



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

Transformer Isolated Barriers  
KF\*\*-ST2-\*\*\* and KF\*\*-SOT2-\*\*\*

Customer:

Pepperl+Fuchs GmbH  
Mannheim  
Germany

Contract No.: P+F 07/06-01

Report No.: P+F 01/09-02D R002

Version V4, Revision R1; September 2011

Stephan Aschenbrenner / Otto Walch

## Management summary

This report summarizes the results of the FMEDAs carried out at the transformer isolated barriers KF\*\*-ST2-\*\*\* and KF\*\*-SOT2-\*\*\*. ‘\*\*\*’ and ‘\*\*\*\*’ stand for the different versions that are available. Table 1 gives an overview and explains the differences.

**Table 1: Version overview**

Type	Supply	Channels	Output / supply	Output 1 / output 2	2 <sup>nd</sup> output
KFD2-ST2-(Ex)1.LB	24 VDC	1	not isolated	not isolated	LB/SC <sup>1</sup>
KFD2-ST2-(Ex)2	24 VDC	2	not isolated	not isolated	channel 2
KFD2-SOT2-(Ex)1.LB	24 VDC	1	isolated	not isolated	LB/SC
KFD2-SOT2-(Ex)2	24 VDC	2	isolated	not isolated	channel 2
KFD2-SOT2-(Ex)1.LB.IO	24 VDC	1	isolated	isolated	LB/SC
KFD2-SOT2-(Ex)2.IO	24 VDC	2	isolated	isolated	channel 2
KFD2-SOT2-(Ex)1.N	24 VDC	1	isolated	n.a.	n.a.
KFD2-SOT2-(Ex)1.R1	24 VDC	1	isolated	n.a.	n.a.
KFA4-SOT2-(Ex)1.LB	100 VAC	1	isolated	not isolated	LB/SC
KFA4-SOT2-(Ex)2	100 VAC	2	isolated	not isolated	channel 2
KFA5-SOT2-(Ex)1.LB	115 VAC	1	isolated	not isolated	LB/SC
KFA5-SOT2-(Ex)2	115 VAC	2	isolated	not isolated	channel 2
KFA6-SOT2-(Ex)1.LB	230 VAC	1	isolated	not isolated	LB/SC
KFA6-SOT2-(Ex)2	230 VAC	2	isolated	not isolated	channel 2

The failure rates used in this analysis are the basic failure rates from 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 boards under evaluation can be considered to be Type A components.

For Type A <sup>2</sup> components the SFF has to be 60% to  $< 90\%$  according to table 2 of IEC 61508-2 for SIL 2 (sub-) systems with a hardware fault tolerance of 0.

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

<sup>1</sup> Collective error message output for LB (Lead Breakage) and SC (Short Circuit) at the input.

<sup>2</sup> 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: Summary of all considered boards<sup>3</sup> – IEC 61508 failure rates**

Name	$\lambda_{\text{Safe}}^4$	$\lambda_{\text{Dangerous}}$	SFF
KFD2-ST2-Ex1	225 FIT	64 FIT	77%
KFD2-SOT2-Ex*	208 FIT	60 FIT	77%
KFA*-SOT2-Ex*	189 FIT	32 FIT	85%
KFD2-SOT2-(Ex)1.N KFD2-SOT2-(Ex)1.R1	186 FIT	21 FIT	89%

**Table 3: Summary of all considered boards – PFD<sub>AVG</sub> values**

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
KFD2-ST2-Ex*	PFD <sub>AVG</sub> = 2.82E-04	PFD <sub>AVG</sub> = 5.64E-04	PFD <sub>AVG</sub> = 1.41E-03
KFD2-SOT2-Ex*	PFD <sub>AVG</sub> = 2.64E-04	PFD <sub>AVG</sub> = 5.27E-04	PFD <sub>AVG</sub> = 1.32E-03
KFA*-SOT2-Ex*	PFD <sub>AVG</sub> = 1.51E-04	PFD <sub>AVG</sub> = 3.03E-04	PFD <sub>AVG</sub> = 7.56E-04
KFD2-SOT2-(Ex)1.N KFD2-SOT2-(Ex)1.R1	PFD <sub>AVG</sub> = 9.21E-05	PFD <sub>AVG</sub> = 1.84E-04	PFD <sub>AVG</sub> = 4.60E-04

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<sub>AVG</sub> values fulfill this requirement to be better than  $10^{-3}$ .

The two channels on each module shall not be used for one safety function as they contain common components.

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.

A user of the transformer isolated barriers KF\*\*-ST2-\*\*\* and KF\*\*-SOT2-\*\*\* 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.

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.

<sup>3</sup> 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 for the “two channel” versions only one channel was considered.

<sup>4</sup> Note that the “Safe” category includes failures that do not cause a spurious trip.



## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	5
2 Project management.....	6
2.1 <i>exida</i> .....	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 <i>exida</i> .....	7
3 Description of the analyzed modules .....	8
3.1 KFD2-ST2-Ex2.....	8
3.2 KFD2-SOT2-Ex2 and KFA*-SOT2-Ex2.....	9
3.3 KFD2-SOT2-Ex1.N and KFD2-SOT2-Ex1.R1.....	10
4 Failure Modes, Effects, and Diagnostics Analysis .....	11
4.1 Description of the failure categories.....	11
4.2 Methodology – FMEDA, Failure rates.....	11
4.2.1 FMEDA.....	11
4.2.2 Failure rates .....	12
4.2.3 Assumptions.....	12
5 Results of the assessment.....	13
5.1 KFD2-ST2-Ex2.....	14
5.2 KFD2-SOT2-Ex2.....	15
5.3 KFA*-SOT2-Ex2.....	16
5.4 KFD2-SOT2-Ex1.N and KFD2-SOT2-Ex1.R1.....	17
6 Terms and Definitions .....	18
7 Status of the document.....	19
7.1 Liability.....	19
7.2 Releases .....	19
7.3 Release Signatures.....	19

## 1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

### Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ( $PFD_{AVG}$ ). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

### Option 2: Hardware assessment with proven-in-use consideration per IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

### Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends Option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

### **This assessment shall be done according to option 1.**

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the transformer isolated barriers KF\*\*-ST2-\*\*\* and KF\*\*-SOT2-\*\*\*. Table 1 gives an overview of the different types which have been assessed.

The information in this report can be used to evaluate whether the transformer isolated barriers KF\*\*-ST2-\*\*\* and KF\*\*-SOT2-\*\*\* meet the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.



## 2 Project management

### 2.1 exida

*exida* is one of the world's leading product certification 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 consulting services, internet based safety engineering tools, detailed product assurance and certification analysis 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    Manufacturer of the transformer isolated barriers.

*exida*                Performed the hardware assessment according to option 1 (see section 1).

Pepperl+Fuchs GmbH contracted *exida* in September 2006 and June 2007 with the FMEDA and PFD<sub>AVG</sub> calculation of the above mentioned boards.

### 2.3 Standards / Literature used

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

N1	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
N3	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
N4	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
N5	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
N6	SN 29500	Failure rates of components
N7	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

## 2.4 Reference documents

### 2.4.1 Documentation provided by the customer

[D1]	51-0377, Index A of 26.07.01	Circuit diagram for KFA*-SOT2-EX2
[D1.1]	043934	Bill of material for KFA5-SOT2-EX2
[D2]	01-6863A of 13.10.04	Circuit diagram for KFD2-SOT2-EX2
[D2.1]	181005 / 802609	Bill of material for KFD2-SOT2-EX2
[D3]	01-6866A of 13.10.04	Circuit diagram for KFD2-ST2-EX2
[D3.1]	181000 / 802610	Bill of material for KFD2-ST2-EX2
[D4]	01-7674 of 03.11.06 (017674.pdf)	Circuit diagram for KFD2-SOT2-EX1.N
[D4.1]	196319_N_BOM.pdf	Bill of material for KFD2-SOT2-EX1.N
[D5]	DDE0979.pdf	Design order for hardware change on KFA*-SOT2-Ex2
[D6]	30-063901-7674 of 03.05.07 (300639.pdf)	Impact analysis on the SIL 2 assessment
[D7]	FS0070EA-25.pdf	Impact analysis for new variant KFD2-SOT2-(Ex)1.R1
[D8]	FS0070EA-25_2.pdf	Circuit diagram "01-9067 of 16.05.11" for KFD2-SOT2-(Ex)1.R1
[D8.1]	238139_R1_BOM.pdf	Bill of material for KFD2-SOT2-(Ex)1.R1

### 2.4.2 Documentation generated by exida

R1	FMEDA KFA-SOT2-EX2 V1 R1.0
R2	FMEDA KFD2-SOT2-EX2 V1 R1.1
R3	FMEDA KFD2-ST2-EX2 V1 R1.1
R4	FMEDA V6.5.4 KFD2-SOT2-EX1.N V1 R1.0.xls of 05.12.06
R5	FMEDA V6.5.4 KFA..-SOT2-EX2 V1 R1.2.xls of 05.07.07

### 3 Description of the analyzed modules

#### 3.1 KFD2-ST2-Ex2

The transformer isolated barrier KFD2-ST2-Ex2 transfers digital signals from the hazardous area.

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

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. 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. Both transistor outputs are galvanically connected to each other and the power supply.

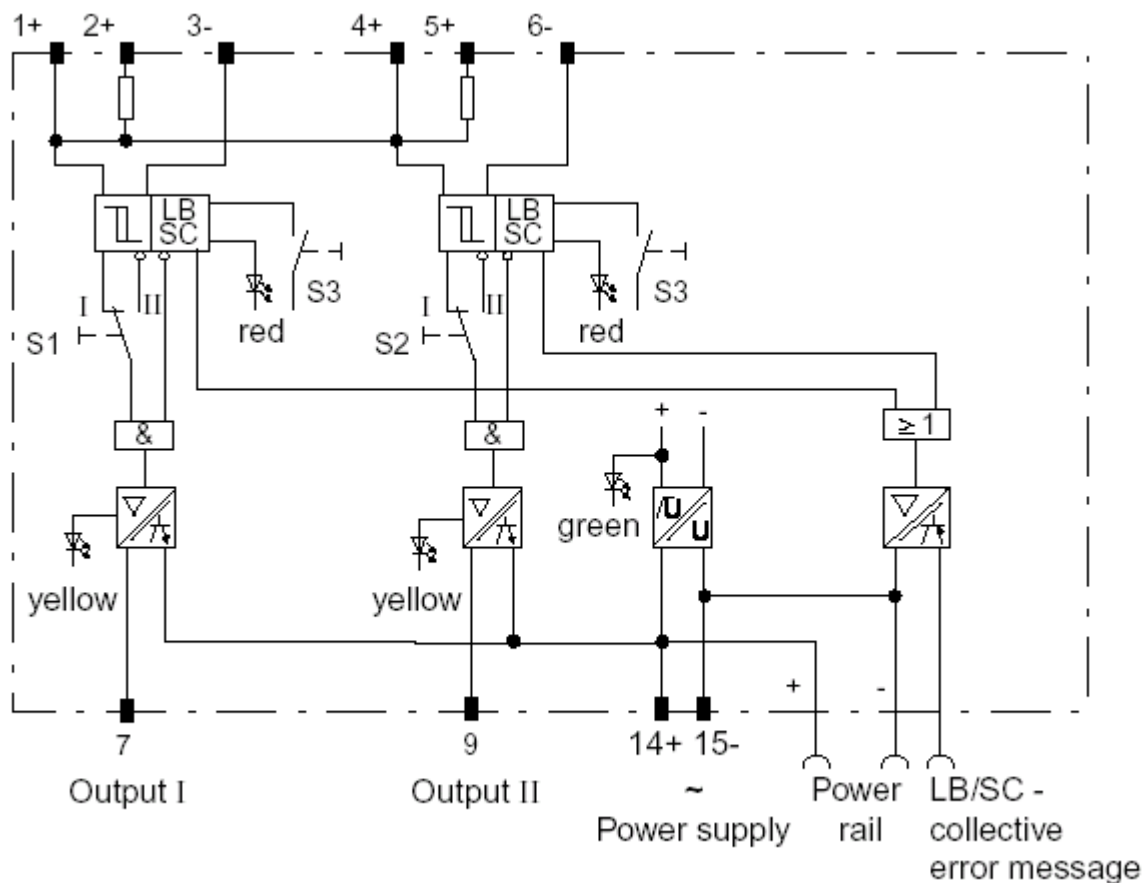


Figure 1: Block diagram of KFD2-ST2-Ex2

**Remark:** The description above is valid accordingly for all other KF\*\*-ST2-\*\*\* versions with the exception that this version has two output channels. The differences between the versions are described in Table 1.



### 3.2 KFD2-SOT2-Ex2 and KFA\*-SOT2-Ex2

The transformer isolated barriers KFD2-SOT2-Ex2 and KFA\*-SOT2-Ex2 transfer digital signals from the hazardous area.

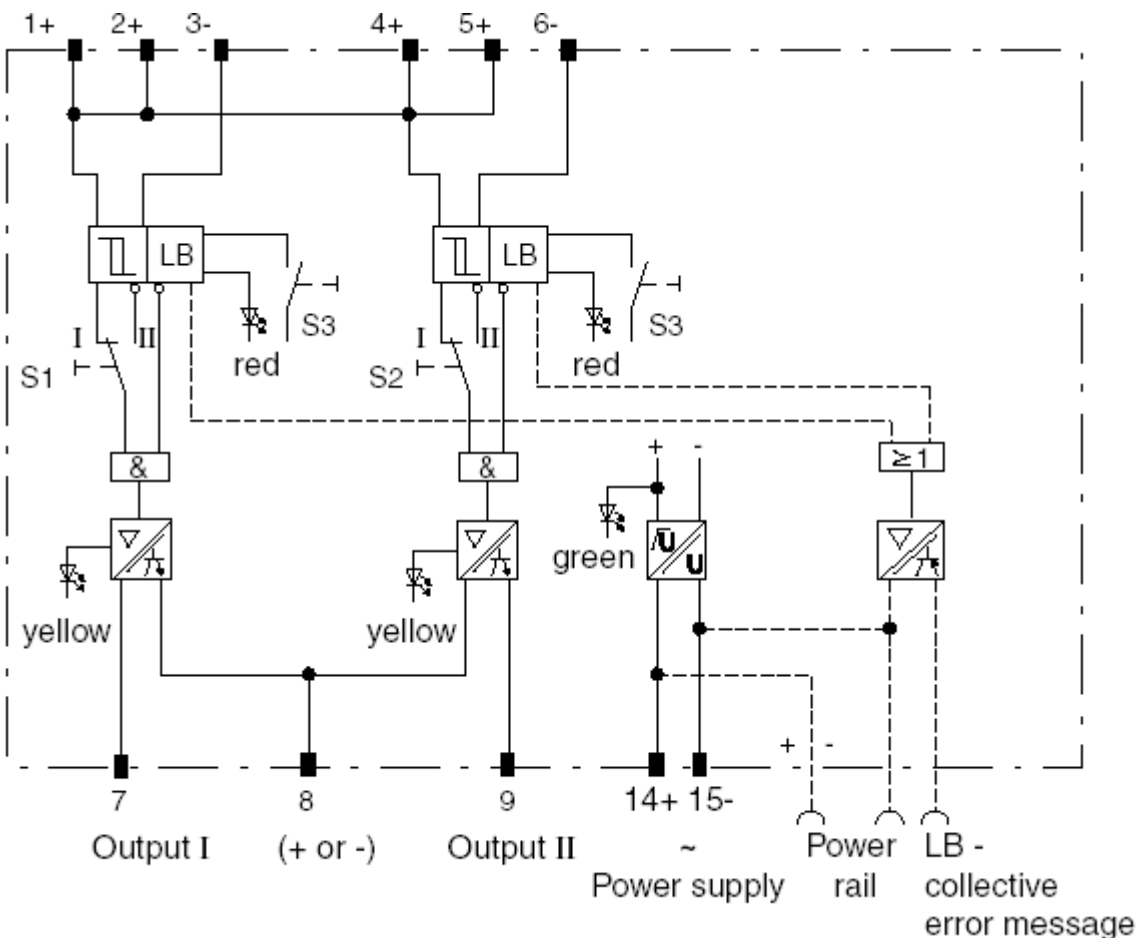
Sensors per DIN EN 60947-5-6 (NAMUR) or mechanical contacts may be used as alarms.

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-SOT2-Ex2 type additionally a LB/SC-combined error signal is transferred via Power Rail to the power feed module.

The intrinsically safe inputs per DIN EN 60079-11 are safely isolated from the output and the power supply. Both transistor outputs are galvanically connected to each other and the power supply in accordance with DIN EN 50178.

The mode of operation for output I (S1) and output II (S2) is reversible.

The hardware change of May 2007 on KFA\*-SOT2-EX2 is considered in this report.



**Figure 2: Block diagram of KFD2-SOT2-Ex2**

**Remark:** The description above is valid accordingly for all other KF\*\*-SOT2-\*\*\* versions with the exception that this version has two output channels. The differences between the versions are described in Table 1.

### 3.3 KFD2-SOT2-Ex1.N and KFD2-SOT2-Ex1.R1

The transformer isolated barriers KFD2-SOT2-Ex1.N and KFD2-SOT2-Ex1.R1 transfer digital signals from the hazardous area.

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

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.

The intrinsically safe inputs per DIN EN 50020 are safely isolated from the output and the power supply. Both transistor outputs are galvanically connected to each other and the power supply in accordance with DIN EN 50178.

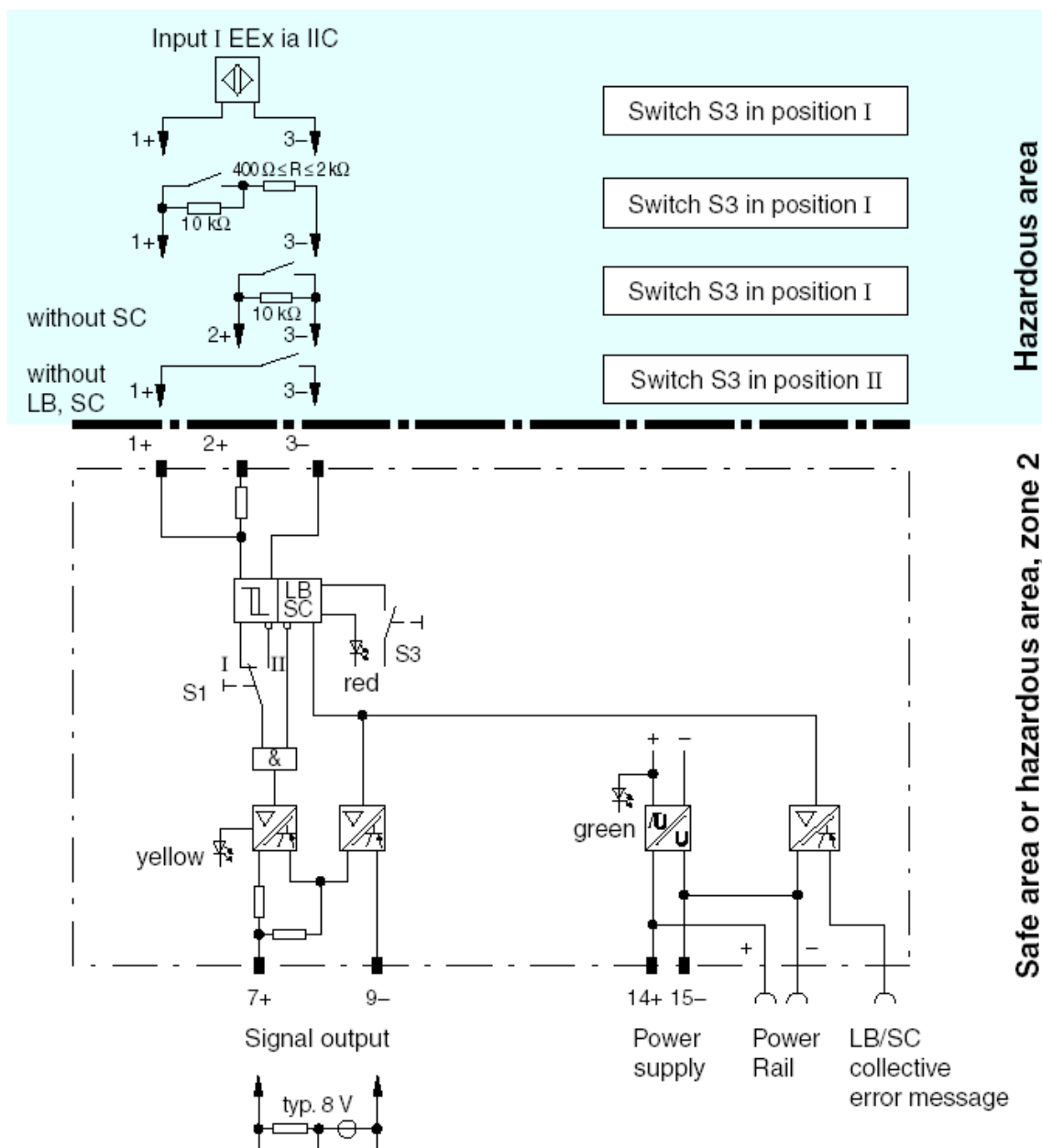


Figure 3: Block diagram of KFD2-SOT2-Ex1.N

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs GmbH and is documented in R1 to R5. Failures were classified according to the following failure categories.

### 4.1 Description of the failure categories

Fail-Safe State	The fail-safe state is defined as the output being de-energized. This corresponds to an input signal of about 1mA (inductive sensor stops oscillating because metal material gets closer) and S1 open which is considered to be the normal mode of operation.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail No Effect	Failure of a component that is part of the safety function but has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.
“Not considered”	Failure mode which was not considered. When calculating the SFF and the $PFD_{AVG}$ this failure mode is divided into 50% safe failures and 50% dangerous failures.
Not part	Failure of a component which 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.

The “No Effect” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508, Edition 2000, the “No Effect” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

### 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 under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostic 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 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 IEC 60654-1, class C. 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 Assumptions

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.
- 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.
- The time to restoration after a safe failure is 8 hours.
- External power supply failure rates are not included.
- 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.
- Only the described versions are used for safety applications.
- The two channels on each module are not used for one safety function as they contain common components.
- All modules are operated in the low demand mode of operation.

## 5 Results of the assessment

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

The two channels on each module shall not be used for one safety function as they contain common components.

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

$\lambda_{total}$  consists of the sum of all component failure rates. This means:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect}^5 + \lambda_{not\ considered}^6$$

$$SFF = 1 - \lambda_{Dangerous}^7 / \lambda_{total}$$

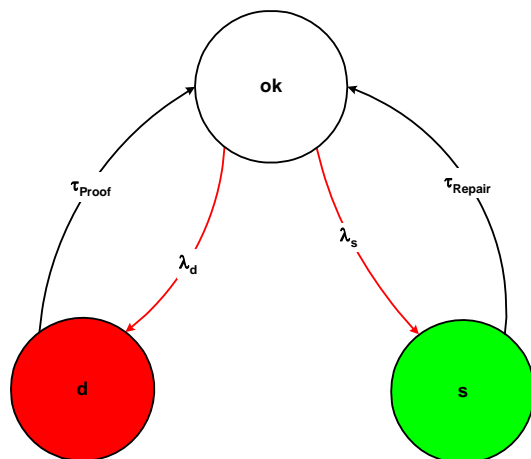
The reason for considering also the “not considered” failure rate for the calculation of the SFF is that the SFF is a measure for the effectiveness of the implemented diagnostic and the percentage of known “safe” failures against all possible component failures.

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

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.

Also the formula described in IEC 61508-6 ( $PFD_{AVG} = \lambda_{dangerous} (1/2 T_{[Proof]} + T_{[Repair]})$ ) can be used to calculate the results.

The proof time was changed using the FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.



Abbreviations:

d	One channel has failed dangerous
s	One channel has failed safe
$\lambda_d$	Failure rate of dangerous failures
$\lambda_s$	Failure rate of safe failures
$T_{Proof}$	Proof time
$\tau_{Proof}$	Proof rate (= $2/T_{Proof}$ )
$T_{Repair}$	Repair time
$\tau_{Repair}$	Repair rate (= $1/T_{Repair}$ )

Figure 4: Markov model

<sup>5</sup> These are all failures that have no impact on the safety function. The behavior of the system is neither dangerous nor safe.

<sup>6</sup> This is the failure rate of failure modes that were not considered.

<sup>7</sup> This is the failure rate of all dangerous undetected failures plus 50% of the “non considered” failures.

## 5.1 KFD2-ST2-Ex2

The FMEDA carried out on the KFD2-ST2-Ex2 board, which is considered to be representative for all KFD2-ST2-Ex\* boards, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{\text{total}} = 2,90\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 9,99\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,33\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{no effect}} = 8,44\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 8,21\text{E-}08 \text{ 1/h}$$

$$\text{SFF} = 77,79\%$$

The PFD was calculated for three different proof test intervals using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD <sub>AVG</sub> = 2.82E-04	PFD <sub>AVG</sub> = 5.64E-04	PFD <sub>AVG</sub> = 1.41E-03

The boxes marked in yellow (  ) mean that the calculated PFD<sub>AVG</sub> 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  $10^{-3}$ . Figure 5 shows the time dependent curve of PFD<sub>AVG</sub>.

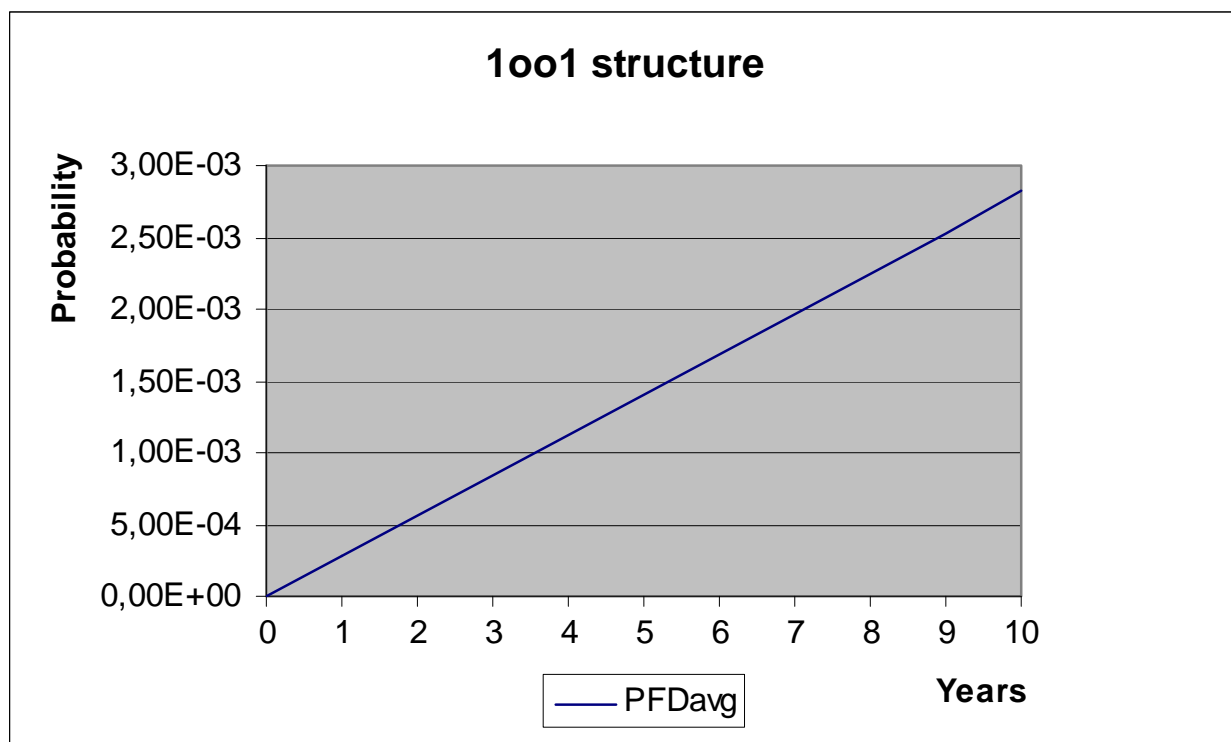


Figure 5: PFD<sub>AVG</sub>(t)

## 5.2 KFD2-SOT2-Ex2

The FMEDA carried out on the KFD2-SOT2-Ex2 board, which is considered to be representative for all KFD2-SOT2-Ex\* boards, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{\text{total}} = 2,68\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 1,00\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,42\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{no effect}} = 7,17\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{not considered}} = 7,18\text{E-}08 \text{ 1/h}$$

$$\text{SFF} = 77,53\%$$

The PFD was calculated for three different proof test intervals using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD <sub>AVG</sub> = 2.64E-04	PFD <sub>AVG</sub> = 5.27E-04	PFD <sub>AVG</sub> = 1.32E-03

The boxes marked in yellow (  ) mean that the calculated PFD<sub>AVG</sub> 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  $10^{-3}$ . Figure 6 shows the time dependent curve of PFD<sub>AVG</sub>.

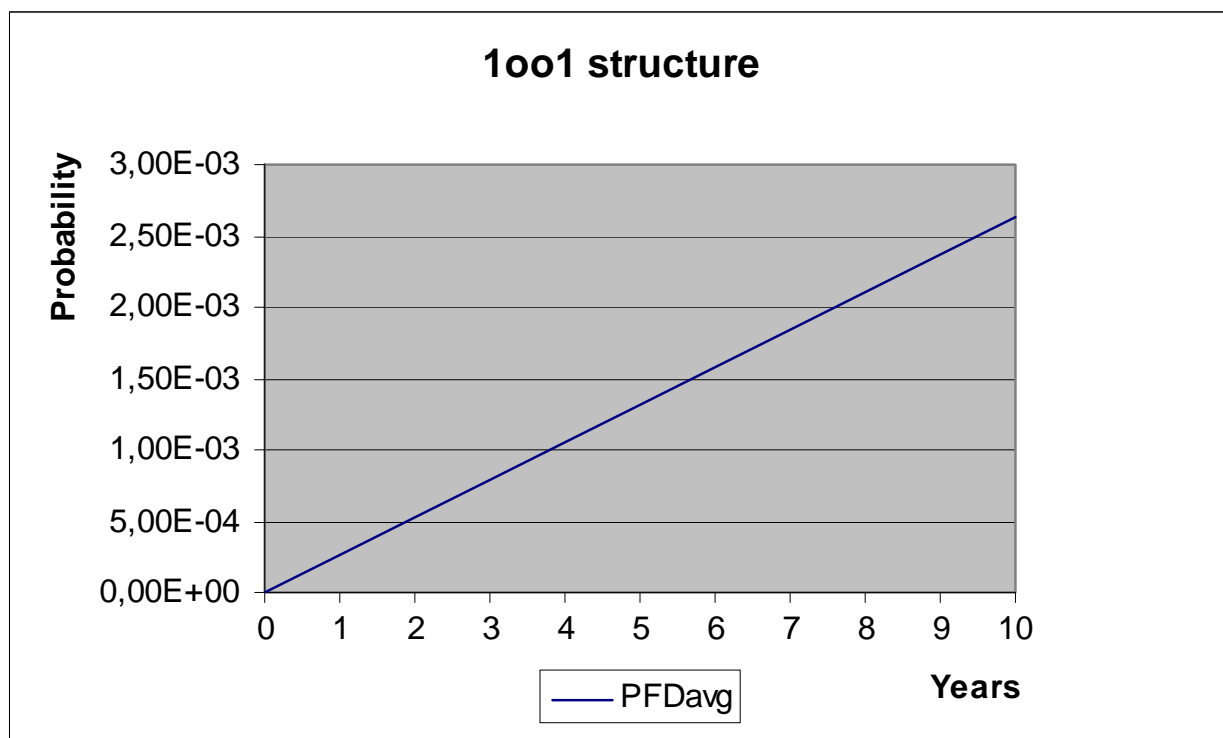


Figure 6: PFD<sub>AVG</sub>(t)

### 5.3 KFA\*-SOT2-Ex2

The FMEDA carried out on the KFA\*-SOT2-Ex2 board with the hardware changes implemented in May 2007, which is considered to be representative for all KFA\*-SOT2-Ex\* boards, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{\text{total}} = 2,20\text{E-}07 \text{ 1/h}$$

$$\lambda_{\text{safe}} = 7,65\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 3,16\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{no effect}} = 1,12\text{E-}07 \text{ 1/h}$$

$$\text{SFF} = 85,66\%$$

The PFD was calculated for three different proof test intervals using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD <sub>AVG</sub> = 1.51E-04	PFD <sub>AVG</sub> = 3.03E-04	PFD <sub>AVG</sub> = 7.56E-04

The boxes marked in yellow (  ) mean that the calculated PFD<sub>AVG</sub> values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 10<sup>-3</sup>. Figure 7 shows the time dependent curve of PFD<sub>AVG</sub>.

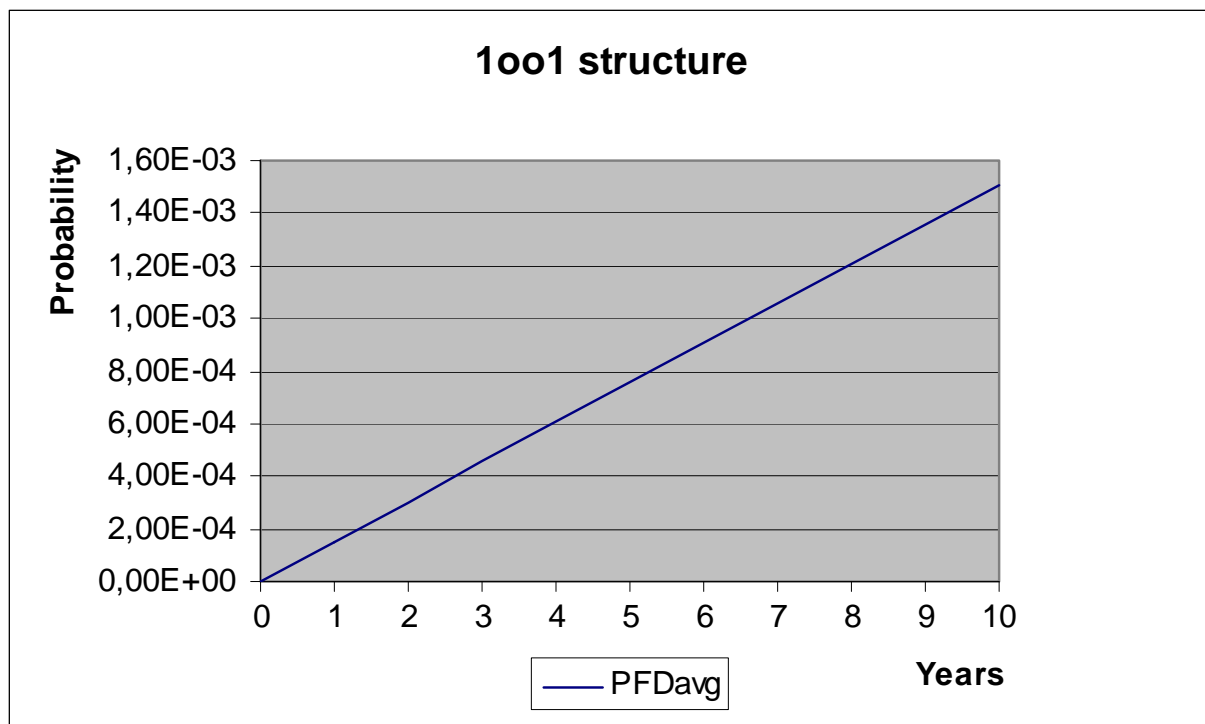


Figure 7: PFD<sub>AVG</sub>(t)



#### 5.4 KFD2-SOT2-Ex1.N and KFD2-SOT2-Ex1.R1

The FMEDA carried out on the KFD2-SOT2-Ex1.N board with the hardware changes implemented in May 2011, which is considered to be representative for both boards, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates and SFF:

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

$$\lambda_{\text{safe}} = 7,83\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{dangerous}} = 2,10\text{E-}08 \text{ 1/h}$$

$$\lambda_{\text{no effect}} = 1,08\text{E-}07 \text{ 1/h}$$

$$\text{SFF} = 89,86\%$$

The PFD was calculated for three different proof test intervals using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD <sub>AVG</sub> = 9.21E-05	PFD <sub>AVG</sub> = 1.84E-04	PFD <sub>AVG</sub> = 4.60E-04

The boxes marked in green (  ) mean that the calculated PFD<sub>AVG</sub> values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $10^{-3}$ . Figure 8 shows the time dependent curve of PFD<sub>AVG</sub>.

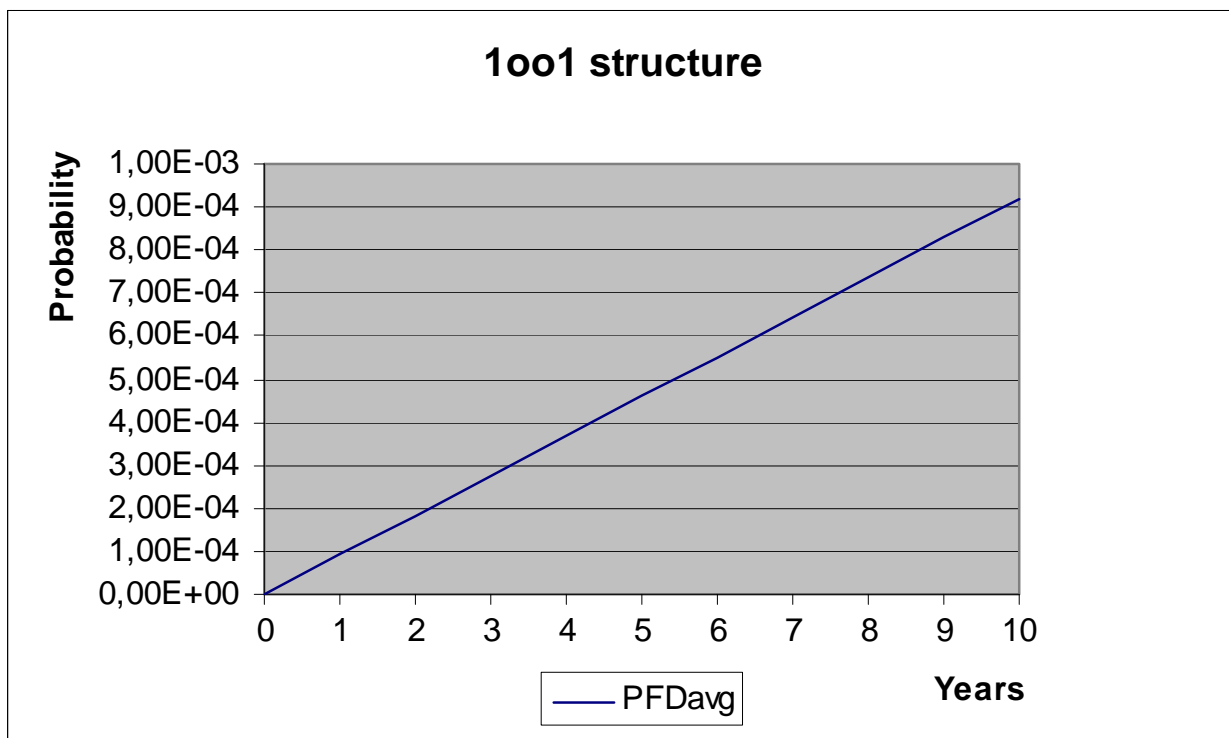


Figure 8: PFD<sub>AVG</sub>(t)

## 6 Terms and Definitions

FMEDA	Failure Mode Effect 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.
$PFD_{AVG}$	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.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
T[Proof]	Proof Test Interval
Type A component	"Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2

## 7 Status of the document

### 7.1 Liability

*exida* prepares FMEDA 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

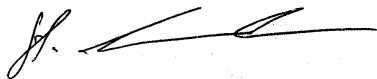
Version History: V4R1: Editorial changes; September 27, 2011  
V4R0: Variant KFD2-SOT2-(Ex)1.R1 added; September 23, 2011  
V3, R1: Editorial changes; July 16, 2007  
V3, R0: Incorporation of hardware changes, see D5 and D6; July 5, 2007  
V2, R2: Review comments incorporated; December 20, 2006  
V2, R1: Table 1 modified; December 8, 2006  
V2, R0: NAMUR and IO versions added; December 6, 2006  
V1, R1.0: Updated schematics and FMEDAs added; April 15, 2005  
V0, R1.0: Initial version, October 25, 2001

Authors: Stephan Aschenbrenner / Otto Walch

Review: V4R0: Michael Kindermann (P+F); September 26, 2011  
V3, R0: Michael Trautmann (P+F); July 16, 2007  
V2, R1: Rudolf Chalupa (*exida*); December 16, 2006  
V2, R0: Harald Eschelbach (P+F); December 7, 2006

Release status: Released to Pepperl+Fuchs GmbH

### 7.3 Release Signatures

A handwritten signature in black ink, appearing to be "S. Aschenbrenner".

---

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

A handwritten signature in black ink, appearing to be "R. Faller".

---

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