IEC 61508 Functional Safety Assessment

Project:
Micro Motion 1700/2700 Coriolis Flowmeter
with Standard or Enhanced Core

Company:
Emerson
Boulder, Colorado
USA

Contract No.: Q20/01-176
Report No.: EMM 08/04-67 R005
Version V3, Revision R0, May 22, 2020
Dave Butler

Management Summary

This report summarizes the results of the Functional Safety Assessment according to IEC 61508 carried out on the:

- Micro Motion 1700/2700 Coriolis Flowmeter with Standard 700 Core Processor
- Micro Motion 1700/2700 Coriolis Flowmeter with Enhanced 800 Core Processor

The Functional Safety Assessment performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Emerson through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.

exida reviewed the manufacturing quality system in use at Emerson

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 Safety Case was prepared, using the *exida* SafetyCaseDB™ tool, and used as the primary audit tool. The Enhanced Core Processor is an upgrade to the previously certified 1700 and 2700 Coriolis Flow and Density Transmitters with the 700 Core Processor. This assessment took into consideration the previous assessment, changes and additions to the product, enhancements to the development process, and the process requirements to implement these changes.

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

The audited development process, as tailored and implemented by the Micro Motion 1700/2700 Coriolis Flowmeter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Micro Motion 1700/2700 Coriolis Flowmeter can be used in a low demand safety related system in a manner where the PFD_{AVG} is within the allowed range for SIL 2 according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the Micro Motion 1700/2700 Coriolis Flowmeter meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the Micro Motion 1700/2700 Coriolis Flowmeter is capable for use in SIL 3 applications in Low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.

This means that the Micro Motion 1700/2700 Coriolis Flowmeter with either the 700 or 800 Core are capable for use in SIL 3 applications in Low or High demand mode 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

1 Purpose and Scope

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

- Micro Motion 1700/2700 Coriolis Flowmeter with Standard 700 Core Processor
- Micro Motion 1700/2700 Coriolis Flowmeter with Enhanced 800 Core Processor

by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508: 2010.

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

- the Micro Motion 1700/2700 Coriolis Flowmeter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the Micro Motion 1700/2700 Coriolis Flowmeter development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

and

- the Micro Motion 1700/2700 Coriolis Flowmeter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out 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 carried out by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* 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.

The assessment was planned by *exida* and agreed to with Emerson.

All assessment steps were continuously documented by *exida* (see [R1] to [R9]).

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 Coriolis Flowmeter with 1700 / 2700 Transmitter
exida	Performed the hardware assessments [R1] and [R2]
exida	Performed the IEC 61508 Functional Safety Assessment

Emerson contracted *exida* in September 2008 with the IEC 61508 Functional Safety Assessment and certification renewal 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): 2010, 2nd ed.	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

Note: Documents revised after the initial audit are listed in 2020 IEC 61508 Functional Safety Surveillance Audit.

2.4.1 Documentation provided by Emerson

[D1]	SafetyCaseDB IEC61508 FSM.esc	1700/2700 Transmitter SafetyCaseDB
[D2]	CP 18, Rev I	Control Procedure 18 - Product Development & Design Control
[D3]	ER-20012896, Rev 0.4, 7/8/08	2400S Series Project Development Plan
[D4]	800 CRDO, Rev 0.4, 11/5/2004	Model 800 Enhanced Core Processor Customer Requirements Document
[D5]	MMI SIL 2700 SASRD_02.doc, Rev 0.2	1700 / 2700 Coriolis Flowmeter System Architecture and Safety Requirements Specification

[D6]	LWI 133, Rev B	Local Work Instruction 133 - System, Architecture and Safety Requirements Guidelines
[D7]	LWI 127, Rev F	Local Work Instruction 127 - Requirements Management Procedure
[D8]	LWI 132, Rev C	Local Work Instruction 132 - Software and Embedded System Project Planning
[D9]	LWI 129, Rev B	Local Work Instruction 129 - Embedded Software Development Procedure
[D10]	LWI 23, Rev F	Local Work Instruction 23 - Software Development Process
[D11]	LWI 188, Rev A	Local Work Instruction 188 - C and C++ Coding Guideline
[D12]	LWI 126, Rev D	Local Work Instruction 126 - Software Quality Assurance Audits Procedure
[D13]	LWI 126 – 800, 9/26/08	Completed Embedded Development Project Audit Checklist (per LWI 126)
[D14]	LWI 24, Rev F	Local Work Instruction 24 - Product Development Configuration Management
[D15]	LWI 130, Rev B	Local Work Instruction 130 - Product and Process Reviews
[D16]	LWI 31, Rev C	Local Work Instruction 31 - Inspection and Test Equipment Calibration
[D17]	CP 36, Rev G	Control Procedure 36 - ECR/ECO Procedure (Engineering Change Request)
[D18]	ER- 20004869, Rev A.3, 8/8/08	800 Series SRS (Software Requirement Specification)
[D19]	80xSDD, Rev 0.4, 1/29/07	80x Series Software Design Description (SDD)
[D20]	80xSDD_Minutes_rev0_1.doc	Software Design Document Review Minutes
[D21]	ER-20008604, Rev K	2400/ECP Enhanced Core Processor Software Release history
[D22]	ECR 021386	Sample ECR showing the SIL requirements
[D23]	CP58, Rev F	Control Procedure 58 - Stop / Resume Ship Procedure
[D24]	CP 58-F1	Stop Ship Authorization Form
[D25]	CP 5 Product Safety.doc, Rev E	Control Procedure 5 - Product Safety
[D26]	LWI 26	Local Work Instruction 26 - Checklist for Safety
[D27]	CP 36-A9, Rev A	SIL Impact Analysis Worksheet (CP36 Attachment 9)
[D28]	ECP800 Version 342 TB Rev 1.doc	Technical Bulletin for ECP800 Ver 3.42 Software Release
[D29]	2700 SIL Validation Test Plan.doc, Ver 1, Sept 2008	2700 Coriolis Flowmeter Safety Validation Test Plan

[D30]	2700 SIL Validation Test Report, Ver 1.0, Nov 2008	2700 Coriolis Flowmeter Safety Validation Test Report
[D31]	DA03001R101.doc	Architecture Diagram for automated DVT Engine
[D32]	2400sManualDVT.xls	800 Manual DVT Tests
[D33]	DVT, 8/18/08	Design Validation Test Report Example
[D34]	LINT, 8/29/08	LINT Results
[D35]	BFSrc.UNIT_TEST_CodeStats.xls	Code Module Unit Test Results summary spreadsheet
[D36]	Review 306, Rev 1.0, 11/15/04	Code review example – Coriolis Meter
[D37]	P/N 20001715, Rev B, 09/2006	Series 1000 and 2000 Transmitters - Configuration and Use Manual
[D38]	LWI 186, Rev A	Local Work Instruction 186 - Safety Manual Creation Guideline
[D39]	P/N 20004482, Rev B	Model 1700 or Model 2700 Transmitter Safety Manual
[D40]	Tools Techniques and Measures per IEC 61508,	IEC 61508 Tables, document shows all tables from IEC 61508 Annex A and B from part 2 and part 3 along with details as to how Micro Motion meets each of the requirements.
[D41]	Training record.jpg, 10/08	Sample of a training record for a SIL team member
[D42]	Control Procedure Index, 10/01/08	Index of Micro Motion Control Procedures
[D43]	LWI index-Boulder, 10/01/08	Local Work Instructions Index for Micro Motion, Boulder
[D44]	PS-00400, June 2002	Product Data Sheet Series 1000 and 2000 transmitters
[D45]	PS-00232, April 2002	Product Data Sheet Micro Motion Flowmeters
[D46]	MM 2700 Fault Injection Summary rev. 2.xls	Fault Injection Test Plan
[D47]	701-081/2004T, Rev 1.0, 2005-Nov-10	TUV Nord Certification Report of the 1700/2700 Coriolis Flowmeter
[D48]	Pegasus Sales FY06 to FY08	Shipments spreadsheet for 1700/2700
[D49]	Pegasus WF FY06 to FY08	Warranty Failure data spreadsheet for 1700/2700
[D50]	ER-0642000, Rev J	700 Core Processor Software Release history
[D51]	IEC Tables, 0.2; 1/7/2008	IEC 61508 Tables, document shows all tables from IEC 61508 Annex A and B from part 2 and part 3 along with details as to how Micro Motion meets each of the requirements.

2.4.2 Documentation generated by *exida*

[R1]	MiMo 08/04-67r1 R001 V2R2, 10/21/2008	FMEDA report, Coriolis Flowmeter 1700 / 2700 Transmitter, with 700 CP
[R2]	MiMo 08/04-67r1 R001 V2R2, 10/21/2008	FMEDA report, Coriolis Flowmeter 1700 / 2700 Transmitter, with 800 ECP
[R3]	MiMO 04-06-22 R001, V2 R2, 4/1/2005	1700/2700 Proven In Use Assessment
[R4]	Field_Failure_Analysis_Micromotion 800 ECP.xls	exida field failure analysis summary spreadsheet to calculate failure rates based on field experience
[R5]	MM 08-09-19 R001, V1 R1, 9/30/2008	800 Enhanced Core Processor Proven In Use Assessment
[R6]	MM 08/04-67 R001, V1 R1	Software Criticality Analysis / HAZOP Report
[R7]	MM 2700 Fault Injection Results-GPS.xls, 10/7/2008	Fault Injection Tests and Results
[R8]	MM 08-04-67 R004 V1R1 IEC 61508 Assessment.doc, 12/9/08	IEC 61508 Functional Safety Assessment for Micro Motion Series 1700/2700 Flowmeters with 700 CP
[R9]	MM 08-04-67 R005 V1R1 IEC 61508 Assessment.doc, 12/9/08	IEC 61508 Functional Safety Assessment for Micro Motion 1700/2700 Coriolis Flowmeter with 800 ECP

3 Product Description

This assessment is for the Micro Motion 1700/2700 Coriolis Flowmeter which consist of a series CMF (Elite), T, F, H, R, DT (700 CP only) or HPC010 (800 ECP only) sensor with a Standard 700 CP or 800 ECP and a 1700 / 2700 transmitter.

The Micro Motion 1700/2700 Coriolis Flowmeter is a smart device used in many different industries for both control and safety applications. The Model 1700 / 2700 features MVD™ technology and diagnostics. It allows for multivariable measurement of mass flow, volume flow, density, and temperature. Output options include frequency, milliamp, discrete in, discrete out, HART, Modbus, Foundation Fieldbus H1, or Profibus-PA; intrinsically safe outputs with one frequency and two milliamp outputs are also available.

The analog milliamp output is used for the safety critical variable (mass flow, volume flow or density); all other outputs are considered outside the scope of Safety Instrumented Systems (SIS) usage.

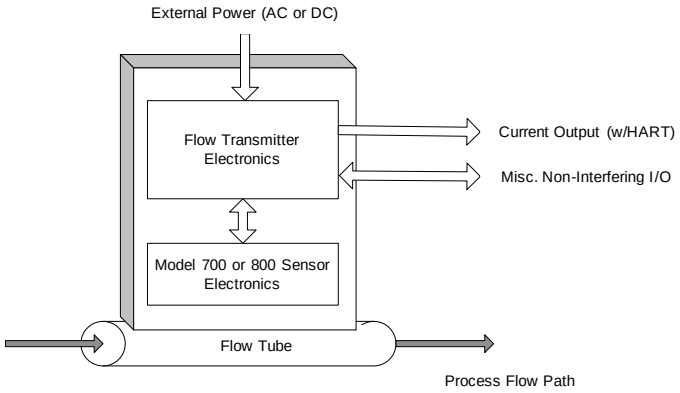


Figure 1 Micro Motion 1700/2700 Coriolis Flowmeter, Parts included in the Assessment

Note: See 2020 IEC 61508 Functional Safety Surveillance Audit section for the current assessed versions information.

In all applications considered, the normal operating condition is when the output mA signal represents the input Flow (or Density) within the Safety Accuracy of 2%. The fail-safe state for when the diagnostics determines there is a fault is configurable and may be either high or low.

The Micro Motion 1700/2700 Coriolis Flowmeter are classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

[1] 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, ed 2. 2010.

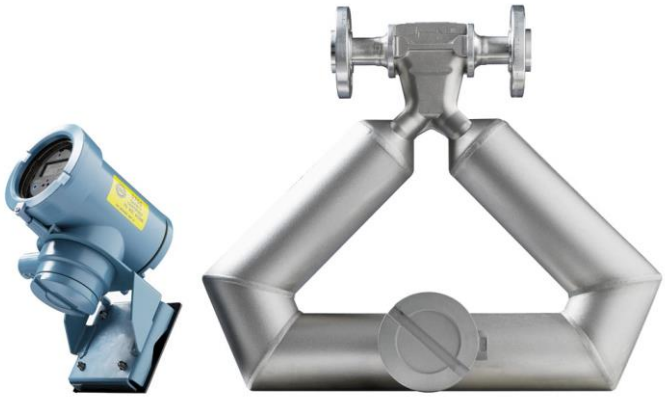


Figure 2 Micro Motion 2700 and an Elite Sensor (CMF100) with 700 CP in a SS housing

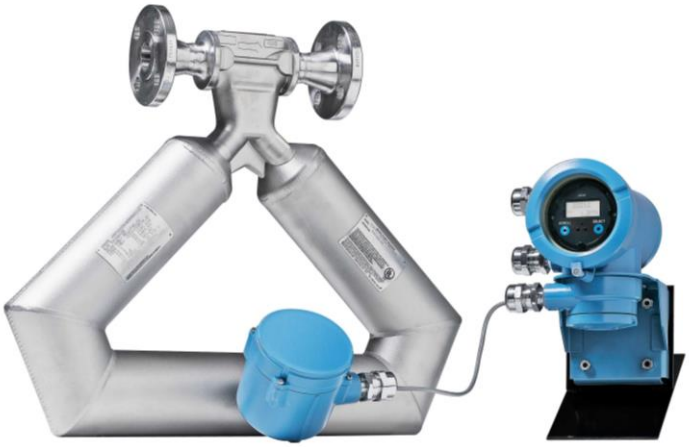


Figure 3 Micro Motion Elite Sensor (CMF100) with 800 ECP and a 2700

3.1 Hardware and Software Version Numbers

Note: see section 6 for updates.

This assessment is applicable to the following hardware and software versions of Micro Motion 1700/2700 Coriolis Flowmeter:

1700 Series	Micro Motion Coriolis Flowmeter with 1700 transmitter with 700 CP or 800 ECP and Analog Output or Intrinsically Safe Output (output codes A or D)
2700 Series	Micro Motion Coriolis Flowmeter with 2700 transmitter with 700 CP or 800 ECP and output codes A, B, C or D
Sensors	Elite, T, F, H, R, DT (700 CP only) or HPC010 (800 ECP only)
Hardware	Based on rev AG BOM (or later)
Software/Firmware (listed versions or later)	1700/2700: v6.6 700 Core: v3.40 or 800 Core: v4.02

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Emerson for this development project against the objectives of the *exida* certification scheme which includes subsets of IEC 61508-1 to -3.

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
  - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
  - Specification process, techniques and documentation
  - Design process, techniques and documentation, including tools used
  - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
  - Verification activities and documentation
  - Modification process and documentation
  - Installation, operation, and maintenance requirements, including user documentation
  - Manufacturing Quality System
- Product design
  - Hardware architecture and failure behavior, documented in a FMEDA
  - Software architecture and failure behavior, documented in a Software Criticality and Software HAZOP report
- Product Field History
  - Hours of field operation
  - Field failure history
- Product Certifications
  - TUV IEC 61508 Certification Report for 1700/2700 Coriolis Flowmeter

The review of the development procedures is described in section 5.1. The review of the product design is described in section 5.3. The review of the product field history is described in section 5.2.

4.2 Assessment level

The Micro Motion 1700/2700 Coriolis Flowmeter with either the 700 or 800 Core have been assessed per IEC 61508 to the following levels:

- SIL 2 capability, single use (Hardware Fault Tolerance = 0)
- SIL 3 capability, redundant use (Hardware Fault Tolerance = 1)

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

5 Results of the IEC 61508 Functional Safety Assessment

exida Certification assessed the development process used by Emerson during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, and 3 [N1]. Some of the development of the Micro Motion 1700/2700 Coriolis Flowmeter was done prior to Micro Motion establishing their fully compliant development process. Consequently, for the evaluation of some of the systematic fault avoidance measures, some weight was given to proven in use considerations to offset the absence of some avoidance items. The most recent and all future modifications to the Micro Motion 1700/2700 Coriolis Flowmeter must be made per the IEC 61508 SIL 3 compliant change/development process.

5.1 Lifecycle Activities and Fault Avoidance Measures

Emerson has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in the SafetyCaseDB [D1].

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the 1700/2700 Coriolis Flowmeter development. The investigation was executed using the *exida* certification scheme which includes 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 Emerson development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

FSM Planning

The functional safety management of any Emerson Safety Instrumented Systems Product development is governed by Control Procedure (CP) 18 [D2]. Micro Motion utilizes a Stage-Gate model for their product development projects. This Stage-Gate process governs all product development activity from the project kick-off through release to production and eventual discontinuance of the product. The Micro Motion Stage-Gate process is derived from the Emerson Stage-Gate process and is divided into 9 phases. For each development Micro Motion creates a Development Management Plan [D3] which defines all of the tasks that must be done to ensure functional safety as well as the person(s) responsible for each task. These processes and the procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management.

Version Control

All documents are under version control as documented in [D1]. Emerson uses PVCS for its revision control of all documents and specifications related to the project. Product documentation is controlled by CP 36 and is managed using Product Data Management (PDM).

Training, Competency recording

Selection of the team members is handled by management in accordance with CP 18. Personnel training records are kept in accordance with IEC 61508 requirements as documented in [D1] and demonstrated in [D41]. Emerson hired *exida* Certification to be the independent assessor per IEC 61508.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in the Development Management Plan [D3], a System Architecture and Safety Requirements Specification (SASRD) [D5] is done for all products that must meet IEC 61508 requirements. The requirements specification contains the product safety constraints, safety integrity requirements, product architecture, and the hardware and software architecture requirements. This document includes block diagrams of the overall architecture, dataflow for both hardware and software as well as identifiers for tracking of the requirements. The SASRS has been reviewed by *exida*. During the assessment, *exida* Certification reviewed the content of the specification for completeness per the requirements of IEC 61508.

Requirements for the project were traced using Requisite Pro. Each requirement identified in the Customer Requirements Document can be traced to a system-level requirement. Each system-level requirement can then be traced to a requirement(s) in the software requirements specification(s) and/or hardware requirements specification(s). These in turn are traceable down to either a test case in the Design Verification Test plan for the software or the Test Spec for the transmitter.

Requirements from **IEC 61508-2, Table B.1** that have been met by Emerson include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, semi-formal methods and checklists. [D40] & [D51] documents more details on how each of these requirements have been met. This meets the requirements of SIL 3.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D3] and [D2]. The hardware design process includes component selection, detailed drawings and schematics, a failure modes, effects and diagnostic analysis (FMEDA), design reviews, the creating of prototypes, and hardware verification tests.

Requirements from **IEC 61508-2, Table B.2** that have been met by Emerson include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, checklists, semi-formal methods, computer aided design tools, simulation, and inspection of the specification. This meets the requirements of SIL 3.

5.1.4 Software Design

During the prior certification process of the similar 1700/2700 Flowmeters with standard 700 core, some additional changes and enhancements to the software process were incorporated by Micro Motion. A Proven in Use analysis was performed on 1700/2700 Flowmeters with the 800 Core (section 5.2). This analysis was supplemented with a Software Criticality Analysis / HAZOP Report [R6] which further details the extra testing and analysis that was used in evaluating the software and its design process. The latest software version for the 800 core also had each of its complex modules fully module tested. Coding standards, code reviews, module testing, LINT testing, fault injection tests boundary value tests, and Design Validation Testing are all techniques now used for changes to the software. This meets the requirements of SIL 3.

5.1.5 Validation

All safety requirements documented in the SASRD [D5] are validated by test or inspection. A validation test specification and plan [D29] was created for the Micro Motion 1700/2700 Coriolis Flowmeter and reviewed as part of the assessment. Each validation test includes an explicit test to the requirement being validated. As part of the assessment, it was verified that all safety requirements were covered by one or more validation tests. Procedures are in place for corrective actions to be taken when tests fail as documented in [D1] and [D17].

Requirements from IEC **61508-2, Table B.3** that have been met by Emerson including functional testing, project management, documentation, and black-box testing. [D40] & [D51] documents more details on how each of these requirements are met. This meets the requirements of SIL 3.

Requirements from IEC **61508-2, Table B.5** that have been met by Emerson include functional testing and functional testing under environmental conditions, Interference surge immunity testing, fault insertion testing, project management, documentation, static analysis, dynamic analysis, and failure analysis, expanded functional testing and black-box testing. [D40] & [D51] documents more details on how each of these requirements has been met. This meets SIL 3.

5.1.6 Verification

The development and verification activities are defined in [D2] and [D3]. Verification activities include the following: Design Review Meetings, Hardware Verification Testing, FMEDA, Module Testing, Module Integration Test, and Software Inspection.

5.1.7 Modifications

Modifications are done per Micro Motion's IEC 61508 SIL 3 compliant ECR/ECO procedure CP 36 [D17]. A large change project would be treated as a new development and is required to go through the full new development process CP 18. Additional automatic measures have been put into place to ensure that a SIL impact analysis is performed when any part or assembly that is a component on a SIL approved device is part of an ECR. This meets the requirements of IEC 61508 SIL 3.

5.1.8 User documentation

Emerson created a Safety Manual for the Micro Motion 1700/2700 Coriolis Flowmeter, [D39]. This safety manual was assessed by *exida*. The final version is compliant with the requirements of IEC 61508. The document includes all required reliability data and operations, maintenance, (or references to) and proof test procedures.

Requirements from IEC 61508-2, Table B.4 that have been met by Emerson include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities, protection against operator mistakes, and operation only by skilled operators. [D40] & [D51] documents more details on how each of these requirements has been met. This meets the requirements for SIL 3.

5.2 Proven in Use

In 2005 the Micro Motion 1700/2700 Coriolis Flowmeter with the 700 Core were evaluated and determined to meet the proven in use requirements of IEC 61508 (See document [R3]). This transmitter has been in the field since 2001. Back in 2005 over 50,000 units had over 300 million

hours of documented run time in the field. Based on field return data, the estimated field failure rate of the device is 6.73E-07 failures per hour. The documented operating hours and field failure rate are sufficient to meet the proven in use requirements for SIL 3.

A second proven in use assessment was done for transmitters with the 800 ECP [R5]. This report showed that although the failure rates were sufficient for proven in use of the hardware, however there were not enough field hours of run time of the latest software version to accept this alone as sufficient proof for a SIL 3 device. Thus the 800 ECP assessment is not wholly based on Proven in Use. This along with the other design measures used in the development of the 800 ECP meets the requirements for systematic capability of IEC 61508.

5.3 Hardware Assessment

To evaluate the hardware design of the Micro Motion 1700/2700 Coriolis Flowmeter, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R1] and [R2]. The FMEDAs were verified using Fault Injection Testing as part of the IEC 61508 assessment [R7].

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA failure rates are derived for each important failure category. The failure rates are valid for the useful life of the devices.

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 analysis shows that the design of the Micro Motion 1700/2700 Coriolis Flowmeter meets the hardware requirements of IEC 61508, SIL 2 @ HFT=0 and SIL 3 @ HFT=1.

6 2020 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Emerson	Manufacturer of the Micro Motion 1700/2700 Coriolis Flowmeter
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Emerson contracted *exida* in February 2017 to perform the surveillance audit for the above Micro Motion 1700/2700 Coriolis Flowmeter with either the 700 or 800 Core. The surveillance audit was conducted remotely with Micro Motion's facility in Boulder, CO - USA during April/May 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 Micro Motion 1700/2700 Coriolis Flowmeter with either the 700 or 800 Core.
- 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 Emerson

Doc ID	Document	Version	Date
[D52]	GWI 03 Technical Bulletins, Service Bulletins and Knowledge Based Articles.docx	Rev. G	11/6/2019
[D53]	GWI 47 Non-conforming Material, Process and System Identification and Data Collection.docx	Rev. AG	9/2/2019
[D54]	GWI 235 RMA Evaluation Writing Standard.docx	Rev. G	8/21/2018
[D55]	GWI 318 Product Development and Design Control.docx	Rev. AH	1/7/2019
[D56]	GWI 320 Temporary Deviation Authorization.docx	Rev. W	3/20/2020
[D57]	GWI 321 Document Control.docx	Rev. R	1/2/2020
[D58]	GWI 336 Design Change Process.docx	Rev. O	3/1/2019
[D59]	GWI 336-A9 SIL Impact Analysis Worksheet.docx	Rev. B	
[D60]	GWI 380 Supplier Quality Manual.docx	Rev. O	12/5/2019
[D61]	LWI 15 Return Material Authorization.docx	Rev. AG	1/26/2018
[D62]	LWI 23 Software Development Process.docx	Rev. AF	6/24/2019
[D63]	LWI 23-A2 C and C++ Coding Standard.docx	Rev. J	9/3/2015
[D64]	LWI 133 Systems Architecture and Safety Requirements Guidelines.docx	Rev. L	8/7/2018
[D65]	LWI 186 Safety Manual Creation Guideline.docx	G	3/15/2019
[D66]	GWI 336-A9 SIL Impact Analysis Worksheet.docx		2/23/2018
[D67]	GWI 336-A9 SIL IAWrB 800v4.6.docx	Version 4.6	6/7/2018
[D68]	SIL Unit Tests.xlsx		2/23/2018
[D69]	MMI-SB-167 Rev A.pdf	Rev. A	5/1/2018
[D70]	FW SCR 0052034 question.msg		5/7/2020
[D71]	Numerous Unit Test scripts (listed in SIL Unit Tests.xlsx)		
[D72]	1000-2000 SRS testcases Traceability.xlsx	Rev. K	8/4/2016
[D73]	800 testcases Traceability.xlsx	Rev. A.13	10/5/2019
[D74]	CR_DATA_26_MAR-2020		3/2020
[D75]	Emerson Automation – 20190927 rev 5 – 20200430.pdf – 1588269832041.pdf	Rev. 5	Exp. 12/2022

6.2.2 Surveillance Documentation generated by *exida*

[R10]	EMM 04-06-22 R004 V4R1 FMEDA 1700-2700 700CP	FMEDA report, 1700 / 2700 Coriolis Flowmeter Series with Standard 700 Core
[R11]	EMM 08-04-67 R001 V4R1 FMEDA 1700-2700 800ECP	FMEDA report, 1700 / 2700 Coriolis Flowmeter Series with Enhanced 800 Core
[R12]	EMM 20-01-176 FFA1 V1R0	Field Failure Analysis - Transmitter 1700_2700, Cores and Sensors.xlsx

6.3 Surveillance Results

6.3.1 Procedure Changes

Only minor changes have been made to procedures since the assessment of model 4200 done in 2019. Since the same procedures are used for both products, they are considered adequate.

6.3.2 Engineering Changes

Lists of Hardware and Software changes since the last audit were reviewed. Each of the changes were judged to be sufficiently evaluated by Micro Motion for functional safety and documented in accordance with Micro Motion's procedures.

6.3.3 Impact Analysis

The SIL Impact Analysis Worksheets for the hardware and software changes were reviewed and found to be adequately documented given the scope of the simple changes made to this mature product.

6.3.4 Field History

Worldwide Shipment and Return information were reviewed for each of the 4 main components of the 1700 / 2700 transmitter. For the returns, the WF-18 (which includes the WF-12 category) information was used. The data used was for the 3-year period between Mar 2017 to Dec 2019. The calculated actual field failure rate is below the predicted failure rate of the FMEDA.

Management holds regular quality meetings to monitor this as well.

6.3.5 Safety Manual

The safety manual has not changed since the last assessment of the Micro Motion 1700/2700 Coriolis Flowmeter. Rev BB is the current version of the safety manual and was found to be publicly available on Micro Motion's website. The contents of the manual were found to be acceptable.

6.3.6 FMEDA Update

The content of the FMEDA analyses were not affected (failure rates, assumptions, etc.), but the reports were updated for formatting and some minor changes to boilerplate text.

6.3.7 Evaluate use of certificate and/or certification mark

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

6.3.8 Previous Recommendations

No previous recommendations needed to be implemented.

6.3.9 Additional Manufacturing locations

In addition to the main design and manufacturing location in Boulder CO, Micro Motion has 4 other sites that are approved to produce Sensors and finished Transmitter assemblies. These are in Chihuahua, Mexico; Nanjing, China; Ede, Netherlands; and Cluj, Romania.

6.3.10 Assessed Configurations / Versions

Some sensor models have been added and others removed in the years since the initial audit. The following table lists the current assessed configurations and Hardware/Software versions:

Table 1 Assessed Configurations / Versions

1700 Series	Micro Motion Coriolis Flowmeter with 1700 transmitter with 700 CP or 800 ECP and Analog Output or Intrinsically Safe Output (output codes A or D)
2700 Series	Micro Motion Coriolis Flowmeter with 2700 transmitter with 700 CP or 800 ECP and output codes A, B, C or D
Sensors	Elite, T, F, H, R, DT (700 CP only) or HPC010 (800 ECP only)
Hardware	Based on rev AG BOM (or later)
Software/Firmware (listed versions or later)	1700/2700: v6.6 700 Core: v3.40 or 800 Core: v4.02

7 Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
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).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
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
Q20/01-176	EMM 08-04-067 R005 V3R0	2020 Renewal; Aligned expiration dates of 1700/2700, 5700 and 4200; DEB, 5/22/2020
Q17/02-079	EMM 08-04-067 R005 V2R1	Updated with 2017 Re-Cert audit, combined 700 and 800 Core reports, and added H & HPC Sensors, G Sauk, 1-May-2017
Q16/01-126	EMM 08-04-067 R005 V1R5	Updated FMEDA report reference, RPC, 2016-03-08
Q16/01-126	EMM 08-04-067 R005 V1R4	Updated for R sensors; updated FMEDA reference, RPC, 2016-01-29
Q14-02-049	EMM 08-04-067 R005 V1R3	Updated for renewal certification to IEC 61508:2010, 2nd ed., JCY, May 22, 2014
Q12-03-010	EMM 08-04-067 R005 V1R2	Updated for renewal certification, JCY, April 30, 2012
Q08/04-067	EMM 08-04-067 R005 V1R1	Revised some terminology, Released to Emerson; December 9, 2008
Q08/04-067	EMM 08-04-067 R005 V1R0	Initial version; November 2008

Authors: Dave Butler

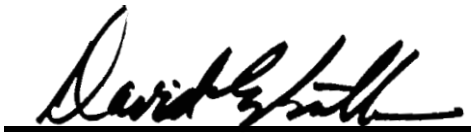
Review: V3, R0: John Yozallinas, May 20, 2020

Release status: Released

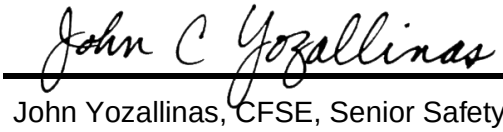
8.3 Future Enhancements

At request of client

8.4 Release Signatures



David Butler, CFSE, Senior Safety Engineer



John Yozallinas, CFSE, Senior Safety Engineer