exida®

61508 SIL 3 CAPABLE

IEC 61508 Functional Safety Assessment

Project:

Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter

Customer:

Magnetrol International, Inc.
Downers Grove, IL
USA

Contract No.: Q09/10-39
Report No.: MAG 09/10-39-R005
Version V1, Revision R3, August 5, 2011
Griff Francis

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

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the:

Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter

The functional safety assessment performed by *exida* consisted of the following activities:

- *exida* assessed the systematic capability through an analysis of proven-in-use data and creation of a detailed safety case against the requirements of IEC 61508.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3. All documents referenced in sections 2.4.1 and 2.4.2 were reviewed and form the basis of this assessment.

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

The Eclipse Enhanced Model 705 3X Level Transmitter was found to meet the requirements of SIL 2 for random integrity @HFT=0, SIL 3 for random integrity @ HFT=1 and SIL 3 for systematic capability.

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

Table of Contents

Management Summary 2

1 Purpose and Scope 4

2 Project management 5

2.1 *exida* 5

2.2 Roles of the parties involved 5

2.3 Standards / Literature used 5

2.4 Reference documents 5

2.4.1 Documentation provided by Magnetrol International, Inc. 5

2.4.2 Documentation generated by *exida* 7

3 Product Description 8

3.1 Scope of Analysis 9

4 IEC 61508 Functional Safety Assessment 9

4.1 Methodology 9

4.2 Assessment level 10

5 Results of the IEC 61508 Functional Safety Assessment 11

5.1.1 Validation 11

5.1.2 Modifications 11

5.1.3 User documentation 11

5.2 Hardware Assessment 12

Terms and Definitions 14

6 Status of the document 15

6.1 Liability 15

6.2 Releases 15

6.3 Future Enhancements 15

6.4 Release Signatures 15

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device excluding the modification process. Certification is based primarily on Proven In Use where any changes to the safety critical portion product require recertification.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 3.

This document shall describe the results of the IEC 61508 functional safety assessment of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter.

2 Project management

2.1 *exida*

exida is one of the world's leading product certification 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 product manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database of process equipment.

2.2 Roles of the parties involved

Magnetrol International, Inc.	Manufacturer of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter
exida	Provided services to support Magnetrol during the evaluation of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter
exida	Performed the IEC 61508 Functional Safety Assessment according to option 2 (see section 1)

Magnetrol International, Inc. contracted *exida* in October 2009 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): 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Magnetrol International, Inc.

	[Safety Case Doc]; rev; date	**description**
[D1]	[D01]; V0R1; 6/3/2010	Functional Safety Management Plan - Not required for PIU with modification restrictions, included for reference
[D2]	[D110]; 10/28/2005	EMC CE COMPLIANCE TEST REPORT Enhanced Model 705 Eclipse Transmitter
[D3]	[D111]; 11/1/2003	WIB Evaluation of Eclipse 705
[D4]	[D119]; 3/29/2011	exida Validation Test Execution Phase Checklist
[D5]	[D150];	exida Functional Safety Assessment Phase Verification

		Checklist
[D6]	[D160]; 6/1/2010	Product Safety Manual
[D7]	[D161]; NA; 7/20/2010	exida Safety Manual Checklist
[D8]	[D162]; 9/1/2007	Eclipse 3X Installation and Operating Manual
[D9]	[D165]; V3R1; 2/11/2010	Failure Modes, Effects and Diagnostics Analysis (FMEDA) Report
[D10]	[D166];	exida FMEDA Document Checklist
[D11]	[D181]; Rev 12; 7/12/2011	Engineering Change Request And Change Notice
[D12]	[D189]; 3/29/2011	exida Modification Phase Verification Checklist
[D13]	[D20]; 5/31/2011	ISO 9001 Certificate
[D14]	[D21]; Rev 1.3; 12/4/2009	Magnetrol SAFETY CRITICAL PRODUCT DEVELOPMENT AND MAINTENANCE
[D15]	[D22]; Rev 23; 8/3/2009	Quality Management System Manual
[D16]	[D23]; Rev 1.1; 7/1/2009	C Coding Standard for Safety Related Software Development
[D17]	[D24]; Rev 14; 7/21/2010	Supply Base Control Plan (Vendor Qualification Procedure)
[D18]	[D25]; 7/27/2009	Magnetrol Software Development Methodology
[D19]	[D26];	Safety Training Records
[D20]	[D27]; Rev 1; 12/16/2010	RMA Processing
[D21]	[D28]; Rev 4; 7/29/2010	Corrective Action Procedure
[D22]	[D29]; Rev 0; 7/14/2011	Customer Notification
[D23]	[D30]; V0 R2; 7/12/2011	Safety Requirements Specification - Not required for PIU with modification restrictions; added for reference
[D24]	[D31];	exida SRS Document Checklist
[D25]	[D32]; 7/13/2011	Safety Requirements Specification Review Meeting Minutes
[D26]	[D45]; 6/2/2005	Enhanced Model 705 Warnings and Faults for SIL 1 and SIL 2
[D27]	[D46]; V1R1; 4/29/2011	Proven Operational Experience Calculation and Report
[D28]	[D47]; 4/29/2011	Eclipse 3X Proven In Use Data
[D29]	[D48]; 3/29/2011	exida Proven In Use Checklist
[D30]	[D53]; 4/5/2010	Fault Injection Test Plan
[D31]	[D54];	exida HW Fault Injection Test Verification Checklist
[D32]	[D55]; see individual schematics;	Eclipse 3x Schematics
[D33]	[D56];	Eclipse 3x schematics with fault injection points
[D34]	[D57]; Rev4; 7/15/2011	Fault Injection Test Results

[D35]	[D68]; 7/26/2011	Component Level FMEDA
[D36]	[D71];	Detailed Software Design Specifications
[D37]	[D80]; 1.0; 6/9/2010	IEC 61508 Tables not covered in FSM Plan

2.4.2 Documentation generated by *exida*

[R1]	MAG 09-10-39 R005 V1R3 IEC 61508 Assessment Eclipse 3X, 5 August 2011	IEC 61508 Functional Safety Assessment, Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter (this report)
[R2]	MAG 09/10-39 R001 V3R1 FMEDA Report , 26 July 2011	Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter FMEDA Report
[R3]	MAG 09/10-39 R004 V1R1 PIU Report , 29 Apr 2011	Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter PIU Analysis-Report

3 Product Description

The Eclipse Enhanced Model 705 Guided Wave 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.

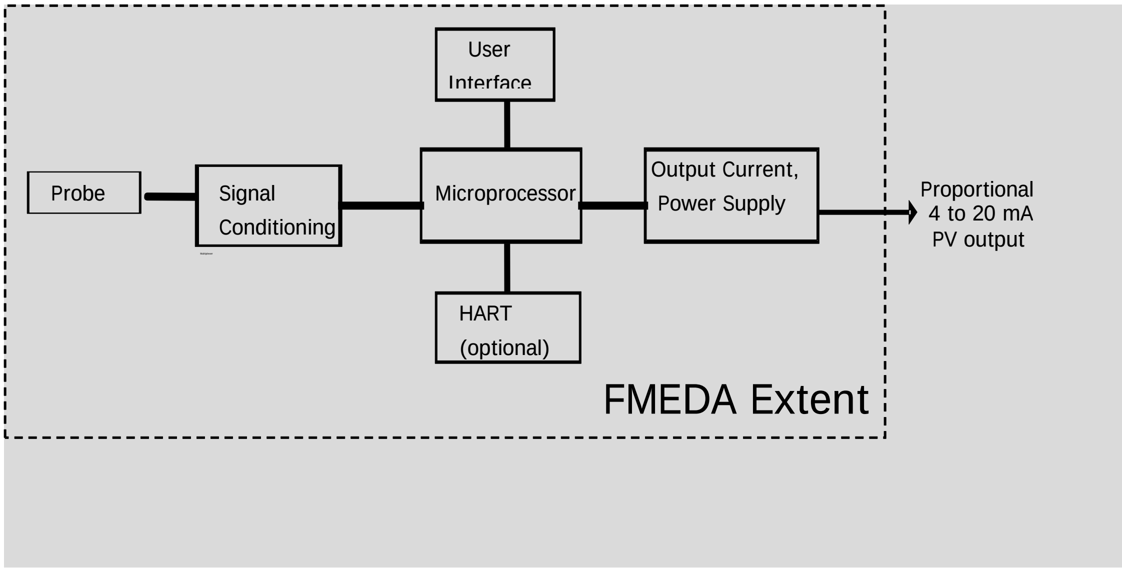

Table 1 lists the versions of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter that have been considered for the hardware assessment.

Table 1 Version overview

	Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter, 705-51Ax-xxx

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.

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.

3.1 Scope of Analysis

The following were considered in this analysis:

Digital Board	094-6052, Rev F
Analog Board	094-6051 Rev M
Wiring Board	094-5062, Rev A

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

The IEC 61508 Functional Safety Assessment was performed based on the information received from Magnetrol International, Inc. and is documented in this section.

4.1 Methodology

As part of the IEC 61508 functional safety assessment, the following aspects have been reviewed:

Documents:

- FMEDA
- safety manual
- instruction manual
- HW fault inject test plan and results verification
- SW design specification
- EMC test report
- Validation test results
- Corrective Action and prevention action plan/process

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 IEC 61508 PIU assessment, the following aspects have been reviewed:

- PIU data 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)

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

- A number of functional safety lifecycle assessment aspects are not required due to PIU assessment:
  - SRS
  - FSM Plan
  - Configuration management
  - Validation of development tools
  - Validation test plan
  - Architecture design
  - Integration and Unit test plans
  - Development process

4.2 Assessment level

The Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter has been assessed per IEC 61508 to the following levels:

- SIL 2 random integrity for single device (Hardware Fault Tolerance = 0)
- SIL 3 random integrity for multiple devices (Hardware Fault Tolerance = 1)

The development procedures were assessed according to PIU criteria as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3 capability) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R2] of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter to document the hardware architecture and failure behavior. The Safety Case created for the Eclipse Enhanced Model 705 3X documents this assessment.

exida assessed failure history of the Eclipse Enhanced Model 705 3X Guided Radar Level Transmitter see [D28] and performed a detailed analysis of the data provided, see [D27]. This PIU assessment is done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the Eclipse Enhanced Model 705 3X documents this assessment.

The requirements of SIL 3 have been met in this area.

5.1.1 Validation

Validation Testing results were reviewed via a set of documented tests (see [D2] and [D3]). As the Eclipse Enhanced Model 705 3X 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 [D25].

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 not permitted to the safety critical portion of the Eclipse Enhanced Model 705 3X as part of this Proven-In-Use certification. Recertification is required for safety critical product changes.

5.1.3 User documentation

Magnetrol International, Inc. created a Safety Manual for the Eclipse Enhanced Model 705 3X, see [D6]. 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.

The analysis shows that the Eclipse Enhanced Model 705 3X meets the systematic capability requirements of IEC 61508 SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the Eclipse Enhanced Model 705 3X, a Failure Modes, Effects, and Diagnostic Analysis was performed by exida. This is documented in [R2]. The FMEDA was verified using Fault Injection Testing, see [D34].

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.

From the FMEDA, failure rates are derived for each important failure category. Table 2 lists these failure rates separately for each output type as reported in the FMEDA reports. The failure rates are valid for the useful life of the devices. Table 3 lists sample PFD_{AVG} results.

Table 2 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}[2]	λ_{dd}	λ_{du}	SFF
Eclipse Enhanced Model 705, 705-51A*-***, Low Trip	0 FIT	600 FIT	847 FIT	154 FIT	90.4%
Eclipse Enhanced Model 705, 705-51A*-***, High Trip	0 FIT	624 FIT	847 FIT	130 FIT	91.9%

Table 3 Sample PFD_{AVG} Results

Device	Proof Test Coverage	PFD_{AVG}	% of SIL 2 Range
Eclipse Enhanced Model 705 3X, 705-51A*-***	94%	1.06E-03	10.6%

For low demand SIL 2 applications, the PFD_{AVG} value of the Safety Instrumented Function needs to be $\geq 10^{-3}$ and $< 10^{-2}$. The FMEDA report [R2] lists the percentage of this budget that the Eclipse Enhanced Model 705 3X uses. Considering a proof test is performed every year, the Eclipse Enhanced Model 705 3X model uses 10.6% of the PFD_{AVG} budget.

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 safety instrumented function (SIF) to verify the design of that SIF.

[2] It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

The architectural constraints requirements of IEC 61508-2, Table 2, are also reviewed. The Safe Failure Fractions (SFF) for both Eclipse Enhanced Model 705 3X configurations are greater than 90%. Therefore the Eclipse Enhanced Model 705 3X can be used in SIL 2 applications, in simplex (single device, HFT = 0) mode and SIL 3 applications in redundant (multiple devices, HFT = 1) mode.

The analysis shows that the design of the Eclipse Enhanced Model 705 3X meets the hardware requirements of IEC 61508 SIL 2, single device (HFT = 0) and SIL 3, multiple devices (HFT = 1).

Terms and Definitions

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 frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
PIU	Proven-In-Use
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).
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
Type A (sub)system	“Non-Complex” (sub)system (using discrete elements); for details see 7.4.4.1.2 of IEC 61508-2
Type B (sub)system	“Complex” (sub)system (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

6 Status of the document

6.1 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.

6.2 Releases

Version:	V1	
Revision:	R3	
Version History:	V0, R1:	Internal Draft; 15 July, 2011
	V1, R1:	ready to release, but changed SIL after final review
	V1, R2:	changed p4 and p11 to clarify the restriction on the safety critical portion only
	V1, R3:	released
Author:	Griff Francis	
Review:	V0, R1:	Rudolf Chalupa
	V1, R1	Rudolf Chalupa
Release status:	Released to Customer	

6.3 Future Enhancements

At request of client.

6.4 Release Signatures

Griff Francis

Griff Francis, Safety Engineer

Rudolf P. Chalupa

Rudolf Chalupa, Senior Safety Engineer