



FMEDA including SFF determination and PFD calculation

Project:

Transformer Isolated Barriers KF**-SR2-***

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 02/4-12

Report No.: P+F 02/4-12 R007

Version V1, Revision R1.4, April 2005

Stephan Aschenbrenner

Management summary

This report summarizes the results of the FMEDAs carried out on the transformer isolated barriers KF**-SR2-***. '***' and '****' stand for the different versions that are available. Table 1 gives an overview and explains the differences.

Depending on the setting of switch S1/S2 (two channel unit) or only S1 (single channel unit) the mode of operation can be configured. The results given in this report are meant for S1/S2 (two channel unit) or only S1 (single channel unit) in position I which is considered to be the normal mode of operation and S1/S2 (two channel unit) or only S1 (single channel unit) in position II which is considered to be the inverse mode of operation. For safety reasons the third switch S3 shall always be set to LB/SC¹ activated (position I).

A FMEDA is one of the steps taken to achieve functional safety certification 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 certification purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview

Type	Supply voltage	Number of channels	Output contacts per channel	Error contact ²	Housing
KFD2-SR2-Ex2.W ³	24 VDC	2	1 change over	-	DIN-rail
KFD2-SR2-Ex1.W	24 VDC	1	1 change over	-	DIN-rail
KFD2-SR2-Ex1.W.LB	24 VDC	1	1(2) change over	yes	DIN-rail
KFA4-SR2-Ex2.W	100 VAC	2	1 change over	-	DIN-rail
KFA4-SR2-Ex1.W	100 VAC	1	1 change over	-	DIN-rail
KFA4-SR2-Ex1.W.LB	100 VAC	1	1(2) change over	yes	DIN-rail
KFA5-SR2-Ex2.W	115 VAC	2	1 change over	-	DIN-rail
KFA5-SR2-Ex1.W	115 VAC	1	1 change over	-	DIN-rail
KFA5-SR2-Ex1.W.LB	115 VAC	1	1(2) change over	yes	DIN-rail
KFA6-SR2-Ex2.W	230 VAC	2	1 change over	-	DIN-rail
KFA6-SR2-Ex1.W	230 VAC	1	1 change over	-	DIN-rail
KFA6-SR2-Ex1.W.LB	230 VAC	1	1(2) change over	yes	DIN-rail
KFD2-SR2-Ex2.2S ⁴	24 VDC	2	2 normally open	-	DIN-rail

The failure rates are based on the Siemens standard SN 29500.

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 10^{-3} .

The KF**-SR2-*** boards are considered to be Type B components.

¹ LB: Lead Breakage, SC: Short Circuit

² Error message output for LB/SC (Lead Breakage / Short Circuit) at the input.

³ W: change over contact

⁴ 2S: 2 normally open contacts per channel

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

However, according to the requirements of IEC 61511-1 draft d1FDIS 15/08/01 section 11.4.4 and the assessment described in section 5.1 a SFF of 60% to < 90% is sufficient for SIL 2 (sub-) systems being Type B components and having a hardware fault tolerance of 0.

The following table shows which boards (considering one input and one output being part of the safety function) fulfill this requirement.

Table 2: Summary of all considered KF-SR2-*** boards⁵**

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
KFD2-SR2-Ex2.W	PFD _{AVG} = 3.17E-04	PFD _{AVG} = 6.33E-04	PFD _{AVG} = 1.58E-03	> 74 %
KFD2-SR2-Ex1.W	PFD _{AVG} = 3.17E-04	PFD _{AVG} = 6.33E-04	PFD _{AVG} = 1.58E-03	> 74 %
KFD2-SR2-Ex1.W.LB	PFD _{AVG} = 3.17E-04	PFD _{AVG} = 6.33E-04	PFD _{AVG} = 1.58E-03	> 74 %
KFA4-SR2-Ex2.W	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA4-SR2-Ex1.W	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA4-SR2-Ex1.W.LB	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA5-SR2-Ex2.W	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA5-SR2-Ex1.W	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA5-SR2-Ex1.W.LB	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA6-SR2-Ex2.W	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA6-SR2-Ex1.W	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFA6-SR2-Ex1.W.LB	PFD _{AVG} = 2.85E-04	PFD _{AVG} = 5.70E-04	PFD _{AVG} = 1.42E-03	> 71 %
KFD2-SR2-Ex2.2S	PFD _{AVG} = 3.70E-04	PFD _{AVG} = 7.39E-04	PFD _{AVG} = 1.85E-03	> 74 %

The boxes marked in yellow () mean that the calculated PFD values are within the allowed range for SIL 2 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 10^{-3} . The boxes marked in green () mean that the calculated PFD values fulfill this requirement to be better than 10^{-3} .

The two channels on each module shall not be used to increase the hardware fault tolerance needed for a higher SIL as they contain common components.

⁵ The results are based on the FMEDAs carried out at the “two channel” versions but are considered to be the same for the “one channel” versions as also for the “two channel” versions only one channel was considered. The table represents the results of the normal mode of operation. The values of the inverse mode of operation are equal or slightly better.

Table of Contents

Management summary	2
1 Purpose and Scope	5
2 Project management	6
2.1 exida.com	6
2.2 Roles of the parties involved	6
2.3 Standards / Literature used	6
2.4 Reference documents	7
2.4.1 Documentation provided by the customer	7
2.4.2 Documentation generated by exida.com	7
3 Description of the analyzed modules	8
3.1 KF**-SR2-***	8
4 Failure Modes, Effects, and Diagnostics Analysis	9
4.1 Description of the failure categories	9
4.2 Methodology – FMEDA, Failure rates	9
4.2.1 FMEDA	9
4.2.2 Failure rates	10
4.2.3 Assumption	10
5 Results of the assessment	11
5.1 Assessment of the KF**-SR2-*** boards	12
5.2 KFD2-SR2-Ex2.W	14
5.3 KFD2-SR2-Ex2.2S	15
5.4 KFA*-SR2-Ex2.W	16
6 Proven-in-use Proof	17
7 Terms and Definitions	18
8 Status of the document	19
8.1 Liability	19
8.2 Releases	19
8.3 Release Signatures	19

1 Purpose and Scope

Hardware assessment with proven-in-use consideration of the software according to IEC 61508 / draft IEC 61511

The hardware assessment contains a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the Probability of Failure on Demand (PFD). In addition it also contains an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This assessment for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced requirements of draft IEC 61511 for sensors, final elements and other PE field devices.

This document shall describe the results of the assessment carried out on the transformer isolated barriers KF**-SR2-***. '**' and '***' stand for the different versions that are available. Table 1 gives an overview and explains the differences.

It shall be assessed whether these boards meet the Probability of Failure on Demand (PFD) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508 / draft IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

Pepperl+Fuchs GmbH contracted *exida.com* in April 2002 with the FMEDA and PFD calculation of the above mentioned devices.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 100 years of cumulative experience in functional safety. Founded by several of world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Pepperl+Fuchs	Manufacturer of the transformer isolated barriers.
<i>exida.com</i>	Did the FMEDAs together with the determination of the Safe Failure Fraction (SFF) and calculated the Probability of Failure on Demand (PFD) using Markov models.

2.3 Standards / Literature used

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

N1	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	d1FDIS IEC 61511-1:2001	Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements
N3	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
N4	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
N5	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	51-0651, Index 0 of 09.02.01	Circuit diagram for KFA*.-SR2-Ex2.W
[D1.1]	Product No. 103373	Bill of material for KFA*.-SR2-EX2.W
[D2]	01-6740A of 17.06.04	Circuit diagram for KFD2-SR2-Ex2.W
[D2.1]	Product No. 132960 / 802524	Bill of material for KFD2-SR2-Ex2.W
[D3]	01-6821A of 09.12.04	Circuit diagram for KFD2-SR2-Ex2.2S
[D3.1]	Product No. 181284 / 802635	Bill of material for KFD2-SR2-Ex2.2S
[D4]	ingeniTRON, 29.07.02	Firmware description of the KF*-SR2-Ex*(.W).* device family
[D5]	ingeniTRON, 29.07.02	Firmware KF*-SR2-Ex*(.W).* flowchart
[D6]	28.06.02	SR2_Statistik.xls
[D7]	28.06.02	Verkauf vs Fehler.xls
[D8]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D9]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D10]	12.02.02	P0205010202 NCDRWorkflow.ppt

2.4.2 Documentation generated by exida.com

R1	FMEDA V5 KFD2 SR2-Ex2.W with uC V1 R1.3.xls of 15.04.05
R2	FMEDA V5 KFA SR2-Ex2.W with uC V1 R1.1.xls of 08.07.04
R3	FMEDA V5 KFD2 SR2-Ex2.2S with uC V1 R1.3.xls of 15.04.05

3 Description of the analyzed modules

3.1 KF**-SR2-***

The transformer isolated barriers KFD2-SR2-*** and KFA*-SR2-*** transfer binary signals from the hazardous area.

Sensors per DIN EN 60947-5-6 (NAMUR) and mechanical contacts may be used.

The control circuits are monitored for lead breakage (LB) and short circuit (SC). The external faults are indicated according to NAMUR NE44 by a red flashing LED. At the KFD2-SR2-*** types additionally a LB/SC-combined error signal is transferred via Power Rail to the power feed module.

The intrinsically safe inputs per DIN EN 50020 are safely isolated from the output and the power supply. The relay outputs are safely isolated from the power supply in accordance with DIN VDE 0106 Section 101 (DIN EN 50178 in case of KFD2-SR2-Ex2.2S). The relay outputs are galvanically isolated from each other in accordance with DIN EN 50178.

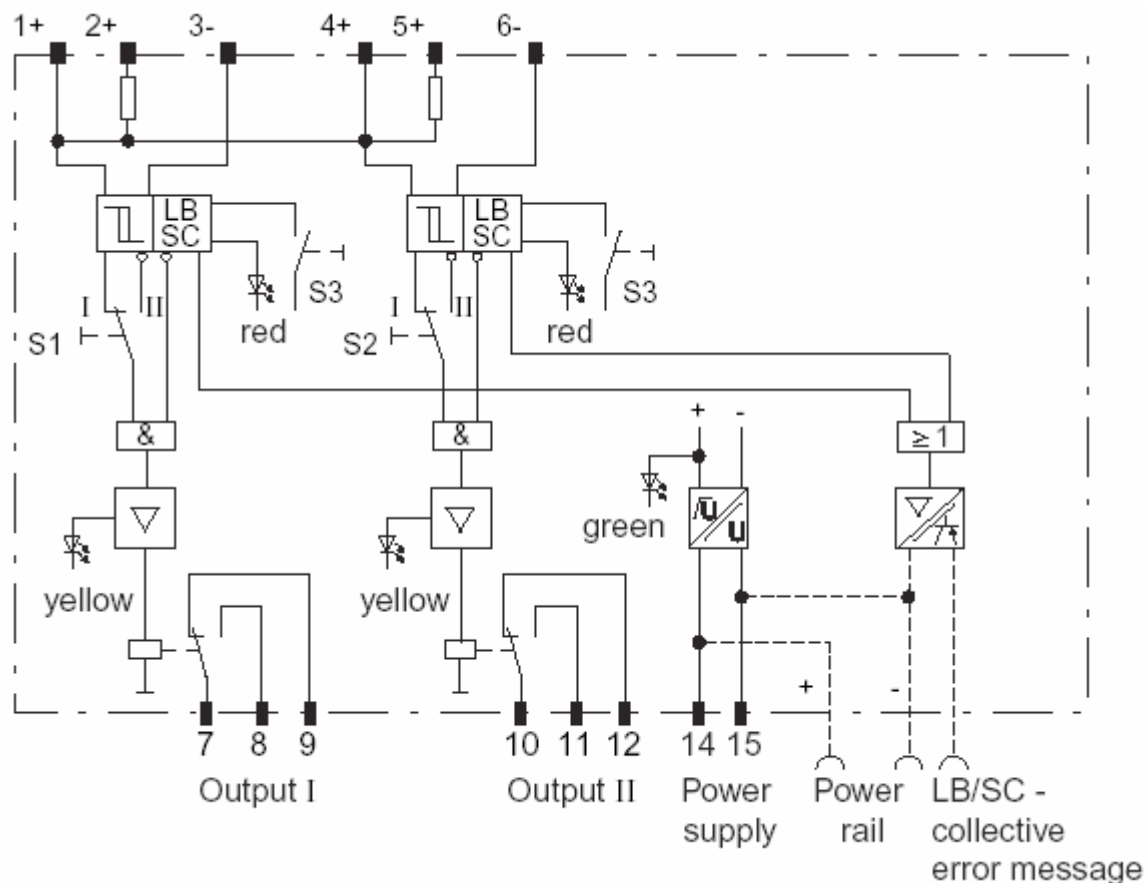


Figure 1: Block diagram of KF**-SR2-***

Remark: The description above is valid accordingly for all other KF**-SR2-*** versions with the exception that this version has two output channels. The differences between the versions are described in Table 1.

4 Failure Modes, Effects, and Diagnostics Analysis

4.1 Description of the failure categories

The **fail-safe state** is defined as the output being de-energized. This corresponds to an input signal of about 1mA and S1:A/B open which is considered to be the normal mode of operation or an input signal of about 4mA and S1:A/B closed which is considered to be the inverse mode of operation.

Failures are categorized and defined as follows:

A **safe** failure (S) is defined as a failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.

A **dangerous** failure (D) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

A "don't care" failure (#) is defined as a failure of a component that is part of the safety function but has no effect on the safety function of the module / (sub)system.

"Not considered" (!) means that this failure mode was not considered. When calculating the SFF and the PFD this failure mode is divided into 50% safe failures and 50% dangerous undetected failures.

"not part" (-) means that 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.

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 change of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an 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 from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida.com* in this FMEDA are from the Siemens SN 29500 failure rate database. 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 similar to ISA 71.01 class D. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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 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.

4.2.3 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the smart transmitter isolator boards.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All component failure modes are known.
- The repair time after a safe failure is 8 hours.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment.
- Only one channel on a module is used to carry out the safety function.
- All modules are operated in the low demand mode of operation.

5 Results of the assessment

exida.com did the FMEDAs together with Pepperl+Fuchs.

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

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

$$\lambda_{\text{total}} = \lambda_{\text{safe}} + \lambda_{\text{dangerous}} + \lambda_{\text{don't care}}^6 + \lambda_{\text{not considered}}^7.$$

$$\text{SFF} = 1 - \lambda_{\text{du}}^8 / \lambda_{\text{total}}$$

The reason for considering also the “not considered” failure rate for the calculation of the SFF is that the SFF is a measure for the effectiveness of the implemented diagnostic and the percentage of known “safe” failures against all possible component failures.

exida.com estimated for the PFD calculation the effect of the “not considered” failures as 50% “safe” failures and 50% “dangerous” failures.

For the FMEDAs failure modes and distributions were used based on information gained from N3 and N4.

For the calculation of the PFD the following Markov model for a 1oo1 system was used. As there are no explicit on-line diagnostics, no state “dd” – dangerous detected is required. As after a complete proof all states are going back to the OK state no proof rate is shown in the Markov models but included in the calculation.

The proof time was changed using the Microsoft® Excel 2000 based FMEDA tool of exida.com as a simulation tool. The results are documented in the following sections.

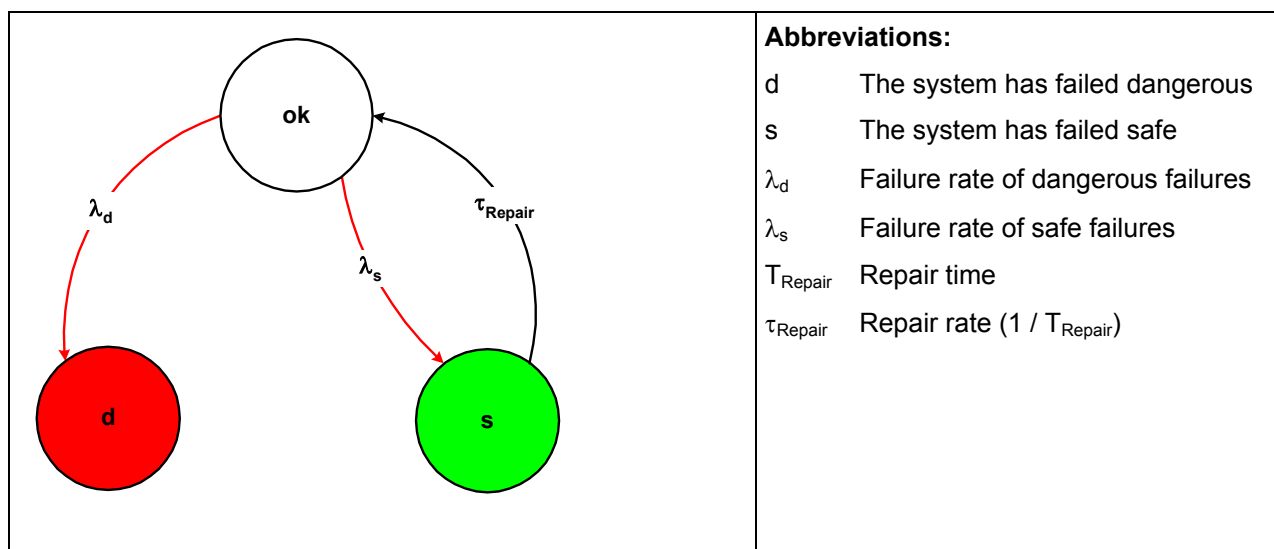


Figure 2: Markov model

⁶ These are all failures that have no impact on the safety function. The behavior of the system is neither dangerous nor safe.

⁷ This is the failure rate of failure modes that were not considered.

⁸ This is the failure rate of all dangerous undetected failures plus 50% of the “non considered” failures.

5.1 Assessment of the KF**-SR2-*** boards

According to IEC 61511-1 draft d1FDIS 15/08/01 section 11.4.4 for all subsystems (e.g., sensor, final elements and non-PE logic solvers) except PE logic solvers the minimum hardware fault tolerance (SFF = 60% - < 90%) specified in Table 5b of this standard may be reduced by one if the devices used comply with all of the following:

- the device is “proven in use” (see section 6 “Proven-in-use Proof”)
- the device allows adjustment of process-related parameters only, e.g., measuring range, upscale or downscale failure direction, etc.;
- the adjustment of the process-related parameters of the device is protected, e.g., jumper, password;
- the function has a SIL requirement less than 4.

Table 5b of IEC 61511-1 draft d1FDIS 15/08/01

(Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers):

SIL	Minimum Hardware Fault Tolerance	
	Does not meet 11.4.4 requirements	Meets 11.4.4 requirements
1	0	0
2	1	0
3	2	1
4	Special requirements apply - See IEC 61508	

This means that if the requirements of section 11.4.4 of IEC 61511-1 draft d1FDIS 15/08/01 are fulfilled a SFF of 60% to < 90% is sufficient for SIL 2 (sub-) systems with a hardware fault tolerance of 0.

The assessment of the KF**-SR2-*** boards has shown that the requirements of IEC 61511-1 draft d1FDIS 15/08/01 section 11.4.4 are fulfilled based on the following argumentation:

Requirement	Argumentation ⁹
Proven-in-use Proof according to the requirements of section 11.5.3 of IEC 61511-1 draft d1FDIS 15/08/01 (see section 6 “Proven-in-use Proof”)	1. The devices are considered to be suitable for use in safety instrumented systems as they were already used for 2 years in identical applications. They are considered to be of low complexity and the probability that they will fail is very low (0,01%). 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D8] to [D10]. The performance of the devices will remain the same. 3. The configuration of the device by the user is of process related parameters only and the configuration of the device is protected against change by the user by mechanical means. 4. Under the responsibility of Pepperl+Fuchs GmbH – no argumentation. 5. Given by the operating instructions for the KF**-SR2-*** boards. 6. Same operational profile. 7. N/A 8. Error message outputs are not part of the safety function and do not jeopardize the required safety instrumented functions. 9. Operating experience of the KF**-SR2-*** boards exist with 152.208.000 operating hours. This is considered to be sufficient taking into account the low complexity of the KF**-SR2-*** boards and the use in SIL 2 safety functions only.
Adjustment of process-related parameters only	No parameters can be adjusted.
Adjustment of process-related parameters is protected	No parameters can be adjusted.
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that for the KF**-SR2-*** boards the minimum hardware fault tolerance (HFT) specified in Table 5b of IEC 61511-1 draft d1FDIS 15/08/01 can be reduced by one. The required SFF of 60% - < 90% for HFT =1 can therefore be applied for HFT = 0.

⁹ The numbering is based on the requirements detailed in section 6 “Proven-in-use Proof”.

5.2 KFD2-SR2-Ex2.W

The FMEDA carried out on the KFD2-SR2-Ex2.W board, which is considered to be representative for all KFD2-SR2-Ex* boards besides the KFD2-SR2-Ex2.2S board, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{\text{total}} = 2,88\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 9,21\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,58\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 7,66\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 9,30\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 6,27\text{E-}08 \text{ 1/h}$$

$$\text{SFF} = 74,86\%$$

The PFD was calculated for three different proof times using the Markov model as described in Figure 2.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.17E-04	PFD_{AVG} = 6.33E-04	PFD_{AVG} = 1.58E-03

The boxes marked in yellow () mean that the calculated PFD values are within the allowed range for SIL 2 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 10^{-3} . The boxes marked in green () mean that the calculated PFD values fulfill this requirement to be better than 10^{-3} .

The following figure shows the result of the PFD calculation for T[Proof] = 1 year.

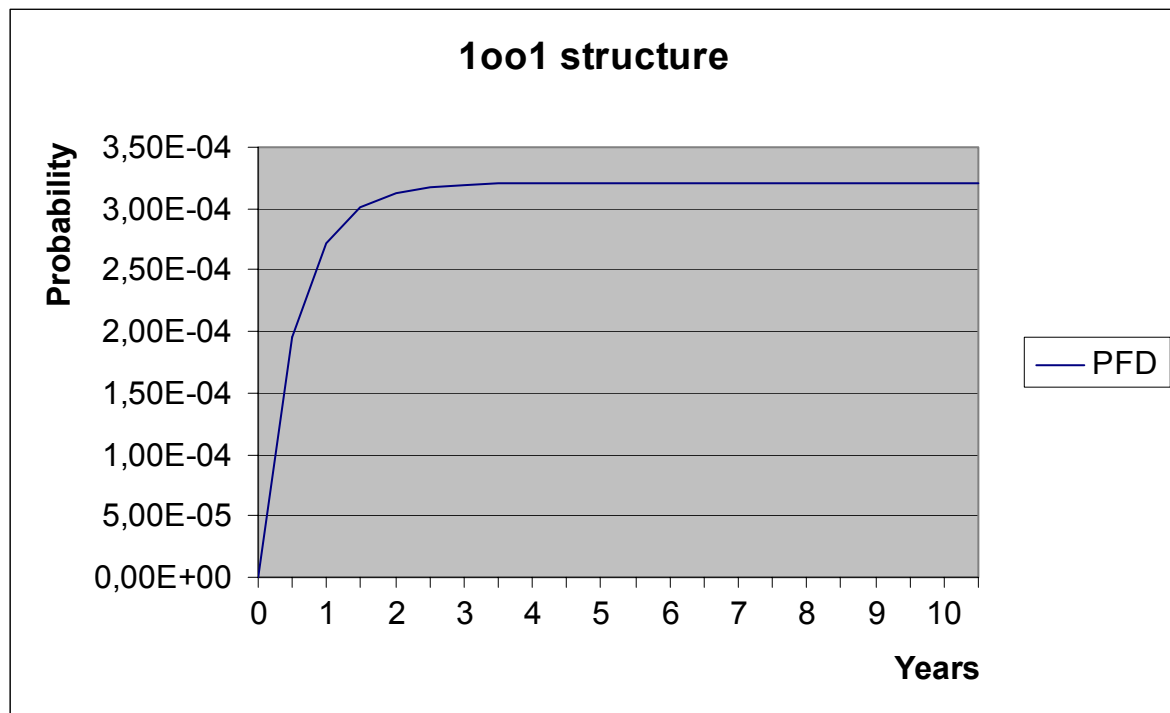


Figure 3: PFD for T[Proof] = 1 year

5.3 KFD2-SR2-Ex2.2S

The FMEDA carried out on the KFD2-SR2-Ex2.2S board leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{\text{total}} = 3,27\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 1,02\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 3,03\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 8,63\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 1,08\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 6,64\text{E-}08 \text{ 1/h}$$

$$\text{SFF} = 74,18\%$$

The PFD was calculated for three different proof times using the Markov model as described in Figure 2.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.70E-04	PFD_{AVG} = 7.39E-04	PFD_{AVG} = 1.85E-03

The boxes marked in yellow () mean that the calculated PFD values are within the allowed range for SIL 2 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 10^{-3} . The boxes marked in green () mean that the calculated PFD values fulfill this requirement to be better than 10^{-3} .

The following figure shows the result of the PFD calculation for T[Proof] = 1 year.

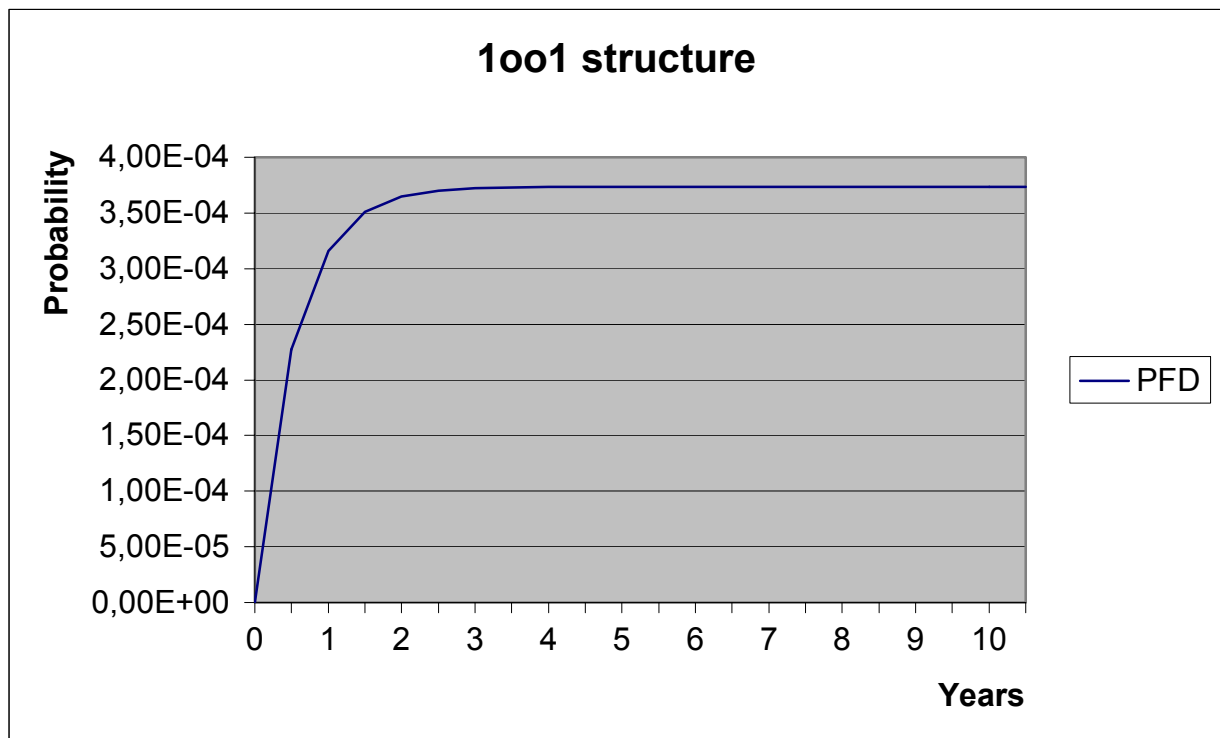


Figure 4: PFD for T[Proof] = 1 year

5.4 KFA*-SR2-Ex2.W

The FMEDA carried out at the KFA*-SR2-Ex2.W board, which is considered to be representative for all KFA*-SR2-Ex* boards, leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{\text{total}} = 2,29\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 7,41\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,71\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{don't care}} = 5,19\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 7,61\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 2,00\text{E-}08 \text{ 1/h}$$

$$\text{SFF} = 71,58\%$$

The PFD was calculated for three different proof times using the Markov model as described in Figure 2.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 2.85E-04	PFD_{AVG} = 5.70E-04	PFD_{AVG} = 1.42E-03

The boxes marked in yellow () mean that the calculated PFD values are within the allowed range for SIL 2 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 10^{-3} . The boxes marked in green () mean that the calculated PFD values fulfill this requirement to be better than 10^{-3} .

The following figure shows the result of the PFD calculation for T[Proof] = 1 year.

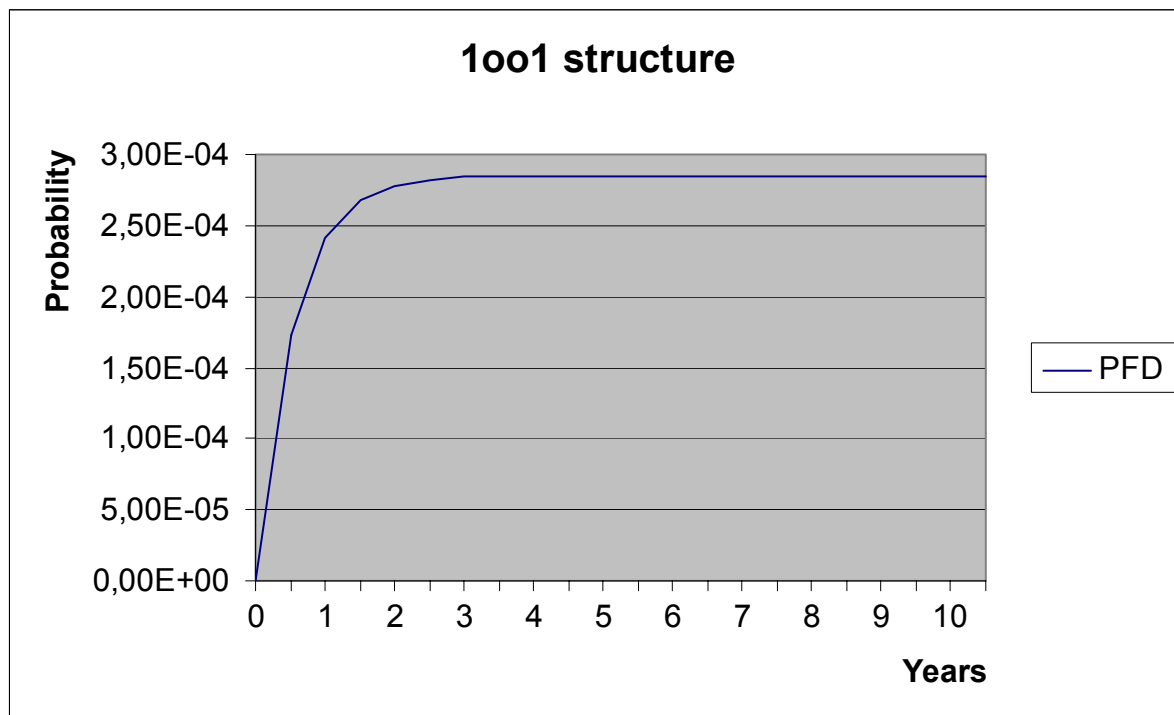


Figure 5: PFD for T[Proof] = 1 year

6 Proven-in-use Proof

1. An assessment shall provide appropriate evidence that the component is suitable for use in the safety instrumented system.
 - This requires that the component is both able to perform the required function(s) and that the previous use of the component has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the safety instrumented system, due to either random hardware failures or systematic faults in hardware or software.
 - In the case of field elements there may be extensive operating experience either in safety or non-safety applications. This can be used as a basis for the assessment.
 - The level of details of the assessment should be in accordance with the complexity of the considered component and with the probability of failure necessary to achieve the required safety integrity level of the safety instrumented function (s).
2. For all devices the assessment shall include the following:
 - consideration of the manufacturers quality management and configuration management systems;
 - consideration of the performance of the device in a similar operating profile.
3. For PE devices (other than those where the configuration of the device by the user is of process related parameters only and where the configuration of the device is protected against change by the user) the following additional details shall be included in the assessment.
 - the precise identification of the component including the hardware and software version used on which operating experience is based;
 - the conditions of use (operational profile) of the component (environment, modes of use, used services, configuration, etc.);
 - the volume of the operating experience (number of systems, periods of operation, etc.).
4. The component shall be compliant with the safety requirements derived from the SIS safety requirements.
5. There shall be adequate documentation to allow integration, operation and maintenance of the component in the safety instrumented system.
6. The assessment of suitability shall be based on the previous use of components having a similar operational profile as the component used within the safety instrumented system taking into account the SIL of the associated SIF.
7. Where there is any difference between the operational profile of the component as experienced previously, and the operational profile of the component when used within the safety instrumented system then any such differences shall be identified and there shall be an assessment based on analysis and testing, as appropriate, to show that the likelihood of systematic faults when used in the safety instrumented system is sufficiently low.
8. Unused features of the component shall be identified in the assessment and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.
9. The operating experience considered necessary to justify proven in use shall be defined taking into account the following:
 - the SIL of the safety instrumented function;
 - the complexity and functionality of the device.

7 Terms and Definitions

FMEDA	Failure Mode Effect and Diagnostic Analysis
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.
PFD	Probability of Failure on Demand
PFD_{AVG}	Average Probability of Failure on Demand
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.
SIL	Safety Integrity Level

8 Status of the document

8.1 Liability

exida.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* 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.

8.2 Releases

Version: V1

Revision: R1.4

Version History: V0, R1.0: Initial version, Aug. 2, 2002

V1, R1.0: Updates and corrections after review of V0, R1.0, Sep. 10, 2002

V1, R1.1: Updates and corrections after review of V1, R1.0, Oct. 7, 2002

V1, R1.2: Editorial changes and behavior with different input signal added;
Jul. 8, 2004

V1, R1.3: Updated schematics and FMEDAs added; Aug. 11, 2004

V1, R1.4: Updated schematics and FMEDAs added; Apr. 15, 2005

Authors: Stephan Aschenbrenner

Review: V0, R1.0 by Harald Eschelbach und Werner Bansemir (P+F), Aug. 20, 2002

V1, R1.0 by Harald Eschelbach und Werner Bansemir (P+F), Oct. 1, 2002

Release status: Released to Pepperl+Fuchs

8.3 Release Signatures



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



Dipl.-Ing. (Univ.) Rainer Faller, Principal Partner