



Failure Modes, Effects and Diagnostic Analysis

Project:

Smart Transmitter Isolators KFD2-STC(V)4-*** and KFD2-CR4-***

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 05/09-21

Report No.: P+F 05/09-21 R024

Version V3, Revision R1, August 2009

Stephan Aschenbrenner

Management summary

This report summarizes the results of the FMEDAs carried out on the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***. Table 1 gives an overview of the different types that belong to the considered smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***.

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

Table 1: Version overview

Type	Current source out	Current sink out	Voltage out	HART	Input config.	Channels ¹
KFD2-STC4-(Ex)1(.H)	X			X	2/3 wire	1 in, 1 out
KFD2-STC4-(Ex)1.2O(.H)	X			X	2/3 wire	1 in, 2 out
KFD2-STC4-(Ex)2(.H)	X			X	2 wire	2 in, 2 out
KFD2-STC4-(Ex)1(.H)-Y		X		X	2/3 wire	1 in, 1 out
KFD2-STC4-(Ex)1.2O(.H)-Y		X		X	2/3 wire	1 in, 2 out
KFD2-STC4-(Ex)2(.H)-Y		X		X	2 wire	2 in, 2 out
KFD2-STV4-(Ex)1-1(.H)			5V	X	2/3 wire	1 in, 1 out
KFD2-STV4-(Ex)1-2(.H)			10V	X	2/3 wire	1 in, 1 out
KFD2-STV4-(Ex)1.2O-1(.H)			5V	X	2/3 wire	1 in, 2 out
KFD2-STV4-(Ex)1.2O-2(.H)			10V	X	2/3 wire	1 in, 2 out
KFD2-STV4-(Ex)2-1(.H)			5V	X	2 wire	2 in, 2 out
KFD2-STV4-(Ex)2-2(.H)			10V	X	2 wire	2 in, 2 out
KFD2-CR4-(Ex)1	X				2/3 wire	1 in, 1 out
KFD2-CR4-(Ex)1.2O	X				2/3 wire	1 in, 2 out
KFD2-CR4-(Ex)2	X				2 wire	2 in, 2 out

Failure rates used in this analysis are basic failure rates from the Siemens standard SN 29500.

According to table 2 / 3 of IEC 61508-1 the PFD_{AVG} / PFH has to be $< 1.00E-03$ / $< 1.00E-07$ 1/h for SIL 3 safety functions and $< 1.00E-02$ / $< 1.00E-06$ 1/h for SIL 2 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to $1.00E-04$ / $1.00E-08$ 1/h for SIL 3 and better than or equal to $1.00E-03$ / $1.00E-07$ 1/h for SIL 2.

The modules under evaluation can be considered to be Type A² subsystems.

¹ The two channels on the *(Ex)2* boards shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

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

For **Type A** subsystems the SFF has to fulfill the requirements as stated in table 2 of IEC 61508-2 which are the following:

	Hardware fault tolerance (HFT)		
	0	1	2
SIL 2	$60\% \leq \text{SFF} < 90\%$	$\text{SFF} < 60\%$	
SIL 3	$90\% \leq \text{SFF} < 99\%$	$60\% \leq \text{SFF} < 90\%$	$\text{SFF} < 60\%$

The following tables show how the above stated requirements are fulfilled.

Table 2: Summary for all listed three wire input versions³ – Failure rates

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	118
Fail low (detected by the logic solver)	20
Fail High (detected by the logic solver)	98
Fail Dangerous Undetected	36
No Effect	192
Not part	212

Table 3: IEC 61508 failure rates

λ_{sd}	λ_{su} ⁴	λ_{dd}	λ_{du}	SFF	DC _s ⁵	DC _D ⁵
0 FIT	192 FIT	118 FIT	36 FIT	89%	0%	76%

Table 4: PFH⁶ / PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 3,60E-08 1/h	PFD _{AVG} = 1,58E-04	PFD _{AVG} = 3,15E-04	PFD _{AVG} = 7,88E-04

The boxes marked in green (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 or 1,00E-07 1/h respectively.

³ The results are based on the FMEDA carried out at the KFD2-STC4-Ex1 version but is considered to be representative for all listed three-wire input boards.

⁴ Note that the SU category includes failures that do not cause a spurious trip

⁵ DC means the diagnostic coverage (safe or dangerous) for the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-*** by the safety logic solver.

⁶ It is assumed that the connected logic solver can detect the output state within a time that allows reacting within the process safety time.

Table 5: Summary for all listed two wire input versions ⁷ – Failure rates

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	111
Fail low (detected by the logic solver)	21
Fail High (detected by the logic solver)	90
Fail Dangerous Undetected	36
No Effect	165
Not part	111

Table 6: IEC 61508 failure rates

λ_{sd}	λ_{su}^4	λ_{dd}	λ_{du}	SFF	DC _S ⁵	DC _D ⁵
0 FIT	165 FIT	111 FIT	36 FIT	88%	0%	75%

Table 7: PFH ⁶ / PFD_{AVG} values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 3,60E-08 1/h	PFD_{AVG} = 1,58E-04	PFD_{AVG} = 3,15E-04	PFD_{AVG} = 7,88E-04

The boxes marked in green (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 or 1,00E-07 1/h respectively.

⁷ The results are based on the FMEDA carried out at the KFD2-STC(V)4-Ex2 version but is considered to be representative for all listed two-wire input boards.

Table 8: Summary for all listed *1.2O* versions ⁸ – Failure rates of input part (HFT=0)

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	71
Fail low (detected by the logic solver)	67
Fail High (detected by the logic solver)	4
Fail Dangerous Undetected	14
No Effect	120
Not part	107

Table 9: IEC 61508 failure rates

λ_{sd}	λ_{su} ⁴	λ_{dd}	λ_{du}	SFF	DC _S ⁵	DC _D ⁵
0 FIT	120 FIT	71 FIT	14 FIT	93%	0%	83%

Table 10: Summary for all listed *1.2O* versions ⁸ – Failure rates of output part (HFT=1)

Failure category	Failure rates (in FIT) ⁹
Fail Dangerous Detected	96
Fail low (detected by the logic solver)	64
Fail High (detected by the logic solver)	32
Fail Dangerous Undetected	44
No Effect	144
Not part	205

Table 11: IEC 61508 failure rates

λ_{sd}	λ_{su} ⁴	λ_{dd}	λ_{du}	SFF	DC _S ⁵	DC _D ⁵
0 FIT	144 FIT	96 FIT	44 FIT	84%	0%	68%

Table 12: PFH ⁶ / PFD_{AVG} values for all listed *1.2O* versions ⁸

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 1,66E-08 1/h	PFD _{AVG} = 7,26E-05	PFD _{AVG} = 1,45E-04	PFD _{AVG} = 3,63E-04

⁸ The outputs of the *1.2O* modules are redundantly evaluated by a SIL3 compliant safety system and treated as a 1oo2 system.

⁹ The failure rates are the ones of one channel.

The boxes marked in yellow (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 3 according to table 2 / 3 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 $1,00E-04$ or $1,00E-08$ 1/h respectively. The box marked in green (■) mean that the calculated PFD_{AVG} value is within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-04$.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of $40^{\circ}C$. For a higher average temperature of $60^{\circ}C$, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-*** 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). A full table of failure rates is presented in sections 5.1 to 5.3 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category 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 failure rates are valid for the useful life of the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***, which is estimated to be 10 years (see Appendix 3).



Table of Contents

Management summary	2
1 Purpose and Scope	8
2 Project management.....	9
2.1 <i>exida</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</i>	10
3 Description of the analyzed modules	11
3.1 KFD2-STC(V)4-Ex1.2O	11
3.2 KFD2-STC(V)4-Ex2	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 Assumptions.....	14
5 Results of the assessment.....	15
5.1 KFD2-STC(V)4-(Ex)1... three-wire input boards	18
5.2 KFD2-STC(V)4-(Ex)2... two-wire input boards	20
5.3 *1.2O* boards	22
6 Terms and Definitions	24
7 Status of the document.....	25
7.1 Liability.....	25
7.2 Releases	25
7.3 Release Signatures.....	25
Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test ..	26
Appendix 2.1: Possible proof tests to detect dangerous undetected faults.....	28
Appendix 3: Impact of lifetime of critical components on the failure rate	29

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

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

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

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

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

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of the FMEDAs carried out on the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***.

It shall be assessed whether these devices meet the average Probability of Failure on Demand (PFD_{AVG}) requirements for low demand mode or the Probability of a dangerous failure per hour for high demand mode and the architectural constraints for SIL 2 / SIL 3 subsystems according to IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.



2 Project management

2.1 exida

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a partnership company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Pepperl+Fuchs Manufacturer of the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***.

exida Performed the hardware assessment according to option 1 (see section 1).

Pepperl+Fuchs GmbH contracted *exida* in September 2005 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2.3 Standards / Literature used

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

N1	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	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]	251-5048B of 10.05.04	Circuit diagram "KFD2-CR4-Ex1(.20)... & KFD2-STC(V)4-Ex1(.20)..."
[D2]	251-5057 of 10.03.04	Circuit diagram "KFD2-CR4-Ex2... & KFD2-STC(V)4-Ex2..."
[D3]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D4]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D5]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D6]	Verkaufszahlen STC4.xls	Statistics of field-feed-back tracking; sold devices
[D7]	3005327A.PDF	Change notice
[D8]	3005366A.PDF	Change notice
[D9]	Email "AW STC4 (neu) Stückzahlen.msg" of 08.11.05	Description of application examples
[D10]	Email "WG STC4 (neu) Rückläufer.msg" of 08.11.05 and email "RE customer returns.msg" of 11.11.05	Statistics of field-feed-back tracking; returned devices
[D11]	STÜLI Vergleich STC4 Versionen.xls of 30.09.08	Parts list comparison between original versions and new (.H) versions
[D12]	DB 192017 STC4-H.pdf	Data sheet "KFD2-STC4-Ex1.H"
[D13]	Impact Analysis FS-0033EA-25.doc	Impact analysis
[D14]	2515048c.pdf	Circuit diagram "KFD2-CR4-Ex1(.20)... & KFD2-STC(V)4-Ex1(.20)..." 251-5048C
[D15]	FMEDA_2_ STC4120 Ex1_SIL3_PT.xls of 18.06.09	
[D16]	FMEDA V6 STC4 Ex1 V1R6.xls of 18.06.09	

2.4.2 Documentation generated by exida

[R1]	FMEDA V6 STC4 Ex1 V1R5.xls of 18.10.05
[R2]	FMEDA V6 STC4 Ex2 V1R1.xls of 18.10.05
[R3]	FMEDA V6 STC4-20 Ex1 HFT0 V1R0.xls of 20.07.09
[R4]	FMEDA V6 STC4-20 Ex1 HFT1 V1R0.xls of 21.07.09
[R5]	Field data evaluation.xls of 09.11.05 (Field data evaluation of operating hours, sold devices and returned devices)

3 Description of the analyzed modules

3.1 KFD2-STC(V)4-Ex1.20

The KFD2-STC(V)4-Ex1.20 board provides a transformer isolated power supply for a transmitter located in a potentially explosive atmosphere. The transmitter may be a three-wire transmitter, a two-wire current sink or a two-wire current source one. The device itself must be located in the safe area. The field current drawn by the transmitter is repeated as two currents in the safe area. The safe area output signals are isolated from the power supply and from each other. The power supply and output terminals are isolated from the hazardous area terminals.

In addition to the transfer of analog current signals from the hazardous area, the unit will transfer signals in the form of an alternating current from the hazardous area or an alternating voltage from the safe area. This allows bi-directional communication between a smart transmitter located in the field and suitable equipment located in the safe area.

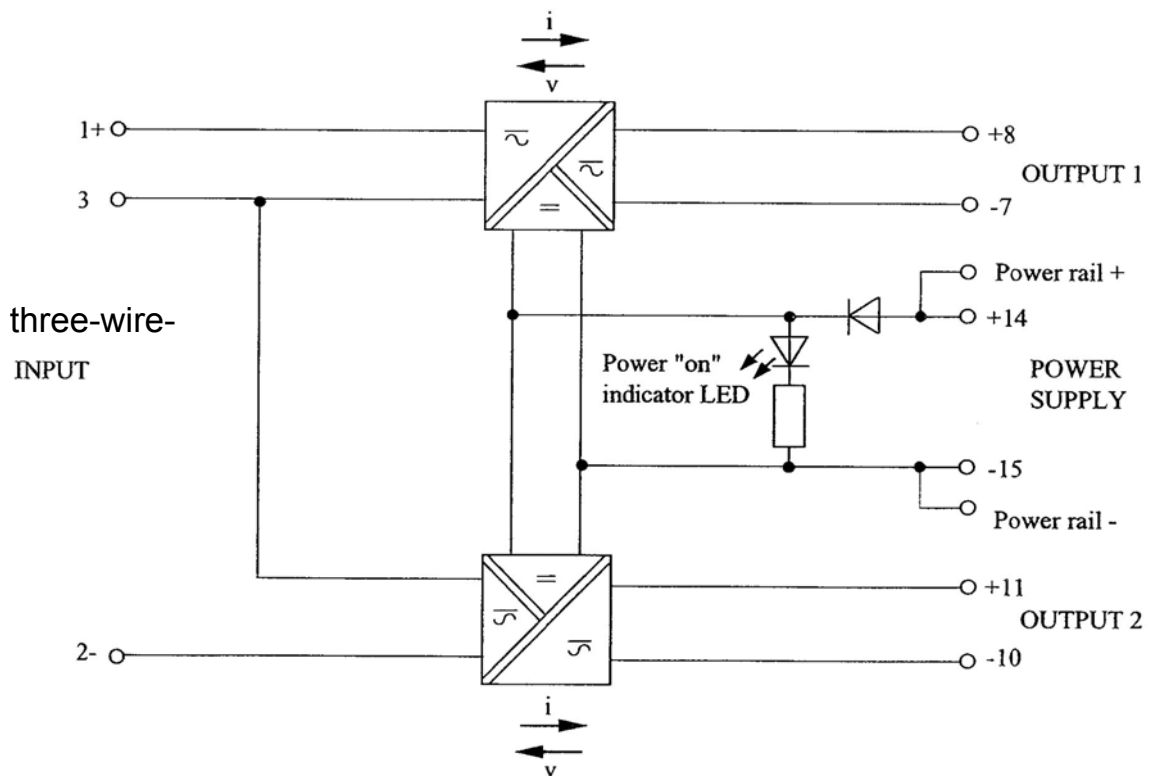


Figure 1: Block diagram of KFD2-STC(V)4-Ex1.20

Remark: The description above is valid accordingly for all other three-wire input channel versions with the exception that this version has two output channels. The differences between the versions are described in Table 1.

3.2 KFD2-STC(V)4-Ex2

The KFD2-STC(V)4-Ex2 is a two channel transformer isolated device providing fully floating power supply for transmitters located in a potentially explosive atmosphere. The device itself must be located in the safe area. The field current drawn by each transmitter is repeated as an identical current in the safe area. The safe area output signal is isolated from the power supply but the two may be connected together externally if required. The power supply and output terminals are isolated from the hazardous area terminals.

In addition to the transfer of analog current signals from the hazardous area, the unit will transfer signals in the form of an alternating current from the hazardous area or an alternating voltage from the safe area. This allows bi-directional communication between a smart transmitter located in the field and suitable equipment located in the safe area.

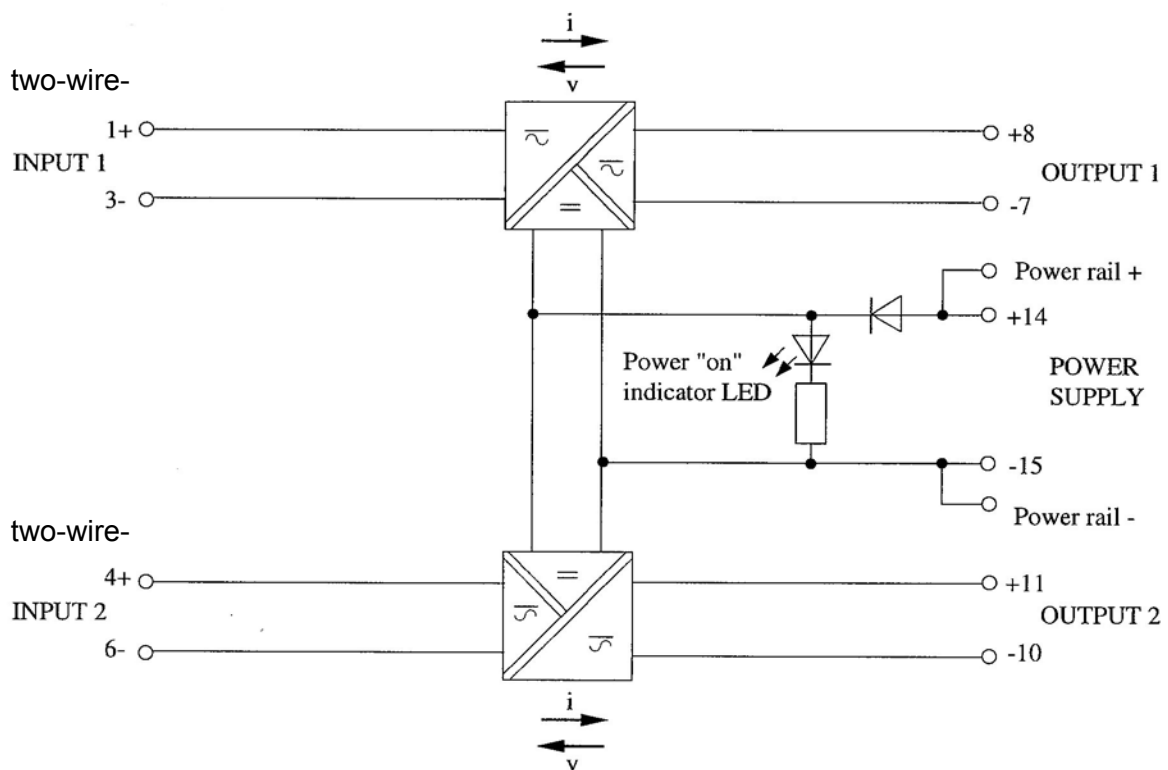


Figure 2: Block diagram of KFD2-STC(V)4-Ex2

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs GmbH and is documented in [R1] to [R4].

4.1 Description of the failure categories

In order to judge the failure behavior of the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output exceeding the user defined threshold.
Fail Safe	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.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (> 20 mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 4 mA)
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function or deviates the output current by not more than 2% full scale. For the calculation of the SFF it is treated like a safe undetected failure.
Not part	Failures of a component which 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.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a fail low or fail high may be detected or undetected depending on the programming of the safety logic solver. Consequently during a Safety Integrity Level (SIL) verification assessment the fail high and fail low categories need to be classified as either detected or undetected.

The "No Effect" failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the "No Effect" failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

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

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***.

- 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 during normal operation.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The two channels on the *(Ex)2* boards are not used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function.
- For SIL3 applications the outputs of the *1.20* modules are redundantly evaluated by a SIL3 compliant safety system and treated as a 1oo2 system.
- The time to restoration after a safe failure is 8 hours.
- The calculation was done for both, the low demand mode and the high demand mode of operation.

- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HDBK-217F. Alternatively, the assumed environment is similar to:
 - IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.
- The application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.

5 Results of the assessment

exida did the FMEDAs together with Pepperl+Fuchs.

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

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

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

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

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

For the *1.20* modules the shut-down path can be redundantly evaluated by a safety system as shown in Figure 3. Therefore these modules were split into two separate subsystems; one representing the single channel input part having a hardware fault tolerance of 0 and one representing the output part having a hardware fault tolerance of 1. This separation is illustrated in Figure 4.

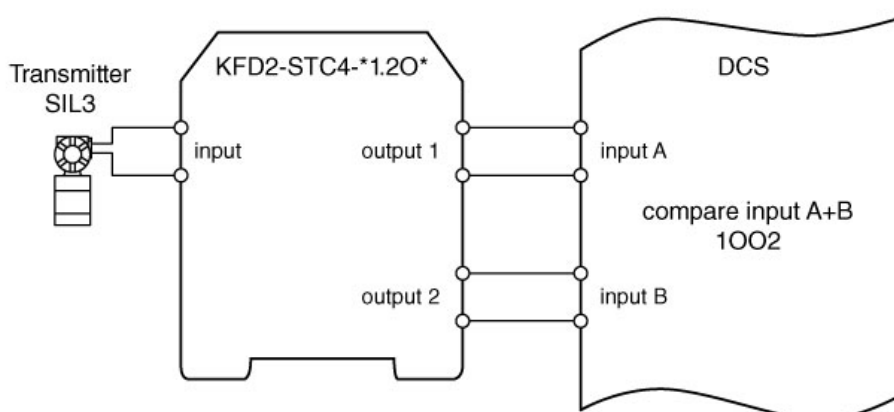


Figure 3: Connection between the *1.20* modules and a safety system

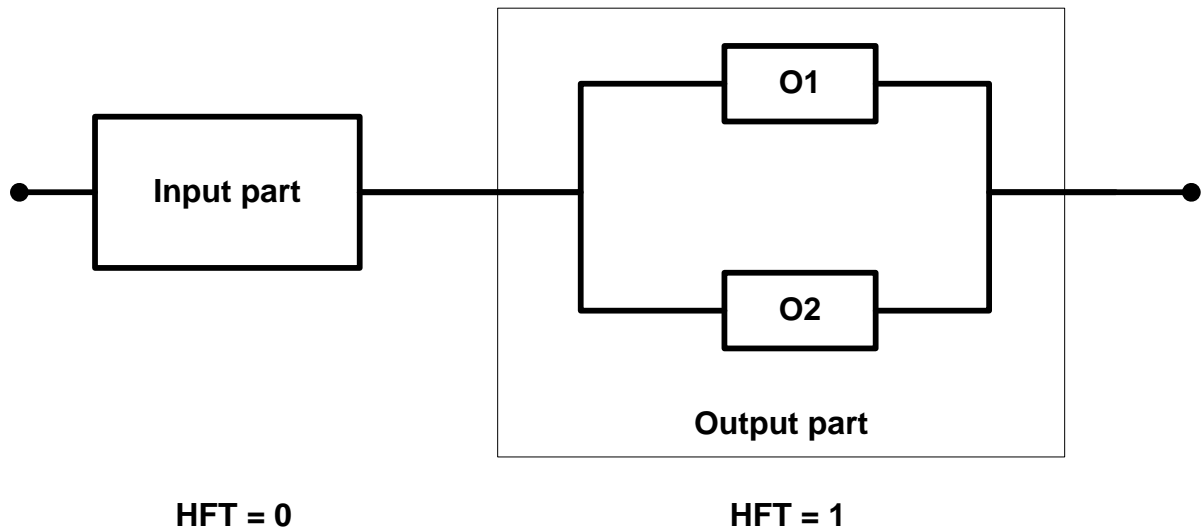


Figure 4: Separation of the *1.20* modules into two subsystems

For the calculation of the PFD_{AVG} the following Markov models for a 1oo1 and a 1oo2 system were used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

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

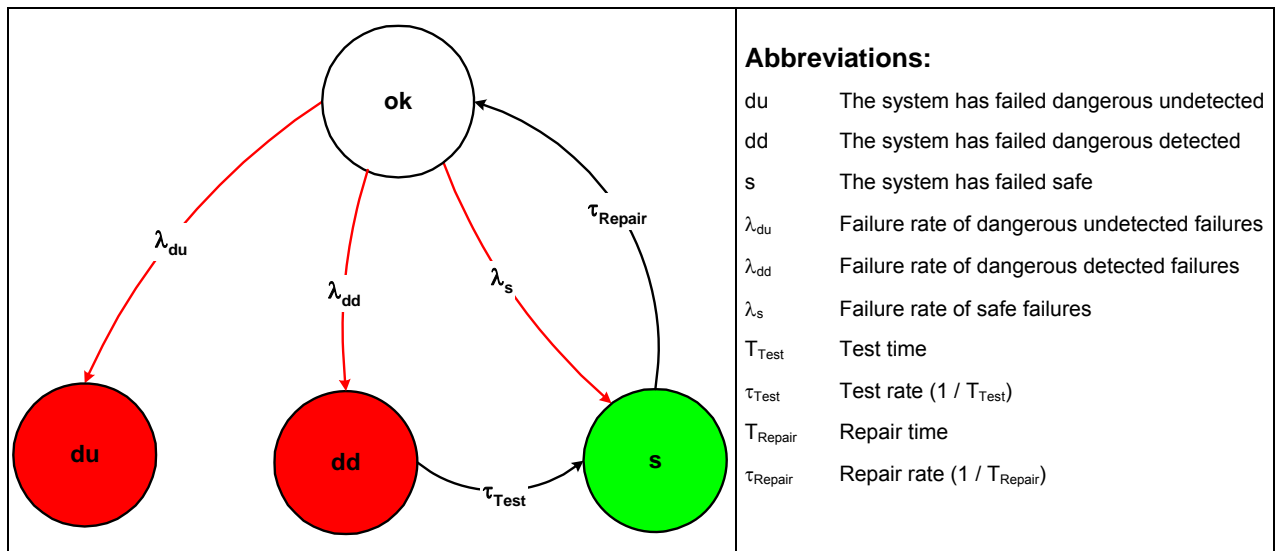


Figure 5: Markov model for a 1oo1 structure

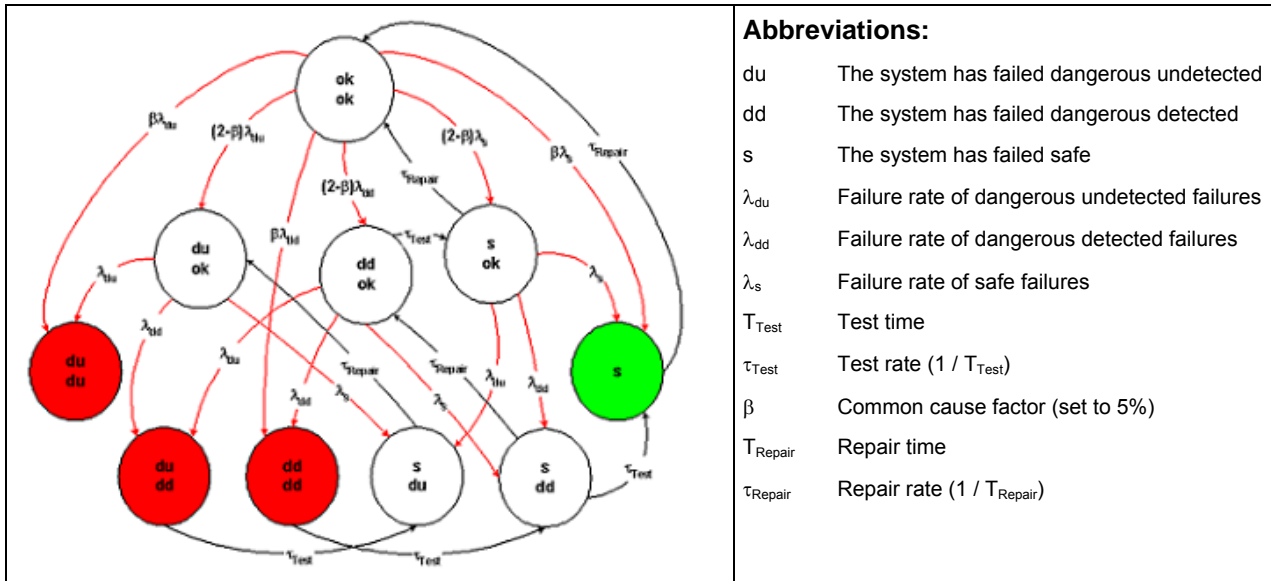


Figure 6: Markov model for a 1oo2 architecture

5.1 KFD2-STC(V)4-(Ex)1... three-wire input boards

The FMEDA carried out on the KFD2-STC(V)4-Ex1 board, which is considered to be representative for all listed three-wire input boards, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

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

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

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

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

$$\lambda_{high} = 2,00E-08 \text{ 1/h}$$

$$\lambda_{low} = 9,84E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,92E-07 \text{ 1/h}$$

$$\lambda_{total} = 3,46E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,12E-07 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 205 \text{ years}$$

These failure rates can be turned over into the following typical failure rates:

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	118
Fail High (detected by the logic solver)	20
Fail low (detected by the logic solver)	98
Fail Dangerous Undetected	36
No Effect	192
Not part	212

Under the assumptions described in section 4.2.3 and 5 the following tables show the failure rates according to IEC 61508:

λ_{sd}	λ_{su}^{10}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	192 FIT	118 FIT	36 FIT	89,60%	0%	76%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 5.

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 3,60E-08 1/h	PFD_{AVG} = 1,58E-04	PFD_{AVG} = 3,15E-04	PFD_{AVG} = 7,88E-04

The boxes marked in green () mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 or 1,00E-07 1/h respectively.

¹⁰ Note that the SU category includes failures that do not cause a spurious trip

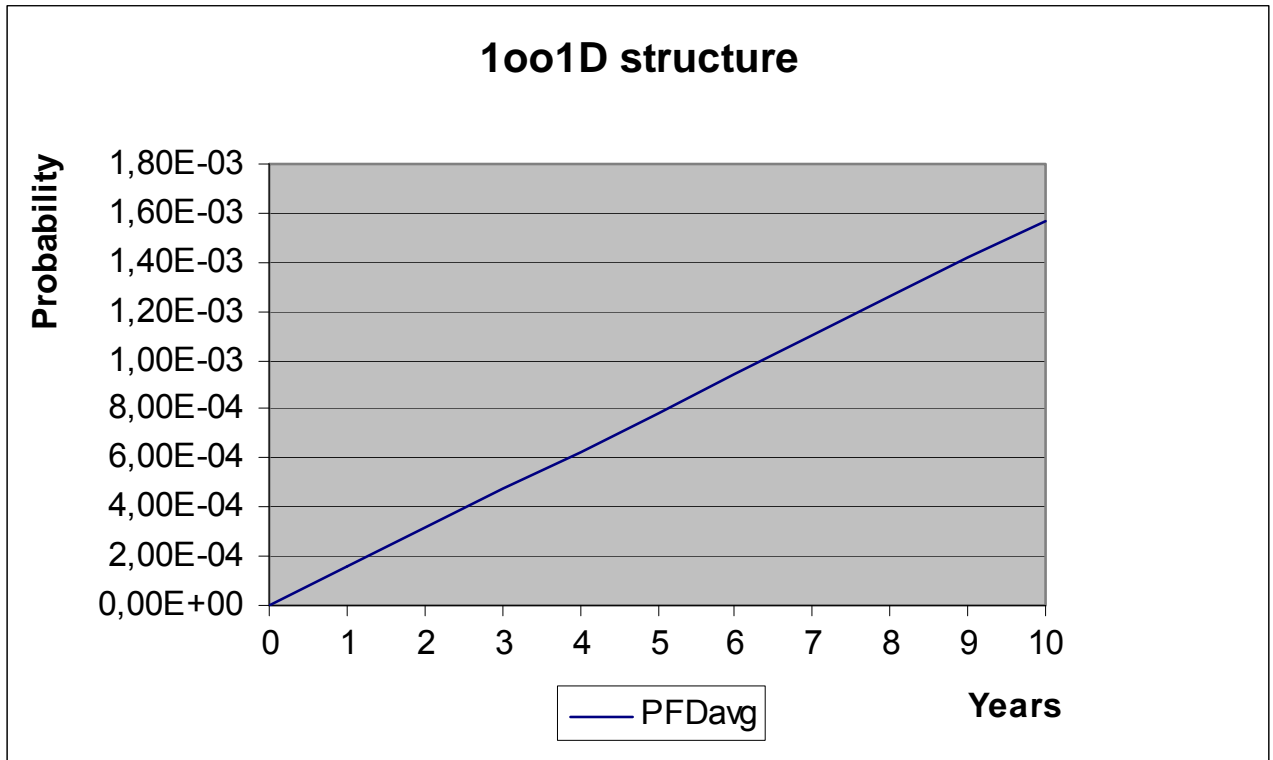


Figure 7: PFD_{AVG}(t)

5.2 KFD2-STC(V)4-(Ex)2... two-wire input boards

The FMEDA carried out on the KFD2-STC(V)4-Ex2 board, which is considered to be representative for all listed two-wire input boards, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

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

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

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

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

$$\lambda_{high} = 2,10E-08 \text{ 1/h}$$

$$\lambda_{low} = 8,98E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,65E-07 \text{ 1/h}$$

$$\lambda_{total} = 3,12E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 1,11E-07 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 270 \text{ years}$$

These failure rates can be turned over into the following typical failure rates:

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	111
Fail High (detected by the logic solver)	21
Fail low (detected by the logic solver)	90
Fail Dangerous Undetected	36
No Effect	165
Not part	111

Under the assumptions described in section 4.2.3 and 5 the following tables show the failure rates according to IEC 61508:

λ_{sd}	λ_{su}^{11}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
0 FIT	165 FIT	111 FIT	36 FIT	88,45%	0%	75%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 5.

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 3,60E-08 1/h	PFD _{AVG} = 1,58E-04	PFD _{AVG} = 3,15E-04	PFD _{AVG} = 7,88E-04

The boxes marked in green (■) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 or 1,00E-07 1/h respectively.

¹¹ Note that the SU category includes failures that do not cause a spurious trip

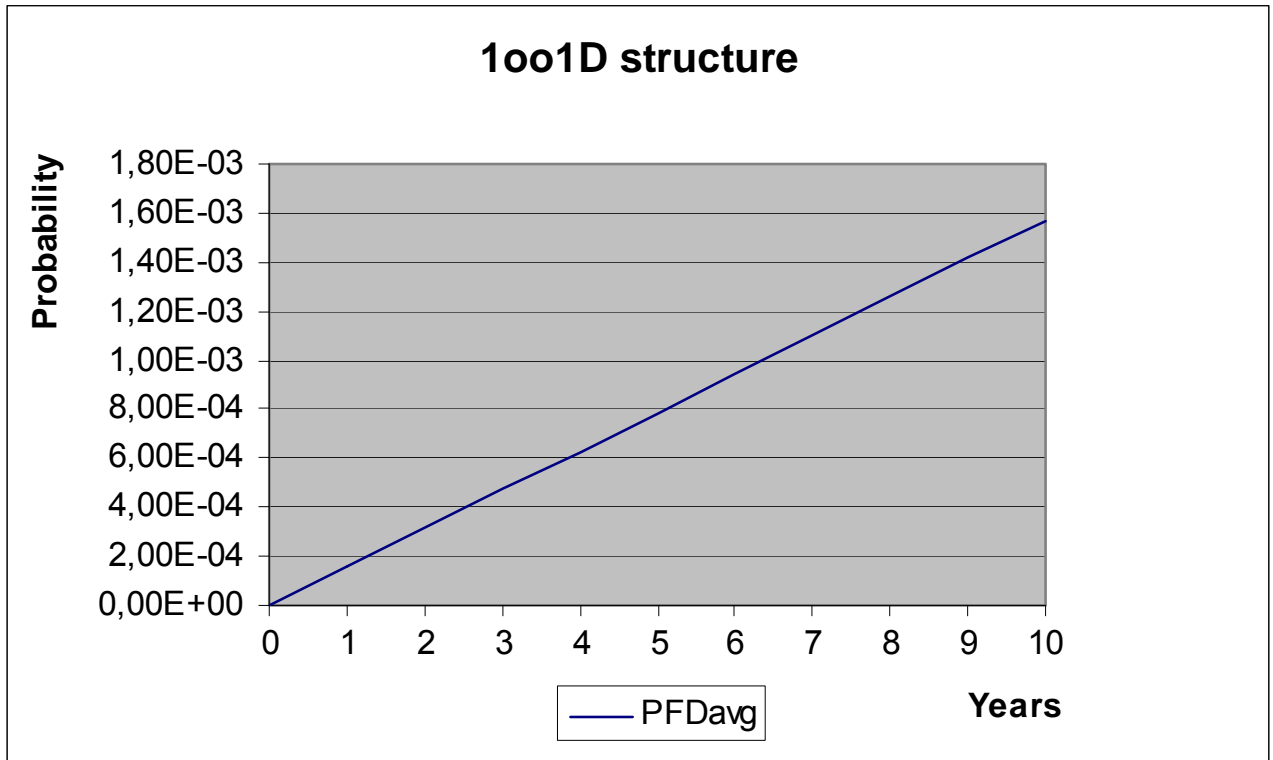


Figure 8: PFD_{AVG}(t)

5.3 *1.20* boards

The FMEDA carried out on the *1.20* boards when redundantly evaluated by a safety system, leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

Input part:

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

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

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

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

$$\lambda_{high} = 4,30E-09 \text{ 1/h}$$

$$\lambda_{low} = 6,73E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,20E-07 \text{ 1/h}$$

$$\lambda_{total} = 2,06E-07 \text{ 1/h}$$

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

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 364 \text{ years}$$

$$SFF = 93,04\% \text{ (HFT} = 0)$$

Redundant output part:

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

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

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

$$\lambda_{du} = 4,38E-08 \text{ 1/h}$$

$$\lambda_{high} = 3,15E-08 \text{ 1/h}$$

$$\lambda_{low} = 6,38E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,44E-07 \text{ 1/h}$$

$$\lambda_{total} = 2,84E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 2,05E-07 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 234 \text{ years}$$

$$SFF = 84,54\% \text{ (HFT} = 1)$$

NOTE: The failure rates are the ones of one channel.

The PFD_{AVG} / PFH value for the *1.20* boards is the sum of the two PFD_{AVG} / PFH values for the two sub-systems.

The PFD_{AVG} was calculated for three different proof test times using the Markov models as described in Figure 5 and Figure 6 considering a common cause factor of $\beta = 5\%$ for the redundant part (max. common cause factor for a logic sub-system according to IEC 61508-6).

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 1,66E-08 1/h	PFD _{AVG} = 7,26E-05	PFD _{AVG} = 1,45E-04	PFD _{AVG} = 3,63E-04

The boxes marked in yellow (□) mean that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 3 according to table 2 / 3 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-04 or 1,00E-08 1/h respectively. The box marked in green (■) mean that the calculated PFD_{AVG} value is within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-04.

6 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 Modes, Effects, and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
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.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTTR	Mean Time To Restoration
PFD _{AVG}	Average Probability of Failure on Demand
PFH	Probability of a dangerous failure per hour
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type A subsystem	"Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

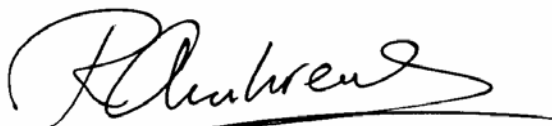
Version History: V3R1: Editorial changes; August 15, 2009
V3R0: Redundant evaluation of *1.20* boards added; July 30, 2009
V2, R3: Versions (.H) added, October 17, 2008
V2, R2: Released version after review, February 8, 2008
V2, R1: Internal review by Stephan Aschenbrenner
V2, R0: Addition of the High demand mode, January 31, 2008
V1, R1.0: Released version after review, November 24, 2005
V0, R1.0: Initial version, Nov. 8, 2005

Authors: Stephan Aschenbrenner

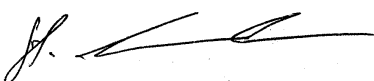
Review: V0, R1.0: Rachel Amkreutz (*exida*); November 18, 2005
Harald Eschelbach (P+F); November 23, 2005

Release status: Released to Pepperl + Fuchs GmbH

7.3 Release Signatures

A handwritten signature in black ink, appearing to read "R. Amkreutz", written over a horizontal line.

Rachel Amkreutz, Safety Engineer

A handwritten signature in black ink, appearing to read "S. Aschenbrenner", written over a horizontal line.

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

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

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Table 13 and Table 14 show an importance analysis of the ten most critical dangerous undetected faults and indicate how these faults can be detected during proof testing.

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

Table 13: KFD2-STC(V)4-(Ex)1... three-wire input boards

Component	% of total λ_{du}	Detection through
IC01	8,34%	100% functional test with monitoring of the expected output signal
T101	8,34%	100% functional test with monitoring of the expected output signal
P002	4,59%	100% functional test with monitoring of the expected output signal
P003	4,59%	100% functional test with monitoring of the expected output signal
C116	4,17%	100% functional test with monitoring of the expected output signal
N101	4,45%	100% functional test with monitoring of the expected output signal
N102	4,45%	100% functional test with monitoring of the expected output signal
C006	3,47%	100% functional test with monitoring of the expected output signal
IC02	3,34%	100% functional test with monitoring of the expected output signal
IC04	3,34%	100% functional test with monitoring of the expected output signal

Table 14: KFD2-STC(V)4-(Ex)2... two-wire input boards

Component	% of total λ_{du}	Detection through
IC01	8,34%	100% functional test with monitoring of the expected output signal
T101	8,34%	100% functional test with monitoring of the expected output signal
P002	4,59%	100% functional test with monitoring of the expected output signal
P100	4,59%	100% functional test with monitoring of the expected output signal
C127	4,17%	100% functional test with monitoring of the expected output signal
N102	4,45%	100% functional test with monitoring of the expected output signal
N103	4,45%	100% functional test with monitoring of the expected output signal
C006	3,47%	100% functional test with monitoring of the expected output signal
IC02	3,34%	100% functional test with monitoring of the expected output signal
IC12	3,34%	100% functional test with monitoring of the expected output signal

Appendix 2.1: Possible proof tests to detect dangerous undetected faults

Proof test 1 consists of the following steps, as described in Table 15.

Table 15 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Force the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-*** 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	Force the smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-*** 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 smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***.

Proof test 2 consists of the following steps, as described in Table 16.

Table 16 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 smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-*** 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 smart transmitter isolators KFD2-STC(V)4-*** and KFD2-CR4-***.

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 4.2.3) 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 which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

Table 17 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 17: Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Name	Schematic	Useful life at 40°C
Capacitor (electrolytic) - Aluminum electrolytic, solid electrolyte	C006	251-5048B 251-5057	Appr. 90 000 Hours ¹²

As the capacitors are the limiting factors with regard to the useful lifetime of the system, the useful lifetime should be limited to 10 years.

¹² The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.