SD00337G/08/EN/02.16
71328224

Functional Safety Manual Proservo NMS5/NMS7

Tank gauge for Liquid level measurement with 4 to 20mA Output or with Alarm Relay Contact Output

Application

Operating minimum (e.g. dry run protection), maximum (e.g. overfill protection) and range monitoring (4 to 20 mA only) of liquids of all types in systems to satisfy particular safety systems requirements as IEC 61508/IEC61511.

The measuring device fulfills the requirements concerning

- Functional safety as per IEC 61508/IEC61511
- Explosion protection (depending on the version)
- Electro magnetic compatibility as per EN 61326
- Electrical safety as per IEC/EN 61010-1

Features and benefits

- Level monitoring (MIN, MAX, range) by 4 to 20 mA or level alarm (MIN, MAX) by relay output up to SIL 2
  - Independently assessed by TUV Nord as per IEC 61508/IEC61511
- Continuous self monitoring
- Continuous measurement

Endress+Hauser
People for Process Automation

Table of contents

Important document information

Notes on safety conventions and symbols

Symbols for Safety Conventions

Symbol	Meaning
 A0011189-EN	**DANGER!** This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.
 A0011190-EN	**WARNING!** This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.
 A0011191-EN	**CAUTION!** This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.
 A0011192-EN	**NOTICE!** This symbol contains information on procedures and other facts which do not result in personal injury.

Symbols for Certain Types of Information

Symbol	Meaning
 A0011182	**Allowed** Indicates procedures, processes or actions that are allowed.
 A0011183	**Recommendation** Indicates procedures, processes or actions that are recommended.
 A0011184	**Forbidden** Indicates procedures, processes or actions that are forbidden.
 A0011193	**Tip** Indicates additional information.

SIL Declaration of conformity

Endress+Hauser
People for Process Automation

SIL-16001

SIL Declaration of Conformity

Functional Safety according to IEC 61508

Endress+Hauser Yamanashi Co., Ltd.
862-1 Mitsukunugi, Sakaigawa-cho, Fuefuki-shi,
Yamanashi Prefecture, 406-0846 Japan

Declares as manufacturer, that the level gauge
Proservo NMS

is suitable for the use in safety-instrumented system according to IEC 61508 / IEC 61511, if the functional safety manual SD00337G/08 and following characteristics are observed:

Product	**Analogue output 4 to 20 mA**	**Alarm relay contact output**
Safety functions	Level Range, Error related to level measurement	Level MAX, Level MIN, Error related to level measurement
SIL [3]	2	
HFT	0	
Device type	Type B	
SFF	94%	95%
PFD_{avg} (T_i = 1 year)	3.63×10^{-4}	2.71×10^{-4}
Proof test interval	Recommended: 2 year	
λ_S [1]	679.19 FIT	635.33 FIT
λ_D [1]	679.19 FIT	635.33 FIT
λ_{DU} [1]	82.97 FIT	61.77 FIT
MTBF [2]	84 years	89 years

[1] according to Siemens SN29500
[2] according to Siemens SN29500, including faults outside the safety function
[3] consideration according to IEC 61511-1 clause 11.4.4

The device, including software and the modification process, was passed on the basis of proven-in-use.

Yamanashi, 1 June 2016
Endress+Hauser Yamanashi Co.,Ltd.

(General Manager)

Introduction

General information on functional safety (SIL)is available at: www.endress.com/SIL (German) or www.endress.com/SIL (English) and in Competence Brochure CPZ002Z “Functional Safety in the Process Industry. Risk Reduction with Safety Instrumented Systems”.

Structure of the measuring system

System configuration

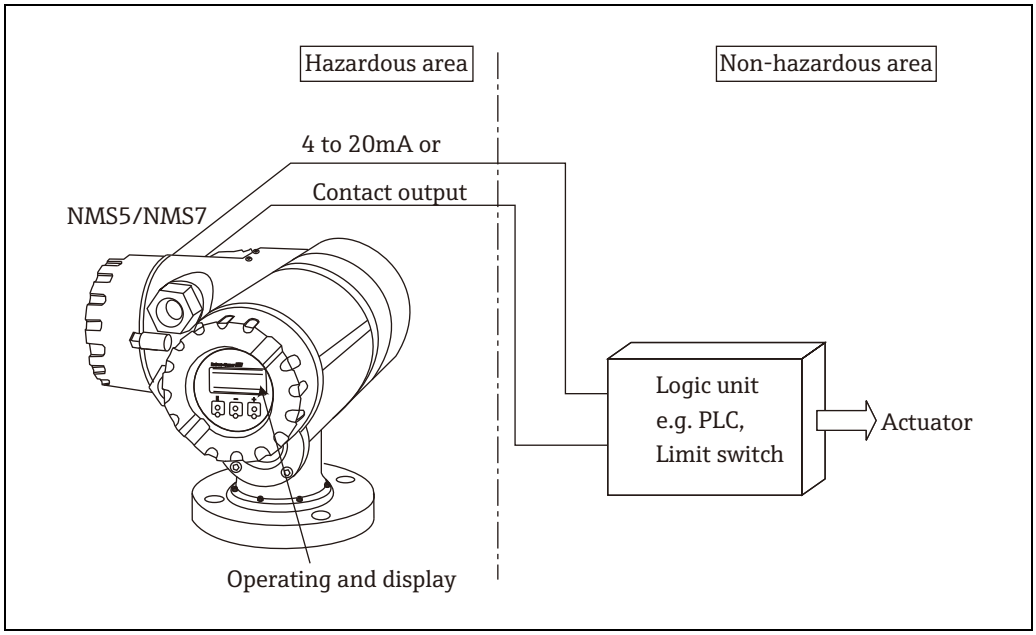

Figure 1: System configuration

Proservo has following safety-related output options that can be used alternatively:

The analog output (4 to 20 mA) in proportion to the level is generated in the Proservo. This is sent to a downstream logic unit (e.g. PLC, limit signal transmitter, etc.) where it is monitored to determine whether it is below or above a specified value.
When Proservo detects an error, the analog output module will output 22mA.

The alarm relay contact output module will set the relay, when overshooting or undershooting a specified level and/or Proservo detected errors. This is sent to a downstream logic unit (e.g. PLC, limit signal transmitter, etc.) where it is monitored to determine whether it is ON or OFF in a specified condition.

Description of use as a protective system

Principle

The Proservo NMS is based on the principle of displacement measuring.
A small displacer is accurately positioned in the liquid medium using servo motor. The displacer suspended on a measuring wire which is wound onto a finely grooved drum housing the instrument.

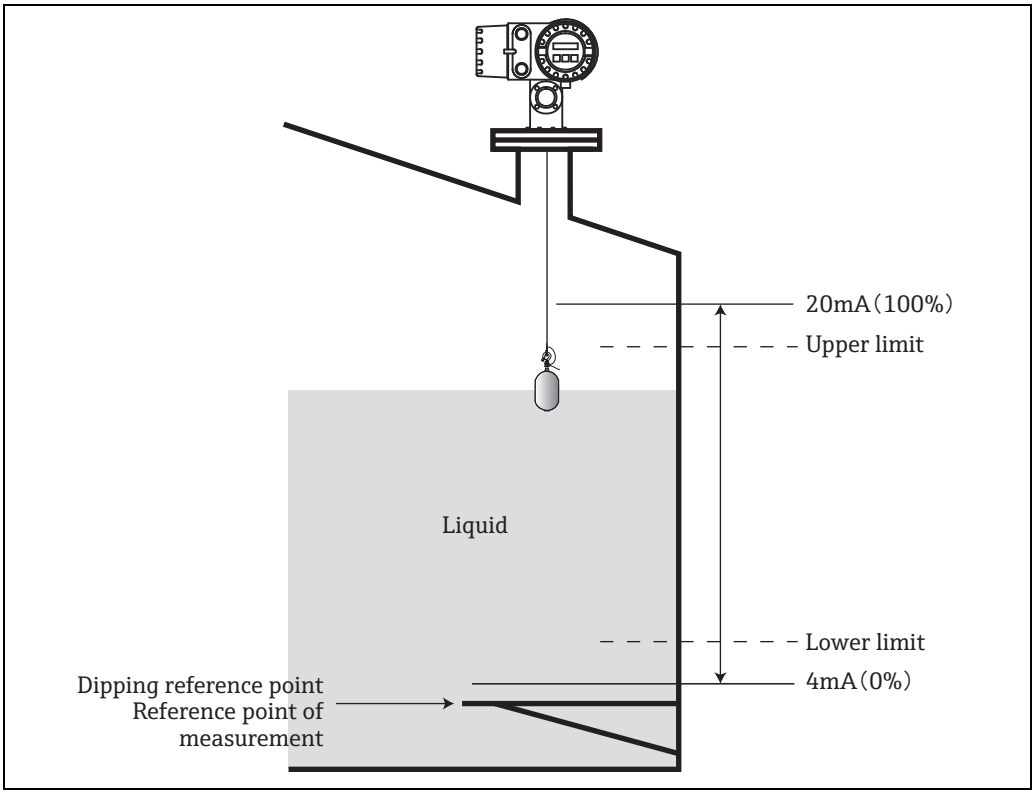

Figure 2: Analog output 4 to 20 mA

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

In this case, the device must be parameterized as follows;

- GVH158 [PRO SAFETY] setting must be "ON".
- GVH250[ASSIGN OUTPUT 1] and /or GVH253[ASSIGN OUTPUT 2] setting must be "LEVEL".

- When Proservo detects an error, the analog output module will output 22mA.
- If GVH158 [PRO SAFETY] setting “OFF”, the current version (Non-SIL approved version) conditions are applied. To enable the SIL function, set the items correctly.

Alarm relay contact output

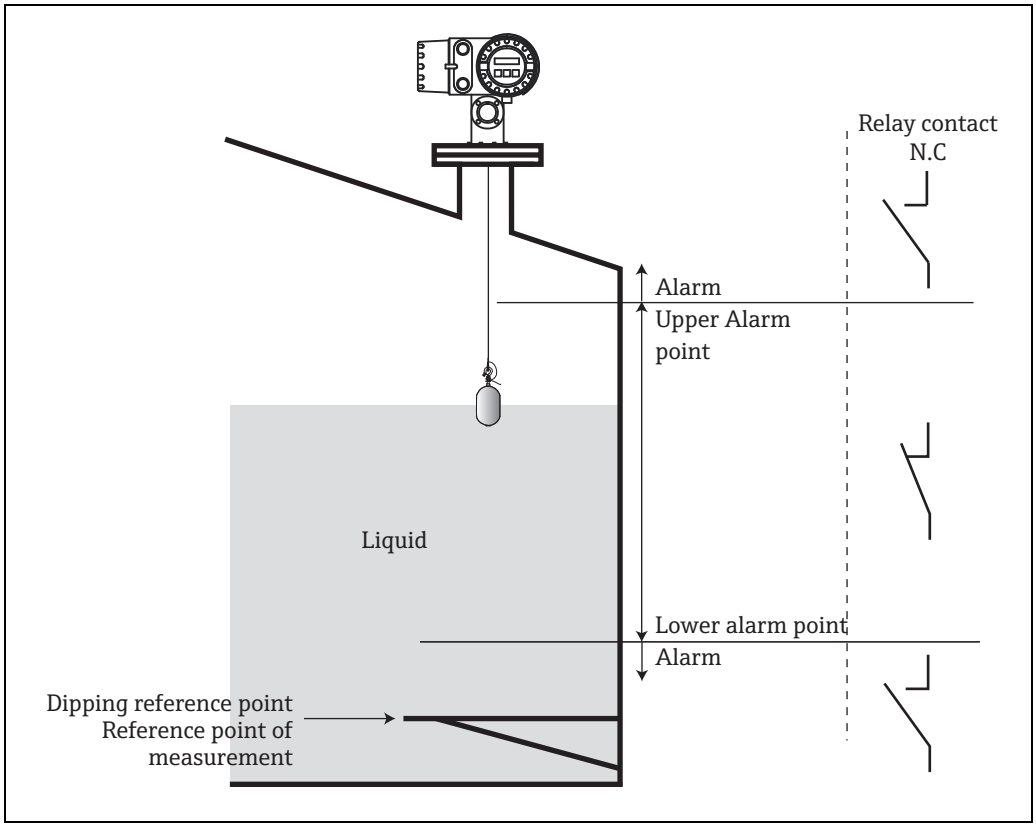

Figure 3: Overspill prevention version

N.C.:
Normally Close the contact at normal operation.
Abnormal operation: under/over the setting level or failure regarding to level measurement.
In this case, the device must be parameterized as follows;

- GVH158 | PRO SAFETY | setting must be "ON".
- GVH241| ASSIGN RELAY | setting must be "LEVEL".

- When Proservo detects an error, I/O-3 (OSP) will set the relays.
- If GVH158 | PRO SAFETY | setting “OFF”, the current version (Non-SIL approved version) conditions are applied. To enable the SIL function, set the items correctly.

Contactable load:
Overspill Prevention version has 2 contact outputs which loads are switched via single floating change-over contact (SPST).
The operator must use suitable measures (e.g. current limiter, fuse) to ensure the relay contact characteristics are not exceeded to each contact: Umax. 200V DC or peak AC, Imax. 0.5A DC or peak AC, Pmax. 15W/VA

Permitted device type

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

Valid device versions or types for safety-related use as follows.

- Feature: a specific letter or digit in the Product specification code.
- Designation: description of a functional category that includes 1 or more variants
- Version: permissible variants represented by a digit or letter.

Proservo NMS5		
Feature	**Designation**	**Version**
010	Pressure rating, Drum chamber material	All
020	Protection class	All
030	Measuring function	All
040	Primary (Digital) output	All
050	Secondary output	2, 3, 4, 5 (*1)
060	Signal input from field units	All
070	Measuring range, Wire material	All
080	Cable entry	All
090	Process connection	All
100	Power supply	All
110	Displacer shape diameter; material	All
120	O-ring; chamber finishing	All
130	Options	All

Proservo NMS7		
Feature	**Designation**	**Version**
010	Protection class	All
020	Measuring function	All
030	Primary (Digital) output	All
040	Secondary output	2, 3, 4, 5 (*1)
050	Signal input from field units	All
060	Measuring range, Wire material	All
070	Cable entry	All
080	Process connection	All
090	Power supply	All
100	Displacer shape diameter; material	All
110	O-ring; chamber finishing	All
120	Nozzle	All
130	Options	All

(1*) safety output 4 to 20mA only
Valid software version: as of 4.27F or later.
Valid hardware version: as of delivery date 18 May 2011.

Secondary output	Safety output
2	4 to 20mA only
3	4 to 20mA only
4	Relay output
5	4 to 20mA only

Supplementary device documentation

Documentation	Contents	Comments
Technical Information TI00452G/08	Function and system design Application Selection Input Output Auxiliary energy Performance characteristics Operating conditions: Environment Operating condition: Process Mechanical construction Human interface Advanced Maintenance Certificates and Approval Ordering information Accessories Supplementary Documentation Appendix	The documentation is available on the Internet. → www.endress.com
Operating Instructions BA00401G/08	Safety Instructions Identification Installation Mounting Wiring Operation Commissioning Maintenance Accessories Diagnosis and Troubleshooting Displacer and Measuring wire Technical data Matrix Appendix	The documentation is supplied with the device. The documentation is also available on the Internet. → www.endress.com
Safety Instructions XA00578G-A/08 [ATEX) XA00582G-A/08 [IECEx] Ex421-439 (FM) Ex540-742 (CSA)	Safety, installation and operating instructions for devices, which are suitable for use in potentially explosion atmospheres.	Safety instructions is depending on the certification. ATEX and IECEx version are supplied with all devices. FM and CSA version are supplied with Ex d[ia] (XP-AIS) version only.

Description of the safety requirements and boundary contents

Safety function

Analog output 4 to 20 mA as safety-related signal

The measuring system's safety functions are:

- Maximum level limit monitoring (overfill protection)
- Minimum level limit monitoring (dry run protection)
- Level range monitoring

The safety-related output signal is fed to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter where it is monitored for the following;

- Overshooting and/or undershooting a specified level limit.
- The occurrence of a fault, e.g. error current (< 4 mA or > 20 mA, interruption or short circuit of the signal line).

Alarm relay contact output as safety-related signal

The measuring system's safety functions are:

- Maximum level limit monitoring (overfill protection)
- Minimum level limit monitoring (dry run protection)

The safety-related output signal is fed to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter where it is monitored for the following;

- Overshooting and/or undershooting a specified level limit, relay open.
- The occurrence of a fault, relay open.

Function safety indicators

Analog output 4 to 20 mA

Characteristic as per IEC 61508	Proservo NMS5/NMS7 with 4 to 20 mA
Safety functions	Range, error related to level measurement
SIL	2
HFT	0
Device type	Type B
Mode of operation	Low demand mode
SFF	94%
λ_S	679.19 FIT
λ_D	679.19 FIT
λ_{DU}	82.97 FIT
PFH [1/h]	8.30×10^{-8}
PFD_{avg} for T_i = 1 year	3.63×10^{-4}
MTBF	84 years
Recommended time interval for proof-testing T_i	2 year
System reaction time	240 ms

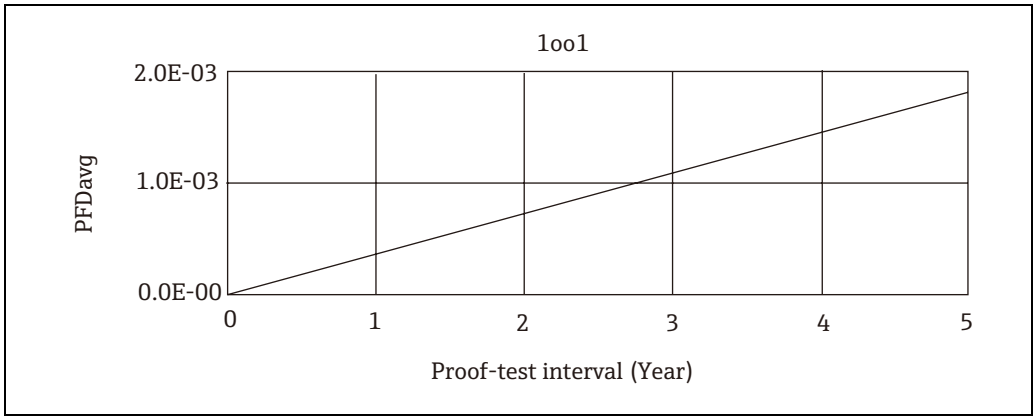

Figure 4: Graph

Dangerous undetected failures in this scenario

An incorrect output signal that deviates from the real measured value by more than 0.3%, but is still in the range of 4 to 20 mA, is considered a dangerous, undetected failure.

Useful lifetime of electrical components

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

Alarm relay contact output

Characteristic as per IEC 61508	Proservo NMS5/NMS7 with 4 to 20 mA
Safety functions	MAX, MIN, error related to level measurement
SIL	2
HFT	0
Device type	Type B
Mode of operation	Low demand mode
SFF	95%
λ_S	635.33FIT
λ_D	635.33FIT
λ_{DU}	61.77FIT
PFH [1/h]	$6.18x10^{-8}$
PFD_{avg} for T_i = 1 year	$2.71x10^{-4}$
MTBF	89 year
Recommended time interval for proof-testing T_i	2 year
System reaction time	240ms

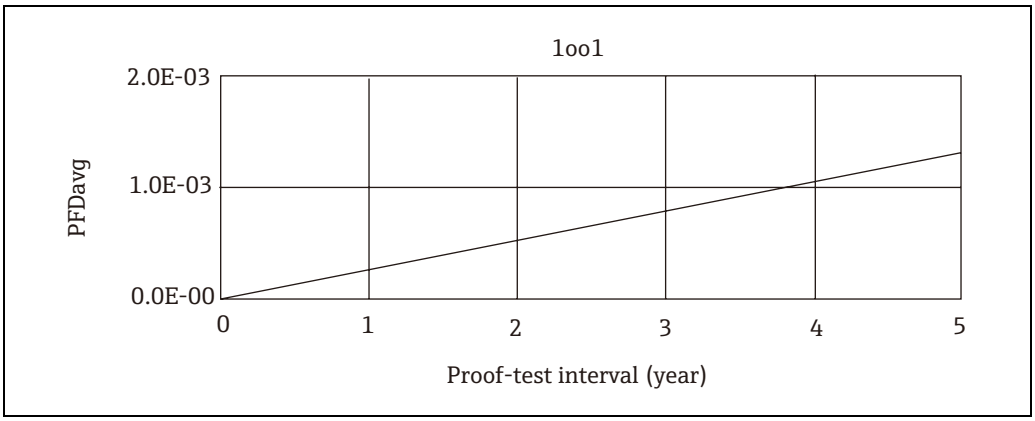

Figure 5: Graph2

Dangerous undetected failures in this scenario
An incorrect output signal that deviates from the real measured value by more than 1mm, but is still in the alarm set point, is considered a dangerous, undetected failure.

Useful lifetime of electrical components
The established failure rates of electrical components apply within the useful lifetime as per IRC 61508-2, section 7.4.9.5 note 3.

Device operation status in operation or in case of error

Behavior of device during power-up
The safe 4 to 20mA output signal and the safe relay contact output signal are available after 10 s after the device is switched on or when the voltage returns.

Device response in the event of device alarms or warning

- 4 to 20 mA
  In the event of device alarm, the output current is 22 mA.

In some cases (e.g. failure of power supply, a cable open circuit and fault in the current output itself, where the error current 22 mA can not be set), output current less than 4 mA or more than 20 mA irrespective of the configured error current (22 mA) can occur.

For alarm monitoring , the logic unit must therefore be able to recognize both HI-alarms (>20 mA) and LOalarms (< 4 mA).

- Relay contact output
  – Overspill Prevention version
  In the event of device alarm, status of the relay contact output moves to open (refer to “Description of use as a protective system/ Alarm Relay Contact output/Overspill Prevention version”).
  In case of power loss, the relay contact output moves to open.

In some cases (e.g. a cable short circuit and fault in the alarm contact output itself, where the error status can not be set), contact output status irrespective of the configured error status occur.

- Alarm and warning message
  Additional information is available in the form of error code on the alarm and warning messages output (refer to “Supplementary device documentation” for details).

Installation

Installation and wiring

Installation and wiring of the device is described in the accompanying Operating Instructions (refer to “Supplementary device documentation” for details).

Commissioning

Commissioning of the device is described in the accompanying Operating Instructions (refer to “Supplementary device documentation” for details).

Proactive Safety Function must be enabled.
If Service Mode [GVH157] is ON and/or Prosafety [GVH158] is OFF, it must be switched as follows;

Service Mode [GVH157]
Open the matrix GVH157, set to “OFF”

Prosafety [GVH158]
Open the matrix GVH158, set to “ON”
Service Mode [GVH157] select ON only when performing maintenance on the Proservo.

Operation

Calibration of the liquid level
Calibration of the liquid level is described in the Operation Instructions (refer to “Supplementary device documentation” for details).

The method of device configuration
Calibrate the liquid level value after initial settings. Usually initial settings are only one time when Proservo NMS is first installed on the tank. Initial settings are described in the Operation Instructions (refer to “Supplementary device documentation” for details).

Method of setting liquid level value may differ according to tank operation conditions. Details are shown in the Operation Instructions (refer to “Supplementary device documentation” for details).

Maintenance

Refer to the relevant Operating Instructions (refer to “Supplementary device documentation” for details). Alternative monitoring measures must be taken to ensure process safety during configuration, proof-testing and maintenance work on the device.

If Service Mode [GVH157] set ON when performing maintenance, it must be switched to OFF when maintenance is finished, and before device is put back into normal operation (refer to “Commissioning”).

Proof-test

Description of the proof-test

Check the operativeness and safety of safety functions at appropriate intervals.
The operator must determine the time intervals (refer to the diagram “Proof-test interval”).
Proof-testing of the device can be performed as follows;

- Check the set value for the alarms.
- Confirm the alarm condition of each set point (input a dummy level value).

Process for proof-test

Analog output 4 to 20mA

1. Confirm the analog output settings in matrix GVH250/251/252/253/254/255.
2. Input a simulation level point to matrix GVH251 (SIM, RELAY, OUT)
3. Confirm output to alarm on the connected external device (e.g. DCS, alarm receiver and/or etc.)

NOTICE The proof-test is deemed to have failed if the expected current value deviates for specific level by > +/-0.3%.

When performing a proof test, record the confirmed test results according to Appendix parts A1 to A5 and B1 to B5 respectively. The recorded data and test results must be stored in a safe place (refer to proof test protocol).

Contact relay output

1. Confirm the relay output settings in matrix GVH241/242/243/245.
2. Input a simulation level point to matrix GVH248 (SIM, RELAY, OUT).
3. Confirm output to alarm on the connected external device (e.g. DCS, alarm receiver and/or etc.).

NOTICE The proof-test is deemed to have failed if the relay does not change the state (refer to proof test protocol).

When performing a proof test, record the confirmed test results according to Appendix parts C1 to C7 and D1to D7 respectively. The recorded data and test results must be stored in a safe place.

⚠ WARNING The Proservo NMS is either an Ex d or Ex d[ia] device. The covers (terminal compartment and/or any electric compartment) must not be open while power is supplied to Proservo NMS (including proof-test). Turn off the power before opening the cover.

When performing a proof-test and the cover(s) is opened, the proof-test should be performed in a non-hazardous area.

Maintenance

Repairs

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

Exception

The following components can be replaced by the customer if the person responsible for doing so has been trained beforehand by Endress+Hauser.

- Display module
- Fuse and lightning arrestor on the terminal board
- O-rings on drum housing cover, terminal cover, display cover, calibration window
- Measuring wire, wire drum and displacer

The replaced components must be sent to Endress+Hauser for the purpose of fault analysis.
Once the components have been replaced, a proof-test must be carried out performed as per test sequence.

In the event of failure of a SIL-labeled Endress+Hauser device, which has been operated in a protection function, the “Declaration of Contamination” with the corresponding note “Used as SIL device in protection system” must be enclosed when the defective device is returned. Refer to the Section “Return” in the Operating Instructions (refer to “Supplementary device documentation” for details).

Appendix

Communication or proof-test protocol

System-specific data		
Company		
Measuring points / Tag No.		
System		
Device type / Order code	NMS53_/ NMS_-_	
Serial number of device		
Name		
Data		
Signature		
Device-specific commissioning data		
Empty calibration		
Full calibration		
Proof test protocol		
Test stage	Set point/Preset	Actual value
A. Analog output 4 to 20mA (1)		
A1. Assign output 1 [GVH250]	☐None ☐ Level ☐Liquid Temp.	
A2. Set value of 0% [GVH251]	mm	-
A3. Set value of 100% [GVH252]	mm	-
A4. Set point for test (1)	mm	mA
A5. Set point for test (2)	mm	mA
B. Analog output 4 to 20mA (2)		
B1. Assign output 1 [GVH253]	☐None ☐ Level ☐Liquid Temp.	
B2. Set value of 0% [GVH254]	mm	-
B3. Set value of 100% [GVH255]	mm	-
B4. Set point for test (1)	mm	mA
B5. Set point for test (2)	mm	mA
C. Relay contact output (1)	[GVH240 set to 1]	
C1. Assign relay [GVH241]	☐ Level ☐Caution ☐Warning ☐Emergency ☐Liquid Temp.	
C2. Relay function [GVH242]	☐High. ☐Low	-
C3. Switching point [GVH243]	mm	-
C4. Relay ON alarm [GVH245]	☐N.O. ☐N.C.	-
C5. Set point for test (1)	mm	Alarm: ☐ON ☐OFF
C6. Set point for test (2)	mm	Alarm: ☐ON ☐OFF
C7. Set point for test (3); if necessary	mm	Alarm: ☐ON ☐OFF
D. Relay contact output (2)	[GVH240 set to 2]	
D1. Assign relay [GVH241]	☐ Level ☐Caution ☐Warning ☐Emergency ☐Liquid Temp.	
D2. Relay function [GVH242]	☐High. ☐Low	-
D3. Switching point [GVH243]	mm	-
D4. Relay ON alarm [GVH245]	☐N.O. ☐N.C.	-
D5. Set point for test (1)	mm	Alarm: ☐ON ☐OFF
D6. Set point for test (2)	mm	Alarm: ☐ON ☐OFF
D7. Set point for test (3); if necessary	mm	Alarm: ☐ON ☐OFF

Test of the relay contact must apply when “Assign relay” preset equal “Level”, “Caution”, “Warning”, “Emergency Error”

*1: Service Mode must be OFF at normal operation.
*2: PROSAFETY must be ON at normal operation.

Definitions and abbreviations

Items	Descriptions
OSP	Overspill Prevention software version
I/O-3	Electronics module containing relay outputs
I/O-5	Electronics module containing analog output 4 to 20mA
Matrix	Refers to the organization of configuration parameters in the Proservo software. Detail is shown in the Operation Instructions (refer to “Supplementary device documentation” for details)
GVH	Refers to the location of configuration parameters in the Proservo software. G: Group describes a specific functional category. V: Vertical describes a specific row in the matrix, from 0-9. H: Horizontal describes a specific column in the matrix, from 0-9.
Power failure	Lower or higher than rated voltage range
Power loss	Shutdown the power
[PRO SAFETY] Prosafety	Proactive Safety Function: Alarm regarding to error of the level measuring function
HTF	Hardware Failure Tolerance
SFF	Safe Failure Fraction
PFH(1-h)	Probability of dangerous Failure per Hour
PFD	Probability of Failure on Demand

Certificate

TÜV NORD

ZERTIFIKAT
CERTIFICATE

Hiermit wird bescheinigt, dass das unten beschriebene Produkt der Firma
This certifies that the product mentioned below from company

Endress+Hauser Yamanashi Co.,Ltd.
862-1 Mitsukunugi Sakaigawa-cho
406-0846 Fuefuki-shi
Japan

die Anforderungen der folgenden Prüfunterlage(n) erfüllt.
fulfills the requirements of the following test regulations.

Geprüft nach: *Tested in accordance with:*	**EN 61508:2010 (SIL 2)**
Beschreibung des Produktes: (Details s. Anlage 1) *Description of product:* *(Details see Annex 1)*	**Füllstandssensor** *Tank level gauge*
Typenbezeichnung: *Type designation:*	**Proservo NMS**
Bemerkungen: *Remarks:*	**Siehe Anlage** *See Annex*

Dieses Zertifikat bescheinigt das Ergebnis der Prüfung an dem vorgestellten Prüfgegenstand. Eine allgemein gültige Aussage über die Qualität der Produkte aus der laufenden Fertigung kann hieraus nicht abgeleitet werden.
This certifies the result of the examination of the product sample submitted by the manufacturer. A general statement concerning the quality of the products from the series manufacture cannot be derived there from.

Registrier-Nr. / *Registration No.* 44 799 16005501
Prüfbericht Nr. / *Test Report No.* 3517 3833
Aktenzeichen / *File reference* 8000455928

Gültigkeit / *Validity*
von / *from* 2016-02-19
bis / *until* 2021-02-18

F. Hegenfeld

Zertifizierungsstelle / *CB*
TÜV NORD CERT GmbH

Essen, 2016-02-19

TÜV NORD CERT GmbH Langemarckstraße 20 45141 Essen www.tuev-nord-cert.de technology@tuev-nord.de

Bitte beachten Sie auch die umseitigen Hinweise
Please also pay attention to the information stated overleaf

www.addresses.endress.com

Endress+Hauser

People for Process Automation