



## **Failure Modes, Effects and Diagnostic Analysis**

Project:  
2120 Level Switch

Company:  
Rosemount Tank Radar  
Sweden

Contract Numbers: Q20/09-098  
Report No.: ROS 20-09-098 R003  
Version V3, Revision R2, January 7, 2021  
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 2120 Level Switch, as described in section 2.4.1. 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 2120 Level Switch. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 2120 Level Switch is a 2/3-wire smart device used to sense whether the process level is above or below a particular point. The 2120 Level Switch contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 2120 Level Switch.

**Table 1 Version Overview**

2120 Level Switch, NAMUR (K) - DRY = On	NAMUR (K) model Level Switch configured as DRY = On, using the NAMUR current output interface (DIN 19234, IEC 60947-5-6) with Off state indicated by < 1 mA and On state indicated by > 2.2 mA
2120 Level Switch, 8/16mA (H) - DRY = On	8/16mA (H) model Level Switch configured as DRY = On, with Off state indicated by 8 mA and On state indicated by 16 mA
2120 Level Switch, PNP/PLC (G) - DRY = On	PNP/PLC (G) model Level Switch configured as DRY = On, with Off state indicated by <100uA and On state indicated by <2.75V difference between the + and OUT terminals
2120 Level Switch, Relay (V) - DRY = On	Relay (V) model Level Switch configured as DRY = On, with Off state indicated by contact between the NC and C terminals and On state indicated by contact between the NO and C terminals

The 2120 Level Switch is classified as a Type B<sup>1</sup> element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2<sub>H</sub>. The 2120 Level Switch, for Models K, H, and G, can be classified as a 2<sub>H</sub> device and meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 at HFT=1). However, due to the IEC 61508-2 Route 2<sub>H</sub> limitation for Diagnostic Coverage, use of Route 2<sub>H</sub> for architectural constraints may not be used for the 2120 Level Switch Model V. The analysis for Model V shows a Safe Failure Fraction between 60% and 90% and therefore meets Route 1<sub>H</sub> hardware architectural constraints for up to SIL 1 at HFT=0 (or SIL 2 at HFT=1).

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

The failure rates listed in this report are based on over 350 billion unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI), see section 4.2.2.

<sup>1</sup> 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.



A user of the 2120 Level Switch 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). A full table of failure rates is presented in section 4.4 along with all assumptions.



## Table of Contents

Management Summary .....	2
1 Purpose and Scope .....	5
2 Project Management .....	6
2.1 <i>exida</i> .....	6
2.2 Standards and literature used .....	6
2.3 <i>exida</i> tools used .....	8
2.4 Reference documents .....	8
2.4.1 Documentation provided by Rosemount Tank Radar .....	8
2.4.2 Documentation generated by <i>exida</i> .....	9
3 Product Description .....	10
4 Failure Modes, Effects, and Diagnostic Analysis .....	12
4.1 Failure categories description .....	12
4.2 Methodology – FMEDA, failure rates .....	13
4.2.1 FMEDA .....	13
4.2.2 Failure rates .....	13
4.3 Assumptions .....	14
4.3.1 User Configuration Restrictions .....	14
4.4 Results .....	15
5 Using the FMEDA Results .....	19
5.1 PFD <sub>avg</sub> calculation .....	19
5.2 <i>exida</i> Route 2 <sub>H</sub> Criteria .....	19
6 Terms and Definitions .....	21
7 Status of the Document .....	22
7.1 Liability .....	22
7.2 Releases .....	23
7.3 Future enhancements .....	23
7.4 Release signatures .....	24
Appendix A Lifetime of Critical Components .....	25
Appendix B Proof Tests to Reveal Dangerous Undetected Faults .....	26
B.1 Suggested Comprehensive Proof Test .....	26
B.2 Suggested Partial Proof Test .....	26
Appendix C <i>exida</i> Environmental Profiles .....	28
Appendix D Determining Safety Integrity Level .....	29
Appendix E Site Safety Index .....	33
E.1 Site Safety Index Profiles .....	33



## 1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 2120 Level Switch. From this, failure rates and example  $PFD_{avg}$  values may be calculated.

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

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



## 2 Project Management

### 2.1 *exida*

*exida* is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person-years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains the largest process equipment database of failure rates and failure modes with over 350 billion unit operating hours.

Roles of the parties involved

Rosemount Tank Radar

Design Center for the 2120 Level Switch

*exida*

Performed the hardware assessment

*exida* most recently modified the hardware assessment in June-2015; updates are noted in section 7.2. No significant hardware changes have been made since then.

### 2.2 Standards and literature used

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

[N1]	IEC 61508-2: 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	<i>exida</i> LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3 <sup>rd</sup> edition, ISA, ISBN 978-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, <a href="http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers">http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers</a>

[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	<a href="http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design">http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design</a>
[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, <a href="http://www.exida.com/resources/whitepapers">www.exida.com/resources/whitepapers</a> , 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, <a href="http://www.exida.com">www.exida.com</a> , 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, <a href="http://www.exida.com">www.exida.com</a> , June 2015.



## 2.3 *exida* tools used

[T1]	V7.1.17	FMEDA Tool
------	---------	------------

## 2.4 Reference documents

### 2.4.1 Documentation provided by Rosemount Tank Radar

[D1]	00813-0100-4030, Rev GB, June 2013	Product Data Sheet, Rosemount 2120 Full-featured Vibrating Fork Liquid Level Switch
[D2]	82953, ISS 2, 22 Dec 2010	Schematic, CIRC.DIAG 2120 NAMUR VERSION
[D3]	82957, ISS 04, 8 May 2012	Schematic, CIRC.DIAG. 2120 8/16mA VERSION
[D4]	71097/1006, ISS 4, 17 Oct 2007	SQUING 2 I.S. APPROVAL DRAWING (shows construction of sensor)
[D5]	SFRS145 Rev 1.5.pdf	Squing2 Upgrade, Software Functional Requirements, Rev 1.5, June 24, 2008
[D6]	2120_2130 Fault Injection results 04_08_10.xlsx	Fault Injection Test Results for 2120 and 2130 models, updated 30 July 2010
[D7]	Manual Supplement 00809-0500-4030, Rev AH, March 2018	Rosemount 2120 Functional Safety Manual
[D8]	Al-elec used in 21xx series.xls, 20 Aug 2014	List of Al-electrolytic capacitors used in 21xx series
[D9]	82954, REV 3, 23 Jan 2014	Schematic, CIRC. DIAG. 2120 PNP/PLC VERSION
[D10]	J32072A, Issue 3, 9 May 2011	Parts List, PCB ASSY 2120 PNP/PLC
[D11]	82955, IS 2, 11 Nov 2010	Schematic, CIRC. DIAG. 2120 RELAY VERSION
[D12]	J3208/2A, Issue 3, 9 May 2011	Parts List, PCB ASSY 2120 RELAY
[D13]	02120-5033, Rev AA, 14 Nov 2014	Schematic, 2120 SELF CHECKING, 2-WIRE VERSION
[D14]	02120-5032-000 PCB BOM.pdf	Parts List, 2120 SELF CHECKING, 2-WIRE VERSION
[D15]	02120-5032, Rev AA, 13 Nov 2014	Assembly Drawing, 2120 SELF CHECKING, 2-WIRE VERSION
[D16]	Diagnostics for Emerson Mobrey 21x0.docx, 26 Jan 2015	List of Diagnostics (compiled by exida with input from client)
[D17]	2130 2 wire FMEDA - Enhanced ModeR55x2.xlsx	FMEDA with comments from Rosemount
[D18]	00809-0100-4030, Rev FA, Dec 2016	Rosemount 2120 Reference Manual





## 2.4.2 Documentation generated by *exida*

[R1]	Mobrey Squing 2 - 8-16mA output - Std Temp Sensor - DRY ON (no self check) - Profile 2_15Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R2]	Mobrey Squing 2 - 8-16mA output - DRY ON (no self check) - wo sensor_14Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R3]	Mobrey Squing 2 - FI Numar IS - DRY ON (no self check) - wo sensor_15Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R4]	Mobrey Squing 2 - FI Numar IS - Std Temp Sensor (no self check) - DRY ON - Profile 2_15Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R5]	Mobrey Squing 2 FMEDA FI Summary Sheet 15Aug2014.xls	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch Summary Sheet
[R6]	Mobrey 2120 - PNP PLC - FI HS Iso DRY ON - wo sensor 20141216_1002.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 PNP/PLC Dry=ON, microcontroller and output sections
[R7]	Mobrey 2120 - PNP PLC - Dry ON - FI Std Temp Sensor 20141217.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 PNP/PLC Dry=ON, sensor and sensor circuitry
[R8]	Mobrey 2120 - Relay Common - DRY ON - wo sensor 20141212.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 Relay Dry=ON, microcontroller and output sections
[R9]	Mobrey 2120 Relay - Std Temp Sensor - DRY ON 20141212.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 Relay Dry=ON, sensor and sensor circuitry
[R10]	Mobrey 2120 - per Relay 20141212.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 Relay (component)
[R11]	Mobrey 2120-2130 FMEDA Summary Sheet_17Jun2015.xls	Failure Modes, Effects, and Diagnostic Analysis – Mobrey 2130/2120 Summary
[R12]	Mobrey 2120_2 Wire _DRY-ON_uC-output_17Jun2015.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 2-wire/Direct Load Dry=ON, microcontroller and output sections
[R13]	Mobrey Std Temp Sensor - DRY ON - Profile 3_17June2015.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 2-wire/Direct Load Dry=ON, sensor and sensor circuitry



### 3 Product Description

The 2120 Level Switch is a smart device used in many different industries for point level sensing applications. It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure.

The 2120 is designed using the tuning fork principle. The 2120 continuously monitors changes in its vibrating fork's natural resonant frequency. When used as a high-level alarm, the liquid rising in the vessel contacts the fork resulting in a reduction of its frequency; this is detected by the electronics which switches the output state to OFF. As a switch the device only supports two valid output conditions defined as the ON and OFF states. Diagnostic annunciation of detectable faults is available via local LED indication and potential transition to the OFF state depending on the type of fault and configured mode of operation.

The device's Mode Switch is used to set the mode of operation for the device. When set to "Dry On" the device is configured for High Level Trip applications and when set to "Wet On" it is configured for Low Level Trip applications.

Note: the Wet=On configuration is outside the scope of the 2120 evaluation.

The 2120 Level Switch is available in different models that support a selection of electrical interfaces. Table 2 is an overview of the models in the FMEDA of the 2120 Level Switch.

Table 2 Version Overview

2120 Level Switch, NAMUR (K) - DRY = On	NAMUR (K) model Level Switch configured as DRY = On, using the NAMUR current output interface (DIN 19234, IEC 60947-5-6) with Off state indicated by < 1 mA and On state indicated by > 2.2 mA
2120 Level Switch, 8/16mA (H) - DRY = On	8/16mA (H) model Level Switch configured as DRY = On, with Off state indicated by 8 mA and On state indicated by 16 mA
2120 Level Switch, PNP/PLC (G) - DRY = On	PNP/PLC (G) model Level Switch configured as DRY = On, with Off state indicated by <100uA and On state indicated by <2.75V difference between the + and OUT terminals
2120 Level Switch, Relay (V) - DRY = On	Relay (V) model Level Switch configured as DRY = On, with Off state indicated by contact between the NC and C terminals and On state indicated by contact between the NO and C terminals

Each electrical interface has interface specific ON and OFF states defined for the interface. The alarm state is considered to be the OFF state by default, following de-energize to trip safety principles.

Figure 1 provides an overview of the 2120 Level Switch and the boundary of the FMEDA.

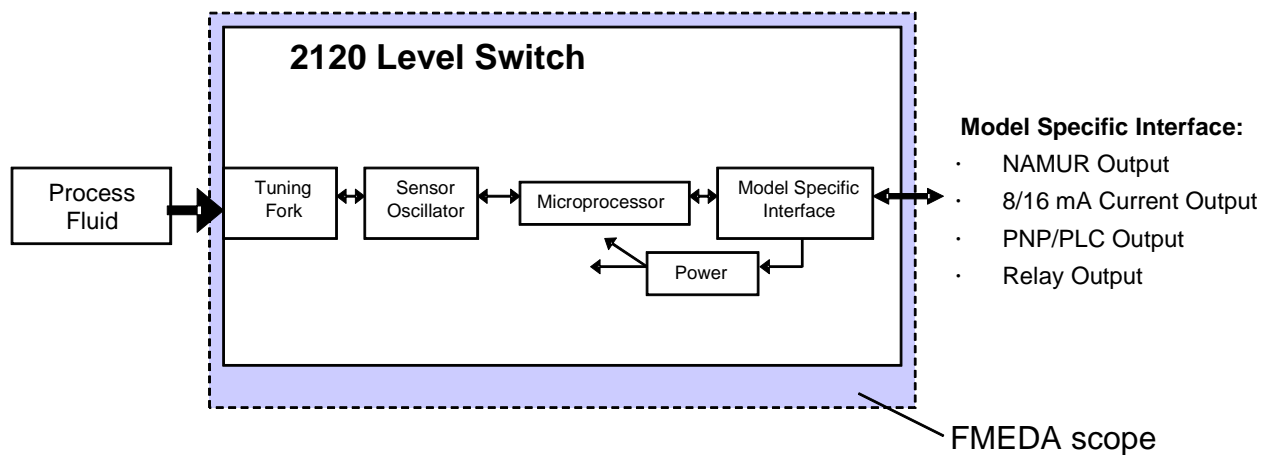


Figure 1 2120 Level Switch, Parts included in the FMEDA

The 2120 Level Switch is classified as a Type B<sup>2</sup> element according to IEC 61508, having a hardware fault tolerance of 0.

<sup>2</sup> Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

## 4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.4.1 and is documented in [R1] to [R13].

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, see Fault Injection Test Report [D6].

### 4.1 Failure categories description

In order to judge the failure behavior of the 2120 Level Switch, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the output goes to the OFF or de-energized state
Fail Safe	Failure that causes the device to go to the defined fail-safe state (OFF) without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (OFF).
Fail Dangerous	Failure that results in output state stuck in the ON state or not transitioning to the OFF state within the expected response time when the process condition at the monitored level position changes from the DRY = On condition.
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 which cause the output signal to go to the predefined alarm state (OFF). Only faults that result in transition to the OFF state are considered detected by the FMEDA.
Fail High	Failure that causes the current output signal to go above the normal High level "On" current ( $>8$ mA for NAMUR; $>17$ mA for 8/16) and may be detected by the Logic Solver. This is not applicable to Transistor or Relay outputs.
Fail Low	Failure that causes the current output signal to go below the normal Low level "Off" current ( $< 0.1$ mA for NAMUR; $<7.5$ mA for 8/16) and may be detected by the Logic Solver. This is not applicable to Transistor or Relay outputs.
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.



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

When using the NAMUR current output interface, a Fail High will appear to be a stuck at ON output state and be dangerous undetected unless detected by shorted field wire diagnostic and properly handled by the capability and programming of the logic solver. The Fail Low will appear to be a stuck at the failsafe OFF output state if not detected and handled differently by open circuit line monitoring. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

## **4.2 Methodology – FMEDA, failure rates**

### **4.2.1 FMEDA**

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

### **4.2.2 Failure rates**

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which was derived using over 350 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates for the NAMUR current output, 8/16 mA current and Relay output versions were chosen to match *exida* Profile 2. The rates for the PNP/PLC version was chosen to match *exida* Profile 3. See Appendix C. The *exida* profile chosen 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 due to random events will be less than the number predicted by these failure rates.

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

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

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



Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ 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 2120 Level Switch.

- Only a single component failure will fail the entire 2120 Level Switch.
- 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 maintenance capability are site specific and therefore cannot be included.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 for the NAMUR, 8/16mA and Relay versions or *exida* Profile 3 for the PNP/PLC, with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- 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.
- Faults only annunciated via LED indication are not considered "detected" by the FMEDA
- Worst-case internal fault detection time is less than one hour.

#### 4.3.1 User Configuration Restrictions

In addition to basic FMEDA assumptions, the following additional application configuration restrictions were also considered as part of this analysis and must be followed for the results presented in this report to be correct.

- The 2120 Level Switch will be used in the standard de-energize to trip mode of operation.
  - use DRY = On modes of operation for high level detection applications
- The 2120 Level Switch worst case response time shall be considered to be the larger of 10 seconds plus the switch setting for response mode of operation.

## 4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 2120 Level Switch FMEDA. All failure rates in this section assume a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix E for an explanation of SSI of 0 (very poor maintenance practices) through SSI of 4 (ideal maintenance practices).

All failure rates in this section assume a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix E for an explanation of SSI of 0 (very poor maintenance practices) through SSI of 4 (ideal maintenance practices).

The failure rates for the 2120 NAMUR (K) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 3.

**Table 3 Failure rates 2120 Level Switch, NAMUR (K) - DRY = On**

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	118	
Fail Dangerous Detected	131	
Fail Detected (detected by internal diagnostics)	107	
Fail High (detected by logic solver)	9	
Fail Low (detected by logic solver)	15	
Fail Dangerous Undetected	24	
No Effect	54	
Annunciation Undetected	4	

The failure rates for the 8/16 mA (H) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 4.

**Table 4 Failure rates 2120 Level Switch, 8/16 mA (H) - DRY = On**

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	136	
Fail Dangerous Detected	152	
Fail Detected (detected by internal diagnostics)	122	
Fail High (detected by logic solver)	9	
Fail Low (detected by logic solver)	21	
Fail Dangerous Undetected	29	
No Effect	107	
Annunciation Undetected	70	



The failure rates for the PNP/PLC (G) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 5.

**Table 5 Failure rates 2120 Level Switch, PNP/PLC (G) - DRY = On**

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	241	
Fail Dangerous Detected	130	
Fail Detected (detected by internal diagnostics)	130	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected	41	
No Effect	197	
Annunciation Undetected	3	

The failure rates for the Relay (V) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 6.

**Table 6 Failure rates 2120 Level Switch, Relay (V) - DRY = On**

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	131	
Fail Dangerous Detected	130	
Fail Detected (detected by internal diagnostics)	130	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected	102	
No Effect	101	
Annunciation Undetected	8	





Table 7 lists the failure rates for the 2120 Level Switch according to IEC 61508. All failure rates in this table assume a Site Safety Index (SSI) of 2 (good site maintenance practices).

**Table 7 Failure rates according to IEC 61508 in FIT**

Device	$\lambda_{SD}$	$\lambda_{SU}^3$	$\lambda_{DD}$	$\lambda_{DU}$	#	SFF <sup>4</sup>
2120 Level Switch, NAMUR (K) - DRY = On	0	118	131	24	58	91.1%
2120 Level Switch, 8/16mA (H) - Dry=On	0	136	152	29	177	90.9%
2120 Level Switch, PNP/PLC (G) - Dry=On	0	241	130	41	200	90.0%
2120 Level Switch, Relay (V) - Dry=On	0	131	130	102	109	72.0%

Where:

$\lambda_{SD}$  = Fail Safe Detected

$\lambda_{SU}$  = Fail Safe Undetected

$\lambda_{DD}$  = Fail Dangerous Detected

$\lambda_{DU}$  = Fail Dangerous Undetected

# = No Effect Failures

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

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1<sub>H</sub> approach according to 7.4.4.2 of IEC 61508-2 or the 2<sub>H</sub> approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2<sub>H</sub> (see Section 5.2).

The 1<sub>H</sub> approach involves calculating the Safe Failure Fraction for the entire element.

The 2<sub>H</sub> 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 meets the *exida* criteria for Route 2<sub>H</sub> which is more stringent than IEC 61508-2. However, due to the IEC 61508-2 Route 2<sub>H</sub> limitation for Diagnostic Coverage, use of Route 2<sub>H</sub> for architectural constraints may not be used for the Model V and the architectural constraints will need to be evaluated per Route 1<sub>H</sub>. Therefore, the 2120 Level Switch can be classified as a 2<sub>H</sub> device for Models K, H, and G. When 2<sub>H</sub> data is used for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 at HFT=1) per Route 2<sub>H</sub>.

The analysis for Model V shows a Safe Failure Fraction between 60% and 90% and therefore meets Route 1<sub>H</sub> hardware architectural constraints for up to SIL 1 at HFT=0 (or SIL 2 at HFT=1).

<sup>3</sup> It is important to realize that the No Effect failures are not included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

<sup>4</sup> Safe Failure Fraction needs to be calculated on (sub)system level



The analysis for Models K, H, and G shows a Safe Failure Fraction between 90% and 99% and therefore meets Route 1<sub>H</sub> hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 at HFT=1).

## 5 Using the FMEDA Results

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

### 5.1 $PFD_{avg}$ calculation

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 coverages for the suggested proof tests are listed in Table 11.

### 5.2 *exida* Route 2<sub>H</sub> Criteria

IEC 61508, ed2, 2010 describes the Route 2<sub>H</sub> alternative to Route 1<sub>H</sub> 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<sub>H</sub>, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" vs. "systematic" [N9] are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

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

## 6 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
<i>exida</i> criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2 <sub>H</sub> Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
PFD <sub>avg</sub>	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type 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: V3, R2: updated after RTR review; JCY, 7-Jan-2021

V3, R1: updated for surveillance audit, cited updated manuals, clarified model assessments, using new report number; JCY, 21-Dec-2020. Q20-09-098.

V2, R2: corrected FIT tables and footnotes for IEC 61508:2010 using [R11]; change ownership to RTR; JCY, 24-Jun-2020. Q20-04-151.

V2, R1: changed to R004 and IEC 61508:2010 certification, 2017-12-22

V1, R7: added 2-wire/Direct Load Switching version, Q15/03-079; 25 June 2015 Griff Francis

V1, R6: added PNP/PLC and Relay versions, Q14/11-048; changed per some requests in 25 Nov 2014 e-mail, changed per some requests in 20 Jan 2015 e-mail; 21 Jan 2015, Griff Francis

V1, R5: changed per customer requests in 11 Sept 2014 e-mail; 16 Oct 2014, Griff Francis

V1, R4: removed observe LED steps from Proof Tests, added higher life time for capacitors used on 8/16mA model.; 21 August 2014, Griff Francis

V1, R3: added second Proof Test, corrected Appendix A to show use of aluminum electrolytic capacitors: 15 August 2014, Griff Francis, Q14/08-015

V1, R2: made changes 1 and 4 requested in an e-mail sent 19 June 2014: 24 June 2014, Griff Francis

V1, R1: updated to IEC 61508:2010; converted to new report template; added 8/16mA model: 6 Jan 2014, Griff Francis, Q13/11-015

V1, R0: Created separate report for 2120 per client request, September 28, 2010

Author(s): Rudolf Chalupa

Release Status: Released to Rosemount Tank Radar

## 7.3 Future enhancements

At request of client.



#### 7.4 Release signatures

A handwritten signature in black ink, appearing to read "William M. Goble", written over a horizontal line.

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink, appearing to read "John C. Grebe Jr.", written over a horizontal line.

John C. Grebe Jr., Principal Engineer

A handwritten signature in black ink, appearing to read "Rudolf P. Chalupa", written over a horizontal line.

Rudolf P. Chalupa, CFSE, Senior Safety Engineer





## Appendix A Lifetime of Critical Components

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime<sup>5</sup> of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the  $PFD_{avg}$  calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 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) – Aluminum electrolytic, non-solid electrolyte	Approx. 10 years
Capacitor (electrolytic) – Aluminum electrolytic, non-solid electrolyte; high temperature versions used on 8/16mA (H) model, see [D8]	Approx. 20 years

It is the responsibility of the end user to maintain and operate the 2120 Level Switch per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

For high demand mode applications, the useful lifetime of the relay is limited by the number of cycles. The useful lifetime of the relay is > 100,000 full scale cycles or 8 to 10 years, whichever results in the shortest lifetime.

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

---

<sup>5</sup> 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 proof test described in Table 9 will detect at least 74% of possible DU failures in the 2120 Level Switch in the DRY = On mode. See Table 11 for a specific model and coverage combination.

**Table 9 Suggested Comprehensive Proof Test**

Step	Action
1.	Inspect the accessible parts of the level switch for any leaks or damage.
2.	Bypass the safety function and take appropriate action to avoid a false trip.
3.	Verify the rotary switch is set to the proper selected mode of operation.
4.	Change process conditions so tuning fork experiences the configured alarm condition and verify the output switches to the OFF state within the expected time period as indicated by the setting of the Mode Switch.
5.	Change process conditions so tuning fork experiences the configured normal condition and verify the output switches to the ON state within the expected time period as indicated by the setting of the Mode Switch.
6.	Remove the bypass and otherwise restore normal operation.

### B.2 Suggested Partial Proof Test

The suggested proof test described in Table 10 will detect at least 68% of possible DU failures in the 2120 Level Switch in the DRY = On mode. See Table 11 for a specific model and coverage combination.

**Table 10 Suggested Partial Proof Test**

Step	Action
1.	Inspect the accessible parts of the level switch for any leaks or damage.
2.	Bypass the safety function and take appropriate action to avoid a false trip.
3.	Verify the rotary switch is set to the proper selected mode of operation.
4.	Apply a bar magnet to the Magnetic Test Point to force the switch to the fail-safe state and confirm that the Safe State was achieved within 2s.
5.	Remove the bar magnet from the Magnetic Test Point and confirm that after 1s the normal operating state of the switch was achieved
6.	Remove the bypass and otherwise restore normal operation.



**Table 11 Combinations of Models and DU Coverages.**

	Comprehensive Proof Test Coverage	Partial Proof Test Coverage
2120 Level Switch, NAMUR (K) - DRY = On	88%	76%
2120 Level Switch, 8/16mA (H) - DRY = On	89%	81%
2120 Level Switch, PNP/PLC (G) - DRY = On	74%	68%
2120 Level Switch, Relay (V) - DRY = On	75%	69%



## Appendix C *exida* Environmental Profiles

Table 12 *exida* Environmental Profiles

<i>exida</i> Profile	1	2	3	4	5	6
<b>Description (Electrical)</b>	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
<b>Description (Mechanical)</b>	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
<b>IEC 60654-1 Profile</b>	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
<b>Average Ambient Temperature</b>	30 C	25 C	25 C	5 C	25 C	25 C
<b>Average Internal Temperature</b>	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
<b>Daily Temperature Excursion (pk-pk)</b>	5 C	25 C	25 C	0 C	25 C	N/A
<b>Seasonal Temperature Excursion (winter average vs. summer average)</b>	5 C	40 C	40 C	2 C	40 C	N/A
<b>Exposed to Elements / Weather Conditions</b>	No	Yes	Yes	Yes	Yes	Yes
<b>Humidity<sup>6</sup></b>	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
<b>Shock<sup>7</sup></b>	10 g	15 g	15 g	15 g	15 g	N/A
<b>Vibration<sup>8</sup></b>	2 g	3 g	3 g	3 g	3 g	N/A
<b>Chemical Corrosion<sup>9</sup></b>	G2	G3	G3	G3	G3	Compatible Material
<b>Surge<sup>10</sup></b>						N/A
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
<b>EMI Susceptibility<sup>11</sup></b>						N/A
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	
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	
<b>ESD (Air)<sup>12</sup></b>	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

<sup>6</sup> Humidity rating per IEC 60068-2-3

<sup>7</sup> Shock rating per IEC 60068-2-6

<sup>8</sup> Vibration rating per IEC 60770-1

<sup>9</sup> Chemical Corrosion rating per ISA 71.04

<sup>10</sup> Surge rating per IEC 61000-4-5

<sup>11</sup> EMI Susceptibility rating per IEC 6100-4-3

<sup>12</sup> 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) [N5] 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 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.

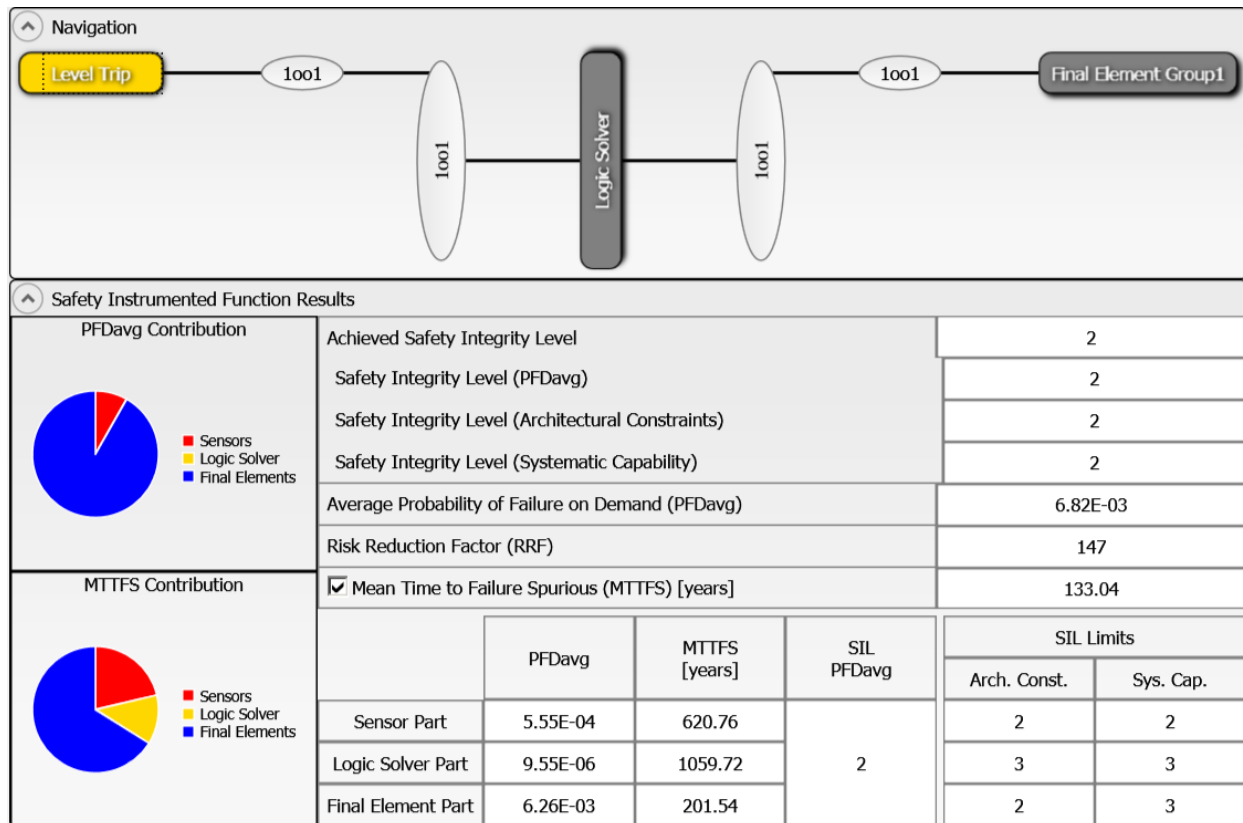
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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:

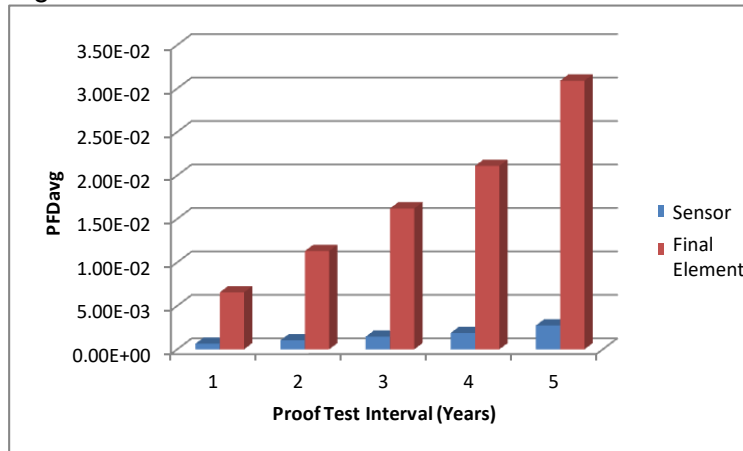
- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

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.



**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.

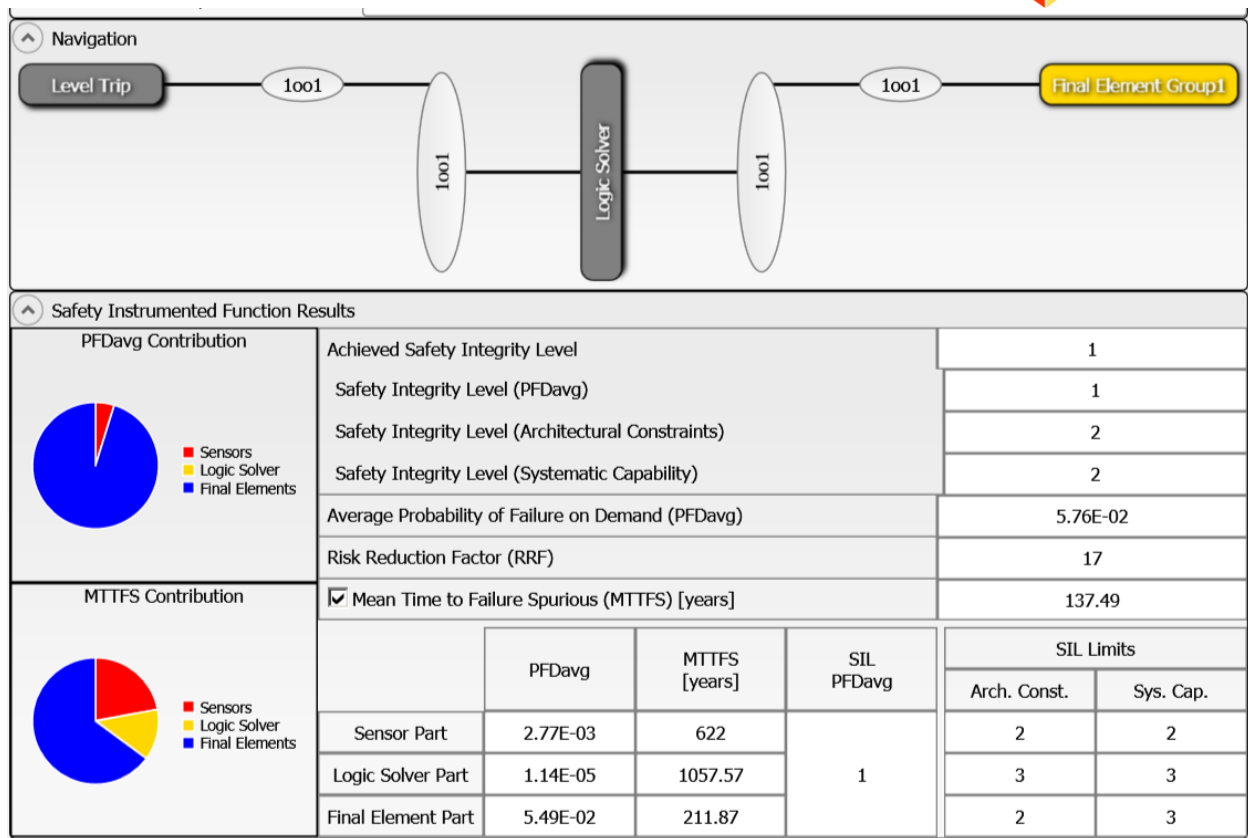


**Figure 3 PFD<sub>avg</sub> versus Proof Test Interval.**

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<sub>avg</sub> for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor 17. The subsystem PFD<sub>avg</sub> contributions are Sensor PFD<sub>avg</sub> = 2.77E-03, Logic Solver PFD<sub>avg</sub> = 1.14E-05, and Final Element PFD<sub>avg</sub> = 5.49E-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 E Site Safety Index

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

### E.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 13 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 13 exida Site Safety Index Profiles**

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