



Füllstand



Druck



Durchfluss



Temperatur

Flüssigkeits-
analyse

Registrierung

Systeme
Komponenten

Services



Solutions

Handbuch zur Funktionalen Sicherheit

RB223

Passivtrenner



Anwendungsbereich

Trennung aktiver 0/4...20 mA Signale von Transmittern, Ventilen und Stellgliedern, welche den besonderen Anforderungen der Sicherheitstechnik nach IEC 61508 genügen sollen.

Der Passivtrenner erfüllt die Anforderungen

- an funktionale Sicherheit gemäß IEC 61508
- an Explosionsschutz (je nach Version)
- an elektromagnetische Verträglichkeit nach IEC 61326 und NAMUR-Empfehlung NE 21.
- an elektrische Sicherheit nach IEC/EN 61010-1

Ihre Vorteile

- Einsatz in einer sicherheitsbezogenen Schutzfunktion bis SIL 3, unabhängig bewertet (Hardware Assessment) durch exida.com nach IEC 61508.

Inhaltsverzeichnis

Herstellererklärung	3
Allgemeines	4
Sicherheitsfunktion mit RB223	4
Aufbau einer Sicherheitsfunktion mit RB223	4
Sicherheitsfunktion zur Grenzwertüberwachung	5
Angaben für die Sicherheitsfunktion	5
Zulässige Gerätetypen	5
Mitgeltende Gerätedokumentationen RB223	6
Installation	6
Montage, Verdrahtung, Inbetriebnahme	6
Wiederholungsprüfungen	6
Verwendung des RB223 in einer Sicherheitseinrichtung	6
Überprüfung des RB223 auf sichere Funktion	6
Reparatur	6
Reparatur	6
Sicherheitstechnische Kenngrößen	7
Spezifische sicherheitstechnische Kenngrößen für RB223	7
Verschaltungsoption 1	7
Verschaltungsoption 2	8
Verschaltungsoption 3	9
Verschaltungsoption 4	10
Exida.com management summary	11
Anhang	15

Herstellererklärung

FMEDA einschließlich SFF-Bestimmung und PFD_{AVG}-Berechnung nach IEC 61508

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

erklärt als Hersteller, dass die Hardware-Bewertung des Passivtrenners

RB223

nach IEC 61508 eine PFD_{AVG} ergibt, die innerhalb des erlaubten Bereichs bis einschließlich SIL 3 liegt nach IEC 61508-1 Tab. 2 und einer Safe Failure Fraction (SFF) > 90,4 %, wenn zugehörige Sicherheitshinweise beachtet werden.

Die FMEDA ergibt folgende Parameter:

Gerätetyp	A	
HFT	0	
	Geräteausgang (NonEx -> Ex) an einem Aktor	Geräteausgang (Ex -> NonEx) an einem Aktor
Prüfintervall	1 Jahr	10 Jahre
SFF ¹⁾	> 90,4 %	> 99,6 %
PFD _{AVG} ²⁾	3,66x10 ⁻⁵	1,31x10 ⁻⁵
MTBF ³⁾	1239 Jahre	1112 Jahre
λ _{safe}	79 FIT	97 FIT
λ _{dangerous}	8 FIT	0,3 FIT

¹⁾ nach Tabelle 2 der IEC61508-2

²⁾ die Werte sind nach IEC 61508-1 innerhalb des für SIL 3 definierten Bereichs

³⁾ gemäß Siemens SN29500

Nesselwang, 12. Dezember 2006

Endress+Hauser Wetzler GmbH+Co. KG



Geschäftsführer



Level



Pressure



Flow



Temperature



Liquid
Analysis



Registration



Systems
Components



Services



Solutions

Allgemeines

Allgemeine Informationen über Funktionale Sicherheit (SIL) sind erhältlich unter: www.de.endress.com/SIL (deutsch) bzw. www.uk.endress.com/SIL (englisch) und in der Kompetenzbroschüre CP002Z "Funktionale Sicherheit in der Prozess-Instrumentierung zur Risikoreduzierung".

Sicherheitsfunktion mit RB223

Aufbau einer Sicherheitsfunktion mit RB223

Sensor, Passivtrenner und Auswerteeinheit bilden zusammen ein sicherheitsbezogenes System, das eine Sicherheitsfunktion ausführt. Die "mittlere Wahrscheinlichkeit gefährbringender Ausfälle des gesamten sicherheitsbezogenen Systems" (PFD_{AVG}) teilt sich auf die Teilsysteme Sensor, Passivtrenner und Auswerteeinheit üblicherweise gemäß Abbildung 1 auf.

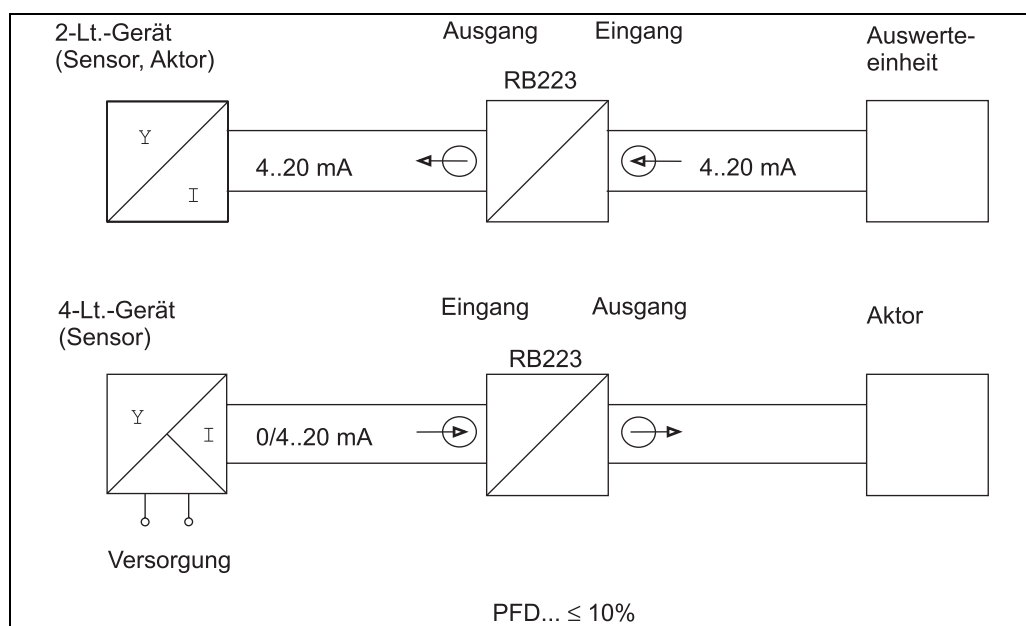


Abb. 1: Anteil des Passivtrenners an der "mittleren Wahrscheinlichkeit gefährbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall" (PFD_{AVG})



Hinweis!

Diese Dokumentation behandelt den RB223 als Teil einer Sicherheitsfunktion.

**Sicherheitsfunktion zur
Grenzwertüberwachung**

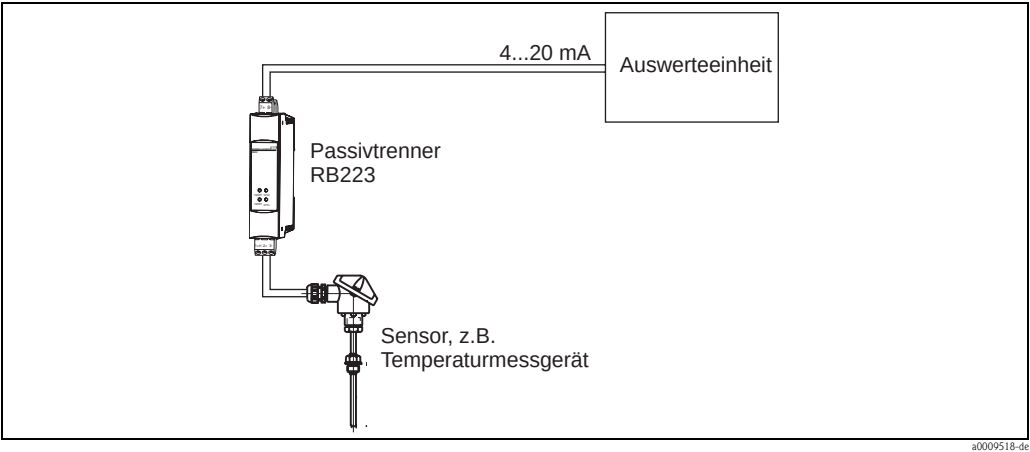


Abb. 2: Sicherheitsfunktion mit RB223

Das Gerät trennt aktive 0/4...20 mA Signale von Transmittern, Ventilen und Stellgliedern. Es verfügt über einen Analogeingang und einen eigensicheren Analogausgang, bzw. einen Ausgang und eigensicheren Eingang. Optional ist das Gerät auch zweikanalig ausgeführt. Der Trenner wird zum eigensicheren Betrieb von Sensoren, Ventilen und Stellgliedern eingesetzt. Das Gerät wird aus der Stromschleife, ohne eigene Hilfsenergie versorgt.

Angaben für die Sicherheitsfunktion



Achtung!
Angaben für die Sicherheitsfunktion sind im Kapitel "Sicherheitstechnische Kenngrößen" aufgeführt.



Hinweis!
MTTR wird mit 8 Stunden angesetzt.
Sicherheitsbezogene Systeme ohne selbstverriegelnde Funktion müssen nach Ausführen der Sicherheitsfunktion innerhalb MTTR in einen überwachten oder anderweitig sicheren Zustand gebracht werden.

Zulässige Gerätetypen

Die in diesem Handbuch enthaltenen Angaben zur Funktionalen Sicherheit sind für die unten angegebenen Geräteausprägungen und ab der genannten Hardwareversion gültig. Anmerkung: Der Passivtrenner RB223 verfügt über keine Software.
Sofern nicht anderweitig angegeben, sind alle nachfolgenden Versionen ebenfalls für Sicherheitsfunktionen einsetzbar. Gültige Geräteausprägungen für sicherheitsbezogenen Einsatz:

RB223 - abc	Benennung	Ausprägung
a	Zulassung	A = Nicht-Ex B = Ex
b	Kanäle	1 = 1 Kanal 2 = 2 Kanäle
c	Übertragungsrichtung	A = Ex → Nicht-Ex B = Nicht-Ex → Ex

Gültige Hardware-Version: ab Hardware-Revision Production_A

Mitgeltende Gerätedokumentationen RB223

Für den Speisetrenner RB223 müssen je nach Ausführung folgende Dokumentationen vorhanden sein:

Zündschutzart/Zertifikat	Betriebsanleitung	weitere Ex-Dokumentation
ATEX II (1) GD [EEx ia] IIC	BA239R	Sicherheitshinweise XA068R

Zündschutzart/Zertifikat	Betriebsanleitung	Control Drawing FM	Control Drawing CSA
FM AIS, I-III, 1, A-G CSA [Ex ia], I-III, A-G		02 20 00 111	02 20 00 112



Achtung!

- Die Installations- und Einstellhinweise sowie die technischen Grenzwerte sind gemäß der Betriebsanleitung (BA239R) zu beachten.
- Für Geräte, die im explosionsgefährdeten Bereich eingesetzt werden, sind zusätzlich die entsprechenden Sicherheitshinweise (XA) bzw. Control Drawings gemäß den obigen Tabellen zu beachten.

Zusätzliche Dokumentation RB223

Für weitere Informationen siehe Technische Information TI132R.

Installation

Montage, Verdrahtung, Inbetriebnahme

Die Montage, Verdrahtung und Inbetriebnahme des RB223 ist in der Betriebsanleitung BA239R beschrieben.



Hinweis!

Zur Gewährleistung der Anlagensicherheit empfiehlt sich eine strikte Trennung sicherheitsbezogener und nicht-sicherheitsbezogener Geräte und Funktionen.

Wiederholungsprüfungen

Verwendung des RB223 in einer Sicherheitseinrichtung

Schutzfunktionen sind in angemessenen Zeitabständen auf ihre Funktionsfähigkeit und Sicherheit zu überprüfen.

Die Zeitabstände sind vom Betreiber festzulegen.

Hierzu kann die "Abb.: Intervall für Wiederholungsprüfung" (siehe Seite 9 bzw. 10) für den RB223 herangezogen werden.

Die Wiederholungsprüfung des RB223 ist gemäß dem nachfolgend beschriebenen Ablauf durchzuführen.

Überprüfung des RB223 auf sichere Funktion

Die Funktionsfähigkeit ist in angemessenen Zeitabständen zu überprüfen, die vom Betreiber festzulegen sind. Die Funktionsfähigkeit kann z.B. über die Simulation von Grenzwerten am Transmitter und die Übertragung auf die Auswerteeinheit überprüft werden.

Reparatur

Reparatur



Die Reparatur des RB223 darf grundsätzlich nur durch Endress+Hauser erfolgen.

Hinweis!

Bei Ausfall eines SIL-gekennzeichneten E+H-Gerätes, das in einer Schutzfunktion betrieben wurde, ist bei der Rücksendung des defekten Gerätes die "Erklärung zur Kontamination und Reinigung" mit dem entsprechenden Hinweis "☒ Einsatz als SIL-Gerät in Schutzeinrichtung" beizulegen.

Die "Erklärung zur Kontamination und Reinigung" finden Sie im Anhang am Ende dieses Handbuchs zur Funktionalen Sicherheit.

Beachten Sie hierzu auch das Kapitel "Rücksendung" in der zugehörigen Betriebsanleitung BA239R.

Sicherheitstechnische Kenngrößen

Spezifische sicherheitstechnische Kenngrößen für RB223

Die nachfolgenden Tabellen geben die sicherheitstechnischen Kenngrößen zur Funktionalen Sicherheit des RB223 für verschiedene Verschaltungsvarianten an.

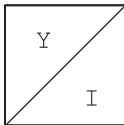
Verschaltungsoption 1

RB223 als Eingangstrenner für eine Sicherheitssteuerung (Nicht-Ex → Ex)

Ex-Seite



2-Lt.-Gerät
(Sensor, Aktor)



4...20 mA

nonEx-Seite

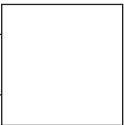
Ausgang

Eingang

RB223

4...20 mA

Auswerte-
einheit



Kenngröße gemäß IEC 61508	Wert
SIL	3
HFT	0
Gerätetyp	A
Betriebsart	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 Jahre

*1 Gemäß Siemens SN29500. Dieser Wert berücksichtigt alle Ausfallarten (siehe "Management Summary").

Gefährliche unerkannte Fehler in dieser Betrachtung:

Als gefährlicher unerkannter Fehler wird ein falsches Ausgangssignal betrachtet, das vom realen Eingangssignal um mehr als 2% abweicht, wobei das Ausgangssignal weiterhin im Bereich von 4...20 mA liegt.

Lebensdauer elektrischer Bauteile:

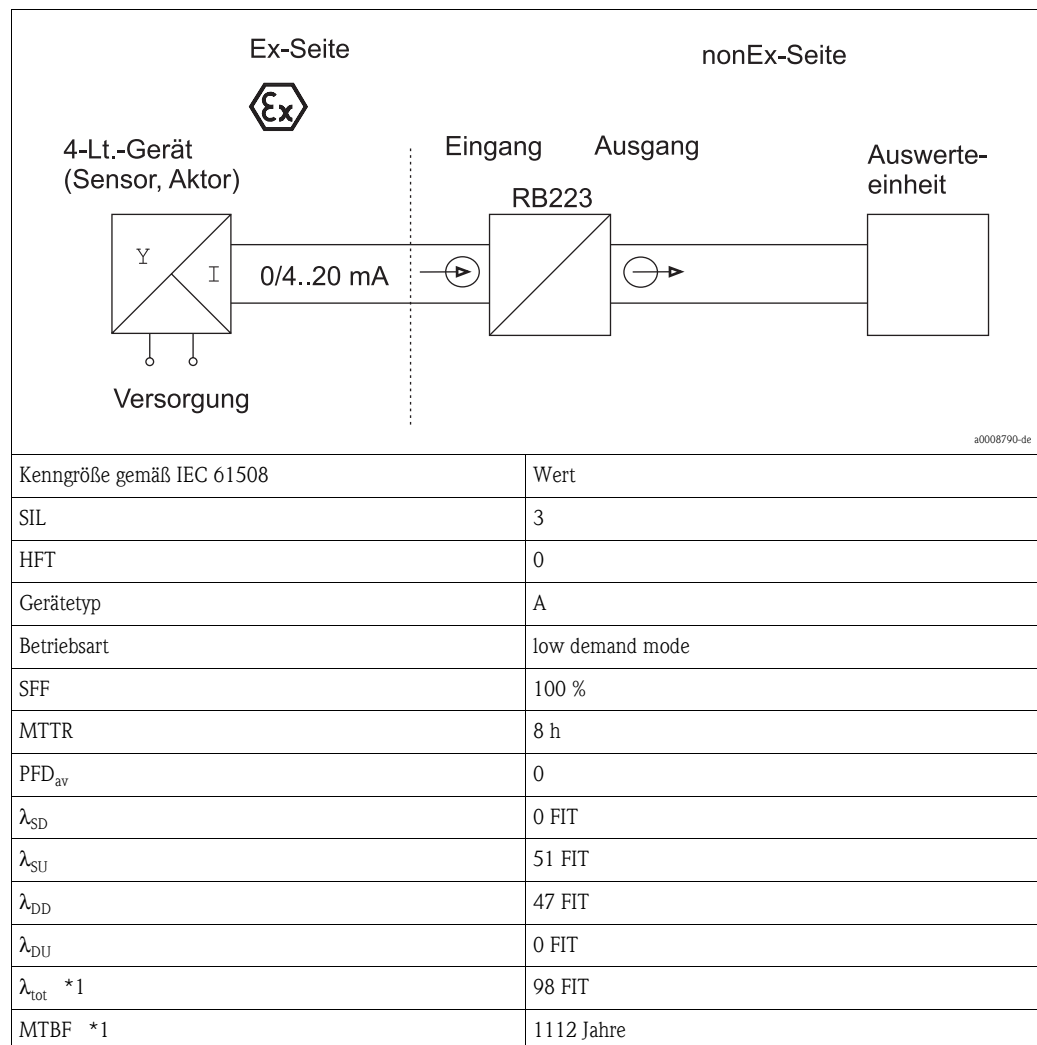
Die zugrunde gelegten Ausfallraten elektrischer Bauteile gelten innerhalb der nutzbaren Lebensdauer gemäß IEC 61508-2 Abschnitt 7.4.7.4. Hinweis 3.



Hinweis!
Der sichere Betrieb des RB223 setzt eine ordnungsgemäße Installation voraus.

Verschaltungsoption 2

RB223 als Eingangstrenner für eine Sicherheitssteuerung (Ex → Nicht-Ex)



*1 Gemäß Siemens SN29500. Dieser Wert berücksichtigt alle Ausfallarten (siehe "Management Summary").

Gefährliche unerkannte Fehler in dieser Betrachtung:

Als gefährlicher unerkannter Fehler wird ein falsches Ausgangssignal betrachtet, das vom realen Eingangssignal um mehr als 2% abweicht, wobei das Ausgangssignal weiterhin im Bereich von 4...20 mA liegt.

Lebensdauer elektrischer Bauteile:

Die zugrunde gelegten Ausfallraten elektrischer Bauteile gelten innerhalb der nutzbaren Lebensdauer gemäß IEC 61508-2 Abschnitt 7.4.7.4. Hinweis 3.

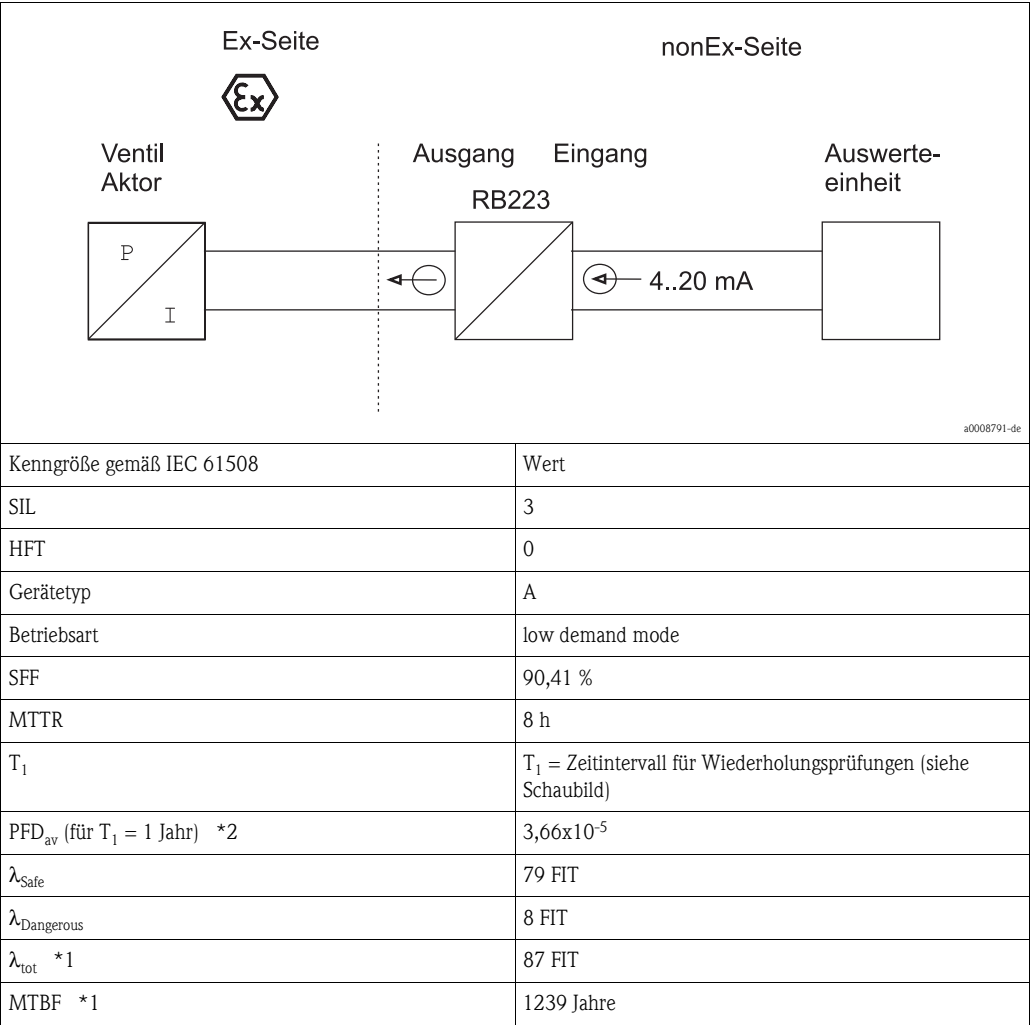


Hinweis!

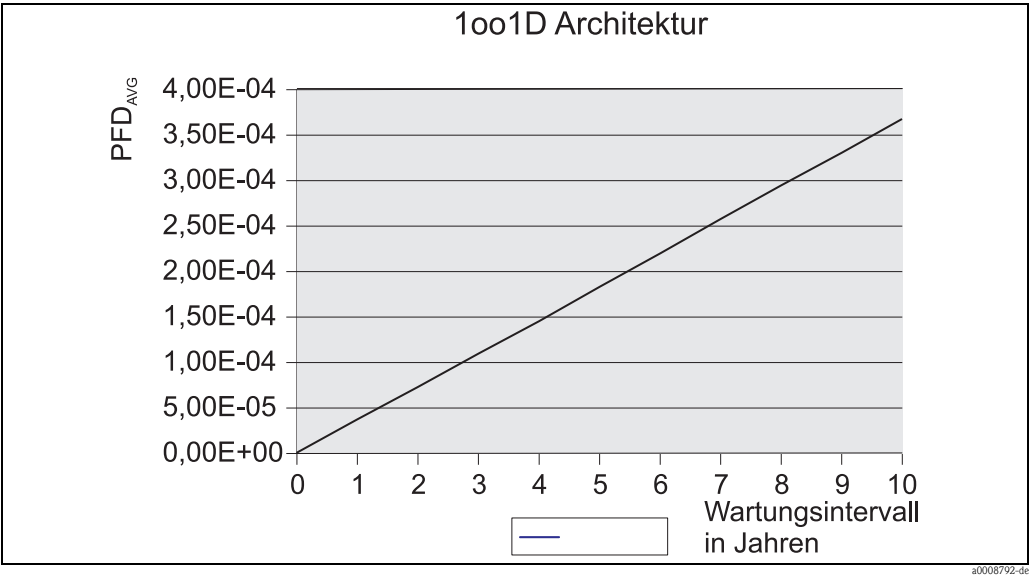
Der sichere Betrieb des RB223 setzt eine ordnungsgemäße Installation voraus.

Verschaltungsoption 3

RB223 als Ausgangstrenner zu einem Aktor (Nicht-Ex → Ex)

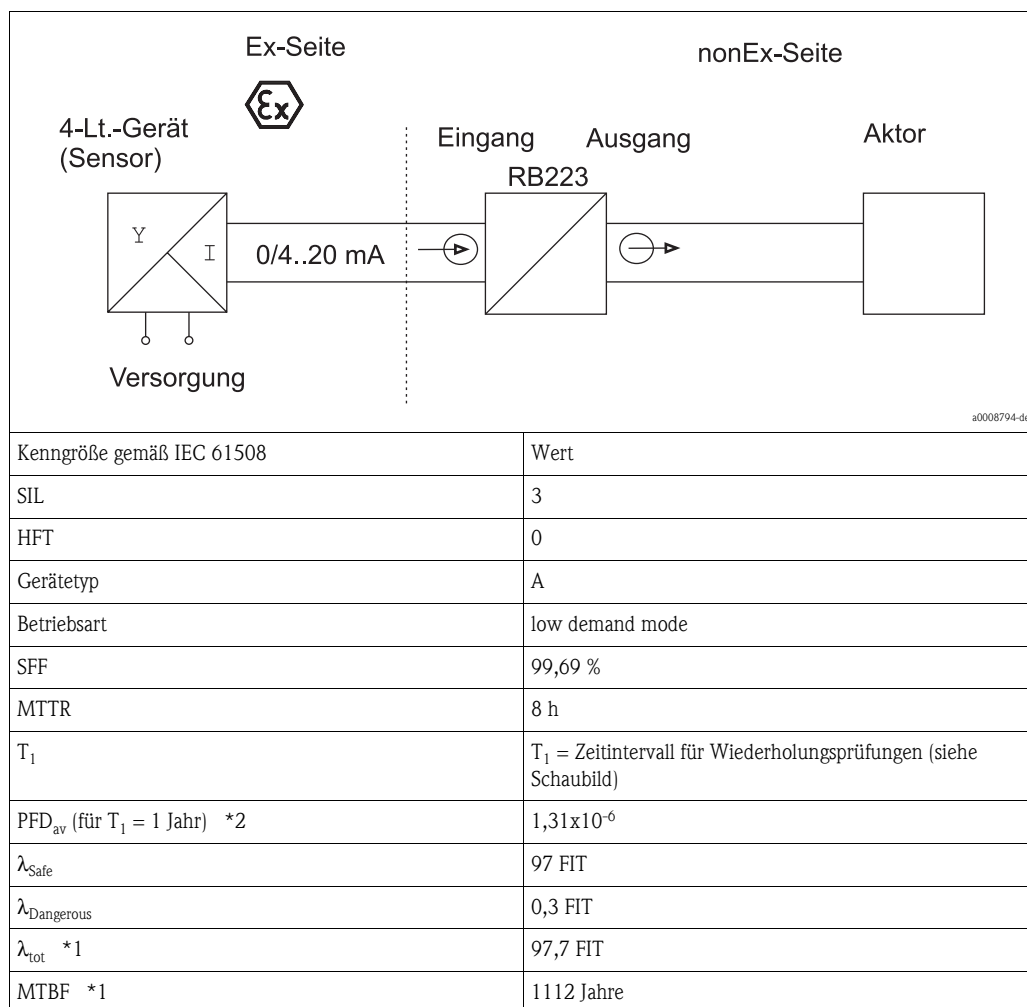


*1 Gemäß Siemens SN29500. Dieser Wert berücksichtigt alle Ausfallarten (siehe "Management Summary").
*2 Bei einer durchschnittlichen Dauereinsatztemperatur nahe 50 °C sollte ein Faktor von 1,3 berücksichtigt werden. Weitere Informationen siehe "Management Summary".



Verschaltungsoption 4

RB223 als Ausgangstrenner zu einem Aktor (Ex → Nicht-Ex)



*1 Gemäß Siemens SN29500. Dieser Wert berücksichtigt alle Ausfallarten (siehe "Management Summary").
 *2 Bei einer durchschnittlichen Dauereinsatztemperatur nahe 50 °C sollte ein Faktor von 1,3 berücksichtigt werden. Weitere Informationen siehe "Management Summary".

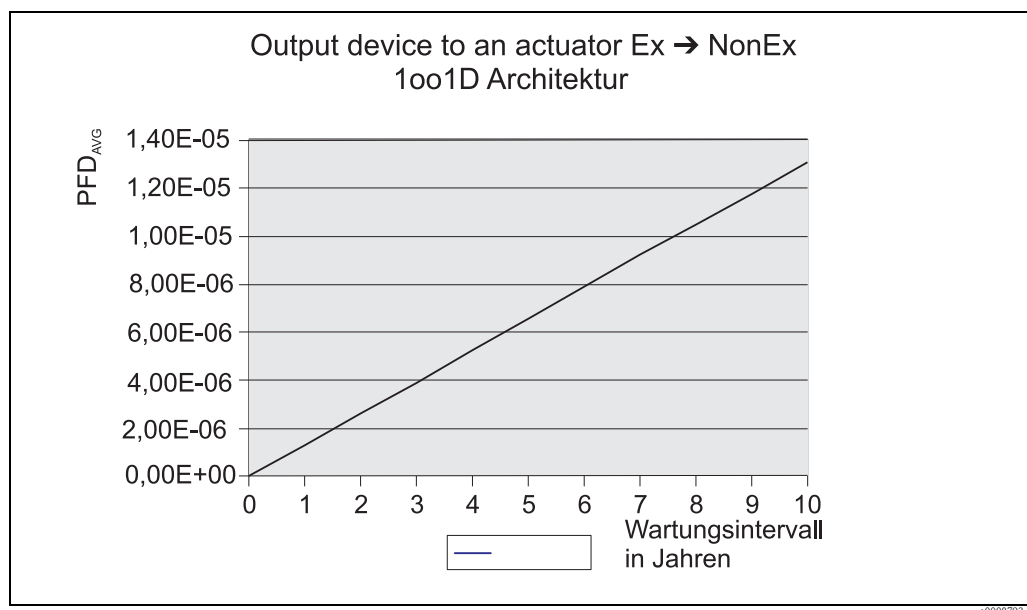


Abb.: PF_{av} in Abhängigkeit vom Zeitintervall für Wiederholungsprüfungen (FMEDA-Bericht Figure 4)

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 40°C. 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 A¹ 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	$\lambda_{\text{dangerous}}$	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	$\lambda_{\text{dangerous}}$	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

Anhang

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 of instrument / 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]

 Pressure / *Druck* _____ [Pa]

 Conductivity / *Leitfähigkeit* _____ [S]

 Viscosity / *Viskosität* _____ [mm²/s]

Deutschland

Endress+Hauser
Messtechnik
GmbH+Co. KG
Colmarer Straße 6
79576 Weil am Rhein

Fax 0800 EHFAXEN
Fax 0800 343 29 36
www.de.endress.com

Vertrieb

- Beratung
- Information
- Auftrag
- Bestellung

Tel. 0800 EHVERTRIEB
Tel. 0800 348 37 87
info@de.endress.com

Service

- Help-Desk
- Feldservice
- Ersatzteile/Reparatur
- Kalibrierung

Tel. 0800 EHSERVICE
Tel. 0800 347 37 84
service@de.endress.com

Technische Büros

- Hamburg
- Berlin
- Hannover
- Ratingen
- Frankfurt
- Stuttgart
- München

Österreich

Endress+Hauser
Ges.m.b.H.
Lehnergasse 4
1230 Wien
Tel. +43 1 880 56 0
Fax +43 1 880 56 335
info@at.endress.com
www.at.endress.com

Schweiz

Endress+Hauser
Metso AG
Kägenstrasse 2
4153 Reinach
Tel. +41 61 715 75 75
Fax +41 61 715 27 75
info@ch.endress.com
www.ch.endress.com

Endress+Hauser 
People for Process Automation