



Results of the IEC 61508 Functional Safety Assessment

Project:
Rosemount 8800D Vortex Flowmeter with
HART (4-20 mA) and "SI" option

Customer:
Emerson
Eden Prairie, MN - USA

Contract No.: Q20-01-099
Report No.: EMM 16-12-042 R001
Version V2, Revision R1, September 25, 2020
Dave Butler

Management Summary

The Functional Safety Assessment of the

Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option

performed by *exida*, consisted of the following activities:

- *exida* assessed the systematic capability through a detailed analysis of Proven-In-Use data provided by Emerson and the creation of a detailed safety case against the requirements of IEC 61508.
- *exida* reviewed and assessed the random capability through a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to ensure that the FMEDA analysis was complete.

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Hardware and software process requirements and all associated design documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were reviewed.

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

The audited development process, as tailored and implemented by the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option development project, complies with the relevant safety management requirements of IEC 61508 up to SIL 3.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option can be used in a low demand safety related system in a manner where the PFD_{AVG} is within the allowed range up to SIL 3 (HFT = 1) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 low demand safety function (with HFT = 0), a SIL 2 high demand safety function (with HFT=1), or a SIL 3 safety function (with HFT = 1).

This means that the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option is capable for use in SIL 2 and SIL 3 applications when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.

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





Table of Contents

Management Summary	2
1 Purpose and Scope	5
1.1 Tools and Methods used for the assessment	5
2 Project Management	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved	6
2.3 Standards / Literature used	6
2.4 Reference documents	6
2.4.1 Documentation provided by Emerson	6
2.4.2 Documentation generated by <i>exida</i>	8
2.5 Assessment Approach	8
3 Product Description	10
3.1 Hardware and Software Version Numbers	10
4 IEC 61508 Functional Safety Assessment Scheme	11
4.1 Product Modifications	11
5 Results of the IEC 61508 Functional Safety Assessment	12
5.1 Lifecycle Activities and Fault Avoidance Measures	12
5.1.1 Safety Lifecycle and Functional Safety Management Planning	12
5.1.2 Tools (and languages)	13
5.1.3 Safety Requirement Specification and System Architecture Design	14
5.1.4 Change and modification management	14
5.1.5 Proven-In-Use	15
5.2 Software Design and Verification	15
5.2.1 Safety Validation	16
5.3 Hardware Design and Verification	16
5.3.1 Hardware Architecture Design and Probabilistic Properties	17
5.4 Safety Manual	17
6 2020 IEC 61508 Functional Safety Surveillance Audit	19
6.1 Roles of the parties involved	19
6.2 Surveillance Methodology	19
6.2.1 Documentation provided by Emerson	20
6.2.2 Surveillance Documentation generated by <i>exida</i>	21
6.3 Surveillance Results	21
6.3.1 Procedure Changes	21



6.3.2	Engineering Changes	21
6.3.3	Impact Analysis.....	21
6.3.4	Field History	21
6.3.5	Safety Manual.....	21
6.3.6	FMEDA Update.....	21
6.3.7	Evaluate use of certificate and/or certification mark	22
6.3.8	Previous Recommendations	22
6.4	Surveillance Audit Conclusion.....	22
7	Terms and Definitions	23
8	Status of the document.....	24
8.1	Liability	24
8.2	Version History	24
8.3	Future Enhancements	24
8.4	Release Signatures	24



1 Purpose and Scope

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

- Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option

by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508:2010. Throughout this report, the product is also known as the “**8800D Vortex Flowmeter.**”

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

- the 8800D Vortex Flowmeter with the technical requirements of IEC 61508, parts 2 and 3, for SIL 3 and the derived product safety property requirements;

and

- the 8800D Vortex Flowmeter development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial requirements of IEC 61508 parts 1, 2 and 3 for SIL 3;

and

- the 8800D Vortex Flowmeter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been performed based on the quality procedures and scope definitions of *exida*.

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

1.1 Tools and Methods used for the assessment

This assessment was performed by using the *exida* Safety Case tool. The Safety Case tool contains the accredited *exida* certification scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

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



2 Project Management

2.1 exida

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 350 billion hours of field failure data.

2.2 Roles of the parties involved

Emerson	Manufacturer of the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option
<i>exida</i>	Performed the hardware assessment [R3]
<i>exida</i>	Performed the Functional Safety Assessment [R1] per the accredited <i>exida</i> certification scheme.

Emerson 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 61508:2010 (Parts 1 – 7):	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
------	----------------------------------	---

2.4 Reference documents

2.4.1 Documentation provided by Emerson

Doc. ID	Project Document Filename	Version
D001	QM 001 Quality Manual Rev C.pdf	C
D003	D003-021 Product Design And Development Process.docx	6
D003b	OP 0415 Product Design and Development Process.docx	B
D004	D004 Configuration and Change Management Work Instruction.docx	7
D005	OP 0830 Product Analysis Process.docx	A
D007	GW1 380 Supplier Quality Manual.docx	K
D010	OP 0210 Quality System Procedure.docx	C
D012	OP 1310 Receiving Inspection Nonconforming Material Control.docx	A
D012b	OP 1320 In-Process Nonconforming Material Control.docx	B
D013	OP 0850 Corrective and Preventive Action.docx	A
D016	D016 Peer Review Work Instruction.docx	8
D019	OP 0834 Customer Notification Process.docx	A
D023	OP 0440 Engineering Change Order.docx	B
D023b	D023b Safety Impact Analysis (SIA) Form.xlsx	A



Doc. ID	Project Document Filename	Version
D026	D026 Project Plan - VA.1signed.pdf	A.1
D027	D027 phoenixSCMP.doc	A
D030	8800Raw.xlsx	Sept.2015
D030b	D030b 8800D_HART Shipments_201509_thru_201705.xlsx	June.2017
D031	8800FieldHistory_jcy.xlsx	Sept.2015
D031b	D031 8800D_HART Failures_201509_thru_201706.xlsx	Jul.2017
D032	Competence Folders	May.2017
D033	D033-34 Training_Competency_Safety_20170501.xlsx	May.2017
D036	ISO 9001 2015 Certificate Eden Prairie.pdf	Jul.2017
D040	D040 SRD Vortex 8800D v3.4a .pdf	v3.4a
D041	D041 SRD Vortex 8800D Peer Review Inspection Report and Consolidated Log.xlsx	3.1
D041b	D041b Vortex_SRD_v3.4a_Safety_Reqs_Checklist.xls	3.4
D043	D043 SRS Vortex 8800D v4.2a .pdf	v4.2a
D045	D045 System Architecture Design Specification.pdf	A.4
D048	D048 VortexHdwrChangesApr2016thruJun2017.xlsx	Jun.2017
D049	SoftwareArchitecture_and_DesignModels.pdf	A.4
D051	class_hostproc_diagrams.pdf	A.3
D051b	class_coproc_diagrams.pdf	A.2
D053	D053 System & Software Architecture Peer Review.xlsm	1
D053b	D053 Vortex_SRS_v4.2a_Safety_Reqs_Checklist.xls	4.2
D053c	D053 SRS Vortex 8800D Peer Review Inspection Report and Consolidated Log.xlsm	4
D056	SRD_to_SRS_to_Software_requirements_traceability.pdf	Sep.2017
D056b	SRS_to_Software_Design_Traceability.pdf	Sep.2017
D058	D058 CodeReview_8800D_mega2561Port.xlsx	Sep.2017
D058b	D058 Peer Review Inspection Report and Consolidated Log Form.xlsm	Sep.2017
D060	D060 87x2D_Coding_Std061410.doc	4
D061	D062 Phoenix128_rep.html	May.2017
D062	D061-62_Phoenix2561_rep.html	May.2017
D063	D063_Phoenix2561_rep_updated.html	May.2017
D063b	D063_Notes.txt	July.2017
D069	D069 Vortex_8800_SVTP_rev1.0a.docx	1.0a
D070	D070 SVTP_PeerReviewInspectionReportandConsolidatedLog.xlsm	0.1
D071	Team_Reviewed_8800D_thunderbird_dvt_plan_20141120.doc	A
D071b	D071-072 8800D_phoenix_dvt_plan.doc	1.4
D074	ValTest Folder	Aug.2017
D074b	Equipment_list.xlsx	Sep.2017
D074c	SSTG_Test_Report_Vortex 8800D_Phoenix Software 5.2.8 Standard Verification.htm	Jun.2017
D075	VT-ID09_Report.docx	Aug.2017
D075b	Vib_report_DVT1.pdf	Jan.2005
D075c	HSGTEMP.xls	Aug.2008
D076	D076 EMC_Report_8800D_RevA.doc	A
D077	Fault Injection Test Results	May.2017
D078	8800D_Manual_00809-0100-4004rev DC.pdf	DC
D079	00809-02xx-4004.pdf	AA
D080	D080 SafetyManualChecklist.docx	Aug.2017
D081	ECO_1061393_Example_SIL_Impact_Analysis.pdf	Sep.2017
D085	D085 8800D_mega2561Port.xlsx	Apr.2017
D085b	D085b 8600D_mega2561Port.xlsx	Apr.2017
D086	D086 VortexSW_Tool_Analysis.pdf	A.1
D088	D029 8800 Hart Safety Impact Analysis (SIA).xlsx	Sep.2017



2.4.2 Documentation generated by *exida*

[R1]	EMM 8800D V2R4 SIL3 SafetyCaseWB-61508 v1.7.3d, Sep.2017	SafetyCase file for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option
[R2]	EMM 16-12-042 R001 V1R2, Oct.2017	IEC 61508 Functional Safety Assessment for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option (This document)
[R3]	ROS 06-03-34 R001 V3R5 FMEDA 8800D.pdf, Sep.2017	FMEDA report for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option
[R4]	EMM Vortex 8800 R3 PIU Spreadsheet.xlsx, Sep.2017	PIU Analysis Report for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option

2.5 Assessment Approach

The certification audit was closely driven by requirements of the accredited *exida* certification scheme which includes subsets filtered from IEC 61508. The assessment was planned by *exida* and agreed with Emerson.

For designs that have been in service for several years and have demonstrated themselves in a variety of applications and conditions, consideration of a Prove-in-Use assessment may be used as a substitute if a product didn't follow a fully compliant IEC 61508 design process. The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during any hardware and software modifications needed to achieve SIL 3 capability for the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option. Other product development aspects prior to these modifications were assessed according to Proven-In-Use (PIU) requirements (see section 5.1.5). The combination of these assessments 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.

As part of the IEC 61508 functional safety assessment for the 8800D Vortex Flowmeter, the following evidence aspects have been reviewed:

- FMEDA
- SRS or product specification
- Safety manual
- Instruction manual
- Hardware fault inject test plan and results verification
- Software architecture design specification
- EMC and environmental test report
- Validation test results
- Corrective Action and prevention action plan/process
- Software and hardware drawings release process
- PIU data collection procedures and operational excellence calculation/report (evidence that the equipment is Proven-In-Use; analysis of field failure rates to ensure that no systematic faults exist in the product)



Several ASICs are used in this product and ASIC development processes are in place. They have been considered to meet the PIU requirements used for the 8800D Vortex Flowmeter and have been considered as Route 2H compliant per the *exida* certification scheme.

No safety related communications are used in this product.

PIU assessment provides for the prevention of systematic failures for pre-existing devices with a proven history of successful operation. As part of the PIU assessment for the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option, some IEC 61508 functional safety assessment requirements are satisfied without further documented evidence:

- Integration and Unit test plans
- Software Coding Standard

The project teams, not individuals, were audited.

3 Product Description



The Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option consists of a meter body and transmitter, and measures volumetric flow rate by detecting the vortices created by a fluid passing by the shedder bar. The meter body is installed in-line with process piping. A sensor is located at the end of the shedder bar which creates a sine wave signal due to the passing vortices. The flowmeter measures the frequency of the sine wave and converts it into a flowrate. The 8800D is available as a dual assembly which consists of two independent flowmeters designed into a single unit. The 8800D is also available as a quad assembly which consists of four independent flowmeters designed into a single unit. For functional safety applications, only the 4 – 20 mA analog output is used as the safety variable. The pulse output may be used for non-safety applications. The analog output may be configured to meet NAMUR NE 43 (3.8 mA to 20.5 mA usable range). The system contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. High trip or Low trip options can be configured. A Logic Solver connecting to the 8800D Vortex Flowmeter must be programmed to monitor the analog output for out of range values.

3.1 Hardware and Software Version Numbers

The versions listed in Table 1 were current when this report was released. For updated versions covered under this certification, refer to the Safety Manual which includes the company webpage where the certified versions and compatibility can be checked.

Table 1: Product Versions

8800D Vortex Flowmeter	Display tag	Safety certified version combinations		
		1	2	3
Firmware	Universal revision	5	5	7
	Transmitter revision	2	3	2
	Software revision	8	4	4
Hardware	Hardware revision	1	2	2



4 IEC 61508 Functional Safety Assessment Scheme

The assessment was executed using the accredited *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team. The assessment was performed based on the information received from Emerson [section 2.4.1] and is documented in the safety case [R1].

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Emerson may make modifications to this product as needed. Modifications that affect the safety functions shall first be reviewed with *exida* prior to release of the modifications.

As part of the accredited *exida* certification 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(s) 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 a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R3] of the 8800D Vortex Flowmeter to document the hardware architecture and failure behavior. The FMEDA report and the Safety Case created for the 8800D Vortex Flowmeter documents this assessment.

exida assessed failure history of the 8800D Vortex Flowmeter [D030, D031] and performed a detailed analysis of the data provided [R4]. This PIU assessment is done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the 8800D Vortex Flowmeter documents this assessment.

The result of the overall assessment can be summarized by the following observations:

The Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option complies with the relevant requirements of IEC 61508 up to SIL 3 applications when considering PIU and when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

5.1 Lifecycle Activities and Fault Avoidance Measures

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team and supported by PIU analysis.

5.1.1 Safety Lifecycle and Functional Safety Management Planning

Objectives

- Structure, in a systematic manner, the phases in the overall and the E/E/PE safety lifecycles that shall be considered to achieve the required functional safety of the E/E/PE safety-related systems.
- Specify the management and technical activities during the overall, E/E/PE and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.
 - Specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PE and software safety lifecycle phase or for activities within each phase.
 - Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
 - Specify the necessary information to be documented in order that all phases of the overall, E/E/PE, and software safety lifecycles can be effectively performed.
 - Document and record all information relevant to the functional safety of the E/E/PE throughout the overall and the E/E/PE safety lifecycles.
 - Select a suitable set of tools for the required safety integrity level, over the whole safety lifecycle, which assists verification, validation, assessment and modification.



Assessment

FSM Plan

An FSM plan [D026] exists to document key areas of functional safety management and act as guidance for future modifications. It identifies the safety lifecycle, competencies and responsibilities of personnel, key safety activities, deliverables, and measures to be used, and software tools.

Documentation, Version Control and Configuration Management

All documents are under version control as required by [D001 and D010]. Configuration Management practices are handled in the FSM plan [D026] and CM plan [D027]. Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

A Modification Procedure [D023] exists that identifies how a modification request is initiated and processed to authorize a Product Modification Request (including hardware and software modifications). A Product Modification Request System exists to support this process.

Emerson has a QMS in place and has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure [D007].

Training and competence recording

The FSM Plan refers to the key people working on the project along with their roles. A competency matrix has been created and includes the following:

- a) Competency requirements for each role on project.
- b) List of people who fulfill each role
- c) List of individual competencies matched to required competencies based on roles that they fill.

Conclusion

The objectives of the standard are fulfilled by the Emerson functional safety management system, internal organizational procedures, product change management processes, and safety lifecycle processes and supported by PIU analysis.

5.1.2 Tools (and languages)

Assessment

All tools which support a phase of the software development lifecycle, and cannot directly influence the safety-related system during its run time (off-line support tools) are documented, including tool name, manufacturer name, version number, use of the tool on this project. This includes validation test tools. All off-line support tools in classes T2 and T3 have a specification or product manual which clearly defines the behavior of the tool and any instructions or constraints on its use. Although PIU covers this, a tool fault analysis [D086] was also performed.

Conclusion

The objectives of the standard are fulfilled by the Emerson internal organizational procedures and functional safety management system processes and supported by PIU analysis.



5.1.3 Safety Requirement Specification and System Architecture Design

Objectives

- Specify the requirements for each E/E/PE system, in terms of the required safety functions and the required safety integrity, to achieve the required functional safety.
- Specify the system architecture design.
- Specify traceability for safety requirements

Assessment

All element safety functions necessary to achieve the required functional safety are specified [D040, D043], including:

- a) functions that enable the equipment under control to achieve or maintain a safe state;
- b) functions related to the detection, annunciation and management of sensor faults;
- c) functions that allow the programmable safety instrumented system to be safely modified;
- d) start-up and restart procedures.

The Safety Requirements and System Architecture Design Review Records [D041, D053b] show support for appropriate design methods. System design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented.

Conclusion

The objectives of the standard are fulfilled by the Emerson functional safety management system and use of requirements management tools and supported by PIU analysis.

5.1.4 Change and modification management

Objectives

- Ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

Assessment

Modifications are initiated with an Engineering Design Change procedure [D023]. Modification Request/Records will document the reason for the change and have a detailed description of the proposed change. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process.

The modification process has been successfully assessed and audited, so Emerson may make modifications to this product as needed. Modifications that affect the safety functions shall first be reviewed with *exida* prior to release of the modifications. An impact analysis [D023b] is performed for any change related to functional safety.

Conclusion

The objectives of the standard are fulfilled by the Emerson functional safety management system, change management procedures, and sustaining product procedures.

5.1.5 Proven-In-Use

In addition to the Design Fault avoidance techniques listed above, a Proven-in-Use evaluation was performed on the 8800D Vortex Flowmeter. Shipment records were used to determine that the 8800D Vortex Flowmeter has greater than 400 million operating hours and has demonstrated a field failure rate less than the predicted failure rates indicated in the FMEDA reports. All components considered in the FMEDA have greater than 100 million operating hours, and diagnostic coverage is shown to be greater than 60% (see [R3] and [R5]). This provides justification for using a Route 2H approach.

Conclusion

The objectives of the standard for Proven-In-Use for SIL 3 are fulfilled by the Emerson field history and return procedures and supported by PIU analysis.

5.2 Software Design and Verification

Objectives

- Create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level.
- Review and evaluate the requirements placed on the software by the hardware architecture of the E/E/PE safety-related system, including the significance of E/E/PE hardware/software interactions for safety of the equipment under control.
- Design and implement software that fulfils the specified software safety requirements with respect to the required safety integrity level, which is analyzable and verifiable, and which is capable of being safely modified.
- To the extent required by the safety integrity level, test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.
- Verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved.

Assessment

The 8800D Vortex Flowmeter Software Architecture Design [D049] contains a description of the software architecture. The design is partitioned into new, modified, or unchanged components and modules. All components described in the architecture are treated as PIU in this release. The design documents list all components along with their criticality (Safety Critical, Safety Related, or Non-Interfering) which indicates their required Systematic Capability. PIU supports this requirement. Semi-formal methods are used to describe the software design. All software components listed in the Software Architecture Design have corresponding Software Designs [D051, D051b] which further partition the design into software modules. The Software Design describes the diagnostics required to detect faults. Formal design reviews [D053, D053c] are held and the results are recorded; action items are identified, assigned, and resolved. Review notes are also included in the design specification history.



Conclusion

The objectives of the standard are fulfilled by the Emerson functional safety management system, internal organizational procedures, software development process, and new product development processes and supported by PIU analysis.

5.2.1 Safety Validation

Objectives

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.
- Validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

Assessment

One or more test cases, or analysis documents, exist for each 8800D Vortex Flowmeter safety requirement (including software safety requirements) as shown by the requirements traceability matrix [D056, D069]. Each test case includes the test objective and pass/fail criteria for the test (inputs, outputs and any other acceptance criteria). The validation test plan [D069] includes the procedure used to properly judge whether the validation test is successful. Dynamic (runtime) analysis/testing was planned and performed in addition to static analysis/testing.

Test results are documented [D074, D074c, D075, D076], including references to the test case and test plan version being executed. Test failures were documented in the test results with references to the change request made for the fix. The analysis of the problem is documented in the change request system. Test tools and test equipment are recorded as part of the test results.

Fault injection testing was planned and performed by Emerson. The results have been analyzed and adjustments have been made to the FMEDA based on these results [D077].

Conclusion

The objectives of the standard are fulfilled by the Emerson functional safety management system, internal organizational procedures, software development process, and new product development processes and supported by PIU analysis.

5.3 Hardware Design and Verification

Objectives

- Create E/E/PE safety-related systems conforming to the specification for the E/E/PE safety requirements (comprising the specification for the E/E/PE safety functions requirements and the specification for the E/E/PE safety integrity requirements).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.



- Demonstrate, for each phase of the overall, E/E/PE and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
- Integrate and test the E/E/PE safety-related systems.

5.3.1 Hardware Architecture Design and Probabilistic Properties

Assessment

Hardware and system architecture design [D045] for the 8800D Vortex Flowmeter has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews [D053] are used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are incorporated into the design. The FMEDA shows that the pulse output functions (not fully covered by PIU demonstration) do not adversely affect the safety integrity of the functions that are used.

To evaluate the hardware design of the 8800D Vortex Flowmeter, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by *exida* for each component in the system. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing [D077] 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. The FMEDA is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. From the FMEDA, failure rates are derived for each important failure category. These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined SIF to verify the design of that SIF.

Conclusion

The objectives of the standard are fulfilled by the Emerson functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices and supported by PIU analysis.

5.4 Safety Manual

Objectives

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

Assessment

The Safety Manual [D079] is provided which identifies and describes the safety functions of the 8800D Vortex Flowmeter, including a description of the input/output interfaces, diagnostic interval, proof testing. The safety function is the proportional flow output on the 4-20 mA analog loop. When internal faults are detected, their effect on the device output is clearly described. Sufficient



information is provided to facilitate the development of an external diagnostics capability (output monitoring) by a safety PLC. HART multidrop mode shall not be used for safety applications.

The Installation Manual [D078] includes valuable information for the user of the 8800D Vortex Flowmeter regarding safe installation, operation, and avoidance of hazards. This document creation is managed on the project and considers user/maintenance friendliness, limited operation modes, and protection against operator mistakes.

Conclusion

The objectives of the standard are fulfilled by the Emerson the safety manual and operation manual.



6 2020 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Emerson	Manufacturer of the Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option
<i>exida</i>	Performed the hardware assessment review
<i>exida</i>	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited <i>exida</i> scheme.

Emerson contracted *exida* in January 2020 to perform the surveillance audit for the above Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option. The surveillance audit was conducted remotely with Emerson’s facility in Eden Prairie, MN, USA during August 2020.

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 Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option.
- 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 – Recommendations from the previous audit are reviewed to see if they have been resolved properly.



6.2.1 Documentation provided by Emerson

Doc ID	Filename	Version
[D1]	00809-0200-4004_SIL_IMPACT_111418.xls	4/15/2020
[D2]	00809-0200-4004_VortexSafetyManualChecklist_AC_V1.pdf	Rev. AC
[D3]	00809-0200-4004_VortexSafetyManual_AC_V1-Marked.pdf	8/26/2020
[D4]	00809-0200-4004_VortexSafteyManual_AC_V1.pdf	Rev. AC
[D5]	08800-0214_SIL_IMPACT_011218.xls	8/21/2019
[D6]	08800-0214_SIL_IMPACT_101817.xls	8/21/2019
[D7]	08800-7018_SIL_IMPACT_121117.xls	4/17/2020
[D8]	08800-7611_SIL_IMPACT_081218.xls	4/20/2020
[D9]	08800-7701_SIL_IMPACT_101717.xlsx	10/17/2017
[D10]	08800-7702_SIL_IMPACT_100219.xls	4/20/2020
[D11]	08800-7726_SIL_IMPACT_082718.xls	4/21/2020
[D12]	8800D-SIS-H7_SRD_0.6_signed.pdf	Rev. 0.6
[D13]	C53392_SIL_IMPACT_010818.xls	8/21/2019
[D14]	C53392_SIL_IMPACT_102417.xls	8/21/2019
[D15]	ChangeHistoryForSIL.xlsx	7/10/2019
[D16]	DiagnosticSummary_533_723.xlsx	8/2/2020
[D17]	Project Plan - RevA.pdf	Rev. A
[D18]	Release_Report_8800_Thunderbird_SIS.pdf	8/31/2020
[D19]	SIA_Hart5-7_20200901.xls	9/1/2020
[D20]	SRS-SIS Peer Review Inspection Report and Consolidated Log.xlsm	Rev. 1
[D21]	SRS-SIS-0_4.pdf	Rev. 1
[D22]	SRS-SIS-0_4_Safety_Reqs_Checklist.xls	8/28/2020
[D23]	Vortex_8800D_scmp_revA.pdf	Rev. A
[D24]	Vortex_8800_SVTP_0.3.pdf	Rev. 0.3
[D25]	Vortex_8800_SVTP_0.3_Verification_Checklist.pdf	8/26/2020
[D26]	Vortex_8800_SVT_Summary_RevA.pdf	Rev. A
[D27]	Vortex_SRD_Safety_Reqs_Checklist_0.6.xls	8/12/2020



6.2.2 Surveillance Documentation generated by *exida*

[R5]	ROS 06-03-34 R001 V3R7	FMEDA report, Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option
[R6]	EMM 8800D V3R0 SIL3 SafetyCaseWB-61508 - 8800D	IEC 61508 SafetyCaseWB for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option
[R7]	EMM 20-01-099 FFA01 V1R0 Field Failure Analysis - 8800D	Field Failure Analysis for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option
[R8]	EMM 20-01-099 PIU01 V1R0 PIU Analysis - 8800D HART	Proven In Use Analysis for Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and "SI" option (firmware only)

6.3 Surveillance Results

6.3.1 Procedure Changes

There were no significant changes to the procedures during the previous certification period.

6.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period. Change requests for some minor enhancements were reviewed and all documentation were found to be acceptable. While the firmware was updated to add HART 7 functionality, it was assessed separately under PIU requirements rather than under Modification Procedures. See section 6.3.4 below.

6.3.3 Impact Analysis

There were no safety-related design changes during the previous certification period.

6.3.4 Field History

The field history of this product was analyzed and found to be consistent with the failure rates predicted by the FMEDA. Note that the field history of updated firmware was also analyzed separately to ensure it meets SC3 PIU requirements. There were no field failures reported that were attributed to the updated firmware.

6.3.5 Safety Manual

The updated safety manual was reviewed and found to be compliant with IEC 61508:2010.

6.3.6 FMEDA Update

The FMEDA was updated as part of this project for format and other minor changes only. Failure rates were not updated.



6.3.7 Evaluate use of certificate and/or certification mark

The Emerson website was searched and no misleading or misuse of the certification or certification marks was found.

6.3.8 Previous Recommendations

Previous recommendations for improvement were reviewed and were resolved satisfactorily to the requirements of IEC 61508.

6.4 Surveillance Audit Conclusion

The result of the Surveillance Audit Assessment can be summarized by the following observations:

The Emerson Rosemount 8800D Vortex Flowmeter with HART (4-20 mA) and “SI” option continues to meet the relevant requirements of IEC 61508:2010 for SIL 3 based on the initial assessment and considering:

- field failure history
- permitted modifications completed on the product
- resolution of past action items
- constraints documented in the Safety Manual, certificate and this report

This conclusion is supported by the updated Safety Case and certification documents.

7 Terms and Definitions

E/E/PE	Electric/Electronic/Programmable Electronic safety-related system
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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PIU	Proven-In-Use
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
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
Q20/01-099	EMM 16-12-042 R001 V2R1	Errors and omissions update; DEB, 25-Sep-2020
Q20/01-099	EMM 16-12-042 R001 V2R0	Surveillance audit and FW update; DEB, 25-Sep-2020
Q16/12-042R2	EMM 16-02-042 R001 V1R2	Updated FMEDA filename and company name; JCY, 6-Oct-2017
Q16/12-042R2	EMM 16-02-042 R001 V1R1	Adjustments and updates after review; JCY, 29-Sep-2017
Q16/12-042R2	EMM 16-02-042 R001 V1R0	Initial draft; JCY, 26-Sep-2017

Review: David Johnson, 17-Sep-2020

Status: Released, 9/18/2020

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

David Butler, CFSE, Evaluating Assessor

David Johnson, CFSE, Certifying Assessor