

Functional Safety Manual RMA42

Process transmitter



Application

1- to 2-channel transmitter power supply with intrinsically safe current inputs, temperature inputs, limit value monitoring with two changeover contacts, mathematics functions and 1 to 2 analog outputs designed to satisfy particular safety systems requirements as per IEC 61508:2010.

The measuring system meets the requirements for

- functional safety as per IEC 61508:2010
- explosion protection (depending on version)
- electromagnetic compatibility as per EN 61326 and NAMUR recommendation NE 21
- electrical safety as per IEC/EN 61010-1

Your benefits

- Suitable for use in a safety function up to SIL 2 in a safety-related system, independently assessed by Exida in accordance with IEC 61508:2010.

Contents

SIL Declaration of Conformity	3
General information	5
Structure of the measuring system	5
System components	5
Description of application as a safety instrumented system ..	5
Permitted devices types	5
Supplementary device documentation	6
Description of safety requirements and boundary conditions	6
Safety function	6
Safety-related signal	10
Restrictions for use in safety-related applications	10
Functional safety parameters	11
Proof-test interval	12
Behavior of device when in operation and in the event of a fault	12
Installation	12
Orientation	12
Operation	12
Maintenance	14
Proof tests	14
Proof-test procedure	14
Repair	15
Repair	15
Appendix	15
Commissioning or proof-test protocol	15

SIL Declaration of Conformity

SIL_00154_02.17

Endress+Hauser 
People for Process Automation

SIL-Konformitätserklärung

Funktionale Sicherheit nach IEC 61508:2010 Beiblatt 1

SIL Declaration of Conformity

Functional Safety according to IEC 61508:2010 Supplement 1

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

erklärt als Hersteller, dass das Gerät

declares as manufacturer, that the device

RMA42

für den Einsatz in sicherheitsrelevanten Anwendungen bis SIL2 nach IEC61508:2010 geeignet ist. In sicherheitsrelevanten Anwendungen sind die Angaben des Handbuchs zur Funktionalen Sicherheit zu beachten.

is suitable for the use in safety-instrumented systems up to SIL2 according to IEC61508:2010.

In safety instrumented systems the instructions of the Safety Manual have to be followed.

Allgemein / General			
Sicherheitsbezogenes Ausgangssignal Safety related output signal	Strom / Current 4...20mA	Spannung / Voltage 2...10V	Relais / Relay ⁶⁾
Fehlersignal fault signal	3,5mA oder / or 22mA	0V oder / or 11V	Relais stromlos / Relay de-energized
Bewertetes Eingangssignal / Funktion Input signal / function	Strom, Spannung, Temperatur, Widerstand current, voltage, temperature, resistance		
Gerätetyp gem. IEC 61508-2 Device type acc. to IEC 61508-2	<input type="checkbox"/> Typ A	<input checked="" type="checkbox"/> Typ B	
Betriebsart Operating mode	<input checked="" type="checkbox"/> Low Demand Mode	<input type="checkbox"/> High Demand	<input type="checkbox"/> Continuous Mode
Gültige Hardware-Version valid hardware version	01.00.zz oder höher/ or higher		
Gültige Firmware-Version valid firmware version	01.03.03 oder höher / or higher		
Handbuch zur Funktionalen Sicherheit/ Functional safety manual	SD00025R/09		
Art der Bewertung Type of evaluation	<input type="checkbox"/>	Vollständige entwicklungsbegleitende HW/SW Bewertung inkl. FMEDA und Änderungsprozess nach IEC 61508-2, 3 Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	<input checked="" type="checkbox"/>	Bewertung über Nachweis der Betriebsbewährung HW/SW inkl. FMEDA und Änderungsprozess nach IEC 61508-2, 3 Evaluation of "Proven-in-use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3	
	<input checked="" type="checkbox"/>	Auswertung von Felddaten HW/SW zum Nachweis "Frühere Verwendung" gem. DIN EN 61511-1 2005 Evaluation of HW/SW field data to verify „prior use" acc. to DIN EN 61511-1 2005	
	<input checked="" type="checkbox"/>	Bewertung durch: Endress+Hauser SE+Co. KG / Report Nr. ASSESS_SIL-ZertVerl-RMA42 Evaluation through: Endress+Hauser SE+Co. KG / report no. ASSESS_SIL-ZertVerl-RMA42	
Prüfungsunterlagen Test documents	Entwicklungsdokumente, Testberichte, Datenblätter development documents, test reports, data sheets		

SIL_00154_02.17

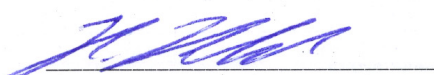
Endress+Hauser 

People for Process Automation

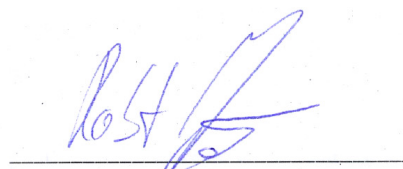
SIL – Integrität / SIL Integrity						
Hardware Sicherheitsintegrität Hardware safety integrity	Einkanaliger Einsatz / Single channel use		<input checked="" type="checkbox"/> SIL 2 fähig / capable		<input type="checkbox"/> SIL 3 fähig / capable	
FMEDA						
Empfohlenes Intervall für Wiederholungsprüfungen / recommended proof test interval	T ₁ = 1 Jahr / year					
Sicherheitsbezogenes Ausgangssignal Safety related output signal	Strom / Current 4...20mA		Spannung / Voltage 2...10V		Relais / Relay	
Anzahl Eingänge / number of inputs	1	2	1	2	1	2
MTBF _{tot} ³⁾ / Jahre / years	95	58	89	60	73	56
SFF	84,4 %	84,9 %	84,6 %	82,4 %	83,3 %	82,7 %
λ _{SD} ²⁾⁴⁾	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT
λ _{SU} ²⁾⁴⁾	0 FIT	0 FIT	0 FIT	0 FIT	445 FIT	521 FIT
λ _{DD} ²⁾⁴⁾	559 FIT	841 FIT	584 FIT	751 FIT	234 FIT	266 FIT
λ _{DU} ²⁾⁴⁾	103 FIT	149 FIT	106 FIT	160 FIT	158 FIT	167 FIT
PFD _{avg} ¹⁾⁴⁾ T ₁ = 1 Jahr / year	4,51 x10 ⁻⁴	6,53 x10 ⁻⁴	4,64 x10 ⁻⁴	7,01 x 10 ⁻⁴	6,92 x10 ⁻⁴	7,31 x10 ⁻⁴
Fehlerreaktionszeit Fault reaction time ⁵⁾	0,4 sec 5 sec	0,4 sec 5 sec	0,4 sec 5 sec	0,4 sec 5 sec	0,4 sec 5 sec	0,4 sec 5 sec

- 1) Die Werte entsprechen SIL 2 nach ISA S84.01. PFD-Werte für andere T1-Werte siehe Handbuch zur Funktionalen Sicherheit. /
The values comply with SIL 2 according to ISA S84.01. PFD values for other T1-values see Functional Safety Manual.
- 2) Gemäß Exida Bericht Nr. E+H 08/02-49. / According to Exida report no. E+H 08/02-49.
- 3) Gemäß Siemens SN29500, einschließlich Fehlern, die außerhalb der Sicherheitsfunktion liegen. /
According to Siemens SN29500, including faults outside the safety function.
- 4) Gültig für gemittelte Umgebungstemperaturen bis zu +40 °C (+104 °F) Bei einer durchschnittlichen Dauereinsatztemperatur nahe +50 °C sollte ein Faktor von 1,3 berücksichtigt werden. /
Valid for average ambient temperature up to +40 °C (+104 °F) For continuous operation at ambient temperature close to +50 °C (+122 °F), a factor of 1,3 should be applied.
- 5) Zeit zwischen Fehlererkennung und Fehlerreaktion. Die Zeit beträgt maximal 0,4 Sekunden. Bei Verwendung von RTD oder Thermoelement als Eingangssignal beträgt die Zeit zur Erkennung eines Leitungsbruches maximal 5 Sekunden. /
Maximum time between error recognition and error response. The maximum time is 0,4 sec. If a RTD or a thermocouple input signal is used the fault reaction time is up to 5 sec for cable open recognition.

Nesselwang, 04.07.2019
Endress+Hauser Wetzlar GmbH+Co. KG



Harald Hertweck
Managing Director



i.V. Robert Zeller
Head of department FEC

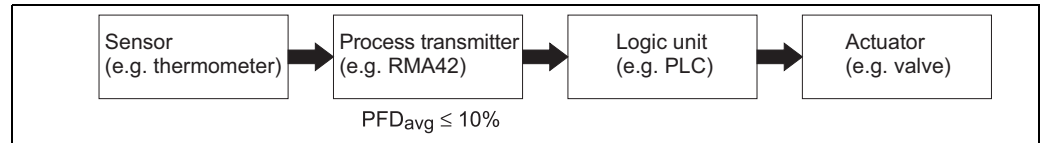
General information

General information on functional safety (SIL) is available at: www.de.endress.com/SIL (German) or www.endress.com/SIL (English) and in the Competence Brochure CP01008Z11EN "Functional safety - SIL safety instrumented systems in the process industry".

Structure of the measuring system

System components

The measuring system's devices are shown in the following diagram (example).



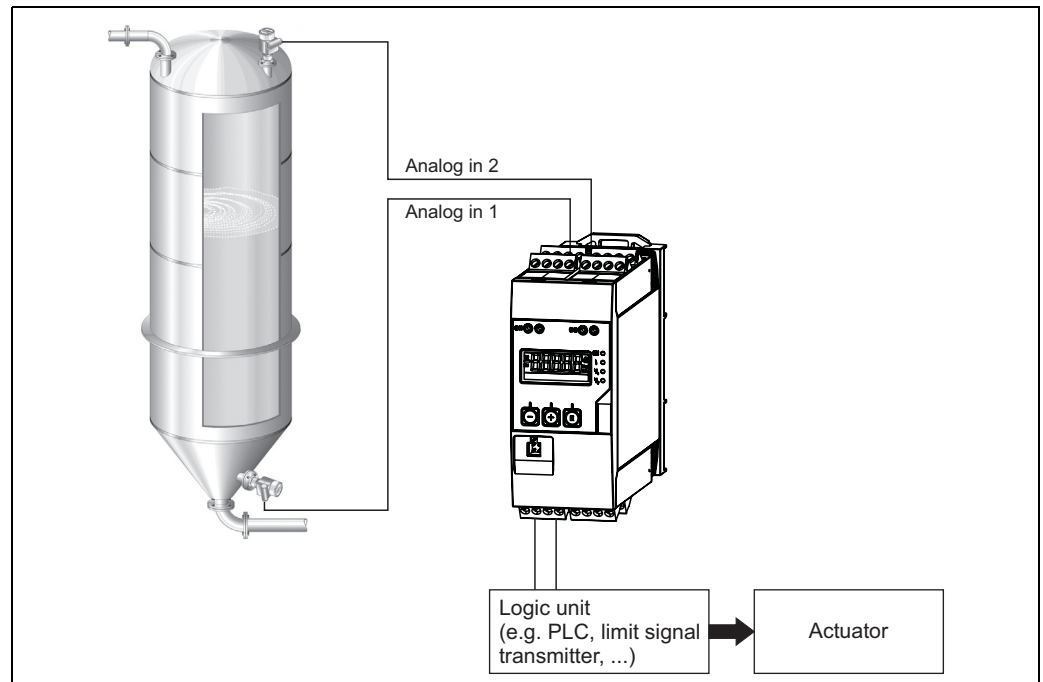
Proportion of "average probability of a dangerous failure on demand of a safety function" (PFD_{AVG}) accounted for by process transmitter



In this documentation the RMA42 is regarded as part of a safety function.

The sensor, process transmitter, logic unit and actuator together form a safety-related system that performs a safety function. The "average probability of a dangerous failure on demand of a safety-related system" (PFD_{avg}) is spread across the sensor, process transmitter, logic unit and actuator subsystems.

Description of application as a safety instrumented system



Example of a "differential pressure" application

Powered by the RMA42 process transmitter, the sensors generate an analog output signal that is proportional to the measured value (4 to 20 mA or 2 to 10 V). Mathematics functions are used to create a new process variable. The process transmitter sends the analog signals that are proportional to the new process variable to a logic unit located downstream, a PLC for example. Limit value monitoring can also be performed directly with the RMA42 via two changeover contacts.

Permitted devices types

The information on functional safety contained in this manual relates to the device versions listed below and are valid as of the specified software and hardware version.

Valid hardware version (electronics): from 01.00.xx

Valid firmware/software version: from 01.03.03 or higher

If changes are made to the device, a modification process compliant with IEC 61508 is applied. Unless otherwise indicated, all subsequent versions can also be used for safety instrumented systems.

Valid device versions for safety-related use:

Feature	Designation	Version
010	Approval	All
020	Input; output	All
590	Additional approval	at least H3 - others are optional

The table indicates the required versions. All other versions can be selected as desired.

Supplementary device documentation

Documentation	Contents	Comment
Technical Information TI00150R/09 (Process transmitter RMA42)	<ul style="list-style-type: none"> ▪ Technical data ▪ Information on accessories 	
Operating Instructions BA00287R/09 (Process transmitter RMA42)	<ul style="list-style-type: none"> ▪ Identification ▪ Installation ▪ Wiring ▪ Operation ▪ Commissioning ▪ Maintenance ▪ Accessories ▪ Troubleshooting ▪ Technical data ▪ Appendix: menu diagrams 	
Safety information depending on the "certificate" version chosen	<ul style="list-style-type: none"> ▪ Safety, installation and operating instructions for devices that are suitable for use in hazardous areas or for overfill prevention (WHG, German Water Resources Act). 	Additional safety instructions (XA, XB, XC, ZE, ZD) are supplied with certified device versions. Please refer to the nameplate for the relevant safety instructions.

Description of safety requirements and boundary conditions

Safety function

An analog output or limit relay can be used if deployed as part of a safety function.

One device can be used to implement several independent safety functions.

All inputs and outputs that do not form part of a safety function may still be used.

The use of non-safety-related inputs and outputs does not have a modifying effect on the safety function.

The following table shows which settings are permitted or prohibited when the RMA42 is used in a safety-related application:

Configuring the input signal:

Setup menu Analog in 1* Analog in 2*	Possible settings	Setting for safety function
Signal type*	4 to 20 mA	permitted
	0 to 20 mA	not permitted
	0 to 10 V	not permitted
	2 to 10 V	permitted
	0 to 5 V	not permitted
	1 to 5 V	not permitted
	± 1 V	not permitted
	± 10 V	not permitted
	± 30 V	not permitted
	± 100 mV	not permitted
	30 to 3000 Ohm	not permitted
	RTD/resistor 2-wire/3-wire/4-wire	permitted
Thermocouple	permitted	
Expert menu Input** Analog in 1** Analog in 2**		
Failure mode**	Fixed value	not permitted
	Invalid	permitted
Namur NE43**	On	permitted
	Off	not permitted

Configuring the current or voltage output:

Setup menu Analog Out 1* Analog Out 2*	Possible settings	Setting for safety function
Assignment*	Analog Input 1	permitted
	Analog Input 2	permitted
	Calc Value 1	permitted
	Calc Value 2	permitted
Signal type*	4 to 20 mA	permitted
	2 to 10 V	permitted
	0 to 20 mA	not permitted
	0 to 10 V	not permitted
	0 to 5 V	not permitted
	1 to 5 V	not permitted
Expert menu Input** Analog Out 1** Analog Out 2**		
Failure mode**	Fixed value	not permitted
	Min	permitted
	Max	permitted

Configuring the relays for limit value monitoring:

Setup menu	Possible settings	Setting for safety function
Relay 1*		
Relay 2*		
Assignment*	Analog input 1*	permitted
	Analog input 2*	permitted
	Calc value 1*	permitted
	Calc value 2*	permitted
Function*	Off	not permitted
	Min	permitted
	Max	permitted
	Gradient	permitted
	OutBand	permitted
	InBand	permitted
Expert menu		
Output**		
Relay 1**		
Relay 2**		
Operation mode**	norm closed	permitted
	norm opened	not permitted
Failure mode**	norm closed	permitted
	norm opened	not permitted

*) Displayed in Setup menu of device software

***) Displayed in Expert menu of device software

For further information, refer to the supplementary device documentation.

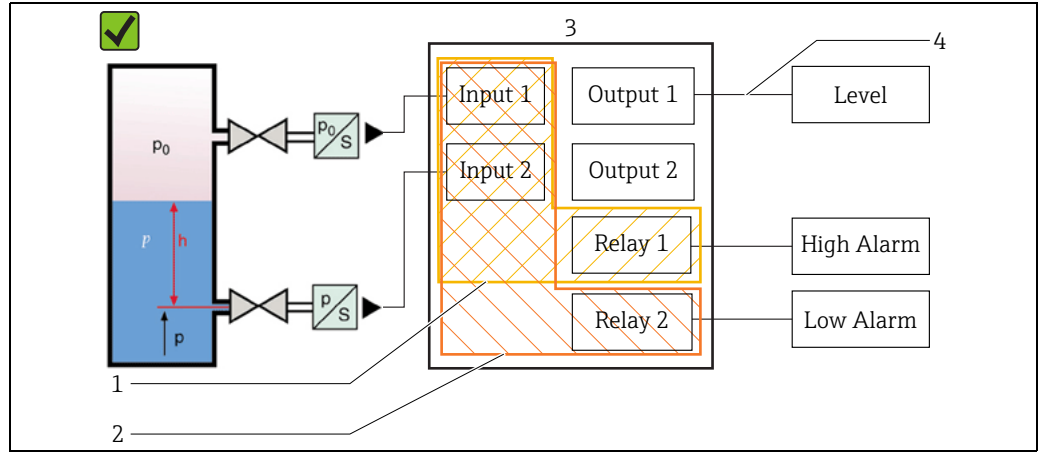
In addition, only certain settings are permitted for some parameters. If the setting of one of these parameters is not a permitted setting, safe operation of the device is no longer guaranteed.

Function group (menu path)	Setting
Expert → Application → Calc value 1/2 → Failure mode	Invalid
Expert → Diagnostics → Simulation → Simulation AO1/2	Off
Expert → Diagnostics → Simulation → Simu relay 1/2	Off

Safety function

Example 1: Level monitoring with differential pressure measurement

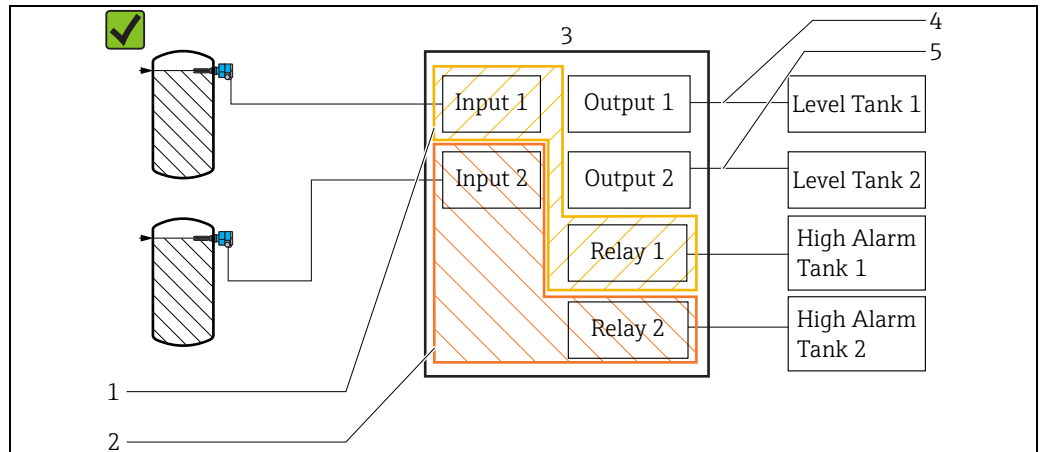
Safety function 1 Calc value (Input 1, Input 2) -> Relay 1 max. level (overflow prevention)
 Safety function 2 Calc value (Input 1, Input 2) -> Relay 2 min. level (dry running protection)
 Process value: Calc value (Input 1, Input 2) -> Output 1 (level)
 (no safety function)



- 1: Safety function 1
- 2: Safety function 2
- 3: Process transmitter
- 4: Output 1 - Process value, not part of the safety function. Output 2 is not used

Example 2: Level monitoring of two tanks

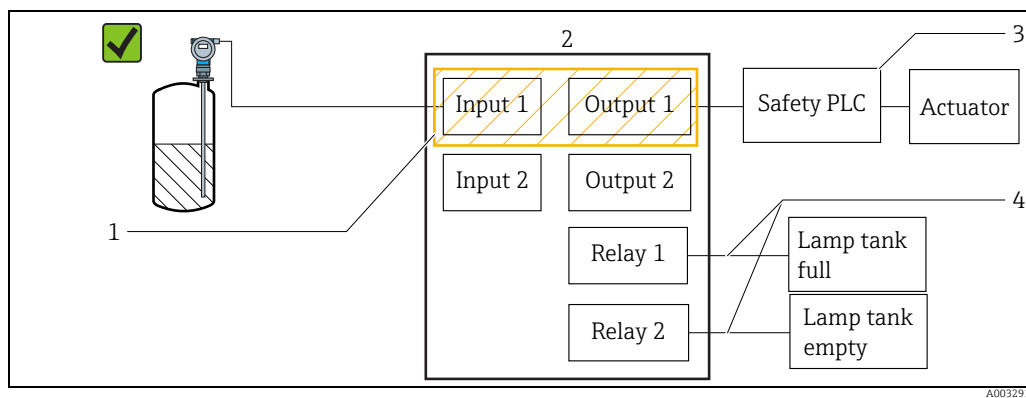
Safety function 1 Input 1 -> Relay 1 max. level tank 1
 Safety function 2 Input 2 -> Relay 2 max. level tank 2
 Process value: Input 1 -> Output 1 (level tank 1),
 (no safety function) Input 2 -> Output 2 (level tank 2)



- 1: Safety function 1
- 2: Safety function 2
- 3: Process transmitter
- 4: Output 1 - Process value, not part of the safety function.
- 5: Output 2 - Process value, not part of the safety function.

Example 3: continuous level monitoring of a tank

Safety function 1 Input 1 -> Output 1 continuous level value tank 1 to safety PLC with actuator
 Process value: Input 1 -> Relay 1 (lamp for full tank),
 (no safety function) Input 1 -> Relay 2 (lamp for empty tank)

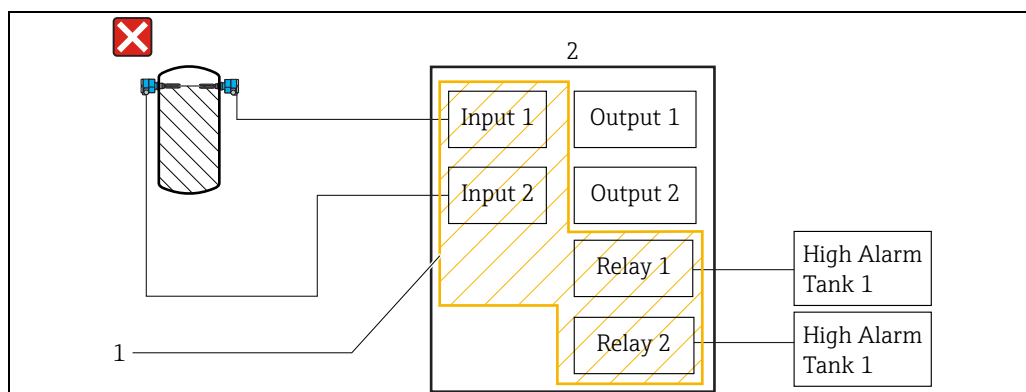


A0032918

- 1: Safety function 1
- 2: Process transmitter
- 3: Input 1 -> Output 1 continuous level value tank 1 to safety PLC with actuator
- 4: Relay 1 (lamp for full tank), Relay 2 (lamp for empty tank)

Example 4: Level monitoring of a tank with 2 channels (NOT PERMITTED!)

Safety function 1 (2 channels for Input 1 -> Relay 1 max. level tank 1
homogeneous redundancy): Input 2 -> Relay 2 max. level tank 1



A0032918

- 1: Safety function 1
- 2: Process transmitter

Safety-related signal

The safety-related signal is the analog output signal 4 to 20 mA or 2 to 10V or the limit relay. All safety measures refer exclusively to the output signal.

The safety-related output signal or limit relay is supplied to a logic unit located downstream, e.g. a programmable logic controller or a limit signal transmitter, where it is monitored for the following events:

- a predefined point level is exceeded
- the occurrence of a fault, e.g. error current as per NE 43 ($\leq 3.6 \text{ mA}$, $\geq 21 \text{ mA}$, interruption or short-circuit in signal line)

Restrictions for use in safety-related applications

- The measuring system must be used in accordance with the application, and attention must be paid to the ambient conditions.
- Follow the instructions for critical process situations and installation conditions in the Operating Instructions ("Installation conditions" section in BA00287R/09).
- The application-specific limits must be observed.
- The specifications in the Operating Instructions must not be exceeded. The accuracy of the safety-related output signal 4 to 20 mA or 2 to 10 V is $\pm 1\%$ of the measuring range.
- Device start-up time: After the device start-up, the safety functions are available following an initialization period of 20 seconds.
- The device must be locked after parameter configuration.
- A complete function test of the safety-related functions must be carried out during commissioning.
- Only vertical orientation is permitted.

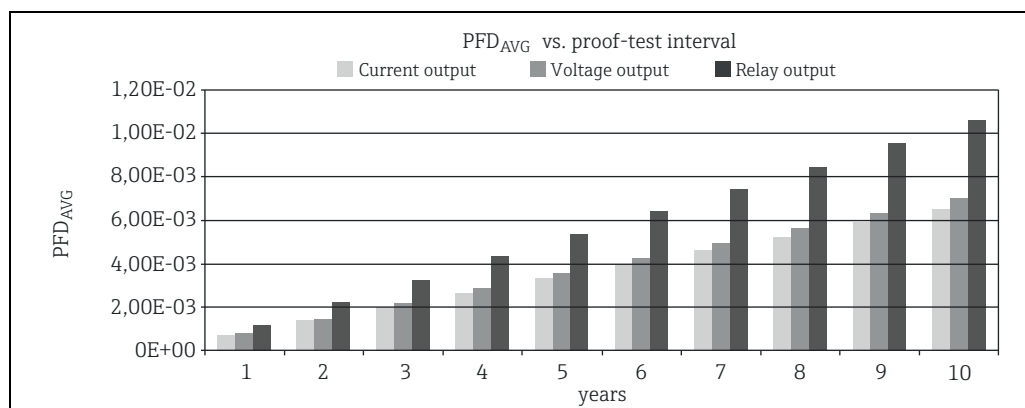
Functional safety parameters The table shows the specific functional safety parameters:

Parameter as per IEC 61508	Value, version 1	Value, version 2	Value, version 3
Safety function	Current output 1 input	Current output 2 inputs	Voltage output 1 input
SIL	2	2	2
HFT	0	0	0
Device type	B	B	B
Operating mode	Low demand mode	Low demand mode	Low demand mode
MTTR	24 hours	24 hours	24 hours
Recommended proof-test interval T_1	1 year	1 year	1 year
SFF	84.4 %	84.9 %	84.6 %
λ_{SD}	0 FIT	0 FIT	0 FIT
λ_{SU}	0 FIT	0 FIT	0 FIT
λ_{DD}	559 FIT	841 FIT	584 FIT
λ_{DU}	103 FIT	149 FIT	106 FIT
λ_{Total}^{*1}	662 FIT	990 FIT	690 FIT
PFD _{avg} (for $T_1 = 1$ year) ^{*2}	4.51×10^{-4}	6.53×10^{-4}	4.64×10^{-4}
MTBF ^{*1}	95 years	58 years	89 years
Fault reaction time ^{*3}	0.4 s / 5 s	0.4 s / 5 s	0.4 s / 5 s

Parameter as per IEC 61508	Value, version 4	Value, version 5	Value, version 6
Safety function	Voltage output 2 inputs	Limit relay 1 input	Limit relay 2 inputs
SIL	2	2	2
HFT	0	0	0
Device type	B	B	B
Operating mode	Low demand mode	Low demand mode	Low demand mode
MTTR	24 hours	24 hours	24 hours
Recommended proof-test interval T_1	1 year	1 year	1 year
SFF	82.4 %	83.3 %	82.7 %
λ_{SD}	0 FIT	0 FIT	0 FIT
λ_{SU}	0 FIT	445 FIT	521 FIT
λ_{DD}	751 FIT	234 FIT	266 FIT
λ_{DU}	160 FIT	158 FIT	167 FIT
λ_{Total}^{*1}	911 FIT	756 FIT	971 FIT
PFD _{avg} (for $T_1 = 1$ year) ^{*2}	7.01×10^{-4}	6.9×10^{-4}	7.3×10^{-4}
MTBF ^{*1}	60 years	78 years	56 years
Fault reaction time ^{*3}	0.4 s / 5 s	0.4 s / 5 s	0.4 s / 5 s

*1	* This value takes into account all failure types. Failure rates of electronic components in accordance with Siemens SN29500. (see "Management Summary - optional")
*2	Where the average temperature when in continuous use is in the region of 50°C, a factor of 1.3 should be taken into account. For further information, see "Management Summary - optional".
*3	Time between fault detection and fault reaction. The time is max. 0.4 seconds. When an RTD or thermocouple is used as the input signal, the time needed to detect a cable open circuit is max. 5 seconds.

Proof-test interval



Proof-test interval as a function of PFD_{avg}

Dangerous undetected failures in this scenario

An incorrect output signal that deviates from the actual measured value by more than 1% but is still in the range of 4 to 20 mA or 2 to 10 V is considered a dangerous, undetected failure.

Operating life of electrical components

The underlying failure rates of electrical components apply within the useful operating life as per IEC 61508-2:2010, section 7.4.9.5. Note 3.

The operating life of the device is determined mainly by the electrolyte capacitors and the ambient temperature. Due to the use of high-quality capacitors, the operating life of the device is 20 years; this assumes an average ambient temperature of 40°C. At higher ambient temperatures, the operating life is shorter.

Behavior of device when in operation and in the event of a fault

The device monitors its inputs as well as its own internal functionalities by means of comprehensive monitoring mechanisms in the device software.

In the event that the device's self-diagnosis function detects a fault, the device reacts as follows:

- Status output (open collector) opens
- Red LED lights up
- Limit relay de-energizes (if activated)
- Analog output issues fault signal (e.g. <3.6mA in failure mode: minimum)
- Display switches to failsafe mode → color of channel affected changes to red and an error is displayed
- Display switches automatically between the active channels and the error display

Installation

All relay outputs used as a safety function must be protected with a 2 A fuse. Alternatively, it is also possible to use a thermomagnetic device circuit breaker or electronic limiter or a miniature circuit breaker with tripping characteristic "Z".

Orientation

The permitted orientations of the device are described in the supplementary device documentation.

Operation

Device behavior when switched on

After it is switched on, the device runs through a diagnostic phase of maximum 20 seconds. During this time, the current output is set to error current ≤ 3.6 mA, the voltage output to 0 V, and the limit relays are de-energized.

Communication via the CDI interface is not possible during the diagnostic phase.

The output signal can only be regarded as safe on successful completion of the diagnostic function.

Behavior of device in the event of alarms and warnings

Analog output:

An fault exists at the output when the assigned input or mathematics channel delivers an error status. The failsafe mode of the output can be configured. The following options can be configured:

Setting	Current output	Voltage output
Min	< 3.6 mA (3.5 mA) ¹⁾	0 V
Max	> 21 mA (22 mA) ¹⁾	11 V

1) actual output value

Limit relay:

An fault exists when the assigned input or mathematics channel delivers an error status. The limit relays are de-energized in the event of a fault.

Alarm and warning messages:

The alarm and warning messages output in the form of error codes provide additional information and are not part of the safety function.

The following table shows the correlation between the error code and the input current/voltage:

Error code*	Meaning	Input current	Input voltage
F041	Sensor/cable open circuit	≤ 2 mA	n/a
F045	Sensor error	2 < x ≤ 3.6 mA ≥ 21 mA	n/a
F101	Below range	≥ 2 mA > 3.6 mA ≤ 3.8 mA (as per Namur)	< 1 V
F102	Above range	> 20.5 mA < 21 mA (as per Namur) ≥ 21 mA (as per Namur)	> 11 V

*) The error codes are listed in the "Diagnosis list" section of Operating Instructions BA00287R/09.

Device configuration

When using the devices in PCS safety instrumented systems, the device configuration must meet the following two requirements:

- Confirmation concept:
Proven, independent verification of the safety-related parameters entered
- Locking concept:
Device locking once configuration is complete (as required by DIN EN 61511-1 §11.6.4 and NE 79 §3)

Device configuration procedure

Device configuration is described in Operating Instructions BA00287R/09. The restrictions detailed in the Safety function section also apply.

Inspection

NOTICE

An inspection of the entire safety function is necessary.

- ▶ Once all of the parameters have been entered, the safety function must be checked before performing the locking sequence!
- ▶ When the device is used as part of a safety function, the complete safety function must be checked after each modification to the device, e.g. a change in the parameter settings.

Locking

⚠ CAUTION

The operation of the device must be locked.

- ▶ Once all of the parameters have been entered and the safety function has been checked, the operation of the device must be locked. This is because a change in the measuring system or in the parameters could compromise the safety function. (→ "Access protection" section of Operating Instructions BA00287R/09).

The configuration software must be locked as follows:

- The device must be locked against access by unauthorized persons;
 - A user code protects the configured parameters: enter 4-digit code: select digit with '+' or '-' and press "E" to confirm the individual digit; once the digit has been confirmed, the cursor moves to the next position, or skips back to the 'System' menu item once the fourth digit has been entered.
 - The lock symbol appears on the display.
- Setup → System → Overfill protect: Select German WHG.



The device status must be changed if the device is configured using the FieldCare PC software, i.e. WHG must be disabled so that parameters can be changed.

Maintenance

No special maintenance work is required on the device.

Proof tests

Safety functions must be tested at appropriate intervals to ensure that they are functioning correctly and are safe.

The time intervals must be specified by the operator.

The "Proof-test interval as a function of PFDavg" diagram (Seite 12) can be used for this purpose.

Proof testing of the device can be performed as follows:

Proof-test procedure

1. Bypass the logic unit or take other appropriate measures to prevent an undesirable reaction in the process.
2. Simulate several defined limit values across the entire input range and verify that the output or limit relay assume a safe state.
 - A safe state means, for example, that $< 3.6\text{mA}$ is present at the current output for at least 4 sec., or that the limit relay is de-energized (see also failsafe mode).
3. Restore the complete operational capability of the loop.
4. Disable the logic unit bypass or restore normal operation in some other way. This test detects approx. 99% of all possible " λ_{DU} " (dangerous undetected) failures of the RMA42 process transmitter.



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

The purpose of a proof test is to detect random device failures. This test does not cover the impact of systematic faults on the safety function, which must be assessed separately. Systematic faults can be caused by operating conditions or corrosion, for example.

Repair

Repair

All repairs to the device must be carried out by Endress+Hauser only.
Please refer to the "Return" section of the associated Operating Instructions .



In the event of failure of a SIL-labeled E+H device operated in a safety function, the "Declaration of Hazardous Material and Decontamination" must be returned with the defective device and include the note "Used as SIL device in safety instrumented system".
The "Declaration of Hazardous Material and Decontamination" can be found in the appendix at the end of this Functional Safety Manual.

Appendix

Commissioning or proof-test protocol

System-specific data	
Company	
Measuring points / TAG no.	
System	
Device type / order code	
Serial number of device	
Name	
Date	
Password (if device-specific)	
Signature	

Device-specific commissioning parameters		
Empty value		
Full value		
Proof-test protocol		
Test stage	Analog output / limit relay	
	Set point	Actual value
Jumper current input	Current: <3.6 mA or > 21 mA Voltage: 0.0 V or 11.0 V Relay: de-energized	
Connect multimeter (accuracy class 1) to current/voltage output		
Imprint a current value of x mA on current output		
Read the current/voltage value at the output and record it (set point e.g. x mA +/- 0.1 mA)		

www.addresses.endress.com
