Failure Modes, Effects and Diagnostic Analysis

Project:
Eclipse Model 706 GWR Level Transmitter

Company:
Magnetrol International
Downers Grove, IL
USA

Contract Number: Q15-12-025
Report No.: MAG Q15-12-025 R001
Version V1, Revision R1, February 10, 2016
John C. Grebe Jr.

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 Eclipse Model 706 GWR Level Transmitter. The hardware version is defined by the assembly drawings in section 2.5. The software version is 1.0gA. 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 Model 706-511*-***. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

Model 706-511*-*** is a loop-powered, 24 VDC level transmitter, based on Guided Wave Radar (GWR) technology. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. The analog output meets NAMUR NE 43 (3.8mA to 20.5mA usable). The transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either low or high upon internal detection of a failure (output state is programmable). The device can be equipped with or without display.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Model 706-511*-***.

Table 1 Version Overview

Option 1	Model 706-511*-***

The Model 706-511*-*** is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H (see Section 5.2). Therefore the Model 706-511*-*** meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The analysis shows that the Model 706-511*-*** 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.

Based on the assumptions listed in 4.3, the failure rates for the Model 706-511*-*** are listed in section 4.4.

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

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.

A user of the Model 706-511*-*** can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

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

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Model 706-511*-***. 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.

A 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 400 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 the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

2.2 Roles of the parties involved

Magnetrol International	Manufacturer of the Model 706-511*-***
exida	Performed the hardware assessment

Magnetrol International contracted *exida* in December 2015 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, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 *exida* tools used

[T1]	V7.1.17	*exida* FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by Magnetrol International

[D1]	094-6067, Rev L, Oct 2014	Schematic, ECLIPSE 4X DIGITAL BOARD
[D2]	094-6068, Rev H, Nov 2012	Schematic, ANALOG BOARD "ECLIPSE 706" (SWEEP GENERATOR)
[D3]	094-6073, Rev C, March 2012	Schematic, WIRING BOARD "ECLIPSE 706"
[D4]	030-9159, Rev AA, Jan 2016	Assembly and BOM, HART DIGITAL PC BOARD
[D5]	030-9160, Rev H, Nov 2012	Assembly and BOM, ANALOG PC BOARD
[D6]	030-9165, Rev F, Oct 2014	Assembly and BOM, WIRING BOARD
[D7]	706-Digital-Board-RevL-FMEDA 2016-01-29.efm	FMEDA with Proof Test Coverage, Digital Board
[D8]	Eclipse4X-Analog-Board Rev H_PTC_2016-01-29.efm	FMEDA with Proof Test Coverage, Analog Board
[D9]	Model 706 Wiring Board07272012_PTC.efm	FMEDA with Proof Test Coverage, Wiring Board
[D10]	Eclipse_706_Housing_PTC_2016-01-29.efm	FMEDA with Proof Test Coverage, Housing
[D11]	Eclipse4X-7Y7-Probe_PTC_2016-01-29.efm	FMEDA with Proof Test Coverage, Probe
[D12]	Model_Model706_SIL_Summary29Jan2016.xlsx	FMEDA Summary with Proof Test Coverage
[D13]	Fault injection testing schematics 10_5_12.pdf	Fault injection points and results on Analog Board

2.5.2 Documentation generated by *exida*

[R1]	706-Digital-Board-RevL-FMEDA 2016-01-292-JCG.efm	FMEDA with Proof Test Coverage including exida updates, Digital Board
[R2]	Model_Model706_SIL_Summary6Feb2016.xlsx	FMEDA Summary with Proof Test Coverage including exida updates
[R3]	FMEDA.xls, Rev, date	Failure Modes, Effects, and Diagnostic Analysis – Model 706-511*-***
[R4]	MAG 15-12-025 R001 V0R1 FMEA Eclipse 706.doc, 20 May 2016	FMEDA report, Model 706-511*-*** (this report)

3 Product Description

Model 706-511*-*** is a loop-powered, 24 VDC level transmitter, based on Guided Wave Radar (GWR) technology. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. The analog output meets NAMUR NE 43 (3.8mA to 20.5mA usable). The transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either low or high upon internal detection of a failure (output state is programmable). The device can be equipped with or without display.

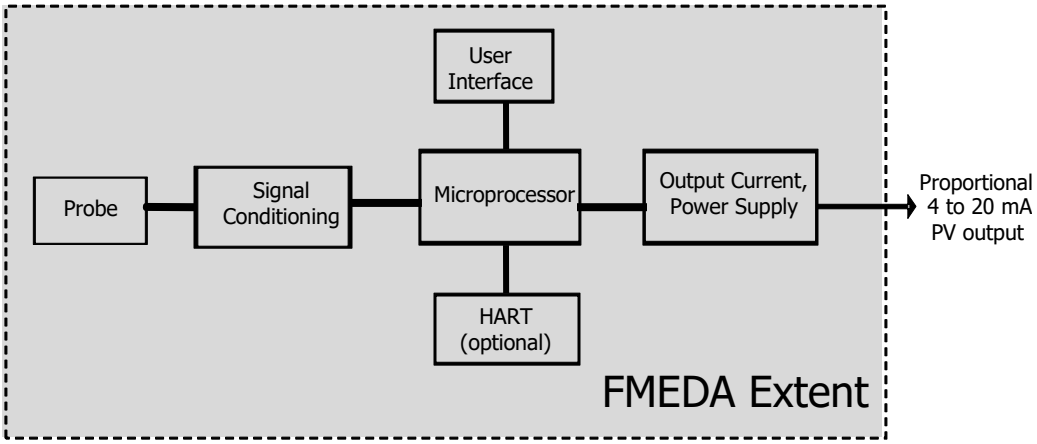


Figure 1 Model 706-511*-***, Parts included in the FMEDA

Guided Wave Radar is based upon the principle of TDR (Time Domain Reflectometry). TDR utilizes pulses of electromagnetic energy transmitted down a probe. When a pulse reaches a surface that has a higher dielectric than the air/vapor in which it is traveling, the pulse is reflected. An ultra high-speed timing circuit precisely measures the transit time and provides an accurate level measurement.

The Guided Wave Radar (GWR) probe must match the application. The probe configuration establishes fundamental performance characteristics. Coaxial, twin element (rod or cable), and single element (rod or cable) are the three basic configurations.

Table 2 gives an overview of the different versions that were considered in the FMEDA of the Model 706-511*-***.

Table 2 Version Overview

Option 1	Model 706-511*-***

The Model 706-511*-*** is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.5.1 and is documented in [R1] to [R4].

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

4.1 Failure categories description

In order to judge the failure behavior of the Model 706-511*-***, 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 the 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.
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 the 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 mA).
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.6 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.
External Leakage	Failure that causes process fluids to leak outside of the valve; External Leakage is not considered part of the safety function and therefore this failure rate is not included in the Safe Failure Fraction calculation.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation needed when Route 2_H failure data is not available.

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).

External leakage failure rates do not directly contribute to the reliability of a component but should be reviewed for secondary safety and environmental issues.

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 100 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 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 wearout 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. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. 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.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Model 706-511*-***.

- Only a single component failure will fail the entire Model 706-511*-***.
- Failure rates are constant; wear-out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Failures caused by operational errors are site specific and therefore are not included.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 2 with temperature limits within the manufacturer’s rating. 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 automatic diagnostics.
- 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.
- Recommended calibration intervals and replacement schedules of the electrochemical cartridge are observed and used to implement frequent proof testing of the device.
- Worst-case internal fault detection time is 15 seconds..
-

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Model 706-511*-*** FMEDA.

Table 3 Failure rates Model 706-511*-***

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		78
Fail Dangerous Detected		756
Fail Detected (detected by internal diagnostics)		598
Fail High (detected by logic solver)		74
Fail Low (detected by logic solver)		84
Fail Dangerous Undetected		61
No Effect		457
Annunciation Detected		0
Annunciation Undetected		29

In addition to the failure rates listed above, the external leakage failure rate of the Model 706-511*-*** is 2 FIT. As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure rates do not directly contribute to the reliability of the transmitter but should be reviewed for secondary safety and environmental issues.

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

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 (see Section 5.2).

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore the Model 706-511*-*** meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

Table 4 lists the failure rates for the Model 706-511*-*** according to IEC 61508.

Table 4 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}
Model 706-511*-***	0	78	748	61

5 Using the FMEDA Results

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

5.1 PFD_{avg} calculation Model 706-511*-***

Using the failure rate data displayed in section 4.4, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix D for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test are listed in Appendix B.

5.2 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:

"based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to

- the amount of field feedback; and
- the exercise of **expert judgment**; and when needed
- the undertake of specific tests,

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

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

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

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" vs. "systematic" are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

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

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
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.
PFD_{avg}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test - It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequently than the proof test; therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
Severe Service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
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, product design changes, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical model number product at some future time. 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, contact the product vendor to verify the current validity of the results.

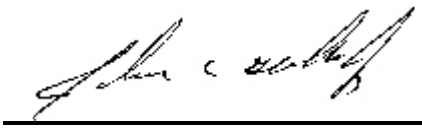
7.2 Releases

Version History:	V1, R1:	Released to Magnetrol International; 2/10/2016
	V0, R1:	Initial Draft; 2/6/2016
Author(s):	John C. Grebe Jr.	
Review:	V0, R1:	William Goble (*exida*); 2/10/16
Release Status:	Released to Magnetrol International	

7.3 Future enhancements

At request of client.

7.4 Release signatures



John C. Grebe Jr., CFSE, Principal Engineer

Dr. William M. Goble, Principal Partner

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[4] 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.

It is the responsibility of the end user to maintain and operate the Model 706-511*-*** 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/site experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant/site experience should be used.

[4] 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 proof test described in Table 5 will detect 84% of possible DU failures in the Model 706-511*-***.

Table 5 Suggested Proof Test – Model 706-511*-***

Step	Action
1.	Bypass the PLC or take other action to avoid a false trip.
2.	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.	Use the Unit's DIAGNOSTICS menu to observe Present Status, and review EVENT HISTORY in the Event Log. 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) Choose the menu DIAGNOSTICS / Present Status. i. Present Status should be OK. b) Choose the menu DIAGNOSTICS / EVENT HISTORY / Event Log i. Any FAULT or WARNING messages must be investigated and understood. ii. Corrective actions should be taken for FAULT messages.
4.	Use the DIAGNOSTICS menu to perform a "CURRENT LOOP TEST". Choose the menu DIAGNOSTICS / ADVANCED DIAGNOSTICS / TRANSMITTER TESTS / Analog Output Test to change the output loop current and confirm the actual current matches the value chosen. a) Send a HART command to the transmitter (or use the local interface) to go to the 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 interface) to go to the 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. Confirm that the ECHO Waveform is normal. The echo curve is dependent on the type of probe used, the installation conditions and the level of process on the probe. Comparison of the present Echo curve to one stored at the time of commissioning the unit gives additional

	confidence of the normal operation of the unit. Use of the DTM and digital communications is necessary for comparison of echo curves. a) 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 FIDUCIAL, Process level, End of Probe and other features. ii. Confirm that the FIDUCIAL appears acceptable. Confirm that FIDUCIAL is located where expected. iii. Confirm that the signal from the process level appears normal and is located as expected. iv. Verify that the baseline of the waveform is smooth and flat. v. Compare to Echo curve from commissioning in the FIDUCIAL area. b) Access the Fiducial Ticks and Fiducial Strength values in the menu DIAGNOSTICS / ADVANCED DIAGNOSTICS / INTERNAL VALUES i. Observe and record: 1. Fiducial Ticks _____ 2. Fiducial Strength._____ ii. Confirm that these values match the previous values. 1. Fiducial Ticks change less than +/- 100 2. Fiducial Strength changes less than +/- 15
6.	Perform 2 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 known 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 shorting the probe at two points. Measure the level from the bottom of the probe to the two points and compare to the transmitter display and current level readings. a) If the calibration is off by more than 2%, call the factory for assistance. b) b. If the calibration is correct, the proof test is complete. c) c. Re-install the probe and transmitter.
9.	Restore loop to full operation.
10.	Remove the bypass from the safety PLC or otherwise restore normal operation.

Appendix C *exida* Environmental Profiles

Table 6 *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[5]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[6]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[7]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[8]	G2	G3	G3	G3	G3	Compatible Material
Surge[9]						
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[10]						
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)[11]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[5] Humidity rating per IEC 60068-2-3
[6] Shock rating per IEC 60068-2-27
[7] Vibration rating per IEC 60068-2-6
[8] Chemical Corrosion rating per ISA 71.04
[9] Surge rating per IEC 61000-4-5
[10] EMI Susceptibility rating per IEC 61000-4-3
[11] ESD (Air) rating per IEC 61000-4-2

Appendix D Determining Safety Integrity Level

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

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N5] and [N8].

These are:

A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;

B. Architecture Constraints (minimum redundancy requirements) are met; and

C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N9].

C. Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD_{avg}) calculation must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restore (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03. See Figure 2.

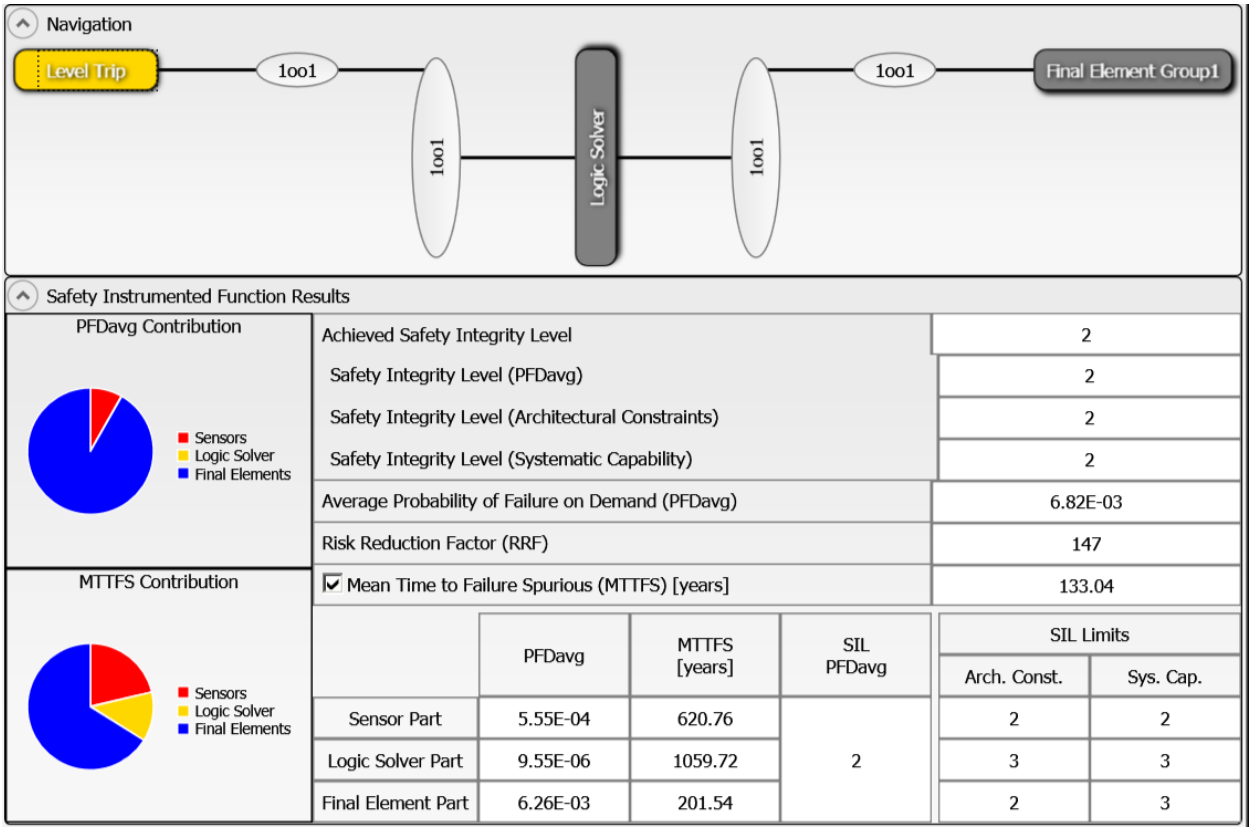


Figure 2: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 3.

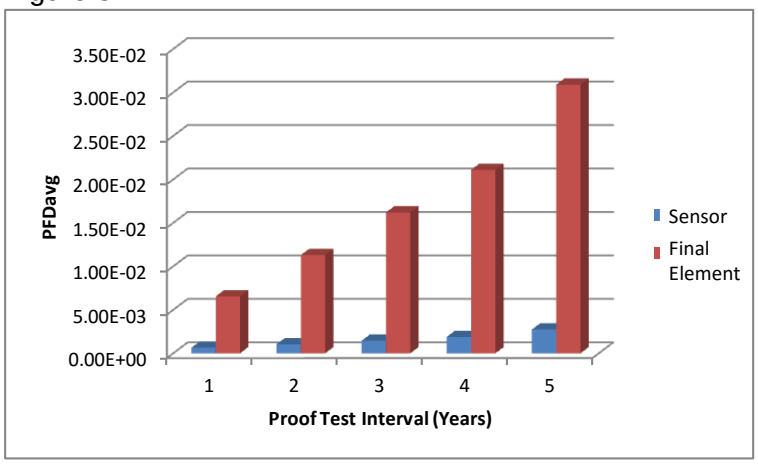


Figure 3 PFD_{avg} versus Proof Test Interval.

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 4).

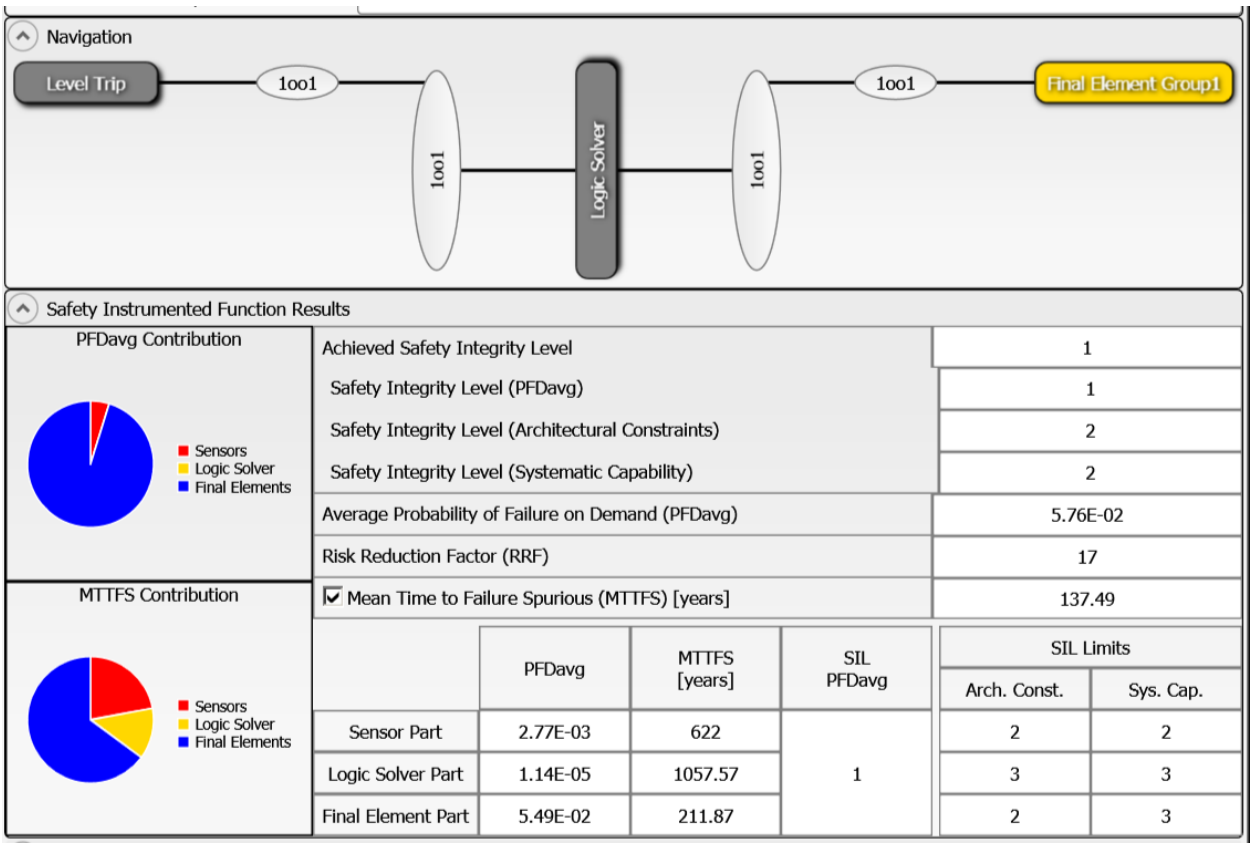


Figure 4: exSILentia results with realistic variables

It is clear that PFD_{avg} results can change an entire SIL level or more when all critical variables are not used.