



IEC 61508 Functional Safety Assessment

Project:

3051S HART Advanced Diagnostics Pressure Transmitter,
option code DA2

Customer:

Rosemount Inc.
(an Emerson Process Management company)
Chanhassen, MN
USA

Contract No.: Q13/10-107

Report No.: ROS 09-10-22 R001

Version V2, Revision R1, September 5, 2014

Ted Stewart

Management summary

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

- Rosemount 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 Inc. through an audit and creation of a detailed assessment against the requirements of IEC 61508.
- *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 ensure that the FMEDA analysis was complete.
- *exida* reviewed the manufacturing quality system in use at Rosemount Inc.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3. A full IEC 61508 Safety Case was prepared using the *exida* SafetyCase tool as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports 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 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 3051S was found to meet the Random Capability requirements for a Type B device of SIL 2@HFT=0, SIL 3@HFT=1 (Route 1_H for models where the SFF ≥ 90% and all models Route 2_H) and Systematic Capability requirements for SC 3 (SIL 3 Capable).

The manufacturer will be entitled to use the Functional Safety Logo.



Table of Contents

Management summary	2
1 Purpose and Scope	4
2 Project management.....	5
2.1 <i>exida</i>	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 Inc.....	5
2.4.2 Documentation generated by <i>exida</i>	7
3 Product Description.....	8
4 IEC 61508 Functional Safety Assessment.....	9
4.1 Methodology.....	9
4.2 Assessment level	9
5 Results of the IEC 61508 Functional Safety Assessment	10
5.1 Lifecycle Activities and Fault Avoidance Measures.....	10
5.1.1 Functional Safety Management	10
5.1.2 Safety Requirements Specification and Architecture Design.....	11
5.1.3 Hardware Design.....	11
5.1.4 Software (Firmware) Design	11
5.1.5 Validation.....	12
5.1.6 Verification.....	12
5.1.7 Modifications.....	13
5.1.8 User documentation.....	13
5.2 Hardware Assessment	14
6 Terms and Definitions	15
7 Status of the document	16
7.1 Liability	16
7.2 Releases	16
7.3 Future Enhancements	16
7.4 Release Signatures	16



1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter by *exida* according to the requirements of IEC 61508: ed2, 2010.

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

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 300 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.

2.2 Roles of the parties involved

Rosemount Inc. Manufacturer of the Rosemount 3051S Advanced HART Diagnostics 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): ed. 2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
------	--------------------------------------	---

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[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
[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
[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
[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
[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 Detailed safety case (internal document)
[R2]	exida 3051S advanced HART diagnostics pressure transmitter FMEDA report, sensor software revision 5 or 6
[R3]	exida 3051S advanced HART diagnostics pressure transmitter FMEDA report, sensor software revision 7 or 8

3 Product Description

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

- Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter: Differential and Gage Coplanar
 - Capacitance technology is utilized for differential Coplanar measurements.
- Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter: Coplanar Absolute, Inline Gage and Absolute
 - Piezoresistive sensor technology is used for the absolute Coplanar and Inline measurements.
- Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter Level
 - A Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter is available as a Level assembly. The Rosemount Pressure Transmitter Level can be used to measure level on virtually any liquid level vessel. Rosemount 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.
- Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter Flowmeter
 - A Rosemount 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.

The Rosemount 3051S Advanced HART Diagnostics Pressure Transmitter is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

The Rosemount 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.

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.

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Rosemount Inc. and is documented here.

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 3051S HDPT has been assessed per IEC 61508 to the following levels:

- SIL 2 capability for a single device
- SIL 3 capability for multiple devices in safety redundant configurations

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.

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 new components in the Rosemount 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 Inc. 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 Rosemount 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 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 [D39]. This process requires that Rosemount Inc. 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 Rosemount 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 Inc. include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, semi-formal methods and checklists. 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 Inc. include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-trying components, checklists, semi-formal methods, computer aided design tools, simulation, and inspection of the specification. 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 Inc. include semi-formal methods, computer aided design tools, defensive programming, modular approach, design and coding standards, structured programming, use of trusted/verified software modules and components, dynamic analysis and testing, data recording and analysis, functional and black box testing, and performance testing. 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 Inc. include functional testing, project management, documentation, black-box testing and field experience. This meets the requirements of SIL 3.

Requirements from IEC **61508-2, Table B.5** that have been met by Rosemount Inc. 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. 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 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.

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 [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 Inc. created a safety manual for the Rosemount 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 Inc. include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities, and protection against operator mistakes. 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] to [R3]) 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 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 Rosemount 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 Rosemount 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 Rosemount 3051S Advanced HART Diagnostics 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
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
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).
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 Releases

Version: V2

Revision: R1

Version History: V2, R1: updated to IEC 61508 2010 standard and incorporated route 2_H; TES; 9/5/14

V1, R3: Incorporated additional comments from Emerson for cross product consistency; 6/16/13 Ted Stewart

V1, R2: Updated from V1R1; left as 2000 standard per Rosemount request;

V1, R1: Updated based on review; July 9, 2010

V0, R1: Draft; July 1, 2010

Authors: Michael Medoff

Review: V0, R1: William M. Goble; July 9, 2010

Release status: Released to Customer

7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Dr. William M. Goble, Principal Partner



Ted Stewart, CFSP, Safety Engineer