Results of the IEC 61508 Functional Safety Assessment

Project:
Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter

Customer:
Magnetrol International, Inc.
Aurora, IL
USA

Contract No.: Q20/10-059
Report No.: 17-11-051 R002
Version V2, Revision R0, February 3, 2021
Dave Butler

Management Summary

The Functional Safety Assessment of the Magnetrol International, Inc.:

- Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter

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

- *exida* assessed the systematic capability through a detailed analysis of proven-in-use data provided by Magnetrol International, Inc. and the creation of a detailed safety case against the requirements of IEC 61508.
- *exida* reviewed and assessed the random capability through a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to ensure that the FMEDA analysis was complete.
- *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 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 design 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 Enhanced Model 705 3X Guided Radar Level Transmitter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, performed to the requirements of IEC 61508, has shown that the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter can be used in a high demand safety related system in a manner where the PFH is within the allowed range for up to SIL 3 according to table 3 of IEC 61508-1.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter can be used in a low demand safety related system in a manner where the PFD_{AVG} is within the allowed range for up to SIL 3 according to table 2 of IEC 61508-1.

The assessment of the FMEDA shows that the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter can meet the requirements for minimum architectural constraints of an element for SIL 2 (HFT = 0 / low demand; or HFT = 1 / high demand) and SIL 3 (HFT = 1).

This means that the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter is capable for use in SIL 2 or SIL 3 applications in Low and High or High demand modes when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 (or later).

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

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the:

- Eclipse Enhanced Model 705 3X Guided Radar 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 Enhanced Model 705 3X Guided Radar Level Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the Eclipse Enhanced Model 705 3X Guided Radar 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 Enhanced Model 705 3X Guided Radar 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 the quality procedures and scope definitions of *exida*.

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 out 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.

All assessment steps were continuously documented by *exida* (see [R1] and [R3]).

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, availability, and cybersecurity with over 500 person-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 350 billion hours of field failure data.

2.2 Roles of the parties involved

Magnetrol International, Inc. Radar Level Transmitter	Manufacturer of the Eclipse Enhanced Model 705 3X Guided
exida	Performed the hardware 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.

[N1]	IEC 61508 (Parts 1 – 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Magnetrol International, Inc.

Note: Documents revised after the 2017 audit are listed in Section 6 2020 IEC 61508 Functional Safety Surveillance Audit.

Doc ID	File, Version, Date	Document Name
D001	Quality Manual, Rev 23, 3-Aug-2009	Quality Management System Manual
D003	New Product Development Process Flow.pdf, 27-Aug-13	Overall Development Process
D003b	Dev Process Steps.xlsx	Overall Development Process- Step Description
D006	Returns Procedure, Rev 1, 16-Dec-2010	Field Return Procedure

Doc ID	File, Version, Date	Document Name
D013	Corrective Action Procedure, Rev 4, 29-Jul-2010	Corrective Action Procedure
D019	Notification Procedure, Rev 0, 14-Jul-2011	Customer Notification Procedure
D021	Software Development Process, 27-Jul-2009	Magnetrol Software Development Methodology
D023	SLA-007.pdf, 00, 08-Jul-13	Modification Procedure
D023c	SKA-002.pdf, 14, 08-Jul-13	Modification Procedure - EC
D026	FSM Plan, V0 R1, 3-Jun-2010	Functional Safety Management Plan
D030	705-51A SHIPMENTS.xlsx, ,	Shipment Records
D030b	705-51A Sales 2015-2017.xlsx, Nov.2017	Shipment Records (2015-17)
D031	705 3X SIL RMAs SUMMARY 080111 TO 091614.xlsx, ,	Field Returns Records
D031b	705 RMAs 2015-2017.xlsx, Nov.2017	Field Returns Records (2015-17)
D033	Sample Training Record	Safety Training Records
D036	1621486-01_QMS_ENG_RR.pdf, 26-Apr-17	ISO 9001 Certificate
D040	SRS, V0 R2, 12-Jul-2011	Safety Requirements Specification
D041	SRS Review, 13-Jul-2011	Safety Requirements Specification Review Meeting Minutes
D047	094-6051, Rev Q, 28-Aug-17	Enhanced 705 Analog PCB Schematic
D047b	094-6052, Rev G, 29-Jun-10	Enhanced 705 Digital PCB Schematic
D047c	094-5062, Rev C, 14-Feb-17	HART Wiring Board Schematic
D048	705 3X SIL 2 CHANGES 100314.xlsx	Hardware Change List
D048b	705 3X SIL 2 Changes 2014-2017.xlsx, 06-Oct-17	List of ECNs on the 3 boards used in the Enhanced Eclipse (2015-17)
D051	Software Design Spec	Detailed Software Design Specification
D060	Coding Standard, Rev 1.1, 1-Jul-2009	C Coding Standard for Safety Related Software Development
D074	SC-1260.1AMDL 705 3X HART 5 TO 6 TESTING.xlsx, 20-Jun-2011	Validation Test Results
D074b	M705 3x HART 5 to 6 Upgrade Common Practice Commands Tests.pdf, 1-Apr-2011	Validation Test Results 2

Doc ID	File, Version, Date	Document Name
D074c	M705 3x HART 5 to 6 Upgrade Data Link Layer Tests.pdf, 1-Apr-2011	Validation Test Results 3
D074d	M705 3x HART 5 to 6 Upgrade Universal Commands Tests.pdf, 1-Apr-2011	Validation Test Results 4
D074e	Exida summary of Rev N schematic changes for Fid Ticks over temperature.xlsx, 1-Apr-2011	Validation Test Results 5
D076	EMC Test Results, 28-Oct-2005	EMC CE COMPLIANCE TEST REPORT Enhanced Model 705 Eclipse Transmitter
D077	Fault Injection List Eclipse 3X Test Results 2011-07-12 Rev4.xls, 17-Jul-2011	Eclipse 3X Fault Injection Test Results
D078	Bulletin 57-600.22, Mar-2017	Eclipse Enhanced Model 705 Software v3.x IO Manual
D079	57-651.3 Eclipse 705 SIL IO.pdf, Mar-2012	Safety Manual
D081	ECN 3177-755 screen shot.docx, 6-Jan-2010	Engineering Change Documentation
D082	rptSILFaults050707.doc, 7-Jul-2005	Eclipse 705 3.x FMEDA SIL 1 and SIL 2 Diagnostic Methods
D088	M705 3X HART 5 TO 6 MIGRATION IMPACT ANALYSIS.docx, 28-Mar-2011	Impact Analysis Record

2.4.2 Documentation generated by *exida*

[R1]	Eclipse 3X IEC61508 SafetyCase 1Aug2011.esc	SafetyCase file for Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter
[R2]	MAG 705 V2R1 Safety Case WB-61508 v1.7.2d.xlsm, 22-Dec-2017	SafetyCase Workbook for Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter
[R3]	Eclipse 3X Faults.pdf, 24-Jun-2011	Fault Injection Points on Schematics
[R4]	MAG 09/10-39 R001, V4R1, 8-Dec-2017	FMEDA report, 705-51A* Transmitter
[R5]	Magnetrol 705 PIU Spreadsheet R2.xlsx, R2, 20-Dec-17	Proven In Use Analysis
[R6]	17-11-051 R002, V1R1, 22-Dec-2017	IEC 61508 Functional Safety Assessment for Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter (This document)

2.5 Assessment Approach

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

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 full 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 Enhanced Model 705 3X Guided Radar Level Transmitter. Other product development aspects prior to these modifications were assessed according to Proven-In-Use (PIU) requirements (see section 5.1.6). 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 Enhanced Model 705 3X Guided Radar Level Transmitter, the following evidence aspects have been reviewed:

- FMEDA
- SRS or product specification
- Safety manual
- Instruction manual
- Hardware fault injection test plan and results verification
- EMC and environmental test report
- Validation test results
- Corrective Action and prevention action plan/process
- Software and hardware drawings release process
- PIU data collection procedures and operational excellence calculation (evidence that the equipment is proven-in-use; analysis of field failure rates to ensure that no systematic faults exist in the 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.

3 Product Description

The Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter 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.

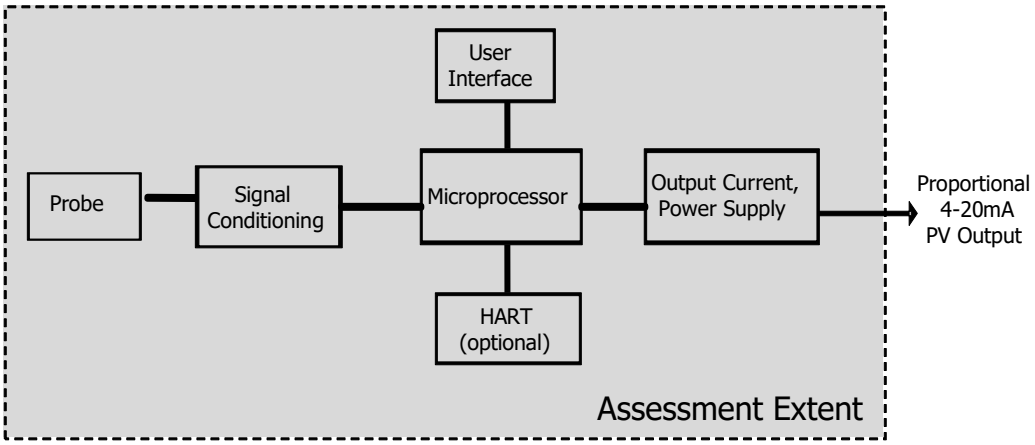


Table 1 lists the versions of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter that have been considered for the hardware assessment.

Table 1 Version overview

Option 1	Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter, 705-51A*-***

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 constant 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.

Choosing the proper Guided Wave Radar (GWR) probe is the most important decision in the application process. The probe configuration establishes fundamental performance characteristics. Coaxial, twin element (rod or cable), and single element (rod or cable) are the three basic configurations. The probe for use with the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter should be selected as appropriate for the application. Careful selection of probe design and materials for a specific application will minimize media build-up on the probe.

The Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0.

[1] Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

3.1 Scope of Analysis

The following were considered in this analysis:

Digital Board	094-6052, Rev G
Analog Board	094-6051, Rev Q
Wiring Board	094-5062, Rev C

The IEC61508 certified 705-51A*-*** will be distinguished from the previous non-certified version by the serial number. The certification will apply to serial numbers starting at 648100-01-001.

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Magnetrol International, Inc. for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1].

All objectives have been successfully considered in the Magnetrol International, Inc. development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements before the development audit.

The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Magnetrol International, Inc. Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter, with IEC 61508.

The assessment was executed using the exida certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements and constraints 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.

As part of the accredited *exida* certification scheme, a surveillance audit is conducted prior to renewal of the certificate. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person(s) in respect to the modifications made.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which shall indicate with respect to the modification:
  - The initiating problem (e.g., results of root cause analysis)
  - The effect on the product / system
  - The elements/components that are subject to the modification
  - The extent of any re-testing
- List of modified documentation
- Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R4] of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter to document the hardware architecture and failure behavior. The FMEDA report and the Safety Case created for the 705-51A* Transmitter documents this assessment.

exida assessed failure history of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter [D030 - D031b] and performed a detailed analysis of the data provided [R5]. This PIU assessment was done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the 705-51A* Transmitter documents this assessment.

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

The Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter complies with the relevant requirements of IEC 61508 SIL 3 applications 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 Validation

Validation Testing results were reviewed via a set of documented tests [D074 – D076]. As the 705-51A* Transmitter consists of simple electrical devices with a straightforward safety function, there is no separate integration testing necessary.

Procedures are in place for corrective actions to be taken when tests fail as documented in [D40].

Items from IEC **61508-2, Table B.3** include functional testing, project management, documentation, and black-box testing (for the considered devices this is similar to functional testing). Field experience and proven-in-use data are included for systematic capability. This meets SIL 3.

Items from IEC **61508-2, Table B.5** include functional testing and functional testing under environmental conditions, interference surge immunity testing, fault insertion testing, project management, documentation, static analysis, dynamic analysis, and failure analysis, expanded functional testing and black-box testing. This meets SIL 3.

5.1.2 Modifications

Modifications are done per the Magnetrol International, Inc. Modification Procedures [D023], [D024] and [D081]. Impact Analyses are performed on changes to safety certified products [D088]. This meets SIL 3.

5.1.3 User documentation

Magnetrol International, Inc. created a Safety Manual for the 705-51A* Transmitter, see [D079]. This safety manual was assessed by *exida.* The final version is considered to be in compliance with the requirements of IEC 61508. The document includes all required reliability data and operations, maintenance, and proof test procedures.

5.1.4 Proven In Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation [R5] was performed on the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter. Shipment records were used to determine that the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter has greater than 45 million operating hours and has demonstrated a field failure rate less than the predicted failure rates indicated in the FMEDA reports. All components considered in the FMEDA are standard components with greater than 100 million operating hours, and diagnostic coverage is shown to be greater than 60% [R4]. This provides justification for using a Route 2_H approach.

The analysis shows that the 705-51A* Transmitter meets the systematic capability requirements of IEC 61508 SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the 705-51A* Transmitter, a Failure Modes, Effects, and Diagnostic Analysis was reviewed by *exida*. This is documented in [R4]. The FMEDA was verified using Fault Injection Testing, see [D077].

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. An FMEDA (Failure Mode Effect and Diagnostic Analysis) 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.

According to IEC 61508-2 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 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H.

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 meet the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the 705-51A* Transmitter 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 architectural constraint type for the 705-51A* Transmitter is B. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

The analysis shows that the design of the 705-51A* Transmitter meets the hardware requirements of IEC 61508 SIL 2, single device (HFT=0) and SIL 3, multiple devices (HFT=1).

6 2020 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Magnetrol International, Inc.	Manufacturer of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Magnetrol International, Inc. contracted *exida* in Jan 2021 to perform the surveillance audit for the above Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter. The surveillance audit was conducted from Sellersville, PA, with the Magnetrol International, Inc.'s facility in Aurora, IL, USA during January 2021.

6.2 Surveillance Methodology

As part of the IEC 61508 functional safety surveillance audit the following aspects have been reviewed:

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if any of the changes could affect the safety function of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the exida Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

6.2.1 Documentation provided by Magnetrol International, Inc.

Doc. ID	Project Document Filename	Version	Date
D101	QAM-001.pdf	Rev. 28	2/28/2020
D102	Business Development		8/27/2013
D103	Dev Process Steps.xlsx		
D104	Electrical Design Methodology.docx	Rev. 1	3/8/2019
D105	Mechanical Design Methodology.docx	Rev. 1	2/11/2019
D106	SDD-001.pdf	Rev. 2	11/10/2017
D107	SPD-005.pdf	Rev. 1	1/11/2019
D108	Technical Product Support	Many	1/29/2021
D109	WGS-002.pdf	Rev. 0	4/25/2017
D110	Magnetrol Training Course - Service Cloud - RMA.pptx		12/15/2015
D111	SQA-038.pdf	Rev. 7	10/3/2019
D112	SQS-001.pdf	Rev. 2	3/1/2018
D113	SQS-003.pdf	Rev. 3	9/30/2019
D114	WQS-001.pdf	Rev. 2	5/14/2019
D115	SQS-004.pdf	Rev. 3	9/30/2019
D116	Product Change Request 9 Firmware Issue 197.docx	Screenshot	
D117	SQA-001.pdf	Rev. 1	7/10/2018
D118	SCE-001.pdf	Rev. 1	12/13/2018
D119	Software Development Methodology.doc		9/4/2015
D120	SPD-006.pdf	Rev. 0	10/13/2017
D121	Tool HAZOP Template.doc	Rev. B	
D122	Impact Analysis Template.doc	Rev. B	
D123	C Language Coding Standard for Firmware Development v 1.9 Highlighted.doc	Rev. 1.9	3/8/2016
D124	Eclipse Model 705 3X Functional Safety Management Plan R1 RELEASED 062518.doc		1/8/2021
D125	57-651.5 Eclipse Enhanced Model 705-51A SIL Certified Safety Manual IO_PROOF1.pdf		2/2/2021
D126	Eclipse Enhanced Model 705 IO.pdf		1/11/2021
D127	705 SIL 2 Changes 2017-2020.xlsx		1/25/2021
D128	705 RMA Date Dec 2014- Oct 2017 SIL Data.xlsx		1/15/2021
D129	ECNs	Many	

6.2.2 Surveillance Documentation generated by *exida*

[R7]	MAG 20-10-059 SACL01 V1R0 Surveillance Audit Checklist - Eclipse 705.xlsx	Surveillance Audit Checklist
[R8]	MAG 20-10-059 FFA01 V1R0 Field Failure Analysis - Eclipse 705.xlsx	Field Failure Analysis

6.3 Surveillance Results

6.3.1 Procedure Changes

Changes to quality and development procedures were reviewed and were found to be consistent with the requirements of IEC 61508. The document identification conventions for some procedures had been changed so some of the changes were simply new identifiers. The baseline safety case was updated.

6.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period. ECNs for minor changes were reviewed and all documentation was found to be acceptable.

6.3.3 Impact Analysis

All required impact analyses were completed properly.

6.3.4 Field History

The field histories of these products were analyzed and found to be consistent with the failure rates predicted by the FMEDA.

6.3.5 Safety Manual

Changes to the updated safety manual were reviewed and found to be compliant with IEC 61508:2010.

6.3.6 FMEDA Update

The FMEDA did not need to be updated for the changes made to the product as the changes were not safety related.

6.3.7 Evaluate use of certificate and/or certification mark

The Magnetrol International, Inc. website was searched and no misleading or misuse of the certification or certification marks was found.

6.3.8 Previous Recommendations

There were no previous recommendations to be assessed at this audit.

6.4 Surveillance Audit Conclusion

The result of the Surveillance Audit Assessment can be summarized by the following observations:

The Magnetrol International, Inc. Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter continues to meet the relevant requirements of IEC 61508 for SIL 3 applications based on the initial assessment and considering:

- field failure history

- permitted modifications completed on the product

This conclusion is supported by the updated safety case and certification documents.

7 Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
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
HART	Highway Addressable Remote Transducer
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.
PFD_{avg}	Average Probability of Failure on Demand
PIU	Proven In Use
Random Capability	The SIL limit imposed by the PFD_{avg} for each element.
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).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
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

8 Status of the document

8.1 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.

8.2 Version History

Contract Number	Report Number	Revision Notes
Q20/10-059	MAG 17-11-051 R003 V2R0	2020 Surveillance Audit; DEB, 2/3/2021
Q17/11/-051	MAG 17-11-051 R002 V1R1	Re-Certified and updated to 61508:2010; GPS, 22-Dec-2017 *Note: This version supersedes and replaces all versions of the previous assessment report MAG 09/10-39 R005*

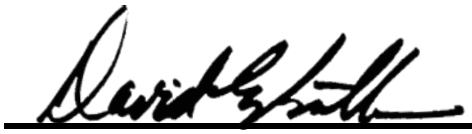
Review: Loren Stewart, V2R0, 2/4/2021

Status: Released

8.3 Future Enhancements

At request of client.

8.4 Release Signatures



David E. Butler, CFSE, exidaCSP, Sr. Safety Engineer

Loren L. Stewart, CFSE, Sr. Safety Engineer