FY01037K/09/EN/01.21
71543127
2021-01-15

Functional Safety Manual
RNO22

Output isolating amplifier, HART-transparent

Endress+Hauser
People for Process Automation

Table of contents

1 Declaration of Conformity

SIL_00469_01.21

Endress+Hauser
People for Process Automation

Manufacturer Declaration

Functional Safety according to IEC 61508:2010
Supplement 1 / NE130 Form B.1

Endress+Hauser Wetzer GmbH+Co. KG Obere Wank 1, 87484 Nesselwang

declares as a manufacturer, that the following active barrier

RNO22-SIL

is suitable for use in safety relevant applications up to SIL2 (HFT=0) rep. SIL3 (HFT=1) according to IEC 61508:2010.

In safety relevant applications according to IEC 61508, the instructions of the Safety Manual have to be followed.

Nesselwang, 13.01.2022
Endress+Hauser Wetzer GmbH+Co. KG

ppa. Harald Müller
Director Technology

i.V. Robert Zeller
Head of Department R&D-Components

1/2

A0047736

1.1 Safety-related characteristic values

SIL_00469_01.21

Endress+Hauser
People for Process Automation

General				
Device designation and permissible types	RNO22 (Order code for "Additional approval": Option LA "SIL")			
Safety-related output signal	4...20mA			
Fault current	≤ 3,6			
Process variable/function	Current transfer			
Safety function(s)	Range 4...20 mA			
Device type acc. to IEC 61508-2	☑ Type A	☐ Type B		
Operating mode	☑ Low Demand Mode	☑ High Demand	☐ Continuous Mode	
Valid Hardware-Version	01.00 or higher			
Valid Software-Version	n/a			
Safety manual	FY01037K/09			
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 IEC61508-2 for devices w/o software			
Evaluation through / certificate no.	DEKRA / Zertifikat Nr. ZP/C034/21			
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	RNO22, Architecture 1oo1	RNO22, Architecture 1oo2		
Safety function	range	range		
λ_{DU} [1) 2)]	38 FIT	3 FIT		
λ_{DD} [1) 2)]	34 FIT	31 FIT		
λ_S [1) 2)]	157 FIT	39 FIT		
SFF - Safe Failure Fraction	83%	96 %		
β, β_D [3)]		2%, 2%		
PFD_{avg} T1 = 1 year [2)] (single channel architecture)	$1{,}67 \cdot 10^{-4}$	$1{,}21 \cdot 10^{-5}$		
PFD_{avg} T1 = 5 years [2)] (single channel architecture)	$8{,}32 \cdot 10^{-4}$	$6{,}13 \cdot 10^{-5}$		
PFH	$3{,}8 \cdot 10^{-8} \cdot$ 1/h	$2{,}8 \cdot 10^{-9} \cdot$ 1/h		
PTC [4)]	95 %			
MTBF [5)]	55 years			
Diagnostic test interval	n/a			
Fault reaction time [6)]	< 2 s			
Process safety time	< 2 s			
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 should be applied
3) Common Cause factor β and β_D of the system, tables in Annex D of IEC 61508-6: 2010
4) PTC = Proof Test Coverage
5) MTBF = Mean time between failures, this value takes into account all failure types of the electronic components according to Siemens SN2950
6) Maximum time between error recognition and error response

2/2

A0047738

2 Document information

2.1 Document function

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.

General information on functional safety (SIL) is available at:
www.endress.com/SIL

2.2 Symbols used

2.2.1 Safety symbols

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

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

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

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

2.2.2 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

1., 2., 3.
Series of steps

Result of a step

1, 2, 3, ...
Item numbers

A, B, C, ...
Views

2.3 Supplementary device documentation

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

The following document types are available in the Downloads area of the Endress+Hauser website (www.endress.com/downloads).

2.3.1 Further applicable documents

- TI01587K
- BA02064K
- KA01483K
- XA02374K

2.3.2 Technical Information (TI)

Planning aid
The document contains all the technical data on the device and provides an overview of the accessories and other products that can be ordered for the device.

2.3.3 Brief Operating Instructions (KA)

Guide that takes you quickly to the 1st measured value
The Brief Operating Instructions contain all the essential information from incoming acceptance to initial commissioning.

2.3.4 Operating Instructions (BA)

Your reference guide
These Operating Instructions contain all the information that is required in various phases of the life cycle of the device: from product identification, incoming acceptance and storage, to mounting, connection, operation and commissioning through to troubleshooting, maintenance and disposal.

2.3.5 Safety Instructions (XA)

Depending on the approval, the following Safety Instructions (XA) are supplied with the device. They are an integral part of the Operating Instructions.

The nameplate indicates the Safety Instructions (XA) that are relevant to the device.

3 Design

3.1 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 firmware and hardware versions.

Unless otherwise specified, all subsequent versions can also be used for safety functions.

A modification process according to IEC 61508 is applied for any device modifications.

Any exemptions from possible combinations of features are saved in the Endress +Hauser ordering system.

Valid device versions for safety-related use:

3.1.1 Ordering features

RNO22 (1-/2-channel)

Feature: 010 "Approval"
Version: all

Feature: 020 "Channel"
Version: all

Feature: 030 "Electrical connection"
Version: all

Feature: 590 "Additional approval"
Version: LA
The **"LA"**version must be selected for use as a safety function as per IEC 61508. All other versions are permitted in addition to LA.

Feature: 620 "Accessory enclosed"
Version: all

Feature: 895 "Marking"
Version: all

3.2 Identification marking

SIL-certified devices are marked with the SIL logo on the nameplate.

3.3 Safety function

The device performs the safety function of galvanic electrically isolated forwarding an input current signal in a proportional (1:1) output signal of 4 mA to 20 mA with a maximum error of 2%.

3.3.1 Safety-related input signal

The safety-related input signal is a 4 to 20 mA current signal.

3.3.2 Safety-related output signal

The safety-related output signal is a 4 to 20 mA current signal that does not deviate from the input signal by more than 2%.

Output values < 3.6 mA are deemed a safe state that must be detected by I/P converters, display units, etc. that are connected downstream or by means of additional evaluation via a controller.

NOTICE

In an alarm condition

- ▶ Ensure that the equipment under control achieves or maintains a safe state.

3.3.3 Reaction times

The process safety time is < 2 s.

3.3.4 Operating mode

RNO22, 1-channel

The device is suited to the following operating modes in accordance with IEC 61508:
- Low demand mode
- High demand mode

You can operate the device in the following safety-relevant modes:

1. SIL 2, SC 3 1oo1: In 1-channel operation

2. SIL 3, SC 3, 1oo2: In redundant 1-channel operation, two 1-channel devices are operated redundantly for a safety application.

RNO22, 2-channel

The device is suited to the following operating modes in accordance with IEC 61508:
- Low demand mode
- High demand mode

You can operate the device in the following safety-relevant modes:

1. SIL 3, SC 3, 1oo2: In 2-channel coupled mode, both channels will be operated redundantly for one safety application.

2. SIL 2, SC 3, 2 x 1oo1: In 2-channel separated mode, each single channel will be operated for a separate safety application.

3. SIL 2, SC 3, 1 x 1oo1: In 1-channel mode, one of the two channels is used for one safety application. The second channel is available for a non safety-related application.

3.3.5 Safety integrity requirements (characteristic safety values)

RNO22, 1-channel

The specified characteristic safety values only refer to the device and do not include the connected actuators.

1-channel operation (SIL 2), 1oo1
- Type A device (as per IEC/EN 61508-2)
- Safety Integrity Level (SIL) 2
- HFT 0
- MTTR 24 h
- Mission Time 20 years
- Architecture 1oo1
- Ambient temperature 40 °C
- Proof test coverage (PTC) 95%

Failure rates

λ_{SU}	λ_{SD}	λ_{DU}	λ_{DD}	SFF	DC_D
156.1	1.03	38.01	34.45	83.44%	47.54%

The overall failure rate is 459.16 FIT. The MTBF is 55 years.

The average probability of failure on demand of the designed function for "low demand" operating mode and the probability of a dangerous failure per hour for "high demand" operating mode are calculated based on the failure rates.

Low demand mode

The following PFD_{avg} values are determined based on the failure rates:

T[PROOF]=	1 year	2 years	3 years	4 years	5 years	6 years	7 years
PFD_{avg}	$1.67 * 10^{-4}$	$3.33 * 10^{-4}$	$5 * 10^{-4}$	$6.66 * 10^{-4}$	$8.32 * 10^{-4}$	$9.99 * 10^{-4}$	$1.17 * 10^{-3}$

The values with a magnitude of $< 10 * 10^{-4}$ mean that the calculated PFD_{avg} values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. They meet the requirement to cover no more than 10% of the safety circuit or are better than or equal to $1.00 * 10^{-3}$.

The values with a magnitude of $> 10 * 10^{-4}$ mean that the calculated PFDavg values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. However, they do not meet the requirement to cover no more than 10% of the safety circuit or are not better than or equal to $1.00 * 10^{-3}$.

High demand mode

The following PFH value is derived from the failure rates:

$PFH = 38.01 * 10^{-9}$

Low demand mode is taken as the basis. In SIL 2 applications, if the percentage of the device for the entire safety circuit is assumed to be a maximum of 10%, the maintenance interval can be increased to up to 6 years.

Safety circuit as per IEC/EN 61508-1

Sensor	Device	Processing	Actuator
25%	< 10%	15%	50%

2 x 1-channel operation (2 x SIL 2 -> SIL 3, 1oo2, 2 x same measuring task)

Using an external comparator, check the two output signals for the maximum permitted error of 2% in order to achieve a possible SIL 3 application.

- Type A device (as per IEC/EN 61508-2)
- Safety Integrity Level (SIL) 3 (1oo2 structure)
- Beta factor 2%
- HFT 1
- MTTR 24 h
- Mission Time 20 years
- Architecture 1oo2
- Ambient temperature 40 °C
- Proof test coverage (PTC) 95%

λ_{SU}	λ_{SD}	λ_{DU}	λ_{DD}	SFF	DC_D
39.26	0.07	2.77	30.75	96.2%	91.73%

The total failure rate λ_{tot} per channel, including the components that do not belong to the safety function, is 1705.32 FIT (as per SN 29500).

The MTBF is 55 years.

The average probability of failure on demand of the designed function for "low demand" operating mode and the probability of a dangerous failure per hour for the "high demand" operating mode are calculated based on the failure rates.

T[PROOF]=	1 year	2 years	3 years	4 years	5 years	6 years	7 years	8 years
PFD_{avg}	$1.21 * 10^{-5}$	$2.43 * 10^{-5}$	$3.66 * 10^{-5}$	$4.89 * 10^{-5}$	$6.13 * 10^{-5}$	$7.37 * 10^{-5}$	$8.62 * 10^{-5}$	$9.87 * 10^{-5}$

The values with a magnitude of $< 10 * 10^{-5}$ mean that the calculated PFD_{avg} values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. They meet the requirement to cover no more than 10% of the safety circuit or are better than or equal to $1.00 * 10^{-4}$.

The values with a magnitude of $> 10 * 10^{-5}$ mean that the calculated PFDavg values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. However, they do not meet the requirement to cover no more than 10% of the safety circuit or are not better than or equal to $1.00 * 10^{-4}$.

High demand mode

The following PFH value is derived from the failure rates:

$PFH = 2.77 * 10^{-9}/h$

The requirements for the PFH value for a SIL 3 system are thus met.

When calculating the PFD_{avg} and PFH values for the 2-channel operating mode, errors with a common cause were taken into account with a β factor of 2% and βD factor of 2%.

The remaining values mean that the calculated PFD_{avg} values are within the permitted range for SIL 3 as per table 2 of IEC/EN 61508-1. However, they do not meet the requirement to cover no more than 10% of the safety circuit or are not better than or equal to $1.00 * 10^{-4}$.

Low demand mode is taken as the basis (PFD_{avg} values). In SIL 3 applications, if the percentage of the device for the entire safety circuit is assumed to be a maximum of 10%, the maintenance interval can be increased to up to 8 years.

Safety circuit as per IEC/EN 61508-1

Sensor	Device	Processing	Actuator
25%	< 10%	15%	50%

RNO22, 2-channel

The specified characteristic safety values only refer to the device and do not include the connected actuators.

2-channel coupled mode (2 x SIL 2 -> SIL 3, 1oo2, 2 x same measuring task)

- Type A device (as per IEC/EN 61508-2)
- Safety Integrity Level (SIL) 2
- HFT 1
- MTTR 24 h
- Mission Time 20 years
- Architecture 1oo2
- Ambient temperature 40 °C
- Proof test coverage (PTC) 95%

λ_{SU}	λ_{SD}	λ_{DU}	λ_{DD}	SFF	DC_D
39.26	0.07	2.77	30.75	96.2%	91.73%

The total failure rate λtot per channel, including the components that are not part of the safety function, is 1705.32 FIT (as per SN 29500).

The MTBF is 55 years.

The average probability of failure on demand of the designed function for "low demand" operating mode and the probability of a dangerous failure per hour for "high demand" operating mode are calculated based on the failure rates.

T[PROOF]=	1 year	2 years	3 years	4 years	5 years	6 years	7 years	8 years
PFD_{avg}	$1.21 * 10^{-5}$	$2.43 * 10^{-5}$	$3.66 * 10^{-5}$	$4.89 * 10^{-5}$	$6.13 * 10^{-5}$	$7.37 * 10^{-5}$	$8.62 * 10^{-5}$	$9.87 * 10^{-5}$

The values with a magnitude of $< 10 * 10^{-5}$ mean that the calculated PFD_{avg} values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. They meet the requirement to cover no more than 10% of the safety circuit or are better than or equal to $1.00 * 10^{-4}$.

The values with a magnitude of $> 10 * 10^{-5}$ mean that the calculated PFDavg values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. However, they do not meet the requirement to cover no more than 10% of the safety circuit or are not better than or equal to $1.00 * 10^{-4}$.

High demand mode

The following PFH value is derived from the failure rates:

$PFH = 2.77 * 10^{-9}$

The requirements for the PFH value for a SIL 3 system are thus met.

When calculating the PFD_{avg} and PFH values for the 2-channel operating mode, errors with a common cause were taken into account with a β factor of 2% and βD factor of 2%.

The remaining values mean that the calculated PFDavg values are within the permitted range for SIL 3 as per table 2 of IEC/EN 61508-1. However, they do not meet the requirement to cover no more than 10% of the safety circuit or are not better than or equal to $1.00 * 10^{-4}$.

Low demand mode is taken as the basis (PFD_{avg} values). In SIL 3 applications, if the percentage of the device for the entire safety circuit is assumed to be a maximum of 10%, the maintenance interval can be increased to up to 8 years.

Safety circuit as per IEC/EN 61508-1

Sensor	Device	Processing	Actuator
25%	< 10%	15%	50%

Two-channel operation (2 x SIL 2, 2 x 1oo1, the two channels are operated individually) and 1-channel operation (SIL 2, 1oo1, only one channel is used, the second channel is available for non safety-relevant applications for example)

- Type A device (as per IEC/EN 61508-2)
- - Safety Integrity Level (SIL) 2 (1oo1 structure)
- HFT 0
- MTTR 24 h
- Mission Time 20 years
- Architecture 1oo1
- Ambient temperature 40 °C
- Proof test coverage (PTC) 95%

λ_{SU}	λ_{SD}	λ_{DU}	λ_{DD}	SFF	DC_D
156	1	38	34.5	83.44%	47.54%

The total failure rate λ_{tot} per channel, including the components that do not belong to the safety function, is 981.31 FIT (as per SN 29500).

The MTBF is 55 years.

The average probability of failure on demand of the designed function for "low demand" operating mode and the probability of a dangerous failure per hour for the "high demand" operating mode are calculated based on the failure rates.

The following PFDavg values are determined based on the failure rates:

The following PFD_{avg} values are determined based on the failure rates:

T[PROOF]=	1 year	2 years	3 years	4 years	5 years	6 years	7 years
PFD_{avg}	$1.67 * 10^{-4}$	$3.33 * 10^{-4}$	$5 * 10^{-4}$	$6.66 * 10^{-4}$	$8.32 * 10^{-4}$	$9.99 * 10^{-4}$	$1.17 * 10^{-3}$

The values with a magnitude of $< 10 * 10^{-4}$ mean that the calculated PFD_{avg} values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. They meet the requirement to cover no more than 10% of the safety circuit or are better than or equal to $1.00 * 10^{-3}$.

The values with a magnitude of $> 10 * 10^{-4}$ mean that the calculated PFDavg values are within the permitted range for SIL 2 in accordance with table 2 of IEC/EN 61508-1. However, they do not meet the requirement to cover no more than 10% of the safety circuit or are not better than or equal to $1.00 * 10^{-3}$.

High demand mode

The following PFH value is derived from the failure rates:

$PFH = 38.01 * 10^{-9}/h$

Low demand mode is taken as the basis. In SIL 2 applications, if the percentage of the device for the entire safety circuit is assumed to be a maximum of 10%, the maintenance interval can be increased to up to 6 years.

Safety circuit as per IEC/EN 61508-1

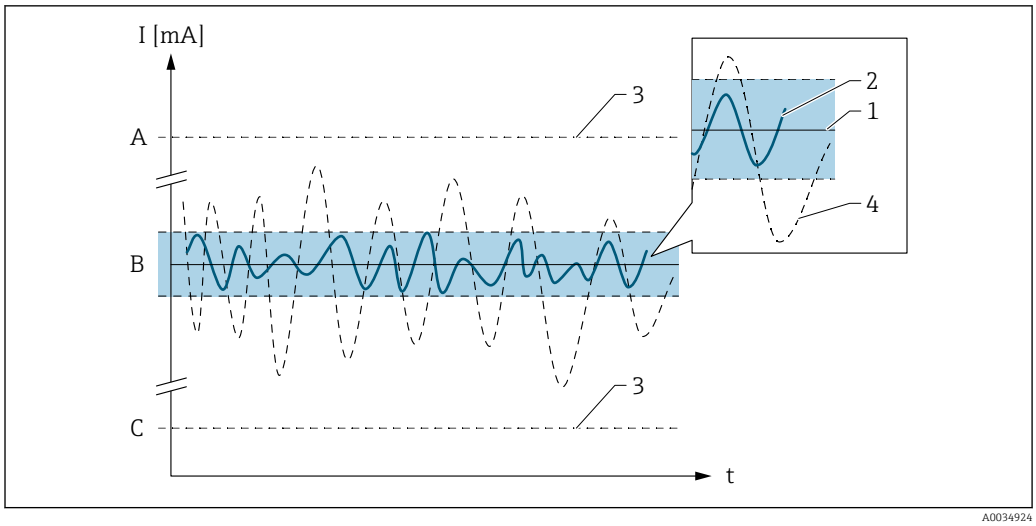
Sensor	Device	Processing	Actuator
25%	< 10%	15%	50%

3.4 Basic conditions for use in safety-related applications

The measuring system must be used correctly for the specific application, taking into account the medium properties and ambient conditions. Carefully follow instructions pertaining to critical process situations and installation conditions from the Operating Instructions. The application-specific limits must be observed. The specifications in the Operating Instructions and the Technical Information must not be exceeded.

3.4.1 Safety-related failures according to IEC/EN 61508

The safety-related failures are classified into different categories according to IEC/EN 61508. The following list shows the implications for the safety-related output signal and the measuring uncertainty.
System response time as per DIN EN 61298-2 => TI/BA



A High alarm ≥ 21 mA
B SIL error range ±2%
C Low alarm ≤ 3.6 mA

No device error
- No failure
- No implications for the safety-related output signal
- Impact on the measuring uncertainty:
  1 – within the specification (TI, BA etc.)

λ_S (Safe)
- Safe failure
- No implications for the safety-related output signal: output signal goes to safe state
- Impact on the measuring uncertainty:
  2 – Moves within the specified SIL error range
  3 – Has no effect

λ_{DD} (Dangerous detected)
- Safe failure
- Implications for the safety-related output signal: results in a failure mode at the output signal
- Impact on the measuring uncertainty:
  3 – Has no effect

λ_{DU} (Dangerous undetected)
- Dangerous failure which cannot be detected
- Implications for the safety-related output signal: can be outside the defined error range
- Impact on the measuring uncertainty:
  4 – May be outside the specified error range

3.4.2 Restrictions for safety-related use

- The failure rates of the components used are constant over the operating time.
- The propagation of errors by the device in the system is not taken into consideration.
- The failure rates of the external power supply are not taken into consideration.
- The specified failure rates relate to an ambient temperature of +40 °C. You must multiply the failure rates by a factor of 2.5 for an ambient temperature of +60 °C. The factor of 2.5 is based on empirical values.
- The supplying power unit must be able to capture an interruption of 20 ms in the supply voltage

3.5 Dangerous undetected failures in this scenario

Dangerous undetected failures are failures where the device does not follow a change in the input signal or deviates from the input signal by more than 2%. (Dangerous detected failures are those that provide a signal of < 3.6 mA.)

3.6 Safety measured error

The measured error specified for SIL is a maximum of 2% from the output signal.

3.7 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.

According to DIN EN 61508-2:2011 section 7.4.9.5 (national footnote N3) appropriate measures taken by the operator can extend the useful lifetime.

4 Commissioning (installation and configuration)

4.1 Requirements for personnel

The personnel for installation, commissioning, diagnostics and maintenance must fulfill the following requirements:

- Trained, qualified specialists must have a relevant qualification for this specific function and task.
- Personnel must be authorized by the plant owner/operator.
- Be familiar with federal/national regulations.
- Before starting work: personnel must read and understand the instructions in the manual and supplementary documentation as well as the certificates (depending on the application).
- Personnel must follow instructions and comply with general policies.

The operating personnel must fulfill the following requirements:

- Personnel are instructed and authorized according to the requirements of the task by the facility's owner-operator.
- Personnel follow the instructions in this manual.

4.2 Installation

The mounting and wiring of the device and the permitted orientations are described in the Operating Instructions pertaining to the device.

A lockable housing in the IP 54 degree of protection is recommended for installation of the devices.

Installation, operation and maintenance must be carried out by technical personnel.

Use modification protection in accordance with IEC/EN 61508-2, Annex A, Table A.17. For example, you can install the device in a control cabinet with a key lock.

Implement measures to counteract temperature increases at the mounting location in accordance with IEC/EN 61508-2, Annex A Table A.16.

4.3 Commissioning

The commissioning of the device is described in the relevant Operating Instructions.

Prior to operating the device in a safety instrumented system, verification must be carried out by means of a test sequence as described in **Section 6 Proof testing**.

- Connect the device in accordance with the installation instructions.
- Make sure that the connected actuator and transmitter correspond to the configuration provided.
- Check the functionality of the device with connected transmitter and actuator to ensure it is functioning properly.
- A calibrated actuator simulator and a calibrated digital multimeter may be required to test the device with connected transmitter.
- Put the safety circuit into operation and check that it is functioning correctly.

4.4 Operation

The operation of the device is described in the Operating Instructions pertaining to the device.

5 Operation

5.1 Normal operation

The green LED (PWR) remains lit constantly during normal operation.

5.2 Start and restart

If a fault occurs during operation, then the output signal is set to a value outside the "normal" signal range of 3.6 to 21 mA in most cases. The connected SIS should thus check the signal values read in to determine if they are valid and take appropriate measures if the values deviate from the normal values.

Make sure that the connected transmitters react to line errors to the sensors.

The required voltages are generated in the device following a shutdown and restart. Signal transmission takes place subsequently without any further measures.

5.3 Safe states

Output values of < 3.6 mA are deemed a safe state that must be detected by I/P converters, display units, etc. connected downstream or by means of additional evaluation via a controller.

5.4 Failure definition

Safe failures in the device are when the device provides an output signal that does not deviate from the input signal by more than 2%.

Dangerous undetected failures are failures where the device does not follow a change in the input signal or deviates from the input signal by more than 2% and is not outside the range.

Dangerous detected failures are failures that provide a signal of < 3.6 mA.

5.5 Diagnostic function (only valid for RNO22, 1-channel)

Diagnostic function via DIP 1 and DIP 2 switches

You must switch on short-circuit detection for safety-related applications, i.e., switches DIP 1 and DIP 2 are in position "II".

NOTICE

The switch position "DIP 1 and DIP 2 = I" is not permitted for safety-related applications.

- In the event of a short-circuit or high-impedance output, the input is switched to high impedance and can be detected on the input side

DIP	Short-circuit detection	
	Off	On
1	I	II
2	I	II

All of the DIP switches are in position "I" when the device is delivered.

NOTICE

DIP switches

- Only switch the DIP switches when the device is de-energized

.

6 Proof testing

The safety-related functionality of the device in the SIL mode must be verified during commissioning, when changes are made to safety-related parameters, and also at appropriate time intervals. This enables this functionality to be verified within the entire safety instrumented system. The time intervals must be specified by the operator.

CAUTION

The safety function is not guaranteed during a proof test

Suitable measures must be taken to guarantee process safety during the test.

- The safety-related output signal 4 to 20 mA must not be used for the protective system during the test.
- The operator specifies the testing interval and this must be taken into account when determining the probability of failure PFD_{avg} of the sensor system.

- The safety-related 4 to 20 mA output signal must not be used for the protective system during testing.
- A completed test must be documented; the template provided in the Appendix can be used for this purpose. (See Section 8.2)
- The operator specifies the test interval and this must be taken into account when determining the probability of failure PFD_{avg} of the sensor system.

If no operator-specific proof testing requirements have been defined, the following is a possible alternative for testing the transmitter depending on the measured variable used for the safety function. The individual proof test coverages (PTC) that can be used for calculation are specified for the test sequences described below.

- Regularly check the entire safety loop in accordance with IEC/EN 61508 and IEC/EN 61511 to ensure it is functioning correctly.
- The test intervals are defined based on the intervals for the individual devices in the safety loop.
- It is the responsibility of the operator to choose the type of test and the intervals within the time-frame specified.
- The test must be carried out in such a way that the correct functioning of the safety instrumented system in conjunction with all of the components is verifiable.
- In SIL 2 applications, the devices must be checked following the maximum maintenance/ test interval at the latest if the percentage of the device for the entire safety circuit is no more than 10%.

6.1 Test sequence

Proof test procedure

Possible method for proof testing to identify dangerous and undetected device faults

A calibrated simulator (current 0.2/4 mA to 20 mA) or actuator simulator and one, or ideally two, calibrated digital multimeters are required to test the devices.

6.1.1 Test sequence for RNO22, 1-channel

1. Take appropriate steps to avoid misuse.

2. Disconnect the safety circuit from subsequent processing.

3. Connect the current simulator to the input of the active barrier/isolating amplifier.

4. Connect the digital multimeters to the input and output of the active barrier/isolating amplifier respectively.

5. Set a signal in the range of 4 to 20 mA at the input of the device, or set a suitable signal at the input of the connected transmitter using the actuator simulator.

6. Measure the current in the active barrier/isolating amplifier. The output must adjust to the same value.

7. Setting ≤ 3.6 mA or > 21 mA verifies that the subsequent processing can detect signals that are out of range and evaluate them accordingly. The device should be tested if the output value deviates from the input value by more than 3 times the specified accuracy rating. In the event of an error replace the device with an equivalent device.

8. Re-establish the entire functionality of the safety circuit once again.

9. Restore normal operation.

6.1.2 Test sequence for RNO22, 2-channel

1. Take appropriate steps to avoid misuse.

2. Disconnect the safety circuit from subsequent processing.

3. Connect the current simulator to the input of the active barrier/isolating amplifier.

4. Connect the digital multimeters to the input and output of the active barrier/isolating amplifier respectively.

5. Set a load of ≥ 100 Ω at the output.

6. Set signals in increments of 2 mA in the range of 4 mA to 20 mA at the input of the device, or set suitable signals at the input of the connected transmitter using the actuator simulator.

7. The output must adjust to the same value.

8. Setting ≤ 3.6 mA verifies that the subsequent processing can detect error signals and evaluate them accordingly. The device should be tested if the output value deviates from

the input value by more than 3 times the specified accuracy rating. In the event of an error replace the device with an equivalent device.

9. Check the input current (< 3.6 mA) in the event of a wire break or short-circuit at the output to test the short-circuit and wire break monitoring.

10. Complete the test for the device's two channels.

11. Re-establish the entire functionality of the safety circuit once again.

12. Restore normal operation.

6.2 Verification criterion

If one of the test criteria from the test sequences described above is not fulfilled, the device may no longer be used as part of a safety instrumented system.

- The purpose of proof-testing is to detect dangerous undetected device failures (λ_{DU}).
- This test does not cover the impact of systematic faults on the safety function, which must be assessed separately.
- Systematic faults can be caused, for example, by process material properties, operating conditions, build-up or corrosion.
- As part of the visual inspection, for example, ensure that all of the seals and cable entries provide adequate sealing and that the device is not visibly damaged.

7 Repair and error handling

7.1 Maintenance

Maintenance instructions and instructions regarding recalibration may be found in the Operating Instructions pertaining to the device.

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

7.2 Repair

Repair means restoring functional integrity by replacing defective components.

Only original Endress+Hauser spare parts may be used here.

The repair must be documented. This includes:

- Serial number of the device
- Date of the repair
- Type of repair
- Person who performed the repair

Components may be repaired/replaced by the customer's specialist staff if original Endress +Hauser spare parts (which can be ordered by the end customer) are used, and if the relevant installation instructions are followed.

A proof test must always be performed after every repair.

Installation Instructions are supplied with the original spare part and can also be accessed in the Download Area at www.endress.com

Send in replaced components to Endress+Hauser for fault analysis.

When returning the defective component, always enclose the "Declaration of Hazardous Material and Decontamination" with the note "Used as SIL device in a safety instrumented system.

Information on returns: http://www.endress.com/support/return-material

7.3 Modification

- **Modifications to SIL devices by the user are not permitted as they can impair the functional safety of the device**
- Modifications to SIL devices on site at the user's plant are possible following approval by the Endress+Hauser manufacturing center
- Modifications to SIL devices must be performed by staff who have been authorized to perform this work by Endress+Hauser
- Only **original spare parts** from Endress+Hauser must be used for modifications
- All modifications must be documented in the Endress+Hauser W@M Device Viewer
- All modifications require a modification nameplate or the replacement of the original nameplate.

7.4 Decommissioning

When decommissioning, the requirements according to IEC 61508-1:2010 section 7.17 must be observed.

7.5 Disposal

If required by the Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), the product is marked with the depicted symbol in order to minimize the disposal of WEEE as unsorted municipal waste. Do not dispose of products bearing this marking as unsorted municipal waste. Instead, return them to Endress+Hauser for disposal under the applicable conditions.

8 Appendix

8.1 Commissioning or proof test report

The following device-specific test report acts as a print/master template and can be replaced or supplemented any time by the customer's own SIL reporting and testing system.

8.1.1 Test Report - Page 1 -

Company/contact person
Tester

Device information
System
Measuring points/TAG no.
Device type/order code
Serial number
Hardware version
SIL checksum

Verification information
Date/time
Performed by
Date/time
Inspector

Verification result	
Overall result	
☐ Pass ☑	☐ Fail ☒

Note

Date Signature Signature of tester

8.1.2 Test Report - Page 2 -

Type of safety function
☐ Safe measurement

Proof testing
☐ Test sequence, 1-channel
☐ Test sequence, 2-channel

This report is based on the specifications in the Functional Safety Manual: FY01037K

Proof test report			
Test stage	**Set point**	**Actual value**	**Verification result**
1. Take appropriate measures to avoid misuse.			☐ Pass ☐ Fail
2. Disconnect the safety circuit from subsequent processing.			☐ Pass ☐ Fail
3. Connect the current simulator to the input of the active barrier/isolating amplifier.			☐ Pass ☐ Fail
4. Connect the digital multimeters to the input and output of the active barrier/isolating amplifier respectively.			☐ Pass ☐ Fail
5. Set a load of ≥ 100 Ω at the output.			☐ Pass ☐ Fail ☐ Not applicable
6. Set a signal in the range of 4 to 20 mA at the input of the device or a suitable signal at the input of the connected transmitter using the actuator simulator.			☐ Pass ☐ Fail ☐ Not applicable
7. Set signals in increments of 2 mA in the range of 4 to 20 mA at the input of the device, or set a suitable signal at the input of the connected transmitter using the actuator simulator.			☐ Pass ☐ Fail ☐ Not applicable
8. Measure the current in the active barrier/isolating amplifier. The output must adjust to the same value.			☐ Pass ☐ fail
9. Setting ≤ 3.6 mA or > 21 mA verifies that the subsequent processing can detect signals that are out of range and evaluate them accordingly. The device should be tested if the output value deviates from the input value by more than 3 times the specified accuracy rating. In the event of an error replace the device with an equivalent device.			☐ Pass ☐ Fail
10. Check the input current (< 3.6 mA) in the event of a wire break or short-circuit at the output to test the short-circuit and wire break monitoring.			☐ Pass ☐ Fail ☐ Not applicable
11. Complete the test for the device's two channels.			☐ Pass ☐ Fail ☐ Not applicable
12. Re-establish the entire functionality of the safety circuit once again.			☐ Pass ☐ Fail
13. Restore normal operation.			☐ Pass ☐ Fail

Note

www.addresses.endress.com

Endress+Hauser

People for Process Automation