Failure Modes, Effects and Diagnostic Analysis

Project:
Pulse isolator 9202

Customer:
PR electronics A/S
Rønde
Denmark

Contract No.: PRelectronics 06/03-19
Report No.: PRelectronics 06/03-19 R018
Version V2, Revision R0; July 2014
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the pulse isolator 9202 with product revision 002. Table 1 gives an overview of the considered types.

Table 1: Type overview

9202B1A (Ex) / 9202A1A (Standard)	Opto-coupler output, one channel
9202B1B (Ex) / 9202A1B (Standard)	Opto-coupler output, two channels
9202B2A (Ex) / 9202A2A (Standard)	NO[1] relay output, one channel
9202B2B (Ex) / 9202A2B (Standard)	NO relay output, two channels
9202B3A (Ex) / 9202A3A (Standard)	NC[2] relay output, one channel
9202B3B (Ex) / 9202A3B (Standard)	NC relay output, two channels

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 above described output types were 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.

The pulse isolator 9202 is considered to be a Type B[3] subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF shall be > 90% for SIL 2 subsystems according to table 3 of IEC 61508-2.

The listed SN29500 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 (25°C ambient temperature plus internal self heating). 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 (daily fluctuation of > 15°C) must be assumed.

The two channels on the two channel devices shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures by the end-user.

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

[1] NO: Normally Open

[2] NC: Normally Closed

[3] Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 2: Summary for opto-coupler output types – Failure rates per IEC 61508

Failure category	Failure rates (in FIT)
Fail Safe (λ_{SAFE})	**276**
Fail safe undetected	119
Residual	157
Fail Dangerous Detected (λ_{DD})	**136**
Fail dangerous detected	93
Annunciation detected	43
Fail Dangerous Undetected (λ_{DU})	**36**
Fail dangerous undetected	35
Annunciation undetected	1
No part	85

Total failure rate (safety function)	**448 FIT**
SFF	**91%**
DC_D	**79%**
MTBF = MTTF + MTTR	**215 years**

SIL AC [4]	**SIL2**

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

Table 3: Summary for relay output types – Failure rates per IEC 61508

Failure category	Failure rates (in FIT)
Fail Safe (λ_{SAFE})	**290**
Fail safe undetected	140
Residual	150
Fail Dangerous Detected (λ_{DD})	**130**
Fail dangerous detected	91
Annunciation detected	39
Fail Dangerous Undetected (λ_{DU})	**47**
Fail dangerous undetected	46
Annunciation undetected	1
No part	85

Total failure rate (safety function)	**467 FIT**
SFF	**90%**
DC_D	**74%**
MTBF = MTTF + MTTR	**207 years**

SIL AC [5]	**SIL2**

A user of the pulse isolator 9202 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 4.4.1 and 4.4.2 along with all assumptions.

It is important to realize that the “residual” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the pulse isolator 9202 (see Appendix 2).

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

Table of Contents

Management summary 2

1 Purpose and Scope 6

2 Project management 7

2.1 *exida* 7

2.2 Roles of the parties involved 7

2.3 Standards / Literature used 7

2.4 Reference documents 8

2.4.1 Documentation provided by the customer 8

2.4.2 Documentation generated by *exida* 8

3 Description of the analyzed module 9

4 Failure Modes, Effects, and Diagnostics Analysis 10

4.1 Description of the failure categories 10

4.2 Methodology – FMEDA, Failure rates 11

4.2.1 FMEDA 11

4.2.2 Failure rates 11

4.3 Assumptions 11

4.4 Results 12

4.4.1 Pulse isolator 9202 with opto-coupler output 13

4.4.2 Pulse isolator 9202 with relay output 14

5 Using the FMEDA results 15

5.1 PFD_{AVG} / PFH calculation 15

6 Terms and Definitions 17

7 Status of the document 18

7.1 Liability 18

7.2 Releases 18

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test 19

Appendix 2: Possible proof tests to detect dangerous undetected faults 20

Appendix 3: Impact of lifetime of critical components on the failure rate 21

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

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

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

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

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

Option 3: Full assessment according to IEC 61508

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

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

This assessment shall be done according to option 3.

This document shall describe the results of the FMEDA carried out on the pulse isolator 9202 with product revision 002. The FMEDA is one part of a full functional safety assessment according to IEC 61508. This FMEDA report supplements the hardware information given in the full IEC 61508 Assessment Report.

The information in this report can be used to evaluate whether a sensor subsystem, including the pulse isolator 9202 meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations 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

PR electronics A/S	Manufacturer of the pulse isolator 9202
exida	Performed the hardware assessment

PR electronics A/S contracted *exida* in January 2007 with the FMEDA and PFD_{AVG} / PFH calculation of the above mentioned device. *exida* was additionally contracted in May 2009 to review an FMEDA with updated PFD_{AVG} / PFH calculations.

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 29500-1:01.2004 SN 29500-1 H1:12.2005 SN 29500-2:12:2004 SN 29500-3:12.2004 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:08.1990 SN 29500-12:03.1994 SN 29500-13:03.1994 SN 29500-14:03.1994	Failure rates of components

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	9202 Schematic V4R0.pdf	Circuit diagram “9202-1-03-SCH” of 16.11.07
[D2]	9202 Software Fault Insertion Test Report V3R0.doc of 21.04.08	SW fault insertion test report V3R0
[D3]	9202 Hardware Fault Insertion Test Report V3R0.doc of 22.04.08	HW fault insertion test report V3R0
[D4]	New A variant to the 9000 series of transmitters with grey terminals.msg of 15.05.14	Description of changes between Ex and standard versions.
[D5]	9202 FMEDA V4R0.xls of 28.03.08	
[D6]	9202 FMEDA V4R6 - opto.xls of 12.05.09	
[D7]	9202 FMEDA V4R6 - relay.xls of 12.05.09	
[D8]	9202 Derating Analysis (V4R2).xls of 22.04.08	
[D9]	Relay-endurance test.doc of 29.08.07	

2.4.2 Documentation generated by *exida*

[R1]	HW Fault Insertion Test 9202 V1R0.doc of 11.04.08
[R2]	SW Fault Insertion Test 9202 V1R1.doc of 05.02.08
[R3]	Comments_SA_FMEDA.txt of 11.04.08

3 Description of the analyzed module

The pulse isolator 9202 converts a NAMUR sensor input signal or the signal from a mechanical switch from hazardous areas to a digital output signal in safe area for use in (safety) PLCs.

The pulse isolator 9202 is considered to be a Type B subsystem with a hardware fault tolerance of 0.

Figure 1 shows the block diagram of the pulse isolator 9202. The FMEDA has been carried out on the pulse isolator 9202 without considering the sensors that can be connected to it as indicated in the figure below.

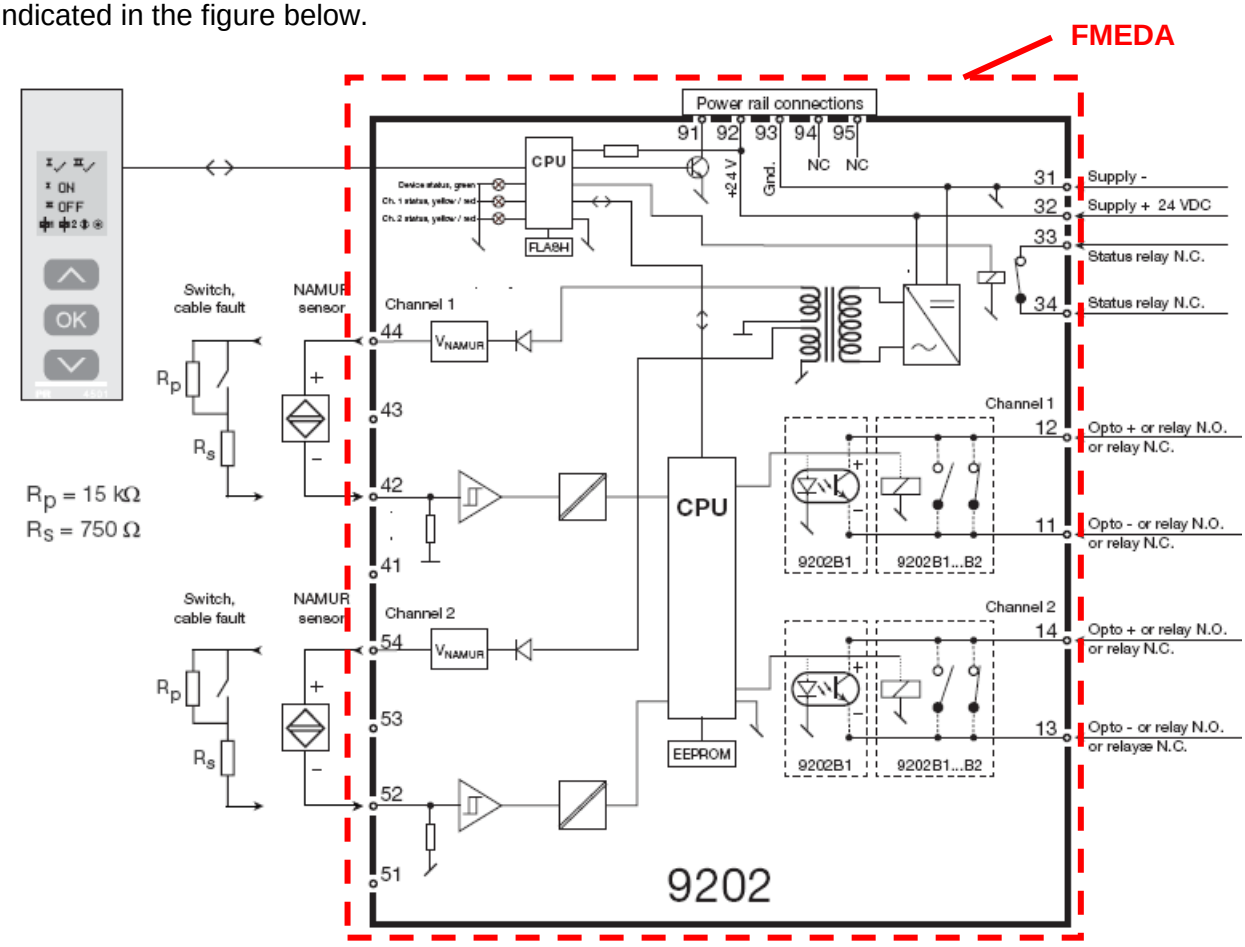

Figure 1: Block diagram of the pulse isolator 9202

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by PR electronics A/S and reviewed by *exida*. The results are documented in [D6] and [D7].

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level, see fault insertion test reports [D2] and [D3].

4.1 Description of the failure categories

In order to judge the failure behavior of the pulse isolator 9202, 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. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
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).
Annunciation	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures. For the calculation of the SFF they are treated like dangerous failures.
Residual	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure. For the calculation of the SFF it is treated like a safe undetected failure.
No part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The reason for this is that not all failure modes have effects that can be accurately classified according to the failure categories listed in IEC 61508.

The “Residual” and “Annunciation” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. The “Residual” 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.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an 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 were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the pulse isolator 9202.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- 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.
- For safety applications only the described outputs are considered.
- Only one input and one output are part of the considered safety function.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 8 hours.
- The worst-case internal fault detection time is 1 minute.

- The output signal is fed to a SIL 2 compliant input board of a safety PLC.
- The two channels on a board are not used for one safety function as they contain common components.
- All relay outputs are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.
- The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C (25°C ambient temperature plus internal self heating). 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 (daily fluctuation of > 15°C) must be assumed. Humidity levels are assumed within manufacturer's rating.

4.4 Results

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:

$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{residual} + \lambda_{annunciation}$

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

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

4.4.1 Pulse isolator 9202 with opto-coupler output

The FMEDA carried out on the pulse isolator 9202 with opto-coupler output leads under the assumptions described in sections 4.3 and 4.4 to the following failure rates:

Failure category	Failure rates (in FIT)
Fail Safe (λ_{SAFE})	**276**
Fail safe undetected	119
Residual	157
Fail Dangerous Detected (λ_{DD})	**136**
Fail dangerous detected	93
Annunciation detected	43
Fail Dangerous Undetected (λ_{DU})	**36**
Fail dangerous undetected	35
Annunciation undetected	1
No part	85

Total failure rate (safety function)	**448 FIT**
SFF	**91%**
DC_D	**79%**
MTBF = MTTF + MTTR	**215 years**

SIL AC [6]	**SIL2**

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

4.4.2 Pulse isolator 9202 with relay output

The FMEDA carried out on the pulse isolator 9202 with relay output leads under the assumptions described in sections 4.3 and 4.4 to the following failure rates:

Failure category	Failure rates (in FIT)
Fail Safe (λ_{SAFE})	**290**
Fail safe undetected	140
Residual	150
Fail Dangerous Detected (λ_{DD})	**130**
Fail dangerous detected	91
Annunciation detected	39
Fail Dangerous Undetected (λ_{DU})	**47**
Fail dangerous undetected	46
Annunciation undetected	1
No part	85

Total failure rate (safety function)	**467 FIT**
SFF	**90%**
DC_D	**74%**
MTBF = MTTF + MTTR	**207 years**

SIL AC [7]	**SIL2**

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

5 Using the FMEDA results

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

5.1 PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) calculation is performed for a single (1oo1) pulse isolator 9202. The failure rate data used in this calculation are displayed in sections 4.4.1 and 4.4.2. The resulting PFD_{AVG} (for a variety of proof test intervals) / PFH values are displayed in Table 4 and Table 5.

Table 4: PFD_{AVG} / PFH values for pulse isolator 9202 with opto-coupler output

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	
PFD_{AVG} = 1.58E-04	PFD_{AVG} = 3.17E-04	PFD_{AVG} = 7.92E-04	PFH = 3.62E-08 1/h [8]

For SIL 2 applications, the PFD_{AVG} value needs to be < 1.00E-02. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year proof test interval of the pulse isolator 9202 with opto-coupler output is approximately equal to 2% of the range.

For SIL 2 applications, the PFH value needs to be < 1.00E-06 1/h. This means that for a SIL 2 application, the PFH value of the pulse isolator 9202 with opto-coupler output is approximately equal to 4% of the range.

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

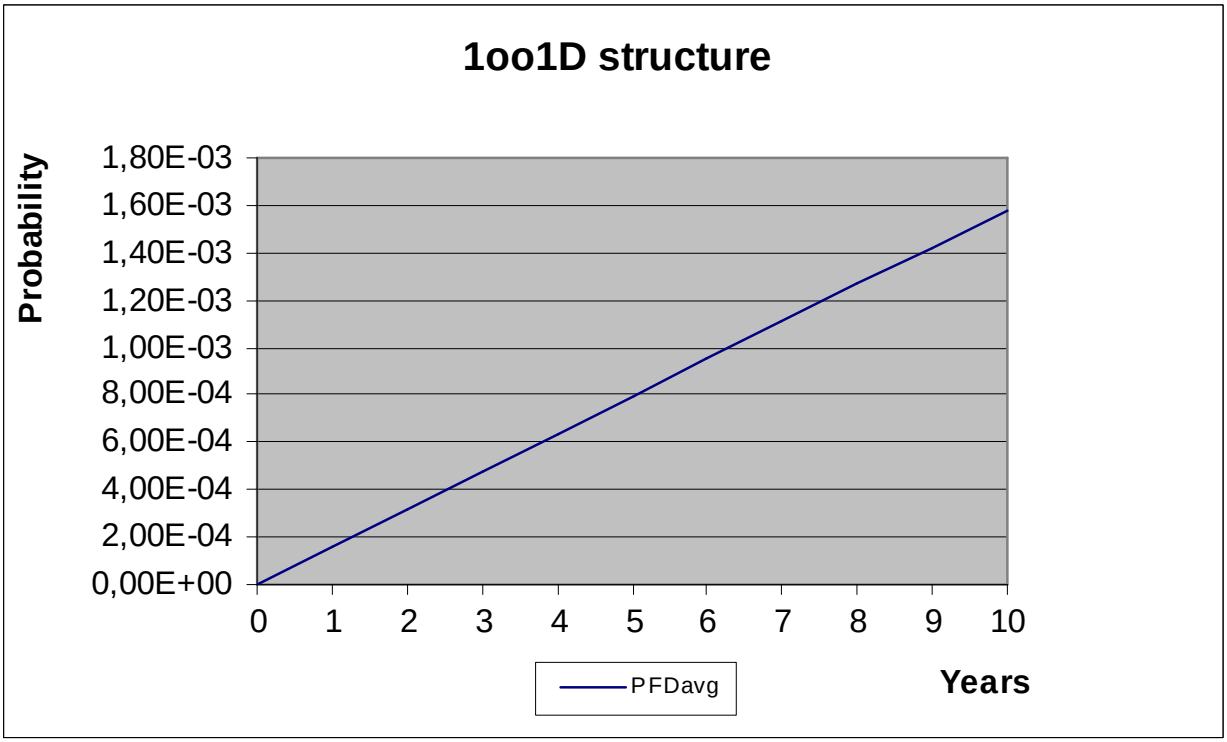

Figure 2: $PFD_{AVG}(t)$

[8] The PFH value is based on an internal fault reaction time of 1 minute. This requires that a connected device can detect the output state within a time that allows reacting within the process safety time.

Table 5: PFD_{AVG} / PFH values for pulse isolator 9202 with relay output

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years	
PFD_{AVG} = 2.04E-04	PFD_{AVG} = 4.08E-04	PFD_{AVG} = 1.02E-03	PFH = 4.67E-08 1/h [10]

For SIL 2 applications, the PFD_{AVG} value needs to be < 1.00E-02. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year proof test interval of the pulse isolator 9202 with relay output is approximately equal to 2% of the range.

For SIL 2 applications, the PFH value needs to be < 1.00E-06 1/h. This means that for a SIL 2 application, the PFH value of the pulse isolator 9202 with relay output is approximately equal to 5% of the range.

Figure 3 shows the time dependent curve of PFD_{AVG}.

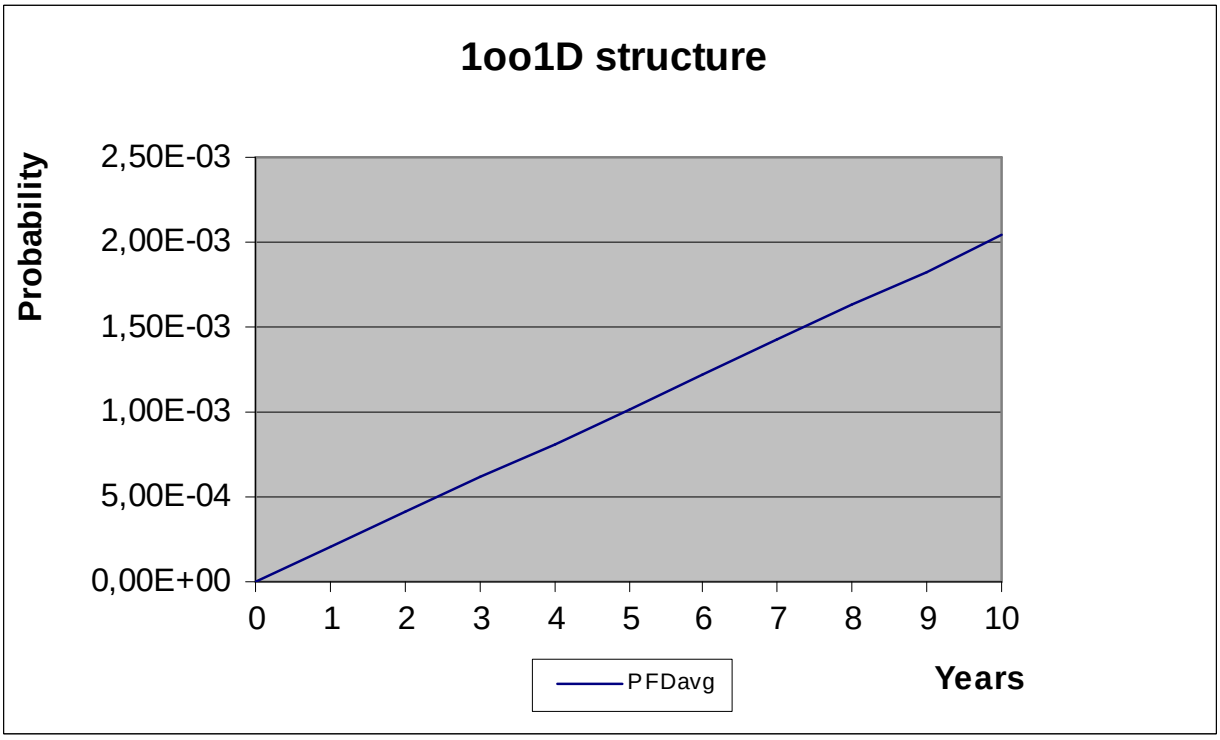

Figure 3: $PFD_{AVG}(t)$

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

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

6 Terms and Definitions

DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof test frequency.
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour. The term “Probability” is misleading, correctly defined it is a Rate.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
Type B subsystem	“Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares 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:	V2R0:	Non-Ex versions added; July 8, 2014
	V1R2:	Purpose and Scope section modified; October 6, 2010
	V1R1:	Updated and released after minor modifications to input circuitry and power rail status circuitry; May, 16 2009
	V1R0:	External review comments incorporated and release; June 5, 2008
	V0R2:	Internal review comments incorporated; May 8, 2008
	V0R1:	Initial version; May 7, 2008
Author:	Mats Gunnmarker, Stephan Aschenbrenner	
Review:	V0R2:	Hans Jørgen Eriksen (PR electronics A/S); June 5, 2008
	V0R1:	Audun Opem (*exida*); May 8, 2008
Release status:	Released to PR electronics A/S as part of a complete functional safety assessment according to IEC 61508	

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

Appendix 2 shall be considered when writing the safety manual as it contains important safety related information.

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 6 and Table 7 show an importance analysis of the most critical dangerous undetected faults and indicate how these faults can be detected during proof testing.

Table 6: Importance Analysis for pulse isolator 9202 with opto-coupler output

Component	% of total λ_{du}	Detection through
IC203	10,70%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC101D	8,56%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T205	7,13%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T210	7,13%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T206	6,42%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T4	4,71%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC202B	4,28%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC202C	4,28%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC202D	4,28%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
R112, R115, R116, R119, R122, R123, R124, R125, R126	4,12%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal

Table 7: Importance Analysis for pulse isolator 9202 with relay output

Component	% of total λ_{du}	Detection through
RE201	43,79%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC101D	6,57%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T205	5,47%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T4	3,61%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC202B	3,28%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC202C	3,28%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
IC202D	3,28%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
R112, R115, R116, R119, R122, R123, R124, R125, R126	3,16%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
T209	2,63%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal
Z2	2,30%	100% functional test with different input signals over the entire range and monitoring of the corresponding output signal

Appendix 2: Possible proof tests to detect dangerous undetected faults

A possible proof test is described in the safety manual for the pulse isolator 9202.

Appendix 3: 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 4.3) this only applies provided that the useful lifetime[9] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, 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 17 shows which components with limited useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} / PFH calculation and what their estimated useful lifetime is.

Table 8 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Relay RE201 [10]	100 000 switching cycles (electrical useful life) 1.00E+07 to 1.50E+07 switching cycles (mechanical useful life)

For high demand mode applications, the useful lifetime of the relay is limited by the number of cycles. The useful lifetime of the relay has to be calculated depending on the actual number of switching cycles.

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

[9] 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.

[10] According to [D9] the test results under the used conditions confirm more switching cycles.