IEC 61508 Functional Safety Assessment

Project:
3051 Pressure Transmitter with 4-20mA HART

Company:
Emerson Automation Solutions (Rosemount, Inc.)
Shakopee, MN
USA

Contract No.: Q18-11-012
Report No.: ROS 13/01-010 R002
Version V3, Revision R1, September 9, 2019
Dave Butler

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

Management Summary

The Functional Safety Assessment of the Rosemount:

- 3051 Pressure Transmitter with 4-20mA HART: Differential and Gage Coplanar
- 3051 Pressure Transmitter with 4-20mA HART: Coplanar Absolute, In-Line Gage and Absolute
- 3051 Level Transmitter with 4-20mA HART
- 3051 Flowmeter with 4-20mA HART

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Rosemount 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 field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Rosemount.

The functional safety assessment was performed to the requirements of IEC 61508:2010. A full IEC 61508 safety case was prepared using the *exida* SafetyCase tool 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 were also 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 3051 Pressure Transmitter with 4-20mA HART 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 3051 Pressure Transmitter with 4-20mA HART can be used in a high demand safety related system in a manner where the PFH is within the allowed range for SIL 2 according to table 3 of IEC 61508-1.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the 3051 Pressure Transmitter with 4-20mA HART can be used in a low demand 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 3051 Pressure Transmitter with 4-20mA HART meets the requirements for architectural constraints of an element such that it can be used to implement a safety function with the following constraints:

- **SIL 2 @ HFT=0, SIL 3 @ HFT=1, Route 1_H where the SFF ≥ 90%**
- **SIL 2 @ HFT=0, SIL 3 @ HFT=1, Route 2_H, Low Demand applications only**
- **SIL 2 @ HFT=1, SIL 3 @ HFT=1, Route 2_H, High Demand application**

This means that the 3051 Pressure Transmitter with 4-20mA HART is capable for use in SIL 2 and SIL 3 applications in Low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual, using the versions specified in section 3.1 of this document.

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

CERTIFIED
IEC 61508
SIL 3 CAPABLE
exida
FS

Table of Contents

1 Purpose and Scope

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

- 3051 Pressure Transmitter with 4-20mA HART

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

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

- the 3051 Pressure Transmitter with 4-20mA HART with the technical IEC 61508-2 and -3 requirements for SIL 3 capability and the derived product safety property requirements

and

- the 3051 Pressure Transmitter with 4-20mA HART 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 capability.

and

- the 3051 Pressure Transmitter with 4-20mA HART hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

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

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

1.1 Tools and Methods used for the assessment

This assessment was carried out 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.

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

2 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

Emerson Automation Solutions (Rosemount, Inc.)	Manufacturer of the 3051 Pressure Transmitter with 4-20mA HART
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

Rosemount contracted *exida* with the IEC 61508 Functional Safety Assessment of the above-mentioned devices.

2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508 (Parts 1 - 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Rosemount

(Second column document identifiers {Dxx} are references to the document in the SafetyCase)

[D1]	{D01}	Functional Safety Management Plan
[D2]	{D02a}	CM Plan checklist from EDP 400-300
[D3]	{D07}	Project Plan
[D4]	{D08}	Project Defined Process Documents
[D5]	{D10}	DOP 1810 Training Procedures
[D6]	{D100}	Integration Test Results
[D7]	{D11}	Safety Competencies
[D8]	{D110}	EMC Test Results
[D9]	{D111}	Validation Test Results

[D10]	{D111a}	ROS Validation Testing Checklist
[D11]	{D112}	Humidity Test results
[D12]	{D113}	Temperature test results
[D13]	{D12}	EDP 400-502 Peer Safety Review
[D14]	{D13}	Training and Competency Matrix
[D15]	{D14}	Safety Instrumented Systems Training Program
[D16]	{D16}	DOP 7 Rosemount Product Development Process
[D17]	{D160a}	Product Safety Manual for 3051
[D18]	{D161a}	WA0007 Safety Manual Checklist
[D19]	{D167}	Product Approvals
[D20]	{D168}	Product Release Version Desscription
[D21]	{D16a}	RMD_G7.3-0001 Product Realization: Project Management Process
[D22]	{D17}	DOP 415 Product Design and Development Process
[D23]	{D18}	DOP 440 Engineering Change Procedure
[D24]	{D19}	DOP 1110 Metrology Procedure
[D25]	{D20}	ISO 9001:2008 Certificate
[D26]	{D21}	DOP 1440: Customer Notification Process
[D27]	{D22}	DP-50111-16 Field Return Analysis Procedure
[D28]	{D23}	Software Coding Standards
[D29]	{D24}	EDP 400-300 Configuration and Change Control Management
[D30]	{D24a}	Configuration Management Plan
[D31]	{D25}	EDP 400-500 Peer Review
[D32]	{D26}	DOP 660 Supplier Corrective Action
[D33]	{D27a}	Corrective And Preventive Action Procedure DOP 8.5
[D34]	{D28}	DOP 1710 Internal Audit Program
[D35]	{D29}	EDP400-600 Quality_Assurance_Procedure
[D36]	{D30}	Safety Integrity Requirements Specification
[D37]	{D32}	SIRS Review
[D38]	{D33}	Customer Requirements Document
[D39]	{D35}	Validation Test Plan
[D40]	{D37}	Safety Validation Plan Review
[D41]	{D38}	Master Test Plan
[D42]	{D40}	Architecture Design Description Document
[D43]	{D40a}	C/T Platform Electronics Architecture
[D44]	{D40b}	System Requirements
[D45]	{D41}	Integration Test Plan

[D46]	{D50}	Detailed Design Description
[D47]	{D53}	Fault Injection Test Plan/Results
[D48]	{D55}	Schematics
[D49]	{D56}	BOM
[D50]	{D57}	HW Component Derating analysis
[D51]	{D58}	HW Verification
[D52]	{D59}	BOM history
[D53]	{D60}	HW Design Guidelines for Test and Manufacture
[D54]	{D61}	HW Requirements Review
[D55]	{D62}	Assembly Drawing
[D56]	{D69}	Hardware Design Phase Verification Checklist
[D57]	{D71}	Detailed Software Design Specification
[D58]	{D73}	SIRS-SW Design Traceability
[D59]	{D78}	SW Architecture Design Review
[D60]	{D79}	Software Architecture and Design Phase Review Log (with review of sw architecture and design checklist)
[D61]	{D81}	WA0007 SIS Checklists
[D62]	{D82}	Software Tools Analysis
[D63]	{D83}	PIU Assessment; IAR Compiler
[D64]	{D90}	PC Lint Configuration file
[D65]	{D90a}	PC Lint resolution example
[D66]	{D90b}	Code Review example
[D67]	{D90c}	PC Lint Results
[D68]	{D91}	Unit Test Records - HW
[D69]	{D92}	Unit Test - SW test plan
[D70]	{D92a}	SW unit test results
[D71]	{D92b}	Test objectives in header file
[D72]	{D92c}	Test objectives in source file
[D73]	{D92d}	Test Techniques to use to develop test plans
[D74]	{D93}	sw module_size_justification
[D75]	{D94}	sw module_test_coverage
[D76]	{D97}	Software DVT Test Plan
[D77]	{D97a}	SW test descriptions
[D78]	{D99a}	Action Items
[D79]	{D127}	Sprint_backlog
[D80]	{D169}	SHA-1 Hash Code for 3051 Pressure Transmitter

2.4.2 Documentation generated by *exida*

[R1]	Rosemount Pressure Transmitter SafetyCase	Detailed safety case documenting results of assessment (internal document, updated)
[R2]	ROS 13/01-010 R001 FMEDA V2 R3; 10/14/16	3051 Pressure Transmitter with 4-20mA HART FMEDA Report
[R3]	ROS 1105075 R001 V1R3 Remote Seal FMEDA_Rosemount.doc; April 29, 2013 or later	Rosemount 1199 Remote Seal FMEDA Report
[R4]	ROS 1304008 R001 V1R0 Primary Elements FMEDA_Rosemount; June 16, 2013 or later	Rosemount Primary Elements FMEDA Report
[R5]	Rosemount Change Audit-3051	Audit of changes for ECO_RTC1053870 {D214}
[R6]	*exida* Modification CL-30Jul12.docx	61508 requirements checklist for Modifications {D216}]

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.

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

- 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 project teams, not individuals were audited.

3 Product Description

The 3051 Pressure Transmitter with 4-20mA HART is available in a wide configuration of solutions to meet the most demanding application needs.

The major components of the 3051 Pressure Transmitter are the sensor module and the electronics housing. The sensor module contains the oil filled sensor system and the sensor electronics. The sensor electronics are installed within the sensor module. The electrical signals from the sensor module are transmitted to the output electronics in the electronics housing and ultimately to the terminal block for connection to the host system. The basic block diagram of the Rosemount differential Coplanar measurement type is shown in Figure 1.

The 3051 Pressure Transmitter with 4-20mA HART series include the following measurement configurations:

- ➢ 3051 Pressure Transmitter with 4-20mA HART: Differential and Gage Coplanar

  The 3051 utilizes capacitance sensor technology for differential Coplanar measurements.

- ➢ 3051 Pressure Transmitter with 4-20mA HART: Coplanar Absolute, In-Line Gage and Absolute

  Piezoresistive sensor technology is used for the absolute Coplanar and In-Line measurements.

- ➢ 3051 Level Transmitter with 4-20mA HART

  A 3051 Pressure Transmitter is available as a Level assembly. The 3051 Level transmitter can be used to measure level on virtually any liquid level vessel. 3051 transmitters and seal systems are designed to offer a flexible solution to meet the performance, reliability, and installation needs of nearly any level measurement application.

- ➢ 3051 4-20mA HART Flowmeter

  A 3051 Pressure Transmitter can be combined with primary elements to offer fully assembled flowmeters. The direct mount flowmeter capability eliminates troublesome impulse lines associated with traditional installations. With multiple primary element technologies available, 3051 flowmeters offer a flexible solution to meet the performance, reliability, and installation needs of nearly any flow measurement application. The flowmeters covered for this assessment are based on the Rosemount 1195, 405, and 485 primary elements. Excluded from the assessment are models with Flo-Tap, remote mount, or temperature input options.

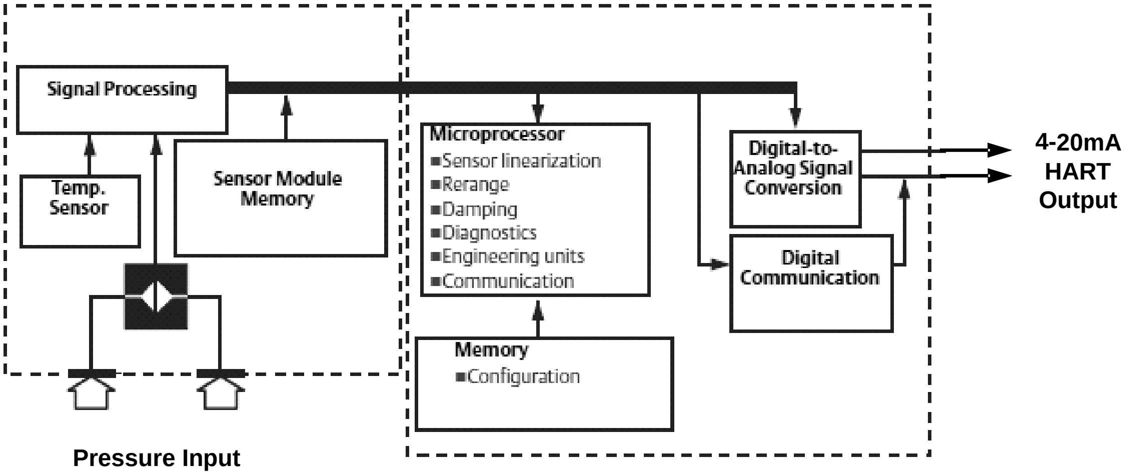

Figure 1 – Rosemount 3051 Pressure Transmitter Block Diagram

Devices used in safety applications with ambient temperatures below -40F (-40C) but does not exceed -76F(-60C) requires options BR5 (-50C) or BR6 (-60C) and QT.

For safety instrumented systems usage, it is assumed that the 4 – 20 mA output is used as the primary safety variable. No other output variants are covered by this assessment.

The 3051 Pressure Transmitter with 4-20mA HART is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0.

The 3051 Pressure Transmitter with 4-20mA HART can be connected to the process using an impulse line, depending on the application the clogging of the impulse line needs to be accounted for, see section 5.1 of the FMEDA reports [R2] to [R4].

3.1 Product Versions

This assessment includes all versions of the models of 3051 Pressure Transmitter with 4-20mA HART with option code QT.

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

4 IEC 61508 Functional Safety Assessment

exida assessed the development process used by Rosemount for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1]. All objectives have been considered in the Rosemount development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements, before the development audit.
The safety case documents the fulfillment of the functional safety management requirements of IEC 61508-1 to -3.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Rosemount3051 Pressure Transmitter with 4-20mA HART, with IEC 61508.

The assessment was executed using the *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the 3051 Pressure Transmitter with 4-20mA HART is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Rosemount 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 shall indicate with respect to the modification:
    - The initiating problem (e.g. results of root cause analysis)
    - The effect on the product / system
    - The elements/components that are subject to the modification
    - The extent of any re-testing
- List of modified documentation
- Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Rosemount 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 3051 Pressure Transmitter with 4-20mA HART 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 has an IEC 61508 compliant development process as defined in [D22]. 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 3051 Pressure Transmitter with 4-20mA HART 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 development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

5.1.2 Safety Lifecycle and FSM Planning

The functional safety management of any Rosemount Safety Instrumented Systems Product development is governed by [D22]. This process requires that Rosemount create a project plan [D3] 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.

5.1.3 Training and competence recording

Competency is ensured by the creation of a competency and training matrix for the project [D14]. 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.

5.1.4 Configuration Management

All documents are under version control as required by [D30].

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

5.1.5 Tools (and languages)

There are no on-line support tools.

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 tool criticalities have been classified and documented. 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. List all T3 and T2 tools along with a reference (file name, document number) to the specification or product manual. The information required for safely using T2 or T3 tools has been documented.

For each tool in class T3, evidence that the tool conforms to its manual through a combination of confidence from use and tool validation. For each tool in class T3, if tool validation was performed, the results of the validation were documented.

5.2 Safety Requirements Specification and Architecture Design

As defined in [D22] a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. For the 3051 Pressure Transmitter with 4-20mA HART, the safety integrity requirements specification (SIRS) [D36] contains a system overview, safety assumptions, and safety requirements sections. During the assessment, *exida* reviewed the content of the specification for completeness per the requirements of IEC 61508: 2010.

Requirements are tracked throughout the development process by the creation of a series of traceability matrices which are included in the following documents: [D36], [D39], [D58], and [D79]. 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 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 include backward traceability between the safety requirements and the perceived safety needs.

5.2.1 Modifications

Modifications are performed per the Rosemount's change management process as documented in [D23] and [D29]. 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 [D22] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D26]. 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.

Requirements from IEC 61508-3, Table A.8 that have been met by the Rosemount modification process include impact analysis, reverify changed software modules, reverify affected software modules, revalidate complete system or regression validation, software configuration management, data recording and analysis, and forward and backward traceability between the software safety requirements specification and the software modification plan (including reverification and revalidation)

The modification process has been successfully assessed and audited, so Rosemount may make modifications to this product as needed. An impact analysis is performed for any change related to functional safety.

5.3 System Design

System or subsystem design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented. The System Architecture Design clearly identifies the SIL of all components in the design.

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.

Formal design reviews are held, and the results recorded; action items are identified, assigned, and resolved.

5.4 Hardware Design and Verification

Hardware design, including both electrical and mechanical design, is done according to [D22]. 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 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, simulation, and inspection of the specification. This meets the requirements of SIL 3.

Verification activities are built into the standard development process as defined in [D22]. Verification activities include the following: Fault Injection Testing, integration testing, FMEDA, peer reviews and both hardware 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 include functional testing, project management, documentation, and black-box testing.

5.4.1 Hardware Architecture Design

Hardware architecture design [D045] 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 guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

5.4.2 Hardware Design / Probabilistic properties

To evaluate the hardware design of the Rosemount3051 Pressure Transmitter with 4-20mA HART, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. The FMEDA was verified using Fault Injection Testing as part of the development, and as part of the IEC 61508 assessment.

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

Failure rates are listed in the FMEDA reports for each important failure category. Refer to the FMEDA ([R2] to [R4]) for a complete listing of the assumptions used and the resulting failure rates.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF.

The FMEDA analysis shows that most of the reviewed 3051 models have a Safe Failure Fraction > 90% (if the logic solver is programmed to detect over-scale and under-scale currents) and therefore those models meet Route 1_H hardware architectural constraints for up to SIL 2 as a single device and SIL 3 with Hardware Fault Tolerance of 1.

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 and the diagnostic coverage is ≥60%. Therefore, all the reviewed 3051 models meet the Route 2_H hardware architectural constraints for up to SIL 2 as a single device when the listed failure rates are used.

If the Rosemount3051 Pressure Transmitter with 4-20mA HART is one part of an element the architectural constraints should be determined for the entire sensor element

The architectural constraint type for the Rosemount3051 Pressure Transmitter with 4-20mA HART Series is B. The required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

The analysis shows that the design of the Rosemount3051 Pressure Transmitter with 4-20mA HART meets the hardware requirements of IEC 61508, SIL 2 @ HFT=0 and SIL 3 @ HFT=1.

5.5 Software (Firmware) Design

Software (firmware) design is done according to [D22]. 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 include fault detection, error detecting codes, failure assertion programming, diverse monitor techniques, stateless software design, retry fault recovery mechanisms, graceful degradation, forward and backward traceability between the software safety requirements specification and software architecture, semi-formal methods, event-driven, with guaranteed maximum response time, static resource allocation, and static synchronization of access to shared resources.

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

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

5.6 Software Verification

Verification activities are built into the standard development process as defined in [D22]. Verification activities include the following: Fault Injection Testing, code reviews, static source code analysis, module testing, integration 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 61508-3, Table A.5 that have been met by Rosemount include dynamic analysis and testing, data recording and analysis, functional and black box testing, performance testing, interface testing, and test management and automation tools.

Requirements from IEC 61508-3, Table A.6 that have been met by Rosemount 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, forward traceability between the software design specification and the software verification plan.

This meets the requirements of SIL 3.

5.7 Safety Validation

Validation Testing is done via a set of documented tests. The validation tests are traceable to the Safety Requirements Specification [D36] in the validation test plan [D39]. 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 [D22].

Requirements from IEC 61508-2, Table B.5 that have been met by Rosemount 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 and black-box testing.

Requirements from IEC 61508-3, Table A.7 that have been met by Rosemount include process simulation, 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.

5.8 Safety Manual

Rosemount created a safety manual for the Rosemount3051 Pressure Transmitter with 4-20mA HART [D17] which addresses all relevant operation and maintenance requirements from IEC 61508. This safety manual was assessed by *exida*. The final version is considered to be in compliance with the requirements of IEC 61508.

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

This meets the requirements for SIL 3.

6 2019 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Rosemount	Manufacturer of the 3051 Pressure Transmitter with 4-20mA HART
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Rosemount contracted *exida* in June 2019 to perform the surveillance audit for the above 3051 Pressure Transmitter with 4-20mA HART. 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 3051 Pressure Transmitter with 4-20mA HART.
- 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.
- 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 Documentation provided by Rosemount for Surveillance

Ref	Description
[E1]	Configuration and Change Management
[E2]]	Control of Monitoring and Measuring Equipment
[E3]	Corrective Action - Preventive Action Process
[E4]	Customer Notification Process
[E5]	Document and Record Management Process
[E6]	Engineering Change Order (ECO) Process
[E7]	Failure Analysis Process
[E8]	How to Write and Assemble a Failure Analysis Laboratory Summary
[E9]	Peer Review Work Instruction
[E10]	Product Design and Development Process
[E11]	Quality Manual
[E12]	Safety-related Systems Verification Checklists
[E13]	Supplier Quality Manual
[E14]	Supply Chain Supplier Corrective Action Process Description
[E15]	Safety Manual - 00809-0100-4007_RevBB_8.20_UF.pdf
[E16]	Compatibility Test results

6.4 Surveillance Documentation generated by *exida*

[R1]	Surveillance Audit Checklist - Rosemount 2051_3051.xlsx	IEC 61508 Surveillance Case for 3051 Pressure Transmitter with 4-20mA HART
[R2]	ROS 18-11-012 V1R0 Field Failure Analysis - 2051_3051.xlsx	Field Failure Analysis for 3051 Pressure Transmitter with 4-20mA HART

6.5 Surveillance Results

6.5.1 Procedure Changes

Changes were made to procedures documented in 6.3. Changed procedures were reviewed and found to be consistent with the requirements of IEC 61508.

6.5.2 Engineering Changes

There were no significant design changes to these products during the previous certification period. Engineering changes and impact analyses for minor changes were reviewed and all documentation was found to be acceptable.

6.5.3 Impact Analysis

There were no safety-related design changes during the previous certification period.

6.5.4 Field History

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

6.5.5 Safety Manual

Reviewed changes to the Safety Manual (00809-0100-4007) and found to meet the relevant requirements of IEC61508.

6.5.6 FMEDA Update

No FMEDA changes were needed for this Surveillance Audit.

6.5.7 Evaluate use of certificate and/or certification mark

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

6.5.8 Previous Recommendations

There were no previous recommendations to be assessed by this assessment.

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 in which the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
Random Capability	The SIL limit imposed by the Architectural Constraints 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 robustness of the design process and the methods used to avoid systematic faults in the design as described in the IEC 61508 tables.
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

8 Status of the Document

8.1 Liability

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

8.2 Releases

Contract Number	Report Number	Revision Notes
Q18/11-012	ROS 13-01-010 R002 V3R1	Update errors and omissions; DEB 9/9/2019
Q18/11-012	ROS 13-01-010 R002 V3R0	Surveillance Audit; DEB; July 26, 2019
Q15/10-010	ROS 13-01-010 R002 V2R3	Included cold temperature; updated template; recertification; TES 10/14/16
Q14/12-011	ROS 13-01-010 R002 V2R2	Updated per customer comments; May 2015; TES
Q14/12-011	ROS 13-01-010 R002 V2R1	Recertification; added surveillance section; April 2015; TES
Q13/01-010	ROS 13-01-010 R002 V1R2	Updated ROS 13/01-010 R001 FMEDA V1 R2; Dec 13, 2013
Q13/01-010	ROS 13-01-010 R002 V1R1	Released March 21, 2013
Q13/01-010	ROS 13-01-010 R002 V1R0	updated from ROS 11/07-062 and updated to incorporate Rosemount feedback/comments for cert; Ted Stewart; March 14, 2013

Original Authors: Michael Medoff, John Yozallinas

Review: V3, R0: Loren Stewart; August 26, 2019

Status: Released

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

David Butler, CFSE, exidaCSP, Evaluating Assessor

Loren L. Stewart, CFSE, Certifying Assessor