



Failure Modes, Effects and Diagnostic Analysis

Project:

Rosemount™ 3051SMV MultiVariable™ Transmitter

Company:

Emerson Automation Solutions

Rosemount Inc.

Shakopee, MN

USA

Contract Number: Q24/07-064

Report No.: ROS 09/05-36 R001

Version V3, Revision R2, August 1, 2024

Rudolf Chalupa / Ted Stewart / John Grebe



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™ 3051SMV MultiVariable™ Transmitter, models 3051SMV_M1, 3051SMV_M2, 3051SMV_M3, 3051SMV_M4, 3051SMV_P1, 3051SMV_P2, 3051SMV_P3, 3051SMV_P4, 3051SMV_P5, 3051SMV_P6, 3051SMV_P7, and 3051SMV_P8. 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 3051SMV. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

Rosemount 3051SMV 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. It utilizes the well proven Rosemount Supermodule in CAN mode feeding a Feature Board that performs advanced diagnostics. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. All other possible output variants are not covered by this report. The device can be equipped with or without display.

Table 1 and Table 2 give an overview of the different versions that were considered in the FMEDA of the Rosemount 3051SMV.

Table 1 Version: Overview, 3051SMV

| | |
|--|--|
| 3051SMV_P1 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P with Process Temperature |
| 3051SMV_P2 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature |
| 3051SMV_P3, 3051SMV_P5, 3051SMV_P6 | Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature |
| 3051SMV_P4, 3051SMV_P7, 3051SMV_P8 | Rosemount 3051SMV, Direct Process Variable Measurement using DP or P without Process Temperature |
| 3051SMV_M1 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature |
| 3051SMV_M2 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature |
| 3051SMV_M3 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature |
| 3051SMV_M4 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature |



Table 2 Version Overview: 3051SMV with Primary Element

| | |
|------------------------------------|--|
| 3051SFA1, 3051SFC1, 3051SFP1 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature |
| 3051SFA2, 3051SFC2, 3051SFP2 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature |
| 3051SFA3, 3051SFC3, 3051SFP3 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature |
| 3051SFA4, 3051SFC4, 3051SFP4 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature |
| 3051SFA5, 3051SFC5, 3051SFP5 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P with Process Temperature |
| 3051SFA6, 3051SFC6, 3051SFP6 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature |
| 3051SFA7, 3051SFC7, 3051SFP7 | Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature |

The Rosemount 3051SMV is classified as a Type B¹ element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H (see Section 5.4). Therefore, the Rosemount 3051SMV 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.

Based on the assumptions listed in 4.3, the failure rates for the Rosemount 3051SMV are listed in section 4.4.

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

The failure rates listed in this report are based on over 250 billion unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures; see section 4.2.2.

A user of the Rosemount 3051SMV can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

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



Table of Contents

| | | |
|------------|--|----|
| 1 | Purpose and Scope | 5 |
| 2 | Project Management | 6 |
| 2.1 | <i>exida</i> | 6 |
| 2.2 | Roles of the parties involved | 6 |
| 2.3 | Standards and literature used | 6 |
| 2.4 | <i>exida</i> tools used | 7 |
| 2.5 | Reference documents | 7 |
| 2.5.1 | Documentation provided by Emerson Automation Solutions | 7 |
| 2.5.2 | Documentation generated by <i>exida</i> | 8 |
| 3 | Product Description | 9 |
| 4 | Failure Modes, Effects, and Diagnostic Analysis | 14 |
| 4.1 | Failure categories description | 14 |
| 4.2 | Methodology – FMEDA, failure rates | 15 |
| 4.2.1 | FMEDA | 15 |
| 4.2.2 | Failure rates | 15 |
| 4.3 | Assumptions | 15 |
| 4.4 | Results | 16 |
| 5 | Using the FMEDA Results | 23 |
| 5.1 | Impulse line clogging | 23 |
| 5.2 | High/Continuous Demand | 23 |
| 5.3 | PFD _{avg} calculation Rosemount 3051SMV | 25 |
| 5.4 | <i>exida</i> Route 2 _H Criteria | 25 |
| 6 | Terms and Definitions | 26 |
| 7 | Status of the Document | 27 |
| 7.1 | Liability | 27 |
| 7.2 | Releases | 27 |
| 7.3 | Future enhancements | 27 |
| 7.4 | Release signatures | 28 |
| Appendix A | Lifetime of Critical Components | 29 |
| Appendix B | Proof Tests to Reveal Dangerous Undetected Faults | 30 |
| B.1 | Partial Proof Test | 30 |
| B.2 | Comprehensive Proof Test | 31 |
| Appendix C | <i>exida</i> Environmental Profiles | 32 |
| Appendix D | Determining Safety Integrity Level | 33 |



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 3051SMV. 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 cybersecurity, and availability with over 400 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion unit operating hours of field failure data.

2.2 Roles of the parties involved

Emerson Automation Solutions Manufacturer of the Rosemount 3051SMV

exida Performed the hardware assessment

Emerson Automation Solutions originally contracted *exida* in May 2009 with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

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

| | | |
|------|--|---|
| [N1] | IEC 61508-2: ed2, 2010 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems |
| [N2] | Electrical Component Reliability Handbook, 4th Edition, 2017 | <i>exida</i> LLC, Electrical Component Reliability Handbook, Fourth Edition, 2017 |
| [N3] | Mechanical Component Reliability Handbook, 4th Edition, 2017 | <i>exida</i> LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2017 |
| [N4] | Goble, W.M. 2010 | Control Systems Safety Evaluation and Reliability, 3 rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods |
| [N5] | IEC 60654-1:1993-02, second edition | Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition |
| [N6] | O'Brien, C. & Bredemeyer, L., 2009 | <i>exida</i> LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9 |



| | | |
|-------|---|--|
| [N7] | Scaling the Three Barriers, Recorded Web Seminar, June 2013, | Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers |
| [N8] | Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013 | http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design |
| [N9] | Random versus Systematic – Issues and Solutions, September 2016 | Goble, W.M., Bukowski, J.V., and Stewart, L.L., Random versus Systematic – Issues and Solutions, exida White Paper, PA: Sellersville, www.exida.com/resources/whitepapers , September 2016. |
| [N10] | Assessing Safety Culture via the Site Safety Index™, April 2016 | Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston, April 2016. |
| [N11] | Quantifying the Impacts of Human Factors on Functional Safety, April 2016 | Bukowski, J.V. and Stewart, L.L., Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York, April 2016. |
| [N12] | Criteria for the Application of IEC 61508:2010 Route 2H, December 2016 | Criteria for the Application of IEC 61508:2010 Route 2H, exida White Paper, PA: Sellersville, www.exida.com , December 2016. |
| [N13] | Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, November 1999 | Goble, W.M. and Brombacher, A.C., Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999. |
| [N14] | FMEDA – Accurate Product Failure Metrics, June 2015 | Grebe, J. and Goble W.M., FMEDA – Accurate Product Failure Metrics, www.exida.com , June 2015. |

2.4 exida tools used

| | | |
|------|---------|------------------|
| [T1] | V7.1.18 | exida FMEDA Tool |
|------|---------|------------------|

2.5 Reference documents

2.5.1 Documentation provided by Emerson Automation Solutions

| | | |
|------|-----------------------|--|
| [D1] | 03151-1514_rev_AE.pdf | Schematic, SCHEMATIC, COPLANAR BRD II, 3051S Drawing No. 03151-1514, Rev. AE |
| [D2] | 03151-1511_rev_AR.pdf | Schematic, SCHEMATIC, COSMOS SUPERMODULE, 3051T, Drawing No. 03151-1511, Rev. AR |
| [D3] | 03151-1540_rev_AC.pdf | Schematic, 3051S P/DP BRD, Drawing No. 03151-1540, |



| | | |
|------|-----------------------|--|
| | | Rev. AC |
| [D4] | 03151-3450_rev_AB.pdf | Schematic, SCHEMATIC DWG, 3051S_MV, FEATURE BRD, HART, RTD , Drawing No. 03151-3450, Rev. AB |
| [D5] | 03151-4264_rev_AA.pdf | Schematic, Terminal Block – Standard, Drawing No. 03151-4264, Rev. AA |

2.5.2 Documentation generated by *exida*

| | | |
|-------|---|---|
| [R1] | CAN Mode SM Coplanar II 3051S Rev_AE.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R2] | CAN Mode SM Inline 3051T Rev_AR.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R3] | 3051S P-DP Brd Common 07132009.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R4] | 3051S P-DP Brd DP Sensor 07132009.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R5] | 3051S P-DP Brd LP Sensor 07132009.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R6] | 3051S_MV Feature Board RTD Sensor 07132009.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R7] | 3051S_MV Feature Board without VDSP 07132009.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R8] | 3051S_MV Feature Board with VDSP 08122009.xls | Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051SMV |
| [R9] | 3051S MV Summary Sheet 2nd Edition SFF 05-19-2017.xls | Failure Modes, Effects, and Diagnostic Analysis - Summary – Rosemount 3051SMV |
| [R10] | ROS 13-04-008 R001 V2R1 Primary Elements FMEDA Rosemount.pdf, June 17, 2021 | FMEDA Report, Primary Elements |
| [R11] | ROS 09-05-36 R001 V3R2 FMEDA Model 3051SMV.DOC, 8/1/2024 | FMEDA report, Rosemount 3051SMV (this report) |

3 Product Description

The Rosemount™ 3051SMV MultiVariable™ Transmitter 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. The Transmitter 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 (output state is programmable). The device is equipped with or without display.

The FMEDA has been performed for 8 different configurations of the Rosemount™ 3051SMV MultiVariable™ Transmitter. Table 3 lists the versions of the 3051SMV transmitter that have been considered for the hardware assessment. The different configurations include the following:

- Two different Feature Boards of Direct Process Variable Measurement and Fully Compensated Mass, Volumetric, and Energy Flow
- Three different measurements of Differential Pressure (DP), Static Line Pressure (P), and Process Temperature (T)
- Two different configurations in the 3051S Super Module Platform of Coplanar and In-Line Static Pressure (P) and Process Temperature (T)

Figure 1 provides an overview of the Rosemount 3051SMV and the boundary of the FMEDA.

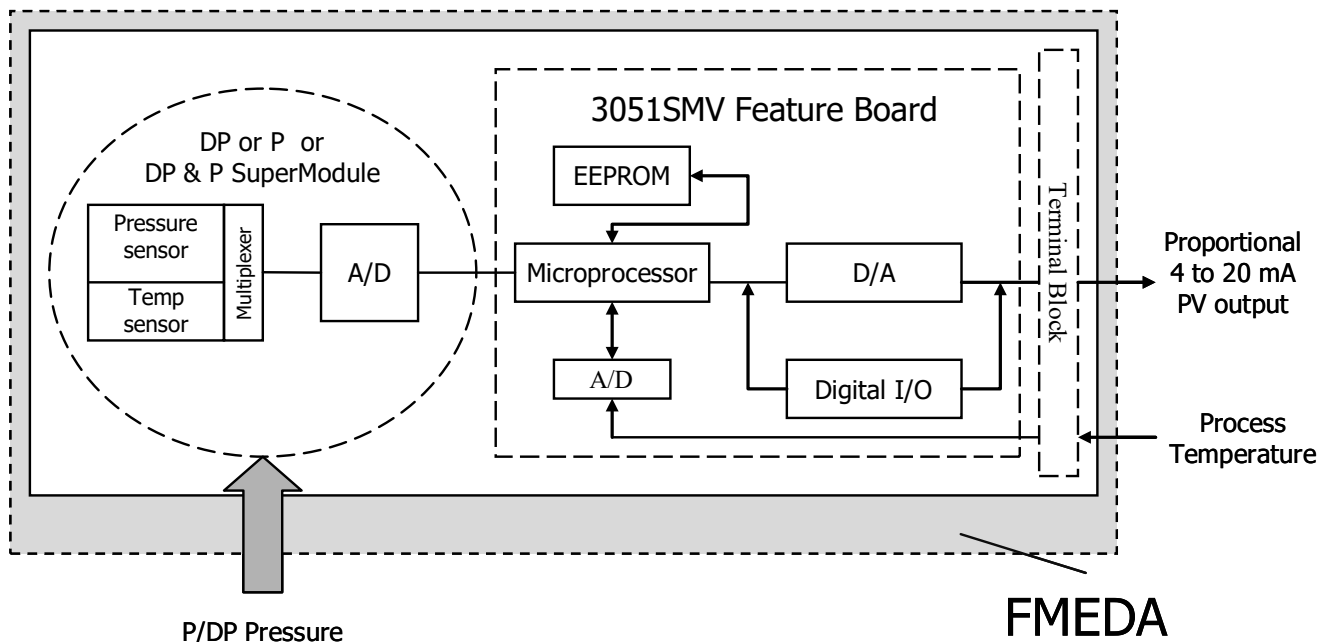


Figure 1 Rosemount 3051SMV, Parts included in the FMEDA



Table 3 Version Overview, 3051SMV

| | |
|--|--|
| 3051SMV_P1 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P with Process Temperature |
| 3051SMV_P2 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature |
| 3051SMV_P3, 3051SMV_P5, 3051SMV_P6 | Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature |
| 3051SMV_P4, 3051SMV_P7, 3051SMV_P8 | Rosemount 3051SMV, Direct Process Variable Measurement using DP or P without Process Temperature |
| 3051SMV_M1 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature |
| 3051SMV_M2 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature |
| 3051SMV_M3 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature |
| 3051SMV_M4 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature |

There are also three Rosemount™ 3051SMV MultiVariable™ Transmitter flowmeter options (see Figure 2):

- Rosemount™ 3051SFA which uses the Rosemount 485: Annubar™ Primary Element
- Rosemount™ 3051SFC which uses the Rosemount 405: Compact Conditioning Orifice Plate Primary Element
- Rosemount™ 3051SFP which uses the Rosemount 1195: Integral Orifice Primary Element

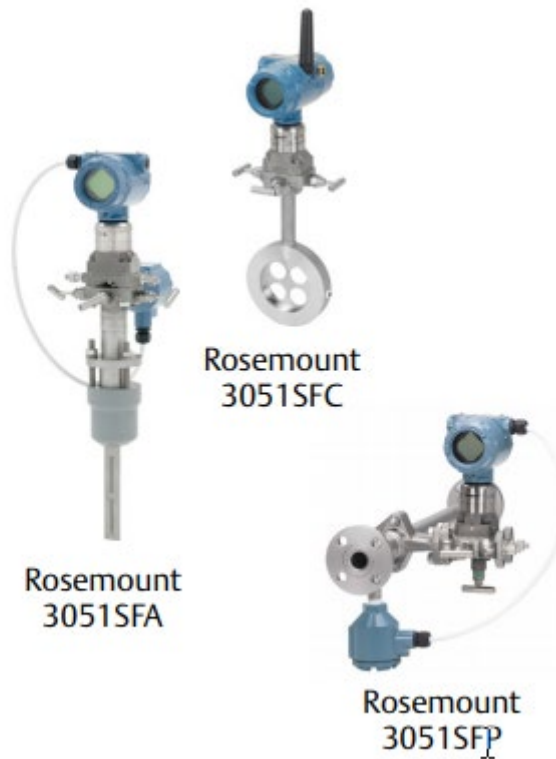


Figure 2 Rosemount 3051SMV, Flowmeter Options

Figure 3 provides an overview of the Rosemount 3051SMV with primary element and the boundary of the FMEDA.

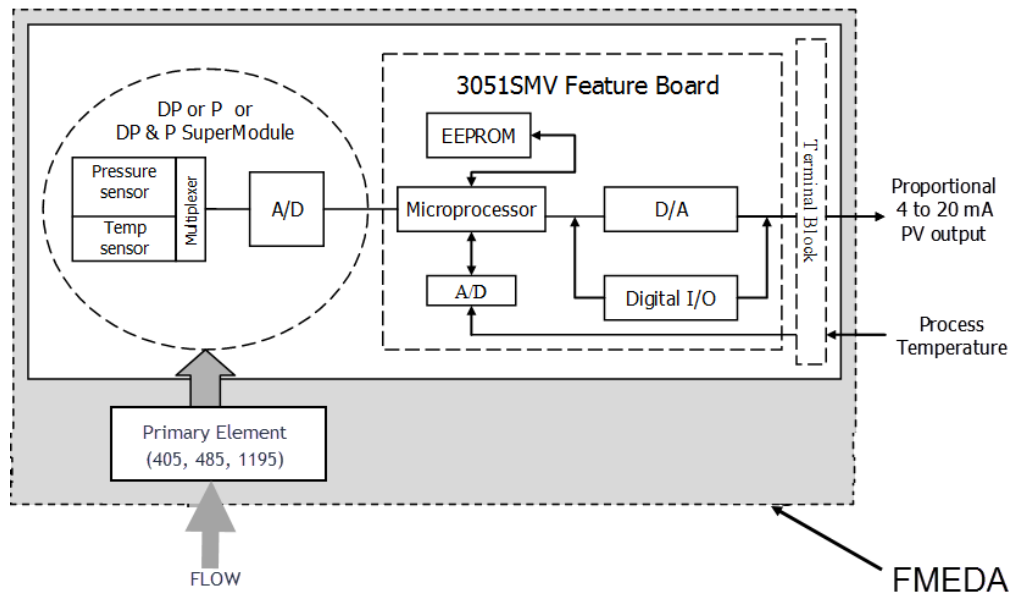


Figure 3 Rosemount 3051SMV with Primary Element, Parts included in the FMEDA

Table 4 lists the versions of the 3051SMV transmitter flowmeter options that have been considered for the hardware assessment.



Table 4 Version Overview, 3051SMV with Primary Element

| | |
|------------------------------------|--|
| 3051SFA1, 3051SFC1, 3051SFP1 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature |
| 3051SFA2, 3051SFC2, 3051SFP2 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature |
| 3051SFA3, 3051SFC3, 3051SFP3 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature |
| 3051SFA4, 3051SFC4, 3051SFP4 | Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature |
| 3051SFA5, 3051SFC5, 3051SFP5 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P with Process Temperature |
| 3051SFA6, 3051SFC6, 3051SFP6 | Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature |
| 3051SFA7, 3051SFC7, 3051SFP7 | Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature |

The Rosemount 3051SMV is classified as a Type B² element according to IEC 61508, having a hardware fault tolerance of 0.

The Rosemount 3051SMV 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.

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



4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.5.1 and is documented in [D1] to [D5].

4.1 Failure categories description

In order to judge the failure behavior of the Rosemount 3051SMV, the following definitions for the failure of the device were considered.

| | |
|---------------------------|---|
| Fail-Safe State | State where the output exceeds 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 Detected | Failure that causes the output signal to go to the predefined alarm state |
| Fail Dangerous | Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within the 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 Detected | 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 detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm. |
| Annunciation Undetected | Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics. |

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures.



4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress. It combines design FMEA techniques with extensions to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each failure mode category [N13, N14].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N3] which were derived using over 250 billion unit operational hours of process industry field failure data from multiple sources and failure data formulas from international standards. The component failure rates are provided for each applicable operational profile and application, see Appendix C. The *exida* profile chosen for this FMEDA was *exida* Profile 2, judged to be the best fit for the product and application information submitted by Emerson Automation Solutions. 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 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 Rosemount 3051SMV.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Rosemount 3051SMV and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.



- The stress levels are specified in the *exida* Profile used for the analysis are limited by the manufacturer's published ratings.
- Practical fault insertion tests have been used when applicable to demonstrate the correctness of the FMEDA results.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed and operated per manufacturer's instructions.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is 1 hour.

4.4 Results

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

Table 5 Failure rates Model 3051SMV-P1

| Failure Category | Failure Rate (FIT) |
|--|--------------------|
| Fail Safe Undetected | 74 |
| Fail Dangerous Detected | 902 |
| Fail Detected (detected by internal diagnostics) | 864 |
| Fail High (detected by logic solver) | 21 |
| Fail Low (detected by logic solver) | 18 |
| Fail Dangerous Undetected | 104 |
| No Effect | 232 |
| Annunciation Undetected | 23 |

The failure rates for the Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature configuration are listed in Table 6.



Table 6 Failure rates Model 3051SMV_P2

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 642 | |
| Fail Detected (detected by internal diagnostics) | 604 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 73 | |
| No Effect | 215 | |
| Annunciation Undetected | 23 | |

The failure rates for the Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature configuration are listed in Table 7.

Table 7 Failure rates Model 3051SMV_P3, 3051SMV_P5, 3051SMV_P6

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 880 | |
| Fail Detected (detected by internal diagnostics) | 842 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 81 | |
| No Effect | 257 | |
| Annunciation Undetected | 19 | |

The failure rates for the Rosemount 3051SMV, Direct Process Variable Measurement using DP or P without Process Temperature configuration are listed in Table 8.



Table 8 Failure rates Model 3051SMV_P4, 3051SMV_P7, 3051SMV_P8

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 620 | |
| Fail Detected (detected by internal diagnostics) | 582 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 50 | |
| No Effect | 240 | |
| Annunciation Undetected | 19 | |

The failure rates for the Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature configuration are listed in Table 9.

Table 9 Failure rates Model 3051SMV_M1

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 987 | |
| Fail Detected (detected by internal diagnostics) | 949 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 150 | |
| No Effect | 232 | |
| Annunciation Undetected | 23 | |

The failure rates for the Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature configuration are listed in Table 10.



Table 10 Failure rates Model 3051SMV_M2

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 727 | |
| Fail Detected (detected by internal diagnostics) | 689 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 119 | |
| No Effect | 215 | |
| Annunciation Undetected | 23 | |

The failure rates for the Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature configuration are listed in Table 11.

Table 11 Failure rates Model 3051SMV_M3

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 831 | |
| Fail Detected (detected by internal diagnostics) | 793 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 127 | |
| No Effect | 220 | |
| Annunciation Undetected | 19 | |

The failure rates for the Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature configuration are listed in Table 12.



Table 12 Failure rates Model 3051SMV_M4

| Failure Category | Failure Rate (FIT) | |
|--|---------------------------|--|
| Fail Safe Undetected | 74 | |
| Fail Dangerous Detected | 705 | |
| Fail Detected (detected by internal diagnostics) | 667 | |
| Fail High (detected by logic solver) | 21 | |
| Fail Low (detected by logic solver) | 18 | |
| Fail Dangerous Undetected | 95 | |
| No Effect | 240 | |
| Annunciation Undetected | 19 | |

The additional failure rates due to the primary element are presented in [R10].

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

Table 13 lists the failure rates for the Rosemount 3051SMV according to IEC 61508.



Table 13 Failure rates according to IEC 61508

| Device | λ_{SD} | λ_{SU}^3 | λ_{DD} | λ_{DU} |
|---|----------------|------------------|----------------|----------------|
| 3051SMV_P1 | 0 | 74 | 902 | 104 |
| 3051SMV_P2 | 0 | 74 | 642 | 73 |
| 3051SMV_P3, 3051SMV_P5, 3051SMV_P6 | 0 | 74 | 880 | 81 |
| 3051SMV_P4, 3051SMV_P7, 3051SMV_P8 | 0 | 74 | 620 | 50 |
| 3051SMV_M1 | 0 | 74 | 987 | 150 |
| 3051SMV_M2 | 0 | 74 | 727 | 119 |
| 3051SMV_M3 | 0 | 74 | 831 | 127 |
| 3051SMV_M4 | 0 | 74 | 705 | 95 |
| 3051SFA1, 3051SFC1, 3051SFP1 – High Trip (normal conditions) | 0 | 82 | 987 | 161 |
| 3051SFA1, 3051SFC1, 3051SFP1 – Low Trip (normal conditions) | 0 | 84 | 987 | 159 |
| 3051SFA2, 3051SFC2, 3051SFP2 – High Trip (normal conditions) | 0 | 82 | 727 | 130 |
| 3051SFA2, 3051SFC2, 3051SFP2 – Low Trip (normal conditions) | 0 | 84 | 727 | 128 |
| 3051SFA3, 3051SFC3, 3051SFP3 – High Trip (normal conditions) | 0 | 82 | 831 | 138 |
| 3051SFA3, 3051SFC3, 3051SFP3 – Low Trip (normal conditions) | 0 | 84 | 831 | 136 |
| 3051SFA4, 3051SFC4, 3051SFP4 – High Trip (normal conditions) | 0 | 82 | 705 | 106 |
| 3051SFA4, 3051SFC4, 3051SFP4 – Low Trip (normal conditions) | 0 | 84 | 705 | 104 |
| 3051SFA5, 3051SFC5, 3051SFP5 – High Trip (normal conditions) | 0 | 82 | 902 | 115 |
| 3051SFA5, 3051SFC5, 3051SFP5 – Low Trip (normal conditions) | 0 | 84 | 902 | 113 |
| 3051SFA6, 3051SFC6, 3051SFP6 – High Trip (normal conditions) | 0 | 82 | 642 | 84 |

³ It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations



| | | | | |
|---|---|----|-----|----|
| 3051SFA6, 3051SFC6, 3051SFP6 – Low Trip (normal conditions) | 0 | 84 | 642 | 82 |
| 3051SFA7, 3051SFC7, 3051SFP7 – High Trip (normal conditions) | 0 | 82 | 880 | 92 |
| 3051SFA7, 3051SFC7, 3051SFP7 – Low Trip (normal conditions) | 0 | 84 | 880 | 90 |

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 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 3051SMV meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The analysis shows that the Rosemount 3051SMV has a Safe Failure Fraction between 60% and 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.



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 3051SMV 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 3051SMV failure rates.

5.2 High/Continuous Demand

If the Rosemount 3051SMV 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 14.

Table 14 PFH with Good Maintenance Assumptions in FIT @ SSI=2

| Application/Device/Configuration | PFH |
|--|-----|
| 3051SMV_P1 | 104 |
| 3051SMV_P2 | 73 |
| 3051SMV_P3, 3051SMV_P5, 3051SMV_P6 | 81 |
| 3051SMV_P4, 3051SMV_P7, 3051SMV_P8 | 50 |
| 3051SMV_M1 | 150 |
| 3051SMV_M2 | 119 |
| 3051SMV_M3 | 127 |
| 3051SMV_M4 | 95 |
| 3051SFA1, 3051SFC1, 3051SFP1 – High Trip (normal conditions) | 161 |
| 3051SFA1, 3051SFC1, 3051SFP1 – Low Trip (normal conditions) | 159 |
| 3051SFA2, 3051SFC2, 3051SFP2 – High Trip (normal conditions) | 130 |
| 3051SFA2, 3051SFC2, 3051SFP2 – Low Trip (normal conditions) | 128 |
| 3051SFA3, 3051SFC3, 3051SFP3 – High Trip (normal conditions) | 138 |
| 3051SFA3, 3051SFC3, 3051SFP3 – Low Trip (normal conditions) | 136 |
| 3051SFA4, 3051SFC4, 3051SFP4 – High Trip (normal conditions) | 106 |
| 3051SFA4, 3051SFC4, 3051SFP4 – Low Trip (normal conditions) | 104 |
| 3051SFA5, 3051SFC5, 3051SFP5 – High Trip (normal conditions) | 115 |
| 3051SFA5, 3051SFC5, 3051SFP5 – Low Trip (normal conditions) | 113 |
| 3051SFA6, 3051SFC6, 3051SFP6 – High Trip (normal conditions) | 84 |



| | |
|--|----|
| 3051SFA6, 3051SFC6, 3051SFP6 – Low Trip (normal conditions) | 82 |
| 3051SFA7, 3051SFC7, 3051SFP7 – High Trip (normal conditions) | 92 |
| 3051SFA7, 3051SFC7, 3051SFP7 – Low Trip (normal conditions) | 90 |

If the Rosemount 3051SMV 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 15.

Table 15 PFH with Good Maintenance Assumptions in FIT @ SSI=2

| Application/Device/Configuration | PFH |
|--|------------|
| 3051SMV_P1 | 1006 |
| 3051SMV_P2 | 715 |
| 3051SMV_P3, 3051SMV_P5, 3051SMV_P6 | 961 |
| 3051SMV_P4, 3051SMV_P7, 3051SMV_P8 | 670 |
| 3051SMV_M1 | 1137 |
| 3051SMV_M2 | 846 |
| 3051SMV_M3 | 958 |
| 3051SMV_M4 | 800 |
| 3051SFA1, 3051SFC1, 3051SFP1 – High Trip (normal conditions) | 1148 |
| 3051SFA1, 3051SFC1, 3051SFP1 – Low Trip (normal conditions) | 1146 |
| 3051SFA2, 3051SFC2, 3051SFP2 – High Trip (normal conditions) | 857 |
| 3051SFA2, 3051SFC2, 3051SFP2 – Low Trip (normal conditions) | 855 |
| 3051SFA3, 3051SFC3, 3051SFP3 – High Trip (normal conditions) | 969 |
| 3051SFA3, 3051SFC3, 3051SFP3 – Low Trip (normal conditions) | 967 |
| 3051SFA4, 3051SFC4, 3051SFP4 – High Trip (normal conditions) | 811 |
| 3051SFA4, 3051SFC4, 3051SFP4 – Low Trip (normal conditions) | 809 |
| 3051SFA5, 3051SFC5, 3051SFP5 – High Trip (normal conditions) | 1017 |
| 3051SFA5, 3051SFC5, 3051SFP5 – Low Trip (normal conditions) | 1015 |
| 3051SFA6, 3051SFC6, 3051SFP6 – High Trip (normal conditions) | 724 |
| 3051SFA6, 3051SFC6, 3051SFP6 – Low Trip (normal conditions) | 722 |
| 3051SFA7, 3051SFC7, 3051SFP7 – High Trip (normal conditions) | 972 |
| 3051SFA7, 3051SFC7, 3051SFP7 – Low Trip (normal conditions) | 970 |



5.3 PFD_{avg} calculation Rosemount 3051SMV

Using the failure rate data displayed in section 4.4, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

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

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

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

5.4 *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" [N9] are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification. [N12]



6 Terms and Definitions

| | |
|-----------------------|---|
| Automatic Diagnostics | Tests performed online internally by the device or, if specified, externally by another device without manual intervention. |
| <i>exida</i> criteria | A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2 _H Route in IEC 61508-2. |
| Fault tolerance | Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3). |
| FIT | Failure in Time (1×10^{-9} failures per hour) |
| FMEDA | Failure Mode Effect and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance |
| PFD _{avg} | Average Probability of Failure on Demand |
| 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: V3, R2: Added section 5.2 for High/Continuous Demand, 1 August 2024
V3, R1: Added primary elements, 2017-07-12
V2, R1: Update to IEC61508:2010 and route 2H; 5/30/17
V1, R3: Minor cosmetic corrections; December 13, 2009
V1, R2: Update based on client comments; December 1, 2009
V1, R1: Released version
V0, R0: Draft; August 27, 2009

Author(s): Rudolf Chalupa, Valerie Motto

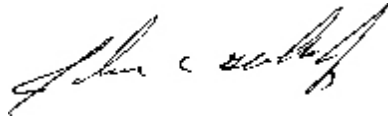
Review: V3, R2: Dan Alley (*exida*); 1 August 2024

Release Status: Released to Emerson Automation Solutions

7.3 Future enhancements

At request of client.

7.4 Release signatures

A handwritten signature in black ink, appearing to read "John C. Grebe Jr.".

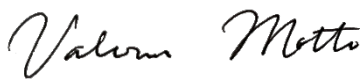
John C. Grebe Jr., CFSE, Principal Engineer

A handwritten signature in black ink, appearing to read "Ted Stewart".

Ted Stewart, CFSP, Safety Engineer

A handwritten signature in black ink, appearing to read "Rudolf P. Chalupa".

Rudolf P. Chalupa, CFSE, Senior Safety Engineer

A handwritten signature in black ink, appearing to read "Valerie Motto".

Valerie Motto, CFSP, Safety Engineer

A handwritten signature in blue ink, appearing to read "Dan Alley".

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 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 lifetime⁴ of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

Table 16 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 16 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 3051SMV per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

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

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

⁴ 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

The suggested proof test, described in Table 17, consists of a power cycle plus reasonability checks of the transmitter output and will detect ~48% of possible DU failures in the Rosemount 3051SMV.

Table 17 Suggested Proof Test – Rosemount 3051SMV

| Step | Action |
|------|--|
| 1. | Bypass the safety function and take appropriate action to avoid a false trip |
| 2. | Use HART communications to retrieve any diagnostics and take appropriate action. |
| 3. | Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value ⁵ . |
| 4. | Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value ⁶ . |
| 5. | Perform a “reasonability check” on the pressure sensor reading and the sensor temperature reading and if applicable the process temperature reading ⁷ . |
| 6. | Remove the bypass and otherwise restore normal operation |

⁵ 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.

⁶ This tests for possible quiescent current related failures.

⁷ This tests for faults in the input multiplexer and A to D converter.



B.2 Comprehensive Proof Test

The comprehensive proof test consists of performing the same steps as the partial suggested proof test but with a two-point calibration of the pressure and temperature sensors in place of the reasonability check of the sensors. This test will detect ~ 90% of possible DU failures in the device.

Table 18 Comprehensive Proof Test

| Step | Action |
|------|--|
| 1. | Bypass the safety function and take appropriate action to avoid a false trip |
| 2. | Use HART communications to retrieve any diagnostics and take appropriate action. |
| 3. | Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value ⁸ . |
| 4. | Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value ⁹ . |
| 5. | Perform a two-point calibration ¹⁰ of the transmitter pressure over the full working range (and process temperature where applicable) |
| 6. | Remove the bypass and otherwise restore normal operation |

⁸ 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.

⁹ This tests for possible quiescent current related failures.

¹⁰ If the two-point calibration is performed with electrical instrumentation, this proof test will not detect any failures of the sensor



Appendix C *exida* Environmental Profiles

Table 19 *exida* Environmental Profiles

| <i>exida</i> 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 |
| Humidity¹¹ | 0-95% Non-Condensing | 0-100% Condensing | 0-100% Condensing | 0-100% Condensing | 0-100% Condensing | N/A |
| Shock¹² | 10 g | 15 g | 15 g | 15 g | 15 g | N/A |
| Vibration¹³ | 2 g | 3 g | 3 g | 3 g | 3 g | N/A |
| Chemical Corrosion¹⁴ | G2 | G3 | G3 | G3 | G3 | Compatible Material |
| Surge¹⁵ | | | | | | |
| 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 Susceptibility¹⁶ | | | | | | |
| 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)¹⁷ | 6 kV | 6 kV | 6 kV | 6 kV | 6 kV | N/A |

¹¹ Humidity rating per IEC 60068-2-3

¹² Shock rating per IEC 60068-2-27

¹³ Vibration rating per IEC 60068-2-6

¹⁴ Chemical Corrosion rating per ISA 71.04

¹⁵ Surge rating per IEC 61000-4-5

¹⁶ EMI Susceptibility rating per IEC 61000-4-3

¹⁷ ESD (Air) rating per IEC 61000-4-2



Appendix D Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). **The numbers used in the examples are not for the product described in this report.**

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N4] and [N7].

These are:

- A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;
- B. Architecture Constraints (minimum redundancy requirements) are met; and
- C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N8].

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

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

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

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 250 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ 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 the first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore, idealistic equations should not be used for actual SIF design verification.

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

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

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

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03. See Figure 4.

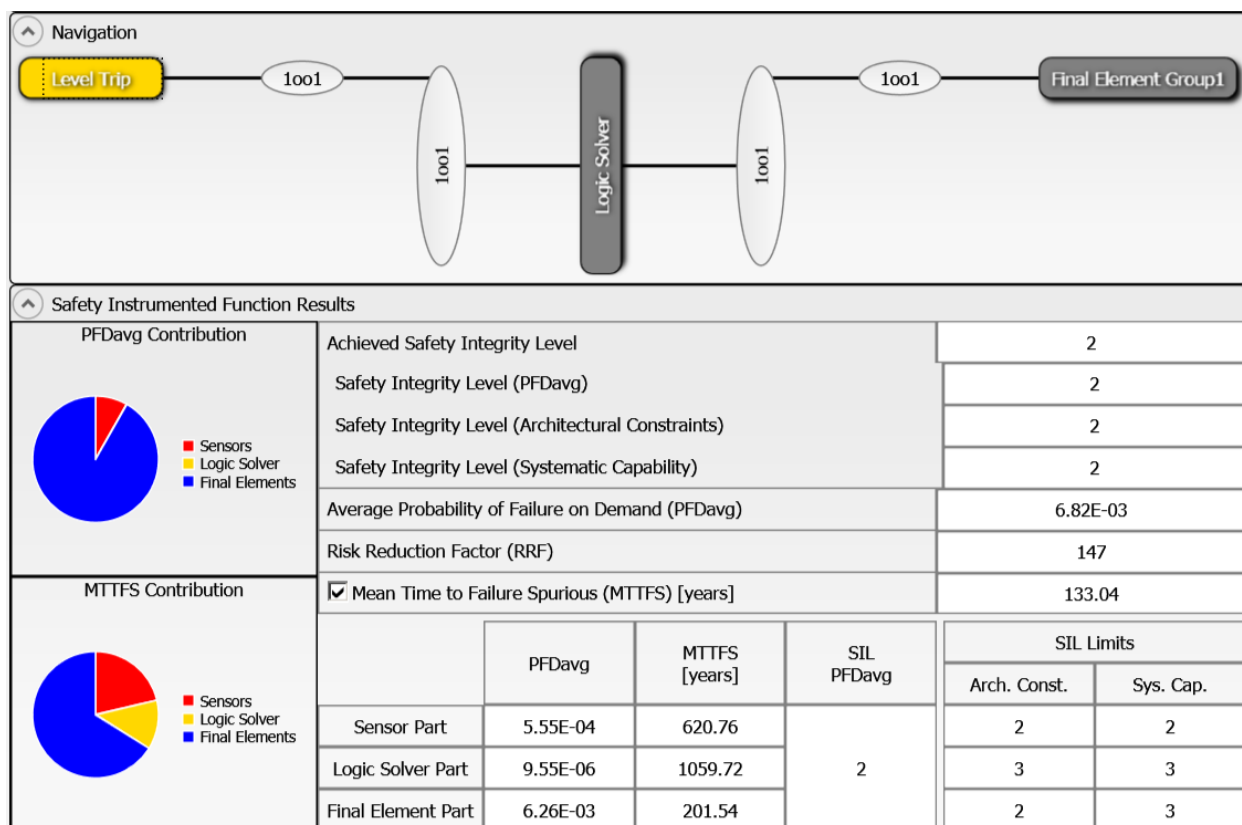


Figure 4: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 5.

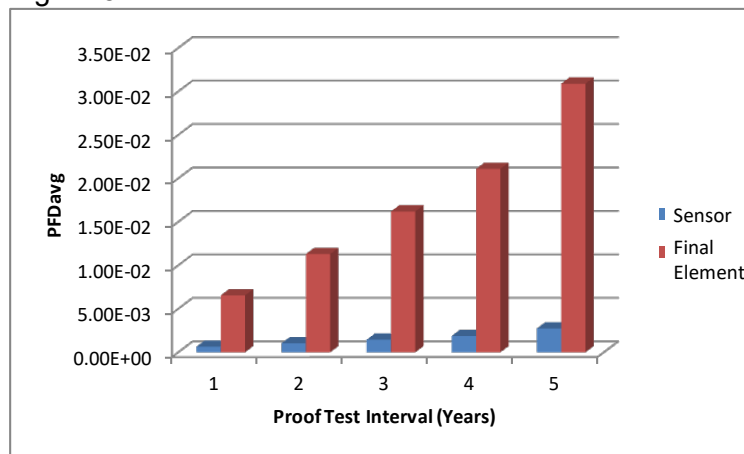


Figure 5 PFD_{avg} versus Proof Test Interval.

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

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

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 6).

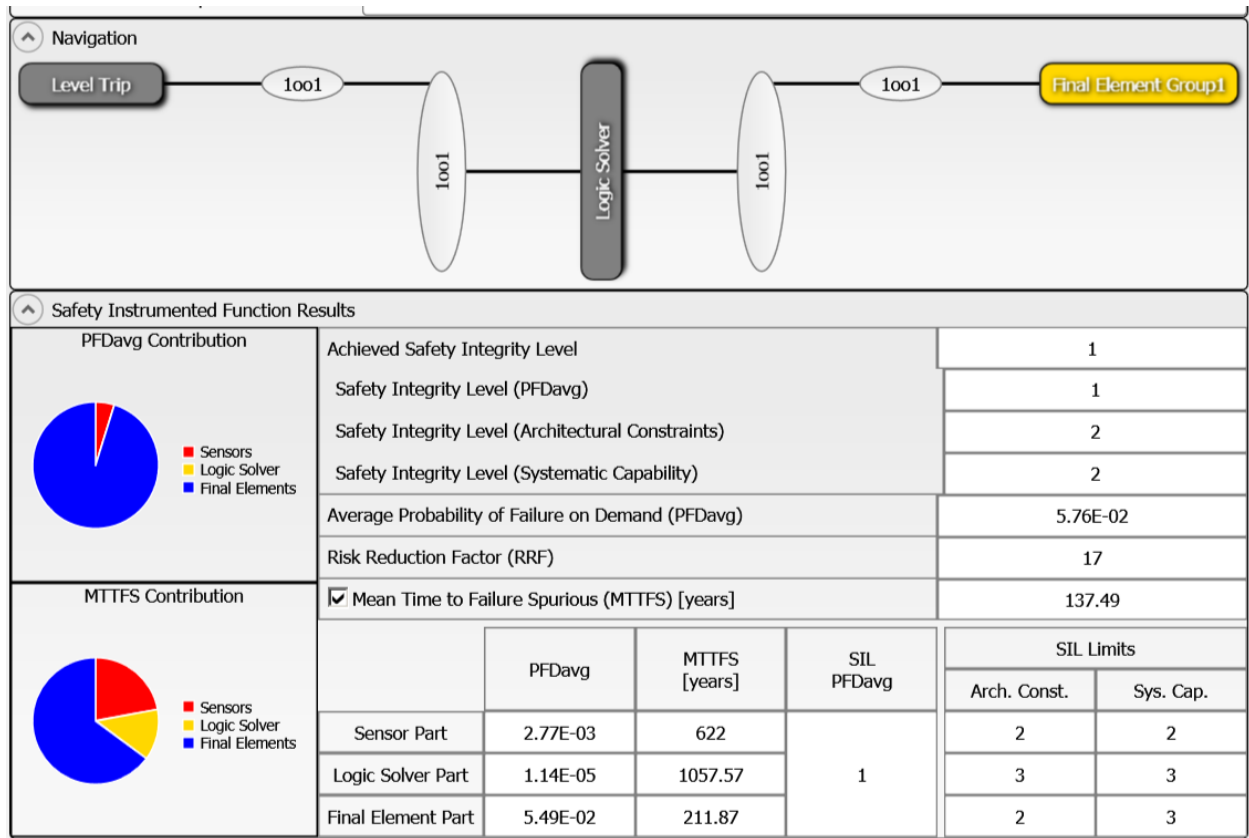


Figure 6: exSILentia results with realistic variables

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

END OF DOCUMENT