

FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device Model Number:
Zener Barriers for Intrinsic Safety Applications

Project:
 X7300 (Product Maintenance)

Pepperl+Fuchs GmbH
Mannheim
Germany


		scale: 1:1	date: 2019-Jun-04
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	
		norm	
			Cert-5207 sheet 1 of 11

Table of content:


1. Report Summary.....	3
2. Types of barriers.....	4
3. Functional description of the barriers.....	5
4. Definition of the failure categories.....	5
5. Assumptions	6
6. Results of the assessment.....	7
7. Possibilities to Reveal Dangerous Undetected Faults during the Proof Test.....	9
8. Periodic Proof Testing	9
9. Useful life time	10
10. Abbreviations	11
11. Literature	11

Reviewers:

Role
Project Leader (PL)
Product Management
Functional Safety Manager

History of this document:

Revision of this document	Reviewed by / [Reviewer abbreviation within the detailed comment list]	Date of Review	Changes since last version
V 0 Rev. 1	Fiebig (DP.DFI), Kindermann (DP.MKI)	2015-Sep-10	Newly created
V 1 Rev. 0	Fiebig (DP.DFI), Kindermann (DP.MKI)	2015-Sep-21	Change sequence of tables, create the final wording and version for EDM
V 1 Rev. 1	Fiebig (DP.DFI), Kindermann (DP.MKI)	2019-Jun-04	Delete the usual tables at the beginning to improve the handling. Clarification of the described types and better assignment of the Z788 and Z888.

 Mannheim	FMEDA – Report Zener Barriers Z... Type	scale: 1:1	date: 2019-Jun-04	
		respons.	DP.DFI	Cert-5207
		approved	norm	

1. Report Summary

This report summarizes the results of the FMEDA's for all barriers in product range at the moment. The product portfolio is categorized in different boards, with different schematics and different assembly and with different circuit diagrams.

In examination of the function of the barriers, three groups with significant difference in safety characteristic values were determined.

For each group, the worst case values for the Type of barriers is given.


The following three Types are distinguished:

1. Complex Zener barriers (includes all AC Zener barriers)
2. Simple Zener barriers
3. Zener barriers with current limitation: Z728.CL and Z810.CL

The different applications as digital input (DI), digital output (DO), analog input (AI) and analog output (AO) were considered. Due to the insignificance of the discrepancies between the different modes of operation, only the results for the AO mode of operation with the **safety function "Signals are transferred from input to output without modification"** are given as they represent the worst case application.

If **two channels of one Zener barrier** are used for one safety function, the values given in the assessment **results need to be doubled**. Due to worst case estimations no additional common cause failures need to be considered.

Failure rates used in this analysis are basic failure rates from the Siemens Standard SN29500.

		scale: 1:1	date: 2019-Jun-04
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	
		norm	
		Cert-5207	
		sheet 3 of 11	

2. Types of barriers

As described in chapter 1, here the categories of Zener barriers.


Type 1: Complex Zener Barriers

Z713	Z813	Z905
Z722 (.H)	Z822 (.H)	Z910
Z728 (.H)(.F)	Z828 (.H)(.F)	Z915 (.1K)
Z772	Z872	Z928
Z778	Z878	Z954
Z779 (.H)(.F)	Z886	Z955
Z786	Channel 1 of Z888 (.H)(.R)	Z960 (.F)
Z787 (.H)(.F)	Z896	Z961 (.H)(.F)
Channel 1 of Z788 (.H)(.R)		Z964
Z796		Z965
		Z966 (.H)(.F)
		Z967
		Z972
		Z978

Type 2: Simple Zener Barriers

Z705	Z810
Z710	Z815 (.1k)(.F)
Z715 (.1k)(.F)	Z857
Z755	Z864
Z757	Z865 (.F)
Z764	Channel 2 of Z888 (.H)(.R)
Z765 (.F)	
Channel 2 of Z788 (.H)(.R)	

Type 3: DC Zener Barriers with current limitation Z728.CL and Z810.CL.

		scale: 1:1	date: 2019-Jun-04
 Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	
		norm	
			Cert-5207
			sheet 4 of 11

3. Functional description of the barriers

The Zener Barrier prevents the transfer of unacceptably high energy from the safe area into the hazardous area.

The output voltage is limited by Zener diodes that start to conduct at too high voltage levels and cause a fuse to blow. In conjunction with this, a resistor is protecting the hazardous area from high currents and pulses.

4. Definition of the failure categories

The FMEDAs was done and are documented in EDM under FS-0117PF-27. In order to judge the failure behaviour the barrier, the following definitions for the failure of the product were considered:

Fail-safe state:

The fail-safe state is defined as the output being de-energized.

Safe failure:

When the output goes to the safe state.

Dangerous failure:

"A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:

- a) leads to a measurement error of more than 2% of full span and prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,
- b) decreases the probability that the safety function operates correctly when required."

No effect failure (Residual, Don't care):

Failure mode of a component that plays a part in implementing the safety function but has no direct effect on the safety function and deviates the output by not more than 2% of full span. These failures are not used within the SFF calculation.

Annunciation failure:

Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit).

Not part:


This component is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate ($\lambda_{\text{total (Safety function)}}$).

Not considered:

The reaction on this failure mode could not be decided. When calculating the SFF this failure mode is divided into 50% no effect and 50% dangerous undetected failures.

Safety Response Time:


The time that is needed to transfer an input signal of a device to its output according to the safety function.

		scale: 1:1	date: 2019-Jun-04
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	Cert-5207
		norm	

5. Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the barriers.

- The device shall claim less than 10 % of the total failure budget for a SIL safety loop.
- For a SIL3 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (Safety Instrumented Function) should be smaller than 10⁻³, hence the maximum allowable PFD_{avg} value would then be 10⁻⁴.
- For a SIL3 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10⁻⁷ per hour, hence the maximum allowable PFH value would then be 10⁻⁸ per hour.
- For a SIL2 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (Safety Instrumented Function) should be smaller than 10⁻², hence the maximum allowable PFD_{avg} value would then be 10⁻³.
- For a SIL2 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10⁻⁶ per hour, hence the maximum allowable PFH value would then be 10⁻⁷ per hour.
- Failure rates are constant, wear out mechanisms are not included.
- Failure rates based on the Siemens standard SN29500.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours.
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (for example: substitution by an equivalent device).
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HDBK-217F. Alternatively, the assumed environment is similar to:
 - IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 °C. Humidity levels are assumed within manufacturer's rating. 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.
- If the customer uses **two channels of one device** (Barrier) for one safety function, he has to **double the values** given in the assessment results.

		scale: 1:1	date: 2019-Jun-04
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	
		norm	
			Cert-5207 sheet 6 of 11

6. Results of the assessment

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 8.0.1 by exida.com. These values are calculated for one channel of the device.

Table 1: Type 1: Complex Zener Barriers, 1oo1 structure

Parameters acc. to EN/IEC 61508:2010	Values
Device Type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Signal transfer to field device
HFT	0
SIL (SC)	2
$\lambda_{sd} + \lambda_{su}$ ¹	9 FIT
λ_{dd}	0 FIT
λ_{du}	8 FIT
λ_{total} (Safety function)	17 FIT
$\lambda_{no\ effect}$	48 FIT
$\lambda_{not\ part}$	0 FIT
PTC	100 %
MTBF ²	1784 years
PFH	$7,70 \cdot 10^{-9}$ 1/h
PFD _{avg} for T ₁ = 1 year	$3,37 \cdot 10^{-5}$
PFD _{avg} for T ₁ = 2 years	$6,74 \cdot 10^{-5}$
PFD _{avg} for T ₁ = 5 years	$1,69 \cdot 10^{-4}$
¹ "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of safety characteristic values. ² acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h This value is calculated for one safety function of a device.	



 Mannheim	FMEDA – Report Zener Barriers Z... Type	scale: 1:1	date: 2019-Jun-04	
		respons.	DP.DFI	Cert-5207
		approved		
		norm	sheet 7 of 11	

Table 2: Type 2: Simple Zener Barriers, 1oo1 structure

Parameters acc. to EN/IEC 61508:2010	Values
Device Type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Signal transfer to field device
HFT	0
SIL (SC)	2
$\lambda_{sd} + \lambda_{su}$ ¹	10 FIT
λ_{dd}	0 FIT
λ_{du}	3 FIT
λ_{total} (Safety function)	13 FIT
$\lambda_{no\ effect}$	46 FIT
$\lambda_{not\ part}$	0 FIT
PTC	100 %
MTBF ²	1968 years
PFH	$2,45 \cdot 10^{-9}$ 1/h
PFD _{avg} for T ₁ = 1 year	$1,07 \cdot 10^{-5}$
PFD _{avg} for T ₁ = 2 years	$2,14 \cdot 10^{-5}$
PFD _{avg} for T ₁ = 5 years	$5,35 \cdot 10^{-5}$
¹ "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of safety characteristic values. ² acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h This value is calculated for one safety function of a device.	

Table 3: Type 3: DC Zener Barriers Z728.CL and Z810.CL, 1oo1 structure

Parameters acc. to EN/IEC 61508:2010	Values
Device Type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Signal transfer to field device
HFT	0
SIL (SC)	2
$\lambda_{sd} + \lambda_{su}$ ¹	6 FIT
λ_{dd}	0 FIT
λ_{du}	12 FIT
λ_{total} (Safety function)	18 FIT
$\lambda_{no\ effect}$	24 FIT
$\lambda_{not\ part}$	0 FIT
PTC	100 %
MTBF ²	2691 years
PFH	$1,19 \cdot 10^{-8}$ 1/h
PFD _{avg} for T ₁ = 1 year	$5,21 \cdot 10^{-5}$
PFD _{avg} for T ₁ = 2 years	$1,04 \cdot 10^{-4}$
PFD _{avg} for T ₁ = 5 years	$2,61 \cdot 10^{-4}$
¹ "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of safety characteristic values. ² acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 24h This value is calculated for one safety function of a device.	

 Mannheim	FMEDA – Report Zener Barriers Z... Type	respons.	DP.DFI	scale: 1:1	date: 2019-Jun-04
		approved		Cert-5207 sheet 8 of 11	
		norm			

7. Possibilities to Reveal Dangerous Undetected Faults during the Proof Test

The Proof test shall reveal the dangerous undetected (du) faults, which have been noticed during the FMEDA.

The proof test procedure is available from www.pepperl-fuchs.com

8. Periodic Proof Testing


The barriers can be proof tested by executing a proof test procedure according to a procedure available from www.pepperl-fuchs.com.

The proof test recognizes dangerous concealed faults that would affect the safety function of the plant.

According to the results of the analysis, the barrier never has to be subjected to a proof test within its useful lifetime when assuming 10% of the failure budget.

It is possible that the device is used under other circumstances than specified within the assumptions for the FMEDA assessment. The calculations for the safety loop can also reveal that the device may claim a different amount of the PFD value (standard is 10%). Both effects can have an influence on the proof test time.

It is the responsibility of the operator to select a suitable proof test time.

		scale: 1:1	date: 2019-Jun-04
	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	
		norm	
Mannheim			Cert-5207 sheet 9 of 11

9. Useful life time

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful life time of components is not exceeded. Beyond this useful life time, the result of the probabilistic calculation is meaningless as the probability of failure significantly increases with time. The useful life time is highly dependent on the component itself and its operating conditions – temperature in particular (for example, the electrolytic capacitors can be very sensitive to the working temperature).

This assumption of a constant failure rate is based on the bathtub curve, which shows the Typical behavior for electronic components.

Therefore it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful life time of each component.


It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful life time is valid.

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 years.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime. Our experience has shown that the useful life time of a Pepperl+Fuchs product can be higher

- if there are no components with reduced life time in the safety path (like electrolytic capacitors, relays, flash memory, opto coupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful life time refers to the (constant) failure rate of the device. The effective life time can be higher.

		scale: 1:1	date: 2019-Jun-04
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	
		norm	
			Cert-5207 sheet 10 of 11

10. Abbreviations

FMEDA	Failure Modes, Effects and Diagnostic Analysis
FIT	Failure in Time in 10^{-9} 1/h
PFD	Probability of dangerous failure on demand
PFH	Probability of dangerous failure per hour
SFF	Safe Failure Fraction
HFT	Hardware Fault Tolerance
SIL	Safety Integrity Level
SC	Systematic Capability
MTBF	Mean Time between Failures
PTC	Proof Test Coverage
T ₁	Proof time
AVG	Average
PLC	Programmable Logic Controller

11. Literature

Manufacturer's Documents

FS-0117PF-27 Calculation of Safety Characteristic Values according to EN 61508:2010

Standards


IEC 61508-1:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – General Part

IEC 61508-2:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Requirements

SN 29500 parts 1 – 13, Failure rates of components

FMD-91, RAC 1991 Failure Mode / Mechanism Distributions

FMD-97, RAC 1997 Failure Mode / Mechanism Distributions

		scale: 1:1	date: 2019-Jun-04
 Mannheim	FMEDA – Report	respons.	DP.DFI
	Zener Barriers Z... Type	approved	Cert-5207
		norm	