Failure Modes, Effects and Diagnostic Analysis

Project:
2140:SIS Vibrating Fork Liquid Level Detector

Company:
Rosemount Tank Radar
Sweden

Contract Number: Q22/11-188
Report No.: RTR 21-01-012 R001
Version V4, Revision R2, February 16, 2023
Rudolf Chalupa

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 2140:SIS Vibrating Fork Liquid Level Detector, hardware and 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 2140:SIS. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 2140 liquid level detector is a 2-wire smart device used to sense whether the process level is above or below a particular point. It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of failure.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 2140:SIS.

Table 1 Version Overview

2140:SIS T0 Wet On	SIS model liquid level detector configured as Wet=On fitted with a standard T0 terminal block. The safe state represents a dry fork.
2140:SIS T0 Dry On	SIS model liquid level detector configured as Dry=On fitted with a standard T0 terminal block. The safe state represents a wet fork.
2140:SIS T1 Wet On	SIS model liquid level detector configured as Wet=On fitted with an optional T1 terminal block. The safe state represents a dry fork.
2140:SIS T1 Dry On	SIS model liquid level detector configured as Dry=On fitted with an optional T1 terminal block. The safe state represents a wet fork.

The 2140:SIS 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 5.2). Therefore the 2140:SIS meets the hardware architectural constraints for up to SIL 2 at HFT=0 or SIL 3 at HFT=1) when the listed failure rates are used.

Based on the assumptions listed in 4.3, the failure rates for the 2140:SIS are listed in section 4.4.

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

Failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.

A user of the 2140:SIS 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 Tank Radar 6

2.5.2 Documentation generated by *exida* 7

3 Product Description 8

4 Failure Modes, Effects, and Diagnostic Analysis 10

4.1 Failure categories description 10

4.2 Methodology – FMEDA, failure rates 11

4.2.1 FMEDA 11

4.2.2 Failure rates 11

4.3 Assumptions 12

4.4 Results 13

5 Using the FMEDA Results 16

5.1 PFD_{avg} calculation 2140:SIS 16

5.2 *exida* Route 2_H Criteria 16

6 Terms and Definitions 17

7 Status of the Document 18

7.1 Liability 18

7.2 Releases 18

7.3 Future enhancements 19

7.4 Release signatures 19

Appendix A Lifetime of Critical Components 20

Appendix B Proof Tests to Reveal Dangerous Undetected Faults 21

B.1 Suggested Comprehensive Proof Test 21

B.2 Suggested Partial Proof Test 21

B.3 Proof Test Coverage 23

Appendix C *exida* Environmental Profiles 24

Appendix D Determining Safety Integrity Level 25

Appendix E Site Safety Index 29

E.1 Site Safety Index Profiles 29

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 2140:SIS. From this, failure rates and example PFD_{avg} values may be calculated.

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

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

2 Project Management

2.1 *exida*

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

2.2 Roles of the parties involved

Rosemount Tank Radar	Design Control and Manufacturer of the 2140:SIS
exida	Performed the hardware assessment

Rosemount Tank Radar contracted *exida* in November 2022 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]	Component Reliability Database, 2022	*exida* Innovation LLC, Component Reliability Database, V4.2.3, 2022
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	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
[N7]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

[N8]	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.
[N9]	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.
[N10]	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.
[N11]	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.
[N12]	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.
[N13]	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 Tank Radar

[D1]	Doc # 02140-5003, Rev AD, 2016-10-20	Schematic Drawing, 2140 Microboard
[D2]	Doc # 02140-5063, Rev AA, 2015-03-12	Circuit Diagram PCB Amplifier 2140
[D3]	Doc # 03031-0655, Rev AF, 2011-04-01	Schematic Diagram, 4-20mA Standard Terminal Block
[D4]	Doc # 03031-0663, Rev AF, 2016-07-13	Schematic Diagram, 4-20mA Transient Terminal Block
[D5]	Doc # 02140-5053, Rev AB, 2018-04-03	Schematic Diagram, Isolator PCB 2140

[D6]	Doc # 71097/1242, Rev 3, 2007-08-11	Approval Drawing Squing 2 Intrinsically Safe High Temperature
[D7]	2140 wired hart new FMEDA-standard term block and isolator board.xlsx, 2016-11-10	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS
[D8]	2140 wired hart new FMEDA-transient term block and isolator board.xlsx, 2016-11-14	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS
[D9]	2140 diagnostic changes.xlsx, 2016-03-12	Diagnostics descriptions
[D10]	System Description for Exida.txt, 2016-03-21	system description for FMEDA report
[D11]	System Block Diagram For Exida.vsd, 2016-03-21	Block diagram for FMEDA report
[D12]	MOB 15-08-12 R001 V2R1 FMEDA 2140 GL MARKUP.pdf, 2017-11-17	Client markup of V2R1 (used to generate V2R2a)
[D13]	TR 4846 2140 wired hart new FMEDA-standard term block and isolator board update 11-10-17.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS T0 (updated)
[D14]	TR 4847 2140 wired hart new FMEDA-transient term block and isolator board update 11-10-17.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS T1 (updated)
[D15]	Doc #02140-5002-0001 Rev AH.pdf, 2022-10-27	Bill of Material, 2140 Microboard

2.5.2 Documentation generated by *exida*

[R1]	2140 wired hart new FMEDA-standard term block - RPC 2016-03-21.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS; Std Term Block
[R2]	2140 wired hart new FMEDA-with transient terminal block- RPC 2016-03-21.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS; Transient Term Block
[R3]	2140 wired hart new FMEDA-standard term block and isolator board RPC 2016-11-15.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2140:SIS; Std Term Block
[R4]	TR 4847 2140 wired hart new FMEDA-transient term block and isolator board update 2023-Feb-16.xlsx	Updated review (with DC) for FMEDA – 2140:SIS; Transient Term Block
[R5]	TR 4846 2140 wired hart new FMEDA-standard term block and isolator board update 2023-Feb-16.xlsx	Updated review (with DC) for FMEDA – 2140:SIS; Std Term Block

3 Product Description

The 2140:SIS vibrating fork liquid level detector is a smart device used in many different industries for point level sensing applications. A vibrating fork sensor is continuously monitored by the product, with changes in its natural resonant frequency being used to determine the condition of the sensor. A 4-20mA current output is used to indicate the liquid level, with discrete, user configurable current levels being set at the current output dependent upon the sensor condition. The 2140:SIS is microprocessor-based and contains internal diagnostics as well as the ability to communicate via the HART digital protocol.

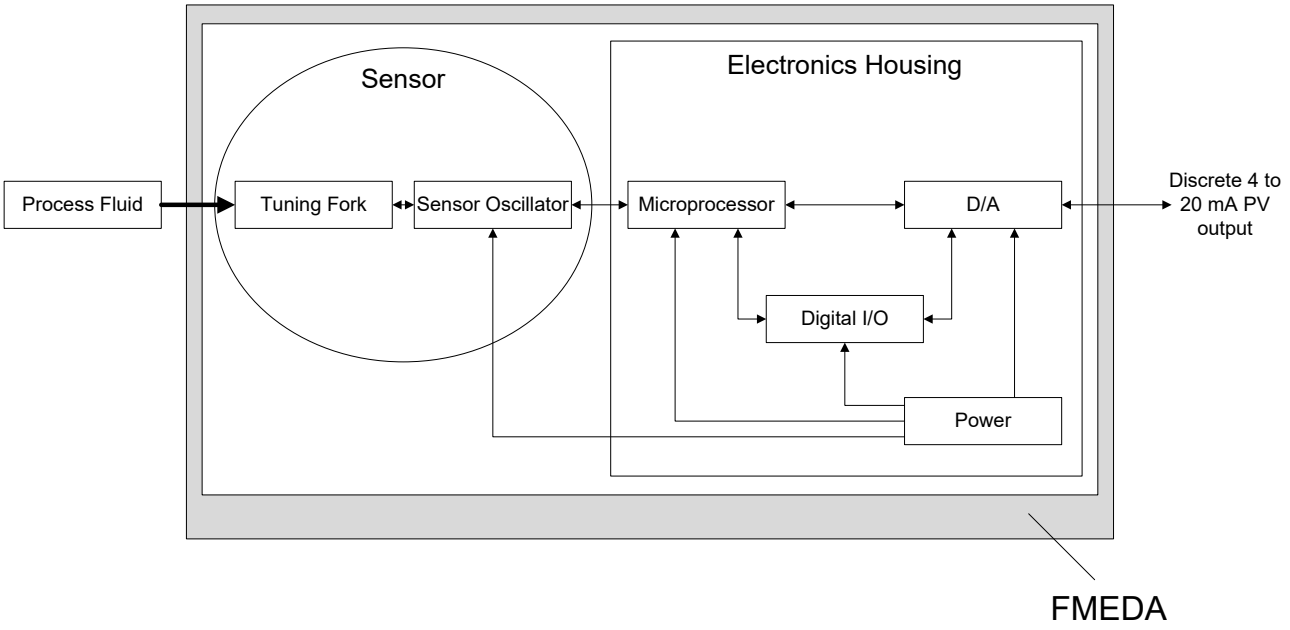


Figure 1 2140:SIS, Parts included in the FMEDA

The 2140:SIS is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

Two terminal block types are available. The T0 type is fitted as standard. When transient protection is required, the T1 type must be specified during product ordering.

Table 2 gives an overview of the different versions considered in the FMEDA of the 2140:SIS.

[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.

Table 2 Version Overview

2140:SIS T0 Wet On	SIS model liquid level detector configured as Wet=On fitted with a standard T0 terminal block. The safe state represents a dry fork.
2140:SIS T0 Dry On	SIS model liquid level detector configured as Dry=On fitted with a standard T0 terminal block. The safe state represents a wet fork.
2140:SIS T1 Wet On	SIS model liquid level detector configured as Wet=On fitted with an optional T1 terminal block. The safe state represents a dry fork.
2140:SIS T1 Dry On	SIS model liquid level detector configured as Dry=On fitted with an optional T1 terminal block. The safe state represents a wet fork.

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] and [R2].

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level. Fault Injection Test results were incorporated into the FMEDA analyses.

4.1 Failure categories description

In order to judge the failure behavior of the 2140:SIS, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the output goes to the predefined alarm state (<3.6mA or >21 mA, user selectable).
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 does not respond to a demand from the process.
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 high alarm output current (> 21 mA).
Fail Low	Failure that causes the output signal to go to the 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 which are only safe and dangerous, both detected and undetected.

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 Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques and parts stress analysis with the extension to identify automatic diagnostic techniques, the failure modes relevant to safety instrumented system design, and proof test coverage. It is a technique recommended to generate failure rates for each failure mode category [N12],[N13].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military, or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Component Reliability Database [N2] which were derived using over 400 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 Profile 2 as this was judged to be the best fit for the product and application information submitted by Rosemount Tank Radar. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

The failure rates are predicted for a Site Safety Index of SSI=2 [N9],[N10] as this level of operation is common in the process industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from *exida*.

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

Accurate plant specific data may be used to check validity of this failure rate data. If a user has data collected from a good proof test reporting system, such as *exida* SILStat™, that indicates higher failure rates, then 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 2140:SIS.

- Only a single component failure will fail the entire 2140:SIS.
- Failure rates are constant; wear-out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Failures caused by operational errors are site specific and therefore are not included.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- 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 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 2140:SIS FMEDA.

Table 3 2140:SIS Failure Rates T0 Wet On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		11
Fail Dangerous Detected		587
Fail Detected (detected by internal diagnostics) [3]	518	
Fail High (detected by logic solver)	34	
Fail Low (detected by logic solver)	35	
Fail Dangerous Undetected		17
No Effect		137
Annunciation Undetected		22

Table 4 2140:SIS Failure Rates T0 Dry On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		15
Fail Dangerous Detected		586
Fail Detected (detected by internal diagnostics)	517	
Fail High (detected by logic solver)	34	
Fail Low (detected by logic solver)	35	
Fail Dangerous Undetected		15
No Effect		137
Annunciation Undetected		22

[3] In the case of 4-20mA transmitters, this Fail Detected (detected by internal diagnostics) category includes Safe Detected, Dangerous Detected, and Annunciation Detected failure rates.

Table 5 Failure rates 2140:SIS T1 Wet On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		23
Fail Dangerous Detected		530
Fail Detected (detected by internal diagnostics) [4]	466	
Fail High (detected by logic solver)	32	
Fail Low (detected by logic solver)	32	
Fail Dangerous Undetected		13
No Effect		135
Annunciation Undetected		20

Table 6 Failure rates 2140:SIS T1 Dry On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		23
Fail Dangerous Detected		531
Fail Detected (detected by internal diagnostics)	467	
Fail High (detected by logic solver)	33	
Fail Low (detected by logic solver)	31	
Fail Dangerous Undetected		12
No Effect		134
Annunciation Undetected		20

Table 7 lists the failure rates for the 2140:SIS according to IEC 61508.

[4] In the case of 4-20mA transmitters, this Fail Detected (detected by internal diagnostics) category includes Safe Detected, Dangerous Detected, and Annunciation Detected failure rates. This applies to Table 3 through Table 6.

Table 7 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF	DC[6]
2140:SIS T0 Wet On	0	11	587	17	97%	90%
2140:SIS T0 Dry On	0	15	586	15	98%	90%
2140:SIS T1 Wet On	0	23	530	13	98%	91%
2140:SIS T1 Dry On	0	23	531	12	98%	91%

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

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 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (see Section 5.2).

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

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

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H, which is more stringent than IEC 61508-2. Therefore the 2140:SIS meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 at HFT=1) when the listed failure rates are used.

[5] 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.

[6] Diagnostic Coverage in this table is calculated using the Dangerous Detected and Dangerous Undetected values that were calculated from the FMEDA, not the λ_{DD} and λ_{DU} listed in Table 7 (i.e., the Dangerous Detected in this DC calculation does not include Safe Detected or Annunciation Detected).

5 Using the FMEDA Results

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

5.1 PFD_{avg} calculation 2140:SIS

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 is listed in Table 11.

5.2 *exida* Route 2_H Criteria

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

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

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

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" vs. "systematic" are checked by *exida*; and

5. every component used in an FMEDA meets the above criteria.

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

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
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
LOI	Local Operator Interface
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
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 marketplace, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three-year period should be sufficient for current usage without significant question.

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

7.2 Releases

Version History:

V4, R2 Corrections to failure rate tables (no impact to SIL or route 1H/2H), 2023-02-16

V4, R1: Surveillance Audit, Replaced SFF with DC since this is 2H VAM, 2023-01-26

V3, R2: Revised after internal and customer review; Updated per latest analysis; RPC/JCY, 18-Mar-2021.

V3, R1: corrections from Nov-2017 for proof test and model designations; allow SC3 with RTR based on re-assessment; JCY, 11-Mar-2021; Q 21-01-012.

V2, R3: change ownership to RTR; JCY, 24-Jun-2020; Q20/04-151

V2, R2b: Recertification, LLS, 2020-03-30

V2, R2a: Updated to reflect model changes, clarify proof tests, 2017-11-21

V2, R1: Updated per sensor isolation redesign, 2016-11-14

V1, R6: Updated partial proof test results, 2016-10-04

V1, R5: Update product name 2016-07-29

V1, R4: Minor corrections 2016-05-23

V1, R3: Minor corrections 2016-05-18

V1, R2: Updated per client feedback; 2016-05-16

V1, R1: Released to Rosemount Measurement Limited; 2016-03-22

V0, R1: Draft; 2016-03-21

Original Author and Creator of FMEDA: Rudolf Chalupa

Reviewer: Molly O'Brien, exida, 26 January 2023

Release Status: Released to Rosemount Tank Radar, 26 January 2023

7.3 Future enhancements

At request of client.

7.4 Release signatures

Rudolf P. Chalupa, CFSE, Senior Safety Engineer

Valerie Motto, Safety Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime[7] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

Table 8 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 8 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 2140:SIS 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.

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

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

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

B.1 Suggested Comprehensive Proof Test

The suggested comprehensive proof test for the 2140:SIS is described in Table 9. Refer to the table in B.3 for the Proof Test Coverages

The suggested comprehensive proof test consists of a setting the output to the min and max, and checking the sensor and associated analog output levels, see Table 9.

Table 9 Suggested Comprehensive Proof Test

Step	Action
1.	Inspect the accessible parts of the liquid level detector for any leaks or damage.
2.	Bypass the safety function and take appropriate action to avoid a false trip.
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.	Change process conditions such that the tuning fork experiences the configured alarm condition and verify the analog output reaches the configured off analog current within the expected time period as indicated by the setting of the Output Delay parameter.
6.	Change process conditions such that the tuning fork experiences the configured normal condition and verify the analog output reaches the configured on analog current within the expected time period as indicated by the setting of the Output Delay parameter.
7.	Remove the bypass and otherwise restore normal operation.

B.2 Suggested Partial Proof Test

The suggested partial proof test for the 2140:SIS is described in Table 10. Refer to the table in B.3 for the Proof Test Coverages

The partial proof test exercises the signal processing and output, but does not test the sensor, see Table 10.

[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.

Table 10 Suggested Partial Proof Test

Step	Action
1.	Inspect the accessible parts of the liquid level detector for any leaks or damage.
2.	Bypass the safety function and take appropriate action to avoid a false trip.
3.	Trigger the device Proof Test using either the appropriate HART command or LOI.
4.	Verify the analog output current reaches the configured low alarm, off, on and high alarm levels and is maintained at that level for one quarter of the Proof Test Duration parameter.
5.	Remove the bypass and otherwise restore normal operation.

B.3 Proof Test Coverage

The Proof Test Coverages for the various product configurations are given in Table 11 and Table 12.

Table 11 Full Proof Test Coverage – 2140:SIS

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
2140:SIS T0 Wet On	7	59%
2140:SIS T0 Dry On	7	55%
2140:SIS T1 Wet On	6	56%
2140:SIS T1 Dry On	5	54%

Table 12 Partial Proof Test Coverage – 2140:SIS

Device	$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
2140:SIS T0 Wet On	12	26%
2140:SIS T0 Dry On	12	20%
2140:SIS T1 Wet On	10	26%
2140:SIS T1 Dry On	9	21%

Appendix C *exida* Environmental Profiles

Table 13 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	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
Humidity[10]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[11]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[12]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[13]	G2	G3	G3	G3	G3	Compatible Material
Surge[14]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[15]						
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)[16]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[10] Humidity rating per IEC 60068-2-3
[11] Shock rating per IEC 60068-2-27
[12] Vibration rating per IEC 60068-2-6
[13] Chemical Corrosion rating per ISA 71.04
[14] Surge rating per IEC 61000-4-5
[15] EMI Susceptibility rating per IEC 61000-4-3
[16] 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 [N6].

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 [N7].

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

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

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

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

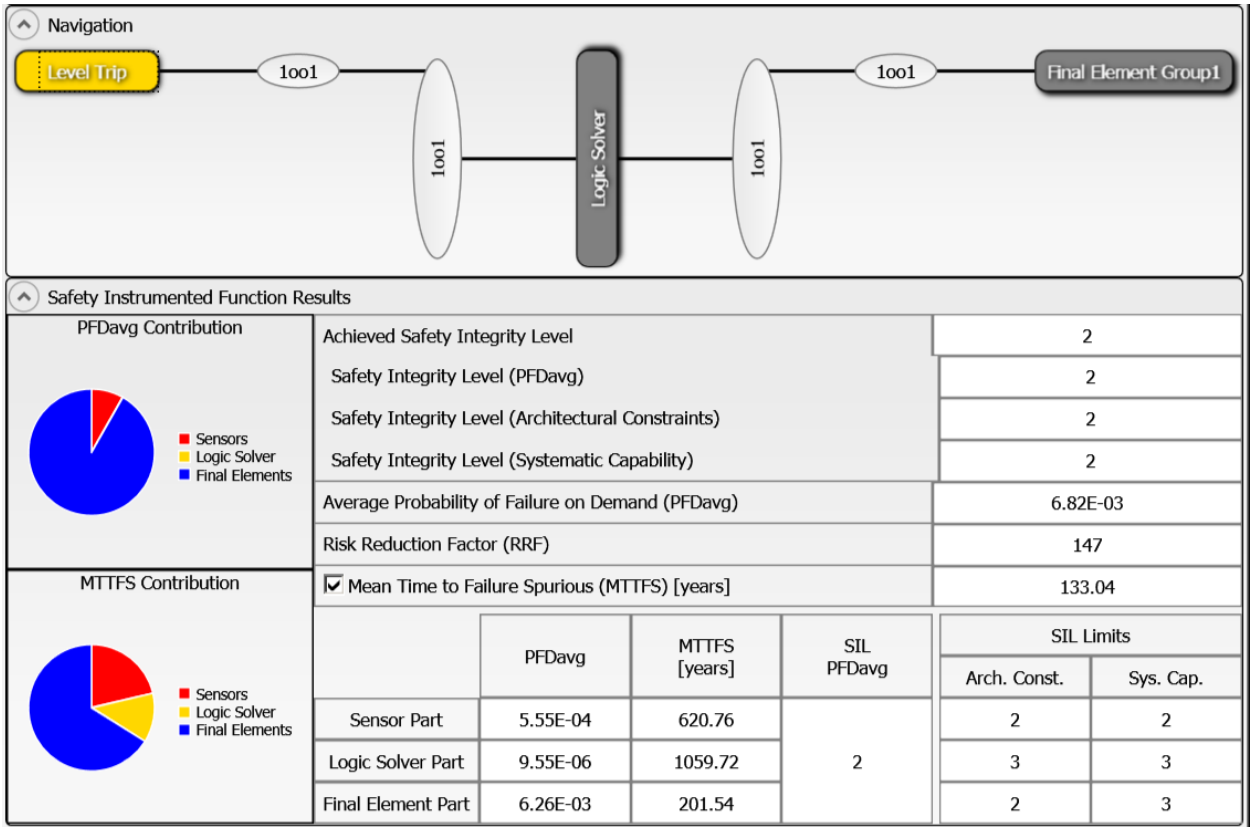
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic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

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

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

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

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



Achieved Safety Integrity Level	2
Safety Integrity Level (PFDavg)	2
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	6.82E-03
Risk Reduction Factor (RRF)	147
☑ Mean Time to Failure Spurious (MTTFS) [years]	133.04

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	5.55E-04	620.76	2	2	2
Logic Solver Part	9.55E-06	1059.72		3	3
Final Element Part	6.26E-03	201.54		2	3

Figure 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.

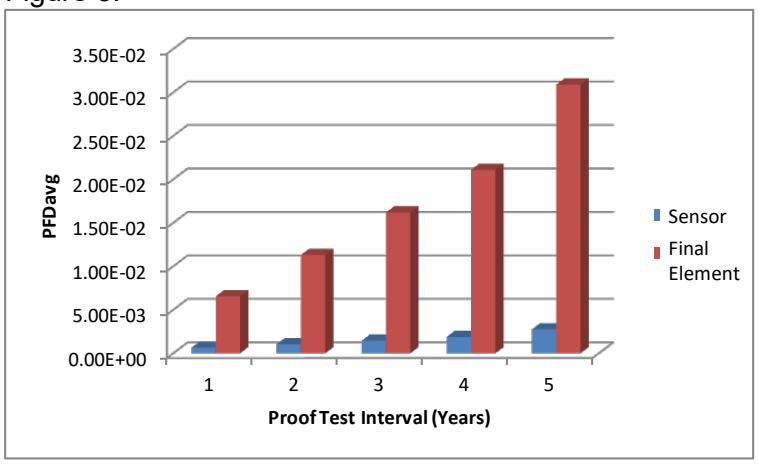
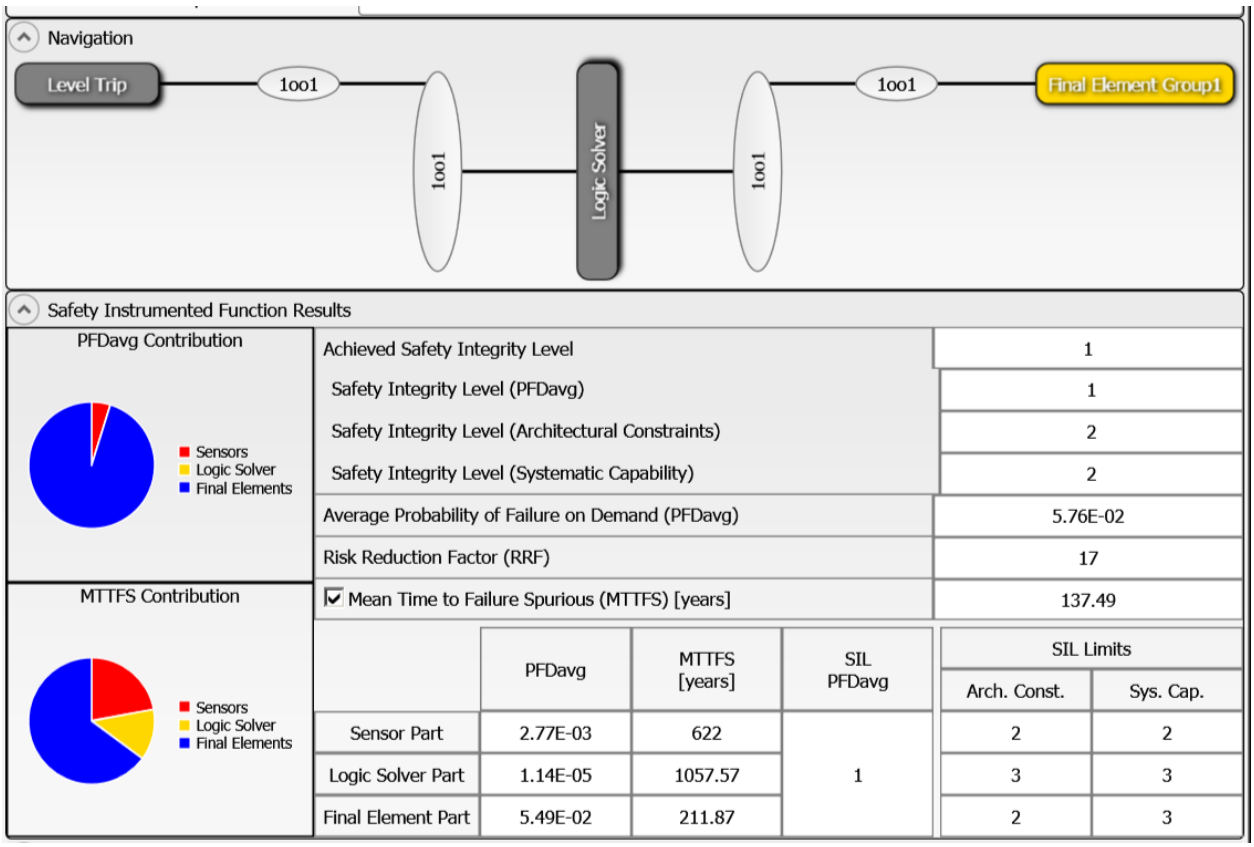


Figure 3 PFD_{avg} versus Proof Test Interval.

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 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 4).



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

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

Figure 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 E Site Safety Index

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

E.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIFs on the site. Table 14 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 14 *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.

E.2 Site Safety Index Failure Rates – 2140:SIS

Failure rates of each individual device in the SIF are increased or decreased by a specific multiplier which is determined by the SSI value and the device itself. It is known that final elements are more likely to be negatively impacted by less-than-ideal end-user practices than are sensors or logic solvers. By increasing or decreasing device failure rates on an individual device basis, it is possible to more accurately account for the effects of site practices on safety performance.

Table 15 lists the failure rates for the 2140:SIS according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Insert other tables from section 4.5 if applicable then delete this sentence.

Table 15 Failure rates for Static Applications with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
2140:SIS T0 Wet On	0	10	528	15
2140:SIS T0 Dry On	0	13	527	14
2140:SIS T1 Wet On	0	20	477	12
2140:SIS T1 Dry On	0	21	479	11