



Failure Modes, Effects and Diagnostic Analysis

Project:

Switch Amplifier KFA6-SR-2.3L

Customer:

Pepperl+Fuchs GmbH

Mannheim

Germany

Contract No.: P+F 05/12-35

Report No.: P+F 05/12-35 R026

Version V1, Revision R0, November 2006

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the switch amplifier KFA6-SR-2.3L.

Depending on the setting of switch S1/S2 the mode of operation can be configured. The results given in this report are meant for S1/S2 in position I which is considered to be the normal mode of operation and S1/S2 in position II which is considered to be the inverse mode of operation. The switch S3 shall always be set to position I (2 channel mode). The switches S4 and S5 can either be set to position I (for push-pull-output of sensor) or to position II (for single NPN or PNP output of sensor).

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 the basic failure rates from the Siemens standard SN 29500.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. 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.

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

The switch amplifier KFA6-SR-2.3L is considered to be a Type A¹ component with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

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

Table 1: IEC 61508 failure rates

| λ_{safe}^2 | $\lambda_{\text{dangerous}}$ | SFF |
|---------------------------|------------------------------|-----|
| 206 FIT | 42 FIT | 83% |

Table 2: PFD_{AVG} values

| T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|-------------------------------|-------------------------------|-------------------------------|
| PFD _{AVG} = 1,84E-04 | PFD _{AVG} = 3,69E-04 | PFD _{AVG} = 9,21E-04 |

¹ Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

² Note that the safe category includes failures that do not cause a spurious trip



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 fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to $1,00E-03$.

Because the Safe Failure Fraction (SFF) is above 60%, the architectural constraints requirements of table 2 of IEC 61508-2 for Type A subsystems with a Hardware Fault Tolerance (HFT) of 0 are also fulfilled.

A user of the switch amplifier KFA6-SR-2.3L 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 5.1 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508, Edition 2000. Note that these failures on their 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 switch amplifier KFA6-SR-2.3L (see Appendix 2).



Table of Contents

| | |
|--|----|
| Management summary | 2 |
| 1 Purpose and Scope | 5 |
| 2 Project management..... | 6 |
| 2.1 <i>exida</i> | 6 |
| 2.2 Roles of the parties involved..... | 6 |
| 2.3 Standards / Literature used..... | 6 |
| 2.4 Reference documents..... | 6 |
| 2.4.1 Documentation provided by the customer..... | 6 |
| 2.4.2 Documentation generated by <i>exida</i> | 6 |
| 3 Description of the analyzed module | 7 |
| 4 Failure Modes, Effects, and Diagnostics Analysis | 8 |
| 4.1 Description of the failure categories..... | 8 |
| 4.2 Methodology – FMEDA, Failure rates | 8 |
| 4.2.1 FMEDA..... | 8 |
| 4.2.2 Failure rates | 8 |
| 4.2.3 Assumptions..... | 9 |
| 5 Results of the assessment | 10 |
| 5.1 KFA6-SR-2.3L..... | 11 |
| 6 Terms and Definitions | 13 |
| 7 Status of the document..... | 14 |
| 7.1 Liability..... | 14 |
| 7.2 Releases | 14 |
| 7.3 Release Signatures..... | 14 |
| Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test .. | 14 |
| Appendix 1.1: Possible proof tests to detect dangerous undetected faults..... | 16 |
| Appendix 2: Impact of lifetime of critical components on the failure rate | 17 |

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 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 development process

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

Option 2 is an 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. In addition, this option includes an assessment of the proven-in-use documentation of the device 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 may help justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices when combined with plant specific proven-in-use records.

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 assessment shall be done according to option 1.

This document shall describe the results of hardware assessment carried out on the switch amplifier KFA6-SR-2.3L.

The information in this report can be used to evaluate whether the switch amplifier KFA6-SR-2.3L 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 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed 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 switch amplifier KFA6-SR-2.3L.

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

Pepperl+Fuchs GmbH contracted *exida* in September 2006 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] | ISBN: 0471133019 John Wiley & Sons | Electronic Components: Selection and Application Guidelines by Victor Meeldijk |
| [N3] | FMD-91, RAC 1991 | Failure Mode / Mechanism Distributions |
| [N4] | FMD-97, RAC 1997 | Failure Mode / Mechanism Distributions |
| [N5] | SN 29500 | Failure rates of components |
| [N6] | 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] | 510726.pdf | Circuit diagram "KFA6-SR-2.3L" Ind. 0 of 31.07.01 |
| [D2] | 107948_eng.pdf | Datasheet "Isolated switch amplifier KFA6-SR-2.3L" of 17.06.05 |

2.4.2 Documentation generated by *exida*

| | |
|------|--|
| [R1] | FMEDA V6.5.4 KFA6-SR-2.3L CONF1 V0R1.xls of 19.09.06 |
| [R2] | FMEDA V6.5.4 KFA6-SR-2.3L CONF2 V0R1.xls of 19.09.06 |

3 Description of the analyzed module

The isolated switch amplifier KFA6-SR-2.3L has two inputs and two relay outputs (change-over contact) and is usable either as a dual channel isolated amplifier or as two-point control (min/max control).

For safety applications only the dual channel setting shall be used.

The inputs are designed in such a way that the signals of sensors which have PNP or NPN output transistors, as well as push-pull outputs, can be processed. In the case of sensors with push-pull outputs the switches S4 or S5 have to be set to position I. For sensors with PNP or NPN output transistors, the switches S4 or S5 have to be set to position II. The operating behavior of the sensor can be selected: NO S1/S2 in position I; NC S1/S2 in position II.

The isolated switch amplifier KFA6-SR-2.3L is considered to be a Type A component with a hardware fault tolerance of 0.

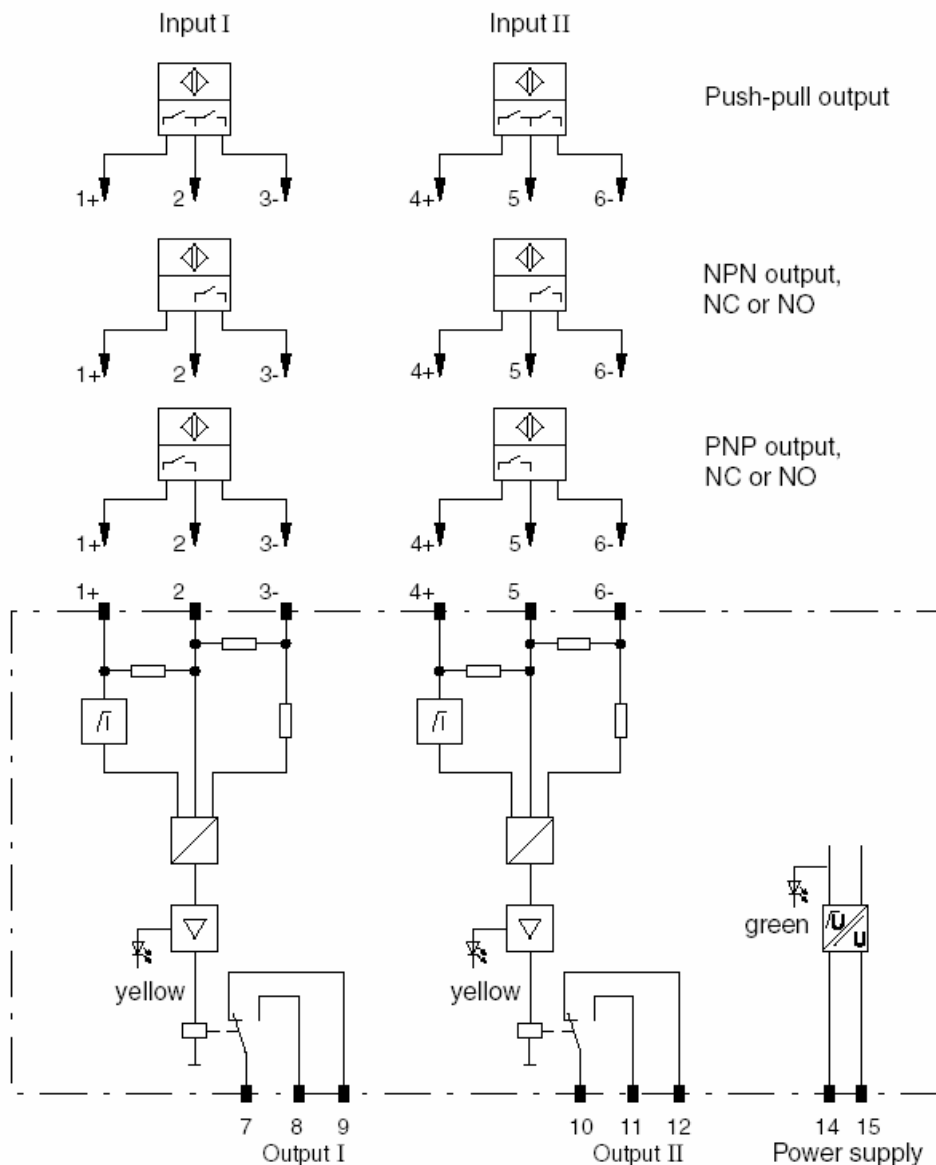


Figure 1: Block diagram of KFA6-SR-2.3L

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] and [R2].

4.1 Description of the failure categories

In order to judge the failure behavior of the switch amplifier KFA6-SR-2.3L, the following definitions for the failure of the product were considered.

| | |
|-----------------|---|
| Fail-Safe State | The fail-safe state is defined as the output being de-energized. |
| Fail Safe | Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process. |
| 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. |
| 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 “No Effect” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508, Edition 2000. In IEC 61508, Edition 2000 the “No Effect” failures are defined as safe 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 diagnostic 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 Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the switch amplifier KFA6-SR-2.3L.

- 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 two channels are not used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function.
- The time to restoration after a safe failure is 8 hours.
- All modules are operated in the low demand mode of operation.
- The MIN/MAX setting is not used for safety related applications.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-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 40°C. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

5 Results of the assessment

exida did the FMEDAs together with Pepperl+Fuchs.

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

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

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

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

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 FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.

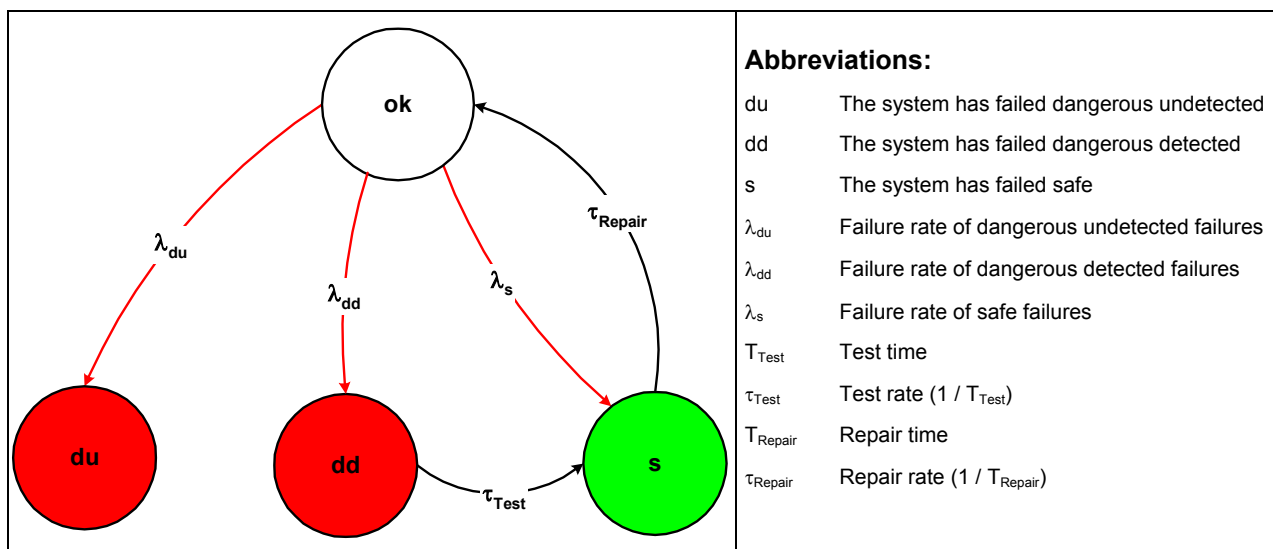


Figure 2: Markov model for a 1oo1D structure

5.1 KFA6-SR-2.3L

The FMEDA carried out on KFA6-SR-2.3L leads under the assumptions described in sections 0 and 5 to the following failure rates:

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

$$\lambda_{su} = 1,21E-07 \text{ 1/h}$$

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

$$\lambda_{du} = 4,21E-08 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 8,53E-08 \text{ 1/h}$$

$$\lambda_{total} = 2,48E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 3,60E-08 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 402 \text{ years}$$

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

| λ_{safe}^3 | $\lambda_{dangerous}$ | SFF |
|--------------------|-----------------------|--------|
| 206 FIT | 42 FIT | 83,05% |

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

| T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|------------------------|------------------------|------------------------|
| $PFD_{AVG} = 1,84E-04$ | $PFD_{AVG} = 3,69E-04$ | $PFD_{AVG} = 9,21E-04$ |

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 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} .

³ Note that the safe category includes failures that do not cause a spurious trip

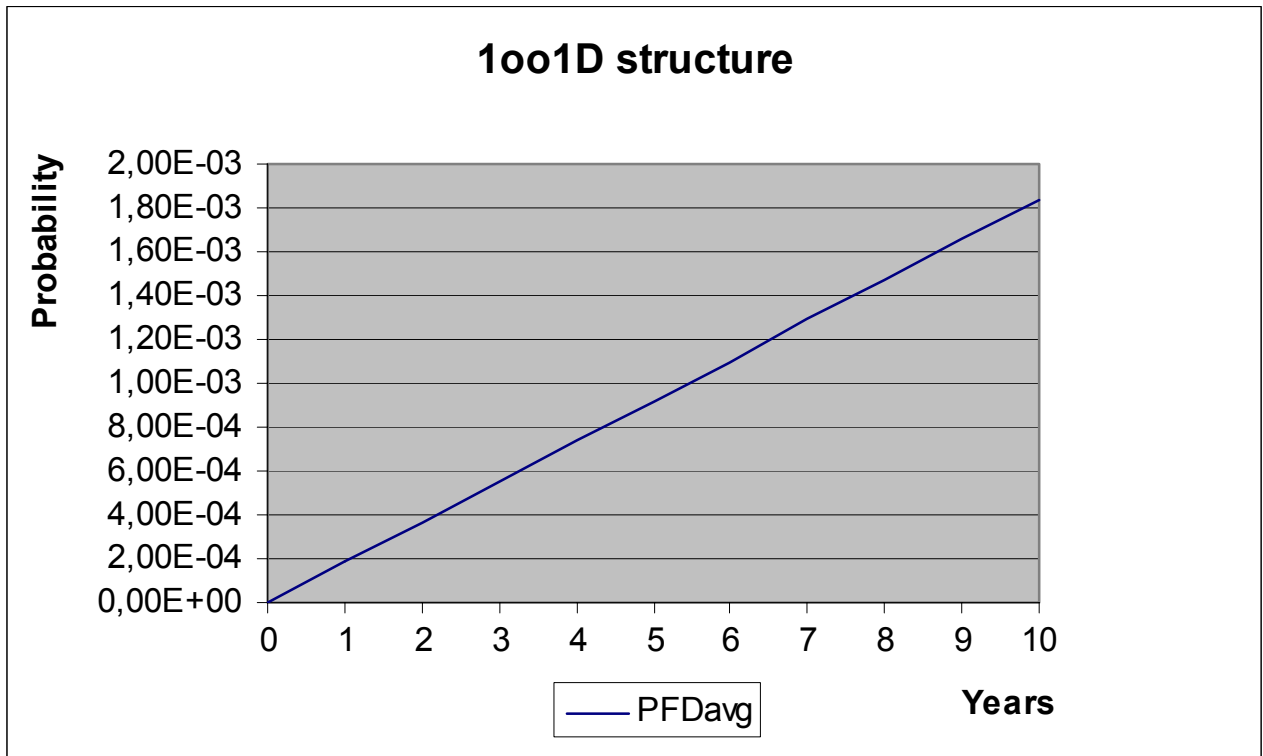


Figure 3: PFD_{AVG}(t)

6 Terms and Definitions

| | |
|------------------|---|
| FIT | Failure In Time (1×10^{-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 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 A component | "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2. |
| T[Proof] | Proof Test Interval |

7 Status of the document

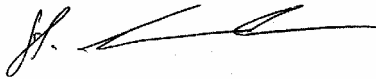
7.1 Liability

exida prepares 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.

7.2 Releases

Version: V1
Revision: R0
Version History: V0, R1: Initial version, November 3, 2006
V1, R0: Review comments incorporated, November 23, 2006
Authors: Stephan Aschenbrenner
Review: V0, R1: Harald Eschelbach (P+F), November 6, 2006
Rudolf Chalupa (*exida*), November 22, 2006
Release status: Released to Pepperl+Fuchs GmbH

7.3 Release Signatures

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

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

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

Dipl.-Ing. (Univ.) Rainer Faller, Principal Partner

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.

Table 3 shows an importance analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing.

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

Table 3: KFA6-SR-2.3L

| Component | % of total λ_{du} | Detection through |
|--------------|---------------------------|--|
| K1.1A | 47,53% | 100% functional test with monitoring of the expected output signal |
| L2.1 | 9,51% | 100% functional test with monitoring of the expected output signal |
| C22.1 | 7,13% | 100% functional test with monitoring of the expected output signal |
| IC5:A | 4,75% | 100% functional test with monitoring of the expected output signal |
| P5.1 | 3,92% | 100% functional test with monitoring of the expected output signal |
| IC3:A, IC3:C | 3,56% | 100% functional test with monitoring of the expected output signal |
| P2.1 | 2,85% | 100% functional test with monitoring of the expected output signal |
| P3.1 | 2,85% | 100% functional test with monitoring of the expected output signal |
| IC9 | 2,38% | 100% functional test with monitoring of the expected output signal |
| C20.1 | 2,38% | 100% functional test with monitoring of the expected output signal |

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

A possible proof test could consist of the following steps, as described in Table 4.

Table 4 Steps for Proof Test

| Step | Action |
|------|--|
| 1 | Take appropriate action to avoid a false trip |
| 2 | Provide a control signal to the switch amplifier KFA6-SR-2.3L to energize / de-energize the output and verify that the output is energized / de-energized. |
| 3 | Restore the loop to full operation |
| 4 | Restore normal operation |

This test will detect more than 90% of possible “du” failures in the switch amplifier KFA6-SR-2.3L.

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 lifetime⁴ of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore 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, electrolytic capacitors can be very sensitive).

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

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

Table 5 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 5: Useful lifetime of electrolytic capacitors contributing to λ_{du}

| Type | Name | Useful life at 40°C |
|---|-------|---------------------------------|
| Capacitor (electrolytic) - Aluminum electrolytic, solid electrolyte | C22.1 | Appr. 90.000 Hours ⁵ |
| Relay | K1.1A | 1.000.000 switching cycles |

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

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

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

⁴ 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.

⁵ The operating temperature has a direct impact on this time. Therefore 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.