IEC 61508 Functional Safety Assessment

Project:

Rosemount 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter
Device Label SW 2.A1 – 2.J0

Customer:

Rosemount Tank Radar
(an Emerson Process Management company)
Gothenburg, Sweden

Contract No.: Q13/06-005
Report No.: ROS 13-06-005 R002
Version V1, Revision R2, March 31, 2014
John Yozallinas

Management Summary

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

5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter

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

- *exida* assessed the development process used by Rosemount Tank Radar through an audit 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.
- *exida* reviewed field failure data to ensure that the FMEDA analysis was complete.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3. A full IEC 61508 Safety Case was prepared, using the *exida* SafetyCase Workbook as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also the user documentation (safety manual) was reviewed.

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

The 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter was found to meet the Random Capability requirements for a Type B element of SIL 2@HFT=0 and SIL 3@HFT=1 and the Systematic Capability requirements for SC 3 (SIL 3 Capable).

The manufacturer will be entitled to use the following Functional Safety Logos.

Table of Contents

1 Purpose and Scope

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

- 5300 4-20mA HART Guided Wave Radar Level and Interface Transmitter

by *exida* according to the requirements of IEC 61508: ed2, 2010.

The result of this assessment 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.

Table 1: Revisions in Assessment Scope

5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter	
Hardware	Model 5301HxxxxxxxxxxxxxxZZ Model 5302HxxxxxxxxxxxxxxZZ Model 5303HxxxxxxxxxxxxxxZZ (Note: transmitters will be marked with “QS” or “QT” at the end of the model number in place of ZZ above)
Software/Firmware	2.A1 – 2.J0

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.

2.2 Roles of the parties involved

Rosemount Tank Radar	Manufacturer of the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter
exida	Performed the IEC 61508 Functional Safety Assessment

Rosemount Tank Radar 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 Rosemount Tank Radar

(Doc IDs are references to the documents within the Safety Case)

Doc ID	Generic Document Name
D001	Quality Manual
D003	Overall Development Process - RPD process
D004b	Configuration Management Process - in SW Development Process
D006	Field Return Procedure
D007	Manufacturer Qualification Procedure
D008	Part Selection Procedure
D010	Quality Management System (QMS) Documentation Change Procedure
D012	Non-Conformance Reporting procedure
D013	Corrective Action Procedure
D016	Action Item List Tracking Procedure - Design Review Guidelines
D019	Customer Notification Procedure – DOP1440
D023	Modification Procedure – Product Change Process
D023b	Modification Procedure - Impact Analysis Template
D023d	Modification Procedure - Failure Analysis Review Procedure
D023e	Modification Procedure - Change Control Board Charter
D030	Shipment Records
D031	Field Returns Records
D033	Training and Competency Records
D036	ISO 900x Cert or equivalent
D040	Safety Requirements Specification
D074	Validation Test Results
D075	Environmental Test Results
D076	EMC Test Results
D077	Fault Injection Test Results
D078	Operation / Maintenance Manual
D079	Safety Manual
D079b	Software Release Notes
D081	Engineering Change Documentation
D082	List of Diagnostics from FMEDA
D087	Digital Signature
D088	Impact Analysis Record

2.5 Documentation generated by *exida*

[R1]	Q13-06-005 - Rosemount 5300 Series Assessment V0R3	Safety Case file for 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter
[R2]	ROS 13-06-005 R002 V1_R2 Assessment Report 5300.Docx	IEC 61508 Functional Safety Assessment for 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter (This document)
[R3]	Q1306005 5300 FMEDA V1R4 Report	IEC 61508 FMEDA for 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter

3 Product Description

The 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter is a smart, two-wire continuous level transmitter based on Time Domain Reflectometry (TDR) principles. Low power nano-second-pulses are guided along an immersed probe. When a pulse reaches the surface, part of the energy is reflected back to the transmitter, and the time difference between the generated and reflected pulse is converted into a distance which calculates the total level or interface level.

It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. For safety instrumented systems usage, the 4 – 20 mA output is used as the primary safety variable. The 5300 Series Level Transmitter is classified as a type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Rosemount Tank Radar and is documented in the safety case database [R1].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software modifications to achieve SIL 3 capability. Other product development aspects prior to these modifications were assessed according to Proven-In-Use 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.

Additionally, 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 61508 compliant design process.

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

Documents:

- FMEDA
- Safety manual
- Instruction manual
- SRS
- HW fault inject test plan and results verification
- EMC and Environmental test results
- Validation test results
- Corrective Action and prevention action plan/process
- Modification Process
- Impact Analysis Records

One ASIC is used in this product. As part of the Proven In Use analysis, it is considered as a standard component in the FMEDA due to the number of operational hours.

No safety related communications are used in this product.

Proven-In-Use (PIU) data assessment [D030] and [D031] 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)
- A number of functional safety lifecycle assessment aspects are not required due to PIU assessment with no future changes permitted:

- SW design specification
- Configuration management
- Validation of development tools
- Validation test plan
- Architecture design
- Integration and Unit test plans

- Product design
  - Hardware architecture and failure behavior, documented in a FMEDA

The review of the development procedures is described in section 5. The review of the product design is described in section 5.2.

4.2 Assessment level

The 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter has been assessed per IEC 61508 to the following levels:

- Systematic Capability SC3 (SIL 3 capability) suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3) according to IEC 61508.
- Architecture Constraint limitations of SIL 2 for a single device and SIL 3 for multiple devices in safety redundant configurations with a Hardware Fault Tolerance of 1.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R3] of the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter to document the hardware architecture and failure behavior. The Safety Case created for the 5300 Series Level Transmitter documents this assessment.

exida assessed failure and operational history of the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter [D030, D031] and performed a detailed analysis of the data provided . This PIU assessment is done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the 5300 Series Level Transmitter documents this assessment.

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

5.1 Lifecycle Activities and Fault Avoidance Measures

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The assessment is supplemented by the PIU analysis. The result of the assessment can be summarized by the following observations:

The audited development process complies with the relevant managerial requirements of IEC 61508 SIL 3 for Route 2s.

5.1.1 Functional Safety Management

Version Control
All documents are under version control as required by [D004b]

Training and Competency recording
Competency is ensured by the maintenance of a competency and training list for the project. The competency document [D033] lists all of those on the project who are working on any of the phases of the safety lifecycle.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D003], a requirements specification is created for all products. For the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter, the requirements specification [D040] contains a system overview, safety assumptions, and safety requirements sections. During the assessment, *exida* reviewed the content of the specification for completeness per the requirements of IEC 61508:2010.

Requirements from **IEC 61508-2, Table B.1** that have been met by Rosemount Tank Radar include project management, documentation, structured specification, and inspection of the specification.

5.1.3 Design

Hardware design, including both electrical and mechanical design, was reviewed as part of the Failure Modes, Effects and Diagnostic Analysis (FMEDA), electrical unit testing, fault injection testing, and review of modifications during the product lifetime.

Requirements from **IEC 61508-2, Table B.2** that have been met by Rosemount Tank Radar include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, computer aided design tools, simulation, and inspection of the specification. This meets the requirements of SIL 3.

5.1.4 Validation

Validation Testing results were reviewed via a set of documented functional tests [D074]. As the 5300 Series Level 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 failures occur as documented in [D006, D012].

Items from IEC **61508-2, Table B.5** include project management, documentation, and black-box 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** included functional testing [D074] and functional testing under environmental conditions [D075], Interference surge immunity testing [D076], fault insertion testing [D077], project management, documentation, static analysis, dynamic analysis, and failure analysis. This meets SIL 3.

5.1.5 Verification

Verification activities are built into the standard development process as defined in [D003] and [D0088]. Verification activities include the following: Fault Injection Testing, FMEDA, and peer reviews. This meets the requirements of IEC 61508 SIL 3.

Requirements from **IEC 61508-2, Table B.3** that have been met by Rosemount Tank Radar include functional testing, project management, documentation, and black-box testing.

Requirements from **IEC 61508-3, Table A.5** that have been met by Rosemount Tank Radar include dynamic analysis and testing, data recording and analysis, functional and black-box testing, and performance testing.

Requirements from **IEC 61508-3, Table A.6** that have been met by Rosemount Tank Radar include functional and black box testing, and performance testing.

Requirements from **IEC 61508-3, Table A.9** that have been met include static analysis, dynamic analysis and testing.

This meets the requirements of SIL 3.

5.1.6 Proven In Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was carried out on the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter. Shipment and field failure records [D030 and D031] were used to determine that the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter have >100 million operating hours and they have demonstrated a field failure rate less than the predicted failure rates indicated in the FMEDA reports. This meets the requirements for Proven In Use for SIL 3.

5.1.7 Modifications

No future modifications are permitted to the certified versions of the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter without reassessment.

5.1.8 User Documentation

Rosemount Tank Radar created a safety manual for the 5300 Series 4-20mA HART Guided Wave Radar Level and Interface Transmitter [D079] which addresses all relevant operation and maintenance requirements from IEC 61508. This safety manual was assessed by *exida*. The final version is considered to be in compliance with the requirements of IEC 61508.

Requirements from IEC **61508-2, Table B.4** that have been met by Rosemount Tank Radar include operation and maintenance instructions, maintenance friendliness, project management, documentation, and limited operation possibilities.

This meets the requirements for SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the 5300 Series Level Transmitter, a Failure Modes, Effects, and Diagnostic Analysis was performed by Rosemount and reviewed by *exida* for each component in the system. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing as part of the development [D077] and as part of the IEC 61508 assessment.

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.

Failure rates are for each important failure category. All failure rate analysis results and useful life limitations are listed in the FMEDA report [R3]. Tables in the FMEDA report list these failure rates for the various configurations of the 5300 Series Level Transmitter. The failure rates listed are valid for the useful life of the devices.

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.

The FMEDA analysis shows that the 5300 Series Level Transmitter has a Safe Failure Fraction > 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore these models meet Route 1H hardware architectural constraints for up to SIL 2 as a single device and up to SIL 3 with Hardware Fault Tolerance of 1.

The failure rate data used for this analysis meets the exida criteria for Route 2H and the diagnostic coverage is ≥60%. Therefore all of the reviewed 5300 Series Level Transmitter meets the Route 2H hardware architectural constraints for up to SIL 2 as a single device when the listed failure rates are used.

If the 5300 Series Level Transmitter is one part of an element, the architectural constraints should be determined for the entire sensor element.

The architectural constraint type for the 5300 Series Level Transmitter is B. The required SIL determines the level of hardware fault tolerance that is required per requirements of IEC 61508 or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

The analysis shows that the design of the 5300 Series Level Transmitter meets the hardware requirements of IEC 61508, SIL 2 @HFT=0 and SIL 3 @ HFT=1.

6 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 demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{AVG}	Average Probability of Failure on Demand (low demand mode)
PFH	Probability of dangerous Failure per Hour (high demand mode)
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).
Systematic Capability	The SIL limit imposed by the robustness of the design process and the methods used to avoid systematic faults in the design as described in the IEC 61508 tables.
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:	V1	
Revision:	R2	
Version History:	V1, R2:	Updated the revision of the FMEDA Report; DEB 3/31/2014
	V1, R1:	Internal review completed 14-Oct-13 JCY
	V1, R0:	Generated from Safety Case and revised per comments after review;

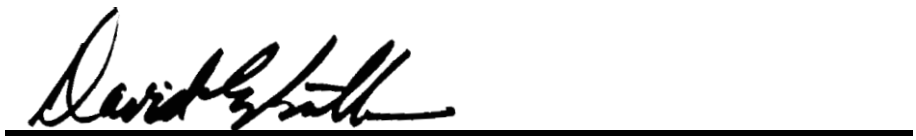
Authors: John Yozallinas
Review: Dave Butler
Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

John Yozallinas, Senior Safety Engineer



Dave Butler, Senior Safety Engineer