Failure Modes, Effects and Diagnostic Analysis

Project:
Rosemount Remote Seals

Company:
Rosemount Inc.
(an Emerson Process Management company)
Chanhassen, MN
USA

Contract Number: Q11/05-075
Report No.: ROS 11/05-075 R001
Version V2, Revision R1, October 8, 2015
Gregory Sauk & William Goble

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 Remote Seals offered by Rosemount for their Pressure Transmitters. 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 Remote Seal. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

A Remote Seal System consists of one or two diaphragm seals, a fill fluid, and either a direct mount or capillary style connection to a pressure transmitter. These devices are used to protect a transmitter from the process conditions. Rosemount Remote Seals (internally designated as 1199) can be attached to Rosemount 3051S, 3051, 2051, 3095, and 2088 differential, gage, and absolute pressure transmitters. Rosemount remote seals are also offered combined with a pressure transmitter as part of Rosemount 3051SAL, 3051L, and 2051L level transmitters.

Table 1 gives an overview of the different versions that were considered in this FMEDA of the Remote Seal. The Thermal Range Expander option has also been included in this analysis.

Table 1 Version Overview

Gage, Absolute, Differential or Level	1 Remote Seal (high side or low side) - High Trip, Normal Service
	1 Remote Seal (high side or low side) - High Trip, Severe Service
	1 Remote Seal (high side or low side) - Low Trip, Normal Service
	1 Remote Seal (high side or low side) - Low Trip, Severe Service
Differential or Level	2 Remote Seals - High Trip, Normal Service
	2 Remote Seals - High Trip, Severe Service
	2 Remote Seals - Low Trip, Normal Service
	2 Remote Seals - Low Trip, Severe Service

An attached Remote Seal is classified as a Type A[1] device that is part of an 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 5.2). Therefore the Remote Seal can be classified as a 2_H device when the listed failure rates are used. When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H. If Route 2_H is not applicable for the entire sensor element, the architectural constraints will need to be evaluated per Route 1_H.

Based on the assumptions listed in 4.3, the incremental failure rates for a Remote Seal System are listed in section 4.4.

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

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

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.

A user of the Remote Seal 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).

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 a Remote Seal System. 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.

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

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety 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 the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

2.2 Roles of the parties involved

Rosemount Inc.	Manufacturer of the Remote Seal System
exida	Performed the hardware assessment

Rosemount contracted *exida* in March 2011 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]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[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

2.4 Reference documents

2.4.1 Documentation provided by Rosemount

[D1]	Exida-Installation.ppt, 25-Jun-2010	1199 FFW Flush Flanges Seal Details
[D2]	exida seal.pdf, 6-Jun-2010	Raw Seal Assy Dwg
[D3]	EXIDA DRAWING, Rev AA	Remote Seal System Assy Dwg
[D4]	RFWSECTION, Rev AA	Remote Seal Cross Section Assy Dwg
[D5]	Rosemount Remote Seals-Exida(2).pptx, 23-Jun-2010	All-Welded Configuration Details
[D6]	01199-1100, Rev AB, 22-Dec-2014	Double Diaphragm Assembly Kit Assy Dwg

2.4.2 Documentation generated by *exida*

[R1]	Rosemount Remote Seal FMEDA TRE-R13.xls, 27-Aug-2015	Failure Modes, Effects, and Diagnostic Analysis – Remote Seal (internal document)
[R2]	ROS 11/05-075 R001, V2R1, 8-Oct-2015	FMEDA report, Rosemount Remote Seals (this report)

3 Product Description

A Remote Seal System consists of one or two diaphragm seals, a fill fluid, and either a direct mount or capillary style connection to a pressure transmitter. These devices are used to protect a transmitter from the process conditions. Rosemount Remote Seals (internally designated as 1199) can be attached to Rosemount 3051S, 3051, 2051, 3095, and 2088 differential, gage, and absolute pressure transmitters. Rosemount remote seals are also offered combined with a pressure transmitter as part of Rosemount 3051SAL, 3051L, and 2051L level transmitters.

A Remote Seal is used in applications where:

- The process fluid can easily foul impulse lines (solids in suspension or highly viscous)
- The process fluid can solidify in impulse lines or the transmitter
- The transmitter must be located in a separate area
- The environmental conditions exceed the ratings of the transmitter

This FMEDA covers the mechanical elements of the Remote Seal and Thermal Range Expander only (Figure 1 and Figure 2).

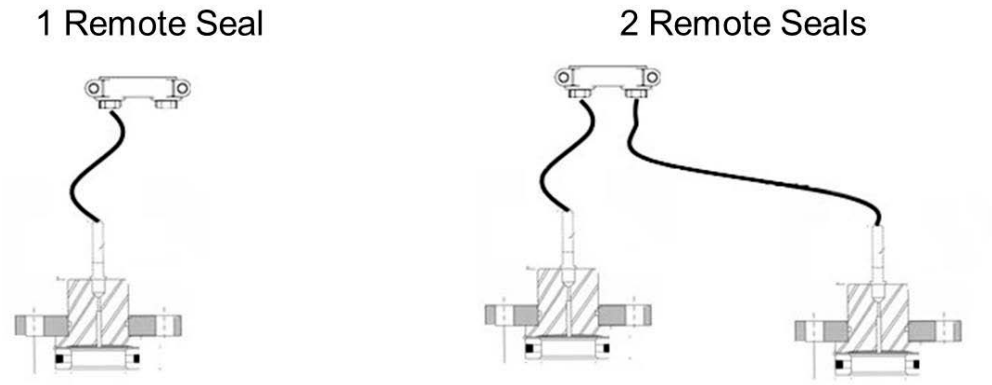


Figure 1 Remote Seals, Parts included in this FMEDA,

Table 2 gives an overview of the different versions that were considered in the FMEDA of the Remote Seal.

Table 2 Version Overview

Gage, Absolute, Differential or Level	1 Remote Seal (high side or low side) - High Trip, Normal Service
	1 Remote Seal (high side or low side) - High Trip, Severe Service
	1 Remote Seal (high side or low side) - Low Trip, Normal Service
	1 Remote Seal (high side or low side) - Low Trip, Severe Service
Differential or Level	2 Remote Seals - High Trip, Normal Service
	2 Remote Seals - High Trip, Severe Service
	2 Remote Seals - Low Trip, Normal Service
	2 Remote Seals - Low Trip, Severe Service

3.1 Remote Seal with Thermal Range Expander options

Also available on some models of transmitters is a Thermal Range Expander (TRE) option. The Rosemount Thermal Range Expander is a remote seal system that uses two different fill fluids separated by an intermediate diagram to extend the operating temperature range of the complete system. This option is beneficial in some applications that would normally be outside of the standard Ambient / Process temperature operating region.

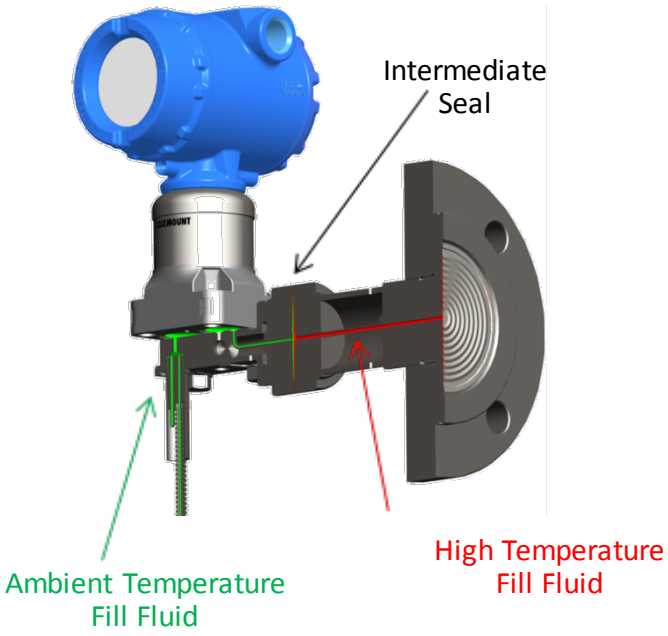


Figure 2: Thermal Range Expander

An attached Remote Seal is classified as a Type A[2] device that is a part of an element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation listed in section 2.4.1 and is documented in [R1].

4.1 Failure categories description

In order to judge the failure behavior of the Remote Seal System, the following definitions for the failure of the device were considered.

Note: as the Remote Seal does not perform a Safety Function on its own, the below states refer to the state of the Transmitter that the Seal(s) is (are) attached to.

Fail-Safe State:

High Trip	State where the output exceeds the user defined threshold.
Low Trip	State where the output is below the user defined threshold.
Fail Safe	Failure that causes the transmitter to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 2% of span 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.
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
External Leakage	Failure that causes process fluids or gases to leak outside of the vessel; External Leakage is not considered part of the safety function and therefore this failure rate 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_H failure data is not available.

External leakage failure rates do not directly contribute to the reliability of the device 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.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension 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 important category (safe detected, safe undetected, dangerous detected, dangerous undetected) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N1] which was derived using over 100 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 3 (General Field Equipment) and Profile 6 (Process Wetted Parts) for the Remote Seals process wetted parts, see Appendix C. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Rosemount. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related wearout failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Rosemount Remote Seals.

- Only a single component failure will fail the entire Remote Seal.
- 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.

- Failures caused by operational errors are site specific and therefore are not included.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 3 (General Field Equipment) and Profile 6 (Process Wetted Parts) for the Remote Seal with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Materials are compatible with the environmental and process conditions.
- The device is installed per the manufacturer's instructions.
- Breakage or plugging of any impulse lines has not been included in the analysis.
- Worst-case internal fault detection time is the Transmitters diagnostic test interval time.
- Transmitter shifts due temperature effects with the added Remote Seal (and the optional Thermal Range Expander Seal) are outside the scope of this analysis as consideration for this is included during the selection of the seal and fill fluid.
- Analysis covers the Rosemount factory installed seals (internally designated as 1199)

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the FMEDA analysis of the Remote Seal.

Incremental Failure Rates that are to be added to the Rosemount Transmitters Failure Rates for Standard Remote Seals are listed in Table 3 and in Table 4 for the Remote Seal with Thermal Range Expander option. Incremental failure rates should be used when adding failure rates to a transmitter FMEDA. This table accounts for duplicate mechanical components that are already included in the transmitter FMEDA failure rates.

Table 3 Incremental Failure Rates for Standard Remote Seal(s)

Failure Category	High Trip		Low Trip	
	Normal	Severe	Normal	Severe
1 Remote Seal (High Side)				
Fail Safe Undetected	0	0	44	74
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	46	76	2	3
No Effect	3	3	3	3
External Leakage	0	0	0	0
1 Remote Seal (Low Side)				
Fail Safe Undetected	44	74	0	0
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	2	3	46	76
No Effect	3	3	3	3
External Leakage	0	0	0	0
2 Remote Seals				
Fail Safe Undetected	41	70	46	77
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	50	83	46	75
No Effect	5	5	5	5
External Leakage	5	10	5	10

Table 4 Incremental Failure Rates for Remote Seal with Thermal Range Expander option(s)

Failure Category	High Trip		Low Trip	
	Normal	Severe	Normal	Severe
1 Remote Seal (High Side)				
Fail Safe Undetected	0	0	53	83
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	55	86	2	3
No Effect	4	4	4	4
External Leakage	0	0	0	0

1 Remote Seal (Low Side)				
Fail Safe Undetected	53	83	0	0
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	2	3	55	86
No Effect	4	4	4	4
External Leakage	0	0	0	0

2 Remote Seals				
Fail Safe Undetected	50	79	56	87
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	60	93	54	85
No Effect	8	8	8	8
External Leakage	5	10	5	10

External leakage failure rates do not directly contribute to the reliability of the Remote Seal 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.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508 (see Section 5.2).

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore the Rosemount Remote Seal 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.

If Route 2_H is not applicable for all devices that constitute the entire element, the architectural constraints will need to be evaluated per Route 1_H.

Table 5 and Table 6 list the Incremental failure rates for Standard Remote Seals and Remote Seal with Thermal Range Expander option according to IEC 61508.

Table 5 Incremental failure rates for Standard Remote Seals according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}
1 Remote Seal (if high side seal) - High Trip, Normal Service	0	0	0	46
1 Remote Seal (if high side seal) - High Trip, Severe Service	0	0	0	76
1 Remote Seal (if high side seal) - Low Trip, Normal Service	0	44	0	2
1 Remote Seal (if high side seal) - Low Trip, Severe Service	0	74	0	3
1 Remote Seal (if low side) - High Trip, Normal Service	0	44	0	2
1 Remote Seal (if low side) - High Trip, Severe Service	0	74	0	3
1 Remote Seal (if low side) - Low Trip, Normal Service	0	0	0	46
1 Remote Seal (if low side) - Low Trip, Severe Service	0	0	0	76
2 Remote Seals - High Trip, Normal Service	0	41	0	50
2 Remote Seals - High Trip, Severe Service	0	70	0	83
2 Remote Seals - Low Trip, Normal Service	0	46	0	46
2 Remote Seals - Low Trip, Severe Service	0	77	0	75

[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.

Table 6 Incremental failure rates for a Remote Seal System with Thermal Range Expander option according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}
1 Remote Seal (if high side seal) - High Trip, Normal Service	0	0	0	55
1 Remote Seal (if high side seal) - High Trip, Severe Service	0	0	0	86
1 Remote Seal (if high side seal) - Low Trip, Normal Service	0	53	0	2
1 Remote Seal (if high side seal) - Low Trip, Severe Service	0	83	0	3
1 Remote Seal (if low side) - High Trip, Normal Service	0	53	0	2
1 Remote Seal (if low side) - High Trip, Severe Service	0	83	0	3
1 Remote Seal (if low side) - Low Trip, Normal Service	0	0	0	55
1 Remote Seal (if low side) - Low Trip, Severe Service	0	0	0	86
2 Remote Seals - High Trip, Normal Service	0	50	0	60
2 Remote Seals - High Trip, Severe Service	0	79	0	93
2 Remote Seals - Low Trip, Normal Service	0	56	0	54
2 Remote Seals - Low Trip, Severe Service	0	87	0	85

The architectural constraint type for the Remote Seal is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

[4] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

5 Using the FMEDA Results

5.1 PFD_{avg} calculation Remote Seal

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 entire sensor 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 the sensor element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates for all the devices in the sensor element and the proof test coverage for the final element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test and the dangerous failure rate after proof test for the Remote Seal are listed in Table 10. This is combined with the dangerous failure rates after proof test for other devices in the sensor element to establish the proof test coverage for the sensor element.

5.2 *exida* Route 2_H Criteria

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

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

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

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

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

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

4. failure definitions, especially "random" vs. "systematic" 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.

5.3 SIL Verification

Three constraints must be checked to fully verify that a design meets a target SIL level. These are:

1. PFH / PFD_{avg} - the probability of dangerous failure must be less than the target number for a set of equipment used in a safety instrumented function. The PFD_{avg} calculation is based on a number of variables but the primary product attribute is the "dangerous undetected" failure rate.

2. Systematic Capability - all products used in a safety instrumented function must meet systematic capability for the target SIL level. This is normally achieved by purchasing a product with IEC 61508 certification for the given SIL level (or better). It may also be done with a prior use justification.

3. Architecture Constraints - For each element in a safety instrumented function, minimum architecture constraints must be met. For this product the constraints in IEC 61508:2010 Route 2_H are recommended as the product meets Route 2_H requirements.

FMEDA reports contain information useful for constraint 1 and constraint 3. It is the responsibility of the Safety Instrumented Function designer to do verification for the entire SIF. *exida* recommends the accurate Markov based exSILentia® tool for this purpose.

5.4 SIF Verification Example

A Rosemount 3051S transmitter is combined with a Rosemount Remote Seal, High Side, High Trip, Severe Service. Failure rates from the Rosemount 3051S coplanar pressure transmitter are added to the incremental failure rates for a high trip Remote Seal in severe service (Table 7).

Table 7 Total Failure Rates for Transmitter and Remote Seal

Component	Failure Rates [1/h]								Arch. Type
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	Res.	
Each Leg									
Rosemount 3051S SIS Coplanar SW Rev 7.0 and above	3.30E-08	5.90E-08	1.82E-07		4.00E-08		8.20E-08	1.38E-07	B
Rosemount 1199: 1 seal, high side, Hi trip, Severe					7.60E-08				A
Total for combination of Rosemount 3051S with Rosemount 1199 Remote Seal	3.30E-08	5.90E-08	1.82E-07		1.16E-07		8.20E-08	1.38E-07	B

These numbers (Table 7) were obtained from the exSILentia™ SIL verification tool which accurately calculates PFD_{avg} (Table 8) using discrete time Markov models.

Table 8 Example SIF Verification Results

Constraint	Result		SIL 2 Requirement	SIL Achieved
Sensor sub-system PFDavg	2.89E-03		PFDavg max. = 0.01	2
Sensor sub-system SIL Capability	Systematic Capability = SC3	exida IEC 61508 Certified	SC2	3
Sensor sub-system Architecture Constraints	HFT=0	Route 2_H Table	HFT=0	2

Sensor sub-system MTTFS: 1396 years

In order to perform the PFDavg calculation part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time: 10 years

Startup time: 24 hours

The SIF operates in Low demand mode.

Equipment Leg (each): Rosemount 1199 Remote Seal (Sys. Cap.: 2/3)
Rosemount 3051S SIS Coplanar SW Rev 7.0 and above (SC3)
High trip
Alarm Setting: Under Range
Diagnostic Filtering: On, Alarm Filtering: On
Trip On Alarm: Off

Beta factor (%) - [%]

MTTR: 24 hours

Proof Test Interval: 12 months

Proof Test Coverage: 49 [%]

Maintenance Capability: MCI 2 (Good – 90%)

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia® tool for this purpose.

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
Device	A device is something that is part of an element; but, cannot perform an element safety function on its own.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
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_{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.
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
Severe Service	Condition that exists when the process material is corrosive or abrasive, as opposed to Clean Service where these conditions 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

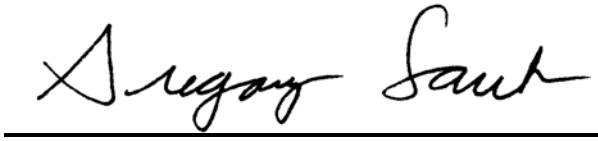
Version History:	V2, R1:	Updated to add the TRE Option Incremental rates and new report format. No change in failure rates from V1R3; October 8, 2015
	V1, R3:	Updated per customer feedback; T. Stewart, April, 24, 2013
	V1, R2:	Updated to include SIF verification example
	V1, R1:	Released to Rosemount; December 3, 2011
	V0, R1:	Draft
Author(s):	Gregory Sauk & William Goble	
Review:	V2, R1:	Client review (Rosemount)
	V2, R0:	Ted Stewart (*exida*)
	V1, R3:	Client review, William Goble (*exida*)
	V1, R1:	Client review
	V0, R1:	William Goble (*exida*)
Release Status:	Released to Rosemount	

7.3 Future enhancements

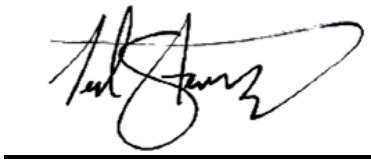
At request of client.

7.4 Release signatures

Dr. William M. Goble, CFSE, Principal Partner



Gregory Sauk, 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 assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[5] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

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

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

Based on general field failure data a useful life period of approximately 10 years is expected for the Remote Seal in normal service.

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

A useful life period for Remote Seals in severe service should be based on plant specific failure data. The *exida's* SILStat™ software from exida is recommended for this data collection.

[5] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The primary failure mode in a Remote Seal is fill leakage. The suggested proof test described in Table 9 will detect 91% of possible DU failures high trip normal service application of the Remote Seal.

Table 9 Suggested Proof Test – Remote Seal

Step	Action
1.	Inspect the Remote Seal for signs of leakage.
2.	Compare the pressure (or differential pressure) reading with another instrument.

Note that if the 3051S DA2 diagnostics option is available on the pressure transmitter, 60% of the leakage failures can be detected by this feature if configured properly.

B.2 Proof Test Coverage

The Proof Test Coverage for the Transmitter and Seal system can be calculated by adding together the DU after Proof Test for the Transmitter and the Seal DU after Proof Test values listed in Table 10.

Table 10 Remote Seals λ_{DU} after Proof Test

Seal Type	Application	$\lambda_{DU}PT^6$ (FIT)
Standard Remote Seal	1 Seal (High Side), High Trip, Normal Service	4.3
	1 Seal (High Side), High Trip, Severe Service	7.2
	1 Seal (High Side), Low Trip, Normal Service	0.2
	1 Seal (High Side), Low Trip, Severe Service	0.3
	1 Seal (Low Side), High Trip, Normal Service	0.2
	1 Seal (Low Side), High Trip, Severe Service	0.3
	1 Seal (Low Side), Low Trip, Normal Service	4.3
	1 Seal (Low Side), Low Trip, Severe Service	7.2
	2 Seals, High Trip, Normal Service	4.7
	2 Seals, High Trip, Severe Service	7.9
	2 Seals, Low Trip, Normal Service	4.3
	2 Seals, Low Trip, Severe Service	7.1
Remote Seal with Thermal Range Expander option	1 Seal (High Side), High Trip, Normal Service	4.8
	1 Seal (High Side), High Trip, Severe Service	7.7
	1 Seal (High Side), Low Trip, Normal Service	0.2
	1 Seal (High Side), Low Trip, Severe Service	0.3
	1 Seal (Low Side), High Trip, Normal Service	0.2
	1 Seal (Low Side), High Trip, Severe Service	0.3
	1 Seal (Low Side), Low Trip, Normal Service	4.8
	1 Seal (Low Side), Low Trip, Severe Service	7.7
	2 Seals, High Trip, Normal Service	5.3
	2 Seals, High Trip, Severe Service	8.4
	2 Seals, Low Trip, Normal Service	4.8
	2 Seals, Low Trip, Severe Service	7.6

Appendix C *exida* Environmental Profiles

Table 11 *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[7]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[8]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[9]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[10]	G2	G3	G3	G3	G3	Compatible Material
Surge[11]						
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[12]						
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)[13]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[7] Humidity rating per IEC 60068-2-3
[8] Shock rating per IEC 60068-2-27
[9] Vibration rating per IEC 60068-2-6
[10] Chemical Corrosion rating per ISA 71.04
[11] Surge rating per IEC 61000-4-5
[12] EMI Susceptibility rating per IEC 61000-4-3
[13] 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}) must be done based on a number of variables including:

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

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

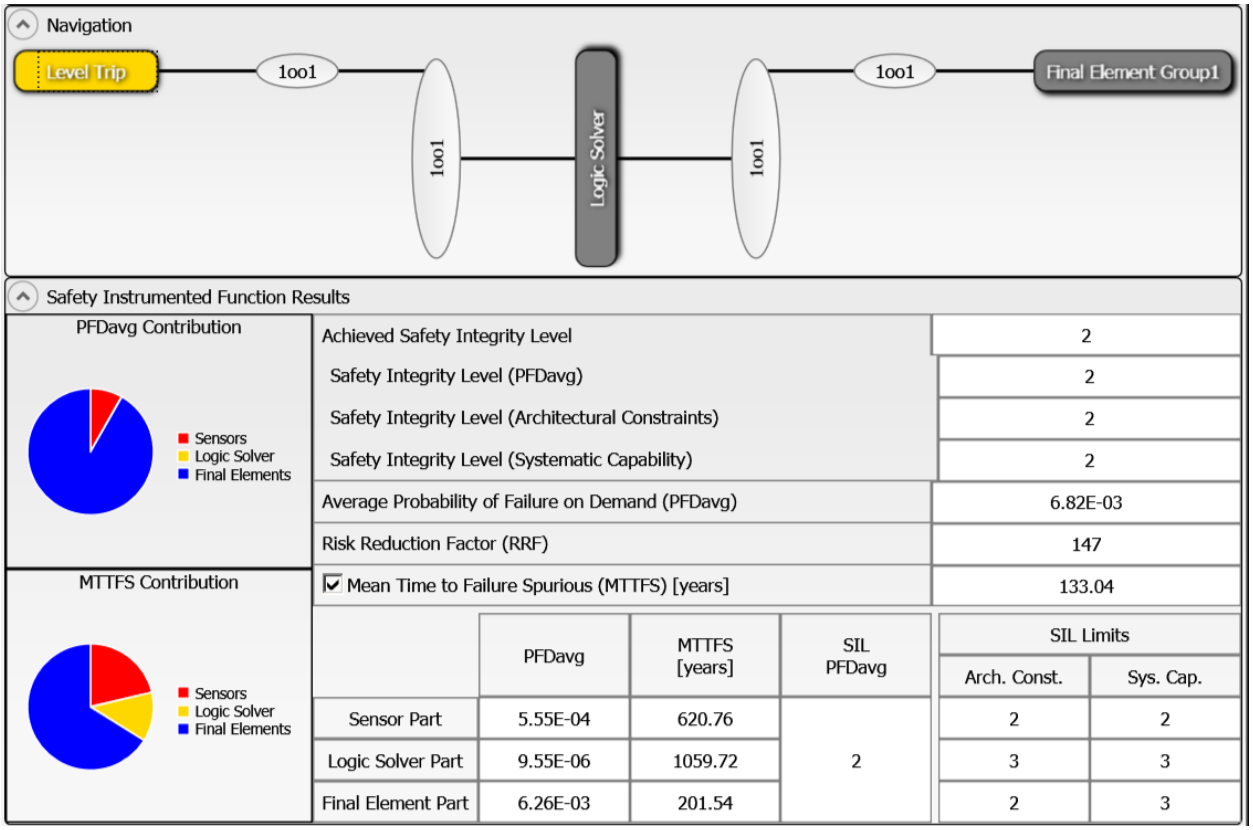
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

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

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

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

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03 (Figure 3).



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 3: exSILentia results for idealistic variables.

If the Proof Test Internal for the sensor and final element is increased in one year increments, the results are shown in Figure 4.

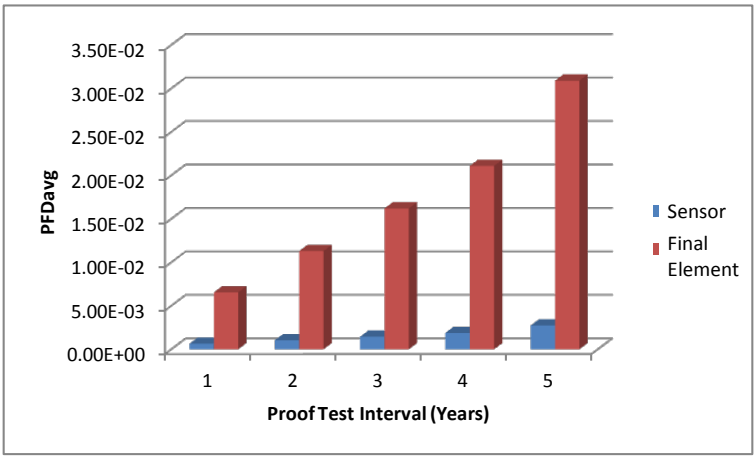


Figure 4: PFD_{avg} versus Proof Test Interval

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

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

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor of 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 5).

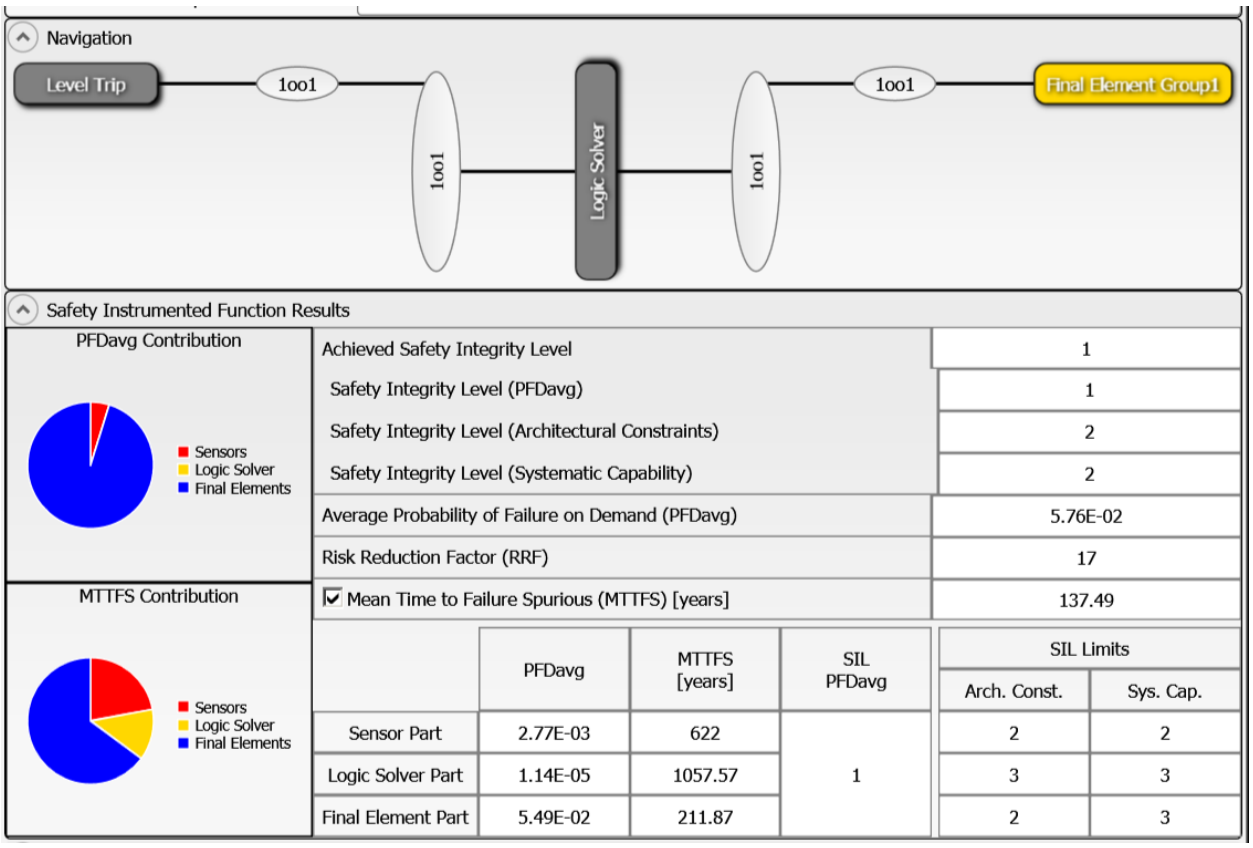


Figure 5: exSILentia results with realistic variables

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