FMEDA and Proven-in-use Assessment

Project:
Universal Frequency Converter (UFC) and Rotation Speed Monitor (DWB)

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 04/03-15
Report No.: P+F 04/03-15 R016
Version V2, Revision R3, September 2007
Stephan Aschenbrenner

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

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Universal Frequency Converters (UFC) with software version 3.00 without display and 4.00 with display and the Rotation Speed Monitors (DWB) with software version 1.24. Table 1 gives an overview of the different versions that belong to the considered devices.

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

Version	Type	Circuit diagram
V1	KFU8-UFC using the current output as safety function	01-6987B „KF**-UFC-**1.* - Amplifier“ 01-7308 „KFU8-… Netzteil / power supply“
V2	KFU8-UFC using the transistor output as safety function	01-6987B „KF**-UFC-**1.* - Amplifier“ 01-7308 „KFU8-… Netzteil / power supply“
V3	KFU8-UFC/DWB using the relay output as safety function	01-6987B „KF**-UFC-**1.* - Amplifier“ 01-7308 „KFU8-… Netzteil / power supply“
V4	KFD2-UFC/DWB using the relay output as safety function	01-6988B „KF**-DWB-**1.D - Amplifier“ 01-7317B „KFD2- Netzteil / power supply“
V5	KFA5/6-DWB using the relay output as safety function	01-6988B „KF**-DWB-**1.D - Amplifier“ 01-4521C „KFA.-D..-…“
V6	KFD2-UFC using the current output as safety function	01-6987B „KF**-UFC-**1.* - Amplifier“ 01-7317B „KFD2- Netzteil / power supply“
V7	KFD2-UFC using the transistor output as safety function	01-6987B „KF**-UFC-**1.* - Amplifier“ 01-7317B „KFD2- Netzteil / power supply“

The different UFC can be equipped with or without display.

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

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be ≥ 1,00E-03 to < 1,00E-02 for SIL 2 safety functions. For systems operating in high demand or continuous mode of operation the PFH value has to be ≥ 1,00E-07 1/h to < 1,00E-06 1/h for SIL 2 safety functions according to table 3 of IEC 61508-1.

For a SIL 2 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value would then be 1,00E-03.

For a SIL 2 application operating in high demand mode of operation the total PFH value of the SIF should be smaller than 1,00E-06 1/h, hence the maximum allowable PFH value would then be 1,00E-07 1/h.

The devices of Table 1 are considered to be Type B[1] components with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

As the above described devices are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the devices 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 5.7.2 the devices are suitable to be used, as a single device, for SIL 2 safety functions.

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

Low / high demand mode of operation and fault reaction time = 5 minutes [2]

Table 2: KFU8-UFC with current output – Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**274**
Fail detected (internal diagnostics or indirectly[3])	140
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	132
Fail Dangerous Undetected	**75**
No Effect	**192**
Annunciation Undetected	**13**
Not part	**34**

Table 3: KFU8-UFC with current output – IEC 61508 failure rates

λ_{SD}	λ_{SU} [4]	λ_{DD}	λ_{DU}	**SFF**	**DC_S [5]**	**DC_D [5]**
0 FIT	205 FIT	274 FIT	75 FIT	86%	0%	78%

Table 4: KFU8-UFC with current output – PFD_{AVG} / PFH values

	T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFH = 7,54E-08 1/h	**PFD_{AVG} = 3,30E-04**	**PFD_{AVG} = 6,60E-04**	**PFD_{AVG} = 1,65E-03**

[1] Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

[2] A fault reaction time of 5 minutes requires also that a connected device can detect the output state within a time that allows reacting within the process safety time.

[3] “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

[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 temperature converters KF**-GUT-(Ex)1.D with trip relays by the safety logic solver.

Table 5: KFU8-UFC with transistor output – Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC$_S$	DC$_D$
41 FIT	392 FIT	61 FIT	84 FIT	85%	9%	42%

Table 6: KFU8-UFC with transistor output – PFD$_{AVG}$ / PFH values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 8,37E-08 1/h	PFD$_{AVG}$ = 3.67E-04	PFD$_{AVG}$ = 7.33E-04	PFD$_{AVG}$ = 1.83E-03

Table 7: KFU8-UFC/DWB with relay output – Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC$_S$	DC$_D$
41 FIT	409 FIT	61 FIT	101 FIT	83%	9%	37%

Table 8: KFU8-UFC/DWB with relay output – PFD$_{AVG}$ / PFH values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 1,01E-07 1/h	PFD$_{AVG}$ = 4.41E-04	PFD$_{AVG}$ = 8.81E-04	PFD$_{AVG}$ = 2.20E-03

Table 9: KFD2-UFC/DWB with relay output – Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC$_S$	DC$_D$
41 FIT	332 FIT	52 FIT	107 FIT	79%	10%	32%

Table 10: KFD2-UFC/DWB with relay output – PFD$_{AVG}$ / PFH values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 1,07E-07 1/h	PFD$_{AVG}$ = 4.66E-04	PFD$_{AVG}$ = 9.32E-04	PFD$_{AVG}$ = 2.33E-03

Table 11: KFA5/6-DWB with relay output – Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC$_S$	DC$_D$
41 FIT	234 FIT	52 FIT	123 FIT	72%	14%	29%

Table 12: KFA5/6-DWB with relay output – PFD$_{AVG}$ / PFH values

	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFH = 1,23E-07 1/h	PFD$_{AVG}$ = 5.39E-04	PFD$_{AVG}$ = 1.08E-03	PFD$_{AVG}$ = 2.69E-03

Table 13: KFD2-UFC with current output – Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**225**
Fail detected (internal diagnostics or indirectly)	117
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	106
Fail Dangerous Undetected	**84**
No Effect	**164**
Annunciation Undetected	**13**
Not part	**34**

Table 14: KFD2-UFC with current output – IEC 61508 failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**
0 FIT	177 FIT	225 FIT	84 FIT	82%	0%	72%

Table 15: KFD2-UFC with current output – PFD_{AVG} / PFH values

	T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFH = 8,40E-08 1/h	**PFD_{AVG} = 3,68E-04**	**PFD_{AVG} = 7,36E-04**	**PFD_{AVG} = 1,84E-03**

Table 16: KFD2-UFC with transistor output – Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**
41 FIT	325 FIT	52 FIT	92 FIT	81%	11%	36%

Table 17: KFD2-UFC with transistor output – PFD_{AVG} / PFH values

	T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFH = 9,24E-08 1/h	**PFD_{AVG} = 4.05E-04**	**PFD_{AVG} = 8.09E-04**	**PFD_{AVG} = 2.02E-03**

High demand mode of operation and fault reaction time < 1 second [6]

Table 18: KFU8-UFC with current output – Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**243**
Fail detected (internal diagnostics or indirectly)	109
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	132
Fail Dangerous Undetected	**107**
No Effect	**192**
Annunciation Undetected	**13**
Not part	**34**

Table 19: KFU8-UFC with current output – IEC 61508 failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	DC_S	DC_D	**PFH**
0 FIT	205 FIT	243 FIT	107 FIT	80%	0%	69%	1,07E-07 1/h

Table 20: KFU8-UFC with transistor output – Failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	DC_S	DC_D	**PFH**
9 FIT	424 FIT	30 FIT	115 FIT	80%	2%	20%	1,15E-07 1/h

Table 21: KFU8-UFC/DWB with relay output – Failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	DC_S	DC_D	**PFH**
9 FIT	440 FIT	30 FIT	132 FIT	78%	2%	18%	1,32E-07 1/h

Table 22: KFD2-UFC/DWB with relay output – Failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	DC_S	DC_D	**PFH**
9 FIT	363 FIT	21 FIT	138 FIT	74%	2%	13%	1,38E-07 1/h

[6] A fault reaction time of 1 second requires also that a connected device can detect the output state within a time that allows reacting within the process safety time.

Table 23: KFA5/6-DWB with relay output – Failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
9 FIT	266 FIT	20 FIT	155 FIT	65%	3%	11%	1,55E-07 1/h

Table 24: KFD2-UFC with current output – Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**194**
Fail detected (internal diagnostics or indirectly)	86
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	106
Fail Dangerous Undetected	**116**
No Effect	**164**
Annunciation Undetected	**13**
Not part	**34**

Table 25: KFD2-UFC with current output – IEC 61508 failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
0 FIT	177 FIT	194 FIT	116 FIT	76%	0%	62%	1,16E-07 1/h

Table 26: KFD2-UFC with transistor output – Failure rates / PFH value

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
9 FIT	356 FIT	21 FIT	124 FIT	75%	2%	14%	1,24E-07 1/h

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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.

The assessment has shown that the Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB) have a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of more than 73%. Based on the verification of "proven-in-use" according to IEC 61508 and its direct relationship to “prior-use” of IEC 61511-1 they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

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

A user of the Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB) 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 for different operating conditions is presented in section 5.1 to 5.6.2 along with all assumptions.

The failure rates are valid for the useful life of the Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB). See Appendix 3.

It is important to realize that the “no effect” failures are included in the “safe” 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 two relay outputs should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain safety function, as they contain common components.

Table of Contents

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

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

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

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

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

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

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

This assessment shall be done according to option 2.

This document shall describe the results of the FMEDAs carried out on the Universal Frequency Converters (UFC) with software version 3.00 without display and 4.00 with display and the Rotation Speed Monitors (DWB) with software version 1.24. Table 1 gives an overview and explains the differences.

It shall be assessed whether these devices meet the average Probability of Failure on Demand (PFD_{AVG}) and the Probability of dangerous Failure per Hour (PFH) 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*

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 like TUV and manufacturers, *exida* is a partnership 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 Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB).
exida	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

Pepperl+Fuchs GmbH contracted *exida* in April 2004, April 2006 and July 2007 with the FMEDA and PFD_{AVG} / PFH 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
N7	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	01-4889A	Circuit diagram “Verstärker KF..-UFC-1”
[D2]	01-4385C	Circuit diagram “Verst. UFC-EX1“
[D3]	01-4812A	Circuit diagram“Verstärker KF..-DWB-1”
[D4]	01-4439D	Circuit diagram “Verstärker KF..-DWB-EX1/EX2..; KF..-DU-EX1..“
[D5]	01-4384C	Circuit diagram“KFU8/KFD2 Netzt.“
[D6]	01-4521A	Circuit diagram “KFA.-D..-EX.”
[D7]	Product No. 106744	Bill of material for Power Supply 24VDC
[D8]	Product No. 050650	Bill of material for Power Supply 115VAC / 230VAC
[D9]	Product No. 106834	Bill of material for Power Supply universal
[D10]	Product No. 050175	Bill of material for Amplifier UFC
[D11]	Product No. 051088	Bill of material for Amplifier DWB AC
[D12]	Product No. 114734	Bill of material for Amplifier DWB universal
[D13]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D14]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D15]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D16]	Auswertung DWB_UFC.xls together with email “WG DWBUFC” of 03.06.04	Statistics of field-feed-back tracking UFC / DWB; sold and returned devices
[D17]	Email of 24.05.04	Application examples
[D18]	Anwendung UFC DWB.doc	Summary document about the hardware and software history and description of application examples
[D19]	1830069H.pdf	Software release information UFC4V00
[D20]	1830070K.pdf	Software release information UFC3V00
[D21]	1830106F.pdf	Software release information DWB1V24
[D22]	Antrag.zip of 24.04.06	Description of the hardware modifications with impact analysis and new circuit diagrams

2.4.2 Documentation generated by *exida*

[R1]	Auswertung – exida1.xls of 09.08.04 (Field data evaluation of operating hours, sold devices and returned devices)
[R2]	FMEDA V5 DWB Relay output KFA5-6 V2 R1.1.xls of 18.06.06
[R3]	FMEDA V5 UFC Current output KFD2 V2 R1.0.xls of 19.05.06
[R4]	FMEDA V5 UFC Current output KFU8 V2 R1.1.xls of 17.06.06
[R5]	FMEDA V5 UFC Transistor output KFD2 V2 R1.0.xls of 19.05.06
[R6]	FMEDA V5 UFC Transistor output KFU8 V2 R1.0.xls of 19.05.06
[R7]	FMEDA V5 UFC-DWB Relay output KFD2 V2 R1.1.xls of 18.06.06
[R8]	FMEDA V5 UFC-DWB Relay output KFU8 V2 R1.1.xlsof 18.06.06
[R9]	V1 FMEDA V5 UFC Current output KFU8 V3R0.xls of 12.09.07
[R10]	V2 FMEDA V5 UFC Transistor output KFU8 V3R0.xls of 12.09.07
[R11]	V3 FMEDA V5 UFC-DWB Relay output KFU8 V3R0.xls of 12.09.07
[R12]	V4 FMEDA V5 UFC-DWB Relay output KFD2 V3R0.xls of 12.09.07
[R13]	V5 FMEDA V5 DWB Relay output KFA5-6 V3R0.xls of 12.09.07
[R14]	V6 FMEDA V5 UFC Current output KFD2 V3R0.xls of 12.09.07
[R15]	V7 FMEDA V5 UFC Transistor output KFD2 V3R0.xls of 12.09.07

3 Description of the analyzed modules

3.1 Universal Frequency Converters (UFC)

The universal frequency converters convert an input frequency into a frequency-proportional current and offer at the same time the possibility to monitor the trip values.

The frequency value for the minimum (4 mA) and the maximum output current (20 mA) is freely configurable.

Also the functions of the switch outputs (2 relay outputs and 1 potential free transistor output) are freely adjustable [trip value display (MIN/MAX alarm), serially switched output, pulse divider output, error signal output].

A start-up override that can be activated externally is integrated as well. The maximum input frequency is 5 kHz. The input and output circuits are galvanically isolated.

The Universal Frequency Converters (UFC) are Type B components with a hardware fault tolerance of 0.

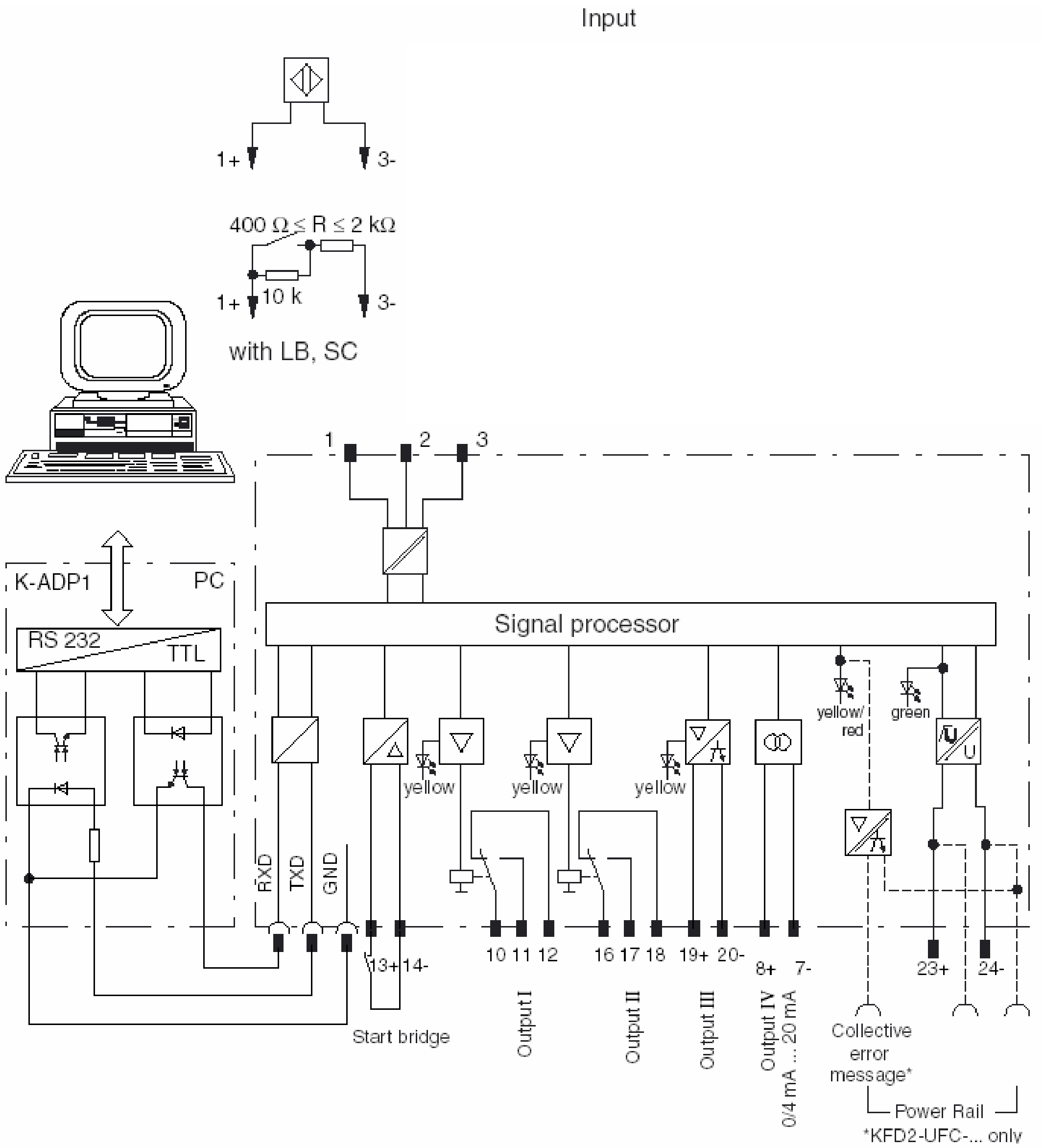


Figure 1: Block diagram of Universal Frequency Converters (UFC)

3.2 Rotation Speed Monitors (DWB)

The rotation speed monitors are able to monitor trip values. The switch points of the two relays can be set freely (MIN/MAX alarm).

A start-up override that can be activated externally is integrated as well. In order to detect short-time interferences or trip value exceeding, a restart inhibit can be activated.

The maximum input frequency is 5 kHz. The input and output circuits are galvanically isolated.

The Rotation Speed Monitors (DWB) are Type B components with a hardware fault tolerance of 0.

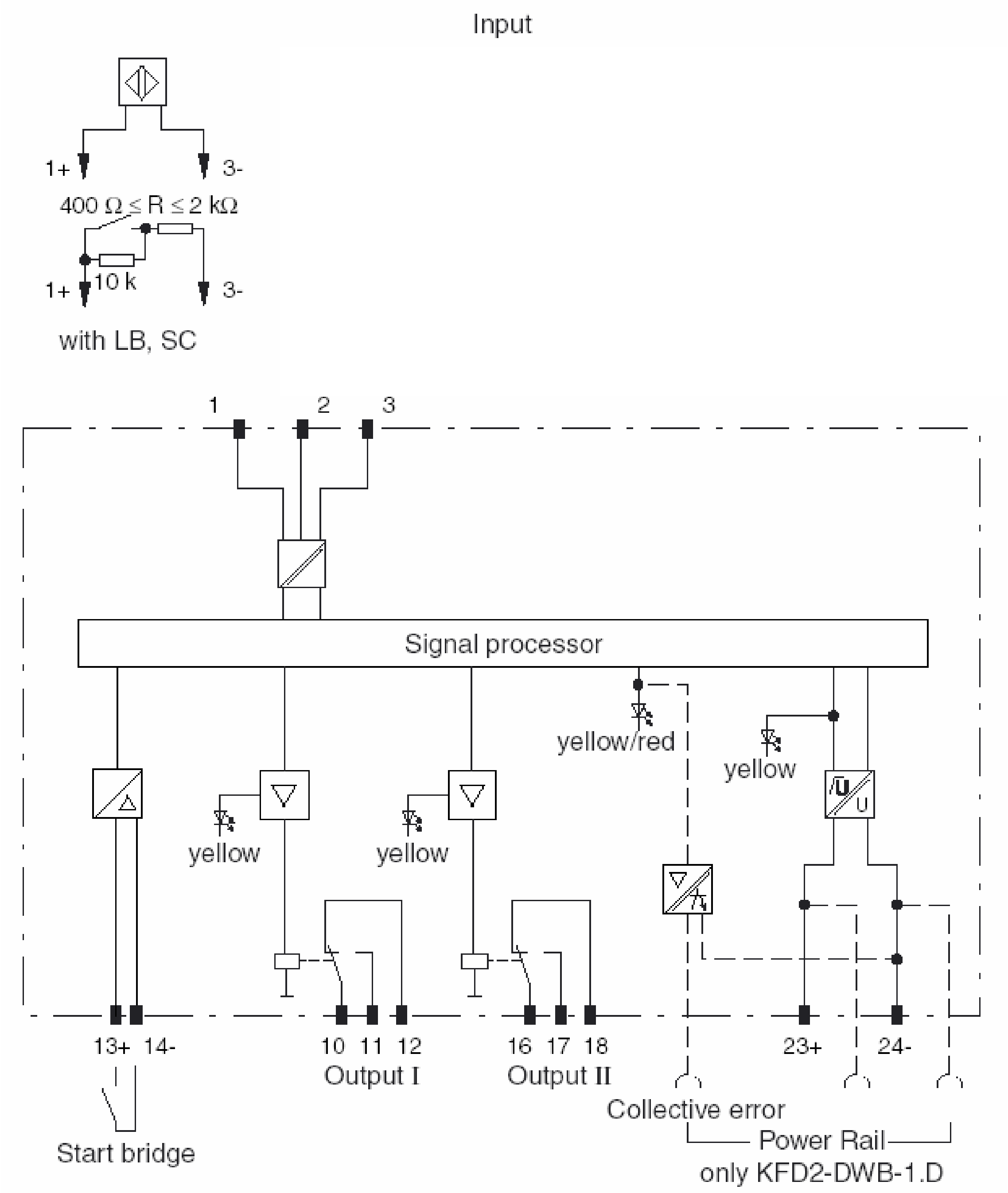


Figure 2: Block diagram of Rotation Speed Monitors (DWB)

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 [R2] to [R15].

4.1 Description of the failure categories

In order to judge the failure behavior of the Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB), the following definitions for the failure of the product were considered.

Current output:

Fail-Safe State
Depending on the application the fail-safe state is defined as the output leading to "fail high" or "fail low".

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

Fail High
Failure that causes the output signal to go to the maximum output current (> 21 mA)

Fail Low
Failure that causes the output signal to go to the minimum output current (< 3.6 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 5% full scale. For the calculation of the SFF it is treated like a safe undetected failure.

Transistor and relay output:

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

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

Fail No Effect
Failure of a component that is part of the safety function but that has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.

General failure categories:

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 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).

Annunciation Undetected
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) and that is not detected by internal diagnostics. 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 programming of the safety logic solver a fail low or fail high can either be dangerous detected or safe detected. Consequently during a Safety Integrity Level (SIL) verification assessment the fail high and fail low categories need to be classified as either safe detected (S) or dangerous detected (DD).

The "No Effect" and "Annunciation Undetected" failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the "No Effect" and "Annunciation Undetected" 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 Assumption

The following assumptions have been made during the FMEDA:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- The repair time after a safe failure is 8 hours.
- 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 temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C (25°C ambient temperature plus internal self heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.
- Short Circuit (SC) detection and Lead Breakage (LB) detection are activated.
- The "HOLD" function is disabled
- Process related parameters are protected by password.
- Sensors are not included in the failure rates listed.
- Because the optional display of the UFC is not part of the safety function, the failure rate of the display is not considered in the calculation.
- The characteristics of the current output are set to NE43 (4..20mA).
- 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:

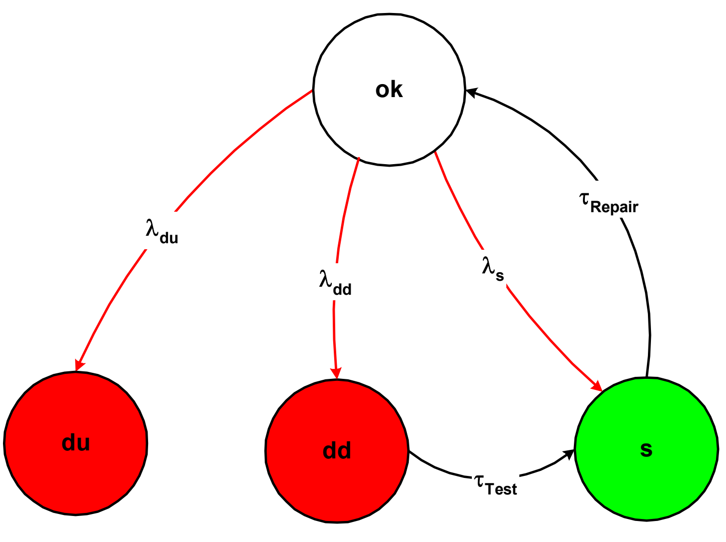
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{don't\ care} + \lambda_{annunciation}$.

SFF = 1 – λ_{du} / λ_{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* as a simulation tool. The results are documented in the following sections.



Abbreviations:

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

Figure 3: Markov model for a 1oo1D structure

5.1 Version V1

5.1.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V1 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 1,40E-07 1/h

λ_{du} = 7,54E-08 1/h

λ_{high} = 2,14E-09 1/h

λ_{low} = 1,32E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

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

λ_{total} = 5,55E-07 1/h

$\lambda_{not\ part}$ = 3,36E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 194 years

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

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**274**
Fail detected (internal diagnostics or indirectly[7])	140
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	132
Fail Dangerous Undetected	**75**
No Effect	**192**
Annunciation Undetected	**13**
Not part	**34**

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

λ_{SD}	λ_{SU} [8]	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**
0 FIT	205 FIT	274 FIT	75 FIT	86,43%	0%	78%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 3.

	T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFH = 7,54E-08 1/h	**PFD_{AVG} = 3,30E-04**	**PFD_{AVG} = 6,60E-04**	**PFD_{AVG} = 1,65E-03**

[7] “indirectly” means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

[8] Note that the SU category includes failures that do not cause a spurious trip

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 4 shows the time dependent curve of PFD_{AVG}.

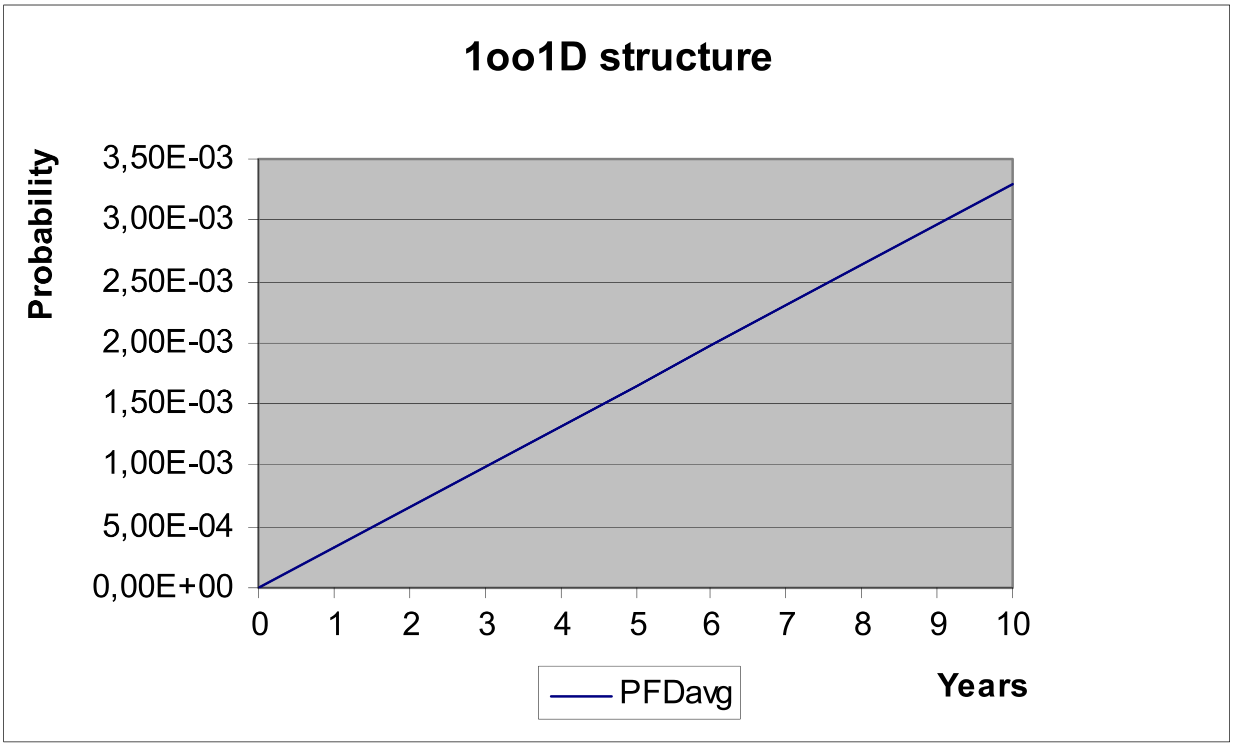


Figure 4: PFD_{AVG}(t) of version V1

5.1.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V1 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 1,09E-07 1/h

λ_{du} = 1,07E-07 1/h

λ_{high} = 2,14E-09 1/h

λ_{low} = 1,32E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

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

λ_{total} = 5,55E-07 1/h

$\lambda_{not\ part}$ = 3,36E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 194 years

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

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**243**
Fail detected (internal diagnostics or indirectly[9])	109
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	132
Fail Dangerous Undetected	**107**
No Effect	**192**
Annunciation Undetected	**13**
Not part	**34**

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**DC$_S$**	**DC$_D$**	**PFH**
0 FIT	205 FIT	243 FIT	107 FIT	80,75%	0%	69%	1,07E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

[9] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

5.2 Version V2

5.2.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V2 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 4,05E-08 1/h

λ_{su} = 1,82E-07 1/h

λ_{dd} = 6,11E-08 1/h

λ_{du} = 8,37E-08 1/h

$\lambda_{annunciation}$ = 1,37E-08 1/h

$\lambda_{no\ effect}$ = 1,96E-07 1/h

λ_{total} = 5,78E-07 1/h

$\lambda_{not\ part}$ = 3,52E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 186 years

Under the assumptions described in sections 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [10]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
41 FIT	392 FIT	61 FIT	84 FIT	85,50%	9%	42%

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
PFH = 8,37E-08 1/h	**PFD_{AVG} = 3.67E-04**	**PFD_{AVG} = 7.33E-04**	**PFD_{AVG} = 1.83E-03**

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 5 shows the time dependent curve of PFD_{AVG}.

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

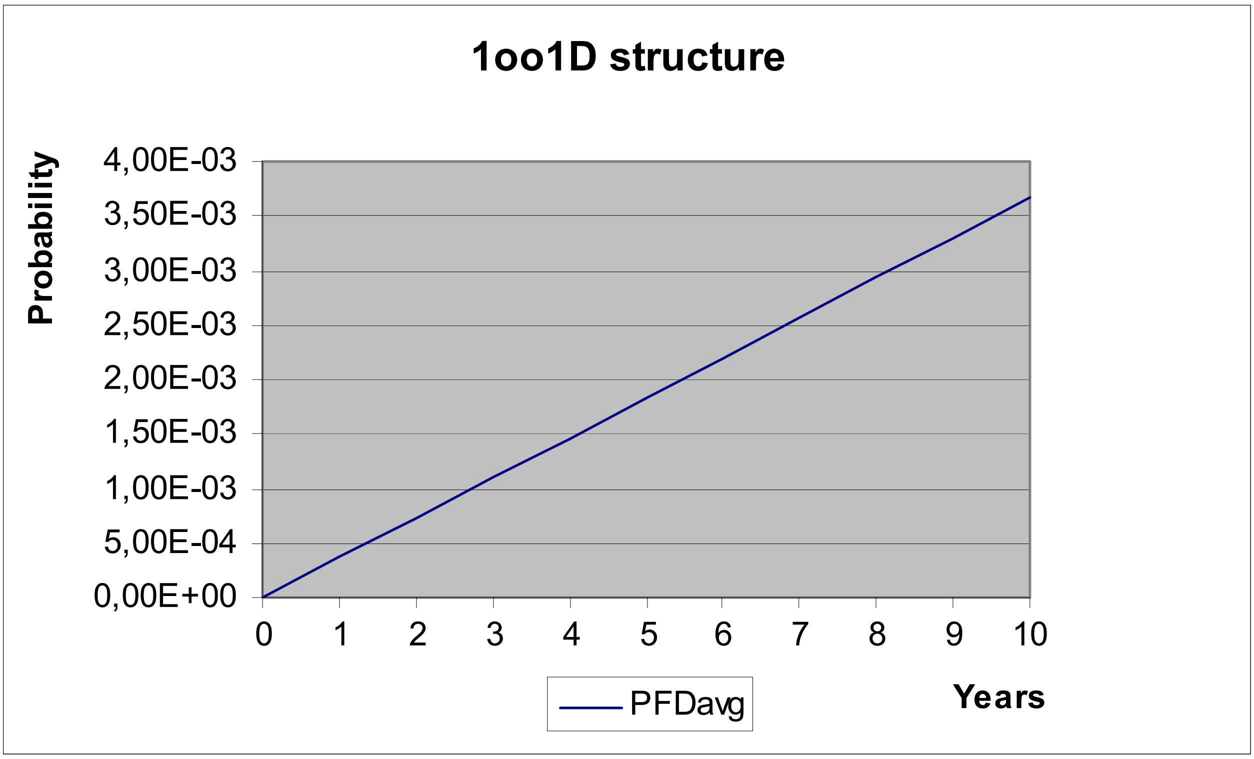


Figure 5: PFD$_{AVG}$(t) of version V2

5.2.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V2 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

λ_{su} = 2,14E-07 1/h

λ_{dd} = 2,96E-08 1/h

λ_{du} = 1,15E-07 1/h

$\lambda_{annunciation}$ = 1,37E-08 1/h

$\lambda_{no\ effect}$ = 1,96E-07 1/h

λ_{total} = 5,78E-07 1/h

$\lambda_{not\ part}$ = 3,52E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 186 years

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**	**PFH**
9 FIT	424 FIT	30 FIT	115 FIT	80,05%	2%	20%	1,15E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

5.3 Version V3

5.3.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V3 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 4,05E-08 1/h

λ_{su} = 1,96E-07 1/h

λ_{dd} = 6,11E-08 1/h

λ_{du} = 1,01E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,99E-07 1/h

λ_{total} = 6,11E-07 1/h

$\lambda_{not\ part}$ = 3,16E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 178 years

Under the assumptions described in sections 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [11]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
41 FIT	409 FIT	61 FIT	101 FIT	83,52%	9%	37%

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**
PFH = 1,01E-07 1/h	**PFD_{AVG} = 4.41E-04**	**PFD_{AVG} = 8.81E-04**	**PFD_{AVG} = 2.20E-03**

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 6 shows the time dependent curve of PFD_{AVG}.

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

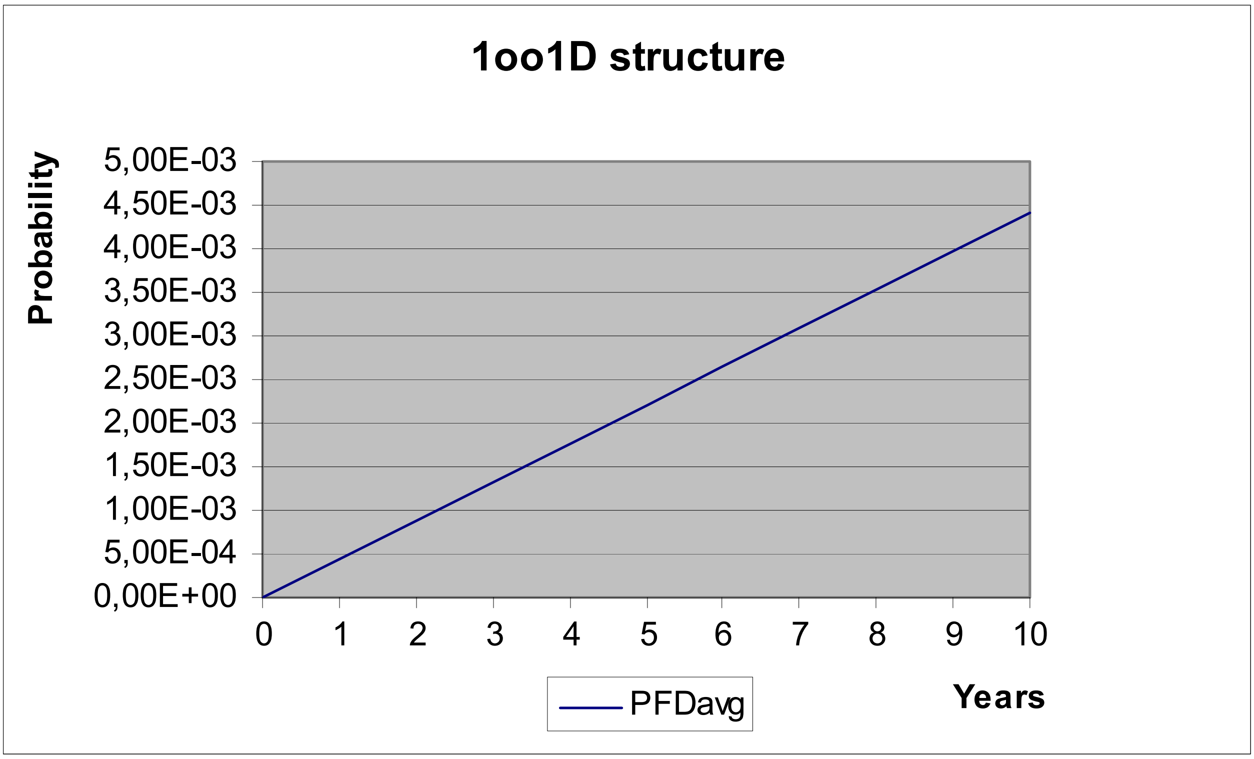


Figure 6: PFD$_{AVG}$(t) of version V3

5.3.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V3 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

λ_{su} = 2,28E-07 1/h

λ_{dd} = 2,96E-08 1/h

λ_{du} = 1,32E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,99E-07 1/h

λ_{total} = 6,11E-07 1/h

$\lambda_{not\ part}$ = 3,16E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 178 years

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
9 FIT	440 FIT	30 FIT	132 FIT	78,36%	2%	18%	1,32E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

5.4 Version V4

5.4.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V4 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 4,05E-08 1/h

λ_{su} = 1,48E-07 1/h

λ_{dd} = 5,24E-08 1/h

λ_{du} = 1,07E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,70E-07 1/h

λ_{total} = 5,31E-07 1/h

$\lambda_{not\ part}$ = 3,30E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 202 years

Under the assumptions described in sections 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [12]	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**
41 FIT	332 FIT	52 FIT	107 FIT	79,94%	10%	32%

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**
PFH = 1,07E-07 1/h	**PFD_{AVG} = 4.66E-04**	**PFD_{AVG} = 9.32E-04**	**PFD_{AVG} = 2.33E-03**

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 7 shows the time dependent curve of PFD_{AVG}.

[12] Note that the SU category includes failures that do not cause a spurious trip

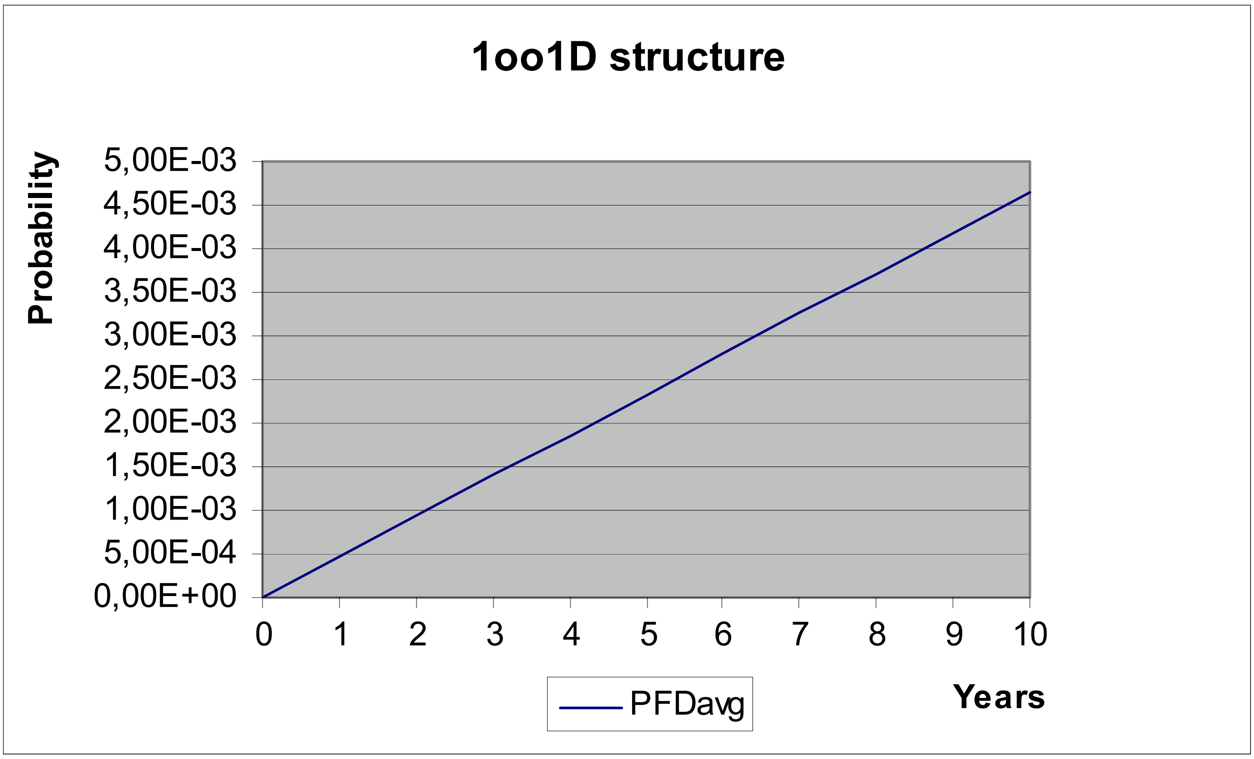


Figure 7: PFD$_{AVG}$(t) of version V4

5.4.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V4 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

λ_{su} = 1,80E-07 1/h

λ_{dd} = 2,09E-08 1/h

λ_{du} = 1,38E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,70E-07 1/h

λ_{total} = 5,31E-07 1/h

$\lambda_{not\ part}$ = 3,30E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 202 years

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
9 FIT	363 FIT	21 FIT	138 FIT	74,01%	2%	13%	1,38E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

5.5 Version V5

5.5.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V5 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 4,05E-08 1/h

λ_{su} = 1,04E-07 1/h

λ_{dd} = 5,18E-08 1/h

λ_{du} = 1,23E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,17E-07 1/h

λ_{total} = 4,49E-07 1/h

$\lambda_{not\ part}$ = 2,04E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 243 years

Under the assumptions described in sections 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [13]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
41 FIT	234 FIT	52 FIT	123 FIT	72,62%	14%	29%

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
PFH = 1,23E-07 1/h	**PFD_{AVG} = 5.39E-04**	**PFD_{AVG} = 1.08E-03**	**PFD_{AVG} = 2.69E-03**

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 8 shows the time dependent curve of PFD_{AVG}.

[13] Note that the SU category includes failures that do not cause a spurious trip

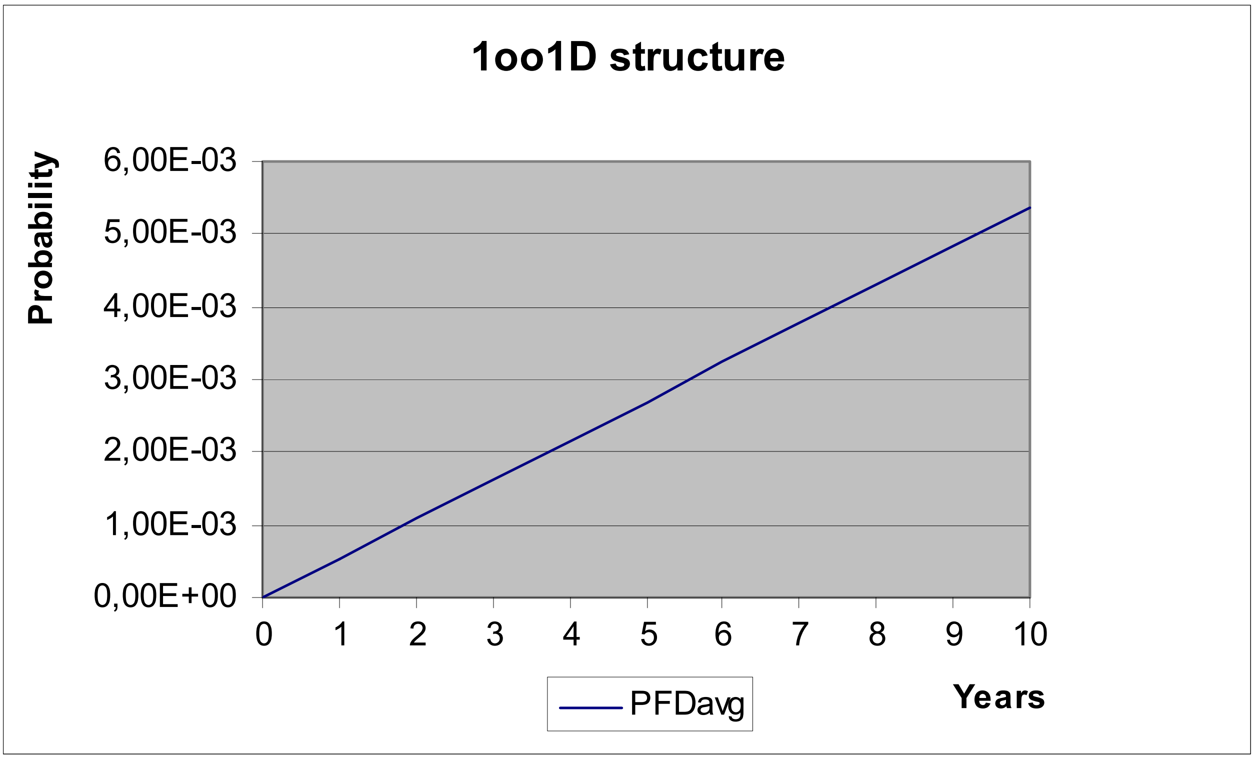


Figure 8: PFD$_{AVG}$(t) of version V5

5.5.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V5 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

λ_{su} = 1,36E-07 1/h

λ_{dd} = 2,03E-08 1/h

λ_{du} = 1,55E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,17E-07 1/h

λ_{total} = 4,49E-07 1/h

$\lambda_{not\ part}$ = 2,04E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 243 years

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
9 FIT	266 FIT	20 FIT	155 FIT	65,61%	3%	11%	1,55E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

5.6 Version V6

5.6.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V6 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 1,17E-07 1/h

λ_{du} = 8,40E-08 1/h

λ_{high} = 2,14E-09 1/h

λ_{low} = 1,06E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,64E-07 1/h

λ_{total} = 4,88E-07 1/h

$\lambda_{not\ part}$ = 3,38E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 219 years

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

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**225**
Fail detected (internal diagnostics or indirectly[14])	117
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	106
Fail Dangerous Undetected	**84**
No Effect	**164**
Annunciation Undetected	**13**
Not part	**34**

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

λ_{SD}	λ_{SU} [15]	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**
0 FIT	177 FIT	225 FIT	84 FIT	82,76%	0%	72%

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 3.

	T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFH = 8,40E-08 1/h	**PFD_{AVG} = 3,68E-04**	**PFD_{AVG} = 7,36E-04**	**PFD_{AVG} = 1,84E-03**

[14] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

[15] Note that the SU category includes failures that do not cause a spurious trip

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 9 shows the time dependent curve of PFD_{AVG}.

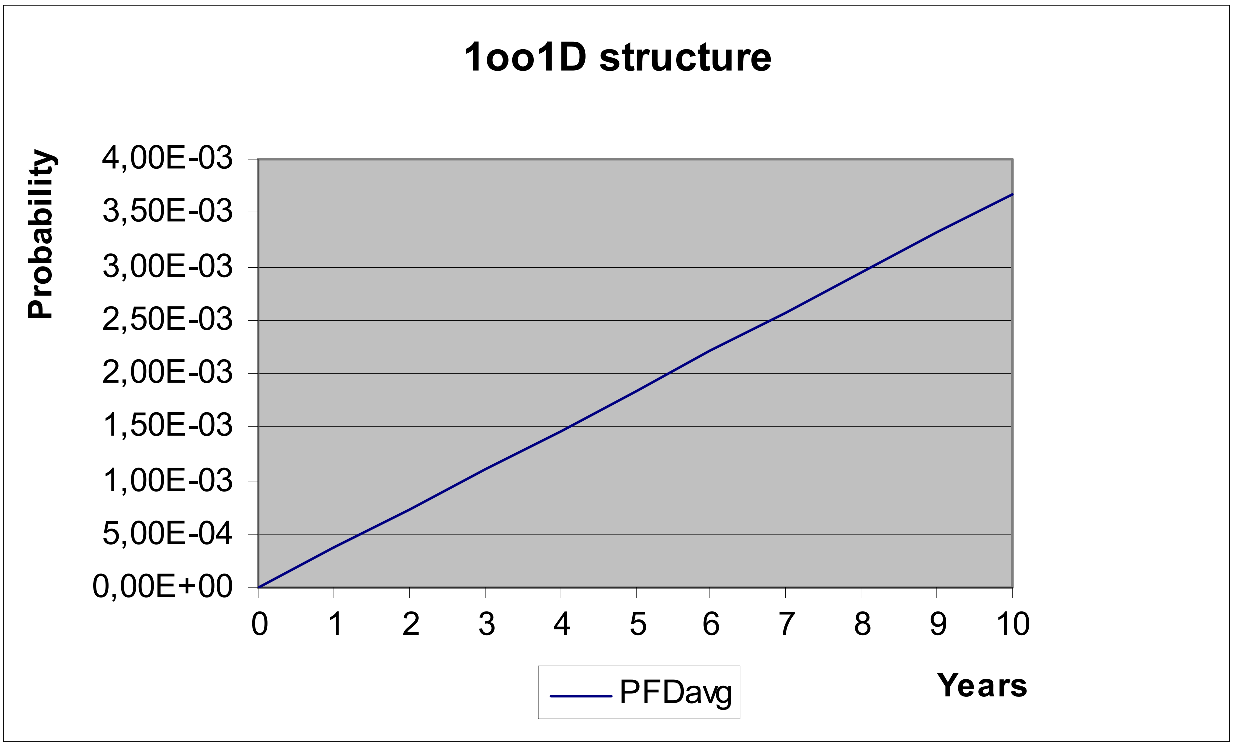


Figure 9: PFD_{AVG}(t) of version V6

5.6.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V6 leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 0,00E-00 1/h

λ_{dd} = 8,59E-08 1/h

λ_{du} = 1,16E-07 1/h

λ_{high} = 2,14E-09 1/h

λ_{low} = 1,06E-07 1/h

$\lambda_{annunciation}$ = 1,34E-08 1/h

$\lambda_{no\ effect}$ = 1,64E-07 1/h

λ_{total} = 4,88E-07 1/h

$\lambda_{not\ part}$ = 3,38E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 219 years

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

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**194**
Fail detected (internal diagnostics or indirectly[16])	86
Fail High (detected by the logic solver)	2
Fail low (detected by the logic solver)	106
Fail Dangerous Undetected	**116**
No Effect	**164**
Annunciation Undetected	**13**
Not part	**34**

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D	PFH
0 FIT	177 FIT	194 FIT	116 FIT	76,30%	0%	62%	1,16E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

[16] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the device setting and are therefore detectable.

5.7 Version V7

5.7.1 Low / high demand mode of operation and fault reaction time = 5 minutes

The FMEDA carried out on the devices summarized as version V7 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 4,05E-08 1/h

λ_{su} = 1,42E-07 1/h

λ_{dd} = 5,24E-08 1/h

λ_{du} = 9,24E-08 1/h

$\lambda_{annunciation}$ = 1,37E-08 1/h

$\lambda_{no\ effect}$ = 1,69E-07 1/h

λ_{total} = 5,10E-07 1/h

$\lambda_{not\ part}$ = 3,54E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 209 years

Under the assumptions described in sections 4.2.3 and 5 the following table shows the failure rates according to IEC 61508:

λ_{SD}	λ_{SU} [17]	λ_{DD}	λ_{DU}	SFF	DC_S	DC_D
41 FIT	325 FIT	52 FIT	92 FIT	81,87%	11%	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
PFH = 9,24E-08 1/h	**PFD_{AVG} = 4.05E-04**	**PFD_{AVG} = 8.09E-04**	**PFD_{AVG} = 2.02E-03**

The boxes marked in yellow (🟨) 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 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 or 1,00E-07 1/h respectively. 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. Figure 10 shows the time dependent curve of PFD_{AVG}.

[17] Note that the SU category includes failures that do not cause a spurious trip

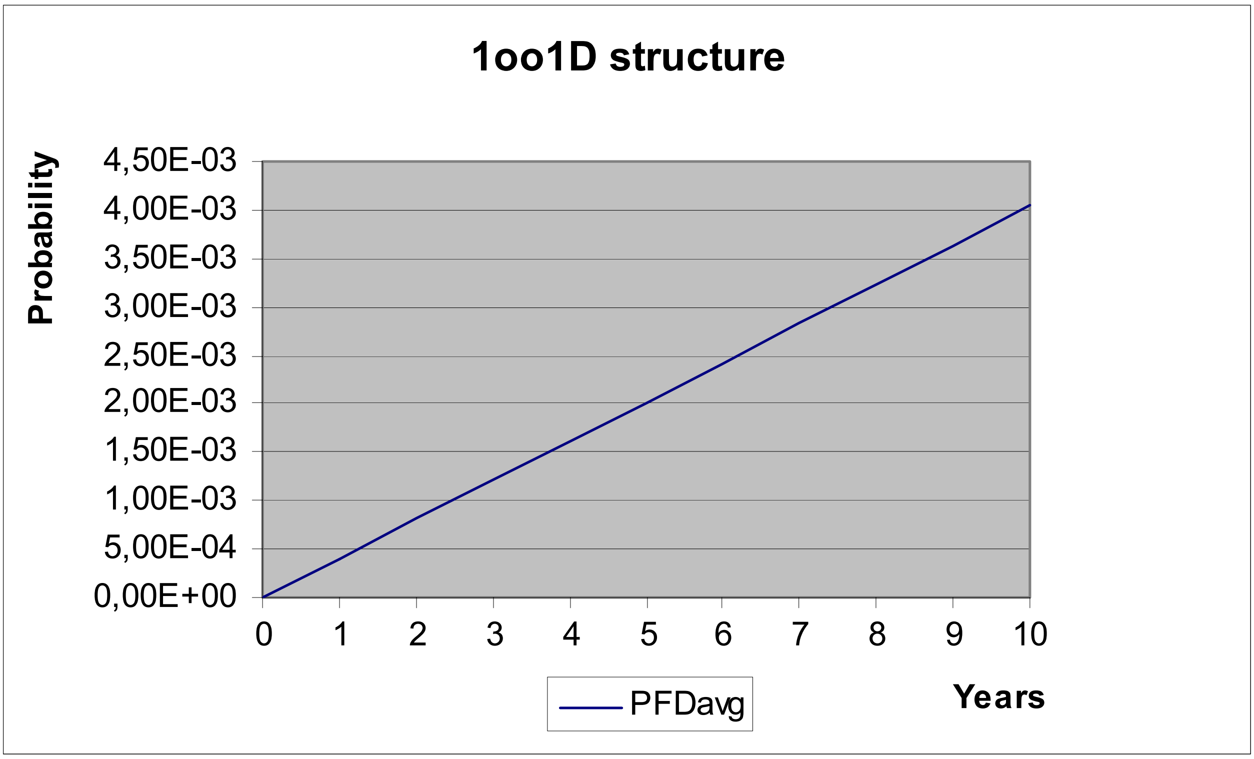


Figure 10: PFD$_{AVG}$(t) of version V7

5.7.2 High demand mode of operation and fault reaction time < 1 second

The FMEDA carried out on the devices summarized as version V7 leads under the assumptions described in section 4.2.3 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

λ_{su} = 1,74E-07 1/h

λ_{dd} = 2,09E-08 1/h

λ_{du} = 1,24E-07 1/h

$\lambda_{annunciation}$ = 1,37E-08 1/h

$\lambda_{no\ effect}$ = 1,69E-07 1/h

λ_{total} = 5,10E-07 1/h

$\lambda_{not\ part}$ = 3,54E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 209 years

Under the assumptions described in sections 4.2.3 and 5 the following tables show the failure rates / PFH value according to IEC 61508:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**DC_S**	**DC_D**	**PFH**
9 FIT	356 FIT	21 FIT	124 FIT	75,70%	2%	14%	1,24E-07 1/h

The box marked in yellow (🟨) mean that the calculated PFH value is within the allowed range for SIL 2 according to table 3 of IEC 61508-1 but does not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-07 1/h.

6 Proven-in-use Assessment

6.1 Definition of the term “Proven-in-use” according to IEC 61508

Reference: IEC 61508-7; B.5.4

Aim: To use field experience from different applications to prove that the safety-related system will work according to its specification.

Description: Use of components or subsystems, which have been shown by experience to have no, or only unimportant, faults when used, essentially unchanged, over a sufficient period of time in numerous different applications.

For field experience to apply, the following requirements must have been fulfilled:

- unchanged specification;
- 10 systems in different applications;
- 10^5 operating hours and at least 1 year of service history.

The field experience is demonstrated through documentation of the vendor and/or operating company. This documentation must contain at least the:

- exact designation of the system and its component, including version control for hardware;
- users and time of application;
- operating hours;
- procedures for the selection of the systems and applications procured to the proof;
- procedures for fault detection and fault registration as well as fault removal.

6.2 “Prior-use” requirements according to IEC 61511-1

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%[18].

The assessment of the Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB) has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

Requirement	**Argumentation**[19]
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 4 years in a wide range of applications. They are considered to be of medium complexity and the probability that they will fail[20] is <1,3% over the entire selling period. During the considered time period the percentage of failed devices was decreasing. 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D13] to [D15]. 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 [D16] to [D17] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience. The hardware modifications were carried out in accordance with an accepted modification process (see [D22]). The following operating experience exist: UFC: More than 210.000.000 operating hours DWB: More than 83.000.000 operating hours This is considered to be sufficient taking into account the medium complexity of the sub-systems 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 user / manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D17] and [D18].

[18] 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…".

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

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

Requirement	**Argumentation**[19]
Adjustment of process-related parameters only	The user can enable or disable short circuit and lead breakage detection and change other process-related parameters. 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 are protected by password.
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB) with a SFF of 60% - < 90% and a HFT = 0 can considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

7 Terms and Definitions

DC_S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof test frequency.
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
PFH	Probability of dangerous Failure per Hour. The term “Probability” is misleading, correctly defined it is a Rate.
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 B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

8 Status of the document

8.1 Liability

exida prepares 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.

8.2 Releases

Version History:	V0, R1.0:	Initial version, May 26, 2004
	V0, R1.1:	Internal review comments integrated, proven-in-use sections updated after receipt of additional information; June 8, 2004
	V1, R1.0:	External review comments integrated; July 19, 2004
	V1, R1.1:	Editorial changes; August 26, 2004
	V1, R1.2:	Operating hours corrected; September 9, 2004
	V2, R1.0:	Updates after hardware modifications; June 18, 2006
	V2, R1.1:	Additional review comments incorporated; July 10, 2006
	V2, R2:	High demand mode of operation added; September 12, 2007
	V2, R3:	Review comments incorporated; September 25, 2007
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida), June 4, 2004
	V0, R1.1:	Harald Eschelbach (P+F), July 15, 2004
	V2, R1.0:	Michael Trautmann (P+F), June 21, 2006
	V2, R2:	Michael Trautmann (P+F), September 17, 2007
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

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 27 to Table 33 show an importance analysis of the ten most critical dangerous undetected faults for the worst-case version and indicate how these faults can be detected during proof testing.

Appendix 2 and 2.1 should be considered when writing the safety manual as they contain important safety related information.

Table 27: Importance Analysis of "du" failures of version V1 (low demand mode)

Component	% of total λ_{du}	Detection through
IC1 (µC-RAM)	19,91%	100% functional test with monitoring of the output signal
U02	17,92%	100% functional test with monitoring of the output signal
G01	7,96%	100% functional test with monitoring of the output signal
IC4	7,96%	100% functional test with monitoring of the output signal
IC5	4,78%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	4,64%	100% functional test with monitoring of the output signal
P24	3,78%	100% functional test with monitoring of the output signal
IC7	2,79%	100% functional test with monitoring of the output signal
P12	2,19%	100% functional test with monitoring of the output signal
P21	2,19%	100% functional test with monitoring of the output signal

Table 28: Importance Analysis of “du” failures of version V2 (low demand mode)

Component	% of total λ_{du}	Detection through
IC1 (µC-RAM)	17,91%	100% functional test with monitoring of the output signal
U02	16,12%	100% functional test with monitoring of the output signal
G01	7,17%	100% functional test with monitoring of the output signal
IC4	7,17%	100% functional test with monitoring of the output signal
U09	6,27%	100% functional test with monitoring of the output signal
IC5	4,30%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	4,18%	100% functional test with monitoring of the output signal
P24	3,40%	100% functional test with monitoring of the output signal
IC7	2,51%	100% functional test with monitoring of the output signal
P12	1,97%	100% functional test with monitoring of the output signal

Table 29: Importance Analysis of “du” failures of version V3 (low demand mode)

Component	% of total λ_{du}	Detection through
K04	19,86%	100% functional test with monitoring of the output signal
IC1 (µC-RAM)	14,90%	100% functional test with monitoring of the output signal
U02	13,41%	100% functional test with monitoring of the output signal
G01	5,96%	100% functional test with monitoring of the output signal
IC4	5,96%	100% functional test with monitoring of the output signal
U03	4,47%	100% functional test with monitoring of the output signal
IC5	3,58%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	3,48%	100% functional test with monitoring of the output signal
P24	2,83%	100% functional test with monitoring of the output signal
IC7	2,09%	100% functional test with monitoring of the output signal

Table 30: Importance Analysis of “du” failures of version V4 (low demand mode)

Component	% of total λ_{du}	Detection through
K04	18,78%	100% functional test with monitoring of the output signal
IC1 (µC-RAM)	14,08%	100% functional test with monitoring of the output signal
U02	12,67%	100% functional test with monitoring of the output signal
G01	5,63%	100% functional test with monitoring of the output signal
IC4	5,63%	100% functional test with monitoring of the output signal
IC5	3,38%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	3,29%	100% functional test with monitoring of the output signal
C11	2,82%	100% functional test with monitoring of the output signal
P24	2,68%	100% functional test with monitoring of the output signal
F4	2,35%	100% functional test with monitoring of the output signal

Table 31: Importance Analysis of “du” failures of version V5 (low demand mode)

Component	% of total λ_{du}	Detection through
K01	16,25%	100% functional test with monitoring of the output signal
IC1 (µC-RAM)	12,19%	100% functional test with monitoring of the output signal
U02	10,97%	100% functional test with monitoring of the output signal
T1	8,13%	100% functional test with monitoring of the output signal
G01	4,88%	100% functional test with monitoring of the output signal
IC4	4,88%	100% functional test with monitoring of the output signal
N05	4,06%	100% functional test with monitoring of the output signal
C01	3,45%	100% functional test with monitoring of the output signal
IC5	2,93%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	2,84%	100% functional test with monitoring of the output signal

Table 32: Importance Analysis of “du” failures of version V6 (low demand mode)

Component	% of total λ_{du}	Detection through
IC1 (µC-RAM)	17,85%	100% functional test with monitoring of the output signal
U02	16,06%	100% functional test with monitoring of the output signal
G01	7,14%	100% functional test with monitoring of the output signal
IC4	7,14%	100% functional test with monitoring of the output signal
IC5	4,28%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	4,16%	100% functional test with monitoring of the output signal
C11	3,57%	100% functional test with monitoring of the output signal
P24	3,39%	100% functional test with monitoring of the output signal
F4	2,97%	100% functional test with monitoring of the output signal
IC7	2,50%	100% functional test with monitoring of the output signal

Table 33: Importance Analysis of “du” failures of version V7 (low demand mode)

Component	% of total λ_{du}	Detection through
IC1 (µC-RAM)	16,23%	100% functional test with monitoring of the output signal
U02	14,61%	100% functional test with monitoring of the output signal
G01	6,49%	100% functional test with monitoring of the output signal
IC4	6,49%	100% functional test with monitoring of the output signal
U09	5,68%	100% functional test with monitoring of the output signal
IC5	3,90%	100% functional test with monitoring of the output signal
IC1 (µC-ROM)	3,79%	100% functional test with monitoring of the output signal
C11	3,25%	100% functional test with monitoring of the output signal
P24	3,08%	100% functional test with monitoring of the output signal
F4	2,71%	100% functional test with monitoring of the output signal

Appendix 2.1: Critical failure modes contributing to λ_{du}

Failures of complex integrated circuits

According to IEC 61508 the normal distribution of the failure rate of complex integrated circuits is 50% safe failures and 50% dangerous failures. In order to achieve a SFF of > 90%, diagnostics with at least medium effectiveness are needed. The Universal Frequency Converters (UFC) and Rotation Speed Monitors (DWB) achieve a SFF of more than 72% with medium diagnostics for the ROM but without any diagnostics for the remaining parts of the micro controller.

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

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[21] 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.

Table 34 shows which electrolytic capacitors are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 34: Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Name	Schematic	Useful life at 40°C
Capacitor (electrolytic) - Aluminum electrolytic, non solid electrolyte	C01, C02 C11	01-4521C 01-7317	Appr. 90 000 Hours[22]
Relay	K01 K04 K04	01-4521C 01-7317 01-7308	2 x 10^7 mechanical operations 1 x 10^5 electrical operations

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime.

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.

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

[21] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

[22] 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.