IEC 61508 Functional Safety Assessment

Project:

644 4-20mA / HART Temperature Transmitter

Customer:

Rosemount Inc.

Emerson Automation Solutions

Shakopee, MN

USA

Contract Number: Q16/12-041

Report No.: ROS 12/04-020 R002

Version V2, Revision R3, November 16, 2017

Loren Stewart

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the Rosemount Inc.r

- 644 4-20mA / HART Temperature Transmitter

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

- *exida* assessed the development process used by Rosemount Inc. through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The investigation 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* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Rosemount Inc.r.

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

The results of the Functional Safety Assessment can be summarized as:

The Rosemount Inc. 644 4-20mA / HART Temperature Transmitter was found to meet the requirements of SIL 2 for random integrity @ HFT=0, SIL 3 for random integrity @ HFT=1 and SIL 3 capable for systematic integrity.

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 Rosemount Inc.:

- 644 4-20mA / HART Temperature Transmitter

by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508.

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

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

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 Inc..

All assessment steps were continuously documented by *exida* (see [R1] - [R2])

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 400 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 250 billion hours of field failure data.

2.2 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 644 4-20mA / HART Temperature Transmitter
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment..

Rosemount Inc.originally contracted *exida* for the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards and 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 2014 audit are highlighted in grey below.

2.4.1 Documentation provided by Rosemount Inc.

3 ID	Name	Version; Date
[D02]	exida Configuration Management Checklist	n/a; 7/27/2012
[D02a]	CM Plan checklist from EDP 400-300	6/27/2012
[D03]	exida Documentation Checklist	n/a; 7/27/2012
[D04]	exida Software Tool Checklist	n/a; 7/21/2012
[D05]	exida Tool Validation Checklists	7/13/2012

[D06]	exida FSM Planning Phase Verification Checklist	n/a; 7/31/2012
[D07]	Project Plan	C.2; 7/11/2012
[D10]	DOP 1810 Training Procedures	R; 1/20/2010
[D11]	Safety Competencies	n/a;
[D12]	EDP 400-502 Peer Safety Review	A; 3/25/2010
[D13]	Training and Competency Matrix	n/a; 7/12/2012
[D14]	Safety Instrumented Systems Training Program	1/23/2012
[D15]	Action Item List	n/a; 5/14/2012
[D16]	DOP 7 Rosemount Product Development Process	B; 4/1/2011
[D16a]	RMD_G7.3-0001 Product Realization: Project Management Process	A; 7/1/2011
[D16b]	Management Review	8/18/2011
[D17]	DOP 415 Product Design and Development Process	I; 10/13/2011
[D17a]	DOP416 SIS Product Design and Development Process	I; 2/1/2012
[D18]	DOP 440 Engineering Change Procedure	AK; 2/1/2011
[D19]	DOP 1110 Metrology Procedure	AA; 1/15/2010
[D19a]	Test Equipment List	n/a; 6/5/2012
[D20]	ISO 9001:2008 Certificate	n/a; 10/7/2011
[D21]	DOP 1440: Customer Notification Process	P; 1/19/2010
[D22]	DP-50111-16 Field Return Analysis Report Procedure	A; 2/2/2010
[D22a]	Failure Analysis Procedure	E; 8/12/2011
[D23]	3144 safety coding standard, C/C++	1.2; 7/31/2010
[D23a]	3144 project coding standard	A.1; 9/13/2010
[D24]	EDP 400-300 Configuration and Change Control Management	C; 5/1/2005
[D24a]	644 Configuration Management Plan	A.2; 5/27/2011
[D25]	EDP 400-500 Peer Review	C; 7/1/2011
[D26]	DOP 660 Supplier Corrective Action	U; 11/10/2010
[D27]	Corrective And Preventive Action website	n/a; n/a
[D27a]	Corrective And Preventive Action Procedure DOP 8.5	AB; 5/10/2011
[D28]	DOP 1710 Internal Audit Program	W; 1/25/2010
[D28a]	Internal PPQA Quality Audit example	5/25/2012
[D29]	EDP400-600 Quality_Assurance_Procedure	D; 6/22/2007
[D29a]	DOP1610- Control of Design Records	R; 1/19/2010

[D30]	Safety Integrity Requirements Specification	A.8; 6/6/2012
[D31]	exida SRS Document Checklist	7/31/2012
[D32]	SIRS Review	0.1; 1/3/2011
[D32a]	SIRS Consolidated Log Review	12/15/2010
[D33]	Customer Requirements Document	A.9; 12/20/2010
[D33a]	CRD Review example	A.8; 12/7/2010
[D34]	Electrical Requirements Spec	A.4; 6/28/2012
[D35]	Validation Test Plan	A.2; 9/15/2011
[D36]	exida Safety Validation Test Plan Checklist	8/2/2012
[D37]	Safety Validation Plan Review	A.1; 9/7/2011
[D39]	SRD-SRS-SIRS Traceability	7/12/2012
[D40]	Architecture Design Description Document	1.1; 7/2/2012
[D40a]	Architecture design review	1.0; 6/29/2012
[D40b]	System Requirements	B.5; 6/6/2012
[D42]	exida Integration Test Plan Checklist	8/2/2012
[D43b]	Derived Requirements Document - SW	A.10; 6/6/2012
[D44]	exida Derived Requirements Document Checklist	8/3/2012
[D47]	Proven In Use Analysis Report for 3144P	V1R2.0, 2/25/2004
[D49]	exida System Architecture Phase Verification Checklist	n/a; 8/9/2012
[D50]	Detailed Design Description - Theory of Operation	0.1; 5/1/2012
[D52a]	ASIC Evaluation and Determination	n/a; 11/3/2011
[D53]	Fault Injection Test Plan/Results	3/27/2012
[D53a]	FIT support details	4/11/2012
[D54]	exida HW Fault Injection Test Verification Checklist	n/a; 8/3/2012
[D55]	Schematics - 00644-7100	AC; 3/12/2012
[D56]	BOM - 00644-7102	AD;
[D57]	HW Component Derating analysis	AB; 12/13/2011
[D58]	HW Design Traceability	4/24/2012
[D60]	HW Design Guidelines for Test and Manufacture	A;
[D61]	HW Requirements Review	A.4; 6/29/2012
[D63]	HW System Test Plan	A.2;
[D63a]	HW Test Plan with test procedure example	1/12/2012

[D64]	HW Test Plan Review	A1; 4/19/2012
[D68]	exida Hardware Design Implementation Verification Checklist	N/a; 8/3/2012
[D69]	Hardware Design Phase Verification Checklist	WA0007-E;
[D71]	Detailed Software Design Specification	0.4; 5/18/2012
[D72]	exida Software Architecture and Design Checklist	NA; 8/6/2012
[D73]	SIRS-SW Design Traceability	5/4/2012
[D74]	644 NG SIS Diagnostics Design	NA; 10/27/2011
[D78]	SW Architecture Design Review	.03; 5/18/2012
[D80a]	IEC 61508 SIL3 Tables for 644 Temperature Transmitter	8/3/2012
[D81]	WA0007 SIS Checklists- blank	H; 11/23/2011
[D82]	Software Tools Analysis	A.2; 8/15/2012
[D83]	PIU Assessment; IAR Compiler for Atmel AVR microprocessors	2/11/2007
[D84]	PIU Assessment: Citadel ASIC Field History	up to FY12-8;
[D90]	PC Lint Configuration file	n/a; 5/14/2012
[D90a]	PC Lint resolution example	n/a; 6/6/2012
[D90b]	Code Review example	5/25/2012
[D90c]	PC Lint Results	6/26/2012
[D91]	Unit Test - HW test plan	02; 7/16/2012
[D91a]	HW unit test results	1.0, 7/2/2012
[D92]	Unit Test - SW test plan	A.1; 7/18/2011
[D92a]	SW unit test results	n/a; 4/17/2012
[D92d]	Test Techniques to use to develop test plans	n/a;
[D97]	Software System Test Plan	A.3; 6/8/2012
[D97a]	SW Test Results Example 1	7/5/2012
[D97b]	SW Test Results Example 2	6/29/2012
[D99]	exida SW Implementation Phase Verification Checklist	n/a; 8/6/2012
[D99a]	Action Items	n/a; 5/14/2012
[D109]	exida Integration Test Execution Phase Checklist	na; 7/26/2012
[D110]	EMC Test Results	100672207MIN-001; 3/28/2012
[D111]	Validation Analysis Report	6/13/2012
[D111a]	ROS Safety Validation Testing Checklist	n/a; 9/7/2011

[D112]	Humidity Test results	HSTP 31; 5/8/2012
[D113]	HALT Vibration/Temperature test results	HSTP 35; 5/8/2012
[D114]	Surge Withstand Capability test results	HSTP 29; 6/6/2012
[D115]	Vibration test results	HSTP 32; 5/8/2012
[D116]	ESD test results	HSTP 27; 6/6/2012
[D119]	exida Validation Test Execution Phase Checklist	n/a; 8/6/2012
[D120]	HW FIT witness	7/26/2012
[D121]	SW test witness	7/27/2012
[D150]	exida Functional Safety Assessment Phase Verification Checklist	n/a; 9/4/2012
[D151]	Functional Safety Assessment Plan	V1R1; 7/27/2012
[D152]	Link Software Modules to Unit Tests: 644_NextGen	NA; 8/16/2012
[D153]	Link Software Modules and Code Reviews: 644 Next_Gen	NA; 8/17/2012
[D154]	CMX-Tiny+ RTOS Upgrade Discussion	NA; 8/20/2012
[D155]	CMX 2.00 Code Review Results	NA; 6/12/2012
[D156]	644_NextGen_Trace_Matrix_SIRS_Procedure	NA; 8/20/2012
[D157]	UnitTest_Health.c	NA; 8/30/2012
[D158]	Measure Block Unit Test Result	NA; 12/20/2011
[D159]	644 SIS / Analog Output Unit Test Results	NA; 12/16/2012
[D160]	Product Safety Manual	MA; 7/30/2012
[D161a]	WA0007 Safety Manual Checklist	H; 7/12/2012
[D165]	Failure Modes, Effects and Diagnostics Analysis (FMEDA) Report	V1R1; 5/15/2012
[D166]	exida FMEDA Document Checklist	n/a; 7/20/2012
[D167]	Product Approvals	n/a; 10/27/2011
[D168]	Product Release - Final Design Review, SW	n/a; 5/9/2012
[D169]	Product Release - Final Design Review, HW	n/a; 2/23/2012
[D170]	Unit Test Checklist - TimeStamps	NA; 8/30/2012
[D171]	Unit Test Checklist - TCDiag	NA; 8/31/2012
[D172]	Unit Test Checklist - FourWireS2	NA; 8/31/2012

[D173]	xCode Complexity Analysis	0.1; 8/30/2012
[D174]	Justification for No Maximum Module Size	0.2; 8/31/2012
[D180]	Impact Analysis Template	n/a; 2/9/2012
[D181]	Impact Analysis Example - SW	6/20/2012
[D182]	HW design change review - ClearQuest:PRD00057739	6/6/2012
[D183]	HW design change review - ECO:RTC1053188	4/9/2012
[D184]	Impact Analysis Example - HW	4/26/2012
[D189]	exida Modification Phase Verification Checklist	5/31/2012
[D200]	exida Safety Manual Checklist	NA; 8/8/2012
[D201]	2017 644 shipment / return data	NA
[D202]	Safety Impact Analysis	7/22/16

3.1.1 Documentation generated by *exida*

[R1]	SafetyCaseDocList_644_July31	Detailed safety case documenting results of assessment (internal document)
[R2]	ROS 11-02-058 R001; V3 R1; 2017-11-16	Rosemount Temperature Transmitter 644 Failure Modes, Effects and Diagnostic Analysis

4 Product Descriptions

This report documents the results of the Functional Safety Assessment performed for the 644 Temperature Transmitter with Hardware version 1 and Device Label SW REV 1.1.X. The 644 Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety, instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The transmitter can be equipped with or without display.

The 644 Temperature Transmitter is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0. Combined with one or two temperature sensing elements, the 644 transmitter becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 644 Temperature Transmitter are:

- 2-, 3-, and 4-wire RTD
- Thermocouple
- Millivolt input (–10 to 100mV)
- 2-, 3-, and 4-wire Ohm input (0 to 2000Ω)

644 HART SIS Capabilities and Options

- Single or Dual sensor inputs for RTD, Thermocouple, mV and Ohm
- DIN A Head mount and Field mount transmitters
- SIL3 Capable: IEC 61508 certified by an accredited 3rd party agency for use in safety instrumented systems up to SIL 3 [Minimum requirement of single use (1oo1) for SIL 2 and redundant use (1oo2) for SIL 3]
- LCD display
- Enhanced display with Local Operator Interface
- Integral Transient Protection
- Diagnostic Suite
- Enhanced accuracy and stability
- Transmitter-Sensor Matching with Callendar Van Dusen constants

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

5 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Rosemount Inc. for this development project against the objectives of the *exida* certification scheme which includes subsets of IEC 61508 -1 to 3. The results of the assessment are documented in [R2].

5.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software. The assessment also includes a review of existing manufacturing quality procedures to ensure compliance to the quality requirements of IEC 61508.

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

- Development process, including:
    - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
    - Specification process, techniques and documentation
    - Design process, techniques and documentation, including tools used
    - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
    - Verification activities and documentation
    - Modification process and documentation
    - Installation, operation, and maintenance requirements, including user documentation
    - Manufacturing Quality System
- Product design
    - Hardware architecture and failure behavior, documented in a FMEDA
    - Software architecture and failure behavior, documented in safety integrity requirement specification

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

5.2 Assessment level

The 644 Temperature Transmitter has been assessed per IEC 61508 to the following levels:

- SIL 2 capability for a single device
- SIL 3 capability for multiple devices in safety redundant configurations with a Hardware Fault Tolerance of 1.

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL3) according to IEC 61508.

6 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Rosemount Inc. for these products against the objectives of IEC 61508 parts 1, 2, and 3, see [N1]. The development of new components in the 644 Temperature Transmitter was done using this development process. The Safety Case was updated with project specific design documents.

6.1 Lifecycle Activities and Fault Avoidance Measures

Rosemount Inc. has an IEC 61508 compliant development process as defined in [D17]. The process defines a safety lifecycle which meets the requirements for a safety lifecycle as documented in IEC 61508. Throughout all phases of this lifecycle, fault avoidance measures are included. Such measures include design reviews, FMEDA, code reviews, unit testing, integration testing, fault injection testing, etc.

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the 644 Temperature Transmitter development. The investigation was executed using subsets of the 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 Rosemount Inc. development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

6.1.1 Functional Safety Management

FSM Planning

The functional safety management of any Rosemount Inc. Safety Instrumented Systems Product development is governed by [D17]. This process requires that Rosemount Inc. create a project plan [D07] which is specific for each development project. The Project Plan defines all of the tasks that must be done to ensure functional safety as well as the person(s) responsible for each task. These processes and the procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management.

Version Control

All documents are under version control as required by [D24a].

Training, Competency recording

Competency is ensured by the creation of a competency and training matrix for the project [D13]. The matrix lists all of those on the project who are working on any of the phases of the safety lifecycle. Specific competencies for each person are listed on the matrix which is reviewed by the project manager. Any deficiencies are then addressed by updating the matrix with required training for the project.

6.1.2 Safety Requirements Specification and Architecture Design

As defined in [D17] a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. For the 644 4-20mA / HART Temperature Transmitter, the requirements specification [D30] contains a system overview, safety assumptions, and safety requirements sections. During the assessment, exida certification reviewed the content of the specification for completeness per the requirements of IEC 61508.

Requirements are tracked throughout the development process by the creation of a series of traceability matrices which are included in the following documents: [D30], [D35], [D39], [D58], [D73], and [D156]. The system requirements are broken down into derived hardware and software requirements which include specific safety requirements. Traceability matrices show how the system safety requirements map to the hardware and software requirements, to hardware and software architecture, to software and hardware detailed design, and to validation tests.

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

Requirements from IEC 61508-3, Table A.1 that have been met by Rosemount Inc. include Forward Traceability between the system safety requirements and the software safety requirements, and Backward traceability between the safety requirements and the perceived safety needs.

[D80a] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

6.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D17]. The hardware design process includes creating a hardware architecture specification, a peer review of this specification, creating a detailed design, a peer review of the detailed design, component selection, detailed drawings and schematics, a Failure Modes, Effects and Diagnostic Analysis (FMEDA), electrical unit testing, fault injection testing, and hardware verification tests.

Requirements from IEC 61508-2, Table B.2 that have been met by Rosemount, Inc. include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, checklists, semi-formal methods, computer aided design tools, and inspection of the specification. This is also documented in [D80a]. This meets the requirements of SIL 3.

6.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D17]. The software design process includes software architecture design and peer review, detailed design and peer review, critical code reviews, static source code analysis and unit test.

Requirements from IEC 61508-3, Table A.2 that have been met by Rosemount Inc. include fault detection, error detecting codes, failure assertion programming, diverse monitor techniques, retry fault recovery mechanisms, graceful degradation, modular approach, use of trusted/verified software elements, forward and backward traceability between the software safety requirements specification and software architecture, semi-formal methods, computer-aided specification and design tools, cyclic behavior, with guaranteed maximum cycle time, time-triggered architecture, and static resource allocation.

Requirements from IEC 61508-3, Table A.3 that have been met by Rosemount Inc. include suitable programming language, strongly typed programming language, language subset, and tools and translators: increased confidence from use.

Requirements from IEC 61508-3, Table A.4 that have been met by Rosemount Inc. include semi-formal methods, computer aided design tools, defensive programming, modular approach, design and coding standards, structured programming, use of trusted/verified software modules and components, and forward traceability between the software safety requirements specification and software design,

This is also documented in [D80a]. This meets the requirements of SIL 3.

6.1.5 Validation

Validation Testing is done via a set of documented tests. The validation tests are traceable to the Safety Requirements Specification [D30] in the validation test plan [D35]. The traceability matrices show that all safety requirements have been validated by one or more tests. In addition to standard Test Specification Documents, third party testing is included as part of the validation testing. All non-conformities are documented in a change request and procedures are in place for corrective actions to be taken when tests fail as documented in [D17].

Requirements from IEC 61508-2, Table B.5 that have been met by Rosemount, Inc. include functional testing, functional testing under environmental conditions, interference surge immunity testing, fault insertion testing, project management, documentation, static analysis, dynamic analysis, and failure analysis, expanded functional testing, black-box testing, “worst-case” testing, and field experience.

Requirements from IEC 61508-3, Table A.7 that have been met by Rosemount, Inc. include process simulation, modeling, functional and black box testing, and forward and backward traceability between the software safety requirements specification and the software safety validation plan.

[D80a] documents more details on how each of these requirements has been met. This meets SIL 3.

6.1.6 Verification

Verification activities are built into the standard development process as defined in [D17]. Verification activities include the following: Fault Injection Testing, static source code analysis, module testing, integration testing, FMEDA, peer reviews and both hardware and software unit testing. In addition, safety verification checklists are filled out for each phase of the safety lifecycle. This meets the requirements of IEC 61508 SIL 3.

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

Requirements from IEC 61508-3, Table A.5 that have been met by Rosemount Inc. include dynamic analysis and testing, data recording and analysis, functional and black box testing, performance testing, test management and automation tools, and forward traceability between the software design specification and module and integration test specifications.

Requirements from IEC 61508-3, Table A.6 that have been met by Rosemount Inc. include functional and black box testing, performance testing, and forward traceability between the system and software design requirements for hardware/software integration and the hardware/software integration test specifications

Requirements from IEC 61508-3, Table A.9 that have been met include static analysis, dynamic analysis and testing, and forward and backward traceability between the software design specification and the software verification plan.

[D80a] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

6.1.7 Modifications

Modifications are done per the Rosemount Inc.'s change management process as documented in [D24]. Impact analyses are performed for all changes once the product is released for integration testing. The results of the impact analysis are used in determining whether to approve the change. The standard development process as defined in [D17] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D21]. This procedure includes identification of the problem, analysis of the problem, identification of the solution, and communication of the solution to the field. This meets the requirements of IEC 61508 SIL 3.

The modification process has been successfully assessed and audited, so Rosemount Inc. may make modifications to this product as needed. or Since this was the initial assessment of 644 Temperature Transmitter's modification procedure according to IEC 61508, it was expected that modifications to the product prior the assessment did not include a functional safety impact analysis. The modification process has been revised to include a functional safety impact analysis. The initial post assessment modification to the 644 Temperature Transmitter shall be audited by *exida* to confirm that a functional safety impact analysis was performed according to Rosemount Inc.'s modification procedure.

- As part of the *exida* scheme a surveillance audit is conducted every 3 years. 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

This meets the requirements of SIL 3.

6.1.8 User documentation

Rosemount Inc. created a safety manual for the 644 Temperature Transmitter [D160] which addresses all relevant operation and maintenance requirements from IEC 61508. This safety manual was assessed by *exida* certification. The final version is considered to be in compliance with the requirements of IEC 61508.

Requirements from IEC 61508-2, Table B.4 that have been met by Rosemount, Inc. include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities, and protection against operator mistakes.

[D80a] documents more details on how each of these requirements has been met. This meets the requirements for SIL 3.

6.2 Hardware Assessment

To evaluate the hardware design of the 644 Temperature Transmitter Failure Modes, Effects, and Diagnostic Analysis's were performed by *exida*. These are documented in [R1].

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. All failure rate analysis results and useful life limitations are listed in the FMEDA report [R1]. Tables in the FMEDA report list these failure rates for the 644 4-20mA / HART Temperature Transmitter under a variety of applications. The failure rates listed are valid for the useful life of the devices.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore, the 644 Temperature Transmitter can be classified as a 2_H device. When 2_H data is used for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H.

If Route 2_H is not applicable for the entire element, the architectural constraints will need to be evaluated per Route 1_H.

Note, as the 644 4-20mA / HART Temperature Transmitter are only one part of a (sub)system, the SFF should be calculated for the entire element combination.

These results must be considered in combination with PFD_{avg} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The architectural constraints requirements of IEC 61508-2, Table 2 also need to be evaluated for each application. It is the end user's responsibility to confirm this for each particular application and to include all components of the element in the calculations.

The analysis shows that the design of the 644 4-20mA / HART Temperature Transmitter can meet the hardware requirements of IEC 61508, SIL 3 and SIL 2 for the 644 4-20mA / HART Temperature Transmitter depending on the complete element design. The Hardware Fault Tolerance and PFD_{avg} requirements of IEC 61508 must be verified for each specific design.

6.3 Recommendations for improvement

During the assessment in 2014, there were a number of cases found where there was either a minor non-conformance or a recommended update to the development process identified. In these cases the issues identified were deemed not to have a significant effect on the overall functional safety of the product. Therefore, these items can be considered recommendations to reduce the risk of non-compliance for future development efforts or modifications. The items found are described below:

- Test environment, tools, configuration and programs used should be included in future integration test plans
- The integration plan shall consider details of those who shall carry out the integration. This information could also be included in another document such as the roles and responsibilities document.
- Coding standard or other document should state that interrupts should only be used if they simplify the design.
- Recommend adding to source code standard the following: Complex calculations are avoided as the basis of branching and loop decisions.
- The analysis made and the decisions taken on whether to continue the integration test or issue a change request, in the case when discrepancies occur should be documented in the integration test results.
- The design specification should document the control flow triggering of the product. This means that the control flow of the product at a high level should be defined including a definition of different tasks or interrupts that will occur along with a description on how those tasks or interrupts will be triggered and what major functions will be executed in each task or interrupt.
- Create a list of all modules along with a link to their unit test results or explanation as to why no module test is needed. This will make it easier to confirm that all applicable modules have been unit tested.
- For SIL 3, when software is changed all functional tests should be re-run. This is highly recommended meaning that written justification is required if only a subset of tests will be re-run. The development process should be updated to indicate that this should be done.
- Software Complexity metrics are calculated, but not analyzed. The development process should be updated to state that modules with complexities above a certain level must be justified. This justification was done for this release, but should be made part of the process so that the justification is done sooner.
- Update process to ensure that unit test checklists are filled out for all unit tests.

- Module tests often show coverage less than 100%. This code has been identified as non-safety critical, so 100% coverage not required. However, in order to ensure that all safety critical code is covered, an explanation should be documented whenever 100% coverage is not achieved.

7 2017 IEC 61508 Functional Safety Surveillance Audit

7.1 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 644 4-20mA / HART Temperature Transmitter
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Rosemount Inc. contracted *exida* in July 2017 to perform the surveillance audit for the above 644 Temperature Transmitter. The surveillance audit was conducted remotely.

7.2 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 644 Temperature 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.

7.3 Surveillance Results

7.3.1 Procedure Changes

There were no changes to the procedures during the previous certification period.

7.3.2 Engineering Changes

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

7.3.3 Impact Analysis

A safety impact analysis for a minor enhancement was reviewed and all documentation was found to be acceptable.

7.3.4 Field History

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

7.3.5 Safety Manual

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

7.3.6 FMEDA Update

The FMEDA was not updated during this surveillance audit.

7.3.7 Evaluate use of certificate and/or certification mark

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

7.3.8 Previous Recommendations

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

8 Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test It is assumed that the Partial Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption, the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Random Capability	The SIL limit imposed by the PFD_{avg} for each element.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

9 Status of the Document

9.1 Liability

exida prepares reports based on methods advocated in International standards. *exida* accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

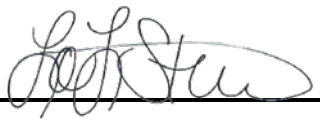
9.2 Releases

Version:	V2	
Revision:	R3	
Version History:	V2, R3:	Recertification update; LLS 11/16/17
	V2, R2:	Updated per customer comments; TES 1/23/15
	V2, R1:	Recertification; TES 11/21/14
	V1, R1:	Updated based on review comments
	V0, R1:	Draft; September 4, 2012
Authors:	Michael Medoff	
Review:	V2, R3:	Ted Stewart 11/16/17
Release status:	RELEASED	

9.3 Future Enhancements

At request of client.

9.4 Release Signatures



Loren L. Stewart, CFSE, Senior Safety Engineer

Ted E. Stewart, CFSP
Program Development & Compliance Manager