FMEDA and Prior-use Assessment

Project:
Smart Repeater KFD2-SCD(2)-*** and
Current/Voltage Repeater KFD2-CD(2)-***

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 03/10-12
Report No.: P+F 03/10-12 R014
Version V1, Revision R1.0, March 2004
Stephan Aschenbrenner

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 hardware assessment with prior-use consideration according to IEC 61508 / IEC 61511 carried out on the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-***. '***' stand for the different versions that are available.

Table 1 gives an overview and explains the differences between the various versions.

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

KFD2	**-SCD**	**-Ex**	*****	**.***	
	S				With HART communication
			1		1 channel
				LK	With lead breakage detection
		Ex			With Ex protection

KFD2	**-(S)CD2**	**-Ex**	*****	**.***	
	S				With HART communication
			1		1 channel
			2		2 channels
				LK	With lead breakage detection
		Ex			With Ex protection

KFD2	**-CD**	**-Ex**	*****	**.32-****	
			1		1 channel
				e.g. 13	Input and output configuration
		Ex			With Ex protection

The failure rates are based on 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_{AVG} value of the SIF must be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** would then be 1,00E-03.

The Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** are considered to be Type A[1] components with a hardware fault tolerance of 0.

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

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

As the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** are supposed to be proven-in-use devices, an assessment of the hardware with additional prior-use demonstration for the device was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 the devices are suitable to be used, as a single device, for SIL 2 safety functions.

Table 2: Summary for KFD2-SCD-*

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
PFD_{AVG} = 1.82E-04	**PFD_{AVG} = 3.63E-04**	**PFD_{AVG} = 9.08E-04**	> 89 %

λ_{sd} = 0,00E-00 1/h = 0 FIT

λ_{su} = 3,46E-07 1/h = 346 FIT

λ_{dd} = 0,00E-00 1/h = 0 FIT

λ_{du} = 4,15E-08 1/h = 42 FIT

Table 3: Summary for KFD2-SCD2-*

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
PFD_{AVG} = 2.90E-04	**PFD_{AVG} = 5.80E-04**	**PFD_{AVG} = 1.45E-03**	> 85 %

λ_{sd} = 0,00E-00 1/h = 0 FIT

λ_{su} = 3,88E-07 1/h = 388 FIT

λ_{dd} = 0,00E-00 1/h = 0 FIT

λ_{du} = 6,63E-08 1/h = 66 FIT

Table 4: Summary for KFD2-CD-* – Voltage output**

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
PFD_{AVG} = 2.80E-04	**PFD_{AVG} = 5.60E-04**	**PFD_{AVG} = 1.40E-03**	> 82 %

λ_{sd} = 0,00E-00 1/h = 0 FIT

λ_{su} = 3,09E-07 1/h = 309 FIT

λ_{dd} = 0,00E-00 1/h = 0 FIT

λ_{du} = 6,40E-08 1/h = 64 FIT

Table 5: Summary for KFD2-CD-* – Current output**

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF
PFD_{AVG} = 2.67E-04	**PFD_{AVG} = 5.35E-04**	**PFD_{AVG} = 1.34E-03**	> 83 %

λ_{sd} = 0,00E-00 1/h = 0 FIT

λ_{su} = 3,14E-07 1/h = 314 FIT

λ_{dd} = 0,00E-00 1/h = 0 FIT

λ_{du} = 6,11E-08 1/h = 61 FIT

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 table 3.1 of ANSI/ISA–84.01–1996 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 functional assessment has shown that the Smart Repeater KFD2-SCD(2)-* and Current/Voltage Repeater KFD2-CD(2)-*** have a $\textbf{PFD}_{\textbf{AVG}}$ within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of > 82%. Based on the verification of "prior use" they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.**

A user of the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** 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 failure rates are presented in section 5.1 to 5.4 along with all assumptions.

It is important to realize that the “don’t care” failures and the “annunciation” failures are classified as “safe undetected” failures according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The two channels on the two channel modules should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain 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.com* 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 consist of an assessment of the software development process

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

Option 2 is an assessment by *exida.com* 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 prior-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.com* 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 Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-***. Table 1 gives an overview of the different types that belong to the considered family.

It shall be assessed whether these boards 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.

2 Project management

2.1 *exida.com*

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

2.2 Roles of the parties involved

Pepperl+Fuchs — Manufacturer of the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-***.

exida.com — Performed the hardware and prior-use assessment according to option 2 (see section 1).

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

2.3 Standards / Literature used

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

N1	IEC 61508-2:2000	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	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	251-5036 of 08.06.02	Circuit diagram for K*D2-SCD-Ex1(.P).LK
[D2]	Product No. 122033	Bill of material for K*D2-SCD-Ex1(.P).LK with information about modifications
[D3]	251-04170 of 14.11.02	Circuit diagram for K*D2-SCD2-Ex2.LK(.P)
[D4]	Product No. 122397	Bill of material for K*D2-SCD2-Ex2.LK(.P) with information about modifications
[D5]	21-0864B of 12.06.02	Circuit diagram for KFD2-CD-Ex1.32**
[D6]	Product No. 071763	Bill of material for KFD2-CD-Ex1.32** with information about modifications
[D7]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D8]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D9]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D10]	Auswertung.xls of 09.01.04	Field data evaluation (sold and returned devices)
[D11]	Liste.doc of 09.01.04	Information about the differences of the considered devices
[D12]	Email of 17.12.03	Information about different applications

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA V5 R0.1 SCD V0 R1.0.xls of 09.01.04
[R2]	FMEDA V5 R0.1 SCD2 V0 R1.0.xls of 09.01.04
[R3]	FMEDA V5 R0.1 CD V0 R1.0.xls of 09.01.04
[R4]	FMEDA V5 R0.1 CD voltage output V0 R1.0.xls of 09.01.04
[R5]	Auswertung - exida.xls of 09.01.04 (Field data evaluation of operating hours, sold devices and returned devices)

3 Description of the analyzed modules

3.1 Smart Repeater KFD2-SCD-***

The Smart Repeater KFD2-SCD-*** is considered to be a Type A component with a hardware fault tolerance of 0.

It is used to drive I/P converters and valve positioners.

A 4..20 mA current is transferred from the safe area to the hazardous area.

Digital signals can be superimposed on the analog values in either the hazardous area or the safe area. A bidirectional communication between a SMART-(HART) device in the field and the corresponding SMART communicator in the safe area is possible.

Lead monitoring, input characteristics

Normal operation:
100 Ohm ... 700 Ohm field current

Lead short circuit:
up to < 50 Ohm load

Lead breakage:
up to > 2 kOhm load when ION = 20 mA

In case of short circuit or lead breakage in the field circuit the input resistance is increased to > 100 kOhm. The field current decreases to < 1 mA, and the red LED flashes.

During normal operation the DC input voltage is lower than 4 V (200 Ohm at 20 mA respectively). The AC input impedance corresponds to the output impedance of the unit.

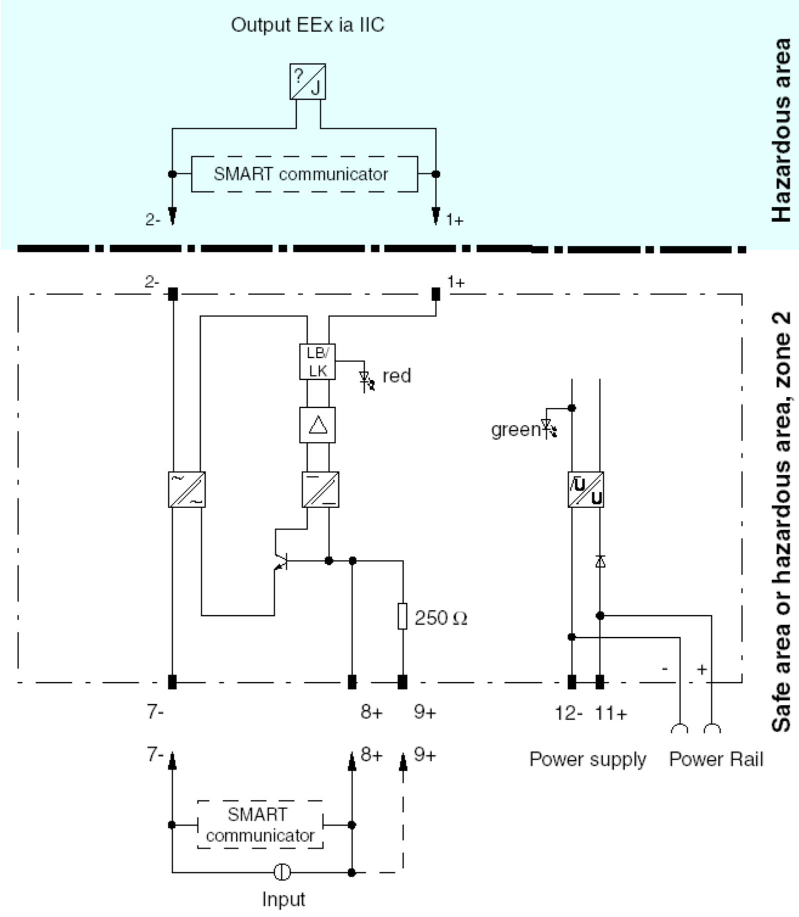


Figure 1: Block diagram of KFD2-SCD-Ex1.LK

3.2 Smart Repeater KFD2-SCD2-***

The Smart Repeater KFD2-SCD2-*** is considered to be a Type A component with a hardware fault tolerance of 0.

It is used to drive I/P converters and valve positioners.

A 4..20 mA current is transferred from the safe area to the hazardous area.

Digital signals can be superimposed on the analog values in either the hazardous area or the safe area. A bidirectional communication between a HART device in the field and the corresponding SMART communicator in the safe area is possible.

Lead breakage (LB) monitoring and short-circuit (SC) monitoring via Power Rail.

Lead monitoring, input characteristics

During lead breakage (> 800 Ohm) and short circuit (< 50 Ohm) the input resistance is >100 kOhm, the field current is < 1 mA and the red LED is flashing.

The voltage drop at the current input (terminal 7-, 8+) is lower than 4 V.

Thus, it corresponds to a compensating resistance of 200 Ohm at 20 mA. The AC input impedance corresponds to the output impedance of the unit.

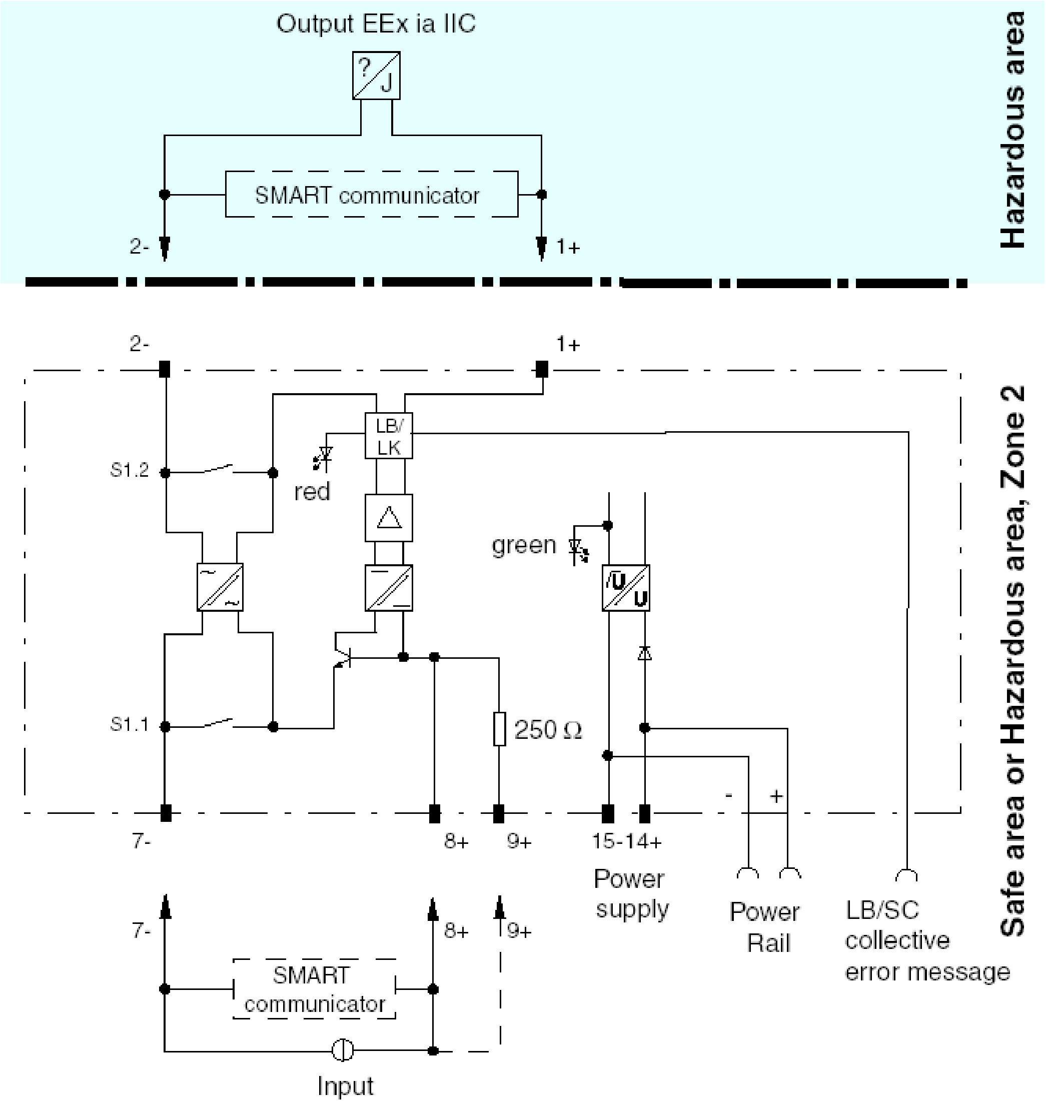


Figure 2: Block diagram of KFD2-SCD2-Ex1.LK as an example for the considered devices

3.3 Current/Voltage Repeater KFD2-CD-***

The KFD2-CD-Ex1.32 transmits an electrical signal from the safe area to the hazardous area. The conversion of a current signal into a voltage signal and vice versa is possible.

The Current/Voltage Repeater KFD2-CD-*** is considered to be a Type A component with a hardware fault tolerance of 0.

It is used to drive I/P converters and valve positioners.

Current input option

A current limit circuit in series to terminal 9 protects the device from damage. The max. voltage drop at the input is 4 VDC.

Voltage input option

The signal is transmitted to terminals 9 and 10 across an amplifier and the DC/DC converter within the allowable voltage range. A voltage limiter circuit protects the amplifier from incorrect input switching and over voltage.

Current output option

The open circuit voltage is DC 24 V within the allowable supply voltage range at terminals 1 and 2. The max. load that can be applied is 850 Ohm.

Voltage output option

At least 20 mA is available within the allowable supply voltage range at terminals 1 and 2 which means that with 10 V output voltage, a load of at least 500 Ohm must be connected.

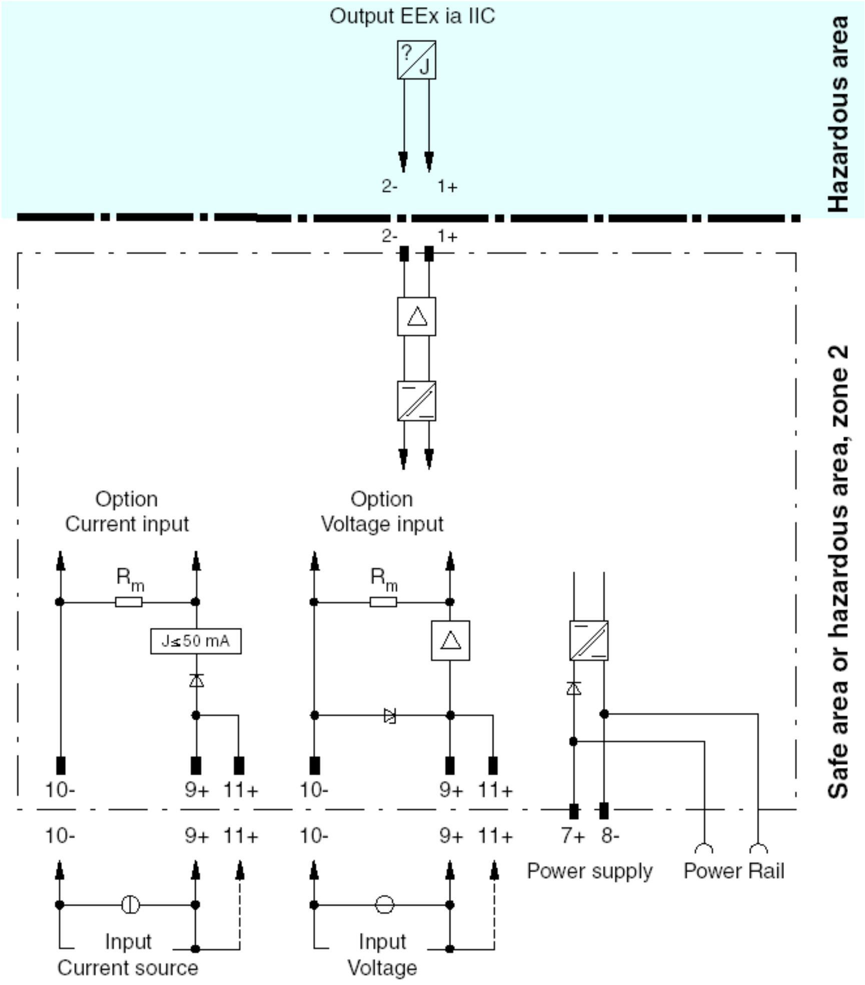


Figure 3: Block diagram of KFD2-CD-Ex1.32

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 [R4].

4.1 Description of the failure categories

The **fail-safe state** is defined as the output being < 4mA (or < 1V / 2V in case of KFD2-CD-***).

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) or deviates the output current by more than 5% of full span.

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

A **fail high** failure (H) is defined as a failure that causes the output signal to go to the maximum output current (> 20mA) or maximum output voltage (> 5V / 10V) in case of KFD2-CD-***.

A **fail low** failure (L) is defined as a failure that causes the output signal to go to the minimum output current (< 4mA) or minimum output voltage (< 1V / 2V) in case of KFD2-CD-***.

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 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 or deviates the output current by not more than 5% of full span. 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) 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.com* in this FMEDA are from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 645-1, 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 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-***.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- 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 and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 645-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- The de-energized state is assumed to be the safe state.
- All modules are operated in the low demand mode of operation.
- The default fail-safe state is "fail low".

5 Results of the assessment

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

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

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

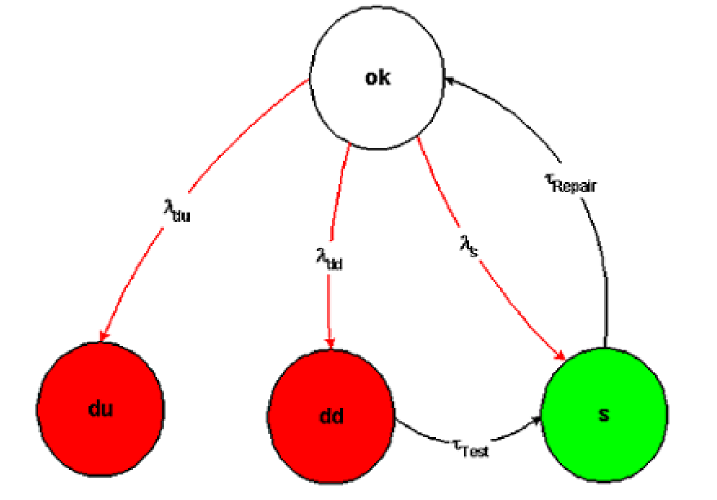
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{don't\ care} + \lambda_{annunciation}$.

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.com* as a simulation tool. The results are documented in the following sections.



Abbreviations:

du	The system has failed dangerous undetected
dd	The system has failed dangerous detected
s	The system has failed safe
λ_{du}	Failure rate of dangerous undetected failures
λ_{dd}	Failure rate of dangerous detected failures
λ_s	Failure rate of safe failures
T_{Test}	Test time
τ_{Test}	Test rate ($1 / T_{Test}$)
T_{Repair}	Repair time
τ_{Repair}	Repair rate ($1 / T_{Repair}$)

Figure 4: Markov model for a 1oo1D structure

5.1 Smart Repeater KFD2-SCD-Ex1(.P).LK

The FMEDA carried out on the Smart Repeater KFD2-SCD-Ex1(.P).LK leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{sd} = 0,00E-00 1/h

$\lambda_{su} = \lambda_{low} + \lambda_{don't\ care}$ = 9,74E-08 1/h + 2,49E-07 1/h = 3,46E-07 1/h

λ_{dd} = 0,00E-00 1/h

$\lambda_{du} = \lambda_{du} + \lambda_{high}$ = 3,74E-08 1/h + 4,04E-09 1/h = 4,15E-08 1/h

λ_{total} = 3,88E-07 1/h

$\lambda_{not\ part}$ = 7,91E-08 1/h

SFF = 89,30%

The PFD_{AVG} 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} = 1.82E-04	**PFD_{AVG} = 3.63E-04**	**PFD_{AVG} = 9.08E-04**

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 table 3.1 of ANSI/ISA–84.01–1996 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 5 shows the time dependent curve of PFD_{AVG}.

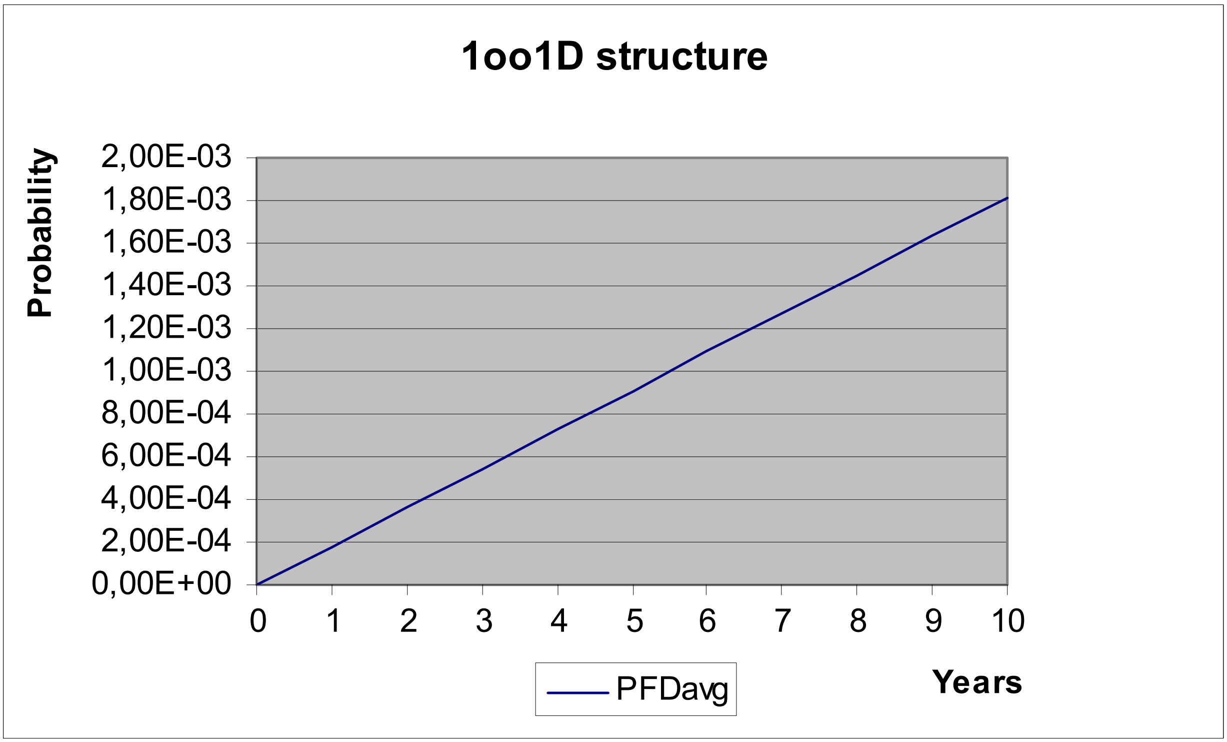


Figure 5: PFD_{AVG}(t)

5.2 Smart Repeater KFD2-SCD2-Ex2.LK(.P)

The FMEDA carried out on the Smart Repeater KFD2-SCD2-Ex2.LK(.P) leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{sd} = 0,00E-00 1/h

$\lambda_{su} = \lambda_{low} + \lambda_{don't\ care} + \lambda_{annunciation}$ = 1,13E-07 1/h + 2,74E-07 1/h + 5,00E-10 1/h = 3,88E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 6,63E-08 1/h

λ_{total} = 4,54E-07 1/h

$\lambda_{not\ part}$ = 1,49E-07 1/h

SFF = 85,39%

The PFD_{AVG} 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} = 2.90E-04	PFD_{AVG} = 5.80E-04	PFD_{AVG} = 1.45E-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 table 3.1 of ANSI/ISA–84.01–1996 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 6 shows the time dependent curve of PFD_{AVG}.

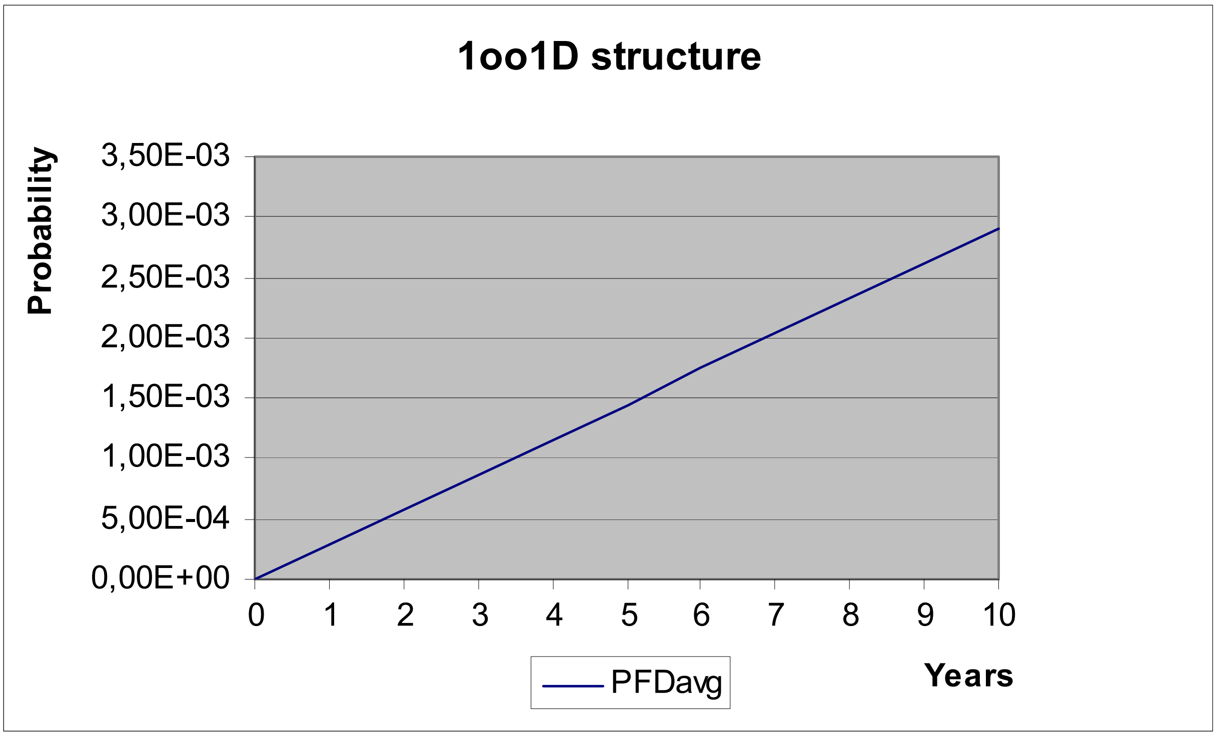


Figure 6: PFD_{AVG}(t)

5.3 Current/Voltage Repeater KFD2-CD-Ex1.32** – voltage output

The FMEDA carried out on KFD2-CD-Ex1.32** with voltage output leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{sd} = 0,00E-00 1/h

λ_{su} = λ_{low} + $\lambda_{don't\ care}$ = 8,13E-08 1/h + 2,28E-07 1/h = 3,09E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = λ_{du} + λ_{high} = 5,27E-08 1/h + 1,13E-08 1/h = 6,40E-08 1/h

λ_{total} = 3,73E-07 1/h

$\lambda_{not\ part}$ = 2,20E-09 1/h

SFF = 82,84%

The PFD_{AVG} 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} = 2.80E-04	**PFD_{AVG} = 5.60E-04**	**PFD_{AVG} = 1.40E-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 table 3.1 of ANSI/ISA–84.01–1996 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 7 shows the time dependent curve of PFD_{AVG}.

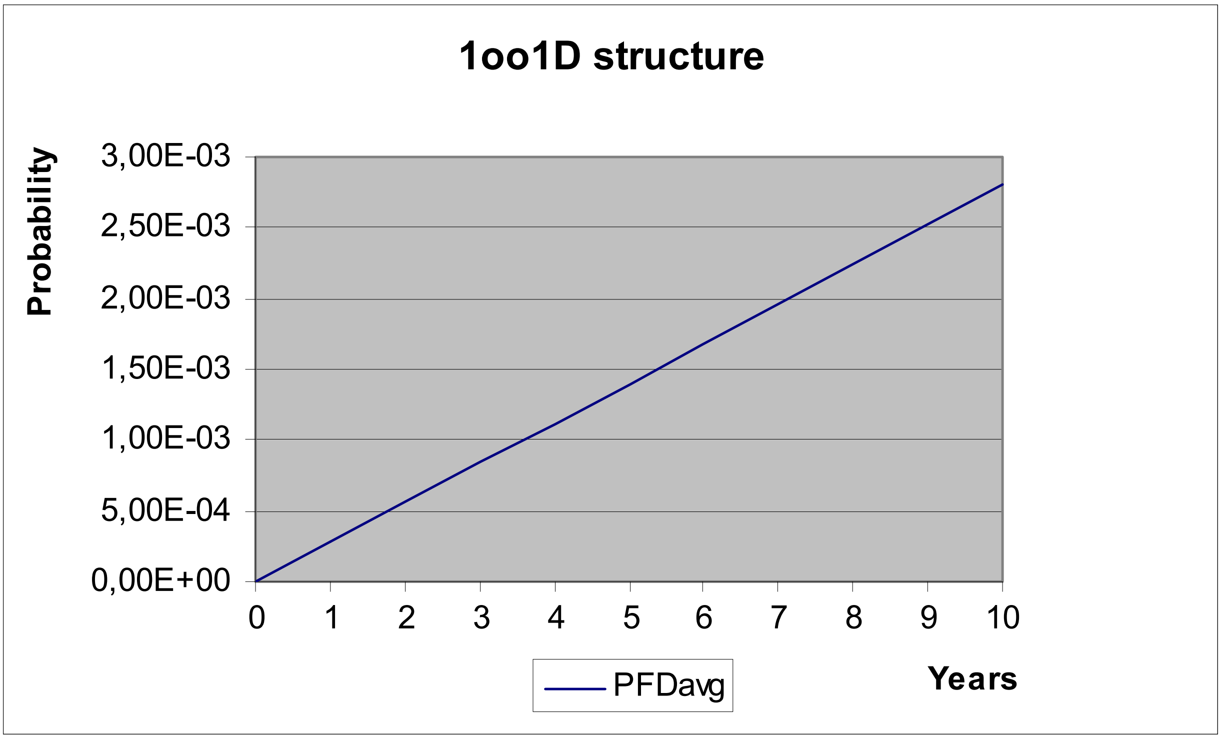


Figure 7: PFD_{AVG}(t)

5.4 Current/Voltage Repeater KFD2-CD-Ex1.32** – current output

The FMEDA carried out on the KFD2-CD-Ex1.32** with current output leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

λ_{sd} = 0,00E-00 1/h

$\lambda_{su} = \lambda_{low} + \lambda_{don't\ care}$ = 8,43E-08 1/h + 2,30E-07 1/h = 3,14E-07 1/h

λ_{dd} = 0,00E-00 1/h

$\lambda_{du} = \lambda_{du} + \lambda_{high}$ = 5,14E-08 1/h + 9,63E-09 1/h = 6,11E-08 1/h

λ_{total} = 3,75E-07 1/h

$\lambda_{not\ part}$ = 7,60E-09 1/h

SFF = 83,73%

The PFD_{AVG} 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} = 2.67E-04	**PFD_{AVG} = 5.35E-04**	**PFD_{AVG} = 1.34E-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 table 3.1 of ANSI/ISA–84.01–1996 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 8 shows the time dependent curve of PFD_{AVG}.

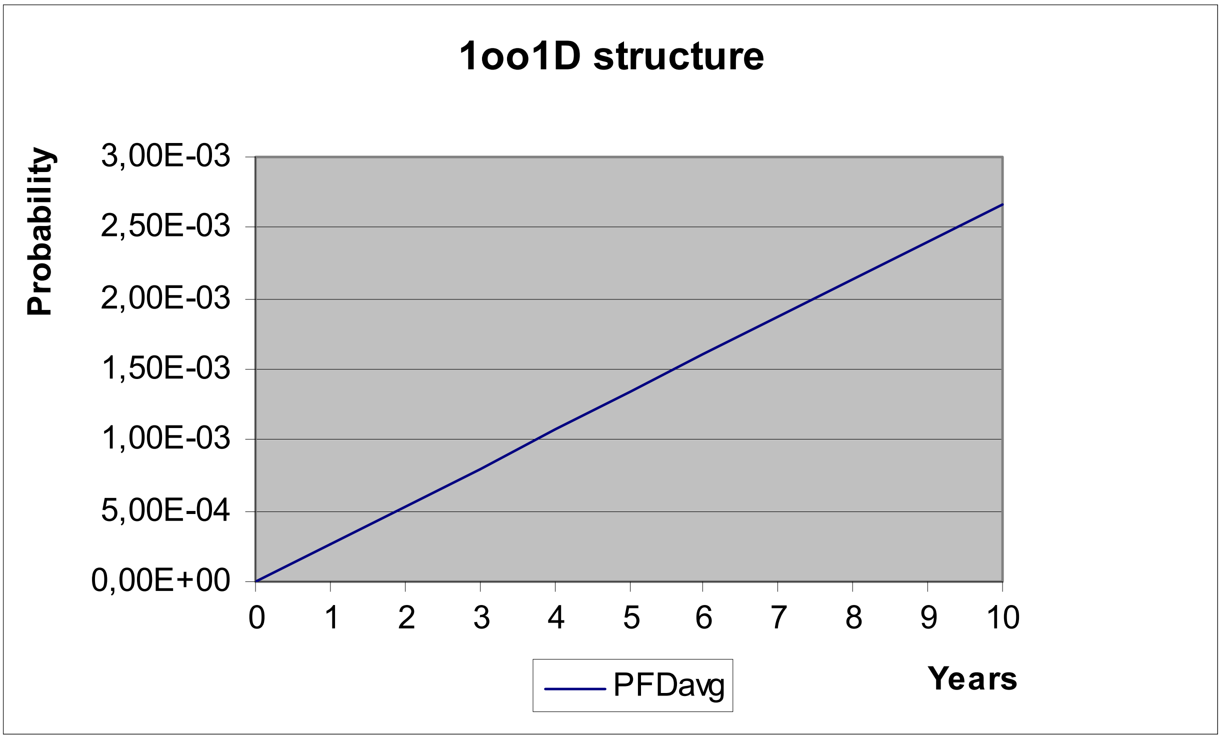


Figure 8: PFD_{AVG}(t)

6 Prior-use Assessment of KFD2-SCD(2)-*** and KFD2-CD(2)-***

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%[2].

This is identical to the requirements on Type A (sub)-systems. The Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** 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 prior use shows the unlikelihood of systematic failures.

The assessment of the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

[2] 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[3]
See Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01	1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 5 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail[4] is low (<0,4%). 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D7] to [D9]. 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 [D10] to [D12] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience (Operating experience of more than 704.000.000 operating hours exists for CD and more than 46.500.000 operating hours for SCD. 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). 3. 11.5.2 is under the responsibility of the user / manufacturer –> no argumentation. 11.5.3 see bullet items before. 4. N/A 5. Under the responsibility of the manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D12]
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 Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** with a SFF of 60% - < 90% and a HFT = 0 can considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

[3] The numbering is based on the requirements detailed in appendix 1.

[4] The probability of failure is the percentage of all returned devices with relevant repair reasons to all sold devices.

7 Terms and Definitions

DC_S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time ($1x10^{-9}$ 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
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.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

8.2 Releases

Version:	V1	
Revision:	R1.0	
Version History:	V0, R1.0:	Initial version, Jan. 15, 2004
	V1, R1.0:	Internal review comments integrated, Mar. 8, 2004
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida.com); Jan. 30, 2004
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

Appendix 2 should be considered when writing the safety manual as it contains important safety related information.

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 to Table 8 show a sensitivity analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Table 6: Sensitivity Analysis of dangerous undetected faults – KFD2-SCD-Ex1(.P).LK

Component	% of total λ_{du}	Detection through
IC9	18,70%	100% functional test over the entire output range
TR3	6,68%	100% functional test over the entire output range
TR4	6,68%	100% functional test over the entire output range
TR6	6,68%	100% functional test over the entire output range
TR7	6,68%	100% functional test over the entire output range
TR9	6,68%	100% functional test over the entire output range
TR10	6,68%	100% functional test over the entire output range
IC7	6,68%	100% functional test over the entire output range
TR12	3,21%	100% functional test over the entire output range
T2	3,21%	100% functional test over the entire output range

Table 7: Sensitivity Analysis of dangerous undetected faults – KFD2-SCD2-Ex2.LK(.P)

Component	% of total λ_{du}	Detection through
TR3	12,07%	100% functional test over the entire output range
TR6	12,07%	100% functional test over the entire output range
TR7	7,55%	100% functional test over the entire output range
TR10	7,55%	100% functional test over the entire output range
TR11	7,55%	100% functional test over the entire output range
TR13	7,55%	100% functional test over the entire output range
IC4	5,28%	100% functional test over the entire output range
TR8	3,77%	100% functional test over the entire output range
IC3	3,02%	100% functional test over the entire output range
IC5	2,41%	100% functional test over the entire output range

Table 8: Sensitivity Analysis of dangerous undetected faults - KFD2-CD-Ex1.32 (voltage output)**

Component	**% of total λ_{du}**	**Detection through**
VR1	56,97%	100% functional test over the entire output range
TR5	9,50%	100% functional test over the entire output range
TR6	9,50%	100% functional test over the entire output range
IC2	4,75%	100% functional test over the entire output range
TR2	2,28%	100% functional test over the entire output range
IC3	2,28%	100% functional test over the entire output range
T2	2,28%	100% functional test over the entire output range
C11	1,90%	100% functional test over the entire output range
C21	1,90%	100% functional test over the entire output range
C24	1,90%	100% functional test over the entire output range

Appendix 2.2: Possible proof tests to detect dangerous undetected faults

Proof test 1 consists of the following steps, as described in Table 9.

Table 9 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the repeater to go to the high alarm current output and verify that the analog current reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
3	Send a HART command to the repeater to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 50% of possible “du” failures in the repeater.

Proof test 2 consists of the following steps, as described in Table 10.

Table 10 Steps for Proof Test 2

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Perform a two-point calibration of the connected transmitter This requires that the transmitter has already been tested without the repeater and does not contain any dangerous undetected faults anymore.
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures in the repeater.

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.1) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is 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, 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_{AVG} calculation is only valid for components that 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 circuits of the Smart Repeater KFD2-SCD(2)-*** and Current/Voltage Repeater KFD2-CD(2)-*** do not contain any electrolytic capacitors that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

However, according to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.