Failure Modes, Effects and Diagnostic Analysis

Project:
KFD2-RCI-(Ex)1 interface module

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 08/07-21
Report No.: P+F 08/07-21 R033
Version V1, Revision R0; November 2009

Stephan Aschenbrenner, Alexander Dimov

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 carried out on the KFD2-RCI-(Ex)1 interface module in the hardware versions listed in the drawings referenced in section 2.4.1.

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.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 2. The analysis has been carried out with the basic failure rates from the Siemens standard SN 29500. However as the comparison between these two databases has shown that the differences are within an acceptable tolerance the failure rates of the *exida* database are listed.

The KFD2-RCI-(Ex)1 interface module is considered to be Type A[1] subsystems.

It is important to realize that the “no effect” failures are included in the “safe” failure category according to IEC 61508:2000. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

A user of the KFD2-RCI-(Ex)1 interface module can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.3.1 along with all assumptions.

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

Table 1: Summary KFD2-RCI-(Ex)1 interface module – IEC 61508 failure rates

	***exida* Profile 2** [2]
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**190**
Fail safe undetected	76
No effect	114
Fail Dangerous Detected (λ_{DD})	**6**
Fail detected (detected by internal diagnostics)	6
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	**7** [3]
Fail dangerous undetected	1
Annunciation undetected	6
No part	489

Total failure rate (safety function)	**203 FIT**
SFF [4]	**96%** [5]
DC_D	**46%**
MTBF	**165 years**

SIL AC [6]	**SIL 3**

The failure rates are valid for the useful life of the KFD2-RCI-(Ex)1 interface module (see Appendix 2)

[2] For details see Appendix 3.

[3] This value corresponds to a PFH of 7.00E-09 1/h.

[4] The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[5] Complete practical fault insertion tests need to be performed to confirm the assumed behavior of the FMEDA.

[6] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

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 ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

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

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

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

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

Option 3: Full assessment according to IEC 61508

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

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

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment carried out on the KFD2-RCI-(Ex)1 interface module in the hardware versions listed in the drawings referenced in section 2.4.1.

The information in this report can be used to evaluate whether a final element subsystem, including the KFD2-RCI-(Ex)1 interface module meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. 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 and parties

Pepperl+Fuchs GmbH	Manufacturer of the KFD2-RCI-(Ex)1 interface module.
exida	Performed the hardware assessment according to option 1 (see section 1) and reviewed the FMEDA provided by the customer.

Pepperl+Fuchs GmbH contracted *exida* in August 2008 with the FMEDA and PFD_{AVG} calculation of the above mentioned device.

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]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	*exida* L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	3521482.pdf of 21.09.2009	List of components for KFD2-RCI-(Ex)1 complete module of 22.05.2009
[D2]	3550257.pdf of 21.09.2009	Circuit board :dimensions/drilling plan and layout
[D3]	3510592c.pdf of 07.09.2009	Schematic drawing KFD2-RCI-(Ex)1 complete module of 22.05.2009
[D4]	3640006.pdf of 07.09.2009	Functional description KFD2-RCI-(Ex)1 reference EDM 364-0006
[D5]	DDE1460C.pdf of 07.09.2009	Requirements profile KFD2-RCI-(Ex)1 DDE1460C of 05.08.2009
[D6]	RE RCI FMEDA.msg of 15.10.09	Feedback on 2nd FMEDA review comments
[D7]	Fmeda-RCI-r1-complete-module.xls of 23.09.09	

2.4.2 Documentation generated by *exida*

[R1]	RE RCI FMEDA.msg of 20.09.09	1st FMEDA review comments
[R2]	Fmeda-RCI-r5-complete-module.xls of 04.10.2009	

3 Description of the analyzed subsystem

The KFD2-RCI-(Ex)1 interface module converts the binary control signal 0/24V provided by an ESD system (emergency-shut down system) to an “digital” 4-20mA (briefly binary 5.2/16mA for SIL conformity) signal that can be recognized by a safety shutdown ON/OFF valve. KFD2-RCI-(Ex)1 interface module is externally powered by a 24V power supply, in order to provide a current loop of I<5mA for HART communication interface.

The upper part (see Figure 1) represents the basic SIL3 path. This circuit is loop-powered by the digital safety signal provided by the ESD system hence, it is inherently safe because there is not any fault that can keep the output energized when the ESD sets a de-energized state (safe state or shut-down state). This circuit can only energize or de-energize the valve. The FMEDA was performed on section 1 in Figure 1.

The lower part is the section that provides the ancillary functions like diagnostic, HART communication pass-through and fault indications, and besides an analog output versus the safe area. From the “functional safety” point of view, this circuit must not jeopardize the SIL3 level of the loop-powered circuit in case of any fault. Over this analogue loop the HART communication can be superimposed, that permits the exchange of digital data between the control room and the field device.

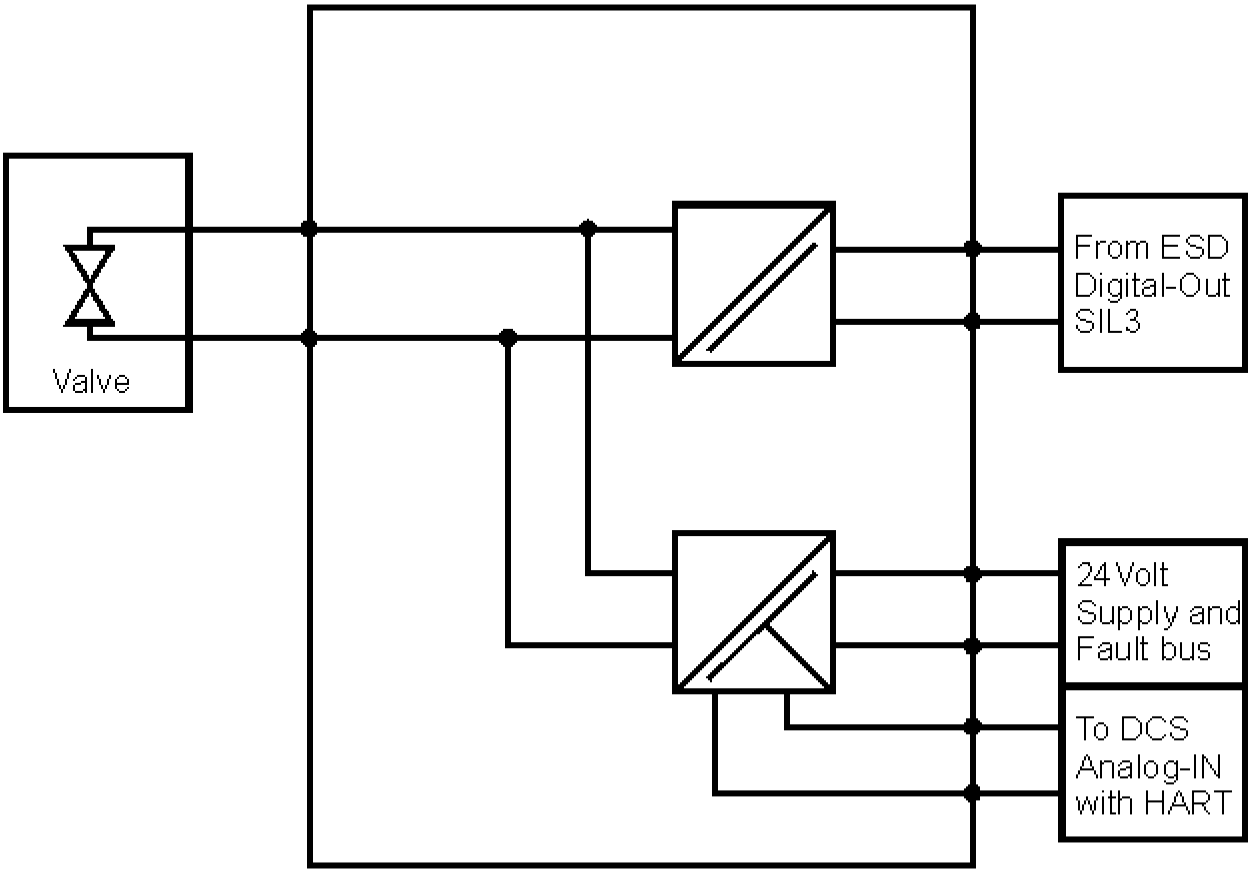

Figure 1: Block diagram of the KFD2-RCI-(Ex)1 interface module

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by Pepperl+Fuchs GmbH and reviewed by *exida*. The results are documented in [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the KFD2-RCI-(Ex)1, the following definitions for the failure of the product were considered.

Fail-Safe State

The fail-safe state is defined as the field output being de-energized. The field output is de-energized when the output current is < 6mA. For this specific module the "safe state" represents a shut-down of the safety loop.

Fail Safe

Failure that causes the subsystem to go to the defined fail-safe state (S) without a demand from the process.

Fail Dangerous

A dangerous failure (D) is defined as a failure that does not respond to a demand from the process.

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 and causes the output signal to go to the predefined alarm state.

No Effect

A no effect failure (#) is defined as a failure of a component that is part of the safety function but has no effect on the safety function or deviates the field output current by not more than ±2 mA. For the calculation of the SFF it is treated like a safe undetected failure..

Annunciation

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). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. For the calculation of the SFF they are treated as “Dangerous Undetected” failures.

No Part

Component that plays no part in implementing the safety function but is 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 not all failure modes have effects that can be accurately classified according to the failure categories listed in IEC 61508:2000.

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 61508.2000 the “No Effect” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions 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 from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 2. 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 *exida* Profile 2. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the KFD2-RCI-(Ex)1 interface module.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- The HART protocol is not part of the considered safety function. It does not transmit any safety critical messages. It only used for setup, calibration and diagnostics purposes.
- The device is installed per manufacturer's instructions.
- Complete practical fault insertion tests can demonstrate that the assumed behavior of the FMEDA.
- 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.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- The input signal is provided by a SIL3 safety PLC.
- Only the described version is used for safety applications.

4.3 Results

For the calculation of the Safe Failure Fraction (SFF) and λ_{total} the following has to be noted:

$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

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

$DC_D = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$

$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part})) + 24\ h$

4.3.1 KFD2-RCI-(Ex)1 interface module

The FMEDA carried out on the KFD2-RCI-(Ex)1 interface module leads under the assumptions described in section 4.2.3 to the following failure rates:

	exida **Profile 2** [7]
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail safe detected	0
Fail Safe Undetected (λ_{SU})	**190**
Fail safe undetected	76
No effect	114
Fail Dangerous Detected (λ_{DD})	**6**
Fail detected (detected by internal diagnostics)	6
Annunciation detected	0
Fail Dangerous Undetected (λ_{DU})	**7** [8]
Fail dangerous undetected	1
Annunciation undetected	6
No part	489

Total failure rate (safety function)	**203 FIT**
SFF [9]	**96%**
DC$_D$	**46%**
MTBF	**165 years**

SIL AC [10]	**SIL 3**

[7] For details see Appendix 3.

[8] This value corresponds to a PFH of 7.00E-09 1/h.

[9] The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[10] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

5 Using the FMEDA results

The following section describes how to apply the results of the FMEDA.

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The following results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

5.1 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) KFD2-RCI-(Ex)1 interface module considering a proof test coverage of 99% (see Appendix 1.1) and a mission time of 10 years. The failure rate data used in this calculation are displayed in section 4.3.1. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 1.

For SIL3 applications, the PFD_{AVG} value needs to be < 1.00E-03.

Table 1: PFD_{AVG} values KFD2-RCI-(Ex)1 interface module

Configuration	T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
KFD2-RCI-(Ex)1	PFD_{AVG} = 3.36E-05	PFD_{AVG} =6.39E-05	PFD_{AVG} =1.55E-04

Figure 2 shows the time dependent curve of PFD_{AVG}.

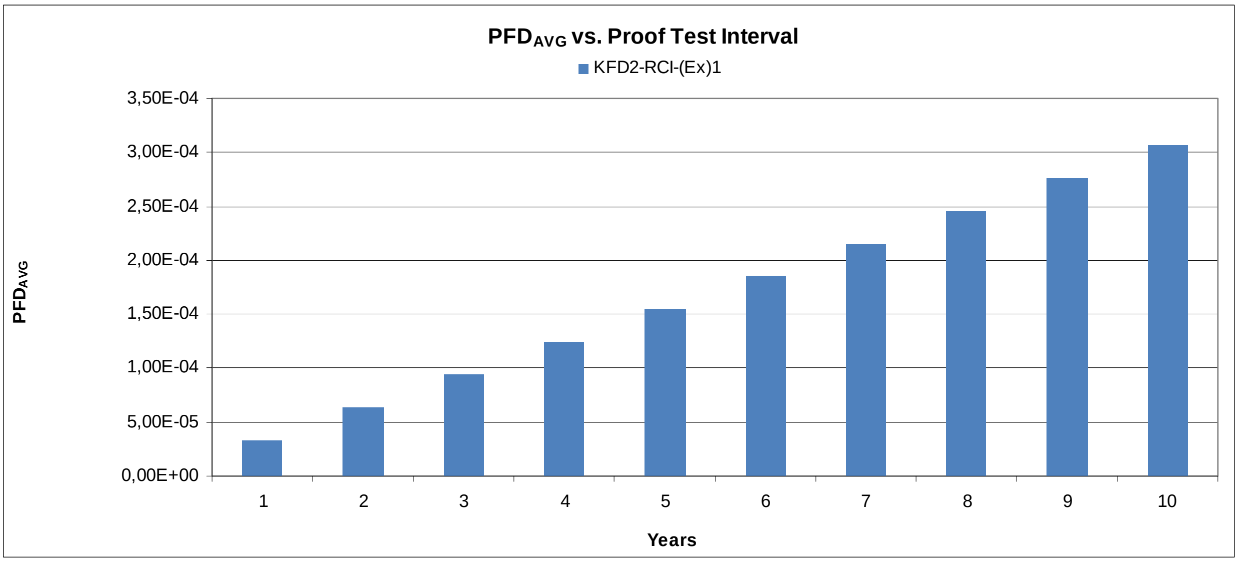

Figure 2: $PFD_{AVG}(t)$

6 Terms and Definitions

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 Modes, Effects, 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 twice the proof test frequency.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
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

7 Status of the document

7.1 Liability

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

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

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

7.2 Releases

Version History:	V1R0:	Review comments incorporated; November 4, 2009
	V0R1:	Initial version; October 19, 2009
Authors:	Stephan Aschenbrenner, Alexander Dimov	
Review:	V0R1:	Rachel Amkreutz (*exida*); November 3, 2009
		Harald Eschelbach (P+F); October 20, 2009
Release status:	Released to Pepperl+Fuchs GmbH	

7.3 Release Signatures

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

Rachel Amkreutz, Safety Engineer

Appendix 1: 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.

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

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 2.

Table 2 Suggested proof test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip
2	Force the KFD2-RCI-(Ex)1 interface module to go to the safe state and verify that the safe state is reached.
3	Verify that both internal current limitations are still working correctly.
4	Restore the loop to full operation.
5	Remove the bypass and otherwise restore normal operation

This test will detect more than 99% of possible “du” failures in the KFD2-RCI-(Ex)1 interface module.

Appendix 2: 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[11] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

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

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

[11] 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.

Appendix 3: Description of the considered profiles

Appendix 3.1: *exida* electronic database

Profile	Profile according to IEC 60654-1	Ambient Temperature [°C]		Temperature Cycle [°C / 365 days]
		Average (external)	Mean (inside box)	
1	B2	30	60	5
2	C3	25	30	25
3	C3	25	45	25

PROFILE 1:

Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.

PROFILE 2:

Low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings.

PROFILE 3:

General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings.