



Failure Modes, Effects and Diagnostic Analysis

Project:

Coriolis Flowmeter 1700 / 2700 Transmitter with 800 ECP

Customer:

Micro Motion

Boulder, CO

USA

Contract No.: MiMo 08/04-67r1

Report No.: MiMo 08/04-67r1 R001

Version V2, Revision R4, October 29, 2008

John C. Grebe - Rachel Amkreutz

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Micro Motion Coriolis Flowmeter using the CMF (Elite), T or F series sensor and 1700 / 2700 transmitter with a 800 ECP (Enhanced Core Processor). A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the flowmeter, electronic and mechanical.

The Coriolis flowmeter with 1700 / 2700 transmitter is a four wire, 4-20mA smart device. This product features MVD™ technology and diagnostics. It is designed specifically for applications where multiple variables are needed simultaneously. It has four optional output modules; the analog/frequency output module (Option Code A); the intrinsically safe output module (Option Code D); channels assigned to default values (Option Code B) and custom configured prior to shipment (Option Code C). The Coriolis flowmeter with 1700 transmitter is available with option codes A and D only. The 2700 transmitter is available with option codes A, B, C and D.

For safety instrumented systems usage it is assumed that one of the 4 – 20 mA outputs is used as the safety variable for mass flow, volume flow or density.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Micro Motion Coriolis Flowmeter.

Table 1 Version Overview

output code A	Micro Motion Coriolis Flowmeter with 1700/2700 transmitter with 800 ECP and analog output (output code A)
output code D	Micro Motion Coriolis flowmeter with 1700/2700 transmitter with 800 ECP and intrinsically safe analog output (output code D)
output codes B and C	Micro Motion Coriolis flowmeter with 2700 transmitter with 800 ECP and analog output (output codes B and C)

The flowmeter with 1700 / 2700 transmitter is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the device has a Safe Failure Fraction between 90 and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets architecture constraints up to SIL 2 @ HFT=0.

The failure rates for the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP and analog output (output code A) are listed in Table 2.

¹ Type B device: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 2 Coriolis Flowmeter, 1700 Transmitter with 800 ECP and analog output (output code A)

Failure category	Failure rate (in FIT)	
	Model Elite, T or F sensor	
Fail Safe Undetected	249	
Fail Dangerous Detected	2494	
Fail Detected (detected by internal diagnostic)	2419	
Fail High (detected by logic solver)	12	
Fail Low (detected by logic solver)	63	
Fail Dangerous Undetected	233	
Residual	436	
Annunciation Undetected	15	

The failure rates for the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP and intrinsically safe analog output (output code D) are listed in Table 3.

Table 3 Coriolis Flowmeter, 1700 Transmitter with 800 ECP and intrinsically safe analog output (output code D)

Failure category	Failure rate (in FIT)	
	Model Elite, T or F sensor	
Fail Safe Undetected	244	
Fail Dangerous Detected	2493	
Fail Detected (detected by internal diagnostic)	2409	
Fail High (detected by logic solver)	19	
Fail Low (detected by logic solver)	65	
Fail Dangerous Undetected	231	
Residual	446	
Annunciation Undetected	15	

The failure rates for the Micro Motion Coriolis flowmeter with 2700 transmitter with 800 ECP and analog output (output codes B and C) are listed in Table 4.

Table 4 Coriolis Flowmeter, 2700 Transmitter with 800 ECP and analog output (output code B and C)

Failure category	Failure rate (in FIT)	
	Model Elite, T or F sensor	
Fail Safe Undetected	246	
Fail Dangerous Detected	2576	
Fail Detected (detected by internal diagnostic)	2493	
Fail High (detected by logic solver)	15	
Fail Low (detected by logic solver)	68	
Fail Dangerous Undetected	230	
Residual	434	
Annunciation Undetected	15	

Table 5 lists the failure rates for the various Micro Motion Coriolis Flowmeter options according to IEC 61508 (assuming logic solver can detect both over-scale and under-scale currents and detected failures are sent low).

Table 5: Failure rates of Micro Motion Coriolis Flowmeter with 800 ECP according to IEC 61508

Device	λ_{SD}	λ_{SU}^2	λ_{DD}	λ_{DU}	SFF ³
Model Elite, T or F sensor – 1700 analog output (output code A)	0 FIT	700 FIT	2494 FIT	233 FIT	93.2%
Model Elite, T or F sensor – 1700 intrinsically safe analog output (output code D)	0 FIT	705 FIT	2493 FIT	231 FIT	93.3%
Model Elite, T or F sensor – 2700 analog output (output code B and C)	0 FIT	695 FIT	2576 FIT	230 FIT	93.4%

All failure rates are valid for the useful life of the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter, see Appendix A.

A user of the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

² It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

³ Safe Failure Fraction needs to be calculated on (sub)system level



Table of Contents

Management summary	2
1 Purpose and Scope	6
2 Project management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved	7
2.3 Standards / Literature used.....	7
2.4 Reference documents	8
2.4.1 Documentation provided by Micro Motion	8
2.4.2 Documentation generated by <i>exida</i>	8
3 Product description	10
4 Failure Modes, Effects, and Diagnostic Analysis	11
4.1 Description of the failure categories.....	11
4.2 Methodology – FMEDA, Failure rates	12
4.2.1 FMEDA.....	12
4.2.2 Failure rates	12
4.3 Assumptions	13
4.4 Results	14
5 Using the FMEDA results.....	17
5.1 PFD _{AVG} calculation Coriolis flowmeter with 1700 / 2700 transmitter	17
6 Terms and Abbreviations	18
7 Status of the document	19
7.1 Liability	19
7.2 Releases	19
7.3 Future enhancements of the document	20
7.4 Release Signatures.....	20
Appendix A: Lifetime of critical components	21
Appendix B: Proof tests to reveal dangerous undetected faults	22
B.1 Proof test 1.....	22
B.2 Proof test 2.....	22
B.3 Proof test 3	24
Appendix C: Common Cause for redundant transmitter configurations	25

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration per IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends Option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

This document shall describe the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter. From these failure rates, the Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 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 partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Micro Motion Manufacturer of the Coriolis flowmeter with 1700 / 2700 transmitter

exida Performed the hardware assessment according to Option 1 (see Section 1)

Micro Motion contracted *exida* in April 2008 with the hardware 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 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	<i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	Safety Equipment Reliability Handbook, 3 rd Edition, 2007	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	Goble, W.M. and Cheddie, H., 2005	Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISA, ISBN 1-55617-909-X

2.4 Reference documents

2.4.1 Documentation provided by Micro Motion

[D1]	EB-3100940, Rev G,	Schematic Diagram, Appvl, R Series Sensor
[D2]	EB-3100316, Rev K,	Schematic Diagram, Appvl, F100S, Sensor
[D3]	EB-3000842, Rev O,	Schematic Diagram, Appvl, CMF100 Sensor
[D4]	ES-20002951, Rev C	Schematic Diagram, 800 BFCore
[D5]	Part:4265.001, Rev B	Schematic Diagram, Output Board schematic
[D6]	4596011, Rev B	Schematic Diagram, Config IO
[D7]	ES-20006853 Rev C	Schematic Diagram, 1700-2700 PWR
[D8]	EB-4000128, Rev G,	Schematic Diagram, Appvl, Titan Sensors
[D9]	3775061 C	Schematic, Analog Feature Bd
[D10]	ES-20002949, Rev B	Schematic, 800 Terminal
[D11]	20002949, Rev D	Spreadsheet, BOM, 800 Terminal
[D12]	20002951, Rev G	Spreadsheet, BOM, 800 BFCore
[D13]	4265014, Rev C	Spreadsheet, BOM, 1700 ISO
[D14]	MMI-20006853 Rev D	Spreadsheet, BOM, 1700-2700 PWR
[D15]	4830014 Rev B	Spreadsheet, BOM, EMI Terminal
[D16]	4596014, Rev C	Spreadsheet, BOM, Config IO
[D17]	PS-00400, June 2002	Product Data Sheet Series 1000 and 2000 transmitters
[D18]	PS-00232, April 2002	Product Data Sheet Micro Motion Flowmeters
[D19]	MM 2700 Fault Injection Summary rev. 2.xls	Fault Injection Test Results
[D20]	20003460, Rev H	Assy, Potted Transmitter, ECP
[D21]	MMI SIL 700 SASRD_0.2.doc	1700/2700 Coriolis Flomenter System, Architecture and Safety Requirements Specification

2.4.2 Documentation generated by *exida*

[R1]	1700 Analog Feature mA Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 18, 2008
[R2]	2700 Config IO mA Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700



		transmitter, July 15, 2008
[R3]	1700-2700 Core CPU for IO sections.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 15, 2008
[R4]	800 Core and flow sensors.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP, July 18, 2008
[R5]	1700-2700 Gemini Main Power.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 16, 2008
[R6]	1700 IS Analog Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 15, 2008
[R7]	1700-2700 EMI term for Feature Bd mA Output.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 18, 2008
[R8]	1700-2700 Two RTD Adder.efm	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 18, 2008
[R9]	1700-2700 MicroMotion Failure Rate Summaries using 800 Core.xls	FMEDA Coriolis flowmeter with 1700 / 2700 transmitter, July 25, 2008
[R10]	MiMO 04-06-22 R005 V2 R2 800 ECP.doc	FMEDA report, Coriolis flowmeter with 1700 / 2700 transmitter, V2, R1, October 22, 2008 (this report)

3 Product description

Micro Motion flowmeters consist of Coriolis sensors and microprocessor-based transmitters that provide mass flow measurement of liquids, gases, and slurries. This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Micro Motion Coriolis Flowmeter, using the CMF (Elite), T or F series sensor and 1700 / 2700 transmitter with an 800 ECP (Enhanced Core Processor).

The Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter is a smart device used in many different industries for both control and safety applications. Model 1700 / 2700 features MVD™ technology and diagnostics. It allows for multivariable measurement of mass flow, volume flow, density, and temperature.

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 below defines the boundaries for the FMEDA.

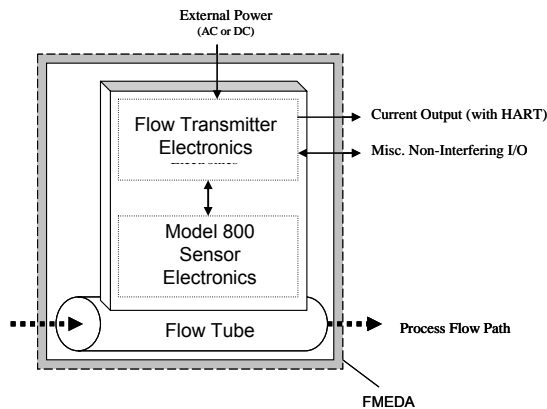


Figure 1, Micro Motion Coriolis Flowmeter, Parts included in the FMEDA

Table 6 gives an overview of the different versions that were considered in the FMEDA.

Table 6 Version Overview

output code A	Micro Motion Coriolis Flowmeter with 1700 transmitter with 800 ECP and analog output (output code A)
output code D	Micro Motion Coriolis flowmeter with 1700 transmitter with 800 ECP and intrinsically safe analog output (output code D)
output codes B and C	Micro Motion Coriolis flowmeter with 2700 transmitter with 800 ECP and analog output (output codes B and C)

The flowmeter with 1700 / 2700 transmitter is classified as a Type B⁴ device according to IEC 61508, having a hardware fault tolerance of 0.

⁴ Type B device: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostics Analysis performed on the Coriolis flowmeter with 1700 / 2700 transmitter is based on the documents provided by the customer (Section 2.4.1) and is documented in [R1] through [R10]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level.

4.1 Description of the failure categories

In order to judge the failure behavior of the Coriolis flowmeter with 1700 / 2700 transmitter, the following definitions for failure of the product were considered during the FMEDA.

Fail-Safe State	State where the process reaches a safe situation. Depending on the application the fail-safe state is defined as the output going to fail low or fail high.
Fail Safe	Failure that causes the module / (sub) system to go to the defined fail-safe state without a demand from the process. Safe failures are split into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 2% of span and that leaves the output within active scale (including frozen output).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous, but is detected by internal diagnostics (these failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (> 21.5mA, output saturate high)
Fail Low	Failure that that causes the output signal to go to the minimum output current. (< 3.6mA, output saturate low)
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Undetected	Failure that does not directly impact safety, but does impact the ability to detect a future fault (such as a fault in the diagnostic circuit) and that is not being diagnosed by internal diagnostics.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2000, the Residual failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

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.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension developed by *exida*. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook which was derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class D (Outdoor Locations). It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter.

- Only a single component failure will fail the entire transmitter.
- Failure rates are constant, wear-out mechanisms are not included
- Propagation of failures is not relevant
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded
- The stress levels are average for an industrial environment and can be compared to the IEC 60654-1, Class Dx (outdoor location) with temperature limits within the manufacturer’s rating. Other environmental characteristics are assumed to be within manufacturer’s rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions
- The device is installed per manufacturer’s instructions
- External power supply failure rates are not included
- Worst-case internal fault detection time is 5 minutes

4.4 Results

Using reliability data extracted from the exida component reliability database the following failure rates resulted from the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter FMEDA.

The failure rates for the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP and analog output (output code A) are listed in Table 7.

Table 7 Coriolis Flowmeter, 1700 Transmitter with 800 ECP and analog output (output code A)

Failure category	Failure rate (in FIT)	
	Model Elite, T or F sensor	
Fail Safe Undetected	249	
Fail Dangerous Detected	2494	
Fail Detected (detected by internal diagnostic)	2419	
Fail High (detected by logic solver)	12	
Fail Low (detected by logic solver)	63	
Fail Dangerous Undetected	233	
Residual	436	
Annunciation Undetected	15	

The failure rates for the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP and intrinsically safe analog output (output code D) are listed in Table 8.

Table 8 Coriolis Flowmeter, 1700 Transmitter with 800 ECP and intrinsically safe analog output (output code D)

Failure category	Failure rate (in FIT)	
	Model Elite, T or F sensor	
Fail Safe Undetected	244	
Fail Dangerous Detected	2493	
Fail Detected (detected by internal diagnostic)	2409	
Fail High (detected by logic solver)	19	
Fail Low (detected by logic solver)	65	
Fail Dangerous Undetected	231	
Residual	446	
Annunciation Undetected	15	

The failure rates for the Micro Motion Coriolis flowmeter with 2700 transmitter with 800 ECP and analog output (output codes B and C) are listed in Table 9.

Table 9 Coriolis Flowmeter, 2700 Transmitter with 800 ECP and analog output (output code B and C)

Failure category	Failure rate (in FIT)	
	Model Elite, T or F sensor	
Fail Safe Undetected	246	
Fail Dangerous Detected	2576	
Fail Detected (detected by internal diagnostic)	2493	
Fail High (detected by logic solver)	15	
Fail Low (detected by logic solver)	68	
Fail Dangerous Undetected	230	
Residual	434	
Annunciation Undetected	15	

These failure rates are valid for the useful lifetime of the product, see Appendix A: Lifetime of critical components

Table 10 lists the failure rates for the various Micro Motion Coriolis Flowmeter options according to IEC 61508 (assuming logic solver can detect both over-scale and under-scale currents and detected failures are sent low).

Table 10: Failure rates of Micro Motion Coriolis Flowmeter with 800 ECP according to IEC 61508

Device	λ_{SD}	λ_{SU}^5	λ_{DD}	λ_{DU}	SFF ⁶
Model Elite, T or F sensor – 1700 analog output (output code A)	0 FIT	700 FIT	2494 FIT	233 FIT	93.2%
Model Elite, T or F sensor – 1700 intrinsically safe analog output (output code D)	0 FIT	705 FIT	2493 FIT	231 FIT	93.3%
Model Elite, T or F sensor – 2700 analog output (output code B and C)	0 FIT	695 FIT	2576 FIT	230 FIT	93.4%

⁵ It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

⁶ Safe Failure Fraction needs to be calculated on (sub)system level



As can be seen from Table 10, the SFF varies with output options and sensor types chosen, but should generally be assumed to be above 90%.

The architectural constraint type for the Coriolis flowmeter with 1700 / 2700 transmitter is B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

5 Using the FMEDA results

5.1 PFD_{AVG} calculation Coriolis flowmeter with 1700 / 2700 transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP and analog output (Output code A) and Model Elite, T or F sensor. The failure rate data used in this calculation is displayed in section 4.4.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 2. As shown in the figure the PFD_{AVG} value for a single Coriolis flowmeter with 1700 / 2700 transmitter with 800 ECP and a proof test interval of 1 year equals 1.91E-03.

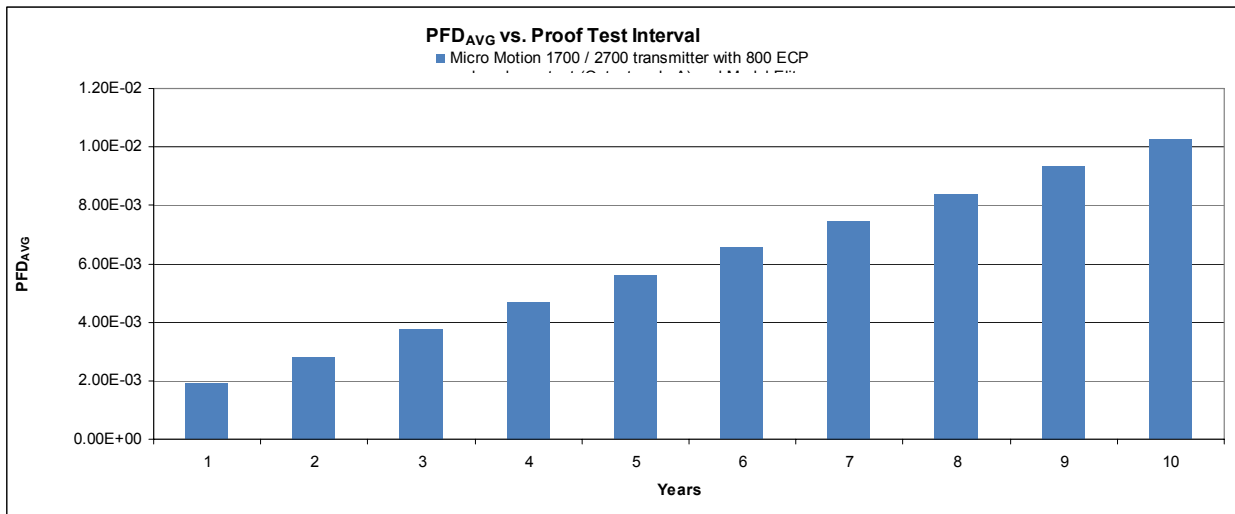


Figure 2 PFD_{AVG} values 1700 / 2700 Coriolis flowmeter

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

For SIL 2 applications, the PFD_{AVG} value needs to be $\geq 10^{-3}$ and $< 10^{-2}$. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 19.1% of the range.

These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Abbreviations

ECP	Enhanced Core Processor
E/E/PES	Electrical/Electronic/Programmable Electronic System
FIT	1×10^{-9} failures per hour
FMEDA	Failure Modes, Effects and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIF	Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	“Non-Complex” component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

exida prepares FMEDA 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.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version:	V2
Revision:	R4
Version History:	V2, R4: Updated per review, MicroMotion, October 29, 2008 V2, R3: Edited per review, W. Goble, October 22, 2008. V2, R2: Updated per most recent template, R. Chalupa, October 17, 2008 V2, R1: Created version for models using 800 ECP; Aug 14, 2008 V1, R3: Management Summary; December 1, 2005 V1, R2: 1700 / 2700 transmitter, Appendix A; November 16, 2005 V1, R1: Released to TÜV for assessment, November 29, 2004 V0, R1: Update to report MiMo 03/05-01 R002, to include fault injection test results, November 29, 2004
Authors:	John C. Grebe – Rachel Amkreutz
Review:	V0, R1: Iwan van Beurden (<i>exida</i>) V1, R2: Al Samson (Micro Motion), November 30, 2005 V2, R1: Rudolf Chalupa, October 17, 2008 V2,R2: William Goble, October 22, 2008



V2, R3: Ezra Sobel (Micro Motion), October 28, 2008

Release status: Released to client

7.3 Future enhancements of the document

At request of client.

7.4 Release Signatures

A handwritten signature in black ink, appearing to read "William M. Goble".

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink, appearing to read "John C. Grebe".

John C. Grebe, Partner

A handwritten signature in black ink, appearing to read "Rachel Amkreutz".

Rachel Amkreutz, Safety Engineer

Appendix A: Lifetime of critical components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method, this only applies provided that the useful lifetime⁷ of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 11 shows which electrolytic capacitors are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 11: Useful lifetime of electrolytic capacitors contributing to λDU

Component	Useful Life
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours
Capacitor (electrolytic) – Aluminum electrolytic, non-solid electrolyte	Approx. 90,000 hours

It is the responsibility of the end user to maintain and operate the Micro Motion Coriolis flowmeter with 1700 / 2700 transmitter per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

The aluminium electrolytic capacitors are the limiting factors with regard to the useful lifetime of the system. The aluminium electrolytic capacitors have an estimated useful lifetime of about 10 years. According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

⁷ Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B: Proof tests to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Proof test 1

Proof test 1 consists of a simple HART driven min to max output test, as described in Table 12. This test will detect approximately 56% of possible DU failures in the transmitter.

Table 12 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value ⁸ .
3	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value ⁹ .
4	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
5	Verify all safety critical configuration parameters
6	Restore the loop to full operation
7	Remove the bypass from the safety PLC or otherwise restore normal operation

B.2 Proof test 2

An alternative proof test 2 consisting of proof test 1 with meter verification, verification of the flowtube temperature measurement and a restart of the sensor (to detect soft errors in RAM) will detect approximately 91% of possible DU failures in the flowmeter resulting in a Proof Test Coverage of 91% for the flowmeter.

⁸ This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

⁹ This tests for possible quiescent current related failures.

Table 13 Steps for Proof Test 2

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value ¹⁰ .
4	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value ¹¹ .
5	Use the HART communicator to read the flowtube temperature sensor reading and check for a reasonable reading based on process temperature.
5	<p>Initiate a “Force Hard Reboot” command via Modbus Coil 41.</p> <p>With a 375 HART Communicator:</p> <ol style="list-style-type: none"> Select 5 – Detailed Setup Select 9 – Modbus Data Select 2 – Write Modbus Data Value Select 1 – Coil Enter in the value “41” – Enter Select 2 – On 375 Display reads “Coil Value is On and Exception Code is 0” 2700 Display (if present) reads “reading Core” Wait ~40 seconds for core processor and 2700 to return to normal operation Select – OK and then exit <p>With Prolink via Modbus</p> <ol style="list-style-type: none"> From the menu – Prolink-Configuration Select Modbus tab Location Type: Coil Starting Address: 41 Value: 1 Select – Write 2700 Display (if present) reads “reading Core” wait ~40 seconds for core processor and 2700 to return to normal operation
6	Perform the meter verification per Section 10.3 of the Configuration and Use Manual.
7	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
8	Verify all safety critical configuration parameters
9	Restore the loop to full operation
10	Remove the bypass from the safety PLC or otherwise restore normal operation

¹⁰ This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

¹¹ This tests for possible quiescent current related failures.



B.3 Proof test 3

For more complete proof test coverage, tests from Proof test 2 can be extended to include a full calibration against a primary standard. This complete calibration along with Proof test 2 will detect an estimated 99% of DU failures.



Appendix C: Common Cause for redundant transmitter configurations

A method for estimating the beta factor is provided in IEC 61508 – 6. Based on this approach, a Beta Factor of 5% may be used based on factors under control of the manufacturer. If the owner-operator of the plant would institute common cause training and maintenance procedures specifically oriented toward common cause defense, a Beta Factor of 2% could be used.

Note that it was assumed that the safety instrumented function would not automatically be shutdown when a diagnostic failure is detected.