IEC 61508 Functional Safety Assessment

Project:
One Series Safety Transmitter

Customer:
United Electric Controls
Watertown, MA
USA

Contract No.: Q17/01-143
Report No.: UEC 1210073 R002
Version V1, Revision R3, May 9, 2017
John Yozallinas

Management Summary

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

One Series Safety Transmitter

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

- *exida* assessed the development process used by United Electric Controls through an audit and creation of a detailed safety case against the requirements of IEC 61508.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed the manufacturing quality system in use at United Electric Controls
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. The primary audit tool was a full IEC 61508 Safety Case, prepared using the *exida* Safety Case tool. Hardware and software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also, the user documentation (safety manual) was reviewed. See section 6 for updated remarks and documentation.

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

The audited development process, as tailored and implemented by the United Electric Controls One Series Safety Transmitter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the One Series Safety 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 One Series Safety Transmitter is capable for use in up to 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 certified versions specified in this document. The PFD_{AVG} and Architectural Constraint requirements of the standard must be verified for each element of the Safety Function.

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

Table of Contents

1 Purpose and Scope

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

- One Series Safety Transmitter

by *exida* according to the requirements of IEC 61508:2010.

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

Table 1: Revisions in Assessment Scope, Updated

One Series Safety Transmitter (Model 2SLP)		
Hardware	Display Board	63136-398 Rev F
	AC Relay Board	63136-399 Rev E
	130 VDC Relay Board	63136-417 Rev A
	30 VDC Relay Board	63136-418 Rev A
Software/Firmware	62161-19 Rev D	

The versions in Table 1 were current when this assessment report version was released. For updated versions covered under this certification, contact the manufacturer to find how the certified versions and compatibility can be checked.

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 400 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

United Electric Controls	Manufacturer of the One Series Safety Transmitter
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment

United Electric Controls contracted *exida* 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

NOTE: See section 6 for updated remarks and documentation.

2.4.1 Documentation provided by United Electric Controls

ID	Document Type	Document Name	Version	Date
D001	Quality Manual	LP 42200 Corporate Policy Manual.doc	J	6/14/2012
D003	Overall Development FS Process	DE 7300107 Design & Development For Functional Safety.doc	B	6/14/2012
D003b	Overall Development Process	DE 73001 Design & Development.doc	F	5/29/2012
D003c	Overall Development FS Process Doc Cover Page	DE 730010701 Functional Safety Design Record.doc	A	

D004	Configuration Management Process	SR113028.D1.4 Configuration Management Plan Rev A.doc	A	7/27/2012
D006	Field Return Procedure	QS 8520104 Processing of a Field Return.doc	E	2/11/2014
D007	Manufacturer Qualification Procedure	PU 74102 Supplier Assessment & Approval.doc	L	12/19/2012
D010	Quality Management System (QMS) Documentation Change Procedure	QS 42301 Document Control.doc	J	3/11/2013
D010b	Quality Records Maintenance Procedure	QS 42401 Quality Records.doc	U	2/20/2014
D012	Non-Conformance Reporting procedure	QS 83001 Control of NC Material.doc	E	6/14/2012
D013	Corrective Action Procedure-IDR	QS 8520101 Corrective Action Process.doc	F	2/4/2014
D013b	Corrective Action Procedure-RMA	QS 8520103 Corrective Action for RM.doc	E	2/11/2014
D023	Modification Procedure	DE 73701 Design Changes.doc	N	5/29/2012
D023b	Impact Analysis Template	DE 730010702 Functional Safety Impact Analysis Form.xls		
D026	FSM Plan or Development Plan, incl action item tracking, tools, competency	SR113028.D1.3 Functional Safety Mgt Plan Rev H.doc	H	3/11/2014
D027	Configuration Management Plan	SR113028.D1.4 Configuration Management Plan Rev A.doc	A	7/27/2012
D033	Training Record - Sample	HR 622010002 Training and Education Form, Sample record for IEC 61508 Training.pdf		
D036	ISO 900x Cert or equivalent	un9156cert.pdf		11/27/2012
D040	Safety Requirements Specification	SR113028.D2.1 Safety Requirements Specification Rev B.doc	B	
D041	Safety Requirements Inspection	SR113028.D2.2 Safety Requirements Specification Inspection Report.docx		

D041b	Safety Requirements Review Checklist	SR113028.D2.4 Safety Requirements Spec Checklist rev A.doc	A	
D041c	Safety Requirements Inspection - Derived Reqs	SR113028.D2.15 Safety Requirements Checklist & Inspection Report.doc		
D044	Marketing Requirements Document	SR113028.D1.1, D1.2 Marketing Product Definition_Syst Req Spec Rev F.doc	F	
D045	System Architecture Design Specification	SR113028.D2.5 System Architecture Description Rev B.doc	B	12/26/2012
D045b	System Architecture Design Review	SR113028.D2.8 System Architecture Inspection Report.docx		
D049	Software Arch Design Specification, incl diagnostics	SR113028.D4.2 Software Architecture Description Rev D.doc	D	9/1/2013
D051	Detailed Software Design Specification	SR113028.D4.10 Detailed Software Design Description.doc	1st	8/23/2013
D051b	Detailed Software Design Review	SR113028.D4.14 Detailed Software Design Inspection Report.docx		
D053	Arch Design Review Record-FMEA	SR113028.D2.6 System Failure Modes and Effects Analysis Rev C.docx	C	2/28/2013
D054	Verification Results	A number of checklists were used at various phases of the development lifecycle.		
D056	Requirements Traceability Matrix, incl SW SRS	SR113028.D2.3 and D2.7 Requirements Traceability Matrix Rev B.xlsx	B	
D057	Software Test Coverage Analysis Report	SR113028 Code Coverage Status.xlsx		
D057b	Software Complexity Analysis Report	Complexity Metrics SR113028.txt		
D058	Code Review Record	SR113028.D4.13 Source Code Inspection Reports.docx		

D058b	Code Review Record-size	SR113028 Module Length Justification 140326.docx		
D059	Fault Injection Test Plan	SR113028.D3.7 Fault Injection Test Spec.docx		9/9/2013
D060	Coding Standard- UEC, incl static analysis resolution	SR113028.D4.1 Software Design and Coding Guidelines Rev D.docx	D	3/27/2014
D060b	Coding Standard- exida	exida C C++ Coding Standard - IEC61508_V1R2.pdf	V1R2	
D061	Static Code Analyzer Configuration Description	"au-exida.lnt" file	1.3	14 Jun 04
D062	Static Code Analysis Results	SR113028 PCLint Test Results.docx		
D064	Module Test Plan	SR113028.D4.15 Unit Test Plan Rev B.docx	B	3/11/2014
D066	module test Results	SR113028.D4.16 Unit Test Results Rev B.doc	B	3/11/2014
D066b	module test Results	Unit Test Value Tables.xlsx		
D066c	module test Results- numerical analysis	Black Box Model.xlsm		
D067	Integration Test Plan	SR113028.D4.20 Integration Test Plan_Spec Rev A.docx	A	
D067b	Integration Test Plan Review	SR113028.D4.22 Integration Test Plan Checklist and Inspection report.docx	A	
D068	Integration Test Results	SR113028.D4.21 Integration Test Report.docx		
D069	Validation Test Plan	SR113028.D5.1 Validation Test Plan Rev B.docx	B	
D070	Validation Test Plan Review Record	SR113028.D5.2 Validation Test Plan Inspection Report.docx		
D071	Environmental Test Plan, incl EMC	SR113028.D5.10 Environmental Stress and EMI_EMC Specification.docx		
D073	Master Action Item Tracking System	SR113028 Master Action Item List.xlsx		Dec snapshot
D074	Validation Test Results	SR113028.D5.11.Safety Validation Test Report.xlsx		

D075	Environmental Test Results-Vibration	SR113028.D5.12 2SLP Vibration Test Report.pdf		11/25/2013
D075b	Environmental Test Results-Shock	SR1134028.D5 Shock Test Report.xlsx		
D076	EMC Test Results-Emissions	SR113028.D5.12 2SLP Emissions Test Report.pdf		11/27/2013
D076b	EMC Test Results-Immunity	SR113028.D5.12 2SLP Immunity Test Report.pdf		11/7/2013
D077	Fault Injection Test Results	SR113028.D3.8 Fault Injection Test Report.docx		11/12/2013
D078	Operation / Maintenance Manual	IM_ONE SAFETY TRANSMITTER.pdf (doc # IM_ONE_SAFETY-02)	02	4/11/2014
D079	Safety Manual	One ST Safety manual.pdf (doc # OneST-SM-02)	02	4/11/2014
D080	Safety Manual Review	SR113028.D2.11 Safety Manual Inspection Report.docx		11-11 13
D086b	Tool HAZOP Report	SR113028.D2.13 Tool Hazop.docx		
D086c	Tool HAZOP Inspection Report	SR113028.D2.14 Tool HAZOP Inspection Report.docx		
D086d	Tool Report supplement	Test Record.pdf		
D087	Digital Signature	62161-19 RevC.PDF	C	3/25/14
D088	Impact Analysis Record-example	Sample Impact Analysis for HW; ECN E4930.pdf		11/19/2013
D088b	Impact Analysis Record-example2	SR113028 Int Test Impact Analysis 130719 - 2.pdf		2/14/2014
D091	SW Release Notes	62161-19 RevB Release Notes.docx	B	
D092	SW Criticality/HAZOP report	SR113028.D4.3 Software Criticality and HAZOP Analysis.doc	1st	5/23/2013
D093	SW Release & Rev Control	DE 7330108 Software Release Rev Control.doc	D	4/7/2014
D094	Site Audit Information	On-Site Audit Summary.msg		3/20/2014

2.4.2 Documentation generated by *exida*

[R1]	UEC OneSeriesSafety Sensor V1R7 Safety Case WB-61508 v1.6.xlsm	SafetyCase for One Series Safety Transmitter
[R2]	UEC 1210073 R002 V1R1 61508 Assessment Report OneSeries.doc	IEC 61508 Functional Safety Assessment for One Series Safety Transmitter (initial report)
[R3]	UE 12-10-073 R001 V2 R2 One Series SAFETY TRANSMITTER FMEDA Report.pdf	FMEDA for One Series Safety Transmitter

3 Product Description

The One Series Safety Transmitter is a 2-wire transmitter that senses the temperature or pressure of a system process and provides outputs to monitor or shut down that system before an unsafe condition occurs. A 4-20 mA output provides an analog indication of the process for use by a safety PLC. The solid-state Safety Relay Output (AC or DC) provides direct control or shut down of a final element based on programmed operating modes and limits. The Switch Status Output is a discrete output that mirrors the function and state of the solid-state relay output. The “I Am Working” (IAW) Output is a discrete output based on self-diagnostics and indicates transmitter health. Any diagnostic failure that causes and IAW fault will force all outputs to the fail-safe state. All four outputs of the One Series Safety Transmitter can be used as safety critical outputs and operate in De-energize To Trip (DTT) mode.

The One Series Safety Transmitter is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0.

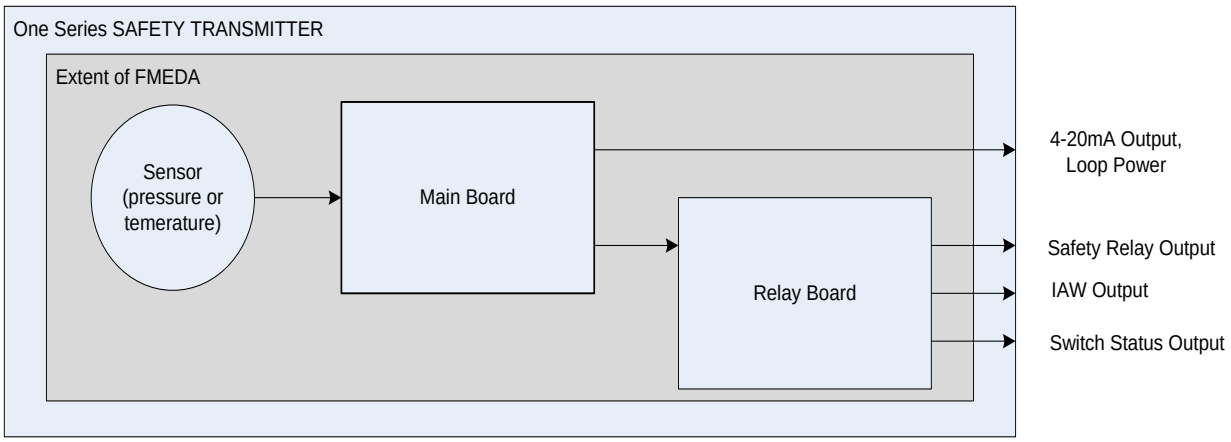

Figure 1: One Series Safety Transmitter

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from United Electric Controls and is documented in the Safety Case [R4].

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.

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

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 a Software Criticality and HAZOP report

The review of the development procedures and product design is described in section 5.

4.2 Assessment level

The One Series Safety Transmitter has been assessed per IEC 61508 to the following levels:

- Systematic Safety Integrity: SIL 3 capable
- Random Safety Integrity: PFD_{AVG} and Architectural Constraints must be verified for each application.

The development procedures were assessed as suitable for use in applications with a maximum Safety Integrity Level of SIL 3 according to IEC 61508.

4.3 Product Modifications

The modification process has been successfully assessed and audited, so United Electric Controls 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, including field history
- 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 and lifecycle phases to be repeated
    - List of modified documentation
    - Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by United Electric Controls during the product development against the objectives of IEC 61508 parts 1, 2, and 3, see [N1]. The development of the One Series Safety 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

United Electric Controls has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D003, D003b, and D004].

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product 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 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 United Electric Controls Safety Instrumented Systems (SIS) product development is governed by a development process [D003 and D003b]. This process requires that United Electric Controls create a project plan which is specific for each development project. The Functional Safety Management Plan [D026] defines all of the tasks that must be done to ensure functional safety as well as the person(s) and role(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 a configuration management plan, [D004] and [D023].

Training, Competency recording

Competency is ensured by the creation of a competency and training table for the project [D026]. The table lists all of those on the project who are working on any of the safety activities of the safety lifecycle. Specific competencies for each person are listed on the table which is reviewed by the project manager. Any deficiencies are then addressed by updating the table with required training for the project.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D003] a safety requirements specification (SRS) [D040] is created for all products that must meet IEC 61508 requirements. For the One Series Safety Transmitter, the requirements specification [D040] contains all the safety functions necessary to achieve the required functional safety as well as non-safety requirements. The SRS goes through peer review [D041] by a cross-functional group with review meetings. The results of the review are documented and all action items are tracked through resolution with a master action item list. During the assessment, *exida* reviewed the content of the specification for completeness per the requirements of IEC 61508.

Traceability between development stages is handled by linking the traceability matrices [D056] with the system and software architecture designs [D045, D045b, D049]. 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 United Electric Controls 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 United Electric Controls include backward traceability between the safety requirements and the perceived safety needs.

The safety case [R4] includes details on how each of these requirements has been met. This meets the requirements of SIL 3.

5.1.3 Design

Hardware design, including both electrical and mechanical design, is done according to [D003] and [D003b]. The hardware design process includes creating a hardware/system architecture specification [D045], a peer review of this specification [D045b], component selection, detailed design (drawings and schematics), a peer review of the detailed design, a Failure Modes, Effects and Diagnostic Analysis (FMEDA) [R7], electrical unit testing, fault injection testing, and hardware verification tests.

Requirements from **IEC 61508-2, Table B.2** that have been met by United Electric Controls include observance of guidelines and standards, project management, documentation, structured design, modularization, checklists, semi-formal methods, computer aided design tools, simulation, and inspection of the specification. This is also documented in the Safety Case [R4]. This meets the requirements of SIL 3.

Software (firmware) design is done according to [D003, D026]. The software design process includes software architecture design [D049] and peer review [D053], detailed design [D051] and peer review [D051b], critical code reviews [D058], static source code analysis [D062] and unit test [D066].

Requirements from **IEC 61508-3, Table A.2** that have been met by United Electric Controls include fault detection, error detecting codes, failure assertion programming, diverse monitor techniques, stateless software design, forward and backward traceability between the software safety requirements specification and software architecture, semi-formal methods, event-driven with guaranteed maximum response time, and static resource allocation.

Requirements from **IEC 61508-3, Table A.3** that have been met by United Electric Controls include suitable programming language with a language subset, and tools and translators evaluation.

Requirements from **IEC 61508-3, Table A.4** that have been met by United Electric Controls include semi-formal methods, computer aided design tools, an integrated development environment, defensive programming, modular design approach and coding standards, structured programming, forward traceability between the software safety requirements specification and software design,

This is also documented in the Safety Case [R4]. This meets the requirements of SIL 3.

5.1.4 Validation

Validation Testing is done via a set of documented tests. The validation tests are traceable to the Safety Requirements Specification [D040] in the validation test plan [D069]. Integration tests [D067] are also part of the validation phase. The traceability matrices [D056] show that all safety requirements have been validated by one or more tests. In addition, third party independent testing is included as part of the environmental validation testing [D076, D076b]. All non-conformities are evaluated and documented in a change request system. Procedures are in place for corrective actions to be taken when tests fail as documented in [D003, D023, and D069].

Requirements from **IEC 61508-2, Table B.5** that have been met by United Electric Controls 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 United Electric Controls include functional and black box testing, and forward and backward traceability between the software safety requirements specification and the software safety validation plan.

The Safety Case [R4] documents more details on how each of these requirements has been met for SIL 3.

5.1.5 Verification

Verification activities are built into the development process as defined in [D003, D026, and D023]. Verification activities include the following: FMEDA, Fault Injection Testing, static source code analysis, peer reviews, and software unit testing. In addition, safety verification checklists are filled out for many phases 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 United Electric Controls include functional testing, project management, documentation, and black-box testing.

Requirements from **IEC 61508-3, Table A.5** that have been met by United Electric Controls include dynamic analysis and testing, data recording and analysis, functional and black box testing, performance testing, interface testing, and test management.

Requirements from **IEC 61508-3, Table A.6** that have been met by United Electric Controls 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.

The Safety Case [R4] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

5.1.6 Modifications

Modifications are done per the United Electric Controls change management process as documented in [D023, D026, D027]. Impact analyses are performed for all changes once the product is released. The results of the impact analysis are used in determining whether to approve the change. The development process as defined in [D003 and D003b] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D012, D013, and D013b]. 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.

United Electric Controls has met the requirements from **IEC 61508-3, Table A.8,** including impact analysis, reverify changed/affected software modules, revalidate complete system or regression validation, software configuration management, forward and backward traceability between the software safety requirements specification and the software modification plan (including reverification and revalidation).

5.1.7 User Documentation

United Electric Controls created a safety manual for the One Series Safety Transmitter [D079] which addresses all relevant operation and maintenance requirements from IEC 61508. This safety manual was assessed by *exida*. It includes safety related information for SIL capability, product type, HFT and failure reporting. The final version is considered to be in compliance with the requirements of IEC 61508. The Installation Manual [D078] includes additional information for the user regarding safe operation and avoidance of hazards. This documentation is managed on the project and considers user/maintenance friendliness, limited operation modes, and protection against operator mistakes.

Requirements from **IEC 61508-2, Table B.4** that have been met by United Electric Controls include operation and maintenance instructions, proof testing, diagnostics interval, systematic and hardware capability, documentation management, and limited operation possibilities.

The Safety Case [R4] 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 One Series Safety Transmitter, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R7]. The FMEDA was verified using Fault Injection Testing [D077] 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.

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) 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.

For pressure applications other than clean service, the user must estimate the failure rate for the clogged impulse line and add this failure rate to the transmitter failure rates.

6 2017 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

United Electric Controls	Manufacturer of the One Series Safety Transmitter
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

United Electric Controls contracted *exida* in January 2017 to perform the surveillance audit for the One Series Safety Transmitter. The surveillance audit was conducted remotely in part, and also onsite at United Electric Controls's facility in Watertown, MA, USA, in April 2017.

6.2 Surveillance Methodology

As part of the IEC 61508 functional safety surveillance audit the following aspects are 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 One Series Safety Transmitter.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The safety manual and any changes are reviewed.
- 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 provided by United Electric Controls

D100	SR113028 Exida RFI's.xlsx	RFI Resolutions
D101b	readme_FieldHist.txt	Field History Log
D103	DE 7300107 Design Development For Functional Safety.doc	Overall Development FS Process update
D103b	DE 73701 Design Changes.doc	Design Change Process update
D104	SRxxxxxx.D4.9 Software Module Code Review Checklist.docx	Code Review Checklist
D105	SRxxxxxx.D4.17 Unit (Module) Test Plan Checklist (template).docx	Unit Test Checklist
D106	SR160005.D5.11 Validation Test Report.xlsx	Validation Test Results - HW update
D107	SR150047.D5.11. Safety Validation Test Report.xlsx	Validation Test Results - SW update
D108	UE ISO Cert.pdf	ISO 900x Cert or equivalent update
D109	IM_ONE ST-05.pdf	Operation / Maintenance Manual- update for DC relay
D111	SRxxxxxx.D1.3 Functional Safety Mgt Plan Rev -.doc	FSM Plan update
D112	DE 730010702 Functional Safety Impact Analysis Form.xls	Impact Analysis Template update
D113	SR113028.D2.3 and D2.7 Req Traceability Matrix Rev C.xlsx	Requirements Traceability Matrix update
D114	SR113028.D4.2 Software Architecture Description Rev E.pdf	Software Arch Design Specification update
D115	SR113028.D4.10 Detailed Software Design Description.pdf	Detailed Software Design Specification update
D115b	Summary of Proposed Changes to ST software.docx	Software Change Summary
D116	IA 16014.pdf	Impact Analysis Record- SW
D116b	IA-17001__SR-160005_ECN-E5976.pdf	Impact Analysis Record- HW
D117	SR160005.D3.2 REV A Circuit Descriptions.docx	HW Design Specification
D117b	6247-710 Rev A.pdf	HW Schematic for DC relay output
D119	readme_HW-SW-Rev.txt	HW/SW Version Release update

6.2.2 Surveillance Documentation updated or generated by *exida*

[R4]	UEC OneSeriesSafety Sensor V2R1 Safety Case WB-61508 v1.6.xlsm	Updated IEC 61508 SafetyCase for One Series Safety Transmitter
[R5]	Q17-01-143 UEC Site Audit Notes.pdf	IEC 61508 Site Audit Report, United Electric Controls

[R6]	UEC 1210073 R002 V1R2 61508 Assessment Report OneSeries.doc	Updated IEC 61508 Functional Safety Assessment for One Series Safety Transmitter (this report)
[R7]	UE 12-10-073 R001 V4 R1 One Series SAFETY TRANSMITTER FMEDA Report.pdf	FMEDA report update for One Series Safety Transmitter
[R8]	UEC 17-01-143 R001 V1R1 Field History Analysis.xls	Field History Analysis for One Series Safety Transmitter
[R9]	UEC 17-01-143 R002 V1R1 Change Audit_UEC ONE Sensor.xls	Change Audit Assessment

6.3 Surveillance Results

An on-site audit was conducted as part of the United Electric Controls One Series Safety Transmitter certification renewal. The results of the audit were successful with no material issues discovered. Software tests were selected based on the regression test plan that was agreed upon at the end of the original assessment project. Tests for two significant software changes were witnessed in application tests and the results were successful.

6.3.1 Procedure Changes

Changes to the Development and Change Management Procedures [D103, 103b] were made based on prior recommendations and organizational improvement methods. These were reviewed and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes & Impact Analysis

Engineering changes (D115b, D116, D116b) to the One Series Safety Transmitter were submitted by United Electric Controls and reviewed during this audit. The changes were made according to well-established and compliant procedures. Details of both hardware and software changes were assessed. Relevant design documentation (D114, D115) was updated as needed. The impact analysis template was updated (D112). Impact Analyses for changes (D116, D116b) were submitted by United Electric Controls and reviewed during this audit. Traceability for requirements and validation testing was updated (D113). Updated test reports were reviewed (D106, D107).

Effects of the changes on product versions are reflected in Table 1 of this report.

6.3.3 Field History

Field failure and shipping history for the One Series Safety Transmitter (D101b) were submitted by United Electric Controls and reviewed during this audit. The actual failure rate compares favorably to and is lower than the prediction FMEDA data and is supported by the field history analysis [R8].

6.3.4 Safety Manual

An Installation and Maintenance manual update (D109) was submitted by United Electric Controls and reviewed during this audit. The safety manual update (D079) was not updated for this audit.

6.3.5 FMEDA Update

The FMEDA report [R7] for the One Series Safety Transmitter was reviewed and updated during this audit. Route 2_H criteria has been met so the SFF is not needed for SIL 2 safety applications. The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

6.3.6 Evaluate use of certificate and/or certification mark.

The United Electric Controls website for the One Series Safety Transmitter was reviewed for proper use of the certificate and certification mark and was found to be in order.

6.3.7 Previous Recommendations

United Electric Controls has a well-established development process. A number of process improvements were recommended by *exida* which have been incorporated into the product development process (D100). Previous recommendations have been reviewed and sufficient action has been taken to improve the process and its deliverables.

7 Terms and Definitions

exida 2_H criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the Route 2_H 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.
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).
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
Q12/10-073	UEC 12-10-073 R002 V1, R1	initial report, corrected doc revs/dates, JCY, 20-Apr-2014
Q17/01-143	UEC 12-10-073 R002 V1, R2	revised for surveillance audit; JCY, 24-Apr-2017
Q17/01-143	UEC 12-10-073 R002 V1, R3	Updated FMEDA report in section 6.2.2; JCY, 9-May-2017

Review: V1, R2: Ted Stewart
Status: Released 9-May-2017
Authors: John Yozallinas

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Evaluating Assessor: John Yozallinas, CFSE, Senior Safety Engineer

Certifying Assessor: Ted E. Stewart, CFSP, Program Development & Compliance Manager