FMEDA and Proven-in-use Assessment

Project:

Temperature Converters
KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 05/03-24

Report No.: P+F 05/03-24 R023

Version V3, Revision R0; March 2010

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 according to IEC 61508 with proven-in-use consideration carried out on the temperature converters KF**-GUT-(Ex)1.D with software version 1V45, KFD2-UT2-(Ex)* with software version 1V46 and HiD2082 with software version 1V48. Table 1 gives an overview of the different types 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: Type overview

Type	Power supply	Ex	Channels	Output	Display
KFD2-GUT-EX1.D	24 VDC	yes	1	Current + Relay	yes
KFU8-GUT-EX1.D	24 VDC / 90-253 VAC	yes	1	Current + Relay	yes
KFD2-GUT-1.D	24 VDC	no	1	Current + Relay	yes
KFU8-GUT-1.D	24 VDC / 90-253 VAC	no	1	Current + Relay	yes
KFD2-UT2-Ex1	24 VDC	yes	1	Current	no
KFD2-UT2-Ex2	24 VDC	yes	2	Current	no
KFD2-UT2-Ex1-1	24 VDC	yes	1	Voltage	no
KFD2-UT2-Ex2-1	24 VDC	yes	2	Voltage	no
KFD2-UT2-1	24 VDC	no	1	Current	no
KFD2-UT2-2	24 VDC	no	2	Current	no
KFD2-UT2-1-1	24 VDC	no	1	Voltage	no
KFD2-UT2-2-1	24 VDC	no	2	Voltage	no
HiD2082	24 VDC	yes	2	Current + Voltage	no

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

The two channels on the two channel devices 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.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be < 1,00E-02 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-03.

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

Type B subsystems 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.

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

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 5.5 the devices might also be used for SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

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

Table 2: KF-GUT-(Ex)1.D with current output – Failure rates**

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**341**
Fail detected (internal diagnostics or indirectly[2])	167
Fail High (detected by the logic solver)	17
Fail low (detected by the logic solver)	157
Fail Dangerous Undetected	**66**
No Effect	**236**
Annunciation Undetected	**2**
Not part	**53**

Table 3: IEC 61508 failure rates

λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}	SFF	DC_S [4]	DC_D [4]
0 FIT	236 FIT	341 FIT	68 FIT	89%	0%	83%

Table 4: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 2,98E-04	**PFD_{AVG} = 5,96E-04**	**PFD_{AVG} = 1,49E-03**

Table 5: KF-GUT-(Ex)1.D with one relay output – IEC 61508 failure rates**

λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}	SFF	DC_S [4]	DC_D [4]
0 FIT	445 FIT	117 FIT	106 FIT	84%	0%	52%

Table 6: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.64E-04	**PFD_{AVG} = 9.29E-04**	**PFD_{AVG} = 2.32E-03**

[2] "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.

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

[4] DC means the diagnostic coverage (safe or dangerous) for the temperature converters by the safety logic solver.

Table 7: KF-GUT-(Ex)1.D with two relay outputs – IEC 61508 failure rates**

λ_{SD}	λ_{SU} [5]	λ_{DD}	λ_{DU}	SFF	DC_S [6]	DC_D [6]
0 FIT	486 FIT	177 FIT	77 FIT	89%	0%	65%

Table 8: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.37E-04	PFD_{AVG} = 6.75E-04	PFD_{AVG} = 1.69E-03

Table 9: KFD2-UT2-(Ex)* with current / voltage output – Failure rates

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**333**
Fail detected (internal diagnostics or indirectly[7])	148
Fail High (detected by the logic solver)	24
Fail low (detected by the logic solver)	161
Fail Dangerous Undetected	**74**
No Effect	**295**
Annunciation Undetected	**5**
Not part	**33**

Table 10: IEC 61508 failure rates

λ_{SD}	λ_{SU} [5]	λ_{DD}	λ_{DU}	SFF	DC_S [6]	DC_D [6]
0 FIT	295 FIT	333 FIT	79 FIT	88%	0%	81%

Table 11: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3,47E-04	PFD_{AVG} = 6,94E-04	PFD_{AVG} = 1,73E-03

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

[6] DC means the diagnostic coverage (safe or dangerous) for the temperature converters by the safety logic solver.

[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.

Table 12: HiD2082 with current / voltage output – Failure rates

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**396**
Fail detected (internal diagnostics or indirectly[8])	147
Fail High (detected by the logic solver)	19
Fail low (detected by the logic solver)	230
Fail Dangerous Undetected	**96**
No Effect	**302**
Annunciation Undetected	**6**
Not part	**46**

Table 13: IEC 61508 failure rates

λ_{SD}	λ_{SU} [9]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [10]	**DC_D** [10]
0 FIT	302 FIT	396 FIT	102 FIT	87%	0%	80%

Table 14: PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFD_{AVG} = 4,45E-04	**PFD_{AVG} = 8,90E-04**	**PFD_{AVG} = 2,22E-03**

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

The assessment has shown that the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 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 84%. The “proven-in-use information” may be used to assist an end user in completing a prior-use justification per IEC 61511-1.

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. For a higher average temperature of 60℃, 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.

[8] “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.

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

[10] DC means the diagnostic coverage (safe or dangerous) for the temperature converters by the safety logic solver.

A user of the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 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 5.3 along with all assumptions.

It is important to realize that the “No Effect” and “Annunciation Undetected” 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 temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 (see Appendix 3).

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 per 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 temperature converters KF**-GUT-(Ex)1.D with software version 1V45, KFD2-UT2-(Ex)* with software version 1V46 and HiD2082 with software version 1V48. 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}) 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 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 temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082.
exida	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

Pepperl+Fuchs GmbH contracted *exida* in November 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
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]	01-5639B of 28.11.03	Circuit diagram “KF..-GUT-(EX)1.D amplifier pcb”
[D2]	01-5582 of 25.02.02	Circuit diagram “KFU8– / KFD2– Netzteil / power supply“
[D3]	Product No. 113604	Bill of material for KFD2-GUT-EX1.D
[D4]	Product No. 113605	Bill of material for KFU8-GUT-EX1.D
[D5]	Product No. 113606	Bill of material for KFD2-GUT-1.D
[D6]	Product No. 113607	Bill of material for KFU8-GUT-1.D
[D7]	Version 0 of 05.06.02	P02.05 Produktpflege.pps
[D8]	Version 0 of 05.04.02	P08.01 Abwicklung von Produktrücklieferungen-0.ppt
[D9]	12.02.02	P0205010202 NCDRWorkflow.ppt
[D10]	Verkaufszahlen GUT.xls	Statistics of field-feed-back tracking; sold devices
[D11]	Mappe1.xls	Statistics of field-feed-back tracking; returned devices
[D12]	Email “KFD2-GUT SIL2 (typical application).msg” of 29.09.05	Application examples
[D13]	Versionen_GUT_FW.pdf	Software history list
[D14]	1830488B.DOC	Software release information for V1.03 (first released version)
[D15]	1830488D.DOC and 1830488E.DOC	Software release information for V1.09
[D16]	1830488f.doc	Software release information for V1.14
[D17]	1830488g_.doc	Software release information for V1.38
[D18]	1830488h.doc	Software release information for V1.42
[D19]	505417.doc	Hardware change notice
[D20]	Beurteilung_aender_109bis142_IndB.doc with CD	Impact analysis with explanations and test reference for software versions V1.09 to V1.42
[D21]	Impact_analyse.zip of 08.01.07	Impact analysis with explanations and test reference for software version V1.45
[D22]	AW KF-GUT-(Ex)1.D.msg of 01.02.07	Feedback to review comments from *exida*
[D23]	Impact_analyse2.zip of 13.02.07	Revised impact analysis for software version V1.45
[D24]	html_doku_1v45.zip of 01.02.07	Description of software changes
[D25]	com_ueberw.HTML	Test cases related to the FMEDA

[D26]	KFD2-UT2 Impact Analysis 19.05.08.doc	Impact analysis for hardware changes to KFD2-UT2 from P.C.B. 05-4047A to 05-4047D
[D27]	RE UT2 – Impactanalyse.msg of 16.05.08	Feedback to review comments from *exida*
[D28]	Impact_FW_KFD2_UT2.zip of 07.11.08, Test_1v46_UT2Teil2.zip of 07.11.08 and Input 2 - User_Table_TC.zip of 09.12.08	Impact analysis for software changes to KFD2-UT2 with explanations and test reference for software versions V1.39 to V1.46
[D29]	UT2 Sales Sept 2007.xls of 14.05.08	Statistics of field-feed-back tracking; sold devices
[D30]	UT2 Rueckl Auswertung.xls of 14.05.08	Statistics of field-feed-back tracking; returned devices
[D31]	FSXXXX_EA_30_desc_hist.pdf of 16.06.08	Description about common design basis for all considered devices
[D32]	2515053e.pdf	Circuit diagram “KFD2-UT2-Ex2(-1)” 251-5053E of 13.11.07
[D33]	2515060f.pdf	Circuit diagram “KFD2-UT2-Ex1(-1)” 251-5060F of 09.04.08
[D34]	2515053f.pdf	Circuit diagram “KFD2-UT2-Ex2(-1)” 251-5053F of 08.01.09
[D35]	2515060g.pdf	Circuit diagram “KFD2-UT2-Ex1(-1)” 251-5060G of 18.02.10
[D36]	2515022d.pdf	Circuit diagram “HiD2082” 251-5022D of 24.07.03
[D37]	fs0029ea-26a - Review SA_coms_PF.xls of 05.02.10	FMEDA for HiD2082
[D38]	fsc010ea-25a.pdf	Impact analysis for hardware changes to KFD2-UT2 from P.C.B. 05-4047D to 05-4047E
[D39]	HiD 2082 proven in use assessment Korrigierte FMEDA Impactanalysen Testergebnisse.msg of 25.01.10	Description of changes
[D40]	Firmw_FMEDA_tests1.zip _HiD2082_1v46 blackbox tests.zip	Impact analysis on differences between firmware of HiD2082 and KFD2-UT2-Ex2 for version V1.39 / V1.46 and test reference for software version V1.46 Impact analysis for software changes to HiD2082 with explanations and test reference for software versions V1.46 to V1.48
[D41]	Field_failures_HID2082_2.xls of 12.01.10	Statistics of field-feed-back tracking; returned devices

2.4.2 Documentation generated by *exida*

[R1]	FMEDA V6 Amplifier GUT 01-5639B with PS and Current output V1.xls of 09.11.05
[R2]	FMEDA V6 Amplifier GUT 01-5639B with PS and Relay V1.xls of 09.11.05
[R3]	FMEDA V6 Amplifier GUT 01-5639B with PS and two relays V1 of 15.04.06
[R4]	FMEDA V6 UT2 V1R0.xls of 23.07.08
[R5]	fs0029ea-26a_V2.xls of 05.02.10
[R6]	Field data evaluation - Stand 0306.xls of 31.03.06 (Field data evaluation of operating hours, sold devices and returned devices)
[R7]	Ausfallratenbestimmung_UT2.xls of 15.05.08 (Field data evaluation of operating hours, sold devices and returned devices)
[R8]	Field_failures_HID2082_2_exida.xls of 01.02.10 (Field data evaluation of operating hours, sold devices and returned devices)

3 Description of the analyzed subsystems

The temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 have been designed for temperature measurement applications.

They convert the signal of an RTD, a TC (thermocouple), a potentiometer or a voltage source to a proportional output current which may be connected to an analog input of the process control system / control unit.

They are equipped with linearization and internal/external cold junction compensation.

A plausibility test performed with a second measuring point is possible for measurements with thermo-elements.

The temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 are Type B subsystems with a hardware fault tolerance of 0.

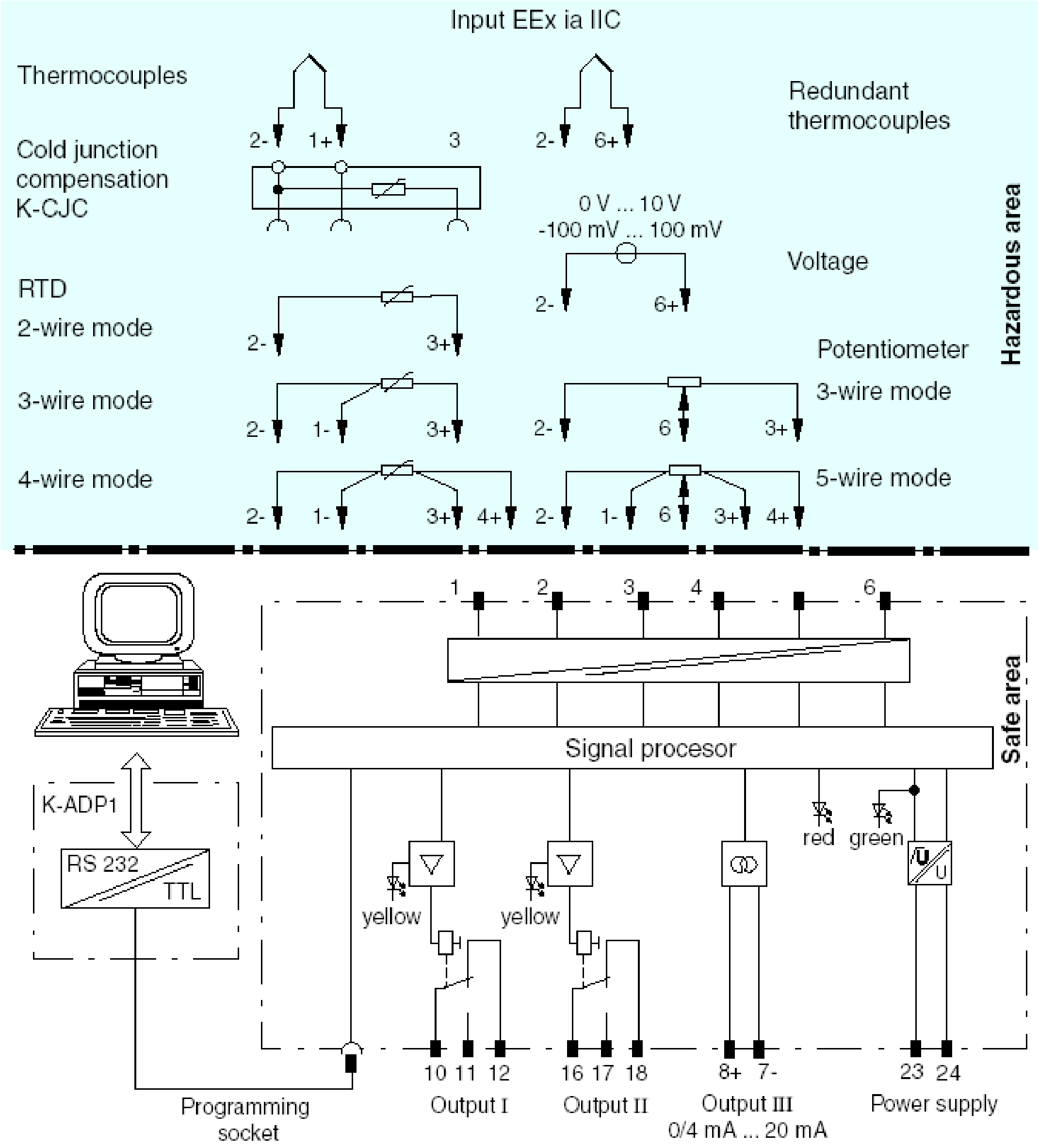


Figure 1: Block diagram of KFU8-GUT-Ex1.D

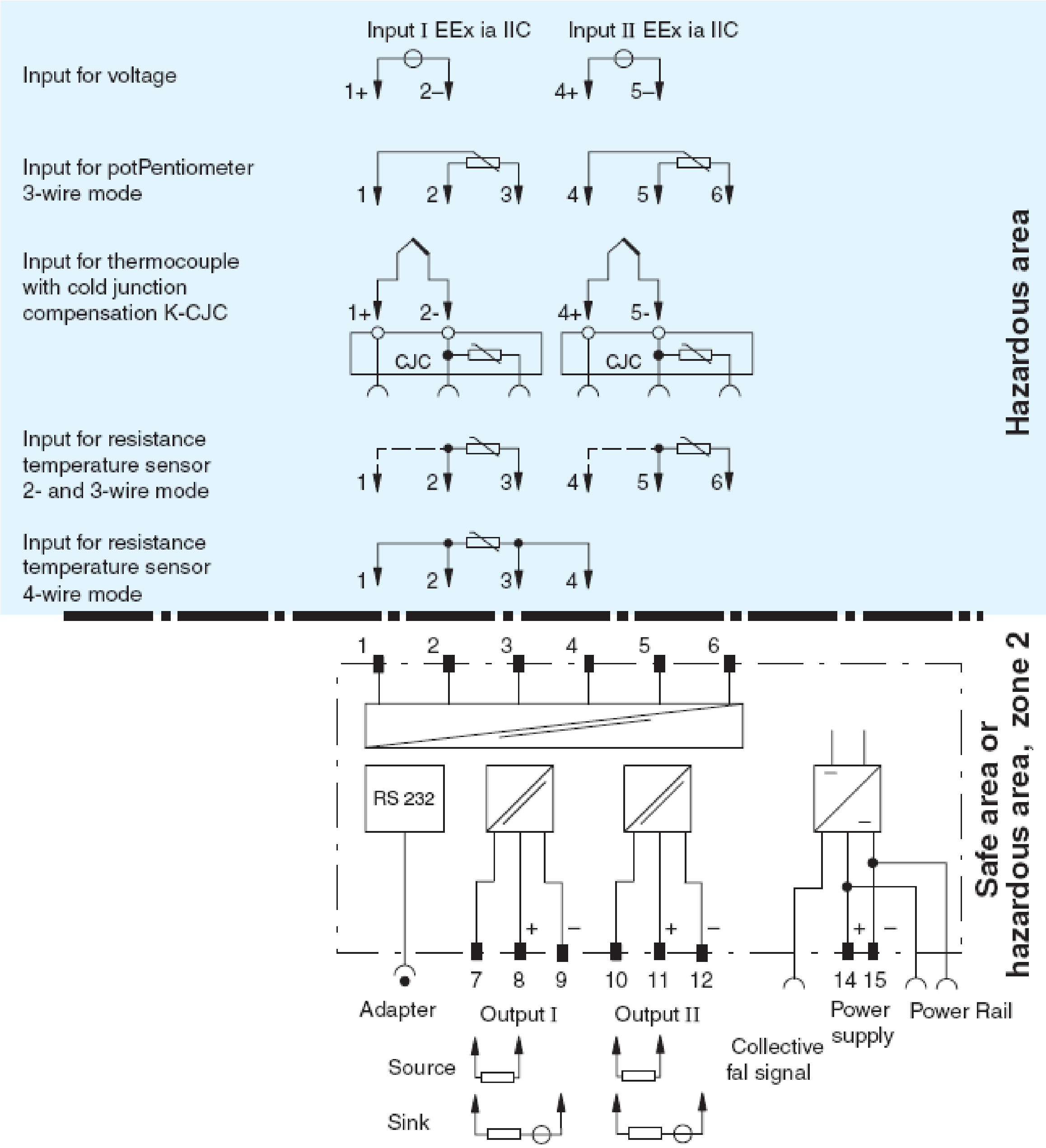

Input I EEx ia IIC
Input II EEx ia IIC
Input for voltage
1+
2–
4+
5–
Input for potPentiometer 3-wire mode
1
2
3
4
5
6
Input for thermocouple with cold junction compensation K-CJC
1+
2-
4+
5-
CJC
CJC
Input for resistance temperature sensor 2- and 3-wire mode
1
2
3
4
5
6
Input for resistance temperature sensor 4-wire mode
1
2
3
4
Hazardous area
1
2
3
4
5
6
RS 232
+
–
+
–
–
–
+
–
7
8
9
10
11
12
14 15
Adapter
Output I
Output II
Power supply
Power Rail
Collective fal signal
Source
Sink
Safe area or hazardous area, zone 2

Figure 2: Block diagram of KFD2-UT2-Ex2

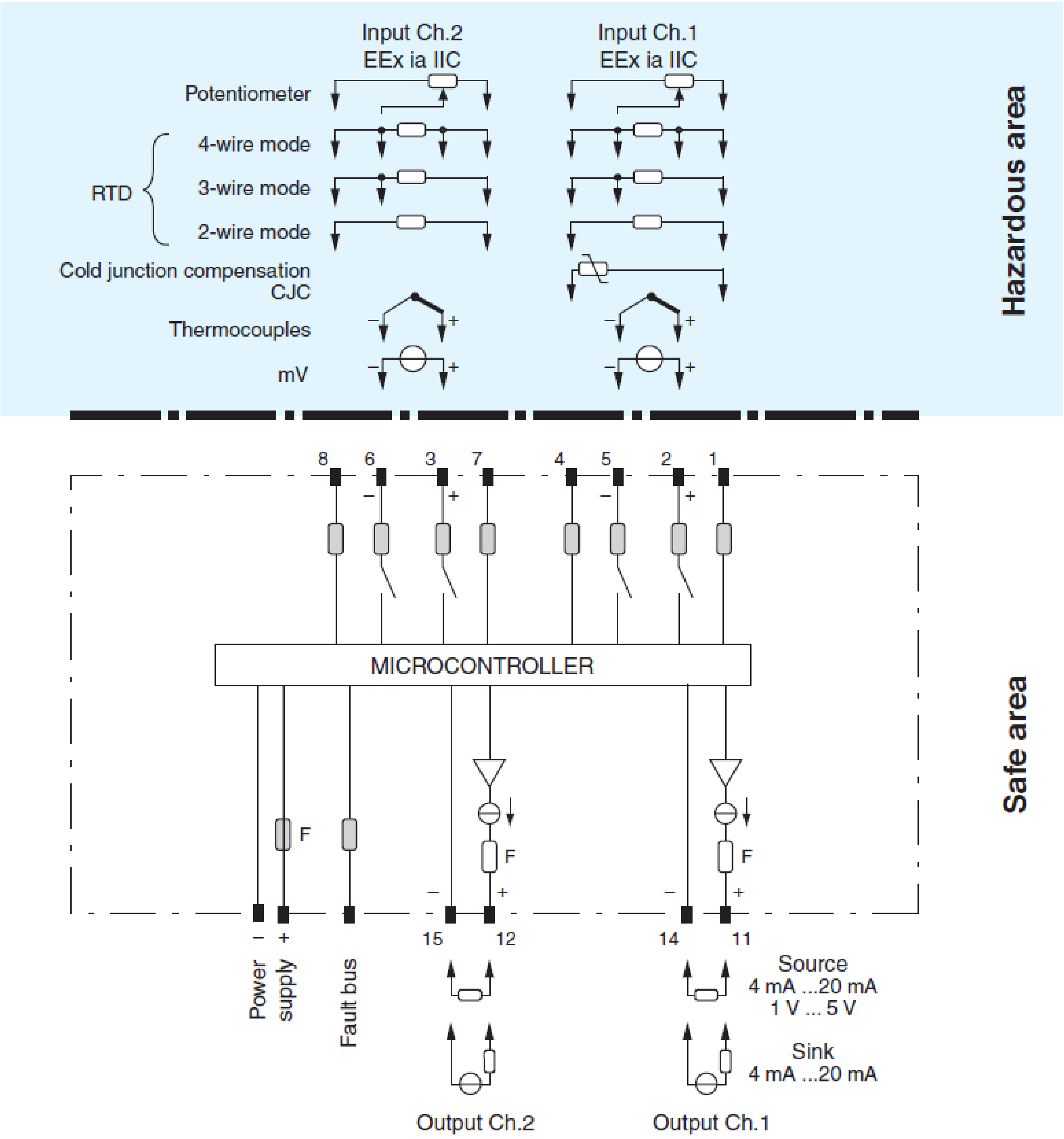


Figure 3: Block diagram of HiD2082

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 [R5]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see test reports [D20], [D25], [D28] and [D40]). This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082, the following definitions for the failure of the product were considered.

Current output:

Fail-Safe State
The fail-safe state is defined as the output exceeding the user defined threshold.

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 (+/- 0.8mA).

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.

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, 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” 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 Assumptions

The following assumptions have been made during the FMEDA of the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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 repair time after a safe failure is 8 hours.
- The test time of the logic solver to react on a dangerous detected failure is 1 hour.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 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 40ºC. Humidity levels are assumed within manufacturer's rating.
- All modules are operated in the low demand mode of operation.
- 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.
- Because the optional display is not part of the safety function, the failure rate of the display is not considered in the calculation.
- Failures during parameterization are not considered.
- Only one input and one output are part of the considered safety function.
- The collective error output which signals if the field wiring is broken or shorted is not considered in the FMEDA and the calculations.
- The relay outputs are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.
- 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 GmbH.

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:

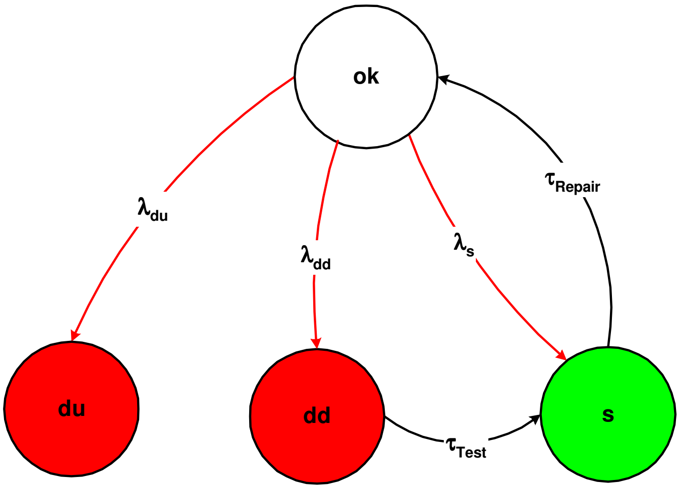
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$

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

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

For the calculation of the PFD_{AVG} the following Markov model for a 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

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



Abbreviations:

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

Figure 4: Markov model for a 1oo1D structure

5.1 KF**-GUT-(Ex)1.D with current output

The FMEDA carried out on the temperature converters KF**-GUT-(Ex)1.D with current output 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} = 1,67E-07 1/h

λ_{du} = 6,64E-08 1/h

λ_{high} = 1,68E-08 1/h

λ_{low} = 1,57E-07 1/h

λ_{au} = 2,20E-09 1/h

$\lambda_{no\ effect}$ = 2,36E-07 1/h

λ_{total} = 6,45E-07 1/h

$\lambda_{not\ part}$ = 5,34E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 163 years

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

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**341**
Fail detected (internal diagnostics or indirectly[11])	167
Fail High (detected by the logic solver)	17
Fail low (detected by the logic solver)	157
Fail Dangerous Undetected	**66**
No Effect	**236**
Annunciation Undetected	**2**
Not part	**53**

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} [12]	λ_{DD}	$\lambda_{DU} = \lambda_{du} + \lambda_{au}$	**SFF**	**DC_S**	**DC_D**
0 FIT	236 FIT	341 FIT	68 FIT	89,46%	0%	83%

[11] "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.

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

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 2,98E-04	**PFD_{AVG} = 5,96E-04**	**PFD_{AVG} = 1,49E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 5 shows the time dependent curve of PFD_{AVG}.

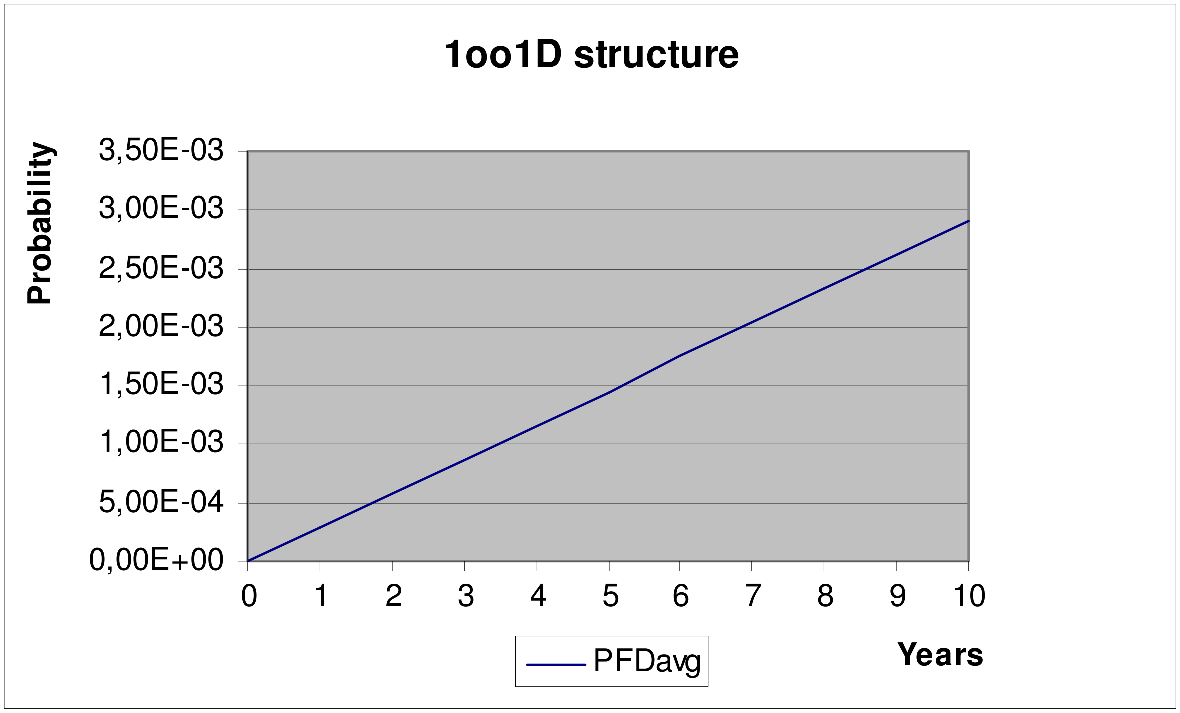


Figure 5: PFD_{AVG}(t)

5.2 KF**-GUT-(Ex)1.D with one relay output

The FMEDA carried out on the temperature converters KF**-GUT-(Ex)1.D with one relay output leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 2,20E-07 1/h

λ_{dd} = 1,17E-07 1/h

λ_{du} = 1,04E-07 1/h

λ_{au} = 2,20E-09 1/h

$\lambda_{no\ effect}$ = 2,25E-07 1/h

λ_{total} = 6,68E-07 1/h

$\lambda_{not\ part}$ = 5,32E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 158 years

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

λ_{SD}	λ_{SU} [13]	λ_{DD}	$\lambda_{DU} = \lambda_{du} + \lambda_{au}$	SFF	DC_S	DC_D
0 FIT	445 FIT	117 FIT	106 FIT	84,13%	0%	52%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.64E-04	PFD_{AVG} = 9.29E-04	PFD_{AVG} = 2.32E-03

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 6 shows the time dependent curve of PFD_{AVG}.

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

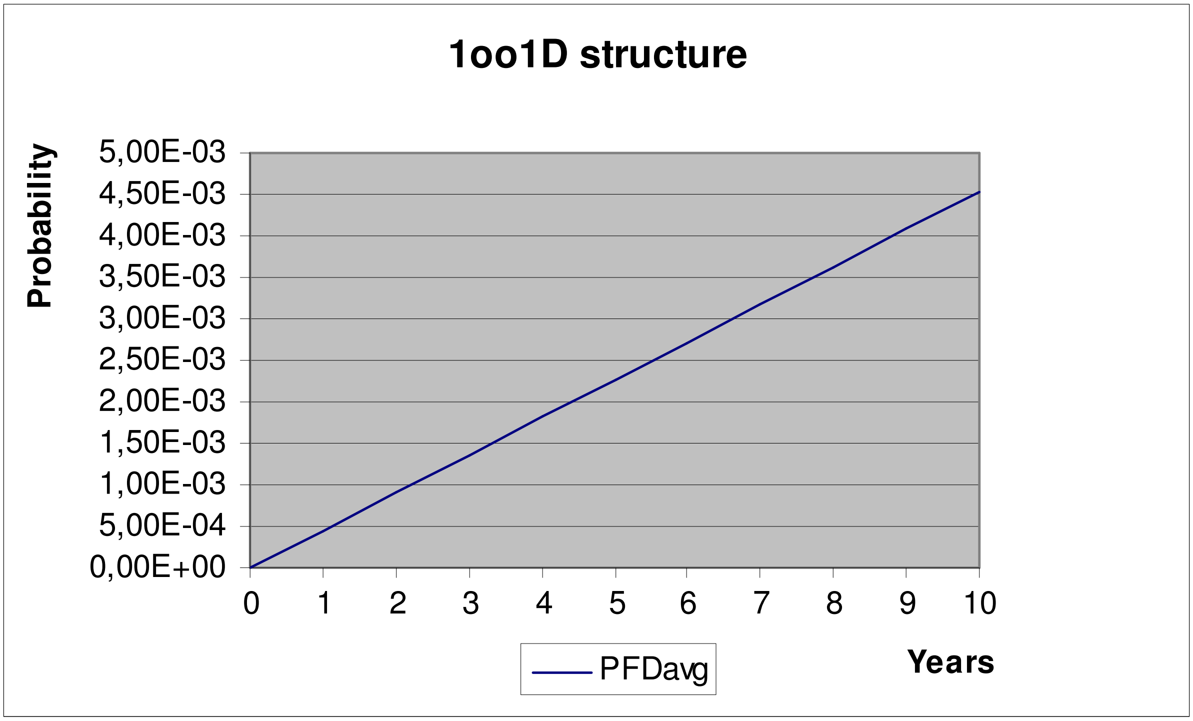


Figure 6: PFD$_{AVG}$(t)

5.3 KF**-GUT-(Ex)1.D with two relay outputs

The FMEDA carried out on the temperature converters KF**-GUT-(Ex)1.D with two relay outputs leads under the assumptions described in section 4.2.3 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 2,56E-07 1/h

λ_{dd} = 1,47E-07 1/h

λ_{du} = 7,33E-08 1/h

λ_{ad} = 3,03E-08 1/h

λ_{au} = 4,09E-09 1/h

$\lambda_{no\ effect}$ = 2,30E-07 1/h

λ_{total} = 7,41E-07 1/h

$\lambda_{not\ part}$ = 5,32E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 144 years

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

λ_{SD}	λ_{SU} [14]	$\lambda_{DD} = \lambda_{dd} + \lambda_{ad}$	$\lambda_{DU} = \lambda_{du} + \lambda_{au}$	SFF	DC_S	DC_D
0 FIT	486 FIT	177 FIT	77 FIT	89,56%	0%	65%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.37E-04	**PFD_{AVG} = 6.75E-04**	**PFD_{AVG} = 1.69E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 7 shows the time dependent curve of PFD_{AVG}.

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

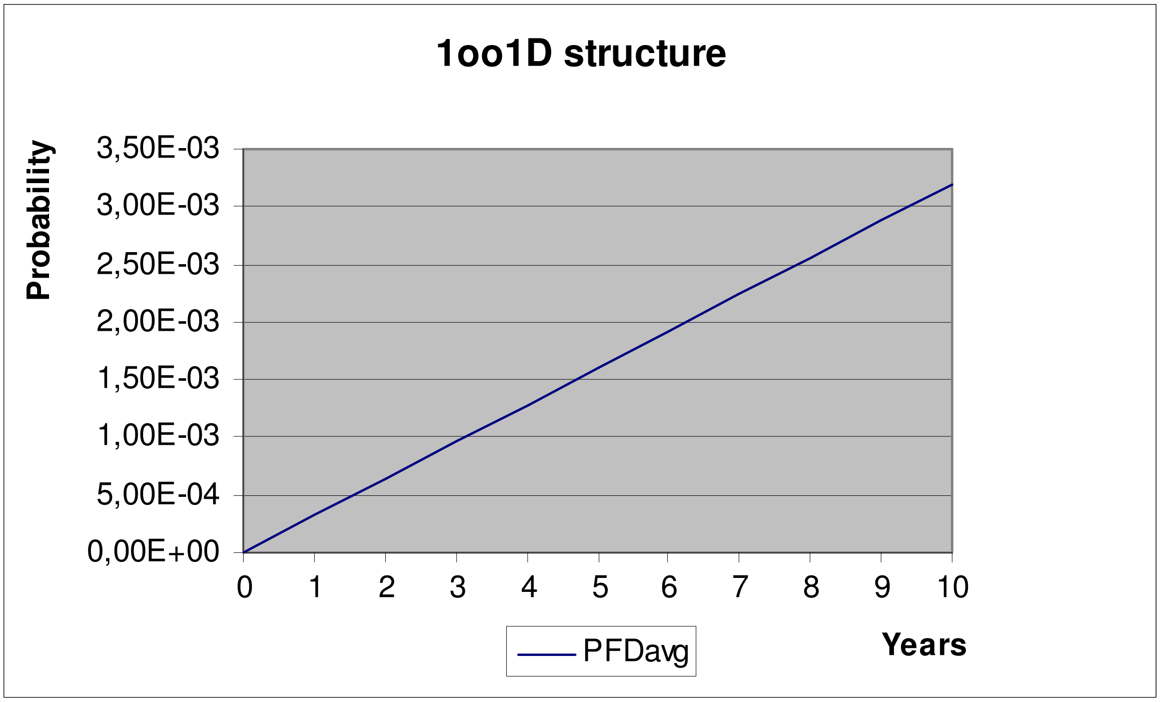


Figure 7: PFD$_{AVG}$(t)

5.4 KFD2-UT2-(Ex)* with current / voltage output

The FMEDA carried out on the temperature converters KFD2-UT2-(Ex)* with current / voltage output 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} = 1,48E-07 1/h

λ_{du} = 7,43E-08 1/h

λ_{high} = 2,36E-08 1/h

λ_{low} = 1,61E-07 1/h

λ_{au} = 4,89E-09 1/h

$\lambda_{no\ effect}$ = 2,95E-07 1/h

λ_{total} = 7,06E-07 1/h

$\lambda_{not\ part}$ = 3,34E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 154 years

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

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**333**
Fail detected (internal diagnostics or indirectly[15])	148
Fail High (detected by the logic solver)	24
Fail low (detected by the logic solver)	161
Fail Dangerous Undetected	**74**
No Effect	**295**
Annunciation Undetected	**5**
Not part	**33**

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} [16]	λ_{DD}	$\lambda_{DU} = \lambda_{du} + \lambda_{au}$	SFF	DC_S	DC_D
0 FIT	295 FIT	333 FIT	79 FIT	88,78%	0%	81%

[15] "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.

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

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3,47E-04	**PFD_{AVG} = 6,94E-04**	**PFD_{AVG} = 1,73E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 5 shows the time dependent curve of PFD_{AVG}.

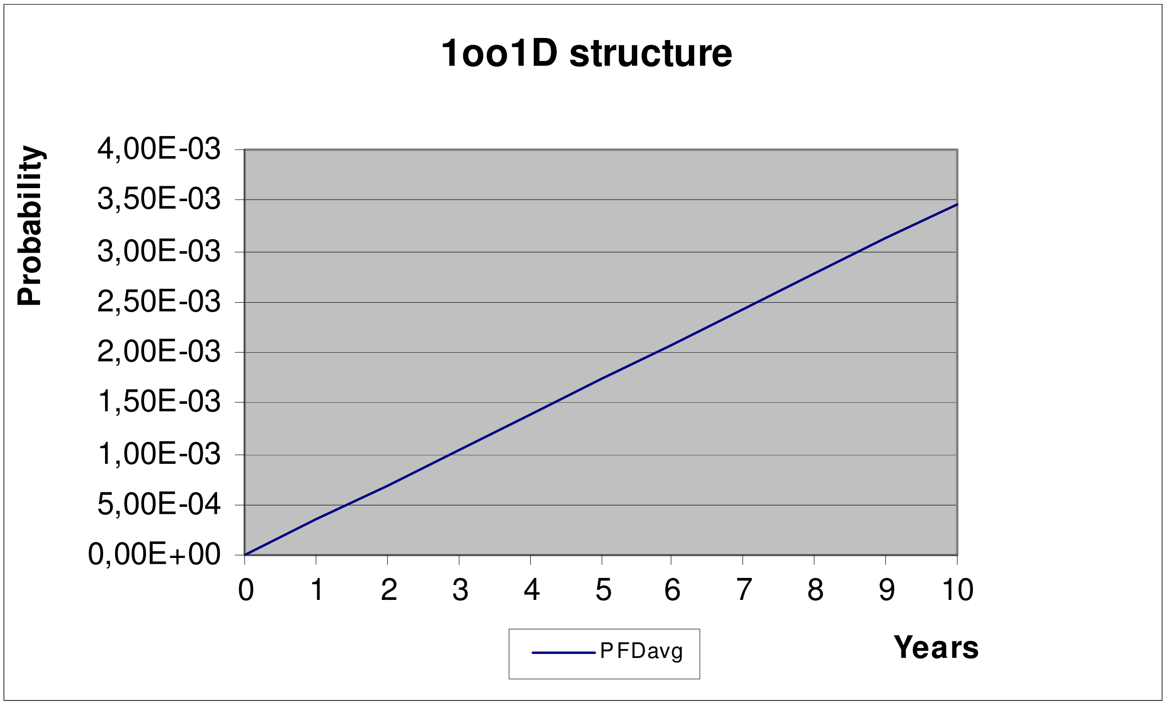


Figure 8: $PFD_{AVG}(t)$

5.5 HiD2082 with current / voltage output

The FMEDA carried out on the temperature converter HiD2082 with current / voltage output 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} = 1,47E-07 1/h

λ_{du} = 9,61E-08 1/h

λ_{high} = 1,86E-08 1/h

λ_{low} = 2,30E-07 1/h

λ_{au} = 5,53E-09 1/h

$\lambda_{no\ effect}$ = 3,02E-07 1/h

λ_{total} = 7,98E-07 1/h

$\lambda_{not\ part}$ = 4,56E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 135 years

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

Failure category	**Failure rates (in FIT)**
Fail Dangerous Detected	**396**
Fail detected (internal diagnostics or indirectly[17])	147
Fail High (detected by the logic solver)	19
Fail low (detected by the logic solver)	230
Fail Dangerous Undetected	**96**
No Effect	**302**
Annunciation Undetected	**6**
Not part	**46**

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} [18]	λ_{DD}	$\lambda_{DU} = \lambda_{du} + \lambda_{au}$	SFF	DC_S	DC_D
0 FIT	302 FIT	396 FIT	102 FIT	87,26%	0%	80%

[17] "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.

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

The PFD_{AVG} was calculated for three different proof test times using the Markov model as described in Figure 4.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4,45E-04	**PFD_{AVG} = 8,90E-04**	**PFD_{AVG} = 2,22E-03**

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 5 shows the time dependent curve of PFD_{AVG}.

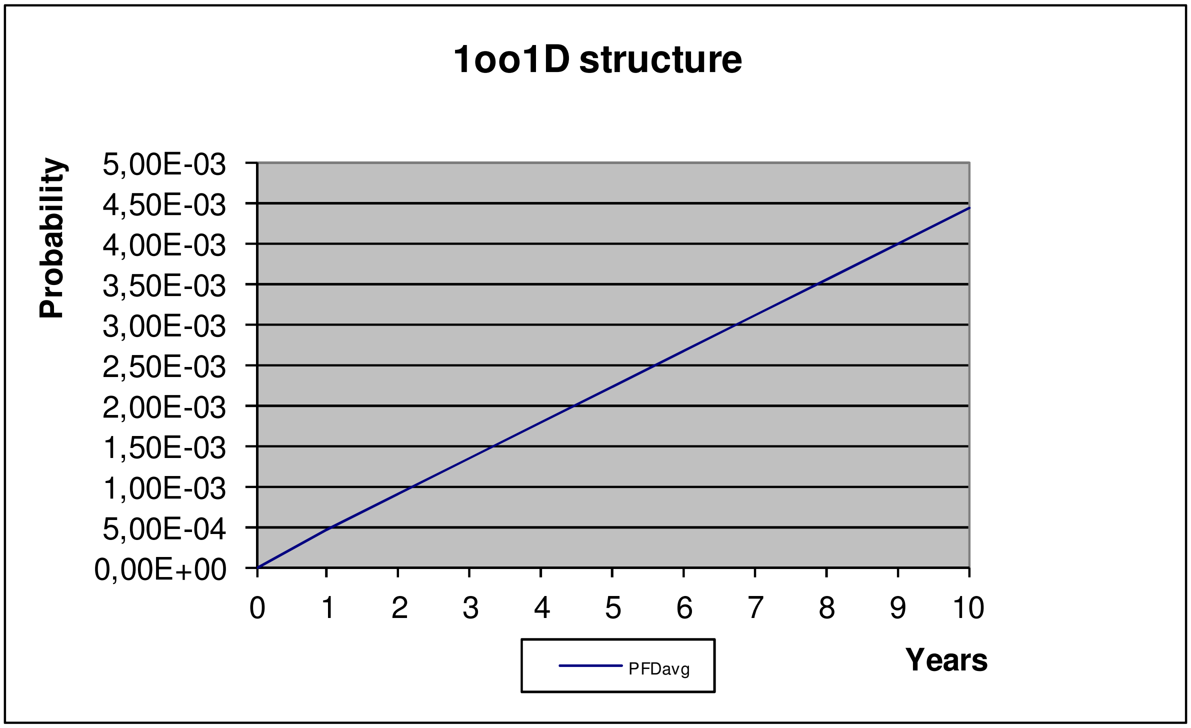


Figure 9: PFD_{AVG}(t)

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 proven by use 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 proof is given 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%[19].

The assessment of the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 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**[20]
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 3 years in a wide range of applications. They are considered to be of medium complexity and the probability that they will fail[21] is <0,4%. 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D7] to [D9]. The assessed sub-system are clearly identified and specified (see Table 1). The field feedback tracking database of Pepperl+Fuchs GmbH together with the explanations given in [D10] to [D12], [D29], [D30] and [D41] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience. The software and hardware modifications were carried out in accordance with an accepted modification process (see [D13] to [D24], [D26] to [D31] and [D38] to [D40]). For KF**-GUT-(Ex)1.D operating experience exist with more than 35.500.000 operating hours for software versions V1.09, V1.14 and V1.38. For KFD2-UT2-(Ex)* operating experience exist with more than 350.000.000 operating hours for software versions V1.39. For HiD2082 operating experience exist with more than 33.000.000 operating hours for software versions V1.39. 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. The collective error output is not part of the safety function and does not jeopardize the required safety instrumented function. 5. Under the responsibility of the user / manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D12].
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

[19] 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…".

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

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

Requirement	Argumentation[20]
	outputs being de-energized or reaching the NAMUR NE43 alarm levels.
Adjustment of process-related parameters is protected	Process related parameters are protected by password.
SIL < 4	The devices shall be assessed for suitability in SIL 2 safety functions only.

This means that the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 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

Low demand mode Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.

PFD_{AVG} Average Probability of Failure on Demand

SFF Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.

SIF Safety Instrumented Function

SIL Safety Integrity Level

Type B subsystem “Complex” subsystem (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:	V3R0:	HiD2082 added; March 10, 2010
	V2, R1:	Editorial changes, December 12, 2008
	V2, R0:	Version KFD2-UT2-(Ex)* added, December 11, 2008
	V1, R2:	Update because of new software version, February 19, 2007
	V1, R1.1:	Appendix 4 modified, April 28, 2006
	V1, R1.0:	Review comments incorporated, April 27, 2006
	V0, R1.0:	Initial version, March 31, 2006
Author:	Stephan Aschenbrenner	
Review:	V2, R0:	Harald Eschelbach (P+F); December 12, 2008
	V0, R1.0:	Harald Eschelbach (P+F); April 3, 2006
		Rachel Amkreutz (exida); April 20, 2006
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 15 to Table 18 show an importance analysis of the ten most critical dangerous undetected faults and indicates 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 15: Importance analysis of "du" failures for KF-GUT-(Ex)1.D with current output**

Component	% of total λ_{du}	Detection through
IC20-2 (µC)	30,10%	100% functional test with different expected output signals over the entire range
IC10-2 (ADC)	20,34%	100% functional test with different expected output signals over the entire range
IC21	9,03%	100% functional test with different expected output signals over the entire range
IC29	4,54%	100% functional test with different expected output signals over the entire range
IC11	1,81%	100% functional test with different expected output signals over the entire range
C104	1,51%	100% functional test with different expected output signals over the entire range
C103	1,51%	100% functional test with different expected output signals over the entire range
C102	1,51%	100% functional test with different expected output signals over the entire range
C120	1,50%	100% functional test with different expected output signals over the entire range
C123	1,50%	100% functional test with different expected output signals over the entire range

Table 16: Importance analysis of “du” failures for KF-GUT-(Ex)1.D with relay output**

Component	% of total λ_{du}	Detection through
K04	24,08%	100% functional test with monitoring of the output signal
IC20-2 (µC)	19,26%	100% functional test with monitoring of the output signal
IC10-2 (ADC)	13,02%	100% functional test with monitoring of the output signal
G200	8,67%	100% functional test with monitoring of the output signal
IC21	5,78%	100% functional test with monitoring of the output signal
U03	4,33%	100% functional test with monitoring of the output signal
IC29	2,90%	100% functional test with monitoring of the output signal
P11	1,59%	100% functional test with monitoring of the output signal
IC11	1,16%	100% functional test with monitoring of the output signal
C120	0,96%	100% functional test with monitoring of the output signal

Table 17: Importance analysis of “du” failures for KFD2-UT2-(Ex)*

Component	% of total λ_{du}	Detection through
IC3-2	26,90%	100% functional test with monitoring of the output signal
IC13-2	18,18%	100% functional test with monitoring of the output signal
IC2	8,07%	100% functional test with monitoring of the output signal
C24, C21, C38, C37, C36	6,73%	100% functional test with monitoring of the output signal
IC10	5,38%	100% functional test with monitoring of the output signal
C31	4,04%	100% functional test with monitoring of the output signal
IC23	4,04%	100% functional test with monitoring of the output signal
IC21	3,23%	100% functional test with monitoring of the output signal
N8, N11, N14, N16	2,69%	100% functional test with monitoring of the output signal
C71, C73	2,69%	100% functional test with monitoring of the output signal

Table 18: Importance analysis of “du” failures for HiD2082

Component	**% of total λ_{du}**	**Detection through**
K3:C and K3:D	24,97%	100% functional test with monitoring of the output signal
IC5-2	20,81%	100% functional test with monitoring of the output signal
IC1-2	14,06%	100% functional test with monitoring of the output signal
IC6	6,24%	100% functional test with monitoring of the output signal
C56, C54, C78, C80, C81	5,20%	100% functional test with monitoring of the output signal
IC11	4,16%	100% functional test with monitoring of the output signal
C72	3,12%	100% functional test with monitoring of the output signal
N30	3,12%	100% functional test with monitoring of the output signal
C24, C29	2,08%	100% functional test with monitoring of the output signal
P21	1,72%	100% functional test with monitoring of the output signal

Appendix 2.1: Possible proof tests to detect dangerous undetected faults

KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)*, HiD2082 with current / voltage output

Proof test 1 consists of the following steps, as described in Table 19.

Table 19 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 temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 to go to the high alarm current / voltage output and verify that the analog current / voltage 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 temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 to go to the low alarm current / voltage output and verify that the analog current / voltage 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 temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 with current / voltage output.

Proof test 2 consists of the following steps, as described in Table 20.

Table 20 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 temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082
4	Restore the loop to full operation
5	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect more than 90% of possible "du" failures in the temperature converters KF**-GUT-(Ex)1.D, KFD2-UT2-(Ex)* and HiD2082 with current / voltage output.

Temperature converter KF-GUT-(Ex)1.D with relay output**

Proof test 1 consists of the following steps, as described in Table 19.

Table 21 Steps for Proof Test 1

Step	Action
1	Take appropriate action to avoid a false trip
2	Force the temperature converter KF**-GUT-(Ex)1.D to reach a defined "MAX" threshold value and verify that the output goes into the safe state.
3	Restore the loop to full operation
4	Restore normal operation

Proof test 2 consists of the following steps, as described in Table 20.

Table 22 Steps for Proof Test 2

Step	Action
1	Take appropriate action to avoid a false trip
2	Force the temperature converter KF**-GUT-(Ex)1.D to reach a defined "MIN" threshold value and verify that the output goes into the safe state.
3	Restore the loop to full operation
4	Restore normal operation

Both tests together will detect approximately 99% of possible "du" failures.

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[22] 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 23 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 23: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life at 40°C
Relay	K03, K04	Approximately 100.000 switching cycles
Capacitor (electrolytic) - Aluminum electrolytic, non solid electrolyte	C31	Approximately 90 000 Hours[23]

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.

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

[22] 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.

[23] 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.

Appendix 4: Using the FMEDA results as an example on KF**-GUT-(Ex)1.D

The temperature converter KF**-GUT-(Ex)1.D with one relay output together with a temperature sensing device becomes a temperature sensor assembly as indicated in Figure 1. Therefore when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered.

Appendix 4.1: KF**-GUT-(Ex)1.D with thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or "burn-out" failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 24 when thermocouples are supplied with the temperature converter KF**-GUT-(Ex)1.D with one relay output. The drift failure mode is primarily due to T/C aging. The temperature converter KF**-GUT-(Ex)1.D with one relay output will detect a thermocouple burn-out failure and drive it's output to the specified failure state.

Table 24 Typical failure rates for thermocouples

Thermocouple Failure Mode Distribution	***Low Stress***	***High Stress***
Open Circuit (Burn-out)	4750 FIT	19000 FIT
Short Circuit (Temperature measurement in error)	50 FIT	200 FIT
Drift (Temperature measurement in error)	200 FIT	800 FIT

A complete temperature sensor assembly consisting of the temperature converter KF**-GUT-(Ex)1.D with one relay output and a thermocouple can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the temperature converter KF**-GUT-(Ex)1.D with one relay output will go to the safe state on detected failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

- λ_{sd} = (5.000 FIT) * (0,95) = 4.750 FIT
- λ_{du} = (5.000 FIT) * (0,05) = 250 FIT

This results in a failure rate distribution, SFF and PFD_{AVG} (assuming T[Proof] = 1 year) to:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**PFD_{AVG}**
4750 FIT	445 FIT	117 FIT	356 FIT	93,72 %	1,56E-03

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions.

Appendix 4.2: KF**-GUT-(Ex)1.D with RTD

The failure mode distribution for an RTD also depends on the application with the key variables being stress level, RTD wire length and RTD type (2/3 wire or 4 wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions with extension wire are shown in Table 25 and Table 26. The temperature converter KF**-GUT-(Ex)1.D with one relay output will detect open circuit and short circuit RTD failures and drive it's output to the specified failure state.

Table 25 Typical failure rates for 4-Wire RTDs with extension wire

RTD Failure Mode Distribution	*Low Stress*	*High Stress*
Open Circuit (Burn-out)	1490 FIT	7390 FIT
Short Circuit (Temperature measurement in error)	590 FIT	730 FIT
Drift (Temperature Measurement in error)	20 FIT	80 FIT

Table 26 Typical failure rates for 2/3-Wire RTDs with extension wire

RTD Failure Mode Distribution	*Low Stress*	*High Stress*
Open Circuit (Burn-out)	1090 FIT	4990 FIT
Short Circuit (Temperature measurement in error)	610 FIT	810 FIT
Drift (Temperature Measurement in error)	400 FIT	1600 FIT

A complete temperature sensor assembly consisting of the temperature converter KF**-GUT-(Ex)1.D with one relay output and a 4-wire RTD can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the temperature converter KF**-GUT-(Ex)1.D with one relay output will go to the safe state on a detected failure of the RTD, the failure rate contribution for the 4-wire RTD in a low stress environment is:

- λ_{sd} = 1.490 FIT + 590 FIT = 2.080 FIT
- λ_{du} = 20 FIT

This results in a failure rate distribution, SFF and PFD_{AVG} (assuming T[Proof] = 1 year) to:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**PFD_{AVG}**
2080 FIT	445 FIT	117 FIT	126 FIT	95,45 %	5,52E-04

The same can be calculated for a complete temperature sensor assembly consisting of the temperature converter KF**-GUT-(Ex)1.D with one relay output and 2/3-wire RTD. Assuming that the temperature converter KF**-GUT-(Ex)1.D with one relay output will go to the safe state on a detected failure of the RTD, the failure rate contribution for the 2/3-wire RTD in a low stress environment is:

- λ_{sd} = 1.090 FIT + 610 FIT = 1.700 FIT
- λ_{du} = 400 FIT

This results in a failure rate distribution, SFF and PFD_{AVG} (assuming T[Proof] = 1 year) to:

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**	**PFD_{AVG}**
1700 FIT	445 FIT	117 FIT	506 FIT	81,72 %	2,22E-03

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions.