Failure Modes, Effects and Diagnostic Analysis

Project:
2120 Level Switch

Company:
Rosemount Measurement Limited
Emerson Process Management
Slough, SL1 4UE
UK

Contract Numbers: Q08/08-57, Q13/11-053, Q14/08-015, Q14/11-048
Report No.: MOB 08/08-57 R002
Version V1, Revision R6, January 22, 2015
John Grebe, Griff Francis

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 2120 Level Switch, hardware and software 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 2120 Level Switch. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

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

Table 1 is an overview of the different versions in the FMEDA of the 2120 Level Switch.

Table 1 Version Overview

2120 Level Switch, NAMUR (K) - DRY = On	NAMUR (K) model Level Switch configured as DRY = On using the NAMUR current output interface (DIN 19234, IEC 60947-5-6) with Off state indicated by < 1 mA and On state indicated by > 2.2 mA
2120 Level Switch, 8/16mA (H) - DRY = On	8/16mA (H) model Level Switch configured as DRY = On with Off state indicated by 8 mA and On state indicated by 16 mA
2120 Level Switch, PNP/PLC (G) - DRY = On	PNP/PLC (G) model Level Switch configured as DRY = On with Off state indicated by <100uA and On state indicated by <3V difference between the + and OUT terminals
2120 Level Switch, Relay (V) - DRY = On	Relay (V) model Level Switch configured as DRY = On with Off state indicated by contact between the NC and C terminals and On state indicated by contact between the NO and C terminals

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

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

2120 Level Switch, NAMUR (K) - DRY = On

2120 Level Switch, 8/16mA (H) - DRY=On

2120 Level Switch, PNP/PLC (G) - DRY=On

[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.

The following version and configuration of the 2120 Level Switch has a safe failure fraction between 60% and 90% and therefore may be used up to SIL 1 as a single device.

2120 Level Switch, Relay (V) - DRY=On

The failure rates for the 2120 NAMUR (K) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 2.

Table 2 Failure rates 2120 Level Switch, NAMUR (K) - DRY = On

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

The failure rates for other 2120 versions are in section 4.4.

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 3 lists the failure rates for the 2120 Level Switch according to IEC 61508.

Table 3 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
2120 Level Switch, NAMUR (K) - DRY = On	0 FIT	118 FIT	131 FIT	24 FIT	91.1%
2120 Level Switch, 8/16mA (H) - Dry=On	0 FIT	136 FIT	152 FIT	29 FIT	90.9%
2120 Level Switch, PNP/PLC (G) - Dry=On	0 FIT	241 FIT	130 FIT	41 FIT	90.0%
2120 Level Switch, Relay (V) - Dry=On	0 FIT	131 FIT	130 FIT	102 FIT	72.0%

A user of the 2120 Level Switch can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

[2] 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.
[3] Safe Failure Fraction needs to be calculated on (sub)system level

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 2120 Level Switch. From this, failure rates and example PFD_{AVG} values may be calculated.

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

An FMEDA is part of 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 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 global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Rosemount Measurement Limited	Manufacturer of the 2120 Level Switch
exida	Performed the hardware assessment

Rosemount Measurement Limited contracted *exida* in December 2013, August 2014 and November 2014 with the hardware assessment of the above mentioned device.

2.3 Standards and literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3nd Edition, 2012	exida LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3nd 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. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

2.4 *exida* tools used

[T1]	V7.1.17	FMEDA Tool
[T2]	Version 3.0.8.758	exSILentia

2.5 Reference documents

2.5.1 Documentation provided by Rosemount Measurement Limited

[D1]	00813-0100-4030, Rev GB, June 2013	Product Data Sheet, Rosemount 2120 Full-featured Vibrating Fork Liquid Level Switch
[D2]	82953, ISS 2, 22 Dec 2010	Schematic, CIRC.DIAG 2120 NAMUR VERSION
[D3]	82957, ISS 04, 8 May 2012	Schematic, CIRC.DIAG. 2120 8/16mA VERSION
[D4]	71097/1006, ISS 4, 17 Oct 2007	SQUING 2 I.S. APPROVAL DRAWING (shows construction of sensor
[D5]	SFRS145 Rev 1.5.pdf	Squing2 Upgrade, Software Functional Requirements, Rev 1.5, June 24, 2008
[D6]	2120_2130 Fault Injection results 04_08_10.xlsx	Fault Injection Test Results for 2120 and 2130 models, updated 30 July 2010
[D7]	Manual Supplement 00809-0500-4030, Rev AC, August 2014	Rosemount 2120 Functional Safety Manual
[D8]	Al-elec used in 21xx series.xls, 20 Aug 2014	List of Al-electrolytic capacitors used in 21xx series
[D9]	82954, REV 3, 23 Jan 2014	Schematic, CIRC. DIAG. 2120 PNP/PLC VERSION
[D10]	J32072A, Issue 3, 9 May 2011	Parts List, PCB ASSY 2120 PNP/PLC
[D11]	82955, IS 2, 11 Nov 2010	Schematic, CIRC. DIAG. 2120 RELAY VERSION
[D12]	J3208/2A, Issue 3, 9 May 2011	Parts List, PCB ASSY 2120 RELAY

2.5.2 Documentation generated by *exida*

[R1]	Mobrey Squing 2 - 8-16mA output - Std Temp Sensor - DRY ON (no self check) - Profile 2_15Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R2]	Mobrey Squing 2 - 8-16mA output - DRY ON (no self check) - wo sensor_14Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R3]	Mobrey Squing 2 - FI Numar IS - DRY ON (no self check) - wo sensor_15Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R4]	Mobrey Squing 2 - FI Numar IS - Std Temp Sensor (no self check) - DRY ON - Profile 2_15Aug2014.efm	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch
[R5]	Mobrey Squing 2 FMEDA FI Summary Sheet 15Aug2014.xls	Failure Modes, Effects, and Diagnostic Analysis – 2120 Level Switch Summary Sheet
[R6]	Mobrey 2120 - PNP PLC - FI HS Iso DRY ON - wo sensor 20141216_1002.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 PNP/PLC Dry=ON, microcontroller and output sections
[R7]	Mobrey 2120 - PNP PLC - Dry ON - FI Std Temp Sensor 20141217.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 PNP/PLC Dry=ON, sensor and sensor circuitry
[R8]	Mobrey 2120 - Relay Common - DRY ON - wo sensor 20141212.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 Relay Dry=ON, microcontroller and output sections
[R9]	Mobrey 2120 Relay - Std Temp Sensor - DRY ON 20141212.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 Relay Dry=ON, sensor and sensor circuitry
[R10]	Mobrey 2120 - per Relay 20141212.efm	Failure Modes, Effects, and Diagnostic Analysis- 2120 Relay (component)
[R11]	Mobrey 2120-2130 FMEDA Summary Sheet_17Dec2014.xls	Failure Modes, Effects, and Diagnostic Analysis – Mobrey 2130/2120 Summary

3 Product Description

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

The 2120 is designed using the tuning fork principle. The 2120 continuously monitors changes in its vibrating fork's natural resonant frequency. When used as a high 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 2120 Level Switch is available in different models that support a selection of electrical interfaces:

- NAMUR to DIN 19234, IEC 60947-5-6 (NAMUR cassette available with I.S approval)
- 8/16 mA Current Output (8/16 mA cassette available with I.S approval)
- PNP/PLC Output
- Relay Output

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 2120 Level Switch and the boundary of the FMEDA.

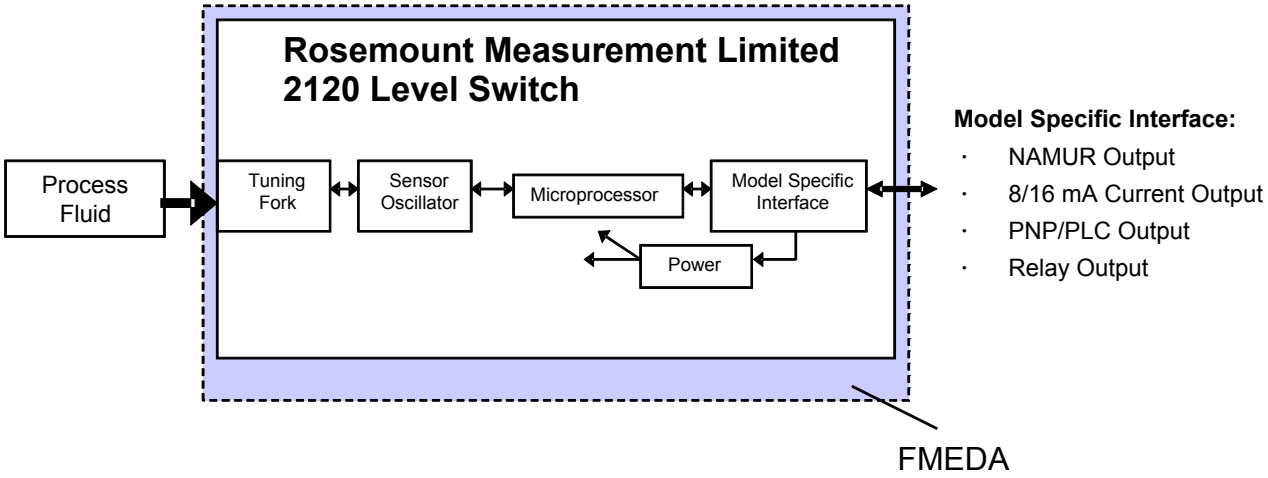


Figure 1 2120 Level Switch, Parts included in the FMEDA

Table 4 is an overview of the different versions in the FMEDA of the 2120 Level Switch.

Table 4 Version Overview

2120 Level Switch, NAMUR (K) - DRY = On	NAMUR (K) model Level Switch configured as DRY = On using the NAMUR current output interface (DIN 19234, IEC 60947-5-6) with Off state indicated by < 1 mA and On state indicated by > 2.2 mA
2120 Level Switch, 8/16mA (H) - DRY = On	8/16mA (H) model Level Switch configured as DRY = On with Off state indicated by 8 mA and On state indicated by 16 mA
2120 Level Switch, PNP/PLC (G) - DRY = On	PNP/PLC (G) model Level Switch configured as DRY = On with Off state indicated by <100uA and On state indicated by <3V difference between the + and OUT terminals
2120 Level Switch, Relay (V) - DRY = On	Relay (V) model Level Switch configured as DRY = On with Off state indicated by contact between the NC and C terminals and On state indicated by contact between the NO and C terminals

The 2120 Level Switch is classified as a Type B[4] element according to IEC 61508, having a hardware fault tolerance of 0.

[4] 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 is performed based on the documentation obtained from Rosemount Measurement Limited and is documented in section 2.5.1.

4.1 Failure categories description

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

Fail-Safe State	State where the output goes to the OFF or de-energized state
Fail Safe	Failure that causes the device to go to the defined fail-safe state (OFF) without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (OFF).
Fail Dangerous	Failure that results in output state stuck in the ON state or not transitioning to the OFF state within the expected response time when the process condition at the monitored level position changes from the 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).
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 2H 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. 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 automatic diagnostic 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 Handbooks [N2] and [N3] which was derived using over ten billion unit operational hours of 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 NAMUR current output, 8/16 mA current and Relay output versions were chosen to match *exida* Profile 2. The rates for the PNP/PLC output version was chosen to match *exida* Profile 3. See Appendix C. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Rosemount Measurement Limited. 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.

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". 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 such as *exida* SILStat™ 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 2120 Level Switch.

- Only a single component failure will fail the entire 2120 Level Switch.
- Failure rates are constant, wear-out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Failures caused by maintenance capability are site specific and therefore cannot be included.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 for the NAMUR, 8/16mA and Relay versions or *exida* Profile 3 for the PNP/PLC version with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed per manufacturer's instructions.
- External power supply failure rates are not included.
- Faults only annunciated via LED indication are not considered "detected" by the FMEDA
- Worst-case internal fault detection time is less than one hour.

4.3.1 User Configuration Restrictions

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

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

The failure rates for the 2120 NAMUR (K) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 5.

Table 5 Failure rates 2120 Level Switch, NAMUR (K) - DRY = On

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

The failure rates for the 8/16 mA (H) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 6.

Table 6 Failure rates 2120 Level Switch, 8/16 mA (H) - DRY = On

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

The failure rates for the PNP/PLC (G) Level Switch with the Standard Temperature Sensor configured as DRY = On are listed in Table 7.

Table 7 Failure rates 2120 Level Switch, PNP/PLC (G) - DRY = On

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

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

Table 8 Failure rates 2120 Level Switch, Relay (V) - DRY = On

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

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

Table 9 lists the failure rates for the 2120 Level Switch according to IEC 61508.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

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.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

SFF = ($\Sigma\lambda_S$ avg + $\Sigma\lambda_{DD}$ avg)/($\Sigma\lambda_S$ avg + $\Sigma\lambda_{DD}$ avg+ $\Sigma\lambda_{DU}$ avg)

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

SFF = ($\Sigma\lambda_S$ + $\Sigma\lambda_{DD}$)/($\Sigma\lambda_S$ + $\Sigma\lambda_{DD}$ + $\Sigma\lambda_{DU}$)

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU}= Fail Dangerous Undetected

Table 9 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF[6]
2120 Level Switch, NAMUR (K) - DRY = On	0 FIT	118 FIT	131 FIT	24 FIT	91.1%
2120 Level Switch, 8/16mA (H) - Dry=On	0 FIT	136 FIT	152FIT	29 FIT	90.9%
2120 Level Switch, PNP/PLC (G) - Dry=On	0 FIT	241 FIT	130 FIT	41 FIT	90.0%
2120 Level Switch, Relay (V) - Dry=On	0 FIT	131 FIT	130 FIT	102 FIT	72.0%

[5] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[6] Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

The following section describes how to apply the results of the FMEDA.

5.1 PFD_{AVG} calculation 2120 Level Switch

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 2120 Level Switch with *exida's* exSILentia tool. 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. Table 10 lists the proof test coverage (see Appendix B) used for the various configurations as well as the results when the proof test interval equals 1 year.

Table 10 Sample PFD_{AVG} Results

Device	Full Proof Test Coverage	PFD_{AVG}	% of SIL 2 Range	Partial Proof Test Coverage	PFD_{AVG}	% of SIL 2 Range
2120 Level Switch, NAMUR (K) - DRY = On	88%	2.24E-04	2%	76%	3.39E-04	3%
2120 Level Switch, 8/16mA (H) - DRY = On	89%	2.55E-04	3%	81%	3.46E-04	3%
2120 Level Switch, PNP/PLC (G) - DRY = On	74%	6.11E-04	6%	68%	6.95E-04	7%

Device	Full Proof Test Coverage	PFD_{AVG}	% of SIL 1 Range	Partial Proof Test Coverage	PFD_{AVG}	% of SIL 1 Range
2120 Level Switch, Relay (V) - DRY = On	75%	1.45E-03	1%	69%	1.69E-03	2%

The resulting PFD_{AVG} Graphs generated from the exSILentia tool for a proof test of 1 year are displayed in Figure **2** and Figure 3.

5.1.1 Full Proof Test

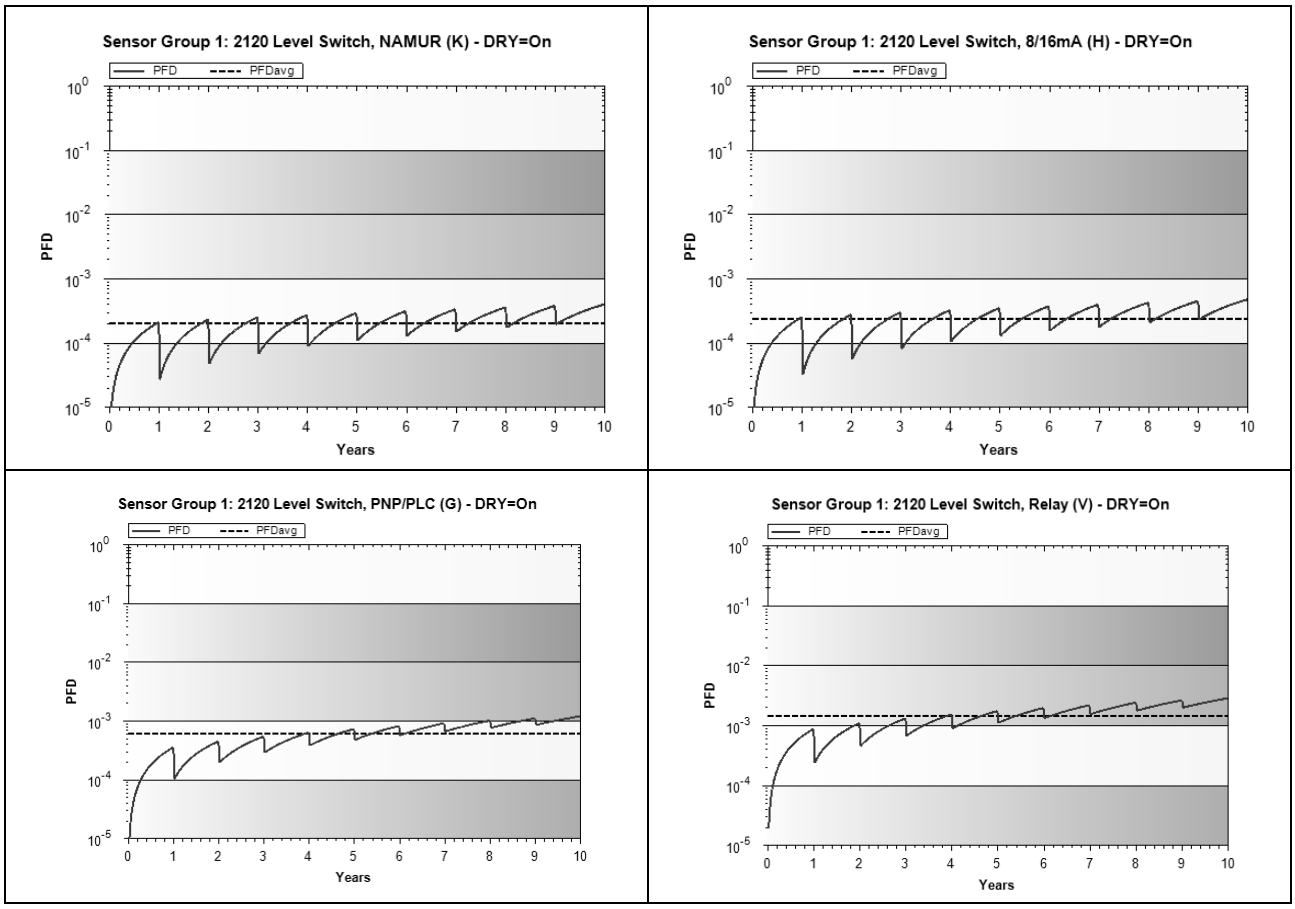


Figure 2 PFD_{AVG} value for a single, 2120 Level Switch with proof test intervals of 1 year using the Full Proof Test.

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 SIL 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. This means that for a SIL 2 application, performing the Full Proof Test with a 1-year Proof Test Interval on the 2120 Level Switch, NAMUR (K) - DRY = On produces a PFD_{AVG} approximately equal to 2% of the range. For the 2120 Level Switch, 8/16mA (H) - DRY = On the PFD_{AVG} is approximately equal to 3% of the range. For the 2120 Level Switch, PNP/PLC (G) - DRY = On the PFD_{AVG} is approximately equal to 6% of the range.

For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, performing the Full Proof Test with a 1-year Proof Test Interval on the 2120 Level Switch, Relay (V) - DRY = On produces a PFD_{AVG} approximately equal to 1% of the range.

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).

5.1.2 Partial Proof Test

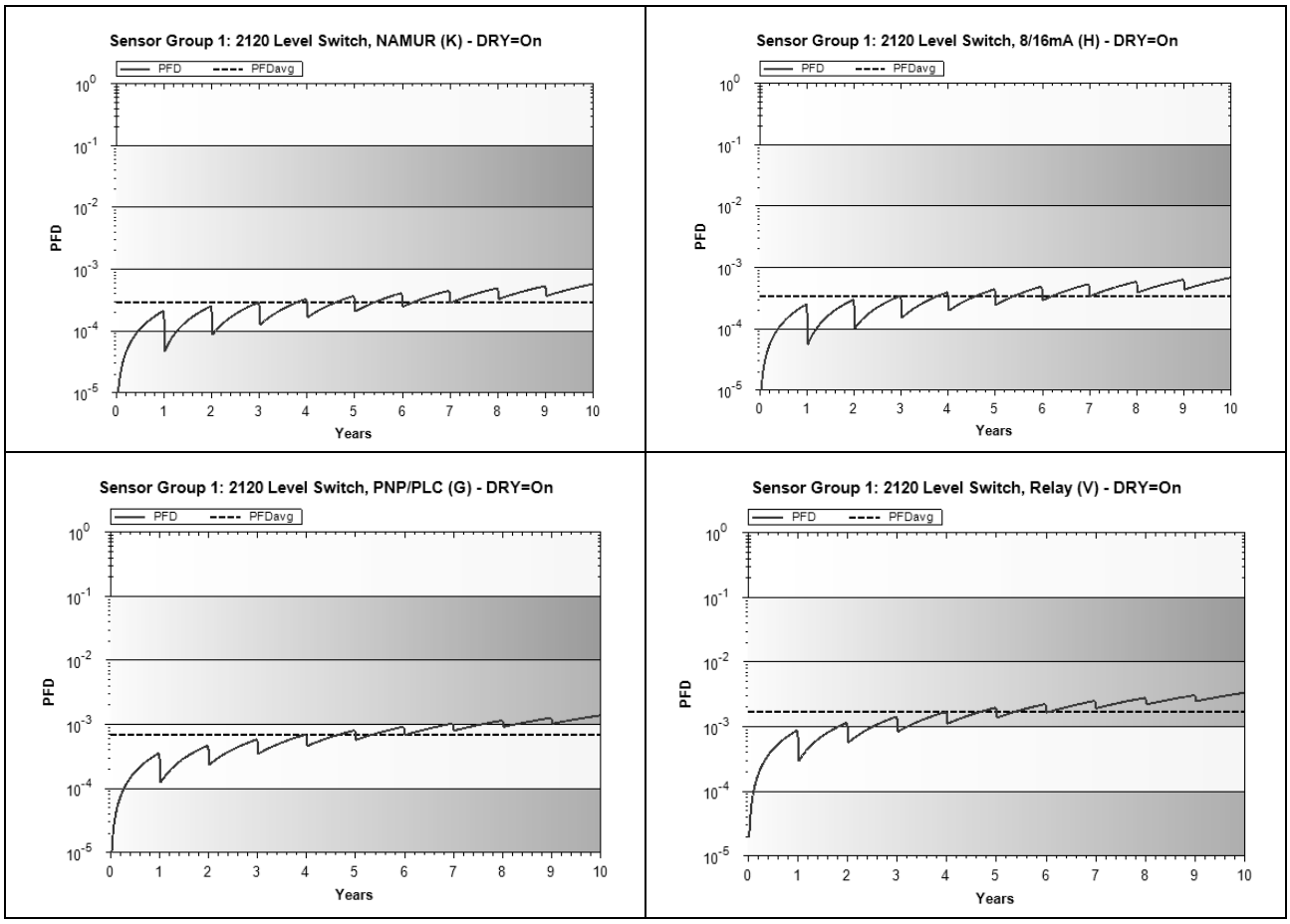


Figure 3 PFD_{AVG} value for a single, 2120 Level Switch with proof test intervals of 1 year using the Partial Proof Test.

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 SIL 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. This means that for a SIL 2 application, performing the Partial Proof Test with a 1-year Proof Test Interval on the 2120 Level Switch, NAMUR (K) - DRY = On produces a PFD_{AVG} approximately equal to 3% of the range. For the 2120 Level Switch, 8/16mA (H) - DRY = On the PFD_{AVG} is approximately equal to 3% of the range. For the 2120 Level Switch, PNP/PLC (G) - DRY = On the PFD_{AVG} is approximately equal to 7% of the range.

For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, performing the Partial Proof Test with a 1-year Proof Test Interval on the 2120 Level Switch, Relay (V) - DRY = On produces a PFD_{AVG} approximately equal to 2% of the range.

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 demand interval for operation made on a safety-related system is greater than twice the proof test interval.
Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
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 A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, 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 History:	V1, R6:	added PNP/PLC and Relay versions, Q14/11-048; changed per some requests in 25 Nov 2014 e-mail, changed per some requests in 20 Jan 2015 e-mail; 21 Jan 2015, Griff Francis
	V1, R5:	changed per customer requests in 11 Sept 2014 e-mail; 16 Oct 2014, Griff Francis
	V1, R4:	removed observe LED steps form Proof Tests, added higher life time for capacitors used on 8/16mA model.; 21 August 2014, Griff Francis
	V1, R3:	added second Proof Test, corrected Appendix A to show use of aluminum electrolytic capacitors: 15 August 2014, Griff Francis, Q14/08-015
	V1, R2:	made changes 1 and 4 requested in an e-mail sent 19 June 2014: 24 June 2014, Griff Francis
	V1, R1:	updated to IEC 61508:2010; converted to new report template; added 8/16mA model: 6 Jan 2014, Griff Francis, Q13/11-015
	V1, R0:	Created separate report for 2120 per client request, September 28, 2010
Author(s):	John Grebe, Griff Francis	

Review:	V1, R6 DRAFT:	Rosemount Measurement Limited, 20 January 2015
	V1, R3:	Rosemount Measurement Limited, 21 August 2014
	V0, R1:	Of combined 2100 models, Jon Keswick, August 20, 2010
	V0, R1:	Of combined 2100 models, Rudolf Chalupa (*exida*); March 4, 2009

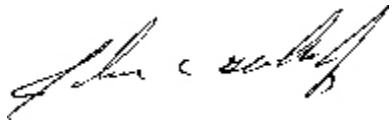
Release Status: Released to Rosemount Measurement Limited

7.3 Future enhancements

At request of client.

Release Signatures

Dr. William M. Goble, Principal Partner



John C. Grebe Jr., Principal Engineer

Griff Francis, Senior Safety Engineer

Appendix A Lifetime of Critical Components

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

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

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 11 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 11 Useful lifetime of components contributing to dangerous undetected failure rate

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

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

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

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

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

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

B.1 Suggested Full Proof Test

The suggested proof test described in Table 12 will detect at least 74% of possible DU failures in the 2120 Level Switch in the DRY = On mode. See Table 14 for a specific model and coverage combination.

Table 12 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 and verify the output switches to the OFF state within the expected time period as indicated by the setting of the Mode Switch.
5.	Change process conditions so tuning fork experiences the configured normal condition and verify the output switches to the ON state within the expected time period as indicated by the setting of the Mode Switch.
6.	Remove the bypass and otherwise restore normal operation.

B.2 Suggested Partial Proof Test

The suggested proof test described in Table 13 will detect at least 68% of possible DU failures in the 2120 Level Switch in the DRY = On mode. See Table 14 for a specific model and coverage combination.

Table 13 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 14 Combinations of Models and DU Coverages.

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

Appendix C *exida* Environmental Profiles

Table 15 *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	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 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[8]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[9]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[10]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[11]	G2	G3	G3	G3	G3	Compatible Material
Surge[12]						
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[13]						
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)[14]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

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