



Failure Modes, Effects and Diagnostic Analysis

Project:

4179B universal trip amplifier

Customer:

PR electronics A/S

Rønde

Denmark

Contract No.: PR Q24/02-170R1

Report No.: PR electronics 24/02-170R1 R034

Version V1, Revision R3; October, 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 4179B universal trip amplifier with hardware version 4179-2-V2R0 and software versions as shown in Table 1 below.

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 Safe Failure Fraction (SFF) can be calculated for a subsystem.

The FMEDA that is described in this report concerns only the hardware of the 4179B universal trip amplifier. For full assessment purposes all requirements of IEC 61508 or ISO 13849 must be considered.

Table 1: Overview of the considered Product

Description	Name	Software version	
		Input CPU	Output CPU
DIN rail mounted universal trip amplifier with current or voltage input and two relay outputs, Normally Open contacts	4179B	V1R0	V4R0

It is only allowed to operate one output relay in a Safety Instrumented Function (SIF). This use case is covered by the FMEDA. It is forbidden to use the other relay in a different SIF.

For safety applications only the described device with the listed hardware and software versions of the 4179B universal trip amplifier have been considered. Any other variant is not covered by this report. As a constraint for the configuration please note the following:

The input must always be configured for positive signals and the measurement range must be offset by at least 5% of configured maximum to enable the detection of a short circuit at the input side.

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N3]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N4]).

The failure rates are valid for the useful life of the 4179B universal trip amplifier (see Appendix A) when operating as defined in the considered scenarios.

The 4179B universal trip amplifier can be considered as a Type B ¹ element with a hardware fault tolerance (HFT) of 0.

The following table shows how the above stated requirements are fulfilled.

¹ Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

Table 2: Summary for 4179B universal trip amplifier – IEC 61508 failure rates

SN 29500 Tamb = 40°C	
Failure category	Failure rates (in FIT)
Safe (λ_S)	249
Dangerous Detected (λ_{DD})	261
Dangerous Undetected (λ_{DU})	54
Diagnostic Faults (λ_{DIAG})	8
Safety Related (λ_{SR})	572
SFF ²	90%
SIL AC ³	SIL 2

Table 3: Safety metrics according to ISO 13849-1

MTTF _D (years)	362 (High)
DC _{avg}	82 % (Low)
Average frequency of a dangerous failure per hour (PFH) ⁴	5.43E-08 1/h
Performance Level (PL) ⁵	d

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

² The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

³ 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. In addition, it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

⁴ The PFH value of 5.43E-08 1/h 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.

⁵ 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	5
2 Project management	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved	6
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
3 Product Description	9
4 Architectural Constraints.....	10
5 Failure Modes, Effects, and Diagnostic Analysis	11
5.1 Failure categories description	11
5.2 Methodology – FMEDA, Failure rates.....	12
5.2.1 FMEDA	12
5.2.2 Failure rates.....	12
5.2.3 Assumptions	13
5.2.4 Restrictions	14
5.3 FMEDA Results	15
5.3.1 4179B with voltage input and two output relays	16
6 Using the FMEDA results	18
6.1 Example PFD _{AVG} / PFH calculation.....	19
7 Terms and Definitions.....	20
8 Status of the document.....	21
8.1 Liability.....	21
8.2 Releases.....	22
8.3 Release Signatures	22
Appendix A: Impact of lifetime of critical components on the failure rate	23
Appendix B: Proof tests to detect dangerous undetected faults	24

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the 4179B universal trip amplifier with hardware version 4179-2-V2R0 and software versions as described in Table 1.

The FMEDA builds the basis for an evaluation whether a sensor / logic / final-element, including the product, meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per hour (PFH) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511 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 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508 or ISO 13849.

2.2 Roles of the parties involved

PR electronics A/S	Manufacturer of the 4179B universal trip amplifier. PR electronics A/S performed the FMEDA of the device under consideration.
--------------------	---

<i>exida</i>	Reviewed the original FMEDA from PR electronics A/S and created the appropriate FMEDA report (this document).
--------------	---

PR electronics A/S contracted *exida* in February 2024 with the FMEDA review and the creation of an FMEDA report for the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	ISO 13849-1:2023	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
[N3]	Component Reliability Database Handbook, 4th Edition Vol. 1 – Electrical Components	exida LLC, Component Reliability Database Handbook, 4th Edition Vol. 1 – Electrical Components
[N4]	SN 29500-1:01.2004 SN 29500-1 H1:07.2013 SN 29500-2:09.2010 SN 29500-3:06.2009 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 29500-11:07.2013 SN 29500-12:02.2008 SN 29500-15:07.2009 SN 29500-16:08.2010	Siemens standard with failure rates for components

2.4 exida tools used

[T1]	SILcal X 1.4.3	FMEDA Tool
[T2]	exSILentia V4.13.0	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	4179B V1R6.3fmx of 14.10.24	SILcal X FMEDA project file V1R6
[D2]	4179B FMEDA appendix.pdf of 26.02.24	FMEDA appendix for [D1] V0R1
[D3]	4179B Microcontrollers.pdf of 19.04.24	Overview of implemented safety measures for the input CPU and the output CPU Rev. V0R4
[D4]	4179B60xx Firmware Design Specification.pdf of 02.10.24	4179B60XX Firmware Design Specification V1R0
[D5]	417963xx Firmware Design Specification.pdf of 28.07.17	417963xx Firmware Design Specification V2R0
[D6]	4179B HW Design Description.pdf of 13.08.24	4179B HW Design Description V1R3
[D7]	4179B Hardware Fault Insertion Test Report.pdf of 26.02.24	4179B Hardware Fault Insertion Test Report V1R0
[D8]	4179B Product description.pdf of 26.02.24	4179B Product description V0R1
[D9]	Difference between 4179 and 4179B.pdf of 01.11.23	Difference between 4179 and 4179B V0R1
[D10]	4179-2-02-PDF.pdf of 12.07.24	Schematic for device 4179B Rev. 4179-2-02
[D11]	4179SMDB_2003.pdf of 27.09.24	BOM for SMD electronic parts Rev. 4179SMDB_2003
[D12]	4179LB_2002.pdf of 12.07.24	BOM for leaded electronic parts Rev. 4179LB_2004

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

3 Product Description

The 4179B universal trip amplifier is an isolated, DIN rail mounted, universal input/output device. It measures AC-signals and converts them into process control signals with two pairs of potential-free relay contacts which can be configured to suit any application. The trip amplifier with window function allows the relay to change state within high and a low setpoint on the input span. The input can be configured for non-standard custom input range, for both voltage and current inputs.

Using the detachable display fronts, the 4179B can be configured for current or voltage input in a wide range. Furthermore, the display enables online monitoring of process and output signals.

The detachable display is optional and therefore, it is not considered by the FMEDA.

Figure 1 shows the block diagram of the 4179B.

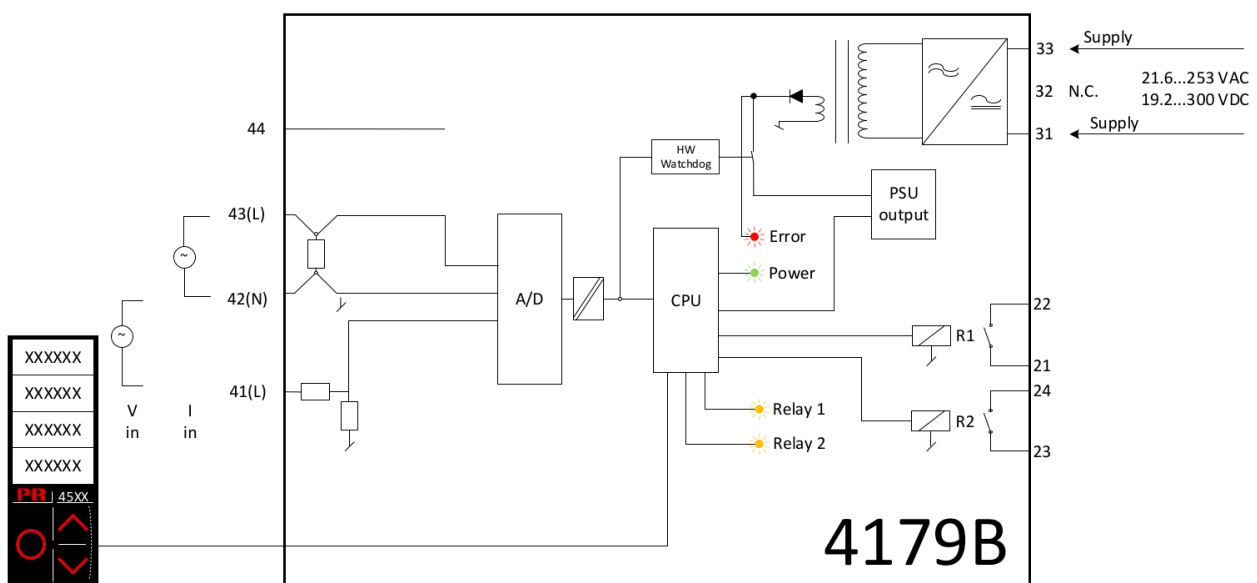


Figure 1: Block diagram for the 4179B universal trip amplifier

Meaning of the status LEDs:

- Green flashing LED 13 Hz indicates normal operation.
- Steady green LED indicates internal error.
- Steady red LED indicates fatal error.
- Yellow LED indicates that relay 1/2 is energized.

The following function is considered as the safety function performed by the 4179B universal trip amplifier:

Safety Function: Input signal observation

In case the input signal is out of the user configured range, the output relay will be de-energized.

4 Architectural Constraints

The architectural constraint type for the 4179B universal trip amplifier 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 the 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 1_H approach.

As the 4179B universal trip amplifier 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 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by PR electronics A/S and is documented in [D1]. *exida* reviewed the FMEDA.

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 [D7]). This resulted in failures that can be classified according to the following failure categories.

5.1 Failure categories description

In order to judge the failure behavior of the 4179B universal trip amplifier, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output relay is de-energized.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: <ul style="list-style-type: none">a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or,b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: <ul style="list-style-type: none">a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,b) decreases the probability that the safety function operates correctly when required.
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 and causes the device to go to the fail-safe state.
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 and does not corrupt the measured input value by more than the user-specified accuracy range.
Diagnostic Failure	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 Part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

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

5.2 Methodology – FMEDA, Failure rates

5.2.1 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) 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.

5.2.2 Failure rates

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N3]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N4]).

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.

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. 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.

Accurate plant specific data may be used for this purpose. 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.

5.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 4179B universal trip amplifier.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. For higher average temperatures, the failure rates should be multiplied with an experience based factor of e.g. 1.5 for 50°C, 2.5 for 60°C and 5 for 80°C.
- 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 measurement / application limits (including pressure and temperature ranges) are considered.
- Materials are compatible with process conditions.
- The device is installed per manufacturer's instructions.
- The correct parameterization is verified by the user.
- Failures during parameterization are not considered.
- The device is locked against unintended operation/modification.
- The two relay outputs are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.
- The two relay outputs are not used for the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components.
- Only one input and one output are part of the safety function. Signal doubling is not used.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The input must always be configured for positive signals and the measurement range must be offset by at least 5% of configured maximum to enable the detection of a short circuit at the input side.
- The worst-case internal fault detection time is 40 seconds. Therefore, a demand for the safety function in high demand mode is only possible every 4000 seconds⁶, which corresponds to 67 minutes.
- All components that are not part of the safety function (e.g. optional displays) and cannot influence the safety function (feedback immune) are excluded.
- External power supply failure rates are not included.

⁶ See IEC 61508-2:2010, paragraph 7.4.4.1.4 and ISO 13849-1:2023, paragraph 6.1.3.2.4

5.2.4 Restrictions

For safety applications the following limitations apply to the configuration and usage of the product:

- Only one output can be used for safety per product.
- Relay configured for 'normally open'. De-energized (open) is assumed to indicate error and must be implemented as safe state.

5.3 FMEDA Results

For the calculations the following has to be noted:

$$\lambda_{SR} = \lambda_S + \lambda_{DD} + \lambda_{DU} + \lambda_{DIAG}$$

IEC 61508:

$$SFF = (\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$$

ISO 13849-1:

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

$$PFH = \lambda_{DU}$$

$$DC_{avg} = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$$

5.3.1 4179B with voltage input and two output relays

The FMEDA carried out on the 4179B, under the assumptions described in section 5.2.3 and the definitions given in section 5.1 and 5.2 leads to the following failure rates:

	SN 29500 Tamb = 40°C
Failure category	Failure rates (in FIT)
Safe (λ_S)	249
Dangerous Detected (λ_{DD})	261
Dangerous Undetected (λ_{DU})	54
Diagnostics (λ_{DIAG})	8
Diagnostic detected ($\lambda_{DIAG,D}$)	5
Diagnostic undetected ($\lambda_{DIAG,U}$)	3
No effect (λ_{NE})	254
No part (λ_{NP})	166
Safety Related (λ_{SR})	572
SFF ⁷	90%
SIL AC ⁸	SIL 2

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

⁷ The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁸ 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. In addition, it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.

Safety metrics according to ISO 13849-1

MTTF_D (years)	362 (High)
DC_{avg}	82 % (Low)
Average frequency of a dangerous failure per hour (PFH)⁹	5.43E-08 1/h
Performance Level (PL)¹⁰	d

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

⁹ The PFH value of 5.43E-08 1/h 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.

¹⁰ 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.

6 Using the FMEDA results

Using the failure rate data given in section 5.3.1 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 4179B is listed in Appendix B. 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 4179B universal trip amplifier 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.

6.1 Example PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 4179B universal trip amplifier with *exida's* exSILentia tool. The failure rate data used in this calculation are given in section 5.3.

A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 4 shows the results for different proof test intervals considering an average proof test coverage of 95% (see Appendix B).

Table 4: 4179B universal trip amplifier – PFD_{AVG} / PFH values

PFH [1/h]	T[Proof]	
	1 year	5 years
5.43E-08	PFD _{AVG} = 3.96E-04	PFD _{AVG} = 1.37E-03

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 4179B universal trip amplifier 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.

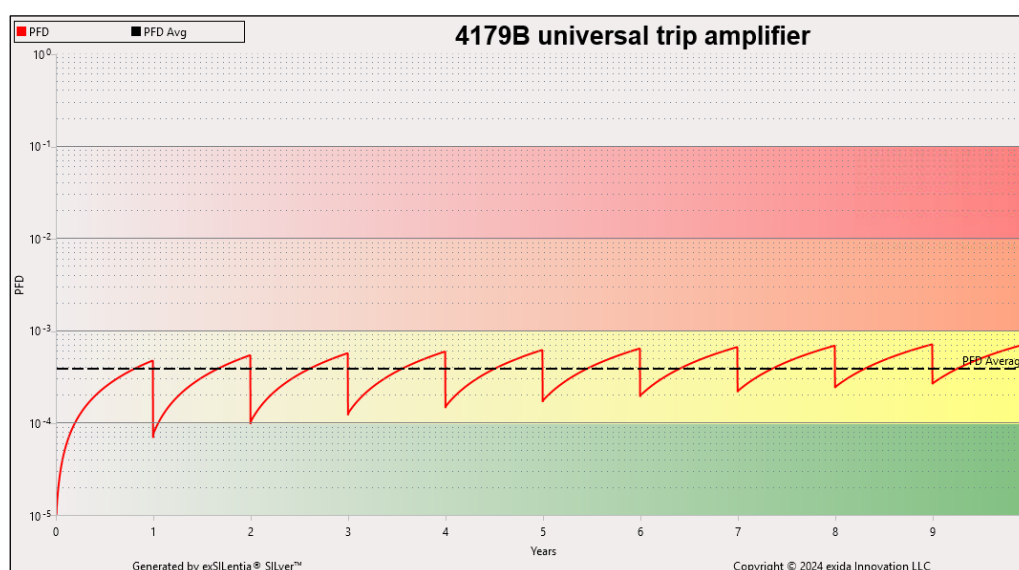


Figure 2: PFD(t) / PFD_{AVG}

7 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

8 Status of the document

8.1 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.

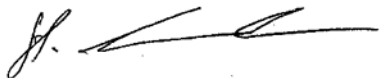
Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification, you may wish to contact the product vendor to verify the current validity of the results.

8.2 Releases

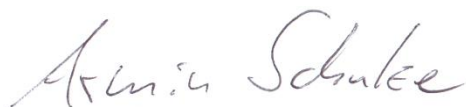
Version History:	V1R3:	Corrected product version in FMEDA report Updated all affected documents in the input document list 2.5.1 according to the updated FMEDA: [D4] / [D6] / [D10] / [D11] / [D12]; October 21, 2024
	V1R2:	Updated FMEDA results in Table 2, Table 3 and in chapter 5.3.1 according to new FMEDA project file [D1] after EMC optimization, changed output CPU software version in Table 1 from V5R0 to V4R0 as requested by PR; October 18, 2024
	V1R1:	Review comments from PR implemented; May 07, 2024
	V1R0:	Review comments from <i>exida</i> implemented; April 26, 2024
	V0R1:	Initial version; April 11, 2024
Authors:	V0R1 to : V1R3	Armin Schulze
Review:	V1R2:	Stephan Aschenbrenner (<i>exida</i>); October 16, 2024 Andreas Essemann (PR); October 18, 2024
	V1R0:	Andreas Essemann (PR); May 06, 2024
	V0R1:	Stephan Aschenbrenner (<i>exida</i>); April 25, 2024

Release status: Released to PR electronics A/S

8.3 Release Signatures



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



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

Appendix A: 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 5.2) this only applies provided that the useful lifetime¹¹ 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 4179B universal trip amplifier per manufacturer's instructions.

Note 3 in IEC 61508-2 states that experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

Table 5 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 5: Components with reduced useful lifetime

Type	Name	Useful lifetime
Relay	RE201, RE202	Approximately 100.000 switching cycles

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relays do not have a real impact on the useful lifetime.

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

¹¹ 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.

Appendix B: Proof tests to detect dangerous undetected faults

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.

A suggested proof test consists of the following steps, as described in Table 6.

Table 6: Suggested proof test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Provide an appropriate input signal to the 4179B which represents a measurement value at the lower limit of the configured range and verify the expected reaction of the output relays.
3	Provide an appropriate input signal to the 4179B which represents a measurement value at the higher limit of the configured range and verify the expected reaction of the output relays.
4	Remove the bypass and otherwise restore normal operation.

This test will detect approximately 95% of possible "DU" failures.