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

Functional safety manual

RB223

Passive barrier

Application

Galvanic isolation of active 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/ IEC 61511-1.

The passive barrier fulfils the requirements concerning

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

SD011R/09/en

Endress+Hauser

People for Process Automation

Table of contents

SIL-06001a/09/e

Manufacturer declaration

FMEDA including SFF determination and PFD_{AVG} calculation according to IEC 61508

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

declares as manufacturer, that the hardware assessment according to IEC 61508 has shown that the passive barrier

RB223

has a PFD_{AVG} within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of > 90.4%, provided the relevant safety instructions are observed.

The FMEDA provides the following parameters:

Device type	A	
HFT	0	
	As output device (NonEx -> Ex) to an actuator	As output device (Ex -> NonEx) to an actuator
Proof test interval	1 year	10 years
SFF [1]	> 90.4 %	> 99.6 %
PFD_{AVG} [2]	3.66×10^{-5}	1.31×10^{-5}
MTBF [3]	1239 years	1112 years
λ_{safe}	79 FIT	97 FIT
$\lambda_{dangerous}$	8 FIT	0.3 FIT

[1] according to table 2 of IEC61508-2
[2] the value complies with SIL 3 according to IEC 61508-1
[3] according to Siemens SN29500

Nesselwang, 12 December 2006

Endress+Hauser Wetzer GmbH+Co. KG

General Manager

Level
Pressure
Flow
Temperature
Liquid Analysis
Registration
Systems Components
Services
Solutions

Endress+Hauser
People for Process Automation

Introduction

General information on functional safety (SIL) can be found under: www.de.endress.com/SIL (German) or www.uk.endress.com/SIL (English) and in the Competence brochure CP002Z "Functional safety in the Process Industry – risk reduction with Safety Instrumented Systems".

Safety function using the RB223

Configuration of a safety function using the RB223

Sensor, active barrier, 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, active barrier, logic unit and actuator sub-systems as per Figure 1.

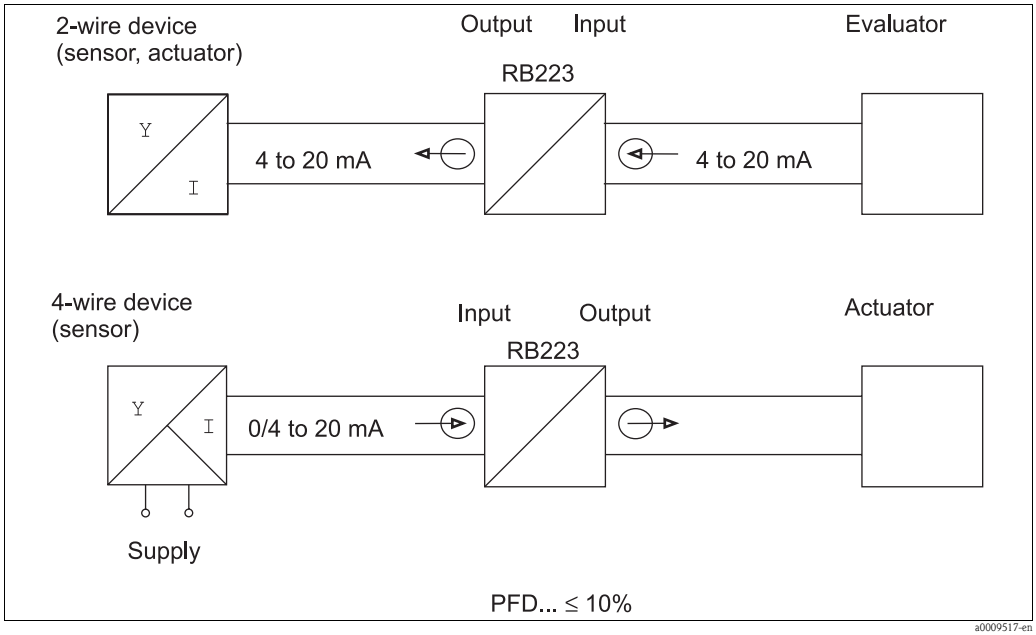


Fig. 1: Share of the passive barrier in the "average probability of dangerous failures of a safety function on demand" (PFD_{AVG})

Note!
This documentation considers the RB223 as a component of a safety function.

Safety function for limit value monitoring

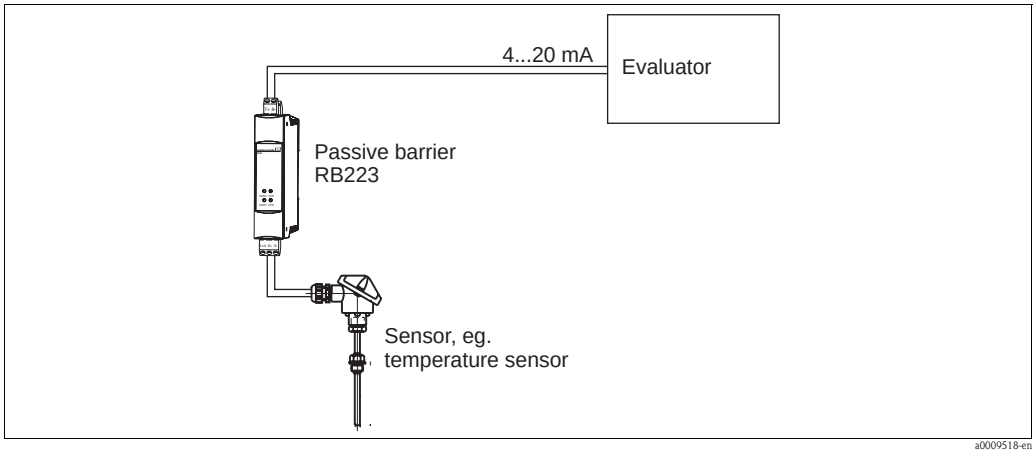


Fig. 2: Safety function with RB223

The device separates active 0/4...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.

Information regarding the safety function

Caution!
Information regarding the safety function can be found in the chapter "Safety-related parameters".

Note!
MTTR is set to 8 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.

Permitted unit versions

The information on functional safety contained in this manual are valid for the unit versions listed below and from the stated hardware revision onwards. Remark: The passive barrier RB223 does not contain any software. Unless stated otherwise, all following versions can also be used in safety functions. Valid unit versions for safety-related usage:

RB223 - abc	**Designation**	**Version**
a	Approval	A = Non-Ex B = Ex
b	Channels	A = 1 channel B = 2 channels
c	Transmission direction	A = Ex ➔ Non-Ex B = Non-Ex ➔ Ex

Hardware assessment valid from hardware revision: Production_A

Supplementary device documentation RB223

Depending on the version, the following documentation must be available for the active barrier RB223:

Explosion protection/Certificates	Operating instructions	Other Ex-Documentation
ATEX II (1) GD [EEx ia] IIC	BA239R	Safety instructions XA068R

Explosion protection/ Certificates	Operating instructions	Control Drawings FM	Control Drawings CSA
FM AIS, I-III, 1, A-G CSA [Ex ia], I-III, A-G		02 20 00 111	02 20 00 112

Caution!
- The installation and setting instructions, and the technical limit values must be observed in accordance with the Operating Instructions (BA239R).
- For devices which are used in explosion-hazardous, the supplementary documentation (XA) resp. Control Drawings must also be used in accordance with the table.

RB223 supplementary documentation
For further information, see Technical Information TI132R.

Installation

Installation, wiring, commissioning

Installation, wiring and commissioning of the RB223 are described in the operating instructions BA239R.

Note!
In order to ensure system safety, it is advisible to strictly separate safety-related and non-safety-related devices and functions.

Iterative tests

Using the RB223 in a safety installation

Protective functions must be tested for operability and safety in suitable intervals.
Intervals are to be defined by the operator.
For this, the figure "Interval for iterative tests" (see pages 9 and 10) can be used for the RB223.
The iterative test of the RB223 must be executed according to the sequence described below.

Testing the RB223 for safe operability

Operability must be tested in suitable intervals, which are to be defined by the operator.
Operability can be tested by means of simulation of limit values at the transmitter and the transfer to the evaluator, for example.

Repair

Repair

The RB223 may only be repaired by Endress+Hauser.

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.

Please note the chapter "Return" in the corresponding Operating Instructions BA239R.

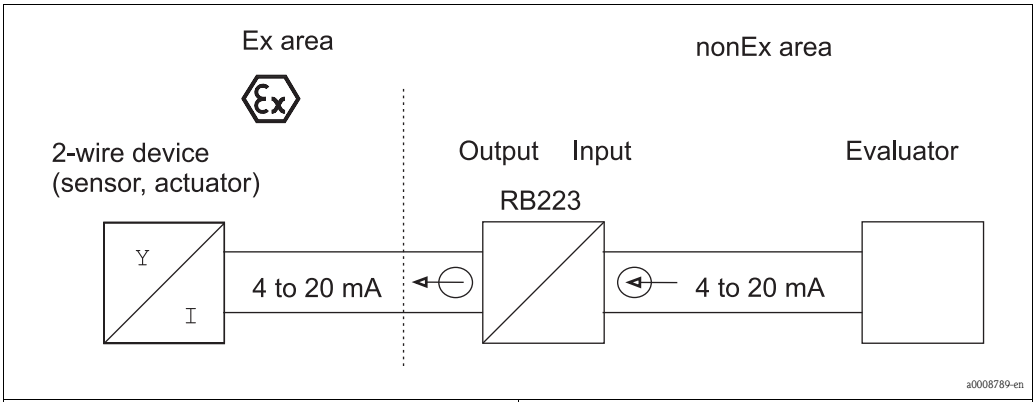
Safety-related parameters

Specific safety-related parameters for RB223

The tables below indicate the safety-related parameters for Functional Safety of the RB223 for various wiring variants.

Wiring option 1

RB223 as input barrier for a safety control (Non-Ex ➔ Ex)



Parameter as per IEC 61508	Value
SIL	3
HFT	0
Device type	A
Operating mode	low demand mode
SFF	100 %
MTTR	8 h
PFD_{av}	0
λ_{SD}	0 FIT
λ_{SU}	45 FIT
λ_{DD}	42 FIT
λ_{DU}	0 FIT
λ_{tot} *1	87 FIT
MTBF *1	1239 years

*1 As per Siemens SN29500. This value accounts for all failure types (see "Management Summary").

Dangerous unrecognized errors in this examination:

An incorrect output signal is considered a dangerous unrecognized error if it deviates from the actual input signal by more than 2 %, with the output signal continuing to be in the range from 4 to 20 mA.

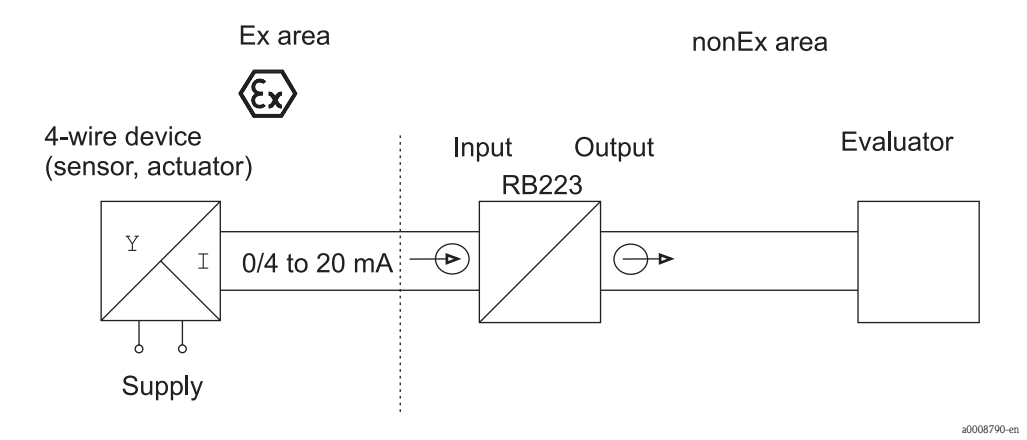
Life span of electrical components:

The underlying failure rates of electrical components are valid within the useful life span as per IEC 61508-2 Section 7.4.7.4. Note 3.

Note!
The safe operation of the RB223 requires correct installation.

Wiring option 2

RB223 as input barrier for a safety control (Ex ➔ Non-Ex)



Parameter as per IEC 61508	Value
SIL	3
HFT	0
Device type	A
Operating mode	low demand mode
SFF	100 %
MTTR	8 h
PFD_{av}	0
λ_{SD}	0 FIT
λ_{SU}	51 FIT
λ_{DD}	47 FIT
λ_{DU}	0 FIT
λ_{tot} *1	98 FIT
MTBF *1	1112 years

*1 As per Siemens SN29500. This value accounts for all failure types (see "Management Summary").

Dangerous unrecognized errors in this examination:

An incorrect output signal is considered a dangerous unrecognized error if it deviates from the actual input signal by more than 2 %, with the output signal continuing to be in the range from 4 to 20 mA.

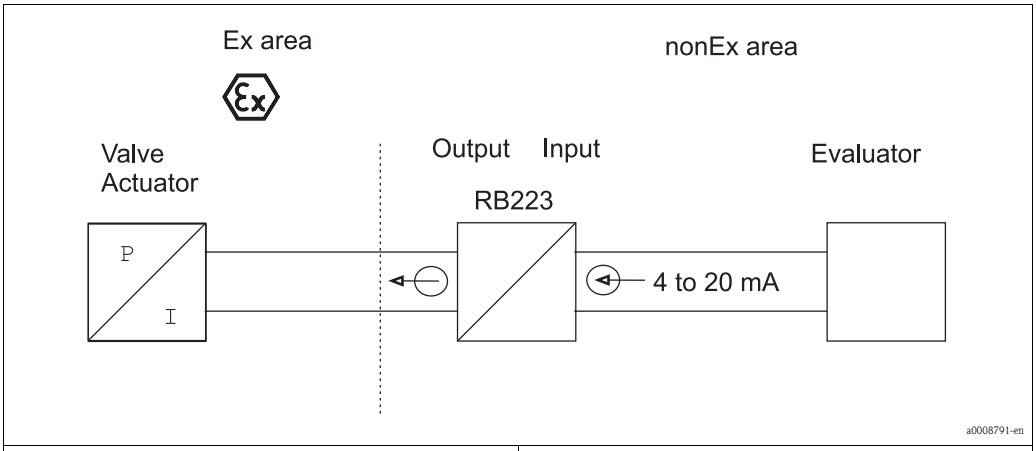
Life span of electrical components:

The underlying failure rates of electrical components are valid within the useful life span as per IEC 61508-2 Section 7.4.7.4. Note 3.

Note!
The safe operation of the RB223 requires correct installation.

Wiring option 3

RB223 as output barrier to an actor (Non-Ex ➔ Ex)



Parameter as per IEC 61508	Value
SIL	3
HFT	0
Device type	A
Operating mode	low demand mode
SFF	90,41 %
MTTR	8 h
T_1	T_1 = time interval for iterative tests (see diagram)
PFD_{av} (for T_1 = 1 year) *2	$3{,}66 \times 10^{-5}$
λ_{Safe}	79 FIT
$\lambda_{Dangerous}$	8 FIT
λ_{tot} *1	87 FIT
MTBF *1	1239 years

*1 As per Siemens SN29500. This value accounts for all failure types (see "Management Summary").
*2 For an average permanent operation temperature near 50 °C, a factor of 1.3 should be accounted for. Further information see "Management Summary".

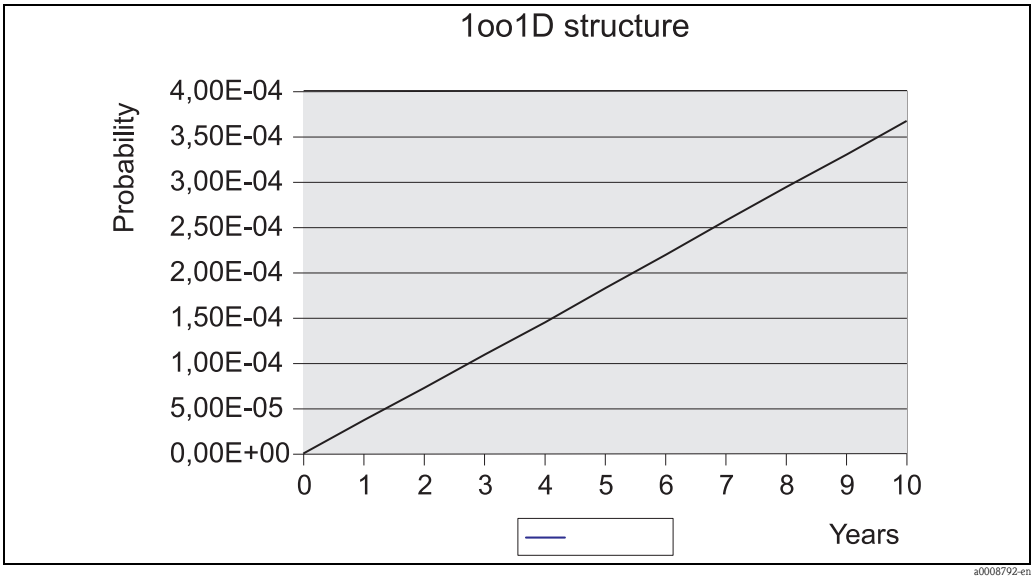
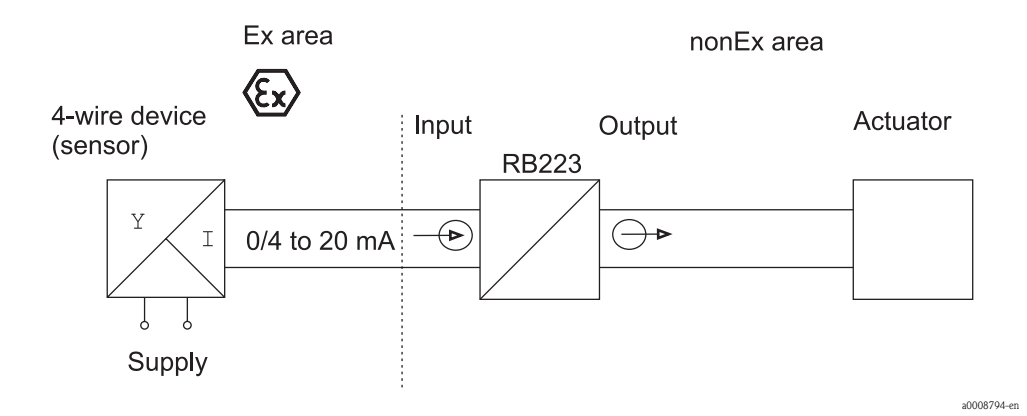


Figure: PFD_{av} against time interval for iterative tests (FMEDA report, Figure 3)

Wiring option 4

RB223 as output barrier to an actor (Ex ➔ Non-Ex)



Parameter as per IEC 61508	Value
SIL	3
HFT	0
Device type	A
Operating mode	low demand mode
SFF	99,69 %
MTTR	8 h
T_1	T_1 = time interval for iterative tests (see diagram)
PFD_{av} (for T_1 = 1 year) *2	$1{,}31 \times 10^{-6}$
λ_{Safe}	97 FIT
$\lambda_{Dangerous}$	0,3 FIT
λ_{tot} *1	97,7 FIT
MTBF *1	1112 years

*1 As per Siemens SN29500. This value accounts for all failure types (see "Management Summary").
*2 For an average permanent operation temperature near 50 °C, a factor of 1.3 should be accounted for. Further information see "Management Summary".

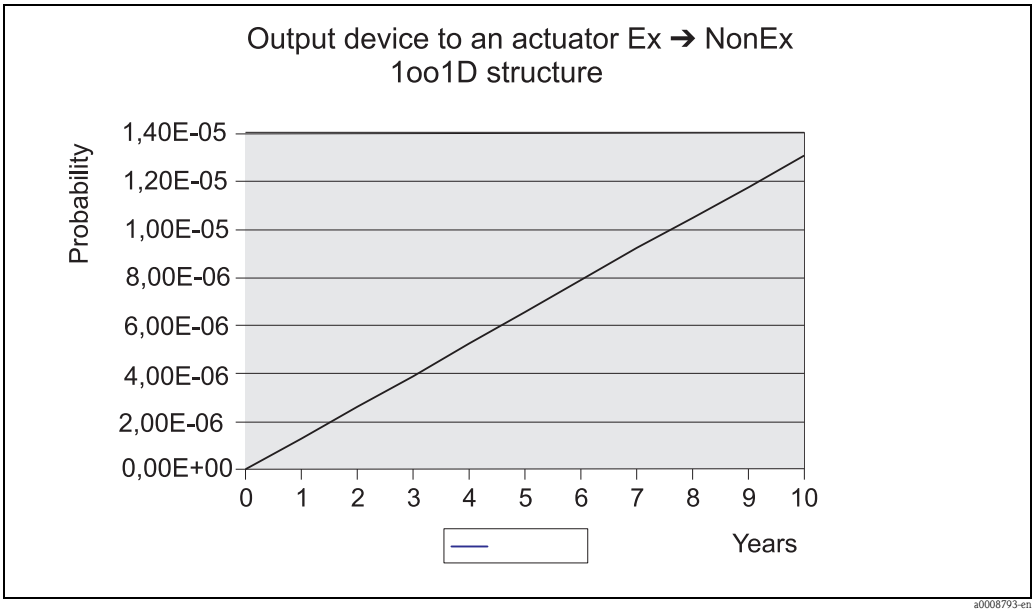


Figure: PFD_{av} against time interval for iterative tests (FMEDA report, Figure 4)

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 06/04-50
Report No.: E+H 06/04-50 R041
Version V1, Revision R0, October 2006
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the loop powered barrier RB223.

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. 71029792	1 channel, no Ex approval
RB223-A2B NonEx -> Ex; part no. 71029793	2 channels, no Ex approval
RB223-B1B NonEx -> Ex; part no. 71029794	1 channel, Ex approval
RB223-B2B NonEx -> Ex; part no. 71029795	2 channels, Ex approval
RB223-B1A Ex -> NonEx; part no. 71029802	1 channel, Ex approval
RB223-A2A Ex -> NonEx; part no. 71029803	2 channels, no Ex approval
RB223-A1A Ex -> NonEx; part no. 71029804	1 channel, no Ex approval
RB223-B2A Ex -> NonEx; part no. 71029805	2 channels, Ex approval

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

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.

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 modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to 1,00E-03.

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

For Type A components the SFF has to be between 90% and 99% according to table 2 of IEC 61508-2 for SIL 3 (sub-) systems with a hardware fault tolerance of 0.

Assuming that the application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled.

[1] Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

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

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**42**
Fail dangerous detected (internal diagnostics or indirectly[2])	0
Fail high (detected by the logic solver)	8
Fail low (detected by the logic solver)	34
Fail Dangerous Undetected	**0**
No Effect	**45**
Not part	**5**

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

λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}	SFF	DC_S [4]	DC_D [4]	PFD_{AVG}
0 FIT	45 FIT	42 FIT	0 FIT	100,00%	0%	100%	0,00E-00

Table 4: RB223 as input device (Ex → NonEx) to a safety PLC – Failure rates

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**47**
Fail dangerous detected (internal diagnostics or indirectly [2])	0
Fail high (detected by the logic solver)	0,3
Fail low (detected by the logic solver)	46,2
Fail Dangerous Undetected	**0**
No Effect	**51**
Not part	**5**

Table 5: RB223 as input device (Ex → NonEx) to a safety PLC – IEC 61508 characteristics

λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}	SFF	DC_S [4]	DC_D [4]	PFD_{AVG}
0 FIT	51 FIT	47 FIT	0 FIT	100,00%	0%	100%	0,00E-00

[2] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[3] Note that the SU category includes failures that do not cause a spurious trip

[4] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Table 6: RB223 as output device (NonEx → Ex) to an actuator – IEC 61508 failure rates

λ_{safe} [5]	$\lambda_{dangerous}$	SFF
79 FIT	8 FIT	90,4%

Table 7: RB223 as output device (NonEx → Ex) to an actuator – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,66E-05	PFD_{AVG} = 1,83E-04	PFD_{AVG} = 3,66E-04

Table 8: RB223 as output device (Ex → NonEx) to an actuator – IEC 61508 failure rates

λ_{safe} [5]	$\lambda_{dangerous}$	SFF
97 FIT	0,3 FIT	99,6%

Table 9: RB223 as output device (Ex → NonEx) to an actuator – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,31E-06	PFD_{AVG} = 6,57E-06	PFD_{AVG} = 1,31E-05

The boxes marked in yellow (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 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-04. The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 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-04.

Because the Safe Failure Fraction (SFF) is above 90%, also the architectural constraints requirements of table 2 of IEC 61508-2 for Type A subsystems with a Hardware Fault Tolerance (HFT) of 0 are fulfilled.

A user of the loop powered barrier RB223 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). A full table of failure rates is presented in sections 5.1 to 5.4 along with all assumptions.

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

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508, Edition 2000. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

[5] Note that the safe category includes failures that do not cause a spurious trip

Appendix

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]

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

People for Process Automation

SD011R/09/en/04.09
FM+SGML 6.0 ProMoDo