FMEDA and Proven-in-use Assessment

Project:
Transmitter Supply Isolators KF**-CRG-***

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 02/11-01
Report No.: P+F 02/11-01 R012
Version V2, Revision R1.1, April 2005
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 Transmitter Supply Isolators KF**-CRG-*** with software version CRG2V10. '**' and '***' stand for the different versions that are available.

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

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

Table 1: Version overview

Type	Supply voltage	Inputs	Outputs
KFD2-CRG-1.D	24 VDC	AI 0/4..20mA	1 AO 0/4..20mA 2 relay outputs
KFD2-CRG-Ex1.D	24 VDC	AI 0/4..20mA Eex ia IIC	1 AO 0/4..20mA 2 relay outputs
KFU8-CRG-1.D	20..90 VDC 48..253 VAC	AI 0/4..20mA	1 AO 0/4..20mA 2 relay outputs
KF U8-CRG-Ex1.D	20..90 VDC 48..253 VAC	AI 0/4..20mA Eex ia IIC	1 AO 0/4..20mA 2 relay outputs

The two relay outputs on each module shall not be used to increase the hardware fault tolerance, needed to achieve a higher SIL for a certain safety function, as they contain common components.

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 $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range. For a SIL 2 application the total PFD_{AVG} value of the SIF must be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the Transmitter Supply Isolators KF**-CRG-*** would then be 1,00E-03.

The Transmitter Supply Isolators KF**-CRG-*** are considered to be Type B 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 Transmitter Supply Isolators KF**-CRG-*** are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the device and its software 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 5.1 a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% to < 90%.

Table 2: Summary for the Transmitter Supply Isolators KF-CRG-*** (relay output)**

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF	DC$_S$	DC$_D$
PFD$_{AVG}$ = 3.94E-04	**PFD$_{AVG}$ = 7.88E-04**	**PFD$_{AVG}$ = 1.97E-03**	> 83 %	3 %	50%

λ_{sd} = 9,00E-09 1/h = 9 FIT

λ_{su} = 3,47E-07 1/h = 347 FIT

λ_{dd} = 8,90E-08 1/h = 89 FIT

λ_{du} = 9,00E-08 1/h = 90 FIT

Table 3: Summary for the Transmitter Supply Isolators KF-CRG-*** (current output)**

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	SFF	DC$_S$	DC$_D$
PFD$_{AVG}$ = 4.14E-04	**PFD$_{AVG}$ = 8.29E-04**	**PFD$_{AVG}$ = 2.07E-03**	> 81 %	0 %	71%

λ_{sd} = 0,00E-00 1/h = 0 FIT

λ_{su} = 1,73E-07 1/h = 173 FIT

λ_{dd} = 2,43E-07 1/h = 243 FIT

λ_{du} = 9,47E-08 1/h = 95 FIT

The boxes marked in yellow (🟨) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03.

The 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°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

The hardware assessment according to IEC 61508 has shown that the Transmitter Supply Isolators KF-CRG-*** have a PFD$_{AVG}$ within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of > 83%. Based on the verification of "prior use" they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.**

A user of Transmitter Supply Isolators KF**-CRG-*** can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). The failure rates are presented in section 5.2 along with all assumptions.

Table of Contents

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment contains a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the software development process

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

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition this option consists of an assessment of the proven-in-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like draft IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 2.

This document shall describe the results of the assessment carried out on the Transmitter Supply Isolators KF**-CRG-*** with software version CRG2V10. Table 1 gives an overview of the different types that belong to the considered family.

It shall be assessed whether these boards meet the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

Pepperl+Fuchs GmbH contracted *exida.com* in November 2002 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

2 Project management

2.1 *exida.com*

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

2.2 Roles of the parties involved

Pepperl+Fuchs	Manufacturer of the Transmitter Supply Isolators KF**-CRG-***.
exida.com	Performed the hardware and proven-in-use assessment according to option 2 (see section 1).

2.3 Standards / Literature used

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

N1	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
N2	IEC 61511-1 First Edition 2003-01	Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements
N3	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
N4	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
N5	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
N6	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	01-4294 of 02.04.01	Circuit diagram for KF..-CRG/CRGN-(Ex)1..
[D2]	1-4384C of 14.04.00	Circuit diagram for KFU8/KFD2 Netzt.
[D3]	Product No. 051097	Bill of material for KFD2-CRG-Ex1.D
[D4]	Product No. 051099	Bill of material for KFU8-CRG-Ex1.D
[D5]	1830076C.pdf of 02.07.03	Software release information for software number 18-30076, Version CRG2V10 Index C
[D6]	Firmwarehistorie CRG.doc 07.07.03	Software history
[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]	SIL2_CRG.doc of 08.07.03	Field data evaluation (operating hours, sold devices) and application examples
[D11]	CRG.xls of 09.07.03	Field data evaluation (returned devices)
[D12]	Email of 09.07.03	Information about returned devices
[D13]	Email of 09.07.03	Information about the adjustment of process-related parameters and the modification process

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA V4 R0.9 KFD2-CRG-Ex1.D V1 R1.0.xls of 04.07.03
[R2]	FMEDA V5 KFD2-CRG-Ex1.D current output V1 R1.0.xls of 31.03.05
[R3]	Minutes of Meeting (Besprechungsbericht 23. - 24.04.03.doc of 24.04.03)
[R4]	CRG - operating hours.xls of 09.07.03 (Field data evaluation of operating hours and sold devices)
[R5]	Rückläufer.xls of 09.07.03 (Field data evaluation of returned devices)

3 Description of the analyzed modules

3.1 Transmitter Supply Isolators KF**-CRG-***

The Transmitter Supply Isolators KF**-CRG-*** are suited for a variety of measuring tasks. 2- and 3-wire transmitters as well as active power supplies with 0/4..20 mA signal can be connected.

Two relays and an active 0/4 mA..20 mA current output are available as outputs.

Both inputs have a lead breakage and short circuit monitoring in the input circuit.

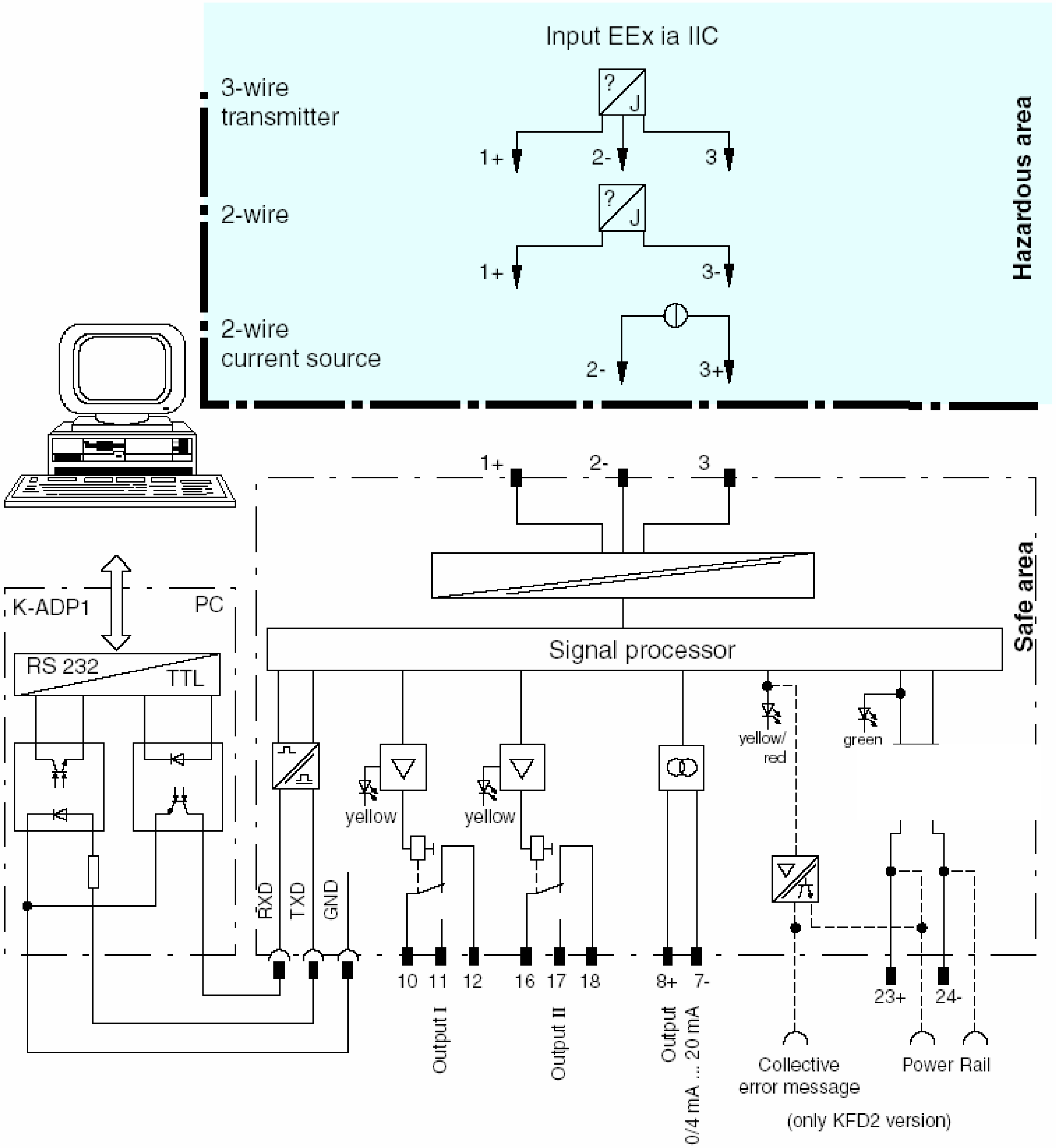


Figure 1: Block diagram of KFD2-CRG-Ex1.D

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs and is documented in [R1] and [R2]. Failures can be classified according to the following failure categories.

4.1 Description of the failure categories

General

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).

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.

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.

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). The output remains energized.

Current output

Fail-Safe State
The fail-safe state is defined as the output going to fail low or fail high.

Fail Dangerous
A dangerous failure (D) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% full scale (+/- 0.8mA).

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

Fail Low
Failure that causes the output signal to go to a minimum output current (< 3,6mA).

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.com* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates are considered to be appropriate for safety integrity level verification calculations. The rates 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 Failure Modes, Effects, and Diagnostic Analysis of the Transmitter Supply Isolators KF**-CRG-***.

- Short Circuit (SC) detection and Lead Breakage (LB) detection are activated.
- Process related parameters are protected by password.
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The current output is configured for 4..20 mA.
- The alarm current is set to “fail low” or “fail high”.
- Failures during parameterization are not considered.
- 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.
- External power supply failure rates are not included.
- All modules are operated in the low demand mode of operation.
- The application program in the safety logic solver is constructed in such a way that fail low and fail high failures are detected regardless of the effect, safe or dangerous, on the safety function.

5 Results of the assessment

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

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

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

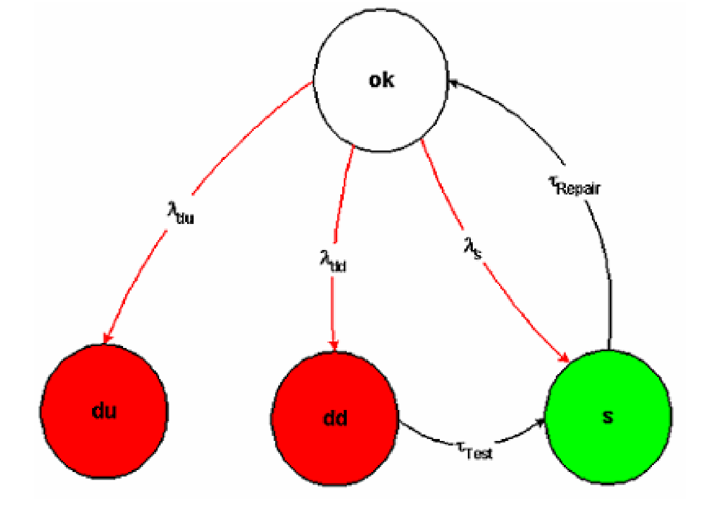
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{don't\ care} + \lambda_{annunciation}$.

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

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

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

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



Abbreviations:

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

Figure 2: Markov model for a 1oo1D structure

5.1 Assessment of the Transmitter Supply Isolators KF**-CRG-***

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%[1].

The assessment of the Transmitter Supply Isolators KF**-CRG-*** has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

[1] IEC 61511-1 First Edition 2003-01 explicitly says "…provided that the dominant failure mode is to the safe state or dangerous failures are detected…".

Requirement	Argumentation[2]
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 2 years in a wide range of applications. They are considered to be of medium complexity and the probability that they will fail[3] is low (<0,6%). 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D11] 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 [D13] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience (Operating experience of more than 33.000.000 operating hours exists. This is considered to be sufficient taking into account the medium complexity of the sub-system and the use in SIL 2 safety functions only). 3. 11.5.2 is under the responsibility of the user / manufacturer –> no argumentation. 11.5.3 see bullet items before. 4. Error message outputs are not part of the safety function and do not jeopardize the required safety instrumented functions. 5. Under the responsibility of the manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D10]
Adjustment of process-related parameters only	The user can enable or disable short circuit and lead breakage detection and change the mode of operation. For safety applications, however short circuit and lead breakage detection shall always be activated and the fail-safe state shall be configured as the outputs being de-energized.
Adjustment of process-related parameters is protected	Process related parameters can be protected by password.
SIL < 4	The device shall be assessed for its suitability in SIL 2 safety functions only.

This means that the Transmitter Supply Isolators KF**-CRG-*** can be considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01. and therefore the minimum hardware fault tolerance (HFT) specified in Table 6 of IEC 61511-1 First Edition 2003-01 can be reduced by one. The required SFF of 60% - < 90% for HFT =1 can therefore be applied for HFT = 0.

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

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

5.2 Transmitter Supply Isolators KF**-CRG-*** (relay output)

The FMEDA carried out on the Transmitter Supply Isolators KF**-CRG-*** (relay output) leads under the assumptions described in section 4.2.1 and 5 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

$\lambda_{su} = \lambda_{su} + \lambda_{don't\ care} + \lambda_{annunciation}$ = 1,67E-07 1/h + 1,77E-07 1/h + 3,36E-09 1/h = 3,47E-07 1/h

λ_{dd} = 8,90E-08 1/h

λ_{du} = 9,00E-08 1/h

λ_{total} = 5,35E-07 1/h

$\lambda_{not\ part}$ = 3,88E-08 1/h

SFF = 83,18%

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 2.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 3.94E-04	PFD_{AVG} = 7.88E-04	PFD_{AVG} = 1.97E-03

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 3 shows the time dependent curve of PFD_{AVG}.

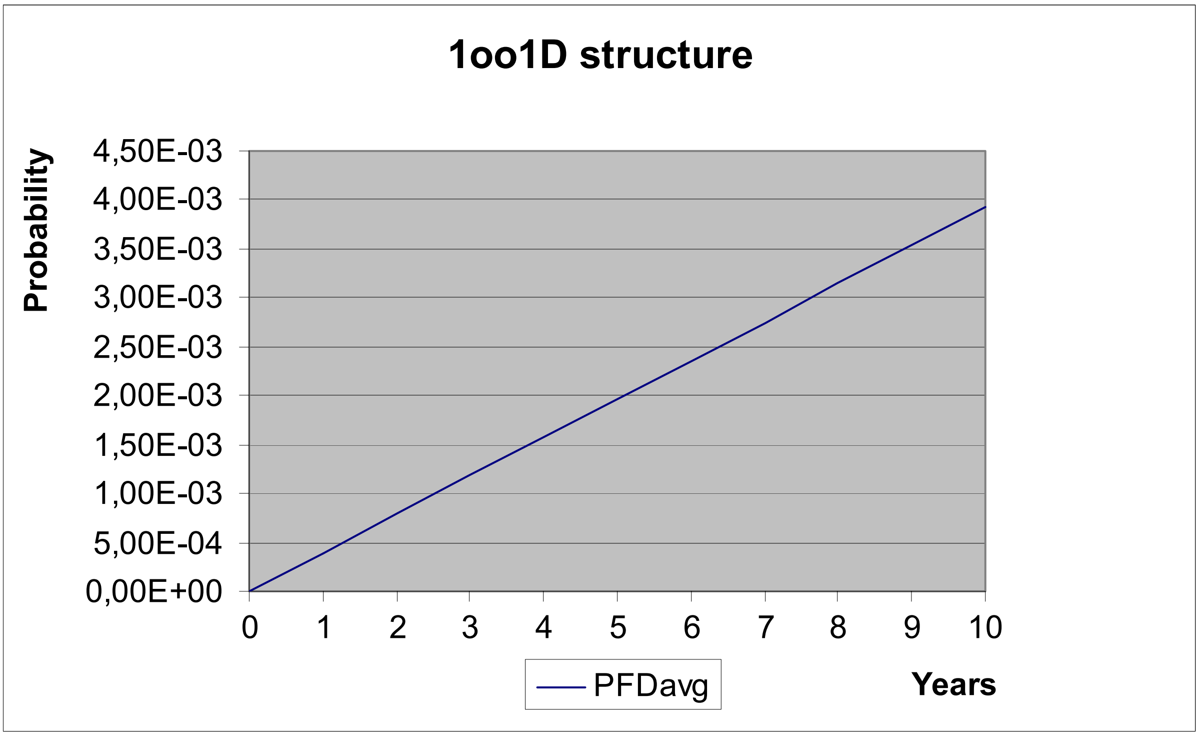


Figure 3: PFD_{AVG}(t)

5.3 Transmitter Supply Isolators KF**-CRG-*** (current output)

The FMEDA carried out on the Transmitter Supply Isolators KF**-CRG-*** (current output) leads under the assumptions described in section 4.2.1 and 5 to the following failure rates and SFF:

λ_{sd} = 9,00E-09 1/h

λ_{su} = 5,63E-08 1/h

λ_{dd} = 6,55E-08 1/h

λ_{du} = 9,47E-08 1/h

λ_{high} = 2,29E-09 1/h

λ_{low} = 1,10E-07 1/h

$\lambda_{annunciation}$ = 3,36E-09 1/h

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

λ_{total} = 5,11E-07 1/h

$\lambda_{not\ part}$ = 5,44E-08 1/h

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

SFF = 81,47%

Failure category		Failure rates (in FIT)
Fail Dangerous Detected		243
Fail detected (int. diag.) = λ_{sd} + λ_{su} [4] + λ_{dd}	131	
Fail high (inherently) = λ_{high}	2	
Fail low (inherently) = λ_{low}	110	
Fail Dangerous Undetected		95
No Effect		170
Annunciation Undetected		3
Not part		54
MTBF = MTTF + MTTR		202 years

The PFD_{AVG} was calculated for three different proof times using the Markov model as described in Figure 2.

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 4.14E-04	PFD_{AVG} = 8.29E-04	PFD_{AVG} = 2.07E-03

[4] These failures are not detected by internal diagnostics but because they lead to the safe state they are detected by the logic solver independent of the user defined fail-safe state ("fail low" or "fail high").

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 3 shows the time dependent curve of PFD_{AVG}.

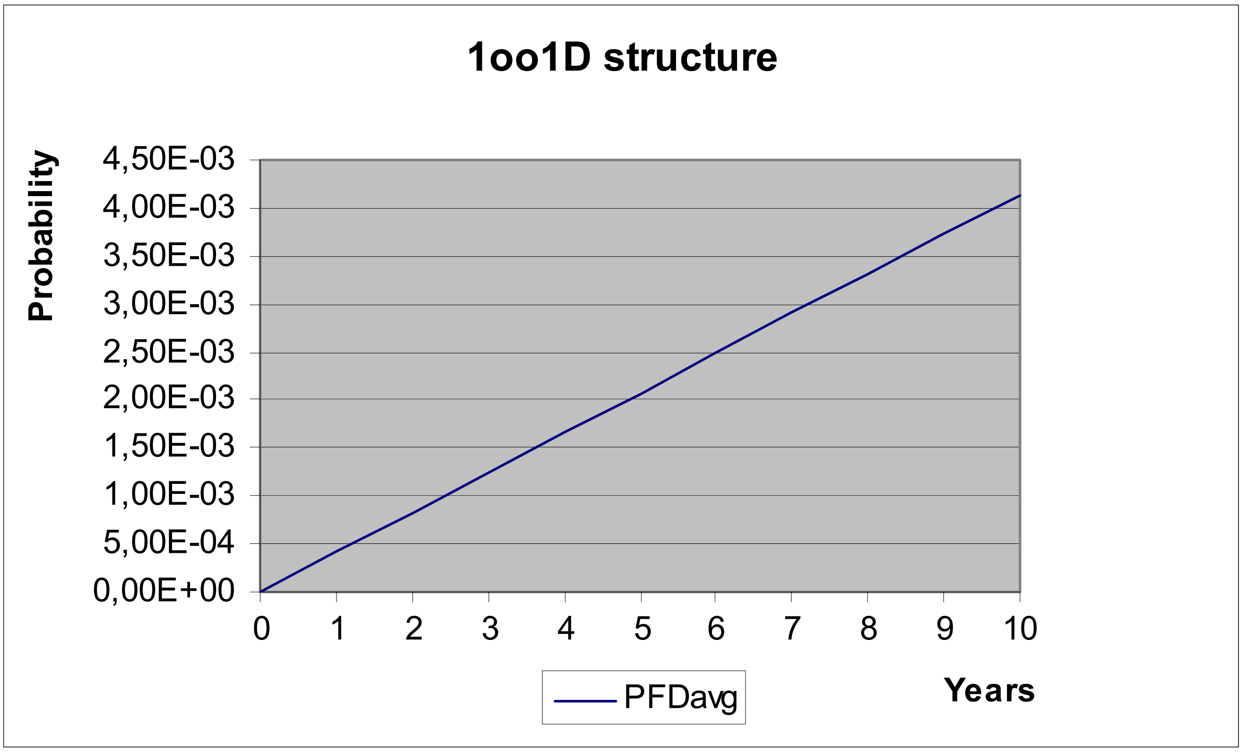


Figure 4: $PFD_{AVG}(t)$

6 Terms and Definitions

DC_S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time ($1x10^{-9}$ 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 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

7 Status of the document

7.1 Liability

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

7.2 Releases

Version:	V2	
Revision:	R1.1	
Version History:	V0, R1.0:	Initial version, July 9, 2003
	V1, R1.0:	Review comments integrated; July 28, 2003
	V1, R1.1:	Editorial changes; August 7, 2003
	V2, R1.0:	Current output added; March 31, 2005
	V2, R1.1:	Review comments integrated; April 4, 2005
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida.com); July 21, 2003
		Stefan Pflüger (P+F); July 25, 2003
	V2, R1.0:	Michael Trautmann (P+F); April 4, 2005
Release status:	Released to Pepperl+Fuchs	

7.3 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 4 and Table 5 show a sensitivity analysis of the ten most critical dangerous undetected faults 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 4: Sensitivity Analysis of dangerous undetected faults (relay output)

Component	% of total λ_{du}	Detection through
IC1	56%	100% functional test
IC9	9%	100% functional test
IC4	7%	100% functional test
G01	7%	100% functional test
U03	5%	100% functional test
IC8	4%	100% functional test
P22	2%	100% functional test
P11	2%	100% functional test
U04	2%	100% functional test
IC10	1%	100% functional test

Table 5: Sensitivity Analysis of dangerous undetected faults (current output)

Component	% of total λ_{du}	Detection through
IC1	53%	100% functional test with monitoring of the output signal
U01	10%	100% functional test with monitoring of the output signal
IC9	8%	100% functional test with monitoring of the output signal
IC4	6%	100% functional test with monitoring of the output signal
G01	6%	100% functional test with monitoring of the output signal
IC8	4%	100% functional test with monitoring of the output signal
IC1	2%	100% functional test with monitoring of the output signal
P22	2%	100% functional test with monitoring of the output signal
U04	2%	100% functional test with monitoring of the output signal
IC10	1%	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 Transmitter Supply Isolators KF**-CRG-*** achieve a SFF of more than 80% without any diagnostics for IC1 and with diagnostics of low effectiveness for IC4.

Failures leading to wrong frequency

Failures which lead to a wrong internal frequency are assumed to be dangerous undetected failures because only no frequency can be detected but not a wrong frequency. The Transmitter Supply Isolators KF**-CRG-*** still achieve a SFF of more than 80% without specific diagnostics for the internal frequency.

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.1) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

The circuit of the Transmitter Supply Isolators KF**-CRG-*** does not contain any electrolytic capacitors that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

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