Results of the IEC 61508 Functional Safety Assessment

Project:
Eclipse 706 Level Transmitter

Customer:
Magnetrol International, Inc.
Aurora, IL
USA

Contract No.: Q15/12-025
Report No.: MAG 15-12-025 R002
Version V2, Revision R0, 6/15/2016
Dave Butler

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management Summary

The Functional Safety Assessment of the Magnetrol International, Inc.

Eclipse 706 Level Transmitter

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Magnetrol International, Inc. through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed the manufacturing quality system in use at Magnetrol International, Inc..

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Hardware and Software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The audited development process, as tailored and implemented by the Magnetrol International, Inc. Eclipse 706 Level Transmitter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the Eclipse 706 Level Transmitter meets the requirements for architectural constraints of an element such that it can be used, with HFT=0, to implement a SIL 2 safety function, or with HFT = 1, to implement a SIL 3 safety function.

This means that the Eclipse 706 Level Transmitter is capable for use in SIL 3 applications in Low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual, and when using the versions specified in 3.1 of this document. The PFD_{avg} of the Safety Instrumented Function must also be calculated and found to be in the SIL 3 range required by IEC 61508 for compliant use.

The manufacturer will be entitled to use the Functional Safety Logo.

CERTIFIED
IEC 61508
SIL 3 CAPABLE
e x i d a
FS

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the: Eclipse 706 Level Transmitter by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508:2010.

The purpose of the assessment was to evaluate the compliance of:

- the Eclipse 706 Level Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the Eclipse 706 Level Transmitter development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

and

- the Eclipse 706 Level Transmitter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out based on *exida*'s quality procedures and scope definitions**.**

The results of this assessment provide the safety instrumentation engineer with the required failure data per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with Magnetrol International, Inc. (see [R5]).

All assessment steps were continuously documented by *exida* (see [R1])

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 based on 100 billion hours of field failure data.

2.2 Roles of the parties involved

Magnetrol International, Inc.	Manufacturer of the Eclipse 706 Level Transmitter
exida	Performed the Hardware assessment [R4]
exida	Performed the Proven In Use assessment [R4]
exida	Performed the Functional Safety assessment [R1] per the accredited *exida* scheme.

Magnetrol International, Inc. contracted *exida* with the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards / Literature used

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

Doc. ID	Standard	Title
[N1]	IEC 61508:2010 Parts 1 – 7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Magnetrol International, Inc.

Doc. ID	Project Document Filename	Version	Date
D001	QMS Manual Rev 25.pdf	Rev. 25	5/26/2015
D003	New Product Development Process Flow.pdf		8/27/2013
D003c	Electrical Design Methodology.docx		3/28/2013
D003d	Mechanical Design Methodology.pdf		2/15/2013
D004	SKA002.pdf	Rev. 15	12/17/2015
D004b	SLA002.pdf	Rev. 8	9/20/2012
D005	RMA Processing Rev. 1.docx	Rev. 1	12/16/2010
D007	SQA038.pdf	Rev. 25	5/12/2014

Doc. ID	Project Document Filename	Version	Date
D010	SPI423.pdf	Rev. 5	9/9/2011
D012	SPI830.pdf	Rev. 11	4/3/2015
D013	Corrective Action Rev. 4.docx	Rev. 4	7/29/2010
D019	SPI723.pdf	Rev. 1	8/18/2012
D019b	SVA001.pdf	Rev. 10	3/11/2015
D021	Software Development Methodology.doc	--	9/4/2015
D021b	SPI SLA009-1.docx	Rev. 0	7/8/2013
D021c	Tool HAZOP Template.doc	Rev. 0	
D023b	Impact Analysis Template.doc	Rev. A	
D023c	SLA007.pdf	Rev. 0	7/8/2013
D026	Eclipse Model 706 Functional Safety Management Plan (PIU) 042716.doc	Rev. 0	4/27/2016
D030	706-xxx-xxx Sales Orders Shipped 1-01-2012 to 1-31-2016.xlsx		1/31/2016
D031	706 RMA SIL.xlsx		2/22/2016
D032	Engineering.pdf	N/A	
D033	training logs 2.docx	Screenshot	
D036	ISO 9001-2008 Certificate - May 2014.pdf		exp.: 5/29/2017
D038	Model 706 Suitability of Tools.doc		3/9/2016
D040	Safety Requirements Specification V0 R1 Eclipse 706 SIGNED 050516.pdf	V0R1	4/5/2016
D040b	Model 706 Diagnostic Indicator Specification.doc		2/26/2016
D040c	Eclipse Model 706 Rev _1.5e_061511.doc	Rev. 1.5f	10/4/2011
D041	Eclipse Model 706 SRS Review Minutes 032316.doc		4/5/2016
D041b	Eclipse Model 706 SRS Checklist 032316.doc		3/23/2016
D043	Model 706 Software Architecture.doc		3/9/2016
D043b	Model 706 System Monitor Design.doc		9/20/2012
D045	Overview of Eclipse 4x Hardware ver1_0.vsd		
D045c	BLOCK-DIAGRAM _ PAGE2.pdf	Rev. B	2/1/2010
D047	030-9159-AA.PDF	Rev. AA	1/11/2016
D047b	030-9160-H.PDF	Rev. H	11/1/2012
D047c	030-9165-F.pdf	Rev. F	10/1/2014
D047d	094-6067-L.pdf	Rev. L	10/1/2014
D047e	094-6068-H.PDF	Rev. H	11/1/2012
D047f	099-6546-X -- Assembly Drawings.PDF	Rev. X	5/14/2015
D048	RMA 51430 and 51639.docx	Screenshot	
D050	Magnetrol 706 Level Transmitter project report_draft.doc	V0R0	1/22/2012

Doc. ID	Project Document Filename	Version	Date
D060	C Language Coding Standard for Firmware Development v 1.9 Highlighted.doc	Rev. 1.9	3/8/2016
D069	Validation Test Spec Plan V0 R1 Eclipse 706 040516.doc	V0R1	4/5/2016
D069b	SVA006.pdf	Rev. 3	9/26/2003
D069c	SVA007.pdf	Rev. 2	9/24/2003
D069d	SVA008.pdf	Rev. 3	9/24/2003
D069e	SVA009.pdf	Rev. 4	5/25/2010
D070	Eclipse Model 706 Validation Test Specification and Plan Review Minutes.doc		3/23/2016
D070b	Validation Test Plan Checklist 032316.doc	Rev. A	
D071	SVA004.pdf	Rev. 7	7/8/2014
D072	SVA003.pdf	Rev. 5	9/24/2008
D072b	Eclipse706EMCTestingJan2012AtMagnetrol.pdf		1/17/2012
D073	ECN Procedure		
D074	Results 20121024.xlsx		10/24/2012
D074b	706 HT Acceptance Test Report Rev D.doc	Rev. D	9/4/2012
D074c	Repeatbility Test report.xlsx		10/17/2012
D074d	Firmware tests.docx	Screenshot	
D074e	706 ProcessDielectricEffectTest.xlsx		9/6/2012
D074f	706 SIL VT Summary V0 R1 SIGNED 061316.pdf	Rev. R1	5/25/2016
D075b	706 Temperature effects testing report .xlsx		9/5/2012
D075c	Humidity Test report.xls		8/16/2012
D075d	Thermal Shock Test Report.xls		8/27/2012
D076	Eclipse 706 EMC Report.pdf		2/14/2013
D077	MAG 15-02-050 R002 V1R1 E3 Fault Injection Test - Completed	V1R1	Mar.2016
D078	57-606.5_Eclipse706_IO.pdf		Feb. 2016
D079	57-657.0 Eclipse Model 706 SIL3 Certified Manual.pdf	57657	6/1/2016
D082	Diagnostic Indicators used in the Model 706 FMEDA 030316.docx	N/A	3/3/2016
D083	MAG 15-12-025 R004 V1R2 PIU Spreadsheet - 706GWR Level Transmitter.xls		4/26/2016
D086	Gimpel PC-lint Ver 9.0 HAZOP.doc	Rev. 0	4/11/2013
D086b	IAR EWARM Ver 6.50 HAZOP.doc	Rev. 0	4/16/2013
D086c	Serena PVCS Ver 8.4 HAZOP.doc	Rev. 1	4/11/2013
D086d	IAR	Many	
D088	Model 706 Issue 197 Impact Analysis.docx	Rev. 1	4/6/205
D088b	Model 706 Rel 1.0fA Firmware Design.docx	Rev. 1.0	6/18/2015
D088c	Model 706 Rel 1.0fA Firmware Test Plan.docx	Rev. 1.0	6/18/2015

Doc. ID	Project Document Filename	Version	Date
D088d	Model 706 Rel 1.0fA Firmware Test Results.pdf	Rev. 1.0	6/18/2015
D091	Model 706 Rel 1.0gA Firmware Design.docx	Rev. 1.27 (1.0gA)	8/20/2015

2.4.2 Documentation generated by *exida*

Doc. ID	*exida* Document Filename	Description
[R1]	MAG 15-12-025 V2R1 IEC 61508 SafetyCaseWB – 706 Xmitter.xlsm	Safety Case Workbook
[R2]	MAG 15-12-025 R002 V2R0	IEC 61508 Functional Safety Assessment for Eclipse 706 Level Transmitter (This Document)
[R3]	MAG 15-12-025 R004 V1R2 PIU Spreadsheet - 706GWR Level Transmitter.xls	PIU Analysis
[R4]	MAG 15-12-025 R001 V1R1 FMEA Eclipse 706.doc	FMEDA Report
[R5]	Q15-12-025 Magnetrol 706 transmitter Certification Proposal	Assessment Plan

2.5 Assessment Approach

The certification audit was closely driven by requirements of the accredited *exida* certification scheme which includes subsets filtered from IEC 61508. The assessment was planned by *exida* and agreed with Magnetrol International, Inc. (see [R5]).

For designs that have been in service for several years and have demonstrated themselves in a variety of applications and conditions, consideration of a proven in use assessment may be used as a substitute if a product didn’t follow a fully compliant IEC 61508 design process. The functional safety assessment includes an assessment of all fault avoidance and fault control measures during any hardware and software modifications needed to achieve SIL 3 capability for the Eclipse 706 Level Transmitter. Product development, occurring prior to these modifications, was assessed according to Proven-In-Use (PIU) requirements (see section 5.1.5). The combination of these assessments demonstrates full compliance with IEC 61508 to the end-user.

The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software.

As part of the IEC 61508 functional safety assessment for the Eclipse 706 Level Transmitter, the following evidence aspects have been reviewed:

- FMEDA
- Product specification
- Safety manual
- Instruction manual
- Modification procedures
- Validation test results
- Corrective Action and prevention action plan/process

- Hardware drawings release process
- PIU data collection procedures and operational excellence calculation/report (evidence that the equipment is proven-in-use; analysis of field failure rates to ensure that no systematic faults exist in the product)

No ASICs are used in this product.

No safety related communications are used in this product.

Proven-In-Use (PIU) assessment provides for the prevention of systematic failures for pre-existing devices with a proven history of successful operation. As part of the PIU assessment for the Eclipse 706 Level Transmitter, a number of IEC 61508 functional safety assessment requirements are satisfied without further documented evidence:

- FSM Plan
- Configuration management
- Validation of development tools
- Validation test plan
- System Architecture design
- Integration and Unit test plans
- Development process

The certification audit was done in Aurora, IL on 2/24/2016.

The project teams, not individuals, were audited.

3 Product Description

Model 706-512*-*** 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.

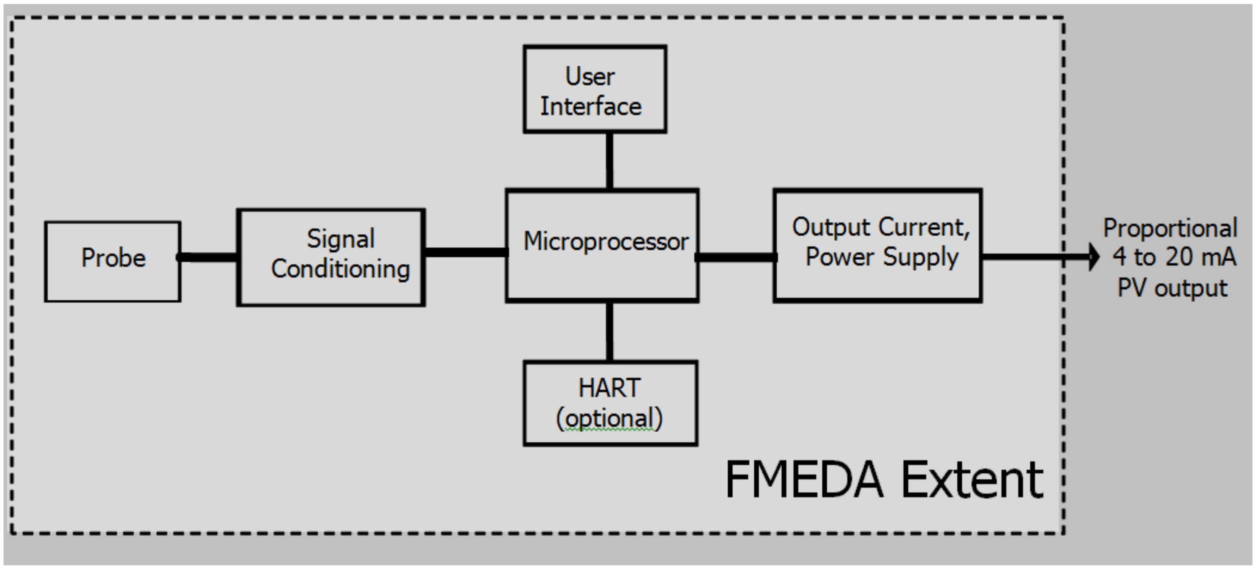

Figure 1 Model 706-512*-***, Parts included in the FMEDA

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.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of Eclipse 706 Level Transmitter:

Variant/Model	Hardware Version	Software Version
706-512x-xxx (HART)	030-9160-001 Rev. K 030-9159-001 Rev. AC 030-9165-001 Rev. F	1.0hA.hex

Table 1- Hardware and Software Versions

4 IEC 61508 Functional Safety Assessment Scheme

The assessment was executed using the accredited exida certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team. The assessment was performed based on the information received from Magnetrol International, Inc. [see section 2.4.1] and is documented in the safety case [R1].

exida audited and assessed project and product documentation for compliance with the functional safety requirements of IEC 61508. During an evaluation period, an assessor updated a safety case with the results of the assessment. The safety case documents the development project's compliance with the functional safety management requirements of IEC 61508, parts 1 through 3. Evaluation was followed by a certification review of the safety case, in which a review of a subset of the most important requirements, and a spot inspection of the remaining requirements, was carried out to ensure high quality of the safety case.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Magnetrol International, Inc. Eclipse 706 Level Transmitter, with IEC 61508.

The results of the assessment show that the Eclipse 706 Level Transmitter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements and constraints specified in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Magnetrol International, Inc. may make modifications to this product as needed.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R4] of the Eclipse 706 Level Transmitter to document the hardware architecture and failure behavior. The FMEDA report and the Safety Case created for the 706 Level Transmitter documents this assessment.

exida assessed failure history of the Eclipse 706 Level Transmitter [D030, D031] and performed a detailed analysis of the data provided [R3]. This PIU assessment is done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the 706 Level Transmitter documents this assessment.

The result of the overall assessment can be summarized by the following observations:

The Eclipse 706 Level Transmitter complies with the relevant requirements of IEC 61508 SIL 3 applications when considering PIU, and when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

5.1 Lifecycle Activities and Fault Avoidance Measures

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team and supported by PIU analysis.

5.1.1 Safety Lifecycle and Functional Safety Management Planning

Reported dangerous failures that occur in the field are captured and analyzed and recommendations are made to minimize the chance for a repeat occurrence of the failure.

Manufacturer has a QMS in place. The Manufacturer has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure.

Conclusion

The objectives of the standard are fulfilled by the Magnetrol International, Inc. functional safety management system and are supported by PIU analysis.

5.1.2 Tools

All tools which support a phase of the software development lifecycle, and cannot directly influence the safety-related system during its run time (Off-line support tools) are documented, including tool name, manufacturer name, version number, use of the tool on this project.

All off-line support tools have been classified as either T3 (safety critical), T2 (safety-related), or T1 (interference free). All off-line support tools in classes T2 and T3 have a specification or product manual which clearly defines the behavior of the tool and any instructions or constraints on its use. List all T3 and T2 tools along with a reference (file name, document number) to the specification or product manual.

A Software Tool Upgrade Procedure exists and is part of the Software Development Procedure as required for projects on which software tools are used. Generally, the approach is taken where a specific tool version is used for the life of the product.

Conclusion

The objectives of the standard are fulfilled by the Magnetrol International, Inc. internal organizational procedures and functional safety management system processes and supported by PIU analysis.

5.1.3 Safety Requirement Specification and System Architecture Design

All of the 706 Level Transmitter's safety functions necessary to achieve the required functional safety are specified, including: functions that enable the EUC to achieve or maintain a safe state; functions related to the detection, annunciation and management of sensor faults; safety accuracy of the measurement.

Environmental limits and extremes are specified.

Safety integrity requirements are specified.

Specific requirements for start-up and restart procedures are specified. The 706 Level Transmitter starts up automatically when power is applied, and does not require human interaction to start.

The 706 Level Transmitter design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented.

The System Architecture Design and Design Review Records show support for appropriate design methods that clearly and precisely describe functionality, interfaces, sequencing/timing relationships.

The System Architecture Design Specification describes that the behavior of the device when a fault is detected is to annunciate the detected fault through an external interface. Diagnostics are listed and specified in D045e. Each software module's design document includes diagnostics designs.

The System Architecture Design clearly identifies which communication interfaces are safety related. There are no external, safety-related digital communications interfaces.

Traceability between Safety Requirements and Validation test cases has been fully implemented and verified.

5.1.4 Change and modification management

A Modification Procedure exists that identifies how a modification request is initiated, and processed, in order to authorize an Engineering Change Request (including hardware and software modifications). A Product Modification Request System exists to support this process. An "add on" procedure further defines the standard ("non-safety") procedure when a change request is for a safety critical product.

The Modification Procedure requires that an Impact Analysis be performed to assess the impact of the modification, including the impact of changes to the software design (which modules are impacted). The results of Impact Analyses are documented.

Modification Request/Records document the reason for the change, a detailed description of the proposed change, which new and existing tests must be run to validate the change, which tests must be re-run to validate that the change did not affect other functionality and what verification must be performed to ensure the development process was carried out properly from the point in the lifecycle at which the modification was initiated.

5.1.5 Proven In Use

There are no functions that are not covered by the PIU demonstration.

The product has been shipping for at least 18 months without any revisions or changes (NOTE: Based on the assumption that installation takes six months.). This is supported by the shipping records and the PIU analysis.

In addition to Design Fault avoidance techniques listed herein, a Proven in Use evaluation was performed on the Eclipse 706 Level Transmitter. Shipment records were used to determine that the Eclipse 706 Level Transmitter has greater than 30,000,000 operating hours and has demonstrated field failure rates less than the predicted failure rates indicated in the FMEDA reports. All components considered in the Low Demand, Type B Device FMEDA are standard components with greater than 100 million operating hours (see [R3] and [R4]). This provides justification for using a Route 2H approach.

5.2 Software Design

The Software Architecture Design contains a description of the software architecture. The design is partitioned into new, existing and/or proprietary (third party) components and modules, which are identified as such. A certified RTOS is used in the software. The runtime libraries (RTLs), which are packaged with the commercial programming too chain and are compliant through a proven-in-use argument. The RTOS, toolchain and RTLs are not intended to be upgraded for the life of the product as stated in the Functional Safety Management Plan.

The Software Architecture Design uses block diagrams, state/transition diagrams, data flow diagrams and other semi-formal notation to specify the software design.

The Software Architecture Design and Detailed Designs are judged as adequate to support compliant modification of the software through use of the Modification Procedure.

5.3 Hardware Architecture Design and Probabilistic Properties

To evaluate the hardware design of the Eclipse 706 Level Transmitter, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by *exida* for each component in the system, and is documented in [R4].

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. The FMEDA is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA, failure rates are derived for each important failure category.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined SIF to verify the design of that SIF.

5.4 Safety Validation

Fault injection testing has been performed on the product as defined in the fault injection test plan. The results have been analyzed and adjustments have been made to the FMEDA based on these results.

Test results are documented including reference to the test case and test plan version being executed.

The EMC/Environmental specifications tested (and passed) were the same as or more stringent than those reviewed and approved by the FMEDA analyst.

5.5 Safety Manual

The Safety Manual is provided to end users, and identifies and describes the functions of the product. The safety function is clearly described, including a description of the output. The effects of internally detected faults on the device output are clearly described. Sufficient information has been provided to facilitate the development of an external diagnostics capability (output monitoring).

The Safety Manual contains the Safety Integrity information needed to incorporate the product into a higher level element or Safety Instrumented Function (SIF), including failure rates, Systematic Capability, hardware architecture constraints, etc.

The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing.

Procedures for maintaining tools and test equipment are listed.

The Installation Manual includes valuable information for the user of the device or system regarding safe operation and avoidance of hazards.

6 Terms and Definitions

Term	Definition
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.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFDAVG	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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 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.

7.2 Releases

Version History:	V2, R0:	updated to allow engineering changes; DEB, 6/15/2016
	V1, R2:	corrected version information; DEB, 4/28/2016
	V1, R1:	updated based on CA review; Dave Butler, 4/25/2016
	V1, R0:	initial draft; Dave Butler, 4/27/2016
Authors:	Dave Butler	
Review:	John Yozallinas, 6/15/2016	
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Dave Butler, Senior Safety Engineer

John C Yozallinas

John Yozallinas, Senior Safety Engineer