



Failure Modes, Effects and Diagnostic Analysis

Project:
Pulse isolator 9202

Customer:
PR electronics A/S
Rønde
Denmark

Contract No.: PR Q23/09-138
Report No.: PR electronics 06/03-19 R018
Version V3, Revision R1; February 2024

Armin Schulze, Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Pulse isolator 9202 with hardware versions 9202SMDB1A-2040, 9202SMDB1B_2041, 9202SMDB2A-2038 and 9202SMDB2B-204. Table 1 gives an overview of the considered product variants.

A Failure Modes, Effects, and Diagnostic Analysis is one of the steps taken to achieve functional safety assessment of a device per IEC 61508 or ISO 13849. From the FMEDA, failure rates are determined and consequently the safety metrics for the corresponding standard can be calculated for a subsystem.

The FMEDA that is described in this report concerns only the hardware of the Pulse isolator 9202. For full assessment purposes all requirements of IEC 61508 or ISO 13849 must be considered.

Table 1: Overview of the considered Product variants

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

For safety applications only the described variants with the described hardware and software versions of the Pulse isolator 9202 have been considered. Any other variants and configurations are not covered by this report.

The Pulse isolator 9202 can be considered as a Type B³ element with a hardware fault tolerance (HFT) of 0.

The failure modes and failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook [N2] for Profile 1. They meet the *exida* criteria for Route 2_H (see Appendix 4). Therefore, the Pulse isolator 9202 can be classified as a 2_H device when the listed failure rates are used. The analysis resulted in a DC (Diagnostic Coverage) of over 60%.

The failure rates are valid for the useful life of the Pulse isolator 9202 (see Appendix 2) when operating as defined in the considered scenarios.

When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 for low demand mode applications or SIL 2 / SIL 3 at HFT=1 for high and low demand mode applications.

The two channels on the dual 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 regard is taken of the possibility of common failures.

¹ NO: Normally Open

² NC: Normally Closed

³ Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

Assuming that, the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled.

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

	<i>exida</i> Profile 1 ⁴
Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	112
Dangerous Detected (λ_{DD})	85
Fail detected (detected by internal diagnostics)	85
Dangerous Undetected (λ_{DU})	41
Total failure rate (safety function)	238
DC ⁵	67%

Table 3: Safety metrics according to ISO 13849-1 for opto-coupler output types

MTTF_D (years)	908 (High)
DC_{avg}	67% (Low)
Average frequency of a dangerous failure per hour (PFH) ⁶	4.09E-08 1/h
Performance Level (PL) ⁷	d

⁴ For details see Appendix 3.

⁵ According to the Route 2_H approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

⁶ The PFH values only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

⁷ The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF_D, DC_{avg} and PFH value of the device itself.

Table 4: Summary for relay output types – Failure rates per IEC 61508

	<i>exida</i> Profile 1 ⁸
Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	108
Dangerous Detected (λ_{DD})	85
Fail detected (detected by internal diagnostics)	85
Dangerous Undetected (λ_{DU})	50
Total failure rate (safety function)	243
DC ⁹	63%

Table 5: Safety metrics according to ISO 13849-1 for relay output types

MTTF_D (years)	848 (High)
DC_{avg}	63% (Low)
Average frequency of a dangerous failure per hour (PFH) ¹⁰	5.01E-08 1/h
Performance Level (PL) ¹¹	d

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

⁸ For details see Appendix 3.

⁹ According to the Route 2_H approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

¹⁰ The PFH value is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

¹¹ The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF_D, DC_{avg} and PFH value of the device itself.

Table of Contents

Management summary	2
1 Purpose and Scope.....	6
2 Project management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved	7
2.3 Standards / Literature used.....	7
2.4 <i>exida</i> tools used	7
2.5 Reference documents.....	8
2.5.1 Documentation provided by the customer	8
2.5.2 Documentation generated by <i>exida</i>	8
3 Product Description.....	9
4 Failure Modes, Effects, and Diagnostic Analysis.....	10
4.1 Failure categories description	10
4.2 Methodology – FMEDA, Failure rates	11
4.2.1 FMEDA	11
4.2.2 Failure rates	11
4.2.3 Assumptions	12
4.3 FMEDA Results	12
4.3.1 Pulse isolator 9202.....	13
4.4 Architectural Constraints.....	15
5 Using the FMEDA results.....	16
5.1 Example PFD _{AVG} / PFH calculation	17
6 Terms and Definitions	19
7 Status of the document	20
7.1 Liability	20
7.2 Releases.....	21
7.3 Release Signatures	21
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test...	22
Appendix 1.1: Possible proof tests to detect dangerous undetected faults	22
Appendix 3: Impact of lifetime of critical components on the failure rate.....	23
Appendix 4: <i>exida</i> Environmental Profiles	24
Appendix 5: <i>exida</i> Route 2 _H Criteria.....	25

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Pulse isolator 9202 with hardware versions 9202SMDB1A-2040, 9202SMDB1B_2041, 9202SMDB2A-2038 and 9202SMDB2B-204.

The FMEDA builds the basis for an evaluation whether a sensor / logic / final-element subsystem, including the product, 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 or ISO 13849.

It **does not** consider any calculations necessary for proving intrinsic safety or an evaluation of the correct device behavior in general. This FMEDA **does not** replace a full assessment according to IEC 61508 or ISO 13849.

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	9202-1-07-PDF of 18.03.2022	Schematic drawings 9202-1-V7R0
[D2]	9202 FMEDA - Opto.xls of 16.11.2023	FMEDA results file revision V4R8 generated by customer
[D3]	9202 FMEDA - Relay.xls of 17.11.2023	FMEDA results file revision V4R8 generated by customer
[D4]	9202SMDB1A_2040.xlsx of 16.11.2023	BOM and Version history of 9202B1A
[D5]	9202SMDB1B_2041.xlsx of 17.11.2023	BOM and Version history of 9202B1B
[D6]	9202SMDB2A_2038.xlsx of 17.11.2023	BOM and Version history of 9202B2A
[D7]	9202SMDB2B_2041.xlsx of 17.11.2023	BOM and Version history of 9202B2B
[D8]	9202 CPU failure distribution estimation.xls of 30.11.2023	Failure distribution for used CPUs revision V0R1
[D9]	9202 Derating Analysis.xls of 30.11.2023	Derating analysis for 9202, V4R2
[D10]	9202_safety_manualv7r0.pdf	Safety Manual V7R0
[D11]	Relay-endurance test.doc of 29.08.07	Relay endurance test documentation

The list above only means that the referenced documents were provided as basis for the FMEDA, but it does not mean that *exida* checked the correctness and completeness of these documents.

2.5.2 Documentation generated by *exida*

[R1]	9202 FMEDA - Opto_CRD_5th_Ed_FIT_values.xls of 02.02.24	FMEDA results file based on [D2] with Route 2 _H compliant failure rate data used from the <i>exida</i> CRD [N3]
[R2]	9202 FMEDA - Relay_CRD_5th_Ed_FIT_values.xls of 02.02.24	FMEDA results file based on [D3] with Route 2 _H compliant failure rate data used from the <i>exida</i> CRD [N3]

3 Product Description

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.

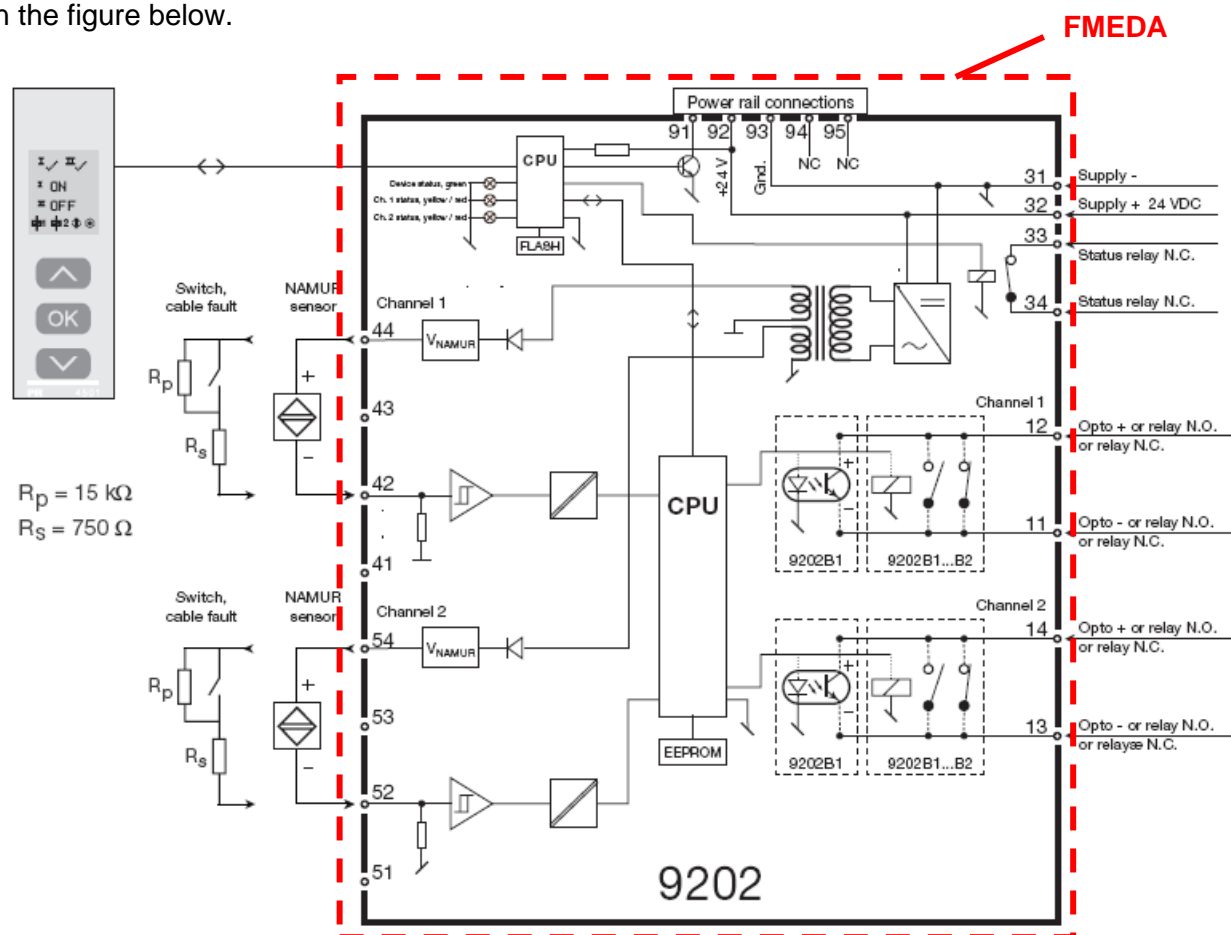


Figure 1: Block diagram of the pulse isolator 9202

The Pulse isolator 9202 is classified as a Type B¹² element according to IEC 61508, having a hardware fault tolerance of 0.

¹² Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The original Failure Modes, Effects, and Diagnostic Analysis was done by **PR electronics A/S** and is documented in [D2] and [D3]. *exida* updated the failure rates from that report to the *exida* CRD (see [N3]) and created the FMEDA documented in [R1] and [R2].

When the effect of a certain component 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 report [D4]). This resulted in failures that can be classified according to the following failure categories.

4.1 Failure categories description

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).
No Effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous 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.

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

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online 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 modes and failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook [N3] for environmental profile 1 (see Appendix 3). The rates were chosen in a way that is appropriate for safety integrity level verification calculations and the intended applications. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 or ISO 13849 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

The user of these numbers is responsible for determining the failure rate applicability to any particular environment.

Accurate plant specific data may be used to check validity of the failure rate data. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.2.3 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.
- The device is installed per manufacturer's instructions.
- 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.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- External power supply failure rates are not included.
- The time of a connected safety PLC to react on a dangerous detected failure and to bring the process to the safe state is identical to MTTR.
- Only the described versions are used for safety applications.
- Only one input and one output are part of the considered safety function.
- Materials are compatible with process conditions.
- The measurement / application limits (including pressure and temperature ranges) are considered.
- Short circuit and lead breakage detection are activated.
- The worst-case internal fault detection time is 10 seconds. Therefore, a demand for the safety function in high demand mode is only possible every 1000 seconds¹³, which corresponds to 17 minutes.
- Soft Error Rates (SER) were considered for relative neutron flux of 4.5 corresponding to 1,600 meters above sea.

4.3 FMEDA Results

For the calculations the following has to be noted:

$$\lambda_{\text{total}} = \lambda_{\text{SD}} + \lambda_{\text{SU}} + \lambda_{\text{DD}} + \lambda_{\text{DU}}$$

IEC 61508:

$$\text{DC} = \lambda_{\text{DD}} / (\lambda_{\text{DD}} + \lambda_{\text{DU}})$$

ISO 13849-1:

$$\text{MTTF}_D [\text{years}] = 1 / ((\lambda_{\text{DD}} + \lambda_{\text{DU}}) * 24 * 365)$$

$$\text{PFH} = \lambda_{\text{DU}}$$

$$\text{DC}_{\text{avg}} = \lambda_{\text{DD}} / (\lambda_{\text{DD}} + \lambda_{\text{DU}})$$

¹³ See IEC 61508-2:2010, paragraph 7.4.4.1.4 and ISO 13849-1:2023, paragraph 6.1.3.2.4

4.3.1 Pulse isolator 9202

The FMEDA carried out on the Pulse isolator 9202 in the product variants Table 1, under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates:

Table 6: Pulse isolator 9202 with opto-coupler output – IEC 61508 failure rates

	<i>exida</i> Profile 1 ¹⁴
Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	112
Dangerous Detected (λ_{DD})	85
Fail detected (detected by internal diagnostics)	85
Dangerous Undetected (λ_{DU})	41
Annunciation (λ_A)	64
No effect ($\lambda_{\#}$)	151
No part (λ_{-})	96
Total failure rate (safety function)	238
DC ¹⁵	67%

Table 7: Safety metrics according to ISO 13849-1 for Pulse isolator 9202 with opto-coupler output

MTTF_D (years)	908 (High)
DC_{avg}	67% (Low)
Average frequency of a dangerous failure per hour (PFH) ¹⁶	4.09E-08 1/h
Performance Level (PL) ¹⁷	d

¹⁴ For details see Appendix 3.

¹⁵ According to the Route 2H approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

¹⁶ The PFH value is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

¹⁷ The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF_D, DC_{avg} and PFH value of the device itself.

Table 8: Pulse isolator 9202 with relay output – IEC 61508 failure rates

<i>exida</i> Profile 1 ¹⁸	
Failure category	Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	108
Dangerous Detected (λ_{DD})	85
Fail detected (detected by internal diagnostics)	85
Dangerous Undetected (λ_{DU})	50
Annunciation (λ_A)	60
No effect ($\lambda_{\#}$)	107
No part (λ_{-})	96
Total failure rate (safety function)	243
DC ¹⁹	63%

Table 9: Safety metrics according to ISO 13849-1 for Pulse isolator 9202 with relay output

MTTF_D (years)	848 (High)
DC_{avg}	63% (Low)
Average frequency of a dangerous failure per hour (PFH) ²⁰	5.01E-08 1/h
Performance Level (PL) ²¹	d

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

¹⁸ For details see Appendix 3.

¹⁹ According to the Route 2H approach from IEC 61508, the DC value together with the device type is sufficient to derive the SIL level of the device. See chapter 4.4 for more details.

²⁰ The PFH value is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

²¹ The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF_D, DC_{avg} and PFH value of the device itself.

4.4 Architectural Constraints

The architectural constraint type for the Pulse isolator 9202 is B. The hardware fault tolerance of the device is 0.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2.

The 1_H approach involves calculating the Safe Failure Fraction (SFF) for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-2.

This FMEDA analysis uses the 2_H approach with the 2_H qualified failure rates from the *exida* component reliability database [N3] (see also Appendix 4). To apply the 2_H approach on a Type B device, the diagnostic coverage has to be at least 60%.

The analysis shows that the Pulse isolator 9202 device series has a diagnostic coverage of 67% for opto-coupler output types and 63% for relay output types. Therefore, it meets the hardware architectural constraints for up to SIL 2.

When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 for low demand mode applications or SIL 2 / SIL 3 at HFT=1 for high and low demand mode applications.

As the Pulse isolator 9202 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

5 Using the FMEDA results

Using the failure rate data given in section 4.3.1 and the failure rate data for the associated element devices, an average Probability of Failure on Demand (PFD_{AVG}) calculation can be performed for the entire Safety Instrumented Function (SIF).

Probability of Failure on Demand (PFD_{AVG}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

To perform an average Probability of Failure on Demand (PFD_{AVG}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{AVG} by making many assumptions about the application and operational policies of a site. Therefore, use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{AVG}) calculation is best accomplished with *exida's* exSILentia tool.

The failure rates for all the devices of the Safety Instrumented Function and the corresponding proof test coverages are required to perform the PFD_{AVG} calculation. The proof test coverage of the suggested proof test for the Pulse isolator 9202 is listed in Appendix 1.1. This has to be combined with the dangerous failure rates after proof test for other devices to establish the proof test coverage for the entire Safety Instrumented Function.

When performing testing at regular intervals, the Pulse isolator 9202 contribute less to the overall PFD_{AVG} of the safety instrumented function.

The following section gives a simplified example on how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) Pulse isolator 9202 with *exida*'s exSILentia tool. The failure rate data used in this calculation are given in section 4.3.1.

A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 10 lists the results for different proof test intervals considering an average proof test coverage of 95% (see Appendix 1.1).

Table 10: Pulse isolator 9202 – PFD_{AVG} / PFH values

Device variants	PFH [1/h]	T[Proof]	
		1 year	4 years
opto-coupler output	4.09E-08	PFD _{AVG} = 2.96E-04	PFD _{AVG} = 7.90E-04
relay output	5.01E-08	PFD _{AVG} = 3.60E-04	PFD _{AVG} = 9.63E-04

For SIL2 the overall PFD_{AVG} shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 1/h.

As the Pulse isolator 9202 is contributing to the entire safety function, it should only consume a certain percentage of the allowed range. Assuming 10% of this range as a reasonable budget, they should be better than or equal to a PFD_{AVG} value of 1.00E-03 or a PFH value of 1.00E-07 1/h, respectively.

With a proof test interval of one year, the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1:2010 and do fulfill the assumption to not claim more than 10% of the allowed range, i.e. to be better than or equal to 1.00E-03 or 1.00E-07 1/h, respectively.

The resulting PFD(t) / PFD_{AVG} graph generated with exSILentia for a proof test interval of one year is displayed in Figure 2 and Figure 3.

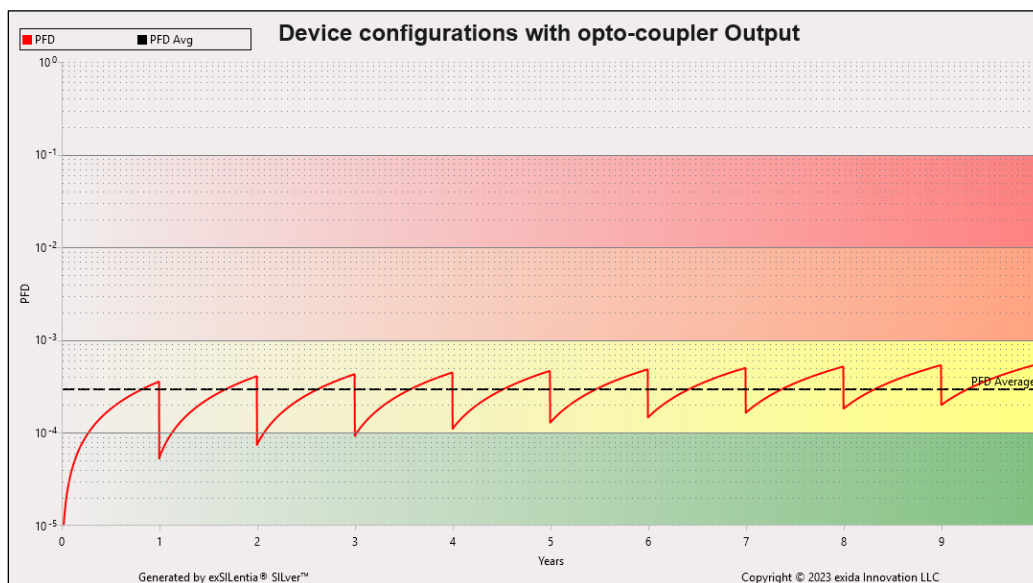


Figure 2: PFD(t) / PFD_{AVG} for the device variants with opto-coupler output

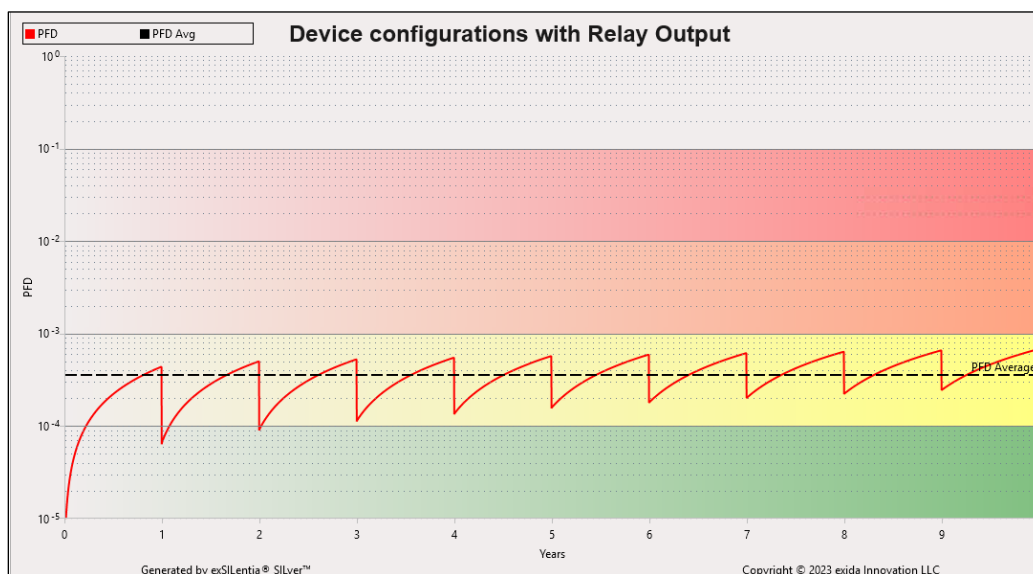


Figure 3: PFD(t) / PFD_{AVG} for the device variants with relay output

6 Terms and Definitions

Internal Diagnostics	Tests performed internally by the device or, if specified, externally by another device without manual intervention.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
DC / DC _{avg}	Diagnostic Coverage of dangerous failures (in %)
FIT	Failure In Time (1×10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.
High demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MTTF _D	Mean Time To dangerous Failure
PFD _{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
PL	Performance Level ISO 13849-1: Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level IEC 61508: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. IEC 62061: discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 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

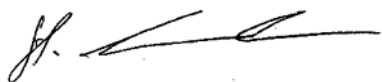
Version History: V3R1: Merged AU and AD failures to general annunciation failures. Those are not part of the analysis; February 1st, 2024
V3R0: Updated to IEC 61508:2010; Route 2H, Includes metrics according to ISO 13849-1; December 22, 2023
V2R0: Non-Ex versions added; July 8, 2014
V1R2: Purpose and 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, Philipp Hanzik

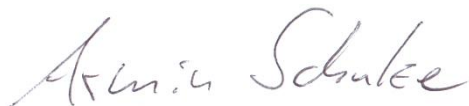
Review: V3R0: Armin Schulze (*exida*); 19.12.2023
V0R2: Hans Jørgen Eriksen (PR electronics A/S); June 5, 2008
V0R1: Audun Opem (*exida*); May 8, 2008

Release status: Released to PR electronics A/S

7.3 Release Signatures

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

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

A handwritten signature in black ink, appearing to read "Armin Schulze", written over a horizontal line.

Dipl.-Ing. (Univ.) Armin Schulze, Safety Engineer

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

According to section 7.4.5.2 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.

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

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.

Appendix 2: Possible proof tests to detect dangerous undetected faults

A possible proof test is described in the safety manual [D10] for the pulse isolator 9202.

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

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2) this only applies provided that the useful lifetime²² of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that the probability 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.

It is the responsibility of the end user to maintain and operate the Pulse isolator 9202 per manufacturer's instructions.

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 11 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Relay RE201 ²³	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.

²² 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.

²³ According to [D11], the test results under the used conditions confirm more switching cycles.

Appendix 4: *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30°C	25°C	25°C	5°C	25°C	25°C
Average Internal Temperature	60°C	30°C	45°C	5°C	45°C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5°C	25°C	25°C	0°C	25°C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5°C	40°C	40°C	2°C	40°C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity²⁴	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock²⁵	10 g	15 g	15 g	15 g	15 g	N/A
Vibration²⁶	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion²⁷	G2	G3	G3	G3	G3	Compatible Material
Surge²⁸						N/A
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility²⁹						N/A
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)³⁰	6kV	6kV	6kV	6kV	6kV	N/A

²⁴ Humidity rating per IEC 60068-2-3

²⁵ Shock rating per IEC 60068-2-27

²⁶ Vibration rating per IEC 60068-2-6

²⁷ Chemical Corrosion rating per ISA 71.04

²⁸ Surge rating per IEC 61000-4-5

²⁹ EMI Susceptibility rating per IEC 6100-4-3

³⁰ ESD (Air) rating per IEC 61000-4-2

Appendix 5: *exida* Route 2_H Criteria

IEC 61508:2010 2nd edition describes the Route 2_H alternative to Route 1_H architectural constraints.

The standard states:

"based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to

- the amount of field feedback; and
- the exercise of **expert judgment**; and when needed
- the undertake of specific tests,

in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508:2010 2nd edition does not give detailed criteria for Route 2_H, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" versus "systematic" are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.