



## **FMEDA and Proven-in-use Assessment**

Project:

Transformer Isolated Amplifiers EG\*-\*\*

Customer:

**Pepperl+Fuchs GmbH**  
Mannheim  
Germany

Contract No.: P+F 03/3-25

Report No.: P+F 03/3-25 R010

Version V2, Revision R1.0, March 2006

Stephan Aschenbrenner

## Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Transformer Isolated Amplifiers EG\*<sup>\*\*</sup>. '\*' and '\*\*' stand for the different versions that are available.

Table 1 gives an overview and explains the differences.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

**Table 1: Version overview**

Type	Relay output	10mA output	Transistor output	Isolated output	Loop monitoring output
EG2(4)-R	2x change over contact	X			
EG2(4)-RLK	2x change over contact	X			10mA
EG2(4)-T		2x 10mA	200mA		
EG2(4)-TLK		2x 10mA	200mA		10mA
EG4-OT		X		100mA	
EG4-OTLK		X		100mA	10mA

This report is also applicable to further options (with Y-letter at the end). Depending on the number behind the Y, various options are keyed (like presets for mode or loop monitoring, while jumpers are replaced by wire links). The changes done in the Y-units are not relevant to functional safety.

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. For a SIL 2 application the total PFD<sub>AVG</sub> value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD<sub>AVG</sub> value for the transformer isolated amplifiers would then be 1,00E-03.

The Transformer Isolated Amplifiers EG\*<sup>\*\*</sup> are considered to be Type A<sup>1</sup> components having a hardware fault tolerance of 0.

For Type A components with a SFF of 60% to < 90% a hardware fault tolerance of 0 according to table 2 of IEC 61508-2 is sufficient for SIL 2 (sub-) systems.

As the Transformer Isolated Amplifiers EG\*<sup>\*\*</sup> are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the devices was carried out. According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.10.2 the devices are suitable to be used for SIL 2 safety functions.

---

Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

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.

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 boards (normal mode) – PFD<sub>AVG</sub> values**

Name	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
EG2-R	PFD <sub>AVG</sub> = 8,29E-05	PFD <sub>AVG</sub> = 4,14E-04	PFD <sub>AVG</sub> = 8,28E-04
EG2-RLK	PFD <sub>AVG</sub> = 9,37E-05	PFD <sub>AVG</sub> = 4,69E-04	PFD <sub>AVG</sub> = 9,37E-04
EG2-T	PFD <sub>AVG</sub> = 9,29E-05	PFD <sub>AVG</sub> = 4,65E-04	PFD <sub>AVG</sub> = 9,29E-04
EG2-TLK	PFD <sub>AVG</sub> = 9,59E-05	PFD <sub>AVG</sub> = 4,79E-04	PFD <sub>AVG</sub> = 9,59E-04
EG4-R	PFD <sub>AVG</sub> = 9,43E-05	PFD <sub>AVG</sub> = 4,71E-04	PFD <sub>AVG</sub> = 9,42E-04
EG4-RLK	PFD <sub>AVG</sub> = 9,96E-05	PFD <sub>AVG</sub> = 4,98E-04	PFD <sub>AVG</sub> = 9,95E-04
EG4-T	PFD <sub>AVG</sub> = 9,64E-05	PFD <sub>AVG</sub> = 4,82E-04	PFD <sub>AVG</sub> = 9,64E-04
EG4-TLK	PFD <sub>AVG</sub> = 1,06E-04	PFD <sub>AVG</sub> = 5,32E-04	PFD <sub>AVG</sub> = 1,06E-03
EG4-OT	PFD <sub>AVG</sub> = 1,23E-04	PFD <sub>AVG</sub> = 6,17E-04	PFD <sub>AVG</sub> = 1,23E-03
EG4-OTLK	PFD <sub>AVG</sub> = 1,29E-04	PFD <sub>AVG</sub> = 6,43E-04	PFD <sub>AVG</sub> = 1,29E-03

**Table 3: Summary of all considered boards (normal mode) – Failure rates**

Name	$\lambda_{sd}$	$\lambda_{su}$	$\lambda_{dd}$	$\lambda_{du}$	SFF
EG2-R	0,00E-00 1/h	9,23E-08 1/h	1,44E-08 1/h	1,89E-08 1/h	84 %
EG2-RLK	0,00E-00 1/h	9,74E-08 1/h	1,44E-08 1/h	2,14E-08 1/h	83 %
EG2-T	0,00E-00 1/h	1,15E-07 1/h	1,44E-08 1/h	2,12E-08 1/h	85 %
EG2-TLK	0,00E-00 1/h	1,21E-07 1/h	1,44E-08 1/h	2,19E-08 1/h	86 %
EG4-R	0,00E-00 1/h	9,65E-08 1/h	1,44E-08 1/h	2,15E-08 1/h	83 %
EG4-RLK	0,00E-00 1/h	9,75E-08 1/h	1,44E-08 1/h	2,27E-08 1/h	83 %
EG4-T	0,00E-00 1/h	1,08E-07 1/h	1,44E-08 1/h	2,20E-08 1/h	84 %
EG4-TLK	0,00E-00 1/h	1,24E-07 1/h	1,44E-08 1/h	2,43E-08 1/h	85 %
EG4-OT	0,00E-00 1/h	1,23E-07 1/h	1,44E-08 1/h	2,82E-08 1/h	83 %
EG4-OTLK	0,00E-00 1/h	1,23E-07 1/h	1,44E-08 1/h	2,94E-08 1/h	82 %

**Table 4: Summary of all considered boards (inverse mode) – PFD<sub>AVG</sub> values**

Name	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
EG2-R	PFD <sub>AVG</sub> = 1,31E-04	PFD <sub>AVG</sub> = 6,53E-04	PFD <sub>AVG</sub> = 1,31E-03
EG2-RLK	PFD <sub>AVG</sub> = 1,42E-04	PFD <sub>AVG</sub> = 7,07E-04	PFD <sub>AVG</sub> = 1,41E-03
EG2-T	PFD <sub>AVG</sub> = 1,41E-04	PFD <sub>AVG</sub> = 7,03E-04	PFD <sub>AVG</sub> = 1,41E-03
EG2-TLK	PFD <sub>AVG</sub> = 1,44E-04	PFD <sub>AVG</sub> = 7,18E-04	PFD <sub>AVG</sub> = 1,44E-03
EG4-R	PFD <sub>AVG</sub> = 1,42E-04	PFD <sub>AVG</sub> = 7,10E-04	PFD <sub>AVG</sub> = 1,42E-03
EG4-RLK	PFD <sub>AVG</sub> = 1,52E-04	PFD <sub>AVG</sub> = 7,60E-04	PFD <sub>AVG</sub> = 1,52E-03
EG4-T	PFD <sub>AVG</sub> = 1,44E-04	PFD <sub>AVG</sub> = 7,21E-04	PFD <sub>AVG</sub> = 1,44E-03
EG4-TLK	PFD <sub>AVG</sub> = 1,54E-04	PFD <sub>AVG</sub> = 7,71E-04	PFD <sub>AVG</sub> = 1,54E-03
EG4-OT	PFD <sub>AVG</sub> = 1,71E-04	PFD <sub>AVG</sub> = 8,55E-04	PFD <sub>AVG</sub> = 1,71E-03
EG4-OTLK	PFD <sub>AVG</sub> = 1,81E-04	PFD <sub>AVG</sub> = 9,05E-04	PFD <sub>AVG</sub> = 1,81E-03

**Table 5: Summary of all considered boards (inverse mode) – Failure rates**

Name	$\lambda_{sd}$	$\lambda_{su}$	$\lambda_{dd}$	$\lambda_{du}$	SFF
EG2-R	1,43E-08 1/h	7,84E-08 1/h	0,00E-00 1/h	2,98E-08 1/h	75 %
EG2-RLK	1,43E-08 1/h	8,37E-08 1/h	0,00E-00 1/h	3,23E-08 1/h	75 %
EG2-T	1,43E-08 1/h	1,01E-07 1/h	0,00E-00 1/h	3,21E-08 1/h	78 %
EG2-TLK	1,43E-08 1/h	1,03E-07 1/h	0,00E-00 1/h	3,28E-08 1/h	78 %
EG4-R	1,43E-08 1/h	8,27E-08 1/h	0,00E-00 1/h	3,24E-08 1/h	74 %
EG4-RLK	1,43E-08 1/h	8,43E-08 1/h	0,00E-00 1/h	3,47E-08 1/h	73 %
EG4-T	1,43E-08 1/h	9,40E-08 1/h	0,00E-00 1/h	3,29E-08 1/h	76 %
EG4-TLK	1,43E-08 1/h	1,06E-07 1/h	0,00E-00 1/h	3,52E-08 1/h	77 %
EG4-OT	1,43E-08 1/h	1,09E-07 1/h	0,00E-00 1/h	3,91E-08 1/h	75 %
EG4-OTLK	1,43E-08 1/h	1,11E-07 1/h	0,00E-00 1/h	4,14E-08 1/h	75 %

A user of the Transformer Isolated Amplifiers EG<sup>\*-\*\*</sup> 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). The complete list of failure rates is presented in section 5.1 to 5.10 along with all assumptions.

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 1,00E-03. 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 do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03.

The two or four channels on each module shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two or four channels may be used in separate safety functions if due regard is taken of the possibility of common failures.



## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	7
2 Project management .....	8
2.1 <i>exida</i> .....	8
2.2 Roles of the parties involved .....	8
2.3 Standards / Literature used .....	8
2.4 Reference documents .....	8
2.4.1 Documentation provided by the customer .....	8
2.4.2 Documentation generated by <i>exida</i> .....	9
3 Description of the analyzed modules .....	10
3.1 EG2(4)-R .....	10
3.2 EG2(4)-RLK .....	12
3.3 EG2(4)-T .....	14
3.4 EG2(4)-TLK .....	16
3.5 EG4-OT .....	18
3.6 EG4-OTLK .....	19
4 Failure Modes, Effects, and Diagnostics Analysis .....	20
4.1 Description of the failure categories .....	20
4.2 Methodology – FMEDA, Failure rates .....	21
4.2.1 FMEDA .....	21
4.2.2 Failure rates .....	21
4.2.3 Assumptions .....	21
5 Results of the assessment .....	22
5.1 EG2-R .....	23
5.1.1 Normal mode .....	23
5.1.2 Inverse mode .....	24
5.2 EG2-RLK .....	25
5.2.1 Normal mode .....	25
5.2.2 Inverse mode .....	26
5.3 EG2-T .....	27
5.3.1 Normal mode .....	27
5.3.2 Inverse mode .....	28
5.4 EG2-TLK .....	29
5.4.1 Normal mode .....	29
5.4.2 Inverse mode .....	30
5.5 EG4-R .....	31
5.5.1 Normal mode .....	31
5.5.2 Inverse mode .....	32
5.6 EG4-RLK .....	33
5.6.1 Normal mode .....	33
5.6.2 Inverse mode .....	34



5.7	EG4-T .....	35
5.7.1	Normal mode.....	35
5.7.2	Inverse mode .....	36
5.8	EG4-TLK.....	37
5.8.1	Normal mode.....	37
5.8.2	Inverse mode .....	38
5.9	EG4-OT .....	39
5.9.1	Normal mode.....	39
5.9.2	Inverse mode .....	40
5.10	EG4-OTLK .....	41
5.10.1	Normal mode.....	41
5.10.2	Inverse mode .....	42
6	Proven-in-use Assessment .....	43
6.1	Definition of the term “Proven-in-use” according to IEC 61508 .....	43
6.2	“Prior-use” requirements according to IEC 61511-1 .....	43
7	Terms and Definitions .....	46
8	Status of the document .....	47
8.1	Liability .....	47
8.2	Releases .....	47
8.3	Release Signatures .....	47
Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01 .....		48
Appendix 1.1	Section 11.5.3 of IEC 61511-1 First Edition 2003-01 .....	48
Appendix 1.2	Section 11.5.4 of IEC 61511-1 First Edition 2003-01 .....	48
Appendix 1.3	Section 11.5.2 of IEC 61511-1 First Edition 2003-01 .....	48
Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test ..		50
Appendix 3: Impact of lifetime of critical components on the failure rate .....		51

## 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 DIN V VDE 0801, IEC 61508 or EN 954-1. 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 ( $PFD_{AVG}$ ).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the software development process

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

Option 2 is an assessment by *exida* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. 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 ( $PFD_{AVG}$ ). In addition this option consists of an assessment of the proven-in-use documentation of the device and its software including the modification process.

This option 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 fault tolerance requirements of 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 DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

### **This assessment shall be done according to option 2.**

This document shall describe the results of the assessment carried out on the Transformer Isolated Amplifiers EG\*-\*\*.

It shall be assessed whether the transformer isolated amplifiers meet the average Probability of Failure on Demand ( $PFD_{AVG}$ ) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

Pepperl+Fuchs GmbH contracted *exida* in April 2003 with the FMEDA and  $PFD_{AVG}$  calculation of the above mentioned devices.

## 2 Project management

### 2.1 *exida*

*exida* is one of the world's leading knowledge companies specializing in automation system safety and availability with over 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida* is a partnership with offices around the world. *exida* 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* 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 Amplifiers EG*-**.
<i>exida</i>	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

### 2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	IEC 61511-1 First Edition 2003-01	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]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N6]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N7]	SN 29500	Failure rates of components

### 2.4 Reference documents

#### 2.4.1 Documentation provided by the customer

[D1]	1-1667 Ind. B	Circuit diagram for EG2-R
[D2]	1-2208 Ind. B	Circuit diagram for EG2-RLK
[D3]	1-1684 Ind. E	Circuit diagram for EG2-T..
[D4]	1-2209 Ind. C	Circuit diagram for EG2-TLK
[D5]	1-1692 Ind. D	Circuit diagram for EG4-R
[D6]	1-2206 Ind. B	Circuit diagram for EG4-RLK
[D7]	1-1696 Ind. D	Circuit diagram for EG4-T..
[D8]	1-2207 Ind. C	Circuit diagram for EG4-TLK



[D9]	1-2539 Ind. A	Circuit diagram for EG4-OT
[D10]	1-3171 Ind. 0	Circuit diagram for EG4-OTLK
[D11]	1-2875 Ind. 0	Circuit diagram "Output Driver"
[D12]	1-2502 Ind. C	Circuit diagram "Trennstufe OT-SDS"
[D13]	1-3916 Ind. C	Circuit diagram "KM/EX und KM/EX-BI"
[D14]	EG_ED.xls of 07.05.03	Field data evaluation (operating hours, sold devices, returned devices)
[D15]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D16]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D17]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D18]	Email of 19.05.03	Examples of applications
[D19]	Email of 20.05.03	Description of changes during the lifetime
[D20]	Email of 23.06.03	Additional field data evaluation (sold devices)

## 2.4.2 Documentation generated by exida

[R1]	FMEDA V4 R0.7 EG2-R relay output V1 R1.0.xls of 18.03.03
[R2]	FMEDA V4 R0.7 EG2-RLK relay output V1 R1.0.xls of 18.03.03
[R3]	FMEDA V4 R0.7 EG2-T 200mA output V1 R1.0.xls of 18.03.03
[R4]	FMEDA V4 R0.7 EG2-RLK current output V1 R1.0.xls of 24.03.03
[R5]	FMEDA V4 R0.7 EG2-TLK 200mA output V1 R1.0.xls of 28.03.03
[R6]	FMEDA V4 R0.7 EG4-OT 100mA output V1 R1.0.xls of 18.03.03
[R7]	FMEDA V4 R0.7 EG4-OTLK 100mA output V1 R1.0.xls of 14.04.03
[R8]	FMEDA V4 R0.7 EG4-R current output V1 R1.0.xls of 18.03.03
[R9]	FMEDA V4 R0.7 EG4-R relay output V1 R1.0.xls of 18.03.03
[R10]	FMEDA V4 R0.7 EG4-RLK relay output V1 R1.0.xls of 20.04.03
[R11]	FMEDA V4 R0.7 EG4-T 200mA output V1 R1.0.xls of 18.03.03
[R12]	FMEDA V4 R0.7 EG4-TLK 200mA output V1 R1.0.xls of 28.03.03
[R13]	FMEDA V4 R0.7 EG2-R relay output inverse V1 R1.0.xls of 27.03.06
[R14]	FMEDA V4 R0.7 EG2-RLK current output inverse V1 R1.0.xls of 27.03.06
[R15]	FMEDA V4 R0.7 EG2-RLK relay output inverse V1 R1.0.xls of 27.03.06
[R16]	FMEDA V4 R0.7 EG2-T 200mA output inverse V1 R1.0.xls of 27.03.06
[R17]	FMEDA V4 R0.7 EG2-TLK 200mA output inverse V1 R1.0.xls of 27.03.06
[R18]	FMEDA V4 R0.7 EG4-OT 100mA output inverse V1 R1.0.xls of 27.03.06
[R19]	FMEDA V4 R0.7 EG4-OTLK 100mA output inverse V1 R1.0.xls of 27.03.06
[R20]	FMEDA V4 R0.7 EG4-R current output inverse V1 R1.0.xls of 27.03.06
[R21]	FMEDA V4 R0.7 EG4-R relay output inverse V1 R1.0.xls of 27.03.06
[R22]	FMEDA V4 R0.7 EG4-RLK relay output inverse V1 R1.0.xls of 27.03.06
[R23]	FMEDA V4 R0.7 EG4-T 200mA output inverse V1 R1.0.xls of 27.03.06
[R24]	FMEDA V4 R0.7 EG4-TLK 200mA output inverse V1 R1.0.xls of 27.03.06

### 3 Description of the analyzed modules

#### 3.1 EG2(4)-R

The transformer isolated amplifier EG2(4)-R transmits digital signals from the hazardous area. Sensors per DIN EN 60947-5-6 (NAMUR) and mechanical contacts may be used. The control circuit can be monitored for lead breakage (LB).

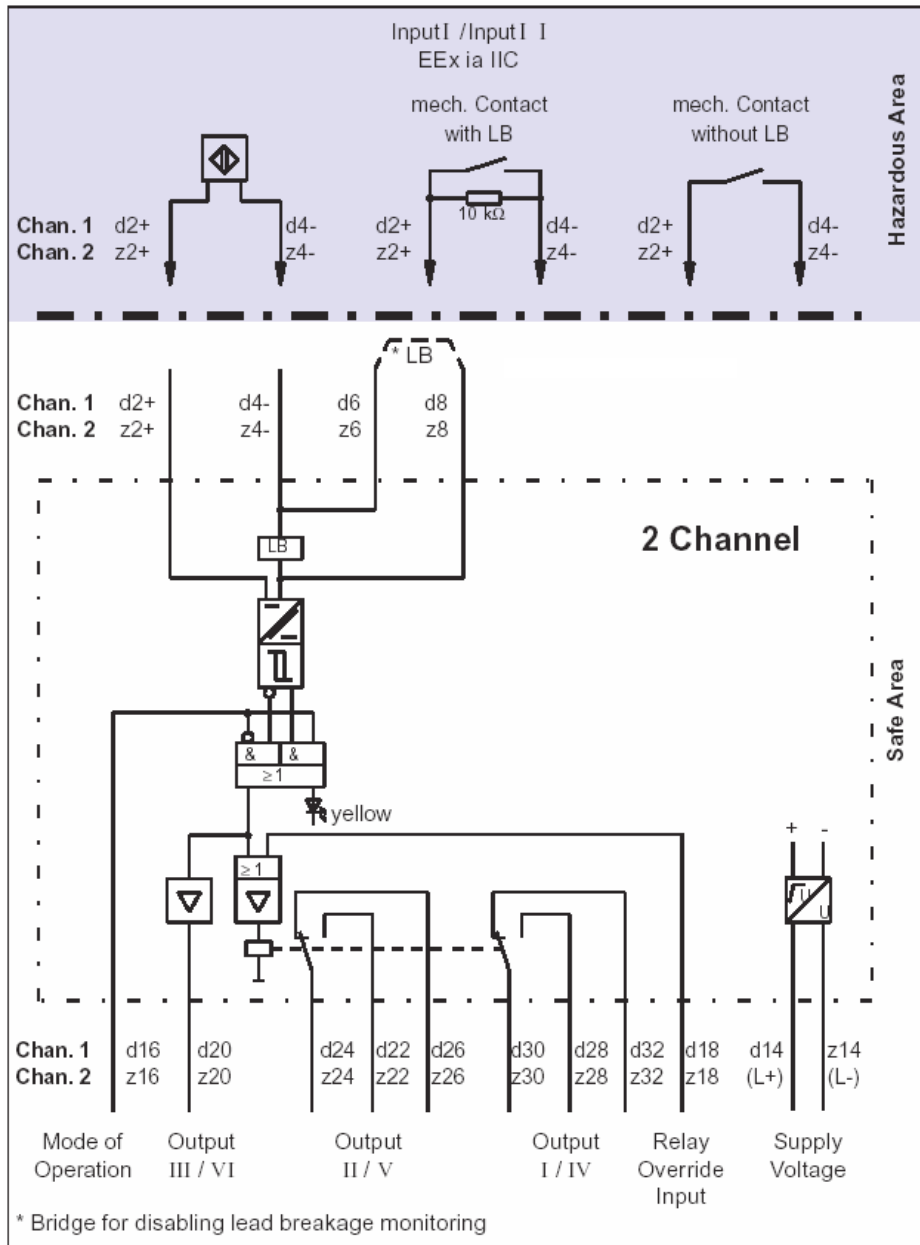


Figure 1: Block diagram of the Transformer Isolated Amplifier EG2-R

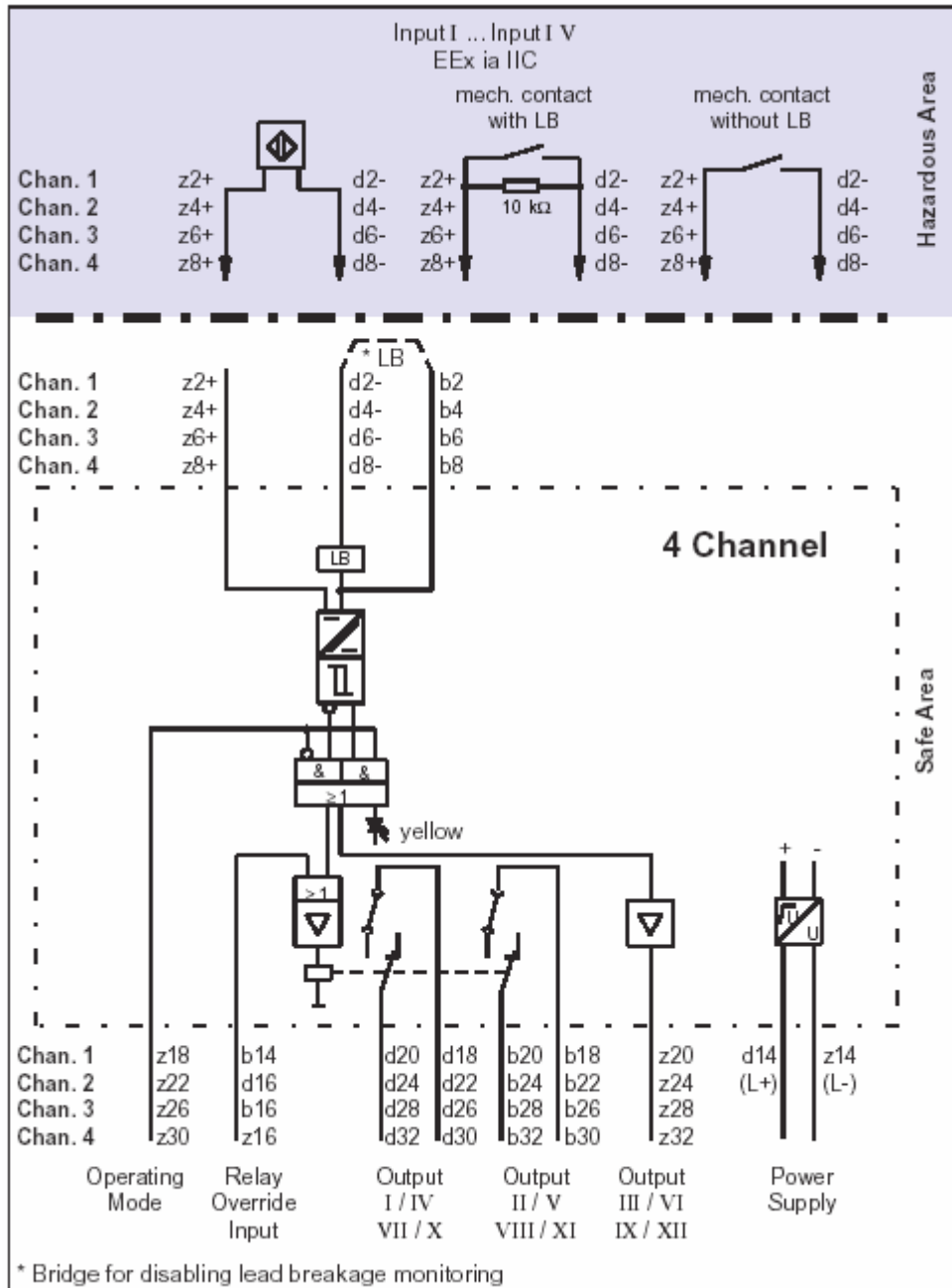


Figure 2: Block diagram of the Transformer Isolated Amplifier EG4-R

### 3.2 EG2(4)-RLK

The transformer isolated amplifier EG2(4)-RLK transmits digital signals from the hazardous area.

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

The control circuit can be monitored for lead breakage (LB) and short circuit (SC).

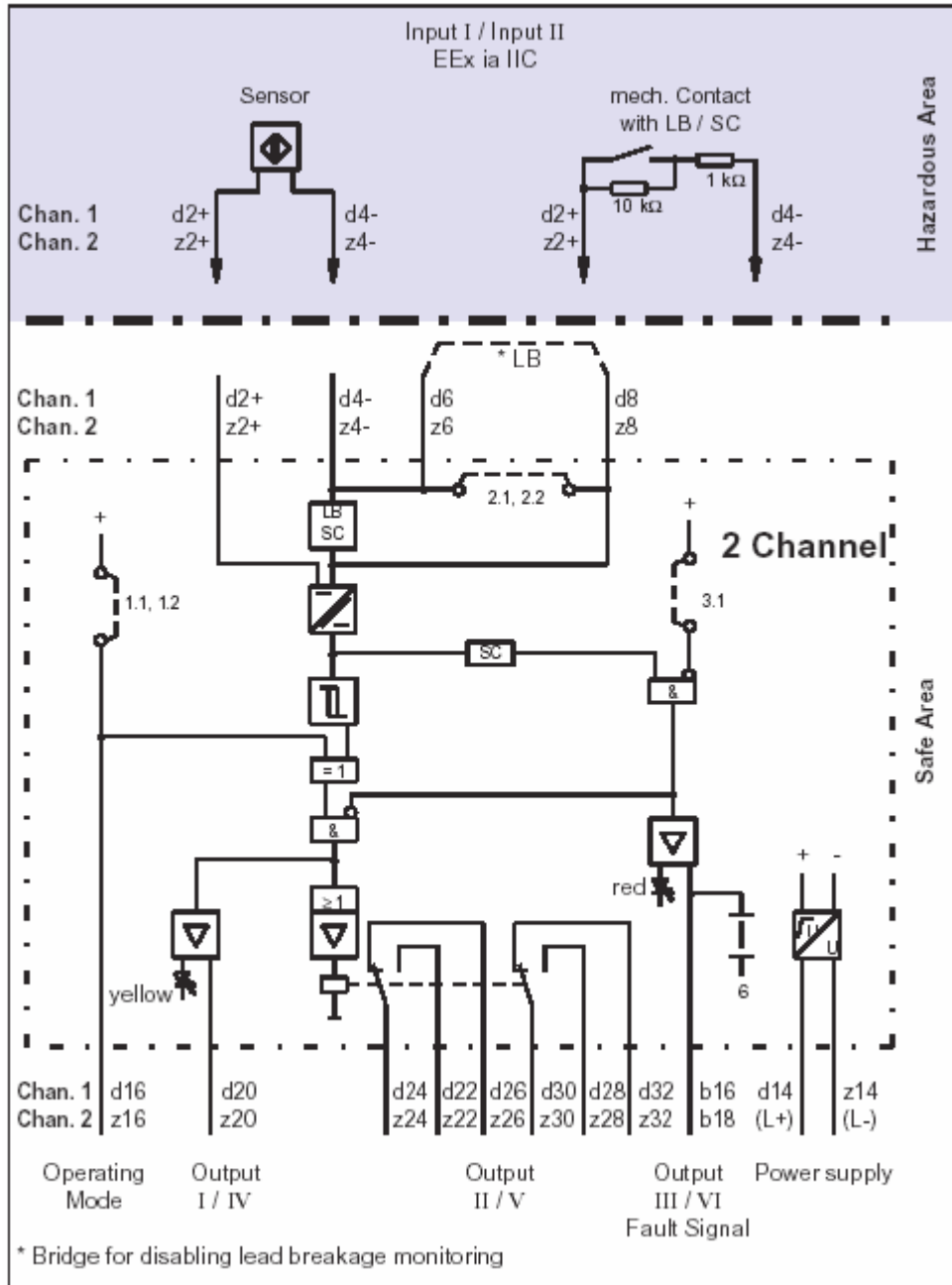


Figure 3: Block diagram of the Transformer Isolated Amplifier EG2-RLK

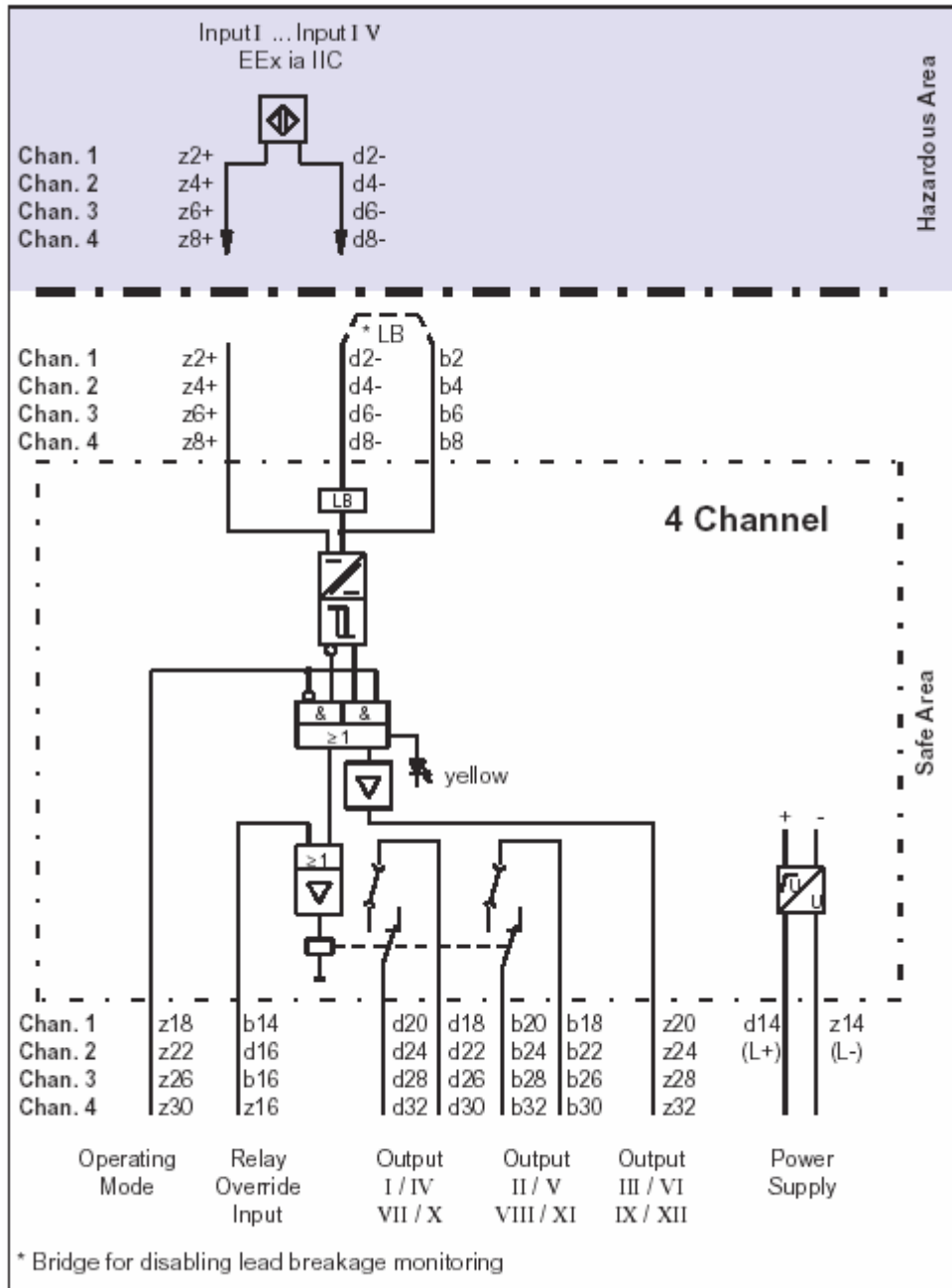


Figure 4: Block diagram of the Transformer Isolated Amplifier EG4-RLK

### 3.3 EG2(4)-T

The transformer isolated amplifier EG2(4)-T transmits digital signals from the hazardous area. Sensors per DIN EN 60947-5-6 (NAMUR) and mechanical contacts may be used. The control circuit can be monitored for lead breakage (LB).

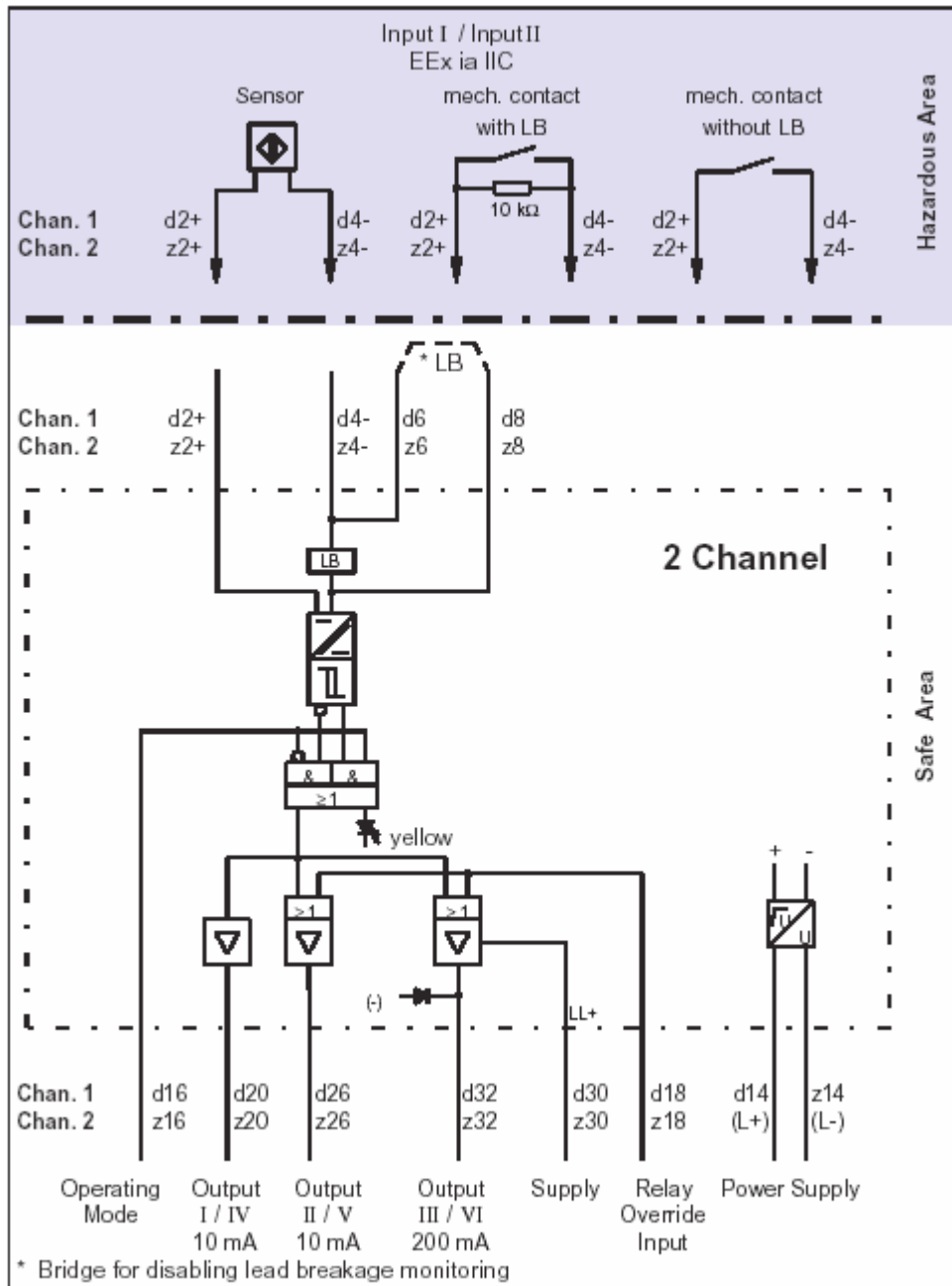


Figure 5: Block diagram of the Transformer Isolated Amplifier EG2-T

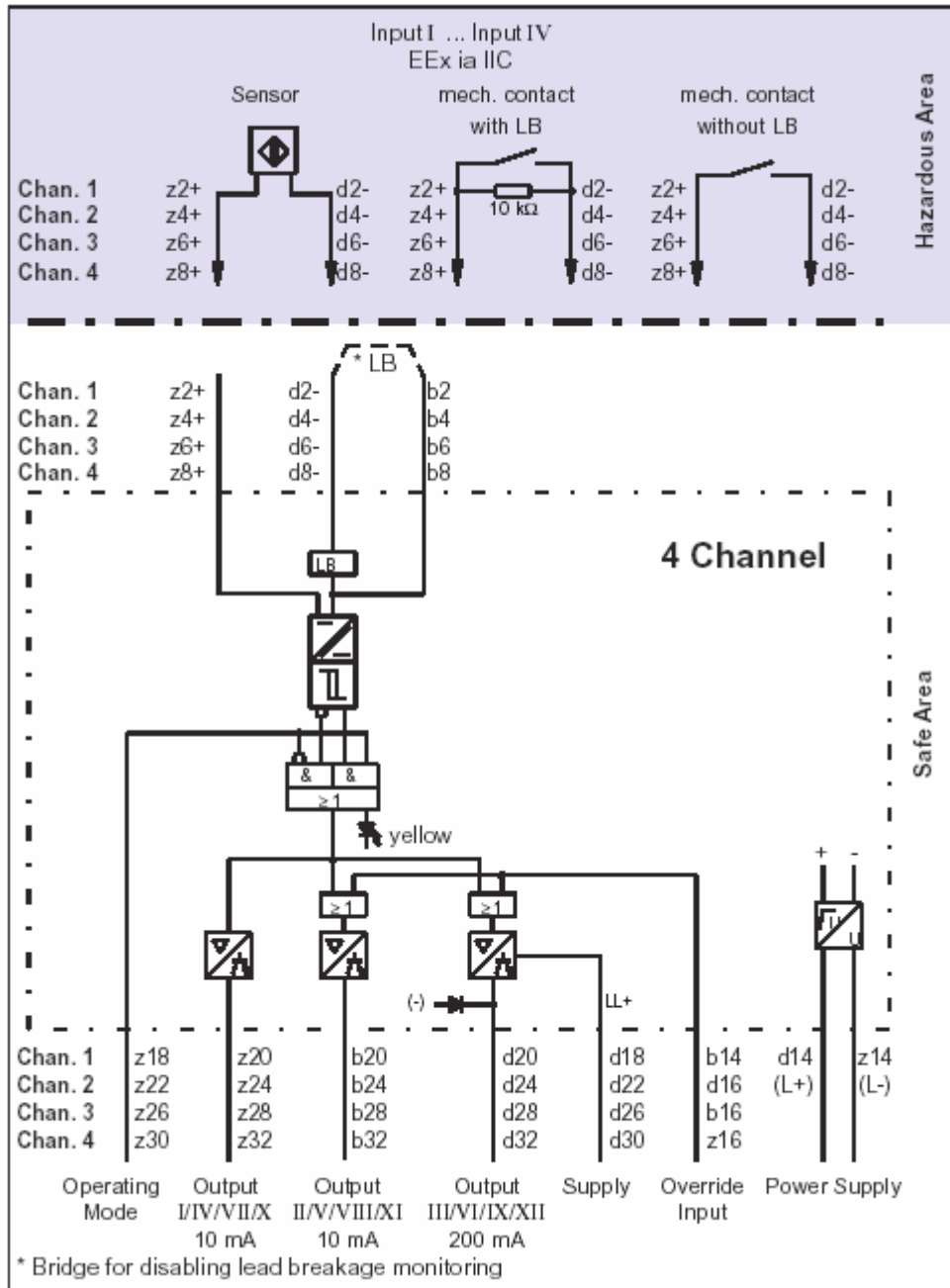


Figure 6: Block diagram of the Transformer Isolated Amplifier EG4-T

### 3.4 EG2(4)-TLK

The transformer isolated amplifier EG2(4)-TLK transmits digital signals from the hazardous area.

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

The control circuit can be monitored for lead breakage (LB) and short circuit (SC).

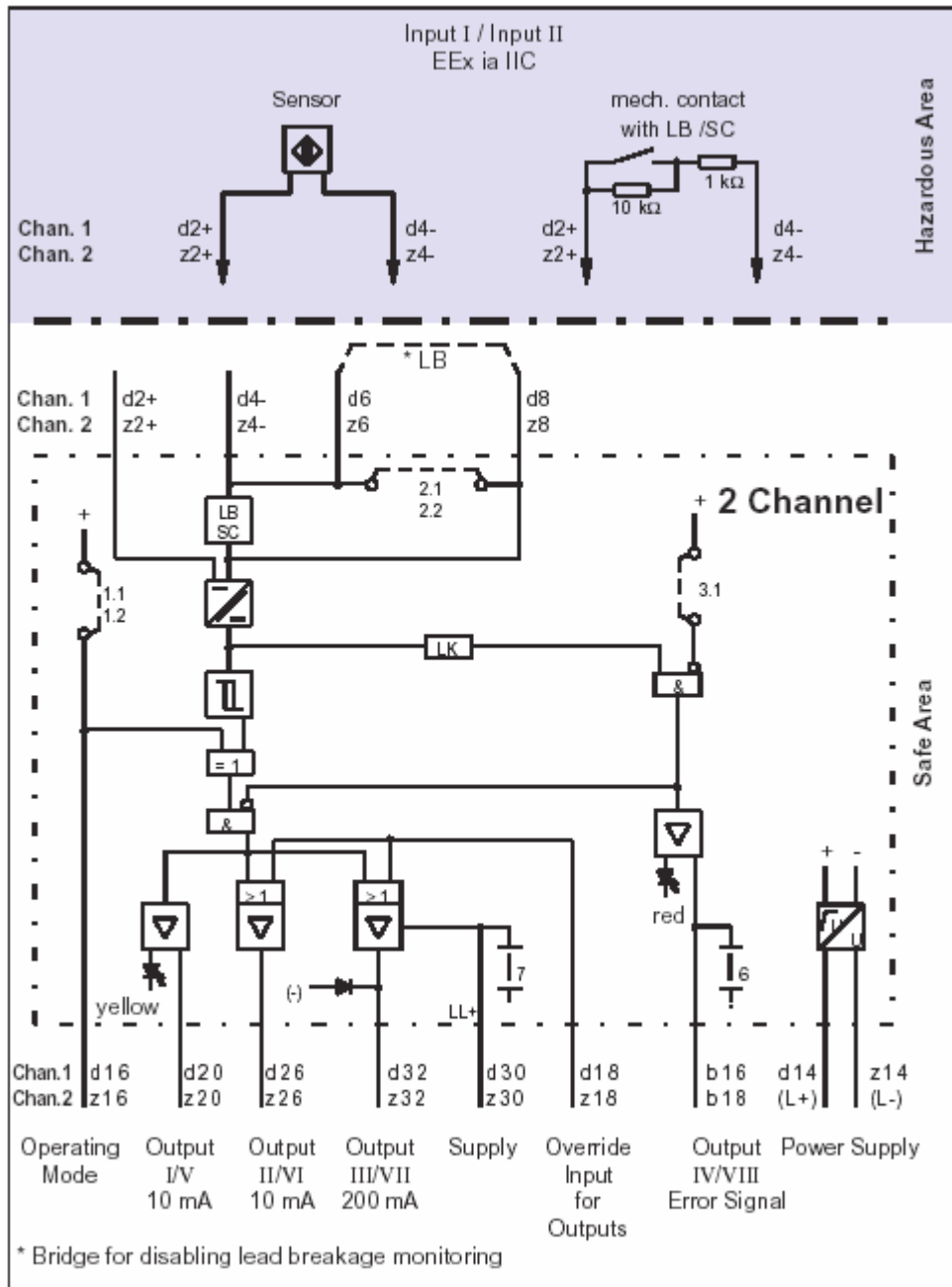


Figure 7: Block diagram of the Transformer Isolated Amplifier EG2-TLK



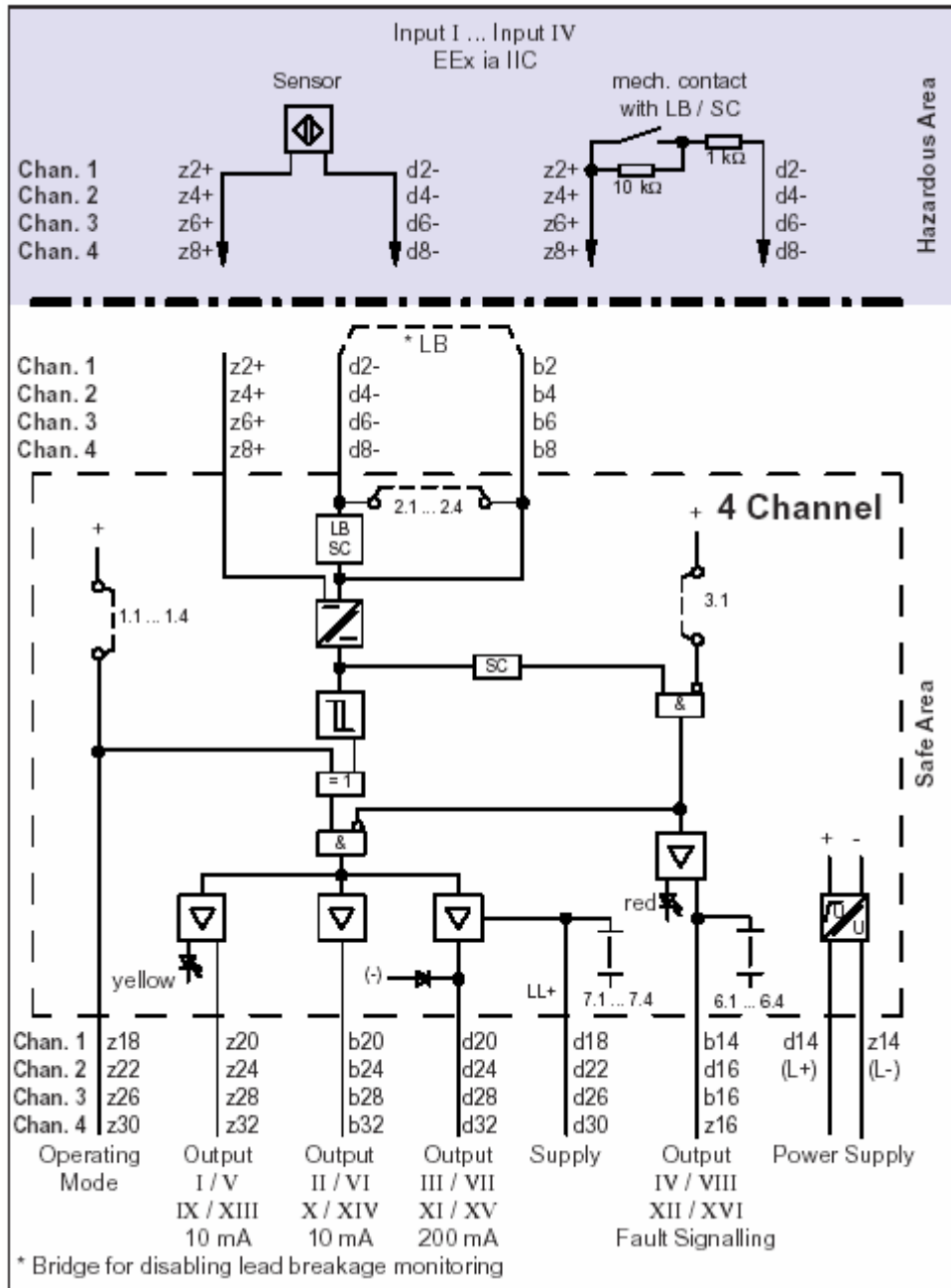


Figure 8: Block diagram of the Transformer Isolated Amplifier EG4-TLK

### 3.5 EG4-OT

The transformer isolated amplifier EG4-OT transmits digital signals from the hazardous area. Sensors per DIN EN 60947-5-6 (NAMUR) and mechanical contacts may be used. The control circuit can be monitored for lead breakage (LB).

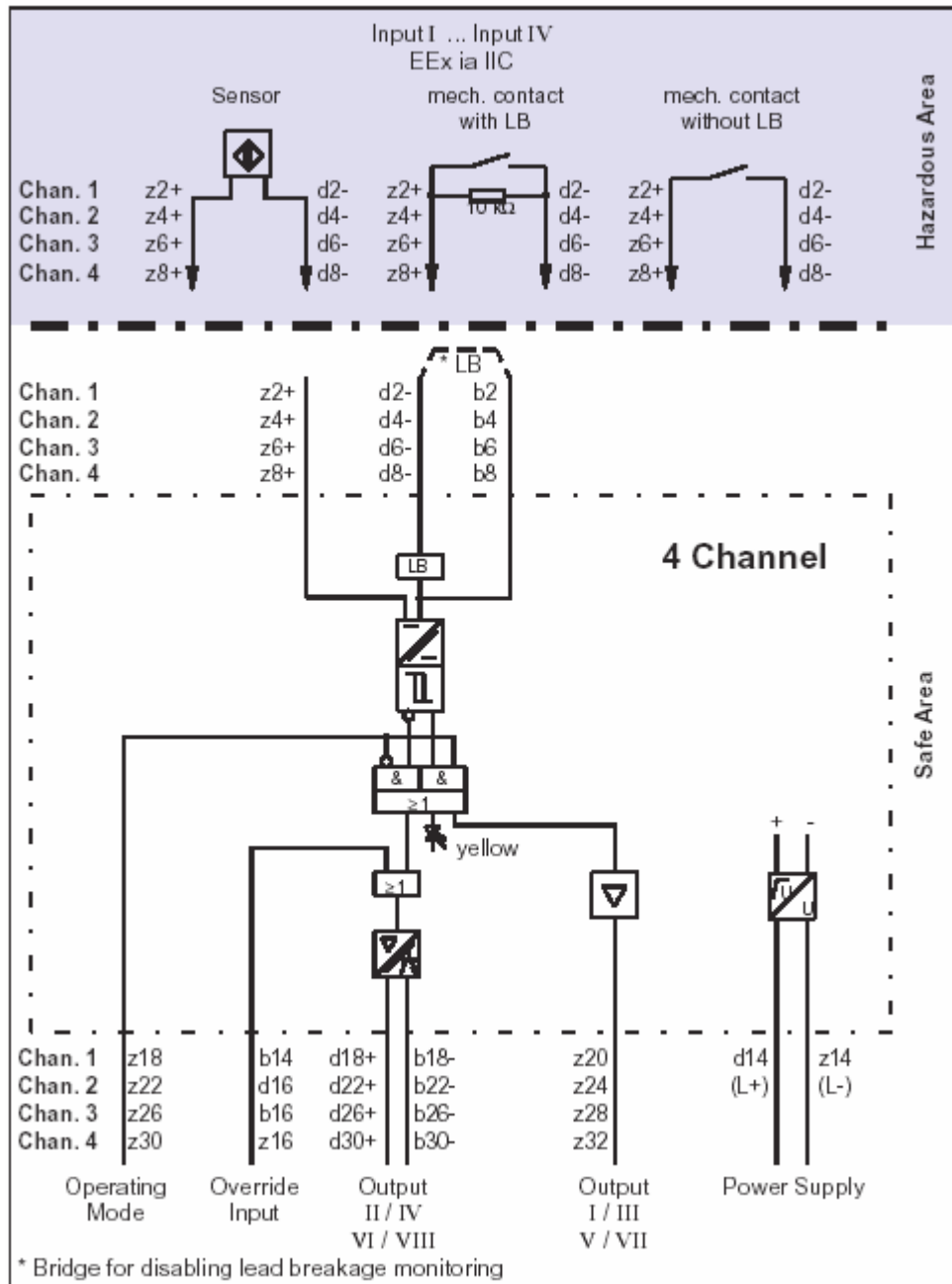


Figure 9: Block diagram of the Transformer Isolated Amplifier EG4-OT

### 3.6 EG4-OTLK

The transformer isolated amplifier EG4-OTLK transmits digital signals from the hazardous area. Sensors per DIN EN 60947-5-6 (NAMUR) and mechanical contacts may be used. The control circuit can be monitored for lead breakage (LB) and short circuit (SC).

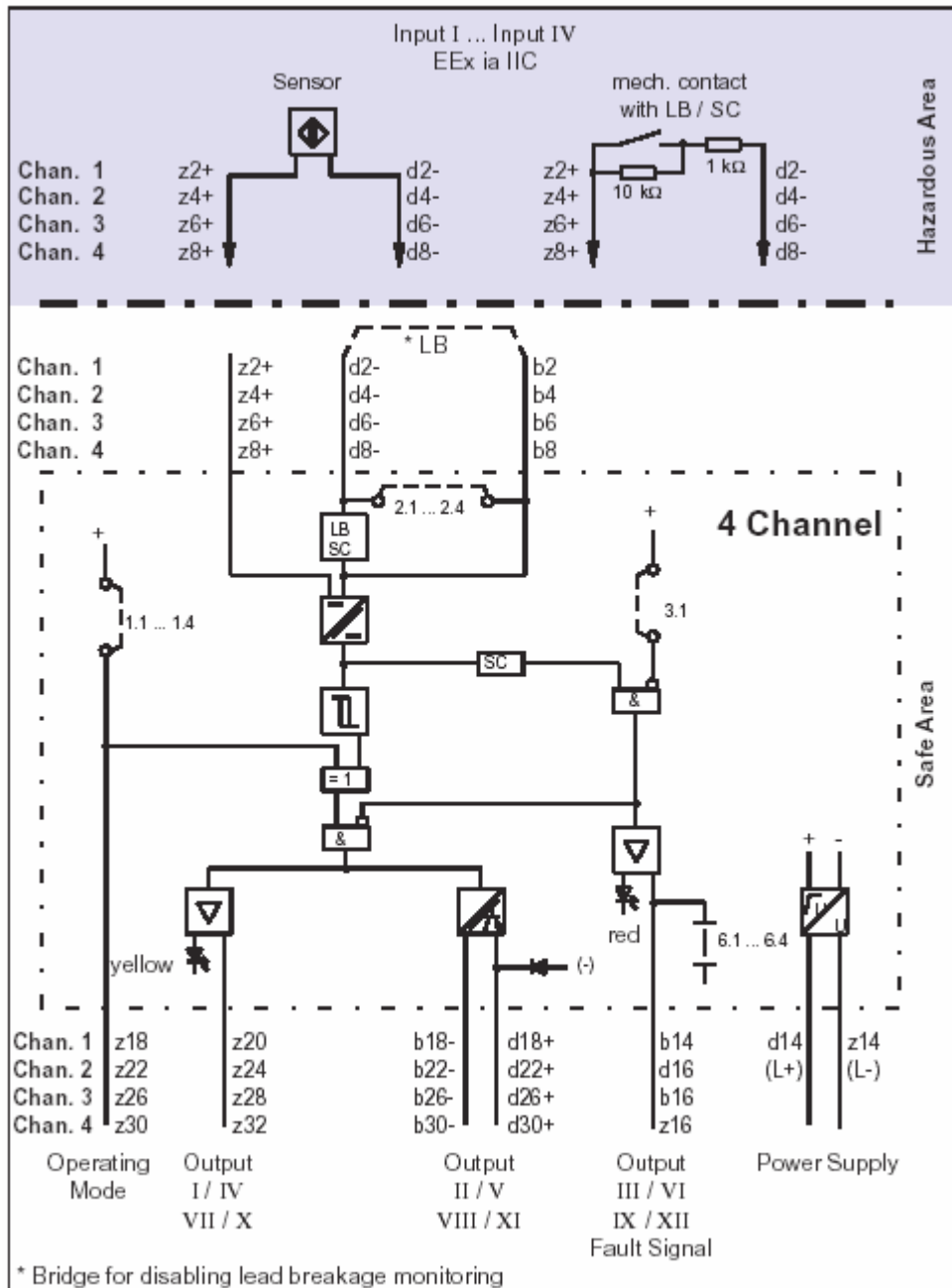


Figure 10: Block diagram of the Transformer Isolated Amplifier EG4-OTLK

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs and is documented in [R1] to [R24].

### 4.1 Description of the failure categories

#### Normal mode

The **fail-safe state** is defined as the output being de-energized (input signal about 1mA (logic low); normal mode is Z18=1).

#### Inverse mode

The **fail-safe state** is defined as the output being de-energized (input signal about 4mA (logic high); inverse mode is Z18=0).

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. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.

A **dangerous undetected** failure (DU) 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 **dangerous detected** failure (DD) is defined as a failure that is dangerous but is detected by the device itself.

An annunciation failure (A) is defined as a failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). For the calculation of the SFF it is treated like a safe undetected failure.

A "no effect" failure (#) is defined as a failure of a component that is part of the safety function but has no effect on the safety function or deviates the output current by not more than 1% of the actual value. For the calculation of the SFF it is treated like a safe undetected failure.

"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 chance 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 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 SN 29500 failure rate database. The rates are considered to be appropriate for safety integrity level verification calculations. The rates 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 Transformer Isolated Amplifiers EG\*-\*\*.

- Short Circuit (SC) detection and Lead Breakage (LB) detection are activated.
- The override function is disabled.
- For devices with relay output the maximum allowed parameters (rated current and switching voltage) are limited to decrease the stress factor for the relays.
- The considered output is representative for other outputs of the assessed device as only worst-case failure rates are indicated.
- Only one input and one output are part of the considered safety function.
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The repair time after a safe failure is 8 hours.
- The test time to react on a dangerous detected failure is 1 hour.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-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.
- All modules are operated in the low demand mode of operation.

## 5 Results of the assessment

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

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:

$$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$$

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

For the FMEDAs failure modes and distributions were used based on information gained from [N3] to [N5].

For the calculation of the  $PFD_{AVG}$  the following Markov model for a 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

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

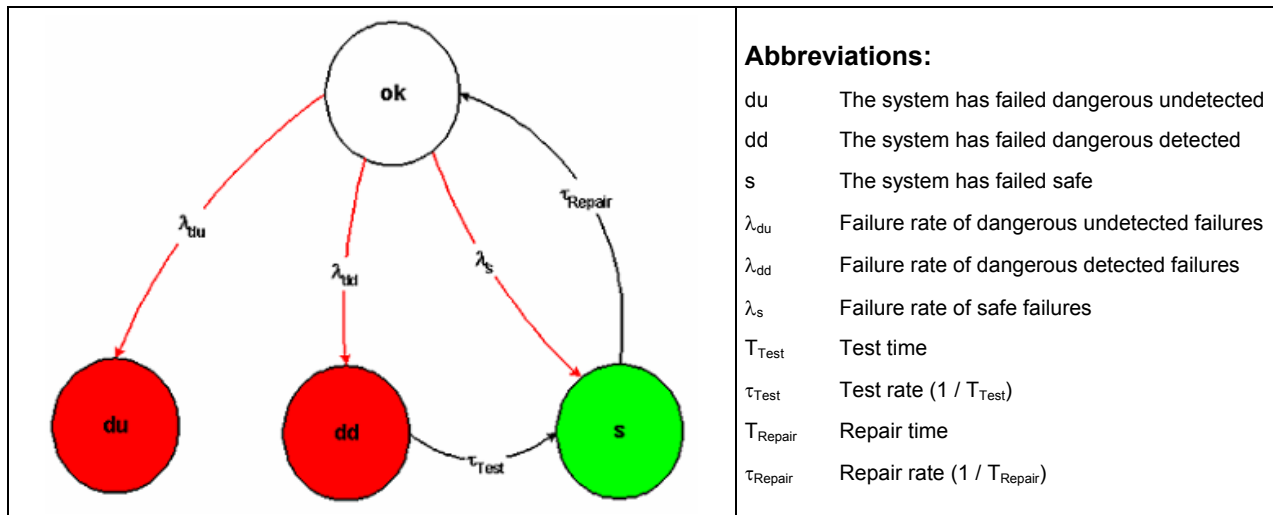


Figure 11: Markov model for a 1oo1D structure

## 5.1 EG2-R

### 5.1.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-R leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,67E-08 \text{ 1/h} + 4,98E-08 \text{ 1/h} + 5,77E-09 \text{ 1/h} = 9,23E-08 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 1,89E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,26E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$\text{SFF} = 84,94\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 8,29E-05$	$\text{PFD}_{\text{AVG}} = 4,14E-04$	$\text{PFD}_{\text{AVG}} = 8,28E-04$

The boxes marked in green (■) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 12 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

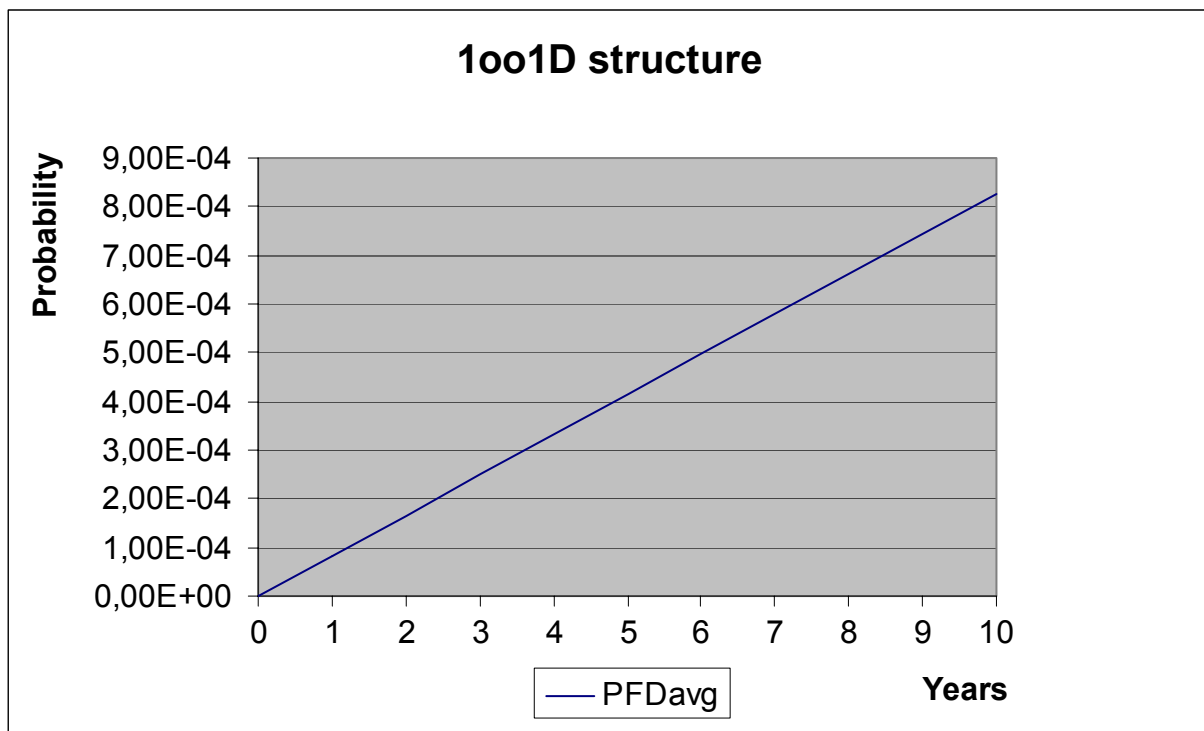


Figure 12:  $\text{PFD}_{\text{AVG}}(t)$  for EG2-R (normal mode)

### 5.1.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-R leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 2,49E-08 \text{ 1/h} + 4,83E-08 \text{ 1/h} + 5,27E-09 \text{ 1/h} = 7,84E-08 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 2,98E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,23E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 5,60E-09 \text{ 1/h}$$

$$SFF = 75,66\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,31E-04</math></b>	<b><math>PFD_{AVG} = 6,53E-04</math></b>	<b><math>PFD_{AVG} = 1,31E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 13 shows the time dependent curve of  $PFD_{AVG}$ .

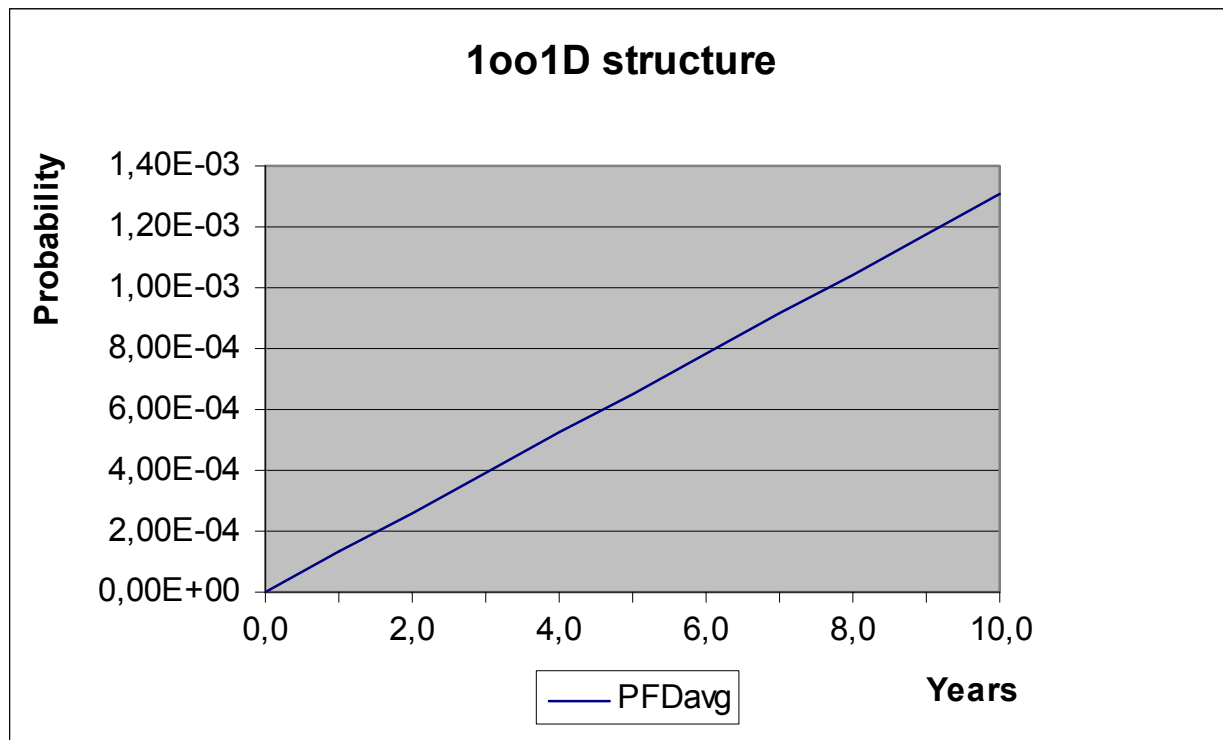


Figure 13:  $PFD_{AVG}(t)$  for EG2-R (inverse mode)



## 5.2 EG2-RLK

### 5.2.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-RLK (relay output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,79E-08 \text{ 1/h} + 5,37E-08 \text{ 1/h} + 5,77E-09 \text{ 1/h} = 9,74E-08 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,14E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,33E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$\text{SFF} = 83,93\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 9,37E-05$	$\text{PFD}_{\text{AVG}} = 4,69E-04$	$\text{PFD}_{\text{AVG}} = 9,37E-04$

The boxes marked in green (■) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 14 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

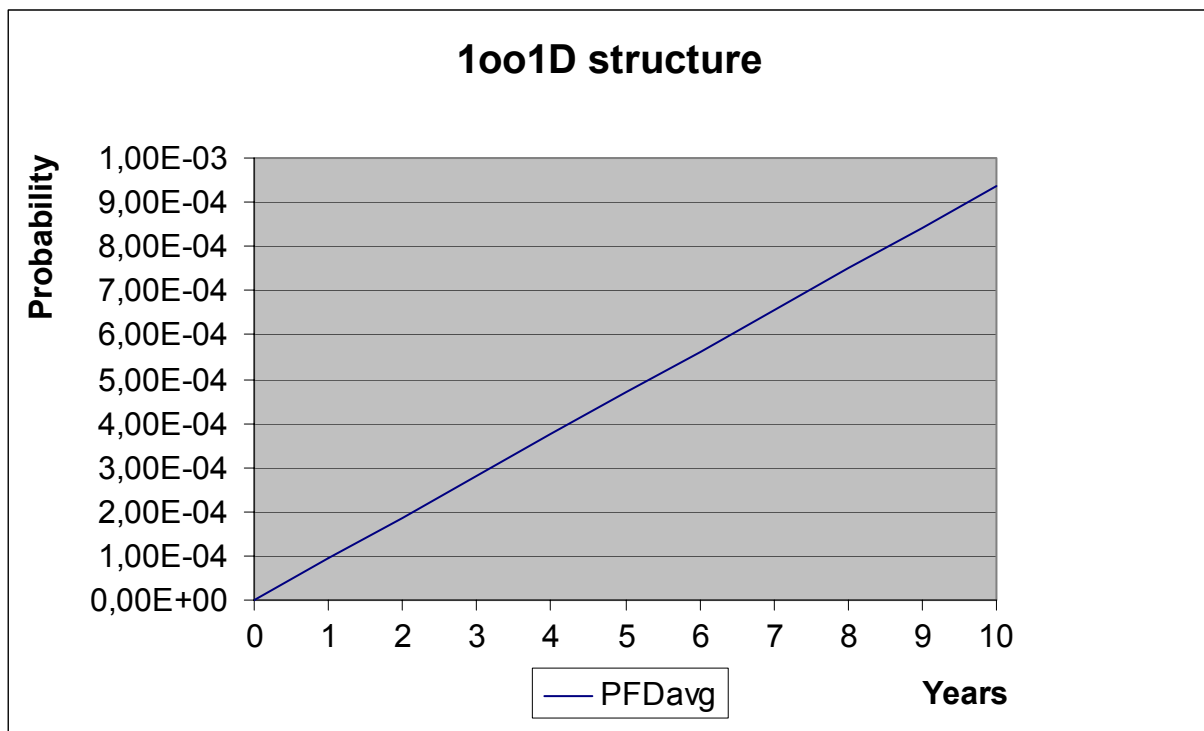


Figure 14:  $\text{PFD}_{\text{AVG}}(t)$  for EG2-RLK (normal mode)

## 5.2.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-RLK (relay output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 2,61E-08 \text{ 1/h} + 5,23E-08 \text{ 1/h} + 5,27E-09 \text{ 1/h} = 8,37E-08 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,23E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,30E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 5,60E-09 \text{ 1/h}$$

$$SFF = 75,18\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,42E-04</math></b>	<b><math>PFD_{AVG} = 7,07E-04</math></b>	<b><math>PFD_{AVG} = 1,41E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 15 shows the time dependent curve of  $PFD_{AVG}$ .

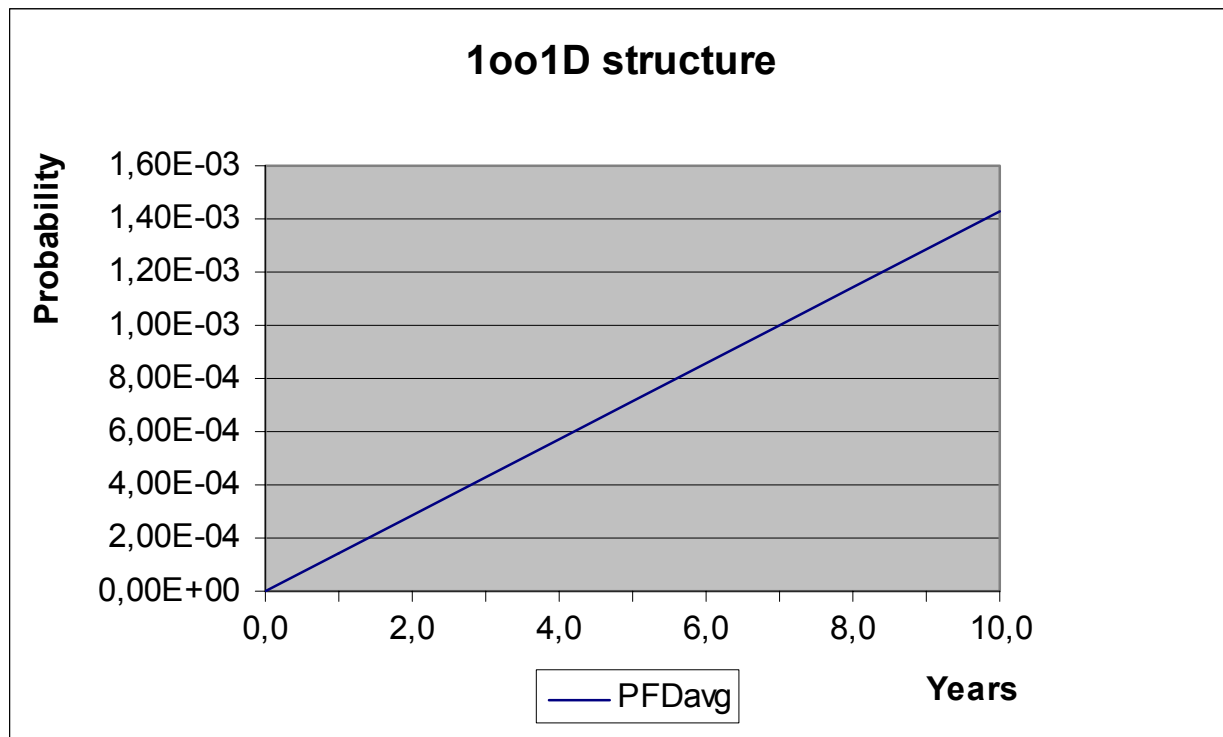


Figure 15:  $PFD_{AVG}(t)$  for EG2-RLK (inverse mode)

### 5.3 EG2-T

#### 5.3.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-T (200mA output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 4,57E-08 \text{ 1/h} + 6,18E-08 \text{ 1/h} + 7,07E-09 \text{ 1/h} = 1,15E-07 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,12E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,50E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$\text{SFF} = 85,87\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 9,29E-05$	$\text{PFD}_{\text{AVG}} = 4,65E-04$	$\text{PFD}_{\text{AVG}} = 9,29E-04$

The boxes marked in green (■) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 16 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

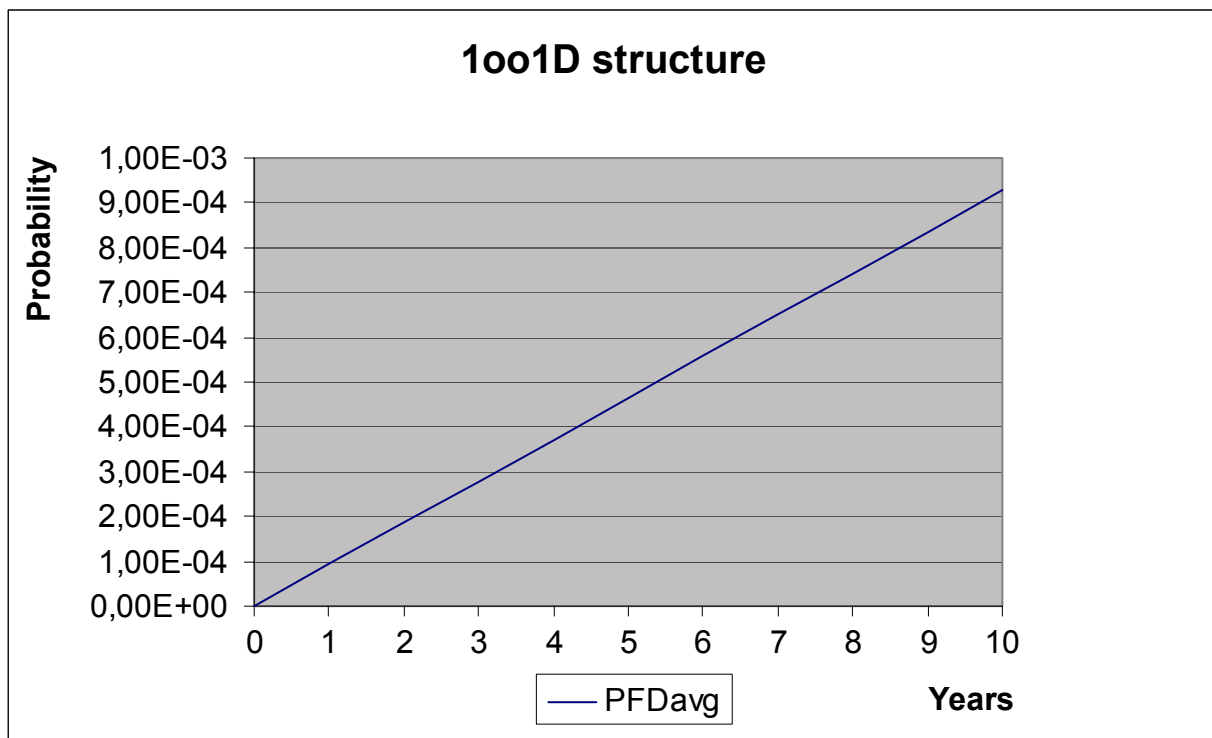


Figure 16:  $\text{PFD}_{\text{AVG}}(t)$  for EG2-T (normal mode)

### 5.3.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-T (200mA output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,38E-08 \text{ 1/h} + 6,04E-08 \text{ 1/h} + 6,57E-09 \text{ 1/h} = 1,01E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,21E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,47E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 5,60E-09 \text{ 1/h}$$

$$SFF = 78,17\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,41E-04</math></b>	<b><math>PFD_{AVG} = 7,03E-04</math></b>	<b><math>PFD_{AVG} = 1,41E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 17 shows the time dependent curve of  $PFD_{AVG}$ .

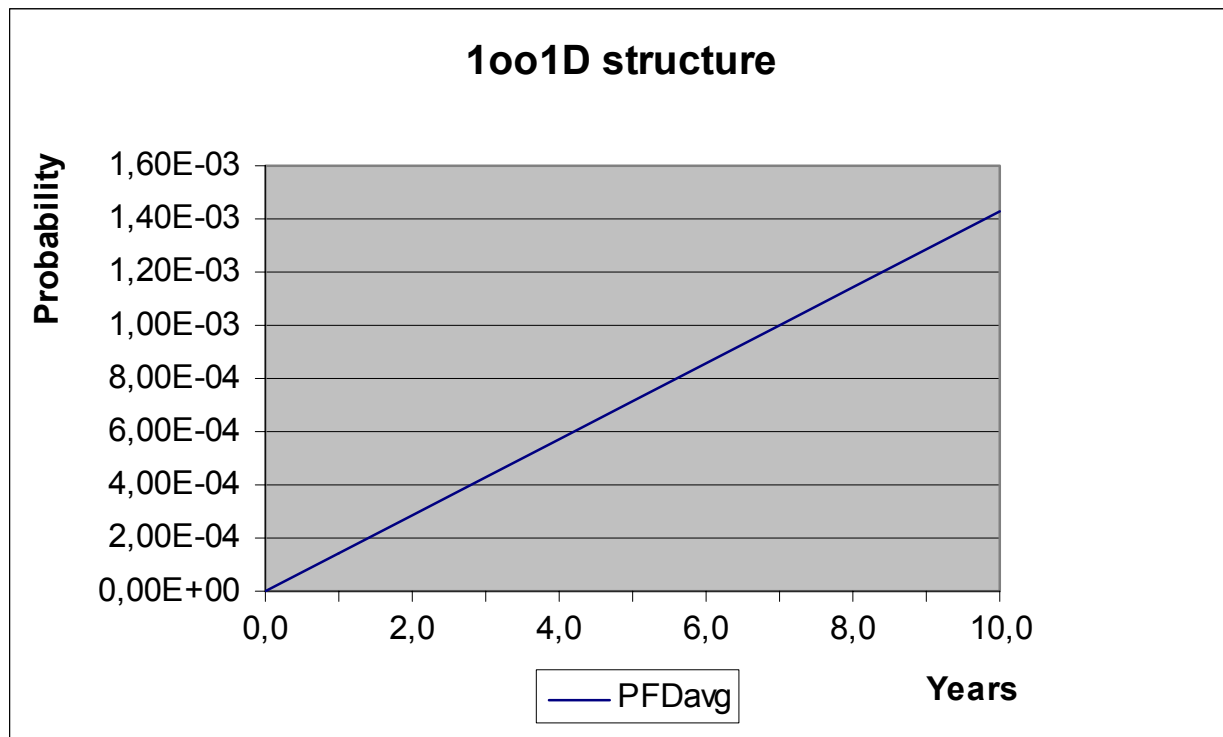


Figure 17:  $PFD_{AVG}(t)$  for EG2-T (inverse mode)

## 5.4 EG2-TLK

### 5.4.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-TLK (200mA output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 4,67E-08 \text{ 1/h} + 6,70E-08 \text{ 1/h} + 7,07E-09 \text{ 1/h} = 1,21E-07 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,19E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,57E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 1,54E-08 \text{ 1/h}$$

$$\text{SFF} = 86,05\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 9,59E-05$	$\text{PFD}_{\text{AVG}} = 4,79E-04$	$\text{PFD}_{\text{AVG}} = 9,59E-04$

The boxes marked in green (■) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 18 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

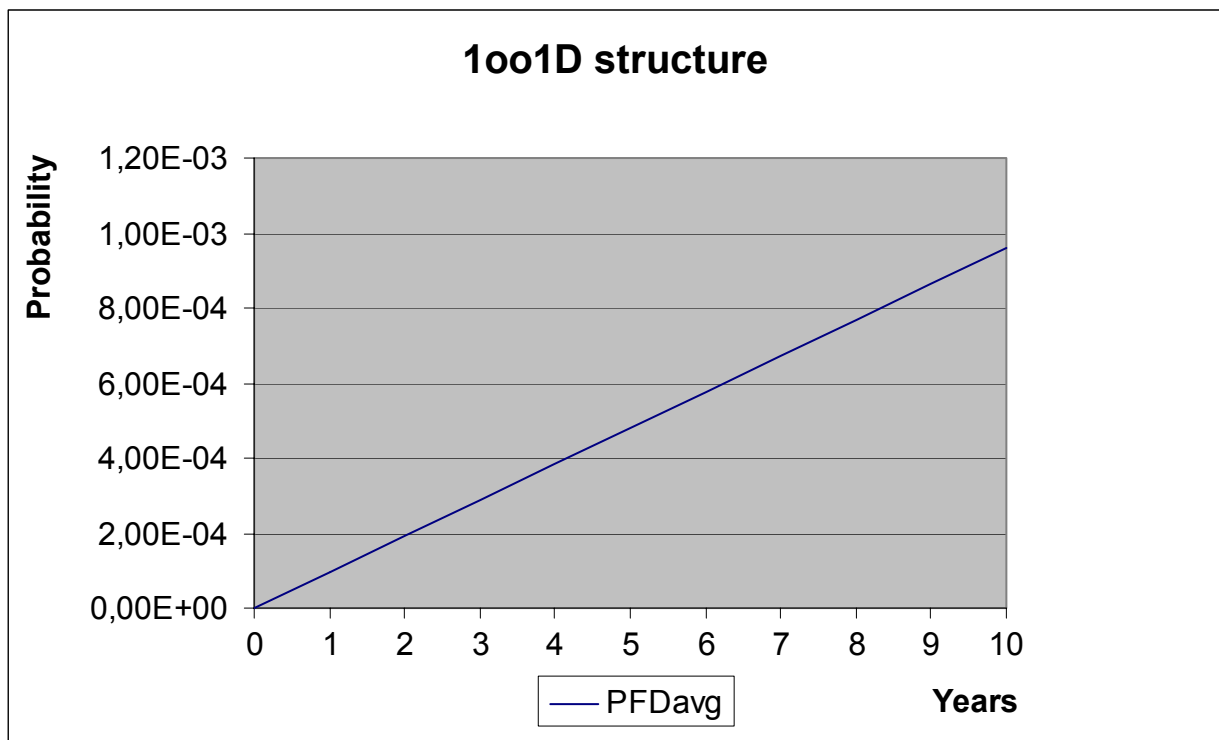


Figure 18:  $\text{PFD}_{\text{AVG}}(t)$  for EG2-TLK (normal mode)

### 5.4.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG2-TLK (200mA output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,48E-08 \text{ 1/h} + 6,13E-08 \text{ 1/h} + 6,57E-09 \text{ 1/h} = 1,03E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,28E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,50E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,26E-08 \text{ 1/h}$$

$$SFF = 78,09\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,44E-04</math></b>	<b><math>PFD_{AVG} = 7,18E-04</math></b>	<b><math>PFD_{AVG} = 1,44E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 19 shows the time dependent curve of  $PFD_{AVG}$ .

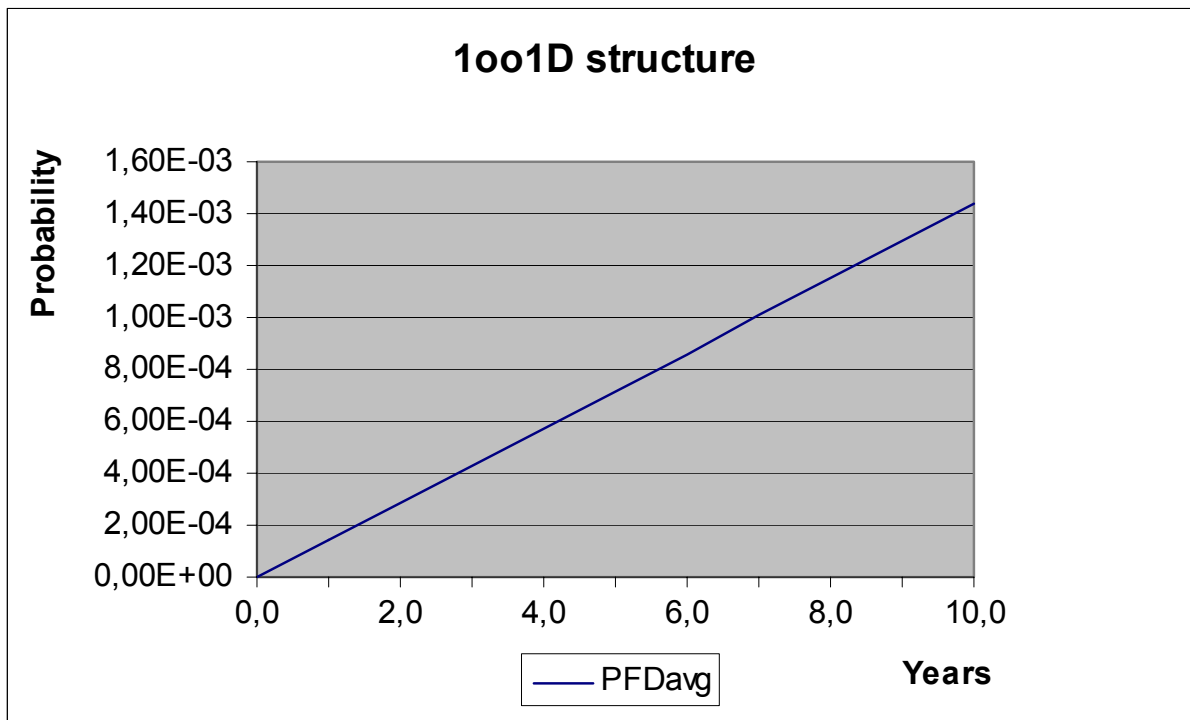


Figure 19:  $PFD_{AVG}(t)$  for EG2-TLK (inverse mode)

## 5.5 EG4-R

### 5.5.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-R (relay output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,95E-08 \text{ 1/h} + 4,96E-08 \text{ 1/h} + 7,39E-09 \text{ 1/h} = 9,65E-08 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,15E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,32E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$SFF = 83,75\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 9,43E-05</math></b>	<b><math>PFD_{AVG} = 4,71E-04</math></b>	<b><math>PFD_{AVG} = 9,42E-04</math></b>

The boxes marked in green (■) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 20 shows the time dependent curve of  $PFD_{AVG}$ .

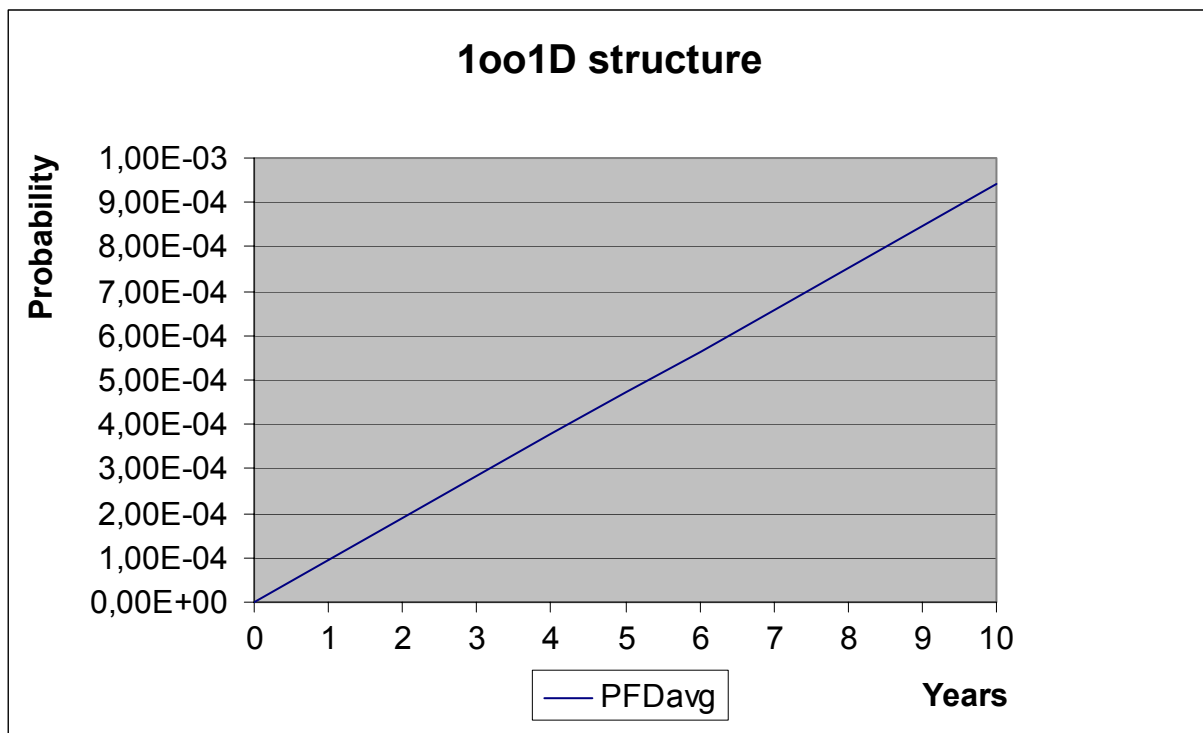


Figure 20:  $PFD_{AVG}(t)$  for EG4-R (normal mode)

### 5.5.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-R (relay output) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 2,77E-08 \text{ 1/h} + 4,81E-08 \text{ 1/h} + 6,89E-09 \text{ 1/h} = 8,27E-08 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,24E-08 \text{ 1/h}$$

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

$$\lambda_{not \text{ part}} = 5,60E-09 \text{ 1/h}$$

$$SFF = 74,93\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{AVG} = 1,42E-04$	$PFD_{AVG} = 7,10E-04$	$PFD_{AVG} = 1,42E-03$

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 21 shows the time dependent curve of  $PFD_{AVG}$ .

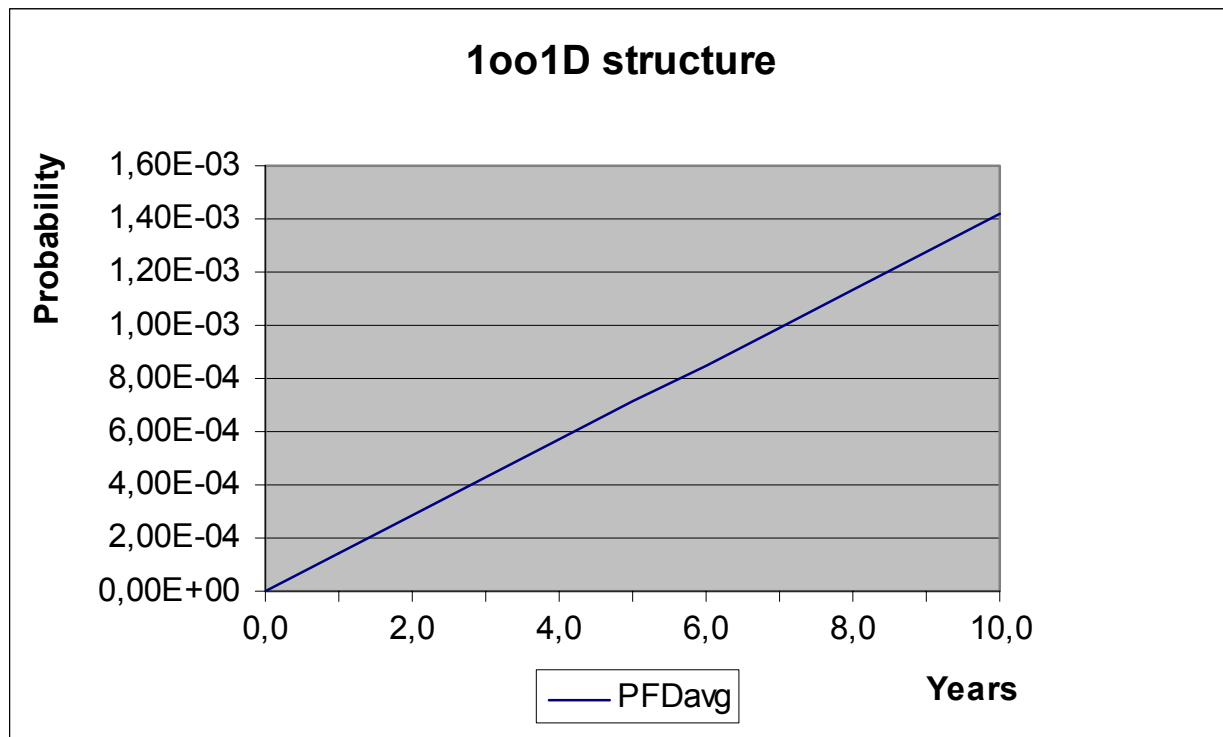


Figure 21:  $PFD_{AVG}(t)$  for EG4-R (inverse mode)



## 5.6 EG4-RLK

### 5.6.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-RLK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,95E-08 \text{ 1/h} + 5,27E-08 \text{ 1/h} + 5,27E-09 \text{ 1/h} = 9,75E-08 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,27E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,35E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$SFF = 83,11\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 9,96E-05</math></b>	<b><math>PFD_{AVG} = 4,98E-04</math></b>	<b><math>PFD_{AVG} = 9,95E-04</math></b>

The boxes marked in green (■) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 22 shows the time dependent curve of  $PFD_{AVG}$ .

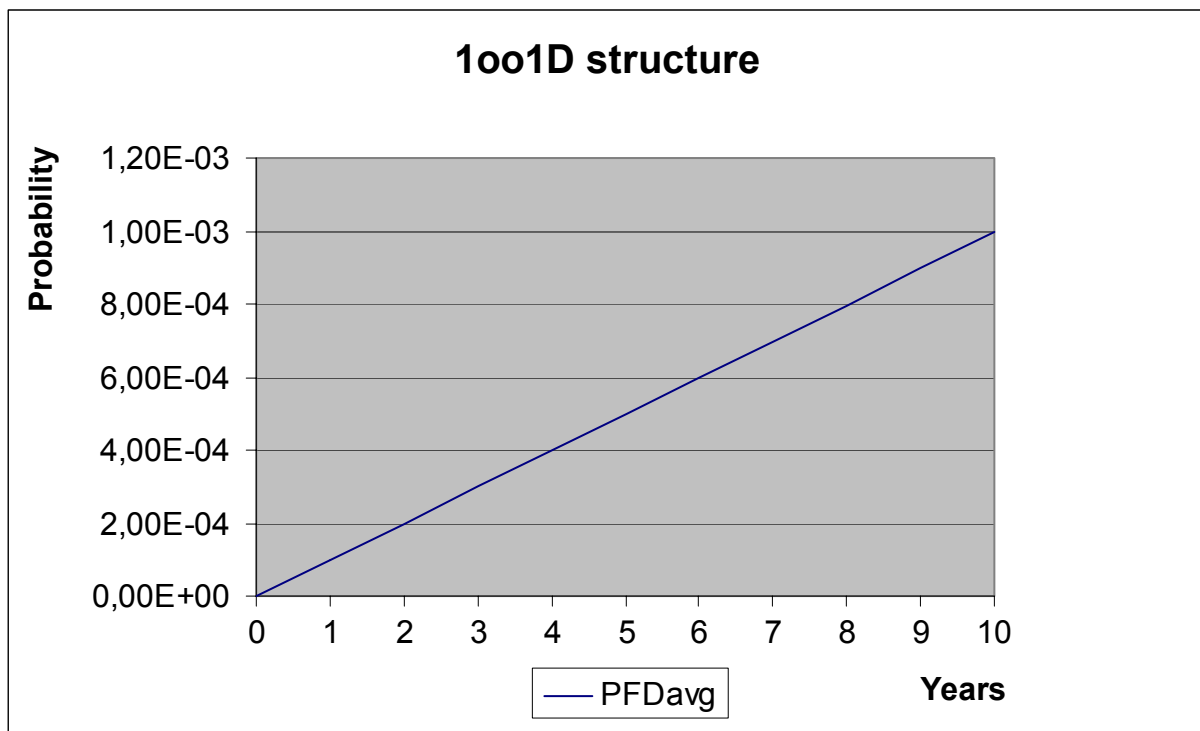


Figure 22:  $PFD_{AVG}(t)$  for EG4-RLK (normal mode)

### 5.6.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-RLK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 2,77E-08 \text{ 1/h} + 5,13E-08 \text{ 1/h} + 5,27E-09 \text{ 1/h} = 8,43E-08 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,47E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,33E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 4,00E-09 \text{ 1/h}$$

$$SFF = 73,93\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,52E-04</math></b>	<b><math>PFD_{AVG} = 7,60E-04</math></b>	<b><math>PFD_{AVG} = 1,52E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 23 shows the time dependent curve of  $PFD_{AVG}$ .

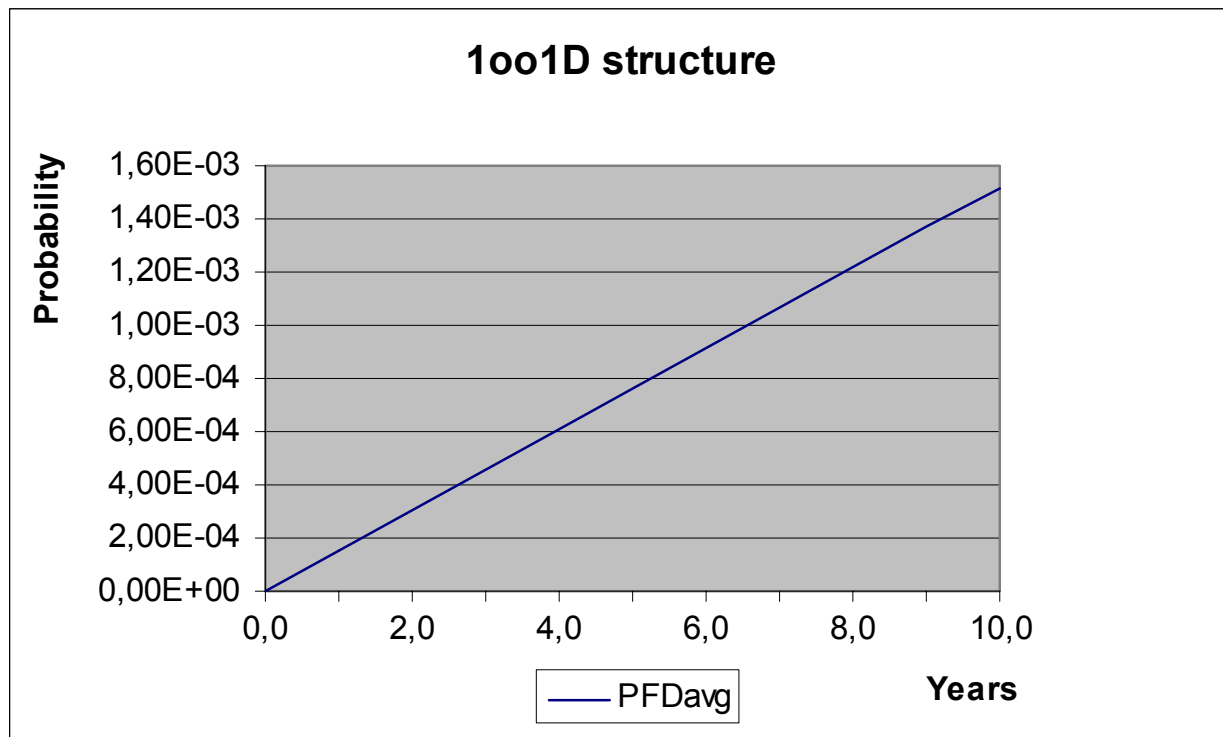


Figure 23:  $PFD_{AVG}(t)$  for EG4-RLK (inverse mode)

## 5.7 EG4-T

### 5.7.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-T leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 4,23E-08 \text{ 1/h} + 5,68E-08 \text{ 1/h} + 8,67E-09 \text{ 1/h} = 1,08E-07 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,20E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,44E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$\text{SFF} = 84,73\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 9,64E-05$	$\text{PFD}_{\text{AVG}} = 4,82E-04$	$\text{PFD}_{\text{AVG}} = 9,64E-04$

The boxes marked in green (■) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 24 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

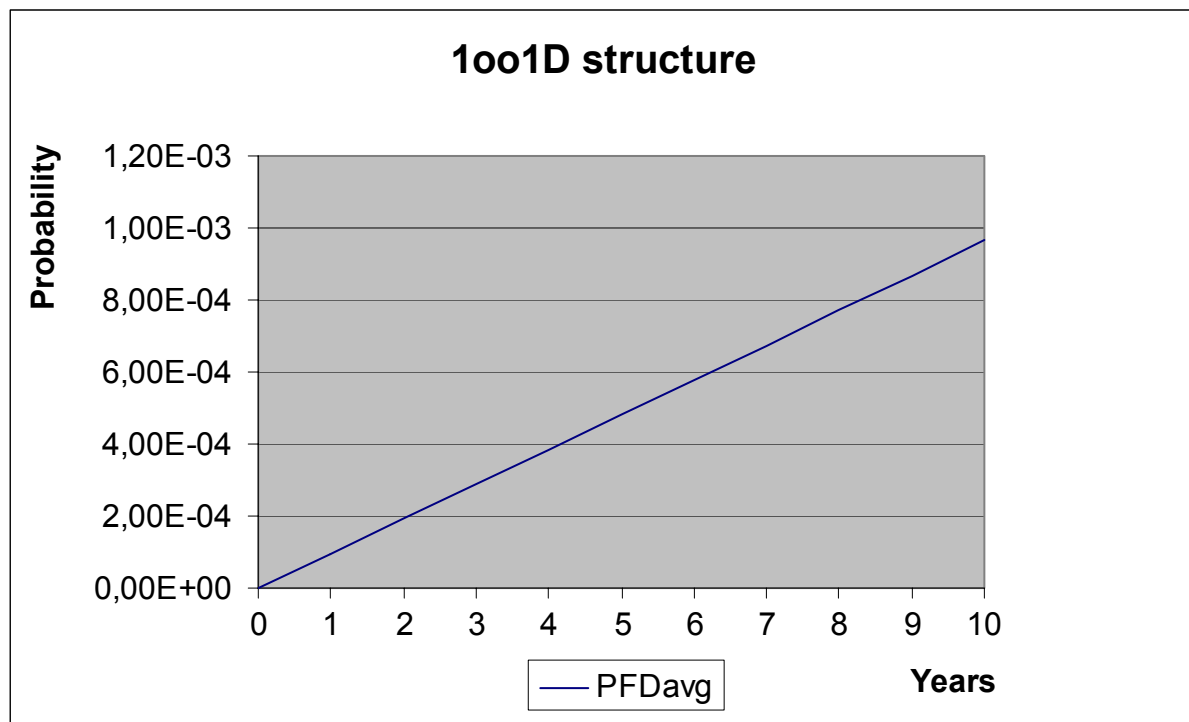


Figure 24:  $\text{PFD}_{\text{AVG}}(t)$  for EG4-T (normal mode)

### 5.7.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-T leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,04E-08 \text{ 1/h} + 5,54E-08 \text{ 1/h} + 8,17E-09 \text{ 1/h} = 9,40E-08 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,29E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,41E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 5,60E-09 \text{ 1/h}$$

$$SFF = 76,67\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,44E-04</math></b>	<b><math>PFD_{AVG} = 7,21E-04</math></b>	<b><math>PFD_{AVG} = 1,44E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 25 shows the time dependent curve of  $PFD_{AVG}$ .

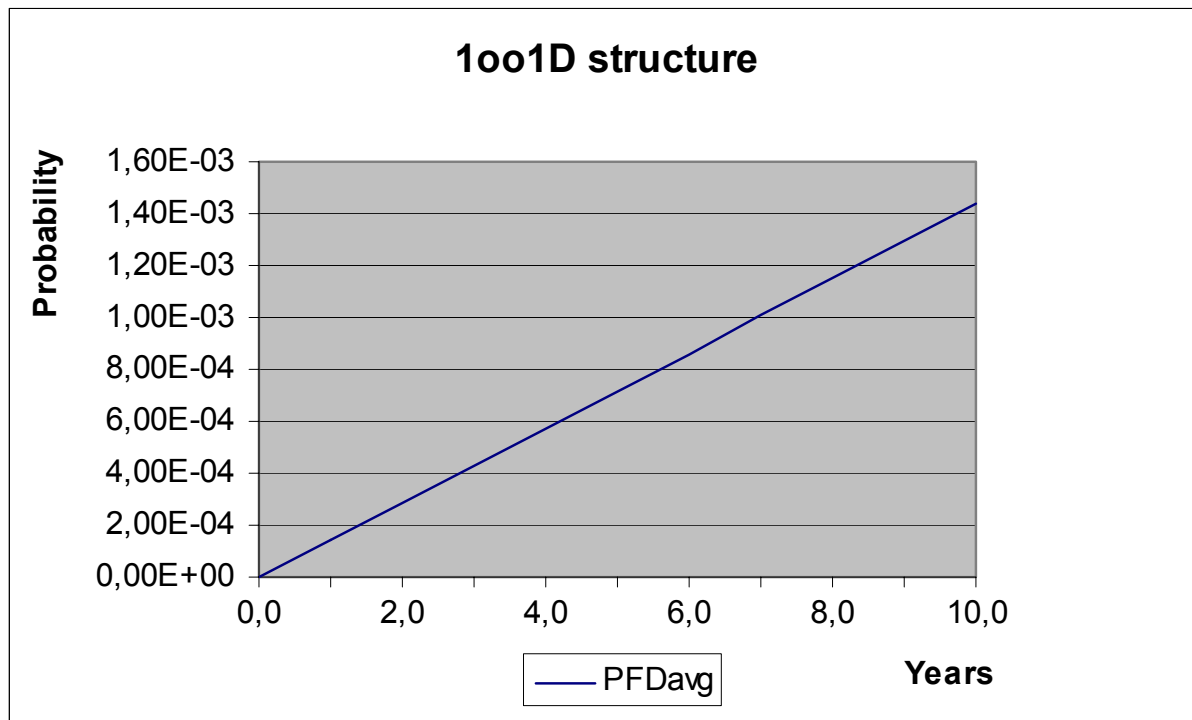


Figure 25:  $PFD_{AVG}(t)$  for EG4-T (inverse mode)

## 5.8 EG4-TLK

### 5.8.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-TLK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 4,93E-08 \text{ 1/h} + 6,80E-08 \text{ 1/h} + 7,07E-09 \text{ 1/h} = 1,24E-07 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,43E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,63E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 1,28E-08 \text{ 1/h}$$

$$\text{SFF} = 85,09\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 1,06E-04$	$\text{PFD}_{\text{AVG}} = 5,32E-04$	$\text{PFD}_{\text{AVG}} = 1,06E-03$

The boxes marked in yellow (  ) mean that the calculated  $\text{PFD}_{\text{AVG}}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 26 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

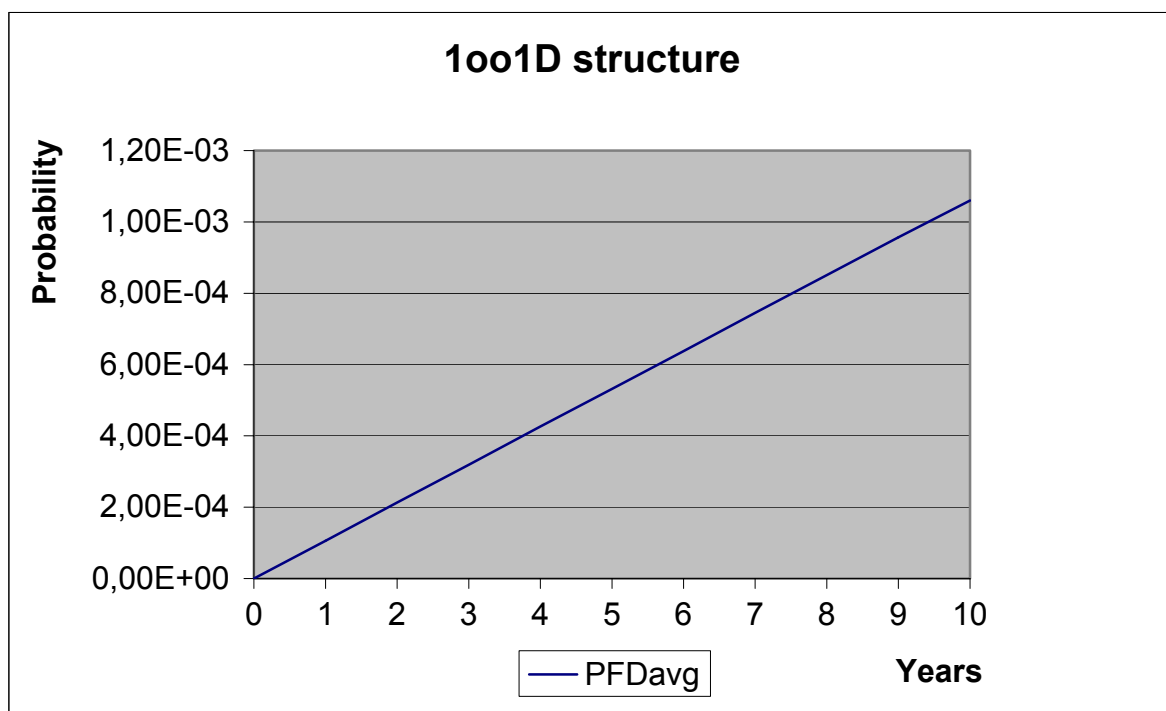


Figure 26:  $\text{PFD}_{\text{AVG}}(t)$  for EG4-TLK (normal mode)

### 5.8.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-TLK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 3,74E-08 \text{ 1/h} + 6,23E-08 \text{ 1/h} + 6,57E-09 \text{ 1/h} = 1,06E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,52E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,56E-07 \text{ 1/h}$$

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

$$SFF = 77,39\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{AVG} = 1,54E-04$	$PFD_{AVG} = 7,71E-04$	$PFD_{AVG} = 1,54E-03$

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 27 shows the time dependent curve of  $PFD_{AVG}$ .

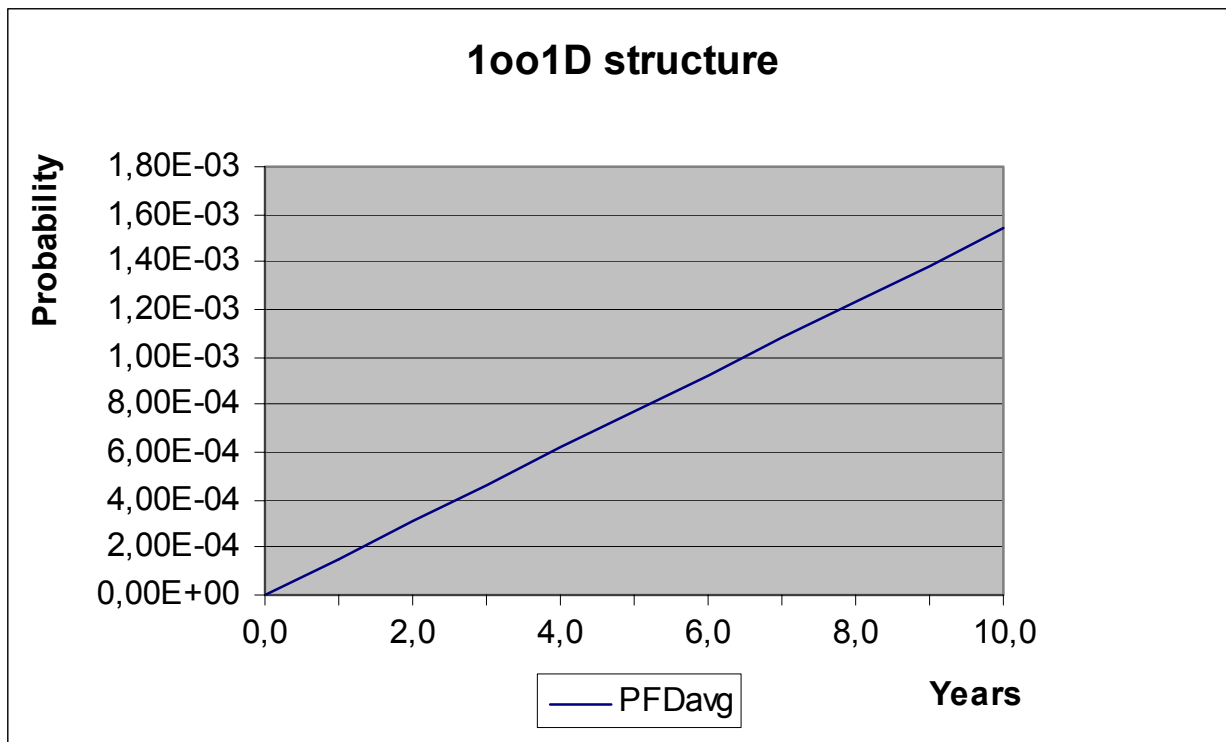


Figure 27:  $PFD_{AVG}(t)$  for EG4-TLK (inverse mode)

## 5.9 EG4-OT

### 5.9.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-OT leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 5,49E-08 \text{ 1/h} + 5,96E-08 \text{ 1/h} + 8,76E-09 \text{ 1/h} = 1,23E-07 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,82E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,66E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,60E-09 \text{ 1/h}$$

$$\text{SFF} = 83,01\%$$

The  $\text{PFD}_{\text{AVG}}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$\text{PFD}_{\text{AVG}} = 1,23E-04$	$\text{PFD}_{\text{AVG}} = 6,17E-04$	$\text{PFD}_{\text{AVG}} = 1,23E-03$

The boxes marked in yellow (  ) mean that the calculated  $\text{PFD}_{\text{AVG}}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $\text{PFD}_{\text{AVG}}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 28 shows the time dependent curve of  $\text{PFD}_{\text{AVG}}$ .

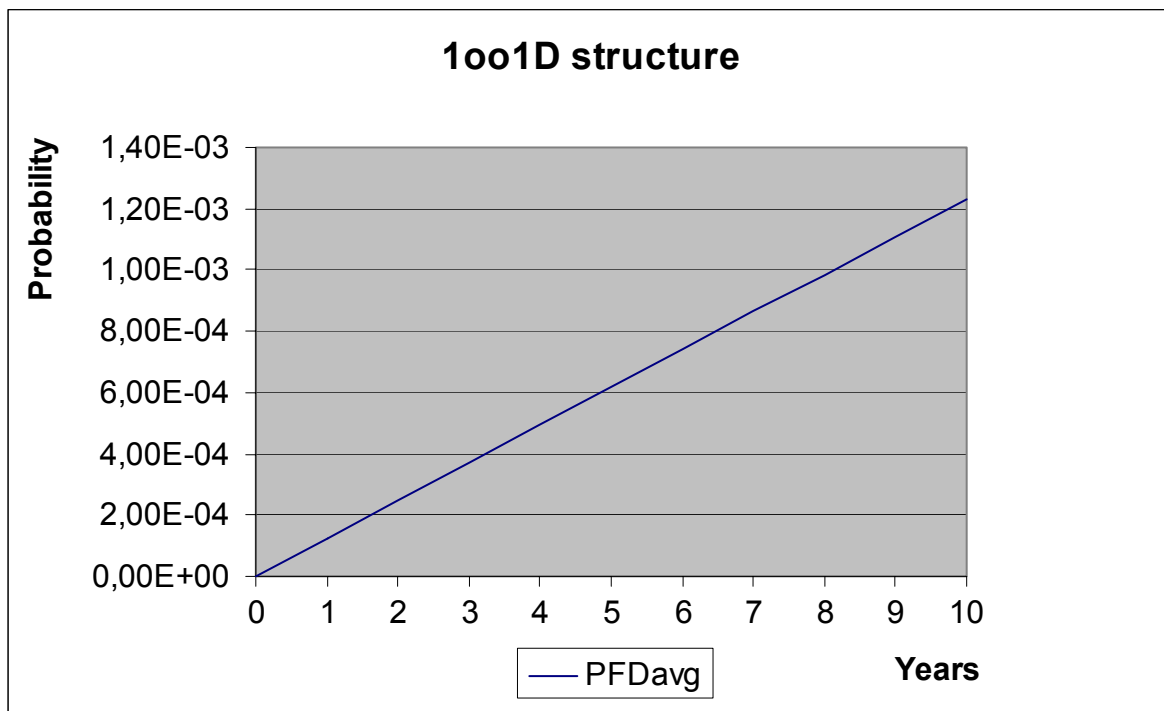


Figure 28:  $\text{PFD}_{\text{AVG}}(t)$  for EG4-OT (normal mode)

### 5.9.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-OT leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 4,30E-08 \text{ 1/h} + 5,82E-08 \text{ 1/h} + 8,26E-09 \text{ 1/h} = 1,09E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 3,91E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,63E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 5,60E-09 \text{ 1/h}$$

$$SFF = 75,99\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,71E-04</math></b>	<b><math>PFD_{AVG} = 8,55E-04</math></b>	<b><math>PFD_{AVG} = 1,71E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 29 shows the time dependent curve of  $PFD_{AVG}$ .

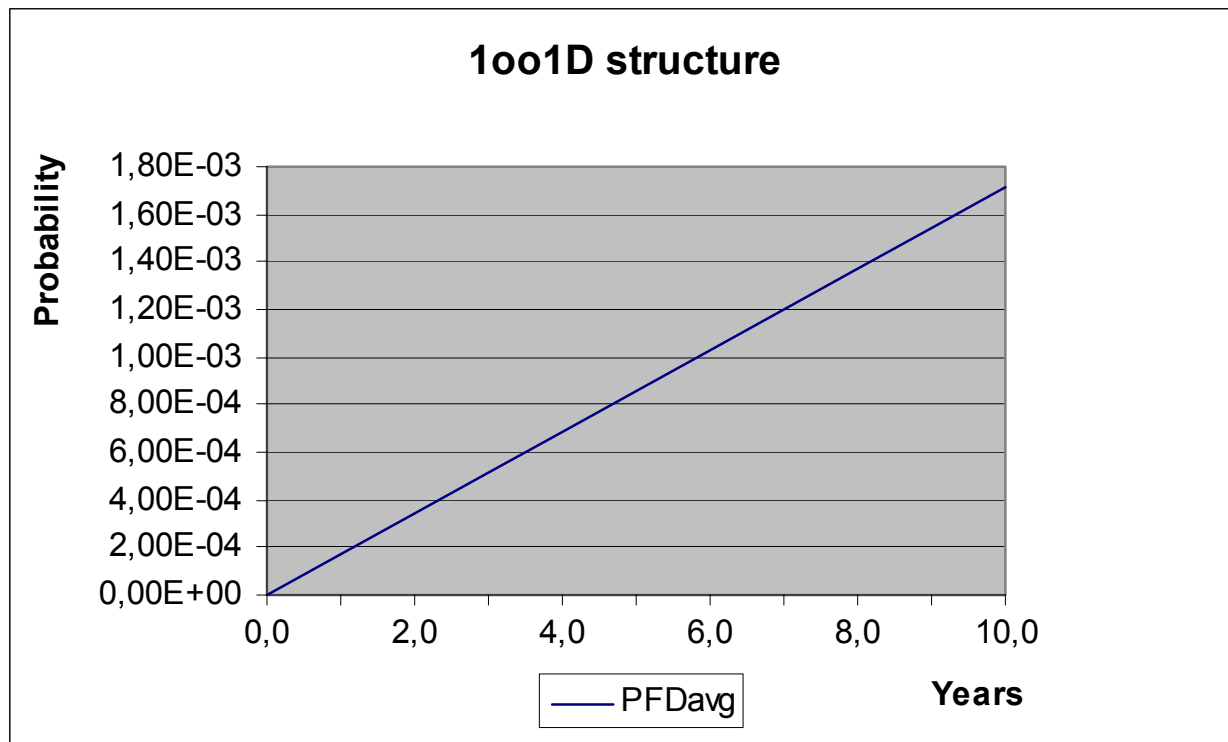


Figure 29:  $PFD_{AVG}(t)$  for EG4-OT (inverse mode)



## 5.10 EG4-OTLK

### 5.10.1 Normal mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-OTLK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 5,43E-08 \text{ 1/h} + 6,22E-08 \text{ 1/h} + 6,64E-09 \text{ 1/h} = 1,23E-07 \text{ 1/h}$$

$$\lambda_{dd} = 1,44E-08 \text{ 1/h}$$

$$\lambda_{du} = 2,94E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,67E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 1,32E-08 \text{ 1/h}$$

$$SFF = 82,40\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
$PFD_{AVG} = 1,29E-04$	$PFD_{AVG} = 6,43E-04$	$PFD_{AVG} = 1,29E-03$

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 30 shows the time dependent curve of  $PFD_{AVG}$ .

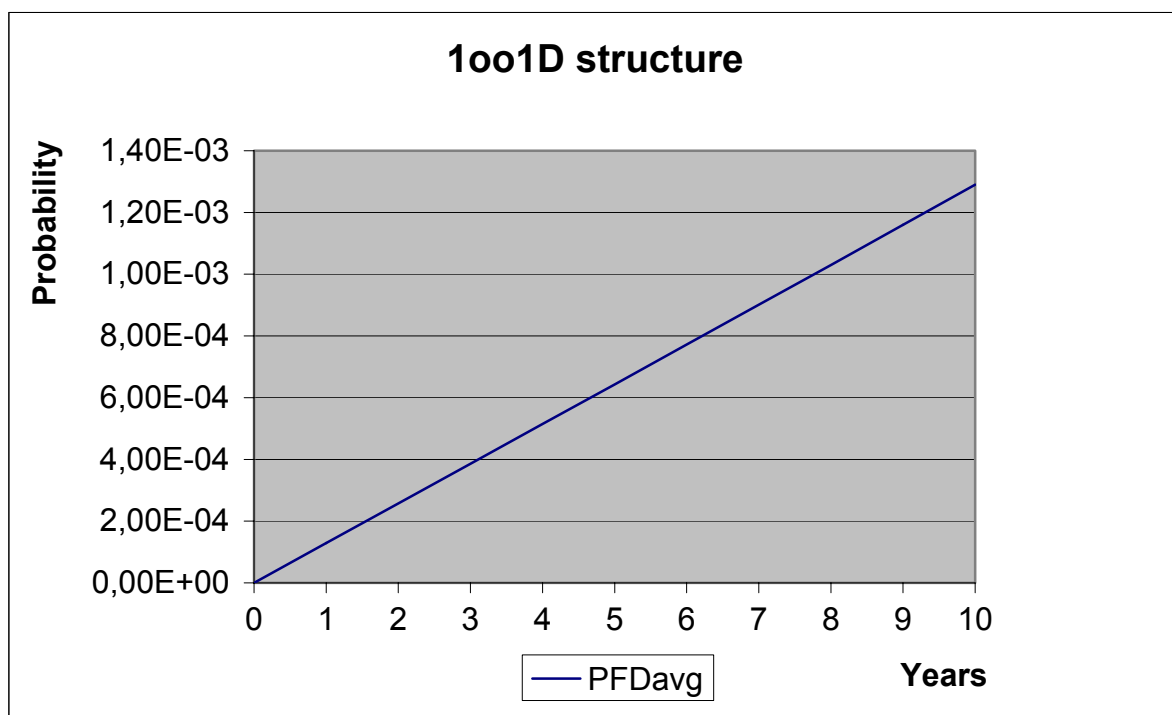


Figure 30:  $PFD_{AVG}(t)$  for EG4-OTLK (normal mode)

### 5.10.2 Inverse mode

The FMEDA carried out on the Transformer Isolated Amplifier EG4-OTLK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$$\lambda_{sd} = 1,43E-08 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{no \text{ effect}} + \lambda_{annunciation} = 4,25E-08 \text{ 1/h} + 6,18E-08 \text{ 1/h} + 6,64E-09 \text{ 1/h} = 1,11E-07 \text{ 1/h}$$

$$\lambda_{dd} = 0,00E-00 \text{ 1/h}$$

$$\lambda_{du} = 4,14E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,67E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 1,36E-08 \text{ 1/h}$$

$$SFF = 75,17\%$$

The  $PFD_{AVG}$  for the transformer isolated amplifier was calculated for three different proof test times using the Markov model as described in Figure 11.

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
<b><math>PFD_{AVG} = 1,81E-04</math></b>	<b><math>PFD_{AVG} = 9,05E-04</math></b>	<b><math>PFD_{AVG} = 1,81E-03</math></b>

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  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  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . Figure 31 shows the time dependent curve of  $PFD_{AVG}$ .

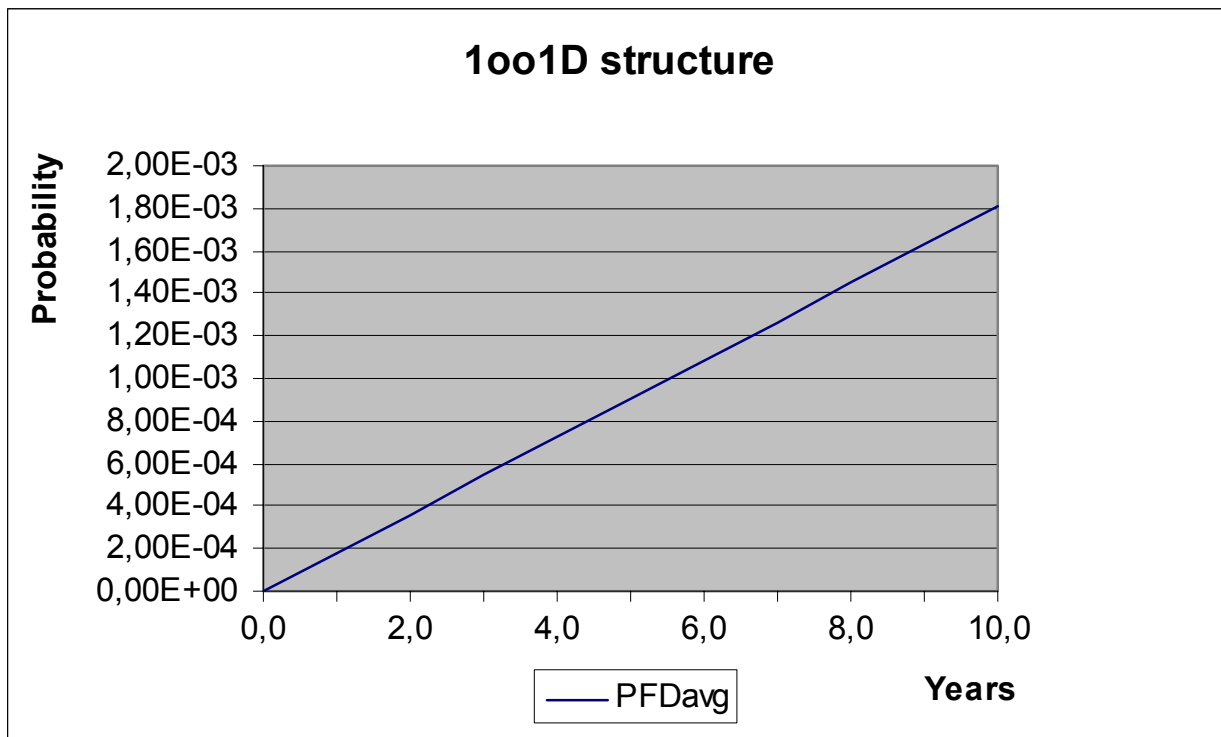


Figure 31:  $PFD_{AVG}(t)$  for EG4-OTLK (inverse mode)

## 6 Proven-in-use Assessment

### 6.1 Definition of the term “Proven-in-use” according to IEC 61508

**Reference:** IEC 61508-7; B.5.4

**Aim:** To use field experience from different applications to prove that the safety-related system will work according to its specification.

**Description:** Use of components or subsystems, which have been shown by experience to have no, or only unimportant, faults when used, essentially unchanged, over a sufficient period of time in numerous different applications.

For proven by use to apply, the following requirements must have been fulfilled:

- unchanged specification;
- 10 systems in different applications;
- 10<sup>5</sup> operating hours and at least 1 year of service history.

The proof is given through documentation of the vendor and/or operating company. This documentation must contain at least the:

- exact designation of the system and its component, including version control for hardware;
- users and time of application;
- operating hours;
- procedures for the selection of the systems and applications procured to the proof;
- procedures for fault detection and fault registration as well as fault removal.

### 6.2 “Prior-use” requirements according to IEC 61511-1

According to IEC 61511-1 First Edition 2003-01 section 11.4.4 for all subsystems (e.g., sensor, final elements and non-PE logic solvers) except PE logic solvers the minimum fault tolerance specified in Table 6 of this standard may be reduced by one if the devices under consideration comply with all of the following:

- the hardware of the device is selected on the basis of prior use (see 11.5.3)
- 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 6 of IEC 61511-1 First Edition 2003-01**  
**(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 First Edition 2003-01 are fulfilled a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems with a SFF of 60% to < 90%<sup>2</sup>.

This is identical to the requirements on Type A (sub)-systems. The Transformer Isolated Amplifiers EG\*-\*\* have been developed before IEC 61508 was published, however, and so IEC 61511-1 First Edition 2003-01 section 11.4.4 is used as a basis for arguing that proven-in-use shows the unlikelihood of systematic failures.

The assessment of the Transformer Isolated Amplifiers EG\*-\*\* has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

---

<sup>2</sup> IEC 61511-1 First Edition 2003-01 explicitly says "...provided that the dominant failure mode is to the safe state or dangerous failures are detected...".

Requirement	Argumentation <sup>3</sup>
See Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01	<ol style="list-style-type: none"> <li>1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 7 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail<sup>4</sup> is low (&lt; 1.5%).</li> <li>2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D14] to [D17]. The assessed sub-system are clearly identified and specified (see Table 1). The field feedback tracking database of Pepperl+Fuchs GmbH together with the explanations given in [D18] demonstrated the performance of the sub-system in similar operating profiles and physical environments and the operating experience (Operating experience of more than 1.000.000.000 operating hours exists. This is considered to be sufficient taking into account the low complexity of the sub-system and the use in SIL 2 safety functions only).</li> <li>3. 11.5.2 is under the responsibility of the manufacturer → no argumentation. 11.5.3 see bullet items before.</li> <li>4. The override function shall be disabled.</li> <li>5. Under the responsibility of the manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D18].</li> </ol>
Adjustment of process-related parameters only	N/A
Adjustment of process-related parameters is protected	N/A
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Transformer Isolated Amplifiers EG\*-\*\* with a SFF of 60% - < 90% and HFT = 0 can be considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

<sup>3</sup> The numbering is based on the requirements detailed in appendix 1.

<sup>4</sup> The probability of failure is the percentage of all returned devices of the EG\*-\*\* family to all sold devices of the EG\*-\*\* family based on the assumption that all returned devices from the field failed.

## 7 Terms and Definitions

FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
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
SIS	Safety Instrumented System
Type A component	“Non-complex” component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2
T[Proof]	Proof Test Interval

## 8 Status of the document

### 8.1 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.

### 8.2 Releases

Version: V2

Revision: R1.0

Version History: V0, R1.0: Initial version; May 15, 2003

V0, R1.1: Review comments integrated; June 26, 2003

V1, R1.0: First official release; July 1, 2003

V2, R1.0: Additional safety function added, layout of report modified;  
March 27, 2006

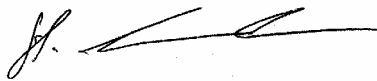
Authors: Stephan Aschenbrenner

Review: V0, R1.0 reviewed by P+F; June 18, 2003

V0, R1.1 reviewed by Rachel van Beurden-Amkreutz (*exida*); June 30, 2003

Release status: Released to Pepperl+Fuchs

### 8.3 Release Signatures



---

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



---

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

## **Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01**

### **Appendix 1.1 Section 11.5.3 of IEC 61511-1 First Edition 2003-01**

#### **(Requirements for the selection of components and subsystems based on prior use)**

1. An assessment shall provide appropriate evidence that the components and sub-systems are suitable for use in the safety instrumented system.
2. The evidence of suitability shall include the following:
  - consideration of the manufacturer's quality management and configuration management systems;
  - adequate identification and specification of the components or sub-systems;
  - demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments;
  - the volume of the operating experience.

### **Appendix 1.2 Section 11.5.4 of IEC 61511-1 First Edition 2003-01**

#### **(Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use)**

3. The requirements of 11.5.2 and 11.5.3 apply.
4. Unused features of the components and sub-systems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.
5. For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider:
  - characteristics of input and output signals;
  - modes of use;
  - functions and configurations used;
  - previous use in similar applications and physical environments.

### **Appendix 1.3 Section 11.5.2 of IEC 61511-1 First Edition 2003-01**

#### **(General Requirements)**

6. Components and sub-systems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with sub-clauses 11.4 and 11.5.3 to 11.5.6, as appropriate.





7. Components and sub-systems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.
8. The suitability of the selected components and sub-systems shall be demonstrated, through consideration of:
  - manufacturer hardware and embedded software documentation;
  - if applicable, appropriate application language and tool selection (see clause 12.4.4).
9. The components and sub-systems shall be consistent with the SIS safety requirements specifications.

## Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 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.

Table 6 shows an importance analysis of the critical dangerous undetected faults of EG2-R (normal mode) and indicates how these faults can be detected during proof testing.

**Table 6: Importance Analysis of dangerous undetected faults**

Component	% of total $\lambda_{du}$	Detection through
P7	53%	100% functional test
IC1	13%	100% functional test
IC2	9%	100% functional test
P1	9%	100% functional test
D1	7%	100% functional test
K2	3%	100% functional test
Other components	< 1%	100% functional test

The other devices behave in a similar way, however, the component names might be different. A 100% functional test is also necessary for the remaining amplifiers to detect undetected failures during proof testing.

### Appendix 3: Impact of lifetime of critical components on the failure rate

According to section 7.4.7.4 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 4.2.3) this only applies provided that the useful lifetime<sup>5</sup> of components is not exceeded. Beyond their useful lifetime (i.e. as the probability of failure significantly increases with time) the results of the probabilistic calculation method is therefore meaningless. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte 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<sub>AVG</sub> 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.

Table 7 shows which electrolytic capacitors are contributing to the dangerous undetected failure rates and what their estimated useful lifetime is.

**Table 7: Useful lifetime of electrolytic capacitors contributing to  $\lambda_{du}$**

Type	Name	Schematic	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	K1.1	1-2207 C	Appr. 500 000 hours
	K2	1-1667 B; 1-1684 E	
	K2.1	1-2208 B; 1-2209 C	
	K5	1-2539 A; 1-1692 D; 1-1696 D	

As there are no aluminium electrolytic capacitors used the only limiting factor is the Tantalum electrolytic capacitor with regard to the useful lifetime of the system, which however, has a useful lifetime of about 57 years.

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

<sup>5</sup> 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.