Failure Modes, Effects and Diagnostic Analysis

Project:

NAMUR Switching Amplifiers
PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P

Customer:

PHOENIX CONTACT GmbH & Co. KG
Blomberg
Germany

Contract No.: Phoenix Contact 05/10-12
Report No.: Phoenix Contact 05/10-12 R002
Version V1, Revision R1.1, March 2006
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE (relay output) and PI-Ex-NAM/TO-P (transistor output).

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.

For safety applications only the described outputs have been considered. All other possible output variants or electronics are not covered by this report.

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 NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P are considered to be Type A[1] components with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 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 tables show how the above stated requirements are fulfilled.

Table 1: Summary PI-Ex-NAM/RNO-NE – Failure rates

λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF	DC_S [3]	DC_D [3]
6 FIT	194 FIT	8 FIT	74 FIT	73%	3%	9%

Table 2: Summary PI-Ex-NAM/RNO-NE – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,25E-04	PFD_{AVG} = 1,62E-03	PFD_{AVG} = 3,25E-03

Table 3: Summary PI-Ex-NAM/TO-P – Failure rates

λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF	DC_S [3]	DC_D [3]
6 FIT	183 FIT	8 FIT	37 FIT	84%	3%	17%

Table 4: Summary PI-Ex-NAM/TO-P – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,62E-04	PFD_{AVG} = 8,08E-04	PFD_{AVG} = 1,62E-03

[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 SU category includes failures that do not cause a spurious trip

[3] DC means the diagnostic coverage (safe or dangerous).

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

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.

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.

A user of the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P 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 and 5.2 along with all assumptions.

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

The failure rates are valid for the useful life of the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P, which is estimated to be between 8 to 12 years (see Appendix 2).

Table of Contents

Management summary 2

1 Purpose and Scope 5

2 Project management 6

2.1 *exida.com* 6

2.2 Roles of the parties involved 6

2.3 Standards / Literature used 6

2.4 Reference documents 7

2.4.1 Documentation provided by the customer 7

2.4.2 Documentation generated by *exida.com* 7

3 Description of the analyzed modules 8

3.1 NAMUR switching amplifier PI-Ex-NAM/RNO-NE 8

3.2 NAMUR switching amplifier PI-Ex-NAM/TO-P 9

4 Failure Modes, Effects, and Diagnostic Analysis 10

4.1 Description of the failure categories 10

4.2 Methodology – FMEDA, Failure rates 10

4.2.1 FMEDA 10

4.2.2 Failure rates 11

4.2.3 Assumptions 11

5 Results of the assessment 12

5.1 NAMUR switching amplifier PI-Ex-NAM/RNO-NE 13

5.2 NAMUR switching amplifier PI-Ex-NAM/TO-P 15

6 Terms and Definitions 17

7 Status of the document 18

7.1 Liability 18

7.2 Releases 18

7.3 Release Signatures 18

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test 18

Appendix 1.1: Possible proof tests to detect dangerous undetected faults 21

Appendix 2: Impact of lifetime of critical components on the failure rate 22

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 NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P.

It shall be assessed whether the described NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P 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 150 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

PHOENIX CONTACT GmbH & Co. KG	Manufacturer of the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P.
exida.com	Performed the hardware assessment according to option 1 (see section 1).

PHOENIX CONTACT GmbH & Co. KG contracted *exida.com* in November 2005 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]	9005691.pdf	Data sheet „PI-Ex-NAM/RNO-NE" TNR 9005691-01 / 02.2003
[D2]	9019217.pdf	Data sheet „PI-Ex-NAM/TO-P" TNR 9019217-00 / 04.2004
[D3]	B9018869	Circuit diagram "BT.PI-Ex-NAM/TO-P" revision 02 of 09.03.05
[D4]	9772794	Circuit diagram "BT. PI-EX-NAM/RNO-NE" revision 05 of 13.09.04
[D5]	PI_EX_NAM_RNO_NE_N_LF_231105.xls of 23.11.05	FMEDA PI-Ex-NAM/RNO-NE – normal mode of operation
[D6]	PI_EX_NAM_RNO_NE_I_LF_231105.xls of 23.11.05	FMEDA PI-Ex-NAM/RNO-NE – inverted mode of operation
[D7]	PI_EX_NAM_TO_P_N_LF_231105.xls of 23.11.05	FMEDA PI-Ex-NAM/TO-P – normal mode of operation
[D8]	PI_EX_NAM_TO_P_I_LF_231105.xls of 23.11.05	FMEDA PI-Ex-NAM/TO-P – inverted mode of operation
[D9]	Antwort AW Review FMEDA.msg of 29.11.05	Email about the contact force of the relay

2.4.2 Documentation generated by *exida.com*

[R1]	PI_EX_NAM_RNO_NE_I_LF__SAreview.xls of 16.11.05
[R2]	PI_EX_NAM_RNO_NE_N_LF_291105__SA.xls of 29.11.05
[R3]	PI_EX_NAM_RNO_NE_I_LF_291105__SA.xls of 29.11.05
[R4]	PI_EX_NAM_TO_P_N_LF_231105__SA.xls of 28.11.05
[R5]	PI_EX_NAM_TO_P_I_LF_231105__SA.xls of 28.11.05

3 Description of the analyzed modules

3.1 NAMUR switching amplifier PI-Ex-NAM/RNO-NE

The NAMUR switching amplifier PI-Ex-NAM/RNO-NE is designed for the operation of proximity sensors and switches in hazardous areas. The signals coming from the hazardous area are transmitted via a relay output to the safety controller installed in the safe area.

The PI-Ex-NAM/RNO-NE has on the output side an N/O contact.

The module has a line fault recognition, which also can be switched on or off via a DIP switch depending on the application. In the event of line errors being detected or supply voltage failure, the output switches to power off mode, i.e. output contact open.

Using a DIP switch on the front of the housing the user can choose between standard and inverse switching behavior.

The NAMUR switching amplifier PI-Ex-NAM/RNO-NE is considered to be a Type A component with a hardware fault tolerance of 0.

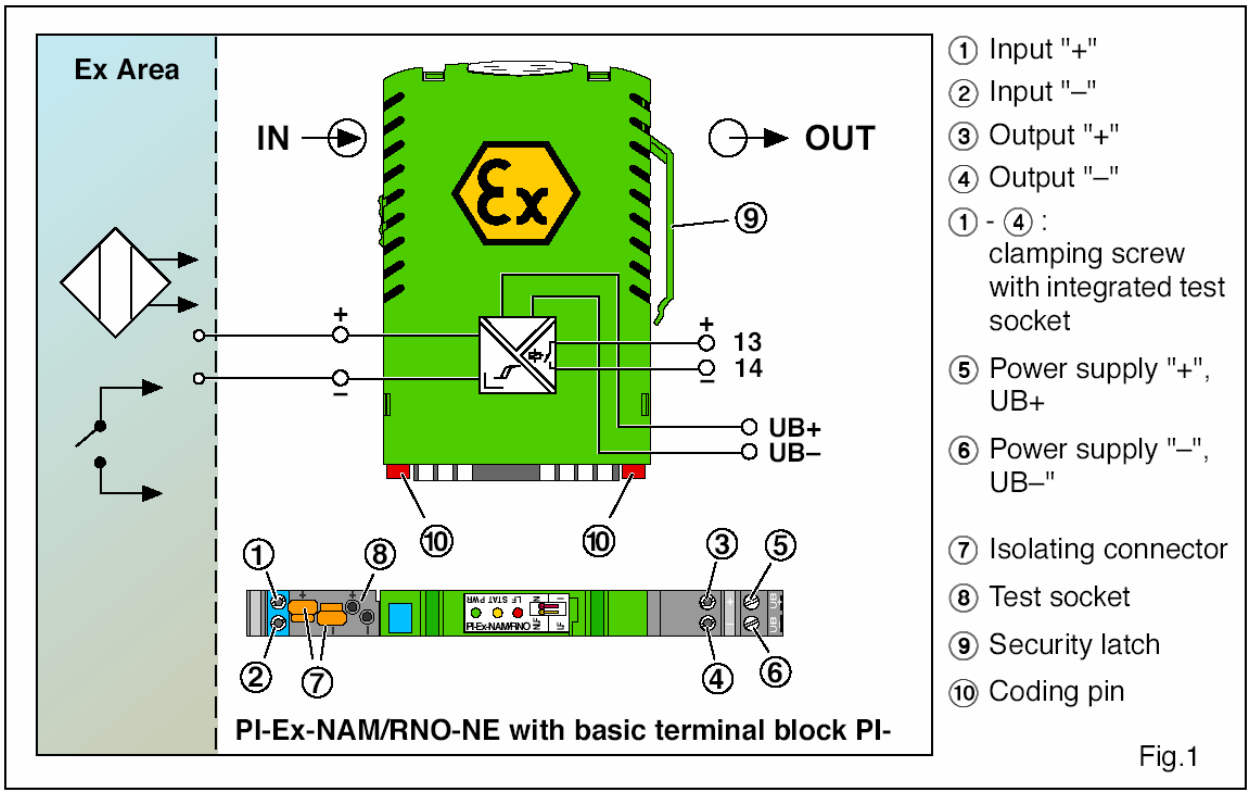


Figure 1: Block diagram

3.2 NAMUR switching amplifier PI-Ex-NAM/TO-P

The NAMUR switching amplifier PI-Ex-NAM/TO-P is designed for the operation of proximity sensors and switches in hazardous areas. The electrically isolated signals coming from the Ex area are transmitted via a transistor to a safety control system installed in the safe area.

At the output side, the PI-Ex-NAM/TO-P has a passive short-circuit-proof NPN transistor that is electrically isolated from the sensor and supply side.

The module has a line fault detection, which also can be switched on or off via a DIP switch depending on the application. If line faults or supply voltage failures are detected the module switches to a de-energized state, i.e. 0 V on the output side.

Using a DIP switch on the front of the housing the user can choose between standard and inverse switching behavior.

The NAMUR switching amplifier PI-Ex-NAM/TO-P is considered to be a Type A component with a hardware fault tolerance of 0.

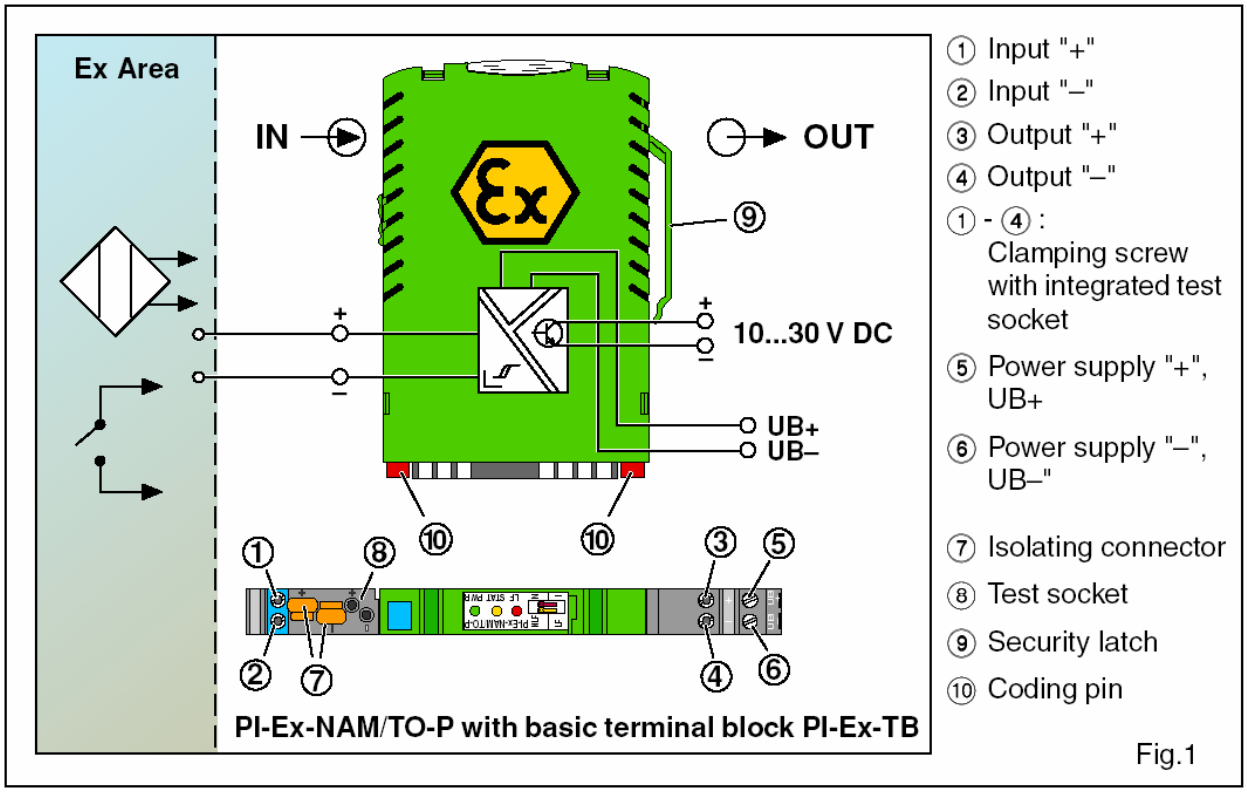


Figure 2: Block diagram

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by PHOENIX CONTACT GmbH & Co. KG and reviewed by *exida.com*. The results are documented in [D5] to [D8] and [R1] to [R5].

4.1 Description of the failure categories

In order to judge the failure behavior of the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P, 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 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 lead breakage or short circuit detection (These failures are converted to the selected 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.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics. For the calculation of the SFF it is treated like a safe undetected failure.
Not part	Failures of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The “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.

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 NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P.

- 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 time to restoration after a safe failure is 8 hours.
- All modules are operated in the low demand mode of operation.
- Lead breakage and short circuit detection are activated.
- External power supply failure rates are not included.
- 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 40ºC. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C 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.

5 Results of the assessment

exida.com reviewed the FMEDAs prepared by PHOENIX CONTACT 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:

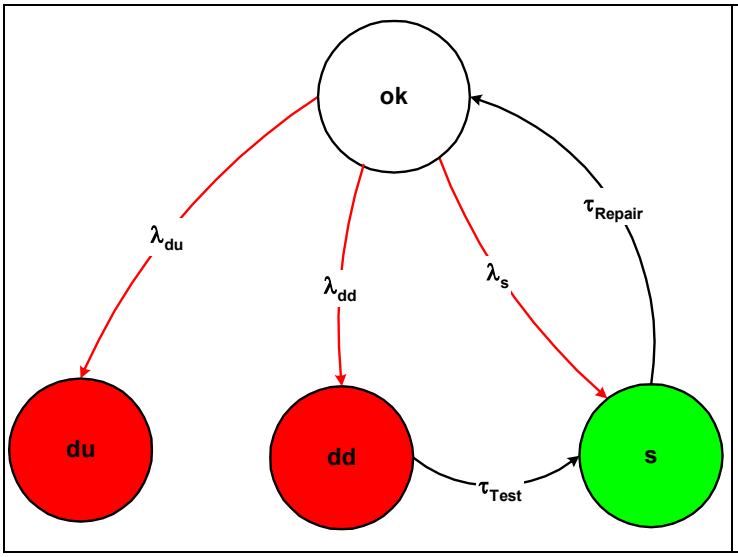
$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect} + \lambda_{annunciation}$

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

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 3: Markov model for a 1oo1D structure

5.1 NAMUR switching amplifier PI-Ex-NAM/RNO-NE

The FMEDA carried out on the NAMUR switching amplifier PI-Ex-NAM/RNO-NE leads under the assumptions described in section 4.2.3 and 5 to the following failure rates:

λ_{sd} = 5,54E-09 1/h (normal mode of operation)

λ_{sd} = 7,14E-09 1/h (inverted mode of operation)

λ_{su} = 1,29E-07 1/h

λ_{dd} = 7,64E-09 1/h (normal mode of operation)

λ_{dd} = 6,04E-09 1/h (inverted mode of operation)

λ_{du} = 7,43E-08 1/h

$\lambda_{annunciation}$ = 1,60E-09 1/h

$\lambda_{no\ effect}$ = 6,41E-08 1/h

λ_{total} = 2,82E-07 1/h

$\lambda_{not\ part}$ = 2,18E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 376 years

Under the assumptions described in section 5 the following table shows the worst case failure rates of the NAMUR switching amplifier PI-Ex-NAM/RNO-NE according to IEC 61508:

λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
6 FIT	194 FIT	8 FIT	74 FIT	73,65%	3%	9%

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} = 3,25E-04	PFD_{AVG} = 1,62E-03	PFD_{AVG} = 3,25E-03

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. Figure 4 shows the time dependent curve of PFD_{AVG}.

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

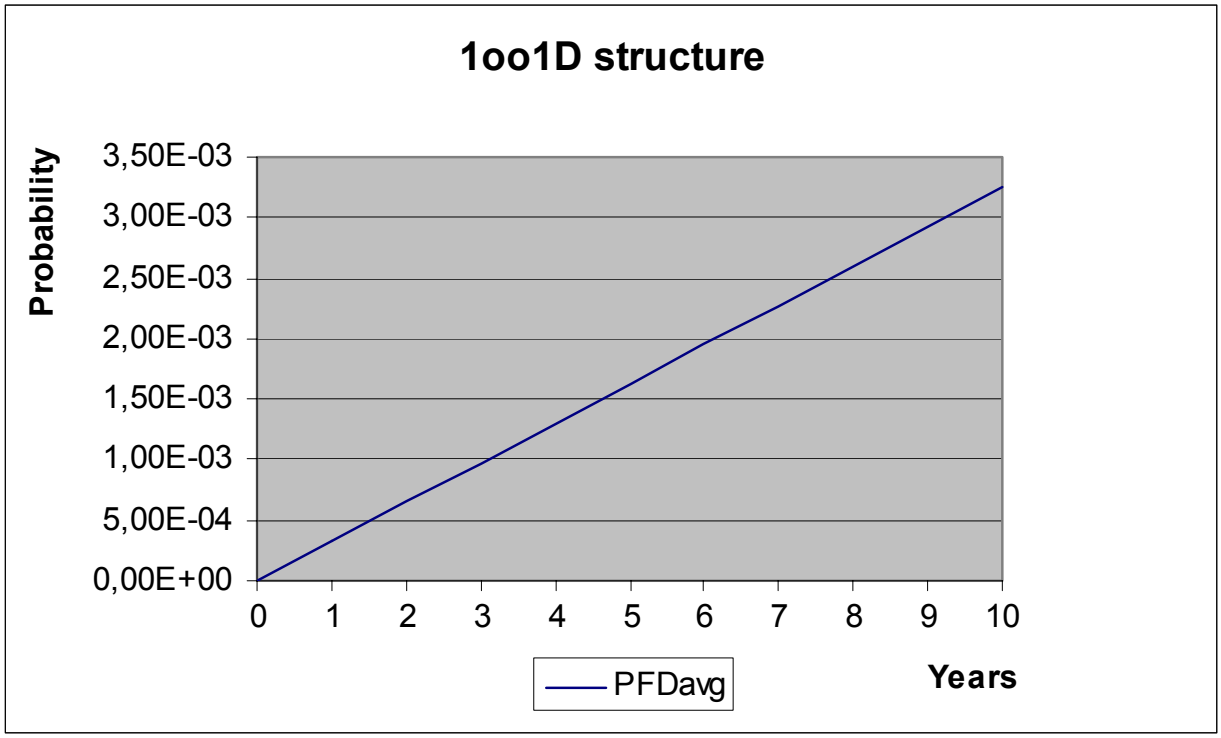


Figure 4: $PFD_{AVG}(t)$

5.2 NAMUR switching amplifier PI-Ex-NAM/TO-P

The FMEDA carried out on the NAMUR switching amplifier PI-Ex-NAM/TO-P leads under the assumptions described in section 4.2.3 and 5 to the following failure rates:

λ_{sd} = 5,54E-09 1/h (normal mode of operation)

λ_{sd} = 1,01E-08 1/h (inverted mode of operation)

λ_{su} = 8,95E-08 1/h

λ_{dd} = 7,64E-09 1/h (normal mode of operation)

λ_{dd} = 3,04E-09 1/h (inverted mode of operation)

λ_{du} = 3,68E-08 1/h

$\lambda_{annunciation}$ = 1,60E-09 1/h

$\lambda_{no\ effect}$ = 9,22E-08 1/h

λ_{total} = 2,33E-07 1/h

$\lambda_{not\ part}$ = 2,18E-08 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 447 years

Under the assumptions described in section 5 the following table shows the worst case failure rates of the NAMUR switching amplifier PI-Ex-NAM/TO-P according to IEC 61508:

λ_{sd}	λ_{su} [5]	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
6 FIT	183 FIT	8 FIT	37 FIT	84,23%	3%	17%

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} = 1,62E-04	PFD_{AVG} = 8,08E-04	PFD_{AVG} = 1,62E-03

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

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

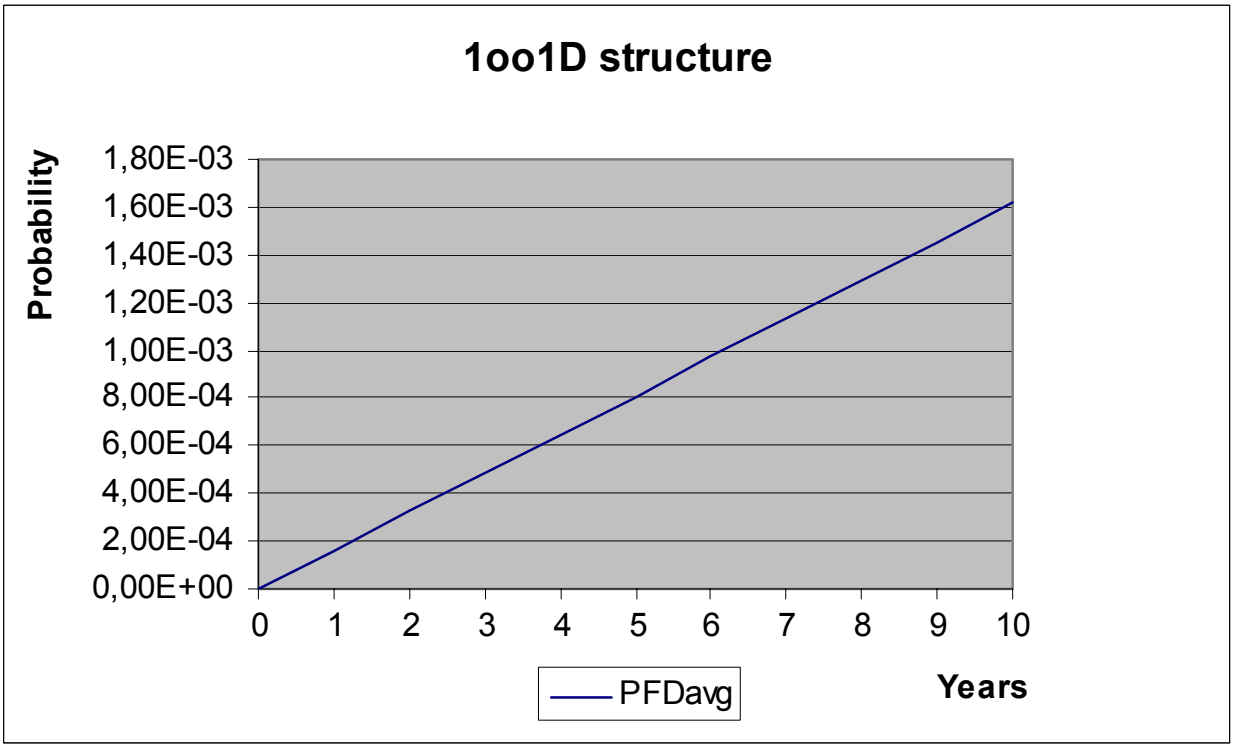


Figure 5: $PFD_{AVG}(t)$

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 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

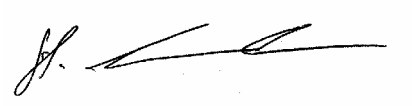
7.1 Liability

exida.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:	V1	
Revision:	R1.1	
Version History:	V0, R1.0:	Initial version; November 28, 2005
	V0, R2.0:	Failure rates corrected; November 29, 2005
	V1, R1.0:	Review comments incorporated; December 5, 2005
	V1, R1.1:	PFD_{AVG} value for PI-Ex-NAM/TO-P at T[Proof]=10 years corrected; March 8, 2006
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Rachel Amkreutz (exida); December 1, 2005
	V0, R2.0:	Winfried Hanke (PHOENIX CONTACT); November 30, 2005
Release status:	Released to PHOENIX CONTACT 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 5 and Table 6 show an importance analysis of the ten 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 5: NAMUR switching amplifier PI-Ex-NAM/RNO-NE

Component	% of total λ_{du}	Detection through
K1	67,33%	100% functional test with monitoring of the expected output signal
IC2	6,06%	100% functional test with monitoring of the expected output signal
V16	3,37%	100% functional test with monitoring of the expected output signal
V5	3,37%	100% functional test with monitoring of the expected output signal
IC3	3,23%	100% functional test with monitoring of the expected output signal
IC4	3,23%	100% functional test with monitoring of the expected output signal
S1	2,42%	100% functional test with monitoring of the expected output signal
V8	2,02%	100% functional test with monitoring of the expected output signal
IC1	1,62%	100% functional test with monitoring of the expected output signal
C23	1,35%	100% functional test with monitoring of the expected output signal

Table 6: NAMUR switching amplifier PI-Ex-NAM/TO-P

Component	% of total λ_{du}	Detection through
V11	16,17%	100% functional test with monitoring of the expected output signal
IC6	12,23%	100% functional test with monitoring of the expected output signal
IC 7	10,19%	100% functional test with monitoring of the expected output signal
V16	6,79%	100% functional test with monitoring of the expected output signal
IC3	6,52%	100% functional test with monitoring of the expected output signal
IC4	6,52%	100% functional test with monitoring of the expected output signal
S1	4,89%	100% functional test with monitoring of the expected output signal
V5	4,48%	100% functional test with monitoring of the expected output signal
V17	4,48%	100% functional test with monitoring of the expected output signal
V8	4,08%	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 consists of the following steps, as described in Table 7.

Table 7 Steps for proof test

Step	Action
1	Take appropriate action to avoid a false trip.
2	Provide an appropriate input signal to the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P to de-energize the output and verify that the output is de-energized.
3	Restore the loop to full operation.
4	Restore normal operation.

This test will detect approximately 99% of possible “du” failures in the NAMUR switching amplifiers PI-Ex-NAM/RNO-NE and PI-Ex-NAM/TO-P.

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.

Table 8 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 8: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life at 40°C
Relay	K1	10.000 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.

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.