Results of the IEC 61508 Functional Safety Assessment

Project:
Rosemount™ 3051S Electronic Remote Sensors (ERS)™ System

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

Contract No.: Q20-07-007
Report No.: ROS 13-10-107 R001
Version V3, Revision R1, September 16, 2020
Ted Stewart

Management Summary

The Functional Safety Assessment of the

Rosemount 3051S Electronic Remote Sensors (ERS) System

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

- *exida* assessed the development process used by Rosemount, Inc. through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The 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, Inc..

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual were also reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The audited development process, as tailored and implemented by the Rosemount 3051S Electronic Remote Sensors (ERS) System development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Rosemount 3051S Electronic Remote Sensors (ERS) System 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 Rosemount 3051S Electronic Remote Sensors (ERS) System can be used in a low demand safety related system in a manner where the PFD_{AVG} is within the allowed range for SIL 3 according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the Rosemount 3051S Electronic Remote Sensors (ERS) System 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 Rosemount 3051S Electronic Remote Sensors (ERS) System is capable for use in SIL 2 and SIL 3 applications in Low demand mode or High demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual, using the versions specified in section 3 of this document.

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

Table of Contents

Management Summary 2

1. Purpose and Scope 6
   - 1.1 Tools and Methods used for the assessment 6

2. Project Management 7
   - 2.1 *exida* 7
   - 2.2 Roles of the parties involved 7
   - 2.3 Standards / Literature used 7
   - 2.4 Reference documents 7
     - 2.4.1 Documentation provided by Rosemount, Inc. 7
     - 2.4.2 Documentation generated by *exida* 9
   - 2.5 Assessment Approach 9

3. Product Description 10
   - 3.1 Software Version Numbers 11

4. IEC 61508 Functional Safety Assessment Scheme 11
   - 4.1 Product Modifications 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 13
     - 5.1.3 Validation 13
     - 5.1.4 Verification 13
     - 5.1.5 Modifications 14
     - 5.1.6 User documentation 14
   - 5.2 Hardware Assessment 15

6. 2020 IEC 61508 Functional Safety Surveillance Audit 17
   - 6.1 Roles of the parties involved 17
   - 6.2 Surveillance Methodology 17
     - 6.2.1 Documentation updated by Rosemount, Inc. 18
     - 6.2.2 Surveillance Documentation generated by *exida* 18
   - 6.3 Surveillance Results 18
     - 6.3.1 Procedure Changes 18
     - 6.3.2 Engineering Changes 18
     - 6.3.3 Impact Analysis 18
     - 6.3.4 Field History 18
     - 6.3.5 Safety Manual 18
     - 6.3.6 FMEDA Update 18
     - 6.3.7 Previous Recommendations 18

7. Terms and Definitions 19
8. Status of the document 20
8.1 Liability 20
8.2 Version History 20
8.3 Future Enhancements 20
8.4 Release Signatures 20

1. Purpose and Scope

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

- Rosemount 3051S Electronic Remote Sensors (ERS) System

by *exida* per 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 3051S Electronic Remote Sensors (ERS) System with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the Rosemount 3051S Electronic Remote Sensors (ERS) System 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 3051S Electronic Remote Sensors (ERS) System 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.

All assessment steps were continuously documented by *exida*.

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, availability and cybersecurity with over 500 person-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 350 billion hours of field failure data.

2.2 Roles of the parties involved

Rosemount, Inc.	Manufacturer of the Rosemount 3051S ERS System
exida	Performed the hardware assessment
exida	Performed the Functional Safety Assessment per *exida's* accredited scheme.

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

Note: Documents revised after the previous audit are highlighted below in grey. Section 6: 2020 IEC 61508 Functional Safety Surveillance Audit lists the updates found during this assessment.

2.4.1 Documentation provided by Rosemount, Inc.

Doc ID	Safetycase ID	Document Name
[D1]	D001	Quality Manual
[D2]	D003	Overall Development Process
[D3]	D004	Configuration Management Process - 3051S ERS System specific
[D4]	D004b	Configuration Management Process - Emerson Process
[D5]	D005	Field Failure Reporting Procedure
[D6]	D006	Field Return Procedure
[D7]	D007	Manufacturer Qualification Procedure

[D8]	D008	Part Selection Procedure - Supplier Quality Manual
[D9]	D008b	Part Selection Procedure - ECO process
[D10]	D010, D010b	Quality Management System (QMS) Documentation Change Procedure
[D11]	D012, D012b, D012c, D012d	Non-Conformance Reporting procedure
[D12]	D013	Corrective Action Procedure
[D13]	D013b	Corrective Action Procedure - Supply Chain Corrective Action
[D14]	D016	Action Item List Tracking Procedure
[D15]	D019	Customer Notification Procedure
[D16]	D021	Software Development Process
[D17]	D021b	Software Tool Qualification Procedure
[D18]	D023	Modification Procedure
[D19]	D023b	Impact Analysis Template
[D20]	D026	FSM Plan or Development Plan
[D21]	D027	Configuration Management Plan
[D22]	D029	Verification Plan
[D23]	D030	Shipment Records
[D24]	D031	Field Returns Records
[D25]	D038	List of Design Tools
[D26]	D040	Safety Requirements Specification
[D27]	D041	Safety Requirements Review Record
[D28]	D043	Software Safety Requirements Specification
[D29]	D045	System Architecture Design Specification
[D30]	D049	High Level Software Design Specification
[D31]	D054, D054b	Verification Results and example
[D32]	D056	Requirements Traceability Matrix
[D33]	D059, D077	Fault Injection Test Plan and Results
[D34]	D060	Coding Standard
[D35]	D069, D070, D074	Validation Test Plan, Record, Results
[D36]	D071, D075	Environmental Test Plan and Results
[D37]	D072, D076, D076b	EMC Test Plan, Results
[D38]	D078	Operation / Maintenance Manual
[D39]	D079	Safety Manual
[D40]	D081	Engineering Change Documentation
[D41]	D088	Impact Analysis Record

2.4.2 Documentation generated by *exida*

[R1]	Q1310-107 - Safety Case WB-61508 V1R4 - 3150S ERS	Baseline Safety Case
[R2]	ROS 10-04-083 R001 V2R5 FMEDA 3051S ERS	FMEDA Report for the 3051S ERS System
[R3]	ROS 13-10-107 R002 V1R1 Safety Communications Analysis ERS	Communications Analysis Report
[R4]	ROS 13-10-107 3051S V1R1 ERS PIU Spreadsheet.xls	Field Failure Analysis Report based on analysis of the 2020 certification period
[R5]	ROS 16-12-041 SC001 V2R0 Safety Case WB-61508 - 3051S ERS	Final Safety Case

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

3. Product Description

The Rosemount 3051S ERS System is a two wire, 4 – 20 mA architecture that calculates differential pressure electronically using two pressure transmitters (primary and secondary) that are linked together with a digital cable. The transmitter system uses standard, well-proven sensor boards in combination with a microprocessor board that performs diagnostics. It is programmed to send its output to a specified failure state, either high or low, when an internal failure is detected.

The bus between the current output microprocessor and the sensor microprocessor has been extended outside the transmitter housing to a second sensor microprocessor with its own housing.

It is assumed that the 4 – 20 mA output is used as a primary safety variable. No other output variants are covered by this report.

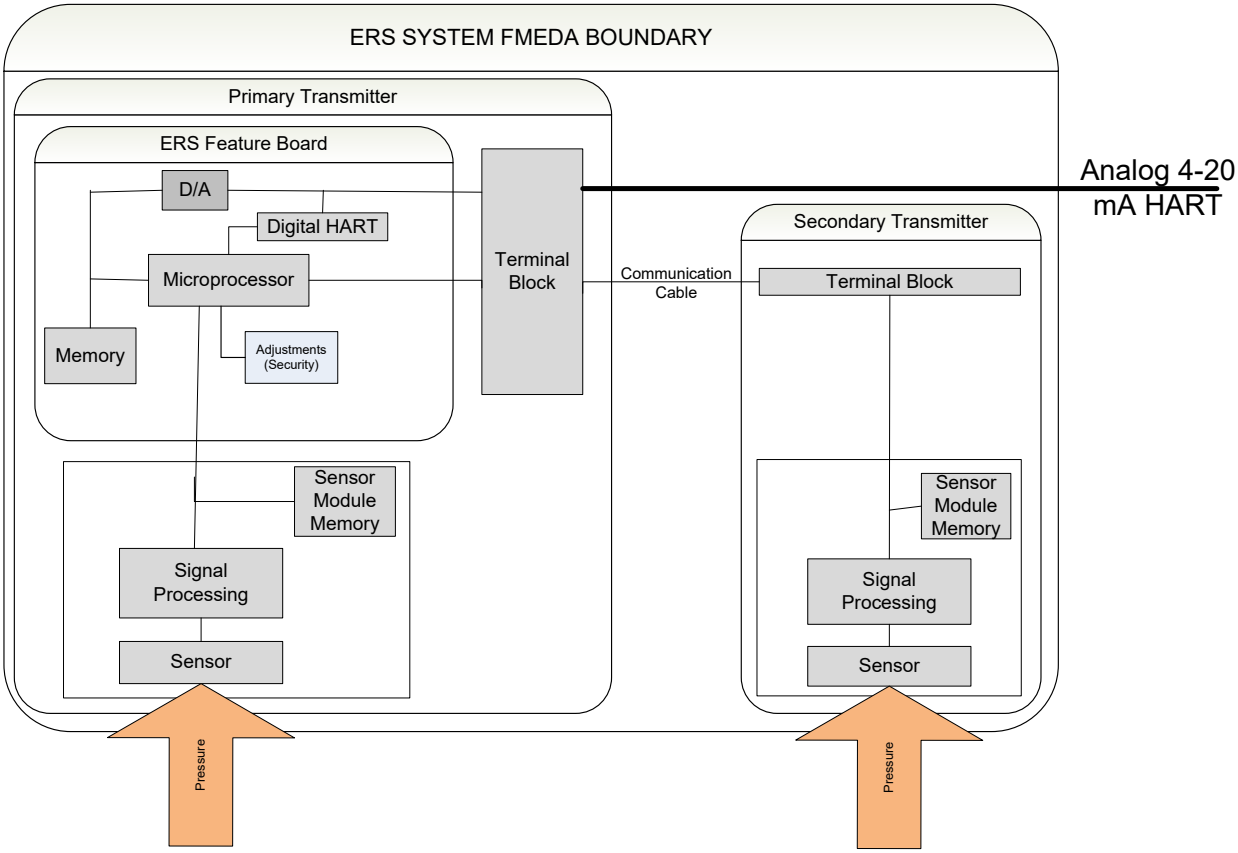


Figure 1: Rosemount 3051S ERS System, Parts included in this certification

3.1 Software Version Numbers

This assessment is applicable to the following hardware and software versions of Rosemount 3051S ERS System:

Model	Software Versions
Rosemount 3051SAL_P	Rev. 57 and above
Rosemount 3051SAL_S	Rev. 57 and above
Rosemount 3051SAM_P	Rev. 57 and above
Rosemount 3051SAM_S	Rev. 57 and above

4. IEC 61508 Functional Safety Assessment Scheme

exida assessed the processes used by Rosemount, Inc., and the engineering work products from those processes, related to the Rosemount 3051S ERS System, in accordance with the objectives of the *exida* certification scheme and the requirements of the IEC 61508 standard. The results of the assessment are documented in [R1].

exida assessed the safety case, which includes documentary evidence, and argues how that evidence demonstrates compliance with the functional safety requirements in IEC 61508 standard. The safety case was created through an assessment of the documentation with respect to the requirements of the IEC 61508 standard. A second, certifying assessment of the safety case was carried out by a second, independent assessor.

The safety case documents the fulfillment of the functional safety requirements of IEC 61508-1 to 3. This assessment report summarizes those findings.

The assessment was carried out, in accordance with *exida*'s certification scheme, which identifies all IEC 61508 standard requirements pertinent to the product's certification, and tailors the assessment to that scope.

The result of the assessment shows that the Product is capable for use in SIL 3 applications, when used properly in a Safety Instrumented Function by adhering to the instructions and constraints found in the Rosemount 3051S ERS System Safety Manual [D39].

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Rosemount, Inc. 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, Inc. during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the Rosemount 3051S ERS System was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Rosemount, Inc. has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D2].

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using the *exida* certification scheme which includes subsets of 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 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 [D2]. This process requires that Rosemount, Inc. create a project plan [D20] 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 [D21].

Training, Competency recording

Competency is ensured by the creation of a competency and training matrix as required by [D2]. 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 [D2] a system requirements document is created for all products that must meet IEC 61508 requirements. For the Rosemount 3051S ERS System, the System Requirements Document [D26] contains a system overview, safety assumptions, constraints, dependencies, and safety requirements sections.

The Product Architecture Design, documented in the System Requirements Document [D26], was assessed and was found to comply with the relevant SIL 3 requirements of the IEC 61508 standard.

5.1.3 Validation

Validation Testing is done via a set of documented tests. The validation test cases, documented in a test specification [D35], are traceable to the safety requirements in the System Requirements Document [D26]. Traces are used to verified that all requirements are tested, by comparing all safety requirements references from the test specification to the list of safety requirements in the System Requirements Document shows that all safety requirements have been validated by one or more validation test cases. In addition to functional testing, third party testing is included as part of the validation plan. All non-conformities uncovered during Validation Testing are documented in change request documentation. Procedures are in place for corrective actions to be taken when tests fail as required by [D2].

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. This meets SIL 3 requirements.

5.1.4 Verification

Verification activities are built into the standard development process as defined in [D2], and include the following: Fault Injection Testing, static source code analysis, integration testing, FMEDA, peer reviews and both hardware and software unit testing. In addition, safety verification checklists are filled out for each required 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.

5.1.5 Modifications

Modifications are done per the Rosemount, Inc.'s change management process as documented in [D18] and [D19]. Impact analyses are performed for all changes once the product is released to production. The results of the impact analysis are used in determining whether to approve the change. The Modification Procedure [D18] is followed and the standard development process is re-entered at the phase specified by the Impact Analysis record, limiting the scope of verification and validation as directed by the Impact Analysis record. The handling of hazardous field incidents and customer notifications is governed by [D15]. This procedure includes identification of the problem, analysis of the problem, identification of the solution, and communication of the solution to the field. This meets the requirements of IEC 61508 SIL 3.

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

5.1.6 User documentation

Rosemount, Inc. created a safety manual for the Rosemount 3051S ERS System [D39] which addresses all relevant operation and maintenance requirements from IEC 61508, and contains safety information which facilitates the proper inclusion of the Rosemount 3051S ERS System into a safety system application. 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.

This meets the requirements for SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the Rosemount 3051S Electronic Remote Sensors (ERS) System, 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.

The FMEDA results must be considered in combination with PFD_{AVG} and architectural constraints 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 Rosemount 3051S ERS System has a Safe Failure Fraction > 90% and therefore, it meets Route 1_H hardware architectural constraints for up to SIL 2 as a single device.

If the Rosemount 3051S ERS System is one part of an element the architectural constraints should be determined for the entire sensor element

The Rosemount 3051S ERS System is a Type B device. The required SIL determines 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.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2.

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 61508-2.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore, the Rosemount 3051S ERS System can be classified as a 2_H device. When 2_H data is used in low demand for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H and used in high demand for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=1 (or SIL 3 @ HFT=1) per Route 2_H.

Note, as the Rosemount 3051S Electronic Remote Sensors (ERS) System are only one part of a (sub)system, the SFF should be calculated for the entire final element combination.

These results must be considered in combination with PFD_{avg} or PFH values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The architectural constraints requirements of IEC 61508-2, Table 2 also need to be evaluated for each final element application. It is the end user's responsibility to confirm this for each particular application and to include all components of the final element in the calculations.

The analysis shows that the design of the Rosemount 3051S Electronic Remote Sensors (ERS) System can meet the hardware requirements of IEC 61508, SIL 3 for the Rosemount 3051S ERS System depending on the complete final element design. The Hardware Fault Tolerance and PFD_{avg} (or PFH) requirements of IEC 61508 must be verified for each specific design.

6. 2020 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Rosemount, Inc.	Manufacturer of the Rosemount 3051S ERS System.
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Rosemount, Inc. contracted *exida*, to perform the surveillance audit for the above Rosemount 3051S ERS System. The surveillance audit was conducted remotely in Sellersville, PA, USA.

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 an of the changes could affect the safety function of the Rosemount 3051S ERS System.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the exida Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

6.2.1 Documentation updated by Rosemount, Inc.

See section 2.4.1 for documents revised during this surveillance audit.

6.2.2 Surveillance Documentation generated by *exida*

See section 2.4.2 for documents revised during this surveillance audit.

6.3 Surveillance Results

6.3.1 Procedure Changes

Changes to the updated procedures were reviewed and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes

No engineering changes occurred since the last assessment.

6.3.3 Impact Analysis

No impact analyses were required.

6.3.4 Field History

Field failure history was analyzed and compared to the failure rates published in the FMEDA Report. The comparison showed that the actual failure rates are less than predicted failure rates.

6.3.5 Safety Manual

The safety manual remained unchanged from the last surveillance audit and continued to be compliant with the IEC 61508 safety manual requirements.

6.3.6 FMEDA Update

The FMEDA Report did not need to be revised during this surveillance period. Since the design remained unchanged, the failure rates remained the same.

6.3.7 Previous Recommendations

Any previous recommendations have been reviewed.

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
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

8. Status of the document

8.1 Liability

exida prepares reports based on methods advocated in International standards. 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
Q20-07-007	ROS 13-07-107 R001 V3R1	Customer Comments; TES 09/16/2020
Q20-07-007	ROS 13-07-107 R001 V3R0	Surveillance Audit; TES 09/1/2020
Q16/02-100	ROS 13-10-107 R001 V2R0	Surveillance Audit; DEB – 5/31/2017
Q13/10-107	ROS 13-10-107 R001 V1R2	Updated revision of the Comm. Analysis Report; DEB – 11/19/2014
Q13/10-107	ROS 13-10-107 R001 V1R1	Updated based on Rosemount comments; DEB – 10/21/2014
Q13/10-107	ROS 13-10-107 R001 V1R0	Initial version; DEB – 9/30/2014

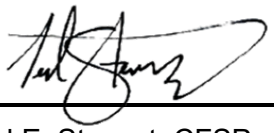
Review: Loren Stewart; 9/1/2020

Status: Released

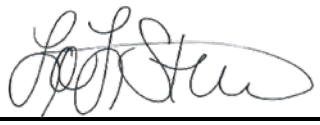
8.3 Future Enhancements

At request of client.

8.4 Release Signatures



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



Loren L. Stewart, CFSE, Senior Safety Engineer