Failure Modes, Effects and Diagnostic Analysis

Project:

Relay couplers
IM73-12-R/24VUC and IM73-12-R/230VAC

Customer:

Hans Turck GmbH & Co. KG
Mühlheim
Germany

Contract No.: TURCK 06/02-16
Report No.: TURCK 06/02-16 R006
Version V1, Revision R1.1, March 2006
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC with the two output relays connected in series.

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.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-4}$ to $< 10^{-3}$ for SIL 3 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-04.

The shut-down path of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC is carried out redundant. Therefore they could be split into two separate subsystems, one representing the input electronics having a hardware fault tolerance of 0, and one representing the shut-down path having a hardware fault tolerance of 1.

For simplicity reasons the analysis, however, was done by considering one of the two relays to be the "diagnostics" for the “primary” relay. A Diagnostic Coverage (DC) of 90% was considered to account for possible common cause failures.

The Relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC 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 90% and 99% according to table 2 of IEC 61508-2 for SIL 3 (sub-) systems with a hardware fault tolerance of 0.

It is important to realize that the “no effect” failures are included in the “safe” 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 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] 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 1: Summary IM73-12-R/24VUC – Failure rates

λ_{safe}	$\lambda_{dangerous}$	SFF
114 FIT	2 FIT	98% [2]

Table 2: Summary IM73-12-R/24VUC – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 9,82E-06	PFD_{AVG} = 4,91E-05	PFD_{AVG} = 9,81E-05

Table 3: Summary IM73-12-R/230VAC – Failure rates

λ_{safe}	$\lambda_{dangerous}$	SFF
116 FIT	2 FIT	98% [3]

Table 4: Summary IM73-12-R/230VAC – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 9,82E-06	PFD_{AVG} = 4,91E-05	PFD_{AVG} = 9,81E-05

The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 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-04.

Because the Safe Failure Fraction (SFF) is above 90%, 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 relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC 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.

The failure rates are valid for the useful life of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC (see Appendix 2).

[2] If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 69% and $\lambda_{dangerous}$ = 20 FIT per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

[3] If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 70% and $\lambda_{dangerous}$ = 20 FIT per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

Table of Contents

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like 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* 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* 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 relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC.

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 3 sub-systems according to 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 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* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Werner Turck GmbH & Co. KG	Manufacturer of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC.
exida	Performed the hardware assessment according to option 1 (see section 1).

Werner Turck GmbH & Co. KG contracted *exida* in February 2006 with the FMEDA and PFD_{AVG} calculation of the above mentioned devices.

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]	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]	d200555.pdf	Data sheet relay couplers
[D2]	12188900.tif	Circuit diagram “MK73-12-R/…v.c” SP 121 889 00 index A of 23.07.97
[D3]	1364366700.pdf	Parts list 12188907 for MK73-12-R/230VAC/K10 index F of 04.03.97
[D4]	1541124992.pdf	Parts list 12188903 for MK73-12-R/24VUC/K10 index E of 20.08.03
[D5]	FMEDA V6 IM73-12-R24VUC V1R1.xls of 20.01.06	
[D6]	FMEDA V6 IM73-12-R230VUC V1R1 Review SA.xls of 02.03.06	
[D7]	FMEDA V6 IM73-12-R230VUC V1R1 HFT1 Review SA.xls of 02.03.06	

2.4.2 Documentation generated by *exida*

[R1]	FMEDA V6 IM73-12-R24VUC V1R1 Review SA.xls of 02.02.06
[R2]	FMEDA V6 IM73-12-R24VUC V1R1 HFT1 Review SA.xls of 02.02.06
[R3]	FMEDA V6 IM73-12-R24VUC V1R2.xls of 02.03.06
[R4]	FMEDA V6 IM73-12-R24VUC V1R2 HFT1.xls of 02.03.06
[R5]	FMEDA V6 IM73-12-R230VAC V1R2.xls of 02.03.06
[R6]	FMEDA V6 IM73-12-R230VAC V1R2 HFT1.xls of 02.03.06

3 Description of the analyzed modules

The two single channel relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC are used to securely isolate binary signals.

Both couplers are equipped with two synchronized output relays with one SPDT contact each.

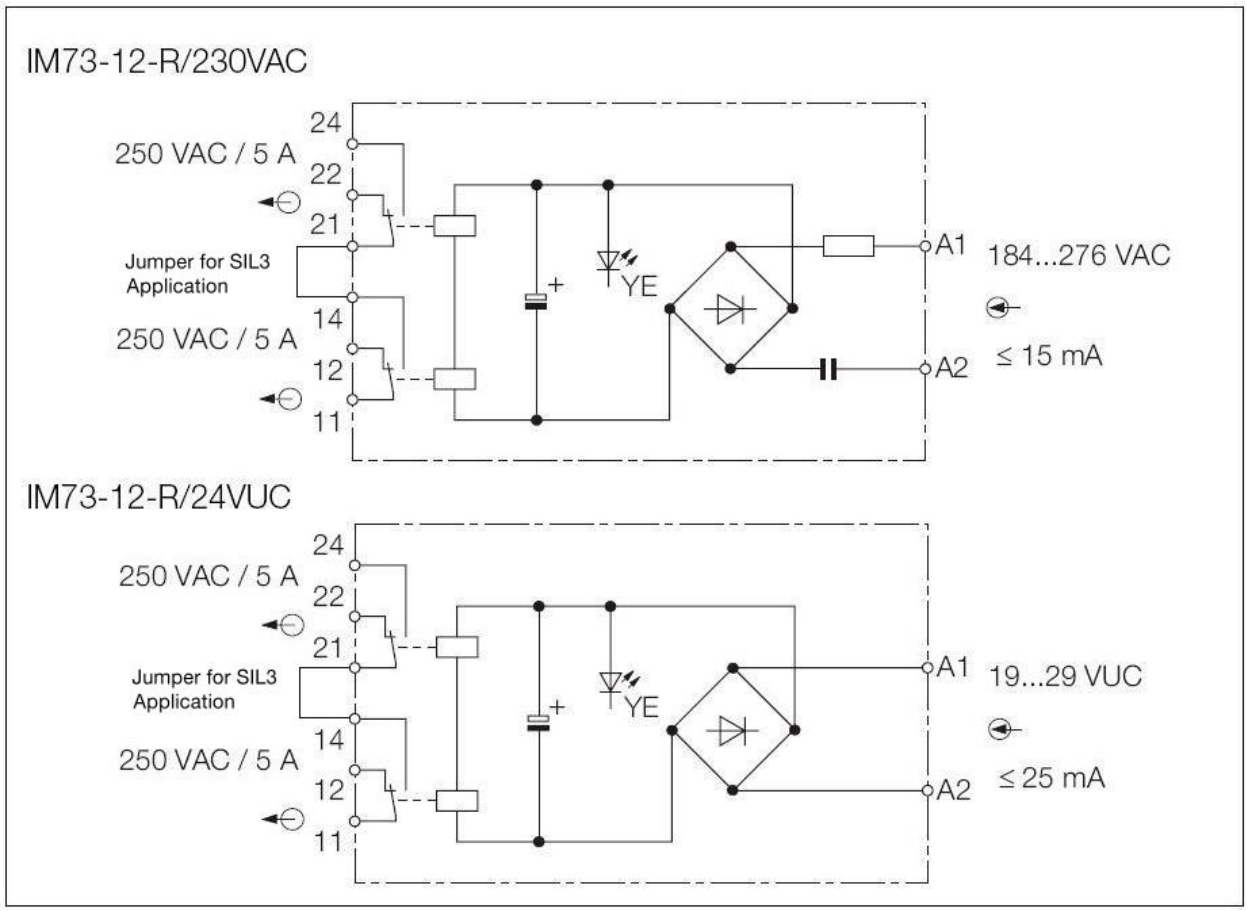


Figure 1: Block diagram of the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC

The relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC are considered to be Type A components with a hardware fault tolerance of 0.

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 [D5] to [D7] and [R1] to [R6]. 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 relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC, 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 internal diagnostics (These failures may be 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” failures and the “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* 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 relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC.

- 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.
- The two relays are connected in series.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- 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 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 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:

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

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

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

The shut-down path for the relay couplers IM73-12-R/24VUC and IM73-12-R/230VAC is carried out redundant. Therefore they could be split into two separate subsystems, one representing the input electronics having a hardware fault tolerance of 0, and one representing the shut-down path having a hardware fault tolerance of 1.

For simplicity reasons the analysis, however, was done by considering one of the two relays to be the "diagnostics" for the “primary” relay. A Diagnostic Coverage (DC) of 90% was considered to account for possible common cause failures.

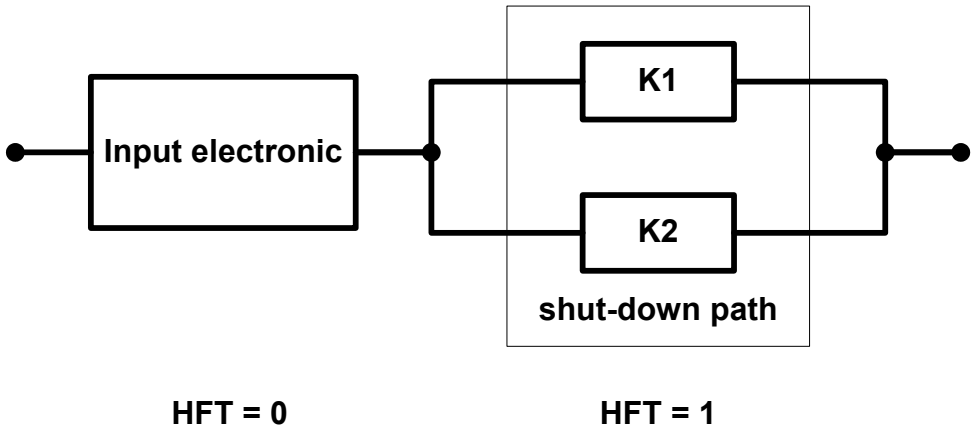
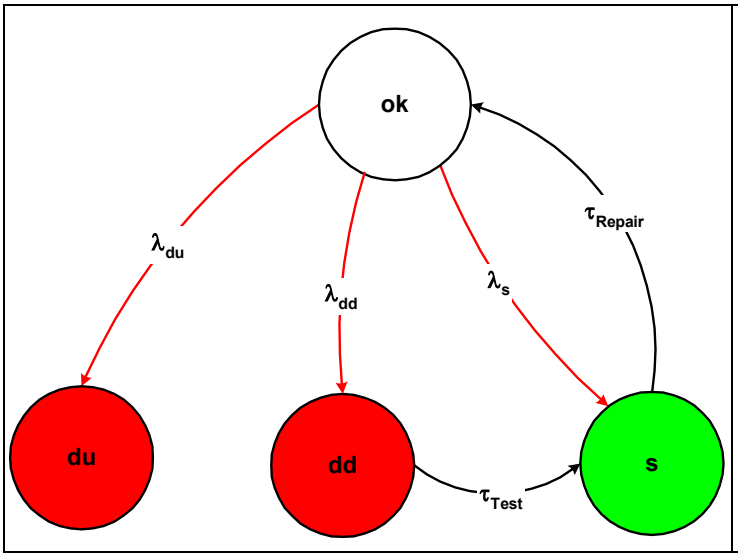


Figure 2: Separation of the relay couplers IM73-12-R into two subsystems

For the calculation of the PFD_{AVG} the following Markov model for 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* 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 Relay coupler IM73-12-R/24VUC

The FMEDA carried out on the relay coupler IM73-12-R/24VUC 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} = 7,21E-08 1/h

λ_{DD} = 1,80E-08 1/h [4]

λ_{DU} = 2,24E-09 1/h

$\lambda_{annunciation}$ = 2,00E-08 1/h [4]

$\lambda_{no\ effect}$ = 4,06E-09 1/h

λ_{total} = 1,16E-07 1/h

$\lambda_{not\ part}$ = 2,20E-09 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 963 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
114 FIT	2 FIT	98,08% [5]

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} = 9,82E-06	PFD_{AVG} = 4,91E-05	PFD_{AVG} = 9,81E-05

The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 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-04. Figure 4 shows the time dependent curve of PFD_{AVG}.

[4] The reason for having “dd” and “annunciation” failures comes from the fact that one of the two relays is considered to be the "diagnostic" for the “primary” relay. A DC of 90% was considered to account for possible common cause failures. The DD and Annunciation failures will actually lead to the fail-safe state and should therefore be considered in spurious trip calculations.

[5] If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 69,52% and $\lambda_{dangerous}$ = 20 FIT per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

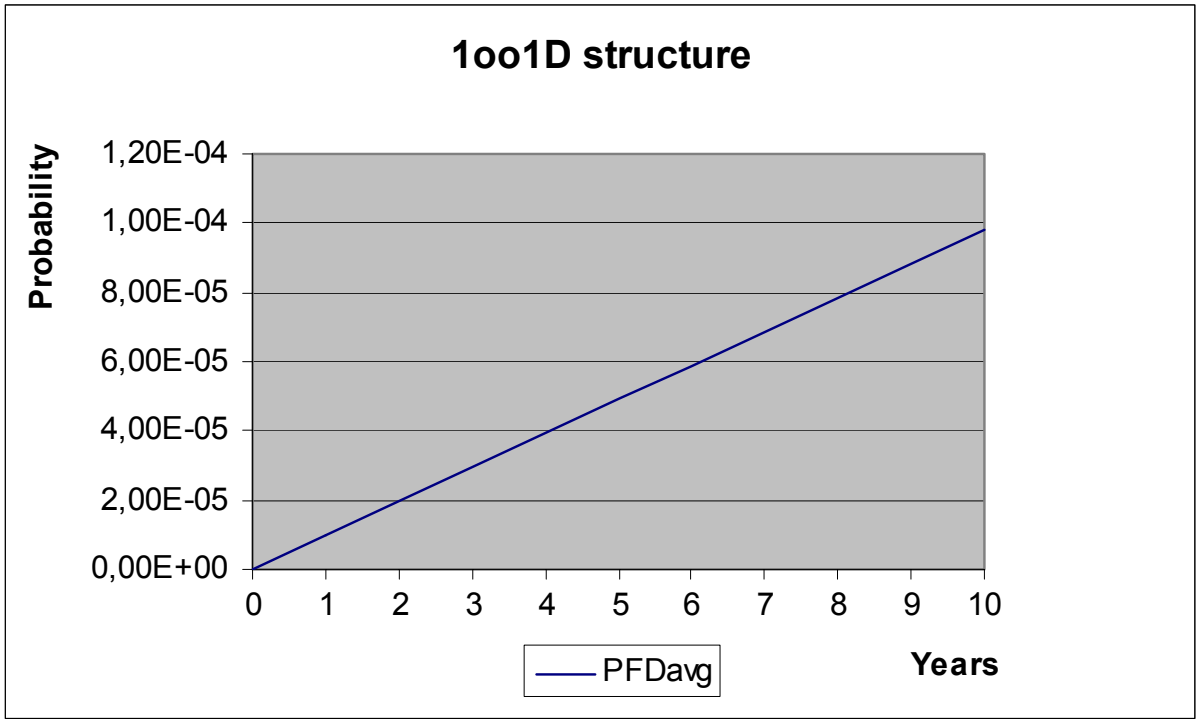


Figure 4: $PFD_{AVG}(t)$

5.2 Relay coupler IM73-12-R/230VAC

The FMEDA carried out on the relay coupler IM73-12-R/230VAC 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} = 7,35E-08 1/h

λ_{DD} = 1,80E-08 1/h [6]

λ_{DU} = 2,24E-09 1/h

$\lambda_{annunciation}$ = 2,00E-08 1/h [6]

$\lambda_{no\ effect}$ = 4,57E-09 1/h

λ_{total} = 1,18E-07 1/h

$\lambda_{not\ part}$ = 2,20E-09 1/h

MTBF = MTTF + MTTR = 1 / (λ_{total} + $\lambda_{not\ part}$) + 8 h = 947 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
116 FIT	2 FIT	98,11% [7]

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} = 9,82E-06	PFD_{AVG} = 4,91E-05	PFD_{AVG} = 9,81E-05

The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 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-04. Figure 5 shows the time dependent curve of PFD_{AVG}.

[6] The reason for having “dd” and “annunciation” failures comes from the fact that one of the two relays is considered to be the "diagnostic" for the “primary” relay. A DC of 90% was considered to account for possible common cause failures. The DD and Annunciation failures will actually lead to the fail-safe state and should therefore be considered in spurious trip calculations.

[7] If the device is considered to be a device with a hardware fault tolerance of 1 then the SFF is 70,37% and $\lambda_{dangerous}$ = 20 FIT per channel. Because the components of the input electronics are not contributing to the dangerous undetected failure rate the complete device can be considered to have a hardware fault tolerance of 1.

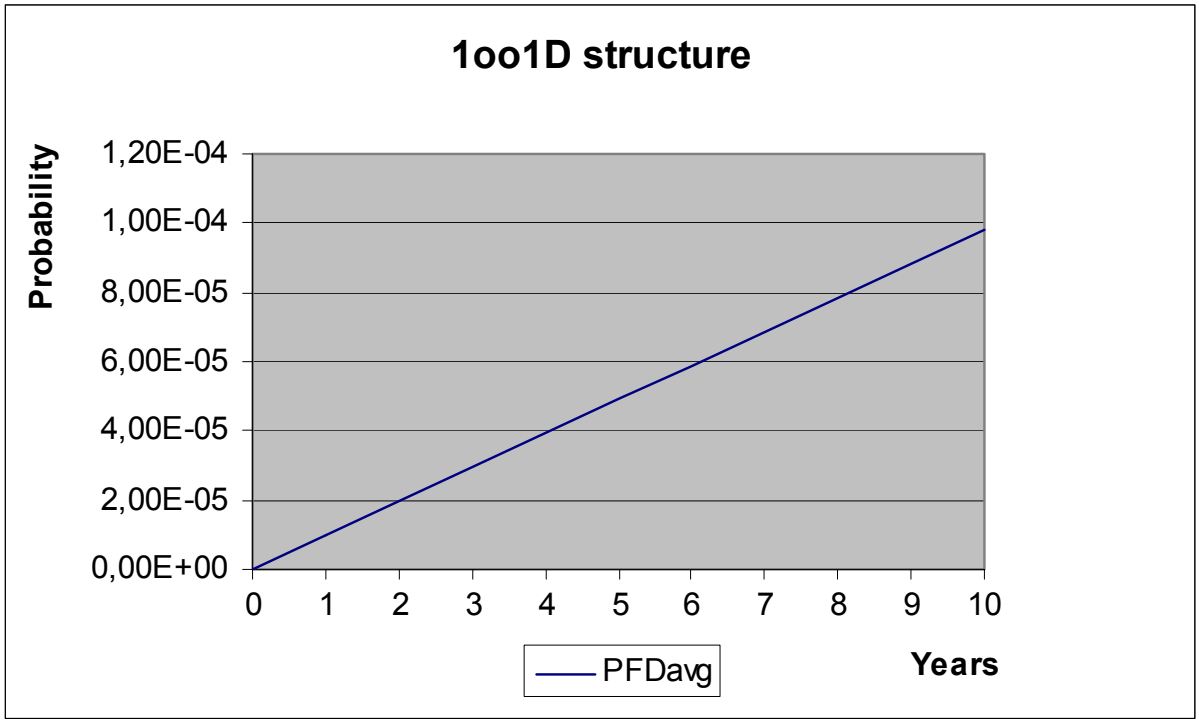


Figure 5: $PFD_{AVG}(t)$

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

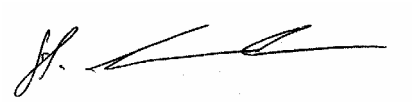
7.1 Liability

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

7.2 Releases

Version:	V1	
Revision:	R1.1	
Version History:	V0, R1.0:	Initial version; March 3, 2006
	V1, R1.0:	Review comments incorporated; March 24, 2006
	V1, R1.1:	Footnotes 4 and 6 corrected; March 27, 2006
Authors:	Stephan Aschenbrenner	
Review:	V0, R1.0:	Review by Frank Seeler (Turck); March 6, 2006
	V0, R1.0:	Review by Rachel Amkreutz (exida); March 24, 2006
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 5 shows an importance analysis of the 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 5: Importance Analysis of "du" failures

Component	% of total λ_{du}	Detection through
K1 (K2)	89,29%	100% functional test with monitoring of the output signal of each relay
X1, X2 , X3, X4	10,71%	100% functional test with monitoring of the output signal of each relay

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

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[8] 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 6 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 6: Useful lifetime of components contributing to λ_{du}

Type	Name	Useful life at 40°C
Relay	K1 (K2)	100.000 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.

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

[8] 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.