Failure Modes, Effects and Diagnostic Analysis

Project:
3051S Electronic Remote Sensors (ERS™) System

Company:
Emerson Automation Solutions
Rosemount Inc.
Shakopee, MN
USA

Contract Number: Q16/12-041
Report No.: ROS 10/04-83 R001
Version V2, Revision R5, May 30, 2017
Loren Stewart

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 3051S Electronic Remote Sensors (ERS™) System. 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 3051S Electronic Remote Sensors (ERS™) System. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 3051S Electronic Remote Sensors (ERS™) System is a two wire, 4 – 20 mA architecture that calculates differential pressure electronically using two pressure sensors that are linked together with a digital cable. The sensor system uses standard, well-proven sensor boards in combination with a microprocessor board that performs diagnostics. It is programmed to send its output to a specified failure state, either high or low, when an internal failure is detected.

It is assumed that the 4 – 20 mA output is used as a primary safety variable. No other output variants are covered by this report.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 3051S Electronic Remote Sensors (ERS™) System.

Table 1 Version Overview

Primary Sensor Models

Model Number	Description
3051SAM_PA	Absolute pressure, coplanar sensor, measurement sensor
3051SAL_PA	Absolute pressure, coplanar sensor, level sensor
3051SAM_PD	Differential pressure, coplanar sensor, measurement sensor
3051SAL_PD	Differential pressure, coplanar sensor, level sensor
3051SAM_PG	Gage pressure, coplanar sensor, measurement sensor
3051SAL_PG	Gage pressure, coplanar sensor, level sensor
3051SAM_PE	Absolute pressure, in-line sensor, measurement sensor
3051SAL_PE	Absolute pressure, in-line sensor, level sensor
3051SAM_PT	Gage pressure, in-line sensor, measurement sensor
3051SAL_PT	Gage pressure, in-line sensor, level sensor

Secondary Sensor Models

Model Number	Description
3051SAM_SA	absolute pressure, coplanar sensor, measurement sensor
3051SAL_SA	absolute pressure, coplanar sensor, level sensor
3051SAM_SD	differential pressure, coplanar sensor, measurement sensor
3051SAL_SD	differential pressure, coplanar sensor, level sensor
3051SAM_SG	gage pressure, coplanar sensor, measurement sensor
3051SAL_SG	gage pressure, coplanar sensor, level sensor
3051SAM_SE	absolute pressure, in-line sensor, measurement sensor
3051SAL_SE	absolute pressure, in-line sensor, level sensor
3051SAM_ST	gage pressure, in-line sensor, measurement sensor
3051SAL_ST	gage pressure, in-line sensor, level sensor

The 3051S Electronic Remote Sensors (ERS™) System is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H (see Section 5.3). Therefore, the 3051S Electronic Remote Sensors (ERS™) System 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 3051S Electronic Remote Sensors (ERS™) System has a Safe Failure Fraction greater than 90% (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 3051S Electronic Remote Sensors (ERS™) System 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 3051S Electronic Remote Sensors (ERS™) System 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 3051S Electronic Remote Sensors (ERS™) System. 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 standards.

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

Rosemount Inc.	Manufacturer of the 3051S Electronic Remote Sensors (ERS™) System
exida	Performed the hardware assessment

Rosemount Inc. contracted *exida* in December 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, 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^{TM}, April 2016	Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index^{TM}, 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 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[D1]	00825-0100-4804	Quick Installation Guide, Rosemount 3051S ERS System; 00825-0100-4804 Rev AB, January 2011
[D2]	Preliminary 3051S PDS.pdf, Rev MA, March 2010	Product Data Sheet, Rosemount 3051S Series; 00813-0100-4801 Rev SB, July 2014
[D3]	3051S User Manual, Rev DA, February 2009	Reference Manual, Rosemount 3051S Series; 00809-0100-4804 Draft Rev AB, October 2014
[D4]	ERS hw architecture.pptx	3051S ERS System Electrical Architecture
[D5]	03151_3750.pdf	Schematic, Feature Board 3051S ERS System

[D6]	03151-1511.pdf	Schematic, In-Line Sensor or Strain Gage Sensor
[D7]	03151-1514.pdf	Schematic, Capacitive Sensor or Metal Cell Sensor
[D8]	03151-4270.pdf, Rev AB	Schematic, Terminal Block, Dual Compartment, 3051S ERS System
[D9]	03151-4280.pdf, Rev AB	Schematic, Terminal Block, Single Compartment, 3051S ERS System

2.4.2 Documentation generated by *exida*

[R1]	3051S ERS Feature Board100510.emf	Failure Modes, Effects, and Diagnostic Analysis – 3051S Electronic Remote Sensors (ERS™) System Feature Board
[R2]	3051S ERS Single Terminal Board100518.emf	Failure Modes, Effects, and Diagnostic Analysis – 3051S Electronic Remote Sensors (ERS™) System Single Terminal Board
[R3]	3051S ERS Dual Terminal Board100516.emf	Failure Modes, Effects, and Diagnostic Analysis – 3051S Electronic Remote Sensors (ERS™) System Dual Terminal Board
[R4]	CAN Mode SM Coplanar II 3051S Rev_AE.xls	Failure Modes, Effects, and Diagnostic Analysis –3051S Electronic Remote Sensors (ERS™) System Coplanar Board
[R5]	CAN Mode SM inline 3051T Rev_AR.xls	Failure Modes, Effects, and Diagnostic Analysis –3051S Electronic Remote Sensors (ERS™) System
[R6]	3051S_ERS_FMEDA Summary r2.xls;	Failure Modes, Effects, and Diagnostic Analysis - Summary –3051S Electronic Remote Sensors (ERS™) System

3 Product Description

The 3051S Electronic Remote Sensors (ERS™) System is a two wire, 4 – 20 mA architecture that calculates differential pressure electronically using two pressure sensors (primary and secondary) that are linked together with a digital cable. The sensor system uses standard, well-proven sensor boards in combination with a microprocessor board that performs diagnostics. It is programmed to send its output to a specified failure state, either high or low, when an internal failure is detected.

The bus between the current output microprocessor and the sensor microprocessor has been extended outside the sensor housing to a second sensor microprocessor with its own housing. This external bus is certified for the ERS system application within particular restrictions as documented in the product installation manual.

It is assumed that the 4 – 20 mA output is used as a primary safety variable. No other output variants are covered by this report.

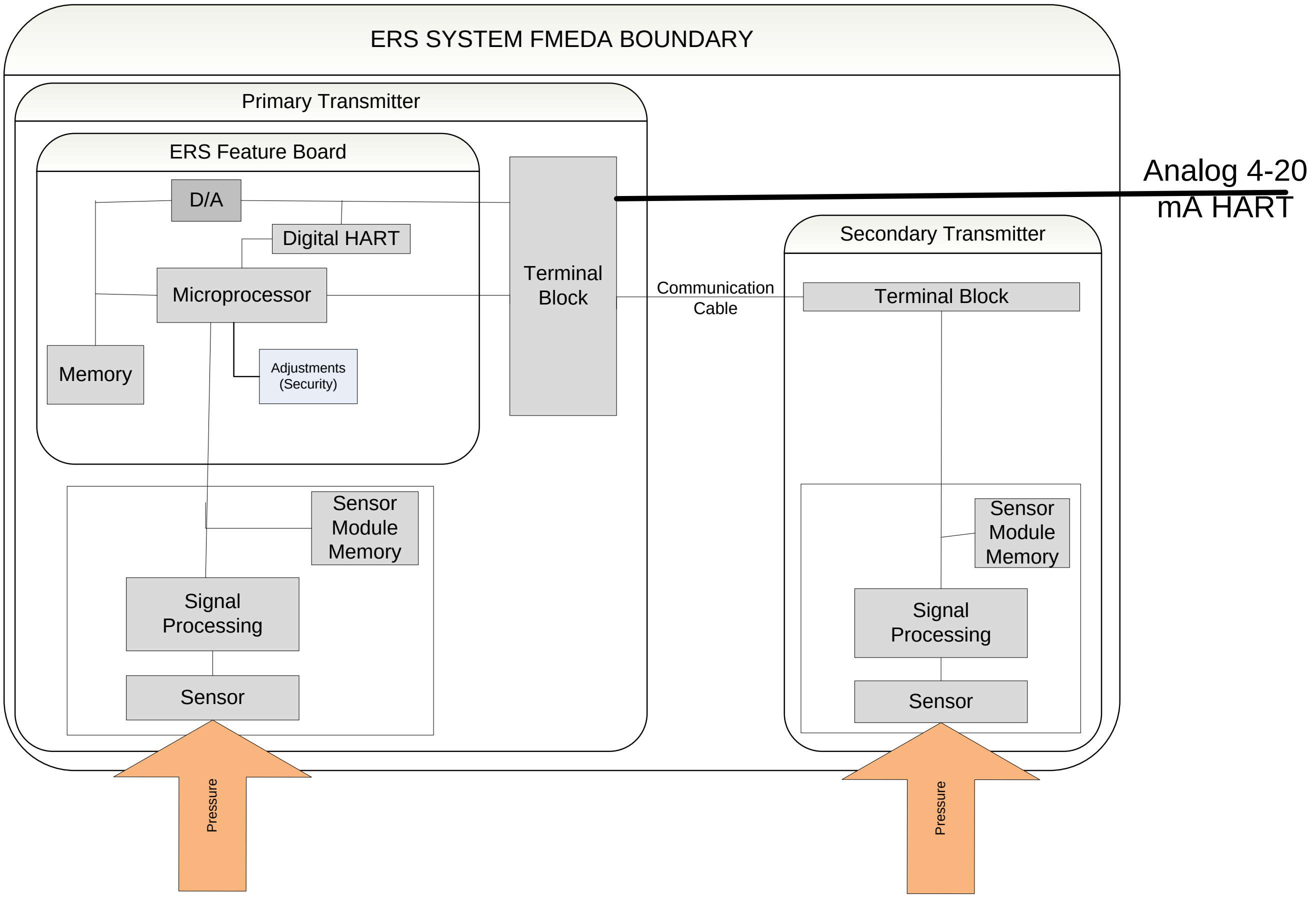


Figure 1 3051S Electronic Remote Sensors (ERS™) System, Parts included in the FMEDA

Table 2 gives an overview of the different Primary and Secondary Sensor Models. A 3051S Electronic Remote Sensors (ERS™) System consists of a Primary and a Secondary sensor.

Table 2 Version Overview

Primary Sensor Models

3051SAM_PA	Absolute pressure, coplanar sensor, measurement sensor
3051SAL_PA	Absolute pressure, coplanar sensor, level sensor
3051SAM_PD	Differential pressure, coplanar sensor, measurement sensor
3051SAL_PD	Differential pressure, coplanar sensor, level sensor
3051SAM_PG	Gage pressure, coplanar sensor, measurement sensor
3051SAL_PG	Gage pressure, coplanar sensor, level sensor
3051SAM_PE	Absolute pressure, in-line sensor, measurement sensor
3051SAL_PE	Absolute pressure, in-line sensor, level sensor
3051SAM_PT	Gage pressure, in-line sensor, measurement sensor
3051SAL_PT	Gage pressure, in-line sensor, level sensor

Secondary Sensor Models

3051SAM_SA	absolute pressure, coplanar sensor, measurement sensor
3051SAL_SA	absolute pressure, coplanar sensor, level sensor
3051SAM_SD	differential pressure, coplanar sensor, measurement sensor
3051SAL_SD	differential pressure, coplanar sensor, level sensor
3051SAM_SG	gage pressure, coplanar sensor, measurement sensor
3051SAL_SG	gage pressure, coplanar sensor, level sensor
3051SAM_SE	absolute pressure, in-line sensor, measurement sensor
3051SAL_SE	absolute pressure, in-line sensor, level sensor
3051SAM_ST	gage pressure, in-line sensor, measurement sensor
3051SAL_ST	gage pressure, in-line sensor, level sensor

The 3051S Electronic Remote Sensors (ERS™) System is classified as a Type B[2] device 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 2.4.1 and is documented in [R1] to [R6].

4.1 Failure categories description

In order to judge the failure behavior of the 3051S Electronic Remote Sensors (ERS™) System, 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 active scale.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
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 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 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 [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 2. It was judged to be the best fit for the product and application information submitted by Rosemount 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 3051S Electronic Remote Sensors (ERS™) System.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire 3051S Electronic Remote Sensors (ERS™) System 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.
- Recommended calibration intervals and replacement schedules of the electrochemical cartridge are observed and used to implement frequent proof testing of the device.
- Worst-case internal fault detection time is 1 hour.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 3051S Electronic Remote Sensors (ERS™) System FMEDA.

Table 3 Failure rates: 3051S Electronic Remote Sensors (ERS™) System for Primary Sensor with Coplanar Sensor and Secondary Sensor with Coplanar Sensor

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	319	
Fail Dangerous Detected	897	
Fail Detected (detected by internal diagnostics)	612	612
Fail High (detected by logic solver)	144	144
Fail Low (detected by logic solver)	141	141
Fail Dangerous Undetected	131	
No Effect	475	
Annunciation Detected	30	
Annunciation Undetected	45	

Table 4 Failure rates: 3051S Electronic Remote Sensors (ERS™) System for Primary Sensor with Coplanar Sensor and Secondary Sensor with In-Line Sensor or Primary Sensor with In-Line Sensor and Secondary Sensor with Coplanar Sensor

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected	237	
Fail Dangerous Detected	996	
Fail Detected (detected by internal diagnostics)	802	802
Fail High (detected by logic solver)	85	85
Fail Low (detected by logic solver)	109	109
Fail Dangerous Undetected	114	
No Effect	442	
Annunciation Detected	32	
Annunciation Undetected	45	

Table 5 Failure rates: 3051S Electronic Remote Sensors (ERS™) System (no seals) for Primary Sensor with In-Line Sensor and Secondary Sensor with In-Line Sensor

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected	156	
Fail Dangerous Detected	1095	
Fail Detected (detected by internal diagnostics)	993	
Fail High (detected by logic solver)	26	
Fail Low (detected by logic solver)	76	
Fail Dangerous Undetected	97	
No Effect	409	
Annunciation Undetected	33	
External Leak	45	

Table 6 Failure rates: 3051S Electronic Remote Sensors (ERS™) System (no 1199 seals) for Primary Sensor with Coplanar Sensor and Secondary Sensor with Coplanar Sensor

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		350
Fail Dangerous Detected		897
Fail Detected (detected by internal diagnostics)	611	
Fail High (detected by logic solver)	144	
Fail Low (detected by logic solver)	141	
Fail Dangerous Undetected		169
No Effect		478
Annunciation Undetected		30
External Leak		50

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 5.3).

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 3051S Electronic Remote Sensors (ERS™) System 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.

Table 7 lists the failure rates for the 3051S Electronic Remote Sensors (ERS™) System according to IEC 61508.

Table 7 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	**SFF**[4]
3051S ERS System, Primary Sensor with Coplanar Sensor + Secondary Sensor with Coplanar Sensor	-	319	897	131	90%
3051S ERS System, Primary Sensor with Coplanar Sensor + Secondary Sensor with In-Line Sensor or Model 3051S ERS System, Primary Sensor with In-Line Sensor + Secondary Sensor with Coplanar Sensor	-	237	996	114	92%
3051S ERS System, Primary Sensor with In-Line Sensor + Secondary Sensor with In-Line Sensor	-	156	1095	97	93%

---

[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 Impulse line clogging

The sensor can be connected to the process using impulse lines; depending on the application, the analysis needs to account for clogging of the impulse lines. The 3051S Electronic Remote Sensors (ERS™) System failure rates that are displayed in section 4.4 are failure rates that reflect the situation where the sensor is used in clean service. Clean service indicates that failure rates due to clogging of the impulse line are not counted. For applications other than clean service, the user must estimate the failure rate for the clogged impulse line and add this failure rate to the 3051S Electronic Remote Sensors (ERS™) System failure rates.

5.2 PFD_{avg} calculation 3051S Electronic Remote Sensors (ERS™) System

Using the failure rate data displayed in section 4.4, 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 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 are listed in Appendix B.

5.3 *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.
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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
PFD_{avg}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test - It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequently than the proof test; therefore, the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption, the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Severe Service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
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:	V2, R5:	Released to Rosemount Inc.; 5/30/17
	V2, R4:	Updated per customer comments; TES November 14, 2014.
	V2, R3:	Updated per customer comments; TES October 23, 2014.
	V2, R2:	Updated per customer comments; TES October 16, 2014.
	V2, R1:	Updated FMEDA to IEC 61508, 2010; TES October 1, 2014.
	V1, R1:	Released to Rosemount Inc.; June 1, 2010
	V0, R1:	Draft; 19 May 2010

Author(s): Loren Stewart

Review: V2, R5: Ted Stewart (*exida*); 5/30/17

Release Status: Released to Rosemount Inc.

7.3 Future enhancements

At request of client.

7.4 Release signatures

Loren Stewart, CFSE, Senior Safety Engineer

Ted Stewart, CFSP, 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 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[5] 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.

Table 8 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 8 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours

It is the responsibility of the end user to maintain and operate the 3051S Electronic Remote Sensors (ERS™) System per manufacturer’s instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

As there are no aluminum electrolytic capacitors used, the limiting factors with regard to the useful lifetime of the system are the tantalum electrolytic capacitors. The tantalum electrolytic capacitors have an estimated useful lifetime of about 50 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 Comprehensive Proof Test

The comprehensive proof test described in Table 9 will detect 87% of possible DU failures in the 3051S Electronic Remote Sensors (ERS™) System.

Table 9 Comprehensive 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.	Perform a two-point calibration[8] of the transmitter over the full working range.
7.	Remove the bypass and otherwise restore normal operation.

---

[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.

[8] If the two-point calibration is performed with electrical instrumentation, this proof test will not detect any failures of the sensor

Appendix C *exida* Environmental Profiles

Table 10 *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[9]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[10]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[11]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[12]	G2	G3	G3	G3	G3	Compatible Material
Surge[13]						
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[14]						
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)[15]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

---

[9] Humidity rating per IEC 60068-2-3
[10] Shock rating per IEC 60068-2-27
[11] Vibration rating per IEC 60068-2-6
[12] Chemical Corrosion rating per ISA 71.04
[13] Surge rating per IEC 61000-4-5
[14] EMI Susceptibility rating per IEC 61000-4-3
[15] 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$^{\text{TM}}$ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

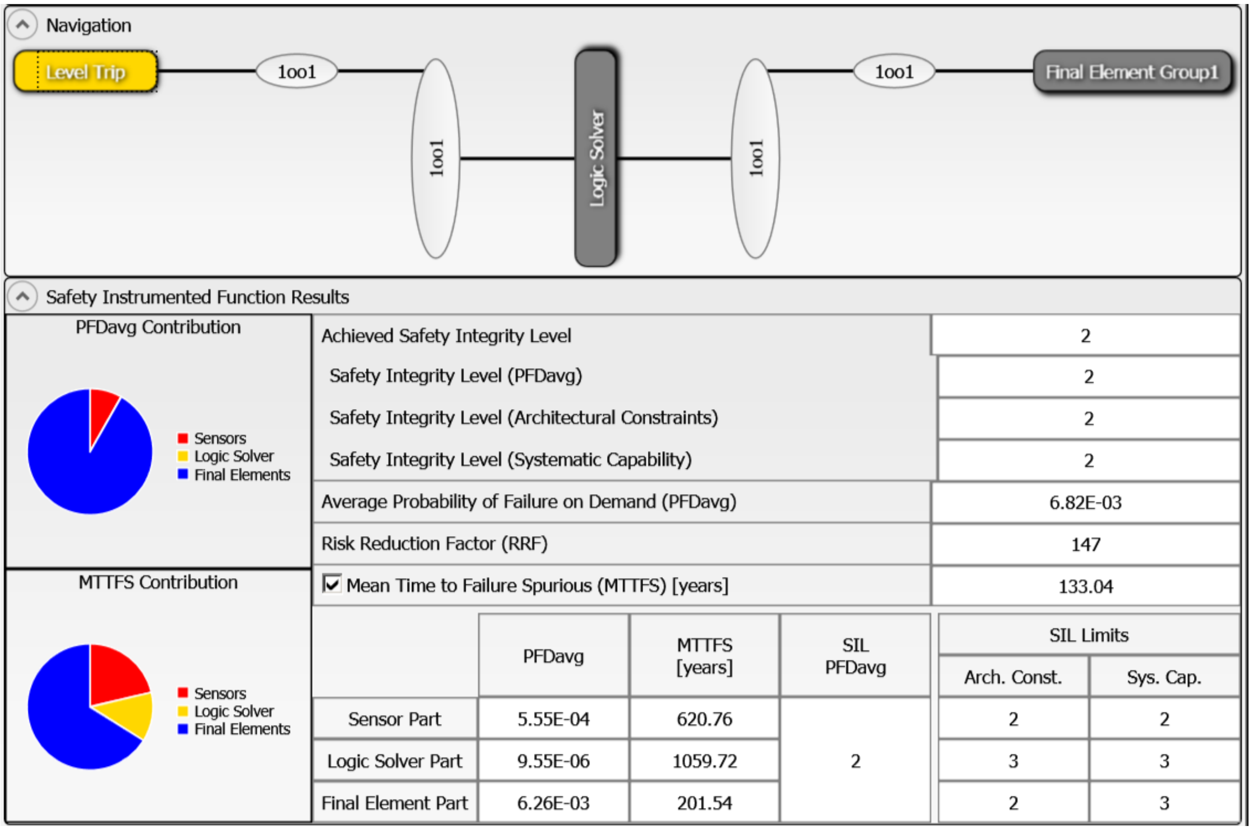
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic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



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.

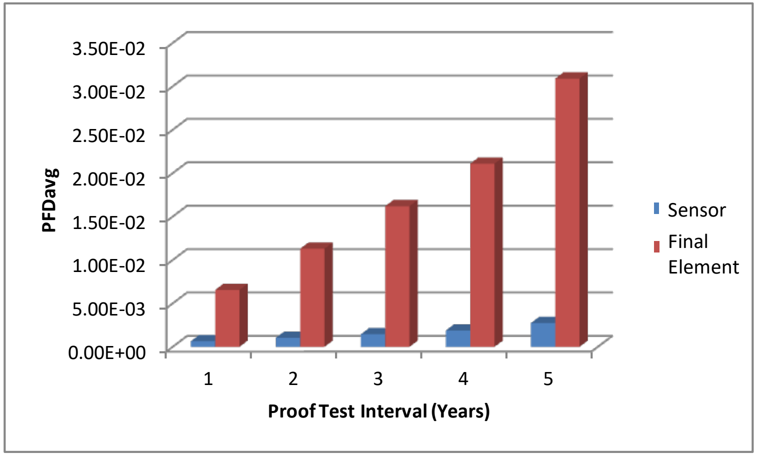
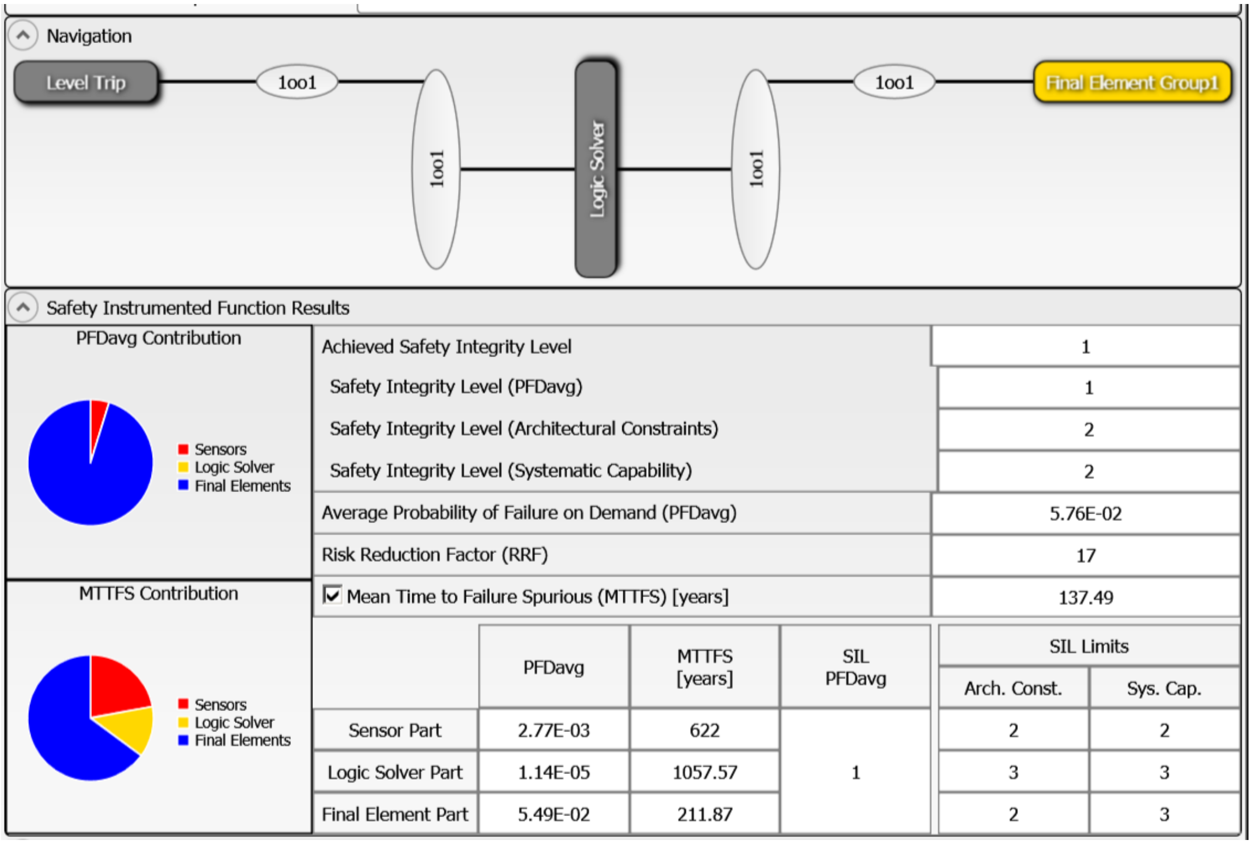


Figure 3 PFD_{avg} versus Proof Test Interval.

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).



Achieved Safety Integrity Level	1
Safety Integrity Level (PFDavg)	1
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	5.76E-02
Risk Reduction Factor (RRF)	17
☑ Mean Time to Failure Spurious (MTTFS) [years]	137.49

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	2.77E-03	622	1	2	2
Logic Solver Part	1.14E-05	1057.57		3	3
Final Element Part	5.49E-02	211.87		2	3

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.