Failure Modes, Effects and Diagnostic Analysis

Project:

Solenoid Drivers
KFD2-SL2-(Ex)1.LK.vvcc
KFD2-SL2-(Ex)*(.B).vvcc

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 06/09-23
Report No.: P+F 06/09-23 R029
Version V2, Revision R3, July 2008

Otto Walch,
Philipp Neumeier

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 FMEDA carried out on the solenoid drivers KFD2-SL2-(Ex)*.**.vvcc[1]. These types are without relays at the output and are equipped with or without fault detection for short circuit and lead breakage.

Table 1: Version overview of the KFD2-SL2-(Ex)*. modules**

Type	Channels	Description[2]
KFD2-SL2-(Ex)1.B	1	without loop monitoring (fault detection for short circuit and lead breakage)
KFD2-SL2-(Ex)1	1	with loop monitoring (fault detection for short circuit and lead breakage)
KFD2-SL2-(Ex)1.LK	1	with loop monitoring and fault signal output (fault detection for short circuit and lead breakage)
KFD2-SL2-(Ex)2.B	2	without loop monitoring (fault detection for short circuit and lead breakage)
KFD2-SL2-(Ex)2	2	with loop monitoring (fault detection for short circuit and lead breakage)

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.

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 module under consideration is only one part of an entire safety function it should not claim more than 10% of this range, i.e. they should be better than or equal to 10^{-3} for SIL 2.

The module under evaluation can be considered to be Type A[3] component.

For **Type A** components the SFF has to be 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 listed SN29500 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 40ºC (25°C ambient temperature plus internal self heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

[1] The term “vvcc” is a placeholder for multiple voltage/current combinations.

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

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

Table 2: Summary of solenoid drivers with regard to SIL 2 requirements

Name	**T[Proof] = 1 year**	**T[Proof] = 2 years**	**T[Proof] = 5 years**	**SFF**	**PFH**
KFD2-SL2-(Ex)1.LK	**PFD$_{AVG}$ = 4.49E-05**	**PFD$_{AVG}$ = 8.98E-05**	**PFD$_{AVG}$ = 2.24E-04**	98 %	10.3 FIT
KFD2-SL2-(Ex)*(.B)	**PFD$_{AVG}$ = 4.25E-05**	**PFD$_{AVG}$ = 8.50E-05**	**PFD$_{AVG}$ = 2.12E-04**	98 %	9.7 FIT

The boxes marked in green (🟩) mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to be better than 10^{-3}.

A user of the Pepperl+Fuchs solenoid drivers can utilize the failure rates given in section 5.1 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-(Ex)2(.B) modules should not be used for one safety function as they contain common components.

Table of Contents

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or 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}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

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

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

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

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

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or 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 provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) equipped with or without fault detection for short circuit and lead breakage.

The information in this report can be used to evaluate whether the solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 Roles of the parties involved

Pepperl+Fuchs	Manufacturer of the solenoid drivers.
exida	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.

Pepperl+Fuchs GmbH contracted *exida* in September 2006 and June 2008 with the FMEDA of the above mentioned module.

2.2 Standards / Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	SN 29500	Failure rates of components
[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]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

2.3 Reference documents

2.3.1 Documentation provided by the customer

[D1]	01-7066 C of 05.09.05	Circuit diagram for KFD-SL2-EX2
[D2]	017937a.pdf	Circuit diagram for KFD2-SL2-(EX)1.LK, date 11.01.2008
[D3]	BOM_200542_SL2_EX1_LK.pdf	Bill of Material KFD2-SL2-(EX)1.LK
[D4]	Changes_Impact_EX1LK_R0V1.pdf	Changes and Impact analysis - Redesign of KFD2-SL2-(EX)1.LK
[D5]	AW KFD2-SL2-(Ex)1.LK SiL Assessment DDE-0870 SP EX2-Version.msg	Email, Jürgen Hochhaus, 26.05.2008
[D6]	Auszug FMEDA KFD2-SL2-(EX)1-LK V0 R1_kom.xls	FMEDA extract for review/failure effect clarification by P+F

[D7]	Block_SL2_Ex2.doc	Block diagrams KFD2-SL2-(Ex)2*
[D8]	Block_SL2_Ex1_LK.doc	Block diagram KFD2-SL2-(Ex)1.LK

2.3.2 Documentation generated by *exida*

[R1]	FMEDA KFD2-SL2-EX2 V2 R4.0 of October 01, 2007
[R2]	FMEDA V6 KFD2-SL2-EX1-LK V0R3.xls of July 3, 2008

3 Description of the analyzed modules

The KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) solenoid drivers supply and switch the intrinsically safe field devices (valves) in hazardous areas.

The devices have 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.

3.1 KFD2-SL2-(Ex)1.LK

The solenoid driver KFD2-SL2-(Ex)1.LK has an additional fault signal output.

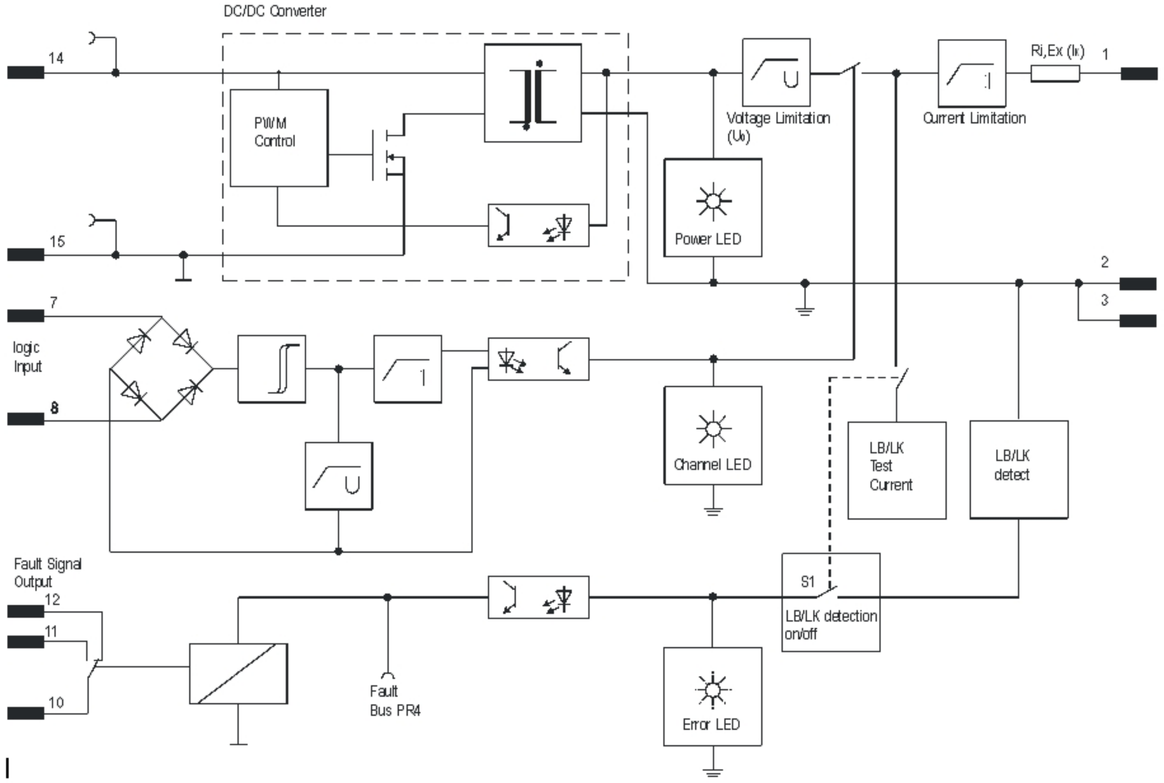


Figure 1: Block diagram of KFD2-SL2-(Ex)1.LK

3.2 KFD2-SL2-(Ex)*(.B)

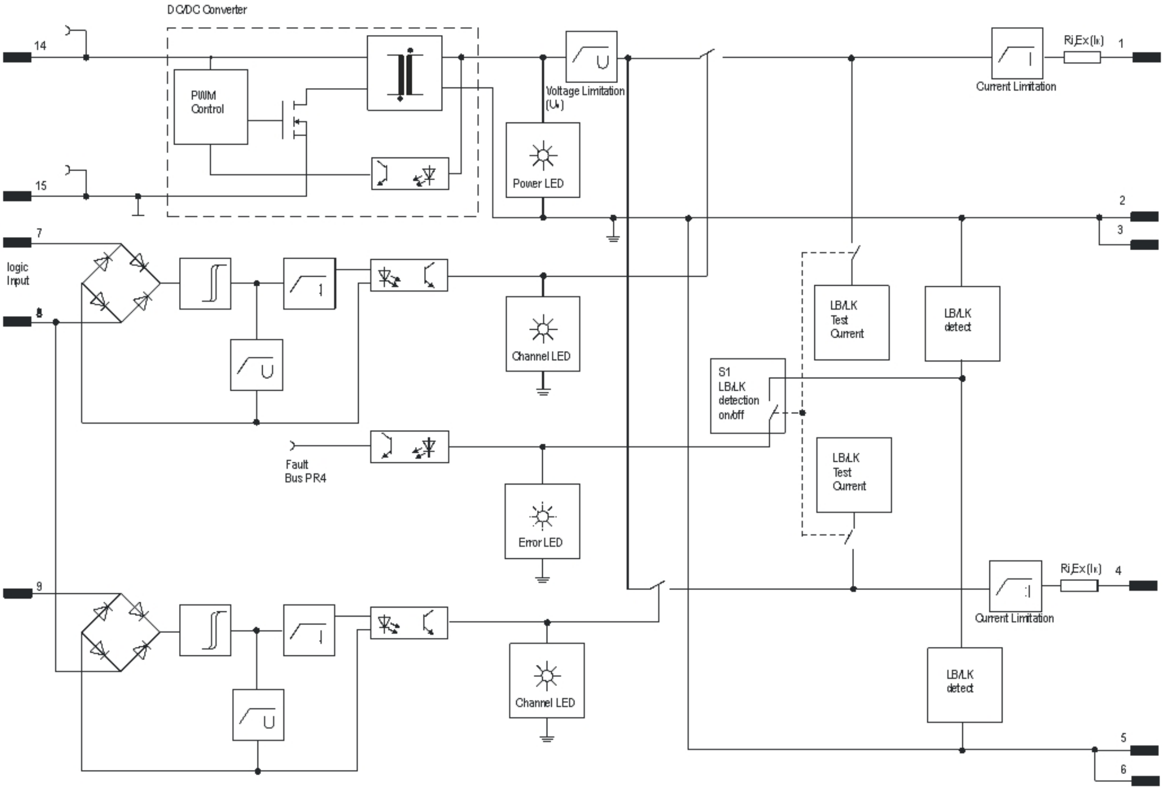


Figure 2: Block diagram of KFD2-SL2-(Ex)2(.B)

4 Failure Modes, Effects, and Diagnostics Analysis

4.1 Description of the failure categories

In order to judge the failure behavior of the solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B), the following definitions for the failure of the product were considered.

Fail-Safe State
The fail-safe state is defined as the output being de-energized.

Fail Dangerous
Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

Fail Dangerous Undetected
Failure that is dangerous and that is not being diagnosed by internal diagnostics.

Fail Dangerous Detected
Failure that is dangerous but is detected by internal diagnostics and signalized via the fault relay (These failures may be converted to the selected fail-safe state).

Residual
Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. For the calculation of the SFF it is treated like a safe undetected failure.

No part
Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The “Residual” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. The “Residual” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the 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, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the solenoid driver KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B).

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Complete practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The time to restoration after a safe failure is 8 hours.
- External power supply failure rates are not included.
- The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment 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 (25°C ambient temperature plus internal self heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed. Humidity levels are assumed within manufacturer’s rating.
- Only the described versions are used for safety applications.

5 Results of the assessment

exida did the FMEDAs together with Pepperl+Fuchs.

The two channels on the KFD2-SL2-(Ex)*(.B) 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:

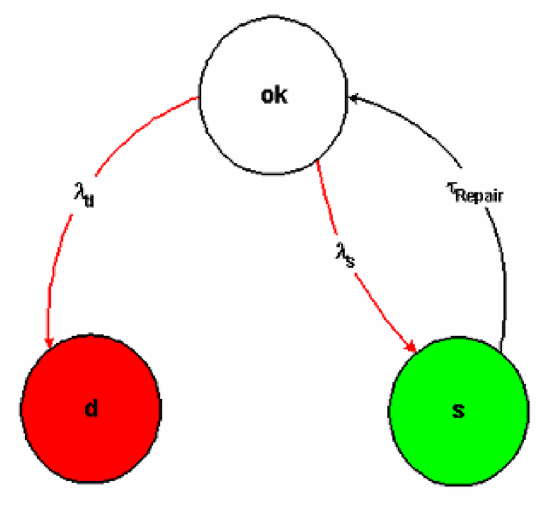
λ_{total} consists of the sum of all component failure rates. This means:

$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{residual}$

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

For the calculation of the PFD_{AVG} the following Markov model for a 1oo1 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 FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.



Abbreviations:

d	One channel has failed dangerous
s	One channel has failed safe
λ_d	Failure rate of dangerous failures
λ_s	Failure rate of safe failures
τ_{Repair}	Repair Time

Figure 3: Markov model

5.1 KFD2-SL2-(Ex)1.LK

The FMEDA carried out on the KFD2-SL2-(Ex)1.LK module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{total}	=	7.14E-07 1/h
λ_{safe}	=	3.38E-07 1/h
$\lambda_{dangerous}$	=	1.03E-08 1/h
$\lambda_{residual}$	=	3.66E-07 1/h
$\lambda_{no\ part}$	=	3.38E-08 1/h
SFF	=	98 %
PFH	=	10.3 FIT

The PFD was calculated for three different proof times using the Markov model as described in Figure 3.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.49E-05	**PFD_{AVG} = 8.98E-05**	**PFD_{AVG} = 2.24E-04**

The boxes marked in green (🟩)mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to be better than 10^{-3}.

Figure 5 shows the time dependent curve of PFD_{AVG}.

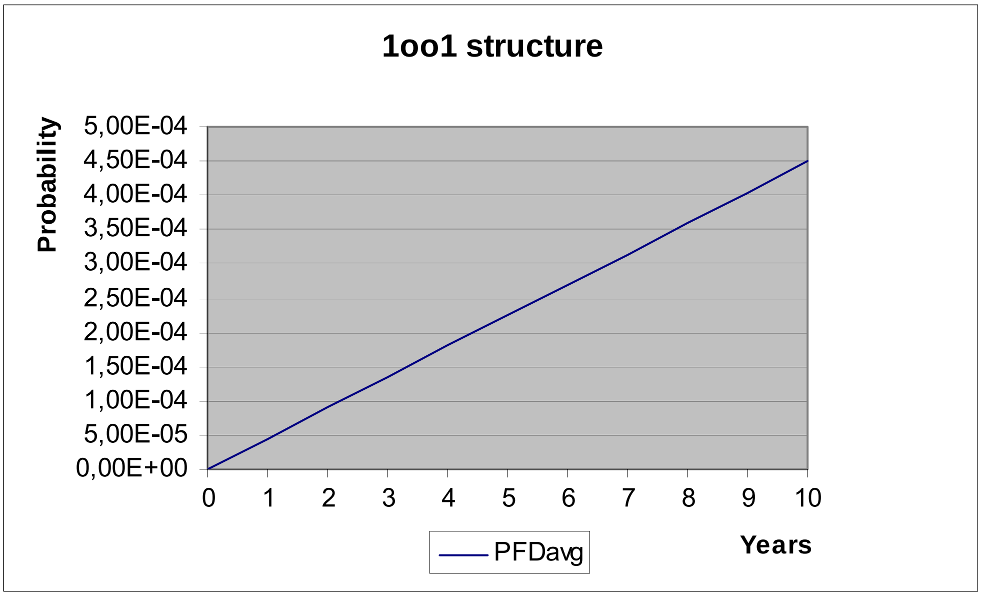


Figure 5: PFD_{AVG}(t)

5.2 KFD2-SL2-(Ex)*(.B)

The FMEDA carried out on the KFD2-SL2-(Ex)*(.B) module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{total}	=	6.52E-07 1/h
λ_{safe}	=	3.20E-07 1/h
$\lambda_{dangerous}$	=	9.70E-09 1/h
$\lambda_{residual}$	=	3.22E-07 1/h
$\lambda_{no\ part}$	=	2.90E-08 1/h
SFF	=	98%
PFH	=	9.7 FIT

The PFD was calculated for three different proof times using the Markov model as described in Figure 3.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD$_{AVG}$ = 4.25E-05	**PFD$_{AVG}$ = 8.50E-05**	**PFD$_{AVG}$ = 2.12E-04**

The boxes marked in green (🟩) mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to be better than 10^{-3}.

Figure 5 shows the time dependent curve of PFD$_{AVG}$.

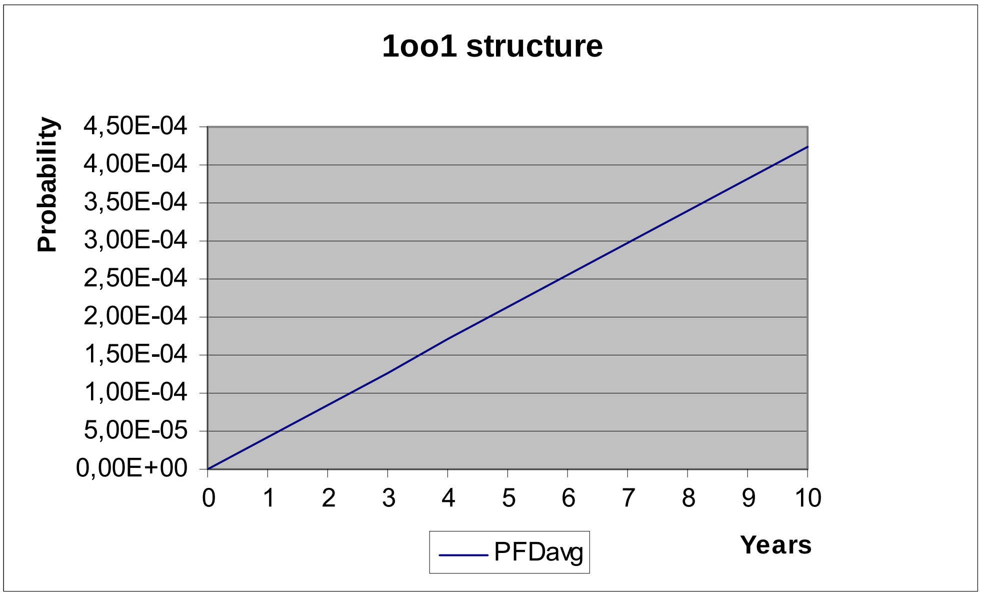


Figure 5: PFD$_{AVG}$(t)

6 Terms and Definitions

FMEDA	Failure Mode Effect and Diagnostic Analysis
PFD	Probability of Failure on Demand
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of a dangerous Failure per Hour
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.
$\lambda_{dangerous}$	Failure rate λ of all dangerous failures
λ_{safe}	Failure rate λ of all safe failures
λ_{total}	Total failure rate λ (overall failure rate of all components)

7 Status of the document

7.1 Releases

Version History:	V1R1	External comments incorporated; October 10, 2007
	V2R0	Philipp Neumeier: Added KFD2-SL2-(Ex)1.LK, July 3, 2008
	V2R1	Pepperl+Fuchs review comments incorporated, July 4, 2008
	V2R2	Pepperl+Fuchs review comments incorporated, July 7, 2008
Authors:	Otto Walch, Philipp Neumeier	
Review:	V0R1	Stephan Aschenbrenner (*exida*); October 1, 2007
	V1R0	Harald Eschelbach (Pepperl + Fuchs); October 2, 2007
	V2R0	Harald Eschelbach (Pepperl + Fuchs); July 3, 2008
	V2R1	Harald Eschelbach (Pepperl + Fuchs); July 7, 2008
Release status:	Released to Pepperl+Fuchs.	

7.2 Release Signatures

Otto Walch

Dipl.-Ing. (FH) Otto Walch, Manager Hazardous Locations

P. Neumeier

Dipl.-Ing. (FH) Philipp Neumeier, Safety Engineer

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

Appendix 1: 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 3 and Table 4 shows an importance analysis of the ten most critical dangerous undetected faults and indicate how these faults can be detected during proof testing.

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

Table 3: Importance Analysis for Solenoid driver KFD2-SL2-(Ex)*(.B)

Component	% of total λ_{du}	Detection through
P12	17,01%	100% functional test with monitoring of the output signal
P7	17,01%	100% functional test with monitoring of the output signal
P10	17,01%	100% functional test with monitoring of the output signal
P5	17,01%	100% functional test with monitoring of the output signal
C30	10,31%	100% functional test with monitoring of the output signal
N14	8,76%	100% functional test with monitoring of the output signal
C18	5,15%	100% functional test with monitoring of the output signal
R57	1,86%	100% functional test with monitoring of the output signal
R23	1,86%	100% functional test with monitoring of the output signal
N5	1,55%	100% functional test with monitoring of the output signal

Table 4: Importance Analysis for Solenoid driver KFD2-SL2-(Ex)1.LK

Component	% of total λ_{du}	Detection through
P7	24,39%	100% functional test with monitoring of the output signal
P12	16,10%	100% functional test with monitoring of the output signal
P5	16,10%	100% functional test with monitoring of the output signal

P10	16,10%	100% functional test with monitoring of the output signal
C30	9,76%	100% functional test with monitoring of the output signal
N14	8,29%	100% functional test with monitoring of the output signal
C18	4,88%	100% functional test with monitoring of the output signal
N5	1,46%	100% functional test with monitoring of the output signal
R57	1,17%	100% functional test with monitoring of the output signal
R23	1,17%	100% functional test with monitoring of the output signal

Appendix 2: 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[4] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolytic capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

The circuit of the Solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) do not contain any components with reduced useful lifetime that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

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

[4] 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.