Failure Modes, Effects and Diagnostic Analysis

Project:
Emerson's Rosemount®
3051S 4-20mA HART Pressure Transmitter
Software Revision 7.0 and above

Company:
Rosemount, Inc.
Shakopee, MN
USA

Contract Number: Q24/07-064
Report No.: ROS 05/05-05 R001
Version V2, Revision R4, August 1, 2024
Valerie Motto

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 Rosemount 3051S 4-20mA HART Pressure Transmitter, Software Revision 7.0 and Above. 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 Rosemount 3051S. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Rosemount 3051S 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.

Below list the versions of the Rosemount 3051S that have been considered in the hardware assessment:

- Rosemount 3051S Coplanar Differential & Coplanar Gage
- Rosemount 3051S Coplanar Absolute, In-line Gage, & In-line Absolute

The Rosemount 3051S is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. (See Section 5.4). Therefore, the Rosemount 3051S meets the hardware architectural constraints for up to up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) as a single device when the listed failure rates are used. If Route 2_H is not applicable for the Rosemount 3051S, the architectural constraints will need to be evaluated per Route 1_H.

The analysis shows that the Rosemount 3051S has a Safe Failure Fraction greater than 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The failure rates for the Rosemount 3051S are listed in Table 1 and Table 2.

A user of the Rosemount 3051S can utilize the listed 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.

---

[1] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Rosemount 3051S. 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 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 300 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 Rosemount 3051S
exida	Performed the hardware assessment

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

2.3 Standards and literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	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

[N8]	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
[N9]	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, Inc.

[D1]	03151-1514	Schematic drawing 3051S pressure transmitter	Rev AB
[D2]	03151-1511	Schematic drawing 3051S pressure transmitter	Rev AL

2.4.2 Documentation generated by *exida*

[R1]	Rosemount Change Audit.xls	Details of assessment (internal document)
[R2]	SM Coplanar II 3051S – with proof test coverage.xls	Detailed FMEDA for Rosemount 3051S Coplanar Board
[R3]	SM In-line 3051T - project projected 081205.xls	Failure Modes, Effects, and Diagnostic Analysis, Rosemount 3051S, In-Line
[R4]	3051S FMEDA Summary 2014-07-23 Rosemount.xls	3051S FMEDA Summary 2014-07-23

3 Product Description

The Rosemount 3051S 4-20mA Pressure Transmitter, Software Revision 7.0 and Above, is a two-wire 4 – 20 mA smart device used in multiple industries for both control and safety applications.

For safety instrumented systems usage, it is assumed that the 4 – 20 mA output is used as the primary safety variable. No other output variants are covered by this report.
The FMEDA has been performed for four different configurations of the 3051S Pressure Transmitter, i.e. Coplanar, In-Line, Level, and Flow configurations. The Rosemount 3051S Pressure Transmitter series include the following measurement configurations:

- Rosemount 3051S 4-20mA HART Pressure Transmitter: Coplanar Differential and Gage Coplanar

  The Rosemount 3051S utilizes capacitance sensor technology for differential Coplanar measurements.

- Rosemount 3051S 4-20mA HART Pressure Transmitter: Coplanar Absolute, In-line Gage and In-line Absolute

  Piezoresistive sensor technology is used for the absolute Coplanar and In-line measurements.

- Rosemount 3051S 4-20mA HART Level Transmitter

  A Rosemount 3051S Pressure Transmitter is available as a Level assembly. The Rosemount 3051S Level transmitter can be used to measure level on virtually any liquid level vessel. Rosemount 3051S transmitters and seal systems are designed to offer a flexible solution to meet the performance, reliability, and installation needs of nearly any level measurement application.

- Rosemount 3051S 4-20mA HART Flowmeter

  A Rosemount 3051S 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 3051S flowmeters offer a flexible solution to meet the performance, reliability, and installation needs of nearly any flow measurement application. The flowmeters covered for this assessment are based on the Rosemount 1195, 405, and 485 primary elements. Excluded from the assessment are models with Flo-Tap, remote mount, or temperature input options.

Devices used in safety applications with ambient temperatures below -40F (-40C) but does not exceed -76F(-60C) requires options BR5 (-50C) or BR6 (-60C) and QT.

The Rosemount 3051S, Software Revision 7.0 and Above is classified as a Type B[6] device according to IEC61508, having a hardware fault tolerance of 0.

The Rosemount 3051S can be connected to the process using an impulse line, depending on the application the clogging of the impulse line needs to be accounted for, see section 5.1.

---

[6] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.4.1 and is documented in 2.4.2.

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 3051S, the following definitions for the failure of the device were considered.

Fail-Safe State	Failure that deviates the process signal or the actual output by more than 2% of span (5% for Flowmeters), 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 (5% for Flowmeters), drifts away from the user defined threshold (Trip Point) and that leaves the output within active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics.
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current (> 21 mA).
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.6 mA).
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.
External Leakage	Failure that causes process fluids to leak outside of the valve; 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.

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 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, fail high, fail low, etc.) 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 [N2] and [N3] 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 2, see Appendix C. The *exida* profile chosen 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 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^{TM} 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 3051S.

- Only a single component failure will fail the entire Rosemount 3051S.
- 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 2 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the safety logic solver is configured to detect under-range (Fail Low) and over-range (Fail High) failures and does not automatically trip on these failures; therefore, these failures have been classified as dangerous detected failures.
- The device is installed per manufacturer's instructions.
- External power supply failure rates are not included.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Rosemount 3051S FMEDA.

Table 1 Failure rates for the Rosemount 3051S, Coplanar Differential & Coplanar Gage

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		82
Fail Dangerous Detected		274
Fail Detected (detected by internal diagnostics)	182	
Fail High (detected by logic solver)	59	
Fail Low (detected by logic solver)	33	
Fail Dangerous Undetected		40
No Effect		138
Annunciation Undetected		5

Table 2 Failure rates for the Rosemount 3051S, Coplanar Absolute, In-line Gage & In-line Absolute

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		80
Fail Dangerous Detected		260
Fail Detected (detected by internal diagnostics)	175	
Fail High (detected by logic solver)	58	
Fail Low (detected by logic solver)	26	
Fail Dangerous Undetected		37
No Effect		115
Annunciation Undetected		7

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 5.4).

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 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 3051S 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 the Rosemount 3051S, the architectural constraints will need to be evaluated per Route 1_H.

Table 3 lists the failure rates for the Rosemount 3051S according to IEC 61508, ed2, 2010.

Table 3 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[7]	λ_{DD}	λ_{DU}	**SFF**[8]
Rosemount 3051S_ Coplanar Differential & Coplanar Gage configuration	-	82	274	40	90%
Rosemount 3051S_ Coplanar Absolute, In-line Gage & In-line Absolute configuration	-	80	260	37	90%

Route 2_H Table

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	
3051S 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	-	82	274	40	-
3051S 4-20mA HART Pressure Transmitter: Coplanar Absolute, In-line Gage & In-line Absolute	-	80	260	37	-
3051S Flowmeter based on 1195, 405, or 485 Primaries					
3051S 4-20mA HART Flowmeter Series[9]	-	90	274	51	-
3051S Level Transmitter: (w/o additional Seal)					
3051S 4-20mA HART Pressure Transmitter	-	82	274	74	-
3051S Transmitter with Remote Seals[10]					

---

[7] 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.

[8] SFF not required for devices certified using Route 2_H data. For information detailing the Route 2_H approach as defined by IEC 61508-2, see Technical Document entitled "Route 2_H SIL Verification for Rosemount Type B Transmitters with Type A Components".

[9] Refer to ROS 13/04-008 R001 V1R0 for the Flowmeter FMEDA report for models that are excluded.

[10] Refer to the Remote Seal (ROS 1105075 R001 V2R1) FMEDA report for the additional failure rates to use when using with attached Remote Seals, or use exSILentia.

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 Rosemount 3051S failure rates that are 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 Rosemount 3051S failure rates.

5.2 High/Continuous Demand

If the Rosemount 3051S is used where an application where the demand interval is short enough that proof testing is impractical but automatic diagnostics are still effective (high demand per IEC 61508) (demand interval >10 hours) the failure rates are listed in Table 4.

Table 4 PFH with Good Maintenance Assumptions in FIT @ SSI=2

Application/Device/Configuration	PFH
Rosemount 3051S Coplanar Differential & Coplanar Gage	40
Rosemount 3051S Coplanar Absolute, In-line Gage, & In-line Absolute	37

If the Rosemount 3051S is used where an application where the demand interval is short enough that proof testing is impractical and automatic diagnostics are also ineffective (continuous demand per IEC 61508) (demand interval ≤10 hours) the failure rates are listed in Table 5.

Table 5 PFH with Good Maintenance Assumptions in FIT @ SSI=2

Application/Device/Configuration	PFH
Rosemount 3051S Coplanar Differential & Coplanar Gage	314
Rosemount 3051S Coplanar Absolute, In-line Gage, & In-line Absolute	297

5.3 PFD$_{AVG}$ calculation Rosemount 3051S

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 element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore, use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix D for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test and the dangerous failure rate after proof test for the Rosemount 3051S are listed in Table 9.

5.4 *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 are 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.
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.
FIT	Failure In Time ($1\text{x}10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode in which the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
Severe service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
SFF	Safe Failure Fraction summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type 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 marketplace, *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 Releases

Version History:	V2, R4:	Proof Test correction (2010 PT #s were not updated in V2R1), Removed failure rate tables from Management Summary, Added Section 5.2 for High/Continuous Demand Failure Rates, Added PFH definition; VAM 8/1/2024
	V2, R3:	included cold temperature; updated template; recertification; TES 10/14/16
	V2, R2:	Modified Section 5 and created Appendix D; TES 8/21/14
		Rosemount comments incorporated; 9/5/14
	V2, R1:	Update to IEC 61508 2010 standard and 2_H, incorporated Rosemount comments; TES 7/9/14
	V1, R4:	Updated to incorporate latest template; customer stayed at IEC 61508 2000 standard and reviewed this FMEDA; TES,
	V1, R3:	Clarify product revision; August 27, 2007
	V1, R2:	Product name, proof tests updated; November 30, 2005
	V1, R1:	Released to Rosemount, Inc.; November 15, 2005
	V0, R1:	Draft; November 14, 2005
Current Author(s):		Valerie Motto
Original Author(s):		Greg Sauk and Ted Stewart
Review:	V2, R4:	Dan Alley (*exida*)
Release Status:		RELEASED to Rosemount, Inc.

7.3 Future enhancements

At request of client.

7.4 Release signatures

William M Goble

Dr. William M. Goble, Principal Partner

Valerie Motto

Valerie Motto, CFSP, Safety Engineer

Dan Alley, CFSE, Senior 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[11] 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 3051S per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

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

---

[11] 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 Partial Proof Test

A suggested proof test consists of an analog output loop test, as described in Table 7 This test will detect approximately 52% of possible DU failures in the Rosemount 3051S, Coplanar configuration, and 62% of possible DU failure for the In-Line configuration.

Table 7 Steps for Partial Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. 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.
3.	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
4.	Restore the loop to full operation.
5.	Remove the bypass from the safety PLC or otherwise restore normal operation.

B.2 Comprehensive Proof Test

The alternative proof test consists of the following steps, as described in Table 8. This test will detect approximately 92% of possible DU failures in the Rosemount 3051S, Coplanar configuration, and 95% of possible DU failure for the In-Line configuration.

Table 8 Steps for Comprehensive Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Perform Partial Proof Test.
3.	Perform a minimum two-point sensor calibration check using the 4-20mA range points as the calibration points and verify that the mA output corresponds to the pressure input value.
4.	Restore the loop to full operation.
5.	Remove the bypass from the safety PLC or 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 3051S

Device	Configuration	Partial	Comprehensive
Rosemount 3051S	Coplanar Differential & Coplanar Gage	49%	92%
	Coplanar Absolute, In-line Gage, & In-line	58%	94%

Appendix C *exida* Environmental Profiles

Table 10 *exida* Environmental Profiles

exida Profile	1	2	3	4	5	6
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[12]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[13]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[14]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[15]	G2	G3	G3	G3	G3	Compatible Material
Surge[16]						
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[17]						
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)[18]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

---

[12] Humidity rating per IEC 60068-2-3
[13] Shock rating per IEC 60068-2-6
[14] Vibration rating per IEC 60770-1
[15] Chemical Corrosion rating per ISA 71.04
[16] Surge rating per IEC 61000-4-5
[17] EMI Susceptibility rating per IEC 6100-4-3
[18] ESD (Air) rating per IEC 61000-4-2

Appendix D Determining Safety Integrity Level

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N5] and [N8].

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 PFDavg 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 [N9].

C. Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD_{avg}) calculation must be done based on a number of variables including:

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

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 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^{TM} software considers all these variables and provides an effective means to calculate PFDavg for any given set of variables.

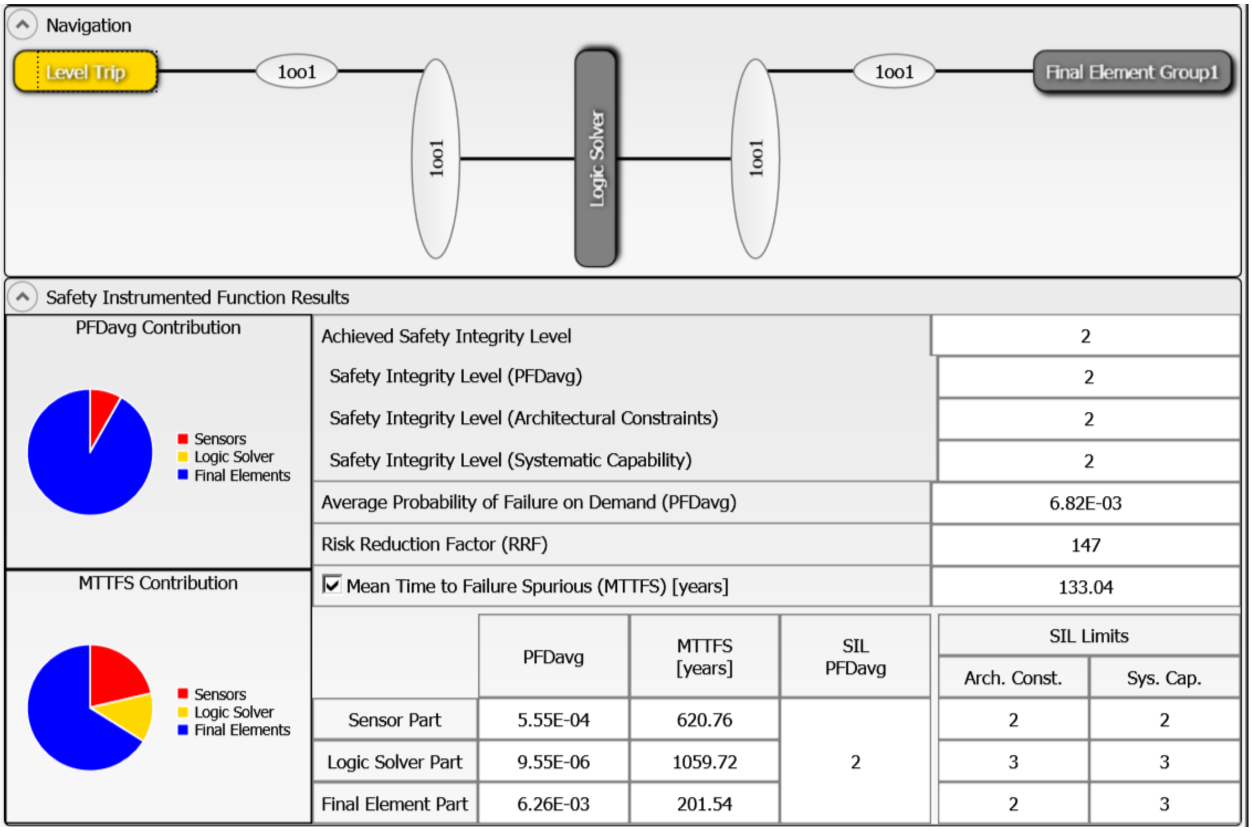
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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 (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 Internal for the sensor and final element is increased in one year increments, the results are shown in Figure 2.

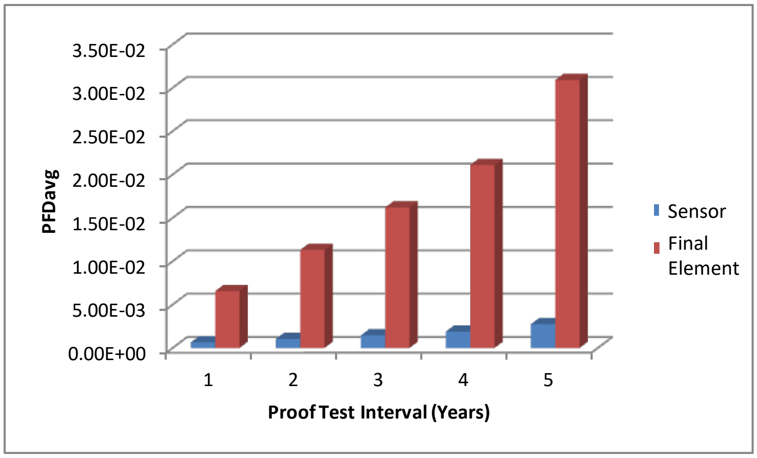
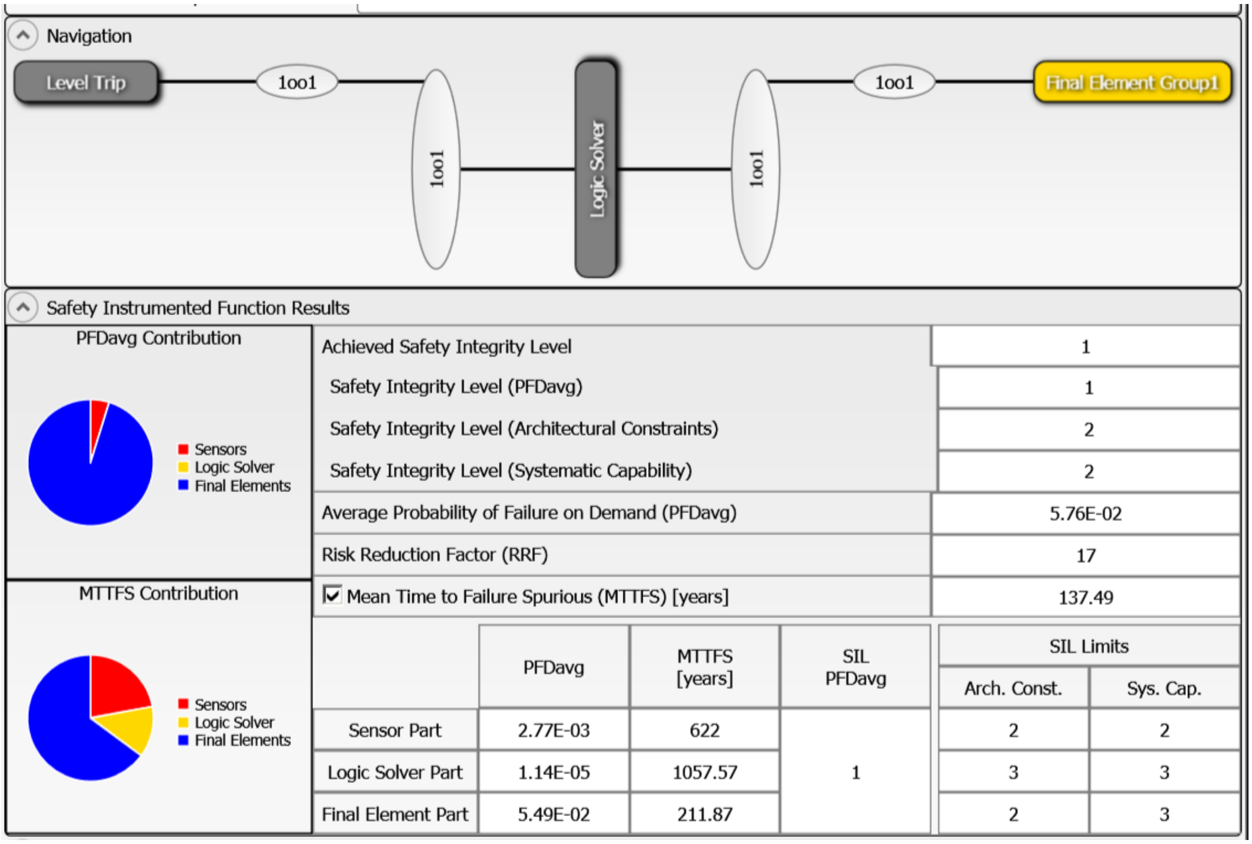


Figure 2 PFDavg versus Proof Test Interval.

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. The subsystem PFDavg contributions are Sensor PFDavg = 2.77E-03, Logic Solver PFDavg = 1.14E-05, and Final Element PFDavg = 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 PFDavg results can change an entire SIL level or more when all critical variables are not used.

END OF DOCUMENT