Failure Modes, Effects and Diagnostic Analysis

Project:
2130 Level Switch

Company:
Rosemount Tank Radar
Sweden

Contract Number: Q23/10-056
Report No.: ROS 20-09-098 R004
Version V4, Revision R2, March 7, 2024
Valerie Motto

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 2130 Level Switch, as described in 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 2130 Level Switch. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 2130 Level Switch is a 2/3-wire smart device used to sense whether the process level is above or below a particular point. The 2130 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 2130 Level Switch.

Table 1 Version Overview

2130 Level Switch, NAMUR (N) - DRY = On	NAMUR (N) model Level Switch with the High Temperature Sensor 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
2130 Level Switch, NAMUR (N) - WET = On	NAMUR (N) model Level Switch with the High Temperature Sensor configured as WET = 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
2130 Level Switch, Relay (D) - DRY = On	Relay (D) model Level Switch with the High Temperature Sensor configured as DRY = On, using ac or dc input power (24 to 264V ac 50/60Hz, 24 to 60V dc) and relay outputs with Off state indicated by SPDT relay output, including Fault Relay option
2130 Level Switch, Relay (D) - WET = On	Relay (D) model Level Switch with the High Temperature Sensor configured as WET = On, using ac or dc input power (24 to 264V ac 50/60Hz, 24 to 60V dc) and relay outputs with Off state indicated by SPDT relay output, including Fault Relay option
2130 Level Switch, 8/16mA (M) - DRY = On	8/16mA (M) model Level Switch with the High Temperature Sensor configured as DRY = On, with Off state indicated by 8 mA and On state indicated by 16 mA
2130 Level Switch, 8/16mA (M) - WET = On	8/16mA (M) model Level Switch with the High Temperature Sensor configured as WET = On, with Off state indicated by 8 mA and On state indicated by 16 mA
2130 Point Level Switch, PNP/PLC (P) - DRY = On	This provides the FMEDA results for the PNP/PLC (P) model Point Level Switch with the High Temperature Sensor configured as DRY = On, using the PNP/PLC 3 wire interface (24 to 60V dc) with Off state indicated by IL<100 µA and On state supporting loads with IL<500 mA
2130 Point Level Switch, PNP/PLC (P) - WET = On	This provides the FMEDA results for the PNP/PLC (P) model Point Level Switch with the High Temperature Sensor configured as WET = On, using the PNP/PLC 3 wire interface (24 to 60V dc) with Off state indicated by IL<100 µA and On state supporting loads with IL<500 mA

2130 Point Level Switch, Direct Load Switching (L) - DRY = On	This provides the FMEDA results for the Direct Load Switching (L) model Point Level Switch with the High Temperature Sensor configured as DRY = On, using the direct load switching 2 wire interface (24 to 264V ac 50/60Hz, 24 to 60V dc) with Off state indicated by IL<3 mA and On state supporting loads with 20 mA< IL<500 mA
2130 Point Level Switch, Direct Load Switching (L) - WET = On	This provides the FMEDA results for the Direct Load Switching (L) model Point Level Switch with the High Temperature Sensor configured as WET = On, using the direct load switching 2 wire interface (24 to 264V ac 50/60Hz, 24 to 60V dc) with Off state indicated by IL<3 mA and On state supporting loads with 20 mA< IL<500 mA

The 2130 Level Switch is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H (see Section 5.2) (and the diagnostic coverage resulting from the analysis exceeds the required 60% threshold). All Models of the 2130 Level Switch can be classified as a 2_H device and meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 at HFT=1). The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements and supported via a calculation of PFH/PFD_{avg}.

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

The failure rates listed in this report are based on over 400 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) [N10], [N11].

A user of the 2130 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).

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

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 2130 Level Switch. From this, failure rates and for each failure mode/category, useful life, and proof test coverage are determined.

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

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, 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 Center for the 2130 Level Switch
exida	Performed the hardware assessment

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

2.3 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	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers

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

2.4 *exida* tools used

[T1]	V2.0.1	FMEDAx Tool

2.5 Reference documents

2.5.1 Documentation provided by Rosemount Tank Radar

[D1]	00809-0100-4130, Rev DC, Jan 2019	Reference Manual- Rosemount 2130 Enhanced Vibrating Fork Liquid Level Switch
[D2]	00813-0100-4130, Rev EE, March 2017	Product Data Sheet- Rosemount 2130 Enhanced Vibrating Fork Liquid Level Switch
[D3]	00825-0100-4130, Rev CE, May 2019	Quick Start Guide- Rosemount 2130 Enhanced Vibrating Fork Liquid Level Switch
[D4]	00809-0500-4130, Rev AL, December 2023	Manual Supplement- Rosemount 2130 Functional Safety Manual
[D5]	02130-5203-ISS-AA	Schematic, CIRC.DIAG 2130 SELF-CHECKING NAMUR VERSION
[D6]	82642, ISS 9, 11 Nov 2010	Schematic, CIRC.DIAG. 2130, RELAY VERSION, SELF-CHECKING
[D7]	02130-5123-ISS-AA	Schematic, CIRC.DIAG. 2130 RELAY ROHS
[D8]	Change History for Schematics.doc, 29 Sep 2013	Change History for Schematics, received in e-mail 26 Sep 2013
[D9]	71097/1006, REV AK	SQUING 2 I.S. APPROVAL DRAWING (shows construction of sensor
[D10]	71097/1242, REV AF	APPROVAL DRG. SQUING 2 I.S. HIGH TEMP (shows construction of high temperature sensor)
[D11]	2130_Fault_Relay_SRD RevAB.docx, 30 Jul 2013	System Requirements Document 2130E/M Fault Relay
[D12]	SFRS145 Rev 1.8.docx, Rev 1.8, 24 Sep 2013	Squing2 Upgrade, Software Functional Requirements Specification
[D13]	2120_2130 Fault Injection results 04_08_10.xlsx	Fault Injection Test Results for 2120 and 2130 models, updated 30 July 2010
[D14]	02130-5213-ISS-AB	Schematic, CIRC.DIAG. 2130 PNP/PLC ROHS
[D15]	K9785/2A, Issue 11, 09/05/11	Parts List for PCB ASSY 2130 PNP/PLC
[D16]	02130-5233-ISS-AA	CIRC.DIAG. 2130 2-WIRE ROHS
[D17]	02130-5243-ISS-AB	CIRC.DIAG. 2130 8/16MA ROHS

2.5.2 Documentation generated by *exida*

[R1]	Mobrey 2130 – NUMAR – DRY ON – wo sensor 20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, NAMUR microcontroller and output, Dry=ON
[R2]	Mobrey 2130 – NUMAR – WET ON – wo sensor 20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, NAMUR microcontroller and output, Wet=ON
[R3]	Mobrey 2130 – NUMAR – DRY ON – High Temp Sensor 20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, NAMUR sensor and sensor interface, Dry=ON
[R4]	Mobrey 2130 – NUMAR – WET ON – High Temp Sensor 20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, NAMUR sensor and sensor interface, Wet=ON
[R5]	Mobrey Squing 2 non IS – FI HIGH Temp Sensor – DRY ON – Profile 3 2017-12-21.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 2-Wire sensor and sensor interface, Dry=ON
[R6]	Mobrey Squing 2 non IS – FI High Temp Sensor – WET ON – Profile 3 2017-12-22.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 2-Wire sensor and sensor interface, Wet=ON
[R7]	Mobrey Squing 2 – 2 Wire – DRY ON – FI HS Iso wo sensor 2017-12-22.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 2-Wire microcontroller and output, Dry=ON
[R8]	Mobrey Squing 2 – 2 Wire – WET ON -FI HS Iso wo sensor 2017-12-22.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 2-Wire microcontroller and output, Wet=ON
[R9]	Mobrey 2130 – Relay Common – DRY ON – wo sensor_20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, Relay microcontroller, Dry=ON
[R10]	Mobrey 2130 – Relay Common – WET ON – wo sensor_20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, Relay microcontroller, Wet=ON
[R11]	Mobrey 2130 non IS – High Temp Sensor – DRY ON – Profile 2_20150201.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, Relay sensor and sensor interface, Dry=ON
[R12]	Mobrey 2130 non IS – High Temp Sensor – WET ON – Profile 2_20150201.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, Relay sensor and sensor interface, Wet=ON
[R13]	Mobrey 2120 – per Relay 20141212.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, Relay, Wet or Dry =ON
[R14]	Mobrey 2120 -Fault Relay option_20141212.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, Fault Relay, Wet or Dry =ON

[R15]	Mobrey 2130 – 8-16mA – DRY ON – High Temp Sensor_20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 8/16mA microcontroller and output, Dry=ON
[R16]	Mobrey 2130 - 8-16mA - DRY ON - wo sensor_20240221.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 8/16mA microcontroller and output, Dry=ON
[R17]	Mobrey 2130 – 8-16mA – WET ON – High Temp Sensor 20150129.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 8/16mA sensor and sensor interface, Wet=ON
[R18]	Mobrey 2130 – 8-16mA – WET ON – wo sensor_20150201.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, 8/16mA microcontroller and output, Wet=ON
[R19]	Mobrey Squing 2 non IS – FI HIGH Temp Sensor – DRY ON – Profile 3 2017-12-21.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, PNP/PLC, sensor and sensor interface, Dry=ON
[R20]	Mobrey Squing 2 – PNP PNC – FI HS Iso DRY ON – wo sensor_corrected 2021-03-30.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, PNP/PLC, microcontroller and output, Dry=ON
[R21]	Mobrey Squing 2 – PNP PNC – FI HS Iso WET ON – wo sensor 2017-12-22.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, PNP/PLC, microcontroller and output, Wet=ON
[R22]	Mobrey Squing 2 non IS – FI High Temp Sensor – WET ON – Profile 3 2017-12-22.nefm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch, PNP/PLC, sensor and sensor interface, Wet=ON
[R23]	2130 FMEDA Summary – Exida_21-Feb-2024_Rev4.xlsx	Failure Modes, Effects, and Diagnostic Analysis – 2130 Level Switch Summary Sheet

3 Product Description

The 2130 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 2130 is designed using the tuning fork principle. The 2130 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. When used as a low-level alarm, the liquid in the tank or pipe drains down past the fork, causing a change of natural frequency that is detected by the electronics and switches the output state.

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.

The 2130 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 2130 Level Switch.

Table 2 Version Overview

2130 Level Switch, NAMUR (N) - DRY = On	NAMUR (N) model Level Switch with the High Temperature Sensor 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
2130 Level Switch, NAMUR (N) - WET = On	NAMUR (N) model Level Switch with the High Temperature Sensor configured as WET = 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
2130 Level Switch, Relay (D) - DRY = On	Relay (D) model Level Switch with the High Temperature Sensor configured as DRY = On, using ac or dc input power (24 to 264V ac 50/60Hz, 24 to 60V dc) and relay outputs with Off state indicated by SPDT relay output, including Fault Relay option
2130 Level Switch, Relay (D) - WET = On	Relay (D) model Level Switch with the High Temperature Sensor configured as WET = On, using ac or dc input power (24 to 264V ac 50/60Hz, 24 to 60V dc) and relay outputs with Off state indicated by SPDT relay output, including Fault Relay option
2130 Level Switch, 8/16mA (M) - DRY = On	8/16mA (M) model Level Switch with the High Temperature Sensor configured as DRY = On, with Off state indicated by 8 mA and On state indicated by 16 mA
2130 Level Switch, 8/16mA (M) - WET = On	8/16mA (M) model Level Switch with the High Temperature Sensor configured as WET = On, with Off state indicated by 8 mA and On state indicated by 16 mA

2130 Point Level Switch, PNP/PLC (P) - DRY = On	This provides the FMEDA results for the PNP/PLC (P) model Point Level Switch with the High Temperature Sensor configured as DRY = On, using the PNP/PLC 3 wire interface (24 to 60V dc) with Off state indicated by IL<100 µA and On state supporting loads with IL<500 mA
2130 Point Level Switch, PNP/PLC (P) - WET = On	This provides the FMEDA results for the PNP/PLC (P) model Point Level Switch with the High Temperature Sensor configured as WET = On, using the PNP/PLC 3 wire interface (24 to 60V dc) with Off state indicated by IL<100 µA and On state supporting loads with IL<500 mA
2130 Point Level Switch, Direct Load Switching (L) - DRY = On	This provides the FMEDA results for the Direct Load Switching (L) model Point Level Switch with the High Temperature Sensor configured as DRY = On, using the direct load switching 2 wire interface (24 to 264V ac 50/60Hz, 24 to 60V dc) with Off state indicated by IL<3 mA and On state supporting loads with 20 mA< IL<500 mA
2130 Point Level Switch, Direct Load Switching (L) - WET = On	This provides the FMEDA results for the Direct Load Switching (L) model Point Level Switch with the High Temperature Sensor configured as WET = On, using the direct load switching 2 wire interface (24 to 264V ac 50/60Hz, 24 to 60V dc) with Off state indicated by IL<3 mA and On state supporting loads with 20 mA< IL<500 mA

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 2130 Level Switch and the boundary of the FMEDA.

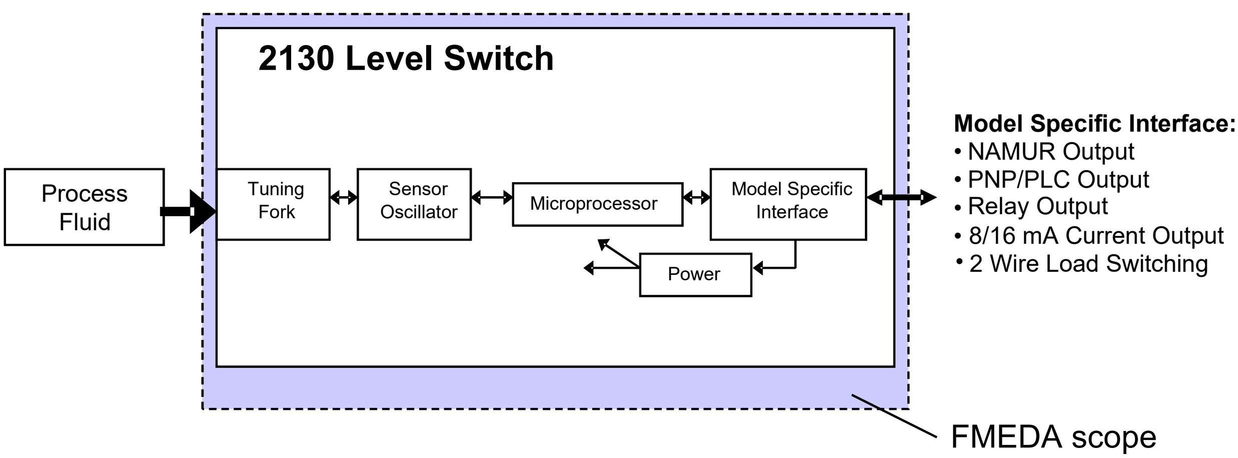


Figure 1 2130 Level Switch, Parts included in the FMEDA

The 2130 Level Switch is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.5.1 and is documented in section 2.5.2.

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level, see Fault Injection Test Report [D13].

4.1 Failure categories description

In order to judge the failure behavior of the 2130 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 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 selected WET/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 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation needed when Route 2_H failure data is not available.

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.

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 standard FMEA techniques and parts stress analysis with extensions 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 [N13], [N14].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Component Reliability Database [N2], [N3] which was derived using:

- Over 400 billion unit operational hours of process industry field failure data from multiple sources.
- Failure data formulas derived from IEC TR 62380, SN 29500 and industry sources.
- Manufacturer Meetings.
- Component Research.

The rates for the NAMUR current output interface, 8/16 mA current output and relay output versions were chosen to match *exida* Profile 2. See Appendix A. 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 A. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant. *exida* has detailed models available to make customized failure rate predictions. Contact *exida* for assistance.

Accurate plant specific data may be used 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 2130 Level Switch.

- Only a single component failure will fail the entire 2130 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 operational errors or maintenance capability 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, or Profile 3 for the PNP/PLC and Direct Load versions. Other environmental characteristics are assumed to be within manufacturer's rating.
- Additional fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The 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 less than 1 hour.
- Relay contacts in the 2130 D version are transient and have over-current protection.
- The enhanced self-check configuration option is enabled.

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 2130 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
  - use WET = On modes of operation for low level detection applications
- The 2130 models of 2130 Level Switch will be configured to run in the Enhanced self-check mode of operation when used in WET = On (low level detection) applications.
- The 2130 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 Failure Rate Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 2130 Level Switch FMEDA. All failure rates in this section assume a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix C 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 C for an explanation of SSI of 0 (very poor maintenance practices) through SSI of 4 (ideal maintenance practices).

The failure rates for the 2130 NAMUR (N) model Level Switch with the High Temperature Sensor configured as DRY = On are listed in Table 3.

Table 3 Failure rates 2130 Level Switch, NAMUR (N) - DRY = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		134
Fail Dangerous Detected		150
Fail Detected (detected by internal diagnostics)	126	
Fail High (detected by logic solver)	9	
Fail Low (detected by logic solver)	15	
Fail Dangerous Undetected		18
No Effect		58
Annunciation Undetected		3.5

The failure rates for the 2130 NAMUR (N) model Level Switch with the High Temperature Sensor configured as WET = On are listed in Table 4.

Table 4 Failure rates 2130 Level Switch, NAMUR (N) - WET = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		16
Fail Dangerous Detected		257
Fail Detected (detected by internal diagnostics)	233	
Fail High (detected by logic solver)	9	
Fail Low (detected by logic solver)	15	
Fail Dangerous Undetected		29
No Effect		58
Annunciation Undetected		3.5

The failure rates for the 2130 Relay (D) model Level Switch using one changeover contact without the FAULT Relay, with the High Temperature Sensor configured as DRY = On are listed in Table 5.

Table 5 Failure rates 2130 Level Switch, Relay (D) - DRY = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		146
Fail Dangerous Detected		148
Fail Detected (detected by internal diagnostics)	148	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		94
No Effect		104
Annunciation Undetected		8

The failure rates for the 2130 Relay (D) model Level Switch using one changeover contact without the Fault Relay, with the High Temperature Sensor configured as WET = On are listed in Table 6.

Table 6 Failure rates 2130 Level Switch, Relay (D) - WET = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		31
Fail Dangerous Detected		253
Fail Detected (detected by internal diagnostics)	253	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		104
No Effect		104
Annunciation Undetected		8

The failure rates for the 2130 Relay (D) model Level Switch with the FAULT Relay, with the High Temperature Sensor configured as DRY = On are listed in Table 7.

Table 7 Failure rates 2130 Level Switch, Relay (D) with Fault Relay - DRY = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		147
Fail Dangerous Detected		148
Fail Detected (detected by internal diagnostics)	148	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		95
No Effect		109
Annunciation Undetected		52

The failure rates for the 2130 Relay (D) model Level Switch with the Fault Relay, with the High Temperature Sensor configured as WET = On are listed in Table 8.

Table 8 Failure rates 2130 Level Switch, Relay (D) with Fault Relay - WET = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		32
Fail Dangerous Detected		253
Fail Detected (detected by internal diagnostics)	253	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		105
No Effect		109
Annunciation Undetected		52

The failure rates for the 8/16 mA (M) model Level Switch with the High Temperature Sensor configured as DRY = On are listed in Table 9.

Table 9 Failure rates 2130 Level Switch, 8/16 mA (M) - DRY = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		155
Fail Dangerous Detected		171
Fail Detected (detected by internal diagnostics)	141	
Fail High (detected by logic solver)	9	
Fail Low (detected by logic solver)	21	
Fail Dangerous Undetected		25
No Effect		118
Annunciation Undetected		83

The failure rates for the 2130 8/16 mA (M) model Level Switch with the High Temperature Sensor configured as WET = On are listed in Table 10.

Table 10 Failure rates 2130 Level Switch, 8/16 mA (M) - WET = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		41
Fail Dangerous Detected		276
Fail Detected (detected by internal diagnostics)	246	
Fail High (detected by logic solver)	9	
Fail Low (detected by logic solver)	21	
Fail Dangerous Undetected		35
No Effect		118
Annunciation Undetected		83

The failure rates for the 2130 PNP/PLC (P) model Point Level Switch with the High Temperature Sensor configured as DRY = On are listed in Table 11.

Table 11 Failure rates 2130 Point Level Switch, PNP/PLC (P) - DRY = On

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		162
Fail Dangerous Detected		165
Fail Detected (detected by internal diagnostics)	165	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		42
No Effect		231
Annunciation Undetected		8

The failure rates for the 2130 PNP/PLC (P) model Point Level Switch with the High Temperature Sensor configured as WET = On are listed in Table 12.

Table 12 Failure rates 2130 Point Level Switch, PNP/PLC (P) - WET = On

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		60
Fail Dangerous Detected		284
Fail Detected (detected by internal diagnostics)	284	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		54
No Effect		239
Annunciation Undetected		8

The failure rates for the 2130 Direct Load Switching (L) model Point Level Switch with the High Temperature Sensor configured as DRY = On are listed in Table 13.

Table 13 Failure rates 2130 Point Level Switch, Direct Load Switching (L) - DRY = On

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		178
Fail Dangerous Detected		155
Fail Detected (detected by internal diagnostics)	155	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		44
No Effect		162
Annunciation Undetected		3

The failure rates for the 2130 Direct Load Switching (L) model Point Level Switch with the High Temperature Sensor configured as WET = On are listed in Table 14.

Table 14 Failure rates 2130 Point Level Switch, Direct Load Switching (L) - WET = On

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		76
Fail Dangerous Detected		278
Fail Detected (detected by internal diagnostics)	278	
Fail High (detected by logic solver)	-	
Fail Low (detected by logic solver)	-	
Fail Dangerous Undetected		55
No Effect		167
Annunciation Undetected		3

Table 15 lists the failure rates for the 2130 Level Switch according to IEC 61508. All failure rates in this section assume a Site Safety Index (SSI) of 2 (good site maintenance practices).

Table 15 Failure rates according to IEC 61508, values in FITs

Device	λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}
2130 Level Switch, NAMUR (N) - DRY = On	0	134	150	18
2130 Level Switch, NAMUR (N) - WET = On	0	16	257	29
2130 Level Switch, Relay (D) with Fault Relay - DRY = On	0	147	148	95
2130 Level Switch, Relay (D) with Fault Relay - WET = On	0	32	253	105
2130 Level Switch, Relay (D) -DRY = On	0	146	148	94
2130 Level Switch, Relay (D) - WET = On	0	31	253	104
2130 Level Switch, 8/16mA (M) - Dry=On	0	155	171	25
2130 Level Switch, 8/16mA (M) - Wet=On	0	41	276	35
2130 Point Level Switch, PNP/PLC (P) - DRY = On	0	162	165	42
2130 Point Level Switch, PNP/PLC (P) - WET = On	0	60	284	54
2130 Point Level Switch, Direct Load Switching (L) - DRY = On	0	178	155	44
2130 Point Level Switch, Direct Load Switching (L) - WET = On	0	76	278	55

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

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

4.5 Proof Test Coverage

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

4.5.1 Suggested Full Proof Test

The suggested proof test described in Table 16 will detect at least 78% of possible DU failures in the 2130 Level Switch versions listed. See Table 18 for a specific model and coverage combination.

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

Table 16 Suggested Full 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 (WET or DRY) 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 (WET or DRY) 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.

4.5.2 Suggested Partial Proof Test

The suggested proof test described in Table 17 will detect at least 77% of possible DU failures in the 2130 Level Switch versions listed. See Table 18 for a specific model and coverage combination.

Table 17 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 18 Combinations of Models and DU Coverages.

Version	Full Proof Test Coverage	Partial Proof Test Coverage
2130 Level Switch, NAMUR (N) - DRY = On	93%	89%
2130 Level Switch, NAMUR (N) - WET = On	95%	92%
2130 Level Switch, Relay (D) - DRY = On	96%	96%
2130 Level Switch, Relay (D) - WET = On	97%	97%
2130 Level Switch, Relay (D) with Fault Relay- DRY = On	97%	96%

2131 Level Switch, Relay (D) with Fault Relay- WET = On	98%	97%
2130 Level Switch, 8/16mA (M) - Dry=On	93%	90%
2130 Level Switch, 8/16mA (M) - Wet=On	95%	93%
2130 Level Switch, PNP/PLC (P) - DRY = On	89%	85%
2130 Level Switch, PNP/PLC (P) - WET = On	86%	81%
2130 Level Switch, Direct Load Switching (L) - DRY = On	78%	77%
2130 Level Switch, Direct Load Switching (L) - WET = On	81%	77%

4.6 Useful Life

The Useful Life of the device predicted by component failure data of 10 years.

4.7 Architecture Constraints

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

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 61508-2.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H (which is more stringent than IEC 61508-2) (and the diagnostic coverage resulting from the analysis exceeds the required 60% threshold). Therefore, the 2130 Level Switch 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.

The architectural constraint type for the 2130 Level Switch is B. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

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 B for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverages for the suggested proof tests are listed in Table 16 and Table 17.

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

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

1. field unit operational hours of 10,000,000 per each component or known common usage of the component for over ten years in at least 10 units; and
2. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
3. failure definitions are realistic without data censoring of failures with both a systematic and random failure cause [N9]; and
4. every component used in an FMEDA meets the above criteria.

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

6 Terms and Definitions

Automatic Diagnostics	Tests automatically performed online internally by the device or, if specified, externally by another device without manual intervention or manual interpretation of the results.
DC	Diagnostic Coverage
exida 2H criteria	A method to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route with more detail and more requirements than specified in IEC 61508-2.
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
PFD_{avg}	Average Probability of Failure on Demand
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 engineering literature and International technical reports. Failure rates are obtained from field failure studies and other sources. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, product design changes, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical model number product at some future time.

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

7.2 Version History

Contract Number	Report Number	Revision Notes
Q23/10-056	ROS 20-09-098 R004 V4 R2	Corrections to PTC for 8/16 mA Dry=ON configuration (Table 18), VAM 7-Mar-2024
Q23/10-056	ROS 20-09-098 R004 V4 R1	Updates in Section 2.5.1, VAM 27-Nov-2023
Q23/10-056	ROS 20-09-098 R004 V4 R0	Surveillance Audit, Update to template, 20-Nov-2023 VAM
Q20/09-098	ROS 20-09-098 R004 V3 R4	correction to cross-reference text for Table 7 and 8; JCY, 14-Jul-2022
Q20/09-098	ROS 20-09-098 R004 V3 R3	updated to harmonize with *.nefm files; JCY, 14-Jun-2021
Q20/09-098	ROS 20-09-098 R004 V3 R2	updated after RTR review; JCY, 7-Jan-2021
Q20/09-098	ROS 20-09-098 R004 V3 R1	updated for surveillance audit and combined all 2130 models in one report, cited updated manuals, clarified model assessments, using new report number; JCY, 21-Dec-2020
Q20/04-151	ROS 20-09-098 R004 V2 R2	removed "P" version since it's covered by [R24]; change ownership to RTR; JCY, 24-Jun-2020
Q14/11-048	MOB 08-08-57 R003 V2 R1	updated data for PNP/PLC version based on new FMEDA [R19], [R20], [R21], [R22] and Q14/11-016; Q14/08-072; added second proof test coverages for B.2; converted to new report template; updated per review comments in 24 Feb 2015 e-mail: 25 February 2015, Griff Francis

Q13/05-084	MOB 08-08-57 R003 V1 R9	added analysis for Fault Relay option to 2130D Relay model; updated to IEC61508:2010; converted to new report template: 30 Sep 2013, Griff Francis
For older revisions, see Q08/08-57		

Reviewer: Rudy Chalupa, *exida*, 7 March 2024

Status: Released, 7 March 2024

7.3 Future enhancements

At request of client.

7.4 Release Signatures

Valerie Motto, CFSP, Safety Engineer

Rudolph P. Chalupa, CFSE, Senior Safety Engineer

Appendix A *exida* Environmental Profiles

Table 19 *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[4]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[5]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[6]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[7]	G2	G3	G3	G3	G3	Compatible Material
Surge[8]						
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[9]						
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)[10]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[4] Humidity rating per IEC 60068-2-3
[5] Shock rating per IEC 60068-2-6
[6] Vibration rating per IEC 60770-1
[7] Chemical Corrosion rating per ISA 71.04
[8] Surge rating per IEC 61000-4-5
[9] EMI Susceptibility rating per IEC 6100-4-3
[10] ESD (Air) rating per IEC 61000-4-2

Appendix B Determining Safety Integrity Level

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

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

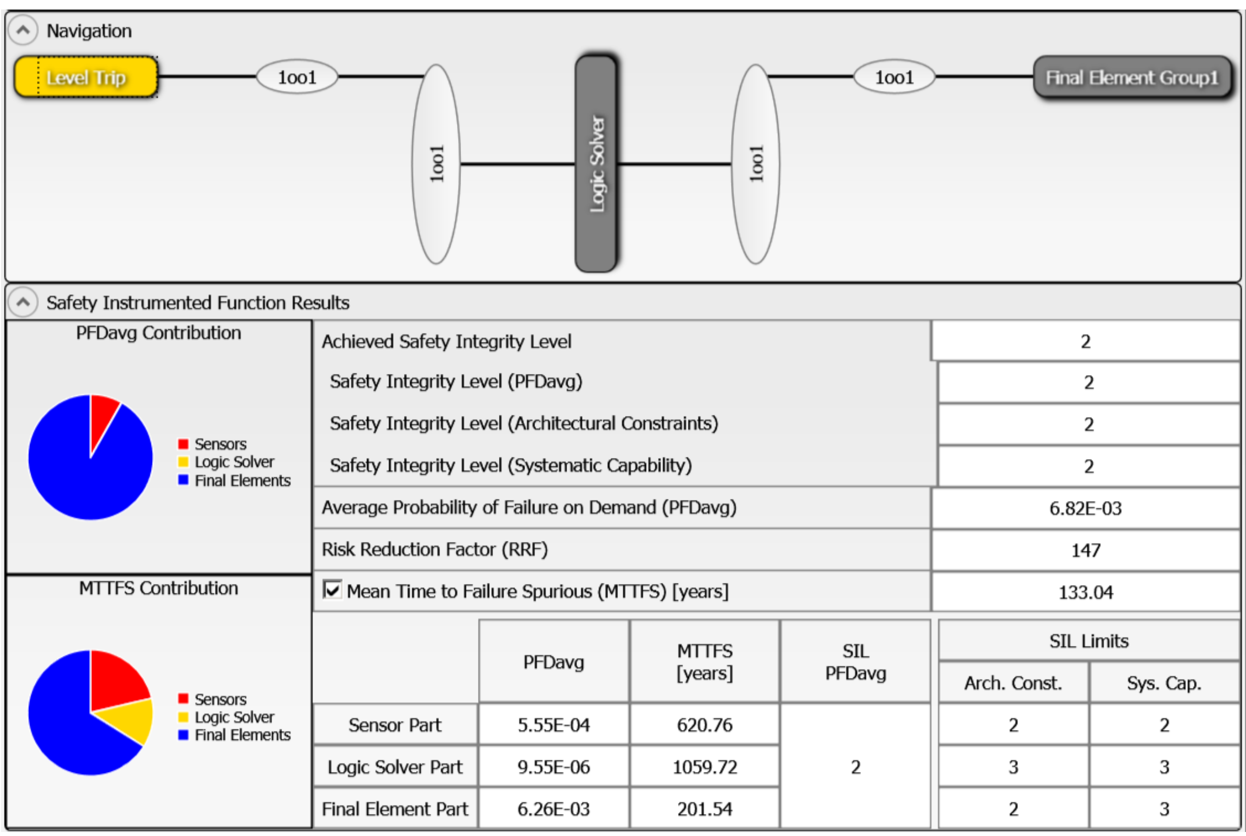
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic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



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.

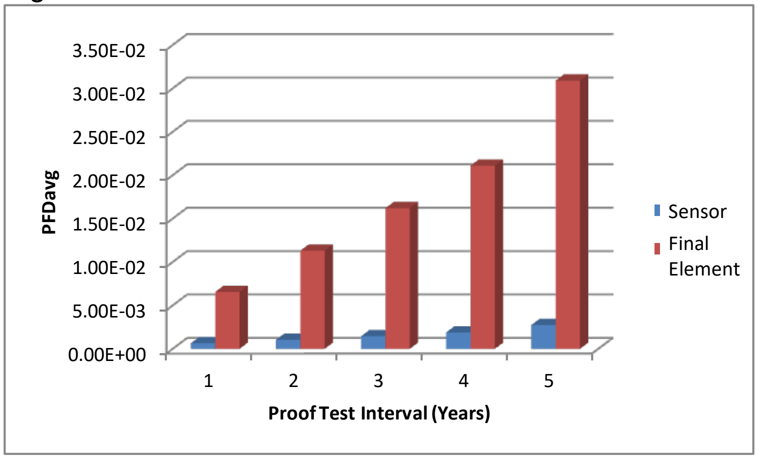
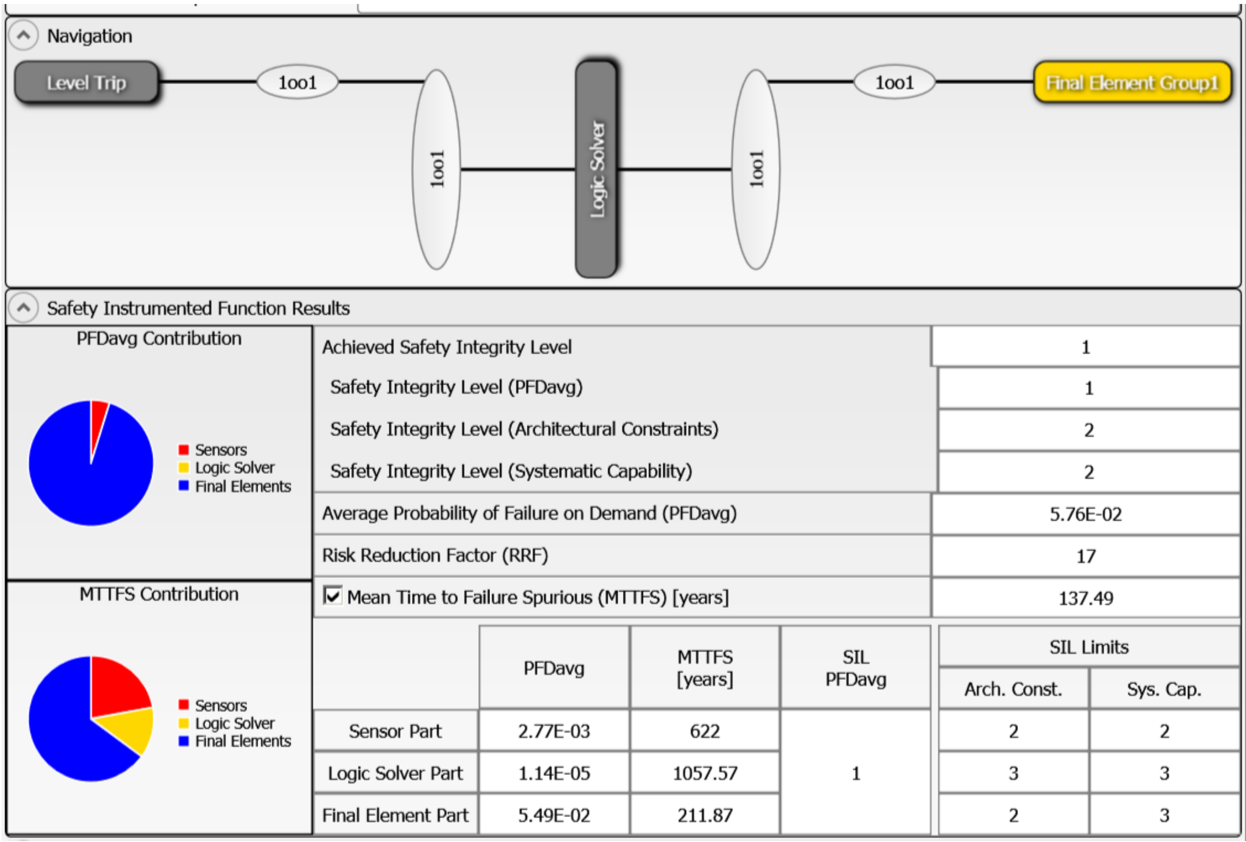


Figure 3 PFD$_{avg}$ versus Proof Test Interval.

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 C Site Safety Index

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

C.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIFs on the site. Table 20 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 20 *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.