IEC 61508 Functional Safety Assessment

Project:
3051S HART Advanced Diagnostics Pressure Transmitter
option code DA2

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

Contract No.: Q18/11-012
Report No.: ROS 09-10-22 R001
Version V3, Revision R1, September 9, 2019
Dave Butler

Management Summary

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

- 3051S Advanced HART Diagnostics Pressure Transmitter

The functional safety assessment 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 3051S HART Diagnostics Pressure Transmitter was found to meet the Systematic Capability requirements of IEC 61508 for up to SC 3 (SIL 3 Capable).

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the 3051S HDPT 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 3051S HDPT can be used in a low demand safety related system in a manner where the PFD_{AVG} is within the allowed range for SIL 2 according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the 3051S HDPT 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 3051S HDPT is capable of use in Low, or High, demand mode SIL 2, or SIL 3, applications when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

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:

- 3051S Advanced HART Diagnostics 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 3051S HDPT with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the 3051S HDPT 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 3051S HDPT 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.

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 3051S Advanced HART Diagnostics Pressure Transmitter
exida	Performed the IEC 61508 Functional Safety Assessment

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): ed. 2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Rosemount

[D03]	3051S HDPT Configuration Management Plan
[D04]	Component Derating Analysis
[D05]	Fault Injection Test Report
[D07]	Code Review Results: cons_log_and_report_ProcessVar2
[D08]	Code Review Results: cons_log_and_report_2
[D10]	Worst Case Scenario Analysis
[D11]	3051S HDPT Fault Injection Test Plan.
[D12]	3051S HDPT Phase 2 Hardware DVT2 Plan
[D13]	3051S HDPT Integration Test Cases and Results

[D14]	3051S HDPT Project Defined Process
[D15]	3051S HDPT Project Plan
[D17]	SafetyManual.xlsx
[D18]	3051S HDPT Phase 2 - SW Design Tools
[D19]	3051S Unit Test Checklists
[D20]	3051S HART Diagnostics Phase 2 SW Flow check and external watchdog
[D23]	3051S HDPT Project Schedule
[D24]	3051S HDPT Coding Standard
[D25]	3051S HDPT Safety Integrity Requirements Specification
[D26]	3051S HDPT SIRS Peer Review Logs
[D27]	3051S HDPT Phase 2 System Test Plan
[D28]	3051S HDPT Safety Validation Test Plan
[D29]	3051S HDPT Safety Validation Test Report
[D30]	3051S HDPT SW Design Tools
[D31]	3051S HDPT Trace Matrix Collection
[D32]	3051S HDPT Unit Test Plan
[D33]	61508 Part 2 Tables
[D34]	61508 Part 3 Tables
[D35]	Example Discrepancy with Impact Analysis
[D36]	DOP 1110 Metrology procedure
[D37]	DOP 440 Engineering Change Procedure
[D38]	Customer Notification Process Description
[D39]	DOP 415 Product Design and Development Process
[D40]	EDP 400-300 Configuration and Change Control Management
[D41]	EDP 400-500 Peer Review
[D44]	Integration Test Logs collection
[D45]	Module Review collection
[D48]	Safety Transmitter Coverage of Internal Data Paths
[D49]	Release Document
[D50]	Release Metrics

[D55]	3051S HDPT SW Analysis & Design Model document collection
[D56]	Safety-related Systems Verification Checklists
[D57]	Supplier Quality Manual
[D58];	3051S HDPT Phase 2 Software Architecture - UML
[D59]	Unit Test collection

2.4.2 Documentation generated by *exida*

[R1]	Rosemount 3051S HDPT SafetyCaseDB	Detailed safety case documenting results of assessment (internal document)
[R2]	ROS 08-11-17 R002 V2R3; 10/14/2016	exida 3051S advanced HART diagnostics pressure transmitter FMEDA report, sensor software revision 7 or 8
[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

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

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 report.
The FMEDA has been performed for four different configurations of the 3051S Pressure Transmitter, i.e. Coplanar, In-Line, Level, and Flow configurations. The 3051S Pressure Transmitter series include the following measurement configurations:

- 3051S Advanced HART Diagnostics Pressure Transmitter: Differential and Gage Coplanar

  The 3051S utilizes capacitance sensor technology for differential Coplanar measurements.

- 3051S Advanced HART Diagnostics Pressure Transmitter: Coplanar Absolute, Inline Gage and Absolute

  Piezoresistive sensor technology is used for the absolute Coplanar and Inline measurements.

- 3051S Advanced HART Diagnostics Pressure Transmitter Level

  A 3051S Advanced HART Diagnostics Pressure Transmitter is available as a Level assembly. The Pressure Transmitter Level can be used to measure level on virtually any liquid level vessel. 3051S 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.

- 3051S Advanced HART Diagnostics Pressure Transmitter Flowmeter

  A 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, Rosemount 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.

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.

The 3051S Advanced HART Diagnostics Pressure Transmitter is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0.

The 3051S Advanced HART Diagnostics Pressure Transmitter 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 report [R2].

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

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following models and software versions of 3051S Advanced HART Diagnostics Pressure Transmitter:

Model	Software Version
3051S…DA2…QT	Sensor SW 7.0 or later

Note that 3051S models that do not have option codes DA2 and QT are not covered by this assessment.

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 3051S Advanced HART Diagnostics Pressure Transmitter, 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 3051S Advanced HART Diagnostics Pressure Transmitter 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 IEC 61508 parts 1, 2, and 3, see [N1]. The development of new components in the 3051S Advanced HART Diagnostics Pressure Transmitter was done using this development process. Two existing components, the 3051 Supermodule and the RTOS, were re-used from previous certified products and met the requirements for proven in use. 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 [D39]. 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 3051S Advanced HART Diagnostics 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 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 Safety Instrumented Systems Product development is governed by [D39]. This process requires that Rosemount create a project plan [D15] 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 [D03].

Training, Competency recording

Competency is ensured by a periodic review process. Periodically (at least once per year) each person's skills will be reviewed against the requirements of their job. Any deficiencies will be identified, and a plan will be created to resolve the deficiencies in a timely manner. Deficiencies can be resolved via external training, self-training and on the job training (experience). All formal training is documented in the training and development database.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D39] a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. For the 3051S Advanced HART Diagnostics Pressure Transmitter, the safety integrity requirements specification (SIRS) [D25] 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.

Requirements are tracked throughout the development process by the creation of a series of traceability matrices [D31]. The system safety requirements are broken down into derived hardware and software 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, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, semi-formal methods and checklists. [D33] 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 [D39]. 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 is also documented in [D33]. This meets the requirements of SIL 3.

5.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D39]. 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.4 and A.5 that have been met by Rosemount 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, dynamic analysis and testing, data recording and analysis, functional and black box testing, and performance testing. This is also documented in [D34]. This meets the requirements of SIL 3.

5.1.5 Validation

Validation Testing is done via a set of documented tests. Because the product consists of a relatively small number of components to be integrated, integration and validation testing has been combined. The validation tests are traceable to the Safety Requirements Specification [D25] in the validation test plan [D28]. The traceability matrices [D31] 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 [D39].

Requirements from IEC 61508-2, Table B.3 that have been met by Rosemount include functional testing, project management, documentation, black-box testing and field experience. [D33] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

Requirements from IEC 61508-2, Table B.5 that have been met by Rosemount include functional testing and functional testing under environmental conditions, Interference surge immunity testing, fault insertion testing, project management, documentation, static analysis, dynamic analysis, and failure analysis, “worst case” analysis, expanded functional testing and black-box testing. [D33] documents more details on how each of these requirements has been met. This meets SIL 3.

5.1.6 Verification

Verification activities are built into the standard development process as defined in [D39]. Verification activities include the following: Fault Injection Testing, static source code analysis, 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 include functional testing, project management, documentation, and black-box testing.

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.

5.1.7 Modifications

Modifications are done per the Rosemount's change management process as documented in [D40]. 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 [D39] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D38]. 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.

5.1.8 User documentation

Rosemount created a safety manual for the 3051S Advanced HART Diagnostics Pressure Transmitter [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, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities, and protection against operator mistakes. [D33] 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 3051S HDPT, 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]) 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% (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 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 of 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 3051S Advanced HART Diagnostics 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 3051S Advanced HART Diagnostics 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 3051S Advanced HART Diagnostics Pressure Transmitter meets the hardware requirements of IEC 61508, SIL 2 @HFT=0 and SIL 3 @ HFT=1.

6 2019 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Rosemount	Manufacturer of the 3051S Advanced HART Diagnostics Pressure Transmitter
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 3051S Advanced HART Diagnostics Pressure 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 3051S Advanced HART Diagnostics Pressure 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.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

6.2.1 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
[E16]	3051s DA2 Renewal for SIS.xlsx

6.3 Surveillance Documentation generated by *exida*

[R1]	Surveillance Audit Checklist - Rosemount 3051s DA2.xlsx	IEC 61508 Surveillance Case for 3051S HDPT
[R2]	ROS 18-11-012 V1R0 Field Failure Analysis – 3051s DA2.xlsx	Field Failure Analysis for 3051S Advanced HART Diagnostics Pressure Transmitter

6.4 Surveillance Results

6.4.1 Procedure Changes

Procedure changes were reviewed and were found to be consistent with the requirements of IEC 61508.

6.4.2 Engineering Changes

There were no engineering changes since the last assessment.

6.4.3 Impact Analysis

There were no engineering changes since the last assessment.

6.4.4 Field History

The operating hours were reviewed for the previous 3 years and successfully meet the requirements of IEC61508.

6.4.5 Safety Manual

The Safety Manual (00809-0100-4801) was reviewed and found to successfully meet the requirements of IEC61508.

6.4.6 FMEDA Update

No FMEDA changes were needed for this Surveillance Audit.

6.4.7 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.

6.4.8 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, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
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 Version History

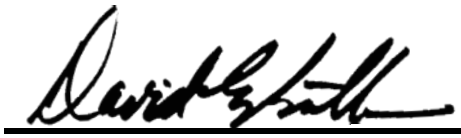
Contract Number	Report Number	Revision Notes
Q18/11-012	ROS 09-10-022 R001 V3R1	Update errors and omissions; DEB 9/9/2019
Q18/11-012	ROS 09-10-022 R001 V3R0	2019 Surveillance Audit; DEB 7/26/2019
Q15/10-010	ROS 09-10-022 R001 V2R2	included cold temperature; updated template; recertification; TES 10/14/16
Q13/10-107	ROS 09-10-022 R001 V2R1	updated to IEC 61508 2010 standard and incorporated route $2_{H;}$ TES; 7/9/14
Q13/04-008	ROS 09-10-022 R001 V1R3	Incorporated additional comments from Emerson for cross product consistency; 6/16/13 Ted Stewart
Q13/04-008	ROS 09-10-022 R001 V1R2	Updated from V1R1; left as 2000 standard per Rosemount request;
Q09/10-022	ROS 09-10-022 R001 V1R1	Updated based on review; July 9, 2010
Q09/10-022	ROS 09-10-022 R001 V0R1	Draft; July 1, 2010

Original Author: Michael Medoff
Original Review: V0, R1: William M. Goble; July 9, 2010
Current Review: V3, R0: Loren Stewart; August 26, 2019
Release status: Released

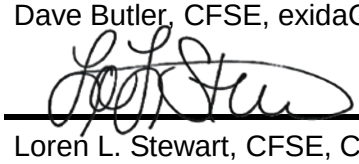
8.3 Future Enhancements

At request of client.

8.4 Release Signatures



Dave Butler, CFSE, exidaCSP, Evaluating Assessor



Loren L. Stewart, CFSE, Certifying Assessor