Results of the IEC 61508 Functional Safety Assessment

Project:
3408 Level Transmitter

Customer:
Rosemount Tank Radar
(an Emerson Company)
Sweden

Contract No.: Q21-06-064r1
Report No.: RTR 21-06-064 R002
Version V1, Revision R1, 11/22/2022
Dave Butler

Management Summary

The Functional Safety Assessment of the Rosemount Tank Radar 3408 Level Transmitter 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 the Rosemount Tank Radar 3408 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 3408 Level Transmitter can be used in a safety related system in a manner where the PFD_{AVG} is within the allowed range for SIL 3 according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the 3408 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 3408 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.

Table of Contents

1 Purpose and Scope

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

3408 Level Transmitter by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508:2010.

The purpose of the assessment was to evaluate the compliance of:

- the 3408 Level Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

  and

- the 3408 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 3408 Level Transmitter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out based on *exida*'s quality procedures and scope definitions.

The results of this assessment provide the safety instrumentation engineer with the required failure data per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried out by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

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

The assessment was planned by *exida* and agreed with Rosemount Tank Radar (see [R2]).

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 person-years of cumulative experience in functional safety and cybersecurity. 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 3408 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.

Doc. ID	Standard	Title
[N1]	IEC 61508:2010 Parts 1 – 7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Tank Radar

Doc. ID	Project Document Filename	Version	Date
D001	DOC-002740 (RTR Quality Manual).pdf	Rev. 13	12/2/2021
D003	DOC-002735 - RTR Product Design and Development Process.docx	Rev. 1.0	3/17/2017
D003b	DOC-006493 (New Product Development Process).pdf	8	12/16/2021
D003c	Blackbird-DE-0006_Iss0.2.pdf	0.2	6/24/2021
D004	DOC-003099 - Part numbering convention.docx	Rev. 1.0	
D004d1	0100-23-1802 Rosemount Inc Record Retention Schedule.pdf	12	Aug.2020
D004d2	DOC-002807 - Principal Record Retention Periods - Sweden.doc	Rev. 1.0	Apr.2010
D004e	DOC-003098 - Archiving of engineering files.docx	Version 3.0	Mar.2017
D004f	DOC-006687 - Configuration and Change Management Work Instruction.docx	Rev. 7	4/20/2018
D005	DOC-010041 (Customer Feedback Process).pdf	1	3/3/2022
D005b	DOC-006487 - Failure Analysis Process Description.docx	10	3/2/2021

Doc. ID	Project Document Filename	Version	Date
D005c	DOC-002943 (RMA Return Documentation).pdf	4	12/27/2021
D005d	DOC-002702 - RMA Process.vdw	1	6/8/2011
D007	DOC-003125 - Supplier Evaluation and Approval Process Description - RTR.docx	Rev. 1.0	12/4/2018
D008	DOC-002990 - Production Part Approval Process (PPAP).docx	3	9/18/2020
D010	DOC-002681 - Document management - Department documents.docx	Rev. 2	9/15/2017
D010b	DOC-002968 - Document Management - Product Development Projects.docx	Rev. 2.0	5/25/2022
D010c	DOC-002682 - Documents and Document management.docx	14	2/11/2022
D012	DOC-002984 - Corrective Action Process (Parts).docx	5	4/19/2021
D013	DOC-003179 - Corrective Action Preventive Action (CAPA) Process.docx	1	
D016	DOC-002963 - Design review guidelines at RTR.docx	1	
D016b	Individual_log.xlsx	Rev. I	11/1/2011
D019	DOC-006349 - Customer Notification Process.docx	9	3/4/2021
D021	GaugeSW-Instr-0008.doc	9.1	12/1/2020
D021d	FMEA (L-003177 Rev2).pdf	Rev. 2	11/22/2021
D023	DOC-004408 (Engineering Change (EC) Process).pdf	14	5/14/2021
D023b	DOC-003051 - Impact analysis template for SIL approved products.docx	1	4/16/2014
D023c	DOC-004409 (Engineering Change (EC) Process Flowchart).pdf	9	5/18/2021
D023d	DOC-003084 - Change Control Board (CCB) Charter.docx	2	12/9/2020
D027	Blackbird-PL-0026.docx	2.2	1/19/2021
D027b	Blackbird-DE-0027.xlsx	12	9/22/2022
D033	Blackbird-PL-0021.docx	2	8/23/2022
D036	RTR ISO 9001_2015_ISO 14001_2015.pdf	n/a	Exp July 2024
D038	GaugeSW-0089.pdf	4	6/27/2022
D040	Blackbird-SP-0014.pdf	3	5/17/2022
D040b	Appendix_A_Blackbird_SP-14_SRD_3_0_Baseline_12_5.pdf	12.5	5/17/2022
D041	GSW_RR_ET_Consolidated Log Form_2_CS_included_exida_data_added.xlsm		5/6/2021
D043	Eagle-Prod_Doc_TH0303.pdf	6	6/17/2022
D043b	Eagle-Prod_Doc_TH0298.pdf	11	6/21/20022
D043c	Blackbird-SP-0028.pdf	2	6/21/2022
D045	Blackbird-DE-0024 (System Architecture Doc).pdf	1	8/5/2021
D045b	Blackbird-DE-0023.pdf	1.1	2/25/2022
D047	D7000006-939_I01.pdf	1	5/20/2022
D047b	D7000005-887_I01.pdf	1	5/20/2022
D047c	03031-3511_AA.pdf	AA	4/13/2022
D049	Eagle-Prod_Doc_TH0003.pdf	7	6/17/2022
D050	Blackbird-RE-0050 (Safety Criticality_HAZOP_FMEA).pdf	1	10/13/2021
D050b	Blackbird-DE-0055.xlsx	2	9/16/2022
D050c	Blackbird-DE-0056.xlsx	1	6/21/2022
D050d	Blackbird-RE-0069.xlsx	3	6/22/2022
D051	Blackbird-SP-0040.pdf	3	6/17/2022
D051b	Blackbird-SP-0029.pdf	3	6/20/2022
D051c	Blackbird-SP-0031.pdf	3	6/20/2022
D053	Blackbird-DE-0048.docx	1	6/20/2022

Doc. ID	Project Document Filename	Version	Date
D054	Blackbird-RE-0130.docx	3	9/18/2022
D055	ROS 21-06-064 R001 V1R2 FMEDA 3408.pdf	V1R2	5/31/2022
D055a	Blackbird-RE-0038_Iss 1.5.xlsx	1.5	5/18/2022
D056	3408_Safety_Validation Test_Cases_Final.docx		10/6/2022
D056b	Blackbird-RE-0137 (Tobias).docx	Rev. 1.2	8/24/2022
D056c	Blackbird-RE-0057 (Blackbird 3408 MCU-P Cross Reference Document).docx	Rev. 1.0	6/21/2022
D056d	Blackbird-RE-0058 (Blackbird 3408 MCU-A Cross Reference Document).docx	Rev. 1.0	6/20/2022
D056e	Blackbird-RE-0059 (Blackbird 3408 MCU-Fw Cross Reference Document).docx	Rev. 1	6/20/2022
D057b	Blackbird-SP-0021.pdf	2	6/23/2022
D058	Blackbird-RE-0131.pdf	1	6/23/2022
D059	Blackbird-SP-0042.pdf	2	2/24/2022
D059b	Blackbird-SP-0038.pdf	2	2/16/2022
D060	GU01-0054.pdf	7	9/6/2013
D060b	GaugeSW-Instr-0014.doc	3	Mar.2011
D060c	GaugeSW-Instr-0011.pdf	8	6/21/2022
D060d	GaugeSW-Instr-0022.docx	3	9/25/2019
D061	GaugeSW-Instr-0001_issue7.doc	7	Apr.2020
D063	Blackbird-RE-0129.pdf	2	6/23/2022
D064	Blackbird-SP-0020.pdf	2	4/11/2022
D064b	Blackbird-PL-0057 (Embeded Software Test Plan).pdf	1	10/22/2021
D069	Blackbird-PL-0054.pdf	2	3/17/2022
D069b	Blackbird-SP-0023 (Safety Validation Test Spec) .pdf	1	11/4/2021
D070	Blackbird-PR-0027.xlsm	1	11/4/2021
D074	Blackbird-RE-0124.pdf	1	6/15/2022
D074b	Blackbird-RE-0135.pdf	1	6/29/2022
D074c	Blackbird-RE-0134.pdf	2	6/27/2022
D076	P112873 (EMC 3408 HART+BLE).pdf		6/3/2022
D077	Blackbird-RE-0108.pdf	1	3/29/2022
D078	3408_RefMan_RevAB_00809-0100-4418_En.pdf	AB	10/1/2022
D078b	3408_PDS_RevAB_00813-0100-4418_En.pdf	AB	10/1/2022
D078c	3408_QSG_00825-0100-4418_RevAA_PREL_220601.pdf	AA	6/1/2022
D079	3408_SafetyManual_00809-0200-4418_RevAA_PREL_220601.pdf	AA	6/1/2022
D080	3408_TechDocs_20220601_SafetyManual_Consolidated Log Form.xlsm		8/18/2022
D081	Blackbird-PR-0018.xlsx		6/15/2022
D082	Blackbird-DE-0022.pdf	1	6/30/2022
D088	Blackbird-RE-0123.pdf	2	6/22/2022
D091	Blackbird-RE-0122.pdf	3	6/20/2022
D092	Blackbird-DE-0026.xlsx	1	4/5/2022
D092b	Screenshot threat analysis 3408.docx	Screenshot	

2.4.2 Documentation generated by *exida*

Doc. ID	exida Document Filename	Description
[R1]	RTR 21-06-064 SC001 V1R2 IEC 61508 - 3408.xlsm	Safety Case Workbook
[R2]	Q21-06-064r1 RTR 3408_Proposal.pdf	Assessment Plan
[R3]	ROS 21-06-064 R001 V1R2 FMEDA 3408.pdf	FMEDA Report

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
  - 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 / probabilistic modeling
- 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 certification audit was done in Mölnlycke on 8/29 - 8/30/2022.

3 Product Description

The Rosemount 3408 is a two-wire transmitter for continuous level measurements over a broad range of liquids and slurries. The measurement principle is fast-sweep Frequency Modulated Continuous Wave (FMCW). The Rosemount 3408 can be used as the level sensor in a Basic Process Control System (BPCS) or as a safety device in a safety instrumented system.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of 3408 Level Transmitter:

Model	Hardware Version	Software Version
3408 Level Transmitter	1.0.0	1.0.0

Table 1- Hardware and Software Versions

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 relevant objectives of the standard have been met by the Rosemount Tank Radar development processes during this development project.

exida audited and assessed project and product documentation for compliance with the functional safety requirements of IEC 61508. During an evaluation period, an assessor updated a safety case with the results of the assessment. The safety case documents the development project's compliance with the functional safety management requirements of IEC 61508, parts 1 through 3. Evaluation was followed by a certification review of the safety case, in which a review of a subset of the most important requirements, and a spot inspection of the remaining requirements, was carried out to ensure high quality of the safety case.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Rosemount Tank Radar 3408 Level Transmitter, with IEC 61508.

The assessment, which was executed using the exida certification scheme, tailors the IEC 61508 requirements to the scope of the development activities and the development team.

The results of the assessment show that the 3408 Level Transmitter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements and constraints specified in the Safety Manual.

4.1 Product Modifications

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

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 documents, 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 3408 Level Transmitter was done per this IEC 61508 SIL 3 compliant development 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 [D01].

This functional safety assessment evaluated the compliance of the processes, procedures and techniques as implemented for the product development, with the requirements of IEC 61508. 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.

Objectives

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

5.1.1 Safety Lifecycle and FSM Planning

Assessment

The functional safety management plan 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.

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

The Manufacturer has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure.

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.

Reported dangerous failures that occur in the field are captured and analyzed and recommendations are made to minimize the chance for a repeat occurrence of the failure.

The software development procedure states that if, at any phase of the software safety lifecycle, a modification is required pertaining to an earlier lifecycle phase, then an impact analysis shall determine:

(1) which software modules are impacted and

(2) which earlier safety lifecycle activities shall be repeated.

Lifecycle Phase Verification results are documented according to the verification plan and available for assessment.

Conclusion:

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

5.1.2 Documentation

Assessment

A document management system, called "Doktor", is employed, which 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
- Contain a table of contents
- Have a revision index which lists versions of the document along with a description of what changed in that version
- Are electronically searchable

Several documents were sampled and found to meet these requirements.

Conclusion

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

5.1.3 Competence and Training

Assessment

The FSM Plan 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:

a) Competency requirements for each role on project.

b) List of people who fulfill each role

c) List of competencies for individuals, matched up to required competencies based on roles that they fill.

d) Training planned to fill any competency gaps.

Conclusion

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

5.1.4 Configuration Management

Assessment

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.

Software releases are formally documented via release notes. At a minimum, the release notes include the release number, a summary of changes to this release and a list of open issues.

Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

Conclusion

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

5.1.5 Tool Qualification and Programming Language

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. 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.

The following information is documented for off-line support tools classified as either T2 or T3:

- All configuration baseline items for which the tool is used.
- The tool configuration (compiler options, batch files, scripts, etc. for each different use of the tool.)

For each tool in class T3, evidence is available that the tool conforms to its specification or manual through a combination of confidence from use and tool validation.

Only one tool is currently listed as T3. It is possible that other tools need to be classified as T3 but further analysis on their use is needed.

For each tool in class T3, if tool validation is performed, the results of the validation should be documented, and the tool validation checklist should be completed. No tool validation was needed, since the only T3 tool has been used for 5 projects and is qualified based on confidence from use.

All tools were qualified, by following the Software Tool Qualification Procedure. Any tools that have been upgraded to new versions after successful qualification have been re-qualified per the upgrade section of the Software Tool Qualification Procedure. Results for each qualification / re-qualification have been documented, indicating that the tool is acceptable for use.

Conclusion

The Tool Qualification and Programming Language objectives of the standard are fulfilled by the Rosemount Tank Radar functional safety management system.

5.2 Safety Requirement

Assessment

All element safety functions necessary to achieve the required functional safety are specified.

Software safety requirements 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 to resolution.

The Safety Requirements Specification (SRS) has been reviewed to verify that it has enough detail such that the required SIL can be achieved during design and implementation and can be assessed.

SRS content is available and sufficient for the duties to be performed. This has been confirmed by the validation testing and assessment.

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

5.3 Modification Management

Assessment

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.

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 to the Functional Safety of the system. The results of an Impact Analysis are documented.

Modification Request/Records will document the reason for the change and have a detailed description of the proposed change.

The impact analysis documents which tests must be run to validate the change and which tests must be re-run to validate that the change did not affect other functionality.

The Software Modification Procedure requires that the changed and affected software modules are reverified after the change has been made.

The Software Modification Procedure requires that all software safety requirements are revalidated unless regression validation for certain modifications is specified in the impact analysis. The level of Regression test is decided in the Impact Analysis (some regression tests are always required).

The Impact Analysis indicates the plan for verification and validation of the modification. The plan is a tailored version of the plan expected for a full verification, based on the SIL, unless the project follows the full RPD process. Note that since this product was assessed for SIL 3, a software change requires full software validation testing of all software safety requirements.

Conclusion

The Modification Management 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

Assessment

System design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented.

SIL 2 for 1oo1 config; SIL3 for 1oo2 config. Techniques and measures to achieve SIL3 have been applied during development.

The System Architecture Design 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.

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 (such as raising an output signal through an external interface or setting an output to the configured safe state).

The System Architecture Design identifies all safety critical interfaces. There are no safety critical network interfaces.

The System Architecture Design identifies design features (such as proof test support) that support maintainability and testability. This shows that these qualities have been considered during design and development and have been verified at review time. Software is not able to be updated by the end user.

All software components or subsystems listed in the Software Architecture Design have corresponding Software Designs which further partition the design into software modules. The design has a focus on simplicity.

The Software Design describes the design of diagnostics features of the software.

Formal design reviews are held, and the results are recorded; action items are identified, assigned, and resolved. A design checklist is completed during design reviews.

The System Architecture requires the use of a specific configuration tool to make configuration changes.

The System Architecture requires the use of a password to access the dedicated configuration tool to make changes.

A database of previously used (well-tried) components is kept. When creating new designs, engineers are encouraged to use previously used components and must provide written justification when they cannot.

An inspection of the system architecture design has been done.

The Software Design expresses the design in terms of:

- functionality
- information flow between elements

- timing constraints
- concurrency/synchronization
- data structures
- structural views
- behavioral views

The Software Design is well understood by the developers and is documented in a way that can be easily verified.

Conclusion

The System Design 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

5.5.1 Hardware Architecture Design

Assessment

Hardware Components used on previous projects are given priority over new components. This is implemented by having a component database, and a procedure which states that approval must be given to use any hardware component not already in the component database.

The 3408 Level Transmitter is included in an enclosure which protects it against water, dust, and other elements/weather conditions. The device has received an ingress protection rating of IP66/67.

The hardware architecture design has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews 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, development process and development guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

Conclusion

The Hardware Architecture Design 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 3408 Level Transmitter, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed for each component in the system. This is documented in [R3]. Assumptions made during the FMEDA were verified using Fault Injection Testing as part of the development (see the Fault Injection Test Results [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 a standard FMEA method with techniques to identify the failure modes relevant to safety instrumented system design and the effects of online diagnostics to mitigate them.

From the FMEDA, failure rates are derived for each important failure category. They are considered in combination with the failure rates of other devices at the system level to calculate a PFD_{avg} for the Safety instrumented Function (SIF) in which the 3408 Level Transmitter is used. The calculated PFD_{avg} is then used to verify that the SIF meets the SIL requirement for PFD_{avg}.

Conclusion

The Hardware Design Analysis 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

Assessment

The Software Architecture Design [D049] contains a description of the software architecture. The design is partitioned into components which are either all new components or treated as new.

The Software Architecture Design uses the following diagram types:

- Logic/Function Block Diagrams
- State Charts / State Transition Diagrams
- Activity Diagrams
- Decision / Truth Tables

The Software Architecture Design and detailed design specifications specify that fault detection techniques are employed to detect software faults. The Software Design describes the design of diagnostics features of the software, including the design features that maintain the safety integrity of program flow and data.

The Software Design describes an acceptable memory allocation strategy.

A software criticality analysis and FMEA was performed for each firmware executable. The reports from those analyses list all components along with their criticality (Safety Critical, Safety Related, or Non-Interfering) and their required Systematic Capability resulting from the analysis. Independence has been achieved by both spatial and temporal separation as documented in the results of the SCA / SW HAZOP.

Conclusion

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

5.7 Software Verification and Integration

Assessment

The Software Architecture Design was reviewed. This review to verify that the architecture fulfills the safety requirements. All action items required to be addressed, were submitted to the action item tracking system and have been 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.

100% structural test coverage of functions, statements and branches is documented by a tool and the output is reviewed for completeness. Some functions/statements are not covered by this analysis and justification for those exceptions has been documented.

The 'C' programming language is used. As shown in table C.1 of IEC 61508-7, the 'C' programming language when used with a defined language subset, a coding standard, and static analysis tools is highly recommended for all SILs. For this project there is a coding standard which defines a language subset and static analysis tools are used to detect potential problems in the source code. Therefore, 'C' can be considered a suitable programming language.

Static Analysis of source code is performed and documented. Cyclomatic complexity also measured and recorded. Written justification is documented for some functions exceeding the complexity metric limit documented in the coding standard. The justification was assessed by examining the relevant function and found to be valid.

The Integration Test Plan requires that Safety Functions are tested during Integration Testing using a functional testing approach.

All Integration Test Cases have been successfully run, per the Integration Test Plan and Integration Test Results have been documented.

For each test, the Integration Test Results Record identifies the Test Case, its version, the version of the product being tested, the tools; and the equipment used, along with their calibration data. In addition, the Integration Test Results Record references the Integration Test Plan including version number.

The Integration Test Plan was reviewed and found to be adequate with regard to its coverage of the Software Safety Requirements, the Software Architecture Design, the Software System Design, the types of tests to be performed and the procedures to be followed. All action items have been resolved or deferred.

Qualified test management and automation tools are used to manage the module and/or integration testing process. These are under version control in the same repository as the target code. They are included in code reviews.

Safety critical expected results for automated test scripts are verified off-line using sample data and compared to the on-line values computed for the same sample data.

The source code standard states that software modules interact with each other through their interfaces which are fully defined and documented, completely prototyped, including name and data type of parameters, and evidence is available that this was followed.

Module Test Results for all safety related modules were produced and documented per the Module Test scripts used in an automated test environment. Execution of selected tests were witnessed by *exida*, and sample results files were reviewed. Most unit tests are automated or manual. Verification of data is included in tests. Result files show a pass/fail output line. No unintended functions were performed. Failures are either fixed immediately or logged with an issue tracker for remediation.

Module test results show that boundary value analysis and equivalence class partitioning was used to determine test cases. These test cases are applied to the interface of the module. Unit Test Checklist in Unit Test Plan states that this should be done. A quick review of several module tests showed that this appeared to be done.

The Integration Test Plan calls for black box testing of all integration levels. Equivalence classes and boundary values have been considered in writing all Integration Test Cases.

Conclusion:

The Software Verification and Integration 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

Assessment

One or more test cases, or analysis documents, exist for each safety requirement (including software safety requirements) as shown by documented requirements traceability. Each test case includes a procedure for the test as well as pass/fail criteria for the test (considering inputs, outputs, etc.).

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 SM entry.

The following information is documented in the test results:

a) a record of validation activities, permitting validation results to be reproduced and/or retraced.

b) The version of the validation plan used to execute the test.

c) The safety function associated with each test case.

d) The tools and equipment and calibration data.

e) The Configuration Identification of the Item Under Test.

Fault injection testing has been performed on the product as defined in the fault injection test plan. The results have been analyzed and adjustments have been made to the FMEDA based on these results.

Conclusion

The Safety Validation 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

Assessment

The Safety Manual is documented. It identifies and describes the functions of the product. The functions are clearly described, 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 development of an external diagnostics capability (output monitoring).

The Safety Manual provides information about failure rates, useful lifetime, device type (A/B), and systematic capability.

The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing.

User documentation specifies all relevant environmental operating ranges.

All routine maintenance tools and activities required to maintain safety are identified and described in the Safety Manual or other reference manuals.

The Safety Manual identifies security measures that are implemented against potential threats or vulnerabilities as identified in a threat analysis. Password protection of configuration is available.

The user manual defines what configuration options and methods exist for the product.

Each software release will be accompanied by release notes which contain the following information:

1. The reason for release of the software element (to clear outstanding anomalies or for the inclusion of additional functionality or both).
2. Details of all outstanding anomalies not fixed in this release
3. Details as to whether the software element is compatible with previous releases of the subsystem and if not, details of the process providing the upgrade path to be followed.
4. Any compatibility issues that exist with other systems
5. List of any requirements not met in this release of software.

Conclusion

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

6 Terms and Definitions

Term	Definition
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time (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.
PFDAVG	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in international standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q21/06-064	RTR 21-06-064 R002 V1R1	Errors and omissions; DEB 11/22/2022
Q21/06-064	RTR 21-06-064 R002 V1R0	Initial Certification; DEB 11/18/2022

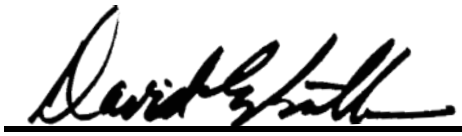
Review/Approved: Ted Stewart, 11/17/2022

Status: Released, 11/22/2022

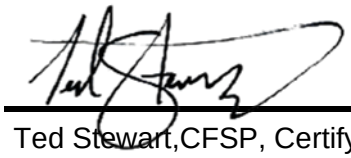
7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Dave Butler, CFSE, Evaluating Assessor



Ted Stewart,CFSP, Certifying Assessor