IEC 61508 Functional Safety Assessment

Project:

DeltaV SIS Smart Logic Solver KJ2201X1-BA1
(including SLS Terminal Block KJ2201X1-HA1 or
SLS Redundant Terminal Block KJ2201X1-JA1)
With Accessories:
DeltaV SIS Aux. ETA Relay Module, KJ2231X1- BA1
DeltaV SIS Aux. DTA Relay Module, KJ2231X1- BB1
DeltaV SIS Relay Diode Module, KJ2231X1-BC1
DeltaV SIS Relay Module, KJ2231X1-EA1
DeltaV SIS Voltage Monitor, KJ2231X1 – EB1
DeltaV SIS End of Line Resistance Module, KJ2231X1-EC1
DeltaV SIS RC Compensator Module, KJ2231X1-ED1
DeltaV SIS Current Limiter, KJ2231X1-EE1

Customer:

Fisher Rosemount Systems, Inc.
(an Emerson Automation Solutions company)
Round Rock, TX
USA

Contract No.: Q17/09-207
Report No.: FRS 09-10-23 R001
Version V2, Revision R1, January 8, 2018
Mike Medoff, John Yozallinas

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the DeltaV SIS. The following system components are in the assessment scope:

DeltaV SIS Smart Logic Solver Including: • DeltaV SIS Simplex Terminal Block • DeltaV SIS Redundant Terminal Block	KJ2201X1-BA1 KJ2201X1-HA1 KJ2201X1-JA1
DeltaV SIS Aux. ETA Relay Module	KJ2231X1-BA1
DeltaV SIS Aux. DTA Relay Module	KJ2231X1-BB1
DeltaV SIS Relay Diode Module	KJ2231X1-BC1
DeltaV SIS Relay Module	KJ2201X1-EA1
DeltaV SIS Voltage Monitor	KJ2231X1-EB1
DeltaV SIS End of Line Resistance Module	KJ2231X1-EC1
DeltaV SIS RC Compensator Module	KJ2231X1-ED1
DeltaV SIS Current Limiter	KJ2231X1-EE1

The functional safety assessment was performed to the requirements of IEC 61508:2010, SIL 3. A full IEC 61508 Safety Case was prepared using the *exida* SafetyCaseDB™ tool as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. User documentation (safety manual) was also reviewed.

- *exida* assessed the modifications performed by Fisher Rosemount Systems, Inc. via an audit and review of modification documents and found that there were no new safety-related changes made since the last such audit.

These products were previously certified to IEC 61508:2000, SIL 3. This assessment focused on assessing the product to the differences introduced by IEC 61508:2010. Based on this assessment, it can be concluded that the Emerson development process meets the requirements of IEC 61508:2010 up to SIL 3.

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

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

The DeltaV SIS Smart Logic Solver with its accessories (DeltaV SIS Aux. ETA Relay Module, DeltaV SIS Aux. DTA Relay Module, DeltaV SIS Relay Diode Module, DeltaV SIS Relay Module, DeltaV SIS Voltage Monitor Module, DeltaV SIS End of Line Resistance Module, DeltaV SIS RC Compensator Module, and DeltaV SIS Current Limiter Module) were found to meet the requirements up to SIL 3. Various configurations of equipment may be used in de-energize to trip or energize to trip modes with limitations, as expressed in Table 1. The PFD_{AVG} and Architectural Constraint requirements of the standard must be verified for each element of the Safety Function.

Table 1: Equipment Configurations and SIL limitations

Device(s) and Usage	Configuration	SFF	SIL
DeltaV SIS Safety PLC (DET)	Simplex	> 99%	SIL 3
DeltaV SIS Safety PLC (DET)	Redundant	> 99%	SIL 3
DeltaV SIS Safety PLC (ET with DD failures considered safe)	Simplex	> 99%	SIL 3
DeltaV SIS Safety PLC (ET with DD failures considered safe)	Redundant	> 99%	SIL 3
DeltaV SIS Safety PLC (ET with DD failures considered dangerous)	Simplex	< 60%	---
DeltaV SIS Safety PLC (ET with DD failures considered dangerous)	Redundant	< 60%	SIL 1
DeltaV SIS Safety PLC with auxiliary relay module	Simplex	> 90%	SIL 2
DeltaV SIS Safety PLC with auxiliary relay module	Redundant	> 90%	SIL 2

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 61508:2010 functional safety assessment of the Fisher Rosemount Systems, Inc., by *exida* according to the requirements of IEC 61508:2010.

Table 2 Products and Revisions in Assessment Scope

DeltaV SIS Smart Logic Solver Including: • DeltaV SIS Simplex Terminal Block • DeltaV SIS Redundant Terminal Block	KJ2201X1-BA1 KJ2201X1-HA1 KJ2201X1-JA1	HW Revision 6.23 Rev Z Rev H Rev J
DeltaV SIS Aux. ETA Relay Module	KJ2231X1-BA1	Rev F
DeltaV SIS Aux. DTA Relay Module	KJ2231X1-BB1	Rev F
DeltaV SIS Relay Diode Module	KJ2231X1-BC1	Rev E
DeltaV SIS Relay Module	KJ2201X1-EA1	Rev F
DeltaV SIS Voltage Monitor	KJ2231X1-EB1	Rev F
DeltaV SIS End of Line Resistance Module	KJ2231X1-EC1	Rev G
DeltaV SIS RC Compensator Module	KJ2231X1-ED1	Rev G
DeltaV SIS Current Limiter	KJ2231X1-EE1	Rev E

The versions in Table 2 were current when this report was released (Jan-2018). Earlier versions were covered by prior assessments. For updated versions covered under this certification, contact Fisher Rosemount Systems, Inc. or the Safety Manual which includes the company webpage where the certified versions and compatibility can be checked.

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. See section 6 for Surveillance Audit details.

The following system components can be used as part of the DeltaV SIS and have been shown to be non-interfering:

DeltaV SISNet Repeater (black channel)	KJ2221X1-BA1
DeltaV SIS Carriers	
• Horizontal	KJ2221X1-EA1 KJ4001X1-BA3 KJ4001X1-BE1 KJ4001X1-NA1 KJ4001X1-NB1
• Vertical	KJ4003X1-BA1 KJ4003X1-BB1 KJ4003X1-BC1 KJ4003X1-BG1 KJ4003X1-BD1 KJ4003X1-BF1 KJ4003X1-BE1
• Other	KJ4010X1-BN1
DeltaV SIS Cable Assemblies	
• Horizontal	KJ4002X1-BF3 KJ4002X1-BF2 KJ4002X1-BF4 KJ4002X1-BF5
• Vertical	KJ4003X1-BH2 KJ4003X1-BH1
• SISNet	KJ4010X1-BL2 KJ4010X1-BL1 KJ4010X1-BL3 KJ4010X1-BM2 KJ4010X1-BM1 KJ4010X1-BM3

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

Fisher Rosemount Systems, Inc.	Manufacturer of the DeltaV SIS system
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment

Fisher Rosemount Systems, Inc. contracted *exida* with the IEC 61508 Functional Safety Assessment of the DeltaV SIS system.

2.3 Standards / Literature used

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

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

2.4 Reference documents

2.4.1 Documentation provided by Fisher Rosemount Systems, Inc.

Note 1: the following table contains documents that have been "merged" into this document list (those labeled "D0.xx"). These documents apply to an earlier assessment of the DeltaV SIS system but are retained for completeness and may be supplanted by newer versions of the same document in this list (those labeled "Dxx").

Note 2: DeltaV SIS Documents revised after the 2014 audit are listed in Section 6, 2017 IEC 61508 Functional Safety Surveillance Audit.

[D0.1]	ImpactAnalysis_080318_10_3_SLS.doc	DeltaV SIS Impact Analysis Report	03/27/2008
[D0.2]	Reduced Status Boolean Design.docx	Design for Reduced Status Booleans	02/15/2008

[D0.3]	SIS_LSDVC_RevN.xls	DeltaV SIL_LSDVC_Block Test Plan and Results	Rev N
[D0.4]	HighDensity_ SIS_SLS_Fault_Detection_RevJ.xls	DeltaV SIS_SLS_Fault_Detection Test Plan and Results	Rev J
[D0.5]	SIS_SLS_Fault_Detection_RevI.xls	DeltaV SIS_SLS_Fault_Detection Test Plan and Results	Rev I
[D0.6]	SIS_Validation_Blocks_RevO.xls	DeltaV SIS_Validation_Blocks Test Plan and Results	Rev O
[D0.7]	Incident_90431.txt	Incident Report 90431	4/22/2008
[D0.9]	SIS_Validation_System_RevL.xls	SIS_Validation_System Test Plan	Rev L
[D0.11]	Incident_90899.txt	Incident Report 90899	4/22/2008
[D0.12]	Review_3597.pdf	SIS – Reduced Status Boolean Concept Design Review Minutes	1/16/2008
[D0.13]	Review_3639.pdf	Reduced Status Booleans – SLS Design Review Minutes	2/7/2008
[D0.14]	Review_3657.pdf	Code Review Minutes	2/18/2008
[D0.15]	Review_3739.pdf	Software Impact Analysis Review Minutes	3/28/2008
[D0.16]	V210x_Formal_Module_Tests.docx	Module Test Results	5/21/2008
[D0.17]	V210x_Informal_Module_Tests.docx	Module Test Results	5/21/2008
[D0.18]	V210x_Lint_Results	PC Lint Results	3/13/2008
[D0.19]	ControlDevice_FMT.doc	Module Test Results	2/13/2008
[D0.20]	ControlIOBlock_FMT.doc	Module Test Results	3/13/2008
[D0.21]	ControlMsgRouter_FMT.doc	Module Test Results	2/13/2008
[D0.22]	ControlSecureWrite_FMT.doc	Module Test Results	2/13/2008
[D0.23]	FMT_DiagSSMonitor.doc	Module Test Results	2/13/2008
[D0.24]	Review_3657.bmp	Code Review Minutes	2/18/2008
[D0.25]	DS Delta V SIS – Simulate for SIS enhancements As-built.doc	Direction Statement for release	3/18/2008
[D0.26]	V2105_SIS_Integration_Test_Results_080424.xls	Integration Test Results	6/6/2008
[D1]	Emerson SLS 1508 v3.2.0.8 Documentation Package	List of all documents for 2011 changes	09/25/2011

[D2]	DSLogicSolverMaintenance.pdf	Logic Solver Maintenance Direction Statement	09/23/2011
[D3]	V12_LogicSolverMaintence.pdf	DeltaV Technology V12 Logic Solver Maintenance	06-Dec-2010
[D4]	DeltaV SIS Safety Manual_2011.pdf	DeltaV SIS Process Safety System Safety Manual, D800032X012	May 2011
[D5]	DeltaV SIS Safety Manual UG_2011.pdf	DeltaV SIS Process Safety System Users Guide, D800033X012	February 2011
[D6]	ImpactAnalysis_110916_LogicSolverMaintenance_Enhancements.pdf	Impact analysis report over the new product enhancement changes.	09/25/2011
[D7]	Impact analysis report over the new product enhancement changes.	Impact analysis report over the new product bug fixes	4/22/2008
[D9]	Module Test / v320x_SLS_Formal_Module_Tests.pdf	Overview of formal module test	09/25/2011
[D11]	Module Test / v320x_SLS_Informal_Module_Tests.pdf	Overview of informal module test	09/25/2011
[D12]	Module Test Reports	Reports on Formal and Informal Module Testing	Various
[D13]	Review_4791.pdf	Concept/Design Review	09/25/2011
[D14]	Review_4814.pdf	Code Review	09/25/2011
[D15]	Review_4947.pdf	Code Review	09/25/2011
[D16]	Review 5143.pdf	Code Review	09/25/2011
[D17]	LINT / v320x_SLS_Lint_Results.txt	SLS v3.2 LINT results	09/25/2011
[D18]	System Validation Test Results	Reports on System Validation Testing	09/25/2011
[D19]	Incident Reports	Detail reports on incidents	09/25/2011
[D20]	ECRN #_ 22014.pdf	EC 22014	03/13/2013
[D21]	DeltaV_SIS_Impact_Analysis_Report-ECRN 22014.doc	Impact analysis for EC22014	04/22/2013
[D22]	ECRN #_ 22174.pdf	EC 22174	09/03/2013
[D23]	ImpactAnalysis_ECRN_22174.docx	Impact analysis for EC22714	09/13/2013

2.4.2 Documentation generated by *exida*

Note: Documents revised by *exida* after the 2014 audit are listed in Section 6, 2017 IEC 61508 Functional Safety Surveillance Audit.

[R0.10]	FRS 06-05-30 R001	IEC 61508 Functional Safety Assessment Report for DeltaV SIS.	V1R1
[R1]	SafetyCase.esc	DeltaV SIS SafetyCaseDB	Jan.2013
[R2]	FRS 09-10-23 R001 V2 R0 IEC 61508 Assessment.doc	IEC 61508 Functional Safety Assessment for DeltaV SIS (IEC 61508:2010)	V2R0
[R3]	Emerson 09-10-23 V1R0 2010 Gap Assessment .xlsx	2010 Gap Assessment	V1R0
[R4]	Emerson 09-10-23 V1R0 Field Failure Analysis.xls	Comparison of predicted versus actual failure rates	V1R0

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 61508:2010, with an advanced, hybrid architecture. The DeltaV SIS Aux. Relay Modules, DeltaV SIS Relay Diode Module, DeltaV SIS Relay Module, DeltaV SIS Voltage Monitor, DeltaV SIS End of Line Resistance Module, DeltaV SIS RC Compensator Module and DeltaV SIS Current Limiter are accessories that can be used with the DeltaV SLS1508 logic solver. These accessories are classified as Type A[2] devices according to IEC 61508:2010. Fisher-Rosemont Systems, Inc. is the original designer and manufacturer of these 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 3.2.0.8 or higher.

3.2 DeltaV SIS Aux. Relay Modules

The DeltaV SIS Aux Relay Modules are suitable for use in both high and low demand safety applications, to extend the voltage and current capability of the DeltaV SLS1508 discrete output and to provide logic inversion for energize to trip applications. The modules are capable of switching up to 2.5A at 250VAC or 2.5A at 24VDC for safety applications.

3.3 DeltaV SIS Voltage Monitor

The DeltaV SIS Voltage Monitor 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.

[1] Type B sub(system): "Complex" elements (using microcontrollers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
[2] Type A sub(system): "Non-complex" elements with well-defined failure modes; for details see 7.4.4.1.2 of IEC 61508-2

3.4 DeltaV SIS Relay Module

The DeltaV SIS Relay Module 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.

3.5 DeltaV SIS End of Line Resistance Module

The Discrete Input channels have line fault detection for detecting open or short circuits in field wiring. The End of Line Resistance Module provides a 12 KΩ resistor in parallel (allows the open circuit detection) and a 2.4 KΩ resistor in series (allows short circuit detection) to provide the appropriate resistance for line fault detection.

3.6 DeltaV SIS RC Compensator Module

When using line monitoring on outputs that are driving inductive loads greater than or equal to 0.8 Henry in simplex or 0.3 Henry in redundant, an RC compensator may be required.

3.7 DeltaV SIS Current Limiter

The SIS Current Limiter limits the current from the SLS Discrete Output channels to levels below the ignition curves for Class 1 Div 2 and Zone 2 installations.

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Fisher Rosemount Systems, Inc. and is documented in the safety case database [R1].

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).

Additional and modified requirements in IEC 61508:2010, as compared with IEC 61508:2000, were identified and used to assess the DeltaV SIS per [R3].

4.2 Assessment level

The DeltaV SIS, DeltaV SIS Aux. Relay Modules, DeltaV SIS Voltage Monitor, DeltaV SIS Current Limiter, DeltaV SIS RC Compensator Module and DeltaV SIS End of Line Resistance Module have been assessed per IEC 61508 to the following levels:

- Systematic Capability: SIL 3 capable
- Random Capability: 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 61508:2010.

4.3 Product Modifications

Fisher Rosemount Systems, Inc. may make modifications to this product as needed, provided that:

- A competent person from Fisher Rosemount Systems, Inc., appointed and agreed with *exida*, judges and approves the modifications. The Emerson Process Systems and Solutions FSMT (Functional Safety Management Team) is currently approved by *exida* to fulfill this role.
- The modification documentation listed below is submitted prior to a renewal of the certification to *exida* for review of the decisions made by the competent person in respect to the modifications made.
    - List of all anomalies reported
    - 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
    - List of modified documentation
    - Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Fisher Rosemount Systems, Inc. during product development against the objectives of IEC 61508 parts 1, 2, and 3, see [N1]. The development of the DeltaV SIS was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Fisher Rosemount Systems, Inc. has an IEC 61508 compliant development process as assessed during prior IEC 61508 certification. This compliant development process is documented in [D01].

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 Modifications

exida assessed the changes made by Emerson for this and previous developments against the modification procedures of IEC 61508 parts 2 and 3 during the 2014 surveillance audit.

A representative subset of all changes was successfully reviewed against the following criteria from IEC 61508. The section number from IEC 61508 is provided in parenthesis.

5.1.1.1 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.

5.1.1.2 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 multiple independent documents (See [D6] and [D7]).

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

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

5.1.1.4 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.

5.1.1.5 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.

5.1.1.6 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.

5.1.1.7 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

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

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

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

All necessary documentation changes are included in the impact analysis

5.1.1.10 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)

For this project, 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.

5.1.1.11 Evidence that Change was re-verified (Part 2, Section 7.8.2.4)

All changes had appropriate verification steps carried out. Verification included inspection (See [D13], [D14], [D15], and [D16]), testing (See [D11]. [D12], and [D18]), and static analysis (See [D17]). Action items from inspections were tracked to closure.

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

A validation test plan was run successfully after the changes were made (See [D18]) for all impacted systems.

5.1.1.13 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 7.8.2.2)

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

5.1.1.14 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.

5.1.1.15 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.

5.1.1.16 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.

5.1.1.17 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.

5.1.1.18 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.

5.1.1.19 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.

5.1.1.20 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).

5.1.1.21 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.

5.1.1.22 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.

5.1.1.23 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.

5.1.1.24 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.

5.1.1.25 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).

5.1.1.26 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 analyses.

5.2 Hardware Assessment

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

6 2017 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Fisher Rosemount Systems, Inc.	Manufacturer of the DeltaV SIS
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Fisher Rosemount Systems, Inc. contracted *exida* in October 2017 to perform the surveillance audit for the DeltaV SIS. This surveillance audit was conducted remotely.

6.2 Surveillance Methodology

As part of the IEC 61508 functional safety surveillance audit the following aspects have been 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 any of the changes could affect the safety function of the DeltaV SIS.
- 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 latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- 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 Fisher Rosemount Systems, Inc.

[D100]	PSS ISO 9001_2015 Certificate_Current.pdf, Oct.2017	ISO 9001 certification update
[D101]	ECRN 22640.pdf, May.2016	WatchDog Timer function change
[D102]	Impact Analysis ECRN 22640 Updated.pdf, Apr.2016	Impact Analysis for WatchDog Timer change
[D103]	SLS WWD Test Report Signed.pdf, Apr.2016	WatchDog Timer voltage trip test report
[D104]	SLS WWD Test Plan.pdf, 14-Oct-2015	WatchDog Timer voltage trip test plan
[D105]	ImpactAnalysis_160608_incident_282964.docx	Change in HART command operation for universal reads
[D106]	Exida SIS Certification.xlsx, Nov.2017	Field Failure and Shipping History, 2014-2017
[D107]	TFS-screenshot2.png, Nov.2017	Source Code Changeset for incident #282964
[D108]	SIS_Validation_System_RevP.xls, Mar.2016	System Validation Test Plan and Results
[D109]	SIS_Validation_Blocks_RevW.xls, Mar.2016	Function Blocks Validation Test Plan and Results
[D110]	SIS_SLS_Fault_Detection_RevK_PLD.xls, Feb.2017	SLS Fault Detection Test Plan and Results
[D111]	SIS_SLS_Fault_Detection_RevK_SafetyCriticalFaults.xls, Feb.2017	SLS Safety Faults Test Plan and Results
[D112]	Hotfix_90287_Review.png, Jun.2016	Code Review Record for SW Change
[D113]	v332x_SLS_Lint_Results.txt, Jun.2016	Static Analysis Results

6.2.2 Surveillance Documentation generated by *exida*

[R5]	FRS 17-09-207 V1R1 Change Audit_Checklist.xls, Jan.2018	IEC 61508 Change Audit Report for DeltaV SIS
[R6]	FRS 17-09-207 R001 V2R0 DeltaV SIS FieldFailureAnalysis.xlsx, Nov.2017	Field History Analysis for DeltaV SIS
[R7]	FRS 04-09-22 R001 V3 R7 FMEDA DeltaV SIS.pdf, Mar.2015	FMEDA Report for DeltaV SIS (former report)

6.3 Surveillance Results

See Section 1 for a summary of the latest DeltaV SIS system hardware versions. The latest DeltaV SIS software version for the Logic Solver is v3.3.2.

6.3.1 Procedure Changes

As part of ongoing process improvements, the Review DataBase was replaced and now uses Code Collaborator to review Impact Analyses.

To facilitate modifications to these DeltaV SIS components, the top-level assembly was removed from the automatic “approval required” list. The “approval required” list now focuses on lower levels of these components (the Schematic and PWA).

These Procedure Changes were reviewed and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period. Several ECRNs for minor changes and enhancements were reviewed and all documentation was found to be acceptable.

6.3.3 Impact Analysis

There were no safety-related design changes during the previous certification period., but all non-safety changes had appropriate impact analysis and reviews.

6.3.4 Field History

The field histories of these products were analyzed and found to be consistent with the failure rates predicted by the FMEDA. Failure analysis and field return processes continue to comply with IEC 61508.

6.3.5 Safety Manual

The safety manual was not updated but was reviewed and found to be compliant with IEC 61508:2010.

6.3.6 FMEDA Update

The FMEDA was not updated as part of this surveillance audit but the current report is listed above [R7]. There were no hardware changes that would make a significant difference in the current FMEDA results.

6.3.7 Evaluate use of certificate and/or certification mark

The Fisher Rosemount Systems, Inc. website was searched and no misleading or misuse of the certification or certification marks was found.

6.3.8 Previous Recommendations

There were no previous recommendations or action items to be assessed at this audit.

7 Terms and Definitions

ECRN	Engineering Change Request Notice
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
PWA	Printed Wiring Assembly
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 Releases

Version:	V2	
Revision:	R1	
Version History:	V2, R1:	updated per surveillance audit and internal review; JCY, 8-Jan-2018
	V2, R0:	Updated assessment to IEC 61508:2010; D. Butler, 17 January 2014. Note that the Safety Relay Module has been added into this assessment report, rather than maintaining a separate report for it and the Voltage Monitor Module.
	V1, R3:	Added Conditioning Components- Current Limiter, RC Compensator, End of Line Resistance Module; Griff Francis, 8 November 2013
	V0, R1:	Draft; April 22, 2010
Authors:	Michael Medoff, William Goble, John Yozallinas	
Review:	V1, R2:	William Goble
	V2, R1:	Ted Stewart
Release status:	released	

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Ted Stewart, CFSP, Program Development & Compliance Manager

John Yozallinas, CFSE, Senior Safety Engineer