Results of the IEC 61508 Functional Safety Assessment

Project:
5700 Coriolis Flowmeter

Customer:
Micro Motion, Inc.
Emerson Process Management
Boulder, CO
USA

Contract No.: Q14-02-064r1
Report No.: EMM 14-06-064 R003
Version V1, Revision R0, September 24, 2105
Dave Butler

Management Summary

The Functional Safety Assessment of the Micro Motion, Inc. 5700 Coriolis Flowmeter development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Micro Motion, Inc. 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 the manufacturing quality system in use at Micro Motion, Inc..

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 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 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 Micro Motion, Inc. 5700 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 5700 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 (HFT = 0) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the 5700 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 5700 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.

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:

- 5700 Coriolis Flowmeter

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 5700 Coriolis Flowmeter with the IEC 61508-2 and -3 technical requirements, and the derived product safety property requirements, for SIL 3;

and

- the 5700 Coriolis Flowmeter development processes, procedures and techniques, as implemented for the safety-related deliverables, with the IEC 61508-1, -2 and -3 management requirements for SIL 3;

and

- the 5700 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 *exida's* quality procedures and scope definitions.

The results of this assessment provide the safety instrumentation engineer with the failure data required by IEC 61508 / IEC 61511 to show that sufficient attention has been paid to systematic failures during the development of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried out using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

To show compliance with the objectives of the standard, evidence and arguments are created and recorded for all requirements relevant to the development project. The evidence and arguments are reviewed to verify that each requirement is covered. This methodology results in more comparable assessments, across multiple projects, even with different assessors. 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 with Micro Motion, Inc. (see [R2]).

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 300 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 100 billion hours of field failure data.

2.2 Roles of the parties involved

Micro Motion, Inc.	Manufacturer of the 5700 Coriolis Flowmeter
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

Micro Motion, Inc. contracted *exida* with the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards / Literature used

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

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

2.4 Reference documents

2.4.1 Documentation provided by Micro Motion, Inc.

Doc. ID	Project Document Filename	Version	Date
D001	MMI Quality Manual.pdf	Rev. AE	7/16/2015
D003	CP 18 Product Development and Design Control.docx	Rev. W	6/16/2015
D003b	GWI 33 Sustaining Engineering Stage Gate Process.docx	Rev. C	4/2/2014
D003c	LWI 127 - Requirements Management Procedure.doc	Rev. F	
D003d	LWI 133 Systems Architecture and Safety Requirements Guidelines.docx	Rev. I	1/16/2015
D003e	LWI 186 Safety Manual Creation Guideline.docx	Rev. C	6/12/2013
D004	LWI 24 - Product Development Configuration Management.doc	Rev. F	
D005	GWI 235 RMA Evaluation Writing Standard.docx	Rev. B	8/3/2012
D006	LWI 15 Return Material Authorization.docx	Rev. AC	4/18/2014
D007	CP 80 Supplier Quality Manual.docx	Rev. G	6/23/2015

Doc. ID	Project Document Filename	Version	Date
D008	CP 20 Temporary Deviation Authorization.docx	Rev. R	5/7/2014
D010	CP 21 Document Control.docx	Rev. M	5/12/2014
D012	GWI 47 Non-conforming Material, Process and System Identification and Data Collection.docx	Rev. Z	3/9/2015
D013b	CP 36 Engineering Change Orders.docx	Rev. J	6/5/2014
D019	CP 05 Product Safety.docx	Rev. I	7/15/2014
D021	LWI 23 Software Development Process.docx	Rev. Y	9/3/2015
D021b	Software Tools.xlsx	1.3	7/10/2014
D023b	CP 36-A9 SIL Impact Analysis Worksheet.docx	Rev. B	
D026	Gen 5 Project Plan.doc	Rev. 0.2	6/17/2014
D026b	Gen 5 Software Project Plan.doc	Rev. 0.3	5/22/2014
D027	Gen 5 Software Project Plan.doc	Rev. 0.3	5/22/2014
D029	LWI 126 - Software Quality Assurance Audits Procedure.doc	Rev. D	
D029b	LWI 130 - Product and Process Reviews.doc	Rev. B	
D032	D032_Job Descriptions and Competency Levels	Many files	
D033	D033_Training Record	Many files	
D034	Gen 5 Software Project Plan.doc	Rev. 0.3	5/22/2014
D036	ISO 9001 cert to 2017.pdf		Expires: 1/4/2017
D040	MMI SIL 5700 SASRD.doc	Rev. 1.1	9/24/2015
D040b	Model 801 Customer Requirements 10-25-2004.pdf	Rev. 1.0	3/27/2014
D040c	RFS Gen 5 Config IO Version 1 S.xls	Rev. S	10/9/2014
D041	FW SIL Doc.msg		3/27/2014
D049	Gen5 SADD.docx	Rev. 1.02	7/2/2015
D050	MicroMotion Gen5 Software HAZOP Report Q1208-109 R001 V1R1.docx	V1R1	12/5/2012
D053	Database Design Review.doc		3/21/2012
D054	5700 Function Classification.xlsx	Rev. 0.1	11/4/2014
D054b	5700C v0.52 Unit Test Report.log		12/12/2014
D054c	5700 Analog Consolidated DVT results.xlsx	Rev. 0.1	
D055	MiMo 14-02-064r1 R001 V1R1 FMEDA 5700.pdf	V1R1	6/23/2015
D056	Gen5 SRS.xlsx	Rev. 2.027	8/7/2015
D058	database.doc		1/14/2013
D059	MM 5700 Fault Injection r1.xls	r1	6/11/2015
D061	D061_Static Code Analyzer Configuration Description		
D062	MMI Statement on Static Analysis Results.docx	Rev. 1.0	8/21/2015
D063	Micro Motion response to request for Static Analysis .docx	Rev. 1.0	8/21/2015
D064b	D064_Module Test Plan	Many files	
D065	Software Unit Test Research.docx		
D067	Gen5 Test Plan.docx	Rev. 1.8	2/13/2014
D069b	5700_PowerSupply_EngValidation_TestPlan_AA2.pdf	Rev. AA2	8/28/2013
D069c	5700_CNFGModule_EngValidation_TestPlan_AA2.pdf	Rev. AA2	10/2/2013
D069d	5700_Display_EngValidation_TestPlan_Results_AA.pdf	Rev. AA	9/20/2013

Doc. ID	Project Document Filename	Version	Date
D069e	5700_CNFGModule_HART.pdf		2/3/2014
D070	RE_ Gen5 Config IO Test Plan-Dawn.pdf		7/11/2013
D070b	Test Plan review_Test team_MOM.xls		12/23/2013
D071	GWI 89 Four Corners Test Procedure.docx	Rev A	5/8/2014
D071b	GWI 101 Electronics Reliability Vibration Procedure.docx	Rev. A	2/25/2015
D071c	Operational Humidity Test_Rev1.pdf		8/12/2014
D072	EMC Testing v3.02.docx		5/1/2015
D073	Enovia PDM		
D074b	5700_PowerSupply_EngValidation_Results_AA2.xlsx	Rev. AA2	8/13/2014
D074c	5700_CNFGModule_EngValidation_Results_AA2.xlsx	Rev. AA2	10/19/2013
D075	5700_CNFGModule_Reliability_Results.xlsx	Rev. AA2	12/11.2014
D076	20141030 - EMC_Report_5700_ConfigIO.pdf		10/30/2014
D077	MM 5700 Fault Injection r1 data.xlsx		6/17/2015
D078	5700-Config-Manual-MMI-20025166.pdf	Rev AA	10/1/2014
D078b	5700-Install-Manual-MMI-20027478.pdf	Rev AC	12/1/2014
D079	5700_SIS_MMI_20029788.pdf	Rev AB	9/1/2015
D079b	5700-PDS-PS-001885.pdf	Rev A	11/1/2014
D080	D080_Safety Manual Review	Many files	
D081	ECO 1049882 History.pdf	Screenshot	3/9/2015
D081b	D081_Engineering Change Documentation	Many files	
D086	Gen5 Tools HAZOP.xlsx		
D087	ER-20026132_AH.doc	Rev AH	8/14/2015
D088	CP 36-A9 SIL Impact Analysis Worksheet for 5700 Config v1.1.docx		2/2/2015
D091	MMI-SB-111 Rev B.pdf	Rev. B	
D091b	MMI-SB-122.pdf	Rev. A	
D092	FW Question about pressure compensation.msg		9/1/2015
D092b	RE SWHAZOP.msg		9/1/2015

2.4.2 Documentation generated by *exida*

[R1]	EMM 14-02-064 V1R1 62508 Safety Case WB - 5700	Safety Case
[R2]	Q14-02-064r1 MMI 5700 Coriolis Flow Meter Proposal	Assessment Plan
[R3]	MiMo 14-02-064r1 R001 V1R1 FMEDA 5700.pdf	FMEDA report
[R4]	EMM 14-02-064 R003 V1R0 61508 Assessment Report - 5700.docx	Assessment Report (this file)

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed with Micro Motion, Inc..

The following IEC 61508 objectives were subject to detailed auditing at Micro Motion, Inc.:

- FSM planning, including
    - Safety Life Cycle definition
    - Scope of the FSM activities
    - Documentation
    - Activities and Responsibilities (training and competence)
    - Configuration management
    - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
    - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including product and software validation
- Hardware-related operation, installation and maintenance requirements

The project teams, not individuals were audited.

The certification audit was done at Micro Motion, in Boulder, CO, on 9/24/2015.

3 Product Description

The Micro Motion, Inc. 5700 Coriolis Flowmeter provides direct mass flow measurement for liquids, gases or slurries with high accuracy. It is especially suited for difficult to measure materials. Unlike many other types of flowmeters it does not require any special mounting, flow conditioning or straight pipe requirements to insure its accuracy. In addition to mass flow it can also directly measure the average density of the material being measured and monitors the temperature. By use of the density and mass flow measurements the more typical volumetric flow rate can also be calculated.

The flow and density measurements are based upon input from two independent pickoff sensors located at opposite ends of the tube. The tube or tubes, depending on the particular sensor, are physically excited to vibrate at their natural frequency. The independent pickoff sensors then measure the resulting difference in phase between the two points. This difference is due to the mass flow resulting in a phase shift between the two sensors from the resulting force of the Coriolis Effect. This product is unique in the scope of flowmeters in the fact that the two sensors always have active signals even at zero flow rate and these signals can be monitored to detect faults and potential interference, even at zero flow, and often before it actually impacts the actual process measurements. Both of the sensors should see signals of the same frequency, relatively the same magnitude and mostly sinusoidal. Diagnostics monitor and insure each of these relationships is within normal range. Detected faults are indicated to the user by use of a defined fault state for the output current outside the normal process range and are also available through the HART interface (This indication is not part of the safety function.).

The product requires a separate input power to power the unit. The 4–20 mA output power can be supplied either internally or via an external loop supply, user configurable.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of 5700 Coriolis Flowmeter:

Device	**Version**
5700 firmware	1.20 and later
Integrated Core Processor firmware	4.14 and later
Enhanced Core Processor firmware	4.14 and later
Standard Core Processor firmware	3.42 and later
5700 hardware	0 and later

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Micro Motion, Inc. for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1]. All objectives have been successfully considered in the Micro Motion, Inc. development processes for the development.

exida assessed the project and procedure documentation with respect to the functional safety management requirements of IEC 61508. An initial evaluation assessment of the development procedures was followed by an evaluation assessment of the project documentation, resulting in final safety case documentation. This was followed by a spot inspection of certain requirements.

The safety case demonstrates the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The assessment was executed using the exida certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the 5700 Coriolis Flowmeter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Micro Motion, Inc. may make modifications to this product as needed.

As part of the *exida* 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 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 Micro Motion, Inc. during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the 5700 Coriolis Flowmeter was in accordance with this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documentation.

5.1 Lifecycle Activities and Fault Avoidance Measures

Micro Motion, Inc. has an IEC 61508 compliant development process, as assessed during the IEC 61508 certification. This compliant development process is documented in [D01].

This functional safety assessment evaluated the compliance of the development processes, procedures and techniques, as implemented for the product development, with the IEC 61508 standard. The assessment was executed using the *exida* certification scheme, which includes subsets of IEC 61508 requirements tailored to the assessment approach taken, and 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 Functional Safety Management

The phases in the overall safety lifecycle required to achieve the targeted functional safety integrity level of the product is documented and structured.

The management and technical activities, performed during the product and software safety lifecycle phases, and necessary for the achievement of the required functional safety of the product, are specified. The responsibilities of the persons, departments and organizations responsible for each safety lifecycle phase are specified. The necessary documentation for the management of functional safety, verification and the functional safety assessment activities has been specified. The necessary information for all phases of the safety lifecycle to be effectively performed has been documented. A suitable set of tools, for the required safety integrity level, over the whole safety lifecycle which assists verification, validation, assessment and modification has been selected.

5.1.2 Safety Lifecycle and FSM Planning

The functional safety management plan defines the safety lifecycle for this project. This includes a definition of the safety activities and documents to be created for this project. This information is communicated via these documents to the entire development team so that everyone understands the safety plan. The Software Development Procedure identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase.

Micro Motion, Inc. has a Quality Management System in place. Micro Motion, Inc. has been ISO 9001 certified. All sub-suppliers have been qualified through a Manufacturer Qualification procedure.

All phases of the safety lifecycle have verification steps described in a verification checklist, which is used to verify each phase.

5.1.3 Documentation

There is a document management system in place. This system controls how all safety relevant documents are changed, reviewed and approved. All safety related documentation is electronically generated and stored, making it easy to access and use the documents. Documentation is required to be properly identifiable, indicate the scope of contents, provide format and content to support navigation/readability/organization, such as titles, headings, tables, etc. Documents are required to have a revision index which lists versions of the document along with a description of what changed in that version.

Several documents were sampled and found to meet these requirements.

5.1.4 Training and competence recording

The Project Plan lists the key people working on the project along with their roles.

Competency requirements have been identified for each role on the project. Individuals have been assigned to each role, considering achieved competencies. Where a competency gap is identified, training has been planned, carried out and documented.

5.1.5 Configuration Management

The configuration of the product to be certified is documented including all hardware and software versions that make up the product. For software this includes source code.

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 software and all associated documentation are properly labeled, stored and controlled during the operational lifetime of the released software.

5.1.6 Tools (and languages)

All tools which support a phase of the software development lifecycle, and cannot directly influence the safety-related system during its run time, are documented, including tool name, manufacturer name, version number and a description of the use of the tool on this project. This includes validation test tools. All off-line support tools have been classified as either T3 (safety critical), T2 (safety-related), or T1 (interference free). 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. An assessment has been carried out for T2 and T3 offline support tools, to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms have been identified, appropriate mitigation measures have been taken.

Configuration and use information has been documented to ensure consistent use of the tools in configuring and building software. Significant confidence in use data is documented for all T3 tools.

5.2 Safety Requirement Specification

All element safety functions necessary to achieve the required functional safety are specified, including diagnostic functions and any functions required to configure the device (offline). All external interfaces have been carefully specified.

Software safety requirements have been created as derived/allocated requirements (from Safety Requirements) and have been made available to the software developers. The SRS has been reviewed in order to verify that the SRS has enough detail such that the required SIL can be achieved during design and implementation, and can be assessed.

SRS content is available and sufficient for the duties to be performed. This has been confirmed by the validation testing and assessment.

5.3 Change and modification management

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

Modification of the product requires that an Impact Analysis be performed to assess the impact of the modification, including the impact of changes on the Functional Safety of the system and to the software design. The results of Impact Analysis are documented and associated with the change request. Modification records document the reason for the change, a description of the proposed change. All changed engineering artifacts, including tests, documentation and software, are documented. The required scope of re-verifying and re-validating the change is documented for each change to ensure that the change is fully tested and that other potentially affected functions were not affected.

Modifications are initiated with an Engineering Design Change procedure [D023]. All changes are first reviewed and analyzed for impact before approval by Micro Motion, Inc. as part of the modification process. Measures to verify and validate the change are developed in accordance with the normal design process.

The modification process has been successfully assessed and audited, so Micro Motion, Inc. may make modifications to this product as needed. An impact analysis [D023b] is performed for any change related to functional safety.

5.4 System Design

Product design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented. The Product Architecture Design clearly identifies the SIL capability of all components, including software components, in the design. If a component has a lower SIL capability than that associated with the safety function(s), then sufficient independence between the components has been documented in a Failure Analysis. The Product Architecture Design describes that the behavior of the device when a fault is detected is to annunciate the detected fault through the output interface.

The Product Architecture Design clearly identifies all safety critical interfaces and a communications analysis has been done to show that these interfaces comply with 7.4.11 of IEC 61508-2. Code protection (information and/or time redundancy) is considered where needed.

The System Architecture Design identifies design features that support maintainability and testability, which shows these qualities have been considered during design and development and have been verified at review time.

The System Architecture requires the use of a password to access the dedicated configuration tool in order to make (offline) changes.

The overall Software Architecture Design has been partitioned into functional modules, supporting simplicity and understandability of the design. The Software Design expresses both the static and dynamic design, in terms of program structure, data structure, functional behavior, information flow, sequencing/timing, synchronization and interface with hardware. The Software Design is well understood by the developers, and is documented in a way that can be easily verified. Semi-formal methods have been used to analyze and document the design.

Formal design reviews are held and the results recorded.

The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow.

5.5 Hardware Design and Verification

The 5700 Coriolis Flowmeter hardware has been designed based on the safety requirements (both safety function requirements and safety integrity requirements). The hardware design and implementation has been verified to meet the specified safety functions and safety integrity requirements. Verification has been demonstrated through testing and evaluation of the hardware phase outputs for correctness and consistency.

5.5.1 Hardware architecture design

The hardware design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented. Hardware components, and indeed modules, used on previous projects are given priority over new components.

A FMEDA analyst has reviewed the design and determined that there are measures against physical environment stresses.

The FSM Plan and development process and guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracing to validation test.

5.5.2 Hardware Design / Probabilistic properties

To evaluate the hardware design of the 5700 Coriolis Flowmeter, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida*, considering each component in the system and effective coverage of all implemented diagnostics. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D77], and 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. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

The product failure rates (λ's) are derived from the results of the FMEDA.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer must calculate the $PFD_{AVG,}$ for each defined safety instrumented function (SIF), to verify the design of a SIF.

5.6 Software Design

The Software Architecture Design contains a description of the software architecture. The design is partitioned into new, existing and/or proprietary (third party) components and modules, which are identified as such.

A software criticality analysis and HAZOP was performed and the report lists all components along with their criticality and their required Systematic Capability. Independence has been achieved by both spatial and temporal separation as documented in the results of the SCA / SW HAZOP and in the Design documentation. Common cause failures are identified in the SW HAZOP as failures of one component that could affect an independent component and defensive measures are listed as Safety Measures.

Semi-formal design notation was used in the design (e.g., State/Transition diagrams, Sequence Diagrams, Structure diagrams, etc.).

The Software Architecture Design specifies that fault detection is employed to detect software faults. Techniques like program flow monitoring, data flow monitoring and CRCs on serial communications data are used. The resulting behavior of the device due to a detected fault is specified.

5.7 Software Verification

Software verification is accomplished through various means. The Software Architecture Design was reviewed. Module tests are created and executed. Structural test coverage is measured, documented and verified to ensure all code is tested at least once. All safety related Source Code Modules have been inspected. Sample code review reports were reviewed to ensure non-conformances are recorded and followed up. Module Test Results for all safety related modules are documented per the Module Test Verification Plan/Specification. Sample results files were reviewed. Results files indicate whether tests pass or fail. Static code analysis tools and code reviews are used to ensure that coding rules, documented in the coding standard, are enforced. Integration testing is done by running validation tests in development, using prototype hardware, prior to releasing code to quality assurance for final integration and validation with release candidate hardware.

Test management tools are used to manage the module and/or integration testing process.

5.8 Safety Validation

Validation Tests exist for each safety requirement (including software safety requirements) as shown by the requirements-to-validation traceability documentation. Each test case includes a procedure for the test as well as pass/fail criteria for the test (inputs, outputs and any other acceptance criteria). Validation test results are documented properly. The EMC/Environmental specifications tested (and passed) were the same as or more stringent than those reviewed and approved by the FMEDA analyst.

Fault injection testing has been performed on the product as defined in the fault injection test plan. The results have been analyzed and adjustments have been made to the FMEDA based on these results. Note that FIT is only required if claimed diagnostic coverage is over 90%.

Validation testing requires simulation of process inputs and timing between input changes (process simulation). This is done by testing the software in the product hardware and simulating the input signal(s) and other process conditions using test fixtures and test equipment.

5.9 Safety Manual

The Safety Manual is provided and identifies and describes (along with the operating manual, installation manual, etc.) the functions of the product. The functions are clearly described, including a description of the input and output interfaces. The behavior of the product's outputs is clearly described for all scenarios where internal faults are detected, including sufficient information to facilitate the development of an external diagnostics capability (output monitoring).

The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing. Procedures for maintaining tools and test equipment are listed.

All routine maintenance tools and activities required to maintain safety are identified and described in the Safety Manual.

The design includes a write-protect switch to prevent unauthorized (and accidental) modification via the HART interface.

The user manual defines what configuration options and methods exist for the product. The safety manual documents procedures required must be used to safely change the device configuration.

6 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FIT	Fault Injection Test
FMEDA	Failure Mode Effect and Diagnostic Analysis
FSM	Functional Safety Management
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
PFH	Probability of dangerous Failure per Hour
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).
SRS	Safety Requirements Specification
V&V	Verification & Validation
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

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

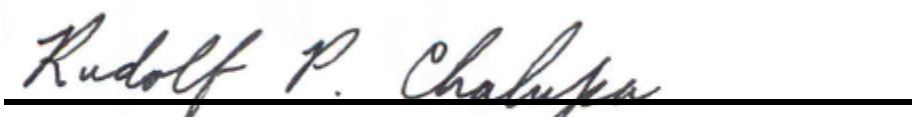
Version History:	V1, R0:	initial draft; Dave Butler, 9/24/2015
Authors:	Dave Butler	
Review:	Rudolf Chalupa exida, 9/22/2015	
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

David Butler, CFSE, Senior Safety Engineer



Rudolf P. Chalupa, Senior Safety Engineer