

Failure Modes, Effects and Diagnostic Analysis

Project:
3051 Pressure Transmitter with 4-20mA HART
(Device Label SW 2.x.x or later / HW 2.x.x or later)

Company:
Rosemount Inc.
Shakopee, MN
USA

Contract Number: Q25/08-049
Report No.: ROS 13/01-010 R001
Version V4, Revision R0, October 28, 2025
Valerie Motto

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

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 3051 Pressure Transmitter with 4-20mA HART, hardware software revision per Section 2.5.1. 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 3051. For full functional safety certification purposes, all requirements of IEC 61508 must be considered.

The Rosemount® 3051 is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. Table 1 gives an overview of the different versions that were considered in the FMEDA of the 3051.

Table 1 Version Overview

Option 1	Emerson's Rosemount® 3051 Pressure Transmitter with 4-20mH HART: Coplanar Differential & Coplanar Gage
Option 2	Emerson's Rosemount® 3051 Pressure Transmitter with 4-20mA HART: Coplanar Absolute, In-Line Gage & Absolute

The 3051 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 meet the *exida* criteria for Route 2_H (see Section 5.4) (and the diagnostic coverage resulting from the analysis exceeds the required 60% threshold). Therefore, as a SIF element, the 3051 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.

The analysis shows that the 3051 has a Safe Failure Fraction above 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents).

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

These failure rates are valid for the useful lifetime of the product, see 4.6.

The failure rates listed in this report are based on over 400 billion unit operating hours of industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI) [N10], [N11].

A user of the 3051 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 4

2 Project Management 5

2.1 *exida* 5

2.2 Roles of the parties involved 5

2.3 Standards and literature used 5

2.4 *exida* tools used 6

2.5 Reference documents 6

2.5.1 Documentation provided by Rosemount Inc. 6

2.5.2 Documentation generated by exida 7

3 Product Description 8

4 Failure Modes, Effects, and Diagnostic Analysis 9

4.1 Failure categories description 9

4.2 Methodology – FMEDA, failure rates 10

4.2.1 FMEDA 10

4.2.2 Failure rates 10

4.3 Assumptions 11

4.4 Failure Rate Results 11

4.5 Proof Test Coverage 13

4.5.1 Suggested Partial Proof Test 13

4.5.2 Suggested Comprehensive Proof Test 14

4.5.3 Proof Test Coverage 14

4.6 Useful Life 15

4.7 Architecture Constraints 15

5 Using the FMEDA Results 16

5.1 Impulse line clogging 16

5.2 High/Continuous Demand 16

5.3 PFD_{avg} calculation 3051 16

5.4 *exida* Route 2_H Criteria 17

6 Terms and Definitions 18

7 Status of the Document 19

7.1 Liability 19

7.2 Version History 19

7.3 Future enhancements 20

7.4 Release signatures 20

Appendix A *exida* Environmental Profiles 21

Appendix B Determining Safety Integrity Level 22

Appendix C Site Safety Index 26

C.1 Site Safety Index Profiles 26

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 3051. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

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

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

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project-oriented consulting services, safety engineering tools, detailed product assurance, ANSI National Accreditation Board (ANAB) accredited functional safety and cybersecurity certification and Irish National Accreditation Board (INAB) accredited machinery safety certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical components and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 3051
exida	Performed the hardware assessment

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

2.3 Standards and literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 4th Edition, 2017	*exida* LLC, Electrical Component Reliability Handbook, Fourth Edition, 2017
[N3]	Mechanical Component Reliability Handbook, 4th Edition, 2017	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2017
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	O'Brien, C., Gavin, R., & Bredemeyer, L., 2023	*exida* LLC., Final Elements in Safety Instrumented Systems, IEC61511 Compliant Systems and IEC 61508 Compliant Products, Second Edition, 2023, ISBN 978-1-934977-24-8

[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 Rosemount Inc.

Documents highlighted in grey have been updated since the last report release.

[D1]	2051-P2 SIRS.doc. Rev C, 20 Jun 2011	Safety Integrity Requirements Specification, C/T HART + LOI Pressure Transmitter
[D2]	Drawing No. 03031-3501 rev. 28, 2021-01-11	Microboard #7 schematic

[D3]	3031-0663.pdf, Rev. AH, 16 August 2023	Transient Protection Terminal Block schematic
[D4]	Drawing No. 3031-0815 rev. AJ, 29 March 2010	Sensor Board IV schematic, used on Rosemount 3051 with capacitive sensors
[D5]	03031-0926.pdf, Rev. AK, 10 August 2023	Sensor 3051TAC schematic, used on Rosemount 3051 with piezoresistive sensors
[D6]	Fault Injection Results.xlsx, Nov 2011	Fault Injection Test Results
[D7]	Drawing No. 02051-3520 rev. AC, 11/06/2013	Drawing Software, 4-20mA / 1-5V HART, UBD #6 (reference to version SW1.0.0)
[D8]	03031-0967.pdf, Rev. AB, 19 December 2024	Sensor Board V schematic, newer version of 03031-0815, used on Rosemount 3051 with capacitive sensors
[D9]	FMEDA Enh 2.0 DAC_rev28.xlsx, 2020-10-05	Rosemount Inc. Microboard 7 FMEDA

2.5.2 Documentation generated by exida

Documents highlighted in grey have been updated since the last report release.

[R1]	FMEDA Enh 2.1 DAC_rev28_3Oct2025.xlsx	Rosemount Inc. Microboard 7 FMEDA reviewed by *exida* and updated by Rosemount Inc.
[R2]	Terminal Board2_ 27Nov2013.efm	Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051 Transient Protected Terminal Board
[R3]	TAC Sensor (T)_ 25Oct2013.efm	Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051 Sensor T Board
[R4]	Sensor IV (C)_ 25Oct2013 .efm	Failure Modes, Effects, and Diagnostic Analysis – Rosemount 3051
[R5]	Sensor V (C)_ 25Oct2013 .efm	Failure Modes, Effects, and Diagnostic Analysis – Rosemount3051
[R6]	2051 3051 FMEDA Summary 2025-10-03.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary – Rosemount 3051
[R7]	Failure Rates for the Certificates_3051 2.x.x -7 October 2025.docx	Summary of failure rates for certificate / report

3 Product Description

The Emerson's Rosemount® 3051 Pressure Transmitter with 4-20mA HART is a two-wire 4 – 20 mA smart device used in multiple industries for both control and safety applications. The transmitter consists of a standard well proven Rosemount Sensor Board in combination with a Microboard that performs advanced process diagnostics. It 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. No other output variants are covered by this report.

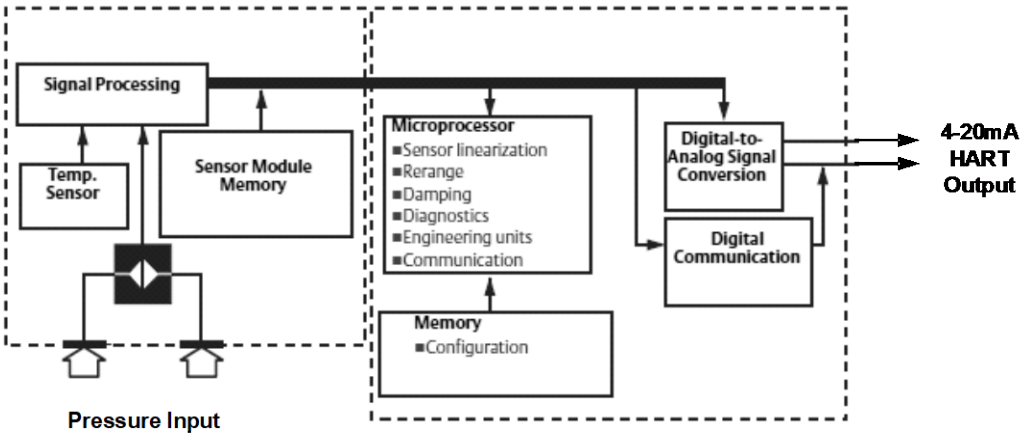


Figure 1 3051, Parts included in the FMEDA

Table 2 gives an overview of the different versions that were considered in the FMEDA of the 3051.

Table 2 Version Overview

Option 1	Emerson's Rosemount® 3051 Pressure Transmitter with 4-20mA HART: Coplanar Differential & Coplanar Gage
Option 2	Emerson's Rosemount® 3051 Pressure Transmitter with 4-20mA HART: Coplanar Absolute, In-Line Gage & Absolute

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

The Coplanar Differential & Coplanar Gage devices measure differential and gage pressure up to 2000 psi.

The Coplanar Absolute devices measure pressure up to 4000 psia.

The In-Line Gage & Absolute transmitters can measure pressures up to 20000 psi.

The 3051 is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

[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 [R1] to [R6].

4.1 Failure categories description

In order to judge the failure behavior of the 3051, 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, drifts toward the user defined threshold (Trip Point) and that leaves the output within the active scale.
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 (<3.75 or >21.75 mA, user selectable).
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. such as Partial Valve Stroke Testing.
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.
External Leakage	Failure that causes process fluids, gas, hydraulic fluids or operating media to leak outside of the valve or actuator; External Leakage is not considered part of the safety function and therefore this failure rate is not included in any of the numbers. External leakage failure rates should be reviewed for secondary safety and environmental issues.

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 and parts stress analysis with extensions to identify automatic diagnostic techniques, the failure modes relevant to safety instrumented system design, useful life, and proof test coverage. 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 ([N2] and [N3]) which were derived using failure data formulas based upon:

- Over 400-billion-unit operational hours of industry field failure data from multiple sources.
- Technical Reports such as IEC TR 62380, SN 29500 and industry sources.
- Manufacturer Meetings.
- Component Research.

The *exida* profile chosen for this FMEDA was 2 as this was judged to be the best fit for the product and application information submitted by Rosemount Inc.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

The failure rates are predicted for a Site Safety Index of SSI=2 [N10], [N11] as this level of operation is common in many industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from *exida*.

The user of these numbers is responsible for determining the failure rate applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix A. 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* for assistance.

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 3051.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire 3051.
- 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.
- The Transmitter is generally applied in relatively clean gas or liquid; therefore, no severe service has been considered in the analysis of the base Transmitter. Refer to the separate Remote Seals analysis for Severe Service applications.
- Breakage or plugging of any inlet lines has not been included in the analysis.
- Soft Error Rates (SER) were considered for relative neutron flux of 1.2 corresponding to 200 meters above sea level.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is less than 1 hour.

4.4 Failure Rate Results

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

Table 3 and Table 4 list the failure rates for the 3051 with a Site Safety Index (SSI) of 2 (good site maintenance practices).

Table 3 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2 (Option 1)

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		52
Fail Dangerous Detected		523
Fail Detected (detected by internal diagnostics)	424	
Fail High (detected by logic solver)	14	
Fail Low (detected by logic solver)	85	
Fail Dangerous Undetected		35
No Effect		191
Annunciation Undetected		14
External Leak		23

Table 4 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2 (Option 2)

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		63
Fail Dangerous Detected		543
Fail Detected (detected by internal diagnostics)	440	
Fail High (detected by logic solver)	18	
Fail Low (detected by logic solver)	85	
Fail Dangerous Undetected		43
No Effect		200
Annunciation Undetected		16
External Leak		23

Table 5 lists the failure rates for the 3051 according to IEC 61508.

Table 5 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2 according to IEC 61508

Application/Device/Configuration	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	#	SFF
Option 1	0	52	523	35	205	94%
Option 2	0	63	543	43	216	93%

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

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

E = External Leaks

The External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure rates do not directly contribute to the reliability of the valve but should be reviewed for secondary safety and environmental issues.

These failure rates are valid for the useful lifetime of the product, see section 4.6.

4.5 Proof Test Coverage

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.

4.5.1 Suggested Partial Proof Test

The suggested proof test for the 3051 is described in Table 6. Refer to the table in 4.5.2 for the Proof Test Coverages.

The suggested proof test consists of a setting the output to the min and max, see Table 6.

Table 6 Suggested Partial 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[4].
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[5].
5.	Inspect the transmitter for any leaks, visible damage or contamination.
6.	Remove the bypass and otherwise restore normal operation.

[4] 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.

[5] This tests for possible quiescent current related failures.

4.5.2 Suggested Comprehensive Proof Test

The suggested proof test for the 3051 is described in Table 6. Refer to the table in 4.5.2 for the Proof Test Coverages.

The suggested proof test consists of a setting the output to the min and max and a calibration check, see Table 6.

Table 7 Suggested 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[6].
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[7].
5.	Inspect the transmitter for any leaks, visible damage or contamination.
6.	Perform a two-point calibration[8] of the transmitter over the full working range.
7.	Remove the bypass and otherwise restore normal operation.

4.5.3 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 8.

Table 8 Proof Test Coverage –3051

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
3051, Option 1, Simple Proof Test	20	44%
3051, Option 1, Comprehensive Proof Test	7	81%
3051, Option 2, Simple Proof Test	28	35%
3051, Option 2, Comprehensive Proof Test	8	81%

[6] 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.
[7] This tests for possible quiescent current related failures.
[8] If the two-point calibration is performed with electrical instrumentation, this proof test will not detect any failures of the sensor

4.6 Useful Life

The Useful Life of the device predicted by component failure data is 50 years..

4.7 Architecture Constraints

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (see Section 5.4).

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 61508-2.

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H (which is more stringent than IEC 61508-2) (and the diagnostic coverage resulting from the analysis exceeds the required 60% threshold). Therefore, as a SIF element, the 3051 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.

The analysis shows that the 3051 has a Safe Failure Fraction above 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents).

The architectural constraint type for the 3051 is B. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

A user of the 3051 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). The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

5 Using the FMEDA Results

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

5.1 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 3051 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 3051 failure rates.

5.2 High/Continuous Demand

If the 3051 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 9.

Table 9 PFH with Good Maintenance Assumptions in FIT @ SSI=2

Application/Device/Configuration	PFH
Option 1	35
Option 2	43

If the 3051 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 10.

Table 10 PFH with Good Maintenance Assumptions in FIT @ SSI=2

Application/Device/Configuration	PFH
Option 1	558
Option 2	587

5.3 PFD_{avg} calculation 3051

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 B 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 Table 8.

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 undertaking of specific tests,
>
> in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

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

1. field unit operational hours of 10,000,000 per each component or known common usage of the component for over ten years in at least 10 units; and
2. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
3. failure definitions are realistic without data censoring of failures with both a systematic and random failure case [N9]; and
4. 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 automatically performed online internally by the device or, if specified, externally by another device without manual intervention or manual interpretation of the results.
DC	Diagnostic Coverage
exida 2H criteria	A method to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route with more detail and more requirements than specified in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
FIT	Failure in Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
PFD_{avg}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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 engineering literature and International technical reports. Failure rates are obtained from field failure studies and other sources. *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.

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

7.2 Version History

Contract Number	Report Number	Revision Notes
Q25/08-049	ROS 13/01-010 R001 V4 R0	Surveillance Audit. Template update. Update to soft error rate calculations on Microboard. VAM 7 October 2025
Q24/07-064	ROS 13/01-010 R001 V3 R5	PFH Definition added to Section 6. VAM 16 August 2024
Q24/07-064	ROS 13/01-010 R001 V3 R4	Minor adjustment to failure rate for rounding error. VAM 1 August 2024
Q22/03-185	ROS 13/01-010 R001 V3 R3	Added high/continuous demand results, RPC, 2023-02-15
Q22/03-185	ROS 13/01-010 R001 V3 R2	updated failure rates based on Sensor IV (03031-0815) and not Sensor V (03031-0967); RPC
Q22/03-185	ROS 13/01-010 R001 V3 R1	Updated per Microboard 7, RPC, 2022-06-30
Q15/10-010	ROS 13/01-010 R001 V2 R3	included cold temperature; updated template; recertification; TES 10/14/16
Q14/12-011	ROS 13/01-010 R001 V2 R2	Updated per Rosemount requests; TES May 2015
Q14/12-011	ROS 13/01-010 R001 V2 R1	Updated for recertification; added appendix D; TES April 2015
Q13/01-010	ROS 13/01-010 R001 V1 R2	Updated Proof Test Coverage; TES and WGF, December 13, 2013
Q13/01-010	ROS 13/01-010 R001 V1 R1	Updated ROS 11/07-062 V1 R7 to current template; T-001 V8R1,; incorporated 2_H capability; TES and GPS, March 13, 2013

Reviewer: Paddy Healy, *exida*, 28th Oct 2025

Status: Released, 28th Oct 2025

7.3 Future enhancements

At request of client.

7.4 Release signatures



Valerie Motto, CFSP, Senior Safety Engineer



Paddy Healy, Senior Safety Engineer

Appendix A *exida* Environmental Profiles

Table 11 *exida* **Environmental Profiles**

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
Average Internal Temperature	60°C	30°C	45°C	10°C	45°C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5°C	25°C	25°C	2°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
Salt/Chemical Corrosion[22]	Low	Medium	Medium	High	High	High
Humidity High[23]	95%	100%	100%	100%	100%	100%
Humidity Low	20%	5%	5%	5%	5%	5%
Mechanical Shock/Vibration[24]	Low	Low	Low	Low	Medium	High
Average Altitude	200 m	200 m	200 m	-50 m	30 m	200 m
Electrical Overstress (EOS)[25]	Low	Medium	Medium	Low	Medium	Medium

[22] Chemical Corrosion rating per ISA 71.04
[23] Humidity ratings per IEC 60068-2-3
[24] Shock rating per IEC 60068-2-27, Vibration rating per IEC 60068-2-6 / IEC 61496-1
[25] EOS levels per IEC 61000-4-5 (Surge) and IEC 61326-3 (EMI Susceptibility)

Appendix B 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 400 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.

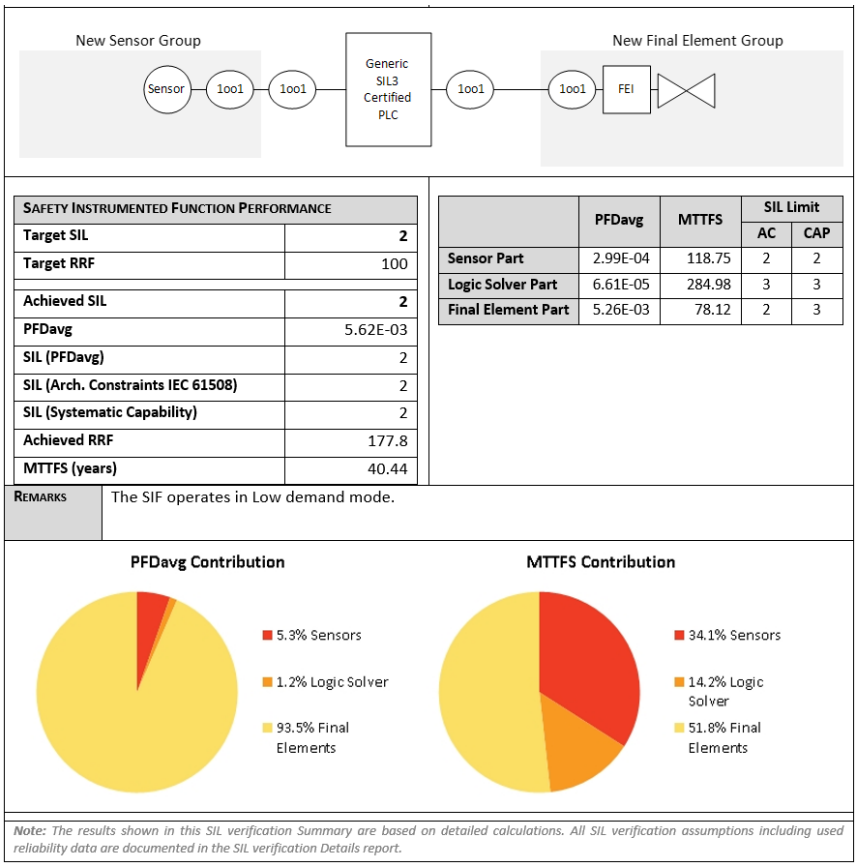
Simplified equations often account for only for the first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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 5.62E-03 which meets SIL 2 with a risk reduction factor of 179. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.99E-04, Logic Solver PFD_{avg} = 6.61E-05, and Final Element PFD_{avg} = 5.26E-03. See Figure 2.



Safety Instrumented Function Performance	
Target SIL	2
Target RRF	100
Achieved SIL	2
PFDavg	5.62E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508)	2
SIL (Systematic Capability)	2
Achieved RRF	177.8
MTTFS (years)	40.44

	PFDavg	MTTFS	SIL Limit	
			AC	CAP
Sensor Part	2.99E-04	118.75	2	2
Logic Solver Part	6.61E-05	284.98	3	3
Final Element Part	5.26E-03	78.12	2	3

Remarks: The SIF operates in Low demand mode.

Note: The results shown in this SIL verification Summary are based on detailed calculations. All SIL verification assumptions including used reliability data are documented in the SIL verification Details report.

Figure 2: exSILentia results for idealistic variables.

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

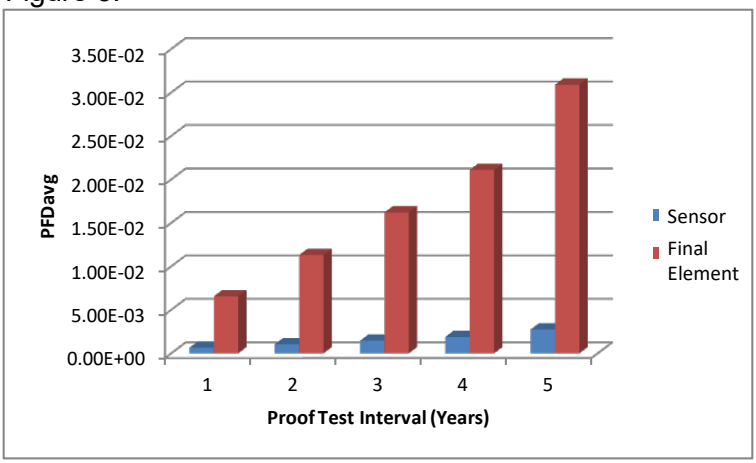


Figure 3 PFD_{avg} versus Proof Test Interval.

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 3.80E-02 which barely meets SIL 1 with a risk reduction factor 26 The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 1.13E-03, Logic Solver PFD_{avg} = 1.55E-04, and Final Element PFD_{avg} = 3.68E-02 (Figure 4).

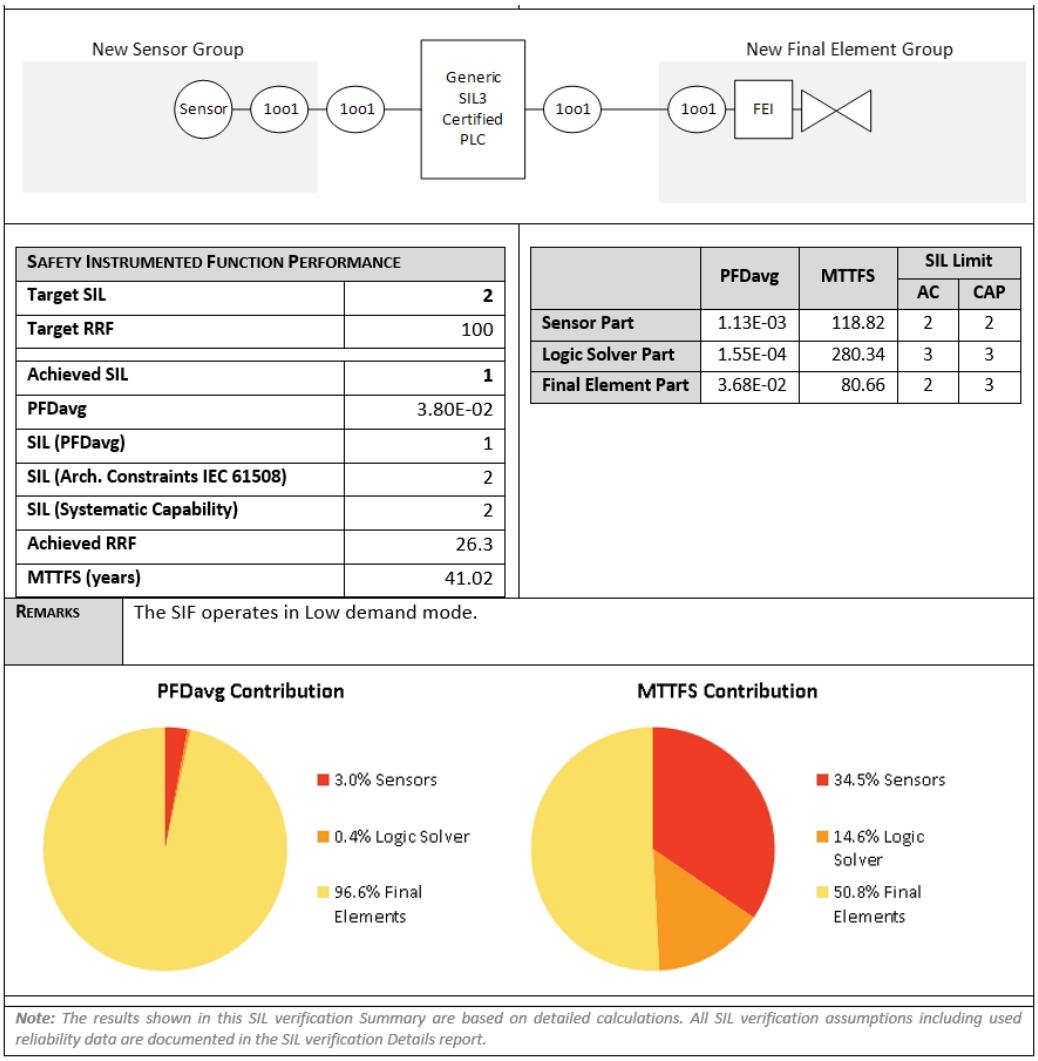


Figure 4: exSILentia results with realistic variables

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

Appendix C Site Safety Index

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

C.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIFs on the site. Table 12 details the interpretation of each SSI level. Note that the levels mirror the levels of SIL assignment and that SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site and therefore there is no degradation in safety performance due to any end-user activities or practices, i.e., that the product inherent safety performance is achieved.
Several factors have been identified thus far which impact the Site Safety Index (SSI). These include the quality of:
Commission Test
Safety Validation Test
Proof Test Procedures
Proof Test Documentation
Failure Diagnostic and Repair Procedures
Device Useful Life Tracking and Replacement Process
SIS Modification Procedures
SIS Decommissioning Procedures
and others

Table 12 *exida* Site Safety Index Profiles

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

END OF DOCUMENT