



IEC 61508 Functional Safety Assessment

Project:

Emerson Automation Solution
Rosemount® 2090 Pressure Transmitter with 4-20mA HART
Device Label SW 1.0.0-1.4.x

Company:

Rosemount Inc.
Shakopee, MN
USA

Contract No.: Q17-11-003

Report No.: ROS 17/11-003 R001

Version V1, Revision R1, January 15, 2018

Ted 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.

© All rights reserved.

Management Summary

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

- Emerson's Rosemount® 2090 Pressure Transmitter with 4-20mA HART

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 creation of a detailed safety case against the requirements of IEC 61508.
- *exida* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior. This included detailed Markov models of the fault tolerant architectures done in order to show accurate average probability of failure on demand.

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 was used as the primary audit tool. Hardware and software 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 by the following statements:

The Emerson's Rosemount® 2090 Pressure Transmitter with 4-20mA HART was found to meet the Random Capability requirements for a Type B element of SIL 2@HFT=0 and SIL 3@HFT=1 (Route_{1H} for models where the SFF ≥ 90% and all models Route 2_H) and the Systematic Capability requirements for SC 3 (SIL 3 Capable).

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



Table of Contents

Management Summary	2
1 Purpose and Scope	4
1.1 Tools and Methods used for the assessment	4
2 Project management.....	5
2.1 exida	5
2.2 Roles of the parties involved	5
2.3 Standards / Literature used	5
2.4 Reference documents	5
2.4.1 Documentation provided by Rosemount	5
2.4.2 Documentation generated by exida	8
2.5 Assessment Approach	8
3 Product Description	10
4 IEC 61508 Functional Safety Assessment.....	11
4.1 Methodology	11
4.2 Assessment level	11
5 Results of the IEC 61508 Functional Safety Assessment.....	12
5.1 Lifecycle Activities and Fault Avoidance Measures	12
5.1.1 Functional Safety Management	12
5.1.2 Safety Requirements Specification and Architecture Design.....	12
5.1.3 Hardware Design.....	13
5.1.4 Software (Firmware) Design	13
5.1.5 Validation.....	14
5.1.6 Verification.....	14
5.1.7 Modifications	15
5.1.8 User documentation.....	15
5.2 Hardware Assessment	16
6 Terms and Definitions.....	17
7 Status of the Document	18
7.1 Liability	18
7.2 Version History.....	18
7.3 Future Enhancements	18
7.4 Release Signatures.....	18

1 Purpose and Scope

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

- Rosemount 2090 Pressure Transmitter

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

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

- the Rosemount 2090 Pressure Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the Rosemount 2090 Pressure Transmitter development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

and

- the Rosemount 2090 Pressure Transmitter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

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

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

1.1 Tools and Methods used for the assessment

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

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

The assessment was planned by *exida* agreed with Rosemount Inc. (see [R4]).

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 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 Emerson's Rosemount 2090 Pressure Transmitter
exida Performed the IEC 61508 Functional Safety Assessment

Rosemount Inc. 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

[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
[D18]	{D161a}	WA0007 Safety Manual Checklist
[D19]	{D167}	Product Approvals
[D20]	{D168}	Product Release Version Description
[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
[D81]		SIS Impact Analysis

[D82]		2090 Product Data Sheet
[D83]	00813-0100-4698, Rev FC	2090F Hygienic PT Product Data Sheet
[D84]	00813-0100-4699, Rev HC	2090P Pulp and Paper PT Product Data Sheet
[D85]	0080902004108 Rev AA	2090 Safety Manual

2.4.2 Documentation generated by *exida*

[R1]	Rosemount Pressure Transmitter SafetyCase	Detailed safety case documenting results of assessment (internal document, updated)
[R2]	ROS 17-11-003 R002 V1R1 2090 FMEDA	Emerson's Rosemount 2090 FMEDA report
[R3]	ROS 17-11-003 Type B 2090 IEC 61508 Certification Application	2090 Certification Application

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 Inc..

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

- 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

Emerson’s Rosemount 2090 Pressure Transmitter with 4-20mA HART is used in the Hygienic, Pulp and Paper industries for both control and safety applications.

The major components of the Rosemount 2090 are the sensor module and the electronics housing. The sensor module contains the oil filled sensor system. The electrical signals from the sensor module are transmitted to the output electronics and then to the terminal block for connection to the host system. The basic block diagram of the Rosemount 2090 is shown in Figure 1.

Emerson’s Rosemount 2090P and Rosemount 2090F are within the scope of this FMEDA where the In-line Gage and Absolute Piezoresistive sensor technology is used for the In-Line measurements.

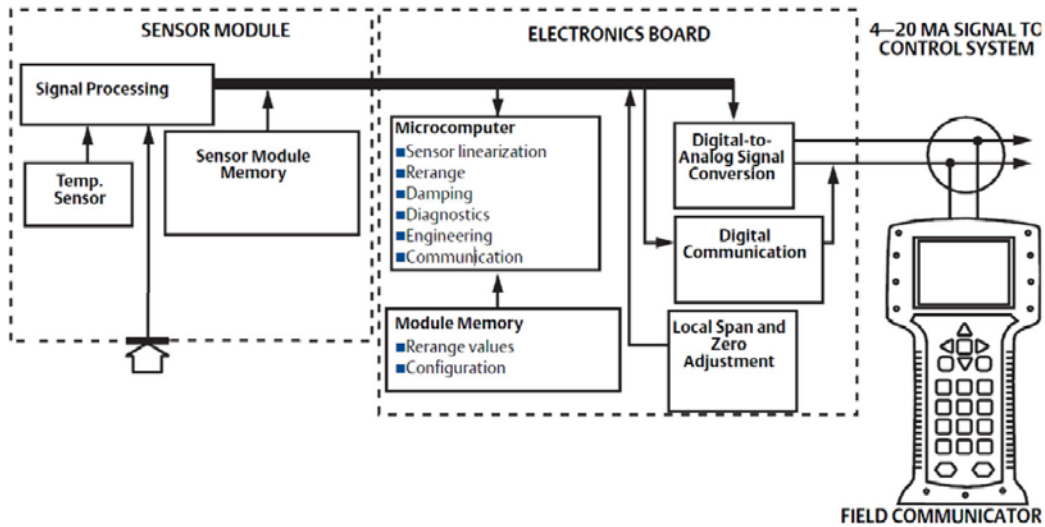


Figure 1 –Rosemount 2090 Pressure Transmitter Block Diagram

The Emerson’s Rosemount 2090 Pressure Transmitter is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

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

The IEC 61508 Functional Safety Assessment was performed based on the information received from Rosemount and is documented in the SafetyCase [R1].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software 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.

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
- 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 5.1. The review of the product design is described in section 5.2.

4.2 Assessment level

The Emerson's Rosemount 2090 Pressure Transmitter has been assessed per IEC 61508 to the following levels:

- Systematic Capability SC3 (SIL 3 capability) as the development procedures were assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3) according to IEC 61508.
- Architecture Constraint limitations of SIL 2 for a single device and SIL 3 for multiple devices in safety redundant configurations with a Hardware Fault Tolerance of 1.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Rosemount Inc. during the product development against the objectives of IEC 61508 parts 1, 2, and 3, see [N1]. The development of the Emerson's Rosemount 2090 Pressure Transmitter was done using this 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 [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 Emerson's Rosemount 2090 Pressure 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 [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.

5.1.2 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 Emerson's Rosemount 2090 Pressure Transmitter, the safety integrity requirements specification (SIRS) [D30] 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: [D30], [D35], [D73], and [D127]. 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 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.

5.1.3 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, simulation, 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 [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, 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 Inc. 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 Inc. 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.

5.1.5 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 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 and black-box testing.

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

5.1.6 Verification

Verification activities are built into the standard development process as defined in [D22]. 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, and black-box testing.

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, interface testing, and test management and automation tools.

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, forward traceability between the software design specification and the software verification plan. [D80a] documents more details on how each of these requirements have been met.

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 [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.

The modification process has been successfully assessed and audited, so Rosemount Inc. may make modifications to this product as needed. The modification process has been revised to include a functional safety impact analysis. The initial post assessment modification to the Rosemount 2090 Pressure 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 SIL 3.

5.1.8 User documentation

Rosemount Inc. created a safety manual for the Emerson's Rosemount® 2090 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 Inc. include operation and maintenance instructions, maintenance friendliness, project management, documentation, and limited operation possibilities. [D80a] documents more details on how each of these requirements have been met.

This meets the requirements for SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the Emerson's Rosemount2090 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 2090 models have a Safe Failure Fraction > 90% (assuming that 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 failure rate data used for this analysis meets the *exida* criteria for Route 2_H and the diagnostic coverage is ≥60%. Therefore, all of the reviewed 2090 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 Emerson's Rosemount 2090 Pressure Transmitter is one part of an element the architectural constraints should be determined for the entire sensor element

The architectural constraint type for the Emerson's Rosemount 2090 Pressure Transmitter 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 Emerson's Rosemount 2090 Pressure Transmitter meets the hardware requirements of IEC 61508, SIL 2 @HFT=0 and SIL 3 @ HFT=1.

6 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time (1×10^{-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. It is assumed that the Partial Stroke Testing, when performed, is 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.
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
HART	Highway Addressable Remote Transducer
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

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

7.2 Version History

Contract Number	Report Number	Revision Notes
Q17-11-003	ROS 17-11-003 R001 V1R1	2090P&F report now released
Q17-11-003	ROS 17-11-003 R001 V1R0	Draft Report

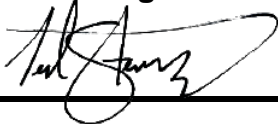
Reviewer: Dr. William Goble; *exida*; Jan. 11, 2018

Status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Ted E. Stewart, CFSP, Program Development & Compliance Manager



Dr. William M. Goble, CFSE, Principal Partner