Failure Modes, Effects and Diagnostic Analysis

Project:
Model F10 Flow Switches

Company:
Magnetrol International, Inc.
Aurora, IL
USA

Contract Number: Q17/07-109
Report No.: MAG 17/07-109 R001
Version V1, Revision R2, September 20, 2017
Steven Close

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 Model F10 Flow Switches, hardware revision as described in Section 2.5.1. 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 F10 Flow Switches. For full functional safety certification purposes, all requirements of IEC 61508 must be considered.

The Magnetrol International, Inc. F10 Flow Switches are vane actuated operated units suitable for use on clean liquids or gas applications for flow alarm.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the F10 Flow Switches.

Table 1 Version Overview

Option 1	Decrease Flow, DPDT Switch, NO (Normally Open)
Option 2	Decrease Flow, DPDT Switch, NC (Normally Closed)
Option 3	Increase Flow, DPDT Switch, NO
Option 4	Increase Flow, DPDT Switch, NC
Option 5	Decrease Flow, SPDT, Switch NO
Option 6	Decrease Flow, SPDT, Switch NC
Option 7	Increase Flow, SPDT, Switch NO
Option 8	Increase Flow, SPDT, Switch NC

The F10 Flow Switches are classified as a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H (see Section 5.2). Therefore, the F10 Flow Switches meet the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

Based on the assumptions listed in 4.3, the failure rates for the F10 Flow Switches 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 F10 Flow Switches 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 A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Table of Contents

1 Purpose and Scope 4

2 Project Management 5

2.1 exida 5

2.2 Roles of the parties involved 5

2.3 Standards and literature used 5

2.4 exida tools used 6

2.5 Reference documents 6

2.5.1 Documentation provided by Magnetrol International, Inc. 6

2.5.2 Documentation generated by exida 11

3 Product Description 12

4 Failure Modes, Effects, and Diagnostic Analysis 15

4.1 Failure categories description 15

4.2 Methodology – FMEDA, failure rates 15

4.2.1 FMEDA 15

4.2.2 Failure rates 16

4.3 Assumptions 16

4.4 Results 17

5 Using the FMEDA Results 18

5.1 PFD_{avg} calculation F10 Flow Switches 18

5.2 exida Route 2_H Criteria 18

6 Terms and Definitions 19

7 Status of the Document 20

7.1 Liability 20

7.2 Version History 20

7.3 Future enhancements 20

7.4 Release signatures 21

Appendix A Lifetime of Critical Components 22

Appendix B Proof Tests to Reveal Dangerous Undetected Faults 23

B.1 Suggested Proof Test 23

B.2 Proof Test Coverage 24

Appendix C exida Environmental Profiles 25

Appendix D Determining Safety Integrity Level 26

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 F10 Flow Switches. 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 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

Magnetrol International, Inc.	Manufacturer of the F10 Flow Switches; performed the hardware assessment.
exida	Reviewed the hardware assessment

Magnetrol International, Inc. contracted *exida* in with the hardware assessment review 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, 4th Edition, 2017	*exida* LLC, Electrical Component Reliability Handbook, Fourth Edition, 2017
[N3]	Mechanical Component Reliability Handbook, 4th Edition, 2017	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2017
[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]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

[N7]	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
[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	Goble, W.M., Bukowski, J.V., and Stewart, L.L., Random versus Systematic – Issues and Solutions, exida White Paper, PA: Sellersville, www.exida.com/resources/whitepapers, September 2016.
[N10]	Assessing Safety Culture via the Site Safety Index™, April 2016	Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston, April 2016.
[N11]	Quantifying the Impacts of Human Factors on Functional Safety, April 2016	Bukowski, J.V. and Stewart, L.L., 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, April 2016.
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	Criteria for the Application of IEC 61508:2010 Route 2H, exida White Paper, PA: Sellersville, www.exida.com, December 2016.
[N13]	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, November 1999	Goble, W.M. and Brombacher, A.C., 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]	FMEDA – Accurate Product Failure Metrics, June 2015	Grebe, J. and Goble W.M., FMEDA – Accurate Product Failure Metrics, www.exida.com, June 2015.

2.4 *exida* tools used

[T1]	V7.1.18	*exida* FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by Magnetrol International, Inc.

[D1]	Doc # 002-7111, Rev T, 2016-02-26	Drawing, Switch Frame Casting, Right Hand
[D2]	Doc # 002-7112, Rev T, 2016-02-26	Drawing, Switch Frame Left Hand Diecasting
[D3]	Doc # 003-7104, Rev G,	Drawing, S2 DPS-1 Terminal Block

	1993-05	
[D4]	Doc # 004-4635, Rev N, 2016-03	Drawing, Adaptor Nut (ANSI B31.3)
[D5]	Doc # 004-5089, Rev H, 1995-10-25	Drawing, Spaded Stem F1000
[D6]	Doc # 004-5090, Rev B, 1986-05-27	Drawing, Spaded Stem F1000
[D7]	Doc # 004-5128, Rev C, 2013-07-09	Drawing, Adjustment Screw
[D8]	Doc # 004-5136, Rev D, 1991-05-31	Drawing, Pivot Pin
[D9]	Doc # 004-5231, Rev D, 1974-4-24	Drawing, Standoff Rod
[D10]	Doc # 004-5232, Rev B, 2000-11	Drawing, Spacer, Mounting Bracket
[D11]	Doc # 004-5331, Rev N, 1997-12-01	Drawing, Enclosing Tube Plug
[D12]	Doc # 004-5342, Rev A, 1982-02	Drawing, Spring Guide, Upper
[D13]	Doc # 004-5412, Rev H, 1997-11-10	Drawing, Attraction Sleeve
[D14]	Doc # 004-5421, Rev V, 2006-08-18	Drawing, Enclosing Tube
[D15]	Doc # 004-5653, Rev R, 2002-01-10	Drawing, Machined Flanges
[D16]	Doc # 004-5802, Rev F, 1994-05-20	Drawing, Hex Head Plug
[D17]	Doc # 004-5962-Rev D, 2014-06-11	Drawing, Spacer F1000
[D18]	Doc # 004-7137-Rev E, 1982-07-29	Drawing, Spacer Pin
[D19]	Doc # 004-7702-Rev D, 1994-08	Drawing, Terminal Lug Rivet
[D20]	Doc # 004-7746-Rev F, 1983-12-23	Drawing, Wire Link
[D21]	Doc # 004-9171-Rev AA,	Drawing, E.P. Base GRP B, C & D
[D22]	Doc # 004-9174, Rev J, 2002-08	Drawing, Tall E.P. Cover
[D23]	Doc # 005-1513, Rev B, 2007-10	Drawing, Tab, Grounding
[D24]	Doc # 005-5407-Rev A,	Drawing, Drain Washer

	1982-02	
[D25]	Doc # 005-5419-Rev E, 1990-06	Drawing, Vane Support Bracket
[D26]	Doc # 005-5602, Rev M, 2014-03-13	Drawing, Vane
[D27]	Doc # 005-5609, Rev E, 2014-06-03	Drawing, Vane Cam
[D28]	Doc # 05-5613, Rev B, 1982-02	Drawing, outer Vane
[D29]	Doc # 005-5614, Rev B, 1987-08-11	Drawing, Vane Spring
[D30]	Doc # 005-5701, Rev K, 1997-02-11	Drawing, Outer Sheath
[D31]	Doc # 005-5702, Rev H, 1992-02-26	Drawing, Inner Sheath
[D32]	Doc # 005-6657, Rev E, 1995-01	Drawing, Baffle Plate
[D33]	Doc # 005-7303, Rev A, 1974-05-10	Drawing, Auxiliary Mounting Bracket
[D34]	Doc # 005-7320, Rev E, 1985-11	Drawing, Rocker Arm, Double Pole
[D35]	Doc # 005-7328, Rev N, 2016-07-05	Drawing, Terminal Block Plate, Double Pole
[D36]	Doc # 05-7331, Rev F, 2004-10	Drawing, R/H Micro Actuator Bracket
[D37]	Doc # 05-7332, Rev E, 2004-10	Drawing, L/H Micro Actuator Bracket
[D38]	Doc # 05-7340, Rev C, 1988-03	Drawing, R/H Micro Mounting Bracket
[D39]	Doc # 05-7341, Rev C, 1988-03	Drawing, L/H Micro Mounting Bracket
[D40]	Doc # 005-7522, Rev G, 2006-08	Drawing, Terminal Strip
[D41]	Doc # 05-7534, Rev H, 1998-01	Drawing, Spring Bracket
[D42]	Doc # 05-7570, Rev J, 2000-10	Drawing, Magnet Clamp (with Fall-Out Stop) for single pole mercury sw.
[D43]	Doc # 009-3158, Rev B, 2008-09-11	Drawing, Micro Switch Hermetically Sealed High Temperature
[D44]	Doc # 010-1202, Rev S, 2017-01-11	Drawing, Cup Point Set Screw

[D45]	Doc # 10-1203, Rev H, 2000-11-07	Drawing, Cup Point Set Screw
[D46]	Doc # 10-1204, Rev Y, 2015-04	Drawing, Cup Point Set Screw
[D47]	Doc # 010-1209, Rev l, 2014-04	Drawing, Oval Point Set Screw
[D48]	Doc # 10-1307, Rev D, 1985-05	Drawing, Self-Tapping Screw
[D49]	Doc # 10-1308, Rev C, 1984-11	Drawing, Self-Tapping Screw
[D50]	Doc # 10-1311, Rev B, 2017-03	Drawing, Green Head Grounding Screw
[D51]	Doc # 010-1402, Rev AY, 2013-06	Drawing, Screw, Round Head Machine (304 SST)
[D52]	Doc # 010-1408, Rev B, 1995-04-24	Drawing, Screws, Machine Round Head
[D53]	Doc # 010-1409, Rev AH, 2014-05-29	Drawing, Screws, Machine Round Head (Brass)
[D54]	Doc # 010-1507, Rev F, 2017-02	Drawing, Flat Head Machine Screw
[D55]	Doc # 010-1555, Rev J, 2010-04	Drawing, Brass Fillister Head Machine Screws
[D56]	Doc # 010-1603, Rev H, 2014-07	Drawing, Brass Binding Head Machine Screws
[D57]	Doc # 010-1607, Rev L, 2010-12	Drawing, Grounding Screw Green Binding Head
[D58]	Doc # 10-2105, Rev G, 2000-07	Drawing, Nuts-Hex
[D59]	Doc # 10-2106, Rev R, 2012-04	Drawing, Nuts - Hex
[D60]	Doc # 010-2918, Rev G, 2009-07	Drawing, "P-M" Nut Electronic Modulevel
[D61]	Doc # 010-2919, Rev G, 2005-06	Drawing, Nut, S-2
[D62]	Doc # 010-3103, Rev Q, 2014-07	Drawing, Standard Tooth Lock Washers
[D63]	Doc # 010-3355, Rev C, 1982-02	Drawing, Washer
[D64]	Doc # 010-3359, Rev AQ, 2014-04	Drawing, Washer Plain (T-316 SST)
[D65]	Doc # 010-4203, Rev S, 2010-04	Drawing, Semi-Tubular Oval Head Rivet

[D66]	Doc # 010-5109, Rev F, 1993-09-23	Drawing, Retaining Ring
[D67]	Doc # 010-5405, Rev G, 2009-07	Drawing, Saddle – Grounding Electronic Modulevel
[D68]	Doc # 011-2542, Rev X, 2015-05	Drawing, Pipe Plug
[D69]	Doc # 012-2201, Rev BH, 2016-10-18	Drawing, O-Ring (Viton)
[D70]	Doc # 013-2321, Rev E, 2005-04	Drawing, S2 Micro Fall Out Spring
[D71]	Doc # 013-6101, Rev Z, 2003-12-19	Drawing, Magnet Alnico Ii Red Dot
[D72]	Doc # 032-4501, Rev F, 2014-05	Drawing, Sheathed Sleeve Assembly
[D73]	Doc # 032-6310, Rev R, 2016-02	Drawing, Enclosing Tube
[D74]	Doc # 032-7203, Rev H, 2014-01	Drawing, Stem Cam, Bracket & Flange Assembly
[D75]	Doc # 032-7207, Rev M, 2014-01	Drawing, Cam, Bracket & Stem Assembly
[D76]	Doc # 032-7301, Rev D, 1982-02	Drawing, Outer Vane And Spring Assembly
[D77]	Doc # 037-4633, Rev A, 2007-06	Drawing, High Temperature Switch And Lead Assembly
[D78]	Doc # 037-7122, Rev E, 2014-11	Drawing, Porcelain Terminal Assembly
[D79]	Doc # 037-7426, Rev D, 2016-04-18	Drawing, Switch Frame Assembly
[D80]	Doc # 037-7904, Rev K, 2016-07-21	Drawing, Actuator Micro Switch
[D81]	Doc # 040-2201, Rev K, 1992-06	Drawing, Model F10 Steel Flange, Sensing Unit
[D82]	Doc # 046-4143, Rev S, 2014-10	Drawing, Ep/Vp Hsg Assy
[D83]	Doc # 047-6011, Rev G, 2016-01-21	Drawing, S2M, Series "9", SPDT High Temperature Switch Mechanism "B" Mech Yellow Dot Magnet
[D84]	Doc # 047-6013, Rev G, 2016-01-21	Drawing, S2M, Series "9", DPDT High Temperature Switch Mechanism Yellow Dot Magnet
[D85]		
[D86]	Magnetrol F10 Flow Switch Sensing Unit Assemblies - Decreasing	FMEDA, Magnetrol F10 Flow Switch Sensing Unit Assemblies - Decreasing Flow Alarm

	Flow Alarm.efm	
[D87]	Magnetrol F10 Flow Switch Sensing Unit Assemblies - Increasing Flow Alarm.efm	FMEDA, Magnetrol F10 Flow Switch Sensing Unit Assemblies - Increasing Flow Alarm
[D88]	Magnetrol S2 Switch Mechanisms - DPDT, DF NC.efm	FMEDA, Magnetrol S2 Switch Mechanisms - DPDT, DF NC
[D89]	Magnetrol S2 Switch Mechanisms - DPDT, DF NO.efm	FMEDA, Magnetrol S2 Switch Mechanisms - DPDT, DF NO
[D90]	Magnetrol S2 Switch Mechanisms - DPDT, IF NC.efm	FMEDA, Magnetrol S2 Switch Mechanisms - DPDT, IF NC
[D91]	Magnetrol S2 Switch Mechanisms - DPDT, IF NO.efm	FMEDA, Magnetrol S2 Switch Mechanisms - DPDT, IF NO
[D92]	Magnetrol S2 Switch Mechanisms - SPDT, DF, NC.efm	FMEDA, Magnetrol S2 Switch Mechanisms - SPDT, DF, NC
[D93]	Magnetrol S2 Switch Mechanisms - SPDT, DF, NO.efm	FMEDA, Magnetrol S2 Switch Mechanisms - SPDT, DF, NO
[D94]	Magnetrol S2 Switch Mechanisms - SPDT, IF, NC.efm	FMEDA, Magnetrol S2 Switch Mechanisms - SPDT, IF, NC
[D95]	Magnetrol S2 Switch Mechanisms - SPDT, IF, NO.efm	FMEDA, Magnetrol S2 Switch Mechanisms - SPDT, IF, NO
[D96]	Magnetrol Switch Housing Assemblies.efm	FMEDA, Magnetrol Switch Housing Assemblies
[D97]	47-602.29, February 2015	Model F10 and F50 Flow Switches IOM

2.5.2 Documentation generated by *exida*

[R1]	exida F10 Flow Switch Sensing Unit Assemblies - Decreasing Flow Alarm.efm	FMEDA, exida F10 Flow Switch Sensing Unit Assemblies - Decreasing Flow Alarm
[R2]	exida F10 Flow Switch Sensing Unit Assemblies - Increasing Flow Alarm	FMEDA, exida F10 Flow Switch Sensing Unit Assemblies - Increasing Flow Alarm
[R3]	MAG 17-07-109 Flow_Switch_FMEDA-Summary.xlsx	F10 Flow Switch Failure Modes, Effects, and Diagnostic Analysis - Summary

3 Product Description

The MAGNETROL F10 Flow Switches are vane actuated operated units suitable for use on clean liquids or gas applications for flow alarm.

The design of MAGNETROL vane-operated F10 Flow Switches are based upon the principle that a magnetic field will penetrate non-magnetic materials such as 316 stainless steel. The vane moves a magnetic attraction sleeve within a nonmagnetic enclosing tube and actuates a switch mechanism. The enclosing tube provides a pressure seal to the chamber and therefore to the process.

This FMEDA is applicable to the Models listed below.

Models: abc-xxxx-dex

Where “abc” describes basic Model Type
“abc” = F10

“d” describes Switch Type
“d” = B, C, D, U, W, X

AND “e” describes Single Switch Mechanism
“e” = K, C, A, 1, 2 - SPDT switches
N, F, D, 8 - DPDT switches

The specific model numbers analyzed on the FMEDAs are shown in the table below along with a listing of their respective subassembly components:

Model Number	F10-4E58-(9C9)*	F10-4E58-(9F9)*
Sensing Unit	040-2201-001	040-2201-001
Switch	047-6010-001	047-6013-001
Housing	046-4143-024	046-4143-024

* The last 3 digits of the specific models listed are not valid with an F10 sensing unit because the switches are suited for high temperature applications where F10 flow switches are not, but the FMEDA is still valid because their construction and failure modes are representative of all similar switch mechanisms.

These models are representative of all F10 Flow Switches listed above and were chosen because they are the most complex.

Figure 1 shows a typical F10 Flow Switch.

Figure 1 F10 Flow Switches, Parts included in the FMEDA

Table 2 gives an overview of the different versions that were considered in the FMEDA of the F10 Flow Switches.

Table 2 Version Overview

Option 1	Decrease Flow, DPDT Switch, NO (Normally Open)
Option 2	Decrease Flow, DPDT Switch, NC (Normally Closed)
Option 3	Increase Flow, DPDT Switch, NO
Option 4	Increase Flow, DPDT Switch, NC
Option 5	Decrease Flow, SPDT, Switch NO
Option 6	Decrease Flow, SPDT, Switch NC
Option 7	Increase Flow, SPDT, Switch NO
Option 8	Increase Flow, SPDT, Switch NC

The F10 Flow Switches are classified as a Type A[2] element according to IEC 61508, having a hardware fault tolerance of 0.

[2] Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

exida performed a review of the Failure Modes, Effects, and Diagnostic Analysis that was was performed based on the Magnetrol International, Inc. documentation [D86] to [D96] in section 2.5.1 and is documented in [R1] to [R3].

4.1 Failure categories description

In order to judge the failure behavior of the F10 Flow Switches, the following definitions for the failure of the device were considered.

Fail-Safe State

Transmitter	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.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics.
No Effect (#)	Failure of a component that is part of the safety function but that has no effect on the safety function.

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.

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 [N3] which were 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 judged to be the best fit for the product and application information submitted by Magnetrol International, Inc.. It is expected that the actual number of field failures 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 the failure rate 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 F10 Flow Switches.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire F10 Flow Switches 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 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.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the F10 Flow Switches FMEDA.

Table 3 Failure rates F10 Flow Switches

Application/Device/Configuration	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	#	SFF
Decrease Flow, DPDT Switch, NO	0	251	0	210	293	55%
Decrease Flow, DPDT Switch, NC	0	151	0	310	291	33%
Increase Flow, DPDT Switch, NO	0	206	0	205	292	50%
Increase Flow, DPDT Switch, NC	0	307	0	200	294	61%
Decrease Flow, SPDT, Switch NO	0	169	0	288	230	37%
Decrease Flow, SPDT, Switch NC	0	135	0	322	230	29%
Increase Flow, SPDT, Switch NO	0	180	0	300	228	38%
Increase Flow, SPDT, Switch NC	0	180	0	300	228	38%

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

According to IEC 61508-2 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 (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 F10 Flow Switches meet the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

As an alternative to establishing architectural constraints via Route 1H or Route 2H, the user of the F10 Flow Switches may establish the architectural constraints for an element using the F10 Flow Switches per 11.4.5 of IEC 61511-1:2016. In which case the architectural constraints are SIL 2 @ HFT=0 (or SIL 3 @ HFT=1).

[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.

5 Using the FMEDA Results

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

5.1 PFD_{avg} calculation F10 Flow Switches

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 coverage for the suggested proof test is listed in Table 5.

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 undertaking 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.
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 Version History

Contract Number	Report Number	Revision Notes
Q17/07-109	MAG 17/07-109 R001 V1, R2	Revised product description in Section 3
Q17/07-109	MAG 17/07-109 R001 V1, R1	Released
Q17/07-109	MAG 17/07-109 R001 V1, R0	Draft

Reviewer: Ted Stewart, *exida*, 9/13/17
Status: Released, 9/20/17

7.3 Future enhancements

At request of client.

7.4 Release signatures

Steven Close, Senior Safety Engineer

Ted E. Stewart, CFSP
Program Development & Compliance Manager

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 determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime[4] 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.

It is the responsibility of the end user to maintain and operate the F10 Flow Switches per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 10 to 15 years is expected for the F10 Flow Switches.

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

[4] 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

The suggested proof test for the F10 Flow Switches is described in Table 4. Refer to the table in B.2 for the Proof Test Coverages.

Table 4 Suggested Proof Test – F10 Flow Switches

Step	Action
1.	Bypass the logic controller or take other action to avoid a false trip.
2.	Perform a detailed inspection of the unit inside and out for physical damage that may impact the structural integrity, and for evidence of environmental or process leaks. Repair or replace if needed.
3.	Using a calibrated multimeter set to measure electrical resistance (ohms), at the field connections measure and record the resistances across the Common (C) and the Normally Closed (NC) contacts, and the Common (C) and the Normally Open (NO) contacts.
4.	Change the process flow to cause the switch mechanism to change states.
5.	Again, measure and record the resistances across the Common (C) and the Normally Closed (NC) contacts, and the Common (C) and the Normally Open (NO) contacts.
6.	Ensure with the multimeter readings that the switch mechanism did in-fact change states at the prescribed flow rate. A closed switch contact should measure less than 1 ohm, and an open contact should measure greater than 5 megaohms.
7.	Repeat steps 3 through 6 for all other sets of switch contacts (if any).
8.	Restore the installation to normal operation.

B.2 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 5.

Table 5 Proof Test Coverage – F10 Flow Switches

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
Decrease Flow, DPDT Switch, NO	20	90%
Decrease Flow, DPDT Switch, NC	21	93%
Increase Flow, DPDT Switch, NO	8	96%
Increase Flow, DPDT Switch, NC	8	96%
Decrease Flow, SPDT, Switch NO	20	93%
Decrease Flow, SPDT, Switch NC	21	94%
Increase Flow, SPDT, Switch NO	9	97%
Increase Flow, SPDT, Switch NC	9	97%

Where $\lambda_{DU}PT$ is the dangerous failures not covered by proof test.

Appendix C *exida* Environmental Profiles

Table 6 *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[5]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[6]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[7]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[8]	G2	G3	G3	G3	G3	Compatible Material
Surge[9]						
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[10]						
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)[11]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[5] Humidity rating per IEC 60068-2-3
[6] Shock rating per IEC 60068-2-27
[7] Vibration rating per IEC 60068-2-6
[8] Chemical Corrosion rating per ISA 71.04
[9] Surge rating per IEC 61000-4-5
[10] EMI Susceptibility rating per IEC 61000-4-3
[11] 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) [N4] 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 250 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.

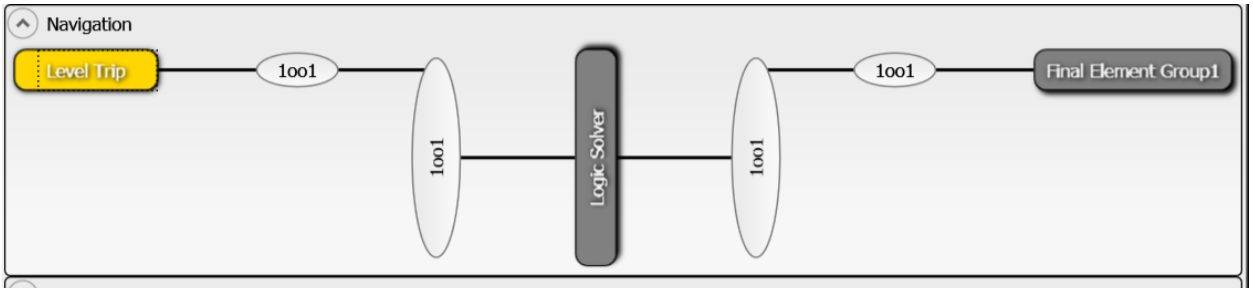
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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

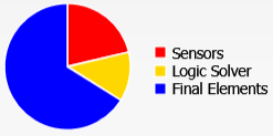
This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03. See Figure 2.



Safety Instrumented Function Results

PFDavg Contribution

MTTFS Contribution



Achieved Safety Integrity Level	2
Safety Integrity Level (PFDavg)	2
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	6.82E-03
Risk Reduction Factor (RRF)	147
☑ Mean Time to Failure Spurious (MTTFS) [years]	133.04

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	5.55E-04	620.76	2	2	2
Logic Solver Part	9.55E-06	1059.72		3	3
Final Element Part	6.26E-03	201.54		2	3

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.

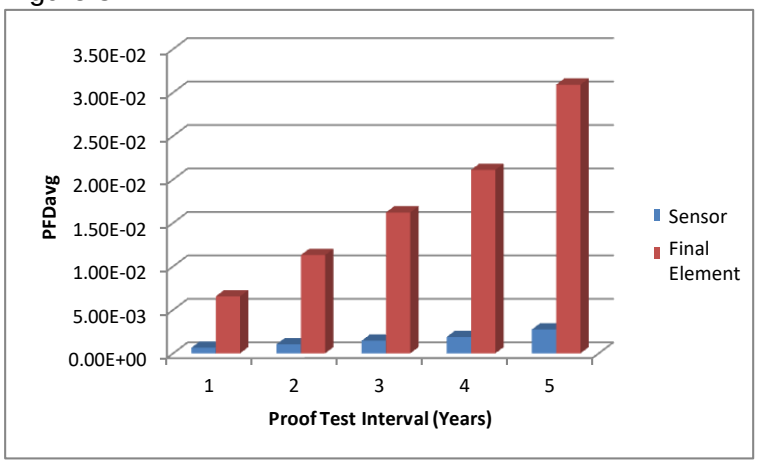


Figure 3 PFD_{avg} versus Proof Test Interval.

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).

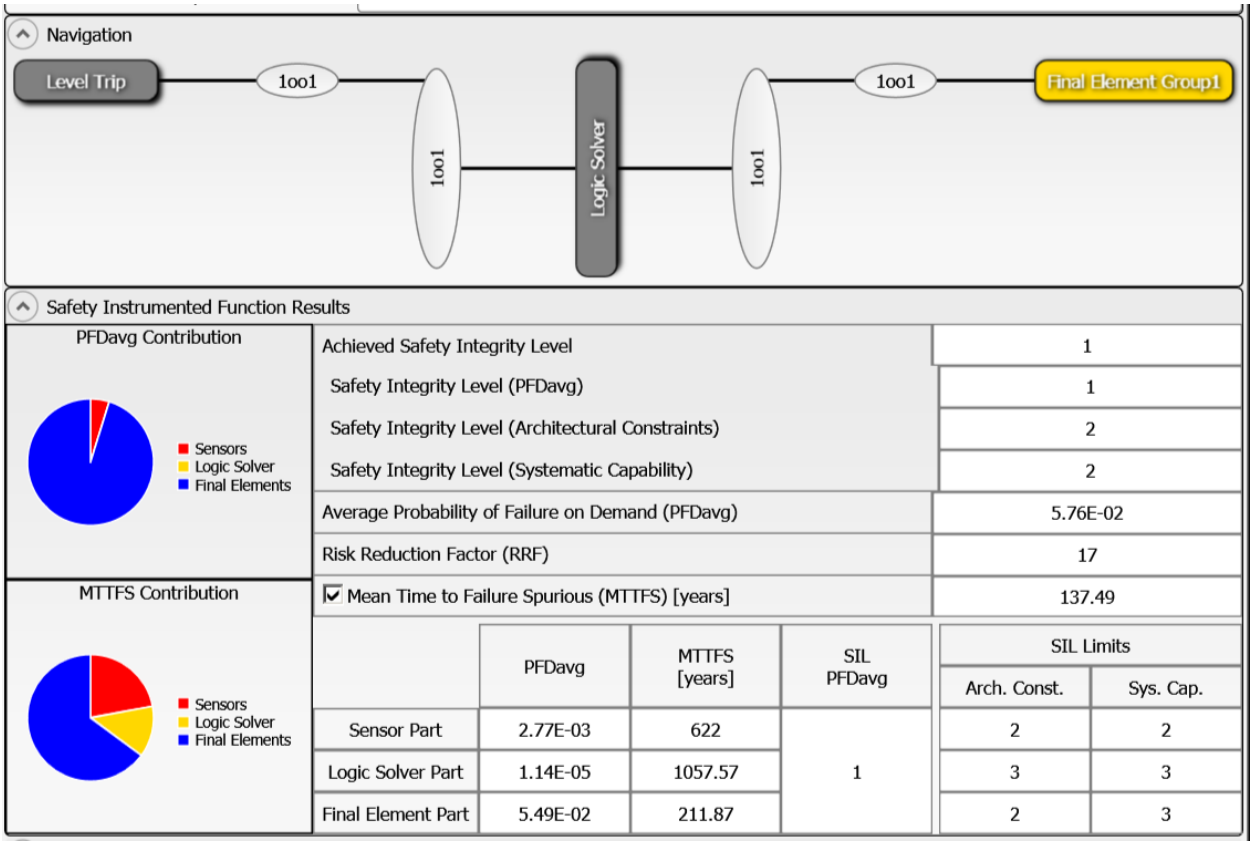


Figure 4: exSILentia results with realistic variables

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