



## **Failure Modes, Effects and Diagnostic Analysis**

Project:  
Pulse Isolator PRecon 5202

Customer:  
PR electronics A/S  
Rønne  
Denmark

Contract No.: PR electronics 05/04-14  
Report No.: PR electronics 05/04-14 R002  
Version V1, Revision R1.1, February 2006  
Audun Opem

## Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the Pulse Isolator PRecon 5202. Table 1 gives an overview of the different types that belong to the considered pulse isolator.

The Pulse Isolator PRecon 5202 is a DIN rail mounted 2-channel pulse isolator with 1 or 2 relay outputs per channel or open NPN collector output. The 2 channels are isolated and independent.

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

**Table 1: Version overview**

PRecon 5202A1	Pulse Isolator, rail mounted, 2-channel, open NPN collector (UL)
PRecon 5202A2	Pulse Isolator, rail mounted, 2-channel, 1 relay per channel (UL)
PRecon 5202A4	Pulse Isolator, rail mounted, 2-channel, 2 relays per channel (UL)
PRecon 5202B1	Pulse Isolator, rail mounted, 2-channel, open NPN collector (ATEX, UL)
PRecon 5202B2	Pulse Isolator, rail mounted, 2-channel, 1 relay per channel (ATEX, UL)
PRecon 5202B4	Pulse Isolator, rail mounted, 2-channel, 2 relays per channel (ATEX, UL)

For safety applications, both the NPN output and the relay outputs were 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 between  $\geq 10^{-3}$  to  $< 10^{-2}$  for SIL 2 safety functions. For systems operating in high demand mode of operation the PFH value has to be  $\geq 10^{-7}$  to  $< 10^{-6}$  for SIL 2 safety functions according to table 3 of IEC 61508-1. 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.

For a SIL 2 application operating in low demand mode the total  $PFD_{AVG}$  value of the SIF should be smaller than 1,00E-02, hence the maximum allowable  $PFD_{AVG}$  value for the sensor part would then be 1,00E-03.

For a SIL 2 application operating in high demand mode the total PFH value of the SIF should be smaller than 1,00E-06 1/h, hence the maximum allowable PFH value for the sensor part would then be 1,00E-07 1/h.

The Pulse Isolator PRecon 5202 is considered to be a Type A<sup>1</sup> component with a hardware fault tolerance of 0.

For type A components with a hardware fault tolerance of 0 the SFF shall be  $> 60\%$  according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

---

<sup>1</sup> Type A component: low complexity E/E/PE safety-related system (not using micro controllers or programmable logic); for details see 7.4.3.1.2 of IEC 61508-2

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

Failure Categories	$l_{sd}$	$l_{su}^2$	$l_{dd}^3$	$l_{du}$	SFF	DC <sub>S</sub>	DC <sub>D</sub>
Pulse Isolator PRecon 5202A/B1	0 FIT	853 FIT	0 FIT	36 FIT	95,95%	0%	5,26%

The PFD<sub>AVG</sub> for the electronics was calculated for three different proof test times using the Markov model as described in Figure 3.

**Table 2: Summary for PRecon 5202A/B1 – PFD<sub>AVG</sub> / PFH values**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 3,58E-08 1/h	PFD <sub>AVG</sub> = 1,57E-04	PFD <sub>AVG</sub> = 7,84E-04	PFD <sub>AVG</sub> = 1,56E-03

Failure Categories	$l_{sd}$	$l_{su}^2$	$l_{dd}^3$	$l_{du}$	SFF	DC <sub>S</sub>	DC <sub>D</sub>
Pulse Isolator PRecon 5202A/B2	0 FIT	820 FIT	0 FIT	32 FIT	96,24%	0%	13,51%

The PFD<sub>AVG</sub> for the electronics was calculated for three different proof test times using the Markov model as described in Figure 3.

**Table 3: Summary for PRecon 5202A/B2 – PFD<sub>AVG</sub> / PFH values**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 3,22E-08 1/h	PFD <sub>AVG</sub> = 1,41E-04	PFD <sub>AVG</sub> = 7,05E-04	PFD <sub>AVG</sub> = 1,41E-03

Failure Categories	$l_{sd}$	$l_{su}^2$	$l_{dd}^3$	$l_{du}$	SFF	DC <sub>S</sub>	DC <sub>D</sub>
Pulse Isolator PRecon 5202A/B4	0 FIT	830 FIT	0 FIT	43 FIT	95,07%	0%	10,41%

The PFD<sub>AVG</sub> for the electronics was calculated for three different proof test times using the Markov model as described in Figure 3.

**Table 4: Summary for PRecon 5202A/B4 – PFD<sub>AVG</sub> / PFH values**

	T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFH = 4,33E-08 1/h	PFD <sub>AVG</sub> = 1,90E-04	PFD <sub>AVG</sub> = 9,48E-04	PFD <sub>AVG</sub> = 1,90E-03

<sup>2</sup> Note that this figure includes failures that do not cause a spurious trip.

<sup>3</sup> The  $\lambda_{dd}$  part is added to the  $\lambda_{safe}$  values as this is not originating from real diagnostics. This figure is the result of dividing between safe (including “No effect”) failures and dangerous failures related to specific failure modes on two components.

The boxes marked in yellow (■) mean that the calculated  $PFD_{AVG}$  / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . The boxes marked in green (■) mean that the calculated  $PFD_{AVG}$  / PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$  respectively  $1,00E-07$ .

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

The failure rates listed above do not include failures resulting from incorrect use of the Pulse Isolator PRecon 5202, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of  $40^{\circ}C$ . For a higher average temperature of  $60^{\circ}C$ , the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the Pulse Isolator PRecon 5202 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 section 5.1 to 5.3 along with all assumptions.

A complete configuration consisting of a Pulse Isolator PRecon 5202 together with a Namur compliant sensor or a mechanical contact becomes a safety input assembly and can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added

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

The failure rates are valid for the useful life of the Pulse Isolator PRecon 5202, which should be limited to 10 years because of the capacitors (see Appendix 2).

## Table of Contents

Management summary .....	2
1 Purpose and Scope.....	6
2 Project management.....	7
2.1 <i>exida.com</i> .....	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 PR electronics A/S .....	8
2.4.2 Documentation generated by <i>exida.com</i> .....	8
3 Description of the analyzed module .....	9
4 Failure Modes, Effects, and Diagnostics Analysis.....	11
4.1 Description of the failure categories .....	11
4.2 Methodology – FMEDA, Failure rates.....	12
4.2.1 FMEDA .....	12
4.2.2 Failure rates .....	12
4.3 Assumptions .....	12
5 Results of the assessment .....	14
5.1 Pulse Isolator PRecon 5202B1.....	15
5.2 Pulse Isolator PRecon 5202B2.....	17
5.3 Pulse Isolator PRecon 5202B4.....	19
5.4 Using the FMEDA results .....	21
6 Terms and Definitions .....	22
7 Status of the document .....	23
7.1 Liability.....	23
7.2 Releases.....	23
7.3 Release Signatures .....	23
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test ..	24
Appendix 1.1: Possible proof tests to detect dangerous undetected faults .....	26
Appendix 2: Impact of lifetime of critical components on the failure rate .....	27

## 1 Purpose and Scope

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

### Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD<sub>AVG</sub>).

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 prior-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD<sub>AVG</sub>). In addition this option consists of an assessment of the prior-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

### Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

### **This assessment shall be done according to option 1.**

This document shall describe the results of the assessment carried out on the Pulse Isolator PRecon 5202. Table 1 gives an overview of the series and explains the differences between the different types.

It shall be assessed whether the transmitter meets the average Probability of Failure on Demand (PFD<sub>AVG</sub>) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508. It **does not** consider any calculations necessary for proving intrinsic safety.

## 2 Project management

### 2.1 exida.com

*exida.com* is one of the world's leading knowledge companies specializing in automation system safety and availability with over 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles of the parties involved

PR electronics A/S                      Manufacturer of the Pulse Isolator PRecon 5202 and performed the FMEDA according to option 1 (see section 1).

*exida.com*                                      Reviewed the FMEDA according to option 1 (see section 1).

PR electronics A/S contracted *exida.com* in October 2005 with the review of the FMEDA and PFD<sub>AVG</sub> calculation of the above mentioned devices.

### 2.3 Standards / Literature used

The services delivered by *exida.com* were performed based on the following standards / literature.

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N3]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N4]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions
[N5]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N6]	SN 29500	Failure rates of components
[N7]	NSWC-98/LE1	Handbook of Reliability Prediction Procedures for Mechanical Equipment
[N8]	IEC 60654-1: 1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

## 2.4 Reference documents

### 2.4.1 Documentation provided by PR electronics A/S

[D1]	5202BY107-UK (0347) Pulse Isolator PRecon 5202B	Data sheet
[D2]	5202BV Pulse Isolator PRecon 5202B	Users Manual
[D3]	5202-1006 of 12.06.2001	Circuit diagram "5202B1/2 2-relay version, NPN output"
[D4]	5202-1101 of 12.06.2001	Circuit diagram "5202B4 4-relay" version
[D5]	5202SMD1 version 2002 dated 06/06-05	Parts list – NPN output (SMD-level)
[D6]	5202SMD2 version 2002 dated 06/06-05	Parts list – 2 relay output (SMD-level)
[D7]	5202SMDB4 version 2006 dated 06/06-05	Parts list – 4 relay output (SMD-level)
[D8]	5202-1 version 2024 dated 10/01-05	Parts list – NPN output (leaded level)
[D9]	5202-2 version 2022 dated 10/01-05	Parts list – 2 relay output (leaded level)
[D10]	5202-4 version 2014 dated 19/09-05	Parts list – 4 relay output (leaded level)

### 2.4.2 Documentation generated by exida.com

[R1]	5202B1 FMEDA final (FMEDA)
[R2]	5202B2 FMEDA final (FMEDA)
[R3]	5202B4 FMEDA final (FMEDA)



### 3 Description of the analyzed module

The Pulse Isolator PRecon 5202B is a galvanically isolated safety barrier for the

- Supply of Namur sensors installed in hazardous area;
- Detection of mechanical contacts installed in hazardous areas.

The Pulse Isolator PRecon 5202A is a non-Ex version of the 5202B.

The devices are used in many different industries for both control and safety applications.

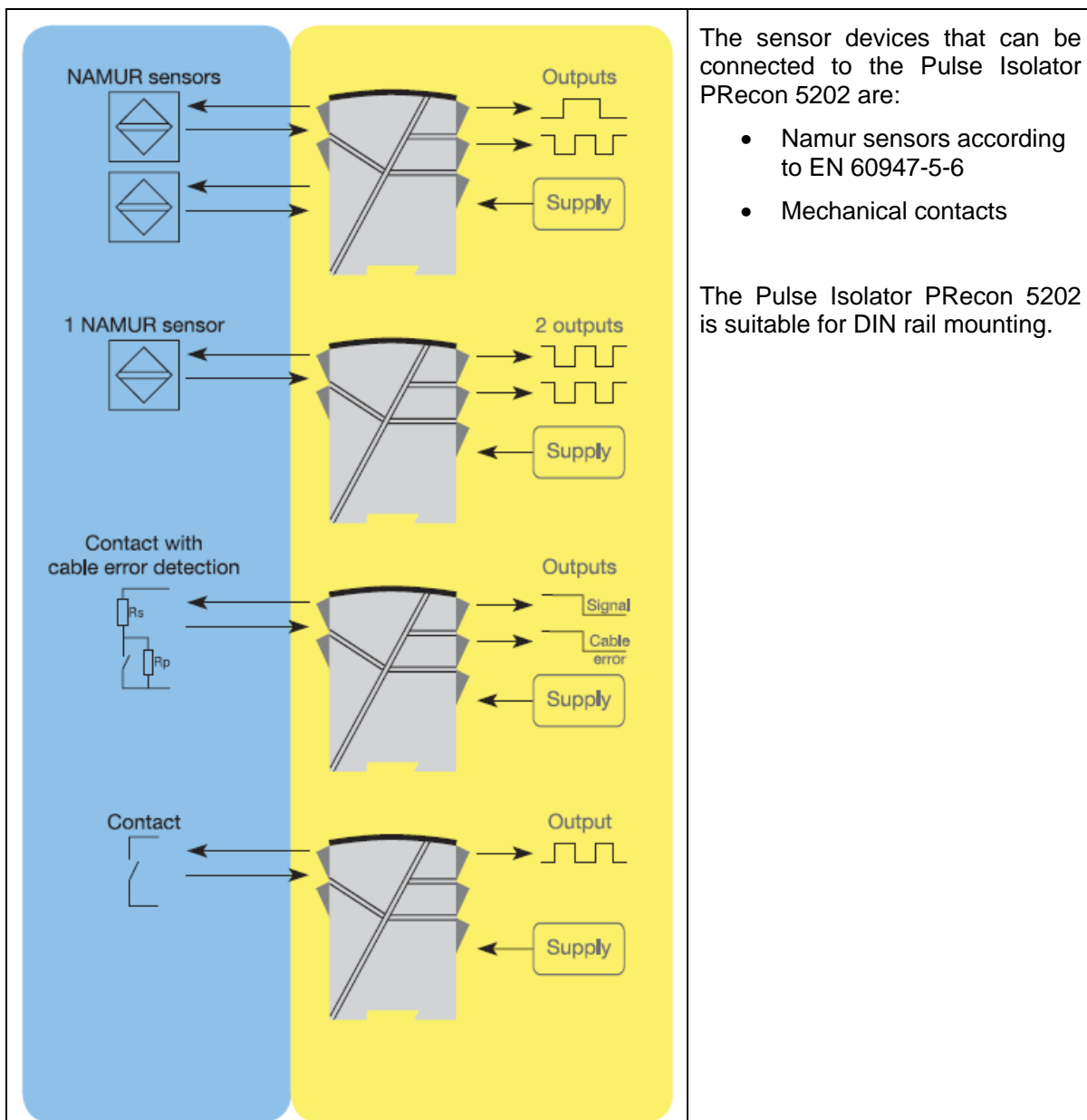


**Figure 1 Pulse Isolator PRecon 5202B**

Configuration of Pulse Isolator PRecon 5202 is performed by the jumpers that are physically located inside the housing.

The Pulse Isolator PRecon 5202 is considered to be a Type A component with a hardware fault tolerance of 0.

The isolator operates with a 2-wire system with different connections depending on the sensor device. The inputs, outputs and the supply are floating and galvanically separated.



The sensor devices that can be connected to the Pulse Isolator PRecon 5202 are:

- Namur sensors according to EN 60947-5-6
- Mechanical contacts

The Pulse Isolator PRecon 5202 is suitable for DIN rail mounting.

**Figure 2: Input configurations with Pulse Isolator PRecon 5202**

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by PR electronics A/S and reviewed by *exida.com*. The results are documented in [R1], [R2] and [R3]. 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. This was then indicated in the FMEDA effects with a (TEST).

This resulted in failures that 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 Pulse Isolator PRecon 5202, 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	A dangerous failure (D) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or where the output does not follow the state of the input.
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).
Fail No Effect	Failure of a component that is part of the safety function but 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 failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. The “No Effect” and “Annunciation Undetected” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the “No Effect” and “Annunciation Undetected” failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

## 4.2 Methodology – FMEDA, Failure rates

### 4.2.1 FMEDA

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

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.com* 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 PRecon 5202:

- 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.
- The repair time after a safe failure is 8 hours.
- The test time of the logic solver to react on a dangerous detected failure is 1 hour.
- 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 40°C. Humidity levels are assumed within manufacturer's rating.
- All modules are suitable for high demand mode of operation.
- The safety function is carried out via 1 input and 1 output channel.
- Both the relay output and the NPN output may be used for safety applications.
- External power supply failure rates are not included.
- The Pulse Isolator PRecon 5202 is a digital device that shall drive the output in the same state as the input. Any deviation of the state of the output compared to the state of the input is considered as a dangerous. The minor delay caused by the relay is not assumed.
- The Pulse Isolator PRecon 5202 is connected to a safety PLC input module that is capable of handling the maximum frequency of the used output configuration:
  - Relay output – 20 Hz
  - NPN output – 5 kHz
- Minimum pulse length of 0.1 ms

## 5 Results of the assessment

exida.com reviewed the FMEDAs performed by PR electronics A/S.

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

$\lambda_{total}$  consists of the sum of all component failure rates. This means:

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

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

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

For the calculation of the  $PFD_{AVG}$  the following Markov model for a 1oo1D system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

The proof test time was changed using the Microsoft® Excel 2000 based FMEDA tool of exida.com as a simulation tool. The results are documented in the following sections.

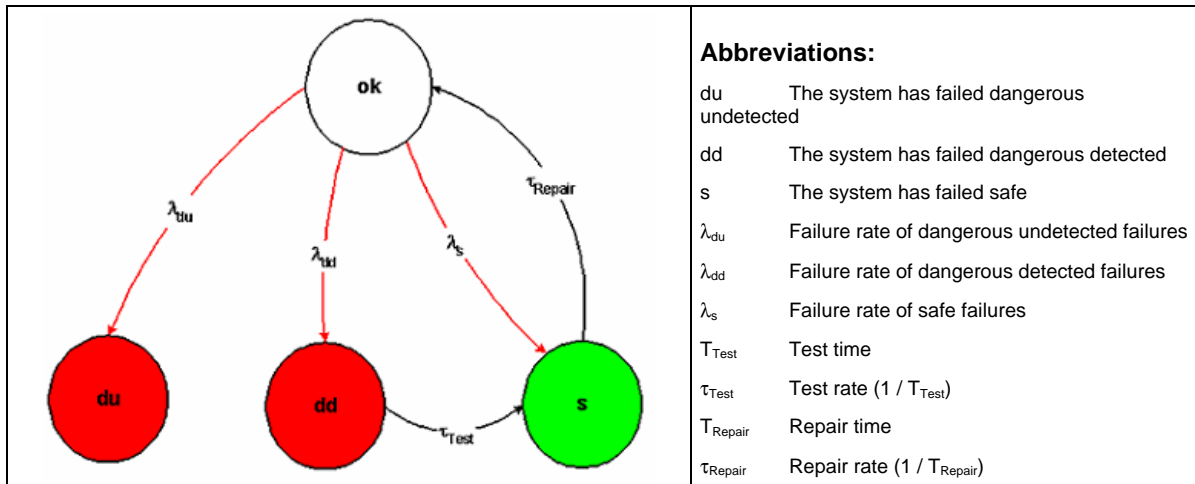


Figure 3: Markov model for a 1oo1D structure

## 5.1 Pulse Isolator PRecon 5202A/B1

The FMEDA carried out on the Pulse Isolator PRecon 5202A/B1 leads under the assumptions described in section 4.3 to the following failure rates:

$\lambda_{su} =$	4,73E-07 1/h
$\lambda_{dd} =$	2,20E-09 1/h
$\lambda_{du} =$	3,58E-08 1/h
$\lambda_{no\ effect} =$	3,78E-07 1/h
$\lambda_{annunciation} =$	3,40E-10 1/h
$\lambda_{total} =$	8,90E-07 1/h
$\lambda_{not\ part} =$	2,15E-07 1/h

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not\ part}) + 8\ h = 103\ years$$

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

Failure Categories	$l_{sd}$	$l_{su}^{2\ above}$	$l_{dd}^{3\ above}$	$l_{du}$	SFF	DC <sub>S</sub>	DC <sub>D</sub>
Pulse Isolator PRecon 5202A/B1	0 FIT	853 FIT	0 FIT	36 FIT	95,95%	0%	5,26%

The  $PFD_{AVG}$  for the electronic part 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
PFH = 3,58E-08 1/h	PFD <sub>AVG</sub> = 1,57E-04	PFD <sub>AVG</sub> = 7,84E-04	PFD <sub>AVG</sub> = 1,56E-03

The boxes marked in yellow (■) mean that the calculated  $PFD_{AVG}$  and PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (■) mean that the calculated  $PFD_{AVG}$  and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 respectively 1,00E-7 1/h. Figure 4 shows the time dependent curve of  $PFD_{AVG}$ .

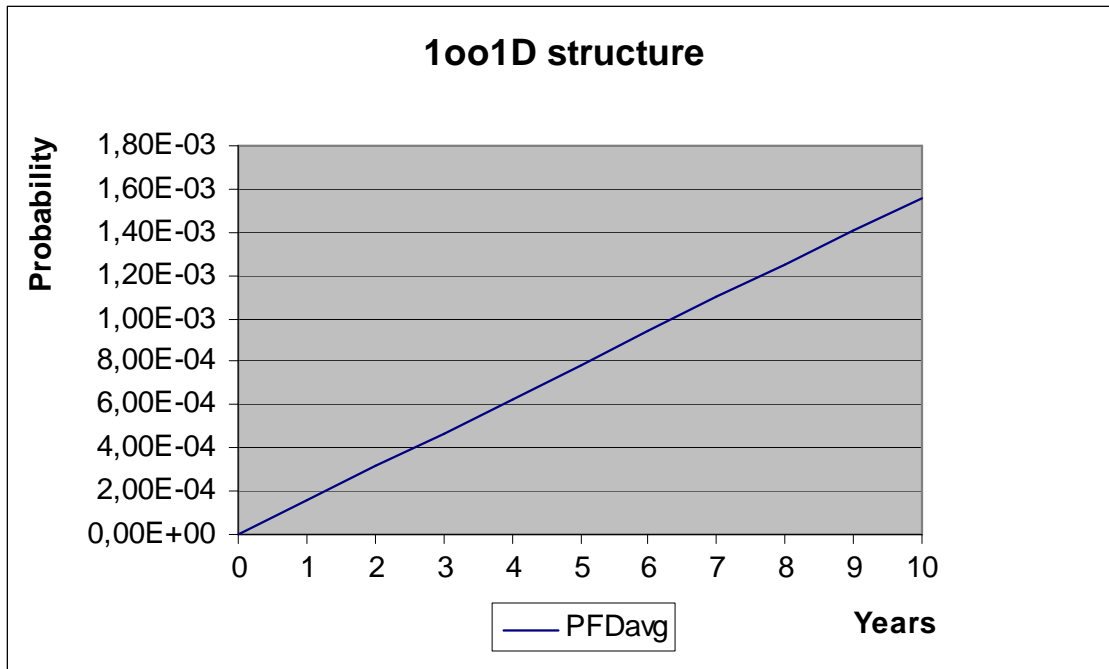


Figure 4: PFD<sub>AVG</sub>(t) 5202A/B1



## 5.2 Pulse Isolator PRecon 5202A/B2

The FMEDA carried out on the Pulse Isolator PRecon 5202A/B2 leads under the assumptions described in section 4.3 to the following failure rates:

$\lambda_{su} =$	4,64E-07 1/h
$\lambda_{dd} =$	4,75E-09 1/h
$\lambda_{du} =$	3,22E-08 1/h
$\lambda_{no\ effect} =$	3,40E-07 1/h
$\lambda_{annunciation} =$	1,11E-08 1/h
$\lambda_{total} =$	8,51E-07 1/h
$\lambda_{not\ part} =$	1,70E-07 1/h

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not\ part}) + 8\ h = 112\ years$$

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

Failure Categories	$l_{sd}$	$l_{su}^{2\ above}$	$l_{dd}^{3\ above}$	$l_{du}$	SFF	DC <sub>S</sub>	DC <sub>D</sub>
Pulse Isolator PRecon 5202A/B2	0 FIT	820 FIT	0 FIT	32 FIT	96,24%	0%	13,51%

The PFD<sub>AVG</sub> for the electronic part 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
PFH = 3,22E-08 1/h	PFD <sub>AVG</sub> = 1,41E-04	PFD <sub>AVG</sub> = 7,05E-04	PFD <sub>AVG</sub> = 1,41E-03

The boxes marked in yellow (■) mean that the calculated PFD<sub>AVG</sub> and PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (■) mean that the calculated PFD<sub>AVG</sub> and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 respectively 1,00E-7 1/h. Figure 5 shows the time dependent curve of PFD<sub>AVG</sub>.

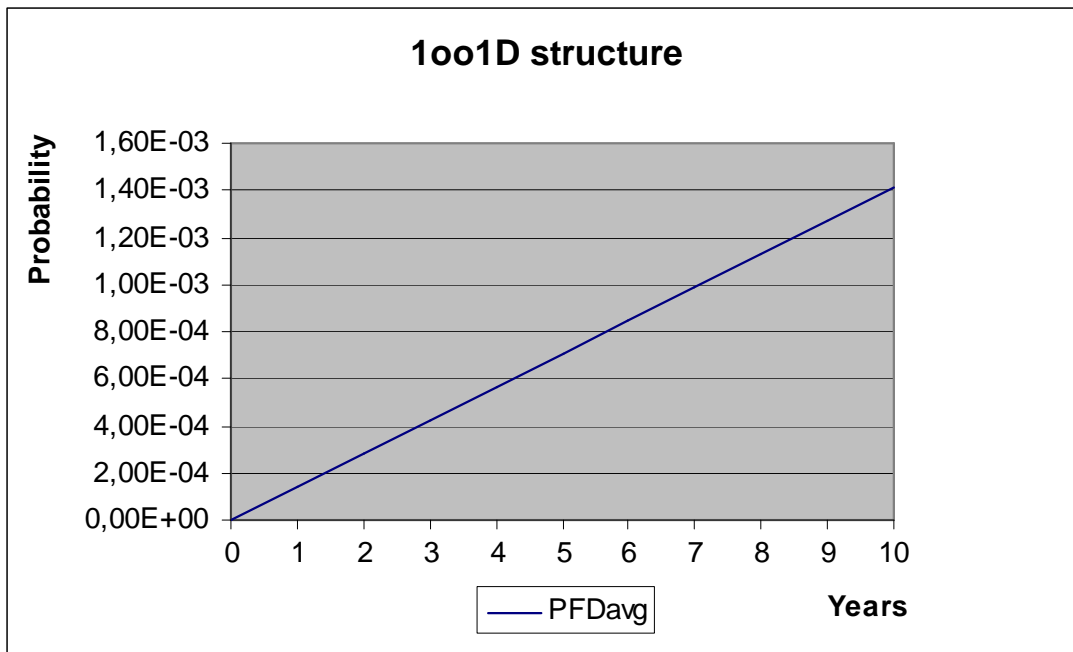


Figure 5: PFD<sub>AVG</sub>(t) 5202A/B2

### 5.3 Pulse Isolator PRecon 5202A/B4

The FMEDA carried out on the Pulse Isolator PRecon 5202A/B4 leads under the assumptions described in section 4.3 to the following failure rates:

$\lambda_{su} =$	4,72E-07 1/h
$\lambda_{dd} =$	4,75E-09 1/h
$\lambda_{du} =$	4,33E-08 1/h
$\lambda_{no\ effect} =$	3,42E-07 1/h
$\lambda_{annunciation} =$	1,11E-08 1/h
$\lambda_{total} =$	8,73E-07 1/h
$\lambda_{not\ part} =$	1,93E-07 1/h

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not\ part}) + 8\ h = 107\ years$$

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

Failure Categories	$l_{sd}$	$l_{su}^{2\ above}$	$l_{dd}^{3\ above}$	$l_{du}$	SFF	DC <sub>S</sub>	DC <sub>D</sub>
Pulse Isolator PRecon 5202A/B4	0 FIT	830 FIT	0 FIT	43 FIT	95,07%	0%	10,41%

The PFD<sub>AVG</sub> for the electronic part 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
PFH = 4,33E-08 1/h	PFD <sub>AVG</sub> = 1,90E-04	PFD <sub>AVG</sub> = 9,48E-04	PFD <sub>AVG</sub> = 1,90E-03

The boxes marked in yellow (■) mean that the calculated PFD<sub>AVG</sub> and PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03. The boxes marked in green (■) mean that the calculated PFD<sub>AVG</sub> and PFH values are within the allowed range for SIL 2 according to table 2 / 3 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 1,00E-03 respectively 1,00E-7 1/h. Figure 6 shows the time dependent curve of PFD<sub>AVG</sub>.

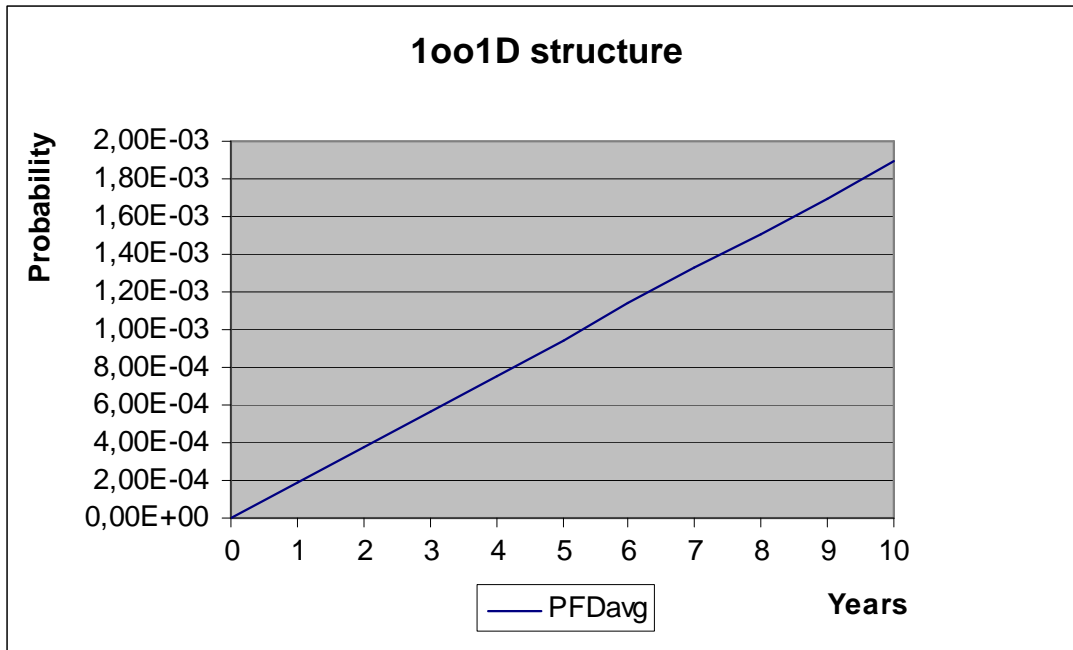


Figure 6: PFD<sub>AVG</sub>(t) 5202A/B4

#### 5.4 Using the FMEDA results

The Pulse Isolator PRecon 5202 together with a Namur compliant sensor according to EN 60947-5-6 or a mechanical contact becomes a safety input assembly as indicated in Figure 2. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the sensor or the mechanical contact must also be considered.

## 6 Terms and Definitions

DC <sub>S</sub>	Diagnostic Coverage of safe failures ( $DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$ )
DC <sub>D</sub>	Diagnostic Coverage of dangerous failures ( $DC_D = \lambda_{dd} / (\lambda_{dd} + \lambda_{du})$ )
FIT	Failure In Time ( $1 \times 10^{-9}$ 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 one per year or 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 one per year and no greater than twice the proof test frequency.
PFD <sub>AVG</sub>	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
SIS	Safety Instrumented System
Type A component	Low complexity E/E/PE safety-related system (not using micro controllers or programmable logic); for details see 7.4.3.1.2 of IEC 61508-2.
T[Proof]	Proof Test Interval

## 7 Status of the document

### 7.1 Liability

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

### 7.2 Releases

Version: V1  
Revision: R1.1  
Version History: V0, R1.0: Initial version; December 12, 2005  
V1, R1.0: Updated after review; December 19, 2005  
V1, R1.1; Updated after review, added PRecon 5202A series,  
February 03, 2006  
Authors: Audun Opem  
Review: V0, R1.0: Rachel van Beurden-Amkreutz  
V1, R1.0 Hans Jørgen Eriksen, PR electronics A/S

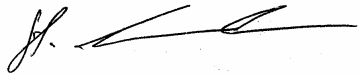
Release status: Released to PR electronics A/S

### 7.3 Release Signatures



---

Audun Opem, Senior Project Manager



---

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

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

Appendix 1 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 5, Table 6 and Table 7 shows an importance analysis of the ten most critical dangerous undetected faults and indicates how these faults can be detected during proof testing

**Table 5: Importance Analysis of “du” failures for 5202A/B1 – NPN output**

Component	% of total $I_{du}$	Detection through
Z106	18,60 %	100% functional test with different expected output signals over the entire range
T1	13,99 %	100% functional test with different expected output signals over the entire range
T7	13,99 %	100% functional test with different expected output signals over the entire range
IC101	7,55 %	100% functional test with different expected output signals over the entire range
SI102	6,99 %	100% functional test with different expected output signals over the entire range
T103	6,99 %	100% functional test with different expected output signals over the entire range
IC5	2,80 %	100% functional test with different expected output signals over the entire range
IC3	2,80 %	100% functional test with different expected output signals over the entire range
IC102	2,80 %	100% functional test with different expected output signals over the entire range
D10	1,68 %	100% functional test with different expected output signals over the entire range

**Table 6: Importance Analysis of “du” failures for 5202A/B2 – 1 relay per channel**

Component	% of total $I_{du}$	Detection through
RE101	34,14 %	100% functional test with different expected output signals over the entire range
T7	15,55 %	100% functional test with different expected output signals over the entire range
IC101	8,38 %	100% functional test with different expected output signals over the entire range



T1	7,78 %	100% functional test with different expected output signals over the entire range
T102	7,76 %	100% functional test with different expected output signals over the entire range
IC5	3,11 %	100% functional test with different expected output signals over the entire range
IC3	3,11 %	100% functional test with different expected output signals over the entire range
D10	1,87 %	100% functional test with different expected output signals over the entire range
T2	1,56 %	100% functional test with different expected output signals over the entire range
T3	1,56 %	100% functional test with different expected output signals over the entire range

**Table 7: Importance Analysis of “du” failures for 5202A/B4 – 2 relays per channel**

Component	% of total $I_{du}$	Detection through
RE101, RE102	50,83 %	100% functional test with different expected output signals over the entire range
T7	15,55 %	100% functional test with different expected output signals over the entire range
T1	7,78 %	100% functional test with different expected output signals over the entire range
IC101	6,24 %	100% functional test with different expected output signals over the entire range
T102	5,78 %	100% functional test with different expected output signals over the entire range
IC5	3,11 %	100% functional test with different expected output signals over the entire range
IC3	3,11 %	100% functional test with different expected output signals over the entire range
D10	1,87 %	100% functional test with different expected output signals over the entire range
T2	1,56 %	100% functional test with different expected output signals over the entire range
T3	1,56 %	100% functional test with different expected output signals over the entire range

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

A possible proof test consists of the following steps, as described in Table 8.

**Table 8 Steps for Proof Test 1**

Step	Action
------	--------

1	Take appropriate action to avoid a false trip.
2	Provide a selection of appropriate input signals to the Pulse Isolator PRecon 5202 covering the used range of the connected NAMUR sensor / mechanical contact and verify the correct switching of the output.
3	Restore the loop to full operation.
4	Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect approximately 90% of possible “du” failures in the device.

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the  $PFD_{AVG}$  calculation is only valid for components that 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 9 shows which electrolytic capacitors are contributing to the dangerous failure rate and therefore to the  $PFD_{AVG}$  calculation and what their estimated useful lifetime is.

**Table 9 Useful lifetime of electrolytic capacitors contributing to  $l_{du}$**

Type	Name	Schematic	Useful life at 40 °C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	C9	5202-1006 sheet 2 of 4 5202-1101 sheet 2 of 4	Approx. 500 000 hours
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	C101	5202-1006 sheet 3 of 4 5202-1101 sheet 3 of 4	Approx. 500 000 hours
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	C201	5202-1006 sheet 4 of 4 5202-1101 sheet 4 of 4	Approx. 500 000 hours
Capacitor (electrolytic) - Aluminium electrolytic, non solid electrolyte	C2, C3, C4, C12, C13	5202-1006 sheet 2 of 4 5202-1101 sheet 2 of 4	Approx. 90 000 hours <sup>4</sup>
Relay	RE101	5202-1006 sheet 3 of 4	6.000 switching cycles
Relay	RE201	5202-1006 sheet 4 of 4	6.000 switching cycles
Relay	RE102	5202-1101 sheet 3 of 4	6.000 switching cycles
Relay	RE202	5202-1101 sheet 4 of 4	6.000 switching cycles

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. The limiting factors with regard to the useful lifetime of the system are the aluminum electrolytic capacitors and the relays. The aluminum electrolytic capacitors have an estimated useful lifetime of about 10 years.

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 for low demand mode applications. For high demand mode applications the relays can be a limiting factor and have to be considered in the useful lifetime assumption.

<sup>4</sup> The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperature follows “The Doubling 10°C Rule” where life is doubled for each 10°C reduction in the operating temperature.