Results of the IEC 61508 Functional Safety Assessment

Project:

Rosemount^{TM} 5408 Level Transmitter

Customer:

Rosemount Tank Radar
Sweden

Contract No.: Q22-09-072
Report No.: ROS 15-01-149 R001
Version V2, Revision R1, December 28, 2022
Loren Stewart

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

Management Summary

The Functional Safety Assessment of the Rosemount 5408 Level Transmitter (4-20mA output version with HART) development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Rosemount Tank Radar 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 Rosemount Tank Radar.

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 Rosemount Tank Radar for their Rosemount 5408 Level Transmitter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Rosemount 5408 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 (HFT = 1) according to table 3 of IEC 61508-1.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Rosemount 5408 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 (HFT = 1) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the Rosemount 5408 Level Transmitter meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the Rosemount 5408 Level Transmitter is capable for use in SIL 3 applications in Low or High demand mode 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 of this document.

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

CERTIFIED
IEC 61508
SIL 3 CAPABLE
exida
FS

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Rosemount 5408 Level Transmitter (4-20mA output version with HART) 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 Rosemount 5408 Level Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the Rosemount 5408 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 Rosemount 5408 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 by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

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

The assessment was planned by *exida* agreed with Rosemount Tank Radar.

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 500 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

Rosemount Tank Radar	Manufacturer of the Rosemount 5408 Level Transmitter
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

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

Note: Documents revised after the previous audit are updated in the tables below.

2.4.1 Documentation provided by Rosemount Tank Radar

ID	Document	Filename	Version	Date
D001	Quality Manual; Part Numbering Convention	DOC-002740 (RTR Quality Manual).pdf	Rev 12	2021-12-02
D003	Overall Development Process - RPD process	DOC-002735 (RTR Product Design and Development Process).docx	Rev 1.0	2017-03-17
D003b	Overall Development Process	DOC-006493 (New Product Development Process).pdf	Rev 8	2021-12-16
D004	Configuration Management Process - Part Number Mgt. System Guide	DOC-006687 (Configuration and Change Management Work Instruction)	Rev 7	2018-04-20

ID	Document	Filename	Version	Date
D004c	Configuration Management Process-Part Number Convention	Part numbering convention 0300-19-505.docx	1	online export
D004d	Configuration Management Process	0100-23-1802 (Rosemount Inc Record Retention Schedule).pdf	Rev 12	Aug 2020
D004e	Configuration Management Process-Part Number Mgt System	DOC-003099 (Part numbering convention)	Rev 1.0	2017-03-17
D004f	Configuration Management Process-Record Archival, non-SW	Archiving of engineering files_EMA00000M7D.docx	3	21-Feb-13
D004g	Configuration Management Process-Record Retention 2	Principal Record Retention Periods - Sweden 0300-19-532.doc	3	Apr.2010, export
D005	Field Failure Reporting Procedure	DOC-002943 (RMA Return Documentation).pdf	Rev. 4	2021-12-27
D005b	Field Failure Evaluation Procedure	0100-23-548 (RMT Failure Analysis Process).pdf	2	online export
D006	Field Return Procedure	DOC-002943 (RMA Return Documentation).pdf	Rev. 4	2021-12-27
D007	Manufacturer Qualification Procedure	DOC-003125 (Supplier Evaluation and Approval Process Description - RTR).docx	Rev. 1.0	2018-12-04
D008	Part Selection Procedure	DOC-002990 (Production Part Approval Process (PPAP)).docx	Rev.3	2020-09-18
D010	Quality Management System (QMS) Documentation Change Procedure	DOC-002681 (Document management - Department documents).docx	Rev.2	2017-09-15
D010b	Quality Management System (QMS) Documentation Change Procedure	DOC-002968 (Document Management - Product Development Projects).docx	Rev.2	2022-05-25
D010c	Quality Management System (QMS) Documentation Change Procedure	DOC-002682 (Documents and Document management).docx	Rev.14	2022-02-11
D012	Non-Conformance Reporting procedure	DOC-002984 (Corrective Action Process (Parts)).docx	Rev.5	2021-04-19
D013	Corrective Action Procedure	DOC-003179 (Corrective Action Preventive Action (CAPA) Process).docx	Rev 1	Jun.2019
D016	Action Item List Tracking Procedure	DOC-002963 (Design review guidelines at RTR).docx	Rev 1	Jun.2019
D019	Customer Notification Procedure	DOC-006349 (Customer Notification Process).docx	Rev.9	2021-03-04
D021	Software Development Process;	GaugeSW-Instr-0008.doc	Rev 9.1	2020-12-29
D021c	Software Development Guide Patterns	GaugeSW-0089.pdf	Rev.4	2022-06-27

ID	Document	Filename	Version	Date
D023	Modification Procedure	DOC-004408 (Engineering Change (EC) Process).pdf	Rev 14	2021-05-14
D023b	Impact Analysis Template	DOC-003051 (Impact analysis template for SIL approved products).docx	Rev.1	2014-04-16
D026	FSM Plan or Development Plan; Skills Matrix; Management Review Record; Job Descriptions and Competency Levels	Eagle-0038.docx	3	Jun.2016
D026b	FSM Plan or Development Plan	DOC-002735 (RTR Product Design and Development Process).docx	Rev 1.0	2017-03-17
D027	Configuration Management Plan	Eagle-0166.docx	3	2-Jun-16
D027b	Configuration Management RACI	Eagle-0404.xlsx	7	10-Oct-16
D029	Verification Plan	Eagle-Prod_Doc_TH0297 Covers both 5408 & 3408	3	Mar. 2019
D036	ISO 900x Cert or equivalent	RTR ISO 9001_2015_ISO 14001_2015.pdf		July 2024
D038	List of Design Tools; Software Tool Qualification Procedure and Report	GaugeSW-0089.docx	Rev.4	2022-06-27
D040	Safety Requirements Specification	Eagle-Prod_Doc_TH0013 4_0.pdf	11	Aug-20
D041	Safety Requirements Review	Eagle-0200.pdf	1.6	24-Sep-15
D043	Software Requirements Specification	Eagle-0114.pdf	12.2	Oct-22
D043b	Software Requirements Specification	Eagle-0174.docx	6	Jun-22
D045	System Architecture Design Specification	Eagle-Prod_Doc_TH0012 SAD.pdf	1	12-Dec-14
D045b	System Architecture Design Specification-Safety Concept	Eagle-Prod_Doc_TH0024.pdf	3	18-Dec-15
D045c	System Architecture Design FMEA Review	Eagle-Prod_Doc_TH0022.pdf	2.1	Jan-16
D045d	System Architecture Design Overview	System FMEA 5X08_rev_0a.pptx	0a	Jan.2015

D047	Schematics / Circuit Diagrams	Recorded in FMEDA report [R3]
		D7000002-814_0L CMH;
		D7000002-811_01 PMK;
		D7000002-817_02 TMH;
		D7000002-823_01 LDT;
				30-Sep-16

D049	High Level Software Design Specification	Eagle-Prod_Doc_TH0003.docx	2	6-Oct-16
D049b	High Level Software Design Overview for FMEA	SW Overview 150120.pptx	n/a	Jan.2015

ID	Document	Filename	Version	Date
D050	SW HAZOP or Criticality Analysis-MCU-C	Eagle-0238.xls	1	12-Feb-15
D050b	SW HAZOP or Criticality Analysis-MCU-A	Eagle-0244.xls	3	7-Oct-15
D050c	SW HAZOP or Criticality Analysis-MCU-P	Eagle-0247.xls	3	10-Oct-16
D051	Detailed Software Design Specification; Software Modules List	Eagle-Prod_Doc_TH0007.docx	2	10-Oct-16
D051b	Detailed Software Design -Aout CPU spec	Eagle-Prod_Doc_TH0006.docx	2	10-Oct-16
D053	Design Review Record	Eagle-0180.pdf	1	21-Nov-14
D053b	Design Review Record-MCU-P SW	Eagle-0182.pdf	1	25-Nov-14
D055b	FMEDA Report summary	Eagle-Prod_Doc_TH0119 1_8.efm.xls	1.10	Mar-17
D055c	FMEDA Details- Proof test coverage	Eagle-Prod_Doc_TH0167 issue 2.xlsx	2	Oct-20
D056	Requirements Traceability Matrix-design	Eagle-Prod_Doc_TH0105.docx	4	7-Oct-16
D056b	Requirements Traceability Matrix-design2	Eagle-Prod_Doc_TH0104.docx	4	7-Oct-16
D056c	Requirements Traceability Matrix- FW V&V	Eagle-0110.doc	3	6-Oct-16
D057	Software Test Coverage Analysis Report	Eagle-Prod_Doc_TH0166.docx	2	6-Oct-16
D057b	Software Test Coverage Analysis Report 2	Eagle-Prod_Doc_TH0170.docx	1	6-Oct-16
D058	Code Review Record; Module test Plan Review Sample	Eagle-0687.pdf	1	30-Sep-16
D059	Fault Injection Test Plan	Eagle-Prod_Doc_TH0115.pdf	7	23-Sep-16
D059b	Fault Injection Test Plan-SW FIT	Eagle-Prod_Doc_TH0114.docx	1	18-Mar-16
D060	Coding Standard-General	GaugeSW-Instr-0022.docx	2	2-Jul-14
D060b	Coding Standard - UML	GaugeSW-Instr-0014.doc	3	15-Mar-11
D060c	Coding Standard - Code Review	GaugeSW-Instr-0011.doc	5	1-Nov-12
D061	Static Code Analyzer Configuration Description	GaugeSW-Instr-0001.doc	6	13-Feb-14
D064	Module Test Plan- SW	Eagle-Prod_Doc_TH0042.docx	2	7-Oct-16
D064b	Module Test Plan- SW	Eagle-Prod_Doc_TH0073.docx	4	Oct.2016

ID	Document	Filename	Version	Date
D066	Module test Results; Integration Test Results; Static Code Analysis Results	Eagle-Prod_Doc_TH0166.docx	2	6-Oct-16
D066b	Module test Results; Integration Test Results; Static Code Analysis Results	Eagle-Prod_Doc_TH0170.docx	1	7-Oct-16
D067	Integration Test Plan	Eagle-Prod_Doc_TH0073.docx	4	Oct.2016
D067b	Integration Test Plan Template	Eagle-Prod_Doc_TH0044.docx	4	Oct.2016
D069	Validation Test Plan; Environmental Test Plan; EMC Test Plan	Eagle-0210.pdf	2	22-Dec-15
D069b	V&V Plan	Eagle-0453.pdf	1.2	30-Sep-16
D070	Validation Test Plan Review	Eagle-0465.pdf	1	21-Dec-15
D074	Validation Test Results; Environmental Test Results	Eagle-0684.pdf	1	30-Sep-16
D076	EMC Test Results	Eagle-0686.pdf	n/a	13-Sep-16
D077	Fault Injection Test Results -HW	Eagle-Prod_Doc_TH0160.pdf	2	25-Sep-16
D077b	Fault Injection Test Results -SW	Eagle-Prod_Doc_TH0163.pdf	1	16-Sep-16
D079	Safety Manual; Operation / Maintenance Manual	00809-0400-4408_En	AB	Sep-21
D080	Safety Manual Review	Safety Manual Review.xlsm- form	n/a	Online export
D081	Engineering Change Documentation	Eagle-0069.pdf	6	Feb-16
D082	List of Diagnostics for FMEDA	Eagle-0007.pdf	2.3	26-Sep-16
D087	Digital Signature	Eagle-Prod_Doc_TH0048.docx	14.00	6-Oct-16
D088	Impact Analysis Record-example	Raptor-RE-0351.docx	6.00	17-Apr-14
D091	SW Release Notes	Eagle-0651.pdf	1.00	6-Oct-16

2.4.2 Documentation generated by *exida*

[R1]	ROS Eagle V3R1 Safety Case WB-61508 v1.7.2e.xlsm	SafetyCase for the Rosemount 5408 Level Transmitter
[R2]	ROS 14-09-201 R001 V3R2 FMEDA 5408.pdf	FMEDA report for the Rosemount 5408 Level Transmitter
[R3]	ROS 14-09-201 5408 V2R1 FFA.xlsx	Field Failure Analysis for Rosemount 5408 Level Transmitter

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 Rosemount Tank Radar.

The following IEC 61508 objectives were subject to detailed auditing at Rosemount Tank Radar:

- FSM planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation management
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / quantitative analysis
- Hardware and system related V&V activities including documentation, verification
  - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

The project teams, not individuals were audited.

3 Product Description

The Rosemount 5408 Level Transmitter is a non-contact radar level transmitter intended for safety instrumented systems. It has a 4-20 mA analog output as its safety output.

The Rosemount 5408 Level Transmitter provides the following safety functions;

- Measure the distance from the micro-wave unit to a liquid substance in a tank. This function is based on a measurement of the delay time between a transmitted micro-wave and the received echo. A FMCW radar sweep is used for this measurement.
- Optionally derive other measurement variables (for example volume) from the measured distance.
- Calculate and emit a 4-20 mA current based on the selected measurement variable.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of the Rosemount 5408 Level Transmitter:

Table 1 Revisions in Assessment Scope

Rosemount 5408 Level Transmitter	
Hardware	Model 5408F **H* (H = 4-20mA output with HART; * = wildcards based on the order selection)
Software/Firmware	1.A8 and higher

The versions in Table 1 were current when this report was released. For updated versions covered under this certification, refer to the Safety Manual which includes the company webpage where the certified versions and compatibility can be checked.

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Rosemount Tank Radar 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 Rosemount Tank Radar development processes for the Rosemount 5408 Level Transmitter.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. The safety case demonstrates 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 Rosemount 5408 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 Rosemount 5408 Level Transmitter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Rosemount Tank Radar may make modifications to this product as needed. All modifications are subject to review during a surveillance audit.

As part of the *exida* 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 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 the development process used by Rosemount Tank Radar during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the Rosemount 5408 Level Transmitter was done per this IEC 61508 SIL 3 compliant process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Rosemount Tank Radar has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D003] and [D003b].

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 the *exida* certification scheme which includes subsets of IEC 61508 requirements tailored to the SIL 3 work scope of the development team. 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.

5.1.1 Functional Safety Management

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- Structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- Specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.
- Specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.
- Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
- Document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.
- Document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.
- Specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed.
- Select a suitable set of tools, for the required safety integrity level, over the whole safety lifecycle which assists verification, validation, assessment and modification.

5.1.2 Safety Lifecycle and FSM Planning

Assessment

The Manufacturer has been ISO 9001 certified [D036]. All sub-suppliers have been qualified through the Manufacturer Qualification procedure [D007], [D007b].

The functional safety management (FSM) plan [D026] defines the safety lifecycle for this project. This includes a definition of the safety activities and input/output documents to be created for this project. This information is communicated via these documents to the entire development team so that everyone understands the safety plan. The development team is involved in all aspects of the project, including safety activities as applicable, and regular meetings and reviews ensure that all relevant members take part and are informed.

All phases of the safety lifecycle have verification steps described in the FSM plan or a separate verification plan for one or more phases. This plan includes criteria, techniques and tools used in the activities. The verification is carried out against this plan.

The Software Development Procedure [D021] identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase. Any tailoring shall be justified, for example if a modification is required.

Conclusion:

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system and new product development processes.

5.1.3 Documentation

Assessment

There is a document management system in place [D010], [D010b]. This system controls how all safety relevant documents are changed, reviewed and approved. All safety related documents are required to meet the following requirements:

- Have titles or names indicating scope of the contents
- Have a revision index which lists versions of the document along with a description of what changed in that version
- Documents are searchable electronically

Several documents were sampled and found to meet these requirements.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system.

5.1.4 Training and competence recording

Assessment

The FSM Plan [D026] lists the key people working on the project along with their roles. A Functional Safety Coordinator is assigned for the project. A competency matrix has been created and includes the following:

- Competency requirements for each role on project.

- List of people who fulfill each role

- List of competencies for each individual matched up to required competencies based on roles that they fill.

- Training planned to fill any competency gaps.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system and internal organizational procedures.

5.1.5 Configuration Management

Assessment

Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification [D004 thru D004g]. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

The configuration of the product to be certified is documented including all hardware and software versions that make up the product. For software this includes source code. Product numbers and versions are well-established.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar organizational release procedures, functional safety management system and new product development processes.

5.1.6 Tools (and languages)

Assessment

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 [D038]. This includes validation test tools. 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. An assessment has been carried out for T2 and T3 offline support tools, to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms are identified, appropriate mitigation measures have been taken.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system.

5.2 Safety Requirement Specification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.

Assessment

All element safety functions necessary to achieve the required functional safety are specified. The FSM plan calls for the creation of the SRS [D040]. Software safety requirements [D043] have been created as design requirements (from Safety Requirements). These requirements have been made available to the software developers and have been reviewed by software developers. The results of the review are documented and all action items are tracked through resolution. Specific requirement for start-up and restart procedures (if required) are specified. All system and operator interfaces necessary to achieve the required functional safety are specified. All safety related constraints between the software and hardware have been documented in the Software Safety Requirements or other suitable requirements document.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system and use of requirements management tools.

5.3 Change and modification management

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

Assessment

A Modification Procedure exists that identifies how a modification request is initiated and processed in order to authorize a Product Modification Request (including hardware and software modifications). A Product Modification Request System exists to support this process. Modifications are initiated with an Engineering Design Change procedure [D023]. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process. The Software Modification Procedure requires that the changed software module is re-verified after the change has been made.

A 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) and on the Functional Safety of the system. The results of an Impact Analysis are documented. An impact analysis [D023b] is performed for any change related to functional safety.

The modification process has been successfully assessed and audited, so Rosemount Tank Radar may make modifications to this product as needed.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system, change management procedures, and sustaining product procedures.

5.4 System Design

Objectives

The objective of the related IEC 61508 requirements of this subclause are to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

Assessment

System design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented. Techniques and measures to achieve SIL3 have been applied during development. The System Architecture Design [D045], [D045b] clearly identifies the SIL of all components in the design. If a component has a lower SIL capability than that associated with the safety function(s), then sufficient independence between the components has been documented with an FMEA or software HAZOP [D050 thru D050c]. The System Architecture Design describes that the behavior of the device when a fault is detected is to take an action which will achieve or maintain a safety state.

The System Architecture Design identifies design features (such as Proof Test) that support maintainability and testability. This shows that these qualities have been considered during design and development and have been verified at review time. Maintenance includes possible software changes in the field, if applicable, including maintaining system safety during and after such changes.

An inspection of the system architecture design has been done. Semi-formal methods will be used to document the design. Specific methods used on this project are UML, flowcharts, sequence diagrams, timing diagrams, activity charts, STD.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system and new product development processes.

5.5 Hardware Design and Verification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
- Integrate and test the E/E/PE safety-related systems.

5.5.1 Hardware architecture design

Assessment

Hardware architecture design [D045] has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews [D053] are used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are incorporated into the design.

The FSM Plan and development process and guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system and new product development processes.

5.5.2 Hardware Design / Probabilistic properties

Assessment

To evaluate the hardware design of the Rosemount 5408 Level Transmitter, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R2]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D77], 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.

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

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices.

5.6 Software Design

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level.
- Review and evaluate the requirements placed on the software by the hardware architecture of the E/E/PE safety-related system, including the significance of E/E/PE hardware/software interactions for safety of the equipment under control.

- Design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analyzable and verifiable, and which is capable of being safely modified.

Assessment

The System Architecture Design contains a description of the software architecture. The design is partitioned into components which are either all new components or treated as new, and fully verified prior to product release. The Software Architecture Design [D049] uses semi-formal methods, such as UML, State Charts / State Transition and Dataflow Diagrams. The Software Architecture Design was reviewed and confirmed that the architecture fulfills the safety requirements. The Software Architecture Design specifies that fault detection techniques are employed to detect software faults. The Software Detailed Design [D051] describes the design features and diagnostics that maintain the safety integrity of data. Any action items to be addressed prior to release were submitted to the action item tracking system and have been resolved.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system.

5.7 Software Verification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- To the extent required by the safety integrity level, test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.
- Verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved.
- Integrate the software onto the target programmable electronic hardware. Combine the software and hardware in the safety-related programmable electronics to ensure their compatibility and to meet the requirements of the intended safety integrity level.

Assessment results

Design reviews [D053b] are part of the overall software development process. Online collaboration tools are used for reviews. Formal design reviews are held and the results recorded; action items are identified, assigned, and resolved.

A modular approach has been used in the software design. Design has been broken up into functions and methods which are modular, and subprograms have a single entry and a single exit.

Static analysis tools [D061] are used; results are reviewed, and errors are resolved or explained. Cyclomatic complexity is also measured and recorded in [D066].

Structural test coverage (entry points, statements, branches) of 100 % is documented by a tool or a manual trace of test coverage. An exported example as HTML is included in [D066b]. The coverage metrics are under version control.

Module Test Results [D066] for all safety related modules were produced and documented per the Module Test Verification Plan/Specification. Sample results files were reviewed; unit tests are automated or manual; verification of data is included in tests; result files show the pass/fail output line.

The Traceability Matrix [D056] shows that for each Software Architecture requirement there is one or more corresponding Software Safety Requirement. (backward traceable). The Traceability Matrix also shows that, for each Software Safety Requirement, there are corresponding Software Design Requirements which cover the Software Safety Requirement. (forward traceable).

Conclusion:

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system, software development process, and new product development processes.

5.8 Safety Validation

Objectives

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.
- Validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

Assessment

One or more test cases, or analysis documents, exist for each safety requirement (including software safety requirements) as shown by the requirements traceability matrix [D056], [D056b]. Each test case includes a procedure for the test as well as pass/fail criteria for the test (inputs, outputs and any other acceptance criteria). The test plan includes the procedure used to properly judge that the validation test is successful or not. Dynamic (runtime) analysis/testing is performed in addition to static analysis/testing.

Fault injection testing [D077] 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 cases are created by looking at the product as a black box, meaning that external inputs are applied to the product and outputs are observed. Equivalence classes, input partitioning testing, and boundary value analysis help determine what input values to use.

Test results are documented, including reference to the test case and test plan version being executed. [D074] is a summary of all validation results, either by test, analysis, or Safety Manual entry. Test cases, procedures and details are included in online servers and exported as needed.

The following information is documented in the test results:

- a record of validation activities, permitting validation results to be reproduced and/or retraced;

- the version of the validation plan used to execute the test. (created and modified version history is recorded);

- the safety function associated with each test case. (safety functions indicated in SRS and linked via tools);

- the tools and equipment and calibration data;

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system, software development process, and new product development processes.

5.9 Safety Manual

Objectives

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

Assessment

The Safety Manual is provided as a separate section of the Reference Manual [D079], and identifies the safety functions of the product, including a description of the input and output interfaces. When internal faults are detected, their effect on the device output is clearly described. Sufficient information is provided to facilitate the handling of external diagnostics capability (output monitoring by PLC).

The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing. Procedures for maintaining tools and test equipment are listed. Routine maintenance tools and activities required to maintain safety are identified and described in the Manual and Appendices. Normal plant and process maintenance procedures are usually enough. Users can add automatic alerts for certain maintenance functions, and other diagnostic alerts can direct troubleshooting activities.

Conclusion

The objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system and the safety manual.

6 2022 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Rosemount Tank Radar	Manufacturer of the Rosemount 5408 Level Transmitter
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Rosemount Tank Radar contracted *exida* to perform the surveillance audit for the above Rosemount 5408 Level Transmitter. The surveillance audit was conducted remotely.

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 Rosemount 5408 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 Rosemount Tank Radar and generated by *exida*

Documents received during this surveillance audit have been documented and updated in section 2.4.

6.3 Surveillance Results

6.3.1 Procedure Changes

Changes and improvements to the Engineering Development Procedures were reviewed as part of other ongoing projects and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes

There were no engineering changes since the last surveillance audit.

6.3.3 Impact Analysis

There were no engineering changes that needed an impact analysis since the last surveillance audit.

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

The updated safety manual was reviewed and found to be compliant with IEC 61508:2010.

6.3.6 FMEDA

There were no changes that needed a FMEDA update since the last surveillance audit.

6.3.7 Evaluate use of certificate and/or certification mark

The Rosemount Tank Radar 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 that needed addressed since the last surveillance audit.

6.4 Surveillance Audit Conclusion

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

The Rosemount 5408 Level Transmitter continues to meet the relevant requirements of IEC 61508:2010 for up to SIL 3 in low or high demand applications based on the initial assessment and considering:

- field failure history

- permitted modifications completed on the product

- FMEDA updates and changes

- resolution of past action items

This conclusion is supported by the updated SafetyCase and certification documents.

7 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.
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
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).
HART	Highway Addressable Remote Transducer
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
Q22/09-072	ROS 15-01-149 R001 V2R1	Renewal; LLS 12/22/2022
Q19/09-114	ROS 15-01-149 R001 V1R3	Revision due to FMEDA update; 5-Dec-2019, ABC
Q19/09-114	ROS 15-01-149 R001 V1R2	Surveillance Audit Assessment; 2-Dec-2019, ABC
Q15/01-149	ROS 15-01-149 R001 V1R1	Initial Release, revised sect 2.4.1 listing after internal and client review; 9-Dec-2016, JCY

Reviewer/Approver: Ted Stewart (*exida*), December 23, 2022
Status: Released, December 28, 2022

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Ted E. Stewart, CFSP, exidaCSP
Certifying Assesser

Loren L. Stewart, CFSE, Evaluating Assessor