Failure Modes, Effects and Diagnostic Analysis

Project:
Primary Elements

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

Contract Number: Q21/06-099
Report No.: ROS 13/04-008 R001
Version V2, Revision R1, June 17, 2021
Gregory Sauk

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Primary Elements. 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 Primary Element. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

A Flowmeter consists of a Primary Element that is attached to one of the following devices: Rosemount 3051, Rosemount 3051S, Rosemount 3051S Multivariable, Rosemount 2051, and Rosemount 3095 differential pressure transmitters. The specific Primary Element that were considered are the 485 Annubar Primary Element, the 405 Compact Primary Element, and the 1195 Integral Orifice Plate.

Note: This report does not include the failure rates for the Rosemount Pressure Transmitter that the Primary Element is attached to.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Primary Element.

Table 1 Version Overview

Model	Application
485 Annubar Primary Element	Process Connection for Flow – High Trip, Clean Service
	Process Connection for Flow – Low Trip, Clean Service
405 Compact Primary Element	Process Connection for Flow – High Trip, Clean Service
	Process Connection for Flow – Low Trip, Clean Service
1195 Integral Orifice Plate	Process Connection for Flow – High Trip, Clean Service
	Process Connection for Flow – Low Trip, Clean Service

The Primary Element is classified as a device that is part of a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. See Section 5.2. Therefore, the Primary Element 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 failure rates for the Primary Element are listed in section 4.4.

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

[1] Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010. / 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 are based on over 350 billion-unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI), see section 4.2.2.

A user of the Primary Element 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 the Primary Element. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

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

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

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, 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 the Primary Element
exida	Performed the hardware assessment

Rosemount Inc. contracted *exida* 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, 4th Edition, 2016	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2016 (pending publication, not publicly available at the time of this report)
[N3]	Safety Equipment Reliability Handbook, 4th Edition, 2015	*exida* LLC, Safety Equipment Reliability Handbook, Fourth Edition, 2015, ISBN 978-1-934977-13-2
[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. , Stewart, L., & Bredemeyer, L., 2018	*exida* LLC., Final Elements in Safety Instrumented Systems IEC 61511 Compliant Systems and IEC 61508 Compliant Products, 2018, ISBN 978-1-934977-18-7
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers

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

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[D1]	00813-0100-4485, Rev EB, May 2013	Product Data Sheet
[D2]	00809-0100-4809, Rev CB, March 2012	Annubar Reference Manual
[D3]	00809-0100-4686; Rev HA, April 2006	Integral Orifice Flowmeter Series
[D4]	01195-1002, Rev AE, 15-Feb-2010	MODEL 1195 INTEGRAL ORIFICE PLATE / FLOWMETER Drawing
[D5]	00405-1001, Rev AO, 9-Mar-2012	MODEL 405 COMPACT FLOWMETER Drawing
[D6]	00485-1011, Rev AF, 15-Feb-2010	MODEL 485 ANNUBAR FLOWMETER SZ 1 FLANGED Drawing
[D7]	00813-0100-4001, Rev MA, May 2012	Rosemount 3051 Pressure Transmitter, Product Data Sheet

2.4.2 Documentation generated by *exida*

[R1]	Rosemount 3051 Flow Adders R2.xls, 12-Feb-2013	Failure Modes, Effects, and Diagnostic Analysis – Primary Element (internal document)
[R2]	ROS 13/04-008 R001,	FMEDA report, Primary Element (this report)

	V2R1, 17-Jun-2021	

3 Product Description

A Flowmeter consists of a Primary Element that is attached to one of the following devices: Rosemount 3051, Rosemount 3051S, Rosemount 3051S Multivariable, Rosemount 2051, and Rosemount 3095 differential pressure transmitters. The purpose of this report is to consider the additional failure rates between these elements when attached to a pressure transmitter.

These elements have the ability to attach onto numerous devices such as a Rosemount 2051, Rosemount 3051, Rosemount 3051S, etc. A user may visit the supplier's website for the technical specifications. A flowmeter measures flow and comes in numerous ways.

A Rosemount Pressure Transmitter can be combined with primary elements to offer fully assembled flowmeters. The direct mount flowmeter capability eliminates troublesome impulse lines associated with traditional installations. With multiple primary element technologies available, Rosemount flowmeters offer a flexible solution to meet the performance, reliability, and installation needs of nearly any flow measurement application.

Note: This report does not include the failure rates for the Rosemount Pressure Transmitter that the Primary Element is attached to.

3.1 Rosemount Flowmeter Series

Rosemount Flowmeters combine the proven pressure transmitter and the latest Primary Element technology: Annubar Averaging, Compact Conditioning Orifice Plate, and Integral Orifice Plate. Flowmeters are factory configured to meet your application needs. Direct or remote mount configurations are available, but only the Direct mount configurations have been included in this analysis. The direct mount flowmeter capability eliminates troublesome impulse lines associated with traditional installations. With multiple primary element technologies available, Rosemount flowmeters offer a flexible solution to meet the performance, reliability, and installation needs of nearly any flow measurement application.

3.2 Annubar Flowmeter

Annubar flowmeters reduce permanent pressure loss by creating less blockage in the pipe. They are ideal for large line size installations when cost, size, and weight of the flowmeter are concerns. This analysis includes the Rosemount Model 485 Sensor and a 3-way Valve Manifold. Not included in this analysis are the 'Flo-tap' models that can be installed and removed from service while the process is running.

3.3 Compact Flowmeter

Compact Conditioning flowmeters reduce straight piping requirements to 2D upstream and 2D downstream from a flow disturbance. These models feature simple installation of the Compact Flowmeter between any existing raised-face flanges. This analysis includes the Rosemount Model 405 Conditioning / Orifice Plate and a 3-way Valve Manifold.

3.4 Integral Orifice Flowmeter

These feature precision honed pipe sections for increased accuracy in small line sizes, and self-centering plate design prevents alignment errors that magnify measurement inaccuracies in small line sizes. This analysis includes the Rosemount Model 1195 Sensor and a 3-way Valve Manifold

Table 3 gives an overview of the different versions that were considered in the FMEDA of the Primary Element.

Table 2 Version Overview

Model	Application
485 Annubar Primary Element	Process Connection for Flow – High Trip, Clean Service
	Process Connection for Flow – Low Trip, Clean Service
405 Compact Primary Element	Process Connection for Flow – High Trip, Clean Service
	Process Connection for Flow – Low Trip, Clean Service
1195 Integral Orifice Plate	Process Connection for Flow – High Trip, Clean Service
	Process Connection for Flow – Low Trip, Clean Service

The Primary Element is classified as a device that is a part of a Type A[2] element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

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

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.

4.1 Failure categories description

In order to judge the failure behavior of the Primary Element, the following definitions for the failure of the device were considered.

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 device 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 hasno effect on the safety function.
External Leakage	Failure that causes process fluids to leak outside of the device; 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 in order to provide a complete set of data needed for design optimization.

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

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

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 350 billion-unit operational hours of process industry field failure data from multiple sources and failure data from various databases. 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 6 (Process Wetted Parts) 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.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Primary Element.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Primary Element, and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.
- The stress levels are specified in the *exida* Profile used for the analysis limited by the manufacturer's published ratings.
- Materials are compatible with the environmental and process conditions.
- The device is installed and operated per the manufacturer's instructions.
- Devices are installed such that the controlled substance will flow through the device in the direction indicated by the flow arrow, located on the device body.

- The devices are generally applied in relatively clean gas or liquid; therefore, no severe service has been considered in the analysis.

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 Primary Element.

Table 3 lists the failure rates for the Primary Element according to IEC 61508 with a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix E for an explanation of SSI.

Table 3 Primary Element incremental Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
Primary Element – High Trip, Clean Service	0	8	0	11	51	93
Primary Element – Low Trip, Clean Service	0	10	0	9	51	93

Incremental failure rates are to be added to the failure rates listed in the transmitter's FMEDA. This analysis included consideration for parts of the Primary Element that replace the applicable transmitter parts that are included in the transmitter FMEDA failure rates.

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

E = External Leaks

As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. 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.

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (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 which is more stringent than IEC 61508. Therefore, the Primary Element meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The architectural constraint type for the Primary Element 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.

5 Using the FMEDA Results

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

5.1 PFD_{avg} calculation Primary Element

Using the failure rate data displayed in section 4.4, and the failure rate data for the associated element devices, an average Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the 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 which may be incorrect. Therefore, the use of pre-calculated PFDavg 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 sensor devices are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test for the Primary Element is listed in Table 5. 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 undertaking of specific tests,
>
> in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

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

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

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

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

4. failure definitions, especially "random" vs. "systematic" 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 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.
Element	A collection of devices that perform an element safety function such as a final element consisting of a logic solver interface, actuator and valve.
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
High demand Mode	Mode, where the demand interval for operation made on a safety-related system is less than twice the proof test interval.
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
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
Severe Service	Condition that exists when material through the device 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).
SSI	Site Safety Index (See Appendix E)
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 *exida* compiled field failure data and a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, product design changes, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical model number product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three-year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years, contact the product vendor to verify the current validity of the results.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q21/06-099	ROS 1304008 R001 V2R1	Revised Useful life and updated to latest template, GPS, 17-Jun-21
Q13/04-008	ROS 1304008 R001 V1R0	Incorporated Rosemount comments; 6/16/13, Ted Stewart
Q13/04-008	ROS 1304008 R001 V0R2	Removed Level per customer request. Only doing Flowmeter
Q13/04-008	ROS 1304008 R001 V0R1	Draft; FMEDA for Flowmeter and Level per customer request

Reviewer: Ted Stewart, *exida*, June 17, 2021

Status: Released, June 17, 2021

7.3 Future enhancements

At request of client.

7.4 Release signatures

Gregory Sauk, CFSE, Senior Safety Engineer

Ted E. Stewart, CFSP, exidaCSP
Program Development & Compliance Manager

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime[3] 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 Primary Element per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

Based on field failure data a useful life period for Primary Elements used in Emerson Application checked non-erosive/abrasive and non-corrosive process environments of 20 years can be expected. When plant experience indicates a shorter useful lifetime for normal service than indicated in this appendix, the number based on plant experience should be used.

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

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

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

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

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

B.1 Suggested Proof Test

The suggested proof test described in Table 4 can be used as a Proof Test for the attached Pressure Transmitter and the Primary Element. This test will detect 95% of the possible DU failure rate adders for high or low trip clean service applications of the Primary Element. Consult the Safety Manual of the Pressure Transmitter for any additional steps needed to fully test the transmitter and for the Transmitter's Proof Test Coverage

Table 4 Suggested Proof Test – Flow Transmitter

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Inspect the Primary Element for any leaks, visible damage or contamination.
3.	Perform a three-point calibration check of the Flow Transmitter by varying the Flow through the Primary Element.
4.	Remove the bypass and otherwise restore normal operation.

Appendix C *exida* Environmental Profiles

Table 5 *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[4]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[5]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[6]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[7]	G2	G3	G3	G3	G3	Compatible Material
Surge[8]						
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[9]						
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)[10]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

4 Humidity rating per IEC 60068-2-3
5 Shock rating per IEC 60068-2-27
6 Vibration rating per IEC 60068-2-6
7 Chemical Corrosion rating per ISA 71.04
8 Surge rating per IEC 61000-4-5
9 EMI Susceptibility rating per IEC 61000-4-3
10 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 IEC 61508:2010. 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 350 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.

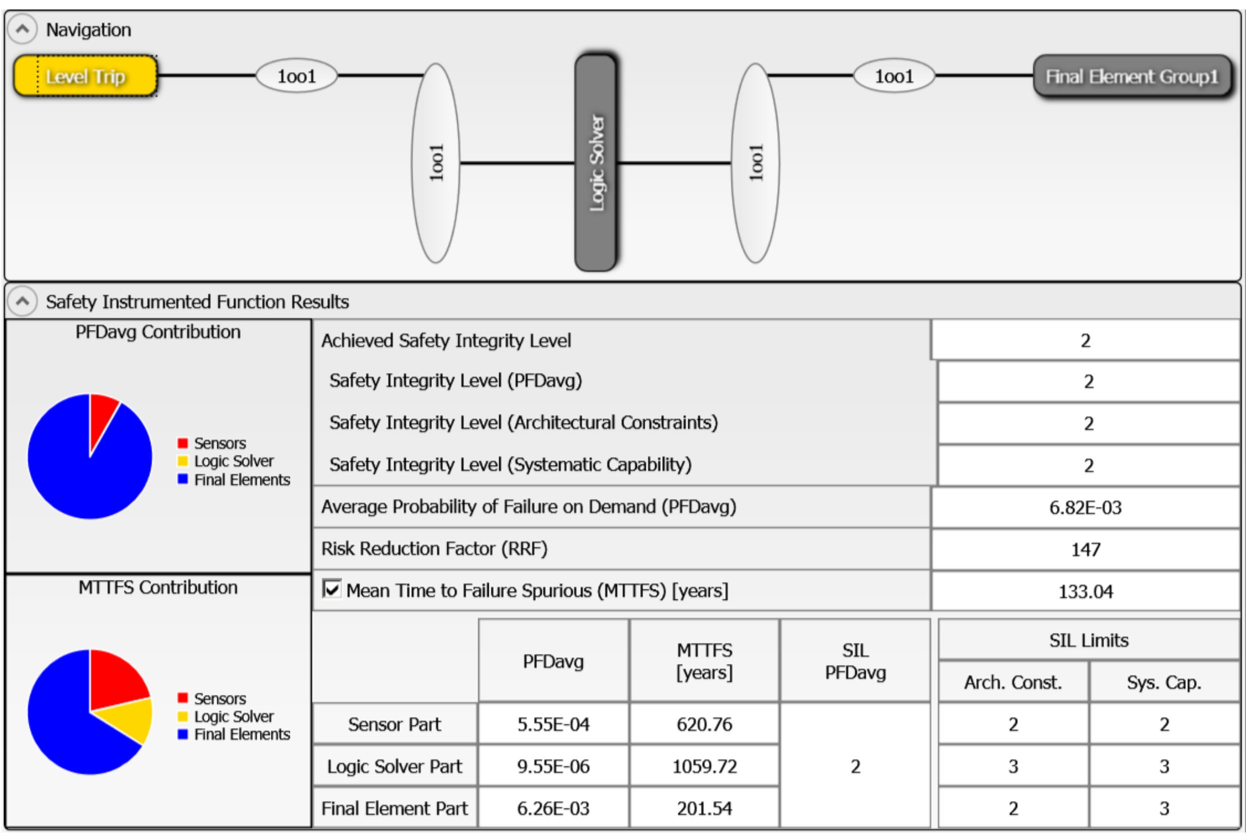
Simplified equations often account for only the first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC 61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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 1).



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 1: 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 2.

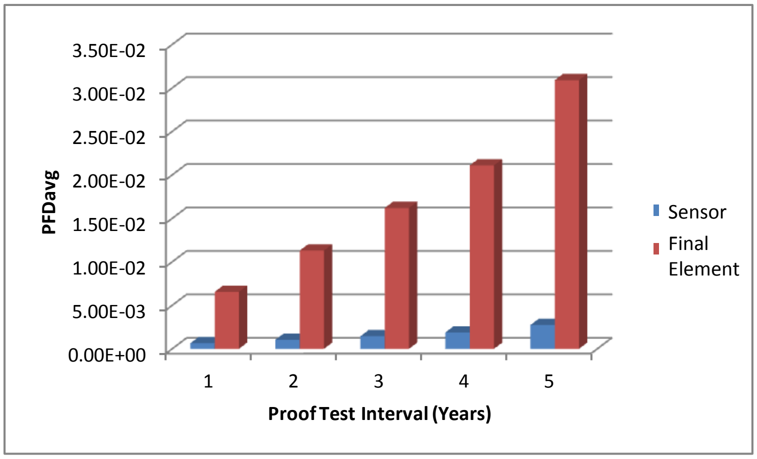
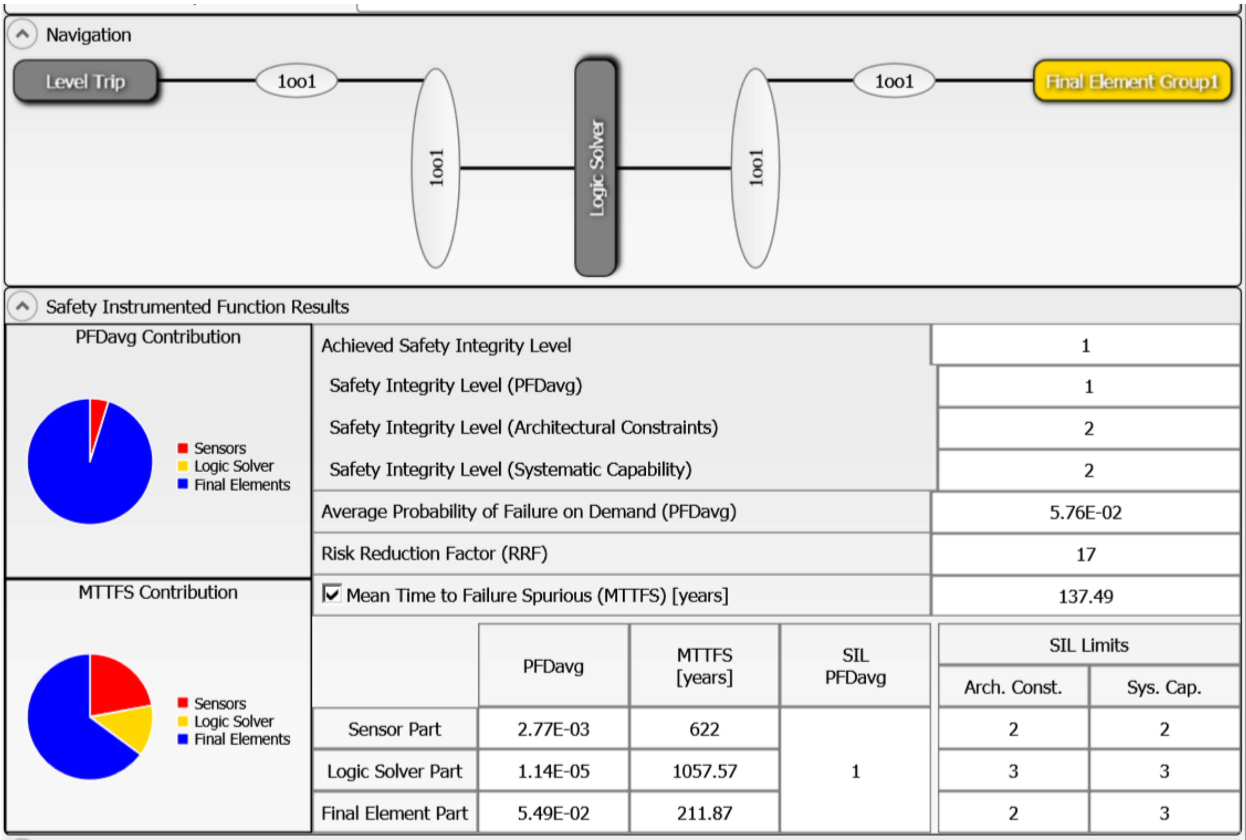


Figure 2: PFD_{avg} versus Proof Test Interval

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 3).



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

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

Figure 3: 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.

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 6 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 6 *exida* Site Safety Index Profiles

Level	Description
SSI 4	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.
SSI 3	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.
SSI 2	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.
SSI 1	Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.
SSI 0	None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.