IEC 61508 Functional Safety Assessment

Project:

644 4-20mA / HART Temperature Transmitter

Device Label SW REV 1.1.x

Customer:

Rosemount Inc.
Chanhassen, MN
USA

Contract No.: Q12/04-020
Report No.: ROS 12/04-020 R002
Version V1, Revision R1, September 5, 2012
Michael Medoff

Management summary

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

➢ 644 4-20mA / HART Temperature Transmitter

The functional safety assessment performed by exida consisted of the following activities:

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

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3. A full IEC 61508 safety case was prepared using the exida SafetyCaseDB tool, and used as the primary audit tool. Hardware and software process requirements and all associated documentation were reviewed. Also, the user documentation (safety manual) was reviewed.

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

The 644 4-20mA / HART Temperature Transmitter was found to meet the requirements of SIL 2 for random integrity @ HFT=0, SIL 3 for random integrity @ HFT=1 and SIL 3 capable for systematic integrity.

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 *exida* 5

2.2 Roles of the parties involved 5

2.3 Standards / Literature used 5

2.4 Reference documents 5

2.4.1 Documentation provided by Rosemount 5

2.4.2 Documentation generated by *exida certification* 10

3 Product Description 11

4 IEC 61508 Functional Safety Assessment 12

4.1 Methodology 12

4.2 Assessment level 12

5 Results of the IEC 61508 Functional Safety Assessment 13

5.1 Lifecycle Activities and Fault Avoidance Measures 13

5.1.1 Functional Safety Management 13

5.1.2 Safety Requirements Specification and Architecture Design 14

5.1.3 Hardware Design 14

5.1.4 Software (Firmware) Design 14

5.1.5 Validation 15

5.1.6 Verification 15

5.1.7 Modifications 16

5.1.8 User documentation 16

5.2 Hardware Assessment 18

5.3 Recommendations for improvement 19

6 Terms and Definitions 21

7 Status of the document 22

7.1 Liability 22

7.2 Releases 22

7.3 Future Enhancements 22

7.4 Release Signatures 22

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition, this option includes an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This option for pre-existing (programmable electronic) devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This assessment shall be done according to option 3.

This document shall describe the results of the IEC 61508 functional safety assessment of the 644 4-20mA / HART Temperature Transmitter**,** which will be referred to as the 644 Temperature Transmitter throughout this document.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge and certification 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 services, internet based safety engineering tools, detailed product assurance and certification analysis 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 644 Temperature Transmitter
exida Certification	Performed the IEC 61508 Functional Safety Assessment according to option 3 (see section 1)

Rosemount, Inc. contracted *exida Certification* with the IEC 61508 Functional Safety Assessment of the above mentioned device.

2.3 Standards / Literature used

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

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

2.4 Reference documents

2.4.1 Documentation provided by Rosemount

ID	Name	Version; Date
[D02]	exida Configuration Management Checklist	n/a; 7/27/2012
[D02a]	CM Plan checklist from EDP 400-300	6/27/2012
[D03]	exida Documentation Checklist	n/a; 7/27/2012
[D04]	exida Software Tool Checklist	n/a; 7/21/2012
[D05]	exida Tool Validation Checklists	7/13/2012
[D06]	exida FSM Planning Phase Verification Checklist	n/a; 7/31/2012
[D07]	Project Plan	C.2; 7/11/2012
[D10]	DOP 1810 Training Procedures	R; 1/20/2010
[D109]	exida Integration Test Execution Phase Checklist	na; 7/26/2012
[D11]	Safety Competencies	n/a;

[D110]	EMC Test Results	100672207MIN-001; 3/28/2012
[D111]	Validation Analysis Report	6/13/2012
[D111a]	ROS Safety Validation Testing Checklist	n/a; 9/7/2011
[D112]	Humidity Test results	HSTP 31; 5/8/2012
[D113]	HALT Vibration/Temperature test results	HSTP 35; 5/8/2012
[D114]	Surge Withstand Capability test results	HSTP 29; 6/6/2012
[D115]	Vibration test results	HSTP 32; 5/8/2012
[D116]	ESD test results	HSTP 27; 6/6/2012
[D119]	exida Validation Test Execution Phase Checklist	n/a; 8/6/2012
[D12]	EDP 400-502 Peer Safety Review	A; 3/25/2010
[D120]	HW FIT witness	7/26/2012
[D121]	SW test witness	7/27/2012
[D13]	Training and Competency Matrix	n/a; 7/12/2012
[D14]	Safety Instrumented Systems Training Program	1/23/2012
[D15]	Action Item List	n/a; 5/14/2012
[D150]	exida Functional Safety Assessment Phase Verification Checklist	n/a; 9/4/2012
[D151]	Functional Safety Assessment Plan	V1R1; 7/27/2012
[D152]	Link Software Modules to Unit Tests: 644_NextGen	NA; 8/16/2012
[D153]	Link Software Modules and Code Reviews: 644 Next_Gen	NA; 8/17/2012
[D154]	CMX-Tiny+ RTOS Upgrade Discussion	NA; 8/20/2012
[D155]	CMX 2.00 Code Review Results	NA; 6/12/2012
[D156]	644_NextGen_Trace_Matrix_SIRS_Procedure	NA; 8/20/2012
[D157]	UnitTest_Health.c	NA; 8/30/2012
[D158]	Measure Block Unit Test Result	NA; 12/20/2011
[D159]	644 SIS / Analog Output Unit Test Results	NA; 12/16/2012
[D16]	DOP 7 Rosemount Product Development Process	B; 4/1/2011
[D160]	Product Safety Manual	MA; 7/30/2012
[D161a]	WA0007 Safety Manual Checklist	H; 7/12/2012
[D165]	Failure Modes, Effects and Diagnostics Analysis (FMEDA) Report	V1R1; 5/15/2012
[D166]	exida FMEDA Document Checklist	n/a; 7/20/2012
[D167]	Product Approvals	n/a; 10/27/2011
[D168]	Product Release - Final Design Review, SW	n/a; 5/9/2012

[D169]	Product Release - Final Design Review, HW	n/a; 2/23/2012
[D16a]	RMD_G7.3-0001 Product Realization: Project Management Process	A; 7/1/2011
[D16b]	Management Review	8/18/2011
[D17]	DOP 415 Product Design and Development Process	I; 10/13/2011
[D170]	Unit Test Checklist - TimeStamps	NA; 8/30/2012
[D171]	Unit Test Checklist - TCDiag	NA; 8/31/2012
[D172]	Unit Test Checklist - FourWireS2	NA; 8/31/2012
[D173]	xCode Complexity Analysis	0.1; 8/30/2012
[D174]	Justification for No Maximum Module Size	0.2; 8/31/2012
[D17a]	DOP416 SIS Product Design and Development Process	I; 2/1/2012
[D18]	DOP 440 Engineering Change Procedure	AK; 2/1/2011
[D180]	Impact Analysis Template	n/a; 2/9/2012
[D181]	Impact Analysis Example - SW	6/20/2012
[D182]	HW design change review - ClearQuest:PRD00057739	6/6/2012
[D183]	HW design change review - ECO:RTC1053188	4/9/2012
[D184]	Impact Analysis Example - HW	4/26/2012
[D189]	exida Modification Phase Verification Checklist	5/31/2012
[D19]	DOP 1110 Metrology Procedure	AA; 1/15/2010
[D19a]	Test Equipment List	n/a; 6/5/2012
[D20]	ISO 9001:2008 Certificate	n/a; 10/7/2011
[D200]	exida Safety Manual Checklist	NA; 8/8/2012
[D21]	DOP 1440: Customer Notification Process	P; 1/19/2010
[D22]	DP-50111-16 Field Return Analysis Report Procedure	A; 2/2/2010
[D22a]	Failure Analysis Procedure	E; 8/12/2011
[D23]	3144 safety coding standard, C/C++	1.2; 7/31/2010
[D23a]	3144 project coding standard	A.1; 9/13/2010
[D24]	EDP 400-300 Configuration and Change Control Management	C; 5/1/2005
[D24a]	644 Configuration Management Plan	A.2; 5/27/2011
[D25]	EDP 400-500 Peer Review	C; 7/1/2011
[D26]	DOP 660 Supplier Corrective Action	U; 11/10/2010
[D27]	Corrective And Preventive Action website	n/a; n/a
[D27a]	Corrective And Preventive Action Procedure DOP 8.5	AB; 5/10/2011
[D28]	DOP 1710 Internal Audit Program	W; 1/25/2010
[D28a]	Internal PPQA Quality Audit example	5/25/2012

[D29]	EDP400-600 Quality_Assurance_Procedure	D; 6/22/2007
[D29a]	DOP1610- Control of Design Records	R; 1/19/2010
[D30]	Safety Integrity Requirements Specification	A.8; 6/6/2012
[D31]	exida SRS Document Checklist	7/31/2012
[D32]	SIRS Review	0.1; 1/3/2011
[D32a]	SIRS Consolidated Log Review	12/15/2010
[D33]	Customer Requirements Document	A.9; 12/20/2010
[D33a]	CRD Review example	A.8; 12/7/2010
[D34]	Electrical Requirements Spec	A.4; 6/28/2012
[D35]	Validation Test Plan	A.2; 9/15/2011
[D36]	exida Safety Validation Test Plan Checklist	8/2/2012
[D37]	Safety Validation Plan Review	A.1; 9/7/2011
[D39]	SRD-SRS-SIRS Traceability	7/12/2012
[D40]	Architecture Design Description Document	1.1; 7/2/2012
[D40a]	Architecture design review	1.0; 6/29/2012
[D40b]	System Requirements	B.5; 6/6/2012
[D42]	exida Integration Test Plan Checklist	8/2/2012
[D43b]	Derived Requirements Document - SW	A.10; 6/6/2012
[D44]	exida Derived Requirements Document Checklist	8/3/2012
[D47]	Proven In Use Analysis Report for 3144P	V1R2.0, 2/25/2004
[D49]	exida System Architecture Phase Verification Checklist	n/a; 8/9/2012
[D50]	Detailed Design Description - Theory of Operation	0.1; 5/1/2012
[D52a]	ASIC Evaluation and Determination	n/a; 11/3/2011
[D53]	Fault Injection Test Plan/Results	3/27/2012
[D53a]	FIT support details	4/11/2012
[D54]	exida HW Fault Injection Test Verification Checklist	n/a; 8/3/2012
[D55]	Schematics - 00644-7100	AC; 3/12/2012
[D56]	BOM - 00644-7102	AD;
[D57]	HW Component Derating analysis	AB; 12/13/2011
[D58]	HW Design Traceability	4/24/2012
[D60]	HW Design Guidelines for Test and Manufacture	A;
[D61]	HW Requirements Review	A.4; 6/29/2012
[D63]	HW System Test Plan	A.2;
[D63a]	HW Test Plan with test procedure example	1/12/2012

[D64]	HW Test Plan Review	A1; 4/19/2012
[D68]	exida Hardware Design Implementation Verification Checklist	N/a; 8/3/2012
[D69]	Hardware Design Phase Verification Checklist	WA0007-E;
[D71]	Detailed Software Design Specification	0.4; 5/18/2012
[D72]	exida Software Architecture and Design Checklist	NA; 8/6/2012
[D73]	SIRS-SW Design Traceability	5/4/2012
[D74]	644 NG SIS Diagnostics Design	NA; 10/27/2011
[D78]	SW Architecture Design Review	.03; 5/18/2012
[D80a]	IEC 61508 SIL3 Tables for 644 Temperature Transmitter	8/3/2012
[D81]	WA0007 SIS Checklists- blank	H; 11/23/2011
[D82]	Software Tools Analysis	A.2; 8/15/2012
[D83]	PIU Assessment; IAR Compiler for Atmel AVR microprocessors	2/11/2007
[D84]	PIU Assessment: Citadel ASIC Field History	up to FY12-8;
[D90]	PC Lint Configuration file	n/a; 5/14/2012
[D90a]	PC Lint resolution example	n/a; 6/6/2012
[D90b]	Code Review example	5/25/2012
[D90c]	PC Lint Results	6/26/2012
[D91]	Unit Test - HW test plan	02; 7/16/2012
[D91a]	HW unit test results	1.0, 7/2/2012
[D92]	Unit Test - SW test plan	A.1; 7/18/2011
[D92a]	SW unit test results	n/a; 4/17/2012
[D92d]	Test Techniques to use to develop test plans	n/a;
[D97]	Software System Test Plan	A.3; 6/8/2012
[D97a]	SW Test Results Example 1	7/5/2012
[D97b]	SW Test Results Example 2	6/29/2012
[D99]	exida SW Implementation Phase Verification Checklist	n/a; 8/6/2012
[D99a]	Action Items	n/a; 5/14/2012

2.4.2 Documentation generated by *exida certification*

[R1]	Rosemount Temperature Transmitter 644	Detailed safety case documenting results of assessment (internal document)
[R2]	ROS 12-04-020 R002, Assessment, V1R1	IEC 61508 Functional Safety Assessment, 644 4-20mA / HART Temperature Transmitter (this report)

3 Product Description

This report documents the results of the Functional Safety Assessment performed for the 644 Temperature Transmitter with Hardware version 1 and Device Label SW REV 1.1.X. The 644 Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The transmitter can be equipped with or without display.

The 644 Temperature Transmitter is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0. Combined with one or two temperature sensing elements, the 644 transmitter becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 644 Temperature Transmitter are:

- 2-, 3-, and 4-wire RTD
- Thermocouple
- Millivolt input (–10 to 100mV)
- 2-, 3-, and 4-wire Ohm input (0 to 2000Ω)

[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 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 644 Temperature Transmitter 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 with a Hardware Fault Tolerance of 1.

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 certification 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 644 Temperature Transmitter was done using this development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Rosemount, Inc. has an IEC 61508 compliant development process as defined in [D17]. The process defines a safety lifecycle which meets the requirements for a safety lifecycle as documented in IEC 61508. Throughout all phases of this lifecycle, fault avoidance measures are included. Such measures include design reviews, FMEDA, code reviews, unit testing, integration testing, fault injection testing, etc.

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the 644 Temperature 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 Emerson Process Management Safety Instrumented Systems Product development is governed by [D17]. This process requires that Emerson Process Management create a project plan [D07] which is specific for each development project. The Project Plan defines all of the tasks that must be done to ensure functional safety as well as the person(s) responsible for each task. These processes and the procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management.

Version Control

All documents are under version control as required by [D24a].

Training, Competency recording

Competency is ensured by the creation of a competency and training matrix for the project [D13]. The matrix lists all of those on the project who are working on any of the phases of the safety lifecycle. Specific competencies for each person are listed on the matrix which is reviewed by the project manager. Any deficiencies are then addressed by updating the matrix with required training for the project.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D17] a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. For the 644 Temperature Transmitter, the requirements specification [D30] contains a system overview, safety assumptions, and safety requirements sections. During the assessment, *exida certification* 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 which are included in the following documents: [D30], [D35], [D39], [D58], [D73], and [D156]. The system requirements are broken down into derived hardware and software requirements which include specific safety requirements. Traceability matrices show how the system safety requirements map to the hardware and software requirements, to hardware and software architecture, to software and hardware detailed design, and to validation tests.

Requirements from **IEC 61508-2, Table B.1** that have been met by Rosemount, Inc. include project management, documentation, structured specification, inspection of the specification, and checklists.

Requirements from **IEC 61508-3, Table A.1** that have been met by Rosemount, Inc. include Forward Traceability between the system safety requirements and the software safety requirements, and Backward traceability between the safety requirements and the perceived safety needs.

[D80a] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D17]. The hardware design process includes creating a hardware architecture specification, a peer review of this specification, creating a detailed design, a peer review of the detailed design, component selection, detailed drawings and schematics, a Failure Modes, Effects and Diagnostic Analysis (FMEDA), electrical unit testing, fault injection testing, and hardware verification tests.

Requirements from **IEC 61508-2, Table B.2** that have been met by Rosemount, Inc. include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, checklists, semi-formal methods, computer aided design tools, and inspection of the specification. This is also documented in [D80a]. This meets the requirements of SIL 3.

5.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D17]. The software design process includes software architecture design and peer review, detailed design and peer review, critical code reviews, static source code analysis and unit test.

Requirements from **IEC 61508-3, Table A.2** that have been met by Rosemount, Inc. include fault detection, error detecting codes, failure assertion programming, diverse monitor techniques, retry fault recovery mechanisms, graceful degradation, modular approach, use of trusted/verified software elements, forward and backward traceability between the software safety requirements specification and software architecture, semi-formal methods, computer-aided specification and design tools, cyclic behavior, with guaranteed maximum cycle time, time-triggered architecture, and static resource allocation.

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

Requirements from **IEC 61508-3, Table A.4** that have been met by Rosemount, Inc. include semi-formal methods, computer aided design tools, defensive programming, modular approach, design and coding standards, structured programming, use of trusted/verified software modules and components, and forward traceability between the software safety requirements specification and software design,

This is also documented in [D80a]. This meets the requirements of SIL 3.

5.1.5 Validation

Validation Testing is done via a set of documented tests. The validation tests are traceable to the Safety Requirements Specification [D30] in the validation test plan [D35]. The traceability matrices show that all safety requirements have been validated by one or more tests. In addition to standard Test Specification Documents, third party testing is included as part of the validation testing. All non-conformities are documented in a change request and procedures are in place for corrective actions to be taken when tests fail as documented in [D17].

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, black-box testing, “worst-case” testing, and field experience.

Requirements from IEC **61508-3, Table A.7** that have been met by Rosemount, Inc. include process simulation, modeling, functional and black box testing, and forward and backward traceability between the software safety requirements specification and the software safety validation plan.

[D80a] 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 [D17]. Verification activities include the following: Fault Injection Testing, static source code analysis, module testing, integration testing, FMEDA, peer reviews and both hardware and software unit testing. In addition, safety verification checklists are filled out for each phase of the safety lifecycle. This meets the requirements of IEC 61508 SIL 3.

Requirements from IEC **61508-2, Table B.3** that have been met by Rosemount, Inc. include functional testing, project management, documentation, black-box testing, and field experience.

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, test management and automation tools, and forward traceability between the software design specification and module and integration test specifications.

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, and forward and backward traceability between the software design specification and the software verification plan.

[D80a] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

5.1.7 Modifications

Modifications are done per the Emerson Process Management's change management process as documented in [D24]. 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 [D17] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D21]. 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). This meets the requirements of SIL 3.

5.1.8 User documentation

Rosemount, Inc. created a safety manual for the 644 Temperature Transmitter [D160] which addresses all relevant operation and maintenance requirements from IEC 61508. This safety manual was assessed by *exida certification*. 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.

[D80a] 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 644 Temperature Transmitter Failure Modes, Effects, and Diagnostic Analysis was performed by exida. This is documented in [D165].

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.

From the FMEDA failure rates are derived for each important failure category. Table 1 lists these failure rates as reported in the FMEDA report for a 644 Temperature Transmitter with a single RTD. Note that these failure rates change based on how the 644 has been configured including the type of sensor that has been connected to it. For complete details on how to calculate these numbers for different configurations, see the FMEDA report [D165]. The failure rates are valid for the useful life of the devices. Based on Emerson endurance test data and general field failure data a useful life period of approximately 50 years is expected for the 644 Temperature Transmitter. This is listed in the FMEDA report.

Table 1 Failure rates according to IEC 61508 – 644 with single RTD (Failure Rates in FITS; 1 FIT = 1 Failure per 10^9 hours)

Failure Categories	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
Low trip	330 FIT	0 FIT	31 FIT	36 FIT	90.9%
High trip	31 FIT	0 FIT	330 FIT	36 FIT	90.9%

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 644 Temperature Transmitter with single 4-wire RTD. The failure rate data used in this calculation is displayed in section **Error! Reference source not found.**. It is assumed that the transmitter output is send low upon detection of failure and the safety function has a low trip point.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} value for a single 644 Temperature Transmitter with single 4-wire RTD, with a proof test interval of 1 year equals 2.17E-04.

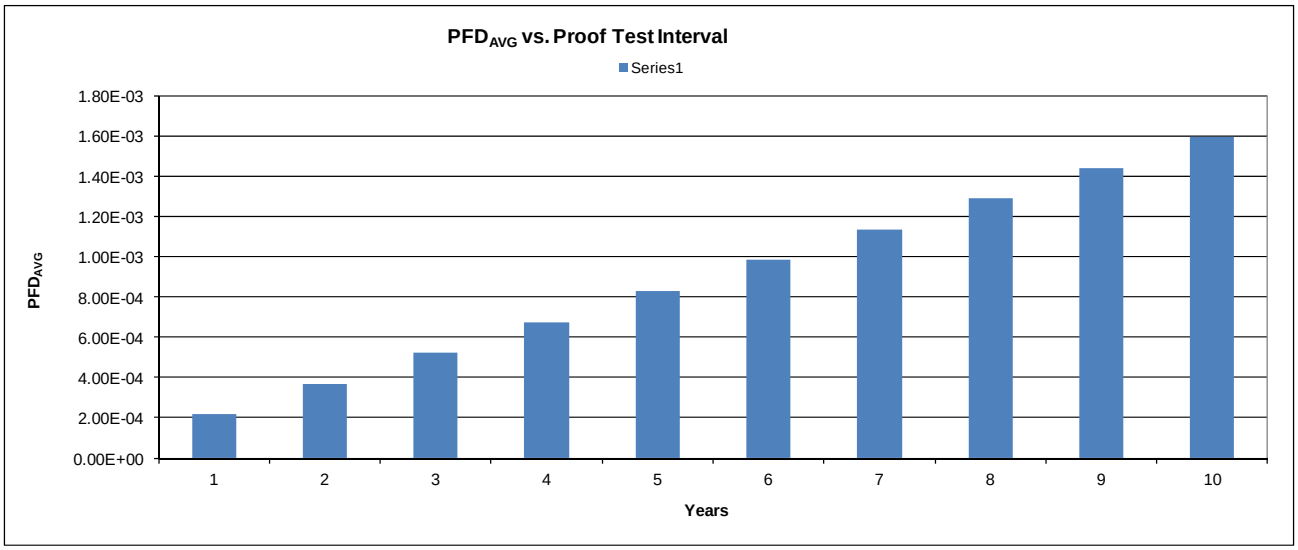


Figure 1: PFD_{AVG} 644 Temperature Transmitter with single RTD

For SIL 2 applications, the PFD_{AVG} value for the safety function needs to be < 10^{-2}. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval of the 644 Temperature Transmitter with single 4-wire RTD is equal to 2.2% of the range. These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

The analysis shows that design of the 644 Temperature Transmitter meets the hardware requirements of IEC 61508, SIL 2 @HFT=0 and SIL 3 @ HFT=1.

5.3 Recommendations for improvement

During the course of the assessment, there were a number of cases found where there was either a minor non-conformance or a recommended update to the development process identified. In all of these cases the issues identified were deemed not to have a significant effect on the overall functional safety of the product. Therefore, these items can be considered recommendations to reduce the risk of non-compliance for future development efforts or modifications. The items found are described below:

- Test environment, tools, configuration and programs used should be included in future integration test plans
- The integration plan shall consider details of those who shall carry out the integration. This information could also be included in another document such as the roles and responsibilities document.
- Coding standard or other document should state that interrupts should only be used if they simplify the design.

- Recommend adding to source code standard the following: Complex calculations are avoided as the basis of branching and loop decisions.
- The analysis made and the decisions taken on whether to continue the integration test or issue a change request, in the case when discrepancies occur should be documented in the integration test results.
- The design specification should document the control flow triggering of the product. This means that the control flow of the product at a high level should be defined including a definition of different tasks or interrupts that will occur along with a description on how those tasks or interrupts will be triggered and what major functions will be executed in each task or interrupt.
- Create a list of all modules along with a link to their unit test results or explanation as to why no module test is needed. This will make it easier to confirm that all applicable modules have been unit tested.
- For SIL 3, when software is changed all functional tests should be re-run. This is highly recommended meaning that written justification is required if only a subset of tests will be re-run. The development process should be updated to indicate that this should be done.
- Software Complexity metrics are calculated, but not analyzed. The development process should be updated to state that modules with complexities above a certain level must be justified. This justification was done for this release, but should be made part of the process so that the justification is done sooner.
- Update process to ensure that unit test checklists are filled out for all unit tests.
- Module tests often show coverage less than 100%. This code has been identified as non-safety critical, so 100% coverage not required. However in order to ensure that all safety critical code is covered, an explanation should be documented whenever 100% coverage is not achieved.

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 ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
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 A (sub)system	"Non-Complex" (sub)system (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B (sub)system	"Complex" (sub)system (using micro controllers or programmable logic); for details see 7.4.3.1.3 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

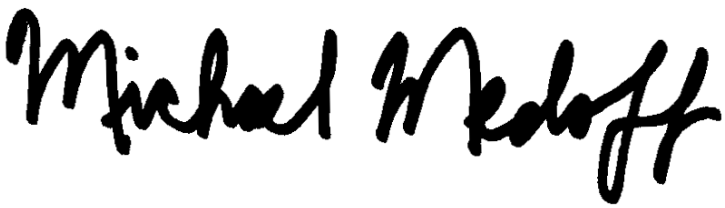
Version:	V1	
Revision:	R1	
Version History:	V1, R1:	Updated based on review comments
	V0, R1:	Draft; September 4, 2012
Authors:	Michael Medoff	
Review:	V0, R1: John Yozallinas	
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

John Yozallinas, Evaluating Assessor



Michael Medoff, Certifying Assessor