



Failure Modes, Effects and Diagnostic Analysis

Project:
Horizontal Float Switches

Company:
Mobrey Limited
Slough, Berks
UK

Contract Number: Q10/08-036
Report No.: EM 10/08-036 R001
Version V1, Revision R2, November 21, 2011
Steven Close

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 Horizontal Float Switches. 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 and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the level switch. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Mobrey Horizontal Float Switches operates on a magnetic principle. One permanent magnet forms part of a float assembly which rises and falls with changing liquid level. A second permanent magnet is positioned within the switch so that the adjacent poles of the two magnets repel each other through a non-magnetic diaphragm. A change of liquid level which moves the float through its permissible travel will cause the float magnet to move and repel the switch magnet to give the snap action operation. Switching is accomplished by the angular movement of the switch magnet being used to operate “push-rods”. These rods bear on contact blades and break one set of contacts while allowing the other set to make. The benefit of this arrangement is that contact force is independent of the magnet.

There are two types of switch mechanisms: 4-contact and 6-contact.

The 4-contact versions are types D and P. Type D has fine silver contacts; type P has gold-plated contacts.

The 6-contact versions are types D6, P6, H6 and B6. Type D6 has fine silver contacts; types P6, H6 and B6 have gold-plated contacts. Types H6 and B6 have a hermetically sealed cover and an inert gas fill. The detail construction of the 6-contact switch mechanisms is slightly different to that of the 4-contact.

Any switch mechanism can be fitted in any body with the exception of the S01, which cannot be fitted with H6 or B6 mechanisms. (The S01 has a deeper lid when fitted with D6 and P6 6-contact switch mechanisms)

There are several versions of floats, with detail differences in material, minimum SG and pressure rating. Higher-pressure types tend to be heavier and therefore have a higher minimum SG capability. These are listed in the schedule.

All the floats have a similar construction consisting of a float, welded together from thin metal pressings, welded to a float adaptor with a drilled hole for the pivot pin, and a welded magnet housing with magnet inside. The float on the F104 is attached to the float adaptor by means of a rigid rod. In general, any float can be used with any body and switch mechanism.

Table 1 is a schedule of part numbers that are included in this FMEDA.

Table 1 Schedule of Part Numbers

Element	Description	Reference
Body (Switch)	General Purpose (Aluminium Bronze Wetside)	01
	General Purpose (Stainless Steel Wetside)	36
	General Purpose (Stainless Steel Wetside)	190
	General Purpose (Stainless Steel Wetside)	440
	General Purpose (Stainless Steel Wetside)	441

	General Purpose (Stainless Steel Wetside)	424
	General Purpose (Stainless Steel Wetside)	425
	General Purpose (Stainless Steel Wetside)	489
	General Purpose (Stainless Steel Wetside)	490
	General Purpose (Stainless Steel Wetside)	428
	General Purpose (Stainless Steel Wetside)	429
	General Purpose (Stainless Steel Wetside)	430
	General Purpose (Stainless Steel Wetside)	431
	General Purpose (Stainless Steel Wetside)	432
	General Purpose (Stainless Steel Wetside)	417
	General Purpose (Stainless Steel Wetside)	418
	General Purpose (Stainless Steel Wetside)	419
	General Purpose (Stainless Steel Wetside)	433
	General Purpose (Stainless Steel Wetside)	434
	General Purpose (Stainless Steel Wetside)	488
	General Purpose (Stainless Steel Wetside)	435
	General Purpose (Stainless Steel Wetside)	436
	General Purpose (Stainless Steel Wetside)	437
	Hazardous Area	250
	Hazardous Area	275
	Hazardous Area	256
	Hazardous Area	257
	Hazardous Area	278
	Hazardous Area	251
	Hazardous Area	254
	Hazardous Area	260
	Hazardous Area	261
	Hazardous Area	253
	Hazardous Area	255
	Hazardous Area	269
	Hazardous Area	272
	Hazardous Area	268
	Hazardous Area	270
	Hazardous Area	271
Switch Mechanism	4 Contact - General	D
	4 Contact - Gold plated contacts	P
	6 Contact - General	D6
	6 Contact - Gold plated contacts	P6
	6 Contact - Hermetically sealed	H6
	6 Contact - Zone 2 areas	B6

Float		F84
		F185
		F93
		F96
		F98
		F104
		F106
		F107

Table 2 gives an overview of the different versions that were considered in the FMEDA of the level switch. Variations other than the switches are considered to have common failure rates.

Table 2 Version Overview

Option 1	4-contact versions - types D and P
Option 2	6-contact versions - types D6, P6, H6 and B6

The level switch is classified as a Type A¹ element according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the device has a Safe Failure Fraction between 0% and 60% and therefore may be used up to SIL 1 as a single device based on hardware architectural constraints.

The failure rates for the level switch are listed in Table 3 and Table 4.

Table 3 Failure rates level switch 4-contact versions - types D and P

Failure Category	Failure Rate (FIT)	
	MAX Detection	MIN Detection
Fail Safe Detected	0	0
Fail Safe Undetected	87	89
Fail Dangerous Detected	0	0
Fail Dangerous Undetected	195	193
Residual	34	34

¹ Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Table 4 Failure rates level switch, 6-contact versions - types D6, P6, H6 and B6

Failure Category	Failure Rate (FIT)	
	MAX Detection	MIN Detection
Fail Safe Detected	0	0
Fail Safe Undetected	167	169
Fail Dangerous Detected	0	0
Fail Dangerous Undetected	275	273
Residual	34	34

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 5 lists the failure rates for the level switch according to IEC 61508.

Table 5 Failure rates according to IEC 61508, 4-contact versions - types D and P (FIT)

Device	λ_{SD}	λ_{SU}^2	λ_{DD}	λ_{DU}	SFF ³
level switch, MAX Detection	0	87	0	195	30.9%
level switch, MIN Detection	0	89	0	193	31.6%

Table 6 Failure rates according to IEC 61508, 6-contact versions - types D6, P6, H6 and B6 (FIT)

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
level switch, MAX Detection	0	167	0	275	37.8%
level switch, MIN Detection	0	169	0	273	38.3%

A user of the 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 Residual failures are no longer included in the Safe Undetected failure category according to IEC 61508 ed2, 2010. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

³ Safe Failure Fraction needs to be calculated on (sub)system level

Table of Contents

Management Summary	2
1 Purpose and Scope.....	7
2 Project Management	8
2.1 <i>exida</i>	8
2.2 Roles of the parties involved	8
2.3 Standards and Literature used.....	8
2.4 <i>exida</i> Tools Used	9
2.5 Reference documents.....	9
2.5.1 Documentation provided by Mobrey Limited.....	9
2.5.2 Documentation generated by <i>exida</i>	10
3 Product Description	11
4 Failure Modes, Effects, and Diagnostic Analysis.....	14
4.1 Failure Categories description.....	14
4.2 Methodology – FMEDA, Failure Rates	14
4.2.1 FMEDA	14
4.2.2 Failure Rates.....	15
4.3 Assumptions	15
4.4 Results.....	16
5 Using the FMEDA Results.....	18
5.1 PFD _{AVG} Calculation level switch	18
6 Terms and Definitions	19
7 Status of the Document.....	20
7.1 Liability.....	20
7.2 Releases.....	20
7.3 Release Signatures.....	21
Appendix A Lifetime of Critical Components.....	22
Appendix B Proof tests to reveal dangerous undetected faults	23
B.1 Suggested Proof Test	23
Appendix C <i>exida</i> Environmental Profiles	24

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 ISO 13849-1. 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 per 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 ISO 13849-1. 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 the Failure Modes, Effects and Diagnostic Analysis carried out on the 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 / IEC 61511.

2.4 **exida** Tools Used

[T1]	2.5.1.7	exSILentia
------	---------	------------

2.5 Reference documents

2.5.1 Documentation provided by Mobrey Limited

[D1]	Doc # IP101, October 2010	Specification Sheet, Mobrey magnetic level switches
[D2]	Doc # M310-1, November 2006	Instruction Manual / Safety Manual
[D3]	Doc # 82266, Rev 4, November 2, 2005	Drawing, S01DB/F84 Switch/Float Combination
[D4]	Doc # PL S01DB/F84, Rev 9, March 13, 2007	Parts List, S01DB/F84 Switch/Float Combination
[D5]	Doc # F84, Rev 17, July 14, 2003	Drawing, Float Subassembly
[D6]	Doc # PL F84, Rev 10, July 14, 2003	Parts List, Float Subassembly
[D7]	Doc # 82265, Rev 4, May 19, 1999	Drawing, Switch Assembly – S01DB Head
[D8]	Doc # PL S01DB, Rev 9, April 26, 2007	Parts List, S01DB Head
[D9]	Doc # G3450, Rev 12, June 26, 2001	Drawing, Magnetic Switch Insert (4 Contact)
[D10]	Doc # PL G3450, Rev 8, June 14, 2005	Parts List, Magnetic Switch Insert (4 Contact)
[D11]	Doc # G4881, Rev 8, February 10, 2003	Drawing, Body Maching - Dumpy
[D12]	Doc # G3614, Rev 5, February 1989	Drawing, Fork (Machining)
[D13]	Doc # G3613, Rev 8, July 29, 1997	Drawing, Switch Base Moulding (4 Contact)
[D14]	Doc # G3755, Rev 8, October 30, 1997	Drawing, Shell Half
[D15]	Doc # G3616, Rev 1, April 1, 1981	Insulation Plate
[D16]	Doc # G3615, Rev 1, April 1, 1981	Magnet Housing & Bushing Assembly

[D17]	Doc # G3615 Sh2, Rev 1, April 1, 1981	Magnet Housing Machining
[D18]	Doc # G3618, Rev 4, July 17, 1991	Push Rod Assembly
[D19]	Doc # G3622, Rev 1, April 1, 1981	Terminal
[D20]	Doc # G3624/C, Rev 5, May 30, 2006	Magnet Housing Casting Assembly
[D21]	Doc # G3717, Rev 16, December 22, 1999	Pivot – Push Rod
[D22]	Doc # G3828, Rev 5, March 7, 1997	Bush, Push Rod
[D23]	Doc # G3952, Rev 6, March 12, 1997	Bush, Magnet Pivot

2.5.2 Documentation generated by *exida*

[R1]	Q10-08-036 Float Assembly.xls, August 23, 2011	Failure Modes, Effects, and Diagnostic Analysis – level switch Float Assembly
[R2]	Q10-08-036 Magnetic Switch Insert- D – P, August 23, 2011	Failure Modes, Effects, and Diagnostic Analysis – Switch Insert D & P
[R3]	Q10-08-036 Magnetic Switch Insert - D6-P6-H6-B6.efm, August 23, 2011	Failure Modes, Effects, and Diagnostic Analysis – Switch Insert D6, P6, H6 & B6.
[R4]	Q10-08-036_Switch Assembly.efm, August 23, 2011	Failure Modes, Effects, and Diagnostic Analysis – Overall Assembly
[R5]	Q10-08-036 Mobrey Level Switch FMEDA Summary.xls, August 23, 2011	Failure Modes, Effects, and Diagnostic Analysis - Summary –level switch
[R6]	EM 10-06-036 R001 V1 R1 Float Switch.doc, 11/21/2011	FMEDA report, level switch (this report)

3 Product Description

The Mobrey Horizontal Float Switches operates on a magnetic principle. One permanent magnet forms part of a float assembly which rises and falls with changing liquid level. A second permanent magnet is positioned within the switch so that the adjacent poles of the two magnets repel each other through a non-magnetic diaphragm. A change of liquid level which moves the float through its permissible travel will cause the float magnet to move and repel the switch magnet to give the snap action operation. Switching is accomplished by the angular movement of the switch magnet being used to operate “push-rods”. These rods bear on contact blades and break one set of contacts while allowing the other set to make. The benefit of this arrangement is that contact force is independent of the magnet.

There are two types of switch mechanisms: 4-contact and 6-contact.

The 4-contact versions are types D and P. Type D has fine silver contacts; type P has gold-plated contacts.

The 6-contact versions are types D6, P6, H6 and B6. Type D6 has fine silver contacts; types P6, H6 and B6 have gold-plated contacts. Types H6 and B6 have a hermetically sealed cover and an inert gas fill. The detail construction of the 6-contact switch mechanisms is slightly different to that of the 4-contact.

Any switch mechanism can be fitted in any body with the exception of the S01, which cannot be fitted with H6 or B6 mechanisms. (The S01 has a deeper lid when fitted with D6 and P6 6-contact switch mechanisms)

There are several versions of floats, with detail differences in material, minimum SG and pressure rating. Higher-pressure types tend to be heavier and therefore have a higher minimum SG capability. These are listed in the schedule.

All the floats have a similar construction consisting of a float, welded together from thin metal pressings, welded to a float adaptor with a drilled hole for the pivot pin, and a welded magnet housing with magnet inside. The float on the F104 is attached to the float adaptor by means of a rigid rod. In general, any float can be used with any body and switch mechanism.

Table 7 is a schedule of part numbers that are included in this FMEDA.

Table 7 Schedule of Part Numbers

Element	Description	Reference
Body (Switch)	General Purpose (Aluminium Bronze Wetside)	01
	General Purpose (Stainless Steel Wetside)	36
	General Purpose (Stainless Steel Wetside)	190
	General Purpose (Stainless Steel Wetside)	440
	General Purpose (Stainless Steel Wetside)	441
	General Purpose (Stainless Steel Wetside)	424
	General Purpose (Stainless Steel Wetside)	425
	General Purpose (Stainless Steel Wetside)	489
	General Purpose (Stainless Steel Wetside)	490
	General Purpose (Stainless Steel Wetside)	428
	General Purpose (Stainless Steel Wetside)	429
	General Purpose (Stainless Steel Wetside)	430

	General Purpose (Stainless Steel Wetside)	431
	General Purpose (Stainless Steel Wetside)	432
	General Purpose (Stainless Steel Wetside)	417
	General Purpose (Stainless Steel Wetside)	418
	General Purpose (Stainless Steel Wetside)	419
	General Purpose (Stainless Steel Wetside)	433
	General Purpose (Stainless Steel Wetside)	434
	General Purpose (Stainless Steel Wetside)	488
	General Purpose (Stainless Steel Wetside)	435
	General Purpose (Stainless Steel Wetside)	436
	General Purpose (Stainless Steel Wetside)	437
	Hazardous Area	250
	Hazardous Area	275
	Hazardous Area	256
	Hazardous Area	257
	Hazardous Area	278
	Hazardous Area	251
	Hazardous Area	254
	Hazardous Area	260
	Hazardous Area	261
	Hazardous Area	253
	Hazardous Area	255
	Hazardous Area	269
	Hazardous Area	272
	Hazardous Area	268
	Hazardous Area	270
	Hazardous Area	271
Switch Mechanism	4 Contact - General	D
	4 Contact - Gold plated contacts	P
	6 Contact - General	D6
	6 Contact - Gold plated contacts	P6
	6 Contact - Hermetically sealed	H6
	6 Contact - Zone 2 areas	B6
Float		F84
		F185
		F93
		F96
		F98
		F104

		F106
		F107



Figure 1 level switch, S01/F84

The level switch is classified as a Type A⁴ element according to IEC 61508, having a hardware fault tolerance of 0.

Table 8 gives an overview of the different versions that were considered in the FMEDA of the level switch. Variations other than the switches are considered to have common failure rates.

Table 8 Version Overview

Option 1	4-contact versions - types D and P
Option 2	6-contact versions - types D6, P6, H6 and B6

⁴ Type A element: “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Mobrey Limited and is documented in [R1] - [R5].

4.1 Failure Categories description

In order to judge the failure behavior of the level switch, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the output corresponds to a tripped condition (high liquid level for MAX detection, low liquid level for MIN detection)
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.

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.

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 [N2] 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 were chosen to match *exida* Profile 4 for process wetted parts and Profile 3 for all others. see Appendix C. 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”. 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 level switch.

- Only a single component failure will fail the entire 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 4 for process wetted parts and profile 3 for all others 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
- Materials are compatible with process conditions

- The device is installed per manufacturer's instructions
- External power supply failure rates are not included

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the level switch FMEDA.

Table 9 Failure rates level switch, 4-contact versions - types D and P

Failure Category	Failure Rate (FIT)	
	MAX Detection	MIN Detection
Fail Safe Detected	0	0
Fail Safe Undetected	87	89
Fail Dangerous Detected	0	0
Fail Dangerous Undetected	195	193
Residual	34	34

Table 10 Failure rates level switch, 6-contact versions - types D6, P6, H6 and B6

Failure Category	Failure Rate (FIT)	
	MAX Detection	MIN Detection
Fail Safe Detected	0	0
Fail Safe Undetected	167	169
Fail Dangerous Detected	0	0
Fail Dangerous Undetected	275	273
Residual	34	34

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

Table 11 lists the failure rates for the level switch according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However as the level switch is only one part of a (sub)system, the SFF should be calculated for the entire sensor / logic / final element combination. 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 11 Failure rates according to IEC 61508, 4-contact versions - types D and P (FIT)

Device	λ_{SD}	λ_{SU}^5	λ_{DD}	λ_{DU}	SFF ⁶
level switch , MAX Detection	0	87	0	195	30.9%
level switch , MIN Detection	0	89	0	193	31.6%

Table 12 Failure rates according to IEC 61508, 6-contact versions - types D6, P6, H6 and B6

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
level switch , MAX Detection	0	167	0	275	37.8%
level switch , MIN Detection	0	169	0	273	38.3%

The architectural constraint type for the level switch is A. 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.

⁵ It is important to realize that the Residual failures are no longer 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

⁶ 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.

5.1 PFD_{AVG} Calculation level switch

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) level switch with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. Table 13 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 13 Sample PFD_{AVG} Results

Device	Proof Test Coverage	PFD _{AVG}	% of SIL 1 Range
4-contact versions - types D and P	99%	9.3E-04	0.9%
6-contact versions - types D6, P6, H6 and B6	99%	1.31E-03	1.3%

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

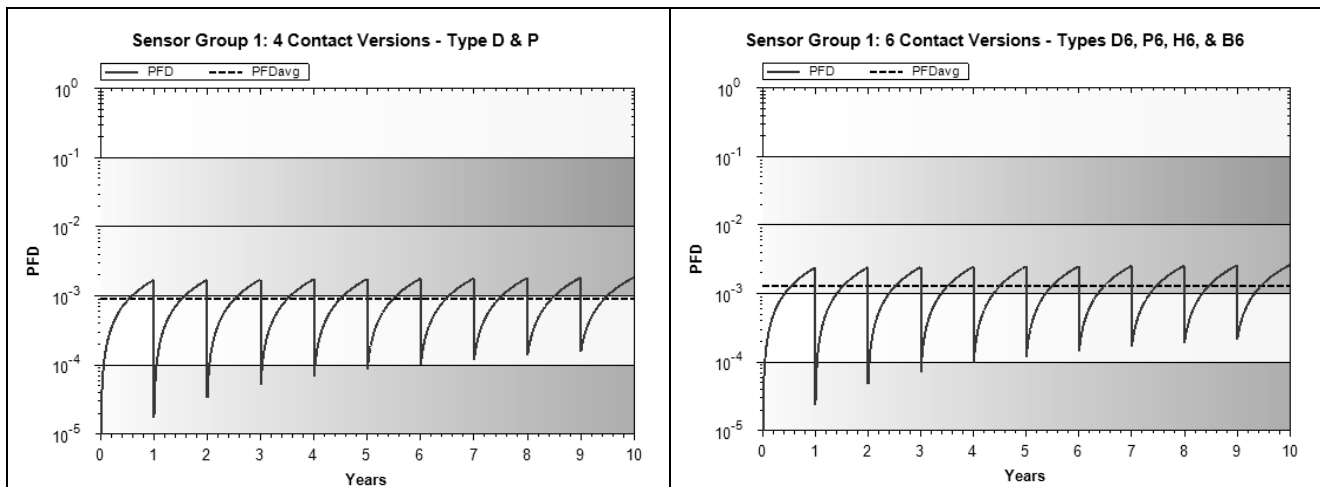


Figure 2: PFD_{avg} value for a single, level switch with proof test interval of 1 year.

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 1 applications, the PFD_{AVG} value needs to be $\geq 10^{-2}$ and $< 10^{-1}$. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of the level switch is approximately equal to 0.9% of the range for 4-contact versions - types D and P and 1.3% for 6-contact versions - types D6, P6, H6 and B6.

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 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: V1

Revision: R2

Version History: V1, R2: Edits per request of Mobrey Limited, November 21, 2011

V1, R1: Released to Mobrey Limited, August 29, 2011

V0, R1: Draft; August 29, 2011

Author(s): Steven Close

Review: V0, R1: William Goble, August 29, 2011

Release Status: Released

Future Enhancements

At request of client.

7.3 Release Signatures

A handwritten signature in black ink, appearing to read "William M. Goble", written in a cursive style.

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink, appearing to read "Steven Close", written in a cursive style.

Steven Close, 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 lifetime⁷ 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.

Based on general field failure data a useful life period of approximately 10 to 15 years is expected for the level switch.

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 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

The suggested proof test consists of a full range cycle of the sensor, see Table 14. This test will detect > 99% of possible DU failures in the device.

NOTE: the test must be performed by actually changing the liquid level; manually moving the float may not detect problems with leaky float or binding.

Table 14 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Increase the liquid level to above the switch's threshold and confirm proper output.
3.	Decrease the liquid level to below the switch's threshold and confirm proper output.
4.	Remove the bypass and otherwise restore normal operation

Appendix C exida Environmental Profiles

Table 15 *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. Non-process wetted components of valves and actuators.	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. Process wetted components.	D1	25	30	35