Failure Modes, Effects and Diagnostic Analysis Review

Project:
Jupiter JM4 Magnetostrictive Level Transmitter

Company:
Magnetrol International
Aurora, IL
USA

Contract Number: Q14/02-065
Report No.: MAG 14/02-065 R001
Version V2, Revision R2, September 17, 2014
Rudolf Chalupa

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Jupiter JM4 Magnetostrictive Level Transmitter, hardware and software revision per 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 Jupiter JM4. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Jupiter JM4 Magnetostrictive Level Transmitter provides an analog output proportional to the level being measured. Its primary components are the electronics assembly, the probe assembly containing the magnetostrictive wire and sensor, and the float(s).Table 1 gives an overview of the different versions that were considered in the FMEDA of the Jupiter JM4.

Table 1 Version Overview

Single Float	One float
Dual Float	Two floats for determining two levels

The Jupiter JM4 is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the has a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The failure rates for the Jupiter JM4 are listed in Table 2.

Table 2 Failure rates Jupiter JM4 Single Float

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		127
Fail Dangerous Detected		1113
Fail Detected (detected by internal diagnostics)	968	
Fail High (detected by logic solver)	70	
Fail Low (detected by logic solver)	75	
Fail Dangerous Undetected		92
No Effect		316
Annunciation Undetected		5

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

Table 3 Failure rates Jupiter JM4 Dual Float

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		129
Fail Dangerous Detected		1113
Fail Detected (detected by internal diagnostics)	968	
Fail High (detected by logic solver)	70	
Fail Low (detected by logic solver)	75	
Fail Dangerous Undetected		110
No Effect		316
Annunciation Undetected		5

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 4 lists the failure rates for the Jupiter JM4 according to IEC 61508, ed2, 2010.

Table 4 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
Single Float	0	127	1113	92	93.1%
Dual Float	0	129	1113	110	91.9%

A user of the Jupiter JM4 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, if needed, is to be calculated on an element 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 review carried out on the Jupiter JM4. From this, failure rates and example PFD_{AVG} values may be calculated.

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

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

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety 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

Magnetrol International	Manufacturer of the Jupiter JM4
Magnetrol International	Performed the hardware assessment
Magnetrol International	contracted *exida* in February 2014 with the hardware review 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]	7.1.18	FMEDA Tool
[T2]	3.2.1.896	exSILentia

2.5 Reference documents

2.5.1 Documentation provided by Magnetrol International

[D1]	Doc # ORI-148.6, December 2011	Brochure
[D2]	Doc # 094-6067, Rev H, November 21, 2013	Schematic Drawing, Digital Board
[D3]	Doc # 094-6076, Rev B, September 2013	Schematic Drawing, Analog Board
[D4]	Doc # 094-6077, Rev B, February 2014	Schematic Drawing, Preamp Board
[D5]	Doc # 094-6073, Rev C, March 2012	Schematic Drawing, Wiring Board
[D6]	JupiterJM4-Digital-Board_FMEDA.efm, 2014-03-21	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Digital Board
[D7]	JupiterJM4AnalogRevB_FMEDA 2014-08-07-PTC-Changes.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Analog Board
[D8]	JupiterJM4PreampRevC_FMEDA 2014-08-07-PTC-changes.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Preamp Board
[D9]	Model 706 Wiring Board07272012_PTC.efm, 2014-03-21	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Wiring Board
[D10]	JUPITER_JM4_Housing_FMEDA.xls, 2014-03-21	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Housing
[D11]	JUPITER_JM4_Probe_FMEDA.efm, 2014-03-21	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Probe
[D12]	JUPITER_JM4_Probe_TwoFloat_FMEDA.efm, 2014-03-21	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Probe, Two Float
[D13]	FMEDA Results Combined Jupiter JM4 2014-08-07ProposedProofTests.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary –Jupiter JM4
[D14]	Fault Injection List Magnetrol Jupiter JM4	Fault Injection Test Report

	2014-07-30.xlsx	
[D15]	Proof Test for Jupiter JM4.docx, 2014-08-08	Recommended proof test

2.5.2 Documentation generated by *exida*

[R1]	JupiterJM4-Digital-Board_FMEDA 2014-08-05.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Digital Board
[R2]	Jupiter4XAnalogRevB_FMEDA 2014-09-17.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Analog Board
[R3]	Jupiter4XPreampRevC_FMEDA 2014-09-04.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Preamp Board
[R4]	Model 706 Wiring Board07272012_PTC 2014-08-05.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Wiring Board
[R5]	JUPITER_JM4_Housing_FMEDA 2014-08-05.xls	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Housing
[R6]	JUPITER_JM4_Probe_FMEDA 2014-08-05.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Probe
[R7]	JUPITER_JM4_Probe_TwoFloat_FMEDA 2014-08-05.efm	Failure Modes, Effects, and Diagnostic Analysis – Jupiter JM4 Probe, Two Float
[R8]	FMEDA Results Combined Jupiter JM4 2014-09-17.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary –Jupiter JM4
[R9]	Fault Injection List Magnetrol Jupiter JM4 2014-07-30.xlsx	Fault Injection Test List
[R10]	MAG 14-02-065 R001 V2R2 FMEDA Jupiter JM4.doc, 09/17/2014	FMEDA report, Jupiter JM4 (this report)

3 Product Description

The Jupiter JM4 Magnetostrictive Level Transmitter provides an analog output proportional to the level being measured. Its primary components are the electronics assembly, the probe assembly containing the magnetostrictive wire and sensor, and the float(s).

The Jupiter JM4 utilizes the engineering principle of magnetostriction and the effect of a magnetic field on the magnetostrictive wire as the basis for operation.

Figure 1 Jupiter JM4, Parts included in the FMEDA

Table 5 gives an overview of the different versions that were considered in the FMEDA of the Jupiter JM4.

Table 5 Version Overview

Single Float	One float
Dual Float	Two floats for determining two levels

The Jupiter JM4 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 as performed based on the documentation obtained from Magnetrol International and is documented in [R10].

When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level, see Fault Injection Test Report [D14].

4.1 Failure categories description

In order to judge the failure behavior of the Jupiter JM4, the following definitions for the failure of the device were considered.

Fail-Safe State	Failure that deviates the process signal or the actual output by more than 2% of span, drifts toward the user defined threshold (Trip Point) and that leaves the output within active scale.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (3.6 or 22 mA, field selectable).
Fail Dangerous	Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within active scale.
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.
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current (> 21.5 mA).
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.8 mA).
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.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. 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 are from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which were 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 were chosen to match *exida* Profile 2, see Appendix C. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Magnetrol International. 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 Jupiter JM4.

- Only a single component failure will fail the entire Jupiter JM4.
- 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 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- 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.
- On the dual float version only the level indicated by the analog output is reviewed.
- Worst-case internal fault detection time is 10 seconds.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Jupiter JM4 FMEDA.

Table 6 Failure rates Jupiter JM4 Single Float

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		127
Fail Dangerous Detected		1113
Fail Detected (detected by internal diagnostics)	968	
Fail High (detected by logic solver)	70	
Fail Low (detected by logic solver)	75	
Fail Dangerous Undetected		92
No Effect		316
Annunciation Undetected		5

Table 7 Failure rates Jupiter JM4 Dual Float

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		129
Fail Dangerous Detected		1113
Fail Detected (detected by internal diagnostics)	968	
Fail High (detected by logic solver)	70	
Fail Low (detected by logic solver)	75	
Fail Dangerous Undetected		110
No Effect		316
Annunciation Undetected		5

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

Table 8 lists the failure rates for the Jupiter JM4 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 8 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF[6]
Single Float	0	127	1113	92	93.1%
Dual Float	0	129	1113	110	91.9%

[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, if needed, is to be calculated on an element level

5 Using the FMEDA Results

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

5.1 PFD_{AVG} calculation Jupiter JM4

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) Jupiter JM4 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 9 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 9 Sample PFD_{AVG} Results

Device	Proof Test Coverage	PFD_{AVG}	% of SIL 2 Range
Jupiter JM4 - Single Float	83%	1.97E-03	20%
Jupiter JM4 - Dual Float	86%	1.96E-03	20%

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

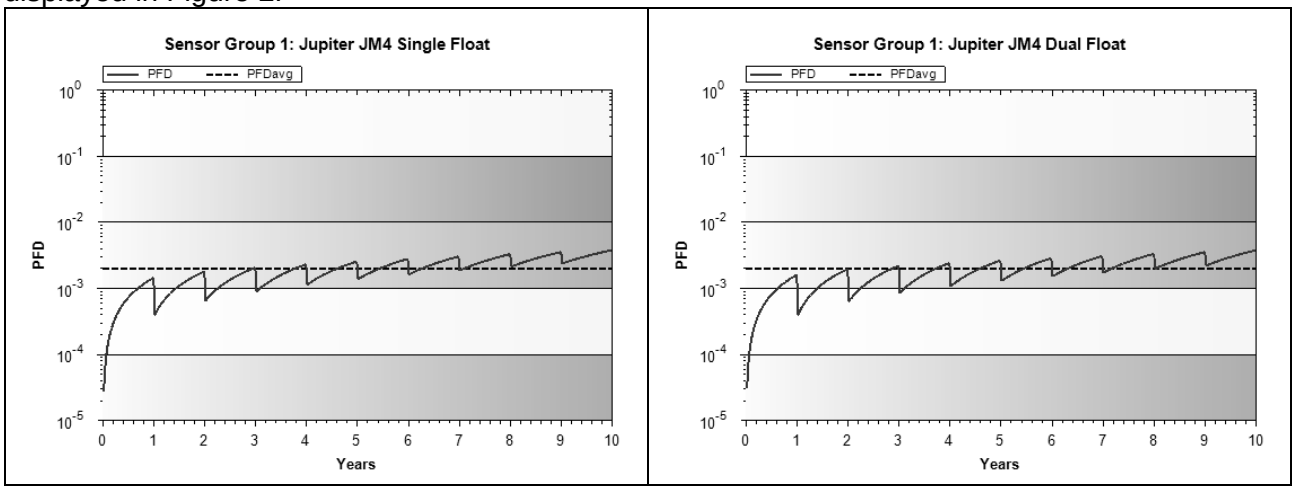


Figure 2 PFD_{AVG} value for a single, Jupiter JM4 with proof test intervals of 1 year.

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 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval of the Jupiter JM4 is approximately equal to 20% 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

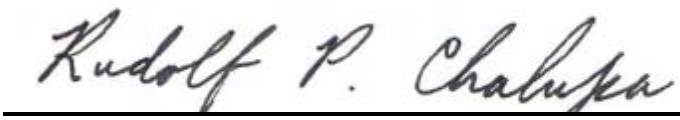
Version:	V2	
Revision:	R2	
Version History:	V2, R2:	Updated fault detection time, proof test coverage, 2014-09-17
	V2, R1:	Updated per client comments, 2014-09-04
	V1, R1:	Released to Magnetrol International; 2014-08-06
	V0, R1:	Draft; 2014-08-05
Author(s):	Rudolf Chalupa	
Review:	V0, R1:	Griff Francis (*exida*); 2014-08-06
Release Status:	Released to Magnetrol International	

7.3 Future enhancements

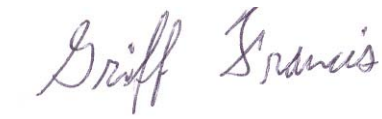
At request of client.

7.4 Release signatures

Dr. William M. Goble, Principal Partner



Rudolf P. Chalupa, Senior Safety 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 17 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 10 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 Jupiter JM4 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.

[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 Proof Test

The suggested Jupiter JM4 proof test consists of a setting the output to the min and max, and a calibration check, see Table 11.

Table 11 Suggested Proof Test

Step	Action
1.	Bypass the safety PLC or take other action to avoid a false trip
2.	Remove power from the Unit. (This clears any potential soft RAM errors.) Inspect the Unit in detail outside and inside for physical damage or evidence of environmental or process leaks. a. Inspect the exterior of the unit housing. If there is any evidence of physical damage that may impact the integrity of the housing and the environmental protection, the unit should be repaired or replaced. b. Inspect the interior of the unit. Any evidence of moisture, from process or environment, is an indication of housing damage, and the unit should be repaired or replaced.
3.	Restore power to the Unit. Use the Unit's "DIAGNOSTICS" menu to observe "Present Status" and to review "EVENT HISTORY". Up to 10 events are stored. The events will be date and time stamped if the internal clock is set and running. It is suggested that the internal clock be set at the time of commissioning of the unit. If the clock is set at the time of the proof test event times are calculated. a. Observe the "Present Status". "Present Status" should be "OK". b. Review the "EVENT HISTORY". i. Messages in the "EVENT HISTORY" must be investigated and understood. ii. Corrective actions should be taken for critical messages that indicate performance may be affected.
4.	Use the Unit's "DIAGNOSTICS" menu to perform a loop current test. Choose the menu "DIAGNOSTIC/ADVANCE DIAGNOSTICS/TRANSMITTER TESTS/Analog Output Test" to change the output loop current and confirm the actual loop current matches the value chosen. a. Send a HART command to the transmitter (or use the local user interface) to go to high alarm current output, 22mA, and verify that the analog current reaches that value. i. This step tests for compliance voltage problems such as low supply voltage or increased wiring resistance. ii. This also tests for current loop control circuitry and adjustment problems. b. Send a HART command to the transmitter (or use the local user interface) to go to low alarm current output, 3.6mA, and verify that the analog current reaches that value. i. This step tests for high quiescent current and supply voltage problems. ii. This also tests for current loop control circuitry and adjustment problems. c. Exit the "Analog Output Test" and confirm that the output returns to original state, with the proper loop current as indicated and controlled by the unit.
5.	Use the "DIAGNOSTICS" menu to observe the present Echo Curve and document typical performance values. Confirm that the ECHO Waveform is normal. The ECHO curve is dependent on the probe used and the level of the process on the probe. It is recommended that a typical ECHO curve be saved at commissioning. Comparison of the ECHO curve at proof test to one stored at the time of commissioning gives additional confidence of the normal operation of the unit. Use of digital communications (HART enhanced DD or DTM) is necessary for comparison of echo curves. For a dual float unit repeat the steps below for the second float and document "Upr Echo Strength" and "Ifc Echo Strength" as well as "Upr Noise / Threshold" and "Ifc Noise / Threshold".

	a. Move the process level so the float is located at a distance of approximately 33% of probe length from the connector end of the probe. b. Choose the menu “DIAGNOSTICS/ECHO CURVES/ View Echo Curve”. i. Observe the present Echo Curve, identify the characteristic portions of the waveform related to the top of the probe and float location. ii. Confirm that signal from the float appears normal and is located as expected. iii. Verify that the baseline of the waveform is normal and does not have evidence of excessive noise. iv. If possible compare to Echo curve from commissioning to assure that performance has not changed significantly. c. Choose the menu “DIAGNOSTICS/ADVANCED DIAGNOSTICS/ INTERNAL VALUES”. i. Observe and record: Upper ___ Interface 1. Echo Strength _____ _____ 2. Lvl Noise / Threshold _____ _____ ii. Confirm that these values match the values observed at commissioning of the unit and/or at previous Proof Tests. 1. Echo Strength change is less than +/- 15. 2. Lvl Noise / Threshold is less than +/- 15.
6.	Perform a two point calibration check of the transmitter by applying level to two points on the probe and compare the transmitter display reading and the current level value to a know reference measurement.
7.	If the calibration is correct the proof test is complete. Proceed to step 9.
8.	If the calibration is incorrect, remove the transmitter and probe from the process. Inspect the probe for build-up or clogging. Clean the probe, if necessary. Perform a bench calibration check by moving the float to two points on the probe. Measure the level from the bottom of the probe to the points and compare to the transmitter display and current level readings. a. If the calibration is off by more than 1%, call the factory for assistance. b. If the calibration is correct, the proof test is complete. Re-install the probe and transmitter and proceed to step 9.
9.	Restore the loop to full operation.
10.	Remove the bypass from the safety PLC or otherwise restore normal operation

B.2 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in **Table 12.**

Table 12 Proof Test Coverage

Device	Proof Test Coverage
Jupiter JM4 - Single Float	83%
Jupiter JM4 - Dual Float	86%

Appendix C *exida* Environmental Profiles

Table 13 *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