Failure Modes, Effects and Diagnostic Analysis

Project:
Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 11/10-085

Report No.: P+F 11/10-085 R036

Version V1, Revision R0, September 2012

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I in the versions listed in the drawings referenced in section 2.4.1. Table 1 gives an overview of the different configurations that belong to the considered Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I.

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: Configuration overview K-LB-*.**

Standard housing type, K-LB-	*	.	*	*
Number of channels:				
1	1			
2	2			
Working voltage:				
30 - 30 V				
6 - 6 V				
Option:				
G - Non-isolated type				

Table 2: Configuration overview P-LB-*.*.*

P-LB-	*	.	*	.	*
Number of channels:					
1	1				
2	2				
A, B, C, D, E, F (see Table 4)					
Protected lines (e.g. 13 or 2356, see Table 4)					

Table 3: Configuration overview F*-LB-I

Screw-in type, F	*	-LB-	*
Thread type:			
S - M20 x 1.5			
P - Pg 13.5			
N - 1/2” NPT			
I - Intrinsic safety EEx ‘i’			
D - Flameproof EEx ‘d’			
ND - Explosion Proof EEx ‘d’ (US)			

Table 4: Description of the letters and numbers used for the lines of P-LB-*.*.* [1]

Letter	Channels	
	1	2
A	1 to 3	1 to 3 / 4 to 6
B	1 to 2	1 to 2 / 4 to 5
C	1 to 2 and 3	2 to 3 / 5 to 6
D	1 to 2 , 3 and 4	1 to 2 and 3 / 4 to 5 and 6
E	2 to 3	2 to 3 / 5 to 6
F	1 to 2, 3 and 6	all

Only the described configurations were analyzed. All other possible variants or electronics are not covered by this report.

Surge protective devices are not considered to be elements according to IEC 61508-4 section 3.4.5 as they are not performing one or more element safety functions. Therefore there is no need to calculate a SFF (Safe Failure Fraction). Only the interference on a safety functions needs to be considered. This interference is expressed in a contribution to the overall PFD_{AVG} / PFH.

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 Pepperl+Fuchs GmbH for the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I. For components which are not listed in the Siemens standard SN 29500 the failure rate has been taken from the *exida* Electrical & Mechanical Component Reliability Handbook.

The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment 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 (daily fluctuation of > 15°C) must be assumed.

The following table shows how the above stated requirements are fulfilled under worst-case assumptions.

[1] All mentioned lines against GND need to be considered additionally.

Table 5: P-LB-1.D.1234 or P-LB-1.F.1236 – Failure rates in FIT [2]

Signal type	4-wire RTD	3-wire RTD	Voltage Source	2-wire RTD	Potentio meter	TC
Safe state	**Threshold**	**Threshold**	**Threshold**	**Threshold**	**Threshold**	**Threshold**
Loop error detection [3]	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**
Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**0**	**0**	**0**	**0**	**0**
Fail Dangerous Detected (λ_{DD})	**43**	**23.1**	**27**	**16**	**12.1**	**8.1**
Fail Dangerous Undetected (λ_{DU})	**16**	**12**	**8.1**	**0.02**	**22.9**	**8**
No effect	143	101	101	41.1	101	41.1
No part	0	66	66.1	145	66.1	145
Total failure rate (interfering with safety function)	**59**	**35.1**	**35.1**	**16.02**	**34**	**16.1**
MTBF	**564 years**					

[2] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[3] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

Table 6: P-LB-1.A.* or P-LB-2.A.* – Failure rates in FIT [4]

Signal type	AI	AO	DI	DO
Safe state	Threshold	I < 4mA	I = 0mA U = 0V	I = 0mA U = 0V
Loop error detection [5]	<3.6mA >21mA	None	SC and LB	None

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**16.1**	**8.1**	**16.1**
Fail Dangerous Detected (λ_{DD})	**16.1**	**0**	**8**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	41.1	41.1	41.1	41.1
No part	0	0	0	0

Total failure rate (interfering with safety function)	**16.1**	**16.1**	**16.1**	**16.1**

MTBF	**1999 years (1 channel device); 999 (2 channel device)**

[4] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[5] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

Table 7: P-LB-*.B.*; P-LB-*.C.*; P-LB-2.D.*; P-LB-*.E.* or P-LB-2.F.* – Failure rates in FIT [6]

Signal type	AI	AO	DI	DO
Safe state	Threshold	I < 4mA	I = 0mA U = 0V	I = 0mA U = 0V
Loop error detection [7]	<3.6mA >21mA	None	SC and LB	None

Fail Safe (λ_{SD}) + (λ_{SU})	0	16.1	8.1	16.1
Fail Dangerous Detected (λ_{DD})	16.1	0	8	0
Fail Dangerous Undetected (λ_{DU})	5.95	5.95	5.95	5.95

No effect	42.1	42.1	42.1	42.1
No part	52	52	52	52

Total failure rate (interfering with safety function)	22.05	22.05	22.05	22.05

MTBF	983 years (1 channel device); 491 (2 channel device)

[6] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[7] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

Table 8: F*-LB-I – Failure rates in FIT [8]

Signal type	AI	AO	DI	DO
Safe state	Threshold	I < 4mA	I = 0mA U = 0V	I = 0mA U = 0V
Loop error detection [9]	<3.6mA >21mA	None	SC and LB	None

Fail Safe (λ_{SD}) + (λ_{SU})	0	6.95	0	6.95
Fail Dangerous Detected (λ_{DD})	6.95	0	6.95	0
Fail Dangerous Undetected (λ_{DU})	0	0	0	0

No effect	20.1	20.1	20.1	20.1
No part	10.1	10.1	10.1	10.1

Total failure rate (interfering with safety function)	6.95	6.95	6.95	6.95

MTBF	3078 years

[8] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[9] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

Table 9: K-LB-1.30; K-LB-2.30; K-LB-1.6 or K-LB-2.6 – Failure rates in FIT [10]

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [11]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**16.1**	**8.1**	**16.1**
Fail Dangerous Detected (λ_{DD})	**16.1**	**0**	**8**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	41.1	41.1	41.1	41.1
No part	0	0	0	0

Total failure rate (interfering with safety function)	**16.1**	**16.1**	**16.1**	**16.1**

MTBF	**1999 years (1 channel device); 999 (2 channel device)**

[10] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[11] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

Table 10: K-LB-1.30G; K-LB-2.30G; K-LB-1.6G or K-LB-2.6G – Failure rates in FIT [12]

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [13]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**15.1**	**8.1**	**15.1**
Fail Dangerous Detected (λ_{DD})	**15.1**	**0**	**7**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	22.1	22.1	22.1	22.1
No part	14	14	14	14

Total failure rate (interfering with safety function)	**15.1**	**15.1**	**15.1**	**15.1**

MTBF	**2233 (1 channel device) 1116 years (2 channel device)**

The failure rates are valid for the useful life of the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I (see Appendix 2).

[12] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[13] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

Table of Contents

1 Purpose and Scope

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I in the versions listed in the drawings referenced in section 2.4.1. Table 1 gives an overview of the different configurations that belong to the considered Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I.

The FMEDA builds the basis for an evaluation whether a sensor or final element subsystem, including the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety or the correct functioning of the surge protective devices.

An FMEDA is part of effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Pepperl+Fuchs GmbH	Manufacturer of the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I.
exida	Performed the hardware assessment.

Pepperl+Fuchs GmbH contracted *exida* in December 2011 with the FMEDA of the above mentioned devices.

2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	SN 29500-1:01.2004 SN 29500-1 H1:07.2011 SN 29500-2:09.2010 SN 29500-3:06.2009 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:07.2011 SN 29500-12:02.2008 SN 29500-15:07.2009 SN 29500-16:08.2010	Failure rates of components
[N3]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	*exida* L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N4]	EMCR Handbook, 2011 Update	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, 2011 Update

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	tdoct0606__eng.pdf	Manual "Surge Protection Barriers"; Part No 87945 10/01 01; issue date 11.2001
[D2]	510595.pdf	Circuit diagram "K-LB-*.*G (non-isolation)" 51-0595 Ind. 0 of 24.09.99
[D3]	510596.pdf	Circuit diagram "K-LB-*.* (non-isolation)" 51-0596 Ind. 0 of 24.09.99
[D4]	510597.pdf	Circuit diagram "P-LB-**" 51-0597 Ind. 0 of 11.10.01
[D5]	510598.pdf	Circuit diagram "P-LB-**" 51-0598 Ind. 0 of 11.10.01
[D6]	510599.pdf	Circuit diagram "P-LB-**" 51-0598 Ind. 0 of 11.10.01
[D7]	510630.pdf	Circuit diagram "F*-LB-*" 51-0630 Ind. 0 of 13.01.00
[D8]	FS0019PF-26A_AI_ 4_20mA.xls of 27.07.12	
[D9]	FS0019PF-26A_AO_4_20mA.xls of 04.06.12	
[D10]	FS0019PF-26A_DI_Namur.xls of 27.07.12	
[D11]	FS0019PF-26A_DO.xls of 04.06.12	
[D12]	FS0019PF-26A2_AI_4_20mA.xls of 27.07.12	
[D13]	FS0019PF-26A2_AO_4_20mA.xls of 04.06.12	
[D14]	FS0019PF-26A2_DI_Namur.xls of 27.07.12	
[D15]	FS0019PF-26A2_DO.xls of 27.07.12	
[D16]	FS0019PF-26A3_AI_4_20mA.xls of 27.07.12	
[D17]	FS0019PF-26A3_AO_4_20mA.xls of 04.06.12	
[D18]	FS0019PF-26A3_DI_Namur.xls of 27.07.12	
[D19]	FS0019PF-26A3_DO.xls of 04.06.12	
[D20]	fs0019PF-26A4_AI_4_20mA.xls of 27.07.12	
[D21]	fs0019PF-26A4_AO_4_20mA.xls of 04.06.12	
[D22]	fs0019PF-26A4_DI_Namur.xls of 27.07.12	
[D23]	fs0019PF-26A4_DO.xls of 18.04.12	
[D24]	FS0019PF-26A5_1.xls of 27.07.12	
[D25]	FS0019PF-26A5_2.xls of 27.07.12	
[D26]	FS0019PF-26A5_3.xls of 27.07.12	
[D27]	FS0019PF-26A5_4.xls of 27.07.12	
[D28]	FS0019PF-26A5_5.xls of 27.07.12	
[D29]	FS0019PF-26A5_6.xls of 27.07.12	
[D30]	FS0019PF-26A6_AI_ 4_20mA.xls of 27.07.12	

[D31]	FS0019PF-26A6_AO_4_20mA.xls of 04.06.12
[D32]	FS0019PF-26A6_DI_Namur.xls of 27.07.12
[D33]	FS0019PF-26A6_DO.xls of 14.05.12

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.4.2 Documentation generated by *exida*

[R1]	P+F 11-10-085 R036 V0R1.doc of 02.07.12 (this report)
[R2]	AW Auftrag bezüglich Surge Protection Barriers 1.msg of 15.02.12
[R3]	AW Auftrag bezüglich Surge Protection Barriers 2.msg of 17.02.12
[R4]	AW Auftrag bezüglich Surge Protection Barriers 3.msg of 27.02.12
[R5]	Feedback_2.msg of 06.07.12

3 Description of the analyzed devices

Figure 1 to Figure 4 give examples on how the surge protective devices are connected to other devices.

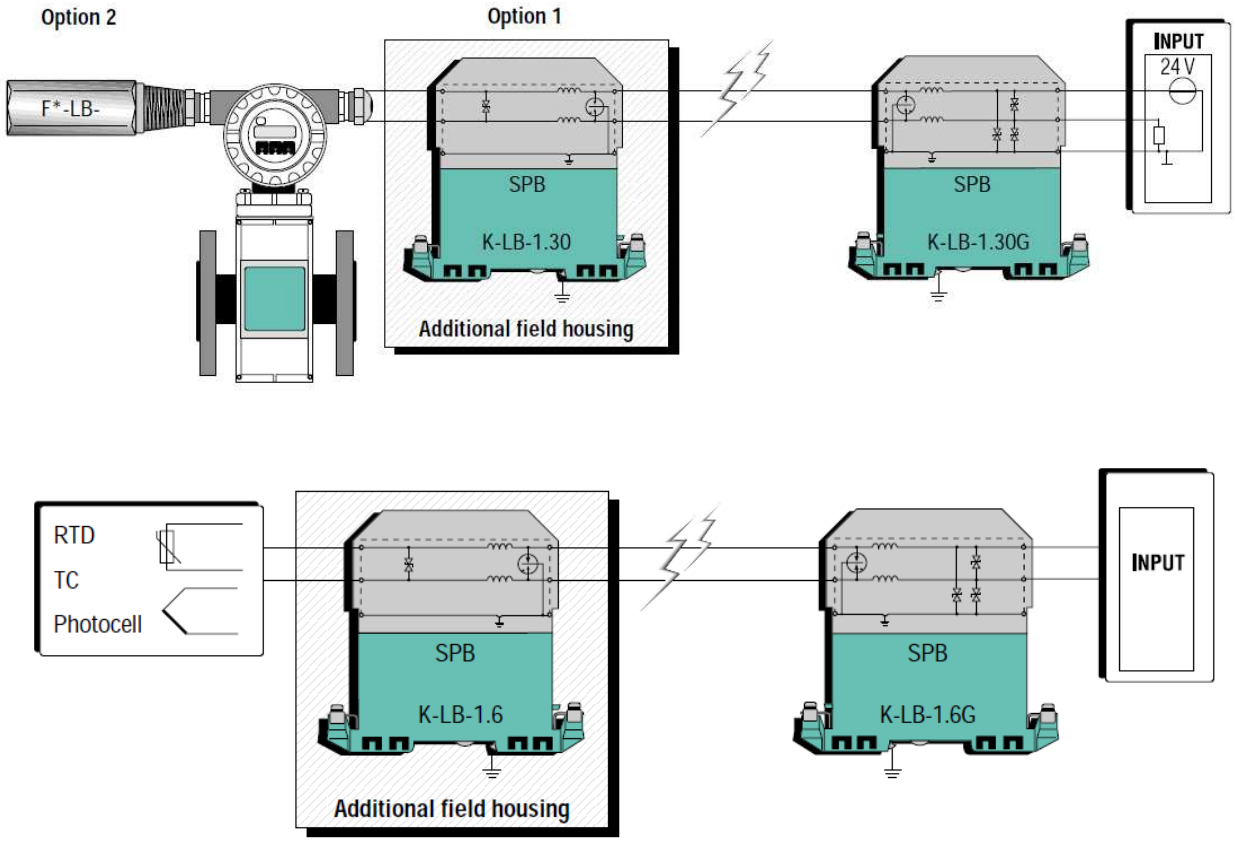


Figure 1: Connection of analog input signals

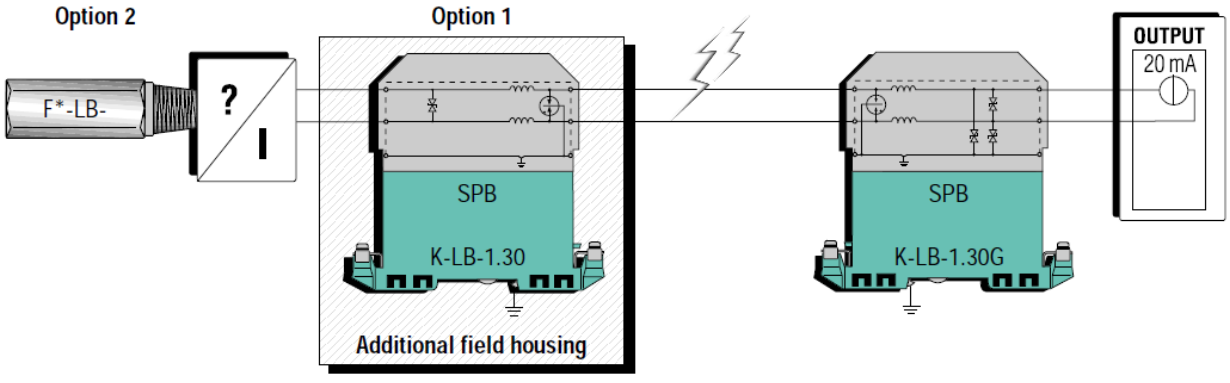


Figure 2: Connection of analog output signals

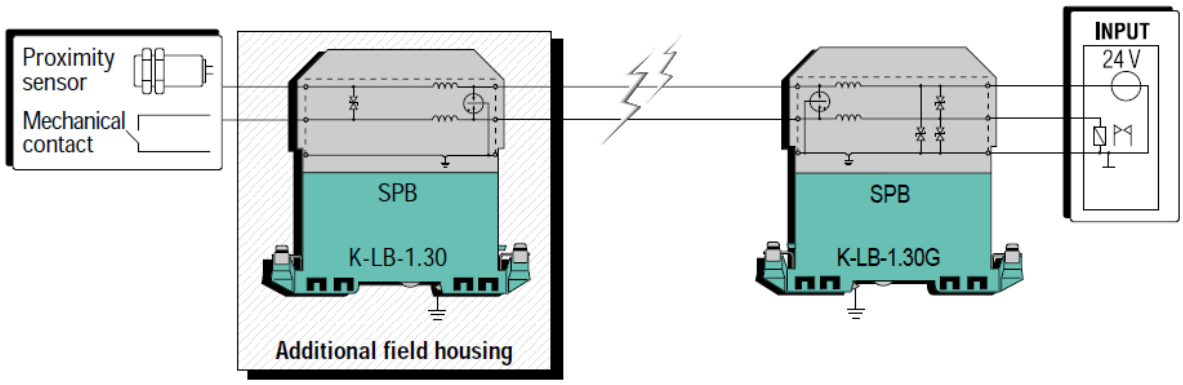


Figure 3: Connection of digital input signals

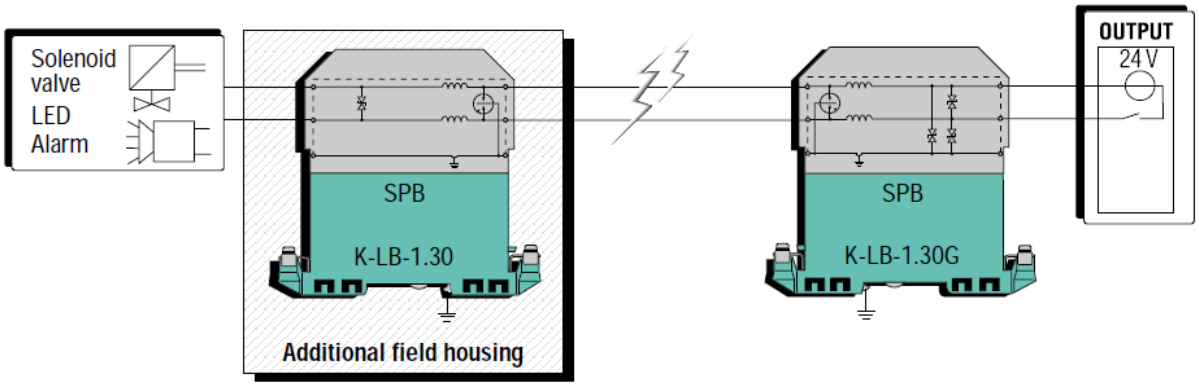


Figure 4: Connection of digital output signals

3.1 P-LB-* Surge protection barrier

This Surge protection Barrier is designed for the use with K-System (KF-Modules) and cannot be used as a standalone device.

By snapping the barriers into a standard KF module, the interface modules are safely protected against voltage surges of different origin (e. g. lightning stroke, switching impulse, etc.). This is achieved by diverting the transient current to ground and limiting the signal line voltage to a safe level for the duration of the surge. The end digits of the model designation correspond to the protected terminals of the respective KF module.

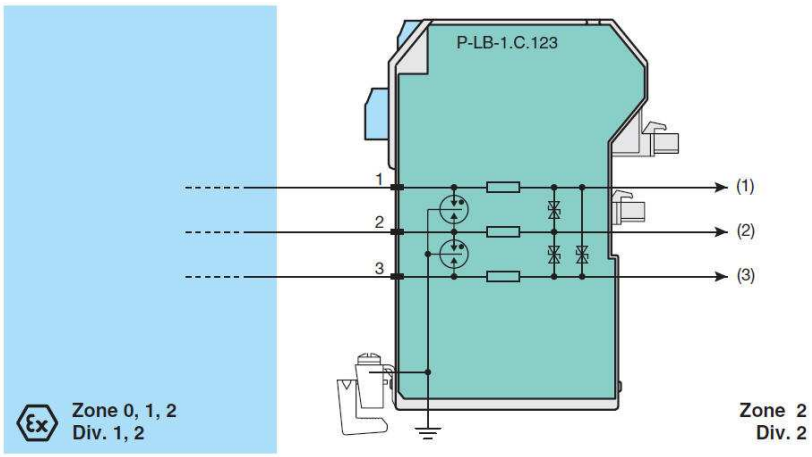


Figure 5: Connection P-LB-*

A list of devices with which the respective versions of the P-LB-* devices may be used is given in the manual [D1].

3.2 F*-LB-I Surge protection barrier

This Surge Protection Barrier limits induced transients of different origin (e. g. lightning stroke, switching impulse, etc.). It is screwed into the housing of the field device that shall be protected.

This is achieved by diverting the transient current to ground and limiting the signal line voltage to a safe level for the duration of the surge. This barrier provides 85 V line-to-line and 500V line to ground clamping voltage for the protected instruments. It also protects instruments that have less than 500V isolation to ground. It is installed in an available conduit or cable gland opening like those found on most process transmitters.

These barriers are connected to the two potentials of one particular signal line to provide safety for this special differential signal and to avoid short circuits between two separate signals.

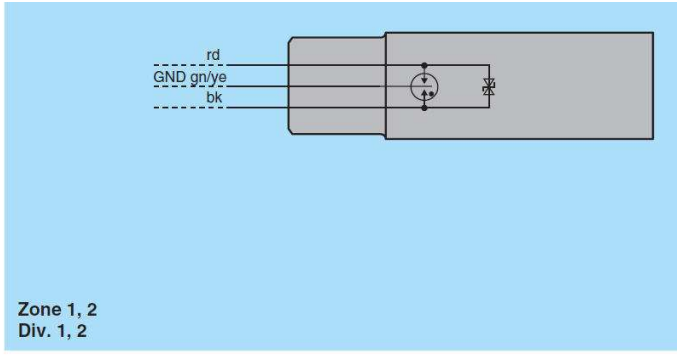


Figure 6: Connection F*-LB-I

3.3 K-LB-* Surge protection Barrier

This Surge Protection Barrier limits induced transients of different origin (e. g. lightning stroke, switching impulse, etc.). It is mounted on a DIN Rail and can be used as a standalone device.

The surge protection is achieved by diverting the transient current to ground and limiting the signal line voltage to a safe level for the duration of the surge. This barrier provides low 45 V line-to-line and 500V line to ground clamping voltage for the protected instruments. It also protects instruments that have more than 500V isolation to ground, such as intrinsic safety isolated barriers, signal conditioners and most field instruments.

The two lines shown here are connected to the two potentials of one particular signal line to provide safety for this special differential signal and to avoid short circuits between two separate signal lines.

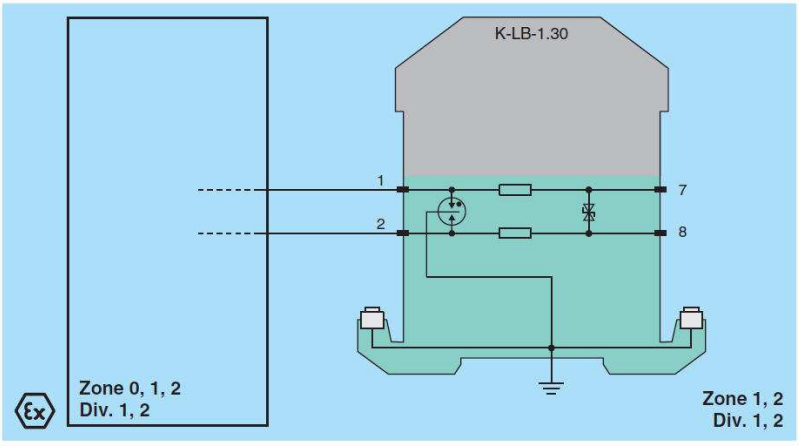


Figure 7: Connection K-LB-*

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by Pepperl+Fuchs GmbH and reviewed by *exida*. The results are documented in [D8] to [D33]. Failures have been classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I, the following definitions for the failure of the product were considered.

Fail-Safe State

AI	The fail-safe state is defined as reaching the user defined threshold value given for each application.
AO	The fail-safe state is defined as the output current being < 4mA.
DI, DO	The fail-safe state is defined as the output being de-energized (Output current = 0mA, Output voltage = 0V).

Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) deviates the output current by more than 2% of full span (in case of AI) or 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.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU).
Dangerous Detected	Failure that is dangerous but is detected by external diagnostics (DD). This corresponds to the NAMUR alarm states < 3.6mA and > 21mA or the detection of a short circuit (> 6mA) or lead breakage.
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.
No part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is a FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are the basic failure rates from the Siemens standard SN 29500. For components which are not listed in the Siemens standard SN 29500 the failure rate has been taken from the *exida* Electrical & Mechanical Component Reliability Handbook [N3] and [N4] which was derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment 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 (daily fluctuation of > 15°C) must be assumed.
- The devices are installed per manufacturer's instructions.
- The devices are used within their specified limits.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- For safety applications only the described configurations are considered.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- Short Circuit and Line Breakage Detection are used/enabled for DI.

4.4 Results

For the calculation of the Mean Time Between Failure (MTBF) the following has to be noted:

λ_{total} consists of the sum of all component failure rates. This means:

$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

MTBF = MTTF + MTTR = $(1 / (\lambda_{total} + \lambda_{no\ effect} + \lambda_{no\ part})) + 24$ h

4.4.1 P-LB-1.D.1234 or P-LB-1.F.1236

The FMEDA carried out on the Surge Protection Barriers P-LB-1.D.1234 or P-LB-1.F.1236 leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates:

Signal type	**4-wire RTD**	**3-wire RTD**	**Voltage Source**	**2-wire RTD**	**Potentio meter**	**TC**
Safe state	**Threshold**	**Threshold**	**Threshold**	**Threshold**	**Threshold**	**Threshold**
Loop error detection [14]	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**	**<3.6mA >21mA**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**0**	**0**	**0**	**0**	**0**
Fail Dangerous Detected (λ_{DD})	**43**	**23.1**	**27**	**16**	**12.1**	**8.1**
Fail Dangerous Undetected (λ_{DU})	**16**	**12**	**8.1**	**0.02**	**22.9**	**8**

No effect	143	101	101	41.1	101	41.1
No part	0	66	66.1	145	66.1	145

Total failure rate (interfering with safety function)	**59**	**35.1**	**35.1**	**16.02**	**34**	**16.1**

MTBF	**564 years**

[14] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

4.4.2 P-LB-1.A.* or P-LB-2.A.*

The FMEDA carried out on the Surge Protection Barriers P-LB-1.A.* or P-LB-2.A.* leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates:

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [15]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**16.1**	**8.1**	**16.1**
Fail Dangerous Detected (λ_{DD})	**16.1**	**0**	**8**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	41.1	41.1	41.1	41.1
No part	0	0	0	0

Total failure rate (interfering with safety function)	**16.1**	**16.1**	**16.1**	**16.1**

MTBF	**1999 years (1 channel device); 999 (2 channel device)**

[15] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

4.4.3 P-LB-*.B.*; P-LB-*.C.*; P-LB-2.D.*; P-LB-*.E.* or P-LB-2.F.*

The FMEDA carried out on the Surge Protection Barriers P-LB-*.B.*; P-LB-*.C.*; P-LB-2.D.*; P-LB-*.E.* or P-LB-2.F.* leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates:

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [16]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**16.1**	**8.1**	**16.1**
Fail Dangerous Detected (λ_{DD})	**16.1**	**0**	**8**	**0**
Fail Dangerous Undetected (λ_{DU})	**5.95**	**5.95**	**5.95**	**5.95**

No effect	42.1	42.1	42.1	42.1
No part	52	52	52	52

Total failure rate (interfering with safety function)	**22.05**	**22.05**	**22.05**	**22.05**

MTBF	**983 years (1 channel device); 491 (2 channel device)**

[16] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

4.4.4 F*-LB-I

The FMEDA carried out on the Surge Protection Barriers F*-LB-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates:

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [17]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**6.95**	**0**	**6.95**
Fail Dangerous Detected (λ_{DD})	**6.95**	**0**	**6.95**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	20.1	20.1	20.1	20.1
No part	10.1	10.1	10.1	10.1

Total failure rate (interfering with safety function)	**6.95**	**6.95**	**6.95**	**6.95**

MTBF	**3078 years**

[17] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

4.4.5 K-LB-1.30; K-LB-2.30; K-LB-1.6 or K-LB-2.6

The FMEDA carried out on the Surge Protection Barriers K-LB-1.30; K-LB-2.30; K-LB-1.6 or K-LB-2.6 leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates:

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [18]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**16.1**	**8.1**	**16.1**
Fail Dangerous Detected (λ_{DD})	**16.1**	**0**	**8**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	41.1	41.1	41.1	41.1
No part	0	0	0	0

Total failure rate (interfering with safety function)	**16.1**	**16.1**	**16.1**	**16.1**

MTBF	**1999 years (1 channel device); 999 (2 channel device)**

[18] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

4.4.6 K-LB-1.30G; K-LB-2.30G; K-LB-1.6G or K-LB-2.6G

The FMEDA carried out on the Surge Protection Barriers K-LB-1.30G; K-LB-2.30G; K-LB-1.6G or K-LB-2.6G leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates:

Signal type	**AI**	**AO**	**DI**	**DO**
Safe state	**Threshold**	**I < 4mA**	**I = 0mA U = 0V**	**I = 0mA U = 0V**
Loop error detection [19]	**<3.6mA >21mA**	**None**	**SC and LB**	**None**

Fail Safe (λ_{SD}) + (λ_{SU})	**0**	**15.1**	**8.1**	**15.1**
Fail Dangerous Detected (λ_{DD})	**15.1**	**0**	**7**	**0**
Fail Dangerous Undetected (λ_{DU})	**0**	**0**	**0**	**0**

No effect	22.1	22.1	22.1	22.1
No part	14	14	14	14

Total failure rate (interfering with safety function)	**15.1**	**15.1**	**15.1**	**15.1**

MTBF	**2233 (1 channel device) 1116 years (2 channel device)**

[19] This error detection has to be provided by the safety loop architecture (e.g. Namur Signal – Line Break and Short Circuit detection, Current loop < 3.6mA and >21mA detection).

5 Using the FMEDA results

The following section describes how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} / PFH calculation

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The following results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) surge protective device considering a proof test coverage of 99% (see Appendix 1.2) and a mission time of 10 years. The failure rate data used in this calculation are displayed in sections 4.4.1 to 4.4.6. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 11 to Table 16.

For SIL2 the overall PFD_{AVG} shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 1/h. As the surge protective devices are contributing to the entire safety function they should only consume a certain percentage of the allowed range. Assuming 5% of this range as a reasonable budget they should be better than or equal to 5.00E-04 or 5.00E-08 1/h, respectively. The calculated PFD_{AVG} (at T[Proof] = 1 year) / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 5% of the allowed range, i.e. to be better than or equal to 5.00E-04 or 5.00E-08 1/h, respectively.

Table 11: PFD_{AVG} / PFH for P-LB-1.D.1234 or P-LB-1.F.1236

	T[Proof] = 1 year	T[Proof] = 5 years	PFH
4-wire RTD	PFD_{AVG} = 7.74E-05	PFD_{AVG} = 3.55E-04	PFH = 1.60E-08 1/h
3-wire RTD	PFD_{AVG} = 5.78E-05	PFD_{AVG} = 2.66E-04	PFH = 1.20E-08 1/h
RTD with TC comp	PFD_{AVG} = 3.93E-05	PFD_{AVG} = 1.80E-04	PFH = 8.10E-09 1/h
2-wire RTD	PFD_{AVG} = 4.79E-07	PFD_{AVG} = 8.26E-07	PFH = 2.00E-11 1/h
Potentiometer	PFD_{AVG} = 1.10E-04	PFD_{AVG} = 5.07E-04	PFH = 2.29E-08 1/h
TC	PFD_{AVG} = 3.84E-05	PFD_{AVG} = 1.77E-04	PFH = 7.97E-09 1/h

Table 12: PFD_{AVG} / PFH for P-LB-*.B.*; P-LB-*.C.*; P-LB-2.D.*; P-LB-*.E.* or P-LB-2.F.*

	T[Proof] = 1 year	T[Proof] = 5 years	PFH
AI	PFD_{AVG} = 2.88E-05	PFD_{AVG} = 1.32E-04	PFH = 5.95E-09 1/h
AO	PFD_{AVG} = 2.84E-05	PFD_{AVG} = 1.32E-04	PFH = 5.95E-09 1/h
DI	PFD_{AVG} = 2.86E-05	PFD_{AVG} = 1.32E-04	PFH = 5.95E-09 1/h
DO	PFD_{AVG} = 2.84E-05	PFD_{AVG} = 1.32E-04	PFH = 5.95E-09 1/h

For SIL3 the overall PFD_{AVG} shall be better than 1.00E-03 and the PFH shall be better than 1.00E-07 1/h. As the surge protective devices are contributing to the entire safety function they should only consume a certain percentage of the allowed range. Assuming 5% of this range as a reasonable budget they should be better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively. The calculated PFD_{AVG} (at T[Proof] = 1 year) / PFH values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 5% of the allowed range, i.e. to be better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively.

Table 13: PFD_{AVG} / PFH for P-LB-1.A.* or P-LB-2.A.*

	T[Proof] = 1 year	T[Proof] = 5 years	PFH
AI	PFD_{AVG} = 3.86E-07	PFD_{AVG} = 3.86E-07	PFH = 0.00E-00 1/h
AO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h
DI	PFD_{AVG} = 1.92E-07	PFD_{AVG} = 1.92E-07	PFH = 0.00E-00 1/h
DO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h

Table 14: PFD_{AVG} / PFH for F*-LB-I

	T[Proof] = 1 year	T[Proof] = 5 years	PFH
AI	PFD_{AVG} = 1.67E-07	PFD_{AVG} = 1.67E-07	PFH = 0.00E-00 1/h
AO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h
DI	PFD_{AVG} = 1.67E-07	PFD_{AVG} = 1.67E-07	PFH = 0.00E-00 1/h
DO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h

Table 15: PFD_{AVG} / PFH for K-LB-1.30; K-LB-2.30; K-LB-1.6 or K-LB-2.6

	T[Proof] = 1 year	T[Proof] = 5 years	PFH
AI	PFD_{AVG} = 3.86E-07	PFD_{AVG} = 3.86E-07	PFH = 0.00E-00 1/h
AO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h
DI	PFD_{AVG} = 1.92E-07	PFD_{AVG} = 1.92E-07	PFH = 0.00E-00 1/h
DO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h

Table 16: PFD_{AVG} / PFH for K-LB-1.30G; K-LB-2.30G; K-LB-1.6G or K-LB-2.6G

	T[Proof] = 1 year	T[Proof] = 5 years	PFH
AI	PFD_{AVG} = 3.62E-07	PFD_{AVG} = 3.62E-07	PFH = 0.00E-00 1/h
AO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h
DI	PFD_{AVG} = 1.68E-07	PFD_{AVG} = 1.68E-07	PFH = 0.00E-00 1/h
DO	PFD_{AVG} = 0.00E-00	PFD_{AVG} = 0.00E-00	PFH = 0.00E-00 1/h

6 Terms and Definitions

AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTBF	Mean Time Between Failure
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
RTD	Resistance Temperature Device
SFF	Safe Failure Fraction summarizes the fraction of failures which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
TC	Thermocouple
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

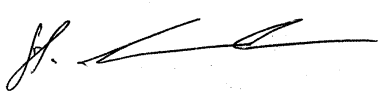
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version History:	V1R0:	Review comments incorporated, September 20, 2012
	V0R2:	First external review comments incorporated; August 7, 2012
	V0R1:	Initial version; July 6, 2012
Author:	Stephan Aschenbrenner	
Review:	V0R2:	Rachel Amkreutz (*exida*); September 18, 2012
		Michael Kindermann (P+F); August 16, 2012
	V0R1:	Michael Kindermann (P+F); July 27, 2012
Release status:	Released to Pepperl+Fuchs GmbH	

7.3 Release Signatures



Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

Rachel Amkreutz, Safety Engineer

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1: Proof test to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 17.

Table 17 Steps for a possible proof Test

Step	Action
1	Bypass the connected safety device(s) or take other appropriate action to avoid a false trip
2	Force the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I to reach predefined output signals over the entire range and verify that the output behaves as expected.
3	Restore the loop to full operation
4	Remove the bypass from the connected safety device(s) or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures of the Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I.

Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime[20] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive).

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 the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime 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 lifetime is valid.

The Surge Protection Barriers K-LB-*.**, P-LB-*.*.* and F*-LB-I do not contain components with reduced useful lifetime which are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation. Therefore there is no limiting factor to the useful lifetime.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[20] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.