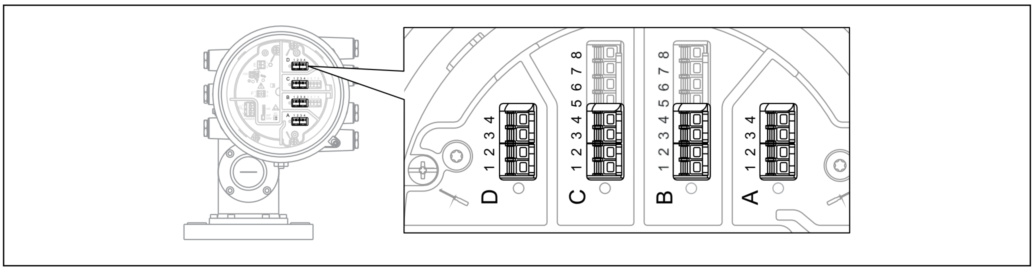
1. Navigate to: Expert → Sensor → Sensor diag → Start self check
2. Set: **Start self check** = **Yes**. If the self check is successful, the following appears: **Result self check**= **Ok**
   ↳ The self check has been passed.
3. Simulate five levels within the range to be monitored. See the procedure for point level monitoring, steps 3 and 4.
4. For every level 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 4 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.



A0032860

1. Deactivate SIL mode. Navigate to: Setup → Advanced setup → Deactivate SIL/WHG and enter the corresponding 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 Ω) between contacts Xy and Xz.
7. Set: **Output simulation** = **Fault 1**.
8. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
9. Set: **Output simulation** = **Simulating inactive**.
10. Check whether the contact is closed (resistance <1 Ω) between contacts Xy and Xz.
11. Set: **Output simulation** = **Fault 2**.
12. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
13. Set: **Output simulation** = **Simulating active**.
14. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
15. Set: **Output simulation** = **Disable**.
16. Reactivate SIL mode as per "Device configuration for safety-related applications" → 📄 14, only points 4, 5, 7, 8, 9. (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 B

- The device has failed the proof test if the expected current value/relay resistance values at a specific level deviate by > ±2 %. For troubleshooting, refer to the Operating Instructions (→ 📄 8). 91 % of dangerous, undetected failures are detected using this test (proof test coverage, PTC = 0.88).
- 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.

Test sequence C (simulation and single-point level detection)

Preparation

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

1. Navigate to: Expert → Sensor → Sensor diagnostics
2. Set: **Start self check** = **Yes**. If the self check is successful, the following appears: **Result self check**= **Ok**.
   ↳ The self check has been passed.
3. Read the actual measured value displayed by the device at any level within the measuring range, e.g. the current level, or determine the actual output current and compare it with the set point defined by the current level.
   ↳ This part of the test is deemed successful if the values are within the required level of accuracy.
4. Navigate to: Diagnostics → Simulation
5. Set: **Simulation distance on** = **On**. Simulate a level directly below (MAX monitoring) or directly above (MIN monitoring) the level limit to be monitored (**Simulation distance** = corresponding value).
6. Read the output current (mA), record it and assess for accuracy.
7. Read the state of the relay contact (Ω), record it and assess for accuracy.
8. Simulate a level directly above (MAX monitoring) or directly below (MIN monitoring) the level limit.
9. Read the output current (mA), record it and assess for accuracy.
10. Read the state of the relay contact (Ω), record it and assess for accuracy.

The device has passed the test if the current values and the state of the relay contact trigger the safety function in step 8 only, and not in step 5.

Procedure for range monitoring

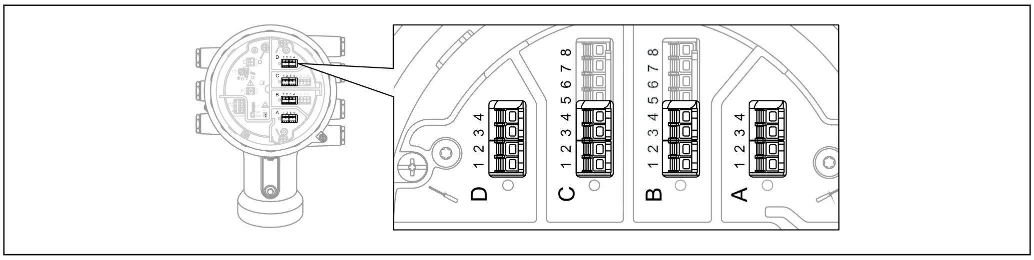
1. Navigate to: Expert → Sensor → Sensor diagnostics
2. Set: **Start self check** = **Yes**. If the self check is successful, the following appears: **Result self check**= **Ok**.
   ↳ The self check has been passed.
3. Read the actual measured value displayed by the device at any level, e.g. the current level, within the measuring range, or determine the actual output current and compare it with the set point defined by the current level.
   ↳ This part of the test is deemed successful if the values are within the required level of accuracy.
4. Simulate five levels within the range to be monitored. See the procedure for point level monitoring (level), steps 4 and 5.
5. For every level 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 5 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.



A0032388

1. Deactivate SIL mode. Navigate to: Setup → Advanced setup → Deactivate SIL/WHG and enter the appropriate 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 Ω) between contacts Xy and Xz.
7. Set: **Output simulation** = **Fault 1**
8. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
9. Set: **Output simulation** = **Simulating inactive**
10. Check whether the contact is closed (resistance <1) between contacts Xy and Xz.
11. Set: **Output simulation** = **Fault 2**
12. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
13. Set: **Output simulation** = **Simulating inactive**
14. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
15. Set: **Output simulation** = **Disable**
16. Reactivate SIL mode as per "Device configuration for safety-related applications" → 📄 14, only points 4, 5, 7, 8, 9. (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 C

- The device has failed the proof test if the expected current value/relay resistance value at a specific level deviates by >±2 %. For troubleshooting, refer to the Operating Instructions→ 📄 8. 95 % of dangerous, undetected failures are detected using this test (Proof test coverage, PTC = 0.95).
- 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 must be entered here. If no access code was defined, the prompt can be acknowledged by pressing the "E" key.

Test sequence D (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 "Digital" safety-related 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)

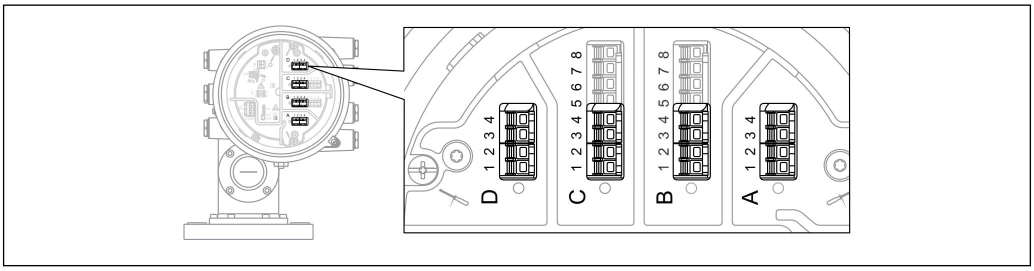
1. Input five current values within the range to be monitored (e.g. by simulation on a connected device).
2. For every current value, read the output current (mA) and the switch status of the relay (Ω), record them and assess for accuracy.

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.



A0032860

1. Deactivate SIL mode. Navigate to: Setup → Advanced setup → Deactivate SIL/WHG and enter the corresponding 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 Ω) between contacts Xy and Xz.
7. Set: **Output simulation** = **Fault 1**.

8. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
9. Set: **Output simulation** = **Simulating inactive**.
10. Check whether the contact is closed (resistance <1 Ω) between contacts Xy and Xz.
11. Set: **Output simulation** = **Fault 2**.
12. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
13. Set: **Output simulation** = **Simulating active**.
14. Check whether the contact is open (resistance >1 MΩ) between contacts Xy and Xz.
15. Set: **Output simulation** = **Disable**.
16. Reactivate SIL mode as per "Device configuration for safety-related applications" → 14, only points 4, 5, 7, 8, 9. (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 D

- The device has failed the proof test if the expected current value/relay resistance values at a specific level deviate by > ±2 %. For troubleshooting, refer to the Operating Instructions (→ 8). 99 % of dangerous, undetected failures are detected using this test (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.

Life cycle

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

Installation

The installation of the device is described in the relevant Operating Instructions (→ 🗎 8).

Commissioning

The commissioning of the device is described in the relevant Operating Instructions (→ 🗎 8).

Operation

The operation of the device is described in the relevant Operating Instructions (→ 🗎 8).

Maintenance

Please refer to the relevant Operating Instructions for information on maintenance and recalibration, (→ 🗎 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. We recommend documenting 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, labelled	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Proof test; test sequence A or B.
Cover, aluminum, sight glass Cover clamp O-ring, housing	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Check the measurement at an arbitrary level.
Electronic box, complete	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Proof test; test sequence A or B.
Housing filters	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. ▪ Proof test; test sequence A or B.
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.
Detector unit, servo	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).
Mainboard cable to the electronics, servo	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Proof check; test sequence A or B
Sensor module, servo	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).
Measuring drum bracket	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ When removing the measuring drum: Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).
Bearing, measuring drum bracket, PTFE	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).
Measuring wire and or wire ring	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).
Cover, drum housing	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Check the measurement at an arbitrary level.
Cover, calibration window/ blind window cover	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Check the measurement at an arbitrary level.

Component	Checking the device after repair
Displacer	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).
Measuring drum	▪ Visual inspection to check whether all parts are present and properly mounted. ▪ Calibration must be carried out again (see Operating Instructions). ▪ Repeat the device commissioning check (Diagnostics → Device check).

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 protective system" when returning the defective device. Please refer to the "Return" section in the Operating Instructions (→ 📄 8).

Modification

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

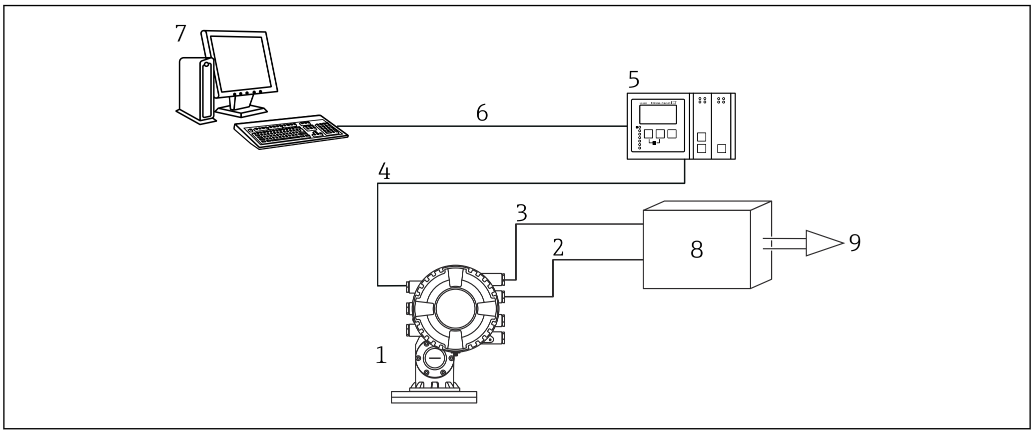
- ▶ Modifications to devices with SIL capability are usually performed in the Endress+Hauser manufacturing center.
- ▶ Modifications to devices with SIL capability onsite at the user's plant are possible following approval by the Endress+Hauser manufacturing center. In this case, the modifications must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

Appendix

Structure of the measuring system

System components

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



A0032783

1 Proservo NMS80/81/83
2 4 to 20 mA line
3 Switch output
4 Fieldbus (e.g. Modbus, V1)
5 Tankvision Tank Scanner NXA820
6 Ethernet
7 Computer with Fieldcare
8 Logic Unit, e.g. PLC, limit signal transmitter
9 Actuator

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 predefined limit value.

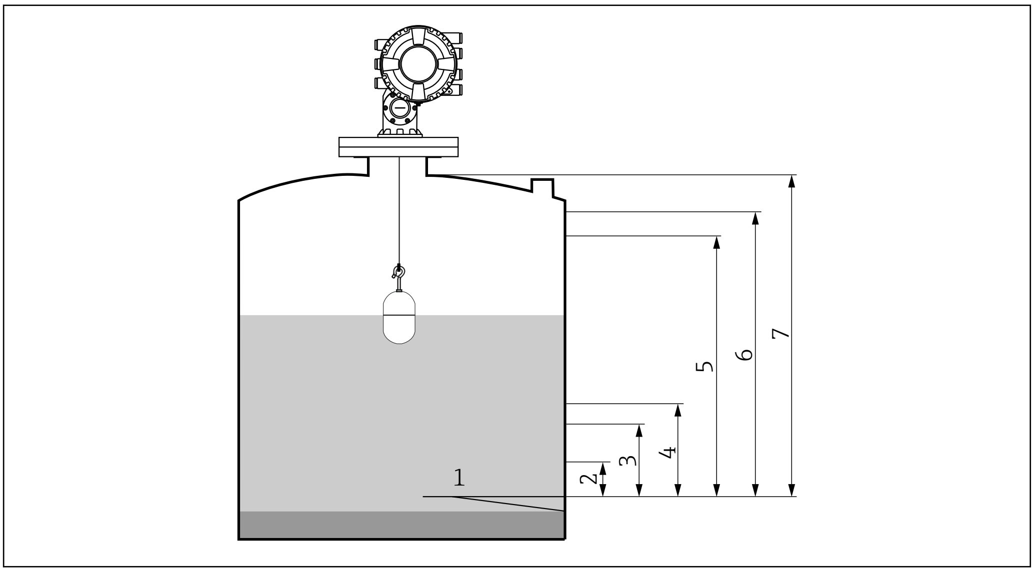
The relay contact is opened if a set level is exceeded or undershot, and if errors are detected. For fault monitoring, the logic unit must recognize an open contact. The current output follows the level. If errors are detected, a failure current is output.

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 Proservo is a high-precision, intelligent tank gauging device. It operates based on the principle of displacement. A small displacer is accurately positioned in the liquid using a multiphase motor. The displacer is suspended from a measuring wire which is wound onto a drum. The device counts the drum rotations in order to determine the measuring distance.

Typical measuring arrangement



A0032821

1 *Datum plate: reference point of the measurement*
2 *Low stop*
3 *4 mA, 0%*
4 *L or LL alarm*
5 *H or HH alarm*
6 *20 mA, 100%*
7 *High stop*

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.

Proof testing

System-specific data	
Company	
Measuring point/TAG no.	
Facility	
Device type/Order code	
Serial number of device	
Name	
Date	
Access code (if individual to each device)	
Locking code used	SIL ❑ 7452
Signature	

Device-specific commissioning parameters	
Upper density	
Process condition	
High stop level	
Low stop level	
Empty	
Tank reference height	

Proof test protocol		
Test step	Set point	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		

Notes on the redundant configuration of multiple sensors

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

The common cause factors ß and $ß_D$ indicated in the table below are minimum values for the device. These must be used when designing the sensor subsystem.

Minimum value ß with homogeneous redundant use	5%
Minimum value $ß_D$ with homogeneous redundant use	2%

The device meets the requirements for SIL 3 in homogeneous redundancy.

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.

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".

71501458

www.addresses.endress.com

Endress+Hauser

People for Process Automation