Results of the IEC 61508 Functional Safety Assessment

Project:
248 Temperature Transmitter

Customer:
Emerson Rosemount
Shakopee, MN
USA

Contract No.: Q16/12-041
Report No.: ROS 16-12-041 R002
Version V1, Revision R0, 5/19/2019
Dave Butler

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management Summary

The Functional Safety Assessment of the Emerson Rosemount 248 Temperature Transmitter development project, performed by *exida,* consisted of the following activities:

- *exida* assessed the development process used by Emerson Rosemount through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed the manufacturing quality system in use at Emerson Rosemount.

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. Hardware and Software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were 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 Emerson Rosemount 248 Temperature Transmitter 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 248 Temperature Transmitter can be used in a low demand safety related system in a manner where the $\mathrm{PFD}_{\mathrm{AVG}}$ is within the allowed range for SIL 3 (HFT = 0) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the 248 Temperature Transmitter meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the 248 Temperature Transmitter is capable for use in SIL 3 applications in Low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.

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

CERTIFIED
IEC 61508
SIL 3 CAPABLE
exida
FS

Table of Contents

1 Purpose and Scope

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

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

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

- the 248 Temperature Transmitter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

  and

- the 248 Temperature Transmitter development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

  and

- the 248 Temperature Transmitter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

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

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 out using the exida Safety Case tool. The Safety Case tool embodies the accredited IEC 61508 exida scheme. It provides a means to identify the IEC 61508 requirements relevant to an assessment and, for each relevant requirement, to document a compliance argument and the evidence (manufacturer documentation) on which the argument is based.

Using this method helps to ensure a complete and consistent method to assessment of products. When the assessor judges that the requirements have been met, the tool summarizes the approach taken and the results of the assessment within an assessment report.

The assessment was planned by *exida* and agreed with Emerson Rosemount (see [R2]).

All assessment steps were continuously documented by *exida* (see [R1])

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

Emerson Rosemount	Manufacturer of the 248 Temperature Transmitter
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

Emerson Rosemount contracted *exida* with the IEC 61508 Functional Safety Assessment of the above-mentioned devices.

2.3 Standards / Literature used

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

Doc. ID	Standard	Title
[N1]	IEC 61508:2010 Parts 1 – 7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Emerson Rosemount

Doc. ID	Project Document Filename	Version	Date
D001	Rosemount Inc. Quality Manual.docx	Rev. 7.0	8/16/2017
D003	Product Design And Development Process.docx	Rev. 8.0	--
D004	Configuration and Change Management Work Instruction.docx	Rev. 7.0	
D005	RMT Failure Analysis Process_02.docx	Rev. 3.0	
D006	Failure Analysis Process Description.docx	Rev. 5.0	
D007	Supplier Quality Manual.doc	Rev. 7.0	10/5/2017
D007b	Supply Chain Supplier Corrective Action Process Description.docx	Rev. 4.0	
D010b	Document and Record Control Process Description.docx	Rev. 3.0	
D012	Corrective Action Preventive Action Process Description.docx	Rev. 4.0	

Doc. ID	Project Document Filename	Version	Date
D016	Peer Review Work Instruction.docx	Rev. 6.0	
D019	Customer Notification Process Description.docx	Rev. 5.0	
D026	2044_Project Plan.docx	Rev. B.2	4/17/2017
D0023	Engineering Change Order (ECO) Process.docx	Rev. 4.0	
D026b	248NG_Project Workbook_Rev-8.0.xlsm	Rev. 8.0	
D027	2044_CMP.doc	Rev. A.5	8/13/2018
D029	2044 Safety-related Systems Verification Checklists.docx		
D034	2044_Training_Competency_Safety.xlsx		12/5/2016
D036	iso-9001-certificate-rosemount-shakopee-chanhassen-eden-prairie-usa-en-79472.pdf	10/7/2017	Exp. 10/7/2020
D040	2044_SIRS.docx	Rev. B	12/11/2015
D040b	2044_SRD.docx	Rev. A	9/1/2015
D041	2044_SIRS_rev0.3 Consolidated Log.xlsm	Rev. 3	6/15/2018
D043	2044_SRS.doc	Rev. A	2/5/2018
D043b	2044_SIS.eap	Snapshot	
D049b	index.htm	Model	4/24/2019
D049c	avenger_init_readback.pdf		11/24/2016
D051	D051_Detailed Software Design Specification	Many	
D051b	248NG - Safety Critical Float Analysis.xlsx		3/28/2019
D053	248NG_FDR.pptx		7/16/2018
D053b	FDRAttendees_Actions.xlsx		7/1/2018
D053e	D053_Design Review Record	Many	
D056	2044_TraceabilityMatrix.xlsm	Rev. 0.13	11/15/2018
D056b	FW Traceability.msg	Screenshot	11/9/2018
D057	Sxx-yy_ut.txt		4/16/2019
D057b	Test result and justification.pptx		4/23/2019
D058	collaborator.png	Screenshot	
D058b	collaborator2.png	Screenshot	
D059	Rosemount 248NG Fault_Injection_Test 20170512.xls		5/12/2017
D059b	Rosemount 248NG Fault_Injection_Test 20170727.xlsx		7/27/2017
D060	3144P_H7D_safety_coding_standard.html	Rev. 1.2	7/31/2010
D060b	3144P_H7D_project_coding_standard.html	Rev. A.1	9/13/2010
D061	au-exida.lnt	v1.0	11/30/2001
D062	lint.out		9/20/2018
D064	2044_STO.doc	A.5	3/15/2018

Doc. ID	Project Document Filename	Version	Date
D065	2044_STO_rev_0.2_Peer_Review_Inspection_Report_and_Consolidated_Log_Form.xlsm		1/18/2016
D066	2044_248NG_Tracking.xlsm	Sprint 11	
D067	2044_SWTP.doc	A.6	7/17/2018
D067c	2044_AO_4-20mA.docx	0.3	9/7/2018
D069	2044_MTP.docx	Rev. A	6/23/2016
D069b	2044_SVTP.docx	Rev. A.1	9/17/2018
D070	2044_SVTP Consolidated Log.xlsm	Rev. 0.1	1/14/2016
D071	2044_HWTP.xlsx	Rev. B.1	
D074	D074_Validation Test Results	Many	
D075	D075_Environmental Test Results	Many	
D076	D076_EMC Test Results	Many	
D077c	D077_Fault Injection Test Results	Many	
D079	R-00809-0100-4825.pdf	Rev. DA	5/1/2019
D081	RTC1052396.pdf		7/22/2016
D081b	02051-3503_SIA.xls		7/22/2016
D081c	644NG_HW_Safety_SIA.xls		7/22/2016
D082	Diagnostic.docx	< sprint 6	
D086	248_NextGen_SW_tools_analysis.docx	rev 0.1	9/21/2017
D086b	D086_Tool Qualification Report	many	
D087	MD5s.xlsx		10/29/2018
D088	ImpactAnalysisA.png	Screenshot	
D088b	ImpactAnalysisB.png	Screenshot	
D088c	ImpactAnalysisC.png	Screenshot	

2.4.2 Documentation generated by *exida*

Doc. ID	exida Document Filename	Description
[R1]	ROS 16-12-041 SC001 V1R1 IEC 61508 248 Xmitter.xlsm	Safety Case
[R2]	ROS 14-12-011 248 Temp Transmitter Certification Proposal R3.pdf	Assessment Plan
[R3]	ROS 16-12-041 R001 V2R1 FMEDA 248.pdf	FMEDA Report

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed with Emerson Rosemount.

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

- FSM planning, including
    - Safety Life Cycle definition
    - Scope of the FSM activities
    - Documentation
    - Activities and Responsibilities (Training and competence)
    - Configuration management
    - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
    - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation

The certification audit was done in Shakopee, MN on 10/24/018.

3 Product Description

The 248 Temperature Transmitter is a two-wire, smart device. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. The transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either low or high upon internal detection of a failure (the output state is programmable).

The 248 transmitter is intended for use as a temperature measurement component in an instrumented system. Figure 1 depicts how it is typically used in a system. Table 1 identifies and describes the external interfaces.

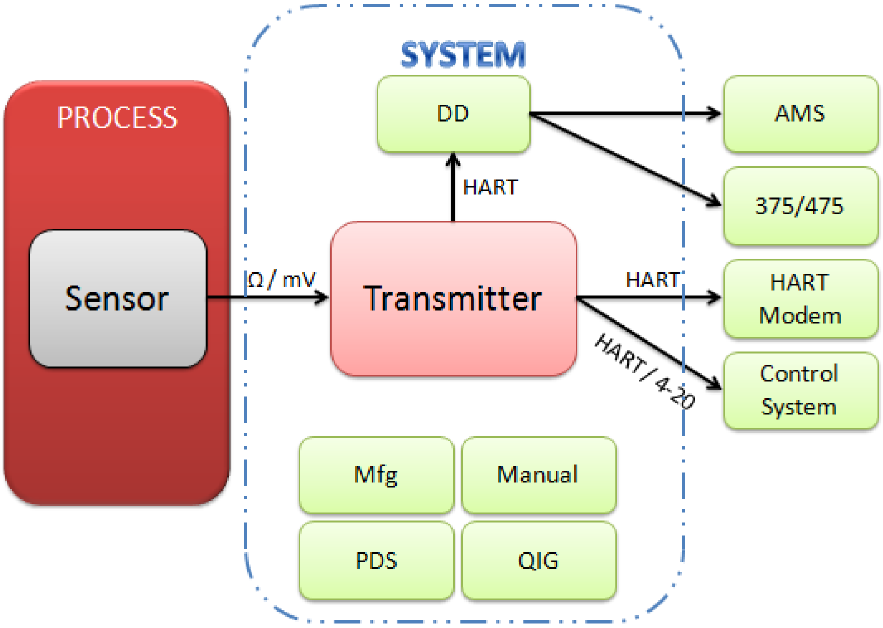

Figure 1 – System block diagram

Interface	Description
4-20	4-20 mA output used to deliver primary variable measurement and alarm/saturation signal.
HART	Digital communication interface used to configure, control, diagnose and monitor the transmitter. Can also be used to transfer measured or derived variable information to a control system.
Ω	Sensor interface in which resistance of sensor is used to transmit information about process temperature (e.g., RTD)
mV	Sensor interface in which voltage, generated by sensor is used to transmit information about process temperature

Table 1 – System Interfaces

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of 248 Temperature Transmitter:

Model	Hardware Version	Software Version
248HA…QT… 248HA…QT…BR5 248HA…QT…BR6	1.0.1	1.0.2

Table 2- Hardware and Software Versions

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Emerson Rosemount for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1]. All relevant objectives of the standard have been met by the Emerson Rosemount development processes during this development project.

exida audited and assessed project and product documentation for compliance with the functional safety requirements of IEC 61508. During an evaluation period, an assessor updated a safety case with the results of the assessment. The safety case documents the development project's compliance with the functional safety management requirements of IEC 61508, parts 1 through 3. Evaluation was followed by a certification review of the safety case, in which a review of a subset of the most important requirements, and a spot inspection of the remaining requirements, was carried out to ensure high quality of the safety case.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Emerson Rosemount 248 Temperature Transmitter, with IEC 61508.

The assessment executed using the exida certification scheme, tailors the IEC 61508 requirements to the scope of the development activities and the development team.

The results of the assessment show that the 248 Temperature Transmitter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements and constraints specified in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Emerson Rosemount may make modifications to this product as needed.

As part of the *exida* scheme a surveillance audit is conducted prior to renewal of the certificate. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made with respect to the modifications made.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which documents, 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 Emerson Rosemount 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 248 Temperature Transmitter 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

Emerson Rosemount has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D01].

This functional safety assessment evaluated the compliance, of the processes, procedures and techniques as implemented for the product development, with the requirements of IEC 61508. 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 Safety Lifecycle and FSM Planning

The functional safety management plan defines the safety lifecycle for this project. This includes a definition of the safety activities and documents to be created for this project. This information is communicated via these documents to the entire development team so that everyone understands the safety plan.

Manufacturer has a QMS in place. The Manufacturer has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure.

The Software Development Procedure identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase.

All phases of the safety lifecycle have verification steps described in the FSM plan or a separate verification plan for one or more phases. This plan includes criteria, techniques and tools used in the activities. The verification is carried out against this plan.

Reported dangerous failures that occur in the field are captured and analyzed and recommendations are made to minimize the chance for a repeat occurrence of the failure.

The software development procedure states that if a modification is required pertaining to an earlier lifecycle phase, then an impact analysis shall determine:

(1) which software modules are impacted and

(2) which earlier safety lifecycle activities shall be repeated.

Lifecycle Phase Verification results are documented according to the verification plan and available for assessment.

5.1.2 Documentation

There is a document management system in place. This system controls how all safety relevant documents are changed, reviewed and approved.

All safety related documents are required to meet the following requirements:

- Have titles or names indicating scope of the contents
- Contain a table of contents
- Have a revision index which lists versions of the document along with a description of what changed in that version
- Documents must be searchable electronically

Several documents were sampled and found to meet these requirements.

5.1.3 Training and competence recording

The FSM Plan lists the key people working on the project along with their roles.

A competency matrix has been created and includes the following:

- Competency requirements for each role on project.
- List of people who fulfill each role
- List of competencies for each individual matched up to required competencies based on roles that they fill.
- Training planned to fill any competency gaps.

5.1.4 Configuration Management

The configuration of the product to be certified is documented including all hardware and software versions that make up the product. For software this includes source code.

Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

5.1.5 Tools (and languages)

All tools which support a phase of the software development lifecycle and cannot directly influence the safety-related system during its run time. Tools are documented, including tool name, manufacturer name, version number, use of the tool on this project. This includes test tools.

All off-line tools have been classified as either T3 (safety critical), T2 (safety-related), or T1 (interference free).

All off-line support tools in classes T2 and T3 have a specification or product manual which clearly defines the behavior of the tool and any instructions or constraints on its use.

An assessment has been carried out for T2 and T3 offline support tools, to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms are identified, appropriate mitigation measures have been taken.

For each tool in class T3, if tool validation was performed, the results of the validation were documented.

The 'C++' programming language is used. As shown in table C.1 of IEC 61508-7, the 'C++' programming language when used with a defined language subset, a coding standard, and static analysis tools is highly recommended for all SILs. For this project there is a coding standard which defines a language subset and static analysis tools (PC LINT) are used to detect potential problems in the source code. Therefore, 'C++' can be considered a suitable programming language for this development project.

5.2 Safety Requirement Specification

All element safety functions necessary to achieve the required functional safety are specified, including, as appropriate:

- functions that enable the EUC to achieve or maintain a safe state
- functions related to the detection, annunciation and management of sensor and actuator faults
- safety accuracy and stability for measurement and control

Software safety requirements have been created as derived/allocated requirements (from Safety Requirements). These requirements have been made available to the software developers and have been reviewed by software developers. The results of the review are documented, and all action items are tracked through resolution.

The safety requirements have been reviewed to verify that they have enough detail such that the required SIL can be achieved during design and implementation and can be assessed.

Safety requirements content is available and sufficient for the duties to be performed. This has been confirmed by the validation testing and assessment.

All system, operator and software interfaces necessary to achieve the required functional safety are specified.

All safety related constraints between the software and hardware have been documented in the Software Safety Requirements or other suitable requirements document.

5.3 Change and modification management

Modifications are initiated with an Engineering Design Change procedure [D023]. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process.

A Modification Procedure requires that an Impact Analysis be performed to assess the impact of the modification, including the impact of changes to the software design and to the Functional Safety of the system. The results of an Impact Analysis are documented.

Modification Request/Records document the reason for the change and have a detailed description of the proposed change.

The impact analysis documents which tests must be run to verify and validate the change and which tests must be re-run to validate that the change did not affect other functionality.

The Software Modification Procedure requires that the changed and affected software modules are reverified after the change has been made.

5.4 Product/Software Architecture Design

The product's architecture design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented.

All components have the same SIL as the target SIL of the safety function.

The System Architecture Design describes that the behavior of the device when a fault is detected is to annunciate the detected fault through an external interface.

The System Architecture Design clearly identifies that communication interfaces are not safety related.

The System Architecture Design identifies design features (such as Proof Test) that support maintainability and testability. This shows that these qualities have been considered during design and development and have been verified at review time.

All software components listed in the Software Architecture Design have corresponding Software Designs which further partition the design into software modules. The design has a focus on simplicity.

The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified.

Formal design reviews are held and the results recorded; action items are identified, assigned, and resolved.

The System Architecture requires the use of a password to access the dedicated configuration tool to make changes.

A database of previously used (well-tried) components is kept. When creating new designs, engineers are encouraged to use previously used components and must provide written justification when they cannot. Any components that are found to have relatively high failure rates are removed from the component database.

Computer Aided Design Tools are used to document the system architecture.

The hardware architecture design has been reviewed.

5.5 Hardware Design and Verification

Hardware Components used on previous projects are given priority over new components. This is implemented by having a component database, and a procedure which states that approval must be given to use any hardware component not already in the component database.

A FMEDA analyst has reviewed the design and determined that there are measures against physical environment stresses.

Hardware architecture design has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews are used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are incorporated into the design.

The FSM Plan and development process and guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

5.5.1 Hardware Design / Probabilistic properties

To evaluate the hardware design of the 248 Temperature Transmitter, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R3]. Assumptions made in the FMEDA were verified using Fault Injection Testing as part of the development (see the Fault Injection Test Plan [D77c]) 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.

From the FMEDA failure rates are derived for each important failure category.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) 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.

5.6 Software Design

The Software Architecture Design contains a description of the software architecture. The design is partitioned into new, existing and/or proprietary (third party) components and modules, which are identified as such.

All components are considered safety critical at the highest SIL as defined in the safety requirements specification for the product.

The Software Design uses modeling to express the design in terms of:

- functionality
- information flow between elements
- sequencing and time relationships
- timing constraints
- data structures
- structural views
- behavioral views

The Software Architecture Design uses the following diagram types:

- State Charts / State Transition Diagrams
- Sequence Diagrams
- Data Flow Diagrams
- Decision / Truth Tables

The Software Design is well understood by the developers and is documented in a way that can be easily verified.

The Software Architecture Design specifies that, for example, the following runtime conditions are periodically executed to detect software faults:

- safety critical data integrity check
- readback of DAC
- sensor open
- sensor short

The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified.

The Software Design describes an acceptable memory allocation strategy.

No criticality analysis is necessary as all modules are developed to SIL 3 requirements.

5.7 Software Verification

The Software Architecture Design was reviewed and confirms that the architecture fulfills the safety requirements and that the notation used is unambiguous. All action items required to be addressed, were recorded in an action item tracking system and have been resolved.

Modular approach; A modular approach has been used in the software design. Design has been broken up into classes and methods which are modular, and subprograms have a single entry and a single exit.

100% structural test coverage of entry points, statements and branches is documented by a tool or a manual trace or is justified in writing if coverage is impractical.

Module Test Results for all safety related modules were produced and documented per the Module Test Verification Plan/Specification; Sample results files were reviewed; unit tests are automated or manual; verification of data is included in tests; result files show the pass/fail output line.

Static Analysis was performed on all source code to enforce many of the rules in the coding standard. Rules not covered by the static analysis tool were enforced by code reviews.

All Integration Test Cases have been successfully run, per the Integration Test Plan and Integration Test Results have been documented.

For each test, the Integration Test Results Record identifies the Test Case, its version, the version of the product being tested, the tools; and the equipment used, along with their calibration data. In addition, the Integration Test Results Record references the Integration Test Plan including version number.

Test management tools are used to manage the module and/or integration testing process.

All safety critical floating-point calculations are verified off-line using sample data and compared to the on-line values computed for the same sample data.

The source code standard states that software modules interact with each other through their interfaces which are fully specified and documented, including all class members, member names member types, operation names, parameters and parameter types, and evidence is available that this was followed.

Module test results show that boundary value analysis was used to determine test cases. These test cases are applied to the interface of the module. Unit Test Checklist in Unit Test Plan states that this should be done. A quick view of several module tests showed that this appeared to be done.

Module test results show that input partitioning and equivalence classes were used to determine test cases.

The Integration Test Plan was reviewed and found to be adequate regarding its coverage of the Software Safety Requirements, the Software Architecture Design, the Software System Design, the types of tests to be performed and the procedures to be followed. All action items have been resolved or deferred.

The Integration Test Plan calls for black-box testing of all integration levels. Equivalence classes and boundary values have been considered in writing all Integration Test Cases. Test case execution includes combining some critical cases at extreme operating boundaries.

5.8 Safety Validation

One or more test cases, or analysis documents, exist for each safety requirement (including software safety requirements) as shown by the requirements traceability matrix. Each test case includes a procedure for the test as well as pass/fail criteria for the test (inputs, outputs and any other acceptance criteria). The validation test plan includes the procedure used to properly judge that the validation test is successful or not. Dynamic (runtime) analysis/testing is performed in addition to static analysis/testing.

Fault injection testing, if required, has been performed on the product as defined in the fault injection test plan. The results have been analyzed and adjustments have been made to the FMEDA based on these results.

Test results are documented including reference to the test case and test plan version being executed.

The EMC/EMI and Environmental specifications were tested (and passed) and were the same as or more stringent than those reviewed and approved by the FMEDA analyst.

The following information is documented in the test results:

- a record of validation activities, permitting validation results to be reproduced and/or retraced.
- The version of the validation plan used to execute the test.
- The safety function associated with each test case.
- The tools and equipment and calibration data.
- The Configuration Identification of the Item Under Test.

Product is not complex enough to warrant performance modeling. There is only one performance parameter in the system (Safety Function Response Time) and this parameter can be sufficiently tested by validation tests.

The Validation Test Plan required simulation of process inputs and timing between input changes (process simulation). This is done by testing the software in the product hardware and simulating the input signal(s) and other process conditions using a test fixture or test equipment.

5.9 Safety Manual

The Safety Manual is provided and identifies and describes the functions of the product. The functions are clearly described, including a description of the input and output interfaces. When internal faults are detected, their effect on the device output is clearly described. Information is provided to facilitate the development of an external diagnostics capability (output monitoring).

The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing. Procedures for maintaining tools and test equipment are listed.

All routine maintenance tools and activities required to maintain safety are identified and described in the Safety Manual.

The Safety Manual states there are no security relevant considerations with this product.

The user manual defines what configuration options and methods exist for the product. The safety manual documents any configurations and/or features that may not be used.

The element does not contain any separately releasable software.

6 Terms and Definitions

Term	Definition
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.
PFDAVG	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).
HART	Highway Addressable Remote Transducer
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

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

7.2 Version History

Contract Number	Report Number	Revision Notes
Q16/12-041	REP 16/12-041 R002 V1R0	Initial Release; DEB 5/19/2019

Review: John Yozallinas, 5/16/2019

Status: Released, 5/19/2019

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Dave Butler, Senior Safety Engineer

John C Yozallinas

John Yozallinas, Senior Safety Engineer