Failure Modes, Effects and Diagnostic Analysis

Project:
Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0

Customer:
Hans Turck GmbH & Co. KG
Mühlheim
Germany

Contract No.: TURCK 04/07-14
Report No.: TURCK 04/07-14 R002
Version V3, Revision R0, February 2014
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0.

Table 1 gives an overview of the different versions that belong to the considered devices.

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

Table 1: Version overview

Type	Description[1]	Parts List / Circuit Diagram
IM1-12Ex-R IM1-12-R	1 input / 2 relay outputs	12296307 of 07.10.04 / 12296307 of 28.09.04
IM1-12Ex-T IM1-12-T	1 input / 2 transistor outputs	12296309 of 07.10.04 / 12296309 of 28.09.04
IM1-22Ex-R IM1-22-R	2 inputs / 2 relay outputs	12296301 of 07.10.04 / 12296301 of 28.09.04
IM1-22Ex-T IM1-22-T	2 inputs / 2 transistor outputs	12296303 of 13.08.04 / 12296303 of 28.09.04
IM1-121Ex-R	1 input / 2 relay outputs (one used as error message output)	12296310 of 07.10.04 / 12296310 of 28.09.04
IM1-121Ex-T	1 input / 2 transistor outputs (one used as error message output)	12296312 of 25.01.05 / 12296312 of 28.09.04
MK13-R-Ex0	1 input / 1 relay output	12296101 of 18.10.04 / 12296100 of 07.10.04

The failure rates used in this analysis are the 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, i.e. they should be better than or equal to 1,00E-03.

The Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0 are considered to be Type A[2] components with a hardware fault tolerance of 0.

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

The following 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.

---

[1] The two channels on a redundant board shall not be used to increase the hardware fault tolerance needed for a higher SIL as they contain common components.

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

Table 2: Summary for MK13-R-Ex0 – Failure rates

λ_{safe}	$\lambda_{dangerous}$	SFF
288 FIT	110 FIT	72%

Table 3: Summary for MK13-R-Ex0 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 4,80E-04	PFD_{AVG} = 2,40E-03	PFD_{AVG} = 4,79E-03

Table 4: Summary for IM1-*-R – Failure rates**

λ_{safe}	$\lambda_{dangerous}$	SFF
299 FIT	110 FIT	73%

Table 5: Summary for IM1-*-R – PFD_{AVG} values**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 4,80E-04	PFD_{AVG} = 2,40E-03	PFD_{AVG} = 4,79E-03

Table 6: Summary for IM1-*-T – Failure rates**

λ_{safe}	$\lambda_{dangerous}$	SFF
267 FIT	85 FIT	75%

Table 7: Summary for IM1-*-T – PFD_{AVG} values**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,72E-04	PFD_{AVG} = 1,86E-03	PFD_{AVG} = 3,71E-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.

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

A user of the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0 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 sections 5.1 to 5.3 along with all assumptions.

The failure rates are valid for the useful life of the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0, which is estimated to be between 8 and 12 years (see Appendix 2).

It is important to realize that the “no effect” 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.

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 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}).

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 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 1.

This document shall describe the results of the hardware assessment carried out on the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0.

It shall be assessed whether the described 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.

It **does not** consider any calculations necessary for proving intrinsic safety.

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 the 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

Werner Turck GmbH & Co. KG	Manufacturer of the considered Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0.
exida.com	Performed the hardware assessment according to option 1 (see section 1).

Werner Turck GmbH & Co. KG contracted *exida.com* in August 2004 with the FMEDA and PFD_{AVG} calculation of the above mentioned device.

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]	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]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	im1_22Ex0_R.pdf	Description of the working principle
[D2]	im1_22Ex0_T.pdf	Description of the working principle
[D3]	D201010.pdf	Data sheet Isolating switching amplifier IM1-12Ex-R 1-channel
[D4]	D201006.pdf	Data sheet Isolating switching amplifier IM1-12Ex-T 1-channel
[D5]	D201014.pdf	Data sheet Isolating switching amplifier IM1-22Ex-R 2-channel

[D6]	D201015.pdf	Data sheet Isolating switching amplifier IM1-22Ex-T 2-channel
[D7]	D201021.pdf	Data sheet Isolating switching amplifier IM1-121Ex-R 1-channel
[D8]	d201030.pdf	Data sheet Isolating switching amplifier IM1-121Ex-T 1-channel
[D9]	MK13_R_Ex0SL.pdf	Parts list 12296101 of 18.10.04
[D10]	MK13_R_Ex0Sch.pdf	Circuit diagram 12296100 of 07.10.04
[D11]	IM1_12ExRSL.pdf	Parts list 12296307 of 07.10.04
[D12]	IM1_12ExRSch.pdf	Circuit diagram 12296307 of 28.09.04
[D13]	IM1_12ExTSL.pdf	Parts list 12296309 of 07.10.04
[D14]	IM1_12ExTSch.pdf	Circuit diagram 12296309 of 28.09.04
[D15]	IM1_22ExRSL.pdf	Parts list 12296301 of 07.10.04
[D16]	IM1_22ExRSch.pdf	Circuit diagram 12296301 of 28.09.04
[D17]	IM1_22ExTSL.pdf	Parts list 12296303 of 13.08.04
[D18]	IM1_22ExTSch.pdf	Circuit diagram 12296303 of 28.09.04
[D19]	IM1_121Ex_R.pdf	Parts list 12296310 of 07.10.04
[D20]	IM1_121_ExRSch.pdf	Circuit diagram 12296310 of 28.09.04
[D21]	IM1_121Ex_T.pdf	Parts list 12296312 of 25.01.05
[D22]	IM1_121_TSch.pdf	Circuit diagram 12296312 of 28.09.04
[D23]	Manual.pdf	Manual of the ASIC
[D24]	SchaltungASIC.pdf	Circuit diagram of the ASIC
[D25]	LayoutASIC.pdf	Layout of the ASIC

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA V6 MK13-R-Ex0 V1 R1.0.xls of 11.03.05
[R2]	FMEDA V6 IM1-12Ex-R V1 R1.0.xls of 11.03.05
[R3]	FMEDA V6 IM1-12Ex-T V1 R1.0.xls of 11.03.05
[R4]	FMEDA V6 ASIC 5V regulator V0 R1.0.xls of 08.03.05
[R5]	FMEDA V6 ASIC 8V regulator V0 R1.0.xls of 07.03.05
[R6]	FMEDA V6 ASIC error signal path V0 R1.0.xls of 08.03.05
[R7]	FMEDA V6 ASIC NAMUR signal path detailed V0 R1.0.xls of 08.03.05
[R8]	FMEDA V6 ASIC PU block V0 R1.0.xls of 07.03.05
[R9]	FMEDA V6 ASIC remaining parts V0 R1.0.xls of 08.03.05
[R10]	FMEDA V6 ASIC partly detailed V0 R1.0.xls of 08.03.05
[R11]	Besprechung ASIC 07.03.05.txt

3 Description of the analyzed modules

The Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0 consist of intrinsically safe input circuits.

They can be connected to sensors according to EN 60947-5-6 (NAMUR), variable resistors or potential-free contacts.

The output circuits, galvanically isolated from the input circuits, consist of either relay outputs or transistor outputs.

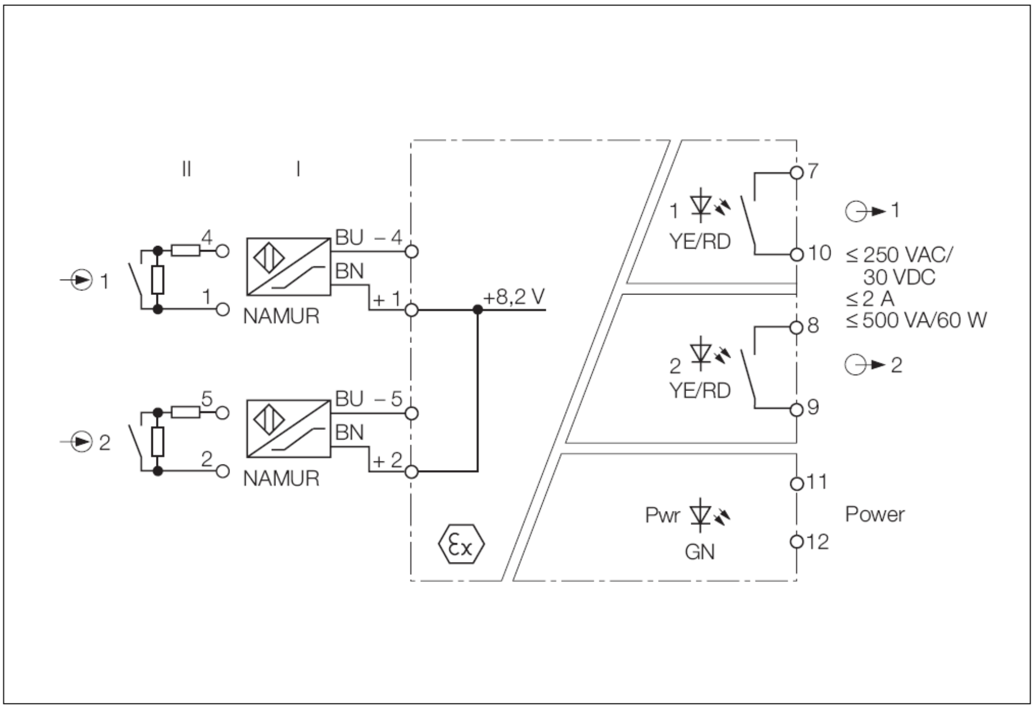


Figure 1: Block diagram of the Isolating Switching Amplifier IM1-22Ex-R

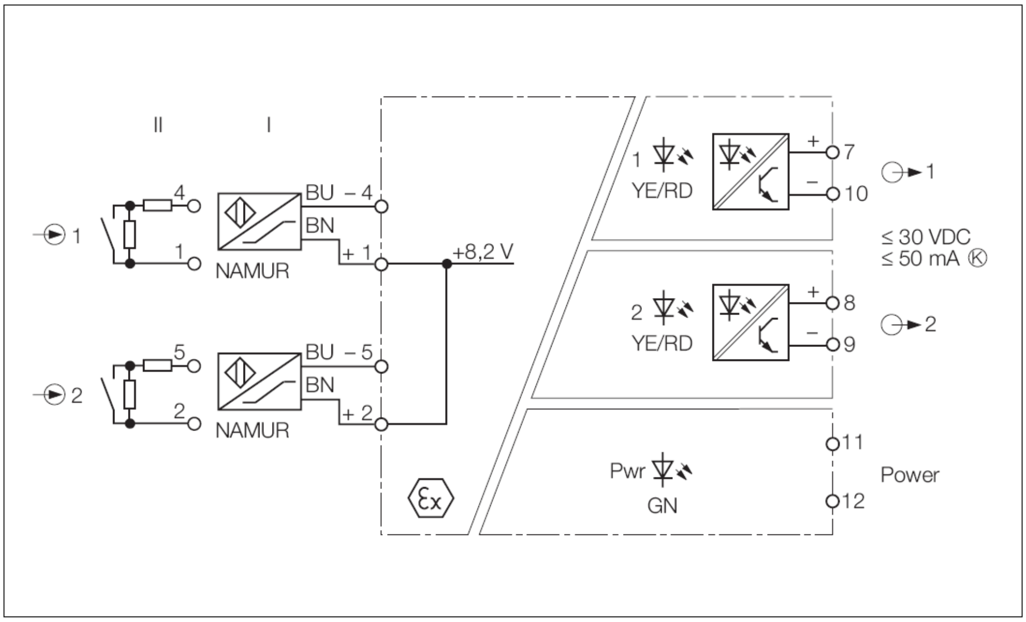


Figure 2: Block diagram of the Isolating Switching Amplifier IM1-22Ex-T

The block diagrams above show the working principal of all considered versions with the exception that the presented block diagrams have two input and two output channels. The differences between the versions are described in Table 1.

The Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0 are considered to be Type A components with a hardware fault tolerance of 0.

Although the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0 are designed with a semi-custom ASIC 724 from ZETEX (see [D23]) they are still considered to be Type A components. The reason is the low complexity, the full analyzability of the used ASIC and the fact that the ASIC does not contain hidden state information such as internal digital registers (see [D24]). It only consists of 103 transistors, 908 resistors and 7 junction capacitors, which can individually be connected (see [D25]).

exida.com did a detailed analysis of the ASIC based on the individual failure modes of the internal transistors, resistors and capacitors (see [R4] to [R11]). Possible dependencies were taken into account with a common cause factor of 25%. The failure rate from the Siemens standard SN 29500 for a bipolar ECL ASIC with 50 to 5000 transistors was multiplied with a safety factor of 2. The resulting 100 FIT were used in the overall analysis for the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Werner Turck GmbH & Co. KG and is documented in [R2] to [R10]. Failures 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 Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0, 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. This corresponds to an input signal of less than 1.4mA (NAMUR signal).
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).
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. In IEC 61508 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 in consideration.

A FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is a 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 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The time to restoration after a safe failure is 8 hours.
- All modules are operated in the low demand mode of operation.
- External power supply failure rates are not included.
- Only one input and one output are part of the safety function
- 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 on a redundant board are not used to increase the hardware fault tolerance needed for a higher SIL as they contain common components.
- 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.

5 Results of the assessment

exida.com did the FMEDAs together with Werner Turck GmbH & Co. KG.

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:

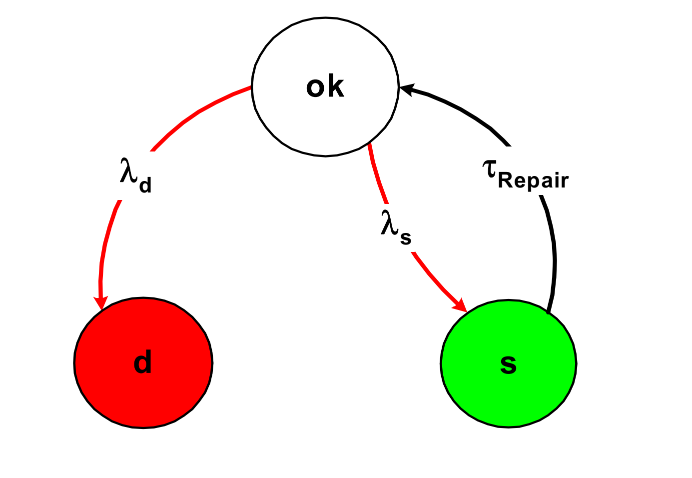
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect}$.

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

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 1oo1 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:

d	The system has failed dangerous
s	The system has failed safe
λ_d	Failure rate of dangerous failures
λ_s	Failure rate of safe failures
T_{Repair}	Repair time
τ_{Repair}	Repair rate ($1 / T_{Repair}$)

Figure 3: Markov model for a 1oo1 structure

5.1 Isolating Switching Amplifier MK13-R-Ex0

The FMEDA carried out on the Isolating Switching Amplifier MK13-R-Ex0 leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 1,66E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 1,10E-07 1/h

$\lambda_{no\ effect}$ = 1,22E-07 1/h

λ_{total} = 3,98E-07 1/h

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

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 279 years

Under the assumptions described in section 5 and the definitions given in section 4.1 the following table shows the failure rates according to IEC 61508:

λ_{safe}	$\lambda_{dangerous}$	**SFF**
288 FIT	110 FIT	72,44%

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

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD$_{AVG}$ = 4,80E-04	**PFD$_{AVG}$ = 2,40E-03**	**PFD$_{AVG}$ = 4,79E-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 and table 3.1 of ANSI/ISA–84.01–1996 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 4 shows the time dependent curve of PFD$_{AVG}$.

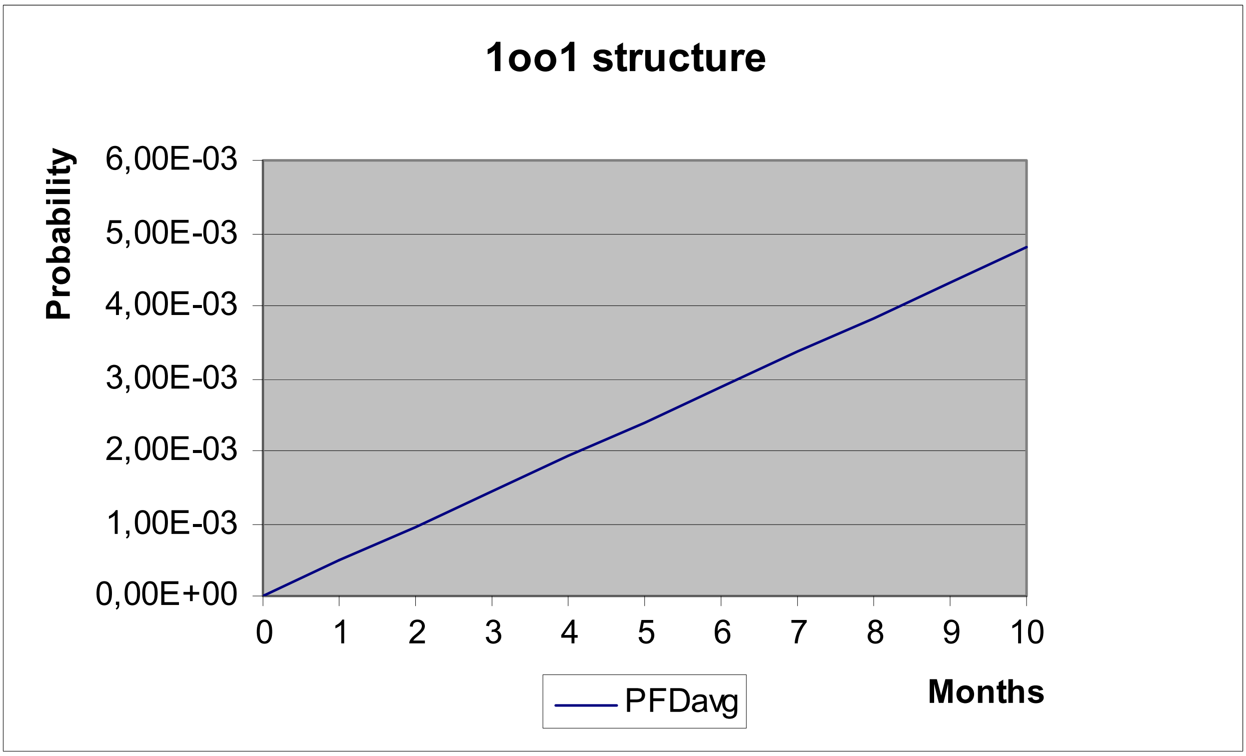


Figure 4: $PFD_{AVG}(t)$

5.2 Isolating Switching Amplifier IM1-***-R

The FMEDA carried out on the Isolating Switching Amplifier IM1-***-R leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 1,72E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 1,10E-07 1/h

$\lambda_{no\ effect}$ = 1,27E-07 1/h

λ_{total} = 4,09E-07 1/h

$\lambda_{not\ part}$ = 1,10E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 272 years

Under the assumptions described in section 5 and the definitions given in section 4.1 the following table shows the failure rates according to IEC 61508:

λ_{safe}	$\lambda_{dangerous}$	SFF
299 FIT	110 FIT	73,15%

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

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 4,80E-04	**PFD_{AVG} = 2,40E-03**	**PFD_{AVG} = 4,79E-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 and table 3.1 of ANSI/ISA–84.01–1996 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 5 shows the time dependent curve of PFD_{AVG}.

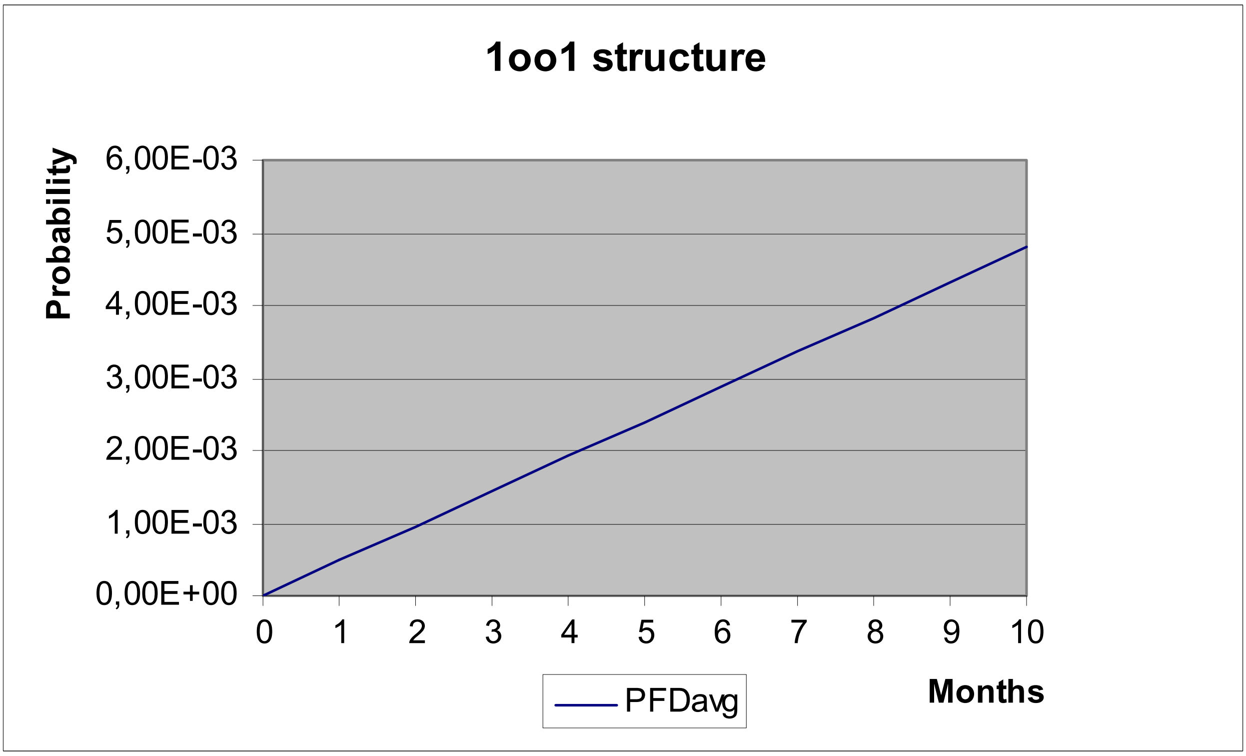


Figure 5: $PFD_{AVG}(t)$

5.3 Isolating Switching Amplifier IM1-***-T

The FMEDA carried out on the Isolating Switching Amplifier IM1-***-T leads under the assumptions described in sections 4.2.3 and 5 to the following failure rates:

λ_{sd} = 0,00E-00 1/h

λ_{su} = 1,44E-07 1/h

λ_{dd} = 0,00E-00 1/h

λ_{du} = 8,49E-08 1/h

$\lambda_{no\ effect}$ = 1,23E-07 1/h

λ_{total} = 3,52E-07 1/h

$\lambda_{not\ part}$ = 1,10E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 314 years

Under the assumptions described in section 5 and the definitions given in section 4.1 the following table shows the failure rates according to IEC 61508:

λ_{safe}	$\lambda_{dangerous}$	SFF
267 FIT	85 FIT	75,89%

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

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,72E-04	**PFD_{AVG} = 1,86E-03**	**PFD_{AVG} = 3,71E-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 and table 3.1 of ANSI/ISA–84.01–1996 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 6 shows the time dependent curve of PFD_{AVG}.

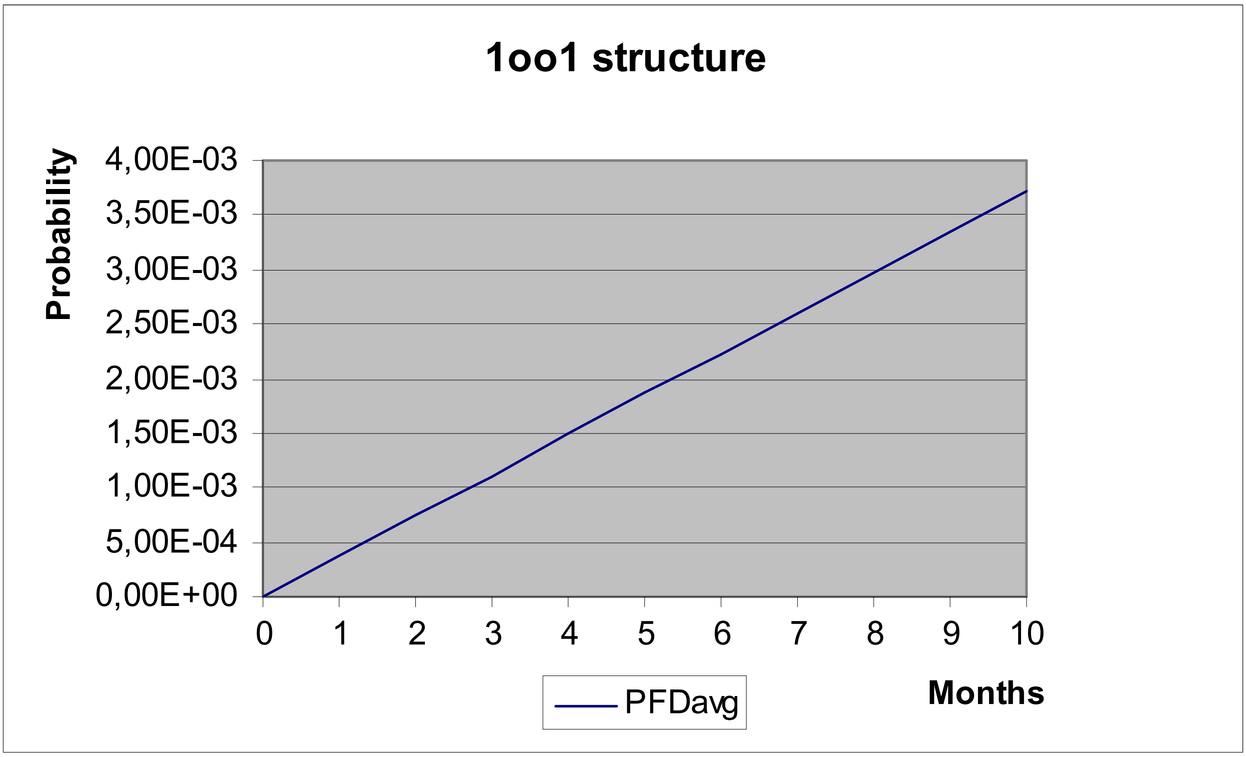


Figure 6: $PFD_{AVG}(t)$

6 Terms and Definitions

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 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.

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:	V3R0:	IM1-12-R, IM1-12-T and IM1-22-T added; February 21, 2014
	V2R0:	IM1-22-R added; February 8, 2013
	V1, R1.0:	External review comments integrated; April 14, 2005
	V0, R2.0:	Internal review comments integrated; March 31, 2005
	V0, R1.0:	Initial version; March 11, 2005
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida.com); March 28, 2005
	V0, R2.0:	Frank Seeler (Werner Turck GmbH & Co. KG); April 13, 2005
Release status:	Released to Werner Turck GmbH & Co. KG	

7.3 Release Signatures

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

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 8, Table 9 and Table 10 show an importance analysis of the most critical dangerous undetected faults and indicate 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 8: Importance Analysis of dangerous undetected faults of MK13-R-Ex0

Component	% of total λ_{du}	Detection through
IC3	60,90%	100% functional test with monitoring of the expected output signal
K1	22,78%	100% functional test with monitoring of the expected output signal
T101	10,03%	100% functional test with monitoring of the expected output signal
IC1	4,10%	100% functional test with monitoring of the expected output signal
D101	0,91%	100% functional test with monitoring of the expected output signal
C101	0,91%	100% functional test with monitoring of the expected output signal
X4	0,18%	100% functional test with monitoring of the expected output signal
R101	0,18%	100% functional test with monitoring of the expected output signal

Table 9: Importance Analysis of dangerous undetected faults of IM1-*-R**

Component	% of total λ_{du}	Detection through
IC4	60,90%	100% functional test with monitoring of the expected output signal
K1	22,78%	100% functional test with monitoring of the expected output signal
T102	10,03%	100% functional test with monitoring of the expected output signal
IC1	4,10%	100% functional test with monitoring of the expected output signal
D100	0,91%	100% functional test with monitoring of the expected output signal
C100	0,91%	100% functional test with monitoring of the expected output signal
X1	0,18%	100% functional test with monitoring of the expected output signal
R100	0,18%	100% functional test with monitoring of the expected output signal

Table 10: Importance Analysis of dangerous undetected faults of IM1-*-T**

Component	% of total λ_{du}	Detection through
IC4	78,73%	100% functional test with monitoring of the expected output signal
T202	12,96%	100% functional test with monitoring of the expected output signal
IC2	5,30%	100% functional test with monitoring of the expected output signal
D100	1,18%	100% functional test with monitoring of the expected output signal
C100	1,18%	100% functional test with monitoring of the expected output signal
X1	0,24%	100% functional test with monitoring of the expected output signal
R100	0,24%	100% functional test with monitoring of the expected output signal
D203	0,18%	100% functional test with monitoring of the expected output signal

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

The proof test consists of the following steps, as described in Table 11.

Table 11 Steps for Proof Test

Step	Action
1	Take appropriate action to avoid a false trip
2	Provide NAMUR control signals to the Isolating Switching Amplifier to open/close the output and verify that the output is open/closed.
3	Restore the loop to full operation
4	Restore normal operation

This test will detect more than 90% of possible “du” failures of the Isolating Switching Amplifier.

Appendix 2: Impact of lifetime of critical components on the failure rate

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) 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 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.

The circuits of the Isolating Switching Amplifiers IM1-**(Ex)-* and MK13-R-Ex0 do not contain any electrolytic capacitors or other components 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. According to section 7.4.7.4 note 3 of IEC 61508-2 experience has shown that the useful lifetime often lies within a range of 8 to 12 years.