Failure Modes, Effects and Diagnostic Analysis

Project:
Universal Transmitters PR4179 and PR4184 with analog output

Customer:
PR electronics A/S
Rønde
Denmark

Contract No.: PR electronics A/S 19-01-034
Report No.: PR electronics A/S 19-01-034 R029
Version V1, Revision R1; May 2019

Jürgen Hochhaus

Management summary

This report summarizes the results of the hardware assessment carried out on the Universal Transmitters PR4179 and PR4184 with analog output, hardware version as specified by the documents listed in 2.5.1 and software version as shown in Table 1 below. Table 1 also gives an overview of the considered variants.

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) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Overview of the considered variants

	Description	Name	Software Version	
			Input CPU	Main CPU
[V1]	DIN rail mounted Universal AC / DC transmitter	PR4179	V1R0	V3R0
[V2]	DIN rail Universal uni-/bipolar transmitter	PR4184	V2R0	V4R0

For safety applications only the described variants of the Universal Transmitters PR4179 and PR4184 with analog output have been considered. All other possible variants and configurations are not covered by this report.

As the transmitters can be configured for different input ranges and signals, the failures rates were evaluated for different configurations. The worst case was identified and used as the bases for the result tables. 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 input, to enable the detection a short circuit input.

The failure modes used in this analysis are from the exida Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N3]).

The Universal Transmitters PR4179 and PR4184 with analog output can be considered to be Type B[1] elements with a hardware fault tolerance of 0.

The following tables show how the above stated requirements are fulfilled for the considered Universal Transmitters PR4179 and PR4184 with analog output.

[1] Type B element: "Complex" subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 2: Summary - Failure rates for [V1] – Universal Transmitter PR4179

Failure category	IEC 61508:2010 [2] Failure rates (in FIT)
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	0
Dangerous Detected (λ_{DD})	443
Dangerous Undetected (λ_{DU})	39

Total failure rate of the safety function (λ_{Total})	482
Safe failure fraction (SFF) [3]	91%
DC	91%

SIL AC [4]	SIL 2

[2] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
[3] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.
[4] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. 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_{AVG} / PFH value.

Table 3: Summary - Failure rates for [V2] - Universal Transmitter PR4184

Failure category	IEC 61508:2010 [5] Failure rates (in FIT)
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**0**
Dangerous Detected (λ_{DD})	**468**
Dangerous Undetected (λ_{DU})	**46**
Total failure rate of the safety function (λ_{Total})	**514**
Safe failure fraction (SFF) [6]	**91%**
DC	**91%**
SIL AC [7]	**SIL 2**

The failure rates are valid for the useful life of the Universal Transmitters PR4179 and PR4184 with analog output (see Appendix A) when operating as defined in the considered scenarios.

[5] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
[6] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.
[7] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. 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_{AVG} / PFH value.

Table of Contents

Management summary 2

1 Purpose and Scope 6

2 Project management 7
- 2.1 exida 7
- 2.2 Roles of the parties involved 7
- 2.3 Standards / Literature used 8
- 2.4 exida tools used 8
- 2.5 Reference documents 9
  - 2.5.1 Documentation provided by the customer 9
  - 2.5.2 Documentation generated by the customer and reviewed by *exida* 9

3 Product Description 10

4 Failure Modes, Effects, and Diagnostic Analysis 13
- 4.1 Description of the failure categories 13
- 4.2 Methodology – FMEDA, Failure rates 14
  - 4.2.1 FMEDA 14
  - 4.2.2 Failure rates 14
  - 4.2.3 Assumptions 15
- 4.3 Results 16
  - 4.3.1 Universal Transmitter PR4179 17
  - 4.3.2 Universal Transmitter PR4184 18

5 Using the FMEDA results 19
- 5.1 Example PFD_{AVG} / PFH calculation 19

6 Terms and Definitions 21

7 Status of the document 22
- 7.1 Liability 22
- 7.2 Releases 22
- 7.3 Release Signatures 22

Appendix A: Lifetime of Critical Components 23

Appendix B: Proof tests to detect dangerous undetected faults 24

Appendix C: Determining Safety Integrity Level 25

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Universal Transmitters PR4179 and PR4184 with analog output, hardware version as specified by the documents listed in 2.5.1 and software version as shown in Table 1.
The FMEDA builds the basis for an evaluation whether an element including the described Universal Transmitters PR4179 and PR4184 with analog output 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. It **does not** consider any calculations necessary for proving intrinsic safety.

2 Project management

2.1 exida

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety cybersecurity, and availability with over 400 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, exida is a global company with offices around the world. exida offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. exida maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion unit operating hours of field failure data.

2.2 Roles of the parties involved

PR electronics A/S	Manufacturer of the Universal Transmitters PR4179 and PR4184 with analog output.
exida	Performed the hardware assessment.

PR electronics A/S contracted exida in January 2019 with the review of the FMEDA of 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]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	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
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N6]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 exida tools used

[T1]	SILcal V8.0.11	FMEDA Tool
[T2]	exSILentia Ultimate V3.3.0.903	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	4179-1-V3R0-SCH.pdf	Schematic diagram and layout printout of PR4179, dated 2017-08-10, V3R0
[D2]	4179 BoM.pdf	Bill of material, received 2019-01-08
[D3]	4179 Microcontrollers.pdf	Failure rate distribution along the parts of the 4179 microcontrollers, received 2019-01-08
[D4]	417960xx Firmware Design Specification.pdf	Main controller firmware specification including software diagnostics V4R0
[D5]	417963xx Firmware Design Specification.pdf	Input controller firmware specification including software diagnostics V2R0
[D6]	4184-1-V4R0-SCH.pdf	Schematic diagram and layout printout of 4184 dated 2018-06-28, V4R0
[D7]	4184 BoM.pdf	Bill of material, received 2019-01-08
[D8]	4184 Microcontrollers.pdf	Failure rate distribution along the parts of the 4184 microcontrollers, received 2019-01-08
[D9]	418460xx Firmware Design Specification.pdf	Main controller firmware specification including software diagnostics V4R0
[D10]	418463xx Firmware Design Specification.pdf	Input controller firmware specification including software diagnostics V2R0
[D11]	4179V100_UK.pdf	Product manual “4179 Universal AC /DC transmitter”
[D12]	4184V100_UK.pdf	Product manual “4184 Universal uni-/bipolar signal transmitter”
[D13]	Action Items.pdf	Answers to review findings, 2018-01-08
[D14]	Action Items Rev2.pdf	Answers to review findings, 2018-01-19
[D15]	Action Items Rev3.pdf	Answers to review findings, 2018-01-28 This file contains an argumentation showing the analysis to identify the worst case configuration

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 the customer and reviewed by *exida*

[R1]	FMEDA - 4179 Current Input – Rev4 of 01.02.2019
[R2]	FMEDA - 4179 Voltage Input – Rev4 of 01.02.2019
[R3]	FMEDA - 4184 Current Input – Rev4 of 01.02.2019
[R4]	FMEDA - 4184 High Voltage Input – Rev4 of 01.02.2019
[R5]	FMEDA - 4184 Low Voltage input – Rev4 of 01.02.2019

3 Product Description

The universal Transmitters PR4179 and PR4184 are isolated, DIN rail mounted, universal input output devices used in many different industries for both signal conversion, monitoring, control and safety applications.

Figure 1 gives an impression on the outline of the devices.

Figure 1: PR4179 Universal AC/DC Transmitter and PR 4184 Universal Signal Transmitter

Using the detachable display fronts the PR4179 and PR4184 can be configured for a wide range of custom input/output types and ranges. Furthermore, the displays enable online monitoring of process and output signals in the transmitters. The supply voltage can be set anywhere between 21.6..253Vac or 19.2..300Vdc.
Both the universal transmitter PR4179 and PR4184 are considered a Type B[8] component with a hardware fault tolerance of 0.

For safety applications, only the 4-20mA (with safety read back enabled) output has been considered for both the PR4179 and PR4184. All other output variant are not covered by this report. Furthermore, the input can be configured for non-standard custom input range and for both voltage and current inputs.
However, the following limitation applied to the input configuration when used in safety applications:

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

[8] Type B element: "Complex" subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Both the PR4179 and the PR4184 can be used with and without the detachable display as these are not considered a part of the FMEDA as they are decoupled from the transmitter. The displays are supplied by the power supply of the PR 4179 or PR4184, but decoupling measures are implemented.

PR4179 functions:

The PR4179 measures AC signals and converters them into standard DC process signals. Figure 2 below shows a block diagram of the universal AC / DC transmitter PR4179:

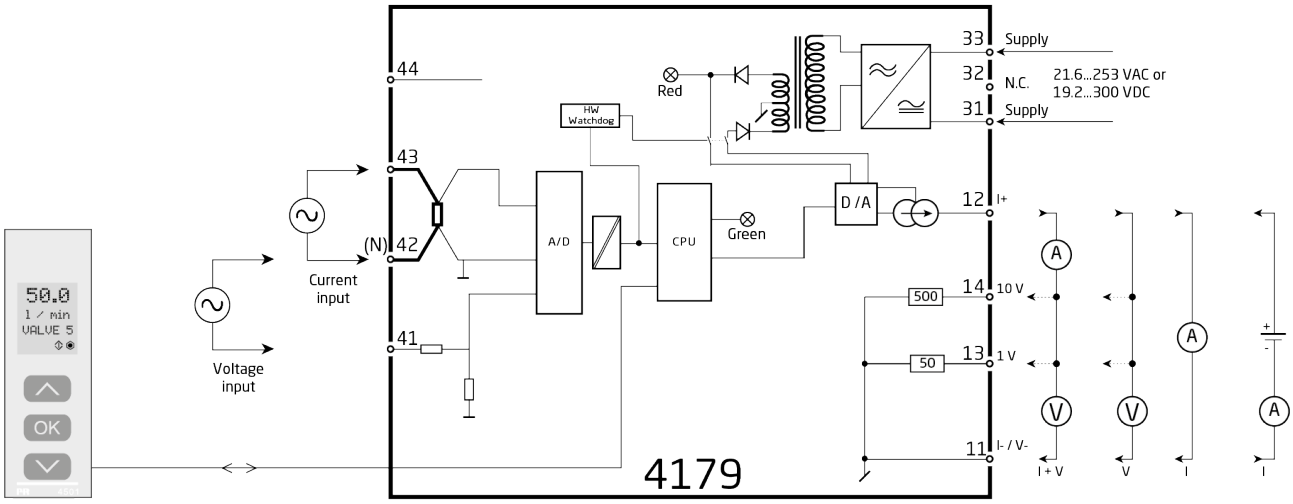


Figure 2: Block and connection diagram for the PR4179 Universal AC / DC Transmitter

Output type(s) and range(s) supported for the PR4179:

- Current: 4-20mA (with safety read back enabled)

Input type(s) and range(s) supported for the PR4179:

- Voltage: Any input range, with the following constraint: The configured minimum input must be at least 5% of maximum input
- Current Any input range, with the following constraint: The configured minimum input must be at least 5% of maximum input

PR4184 functions:

The PR4184 measures a wide range of DC signals and converters them into standard DC process signals. Furthermore, the 4184 can be used to convert standard process control signals into non-standard output signals for controlling a large variety of systems.
Figure 3 below shows a block diagram of the Universal Signal Transmitter PR4184:

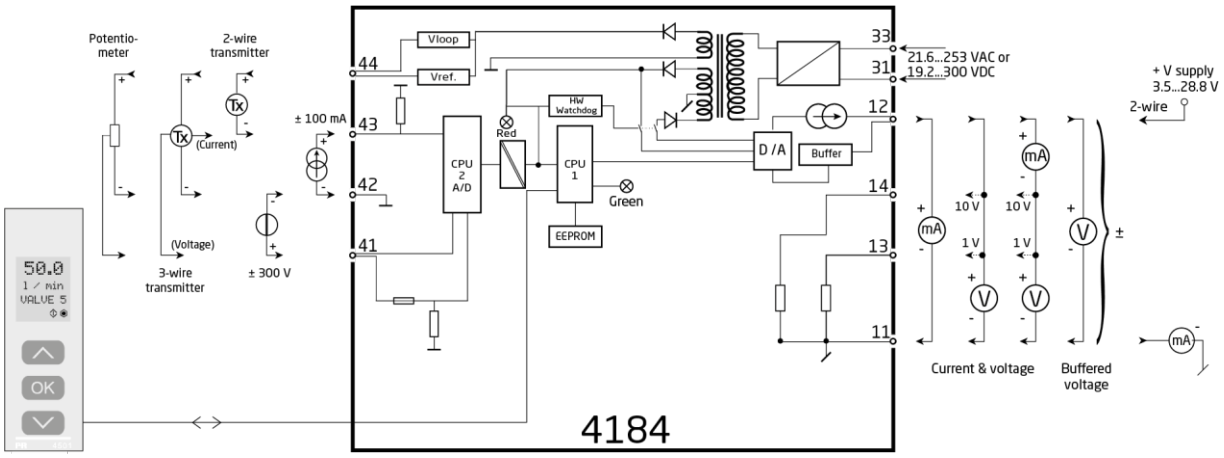


Figure 3: Block and connection diagram for the PR4184 Universal Signal Transmitter

Output type(s) and range(s) supported for the PR4184:

- Current: 4-20mA (with safety read back enabled)

Input type(s) and range(s) supported for the PR4184:

- Voltage: Any input range, with the following constraints: Inputs must be positive and the configured minimum input must be at least 5% of maximum input.
- Current: Any input range, with the following constraints: Inputs must be positive and the configured minimum input must be at least 5% of maximum input.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with PR electronics A/S and is documented in [R1] to [R5].

4.1 Description of the failure categories

In order to judge the failure behavior of the Universal Transmitters PR4179 and PR4184 with analog output , the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as output reaching the user defined threshold value.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: 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: a) deviates the output current by more than 2% of full span and 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.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed.
Dangerous Detected	Failure that is dangerous but is detected by internal or external testing.
Fail high	A fail high failure (H) is defined as a failure that causes the output signal to go to the maximum output current (> 21mA).
Fail low	A fail low failure (L) is defined as a failure that causes the output signal to go to the minimum output current (< 3.6mA).
Annunciation	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures.
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.

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 modes used in this analysis are from the exida Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N3]). 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 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 their 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.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Universal Transmitters PR4179 and PR4184 with analog output.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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.
- 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 correct parameterization is verified by the user.
- The safety accuracy for all configurations is 2% of full span.
- The input must always be configured for a positive signals and the measurement range must be offset by at least 5% of configured maximum input, to enable the detection a short circuit input.
- The device is locked against unintended operation/modification.
- The worst-case diagnostic test rate and reaction time is 40s for PR4179 and 65s for the PR4184.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) is considered to be 24 hours.
- The Universal Transmitters PR4179 and PR4184 with analog output are installed per the manufacturer's instructions.
- 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.
- Only the described variants are used for safety applications.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- All components that are not part of the safety function (e.g. optional displays) and cannot influence the safety function (feedback immune) are excluded.
- Only the 4-20mA (with safety read back enabled) output is used.

4.3 Results

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

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

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 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 assessment supports the 1_H approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg}) / (\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg} + \Sigma\lambda_{DU} \text{ avg})$
When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

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

Where:

$\lambda_S =$ Fail Safe

$\lambda_{DD} =$ Fail Dangerous Detected

$\lambda_{DU} =$ Fail Dangerous Undetected

As the Universal Transmitters PR4179 and PR4184 with analog output is only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.3.1 Universal Transmitter PR4179

The FMEDA carried out on the Universal Transmitter PR4179 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 4: Failure rates for [V1] – Universal Transmitter PR4179

Failure category	IEC 61508:2010 [9] Failure rates (in FIT)
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**0**
Dangerous Detected (λ_{DD})	**443**
Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly [10]	239
High (λ_{H}); detected by the logic solver	4
Low (λ_{L}); detected by the logic solver	200
Annunciation Detected (λ_{AD})	0
Dangerous Undetected (λ_{DU})	**39**
Annunciation Undetected (λ_{AU})	22
No effect ($\lambda_{\#}$)	258
No part (λ_{-})	145
Total failure rate of the safety function (λ_{Total})	**482**
Safe failure fraction (SFF) [11]	**91%**
DC	**91%**
SIL AC [12]	**SIL 2**

[9] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
[10] "indirectly" means that these failures are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.
[11] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.
[12] 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_{AVG} / PFH value.

4.3.2 Universal Transmitter PR4184

The FMEDA carried out on Universal Transmitter PR4184 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.

In redundant sensor configuration, two sensors are measured and evaluated. The two results are compared; the output is set to the safe state if the difference between the evaluated values exceeds a defined limit.

Table 5: Failure rates for [V2] - Universal Transmitter PR4184

Failure category	IEC 61508:2010 [13] Failure rates (in FIT)
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**0**
Dangerous Detected (λ_{DD})	**468**
Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly [14]	228
High (λ_{H}); detected by the logic solver	11
Low (λ_{L}); detected by the logic solver	229
Annunciation Detected (λ_{AD})	0
Dangerous Undetected (λ_{DU})	**46**
Annunciation Undetected (λ_{AU})	21
No effect ($\lambda_{\#}$)	374
No part (λ_{-})	192
Total failure rate of the safety function (λ_{Total})	**514**
Safe failure fraction (SFF) [15]	**91%**
DC	**91%**
SIL AC [16]	**SIL 2**

[13] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
[14] "indirectly" means that these failures are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.
[15] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.
[16] 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_{AVG} / PFH value.

5 Using the FMEDA results

Using the failure rate data displayed in section 4.3, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{AVG}) calculation can be performed for the entire safety function.
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.
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. See Appendix C for a complete description of how to determine the Safety Integrity Level for an entire safety function. The mission time used for the calculation depends on the PFD_{AVG} target and the useful life of the product. The failure rates for all the devices of the safety function are required to perform the PFD_{AVG} calculation
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) PR4184 Universal Signal Transmitter with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.3.2. A mission time of 10 has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 6 shows the results.

Table 6: [V2] – PFD_{AVG} / PFH values

	PFH [17]	Proof test interval	
		T[Proof] = 1 year	T[Proof] = 5 years
PR4184	PFH = 4.6 E-08 1/h	PFD_{AVG} = 2.31E-04	PFD_{AVG} = 1.03 E-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 Universal Transmitters PR4179 and PR4184 with analog output are contributing to the entire safety function they 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 1.00E-03 or 1.00E-07 1/h, respectively. For the PR4179 and PR4184, the calculated PFH value and the PFD_{AVG} with a proof test interval of 1 year is within the allowed range for SIL 2 according to table 2 of IEC 61508-1 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 PFD_{AVG} in case of a proof test interval of 5 years slightly exceeds the assumed 10% of the allowed range, i.e. 1.00E-03. But the device may be used also for SIL2 low demand application based on a careful consideration of the failure rates of the other elements in the loop.

[17] The PFH value is based on a worst-case diagnostic test rate and a reaction time of 60s. The ratio of the diagnostic test rate to the demand rate shall equal or exceed 100.

The resulting PFD_{AVG} graphs generated from the exSILentia tool for a proof test interval of 1 year is displayed in Figure 4.

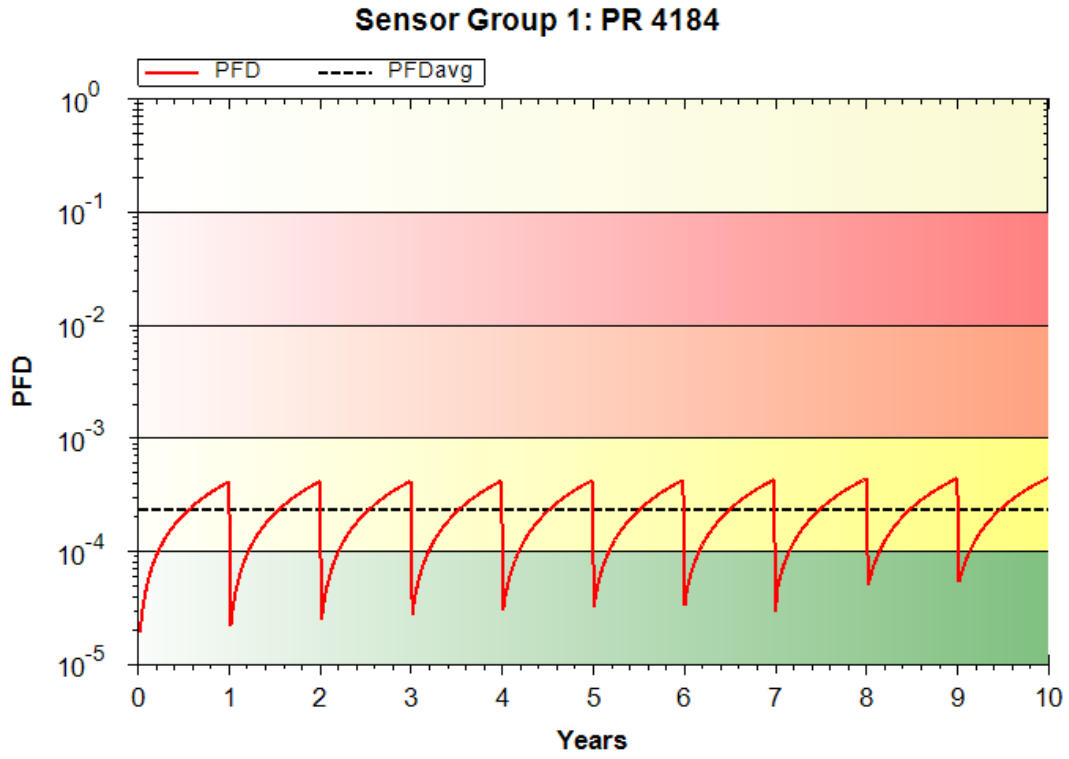


Figure 4: $PFD_{AVG}(t)$

6 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
DC	Diagnostic Coverage of dangerous failures (DC = λ_{DD} / (λ_{DD} + λ_{DU}))
FIT	Failure In Time (1x10^{-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.
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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.
Type B element	“Complex” element (using 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.

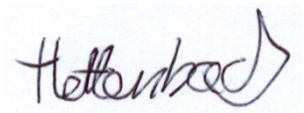
Most products also tend to undergo incremental changes over time. If an exida FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version History:	V1R1:	Editorial changes in chapter 5 and Appendix B; May 2, 2019
	V1R0:	Review comments incorporated; Mar 7, 2019
	V0R2:	Review comments incorporated; Feb 19, 2019
	V0R1:	Initial version; Feb 5, 2019
Authors:	Jürgen Hochhaus	
Review:	V0R2:	Marc Falkenløwe Østvand, PR electronics; Mar 4, 2019
	V0R1:	Jan Hettenbach, exida; Feb 18, 2019
	Release status: released	

7.3 Release Signatures

Dipl.-Ing. (FH) Jürgen Hochhaus, Senior Safety Engineer



Dipl. -Ing. (Univ.) Jan Hettenbach, Senior Safety Engineer

Appendix A: Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[18] 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.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

The Universal Transmitters PR4179 and PR4184 with analog output do not contain components with reduced useful lifetime which are contributing to the dangerous undetected failure rate and therefore to the PFDAVG calculation. Therefore, there is no limiting factor to the useful lifetime.

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

[18] 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 Table 7.

Table 7 Steps for Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Provide an appropriate a input signal, representing a measurement value at the lower limit of configured range, to the Universal Transmitter PR4179 / Universal Transmitter PR4184 and verify the expected signal input/output conditions for the interfaces.
3.	Provide an appropriate input signal, representing a measurement value at the higher limit of configured range, to the Universal Transmitter PR4179 / Universal Transmitter PR4184 and verify the expected signal input/output conditions for the interfaces.
4.	Remove the bypass and otherwise restore normal operation.

This test will detect 99% of possible “du” failures.

Appendix C: Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). The numbers used in the examples are not for the product described in this report.

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL), see [N4] and [N5].

These are:

A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;

B. Architecture Constraints (minimum redundancy requirements) are met; and

C. a PFD_{AVG} / PFH calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC 61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N6].

C. 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.

A Probability of Failure on Demand (PFD_{AVG}) calculation must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restoration (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the exida FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{AVG} for any given set of variables.

Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC 61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{AVG} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the ones of the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{AVG} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{AVG} contributions are Sensor PFD_{AVG} = 5.55E-04, Logic Solver PFD_{AVG} = 9.55E-06, and Final Element PFD_{AVG} = 6.26E-03 (Figure 5).

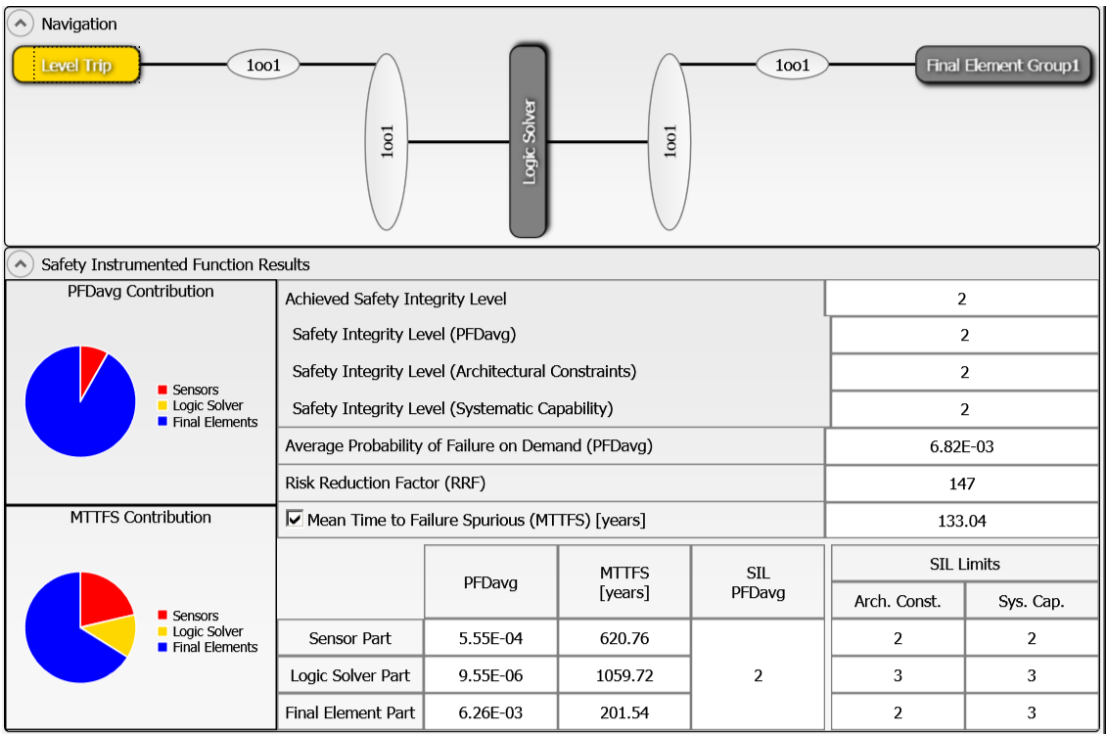


Figure 5: exSILentia results for idealistic variables

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 6.

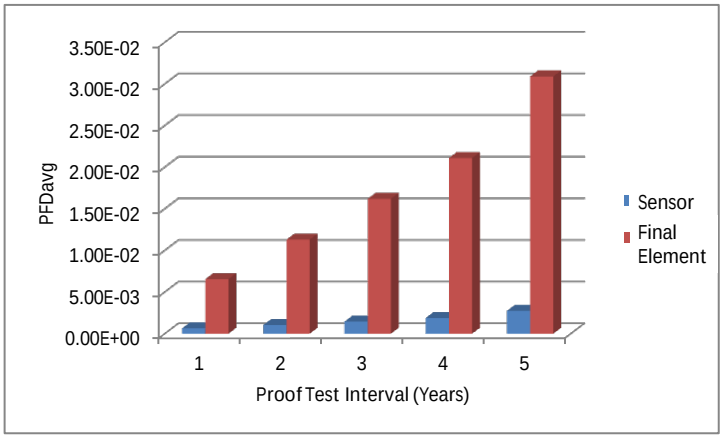


Figure 6: PFD_{AVG} versus Proof Test Interval

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{AVG} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFD_{AVG} contributions are Sensor PFD_{AVG} = 2.77E-03, Logic Solver PFD_{AVG} = 1.14E-05, and Final Element PFD_{AVG} = 5.49E-02 (Figure 7).

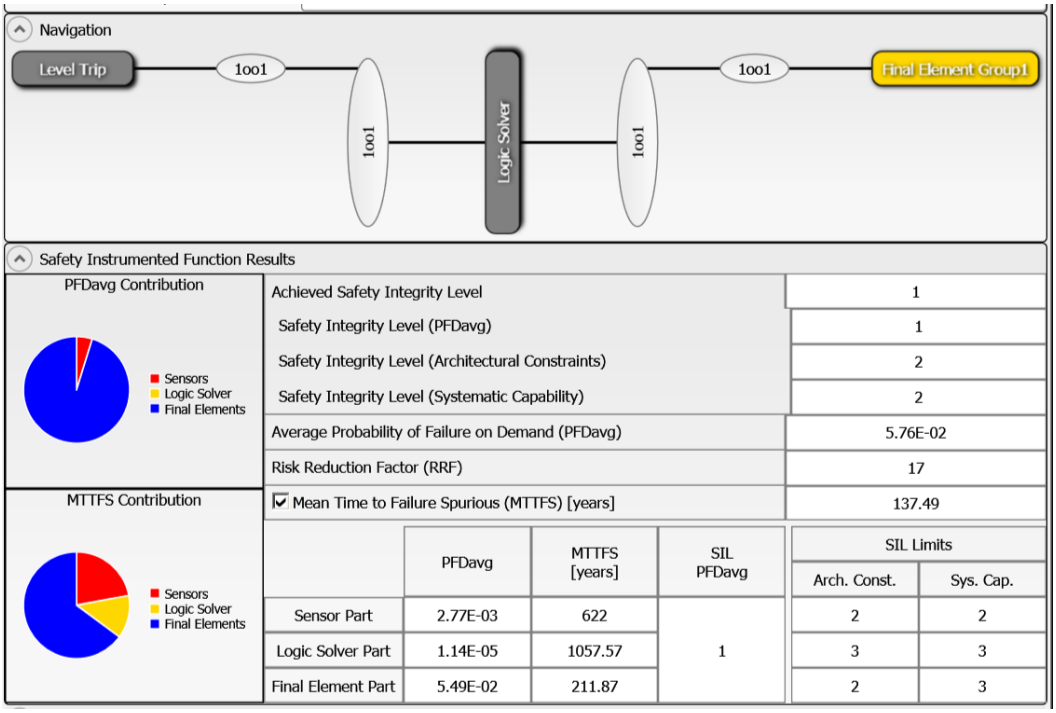


Figure 7: exSILentia results with realistic variables

It is clear that PFD_{AVG} results can change an entire SIL level or more when all critical variables are not used.