



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

Emerson Automation Solution  
Rosemount® 2090 Pressure Transmitter with 4-20 mA HART  
Device Label SW 1.0.0-1.4.x

Company:

Rosemount Inc.  
Shakopee, MN  
USA

Contract No.: Q17/11-003

Report No.: ROS 11/07-062 R004

Version V2, Revision R4, January 15, 2018

Ted Stewart

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

© All rights reserved.

## Management Summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART, Device Label SW 1.0.0-1.4.x. 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 and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the Rosemount 2090 Pressure Transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Rosemount 2090 Pressure Transmitter is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage, it is assumed that the 4 – 20 mA output is used as the primary safety variable.

Table 1 lists the versions of the Rosemount 2090 Pressure Transmitter that have been considered for the hardware assessment.

**Table 1 Version Overview**

Option 1	Emerson's Rosemount 2090 Pressure Transmitter with 4-20mA In-Line
----------	---

The Rosemount 2090 Pressure Transmitter is classified as a Type B<sup>1</sup> device according to IEC 61508, having a hardware fault tolerance of 0.

The failure rates for the Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART are listed in Table 2.

**Table 2 Failure rates Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART**

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	94
Fail Dangerous Detected	279
Fail Detected (detected by internal diagnostics)	222
Fail High (detected by logic solver)	29
Fail Low (detected by logic solver)	28
Fail Dangerous Undetected	41
No Effect	88
Annunciation Undetected	14
External Leak	23

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

<sup>1</sup> 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.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

The analysis shows that the reviewed 2090 models have a Safe Failure Fraction  $\geq 90\%$  (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets Route 1<sub>H</sub> hardware architectural constraints for up to SIL 2 as a single device.

The failure rate data used for this analysis meets the *exida* criteria for Route 2<sub>H</sub> and the diagnostic coverage is  $\geq 60\%$ . Route 2<sub>H</sub> has over 25 billion supporting operating hours. Therefore, the reviewed Rosemount® 2090 meets the hardware architectural constraints for up to SIL 2 as a single device when the listed failure rates are used.

Table 3 lists the failure rates for the Rosemount 2090 Pressure Transmitter according to IEC 61508, ed2, 2010.

**Table 3 Failure rates according to IEC 61508 in FIT for the Rosemount 2090 Pressure Transmitter**

Device	$\lambda_{SD}$	$\lambda_{SU}^2$	$\lambda_{DD}$	$\lambda_{DU}$	SFF <sup>3</sup>
2090 4-20mA In-Line Pressure Transmitter	-	94	279	41	90%

A user of the Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART 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). A full table of failure rates is presented in section 4.4 along with all assumptions.

<sup>2</sup> 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.

<sup>3</sup> Safe Failure Fraction is calculated for the entire element when following Route 1<sub>H</sub>, or is not required when following Route 2<sub>H</sub> architectural constraints, for details see 7.4.4 of IEC 61508, ed2, 2010

## Table of Contents

Management Summary .....	2
1 Purpose and Scope .....	6
2 Project Management.....	7
2.1 exida .....	7
2.2 Roles of the parties involved .....	7
2.3 Standards / Literature used .....	7
2.4 exida Tools Used.....	8
2.5 Reference Documents.....	8
2.5.1 Documentation provided by Rosemount Inc. ....	8
2.5.2 Documentation generated by exida .....	9
3 Product Description .....	10
3.1 Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART .....	10
4 Failure Modes, Effects, and Diagnostics Analysis .....	11
4.1 Failure categories description.....	11
4.2 Methodology – FMEDA, failure rates.....	12
4.2.1 FMEDA.....	12
4.2.2 Failure rates .....	12
4.3 Assumptions .....	13
4.4 Results.....	14
5 Using the FMEDA results .....	16
5.1 Impulse line clogging.....	16
5.2 PFD <sub>AVG</sub> Calculation – Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART .....	16
5.3 exida Route 2 <sub>H</sub> Criteria .....	17
6 Terms and Definitions.....	18
7 Status of the Document .....	19
7.1 Liability.....	19
7.2 Version History.....	19
7.3 Future Enhancements.....	19
7.4 Release Signatures.....	19
Appendix A Lifetime of Critical Components.....	20
Appendix B Proof tests to reveal dangerous undetected faults .....	21
B.1 Suggested Partial Proof Test.....	21
B.2 Suggested Comprehensive Proof Test.....	22
B.3 Proof Test Coverage .....	22

Appendix C exida Environmental Profiles ..... 23  
Appendix D Determining Safety Integrity Level..... 24  
Appendix E Site Safety Index ..... 28  
    E.1 Site Safety Index Profiles ..... 28  
    E.2 Site Safety Index Failure Rates ..... 29

## 1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) carried out on the Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART. From this, failure rates and example  $PFD_{AVG}$  values may be calculated.

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.

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

### 2.2 Roles of the parties involved

Rosemount Inc.                                      Manufacturer of Emerson's Rosemount 2090 Pressure Transmitter  
*exida*    Performed the hardware assessment

Rosemount Inc. contracted *exida* with the hardware assessment of the above-mentioned device.

### 2.3 Standards / Literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	<i>exida</i> LLC, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3 <sup>rd</sup> 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	<i>exida</i> 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, <a href="http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers">http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers</a>
[N8]	Meeting Architecture Constraints in SIF Design,	<a href="http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design">http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design</a>

	Recorded Web Seminar, March 2013	
[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, <a href="http://www.exida.com/resources/whitepapers">www.exida.com/resources/whitepapers</a> , 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, <a href="http://www.exida.com">www.exida.com</a> , 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, <a href="http://www.exida.com">www.exida.com</a> , June 2015.

## 2.4 exida Tools Used

[T1]	Tool Version 7.1.17	FMEDA Tool
[T2]	Tool Version 3.0.8.758	exSILentia

## 2.5 Reference Documents

### 2.5.1 Documentation provided by Rosemount Inc.

(Reference documents list hidden due to their proprietary nature.)



## 2.5.2 Documentation generated by *exida*

[R1]	MicroBoard_25Oct2013.emf	Failure Modes, Effects, and Diagnostic Analysis – Rosemount 2090 Pressure Transmitter Microboard
[R2]	Terminal Board2.emf	Failure Modes, Effects, and Diagnostic Analysis – Emerson’s Rosemount® Pressure Transmitter with 4-20 mA HART Transient Protected Terminal Board
[R3]	TAC Sensor (T)_1Feb2012.emf	Failure Modes, Effects, and Diagnostic Analysis – Emerson’s Rosemount Pressure Transmitter with 4-20 mA HART Sensor T Board
[R4]	FMEDA Summary_1Feb2012.xls	Failure Modes, Effects, and Diagnostic Analysis - Summary – Emerson’s Rosemount Pressure Transmitter with 4-20 mA HART
[R5]	ROS 17-11-003 R002 V1R1 2090 FMEDA-web.doc	FMEDA report, Emerson’s Rosemount 2090 Pressure Transmitter with 4-20 mA HART (this report)
[R6]	Rosemount 2090 FMEDA 04-19-2016.efm	Failure Modes, Effects, and Diagnostic Analysis - Summary – Emerson’s Rosemount 2090 Transmitter with 4-20 mA HART

### 3 Product Description

#### 3.1 Emerson’s Rosemount 2090 Pressure Transmitter with 4-20 mA HART

Emerson’s Rosemount 2090 Pressure Transmitter with 4-20 mA HART is used in the Hygienic, Pulp and Paper industries for both control and safety applications.

The major components of the Rosemount 2090 are the sensor module and the electronics housing. The sensor module contains the oil filled sensor system. The electrical signals from the sensor module are transmitted to the output electronics and then to the terminal block for connection to the host system. The basic block diagram of the Rosemount 2090 is shown in Figure 1.

Emerson’s Rosemount 2090P and Rosemount 2090F are within the scope of this FMEDA where the In-line Gage and Absolute Piezoresistive sensor technology is used for the In-Line measurements.

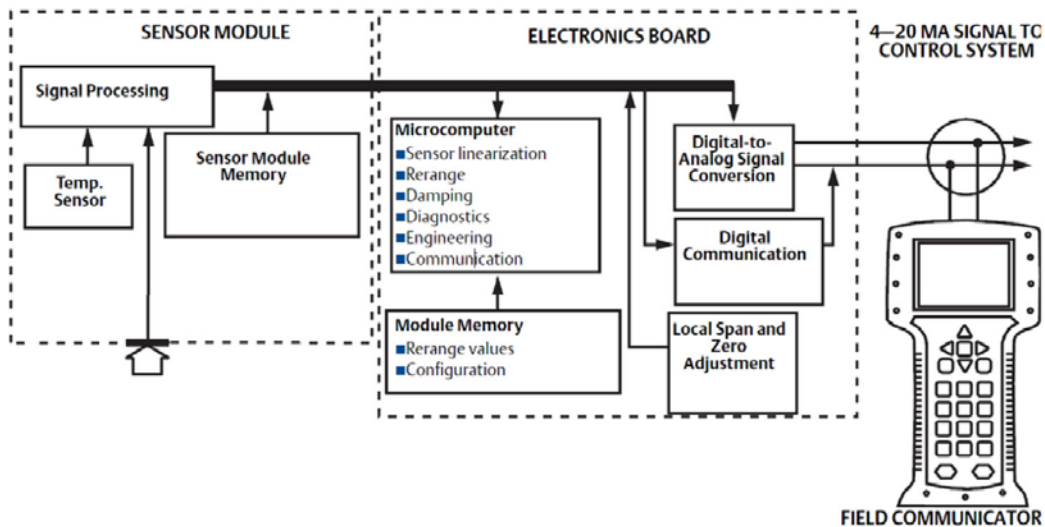


Figure 1 –Rosemount 2090 Pressure Transmitter Block Diagram

The Rosemount 2090 Pressure Transmitter is classified as a Type B<sup>4</sup> device according to IEC 61508, having a hardware fault tolerance of 0.

<sup>4</sup> Type B device: “Complex” component (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

## 4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on documentation obtained from Rosemount Inc. and is documented in 2.5.1.

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. This resulted in failures that can be classified according to the following failure categories.

### 4.1 Failure categories description

In order to judge the failure behavior of the Rosemount 2090 Pressure Transmitter, the following definitions for the failure of the product 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
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current
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.
External Leak	Failure that causes process fluids to leak inside the instrument or to the environment. External leakage is not considered part of the safety function and therefore this failure is not included in the Safe Failure Fraction calculation.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore, they are not used for the Safe Failure Fraction calculation needed when Route 2<sub>H</sub> failure data is not available.

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. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

External leakage failure rates do not directly contribute to the reliability of a component but should be reviewed for secondary safety and environmental issues.

## 4.2 Methodology – FMEDA, failure rates

### 4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

### 4.2.2 Failure rates

The 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] 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 as this 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.

numbers shall be used.

### 4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Rosemount 2090 Pressure Transmitter.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 with temperature limits within the manufacturer's rating. *exida* Profile 6 was used for the process wetted components. Other environmental characteristics are assumed to be within manufacturer's rating.
- 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 per manufacturer's instructions.
- The Transmitter is generally applied in relatively clean gas or liquid; therefore, no severe service has been considered in the analysis of the base Transmitter.
- Breakage or plugging of any inlet lines has not been included in the analysis.
- External power supply failure rates are not included.
- Worst-case internal fault detection is less than one hour.

## 4.4 Results

Using reliability data extracted from the *exida* component reliability database the following failure rates resulted from the Rosemount 2090 Pressure Transmitter FMEDA.

Table 4 lists the failure rates for the Rosemount 2090 Pressure Transmitter according to IEC 61508, ed2, 2010.

**Table 4 Failure rates for Emerson’s Rosemount 2090 Pressure Transmitter with 4-20 mA HART**

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	94	
Fail Dangerous Detected	279	
Fail Detected (detected by internal diagnostics)	222	
Fail High (detected by logic solver)	29	
Fail Low (detected by logic solver)	28	
Fail Dangerous Undetected	41	
No Effect	88	
Annunciation Undetected	14	
External Leak	23	

External leakage failure rates do not directly contribute to the reliability of the device but should be reviewed for secondary safety and environmental issues.

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

Table 5 lists the failure rates for the Rosemount 2090 Pressure Transmitter according to IEC 61508, ed2, 2010.

**Table 5 Failure rates according to IEC 61508 in FIT for the Rosemount 2090 Pressure Transmitter**

Device	$\lambda_{SD}$	$\lambda_{SU}^6$	$\lambda_{DD}$	$\lambda_{DU}$	SFF <sup>7</sup>
2090 4-20mA In-Line Pressure Transmitter	-	94	279	41	90%

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1<sub>H</sub> approach according to 7.4.4.2 of IEC 61508 or the 2<sub>H</sub> approach according to 7.4.4.3 of IEC 61508.

The 1<sub>H</sub> approach involves calculating the Safe Failure Fraction for the entire element.

<sup>6</sup> 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.

<sup>7</sup> Safe Failure Fraction is calculated for the entire element when following Route 1<sub>H</sub>, or is not required when following Route 2<sub>H</sub> architectural constraints, for details see 7.4.4 of IEC 61508, ed2, 2010

The 2<sub>H</sub> approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The analysis shows that the reviewed Rosemount 2090 has a Safe Failure Fraction > 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets Route 1<sub>H</sub> hardware architectural constraints for up to SIL 2 as a single device.

The failure rate data used for this analysis meets the *exida* criteria for Route 2<sub>H</sub> and the diagnostic coverage is ≥60%. Route 2<sub>H</sub> has over 25 billion supporting operating hours. Therefore, the reviewed Rosemount® 2090 meets the hardware architectural constraints for up to SIL 2 as a single device when the listed failure rates are used.

The Hardware Random Capability for the Rosemount 2090 Pressure Transmitter for both the Route 1<sub>H</sub> and Route 2<sub>H</sub> approach is SIL 2 @HFT=0 and SIL 3 @HFT=1.

The architectural constraint type for the Rosemount 2090 Pressure Transmitter is a Type B Element. The required SIL determines the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

## 5 Using the FMEDA results

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

### 5.1 Impulse line clogging

The transmitter 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 Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART failure rates displayed in section 4.4 are failure rates that reflect the situation where the transmitter 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 Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART failure rates.

### 5.2 PFD<sub>AVG</sub> Calculation – Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART

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<sub>avg</sub>) calculation can be performed for the element.

Probability of Failure on Demand (PFD<sub>avg</sub>) 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<sub>avg</sub>) 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<sub>avg</sub> 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<sub>avg</sub>) 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<sub>avg</sub> 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<sub>avg</sub> calculation. The proof test coverage for the suggested proof test and the dangerous failure rate after proof test for the Emerson's Rosemount 2090 Pressure Transmitter with 4-20 mA HART are listed in Table 9.



### 5.3 *exida* Route 2<sub>H</sub> Criteria

IEC 61508, ed2, 2010 describes the Route 2<sub>H</sub> alternative to Route 1<sub>H</sub> 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<sub>H</sub>, *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" 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.

## 6 Terms and Definitions

Automatic diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
<i>exida</i> criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2 <sub>H</sub> Route in IEC 61508-2.
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD <sub>AVG</sub>	Average Probability of Failure on Demand
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
Severe service	Condition that exists when the process media 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, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three-year period should be sufficient for current usage without significant question.

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

### 7.2 Version History

Contract Number	Report Number	Revision Notes
Q17/11-003	ROS 17-11-003 R002 V1R1	2090P&F report now released
Q17/11-003	ROS 17-11-003 R002 V1R0	Draft

Reviewer: William Goble, *exida*, Jan. 11, 2018

Status: Released

### 7.3 Future Enhancements

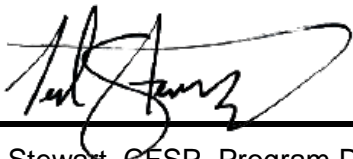
At request of client.

### 7.4 Release Signatures



---

Dr. William M. Goble, CFSE, Principal Partner



---

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 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<sup>8</sup> 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 6 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 6 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 Rosemount 2090 Pressure Transmitter 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 tantalum electrolytic capacitors are the limiting factors with regard to the useful lifetime of the system. The tantalum electrolytic capacitors that are used in the Rosemount 2090 Pressure Transmitter have an estimated useful lifetime of about 50 years.

---

<sup>8</sup> 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 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 Partial Proof Test

The suggested proof test described in Table 7 will detect 41% of possible DU failures in the Rosemount 2090 Pressure Transmitter.

**Table 7 Steps for Simple Proof Test**

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 <sup>9</sup> .
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 <sup>10</sup> .
5.	Inspect the Transmitter for any leaks, visible damage or contamination.
6.	Remove the bypass and otherwise restore normal operation

---

<sup>9</sup> 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.

<sup>10</sup> This tests for possible quiescent current related failures.

## B.2 Suggested Comprehensive Proof Test

The suggested proof test described in Table 8 will detect 90% of possible DU failures in the Rosemount 2090 Pressure Transmitter.

**Table 8 Steps for Comprehensive Proof Test**

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 <sup>11</sup> .
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 <sup>12</sup> .
5.	Inspect the Transmitter for any leaks, visible damage or contamination.
6.	Perform a two-point calibration validation of the transmitter over the full working range.
7.	Remove the bypass and otherwise restore normal operation

## B.3 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 9.

**Table 9 Proof Test Coverage – Rosemount 2090 Pressure Transmitter**

Device	Simple	Comprehensive
Rosemount 2090 Pressure Transmitter	41%	90%

---

<sup>11</sup> 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.

<sup>12</sup> This tests for possible quiescent current related failures.

## Appendix C *exida* Environmental Profiles

Table 10 *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
<b>Description (Electrical)</b>	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
<b>Description (Mechanical)</b>	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
<b>IEC 60654-1 Profile</b>	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
<b>Average Ambient Temperature</b>	30 C	25 C	25 C	5 C	25 C	25 C
<b>Average Internal Temperature</b>	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
<b>Daily Temperature Excursion (pk-pk)</b>	5 C	25 C	25 C	0 C	25 C	N/A
<b>Seasonal Temperature Excursion (winter average vs. summer average)</b>	5 C	40 C	40 C	2 C	40 C	N/A
<b>Exposed to Elements / Weather Conditions</b>	No	Yes	Yes	Yes	Yes	Yes
<b>Humidity<sup>13</sup></b>	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
<b>Shock<sup>14</sup></b>	10 g	15 g	15 g	15 g	15 g	N/A
<b>Vibration<sup>15</sup></b>	2 g	3 g	3 g	3 g	3 g	N/A
<b>Chemical Corrosion<sup>16</sup></b>	G2	G3	G3	G3	G3	Compatible Material
<b>Surge<sup>17</sup></b>						
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	
<b>EMI Susceptibility<sup>18</sup></b>						
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	
<b>ESD (Air)<sup>19</sup></b>	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

<sup>13</sup> Humidity rating per IEC 60068-2-3

<sup>14</sup> Shock rating per IEC 60068-2-6

<sup>15</sup> Vibration rating per IEC 60770-1

<sup>16</sup> Chemical Corrosion rating per ISA 71.04

<sup>17</sup> Surge rating per IEC 61000-4-5

<sup>18</sup> EMI Susceptibility rating per IEC 6100-4-3

<sup>19</sup> 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<sub>avg</sub> 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<sub>avg</sub>) 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<sub>avg</sub>) 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 PFDavg 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 PFDavg 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 PFDavg of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFDavg contributions are Sensor PFDavg = 5.55E-04, Logic Solver PFDavg = 9.55E-06, and Final Element PFDavg = 6.26E-03. See Figure 2.

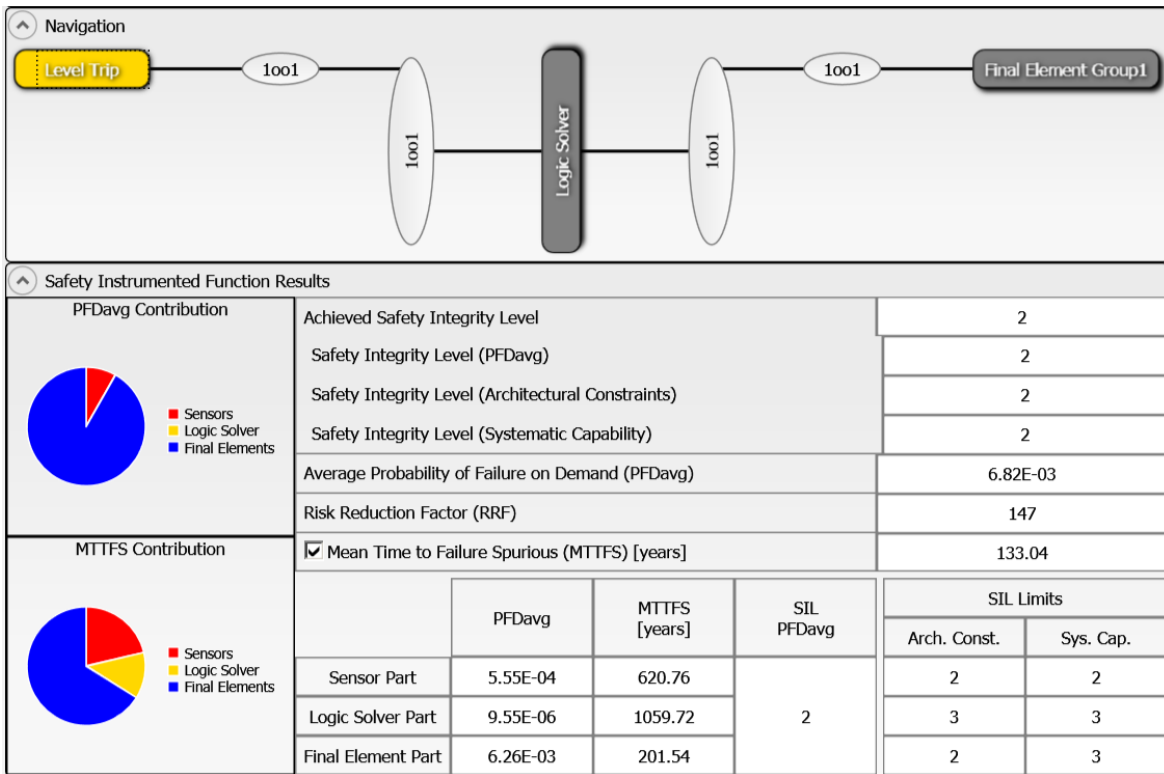


Figure 2: exSILentia results for idealistic variables.

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

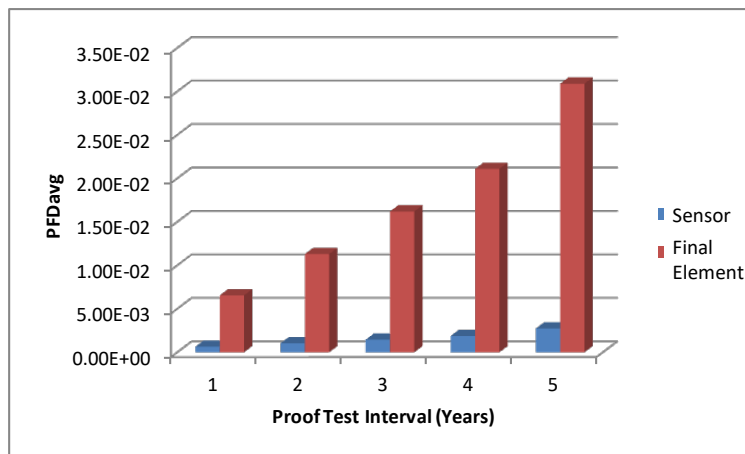


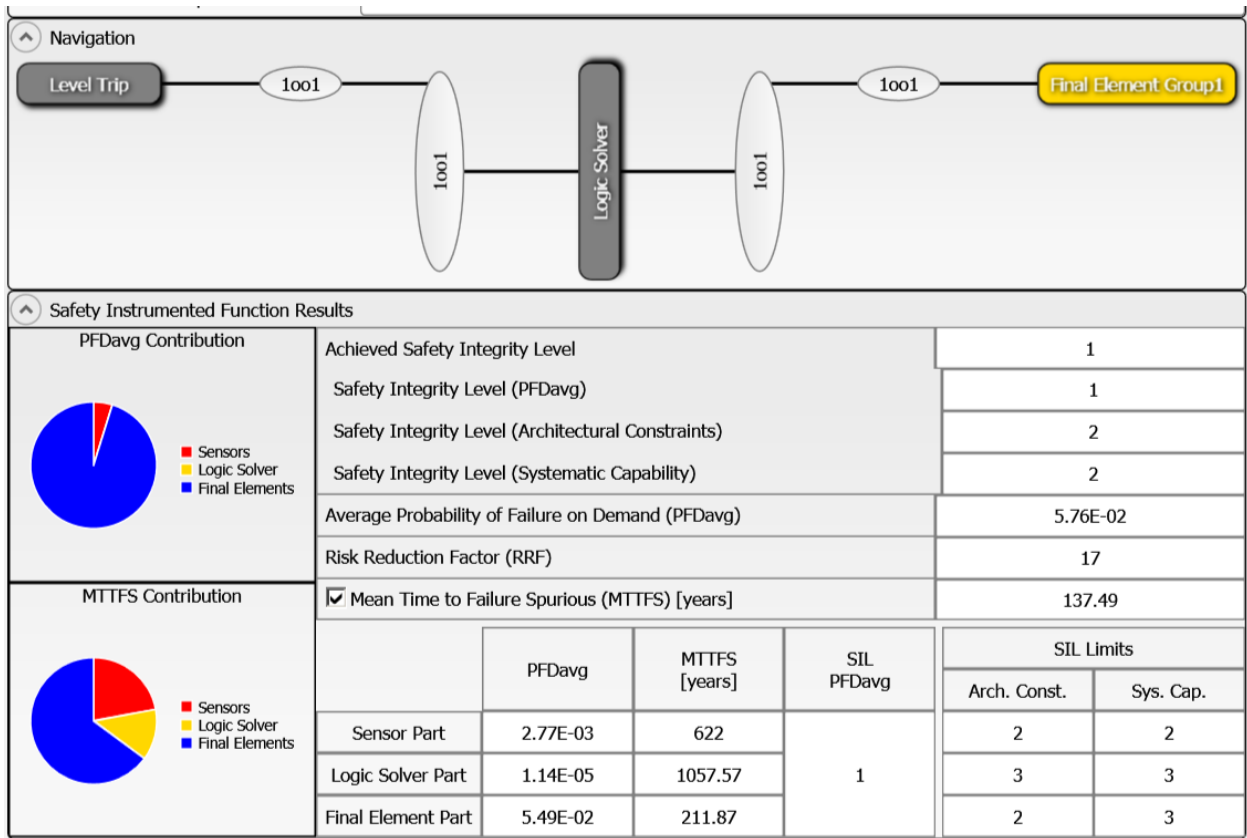
Figure 3 PFDavg versus Proof Test Interval.

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 PFDavg for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFDavg contributions are Sensor PFDavg = 2.77E-03, Logic Solver PFDavg = 1.14E-05, and Final Element PFDavg = 5.49E-02 (Figure 4).



**Figure 4: exSILentia results with realistic variables**

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

## Appendix E Site Safety Index

Numerous field failure studies have shown that the failure rate for a specific device (same Manufacturer and Model number) will vary from site to site. The Site Safety Index (SSI) was created to account for these failure rates differences as well as other variables. The information in this appendix is intended to provide an overview of the Site Safety Index (SSI) model used by *exida* to compensate for site variables including device failure rates.

### E.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 11 details the interpretation of each SSI level. Note that the levels mirror the levels of SIL assignment and that SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site and therefore there is no degradation in safety performance due to any end-user activities or practices, i.e., that the product inherent safety performance is achieved.

Several factors have been identified thus far which impact the Site Safety Index (SSI). These include the quality of:

- Commission Test
- Safety Validation Test
- Proof Test Procedures
- Proof Test Documentation
- Failure Diagnostic and Repair Procedures
- Device Useful Life Tracking and Replacement Process
- SIS Modification Procedures
- SIS Decommissioning Procedures and others

**Table 11 *exida* Site Safety Index Profiles**

Level	Description
<b>SSI 4</b>	Perfect - Repairs are always correctly performed, Testing is always done correctly and on schedule, equipment is always replaced before end of useful life, equipment is always selected according to the specified environmental limits and process compatible materials. Electrical power supplies are clean of transients and isolated, pneumatic supplies and hydraulic fluids are always kept clean, etc. Note: This level is generally considered not possible but retained in the model for comparison purposes.
<b>SSI 3</b>	Almost perfect - Repairs are correctly performed, Testing is done correctly and on schedule, equipment is normally selected based on the specified environmental limits and a good analysis of the process chemistry and compatible materials. Electrical power supplies are normally clean of transients and isolated, pneumatic supplies and hydraulic fluids are mostly kept clean, etc. Equipment is replaced before end of useful life, etc.
<b>SSI 2</b>	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.
<b>SSI 1</b>	Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.
<b>SSI 0</b>	None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.

## **E.2 Site Safety Index Failure Rates**

Failure rates of each individual device in the SIF are increased or decreased by a specific multiplier which is determined by the SSI value and the device itself. It is known that final elements are more likely to be negatively impacted by less than ideal end-user practices than are sensors or logic solvers. By increasing or decreasing device failure rates on an individual device basis, it is possible to more accurately account for the effects of site practices on safety performance.