Failure Modes, Effects and Diagnostic Analysis

Project:
1700 / 2700 Coriolis Flowmeter series with Enhanced 800 Core

Company:
Micro Motion, Inc.
Emerson
Boulder, CO
United States

Contract Number: Q17/02-079
Report No.: EMM 08/04-67 R001
Version V3, Revision R5, April 28, 2017
Rudolf Chalupa - Gregory Sauk

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 1700 / 2700 Coriolis Flowmeter series with Enhanced 800 Core, hardware and software revision per Section 2.5. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the 1700 / 2700 Flowmeter. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 1700 / 2700 Flowmeter is a four wire, 4-20mA smart device. This product features MVD™ technology and diagnostics. It is designed specifically for applications where multiple variables are needed simultaneously. It has four optional output modules: the Analog/Frequency output module (Option Code A); the Intrinsically Safe output module (Option Code D); channels assigned to default values (Option Code B) and custom configured prior to shipment (Option Code C). The Coriolis flowmeter with the 1700 transmitter is available with option codes A and D only. The Coriolis flowmeter with the 2700 transmitter is available with option codes A, B, C and D.

For safety instrumented systems usage it is assumed that one of the 4 – 20 mA outputs is used as the safety variable for mass flow, volume flow or density.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 1700 / 2700 Flowmeter.

Table 1 Version Overview

1700 Series	Micro Motion Coriolis Flowmeter with 1700 transmitter with 800 ECP and Analog Output or Intrinsically Safe Output (output codes A or D)
2700 Series	Micro Motion Coriolis Flowmeter with 2700 transmitter with 800 ECP and output codes A, B, C or D
Sensors	Elite, T, HPC010P, F, H or R

The 1700 / 2700 Flowmeter is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the 1700 / 2700 Flowmeter has a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

Based on the assumptions listed in 4.3, the failure rates for the 1700 / 2700 Flowmeter are listed in section 4.4.

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

The failure rates listed in this report are based on over 250 billion unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI), see section 4.2.2.

A user of the 1700 / 2700 Flowmeter 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).

[1] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 1700 / 2700 Flowmeter. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

The information in this report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

A FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in cybersecurity, automation system safety 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

Micro Motion, Inc. Manufacturer of the 1700 / 2700 Flowmeter

exida Performed the hardware assessment

Micro Motion, Inc. contracted *exida* in January 2016 with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

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

[N1]	IEC 61508-2: ed2, 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]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers

[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N9]	Random versus Systematic – Issues and Solutions, September 2016	http://www.exida.com/Resources/Whitepapers/random-versus-systematic-failures-issues-and-solutions
[N10]	Bukowski, J.V. and Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
[N11]	Bukowski, J.V. and Stewart, L.L., April 2016	Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	*exida* White Paper, Sellersville, PA www.exida.com
[N13]	Goble, W.M. and Brombacher, A.C., November 1999, Vol. 66, No. 2	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
[N14]	Grebe, J. and Goble W.M.,FMEDA – Accurate Product Failure Metrics, June 2015	http://www.exida.com/Resources/Whitepapers/FMEDA-Accurate-Product-Failure-Metrics

2.4 *exida* tools used

[T1]	V7.1.18	*exida* FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by Micro Motion, Inc.

[D1]	EB-3100940, Rev G,	Schematic Diagram, Appvl, R Series Sensor
[D2]	EB-3100316, Rev K,	Schematic Diagram, Appvl, F100S Sensor
[D3]	EB-3000842, Rev O,	Schematic Diagram, Appvl, CMF100 Sensor
[D4]	ES-20002951, Rev C	Schematic Diagram, 800 BFCore
[D5]	Part:4265.001, Rev B	Schematic Diagram, Output Board schematic
[D6]	4596011, Rev B	Schematic Diagram, Config IO
[D7]	ES-20006853, Rev C	Schematic Diagram, 1700-2700 PWR
[D8]	EB-4000128, Rev G,	Schematic Diagram, Appvl, Titan Sensors
[D9]	3775061, Rev C	Schematic, Analog Feature Bd
[D10]	ES-20002949, Rev B	Schematic, 800 Terminal

[D11]	20002949, Rev D	Spreadsheet, BOM, 800 Terminal
[D12]	20002951, Rev G	Spreadsheet, BOM, 800 BFCore
[D13]	4265014, Rev C	Spreadsheet, BOM, 1700 ISO
[D14]	MMI-20006853, Rev D	Spreadsheet, BOM, 1700-2700 PWR
[D15]	4830014, Rev B	Spreadsheet, BOM, EMI Terminal
[D16]	4596014, Rev C	Spreadsheet, BOM, Config IO
[D17]	PS-00400, June 2002	Product Data Sheet Series 1000 and 2000 transmitters
[D18]	PS-00232, April 2002	Product Data Sheet Micro Motion Flowmeters
[D19]	MM 2700 Fault Injection Summary rev. 2.xls	Fault Injection Test Results
[D20]	20003460, Rev H	Assy, Potted Transmitter, ECP
[D21]	MMI SIL 700 SASRD_0.2.doc	1700/2700 Coriolis Flowmeter System, Architecture and Safety Requirements Specification
[D22]	E-10018200, Rev CD, 2011-04-18	Drawing, Com Assy F200/R200/H200
[D23]	E-0417000,Rev EF, 2014-11-24	Drawing, Com Assy F050/H050/K050/R050
[D24]	E-0416500, Rev EG, 2014-12-10	Drawing, Com Assy F025/H025/K025/R025
[D25]	E-0417500, RevEI, 2015-11-05	Drawing, Com Assy F100/R100/H100
[D26]	ER-20022547, Rev AD, 1-Sep-16	HPC010 Sensor Assy Drawing
[D27]	PS-002073, Rev A, Dec-2016	HPC010P Ultra High Pressure Flowmeter Product Data Sheet
[D28]	PS-00599, Rev N, Sep-2016	H-Series Hygienic Coriolis Flow and Density Meters Product Data Sheet

2.5.2 Documentation generated by *exida*

[R1]	1700 Analog Feature mA Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 18, 2008
[R2]	2700 Config IO mA Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 15, 2008
[R3]	1700-2700 Core CPU for IO sections.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 15, 2008
[R4]	800 Core and flow sensors.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP, July 18, 2008
[R5]	1700-2700 Gemini Main Power.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 16, 2008
[R6]	1700 IS Analog Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 15, 2008

[R7]	1700-2700 EMI term for Feature Bd mA Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 18, 2008
[R8]	1700-2700 Two RTD Adder.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 18, 2008
[R9]	1700-2700 MicroMotion Failure Rate Summaries using 800 Core.xls	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 25, 2008
[R10]	1700-2700 MicroMotion Failure Rate Summaries using 800 Core inc PT_16Apr2014.xls	FMEDA Summary 1700 / 2700 Flowmeter, various models
[R11]	MM 2700 Fault Injection Results-GPS.xls, Oct 2008	Fault Injection Test Results from Oct 2008 Site Visit (included here because not previously listed)

3 Product Description

Micro Motion flowmeters consist of Coriolis sensors and microprocessor-based transmitters that provide mass flow measurement of liquids, gases, and slurries. This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Micro Motion Coriolis Flowmeter, using the CMF (Elite), R, T, F, H or HPC010P series sensors and a 1700 / 2700 transmitter with an 800 ECP (Enhanced Core Processor).

The Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter is a smart device used in many different industries for both control and safety applications. Model 1700 / 2700 features MVD™ technology and diagnostics. It allows for multivariable measurement of mass flow, volume flow, density, and temperature.

The analog milliamp output is used for the safety critical variable (mass flow, volume flow or density); all other outputs are considered outside the scope of safety instrumented systems (SIS) usage.

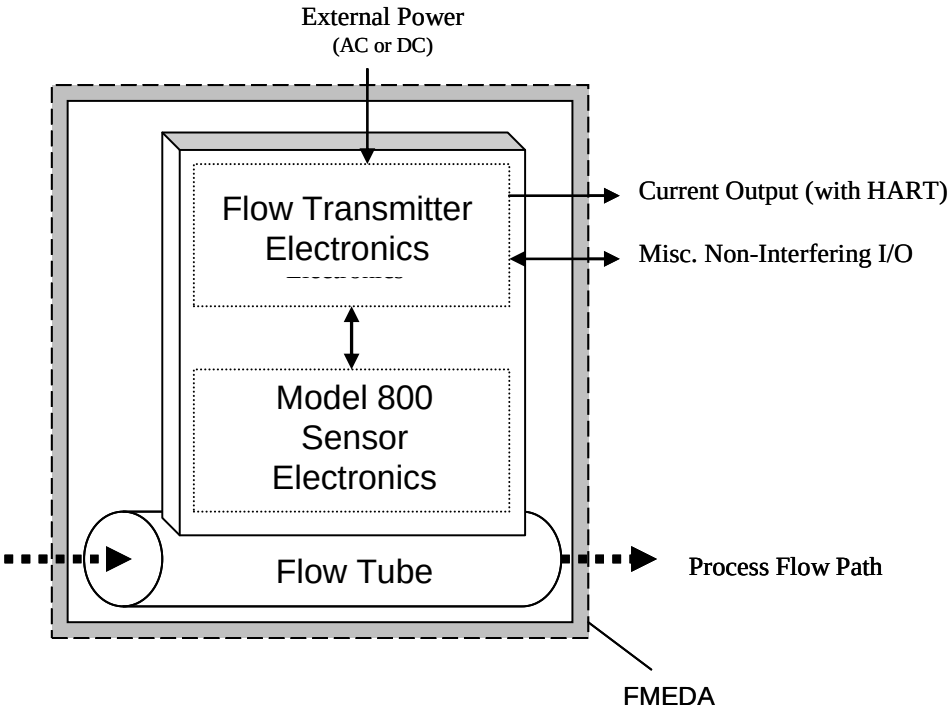


Figure 1 1700 / 2700 Flowmeter, parts included in the FMEDA

Table 2 gives an overview of the different versions and Sensors that were considered in the FMEDA of the 1700 / 2700 Flowmeter.

Table 2 Version Overview

1700 Series	Micro Motion Coriolis Flowmeter with 1700 transmitter with 800 ECP and Analog Output or Intrinsically Safe Output (output codes A or D)
2700 Series	Micro Motion Coriolis Flowmeter with 2700 transmitter with 800 ECP and output codes A, B, C or D
Sensors	Elite, T, HPC010P, F, H or R

The 1700 / 2700 Flowmeter is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

[2] Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.5.1 and is documented in [R1] to [R11].

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level, see Fault Injection Test Report [D19].

4.1 Failure categories description

In order to judge the failure behavior of the 1700 / 2700 Flowmeter, the following definitions for the failure of the device were considered.

Fail-Safe State	Failure that deviates the process signal or the actual output by more than 2% of span, drifts toward the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (default downscale, 2.0mA).
Fail Dangerous	Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics.
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current (> 21 mA).
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.6 mA).
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Detected	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 detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.
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.

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures.

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress. It combines design FMEA techniques with extensions to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each failure mode category [N13, N14].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which was derived using over 250 billion unit operational hours of process industry field failure data from multiple sources and failure data formulas from international standards. The component failure rates are provided for each applicable operational profile and application, see Appendix C. The *exida* profile chosen for this FMEDA was profile 3, as this was judged to be the best fit for the product and application information submitted by Micro Motion, Inc.. 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.

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

The failure rates are predicted for a Site Safety Index of SSI=2 [N10, N11] as this level of operation is common in the process industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from *exida*.

The user of these numbers is responsible for determining their applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. 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. *exida* has detailed models available to make customized failure rate predictions. Contact *exida.*

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 1700 / 2700 Flowmeter.

- The worst case assumption of a series system is made. Therefore only a single component failure will fail the entire 1700 / 2700 Flowmeter and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.
- The stress levels are specified in the *exida* Profile used for the analysis are limited by the manufacturer's published ratings.
- Practical fault insertion tests have been used when applicable to demonstrate the correctness of the FMEDA results.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed and operated per manufacturer's instructions.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is 5 minutes.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 1700 / 2700 Flowmeter FMEDA.

Table 3 Failure rates for 1700 output codes A or D, and 2700 output codes A, B, C or D

Failure category	Failure Rate (FIT)	
	Sensor Models: Elite, T, HPC010P, F, H or R	
Fail Safe Undetected		249
Fail Dangerous Detected		2497
Fail Detected (detected by internal diagnostic)	2422	
Fail High (detected by logic solver)	12	
Fail Low (detected by logic solver)	63	
Fail Dangerous Undetected		233
No Effect		436
Annunciation Undetected		15

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

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 or the 2_H approach according to 7.4.4.3 of IEC 61508 (see Section 5.2).

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.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore, the 1700 / 2700 Flowmeter meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The analysis shows that the 1700 / 2700 Flowmeter has a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

Table 4 lists the failure rates for the 1700 / 2700 Flowmeter according to IEC 61508.

Table 4 Failure rates for 1700 / 2700 Flowmeters according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	SFF[4]
Sensor Models: Elite, T, HPC010P, F, H or R with 1700 output codes A or D, and 2700 output codes A, B, C or D	0	249	2497	233	92.2%

[3] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[4] Safe Failure Fraction if needed, is to be calculated on an element level

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 PFD_{avg} calculation 1700 / 2700 Flowmeter

Using the failure rate data displayed in section 4.4, 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 element.

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 D for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverages for the suggested proof tests are listed in Appendix B.

5.2 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:

> "based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to
>
> - the amount of field feedback; and
> - the exercise of **expert judgment**; and when needed
> - the undertake of specific tests,
>
> in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508, ed2, 2010 does not give detailed criteria for Route 2_H, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and

2. a device and all of its components have been installed in the field for one year or more; and

3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and

4. failure definitions, especially "random" vs. "systematic" [N9] are checked by *exida*; and

5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification [N12].

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
ECP	Enhanced Core Processor
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
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).
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
PFD_{avg}	Average Probability of Failure on Demand
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
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 A element	"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
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

7 Status of the Document

7.1 Liability

exida prepares FMEDA 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, product design changes, 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 model number 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, contact the product vendor to verify the current validity of the results.

7.2 Releases

Version History:

V3, R5: Added H and HPC sensors, added meets 2_H requirements. G Sauk, 28-Apr-2017

V3, R4: Restored extended proof tests, R. Chalupa, 2016-03-08

V3, R3: Added R sensors, used latest template, R. Chalupa, 2016-01-28

V3, R2: changed Failure Category "Residual" to "No Effect", changed report name to match previous report version, changed file name to match report name; Griff Francis, 25 Apr 2014

V3, R1: calculations done per [N1]; used latest report template V8R2; Griff Francis, 17 Apr 2014

V2, R4: Updated per review, MicroMotion, October 29, 2008

V2, R3: Edited per review, W. Goble, October 22, 2008.

V2, R2: Updated per most recent template, R. Chalupa, October 17, 2008

V2, R1: Created version for models using 800 ECP; Aug 14, 2008

Author(s): Rudolf Chalupa - Gregory Sauk

Review:

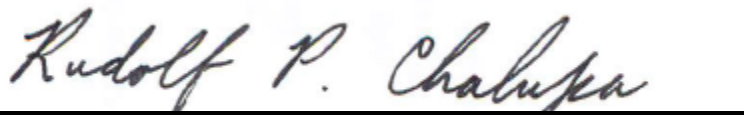
V2, R1:	Rudolf Chalupa, (*exida)* October 17, 2008
V2, R2:	William Goble, October 22, 2008
V2, R3:	Ezra Sobel (Micro Motion), October 28, 2008
V3, R1:	Rudolf Chalupa, (*exida)*, April 16, 2014
V3, R3:	Ted Stewart, (*exida)*, January 31, 2016
V3, R5:	John Yozallinas, (*exida)* , April 28, 2017

Release Status: Released to Micro Motion, Inc.

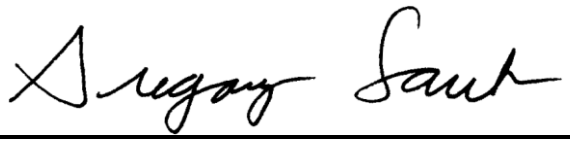
7.3 Future enhancements

At request of client.

7.4 Release signatures



Rudolf P. Chalupa, CFSE, Senior Safety Engineer



Gregory Sauk, CFSE, 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 4.2.2) this only applies provided that the useful lifetime[5] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the 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 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.

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

Table 5 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) – Aluminum electrolytic, non-solid electrolyte	Approx. 90,000 hours

It is the responsibility of the end user to maintain and operate the 1700 / 2700 Flowmeter per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

The limiting factors with regard to the useful lifetime of the system are the aluminum electrolytic capacitors. The aluminum electrolytic capacitors have an estimated useful lifetime of about 10 years.

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

[5] 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 Reveal 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 automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test 1

A simple suggested proof test consisting of setting the output to the min and max, and a calibration check as described in Table 6 will detect 56% of the possible DU failures in the 1700 / 2700 Flowmeter.

Table 6 Suggested Proof Test – Transmitter

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Use HART communications to retrieve any diagnostics and take appropriate action.
3.	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value[6].
4.	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value[7].
5.	Inspect the transmitter for any leaks, visible damage or contamination.
6.	Verify all safety critical configuration parameters
7.	Remove the bypass and otherwise restore normal operation.

B.2 Suggested Proof Test 2

An alternative proof test listed in Table 7, consisting of Proof Test 1 along with actual flow verification plus verification of the flow tube temperature measurement and a restart of the sensor (to detect soft errors in RAM) will detect 91% of the possible DU failures in the 1700 / 2700 Flowmeter. This proof test in combination with the other automatic diagnostics/detection will detect 99% of the possible Dangerous failures in the 1700 / 2700 Flowmeter.

[6] This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
[7] This tests for possible quiescent current related failures.

Table 7 Suggested Proof Test 2

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value[8].
4	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value[9].
5	Use the HART communicator to read the flow tube temperature sensor reading and check for a reasonable reading based on process temperature.
5	Initiate a "Force Hard Reboot" command via Modbus Coil 41. With a 375 HART Communicator: a. Select 5 – Detailed Setup b. Select 9 – Modbus Data c. Select 2 – Write Modbus Data Value d. Select 1 – Coil e. Enter in the value "41" – Enter f. Select 2 – On g. 375 Display reads "Coil Value is On and Exception Code is 0" h. 2700 Display (if present) reads "reading Core" i. Wait ~40 seconds for core processor and 2700 to return to normal operation j. Select – OK and then exit With Prolink via Modbus a. From the menu – Prolink-Configuration b. Select Modbus tab c. Location Type: Coil d. Starting Address: 41 e. Value: 1 f. Select – Write g. 2700 Display (if present) reads "reading Core" h. wait ~40 seconds for core processor and 2700 to return to normal operation
6	Perform the meter verification per Section 10.3 of the Configuration and Use Manual.
7	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
8	Verify all safety critical configuration parameters
9	Restore the loop to full operation
10	Remove the bypass from the safety PLC or otherwise restore normal operation

[8] This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
[9] This tests for possible quiescent current related failures.

B.3 Suggested Proof Test 3

For more complete proof test coverage, tests from Proof test 2 can be extended to include a full calibration against a primary standard. This complete calibration along with Proof test 2 will detect an estimated 99% of the DU failures. The suggested proof test in combination with the other automatic diagnostics/detection will detect 99.9% of the possible Dangerous failures in the 1700 / 2700 Flowmeter. See Table 8 for a comparison of the different proof tests.

Table 8 Proof Test Results – 1700 / 2700 Flowmeter

Device	$\lambda_{DU}PT$[10] (FIT)	Proof Test Coverage
		With Internal and Logic Solver Diag/Detection
1700 / 2700 Flowmeter, Proof Test 1	103	56%
1700 / 2700 Flowmeter, Proof Test 2	21.0	91%
1700 / 2700 Flowmeter, Proof Test 3	2.3	99%

[10] $\lambda_{DU}PT$ = Dangerous undetected failure rate after performing the recommended proof test.

Appendix C *exida* Environmental Profiles

Table 9 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[11]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[12]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[13]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[14]	G2	G3	G3	G3	G3	Compatible Material
Surge[15]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[16]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[17]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[11] Humidity rating per IEC 60068-2-3
[12] Shock rating per IEC 60068-2-27
[13] Vibration rating per IEC 60068-2-6
[14] Chemical Corrosion rating per ISA 71.04
[15] Surge rating per IEC 61000-4-5
[16] EMI Susceptibility rating per IEC 61000-4-3
[17] ESD (Air) rating per IEC 61000-4-2

Appendix D 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) [N5] and [N7].

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} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. 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 [N8].

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 Restore (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. IEC61508-6 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 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. See Figure 2.

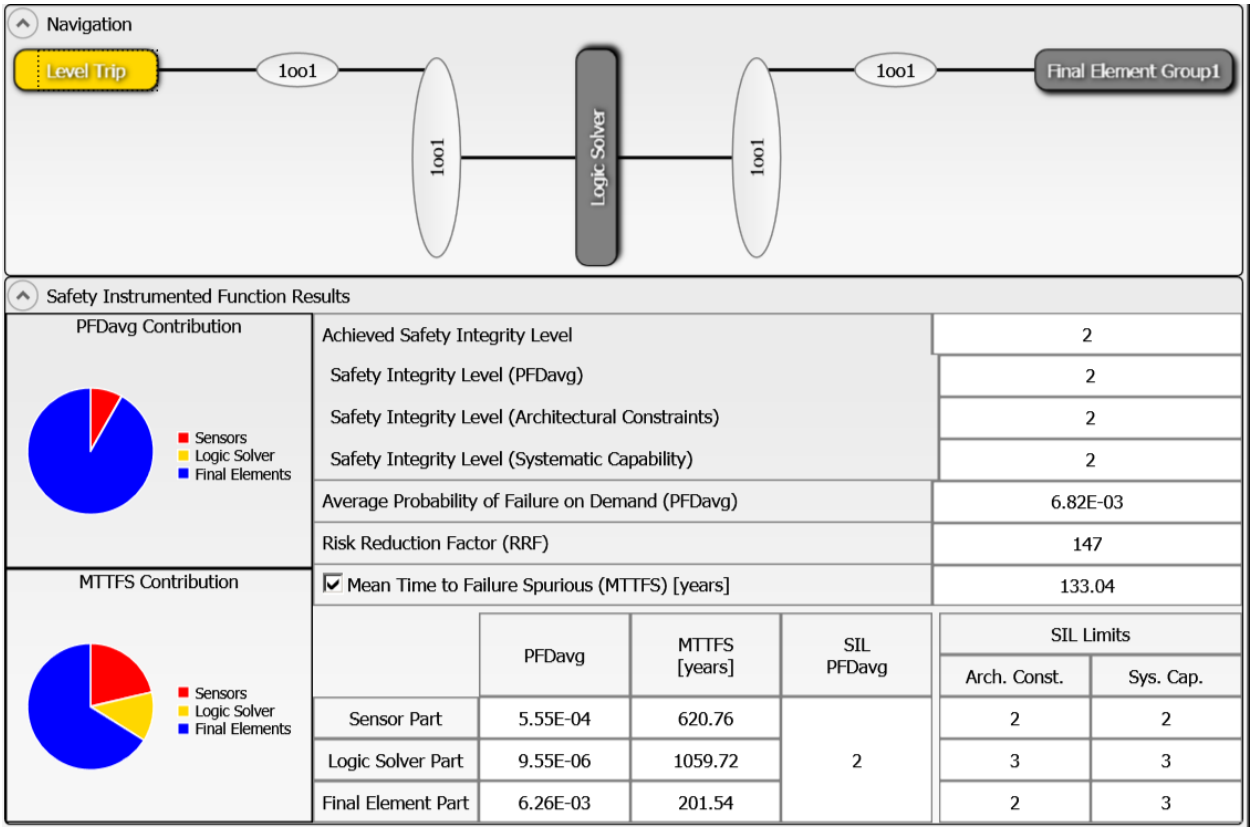


Figure 2: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 3.

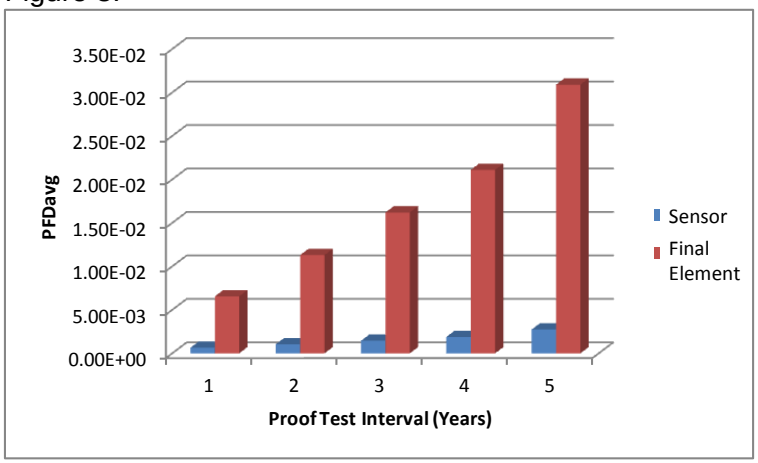


Figure 3 PFD_{avg} versus Proof Test Interval.

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 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 4).

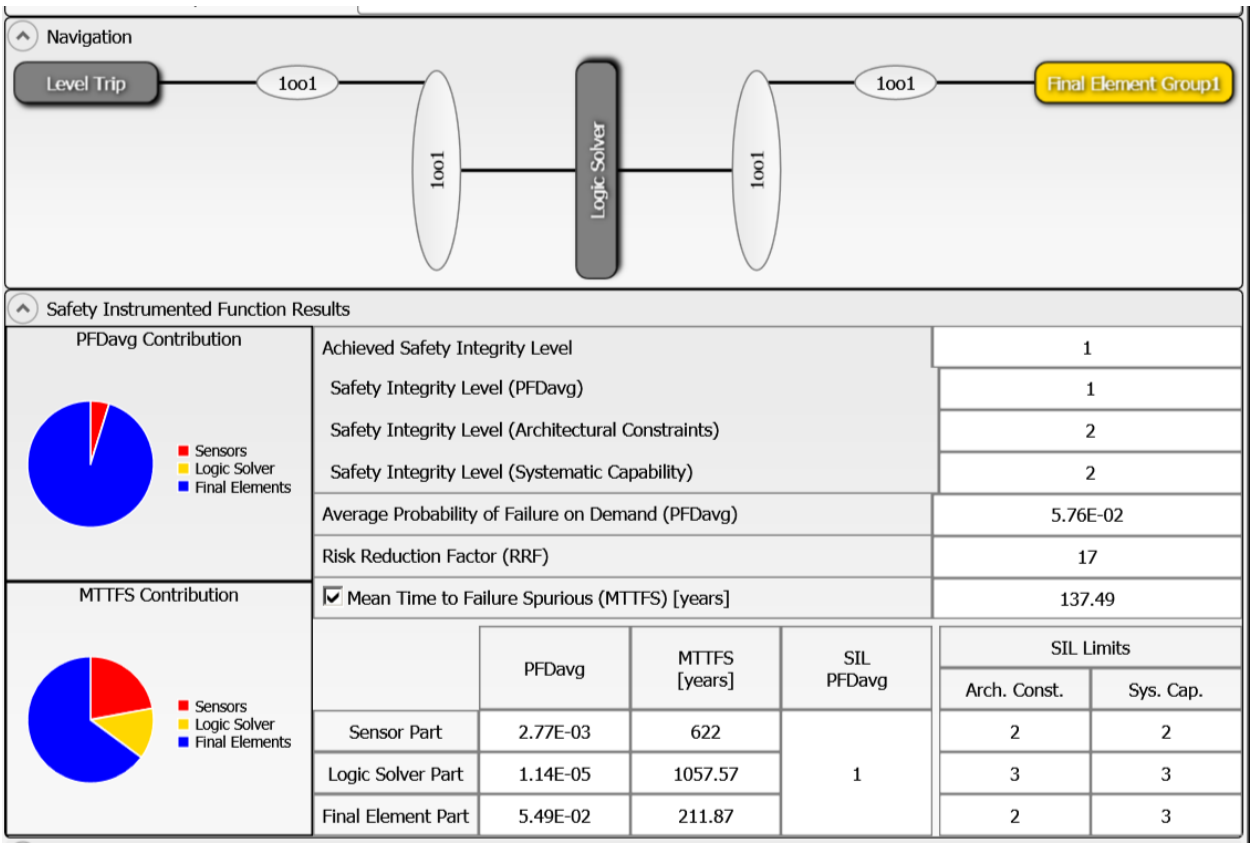


Figure 4: exSILentia results with realistic variables

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