



FMEDA and Proven-in-use Assessment

Project:

Smart Repeater KFD0-SCS-(Ex)1.55 and
DC Repeater KFD0-CS-(Ex)*.5*(P)

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 03/07-04

Report No.: P+F 03/07-04 R013

Version V1, Revision R1.2, July 2005

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Smart Repeater KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P). ‘*’ 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 overview¹

K	F	D0	-CS	-Ex	*	.5*	(P)	
					1			1 channel
					2			2 channels
						0		Accuracy 0,1%
						1		Accuracy 1%
						3		Less voltage drop in the loop
							P	With polarity protection
				Ex				With Ex protection

K	F	D0	-*CS	-Ex	*	.5*	
					1		1 channel
						5	Accuracy 0,3%
				Ex			With Ex protection
			S				HART compatible

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 $\geq 10^{-3}$ 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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) would then be 1,00E-03.

The Smart Repeater KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) are considered to be Type A² components with a hardware fault tolerance of 0.

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.

¹ This report also includes the non-Ex versions of all mentioned types.

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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-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.

Assuming that a connected safety logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on the application (see section 4.3). The following tables show how the above stated requirements are fulfilled based on the different applications.

Summary for KFD0-SCS-(Ex)1.55

Table 2: Summary as current repeater³ – Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S ⁴	DC _D
Low trip	36 FIT	74 FIT	33 FIT	24 FIT	85,65%	33%	58%
High trip	33 FIT	74 FIT	36 FIT	24 FIT	85,65%	31%	60%

Table 3: Summary as current repeater – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 1.05E-04	PFD _{AVG} = 2.09E-04	PFD _{AVG} = 5.23E-04

Table 4: Summary as current driver²– Failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	140 FIT	0 FIT	26 FIT	84,19%	0%	0%

Table 5: Summary as current driver– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 1.15E-04	PFD _{AVG} = 2.31E-04	PFD _{AVG} = 5.76E-04

³ See section 3.3 for further explanations of applications as current repeater and current driver

⁴ DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for the considered devices

Summary for KFD0-CS-(Ex)*.50(P)

Table 6: Summary as current repeater– Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	22 FIT	150 FIT	37 FIT	49 FIT	80,84%	13%	43%
High trip	37 FIT	150 FIT	22 FIT	49 FIT	80,84%	20%	31%

Table 7: Summary as current repeater– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 2.17E-04	PFD _{AVG} = 4.33E-04	PFD _{AVG} = 1.08E-03

Table 8: Summary as current driver– Failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	206 FIT	0 FIT	51 FIT	80,06%	0%	0%

Table 9: Summary for as current driver– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 2.25E-04	PFD _{AVG} = 4.50E-04	PFD _{AVG} = 1.13E-03

Summary for KFD0-CS-(Ex)*.51(P)

Table 10: Summary as current repeater– Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	22 FIT	63 FIT	36 FIT	39 FIT	75,47%	26%	48%
High trip	36 FIT	63 FIT	22 FIT	39 FIT	75,47%	36%	36%

Table 11: Summary as current repeater– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 1.70E-04	PFD _{AVG} = 3.41E-04	PFD _{AVG} = 8.51E-04

Table 12: Summary as current driver– Failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	118 FIT	0 FIT	41 FIT	74,21%	0%	0%

Table 13: Summary as current driver– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 1.79E-04	PFD _{AVG} = 3.58E-04	PFD _{AVG} = 8.95E-04

Summary for KFD0-CS-(Ex)*.53(P)

Table 14: Summary as current repeater– Failure rates

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	19 FIT	51 FIT	36 FIT	9 FIT	91,90%	27%	80%
High trip	36 FIT	51 FIT	19 FIT	9 FIT	91,90%	41%	68%

Table 15: Summary as current repeater– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 4.07E-05	PFD _{AVG} = 8.13E-05	PFD _{AVG} = 2.03E-04

Table 16: Summary as current driver– Failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	103 FIT	0 FIT	11 FIT	90,16%	0%	0%

Table 17: Summary as current driver– PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD _{AVG} = 4.94E-05	PFD _{AVG} = 9.88E-05	PFD _{AVG} = 2.47E-04

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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) have a PFD_{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 > 74%. Based on the verification of "proven-in-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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) 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 5.8 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.

Table of Contents

Management summary	2
1 Purpose and Scope	8
2 Project management	9
2.1 <i>exida.com</i>	9
2.2 Roles of the parties involved	9
2.3 Standards / Literature used	9
2.4 Reference documents	10
2.4.1 Documentation provided by the customer	10
2.4.2 Documentation generated by <i>exida.com</i>	10
3 Description of the analyzed modules	11
3.1 Smart Repeater KFD0-SCS-Ex1.55	11
3.2 DC Repeater KFD0-CS-Ex1.50P (.51P) (.53P)	12
3.3 Typical applications of the analyzed modules	12
4 Failure Modes, Effects, and Diagnostics Analysis	13
4.1 Description of the failure categories	13
4.2 Methodology – FMEDA, Failure rates	14
4.2.1 FMEDA	14
4.2.2 Failure rates	14
4.2.3 Assumption	14
4.3 Behavior of the safety logic solver	15
5 Results of the assessment	16
5.1 Smart Repeater KFD0-SCS-(Ex)1.55 – current repeater	17
5.2 Smart Repeater KFD0-SCS-(Ex)1.55 – current driver	18
5.3 DC Repeater KFD0-CS-(Ex)*.50(P) – current repeater	19
5.4 DC Repeater KFD0-CS-(Ex)*.50(P) – current driver	20
5.5 DC Repeater KFD0-CS-(Ex)*.51(P) – current repeater	21
5.6 DC Repeater KFD0-CS-(Ex)*.51(P) – current driver	22
5.7 DC Repeater KFD0-CS-(Ex)*.53(P) – current repeater	23
5.8 DC Repeater KFD0-CS-(Ex)*.53(P) – current driver	24
6 Proven-in-use Assessment of KFD0-SCS-(Ex)1.55 and KFD0-CS-(Ex)*.5*(P)	25
7 Terms and Definitions	27
8 Status of the document	28
8.1 Liability	28
8.2 Releases	28
8.3 Release Signatures	28
Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01	29
Appendix 1.1 Section 11.5.3 of IEC 61511-1 First Edition 2003-01	29
Appendix 1.2 Section 11.5.4 of IEC 61511-1 First Edition 2003-01	29

Appendix 1.3 Section 11.5.2 of IEC 61511-1 First Edition 2003-01	29
Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test.....	31
Appendix 3: Impact of lifetime of critical components on the failure rate.....	33

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 contains a FMEDA to determine the fault behavior and the different failure rates resulting in 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 contain any software assessment.

Option 2: Hardware assessment with proven-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 contains a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition this option consists of an assessment of the proven-in-use documentation of the device 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 draft 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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P). 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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P).

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

Pepperl+Fuchs GmbH contracted *exida.com* in July 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]	251-0313C	Circuit diagram for KFD0-CS-Ex*.50(P), KFD0-CS-Ex*.51(P) and KFD0-CS-Ex*.53(P)
[D2]	Product No. 072143	Bill of material for KFD0-CS-Ex1.50P
[D3]	Product No. 072147	Bill of material for KFD0-CS-Ex1.51P
[D4]	Product No. 072150	Bill of material for KFD0-CS-Ex1.53P
[D5]	Product No. 051099	Bill of material for KFU8-CRG-Ex1.D
[D6]	056.807-0022 of 19.09.02	Circuit diagram for KFD0-SCS-Ex1.55
[D7]	KFD0-SCS-Ex1.55 Stueckliste.pdf of 16.07.03	Bill of material for KFD0-SCS-Ex1.55
[D8]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D9]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D10]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D11]	Email of 21.07.03	Information about modifications on CS because of ATEX and change to SMD
[D12]	3005211.pdf	Document change notice of 20.01.03
[D13]	3005211A.pdf	Document change notice of 21.05.03
[D14]	Email of 25.07.03	Field data evaluation SCS (sold devices)
[D15]	Email of 28.07.03	Field data evaluation CS (sold devices)
[D16]	KFD0-CS.xls of 28.07.03	Field data evaluation CS (returned devices)
[D17]	KFD0-SCS-Ex1.xls of 28.07.03	Field data evaluation SCS (returned devices)
[D18]	Email of 22.07.03	Information about differences between the CS versions 50, 51 and 53
[D19]	FIT analysis.xls of 21.07.03	Documentation about executed fault insertion tests done by Knick for KFD0-SCS-Ex1.55
[D20]	Email of 19.09.03	Information about different applications
[D21]	Email of 23.06.05	Information about non-Ex versions

2.4.2 Documentation generated by exida.com

[R1]	FMEDA V4 R0.9 SCS Ausgangstrenner V1 R0.1.xls of 21.07.03
[R2]	FMEDA V4 R0.9 SCS Speisetrenner V1 R0.1.xls of 21.07.03
[R3]	FMEDA V4 R0.9 CS 50 Ausgangstrenner V1 R0.1.xls of 21.07.03
[R4]	FMEDA V4 R0.9 CS 50 Speisetrenner V1 R0.1.xls of 21.07.03
[R5]	FMEDA V4 R0.9 CS 51 Ausgangstrenner V1 R0.1.xls of 18.09.03
[R6]	FMEDA V4 R0.9 CS 51 Speisetrenner V1 R0.1.xls of 18.09.03
[R7]	FMEDA V4 R0.9 CS 53 Ausgangstrenner V1 R0.1.xls of 18.09.03
[R8]	FMEDA V4 R0.9 CS 53 Speisetrenner V1 R0.1.xls of 18.09.03
[R9]	Field data CS-SCS.xls of 18.09.03 (Field data evaluation of operating hours)

3 Description of the analyzed modules

3.1 Smart Repeater KFD0-SCS-Ex1.55

The universal module KFD0-SCS-Ex1.55 does not require auxiliary power for the isolation of 4..20 mA current loops. The module isolates 4..20 mA signals from transmitters and positioners and is therefore, bidirectionally HART compatible. The HART transmitters and HART positioners may thus, be configured in the safe area as well as the hazardous area.

The Smart Repeater KFD0-SCS-Ex1.55 is considered to be a Type A component with a hardware fault tolerance of 0.

Lead breakage monitoring is possible by means of the reaction of the field current signal to the safe area, which means the control system must monitor whether the 4..20 mA range was exceeded or short circuit.

The module may also be used for controlling Ex-i valves, light signals, etc. based on the internal voltage limits (safe area). Terminals 8- and 9+ in this case are driven with a 24 V binary signal.

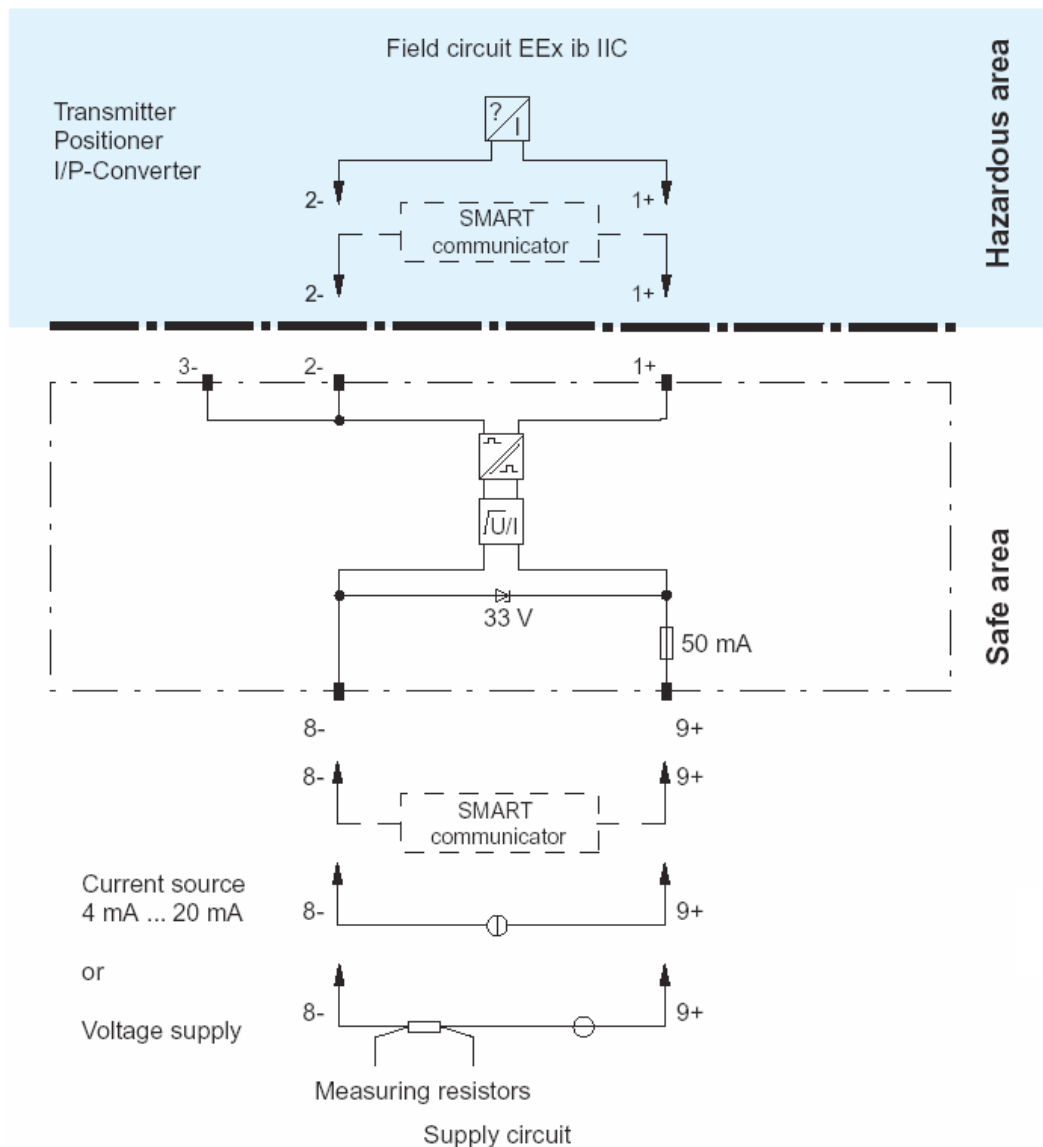


Figure 1: Block diagram of KFD0-SCS-Ex1.55

3.2 DC Repeater KFD0-CS-Ex1.50P (.51P) (.53P)

Each channel works like a "DC current isolator". Both channels have separate reverse polarity protection. The input and output are galvanically isolated from each other.

Their increased current range and the higher accuracy allow for differentiation between normal operation, fire alarm, lead breakage and short circuit currents in the safe area. In many cases they may also be used for controlling I/P converters.

A separate power supply with auxiliary power is not required. The 2 channel version allows for the connection of 2 independent circuits in a single housing.

The DC Repeaters KFD0-CS-Ex1.5*P are considered to be Type A components with a hardware fault tolerance of 0.

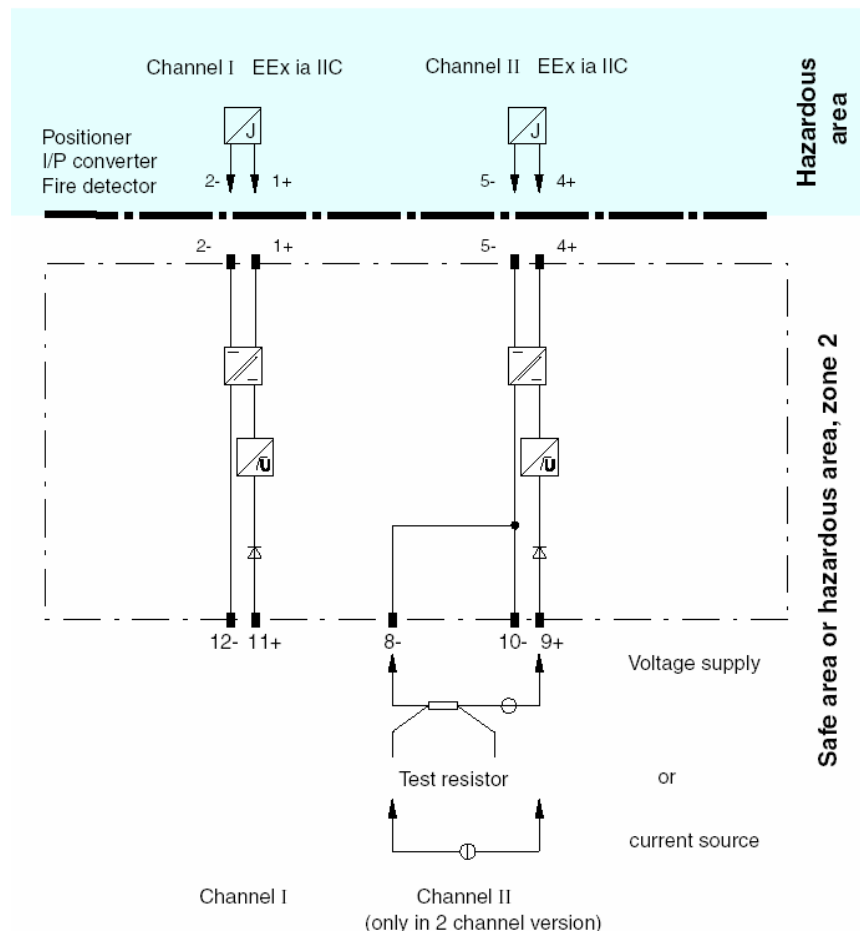


Figure 2: Block diagram of KFD0-CS-Ex1.50P as an example for the considered devices

3.3 Typical applications of the analyzed modules

Current Repeater (Input 24V, Output 4..20mA back to input):

- The isolation of a current signal from fire detectors or similar sensors. In this case, a voltage source can be connected to the safe area terminals. A specific measurement current across a passive sensor can be measured in the safe area with a series resistor.

Current Driver (Input 4..20mA, Output 4..20mA):

- The isolation of current loops for the control of positioner, I/P converters etc. A current source is connected to the safe area terminals.

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 [R8]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level. This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

Depending on the application the **fail-safe state** is defined as the output being $< 3.6\text{mA}$ or $> 22\text{mA}$. De-energize to trip function.

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 the actual value.

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 ($> 22\text{mA}$).

A **fail low** failure (L) is defined as a failure that causes the output signal to go to the minimum output current ($< 3.6\text{mA}$).

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. 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 ISA 71.01 class D. 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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P).

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The repair time after a safe failure is 8 hours.
- The test time of the logic solver to react on a dangerous detected failure is 1 hour.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment and can be compared to the Ground Benign classification.
- In case the considered devices are working as current drivers the de-energized state is assumed to be the safe state.
- All modules are operated in the low demand mode of operation.

4.3 Behavior of the safety logic solver

Depending on the application, the following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value is below a predefined low set value. A current < 3.6mA (Fail Low) is below the specified trip-point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 22mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by a connected logic solver. The SPLC Detection Behavior in Table 18 represents the under-range and over-range detection capability of the connected safety logic solver.

Table 18 Application example

Application	SPLC Detection Behavior	λ_{low}	λ_{high}
Low trip	< 4mA	= λ_{sd}	= λ_{du}
Low trip	> 20mA	= λ_{su}	= λ_{dd}
Low trip	< 4mA and > 20mA	= λ_{sd}	= λ_{dd}
Low trip	-	= λ_{su}	= λ_{du}
High trip	< 4mA	= λ_{dd}	= λ_{su}
High trip	> 20mA	= λ_{du}	= λ_{sd}
High trip	< 4mA and > 20mA	= λ_{dd}	= λ_{sd}
High trip	-	= λ_{du}	= λ_{su}

In this analysis it is assumed that the safety logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

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:

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

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

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.

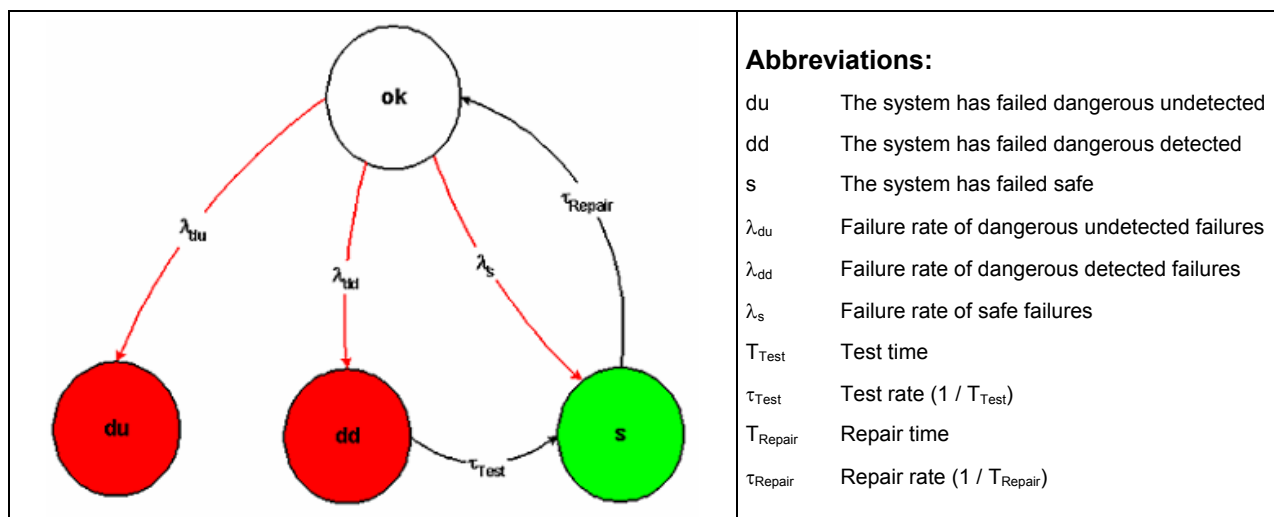


Figure 3: Markov model for a 1oo1D structure

5.1 Smart Repeater KFD0-SCS-(Ex)1.55 – current repeater

The FMEDA carried out on the Smart Repeater KFD0-SCS-(Ex)1.55 as current repeater leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 0,00E-00 \text{ 1/h} + 6,34E-08 \text{ 1/h} + 1,06E-08 \text{ 1/h} = 7,40E-08 \text{ 1/h}$$

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

$$\lambda_{du} = 2,39E-08 \text{ 1/h}$$

$$\lambda_{high} = 3,27E-08 \text{ 1/h}$$

$$\lambda_{low} = 3,60E-08 \text{ 1/h}$$

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

$$\lambda_{\text{not part}} = 0,00E-00 \text{ 1/h}$$

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	36 FIT	74 FIT	33 FIT	24 FIT	85,65%	33%	58%
High trip	33 FIT	74 FIT	36 FIT	24 FIT	85,65%	31%	60%

The PFD_{AVG} 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} = 1.05E-04	PFD _{AVG} = 2.09E-04	PFD _{AVG} = 5.23E-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 4 shows the time dependent curve of PFD_{AVG}.

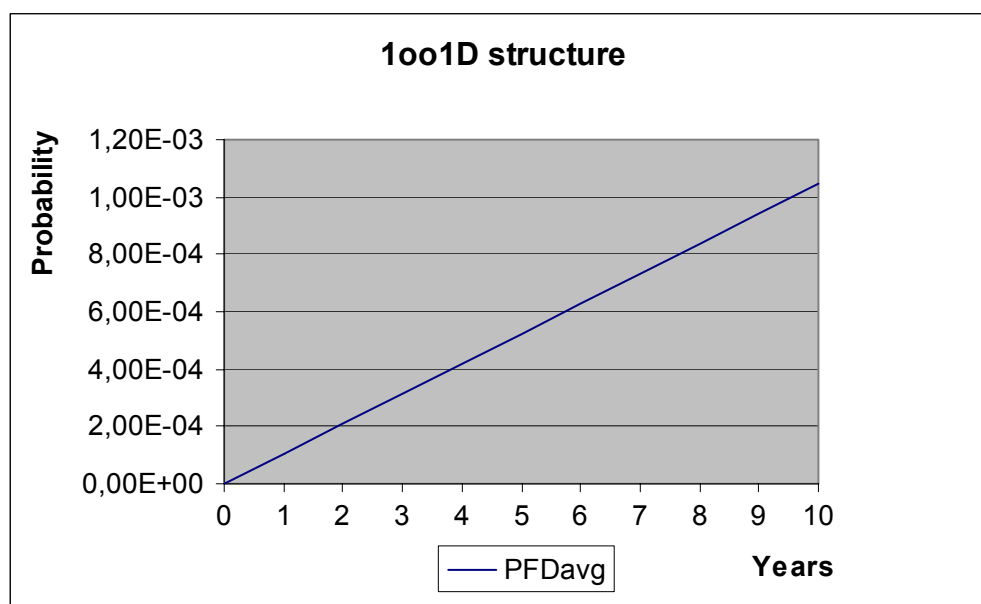


Figure 4: PFD_{AVG}(t)

5.2 Smart Repeater KFD0-SCS-(Ex)1.55 – current driver

The FMEDA carried out on the Smart Repeater KFD0-SCS-(Ex)1.55 as current driver leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{low} + \lambda_{don't \text{ care}} + \lambda_{annunciation} = 5,71E-08 \text{ 1/h} + 7,25E-08 \text{ 1/h} + 1,06E-08 \text{ 1/h} = 1,40E-07 \text{ 1/h}$$

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

$$\lambda_{du} = 2,63E-08 \text{ 1/h}$$

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

$$\lambda_{not \text{ part}} = 0,00E-00 \text{ 1/h}$$

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	140 FIT	0 FIT	26 FIT	84,19%	0%	0%

The PFD_{AVG} 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} = 1.15E-04	PFD _{AVG} = 2.31E-04	PFD _{AVG} = 5.76E-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}.

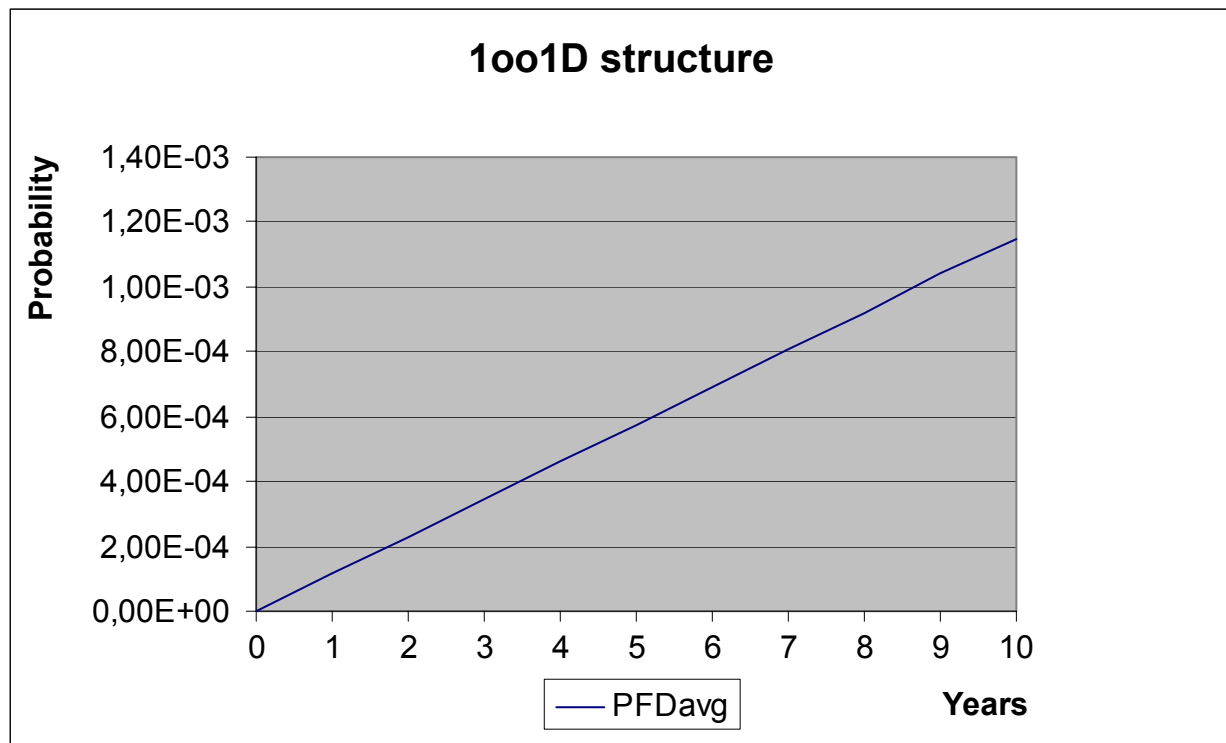


Figure 5: PFD_{AVG}(t)

5.3 DC Repeater KFD0-CS-(Ex)*.50(P) – current repeater

The FMEDA carried out on KFD0-CS-(Ex)*.50(P) as current repeater leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 0,00E-00 \text{ 1/h} + 1,49E-07 \text{ 1/h} + 1,35E-09 \text{ 1/h} = 1,50E-07 \text{ 1/h}$$

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

$$\lambda_{du} = 4,94E-08 \text{ 1/h}$$

$$\lambda_{high} = 3,66E-08 \text{ 1/h}$$

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

$$\lambda_{total} = 2,58E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 0,00E-00 \text{ 1/h}$$

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	22 FIT	150 FIT	37 FIT	49 FIT	80,84%	13%	43%
High trip	37 FIT	150 FIT	22 FIT	49 FIT	80,84%	20%	31%

The PFD_{AVG} 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} = 2.17E-04	PFD _{AVG} = 4.33E-04	PFD _{AVG} = 1.08E-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}.

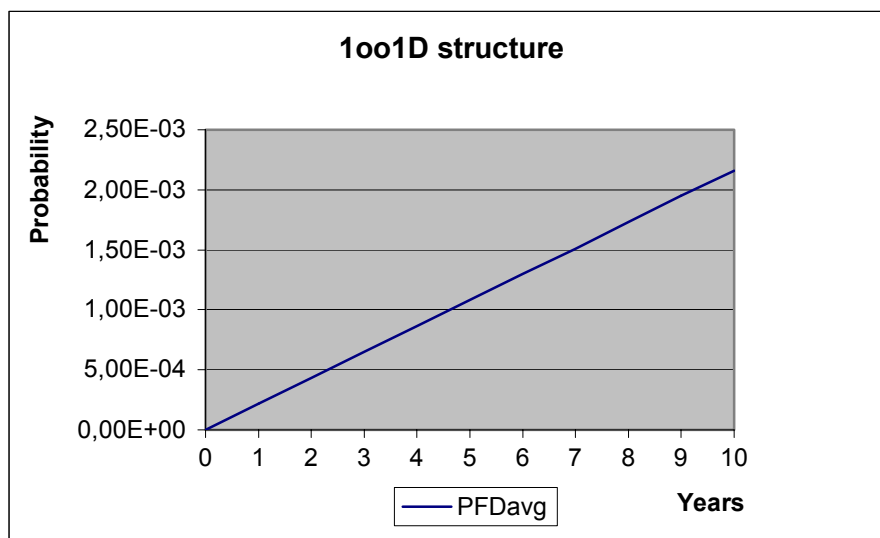


Figure 6: PFD_{AVG}(t)

5.4 DC Repeater KFD0-CS-(Ex)*.50(P) – current driver

The FMEDA carried out on KFD0-CS-(Ex)*.50(P) as current driver leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{low} + \lambda_{don't \text{ care}} + \lambda_{annunciation} = 5,61E-08 \text{ 1/h} + 1,49E-07 \text{ 1/h} + 1,35E-09 \text{ 1/h} = 2,06E-07 \text{ 1/h}$$

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

$$\lambda_{du} = 5,14E-08 \text{ 1/h}$$

$$\lambda_{total} = 2,58E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 0,00E-00 \text{ 1/h}$$

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	206 FIT	0 FIT	51 FIT	80,06%	0%	0%

The PFD_{AVG} 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} = 2.25E-04	PFD _{AVG} = 4.50E-04	PFD _{AVG} = 1.13E-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}.

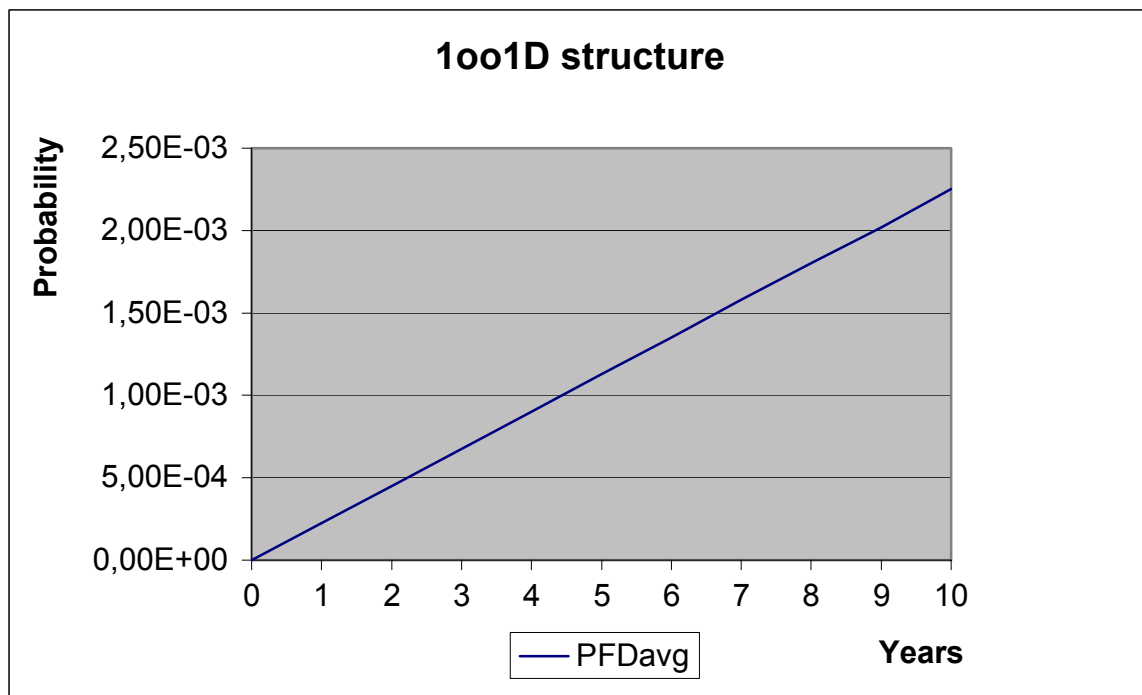


Figure 7: PFD_{AVG}(t)

5.5 DC Repeater KFD0-CS-(Ex)*.51(P) – current repeater

The FMEDA carried out on KFD0-CS-(Ex)*.51(P) as current repeater leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 0,00E-00 \text{ 1/h} + 6,13E-08 \text{ 1/h} + 1,35E-09 \text{ 1/h} = 6,27E-08 \text{ 1/h}$$

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

$$\lambda_{du} = 3,89E-08 \text{ 1/h}$$

$$\lambda_{high} = 3,56E-08 \text{ 1/h}$$

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

$$\lambda_{total} = 1,59E-07 \text{ 1/h}$$

$$\lambda_{\text{not part}} = 0,00E-00 \text{ 1/h}$$

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	22 FIT	63 FIT	36 FIT	39 FIT	75,47%	26%	48%
High trip	36 FIT	63 FIT	22 FIT	39 FIT	75,47%	36%	36%

The PFD_{AVG} 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} = 1.70E-04	PFD _{AVG} = 3.41E-04	PFD _{AVG} = 8.51E-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 8 shows the time dependent curve of PFD_{AVG}.

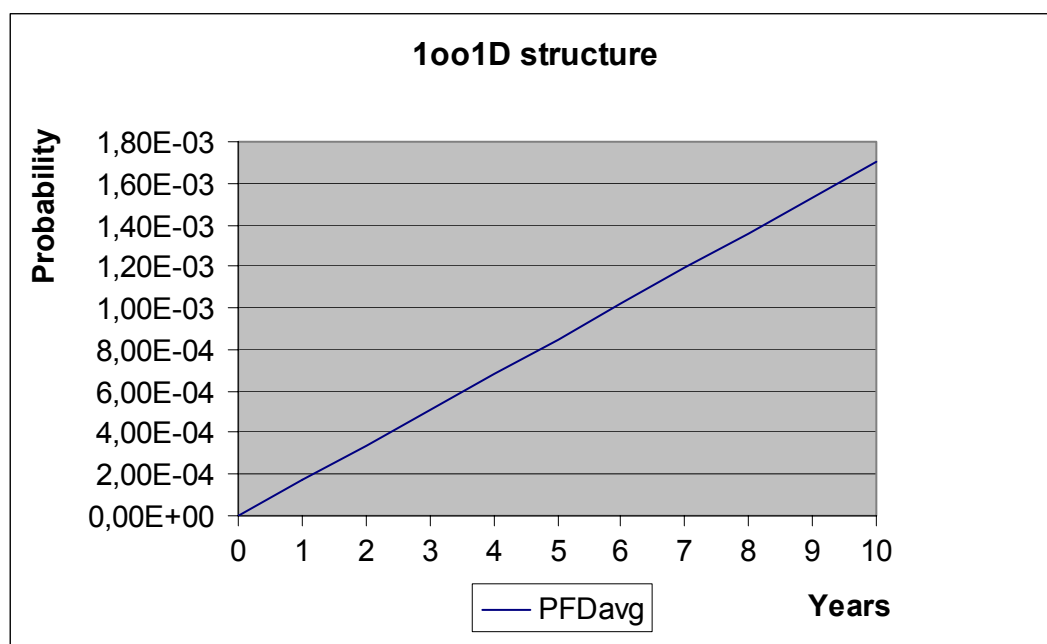


Figure 8: PFD_{AVG}(t)

5.6 DC Repeater KFD0-CS-(Ex)*.51(P) – current driver

The FMEDA carried out on KFD0-CS-(Ex)*.51(P) as current driver leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{low} + \lambda_{don't \text{ care}} + \lambda_{annunciation} = 5,51E-08 \text{ 1/h} + 6,13E-08 \text{ 1/h} + 1,35E-09 \text{ 1/h} = 1,18E-07 \text{ 1/h}$$

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

$$\lambda_{du} = 4,09E-08 \text{ 1/h}$$

$$\lambda_{total} = 1,59E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 0,00E-00 \text{ 1/h}$$

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	118 FIT	0 FIT	41 FIT	74,21%	0%	0%

The PFD_{AVG} 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} = 1.79E-04	PFD _{AVG} = 3.58E-04	PFD _{AVG} = 8.95E-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 9 shows the time dependent curve of PFD_{AVG}.

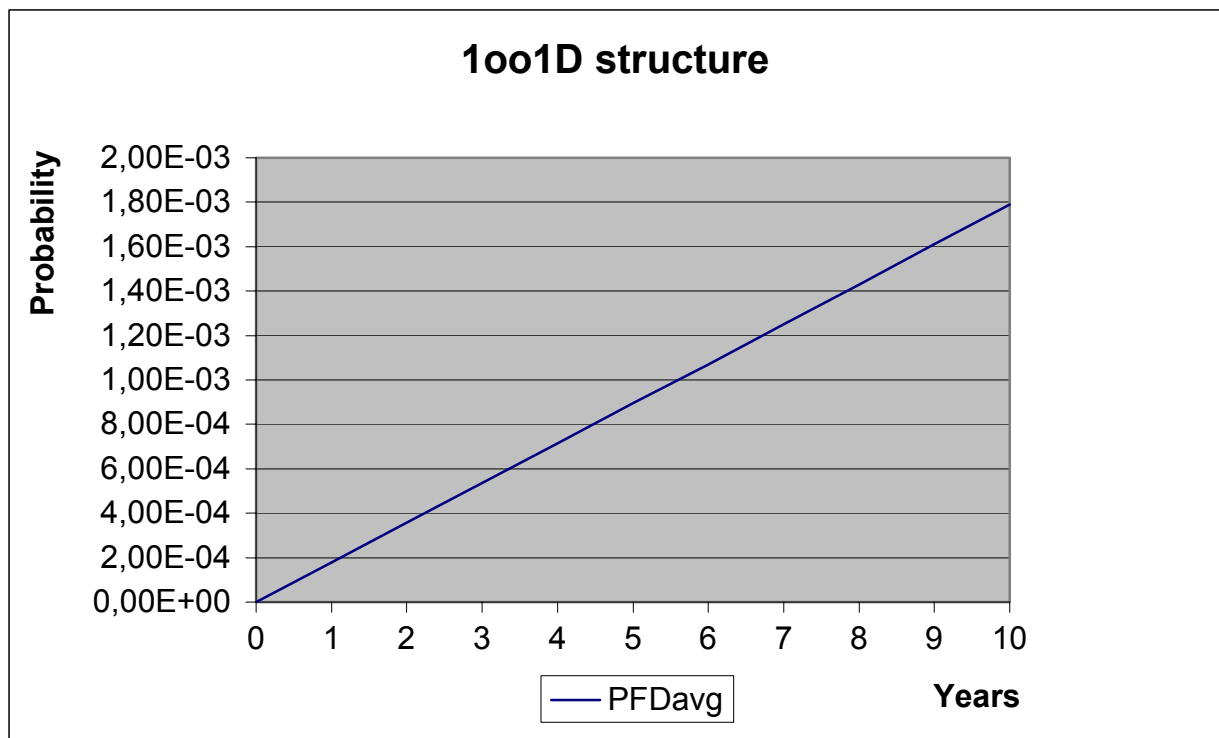


Figure 9: PFD_{AVG}(t)

5.7 DC Repeater KFD0-CS-(Ex)*.53(P) – current repeater

The FMEDA carried out on KFD0-CS-(Ex)*.53(P) as current repeater leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{su} + \lambda_{\text{don't care}} + \lambda_{\text{annunciation}} = 0,00E-00 \text{ 1/h} + 4,93E-08 \text{ 1/h} + 1,35E-09 \text{ 1/h} = 5,07E-08 \text{ 1/h}$$

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

$$\lambda_{du} = 9,28E-09 \text{ 1/h}$$

$$\lambda_{high} = 3,56E-08 \text{ 1/h}$$

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

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

$$\lambda_{\text{not part}} = 0,00E-00 \text{ 1/h}$$

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
Low trip	19 FIT	51 FIT	36 FIT	9 FIT	91,90%	27%	80%
High trip	36 FIT	51 FIT	19 FIT	9 FIT	91,90%	41%	68%

The PFD_{AVG} 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} = 4.07E-05	PFD _{AVG} = 8.13E-05	PFD _{AVG} = 2.03E-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 10 shows the time dependent curve of PFD_{AVG}.

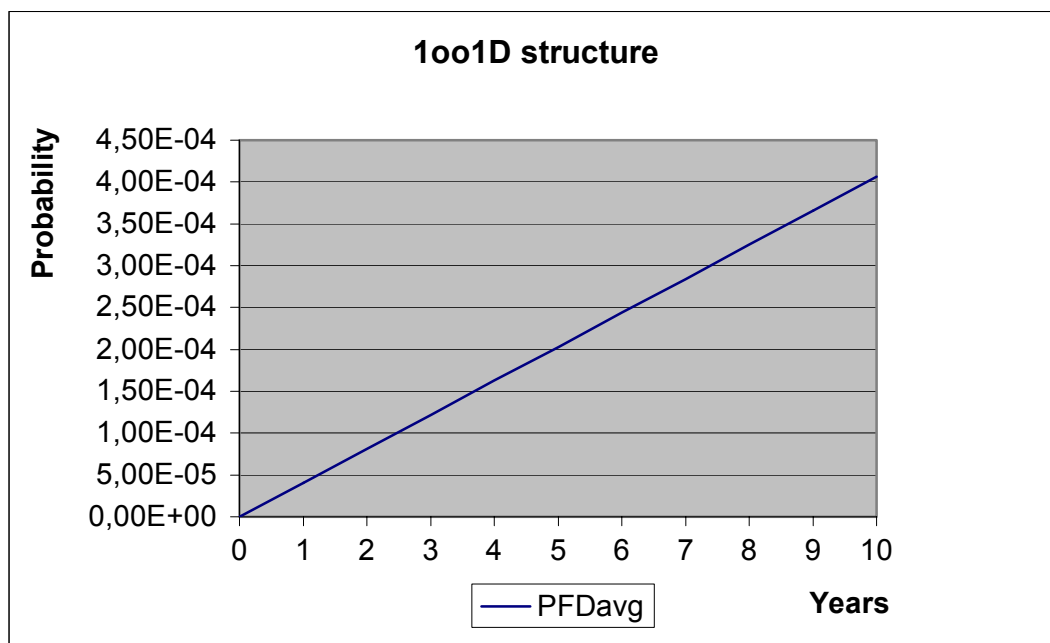


Figure 10: PFD_{AVG}(t)

5.8 DC Repeater KFD0-CS-(Ex)*.53(P) – current driver

The FMEDA carried out on KFD0-CS-(Ex)*.53(P) as current driver leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

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

$$\lambda_{su} = \lambda_{low} + \lambda_{don't \text{ care}} + \lambda_{annunciation} = 5,27E-08 \text{ 1/h} + 4,93E-08 \text{ 1/h} + 1,35E-09 \text{ 1/h} = 1,03E-07 \text{ 1/h}$$

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

$$\lambda_{du} = 1,13E-08 \text{ 1/h}$$

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

$$\lambda_{not \text{ part}} = 0,00E-00 \text{ 1/h}$$

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	103 FIT	0 FIT	11 FIT	90,16%	0%	0%

The PFD_{AVG} 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} = 4.94E-05	PFD _{AVG} = 9.88E-05	PFD _{AVG} = 2.47E-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 11 shows the time dependent curve of PFD_{AVG}.

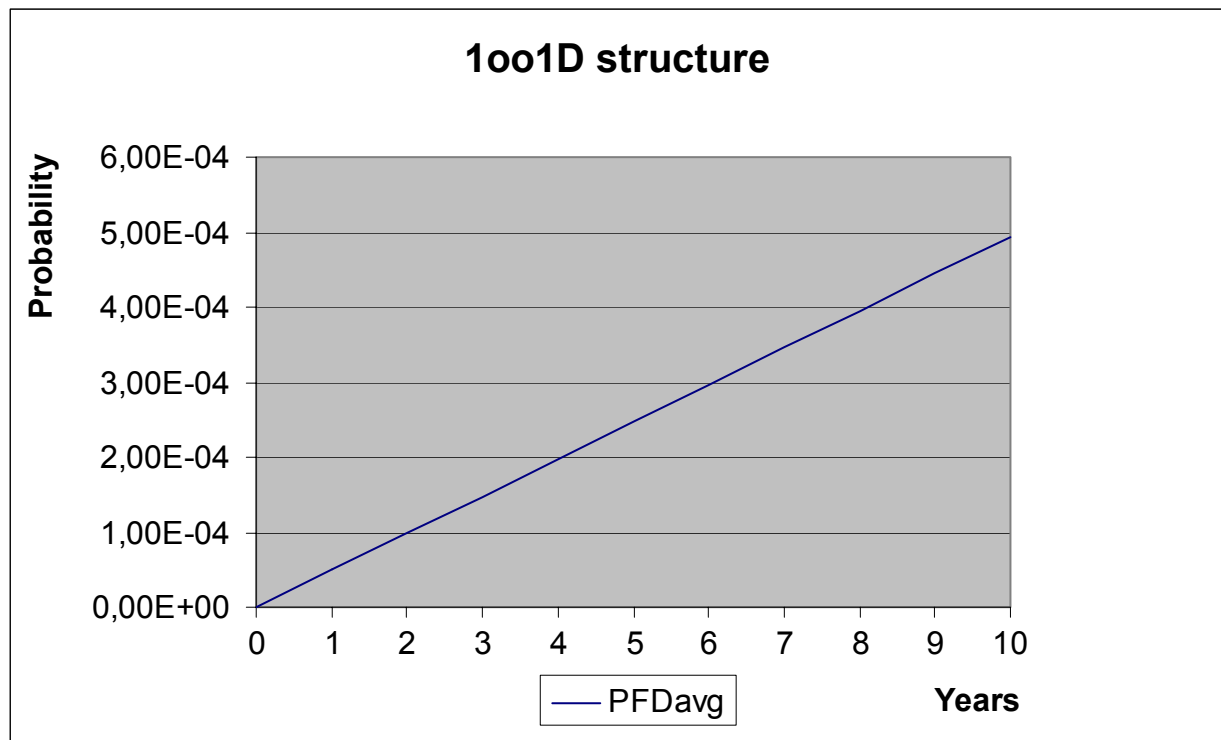


Figure 11: PFD_{AVG}(t)

6 Proven-in-use Assessment of KFD0-SCS-(Ex)1.55 and KFD0-CS-(Ex)*.5*(P)

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%⁵.

This is identical to the requirements on Type A (sub)-systems. The Smart Repeater KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) 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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

⁵ 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 ⁶
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 fail⁷ is low (<0,3% for SCS and <0,7% for CS). 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D8] to [D13]. 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 [D14] to [D17] and [D21] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience (Operating experience of more than 104.500.000 operating hours exists for SCS and more than 215.000.000 operating hours for CS. 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 [D21]
Adjustment of process-related parameters only	The user can enable or disable short circuit and lead breakage detection and change the mode of operation. For safety applications, however short circuit and lead breakage detection shall always be activated and the fail-safe state shall be configured as the outputs being de-energized.
Adjustment of process-related parameters is protected	Process related parameters can be protected by password.
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Smart Repeater KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) with a SFF of 60% - < 90% and a HFT = 0 can be considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

⁶ The numbering is based on the requirements detailed in appendix 1.

⁷ 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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD _{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
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

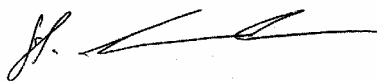
8.1 Liability

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: R1.2
Version History: V0, R1.0: Initial version, Sep. 18, 2003
V0, R1.1: Editorial changes, Name of KFD0-CS-Ex*.5*(P) corrected; Sep. 22, 2003
V1, R1.0: First released version, review comments integrated; Oct. 27, 2003
V1, R1.1: Changes after review by P+F; Dec. 4, 2003
V1, R1.2: Non-Ex versions added, report format updated; Jul. 18, 2005
Authors: Stephan Aschenbrenner
Review: V0, R1.1: Rachel van Beurden-Amkreutz (*exida*), Oct. 21, 2003
V1, R1.0: Harald Eschelbach (P+F), Nov. 18, 2003
Release status: Released to Pepperl+Fuchs

8.3 Release Signatures



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



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

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

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

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

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

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

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

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

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

(General Requirements)

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

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

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

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 19 to Table 22 show a sensitivity analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

Table 19: Sensitivity Analysis of dangerous undetected faults - KFD0-SCS-(Ex)1.55

Component	% of total λ_{du}	Detection through
H2	7,98%	100% functional test
H1	6,84%	100% functional test
H3	6,84%	100% functional test
D2	6,08%	100% functional test
C3	6,07%	100% functional test
C4	6,07%	100% functional test
C13	6,07%	100% functional test
C14	6,07%	100% functional test
C15	6,07%	100% functional test
C16	6,07%	100% functional test

Table 20: Sensitivity Analysis of dangerous undetected faults - KFD0-CS-(Ex)*.50(P)

Component	% of total λ_{du}	Detection through
VR4	40,82%	100% functional test
IC2	7,78%	100% functional test
VR1	5,83%	100% functional test
VR3	5,83%	100% functional test
TR2	5,54%	100% functional test
TR3	5,54%	100% functional test
TR1	4,86%	100% functional test
TR4	4,86%	100% functional test
IC1	3,11%	100% functional test
C3	1,94%	100% functional test

Table 21: Sensitivity Analysis of dangerous undetected faults - KFD0-CS-(Ex)*.51(P)

Component	% of total λ_{du}	Detection through
VR4	51,34%	100% functional test
IC2	9,78%	100% functional test
TR2	6,97%	100% functional test
TR3	6,97%	100% functional test
TR1	6,11%	100% functional test
TR4	6,11%	100% functional test
IC3	1,96%	100% functional test
IC6	1,47%	100% functional test
IC4	1,47%	100% functional test
IC5	1,47%	100% functional test

Table 22: Sensitivity Analysis of dangerous undetected faults - KFD0-CS-(Ex)*.53(P)

Component	% of total λ_{du}	Detection through
IC2	35,46%	100% functional test
TR4	22,16%	100% functional test
IC3	7,09%	100% functional test
IC4	5,32%	100% functional test
IC5	5,32%	100% functional test
IC6	5,32%	100% functional test
D5	4,43%	100% functional test
D6	4,43%	100% functional test
D7	4,43%	100% functional test
D8	4,43%	100% functional test

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 KFD0-SCS-(Ex)1.55 and DC Repeater KFD0-CS-(Ex)*.5*(P) 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.