IEC 61508 Functional Safety Assessment

Project:
3144 4-20mA / HART Temperature Transmitter
Device Label SW REV 1.1.X

Customer:
Rosemount Inc.
Emerson Automation Solutions
Shakopee, MN
USA

Contract Number: Q16/12-041
Report No.: ROS 11-02-57 R002
Version V2, Revision R3, November 16, 2017
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

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the 3144 Temperature Transmitter

- 3144 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..

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. 3144 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.:

- 3144 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 3144 4-20mA / HART Temperature Transmitter
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment..

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

Rosemount Inc. originally contracted exida in November 2011 with the original IEC 61508 Functional Safety Assessment of the above mentioned device and to recertify the product in July 2014.

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.

Ref.	Document ID	Document Description	Revision
[D1]	DOP 416	Safety Instrumented Systems Product Design and Development Process	Rev I; 2/1/12
[D2]	DOP 440	Engineering Change Order	Rev AK; 2/1/11
[D3]	EDP 400-500	Peer Review Procedure	Rev A.1
[D4]	EDP 400-300	Configuration and Change Management Procedure	Rev C
[D5]	701-063/2003T	TUV Certification Report of the 3144P SIS Temperature Transmitter	Rev 1.0
[D6]	03144-2108.pdf	Schematic, 3144P Electronics Board Fieldmount	2/16/17 Rev AP
[D7]	3144P_SIA	3144P Safety Impact Analysis	2/1/17
[D8]	SafetyRequirements.pdf	Safety Requirements Specification	Rev C.1
[D9]	SAS2550/04	TUV Certificate for 3144P SIS Temperature Transmitter	10/27/2004
[D10]	3144P_STD_SIS- HSTP.doc	Hardware System Test Plan for the 3144P HART Temperature Transmitter	Rev. A
[D11]	3144P_STD_SIS- STP.doc	Software System Test Plan for the 3144P HART Temperature Transmitter	Rev. A.5
[D12]	3144P HART SCCT.htm	Minutes of Software Configuration Control Team meeting 5/23/06	12/14/06
[D13]	3144P STD/SIS SCCT.htm	Minutes of Software Configuration Control Team meeting 11/30/06	12/14/06
[D14]	3144P_STD_SIS_ Accuracy.xls	Test Results for Accuracy Test	12/14/06
[D15]	3144P_std_sis_code_ cons_log_and_report.xls	Inspection Report for 3144P Code Changes (Discrepancies and Merge	12/14/06

		Standard with SIS)	
[D16]	3144P_std_sis_pdp.xls	3144P Project Defined Process	Rev. B
[D17]	3144P_std_sis_sirs_ cons_log_and_report.xls	Inspection Report for Safety Requirements Specification	Rev. C.0
[D18]	3144P_std_sis_stp_ cons_log_and_report.xls	Inspection Report for Software System Test Plan	Rev. 0.1
[D19]	Schematic Review Notes.doc	Design Review Minutes	11/18/05
[D20]	Summary_TraceMatrix.xls	Requirements Traceability Matrix	2/12/07
[D21]	HTP-3144_AD589 replacement.doc	Hardware System Test Plan for the 3144 HART (headmount) transmitter	Rev. B
[D21a]	W__3144PH_source_ embedded_it_results_ 3144p_std_sis_it_re.pdf	Integration Test Report	12/14/2006
[D21b]	User Manual Updates	Scanned copy of marked up user manual. This copy lists changes that will be made to the user manual for this release	12/20/06
[D22]	00825-0100-4021	3144P Quick Installation Guide	Rev. DA
[D23]	00809-0100-4021	3144P Reference Manual	Rev. EA
[D24]	00813-0100-4021	3144P Product Data Sheet	Rev. GA
[D25]	PRD00030658.DOC	Impact Analysis for PRD #00030658	2/6/07
[D26]	PRD00030659.DOC	Impact Analysis for PRD #00030659	2/5/07
[D27]	PRD00030666.DOC	Impact Analysis for PRD #00030666	2/5/07
[D28]	PRD00030667.DOC	Impact Analysis for PRD #00030667	2/5/07
[D29]	PRD00030671.DOC	Impact Analysis for PRD #00030671	2/8/07
[D30]	PRD00030677.DOC	Impact Analysis for PRD #00030677	2/6/07
[D31]	PRD00031035.DOC	Impact Analysis for PRD #00031035	2/8/07
[D32]	PRD00031473.DOC	Impact Analysis for PRD #00031473	2/8/07
[D33]	3144p_std_sis_srs.html	Software Requirements	Rev B.2

		Specification for the 3144P HART® Standard/Safety Temperature Transmitter Project	
[D34]	AO_4-20mA.doc	4-20 mA Ranging Test Results Summary	12/20/06
[D35]	Various	4-20 mA Ranging Detailed Test Results Data	12/13/06
[D36]	AlarmCharacteristics_ 3144P_SIS.doc	Alarm Characteristic Test Results Summary	1/16/07
[D37]	Various	Alarm Characteristic Test Results Data	12/13/06
[D38]	Continuity.doc	Strip Chart Continuity Test Results Summary	2/9/07
[D39]	Various	Strip Chart Continuity Test Results Data	12/13/06 & 2/6/07
[D40]	Diagnostics-Pt1.doc	Diagnostics Part 1 Test Results Summary	2/6/07
[D41]	Diagnostics-Pt1_SIS_STD.xls	Diagnostics Part 1 Test Results Data	1/31/07
[D42]	LCD_Meter.doc	LCD Meter Test Results	2/12/07
[D43]	Open_Sensor_Detection_ 3144P_STD_SIS.doc	Open Sensor Detection Test Results Summary	1/16/07
[D44]	Various	Open Sensor Detection Test Results Data	12/13/06
[D45]	Accuracy-3144P_STD_ SIS.doc	Accuracy Test Results Summary	2/8/07
[D46]	3144P_STD_SIS_ Accuracy.xls	Accuracy Test Results Data	2/5/07
[D47]	TempEffect_3144P_STD_ SIS.doc	Temperature Effect Test Results Summary	2/9/07
[D48]	3144p_STD_Safety_ tempeffects.xls	Temperature Effect Test Results Data	2/9/07
[D49]	NC604145	EMC Test Result Summary	Rev. A
[D50]	3144p_std_sis_it_report.html	3144P Integration Test Report	2/12/07
[D51]	Mohajer Training Records.xls	Training Records/Competency Report	2/12/07
[D52]	3144p_std_sis_ LiteratureReview02092007.doc	Meeting Minutes from User Documentation Review	2/12/07
[D53]	3144p_std_sis_EmulatorTests.doc	3144 Safety as Standard Emulator Test Results	2/12/07
[D54]	RTC 1020023 Testing.pdf	Test Results for ECO	2/12/07

		#RTC1020023	
[D55]	Layout Review Notes	Minutes from Layout Review Meeting	2/9/07
[D56]	Various	Markup for user manual updates from user documentation review	2/12/07
[D57]	3144P_H7D_SIA_PRD00112145.doc	Completed Impact Analysis Form for change to product	1/18/2012
[D58]	3144P_H7D_SIA_PRD00112195.doc	Completed Impact Analysis Form for change to product	1/19/2012
[D59]	3144P_H7D_SIA_PRD00112196.doc	Completed Impact Analysis Form for change to product	1/19/2012
[D60]	DanHerzogEduExp.pdf	Competency report for Dan Herzog	4/13/2012
[D61]	Manual_cons_log_and_report.xls	User Manual Inspection report	12/12/2012
[D62]	SW_Professional_Development Analysis_adammat.pdf	Competency Report for Adam Mateen	3/29/2012
[D63]	SW_Professional_Development Analysis_JeffRoberts.pdf	Competency Report for Jeff Roberts	4/2/2012
[D64]	SW_Professional_Development Analysis_VivekS.pdf	Competency Report for Vivek Shinde	3/30/2012
[D65]	SW_Professional_Development Analysis_YuryK.pdf	Competency Report for Yury Kuznetsov	3/30/2012
[D66]	3144P_H7D_SIA_PRD00XXXXXX.doc	Completed Impact Analysis Forms for changes to product documented by PRD00XXXXXX where XXXXXX = 057645, 057821, 057869, 057888, 057905, 057910, 112026, 112053, 112081, 112127, 112145, 112164, 112195, 112196, 112203, 112278, 112293, 112297, 112298, 112301, 112339, 112358, 112449, 112468, and 112478	Various
[D67]	3144P_H7D_SIA_Software.xls	Impact analysis for planned software changes.	Rev 0.4
[D68]	SafetyChcklist.pdf	Completed signed safety manual review checklist	4/12/2012
[D69]	3144P_H7D_Software_Fault_Injection Testing.doc	Software fault injection test results	1/26/2012
[D70]	3144P_HART7_DraftManual_	3144P Temperature	Rev. GA

	20120419.pdf	Transmitter Reference Manual (includes safety manual)	
[D71]	3144NextGenTrainingCompetency	Training and Competency Matrix	n/a; 7/12/2012
[D72]	3144 H7D SVTP Rev B.2	SRD-SRS-SIRS Traceability	
[D73]	3144_SRD-to-ERS-SIRS-HSTP-SVTP_Traceability_Rev1	SIRS-SW Design Traceability	.03; 5/18/2012
[D74]	DOP 1440: Customer Notification Process	DOP 1440: Customer Notification Process	P; 1/19/2010
[D75]	644HA and 3144P Data	3144P and 644 Shipment / Return	N/A

2.4.2 Documentation generated by *exida*

[R1]	Rosemount 3144 Change Audit.xls	Detailed safety case documenting results of assessment (internal document)
[R2]	ROS 11-02-057 R001, V3 R1, 11/14/2017	3144P SIS Temperature Transmitter FMEDA Report

3 Product Descriptions

3.1 3144P Temperature Transmitter

This report documents the results of the Assessment performed for the 3144P 4-20mA HART Temperature Transmitter Hardware version 20 and Software version 1.1.X (Device Label SW REV 1.1.X). The 3144P Temperature Transmitter is a 2 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 3144P Temperature Transmitter is classified as a Type B device according to IEC 61508 (See section 7.4.3.1.3 of IEC 61508-2), having hardware fault tolerance of 0. Combined with one or two temperature sensing elements, the 3144P becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 3144P transmitter are:

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

4 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].

4.1 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

Assessment level

The 3144 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

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.

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

4.2 Assessment level

The 3144 Temperature Transmitter has been assessed per IEC 61508 to the following levels:

- SIL 3capability

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

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Rosemount Inc. for these products against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 see [N1]. The development of the 3144 Temperature 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 Inc. has an IEC 61508 compliant development process as defined in **Error! Reference source not found.**. 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.

5.1.1 Functional Safety Management

FSM Planning
The functional safety management of any Rosemount Inc. Safety Instrumented Systems Product development is governed by **Error! Reference source not found.**. 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 [D4].

Training, Competency recording

Competency is ensured by the creation of a competency and training matrix for the project [D71]. 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.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D1] a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. For the 3144 4-20mA / HART Temperature Transmitter, the requirements specification [D8] 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: [D8], [D20], [D72], and [D73]. 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.

This meets the requirements of SIL 3.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D1]. 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.

5.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D1]. 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 meets the requirements of SIL 3.

5.1.5 Validation

Validation Testing is done via a set of documented tests. The validation tests are traceable to the Safety Requirements Specification [D8] in the validation test plan]. 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 [D1].

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.

This meets SIL 3.

5.1.6 Verification

Verification activities are built into the standard development process as defined in [D1]. 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.

This meets the requirements of SIL 3.

5.1.7 Modifications

Modifications are done per the Rosemount Inc.'s change management process as documented in [D4]. 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 [D1] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D74]. 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 3144 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 3144 Temperature Transmitter shall be audited by *exida* to confirm that a functional safety impact analysis was performed according to 3144 Temperature Transmitter'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

- o Regression test plans

This meets the requirements of SIL 3.

5.1.8 User documentation

Rosemount Inc. created a safety manual for the 3144 Temperature Transmitter [D70] 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.

5.2 Hardware Assessment

To evaluate the hardware design of the 3144 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 3144 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 meet the *exida* criteria for Route 2_H. Therefore, the 3144 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 3144 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 3144 4-20mA / HART Temperature Transmitter can meet the hardware requirements of IEC 61508, SIL 3 and SIL 2 for the 3144 4-20mA / HART Temperature Transmitter. The Hardware Fault Tolerance and PFD_{avg} requirements of IEC 61508 must be verified for each specific design.

6 2017 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 3144 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.

3144 Temperature Transmitter contracted *exida* in July 2017 to perform the surveillance audit for the above 3144 Temperature 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 3144 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.

6.3 Surveillance Results

6.3.1 Procedure Changes

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

6.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period.

6.3.3 Impact Analysis

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

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 Update

The FMEDA did not have to be updated for this surveillance audit.

6.3.7 Evaluate use of certificate and/or certification mark

The 3144 Temperature Transmitter 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 to be assessed at this audit.

6.3.9 Non-Sis Feature

Reviewed Rosemount X-Well and noted that it would not be offered alongside the PT Option (Rosemount X-well).

7 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

8 Status of the Document

8.1 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.

8.2 Releases

Version:	V2	
Revision:	R3	
Version History:	V0, R1:	Draft, April 27, 2012
	V1, R1:	Updated based on comments on FMEDA report, May 14, 2012
	V1, R2:	Added 4-20mA HART to the product name and removed Option code QS or QT from the name as this is no longer required to indicate the safety certified version.
	V2, R1:	Recertification; FMEDA update, TES 11/21/14
	V2, R2:	Updated per customer comments; TES 2/6/15
	V2, R3:	Recert and Updated to IEC61508:2010; LLS 11/16/17
	Review:	V2, R3 Ted Stewart
Release status:	RELEASED	

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Loren L. Stewart, CFSE, Senior Safety Engineer

Ted E. Stewart, CFSP
Program Development & Compliance Manager