



Failure Modes, Effects and Diagnostic Analysis

Project:

Mobrey 2130 Vibrating Fork Point Level Switch

Company:

Mobrey Measurement
SLOUGH, SL1 4UE
UK

Contract Number: Mobrey Q08/08-57

Report No.: MOB 08/08-57 R003

Version V1, Revision R5, September 28, 2010

John Grebe

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Mobrey 2130 Vibrating Fork Point Level Switch, hardware and software as described in [D1] - [D9]. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification of a device per IEC 61508. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the 2130 Point Level Switch. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 2130 Point 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 Point 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 Point Level Switch.

Table 1 Configuration Overview

2130 Point Level Switch, NAMUR (N) - DRY = On	This provides the FMEDA results for the NAMUR (N) model Point 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 $< 1 \text{ mA}$ and On state indicated by $> 2.2 \text{ mA}$
2130 Point Level Switch, NAMUR (N) - WET = On	This provides the FMEDA results for the NAMUR (N) model Point 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 $< 1 \text{ mA}$ and On state indicated by $> 2.2 \text{ mA}$
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 $I_L < 100 \mu\text{A}$ and On state supporting loads with $I_L < 500 \text{ mA}$
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 $I_L < 100 \mu\text{A}$ and On state supporting loads with $I_L < 500 \text{ mA}$
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 $I_L < 3 \text{ mA}$ and On state supporting loads with $20 \text{ mA} < I_L < 500 \text{ mA}$
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 $I_L < 3 \text{ mA}$ and On state supporting loads with $20 \text{ mA} < I_L < 500 \text{ mA}$
2130 Point Level Switch, Relay (D) - DRY = On	This provides the FMEDA results for the Relay (D) model Point 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



2130 Point Level Switch, Relay (D) - WET = On	This provides the FMEDA results for the Relay (D) model Point 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
---	---

The failure rates for the 2130 NAMUR (N) model Point Level Switch with the High Temperature Sensor configured as DRY = On are listed in Table 2.

Table 2 Failure rates 2130 Point Level Switch, NAMUR (N) - DRY = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	133.7	
Fail Dangerous Detected	151.2	
Fail Detected (detected by internal diagnostics)	127.5	
Fail High (detected by logic solver)	9.0	
Fail Low (detected by logic solver)	14.7	
Fail Dangerous Undetected	17.5	
Residual	58.3	
Annunciation Undetected	3.5	

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

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

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	16.5	
Fail Dangerous Detected	259.1	
Fail Detected (detected by internal diagnostics)	235.4	
Fail High (detected by logic solver)	9.0	
Fail Low (detected by logic solver)	14.7	
Fail Dangerous Undetected	26.1	
Residual	58.3	
Annunciation Undetected	3.5	



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 4.

Table 4 Failure rates 2130 Point Level Switch, PNP/PLC (P) - DRY = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	178.6
Fail Dangerous Detected	171.9
Fail Detected (detected by internal diagnostics)	171.9
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	50.8
Residual	236.3
Annunciation Undetected	7.9

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 5.

Table 5 Failure rates 2130 Point Level Switch, PNP/PLC (P) - WET = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	60.4
Fail Dangerous Detected	283.8
Fail Detected (detected by internal diagnostics)	283.8
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	53.5
Residual	239.3
Annunciation Undetected	7.9



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 6.

Table 6 Failure rates 2130 Point Level Switch, Direct Load Switching (L) - DRY = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	194.4
Fail Dangerous Detected	170.6
Fail Detected (detected by internal diagnostics)	170.6
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	45.0
Residual	167.3
Annunciation Undetected	3.1

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 7.

Table 7 Failure rates 2130 Point Level Switch, Direct Load Switching (L) - WET = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	76.4
Fail Dangerous Detected	278.4
Fail Detected (detected by internal diagnostics)	278.4
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	54.8
Residual	167.3
Annunciation Undetected	3.1

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

Table 8 Failure rates 2130 Point Level Switch, Relay (D) - DRY = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	150.5
Fail Dangerous Detected	142.9
Fail Detected (detected by internal diagnostics)	142.9
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	104.6
Residual	107.5
Annunciation Undetected	8.1

The failure rates for the 2130 Relay (D) model Point Level Switch with the High Temperature Sensor configured as WET = On are listed in Table 9.

Table 9 Failure rates 2130 Point Level Switch, Relay (D) - WET = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	33.5
Fail Dangerous Detected	240.9
Fail Detected (detected by internal diagnostics)	240.9
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	116.8
Residual	105.0
Annunciation Undetected	8.1

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

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

Table 10 lists the failure rates for the 2130 Point Level Switch according to IEC 61508.

Table 10 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}^1	λ_{DD}	λ_{DU}	SFF ²
2130 Point Level Switch, NAMUR (N) - DRY = On	0 FIT	195.5 FIT	151.2 FIT	17.5 FIT	95.2%
2130 Point Level Switch, NAMUR (N) - WET = On	0 FIT	78.3 FIT	259.1 FIT	26.1 FIT	92.8%
2130 Point Level Switch, PNP/PLC (P) - DRY = On	0 FIT	422.8 FIT	171.9 FIT	50.8 FIT	92.1%
2130 Point Level Switch, PNP/PLC (P) - WET = On	0 FIT	307.6 FIT	283.8 FIT	53.5 FIT	91.7%
2130 Point Level Switch, Direct Load Switching (L) - DRY = On	0 FIT	364.8 FIT	170.6 FIT	45.0 FIT	92.2%
2130 Point Level Switch, Direct Load Switching (L) - WET = On	0 FIT	246.9 FIT	278.4FIT	54.8 FIT	90.6%
2130 Point Level Switch, Relay (D) - DRY = On	0 FIT	266.1 FIT	142.9 FIT	104.6 FIT	79.6%
2130 Point Level Switch, Relay (D) - WET = On	0 FIT	146.6 FIT	240.9 FIT	116.8 FIT	76.8%

The 2130 Point Level Switch is classified as a Type B³ device according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the following models have a safe failure fraction between 90% and 99%⁴ (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 2 as a single device:

- 2130 Point Level Switch, NAMUR (N) - DRY = On
- 2130 Point Level Switch, PNP/PLC (P) - DRY = On
- 2130 Point Level Switch, Direct Load Switching (L) - DRY = On
- 2130 Point Level Switch, NAMUR (N) - WET = On
- 2130 Point Level Switch, PNP/PLC (P) - WET = On
- 2130 Point Level Switch, Direct Load Switching (L) - WET = On

¹ It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

² Safe Failure Fraction needs to be calculated on (sub)system level

³ Type B device: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.



All other versions and configurations of the 2130 Point Level Switch have a safe failure fraction between 60% and 90% and therefore may be used up to SIL 1 as a single device. These models are listed as follows:

2130 Point Level Switch, Relay (D) - DRY = On

2130 Point Level Switch, Relay (D) - WET = On

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

A user of the 2130 Point 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	10
2 Project Management	11
2.1 <i>exida</i>	11
2.2 Roles of the parties involved	11
2.3 Standards and Literature used	11
2.4 Reference documents	12
2.4.1 Documentation provided by Mobrey Measurement	12
2.4.2 Documentation generated by <i>exida</i>	12
3 Product Description	14
4 Failure Modes, Effects, and Diagnostic Analysis	16
4.1 Failure Categories description	16
4.2 Methodology – FMEDA, Failure Rates	17
4.2.1 FMEDA	17
4.2.2 Failure Rates	17
4.3 Assumptions	18
4.3.1 User Configuration Restrictions	19
4.4 Results	19
5 Using the FMEDA Results	25
5.1 PFD _{AVG} Calculation 2130 Point Level Switch	25
6 Terms and Definitions	27
7 Status of the Document	28
7.1 Liability	28
7.2 Releases	28
7.3 Future Enhancements	28
7.4 Release Signatures	29
Appendix A Lifetime of Critical Components	30
Appendix B Proof tests to reveal dangerous undetected faults	31
B.1 Suggested Proof Test	31

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by exida according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by exida according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects and Diagnostic Analysis carried out on 2130 Point Level Switch. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

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

2 Project Management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 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 partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Mobrey Measurement

Manufacturer of the 2130 Point Level Switch

exida

Performed the hardware assessment according to Option 1 (see Section 1)

Mobrey Measurement contracted *exida* in August 2008 with the hardware assessment of the above-mentioned device.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	<i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	Goble, W.M. and Cheddie, H., 2005	Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISA, ISBN 1-55617-909-X

2.4 Reference documents

2.4.1 Documentation provided by Mobrey Measurement

[D1]	pcb installation manual.pdf	Installation and Instruction Booklet, IP2025/PCB, April 2006, Rev. AA
[D2]	DS_ip2024.pdf	Mobrey Squing 2 vibrating fork point level measurement, IP2024, June 04
[D3]	82640-iss5.pdf	Schematic, CIRC.DIAG. SQUING I.S., Drawing No. 82640, 9/10/07
[D4]	82641-iss8.pdf	Schematic, CIRC.DIAG. SQUING 2/2120 / 2130 SELF-CHECKING, PNP/PLC VERSION, Drawing No. 82641, 24/10/07
[D5]	82642-iss7.pdf	Schematic, CIRC.DIAG. SQUING 2/2120 / 2130 SELF-CHECKING, RELAY VERSION, Drawing No. 82642, 22/10/07
[D6]	82643-iss7.pdf	Schematic, CIRC.DIAG. SQUING 2/2120 / 2130 SELF-CHECKING, 2 WIRE VERSION, Drawing No. 82643, 22/10/07
[D7]	71097_1006-iss4.pdf	SQUING 2 I.S. APPROVAL DRAWING, Drawing No. 71097/1006, 3/5/01
[D8]	71097_1242-iss3.pdf	APPROVAL DRG. SQUING 2 I.S. HIGH TEMP, Drawing No. 71097/1242, 12/9/07
[D9]	SFRS145 Rev 1.5.pdf	Squing2 Upgrade, Software Functional Requirements, Rev 1.5, June 24, 2008

2.4.2 Documentation generated by *exida*

[R1]	Mobrey Squing 2 - FI Numar IS - DRY ON - wo sensor.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R2]	Mobrey Squing 2 - FI Numar IS - WET ON - wo sensor.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R3]	Mobrey Squing 2 - FI Numar IS - High Temp Sensor - DRY ON - Profile 2.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R4]	Mobrey Squing 2 - FI Numar IS - High Temp Sensor - WET ON - Profile 2.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R5]	Mobrey Squing 2 - PNP PNC - FI HS Iso DRY ON - wo sensor 06192010.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R6]	Mobrey Squing 2 - PNP PNC -	Failure Modes, Effects, and Diagnostic Analysis –

	FI HS Iso WET ON - wo sensor 06192010.efm	2130 Point Level Switch
[R7]	Mobrey Squing 2 non IS - FI High Temp Sensor - DRY ON - Profile 3.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R8]	Mobrey Squing 2 non IS - FI High Temp Sensor - WET ON - Profile 3.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R9]	Mobrey Squing 2 - 2 Wire - DRY ON - FI HS Iso wo sensor 08192009.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R10]	Mobrey Squing 2 - 2 Wire - WET ON -FI HS Iso wo sensor 08192009.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R11]	Mobrey Squing 2 - Relay Common - DRY ON - wo sensor.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R12]	Mobrey Squing 2 - Relay Common - WET ON - wo sensor.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R13]	Mobrey Squing 2 non IS - High Temp Sensor - DRY ON - Profile 2.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R14]	Mobrey Squing 2 non IS - High Temp Sensor - WET ON - Profile 2.efm	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch
[R15]	Mobrey Squing 2 FMEDA FI Summary Sheet 08192010.xls	Failure Modes, Effects, and Diagnostic Analysis – 2130 Point Level Switch Summary Sheet
[R16]	MOB 08-08-57 R003 V1 R5 FMEDA 2130.doc, 09/28/2010	FMEDA report, 2130 Point Level Switch (this report)

3 Product Description

The Mobrey 2130 Vibrating Fork Point 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 alarm and the liquid rising in the vessel contacts with the fork resulting in a reduction of its frequency; this is detected by the electronics which in turn switch 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 2130 Point Level Switch is available in different models that support a selection of electrical interfaces:

- Intrinsically Safe (IS) NAMUR to DIN 19234, IEC 60947-5-6
- Solid state PNP output for direct interface to PLCs (three wire) 24 to 60V dc
- Direct load switching (two wire) 24 to 264V ac 50/60Hz, 24 to 60V dc
- Single Pole Changeover (DPCO) relay for voltage free contacts

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

Figure 1 provides an overview of the 2130 Point Level Switch and the boundary of the FMEDA.

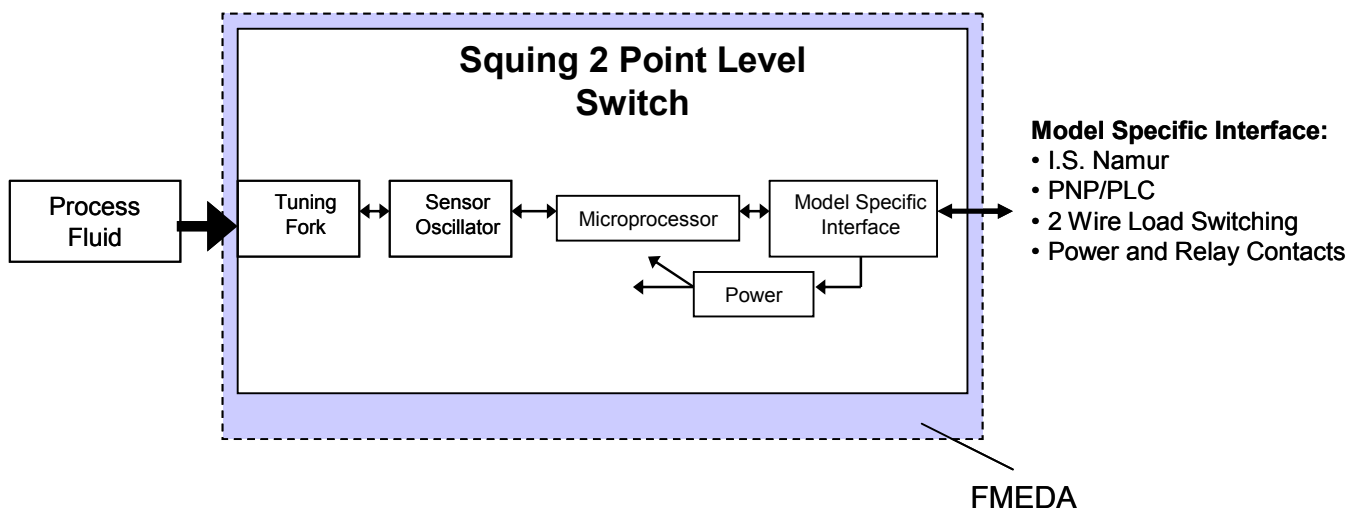


Figure 1 2130 Point Level Switch, Parts included in the FMEDA

Table 11 gives an overview of the different versions that were considered in the FMEDA of the 2130 Point Level Switch.

Table 11 Version Overview

2130 Point Level Switch, NAMUR (N) - DRY = On	This provides the FMEDA results for the NAMUR (N) model Point 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 Point Level Switch, NAMUR (N) - WET = On	This provides the FMEDA results for the NAMUR (N) model Point 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 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 $I_L < 100 \mu A$ and On state supporting loads with $I_L < 500 \text{ mA}$
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 $I_L < 100 \mu A$ and On state supporting loads with $I_L < 500 \text{ mA}$
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 $I_L < 3 \text{ mA}$ and On state supporting loads with $20 \text{ mA} < I_L < 500 \text{ mA}$
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 $I_L < 3 \text{ mA}$ and On state supporting loads with $20 \text{ mA} < I_L < 500 \text{ mA}$
2130 Point Level Switch, Relay (D) - DRY = On	This provides the FMEDA results for the Relay (D) model Point 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
2130 Point Level Switch, Relay (D) - WET = On	This provides the FMEDA results for the Relay (D) model Point 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

The 2130 Point Level Switch is classified as a Type B⁵ device according to IEC 61508, having a hardware fault tolerance of 0.

⁵ Type B device: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Mobrey Measurement and is documented in [R1] through [R16].

4.1 Failure Categories description

In order to judge the failure behavior of the 2130 Point 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 is detected and 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 Namur output signal to go significantly above expected output current (>8 mA) and may be detected by shorted field wire monitoring (Namur only).
Fail Low	Failure that causes the Namur output signal to go to the under-range or low alarm output current(< 0.1 mA) and may be detected by open field wire monitoring (Namur only).
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.
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 2000, the Residual failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

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

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook which was derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates for the the NAMUR current output interface and relay output versions were chosen to *match exida* Profile 2, see Table 12. Due to potentially higher internal power dissipation the rates for the PNP/PLC 3 wire interface and the direct load switching 2 wire interface versions were chosen to *match exida* Profile 3. 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.

Table 12 exida Environmental Profiles

EXIDA ENVIRONMENTAL PROFILE	GENERAL DESCRIPTION	PROFILE PER IEC 60654-1	AMBIENT TEMPERATURE [°C]		TEMP CYCLE [°C / 365 DAYS]
			AVERAGE (EXTERNAL)	MEAN (INSIDE BOX)	
1 Cabinet Mounted Equipment	Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings	B2	30	60	5
2 Low Power /Mechanical Field Products	Mechanical / low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings	C3	25	30	25
3 General Field Equipment	General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings	C3	25	45	25
4 Unprotected Mechanical Field Products	Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation.	D1	25	30	35

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however, should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. 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.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 2130 Point Level Switch.

- Only a single component failure will fail the entire 2130 Point 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
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 or Profile 3 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online 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
- 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 2130 Point 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 Point 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 Point Level Switch will worst case response time shall be considered to be the larger of 10 seconds and 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 FMEDA.



The failure rates for the 2130 NAMUR (N) 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, NAMUR (N) - DRY = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	133.7	
Fail Dangerous Detected	151.2	
Fail Detected (detected by internal diagnostics)	127.5	
Fail High (detected by logic solver)	9.0	
Fail Low (detected by logic solver)	14.7	
Fail Dangerous Undetected	17.5	
Residual	58.3	
Annunciation Undetected	3.5	

The failure rates for the 2130 NAMUR (N) 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, NAMUR (N) - WET = On

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected	16.5	
Fail Dangerous Detected	259.1	
Fail Detected (detected by internal diagnostics)	235.4	
Fail High (detected by logic solver)	9.0	
Fail Low (detected by logic solver)	14.7	
Fail Dangerous Undetected	26.1	
Residual	58.3	
Annunciation Undetected	3.5	



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 15.

Table 15 Failure rates 2130 Point Level Switch, PNP/PLC (P) - DRY = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	178.6
Fail Dangerous Detected	171.9
Fail Detected (detected by internal diagnostics)	171.9
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	50.8
Residual	236.3
Annunciation Undetected	7.9

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 16.

Table 16 Failure rates 2130 Point Level Switch, PNP/PLC (P) - WET = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	60.4
Fail Dangerous Detected	283.8
Fail Detected (detected by internal diagnostics)	283.8
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	53.5
Residual	239.3
Annunciation Undetected	7.9



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 17.

Table 17 Failure rates 2130 Point Level Switch, Direct Load Switching (L) - DRY = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	194.4
Fail Dangerous Detected	170.6
Fail Detected (detected by internal diagnostics)	170.6
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	45.0
Residual	167.3
Annunciation Undetected	3.1

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 18.

Table 18 Failure rates 2130 Point Level Switch, Direct Load Switching (L) - WET = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	76.4
Fail Dangerous Detected	278.4
Fail Detected (detected by internal diagnostics)	278.4
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	54.8
Residual	167.3
Annunciation Undetected	3.1



The failure rates for the 2130 Relay (D) model Point Level Switch with the High Temperature Sensor configured as DRY = On are listed in Table 19.

Table 19 Failure rates 2130 Point Level Switch, Relay (D) - DRY = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	150.5
Fail Dangerous Detected	142.9
Fail Detected (detected by internal diagnostics)	142.9
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	104.6
Residual	107.5
Annunciation Undetected	8.1

The failure rates for the 2130 Relay (D) model Point Level Switch with the High Temperature Sensor configured as WET = On are listed in Table 20.

Table 20 Failure rates 2130 Point Level Switch, Relay (D) - WET = On

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	33.5
Fail Dangerous Detected	240.9
Fail Detected (detected by internal diagnostics)	240.9
Fail High (detected by logic solver)	-
Fail Low (detected by logic solver)	-
Fail Dangerous Undetected	116.8
Residual	105.0
Annunciation Undetected	8.1

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

Table 21 lists the failure rates for the 2130 Point Level Switch according to IEC 61508. The Safe Failure Fraction is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formulas for SFF: $SFF = 1 - \lambda_{DU} / \lambda_{TOTAL}$

Table 21 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}^6	λ_{DD}	λ_{DU}	SFF ⁷
2130 Point Level Switch, NAMUR (N) - DRY = On	0 FIT	195.5 FIT	151.2 FIT	17.5 FIT	95.2%
2130 Point Level Switch, NAMUR (N) - WET = On	0 FIT	78.3 FIT	259.1 FIT	26.1 FIT	92.8%
2130 Point Level Switch, PNP/PLC (P) - DRY = On	0 FIT	422.8 FIT	171.9 FIT	50.8 FIT	92.1%
2130 Point Level Switch, PNP/PLC (P) - WET = On	0 FIT	307.6 FIT	283.8 FIT	53.5 FIT	91.7%
2130 Point Level Switch, Direct Load Switching (L) - DRY = On	0 FIT	364.8 FIT	170.6 FIT	45.0 FIT	92.2%
2130 Point Level Switch, Direct Load Switching (L) - WET = On	0 FIT	246.9 FIT	278.4FIT	54.8 FIT	90.6%
2130 Point Level Switch, Relay (D) - DRY = On	0 FIT	266.1 FIT	142.9 FIT	104.6 FIT	79.6%
2130 Point Level Switch, Relay (D) - WET = On	0 FIT	146.6 FIT	240.9 FIT	116.8 FIT	76.8%

The architectural constraint type for the 2130 Point Level Switch is B. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

⁶ It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

⁷ Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA using the 2130 Point Level Switch for example calculations.

5.1 PFD_{AVG} Calculation 2130 Point Level Switch

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) 2130 Point Level Switch. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. For the proof tests a proof test coverage of 90% has been assumed, see Appendix A.

The resulting PFD_{AVG} values for the 2130 Point Level Switch models configured for high level alarm as DRY=On for a variety of proof test intervals are displayed in Figure 2. As shown in the graph the PFD_{AVG} value for a single 2130, NAMUR 2130 Point Level Switch configured as DRY=On, with a proof test interval of 1 year equals 1.5E-4.

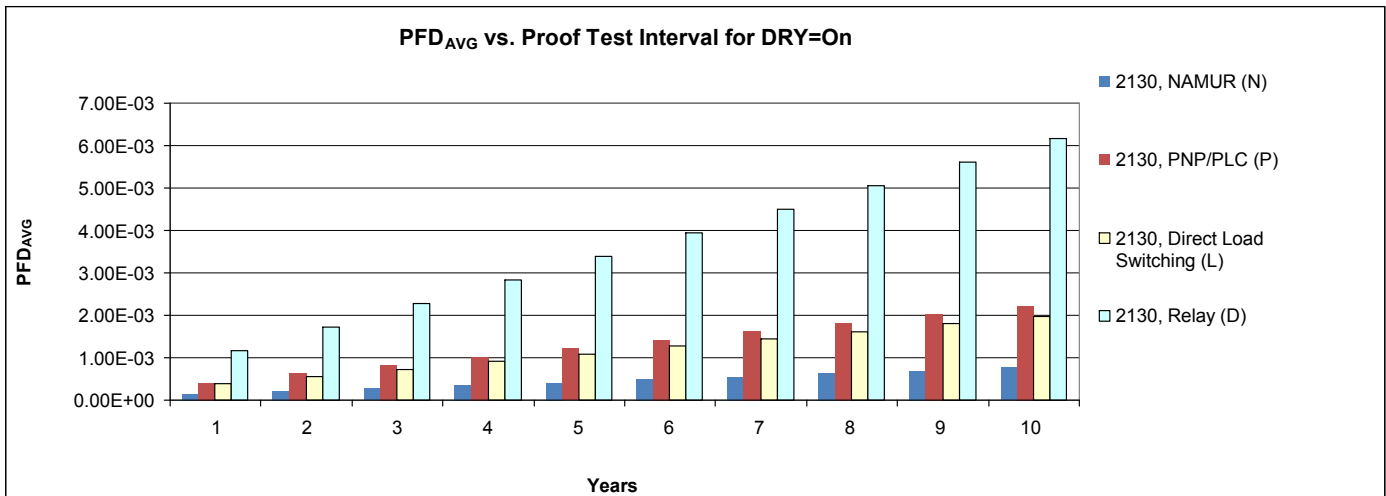


Figure 2 PFD_{AVG}(t) 2130 Point Level Switch configured for DRY=On

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

For a SIL 2 application, the PFD_{AVG} value needs to be $\geq 10^{-3}$ and $< 10^{-2}$. This means that for a SIL 2 application using the 2130, NAMUR 2130 Point Level Switch configured as DRY=On, the PFD_{AVG} for a 1-year Proof Test Interval the 2130 Point Level Switch is approximately equal to 1.5% of the SIL 2 range. For a SIL 2 application using the 2130 PNP/PLC configured as DRY=On, the PFD_{AVG} for a 1-year Proof Test Interval the 2130 Point Level Switch is approximately equal to 4.3% of the SIL 2 range.

Figure 3 similarly shows the resulting PFD_{AVG} values for the 2130 Point Level Switch models configured for low level alarm as WET=On for a variety of proof test intervals.

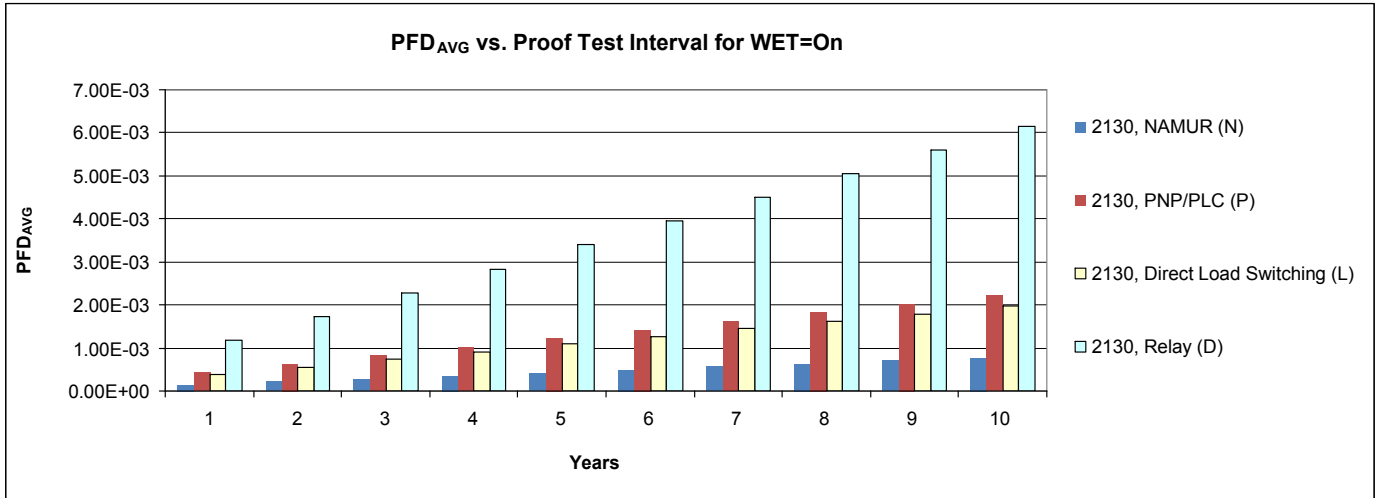


Figure 3 PFD_{AVG}(t) 2130 Point Level Switch configured for WET=On

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Definitions

FIT	Failure In Time (1x10 ⁻⁹ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD _{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	“Non-Complex” component (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 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, 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 product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version: V1

Revision: R5

Version History: V1, R5: Changed report number to R003 and limited to 2130 models, September 28, 2010

V1, R4: Minor corrections after internal review, August 24, 2010

V1, R3: Updated after Fault Injection testing, August 19, 2010

V1, R2: Minor corrections to 2 Wire data, March 26, 2009

V1, R1: Released to Mobrey Measurement; March 4, 2009

V0, R1: Draft; February 19, 2009

Author(s): John Grebe

Review: V1, R3: Jon Keswick, August 20, 2010

V0, R1: Rudolf Chalupa (*exida*); March 4, 2009

Release Status: Released to Mobrey Measurement

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 above a solid black horizontal line.

Dr. William M. Goble, Principal Partner

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

John C. Grebe Jr., Principal Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.7.4 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 lifetime⁸ 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 25 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 22 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours

It is the responsibility of the end user to maintain and operate the 2130 Point Level Switch per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

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

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

⁸ 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 7.4.3.2.2 f) of IEC 61508-2, proof tests shall be undertaken to reveal dangerous faults which are undetected by 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 Proof Test

A suggested proof test is described in Table 23. This test will detect > 90% of possible DU failures in the 2130 Point Level Switch.

Table 23 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Observe the local LED indicator to discover any diagnostics and take appropriate action.
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
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
6.	Observe LED color and confirm the unit is operating in the “Enhanced self-check” mode of operation
7.	Remove the bypass and otherwise restore normal operation