



## **Results of the IEC 61508 Functional Safety Assessment**

Project:

E3 Modulelevel® Liquid Level Displacer Transmitter

Customer:

**Magnetrol International, Inc.**

Aurora, IL

USA

Contract No.: Q15/02-050

Report No.: MAG 15-02-050 R002

Version V1, Revision R2, 9/1/2016

Dave Butler



## Management Summary

The Functional Safety Assessment of the Magnetrol International, Inc.

E3 Modulelevel® Liquid Level Displacer 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. E3 Modulelevel® 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 E3 Modulelevel® 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 E3 Modulelevel® 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 of the product specified in section 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.





## Table of Contents

Management Summary .....	2
1 Purpose and Scope .....	5
1.1 Tools and Methods used for the assessment .....	5
2 Project Management.....	6
2.1 <i>exida</i> .....	6
2.2 Roles of the parties involved .....	6
2.3 Standards / Literature used .....	6
2.4 Reference documents .....	6
2.4.1 Documentation provided by Magnetrol International, Inc. ....	6
2.4.2 Documentation generated by <i>exida</i> .....	8
2.5 Assessment Approach .....	8
3 Product Description .....	10
3.1 Hardware and Software Version Numbers .....	11
4 IEC 61508 Functional Safety Assessment Scheme.....	11
4.1 Product Modifications .....	12
5 Results of the IEC 61508 Functional Safety Assessment.....	12
5.1 Lifecycle Activities and Fault Avoidance Measures .....	12
5.1.1 Safety Lifecycle and Functional Safety Management Planning .....	12
5.1.2 Tools .....	12
5.1.3 Safety Requirement Specification and System Architecture Design.....	13
5.1.4 Change and modification management .....	13
5.1.5 Proven In Use.....	14
5.2 Software Design.....	14
5.3 Hardware Architecture Design and Probabilistic Properties.....	14
5.4 Safety Validation .....	15
5.5 Safety Manual .....	15
6 Terms and Definitions.....	15
7 Status of the document.....	17
7.1 Liability.....	17
7.2 Releases.....	17
7.3 Future Enhancements.....	17
7.4 Release Signatures.....	17



## 1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the E3 Modulelevel® 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 E3 Modulelevel® Level Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the E3 Modulelevel® 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 E3 Modulelevel® 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* and 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 E3 Modulelevel® Level Transmitter
<i>exida</i>	Performed the Hardware assessment [R4]
<i>exida</i>	Performed the Proven In Use assessment [R3]
<i>exida</i>	Performed the Functional Safety assessment [R1] per the accredited <i>exida</i> 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
D003b	Dev Process Steps.xlsx		
D003c	Electrical Design Methodology.docx	Rev. 1	7/27/2016
D003d	Mechanical Design Methodology.pdf		2/15/2013
D004	SKA002.pdf	Rev. 15	12/17/2015
D004b	SLA002.pdf	Rev. 8	9/20/2016
D005	RMA Processing Rev. 1.docx	Rev. 1	12/16/2010



D007	SQA038.pdf	Rev. 25	5/12/2014
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
D016b	Product Change Request 9 Firmware Issue 197.docx	Screenshot	
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	Model E3 Modulelevel Functional Safety Management Plan V0 R1 SIGNED 051116.pdf	Rev. 1	5/11/2016
D027	099-6537-M.pdf	Rev. M	9/1/2015
D030	E3x-xxx-xxx Sales Orders Shipped 1-01-2008 to 2-05-2015.xlsx		2/5/2016
D031	RMA on E3.xlsx		
D032	Engineering.pdf	N/A	
D036	ISO 9001-2008 Certificate - May 2014.pdf		exp.: 5/29/2017
D038	E3 Modulelevel Suitability of Tools.doc	Rev. 0	4/22/2016
D040	Model E3 Modulelevel Safety Requirements Specification V0 R2 SIGNED 082216.pdf	V0R2	8/22/2016
D041	Model E3 Modulelevel SRS and VTPS V0 R2 Review Minutes 082216.doc		8/22/2016
D045	E3 System and Hardware Architecture R2 081916.docx	Rev. 2	8/19/2016
D045b	2. E3 Analog board, theory of operation, 10-31-11.docx		10/31/2011
D045c	E3 Modulelevel HART Firmware Overview.doc		8/3/2016
D045d	E3Mod_MeasTask_Sfwr_Overview.doc		1/29/2009
D047	D047_Schematics _ Circuit Diagrams	Many	
D048	E3ExplodedComponentECNList.xlsx		
D049b	measengdesc1.doc		8/26/2013
D049c	Modulelevel3 Device Status.doc		10/7/2008
D052	E3 Modulelevel Change History1.1aA-1.1cA.doc	1.1aA - 1.1cA	10/15/2015
D059	E3 2016 Fault Injection Tests.mht		3/16/2016
D060	C Language Coding Standard for Firmware Development v 1.9 Highlighted.doc	Rev. 1.9	3/8/2016
D069	Model E3 Modulelevel Validation Test Spec and Plan V0 R2 SIGNED 082216.pdf	V0R2	8/22/2016
D071	SVA004.pdf	Rev. 7	7/8/2014
D072	SVA003.pdf	Rev. 5	9/24/2008



D074	E3 SIL VT Summary V0 R2.pdf	V0R2	8/22/2016
D075	E3 Environ Test Report.pdf		11/6/2009
D075b	E3 Modulelevel High Temp.pdf		9/2/2014
D075c	Modulelevel E3 High Temp.pdf		3/17/2014
D075d	E3 and 355 Shock Vib.doc		4/15/2008
D075e	Test 9 Humidity.pdf		4/15/2008
D076	E3 Modulelevel EMC RPT.pdf		11/11/2008
D077b	MAG 15-02-050 R002 V1R1 E3 Fault Injection Test - Completed.xls		3/28/2016
D078	48-635.6 E3 Modulelevel HART IO.pdf		
D079	48-651 0 E3 Modulelevel SIL 3 Certified Manual R2 082216.pdf	DRAFT	8/22/2016
D080	On-site discussion revealed that while reviews are done, records are not retained.		
D081	ECR 3051-00233.jpg	Screenshot	
D081b	PCR Number 24.docx	Screenshot	8/23/2016
D086	Gimpel PC-lint Ver 9.0 HAZOP.doc	Rev. 0	4/11/2013
D086b	Serena PVCS Ver 8.4 HAZOP.doc	Rev. 1	4/11/2013
D088	Impact Analysis E3 Modulelevel Firmware Issue 2.docx		8/16/2016

## 2.4.2 Documentation generated by *exida*

Doc. ID	<i>exida</i> Document Filename	Description
[R1]	MAG 15-02-050 V1R0 SafetyCaseWB - E3.xlsm	Safety Case Workbook
[R2]	MAG 15-02-050 R002 V1R1 IEC 61508 Assessment Report - E3.docx	IEC 61508 Functional Safety Assessment for E3 Modulelevel® Level Transmitter (This Document)
[R3]	MAG 15-02-050 V1R0 PIU Analysis – E3.xlsm	PIU/Failure Analysis
[R4]	MAG 15-02-050 R001 V1R1 FMEDA E3.pdf	FMEDA Report
[R5]	Q15-02-050 E3 Modulelevel Magnetrol Certification Proposal Rev3.pdf	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 E3 Modulelevel® Liquid Level Displacer 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 E3 Modulelevel® Liquid Level Displacer Transmitter, the following evidence aspects have been reviewed:

- FMEDA
- Product specification
- Safety manual
- Instruction manual
- 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 ASIC/PLDs 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 E3 Modulelevel® 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

The E3 Modulevel<sup>®</sup> Liquid Level Displacer Transmitter is a loop-powered, two-wire, 24 VDC level transmitter which utilizes buoyancy in combination with a range spring and a linear variable differential transformer to detect and convert liquid level movement into a 4–20 mA output signal.

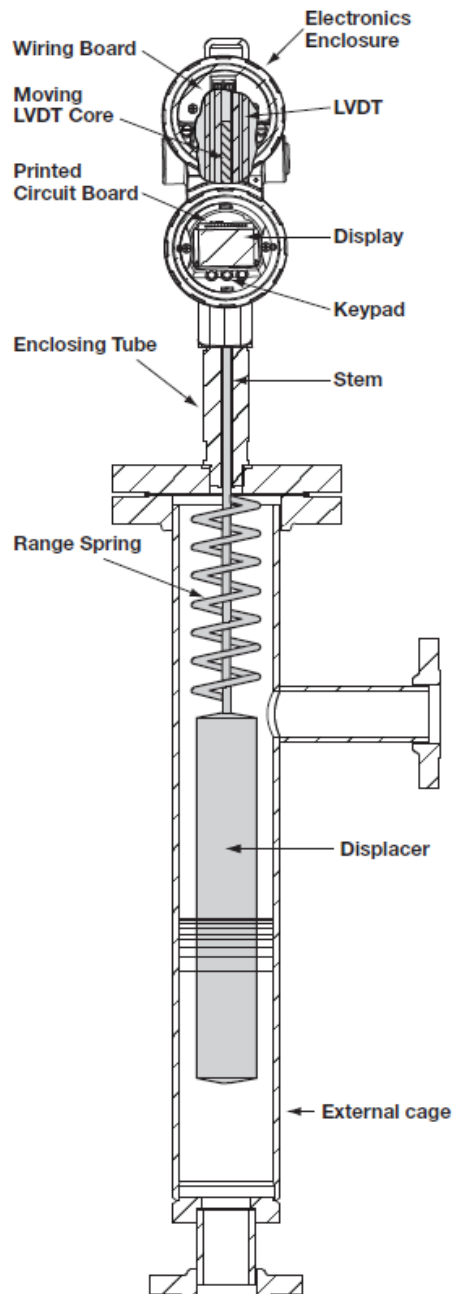


Figure 1 E3, Parts included in the FMEDA

Table 1 gives an overview of the different versions that were considered in the FMEDA of the E3 Modulelevel® Level Transmitter.

E3 Local	The electronics and display are mounted at the displacer assembly
E3 Remote	The electronics and display are mounted remotely from the displacer assembly

**Table 1 Version Overview**

The E3 is classified as a Type B element according to IEC 61508, having a hardware fault tolerance of 0.

### 3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions, and later versions, of E3 Modulelevel® Level Transmitter:

Variant/Model	Hardware Version	Software Version
E3x-xxxx-Sxx - 4-20 mA/HART, SIL 2	(Wiring Board) 030-9151-001 Rev. Q, or later (Digital Board) 030-9145-001 Rev. AG, or later (Analog Board) 030-2475-001 Rev. E, or later (Remote Board) 030-3609-003 Rev. E, or later	Dig.Bd. FW - 1.1cA, or later

**Table 2- 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. E3 Modulelevel® Level Transmitter, with IEC 61508.

The results of the assessment show that the E3 Modulelevel® 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 directed by the corresponding procedures.

## 5 Results of the IEC 61508 Functional Safety Assessment

*exida* assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R4] of the E3 Modulelevel® Level Transmitter to document the hardware architecture and failure behavior. The FMEDA report and the Safety Case created for the E3 Modulelevel® Level Transmitter documents this assessment.

*exida* assessed failure history of the E3 Modulelevel® 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 E3 Modulelevel® Level Transmitter documents this assessment.

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

**The E3 Modulelevel® 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. All T3 and T2 tools are listed, 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 E3 Modulelevel® 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 E3 Modulelevel® Level Transmitter starts up automatically when power is applied, and does not require human interaction to start.

The E3 Modulelevel® 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 D049c. 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 E3 Modulelevel® Level Transmitter. Shipment records were used to determine that the E3 Modulelevel® 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. The runtime libraries (RTLs), which are packaged with the commercial programming tool chain, 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 E3 Modulelevel® 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, 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 ( $1 \times 10^{-9}$ 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: V1, R2: corrections and minor changes; Dave Butler, 9/1/2016  
V1, R1: updated documents for software modification; Dave Butler, 8/29/2016  
V1, R0: initial draft; Dave Butler, 8/23/2016

Authors: Dave Butler

Review: John Yozallinas, 8/8/2016

Release status: Released

### 7.3 Future Enhancements

At request of client.

### 7.4 Release Signatures

A handwritten signature in black ink, appearing to read "Dave Butler", written over a solid black horizontal line.

Dave Butler, Senior Safety Engineer

A handwritten signature in black ink, appearing to read "John C. Yozallinas", written over a solid black horizontal line.

John Yozallinas, Senior Safety Engineer