IEC 61508 Functional Safety Assessment

Project:
3144P Safety Certified Temperature Transmitter

Customer:
Emerson Process Management
Rosemount Inc.
Chanhassen, MN
USA

Contract No.: Q06/09-33
Report No.: ROS 06-09-33 R001
Version V1, Revision R1, February 13, 2007
Michael Medoff

Management summary

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

- 3144P Safety Certified Temperature Transmitter

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

- exida assessed the modifications performed by Emerson by an on-site audit and creation of a detailed safety case against the requirements of IEC 61508.
- exida 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 2 for hardware and SIL 3 for the design process. This product was previously certified to IEC 61508, SIL 2 for hardware and SIL 3 for software by TUV (Certificate-Register-No.: SAS2550/04). Based on this assessment, it can be concluded that the Emerson development process meets the requirements of IEC 61508 for SIL 3. As a result this latest assessment focused on reviewing the changes made to the product. The changes were assessed against section 7.8 of IEC 61508 part 2 (E/E/PES Modification) and section 7.8 of part 3 (Software Modification). A partial IEC 61508 Safety Case was prepared, focusing specifically on the modification process, and used as the primary audit tool. Modification 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 3144P was found to meet the requirements of SIL 2 for random integrity @ HFT=0, SIL 3 for random integrity @ HFT=1 and SIL 3 for systematic integrity.

Table of Contents

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.

Option 4: Assessment of Modifications according to IEC 61508 for previously certified products

Option 4 only applies to products that have already been certified to 61508 and have undergone changes. The changes are assessed specifically against the modification sections of IEC 61508 (Section 7.8 of part 2 and 7.8 of part 3).

This assessment shall be done according to option 4.

This document shall describe the results of the IEC 61508 functional safety assessment of the 3144P Safety Certified Temperature Transmitter.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail 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

Emerson Process Management	Manufacturer of the 3144P Temperature Transmitter
exida	Performed the IEC 61508 Functional Safety Assessment according to option 4 (see section 1)

Emerson Process Management contracted *exida* in September 2006 with the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508 (Parts 1 - 7): 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Emerson Process Management

Ref.	Document ID	Document Description	Revision
[D1]	DOP 416	Safety Instrumented Systems Product Design and Development Process	Rev E
[D2]	DOP 440	Engineering Change Order	Rev AE
[D3]	EDP 400-500	Peer Review Procedure	Rev A.1
[D4]	EDP 400-300	Configuration and Change Management Procedure	Rev C
[D5]	701-063/2003T	TUV Certification Report of the 3144P SIS Temperature Transmitter	Rev 1.0
[D6]	03144-2108 AH to AJ.pdf	Schematic marked up with changes	4/4/2006
[D7]	3144P_Safety_ SIA1.xls	Safety Impact Analysis for Hardware changes	2/12/2007

[D8]	SafetyRequirements.pdf	Safety Requirements Specification	Rev C.1
[D9]	SAS2550/04	TUV Certificate for 3144P SIS Temperature Transmitter	10/27/2004
[D10]	3144P_STD_SIS- HSTP.doc	Hardware System Test Plan for the 3144P HART Temperature Transmitter	Rev. A
[D11]	3144P_STD_SIS- STP.doc	Software System Test Plan for the 3144P HART Temperature Transmitter	Rev. A.5
[D12]	3144P HART SCCT.htm	Minutes of Software Configuration Control Team meeting 5/23/06	12/14/06
[D13]	3144P STD/SIS SCCT.htm	Minutes of Software Configuration Control Team meeting 11/30/06	12/14/06
[D14]	3144P_STD_SIS_ Accuracy.xls	Test Results for Accuracy Test	12/14/06
[D15]	3144P_std_sis_code_ cons_log_and_report.xls	Inspection Report for 3144P Code Changes (Discrepancies and Merge Standard with SIS)	12/14/06
[D16]	3144P_std_sis_pdp.xls	3144P Project Defined Process	Rev. B
[D17]	3144P_std_sis_sirs_ cons_log_and_report.xls	Inspection Report for Safety Requirements Specification	Rev. C.0
[D18]	3144P_std_sis_stp_ cons_log_and_report.xls	Inspection Report for Software System Test Plan	Rev. 0.1
[D19]	Accuracy-3144P_STD_ SIS.doc	Test Report for Accuracy Test	12/14/06
[D20]	Approvals.pdf	Approvals Listing for ECO #RTC1021941	12/14/06
[D21]	HTP-3144_AD589 replacement.doc	Hardware System Test Plan for the 3144 HART (headmount) transmitter	Rev. B
[D22]	Individual_log-HWtest_ Linda.xls	Individual Inspection Log for Hardware System Test Plan	Rev. A
[D23]	Individual_log-HWtest_ Scott.xls	Individual Inspection Log for Hardware System Test Plan	12/14/2006
[D24]	IntegrationTestSpec.pdf	Integration Test Specification	Rev. C.1
[D25]	It_dat.log	Automated Integration Test Results	12/8/2006
[D16]	It_manual4_dat.log	Manual Integration Test Results	12/8/2006
[D17]	Lint_SIS.out	LINT Output	7/10/2006
[D18]	Lint_STD_SIS.out	LINT Output	12/8/2006
[D19]	Schematic Review Notes.doc	Design Review Minutes	11/18/05

[D20]	Summary_TraceMatrix.xls	Requirements Traceability Matrix	2/12/07
[D21]	W__3144PH_source_ embedded_it_results_ 3144p_std_sis_it_re.pdf	Integration Test Report	12/14/2006
[D21]	User Manual Updates	Scanned copy of marked up user manual. This copy lists changes that will be made to the user manual for this release	12/20/06
[D22]	00825-0100-4021	3144P Quick Installation Guide	Rev. DA
[D23]	00809-0100-4021	3144P Reference Manual	Rev. EA
[D24]	00813-0100-4021	3144P Product Data Sheet	Rev. GA
[D25]	PRD00030658.DOC	Impact Analysis for PRD #00030658	2/6/07
[D26]	PRD00030659.DOC	Impact Analysis for PRD #00030659	2/5/07
[D27]	PRD00030666.DOC	Impact Analysis for PRD #00030666	2/5/07
[D28]	PRD00030667.DOC	Impact Analysis for PRD #00030667	2/5/07
[D29]	PRD00030671.DOC	Impact Analysis for PRD #00030671	2/8/07
[D30]	PRD00030677.DOC	Impact Analysis for PRD #00030677	2/6/07
[D31]	PRD00031035.DOC	Impact Analysis for PRD #00031035	2/8/07
[D32]	PRD00031473.DOC	Impact Analysis for PRD #00031473	2/8/07
[D33]	3144p_std_sis_srs.html	Software Requirements Specification for the 3144P HART® Standard/Safety Temperature Transmitter Project	Rev B.2
[D34]	AO_4-20mA.doc	4-20 mA Ranging Test Results Summary	12/20/06
[D35]	Various	4-20 mA Ranging Detailed Test Results Data	12/13/06
[D36]	AlarmCharacteristics_ 3144P_SIS.doc	Alarm Characteristic Test Results Summary	1/16/07
[D37]	Various	Alarm Characteristic Test Results Data	12/13/06
[D38]	Continuity.doc	Strip Chart Continuity Test Results Summary	2/9/07
[D39]	Various	Strip Chart Continuity Test Results Data	12/13/06 & 2/6/07
[D40]	Diagnostics-Pt1.doc	Diagnostics Part 1 Test Results Summary	2/6/07
[D41]	Diagnostics-Pt1_SIS_STD.xls	Diagnostics Part 1 Test Results Data	1/31/07

[D42]	LCD_Meter.doc	LCD Meter Test Results	2/12/07
[D43]	Open_Sensor_Detection_ 3144P_STD_SIS.doc	Open Sensor Detection Test Results Summary	1/16/07
[D44]	Various	Open Sensor Detection Test Results Data	12/13/06
[D45]	Accuracy-3144P_STD_ SIS.doc	Accuracy Test Results Summary	2/8/07
[D46]	3144P_STD_SIS_ Accuracy.xls	Accuracy Test Results Data	2/5/07
[D47]	TempEffect_3144P_STD_ SIS.doc	Temperature Effect Test Results Summary	2/9/07
[D48]	3144p_STD_Safety_ tempeffects.xls	Temperature Effect Test Results Data	2/9/07
[D49]	NC604145	EMC Test Result Summary	Rev. A
[D50]	3144p_std_sis_it_report.html	3144P Integration Test Report	2/12/07
[D51]	Mohajer Training Records.xls	Training Records/Competency Report	2/12/07
[D52]	3144p_std_sis_ LiteratureReview02092007.doc	Meeting Minutes from User Documentation Review	2/12/07
[D53]	3144p_std_sis_EmulatorTests.doc	3144 Safety as Standard Emulator Test Results	2/12/07
[D54]	RTC 1020023 Testing.pdf	Test Results for ECO #RTC1020023	2/12/07
[D55]	Layout Review Notes	Minutes from Layout Review Meeting	2/9/07
[D56]	Various	Markup for user manual updates from user documentation review	2/12/07

2.4.2 Documentation generated by *exida*

[R1]	3144P Audit – 12-14-2006.xls	Detailed safety case documenting results of assessment (internal document)
[R2]	ROS 04-08-19 R003, FMEDA, V2R1, 7/26/2006	3144P SIS Temperature Transmitter FMEDA Report
[R3]	ROS 06-09-33 R001, V1R1, 2/13/07	IEC 61508 Functional Safety Assessment, 3144P (this report)

3 Product Description

3.1 3144P Safety Certified Temperature Transmitter

The 3144P Safety Certified Temperature Transmitter is a 2 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 3144P Safety Certified Temperature Transmitter is classified as a Type B device according to IEC 61508 (See section 7.4.3.1.3 of IEC 61508-2), having hardware fault tolerance of 0. Combined with one or two temperature sensing elements, the 3144P becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 3144P safety certified transmitter are:

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

4 IEC 61508 Functional Safety Assessment

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

4.1 Methodology

The full functional safety assessment includes an assessment of all changes made in comparison to the modification requirements of IEC 61508 (Section 7.8 of part 2 and 7.8 of part 3). In addition a Hardware FMEDA was performed to determine the safe failure fraction (SFF) and the average probability of failure on demand (PFD_{AVG}).

4.2 Assessment level

The 3144P has been assessed per IEC 61508 to the following levels:

- SIL 2 capability for a single device
- SIL 3 capability for multiple devices

The development procedures have been previously assessed by TUV as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL3) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the changes made by Emerson for this development against the modification procedures of IEC 61508 parts 2 and 3. The assessment was done on December 14, 2006 on-site at Chanhassen, MN. Additionally a detailed safety case was completed, see [R2]. The specific part of 61508 and section number are given in parenthesis for each item below.

All changes were successfully reviewed against the following criteria from IEC 61508:

5.1 Detailed Specification of the Modification or Change (Part 2, Section 7.8.2.1a)

A detailed specification of all modifications are included in the impact analysis document.

5.2 Impact Analysis (Part 2, Section 7.8.2.1b)

All changes include a detailed safety impact analysis. The impact analysis details which phases of the development process need to be repeated and what output is required from each phase. The impact analysis is documented in either the change control system or in an independent document. For software, the impact analysis includes a complete listing of all changed software modules.

5.3 Approvals for changes (Part 2, Section 7.8.2.1c)

Approvals for all changes are documented via the change history in the software change request system and via electronic approvals for Engineering Change Orders (ECO's). Both of these can easily be reviewed on-line.

5.4 Progress of Changes (Part 2, Section 7.8.2.1d)

Progress of all changes is documented via the change history in the software change request system and via electronic approvals for Engineering Change Orders (ECO's). Both of these can easily be reviewed on-line.

5.5 Test Cases Including Revalidation Data (Part 2, Section 7.8.2.1e)

Test cases are documented as part of the impact analysis for all changes

5.6 E/E/PES configuration management history (Part 2, Section 7.8.2.1f)

Configuration Management history is documented via the version control system for all changes. In addition, all documents include the configuration management history within the document.

5.7 Deviation from normal operations and conditions (Part 2, Section 7.8.2.1g)

Deviations from normal operations and conditions is discussed in the impact analysis or FMEDA for all changes

5.8 Necessary changes to system procedures (Part 2, Section 7.8.2.1h)

Any changes to system procedures are documented in the impact analysis.

5.9 Necessary changes to documentation (Part 2, Section 7.8.2.1i)

All necessary documentation changes are included in the impact analysis

5.10 Modifications shall be performed with at least the same level of expertise, automated tools (see 7.4.4.2 of IEC61508-3), and planning and management as the initial development of the E/E/PE safety-related systems (Part 2, Section 7.8.2.3)

Management assures that changes are carried out by qualified engineers. Engineer's qualifications are tracked via an on-line system. Identical tools to the original development were used. An impact analysis is the basis for planning of each change.

5.11 Evidence that Change was reverified (Part 2, Section 7.8.2.4)

All changes had appropriate verification steps carried out. Verification included inspection, testing, and static analysis. Action items from inspections were tracked to closure.

5.12 For SIL 3, Entire System Must be validated (Table A.8)

Entire system was validated, however there were a few standard validation tests that were deemed not necessary to run because they were not impacted by any of the changes.

5.13 A modification shall be initiated only on the issue of an authorized software modification request under the procedures specified during safety planning (Part 3, Section 7.8.2.1)

All software changes submitted to the change control system and are authorized by CCT (Change Control Team)

5.14 All modifications which have an impact on the functional safety of the E/E/PE safety-related system shall initiate a return to an appropriate phase of the software safety lifecycle. All subsequent phases shall then be carried out in accordance with the procedures specified for the specific phases in accordance with the requirements in this standard. Safety planning (see clause 6) should detail all subsequent activities (Part 3, Section 7.8.2.5)

The impact analysis documents which phases need to be repeated and the phases are carried out according to standard procedures.

5.15 The safety planning for the modification of safety-related software shall include identification of staff and specification of their required competency. (Part 3, 7.8.2.6a)

Competency forms are on file for all engineers that worked on the project. Identification of staff is included in the PRD system and the ECN system.

5.16 The safety planning for the modification of safety-related software shall include a detailed specification for the modification (Part 3, Section 7.8.2.6b)

A detailed specification of the modification is included in the impact analysis.

5.17 The safety planning for the modification of safety-related software shall include verification planning (Part 3, Section 7.8.2.6c)

Verification planning is included in the impact analysis.

5.18 The safety planning for the modification of safety-related software shall include the scope of re-validation and testing of the modification to the extent required by the safety integrity level. For SIL 3 entire system must be revalidated. (Part 3, Section 7.8.2.6d)

The validation test plan documented exactly which tests would be run. The entire system was revalidated, however there were a few standard validation tests that were deemed not necessary to run because they were not impacted by any of the changes.

5.19 Modification shall be carried out as planned (Part 3, Section 7.8.2.7)

Documentation showed that all of the work was carried out as planned.

5.20 Details of all modifications shall be documented, including references to the modification/retrofit request (Part 3, Section 7.8.2.8a)

The impact analysis references the modification request via the PRD ID (Unique identifier for each software change request)

5.21 Details of all modifications shall be documented, including references to the results of the impact analysis which assesses the impact of the proposed software modification on the functional safety, and the decisions taken with associated justifications; (Part 3, Section 7.8.2.8b)

The impact analysis documentation contains this information.

5.22 Details of all modifications shall be documented, including references to software configuration management history (Part 3, Section 7.8.2.8c)

The software configuration management history is documented and stored in the version control system. By looking at this system on-line, I was able to confirm that the software configuration management history was updated to account for the changes made.

5.23 Details of all modifications shall be documented, including references to deviation from normal operations and conditions (Part 3, Section 7.8.2.8d)

This was documented in the impact analysis.

5.24 Details of all modifications shall be documented, including references to all documented information affected by the modification activity (Part 3, Section 7.8.2.8e)

The impact analysis included a listing of all documents that would be updated based on this change.

5.25 Information (for example a log) on the details of all modifications shall be documented. The documentation shall include the re-verification and revalidation of data and results. (Part 3, Section 7.8.2.9)

Details of all modifications are included in the impact analysis. Documentation exists for re-verification (test reports, inspection reports, and static analysis results) and re-validation (test report).

5.26 The assessment of the required modification or retrofit activity shall be dependent on the results of the impact analysis and the software safety integrity level. (Part 3, Section 7.8.2.10)

The assessment was based on the results of the impact analysis and Rosemount's standard procedures which have been certified to SIL 3 previously.

5.27 Hardware Assessment

To evaluate the hardware design of the 3144P Temperature Tansmitter, a Failure Modes, Effects, and Diagnostic Analysis was performed by exida. This is documented in [R1].

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. 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 3144P. This is listed in the FMEDA reports.

Table 1 Failure rates according to IEC 61508 – 3144P Safety Certified Transmitter with single RTD

Failure Categories	λ_{sd}	λ_{su} [1]	λ_{dd}	λ_{du}	SFF
Low Trip	2311 FIT	112 FIT	28 FIT	59 FIT	97.6%
High Trip	28 FIT	112 FIT	2311 FIT	59 FIT	97.6%

Using Markov modeling, an average Probability of Failure on Demand (PFD_{AVG}) calculation was performed for the 3144P. Summary results for these configurations are shown in Table 2.

Table 2 PFD_{AVG} for the 3144P

Configuration	Device	Proof Test Interval (years)	PFD_{AVG}
1oo1	3144P Safety Certified Temperature Transmitter with single 4 wire RTD	1	2.58E-04
		5	1.29E-03
		10	2.58E-03

For SIL 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year proof test interval of the 3144P temperature transmitter, with a single 4 wire RTD is equal to 2.6% of the range.

The analysis shows that design of the 3144P meets the hardware requirements of IEC 61508, SIL 2 @HFT=0 and SIL 3 @ HFT=1.

[1] It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

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

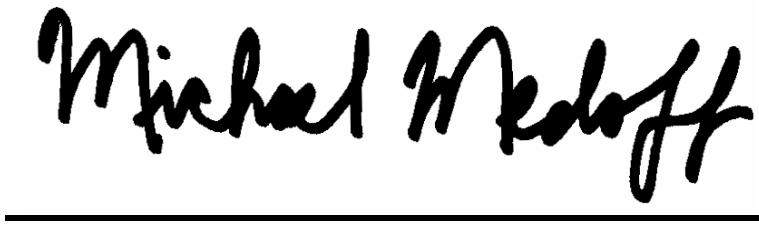
Version:	V1	
Revision:	R1	
Version History:	V0, R1:	Draft sent to Emerson, February 6, 2007
	V1, R1:	Final Version, February 13, 2007
	Review:	V1, R1: Bill Goble, February 13, 2007
Release status:	Draft	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Dr. William M. Goble, Principal Partner



Michael Medoff, Senior Safety Engineer