Functional safety manual
RB223
Passive barrier

Application
Galvanic isolation of active 0/4 to 20 mA signals from transmitters, valves and adjusters, when used in safety relevant applications to satisfy particular safety systems requirements as per IEC 61508:2010 (Edition 2.0).

The passive barrier fulfills the requirements concerning
- Functional safety as per IEC 61508:2010 (Edition 2.0)
- Explosion protection (depending on the version)
- Electromagnetic compatibility as per IEC 61326 series and NAMUR recommendation NE 21
- Electrical safety as per IEC/EN 61010-1

Your benefits
- Used in safety relevant applications to satisfy particular safety systems requirements up to SIL 3,
  – independently evaluated (Hardware Assessment) by exida.com as per IEC 61508:2010 (Edition 2.0)

Endress+Hauser
People for Process Automation

Table of contents

SIL Declaration of Conformity

SIL-13002a/09

Endress+Hauser
People for Process Automation

SIL-Declaration of Conformity

Functional Safety according to IEC 61508 / 61511
Supplement 1 / NE130 Form B.1 and IGR 49-02-15 Datasheet 1

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

declares as manufacturer, that the following type of the

RB223

is suitable for the use in safety-instrumented systems according to IEC61508, if the safety instructions and following parameters are observed.

This declaration of conformity is only valid for products being in the delivery status and produced after the following date of issue.

Nesselwang, 03.12.2013
Endress+Hauser Wetzer GmbH+Co. KG

Harald Hertweck
Managing Director

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

1/2

SIL-13002a/09

Endress+Hauser
People for Process Automation

General				
Device designation and permissible types	Passive barrier, type RB223-xxA, type RB223-xxB			
Safety-related output signal	4...20mA			
Fault current	≤ 3.6mA or ≥ 21mA			
Process variable/function	loop current			
Safety function(s)	4..20mA output signal			
Device type acc. to IEC 61508-2	☒ Type A	☐ Type B		
Operating mode	☒ Low Demand Mode	☒ High Demand or Continuous Mode		
Valid Hardware-Version	01.03.xx			
Valid Software-Version	n/a			
Safety manual	SD00011R/09			
Type of evalutation (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		
Assessment through – report no.	Exida E+H Wetzer 13/03-087 R041			
Test documents	Develop. documents	Test reports	Data sheets	
SIL - Integrity				
Systematic safety integrity		☐ SIL 2 capable	☒ SIL 3 capable	
Hardware safety integrity	Single channel use (HFT = 0)	☐ SIL 2 capable	☒ SIL 3 capable	
	Multi channel use (HFT ≥1)	☐ SIL 2 capable	☐ SIL 3 capable	

FMEDA				
Safety function	Measurement signal output			
Application	RB223-A to a safety PLC	RB223-A to an actuator	RB223-B to a safety PLC	RB223-B to an actuator
λ_{DU} *1)	0 FIT	0 FIT	0 FIT	5 FIT
λ_{DD} *1)	47 FIT	47 FIT	44 FIT	39 FIT
λ_{SU} *1)	0 FIT	0 FIT	0 FIT	0 FIT
λ_{SD} *1)	0 FIT	0 FIT	0 FIT	0 FIT
SFF - Safe Failure Fraction	100 %	100 %	100 %	88 %
PTC *2)	99 %	99 %	99 %	99 %
λ_{total} *1)	47 FIT	47 FIT	44 FIT	44 FIT
Diagnostic test interval / fault reaction time *3)	n/a / n/a	n/a / n/a	n/a / n/a	n/a / n/a

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 breakdown per 10^9 h
*2) PTC = Proof Test Coverage (Diagnostic coverage for manual proof tests)
*3) A-type devices no diagnostic time and fault reaction time

2/2

Introduction

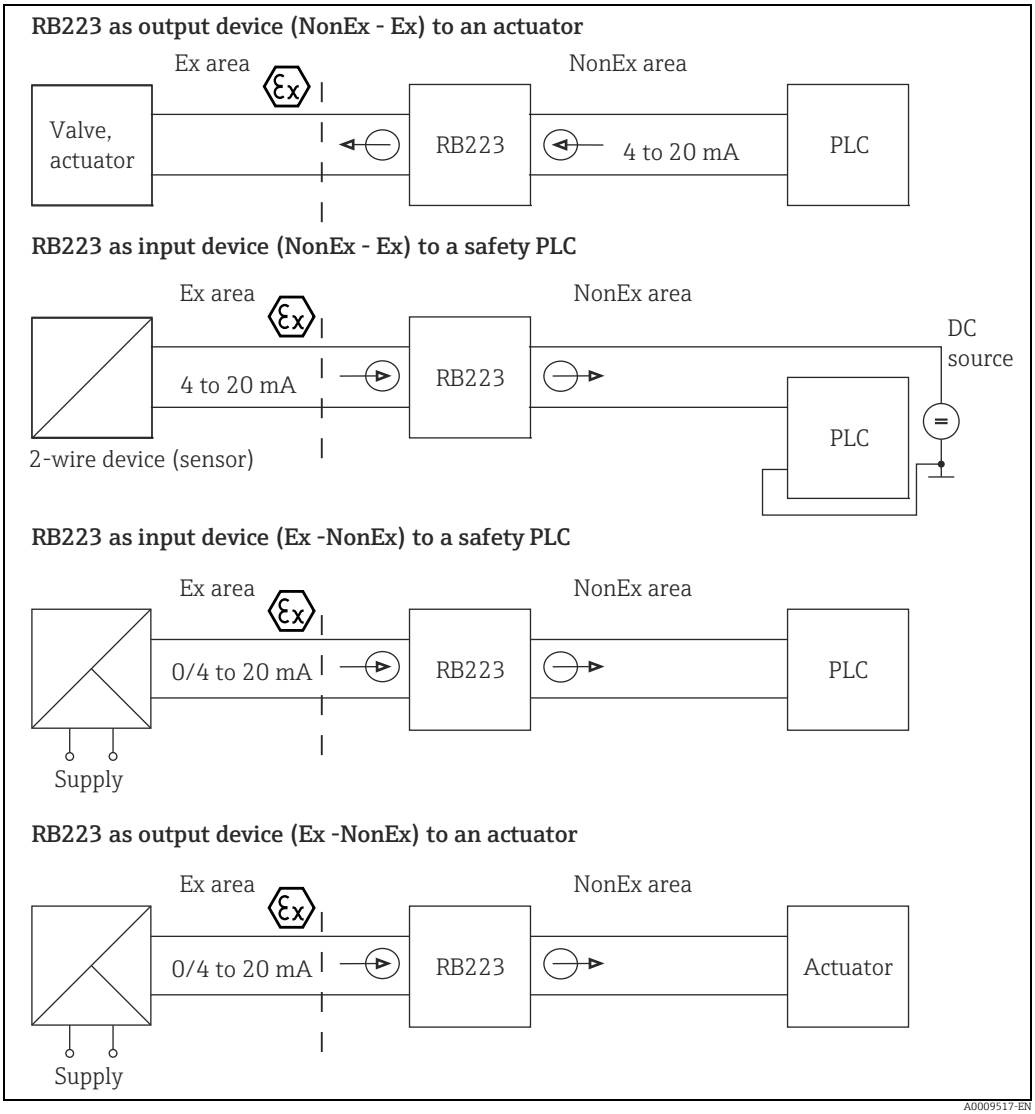
Introduction

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 CP002Z "Functional Safety in the Process Industry - Risk Reduction with Safety Instrumented Systems".

Measuring system design

System components

The diagram below displays a measuring system with exemplary devices.

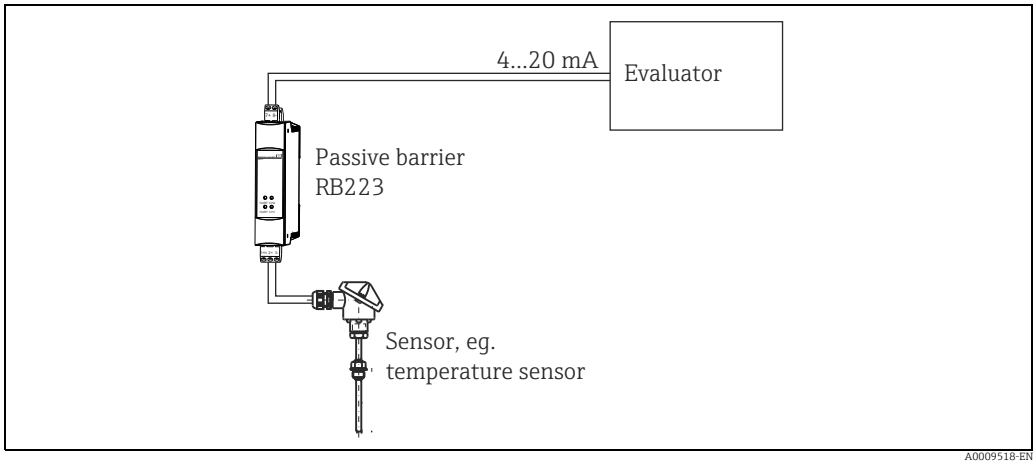


Part of the passive barrier at the "average probability of failure on demand of a safety-related system" (PFD_{AVG})

This documentation treats the RB223 as part of the safety function.

Sensor, passive barrier and logic unit form a safety-related system, which carries out a safety function. The "average probability of failure on demand of the entire safety-related system" (PFDavg) is divided among the sensor, passive barrier and logic unit.

Description of the application as a safety-instrumented system



Example of the application "limit value monitoring"

The device separates active 4...20 mA signals of transmitters, valves and actuators. It comprises an analog input and an intrinsically safe analog output, or an output and an intrinsically safe input respectively.
As an option, the device is available as a 2-channel device. The barrier is implemented for the intrinsically safe operation of sensors, valves and actuators.
The device is supplied from the current loop, it has no separate power supply.

Permitted device types

The functional safety assessment described in this manual applies to the device versions listed below and is valid from the stated software and hardware versions.

Valid hardware version (electronics): from **01.00.00** (Hardware revision Production_A)
In the event of device modifications, a modification process compliant with IEC 61508 is applied. Unless otherwise indicated, all subsequent versions can also be used for safety-instrumented systems.

Device versions valid for use in safety-related applications:

Feature	Designation	Version
010	Approval	A, B, C, D
020	Channels	1, 2
030	Transmission direction	A, B

Further applicable device documentation RB223

Documentation	Contents	Notes
Technical Information TI132R/09	▪ Technical data ▪ Notes on accessories	
Operating Instructions BA239R/09	▪ Identification ▪ Installation ▪ Wiring ▪ Operation ▪ Commissioning ▪ Maintenance ▪ Accessories ▪ Troubleshooting ▪ Technical data ▪ Appendix: Presentation of menus	
Safety instructions depending on the chosen "Approval" feature.	Safety, installation and operating instructions for devices, which are suitable for use in potentially explosive atmospheres	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

When used as part of a safety function the measuring signal of the output side 4 to 20 mA can be used.

Safety-related signal

The safety-related signal is the analog measurement signal of the output side 4 to 20mA. All safety measures refer exclusively to the output signal.
The safety-related output signal is sent to a downstream logic unit, e.g. a programmable logic controller or a limit signal transmitter, and monitored there to establish if:

- A specified limit has been overshot
- A fault has occurred, e.g. error current in accordance with Namur recommendation 43 (≤ 3.6 mA, ≥ 21mA, signal cable disconnection or short-circuit).

Restrictions for use in safety-related applications

- The designated use of the measuring system and environmental conditions must be observed.
- Notes on critical process situations and installation conditions from the operating instructions (Chapter 4 in BA239R/09) have to be observed.
- Observe application-specific restrictions.
- The specifications from the Operating Instructions must not be violated.
- The device must be secured against unintentional operation / modification.
- Only one input and one output are part of the safety function under consideration
- A complete function test of the safety-related functions has to be carried out during commissioning.

MTTR is set to 24 hours.
Safety-related systems without self-locking function must be brought to a monitored or otherwise safe state within MTTR after executing the safety function.

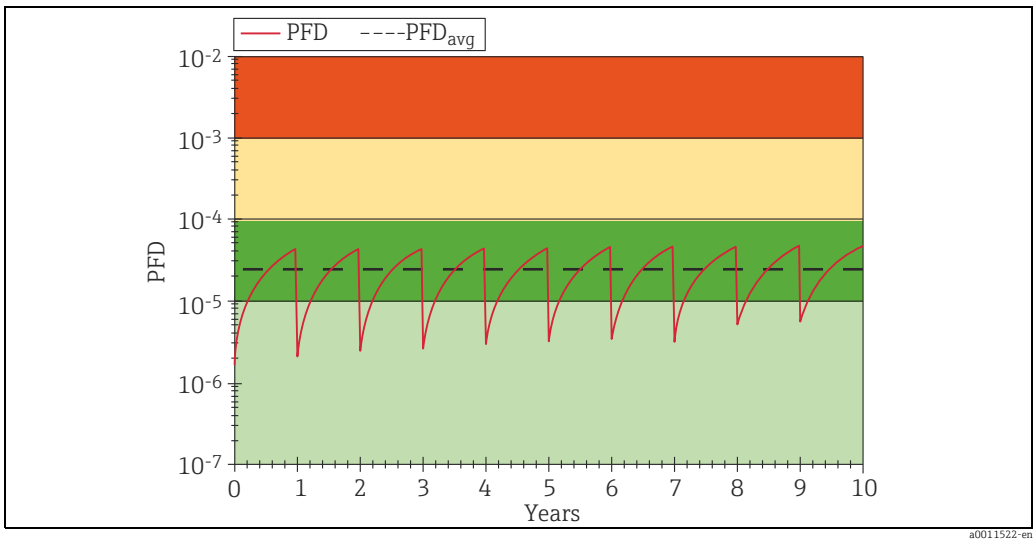
Functional safety parameters

The table shows specific parameters relating to functional safety:

Parameter as per IEC 61508	RB223-A to a safety PLC	RB223-A to an actuator	RB223-B to a safety PLC	RB223-B to an actuator
Protection function	Output side 4 to 20mA	Output side 4 to 20mA	Output side 4 to 20mA	Output side 4 to 20mA
SIL AC	3	3	3	3
HFT	0	0	0	0
Device type	A	A	A	A
Operating mode	Low/high demand mode	Low/high demand mode	Low/high demand mode	Low/high demand mode
MTTR	24 hours	24 hours	24 hours	24 hours
Recommended proof-test interval T[Proof]	1 year	1 year	1 year	1 year
SFF	100 %	100 %	100 %	88 %
λ_{SD}	0 FIT	0 FIT	0 FIT	0 FIT
λ_{SU}	0 FIT	0 FIT	0 FIT	0 FIT
λ_{DD}	47 FIT	47 FIT	44 FIT	39 FIT
λ_{DU}	0 FIT	0 FIT	0 FIT	5 FIT
λ_{Total} *1	47 FIT	47 FIT	44 FIT	44 FIT
PFD_{avg} (for T[Proof] = 1 year) *2	1.06×10^{-6}	1.06×10^{-6}	1.06×10^{-6}	2.48×10^{-5}
PFH	0	0	0	5×10^{-9}
MTBF *1	1188 years	1188 years	1188 years	1188 years

*1	This value takes into account all failure types. Failure rates of electronics 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".

Proof-test interval



Proof-test interval depending on the PFDavg

Operating life of electrical components

The underlying failure rates of electrical components apply within the usable operating life in accordance with IEC 61508-2:2010 Section 7.4.9.5 Note 3.

According to DIN EN 61508-2:2011 Note 3 [N3)], longer operating life spans can be reached through suitable measures by the manufacturer and the operator.

Installation

Installation, wiring, commissioning
Installation, wiring and commissioning of the device are described in the current Operating Instructions BA239R/09.

Maintenance

No special maintenance work is required on the device.

Proof tests

Proof tests

Safety functions must be tested at appropriate intervals to ensure that they are functioning correctly and are safe. The intervals must be specified by the operator.
The "Proof-test interval depending on the PFDavg" graphic can be used for this purpose.
The device proof test can be performed as follows:

Procedure for proof test

Steps to test the RB223 as an input barrier for a safety PLC

1. Bypass the logic unit or take other suitable measures to prevent an unwanted reaction in the process.
2. Simulate several defined limit values across the entire range on the passive barrier RB223 and verify that the output or the limit relays go to a safe state.
3. Simulate the upper and lower alarm limit value on the passive barrier RB223 and verify that the output shows the expected behavior.
4. Disable bypassing of the logic unit or restore normal operation in some other way.

Steps to test the RB223 as an input barrier for an actuator

1. Bypass the logic unit or take other suitable measures to prevent an unwanted reaction in the process.
2. Feed 3.6 mA control signal to the RB223 in order to open / close the valve and verify that the valve is opened / closed.
   The prerequisite for this is that the valve has been successfully tested without the passive barrier and does not contain any dangerous undetected errors.
3. Feed a 4 to 20 mA control signal in 1 mA steps to the passive barrier in order to open / close the valve and verify that the valve opens / closes accordingly.
   The prerequisite for this is that the valve has been successfully tested without the passive barrier and does not contain any dangerous undetected errors.
4. Disable bypassing of the logic unit or restore normal operation in some other way.

This test detects approx. 99% of all possible "du" (dangerous undetected) failures of the RB223 passive barrier.

NOTICE

The device may no longer be used as part of a safety-instrumented system if one of the criteria of the test procedures described above is not fulfilled.

- The proof test is used to detect random device failures. It does not cover the influence of systematic faults on the safety function, which must be checked separately. Operating conditions or corrosion, for example, can cause systematic faults.

Repair

Repair

All repairs to the RB223 must be carried out by Endress+Hauser only.
In the event of failure of a SIL-labeled Endress+Hauser device, which has been used in a safety-instrumented system, the "Declaration of Hazardous Material and De-contamination", with the corresponding note "Used as SIL device in a Safety Instrumented System", must be enclosed when the defective device is returned.
Please read the information in the Section "Return" of the appropriate Operating Instructions".

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		
Proof-test protocol		
Test stage	Measurement signal (output)	
	Set point	Actual
Jumper current input	Current: ≤ 3.6 mA or ≥ 21mA	
e.g. to logic unit: Connect multimeter (accuracy class 1) to output side (7+ and 8- or 9+ and 10-). e.g. to actuator: Connect multimeter (accuracy class 1) to output side (1+H or 2+ and 3- or 4+H or 5+ and 6-)		
e.g. to logic unit: Feed a current of x mA on the input side (1+H or 2+ and 3- or 4+H or 5+ and 6-) e.g. to an actuator: Feed a current value of x mA on the input side (7+ and 8- or 9+ and 10-)		
Read the current/voltage value on the output side and record it (set point e.g. x mA +/- 0.1 mA)		

Exida.com management summary

Failure Modes, Effects and Diagnostic Analysis

Project:
Barrier RB223 (loop powered)

Customer:
Endress+Hauser Wetzer GmbH + Co. KG
Nesselwang
Germany

Contract No.: E+H Wetzer 13/03-087
Report No.: E+H Wetzer 13/03-087 R041
Version V2, Revision R1; July 2013

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the loop powered barrier RB223 with hardware version as shown in the referred circuit diagrams (see section 2.5.1). Table 1 gives an overview of the different versions that belong to the considered devices.

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.

Table 1: Version overview

Type	Description
RB223-A1B NonEx -> Ex; SAP no. 71044040	1 channel, no Ex approval
RB223-A2B NonEx -> Ex; part no. 71044046	2 channels, no Ex approval
RB223-B1B NonEx -> Ex; part no. 71044040	1 channel, Ex approval
RB223-B2B NonEx -> Ex; part no. 71044046	2 channels, Ex approval
RB223-A1A Ex -> NonEx; part no. 71044043	1 channel, no Ex approval
RB223-A2A Ex -> NonEx; part no. 71044047	2 channels, no Ex approval
RB223-B1A Ex -> NonEx; part no. 71044043	1 channel, Ex approval
RB223-B2A Ex -> NonEx; part no. 71044047	2 channels, Ex approval

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500. This failure rate database is specified in the safety requirements specification from Endress+Hauser Wetzer GmbH + Co. KG for the loop powered barrier RB223.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

The loop powered barrier RB223 can be considered to be a Type A[1] element with a hardware fault tolerance of 0.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the loop powered barrier RB223 with 4..20 mA current output communicates detected faults by an alarm output current ≤ 3.6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled.

[1] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

Table 2: RB223 as input device (NonEx → Ex) to a safety PLC – IEC 61508 failure rates

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**44**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	11
Fail Low (λ_{L})	33
Fail Dangerous Undetected (λ_{DU})	**0**

No effect	41
No part	11

Total failure rate of the safety function (λ_{Total})	**44**
Safe failure fraction (SFF) [2]	**100%**
DC_D	**0%**

SIL AC [3]	**SIL 3**

[2] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[3] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled.

Table 3: RB223 as input device (Ex → NonEx) to a safety PLC – IEC 61508 failure rates

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**47**
Fail Dangerous Detected (λ_{dd})	0
Fail High (λ_{H})	0
Fail Low (λ_{L})	47
Fail Dangerous Undetected (λ_{DU})	**0**

No effect	45
No part	8

Total failure rate of the safety function (λ_{Total})	**47**
Safe failure fraction (SFF) [4]	**100%**
DC_D	**0%**

SIL AC [5]	**SIL 3**

[4] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[5] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled.

Table 4: RB223 as output device (NonEx → Ex) to an actuator – IEC 61508 failure rates

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**39**
Fail Dangerous Detected (λ_{dd})	0
Fail Low (λ_{L})	39
Fail Dangerous Undetected (λ_{DU})	**5**
Fail Dangerous Undetected (λ_{du})	0
Fail High (λ_{H})	5

No effect	41
No part	11

Total failure rate of the safety function (λ_{Total})	**44**
Safe failure fraction (SFF) [6]	**88%**
DC_D	**88%**

SIL AC [7]	**SIL 2**

[6] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[7] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled.

Table 5: RB223 as output device (Ex → NonEx) to an actuator – IEC 61508 failure rates

Failure category	Siemens SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**47**
Fail Dangerous Detected (λ_{dd})	0
Fail Low (λ_{L})	47
Fail Dangerous Undetected (λ_{DU})	**0**
Fail Dangerous Undetected (λ_{du})	0
Fail High (λ_{H})	0
No effect	45
No part	8
Total failure rate of the safety function (λ_{Total})	**47**
Safe failure fraction (SFF) [8]	**100%**
DC_D	**0%**
SIL AC [9]	**SIL 3**

The failure rates are valid for the useful life of the loop powered barrier RB223 (see Appendix 2).

[8] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply that all related IEC 61508 requirements are fulfilled.

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* _____ [mm^2/s]

www.addresses.endress.com

Endress+Hauser

People for Process Automation