IEC 61508 Functional Safety Assessment

Project:

DeltaV SIS
DeltaV SIS Relay Module, KJ2231X1- EA1
DeltaV SIS Voltage Monitor, KJ2231X1 – EB1

Customer:

Emerson Process Management
Fisher Rosemount Systems
Austin, TX
USA

Contract No.: Q07/11-05
Report No.: FRS 07-11-05 R002
Version V1, Revision R2, July 1, 2008
Michael Medoff

Management summary

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

- DeltaV SIS
- DeltaV SIS Relay Module, KJ2231X1- EA1
- DeltaV SIS Voltage Monitor, KJ2231X1 – EB1

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.

These products were previously certified to IEC 61508, SIL 3 (See [D10]). Based on this certification, 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.

See section 3 of this document for details on which hardware and software versions have been included in this assessment.

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

The DeltaV SIS, DeltaV SIS Relay Module and DeltaV SIS Voltage Monitor were found to meet the requirements of SIL 3, single use (HFT = 0).

Table of Contents

1 Purpose and Scope

Generally four options exist when doing an assessment of sensors, logic solvers 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 DeltaV SIS, DeltaV SIS Relay Module, and DeltaV SIS Voltage Monitor.

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 DeltaV SIS, DeltaV SIS Relay Module, and DeltaV SIS Voltage Monitor
exida	Performed the IEC 61508 Functional Safety Assessment according to option 4 (see section 1)

Emerson Process Management contracted *exida* in December 2007 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

[D1]	ImpactAnalysis_080318_10_3_SLS.doc	DeltaV SIS Impact Analysis Report	03/27/2008
[D2]	Reduced Status Boolean Design.docx	Design for Reduced Status Booleans	02/15/2008
[D3]	SIS_LSDVC_RevN.xls	DeltaV SIL_LSDVC_Block Test Plan and Results	Rev N
[D4]	HighDensity_ SIS_SLS_Fault_Detection_RevJ.xls	DeltaV SIS_SLS_Fault_Detection Test Plan and Results	Rev J
[D5]	SIS_SLS_Fault_Detection_RevI.xls	DeltaV SIS_SLS_Fault_Detection Test Plan and Results	Rev I

[D6]	SIS_Validation_Blocks_RevO.xls	DeltaV SIS_Validation_Blocks Test Plan and Results	Rev O
[D7]	Incident_90431.txt	Incident Report 90431	4/22/2008
[D9]	SIS_Validation_System_RevL.xls	SIS_Validation_System Test Plan	Rev L
[D10]	FRS 06-05-30 R001	IEC 61508 Functional Safety Assessment Report for DeltaV SIS.	V1R1
[D11]	Incident_90899.txt	Incident Report 90899	4/22/2008
[D12]	Review_3597.pdf	SIS – Reduced Status Boolean Concept Design Review Minutes	1/16/2008
[D13]	Review_3639.pdf	Reduced Status Booleans – SLS Design Review Minutes	2/7/2008
[D14]	Review_3657.pdf	Code Review Minutes	2/18/2008
[D15]	Review_3739.pdf	Software Impact Analysis Review Minutes	3/28/2008
[D16]	V210x_Formal_Module_Tests.docx	Module Test Results	5/21/2008
[D17]	V210x_Informal_Module_Tests.docx	Module Test Results	5/21/2008
[D18]	V210x_Lint_Results	PC Lint Results	3/13/2008
[D19]	ControlDevice_FMT.doc	Module Test Results	2/13/2008
[D20]	ControlIOBlock_FMT.doc	Module Test Results	3/13/2008
[D21]	ControlMsgRouter_FMT.doc	Module Test Results	2/13/2008
[D22]	ControlSecureWrite_FMT.doc	Module Test Results	2/13/2008
[D23]	FMT_DiagSSMonitor.doc	Module Test Results	2/13/2008
[D24]	Review_3657.bmp	Code Review Minutes	2/18/2008
[D25]	DS Delta V SIS – Simulate for SIS enhancements As-built.doc	Direction Statement for release	3/18/2008
[D26]	V2105_SIS_Integration_Test_Results_080424.xls	Integration Test Results	6/6/2008

2.4.2 Documentation generated by *exida*

[R1]	DeltaV Change Audit.xls	Detailed safety case documenting results of assessment (internal document)
[R2]	Emerson 07-11-05 R002 V1 R1 IEC 61508 Assessment.doc	IEC 61508 Functional Safety Assessment, DeltaV SIS (this report)

3 Product Description

The DeltaV SIS SLS1508 is a safety logic solver. The DeltaV SLS1508 is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0. DeltaV SIS Relay Module and DeltaV SIS Voltage Monitor are accessories that can be used with the DeltaV SLS1508 logic solver. The DeltaV SIS Relay Module, and DeltaV SIS Voltage Monitor are classified as Type A[2] devices according to IEC 61508, having a fault tolerance of 0. Fisher-Rosemont Systems, Inc. is the original designer and manufacturer of the DeltaV SIS, DeltaV SIS Relay, and DeltaV SIS Voltage Monitor modules.

3.1 DeltaV SIS Logic Solver

The DeltaV SIS Logic Solver is a compact logic solver that can handle up to 16 I/O channels in any combination of HART AI, HART AO, DI and DO including line fault detection on all I/O. The DeltaV SLS1508 hardware version considered is 4.0 or higher and the software version considered is 2.1.0.5 or higher.

3.2 DeltaV SIS Relay Module

The DeltaV SIS Relay Module (model number KJ2231X1- EA1) is suitable for use in both high and low demand de-energize to trip safety applications, to extend the voltage and current capability of the DeltaV SLS1508 discrete output. It is capable of switching up to 2.5A at 250VAC or 2.5A at 24VDC for safety applications following de-energize to trip conventions by disconnecting field power when de-energized.

Two sets of output switches are provided controlled by one common input. DC Mode of operation is configured to provide two independent sets of DC input power while the AC mode of operation is configured to switch both sides of the AC input power.

The DeltaV SIS Relay Module contains three relays from different manufacturers. A relay coil is energized for all three relays in normal operation. If a demand occurs, the SLS1508 removes the power from the coil for all three relays at the same time. Each relay can be proof tested.

The DeltaV SIS Relay Module hardware revision considered is revision A or higher.

[1] Type B sub(system): "Complex" sub(system) (using microcontrollers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

[2] Type A sub(system): "Non-complex" sub(system) with well defined failure modes; for details see 7.4.3.1.2 of IEC 61508-2

3.3 DeltaV SIS Voltage Monitor

The DeltaV SIS Voltage Monitor (model number KJ2231X1 – EB1) provides two independent sets of voltage monitoring circuitry in one device where each is suitable for use in both high and low demand de-energize to trip applications to extend the voltage input monitoring capability of the SLS1508. It also supplies a secondary output for non-safety critical monitoring for each input.

The state of both outputs for an associated input is controlled by the voltage level of the input with the outputs going to the de-energized state when the input goes below a specified value.

It is designed to be used with DeltaV SLS1508 to drive a logic solver's discrete input channel or a series 2 DI dry contact channel based on the output of the SIS Relay Module. The Voltage Monitor has the following connections:

- Two four pin connection blocks, one for each voltage monitoring channel for connection to DC or AC power source being monitored.
- Two four pin connection blocks , one for each voltage monitoring channel for connecting the output to a SLS monitored DI channel and a DI, dry contact channel.

The DeltaV SIS Voltage Monitor hardware revision considered is revision A or higher.

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 a representative subset 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).

4.2 Assessment level

The DeltaV SIS, DeltaV SIS Relay Module, and DeltaV SIS Voltage Monitor has been assessed per IEC 61508 to Safety Integrity Level 3.

The development procedures have been previously assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL3) according to IEC 61508 (see [D10])

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 remotely in May and June of 2008. Additionally, a detailed safety case was completed. The specific part of 61508 and section number are given in parenthesis for each item below.

A representative subset of 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)

Detailed specifications of all modifications are included in the impact analysis document and in the Issue Tracking Database.

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 an independent document (See [D1]). A listing of all changed software modules is included in the review database (See [D24]).

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

Approvals for all changes are documented in the issue tracking database.

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

Progress of all changes is documented via the change history in the issue tracking database.

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

Integration test cases are documented in the issue tracking database. Validation test cases are documented in the validation test plans.

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 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. For this project, all engineers had been involved in the initial development. The Project Plan documents which fixes will be assigned to each release. The issue tracking system is used to track work assignments. Identical tools to the original development were used.

5.11 Evidence that Change was re-verified (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)

Complete validation test plan was run successfully after the changes were made (See [D3] through [D9])

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 are submitted to the issue tracking system and authorized by the development manager.

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)

This identification of staff is documented in the issue tracking system. Required competency is not specifically documented, but the changes were made by experienced developers from the original development team.

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)

This information was included in the issue tracking system and the impact analysis document.

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

This information was included in the impact analysis document.

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 impact analysis stated that the entire system would be revalidated.

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

Documentation in the issue tracking system 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 issue ID from the issue tracking system (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.

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 and the issue tracking system. Documentation exists for re-verification (test reports, review reports, and static analysis results) and re-validation (test reports).

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 of the modifications was based on the results of the impact analysis

5.27 Hardware Assessment

No hardware changes were made, so no assessment of the hardware is required.

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

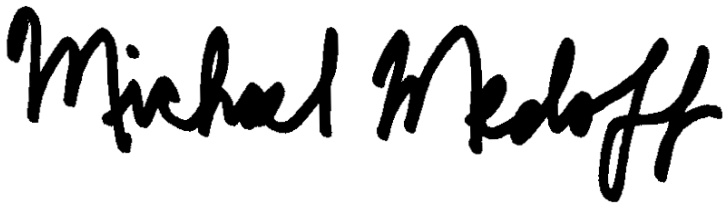
Version:	V1	
Revision:	R2	
Version History:	V1, R2:	Updated HW and SW revision numbers; July 1, 2008
	V1, R1:	Updated based on comments; June 18, 2008
	V0, R1:	Draft; June 9, 2008
Authors:	Michael Medoff	
Review:	V0, R1:	Iwan van Buerden;
Release status:	Released to customer	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Iwan van Buerden, Director of Engineering



Michael Medoff, Senior Safety Engineer