exida.com

excellence in dependable automation

FMEDA including SFF determination and PFD calculation

Project:

Solenoid Drivers
K*D2-S*-Ex1(.P).** and KFD2-SL2-Ex*.**

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 01/11-10
Report No.: P+F 01/11-10 R004

Version V1, Revision R1.1, November 2002

Stephan Aschenbrenner

CONFIDENTIAL INFORMATION

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management summary

This report summarizes the results of the FMEDAs carried out on the solenoid drivers K*D2-S*-Ex1(.P).** and KFD2-SL2-Ex*.** ‘*’ and ‘**’ stand for the different versions that are available. Table 1 and 2 give an overview and explain the differences.

Table 1: Version overview of the K*D2-S*-Ex1(.P). modules**

K	*	D2	-S	*	-Ex1	(.P)	.**	
	H							Srew Terminals
	F							Plug-in Terminals
				D				Without Logic Input
				L				With Logic Input
						.P		With Power Rail Option
							.17	Output voltage 17.2V
							.36	Output voltage 25.9V
							.48 (90A)[1]	Output voltage 25.2V

Table 2: Version overview of the KFD2-SL2-Ex*. modules**

Type	Channels	Output	Description[2]
KFD2-SL2-EX1	1	without relay	with fault detection for short circuit and lead breakage
KFD2-SL2-EX1.B	1	without relay	without fault detection
KFD2-SL2-EX1.LK	1	with additional relay for fault detection	with fault detection for short circuit and lead breakage
KFD2-SL2-EX2	2	without relay	with fault detection for short circuit and lead breakage
KFD2-SL2-EX2.B	2	without relay	without fault detection

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

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be 10^{-4} to < 10^{-3} for SIL 3 safety functions and 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^{-4} for SIL 3 and better than or equal to 10^{-3} for SIL 2.

The modules under evaluation can be considered to be Type A components.

For **Type A** components the SFF has to between 90% and 99% for SIL 3 (sub-) systems and between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

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

[1] (90A): 45 mA output current instead of 35 mA.

[2] These additional features are not part of the safety function and therefore not considered in the calculations.

Table 3: Summary of all considered modules with regard to SIL 3 requirements

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
KFD2-SD-Ex1.17	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	100 %
KFD2-SL-Ex1.17	**PFD_{AVG} = 6.03E-05**	**PFD_{AVG} = 1.21E-04**	**PFD_{AVG} = 3.01E-04**	> 95 %
KFD2-SD-Ex1.36	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	100 %
KFD2-SL-Ex1.36	**PFD_{AVG} = 5.44E-05**	**PFD_{AVG} = 1.09E-04**	**PFD_{AVG} = 2.72E-04**	> 96 %
KFD2-SD-Ex1.48 (90A)	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	100 %
KFD2-SL-Ex1.48 (90A)	**PFD_{AVG} = 6.03E-05**	**PFD_{AVG} = 1.21E-04**	**PFD_{AVG} = 3.01E-04**	> 95 %
KFD2-SL2-Ex*.**[3]	**PFD_{AVG} = 2.04E-04**	**PFD_{AVG} = 4.09E-04**	**PFD_{AVG} = 1.02E-03**	> 93 %

The boxes marked in yellow (🟨) mean that the calculated PFD values are within the allowed range for SIL 3 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^{-4}. The boxes marked in green (🟩) mean that the calculated PFD values fulfill this requirement to be better than 10^{-4}. The boxes marked in red (🟥) mean that the calculated PFD values do not fulfill the requirements for SIL 3 according to table 2 of IEC 61508-1.

Table 4: Summary of all considered modules with regard to SIL 2 requirements

Name	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
KFD2-SD-Ex1.17	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	100 %
KFD2-SL-Ex1.17	**PFD_{AVG} = 6.03E-05**	**PFD_{AVG} = 1.21E-04**	**PFD_{AVG} = 3.01E-04**	> 95 %
KFD2-SD-Ex1.36	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	100 %
KFD2-SL-Ex1.36	**PFD_{AVG} = 5.44E-05**	**PFD_{AVG} = 1.09E-04**	**PFD_{AVG} = 2.72E-04**	> 96 %
KFD2-SD-Ex1.48 (90A)	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	**PFD_{AVG} = 0.00E+00**	100 %
KFD2-SL-Ex1.48 (90A)	**PFD_{AVG} = 6.03E-05**	**PFD_{AVG} = 1.21E-04**	**PFD_{AVG} = 3.01E-04**	> 95 %
KFD2-SL2-Ex*.**[3]	**PFD_{AVG} = 2.04E-04**	**PFD_{AVG} = 4.09E-04**	**PFD_{AVG} = 1.02E-03**	> 93 %

The boxes marked in yellow (🟨) mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 10^{-3}. The boxes marked in green (🟩) mean that the calculated PFD values fulfill this requirement to be better than 10^{-3}.

A user of the Pepperl+Fuchs solenoid drivers can utilize the failure rates given in sections 5.1 to 5.7 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 two channels on the KFD2-SL2-Ex2.** modules should not be used for one safety function as they contain common components.

[3] The results are based on the FMEDA carried out on the “one channel” version but are considered to be also valid for the “two channel” version as also for the “two channel” version only one channel is considered with regard to a safety function.

Table of Contents

Management summary 2
1 Purpose and Scope 5
2 Project management 5
2.1 Roles of the parties involved 5
2.2 Standards / Literature used 5
2.3 Reference documents 6
2.3.1 Documentation provided by the customer 6
2.3.2 Documentation generated by *exida.com* 6
3 Description of the analyzed modules 7
3.1 KFD2-SD-Ex1.** 7
3.2 KFD2-SL-Ex1.** 7
3.3 KFD2-SL2-Ex1.** 8
4 Failure Modes, Effects, and Diagnostics Analysis 9
4.1 Description of the failure categories 9
4.2 Methodology – FMEDA, Failure rates 9
4.2.1 FMEDA 9
4.2.2 Failure rates 9
4.2.3 Assumption 10
5 Results of the assessment 10
5.1 KFD2-SD-Ex1.17 15
5.2 KFD2-SL-Ex1.17 16
5.3 KFD2-SD-Ex1.36 17
5.4 KFD2-SL-Ex1.36 18
5.5 KFD2-SD-Ex1.48 19
5.6 KFD2-SL-Ex1.48 20
5.7 KFD2-SL2-Ex1 21
6 Terms and Definitions 22
7 Status of the document 22
7.1 Releases 22

1 Purpose and Scope

This report shall describe the results of the FMEDAs carried out on the solenoid drivers K*D2-S*-Ex1(.P).** and KFD2-SL2-Ex*.**. '*' and '**' stand for the different versions that are available. Table 1 and 2 give an overview and explain the differences.

It shall be assessed whether these modules meet the Probability of Failure on Demand (PFD) requirements for SIL 3 sub-systems according to IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

Pepperl+Fuchs GmbH contracted *exida.com* in December 2001 with the FMEDA and PFD calculation of the above mentioned modules.

2 Project management

2.1 Roles of the parties involved

Pepperl+Fuchs	Manufacturer of the solenoid drivers.
exida.com	Did the FMEDAs together with the determination of the Safe Failure Fraction (SFF) and calculated the Probability of Failure on Demand (PFD) using Markov models.

2.2 Standards / Literature used

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

N1	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2		Electronic Components: Selection and Application Guidelines by Victor Meeldijk John Wiley & Sons; ISBN: 0471133019
N3		Failure Mode / Mechanism Distributions FMD-91, RAC 1991
N4	SN 29500	Failure rates of components

2.3 Reference documents

2.3.1 Documentation provided by the customer

[D1]	251-0328B of 29.06.01	Circuit diagram for KFD2-SD-Ex1.17
[D2]	251-0330B of 29.06.01	Circuit diagram for KFD2-SL-Ex1.17
[D3]	251-0334B of 29.06.01	Circuit diagram for KFD2-SD-Ex1.48
[D4]	251-0335B of 29.06.01	Circuit diagram for KFD2-SL-Ex1.48
[D5]	252-1187G	Bill of material for the above mentioned units
[D6]	251-0440A of 16.11.00	Circuit diagram for KFD2-SD-Ex1.36
[D6.1]	252-1042F	Bill of material for KFD2-SD-Ex1.36
[D7]	251-0442A of 16.11.00	Circuit diagram for KFD2-SL-Ex1.36
[D7.1]	252-1043G	Bill of material for KFD2-SL-Ex1.36
[D8]	51-0621 Ind. A of 22.02.00	Circuit diagram for KFD2-SL2-Ex1
[D8.1]	098078	Bill of material for KFD2-SL2-Ex1

2.3.2 Documentation generated by *exida.com*

R1	FMEDA KFD2-SD-Ex1.17 V1 R1.0 – Results of 05.02.02
R2	FMEDA KFD2-SD-Ex1.17 V1 R1.0 – Analysis of 05.02.02
R3	FMEDA KFD2-SL-Ex1.17 V1 R1.0 – Results of 05.02.02
R4	FMEDA KFD2-SL-Ex1.17 V1 R1.0 – Analysis of 05.02.02
R5	FMEDA KFD2-SD-Ex1.36 V1 R1.0 – Results of 05.02.02
R6	FMEDA KFD2-SD-Ex1.36 V1 R1.0 – Analysis of 05.02.02
R7	FMEDA KFD2-SL-Ex1.36 V1 R1.0 – Results of 05.02.02
R8	FMEDA KFD2-SL-Ex1.36 V1 R1.0 – Analysis of 05.02.02
R9	FMEDA KFD2-SD-Ex1.48 V1 R1.0 – Results of 05.02.02
R10	FMEDA KFD2-SD-Ex1.48 V1 R1.0 – Analysis of 05.02.02
R11	FMEDA KFD2-SL-Ex1.48 V1 R1.0 – Results of 05.02.02
R12	FMEDA KFD2-SL-Ex1.48 V1 R1.0 – Analysis of 05.02.02
R13	FMEDA KFD2-SL2-Ex1 V1 R1.0 – Results of 05.02.02
R14	FMEDA KFD2-SL2-Ex1 V1 R1.0 – Analysis of 05.02.02

3 Description of the analyzed modules

3.1 KFD2-SD-Ex1.**

The KFD2-SD-Ex1.** transformer isolated solenoid driver/power supply is a 4 terminal device which may be used to power a load in a hazardous area. The unit can be used to drive either certified intrinsically safe equipment or "simple apparatus".

The schematic circuit helps to show how the unit operates. The DC/DC converter is powered from terminals 7 and 8.

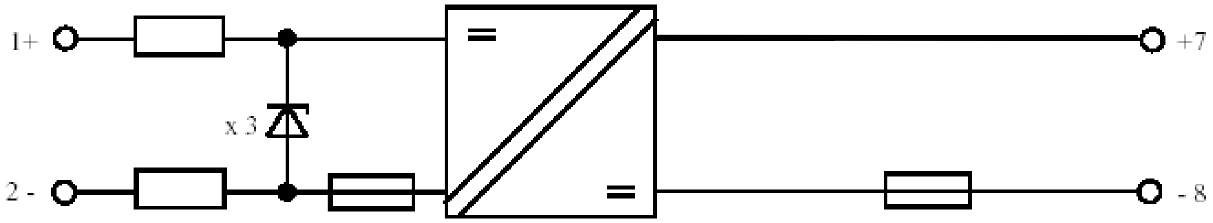


Figure 1: Block diagram of K*D2-SD-Ex1.**

3.2 KFD2-SL-Ex1.**

The KFD2-SL-Ex1.** transformer isolated solenoid driver/power supply is a 6 terminal device which may be used to power a load in a hazardous area and which can be controlled (on or off) by a signal from a low voltage logic circuit.

The unit can be used to drive either certified intrinsically safe equipment or "simple apparatus".

The schematic circuit helps to show how the unit operates. The DC/DC converter is powered from terminals 11 and 12 (or from the power-rail terminals).

When no voltage is applied to logic terminals 7 and 8 the DC/DC converter is disabled. When a suitable voltage is applied to terminals 7 and 8 OPT1 switches on and enables the DC/DC converter.

Terminals 7 and 8 may be connected into a logic circuit, or computer output, or may be switched by a relay. They are completely isolated from the power supply terminals but may be linked to them if required, e.g. 7 and 11 might be connected together and 8 switched to 12 for control purposes.

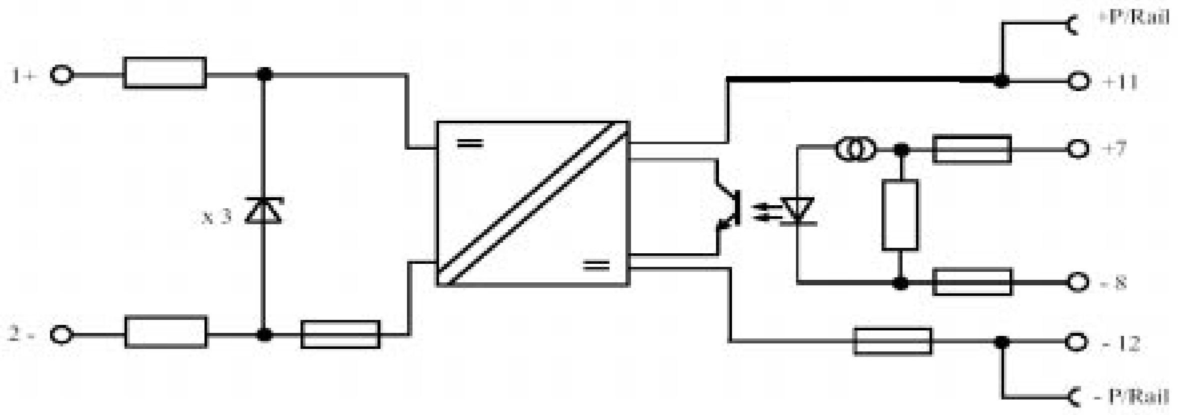


Figure 2: Block diagram of K*D2-SL-Ex1.**

3.3 KFD2-SL2-Ex1.**

The KFD2-SL2-Ex1.** solenoid driver supplies and switches the intrinsically safe field device (valve) in hazardous areas.

The device has a logic input that is isolated from the power supply.

The field devices are controlled by means of these logic inputs.

Voltage signals in a range of DC 16 V .... 30 V are accepted as 1-signals. The 0-signal must be within a range of DC 0 V... 5 V.

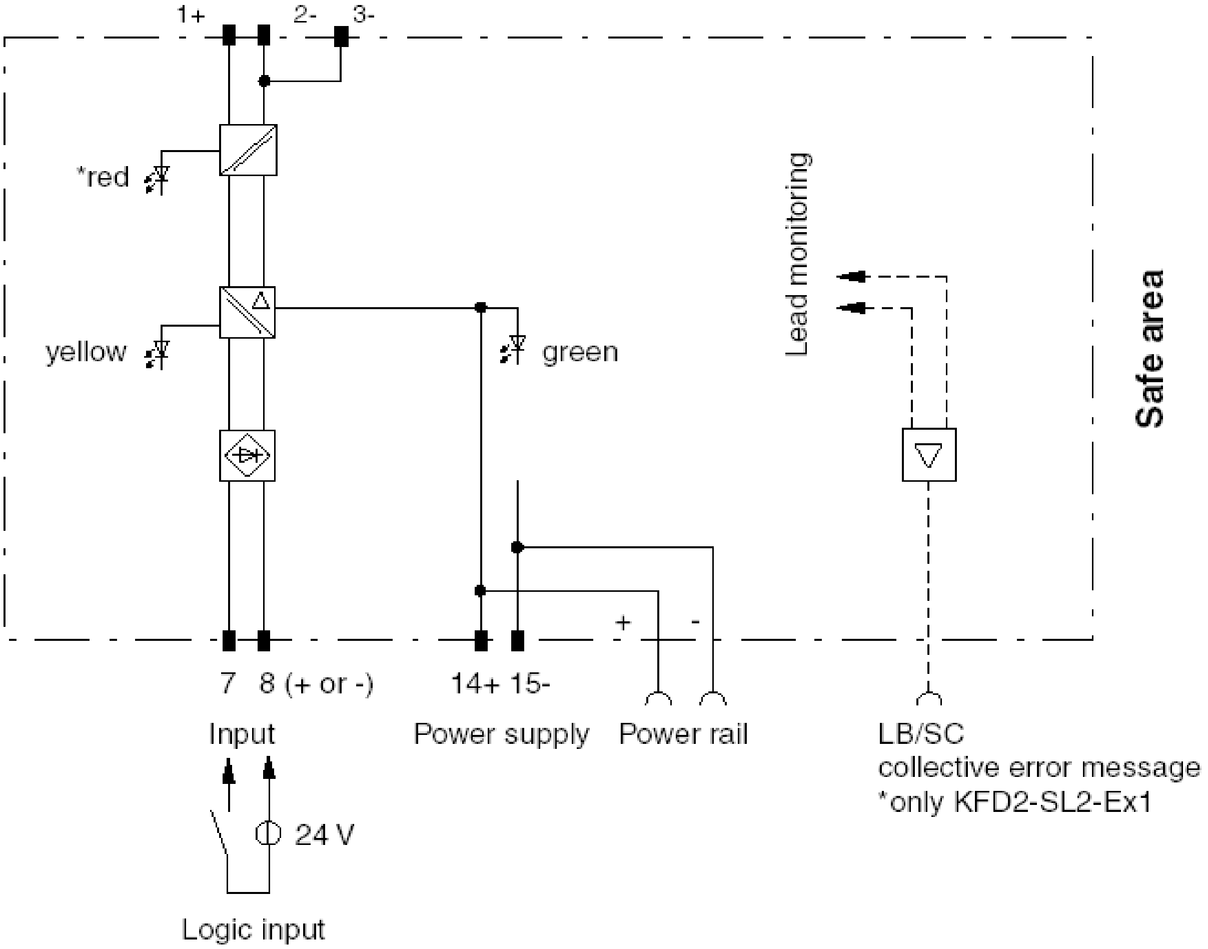


Figure 3: Block diagram of KFD2-SL2-Ex1.**

Remark: The description above is valid accordingly for the KFD2-SL2-Ex2.** version with the exception that this version has two output channels.

4 Failure Modes, Effects, and Diagnostics Analysis

4.1 Description of the failure categories

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

Failures are categorized and defined as follows:

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

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

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

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

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

The failure rate data used by *exida.com* in this FMEDA are from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. It is expected that actual field failure results with average environmental stress will be superior to the results predicted by these numbers.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data is preferable to general industry average data. Industrial plant sites with high levels of stress must use failure rate data that is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumption

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

Failure rates are constant, wear out mechanisms are not included.

Propagation of failures is not relevant.

All component failure modes are known.

The repair time after a safe failure is 8 hours.

The average temperature over a long period of time is 40°C.

The stress levels are average for an industrial environment.

All modules are operated in the low demand mode of operation.

5 Results of the assessment

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

The two channels on the KFD2-SL2-Ex2.** modules should 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:

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

$_{\text{total}} = {}_{\text{safe}} + {}_{\text{dangerous}} + {}_{\text{don't care}}$[4] $+ {}_{\text{not considered}}$[5].

SFF = 1 – $_{\text{du}}$[6] / $_{\text{total}}$

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

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

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

[5] This is the failure rate of failure modes that were not considered.

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

For the FMEDAs the following failure modes and below mentioned distributions were used. The gray highlighted failure modes were not considered as this is not required for SIL 3 compliant Type A components with a hardware fault tolerance of 0 (see table A.1 of IEC 61508-2, medium effectiveness). However, they are included in the calculation with the assumption that 50% of these failure modes are safe failures and 50% are dangerous failures.

Resistor

Failure Mode	Distribution (in %)
Short	5
Open	59
Drift	36

Resistor variable

Failure Mode	Distribution (in %)
Short	7
Open	53
Erratic output	40

Resistor wire-wound

Failure Mode	Distribution (in %)
Short	9
Open	65
Parameter change	26

Capacitor ceramic

Failure Mode	Distribution (in %)
Short	49
Open	22
Change in value	29

Capacitor Al-ELKO

Failure Mode	Distribution (in %)
Short	53
Open	35
Electrolyte leak	10
Decrease in capacitance	2

Capacitor Plastic

Failure Mode	Distribution (in %)
Short	40
Open	42
Change in value	18

Fuse

Failure Mode	Distribution (in %)
Fail to open	49
Premature open	8
Slow to open	43

Inductivity

Failure Mode	Distribution (in %)
Short	50
Open	50

Transformer

Failure Mode	Distribution (in %)
Short	42
Open	42
Parameter change	16

Universal Diode

Failure Mode	Distribution (in %)
Short	49
Open	36
Drift	15

Zener Diode (voltage protection)

Failure Mode	Distribution (in %)
Short	20
Open	45
Parameter change	35

Suppressor Diode

Failure Mode	Distribution (in %)
Short	100

Transistor

Failure Mode	Distribution (in %)
Short CE	50
Short CB	10
Short EB	10
Open CE	25
1/10 beta; current gain	5

FET MOS

Failure Mode	Distribution (in %)
Output stuck-at-1	5
Output stuck-at-0	22
Short	51
Open	5
Parameter change	17

Logic CMOS

Failure Mode	Distribution (in %)
Output stuck-at-1	8
Output stuck-at-0	9
Input open	36
Output open	36
Supply open	11

Opto-coupler

Failure Mode	Distribution (in %)
Short	50
Open	50

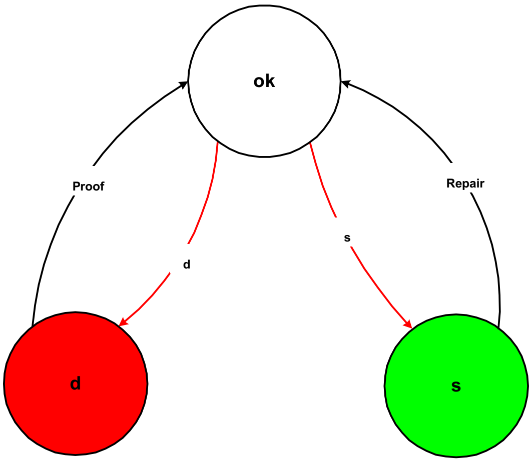
Comparator

Failure Mode	Distribution (in %)
Stuck-at-1	30
Stuck-at-0	30
Short	15
Open	15
Drift	5
Function	5

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} = ${}_{dangerous}$ (1/2 $T_{[Proof]}$ + $T_{[Repair]}$) can be used to calculate the results.

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



Abbreviations:

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

Figure 4: Markov model

5.1 KFD2-SD-Ex1.17

The FMEDA carried out on the KFD2-SD-Ex1.17 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

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

$_{\text{safe}}$ = 1,33E-07 1/h

$_{\text{dangerous}}$ = 0,00E+00 1/h

$_{\text{don't care}}$ = 8,76E-08 1/h

$_{\text{not considered}}$ = 0,00E+00 1/h

SFF = 100,00%

Because no dangerous failures are possible the PFD = 0, which means that the KFD2-SD-Ex1.17 module can be used for all applications.

5.2 KFD2-SL-Ex1.17

The FMEDA carried out on the KFD2-SL-Ex1.17 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$_{\text{total}}$ = 3,11E-07 1/h

$_{\text{safe}}$ = 1,55E-07 1/h

$_{\text{dangerous}}$ = 1,36E-08 1/h

$_{\text{don't care}}$ = 1,42E-07 1/h

$_{\text{not considered}}$ = 3,00E-10 1/h

SFF = 95,58%

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

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD$_{AVG}$ = 6.03E-05	**PFD$_{AVG}$ = 1.21E-04**	**PFD$_{AVG}$ = 3.01E-04**

The boxes marked in yellow (🟨) mean that the calculated PFD values are within the allowed range for SIL 3 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^{-4}. The boxes marked in green (🟩) mean that the calculated PFD values fulfill this requirement to be better than 10^{-4}.

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

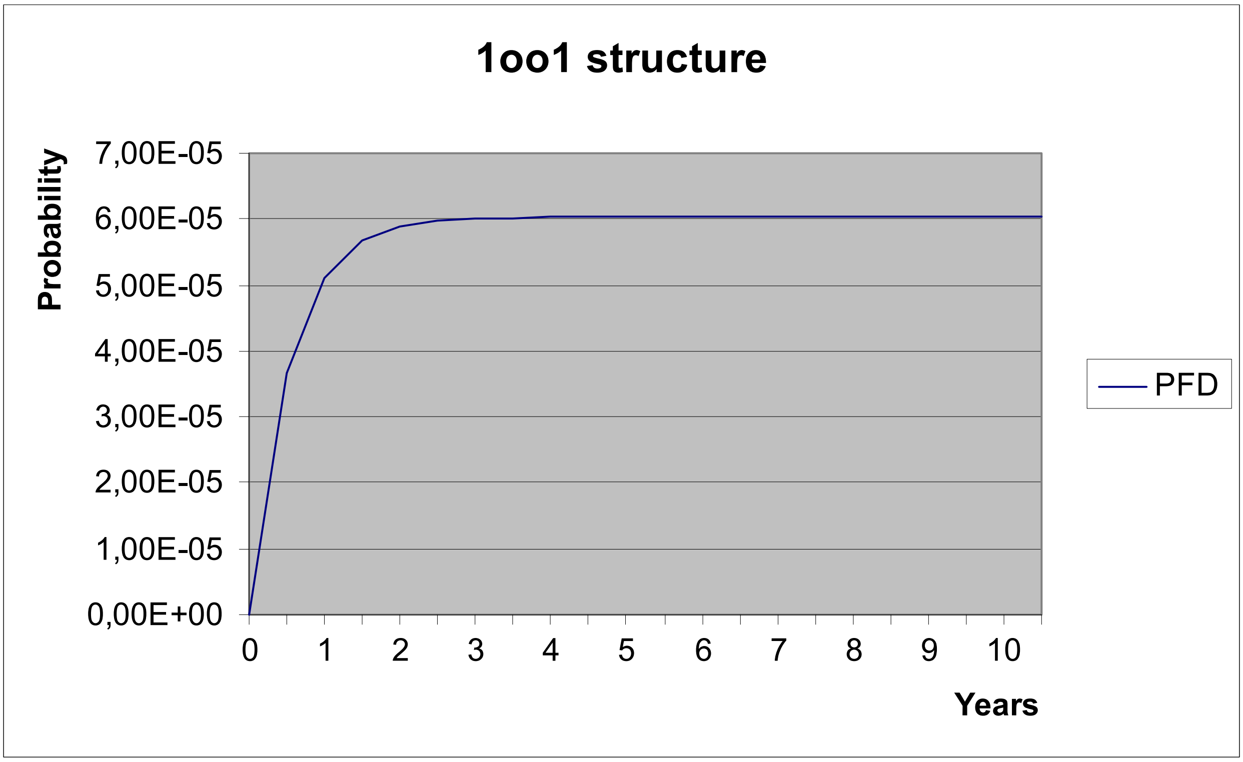


Figure 5: PFD for T[Proof] = 1 year

5.3 KFD2-SD-Ex1.36

The FMEDA carried out on the KFD2-SD-Ex1.36 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$_{\text{total}}$ = 2,15E-07 1/h

$_{\text{safe}}$ = 8,55E-08 1/h

$_{\text{dangerous}}$ = 0,00E+00 1/h

$_{\text{don't care}}$ = 1,30E-07 1/h

$_{\text{not considered}}$ = 0,00E+00 1/h

SFF = 100,00%

Because no dangerous failures are possible the PFD = 0, which means that the KFD2-SD-Ex1.36 module can be used for all applications.

5.4 KFD2-SL-Ex1.36

The FMEDA carried out on the KFD2-SL-Ex1.36 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$_{\text{total}}$ = 3,18E-07 1/h

$_{\text{safe}}$ = 1,16E-07 1/h

$_{\text{dangerous}}$ = 1,23E-08 1/h

$_{\text{don't care}}$ = 1,90E-07 1/h

$_{\text{not considered}}$ = 1,50E-10 1/h

SFF = 96,09%

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

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 5.44E-05	**PFD_{AVG} = 1.09E-04**	**PFD_{AVG} = 2.72E-04**

The boxes marked in yellow (🟨) mean that the calculated PFD values are within the allowed range for SIL 3 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^{-4}. The boxes marked in green (🟩) mean that the calculated PFD values fulfill this requirement to be better than 10^{-4}.

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

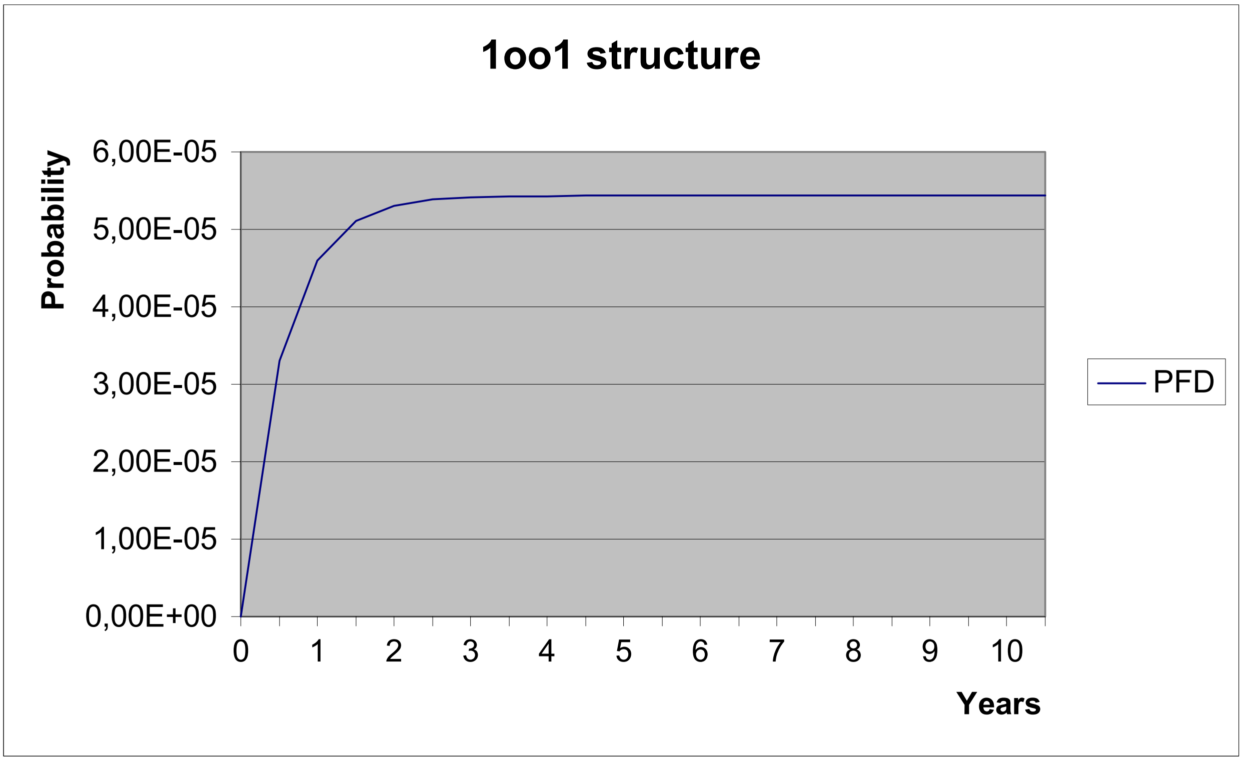


Figure 6: PFD for T[Proof] = 1 year

5.5 KFD2-SD-Ex1.48

The FMEDA carried out on the KFD2-SD-Ex1.48 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

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

$_{\text{safe}}$ = 1,33E-07 1/h

$_{\text{dangerous}}$ = 0,00E+00 1/h

$_{\text{don't care}}$ = 8,76E-08 1/h

$_{\text{not considered}}$ = 0,00E+00 1/h

SFF = 100,00%

Because no dangerous failures are possible the PFD = 0, which means that the KFD2-SD-Ex1.48 module can be used for all applications.

5.6 KFD2-SL-Ex1.48

The FMEDA carried out on the KFD2-SL-Ex1.48 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$_{\text{total}}$ = 2,81E-07 1/h

$_{\text{safe}}$ = 1,27E-07 1/h

$_{\text{dangerous}}$ = 1,36E-08 1/h

$_{\text{don't care}}$ = 1,40E-07 1/h

$_{\text{not considered}}$ = 3,00E-10 1/h

SFF = 95,11%

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

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 6.03E-05	PFD_{AVG} = 1.21E-04	PFD_{AVG} = 3.01E-04

The boxes marked in yellow (🟨) mean that the calculated PFD values are within the allowed range for SIL 3 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^{-4}. The boxes marked in green (🟩) mean that the calculated PFD values fulfill this requirement to be better than 10^{-4}.

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

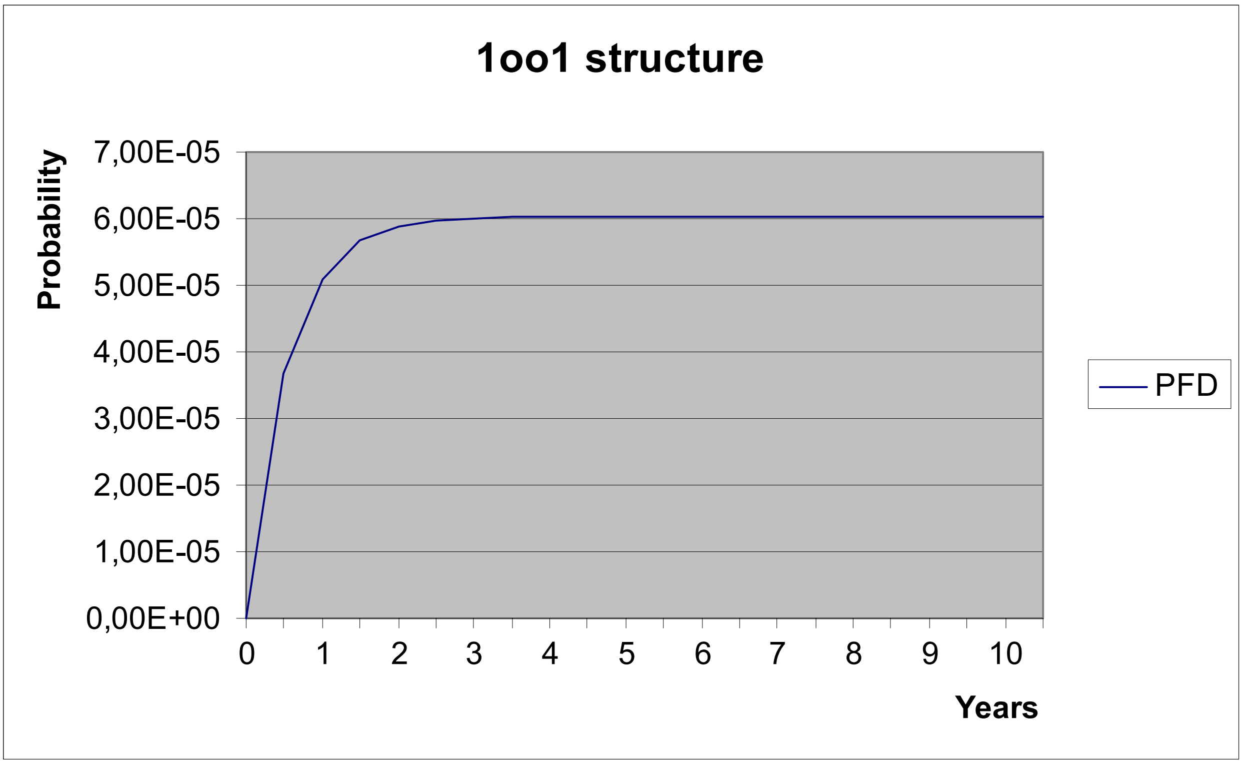


Figure 7: PFD for T[Proof] = 1 year

5.7 KFD2-SL2-Ex1

The FMEDA carried out on the KFD2-SL2-Ex1 module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

$_{\text{total}}$ = 7,02E-07 1/h

$_{\text{safe}}$ = 3,14E-07 1/h

$_{\text{dangerous}}$ = 4,67E-08 1/h

$_{\text{don't care}}$ = 3,42E-07 1/h

$_{\text{not considered}}$ = 0,00E+00 1/h

SFF = 93,35%

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

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 2.04E-04	**PFD_{AVG} = 4.09E-04**	**PFD_{AVG} = 1.02E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD values are within the allowed range for SIL 3 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^{-4}. The boxes marked in red (🟥) mean that the calculated PFD values do not fulfill the requirements for SIL 3 according to table 2 of IEC 61508-1.

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

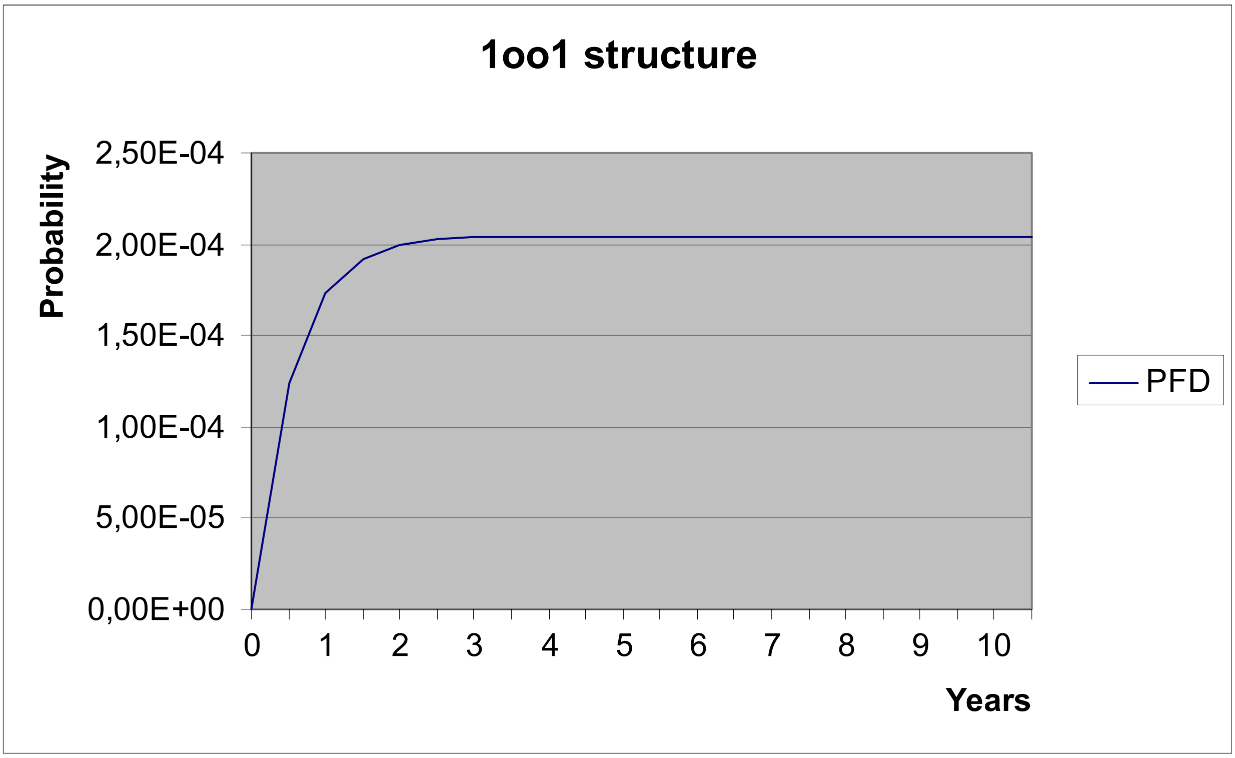


Figure 8: PFD for T[Proof] = 1 year

6 Terms and Definitions

FMEDA	Failure Mode Effect and Diagnostic Analysis
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
total	Total failure rate (overall failure rate of all components)
safe	Failure rate of all safe failures
dangerous	Failure rate of all dangerous failures
du	Failure rate of dangerous undetected failures
PFD	Probability of Failure on Demand
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System

7 Status of the document

7.1 Releases

Version:	V1	
Revision:	R1.1	
Version History:	V0, R1.0:	Initial version, Feb. 5, 2002
	V0, R1.1:	Changes after review by Pepperl+Fuchs, Feb. 8, 2002 Editorial changes Additional table for SIL 2 added Description of the modules corrected
	V1, R1.0:	Changes after second review by Pepperl+Fuchs, Feb. 14, 2002 Editorial changes Separate table for the KFD2-SL2-Ex*.** modules added
	V1, R1.1:	KFD2-SD-Ex1.48 and KFD2-SL-Ex1.48 changed to KFD2-SD-Ex1.48 (90A) and KFD2-SL-Ex1.48 (90A) to include an additional type
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0 reviewed by Pepperl+Fuchs, Feb. 7, 2002	
	V0, R1.1 reviewed by Pepperl+Fuchs, Feb. 12, 2002	
Release status:	Released to Pepperl+Fuchs	