Level | Pressure | Flow | Temperature | Liquid Analysis | Registration | Systems Components | Services | Solutions

Functional safety manual

RMA422

Process Transmitter

Application

1 to 2-channel transmitter power supply with intrinsically safe current inputs, limit value monitoring with 2 change-over contacts, mathematic functions and 1 to 2 analog outputs to satisfy particular safety systems requirements as per IEC 61508/ IEC 61511-1 (FDIS).

The measuring device fulfils the requirements concerning

- Functional safety as per IEC 61508/IEC 61511-1
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per IEC 61326.

Your benefits

- Use in a safety-instrumented system up to SIL 2, independently evaluated (Functional Assessment) by exida.com as per IEC 61508/ IEC 61511-1

SD009R/09/en

Endress+Hauser

People for Process Automation

Table of contents

SIL-04001a/09/e

SIL Declaration of Conformity

Functional safety of a process transmitter according to IEC 61508/IEC 61511

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

declares as manufacturer, that the process transmitter

RMA 422









is suitable for the use in a safety-instrumented system according to standard IEC 61511-1, provided the relevant safety instructions are observed.

The FMEDA provides the following parameters:

Product	RMA 422 with analogue output						RMA 422 with limit contact	
Analogue input	1			2			1	2
SIL	2							
Proof test interval	1 year							
Device type	B							
HFT [1]	0 (single channel use)							
SFF	> 86 %						> 85 %	
PFD_{AVG} [2]	3.90×10^{-4}			4.50×10^{-4}			3.86×10^{-4}	4.46×10^{-4}
MTBF [3]	160 years			139 years			154 years	134 years
Safety function [4] monitoring	low level	high level	range	low level	high level	range		
λ_{sd} in FIT	245	55	291	283	69	343	9	9
λ_{su} in FIT	286	286	286	328	328	328	493	587
λ_{dd} in FIT	60	250	14	74	289	14	14	14
λ_{du} in FIT	89	89	89	103	103	103	88	102

[1] according to clause 11.4.4 of IEC 61511-1
[2] the value complies with SIL2 according to ISA S84.01 and IEC 61511-1
[3] according to Siemens SN29500
[4] assuming setting of 4 to 20 mA

The device including the modification process was assessed on the basis of prior use.

Nesselwang, 30 January 2004

Endress+Hauser Wetzer GmbH+Co. KG

General manager

Endress+Hauser
The Power of Know How

Introduction

Abbreviations, standards and terms

Abbreviations

Explanation to the abbreviations used can be found in the SIL-Brochure (SI002Z/11).

Relevant standards

Standard	Explanation
IEC 61508, Part 1 – 7	Functional safety of electrical/electronic/programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)
IEC 61511 Part 1 – 3 (FDIS)	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)

Terms

Term	Explanation
Dangerous failure	Failure with the potential to put the safety-related system in a dangerous or non-functional condition.
Safety-related system	A safety-related system performs the safety functions that are required to achieve or maintain a safe condition e.g. in a plant. Example: temperature measuring device – logic unit (e.g. limit signal generator) – valve form a safety-related system.
Safety function	Defined function, which is performed by a safety-related system with the aim of achieving or maintaining a safe condition for the plant, considering a specified dangerous incident. Example: limit temperature monitoring

Determining the Safety Integrity Level (SIL)

The achievable Safety Integrity Level is determined by the following safety-related parameters:
- Average Probability of Failure on Demand (PFD_{AVG})
- Hardware Fault Tolerance (HFT) and
- Safe Failure Fraction (SFF).

The specific safety-related parameters for the RMA422, as a part of a safety function, are listed in the "Safety-related parameters" chapter.

The following table displays the dependence of the "Safety Integrity Level" (SIL) on the "Average Probability of Failure on Demand" (PFD_{AVG}). Here, the "Low demand mode" has been observed, i.e. the requirement rate for the safety-related system is maximum once a year.

Safety Integrity Level (SIL)	PFD_{AVG} (Low demand mode)
4	$\geq 10^{-5} ... < 10^{-4}$
3	$\geq 10^{-4} ... < 10^{-3}$
2	$\geq 10^{-3} ... < 10^{-2}$
1	$\geq 10^{-2} ... < 10^{-1}$

Sensor, process transmitter, logic unit and actuator together form a safety-related system, which performs a safety function. The "Average Probability of Failure on Demand" (PFD_{AVG}) is usually divided up into the sensor, process transmitter, logic unit and actuator sub-systems as per Figure 1.

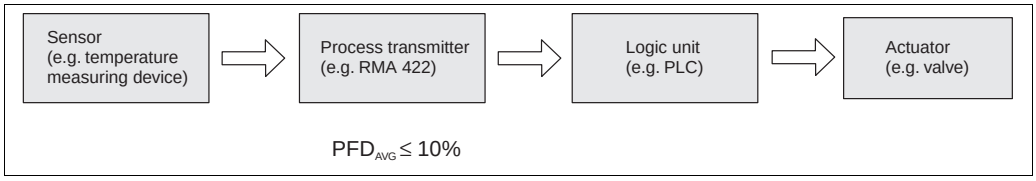

Fig. 1: Share of the process transmitter in the "average probability of dangerous failure on demand" (PFD_{AVG}

Note!
This documentation considers the RMA422 as a component of a safety function.

Safety Integrity Level RMA422 (Type B)
The following table displays the achievable "Safety Integrity Level" (SIL) of the entire safety-related system for type B systems depending on the "Safe Failure Fraction" (SFF) and the "Hardware Fault Tolerance" (HFT). Type B systems are, for example, sensors with complex components such as ASICs (→ see also IEC 61508, Part 2).

Safe Failure Fraction (SFF)	**Hardware Fault Tolerance (HFT)**		
	0	**1 (0)[1)]**	**2 (1)[1]**
< 60%	not permitted	SIL 1	SIL 2
60 ...< 90 %	SIL 1	**SIL 2**	SIL 3
90 ...< 99 %	SIL 2	SIL 3	–
≥ 99 %	SIL 3	–	–

1) In accordance with IEC 61511-1 (FDIS), Clause 11.4.4, the "Hardware Fault Tolerance" (HFT) can be reduced by one (values in brackets), if the following conditions are true for devices using sensors and actuators with complex components:
– The device is "proven in use".
– The device allows adjustment of process-related parameters only, e.g. measuring range, upscale or downscale failure direction, etc.
– The adjustment level of the process-related parameters of the device is protected, e.g. by jumper, password (here: numeric code or key combination)
– The function has a "Safety Integrity Level" (SIL) requirement less than 4.
All conditions are true for the RMA422.

Safety function with RMA422

Safety function for limit temperature monitoring

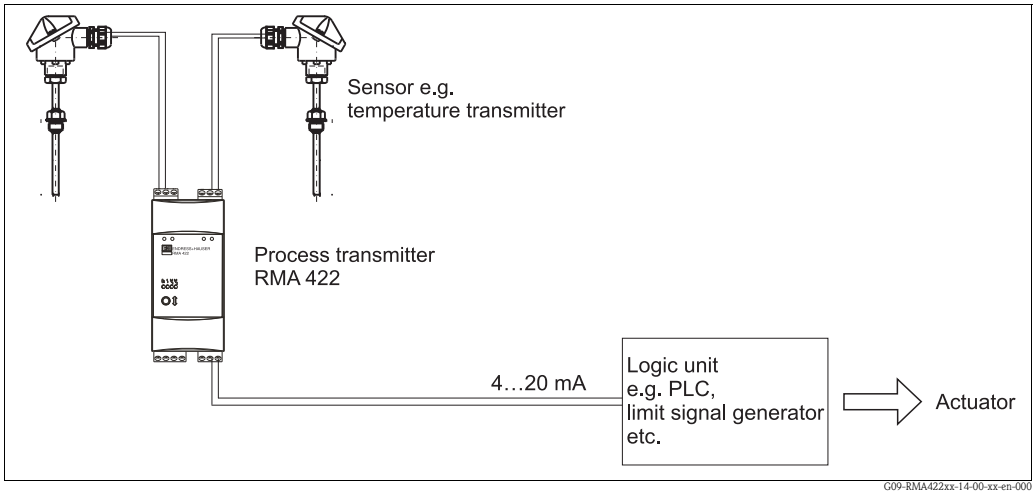

Fig. 2: Safety function with analog output

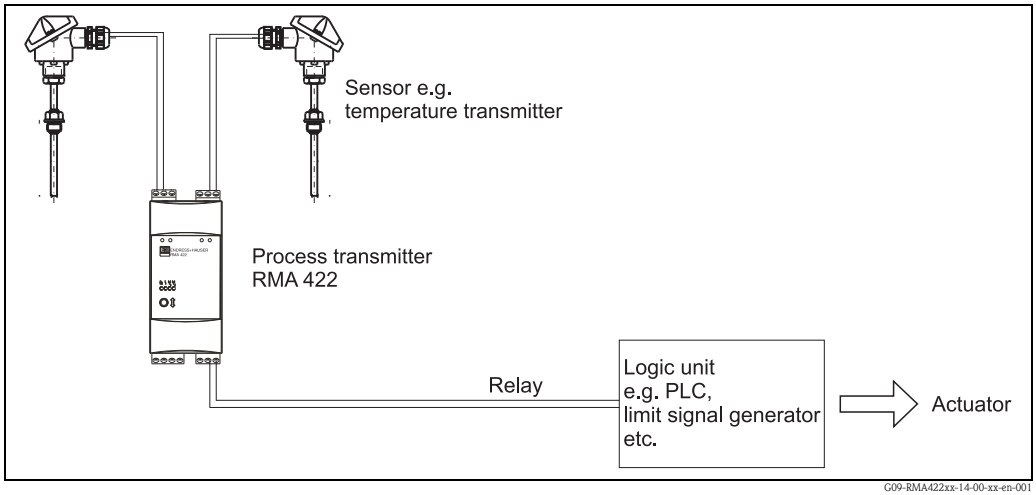

Fig. 3: Safety function with relay

The sensors, powered by the RMA422 process transmitter, generate an analog signal (4 to 20 mA) in proportion to the measured value. Mathematic functions allow the formation of a new process variable. The process transmitter makes the analog signals in proportion to the new process variable available to a downstream logic unit, such as a PLC. The limit values can also be monitored directly with the RMA422 by means of 2 change-over contacts.

Safety function data

Caution!
The data for the safety functions are listed in the "Safety-related parameters" chapter.

Note!
MTTR is set at eight hours.
Safety-related systems without a self-locking function must be monitored or set to an otherwise safe state after carrying out the safety function within MTTR.

Unit version

SIL from serial number: 5C00104114, December 2002

Supplementary device documentation RMA422

Depending on the version, the following documentation must be available for the Process transmitter RMA422:

Explosion protection/Certificates	Operating instructions	Other Ex-Documentation
none	BA103R	none
ATEX II(1)GD [EEx ia] IIC	BA103R	Safety instructions XA003R

Caution!
- The installation and setting instructions, and the technical limit values must be observed in accordance with the Operating Instructions (BA103R).
- For devices which are used in explosion-hazardous, the supplementary documentation (XA) resp. Control Drawings must also be used in accordance with the table.

RMA422 supplementary documentation
For further information, see Technical Information TI072R.

Commissioning and iterative tests

Using the RMA422 for continuous measurements

The operability of the safety installation must be tested at appropriate time intervals. It is the responsibility of the user to select the type of check and the intervals in the specified time frame. The test must be completed in such a way that the fault free function of the safety installation combined with all components can be validated.

Settings

Settings

It is possible to set up on the RMA422. When used as part of a safety function, an analog signal or a limit relay can be used. Please refer to the following table for information on the settings which are permitted or not when using the RMA422 in a safety-related application.

RMA422 with current output:

Parameter	Setting up selections	Setting for safety function
Output range	4-20 mA	permitted
	0-20 mA	not permitted
	0-10 V	not permitted
Fault condition	hold	not permitted
	min	permitted
	max	permitted

RMA422 with relay:

Parameter	Setting up selections	Setting for safety function
Operating mode	off	not permitted
	min	permitted
	max	permitted
	trd	permitted
	alarm	permitted
	min-	not permitted
	max-	not permitted
	trd-	not permitted

For further information see the BA103R operating instructions.

Caution!
Check the safety function after entering all the parameters.

Locking

Device operation has to be locked to protect the process-related parameters from being altered. This is done using a code which is selected by the user.

Parameter	Setting up selection	Setting for safety function
User code	0000 to 9999	0001 to 9999 (0000 is not permitted, because no user code is active)

Safety-related parameters

Specific safety-related parameters for RMA422

The table displays the specific safety-related parameters for the RMA422:

	With analog input 4-20 mA and analog output 4-20 mA	With 2 analog inp. 4-20 mA and analog output 4-20 mA	With analog input 4-20 mA and relay	With 2 analog inp. 4-20 mA and relay
SIL	SIL 2	SIL 2	SIL 2	SIL 2
HFT	0	0	0	0
SFF	> 86%	> 86%	> 85%	> 85%
PFD_{AVG}	$3{,}90 \times 10^{-4}$	$4{,}50 \times 10^{-4}$	$3{,}86 \times 10^{-4}$	$4{,}46 \times 10^{-4}$
TI [1]	annual	annual	annual	annual

1) complete function test

PFD_{AVG} dependent on selected maintenance interval

The following diagram presents the dependence of the PFD_{AVG} on the maintenance interval. The PFD_{AVG} increases as the maintenance interval increases.

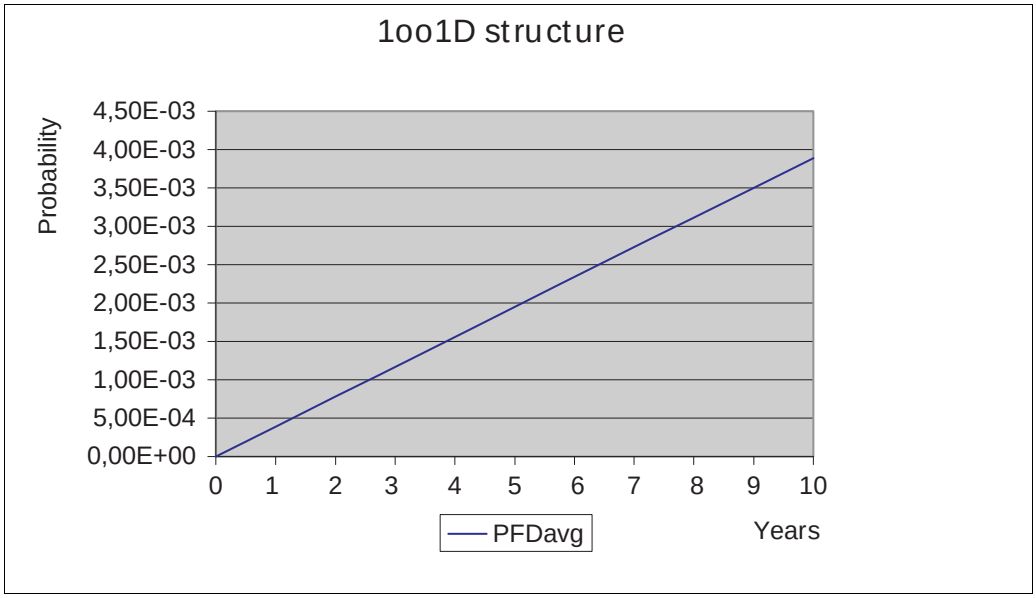

Fig. 4: "Average probability of dangerous failure on demand" (PFD_{AVG}) depending on the maintenance interval selected for the RMA422 with analog input 4-20 mA and analog output 4-20 mA.

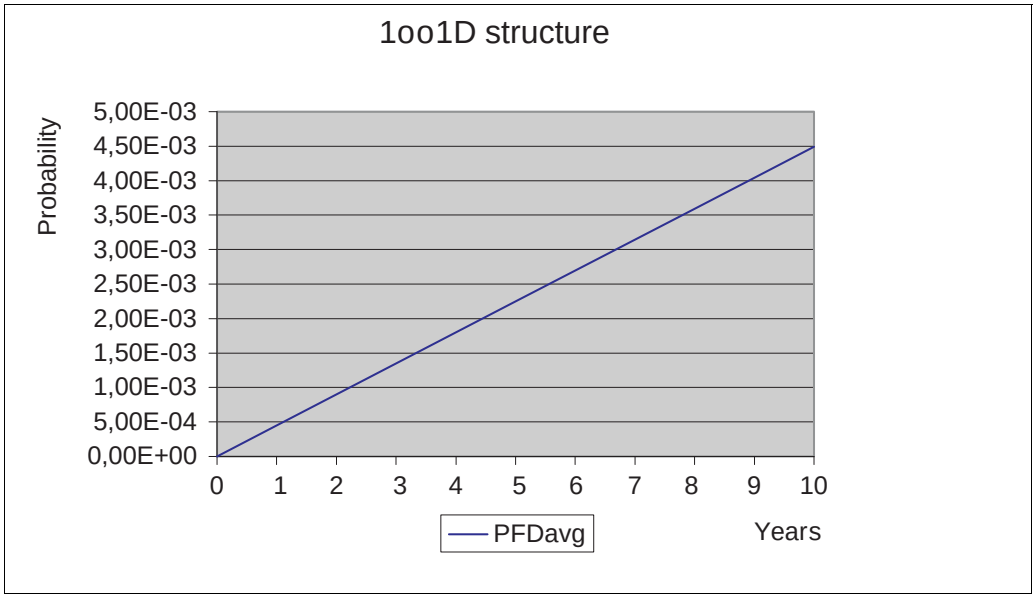

Fig. 5: "Average probability of dangerous failure on demand" (PFD_{AVG}) depending on the maintenance interval selected for the RMA422 with 2 analog inputs 4-20 mA and analog output 4-20 mA.

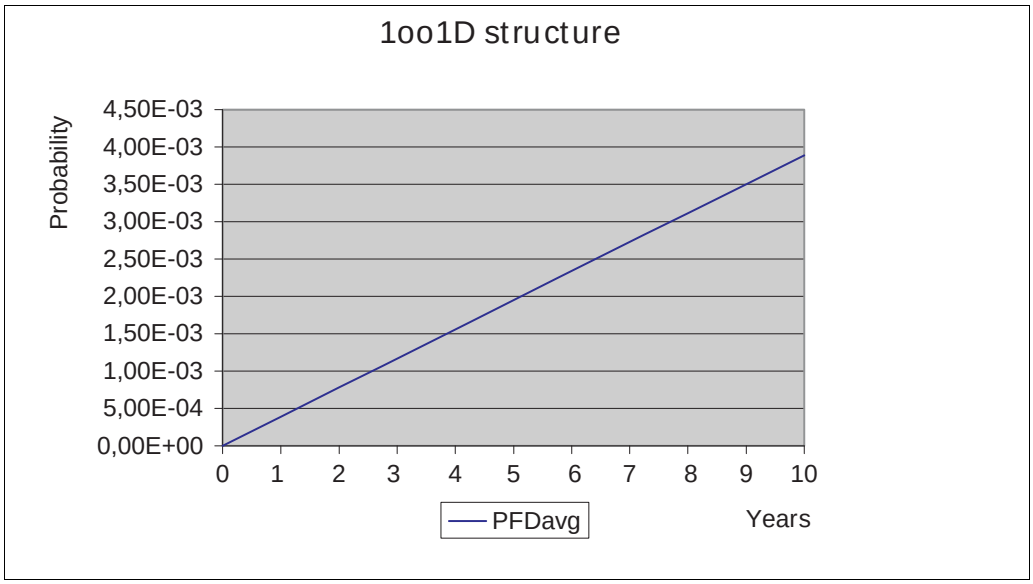

Fig. 6: "Average probability of dangerous failure on demand" (PFD_{AVG}) depending on the maintenance interval selected for the RMA422 with analog input 4-20 mA and relay.

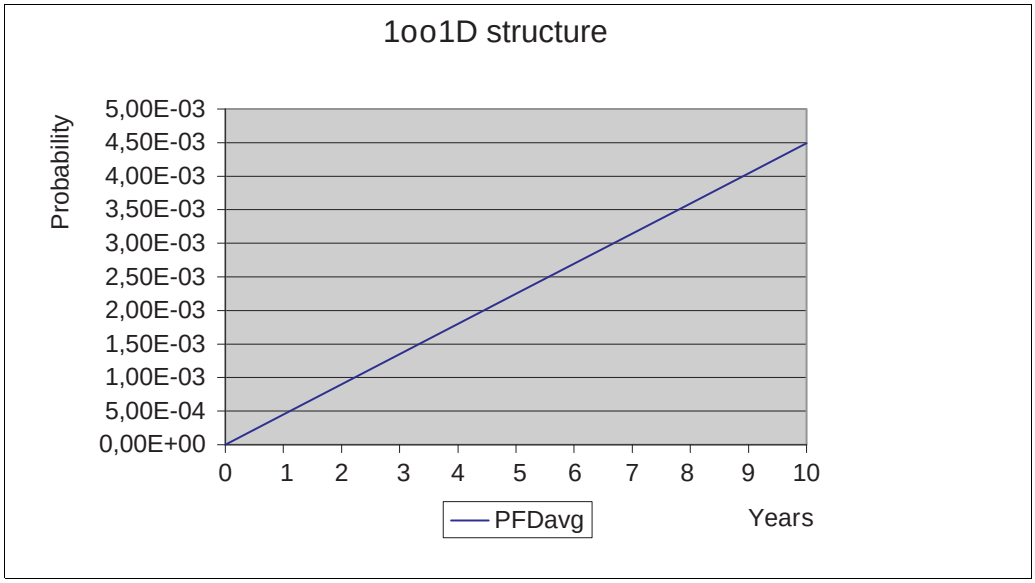

Fig. 7: "Average probability of dangerous failure on demand" (PFD_{AVG}) depending on the maintenance interval selected for the RMA422 with 2 analog inputs 4-20 mA and relay.

Repair

Repair

Note!
Together with the failed, SIL-marked E+H device, having been operated in a functional safety application, the form "Declaration of Hazardous Material and De-Contamination" containing the appropriate information "☒ Used as SIL device in a Safety Instrumented System" has to be returned.
The "Declaration of Hazardous Material and De-Contamination" can be found in the Appendix at the end of this Functional Safety Manual.

FMEDA and Prior-use Assessment

Project:
Process Transmitter RMA 422

Customer:

Endress+Hauser Wetzer GmbH + Co. KG
Nesselwang
Germany

Contract No.: E+H 03/02-17
Report No.: E+H 03/02-17 R021
Version V1, Revision R1.0, January 2004
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with prior-use consideration according to IEC 61508 / IEC 61511 carried out on the Process Transmitter RMA 422 with software version V 1.12.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. However, as the module under consideration is only one part of an entire safety function it should not claim more than 10% of this range. For a SIL 2 application the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the process transmitter would then be 1,00E-03.

The Process Transmitter RMA 422 is considered to be a Type B[1] component with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

For safety applications only the current or relay output shall be used. All other possible output variants or electronics are not covered by this report.

As the Process Transmitter RMA 422 is supposed to be a proven-in-use device, an assessment of the hardware with additional prior-use demonstration for the device was carried out. The prior-use investigation was based on field return data collected and analyzed by Endress+Hauser Wetzer GmbH + Co. KG.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.2 the device is considered to be suitable for use in SIL 2 safety functions. The decision on the usage of prior-use devices, however, is always with the end-user.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on whether the Process Transmitter RMA 422 is used in an application for “low level monitoring”, “high level monitoring” or “range monitoring”. For these applications the following tables show how the above stated requirements are fulfilled.

Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 1: Summary for RMA 422 with current output and one input – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,90E-04	PFD_{AVG} = 1,95E-03	PFD_{AVG} = 3,89E-03

Table 2: Summary for RMA 422 with current output and one input – Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	245 FIT	286 FIT	60 FIT	89 FIT	> 86%	46%	40%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	55 FIT	286 FIT	250 FIT	89 FIT	> 86%	16%	74%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	291 FIT	286 FIT	14 FIT	89 FIT	> 86%	50%	14%

Table 3: Summary for RMA 422 with current output and two inputs – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 4,50E-04	PFD_{AVG} = 2,25E-03	PFD_{AVG} = 4,49E-03

Table 4: Summary for RMA 422 with current output and two inputs – Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	283 FIT	328 FIT	74 FIT	103 FIT	> 86%	46%	42%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	69 FIT	328 FIT	289 FIT	103 FIT	> 86%	17%	74%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	343 FIT	328 FIT	14 FIT	103 FIT	> 86%	51%	12%

[2] DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for RMA 422.

Table 5: Summary for RMA 422 with relay output and one input – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,86E-04	PFD_{AVG} = 1,93E-03	PFD_{AVG} = 3,85E-03

Table 6: Summary for RMA 422 with relay output and one input – Failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
9 FIT	493 FIT	14 FIT	88 FIT	> 85%	2%	14%

Table 7: Summary for RMA 422 with relay output and two inputs – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 4,46E-04	PFD_{AVG} = 2,23E-03	PFD_{AVG} = 4,45E-03

Table 8: Summary for RMA 422 with relay output and two inputs – Failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
9 FIT	587 FIT	14 FIT	102 FIT	> 85%	2%	12%

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03.

The functional assessment has shown that the Process Transmitter RMA 422 has a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of > 85%. Based on the verification of "prior use" it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the Process Transmitter RMA 422 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). The complete list of failure rates is presented in section 5.1 to 5.4 along with all assumptions.

The two inputs and the two outputs on each module shall not be used to increase the hardware fault tolerance, needed to achieve a higher SIL for a certain safety function, as they contain common components. The two inputs are only allowed to be used to combine two safety critical input signals using the basic mathematics modes of addition / subtraction / multiplication to calculate further process values.

It is important to realize that the “don’t care” failures and the “annunciation” failures are classified as “safe undetected” failures according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

Declaration of Hazardous Material and De-Contamination

Endress+Hauser

People for Process Automation

Declaration of Hazardous Material and De-Contamination
Erklärung zur Kontamination und Reinigung

RA No. ☐☐☐☐☐☐☐☐

Please reference the Return Authorization Number (RA#), obtained from Endress+Hauser, on all paperwork and mark the RA# clearly on the outside of the box. If this procedure is not followed, it may result in the refusal of the package at our facility.
Bitte geben Sie die von E+H mitgeteilte Rücklieferungsnummer (RA#) auf allen Lieferpapieren an und vermerken Sie diese auch außen auf der Verpackung. Nichtbeachtung dieser Anweisung führt zur Ablehnung ihrer Lieferung.

Because of legal regulations and for the safety of our employees and operating equipment, we need the "Declaration of Hazardous Material and De-Contamination", with your signature, before your order can be handled. Please make absolutely sure to attach it to the outside of the packaging.
Aufgrund der gesetzlichen Vorschriften und zum Schutz unserer Mitarbeiter und Betriebseinrichtungen, benötigen wir die unterschriebene "Erklärung zur Kontamination und Reinigung", bevor Ihr Auftrag bearbeitet werden kann. Bringen Sie diese unbedingt außen an der Verpackung an.

Type ofi nstrument / sensor
Geräte-/Sensortyp _____

Serial number
Seriennummer _____

☐ Used as SIL device in a Safety Instrumented System / *Einsatz als SIL Gerät in Schutzeinrichtungen*

Process data/ *Prozessdaten*

Temperature / *Temperatur* _____ [°C]
Conductivity / *Leitfähigkeit* _____ [S]
Pressure / *Druck* _____ [Pa]
Viscosity / *Viskosität* _____ [mm²/s]

Instruments International

Endress+Hauser
Instruments International AG
Kaegenstrasse 2
4153 Reinach
Switzerland

Tel. +41 61 715 81 00
Fax +41 61 715 25 00
www.endress.com
info@ii.endress.com

Endress+Hauser

SD009R/09/en/13.10
FM+SGML 6.0 ProMoDo