Proven In Use Assessment

Project:
MVD 1700/2700 Flow Transmitter

Customer:

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

Contract No.: MiMo 04/06-22
Report No.: MiMo 04/06-22 R001
Version V1, Revision R1, October 4, 2004
William M. Goble - Iwan van Beurden

Management summary

This document describes the Proven In Use Assessment for the Micro Motion MVD 1700/2700 Flow Transmitter based on the MVD 1700/2700 Field Failure Report [D1] provided by Micro Motion.

The Proven In Use Assessment is performed per prior use requirements in the functional safety standard IEC 61508. Where applicable the interpretation of the requirements was performed per the internal exida.com Proven In Use Evaluation Criteria document.

Based on a worst case analysis, it is concluded that the Micro Motion MVD 1700/2700 Flow Transmitter meets the quantitative prior use requirements based on the field return information.

From the field return data provided a worst case overall device field failure rate was derived.

$\lambda =$ $673 * 10^{-9}$ failures per hour

Since this experienced (worst case) field failure rate is smaller than the failure rate calculated in the FMEDA (random failures only) for the MVD 1700/2700 Flow Transmitter there is no indication of any systematic failures.

Table of Contents

Management summary 2

1 Purpose and Scope 4

2 Project management 5

2.1 *exida.com* 5

2.2 Roles of the parties involved 5

2.3 Standards / Literature used 5

2.4 Reference documents 5

2.4.1 Documentation provided by the customer 5

2.4.2 Documentation generated by exida.com 5

3 Proven In Use Assessment 6

3.1 IEC 61508 Proven In Use requirements 6

3.1.1 IEC 61508-2 Clause 7.4.7.6 6

3.1.2 IEC 61508-2 Clause 7.4.7.7 7

3.1.3 IEC 61508-2 Clause 7.4.7.8 8

3.1.4 IEC 61508-2 Clause 7.4.7.9 8

3.1.5 IEC 61508-2 Clause 7.4.7.10 8

3.1.6 IEC 61508-2 Clause 7.4.7.11 9

3.1.7 IEC 61508-2 Clause 7.4.7.12 9

4 Terms and Definitions 10

5 Status of the document 11

5.1 Liability 11

5.2 Releases 11

5.3 Future Enhancements 11

5.4 Release Signatures 11

Appendix A *exida* Key Proven In Use Criteria 12

A.6.1 ISO9000 or better 13

A.6.2 Field Failure Return Procedures 13

A.6.3 Version / Modification Control 13

A.6.4 Development Process 13

1 Purpose and Scope

This document describes the Proven In Use Assessment for the Micro Motion MVD 1700/2700 Flow Transmitter based on the MVD 1700/2700 Field Failure Report [D1] provided by Micro Motion.

The Proven In Use Assessment is performed per prior use requirements in the functional safety standard IEC 61508. Where applicable the interpretation of the requirements was performed per the internal exida.com Proven In Use Evaluation Criteria document.

The actual Proven In Use Assessment is described in chapter 3 of this document. This chapter provides an overview of specific IEC 61508 requirements relating to prior use of equipment and the benefits of performing a Proven In Use Assessment for claims on the achieved Safety Integrity Level of an equipment item.

Specific subjects addressed are the IEC 61508 Proven In Use requirements in section 3.1. Note that the modification process which is usually considered in a Proven In Use assessment is considered outside the scope of this report as the modification process will be assessed as part of the IEC 61508 certification.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 100 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Micro Motion, Inc. Manufacturer of the MVD 1700/2700 Flow Transmitter

exida.com Project leader of the Proven In Use Assessment

Micro Motion, Inc. contracted *exida.com* with the product IEC 61508 certification assistance of the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	IEC 61511: 2003	Functional Safety – Safety Instrumented Systems for the process industry sector
[N3]	Proven In Use Evaluation Criteria, R0.3, July 2003	exida.com Proven In Use Evaluation Criteria, Internal document

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	MVD 1700/2700 Field Failure Report, August 27, 2004	Field Failure Report provided by Micro Motion, Inc. to exida as partial requirement towards IEC 61508 certification for Micro Motion's MVD transmitter models 1700/2700

2.4.2 Documentation generated by exida.com

[R1]	MiMo 04-06-22 R001 v1r1 MVD 1700_2700_PIU .doc, October 4, 2004	Proven In Use Assessment report Micro Motion MVD 1700/2700 Flow Transmitter, Internal Draft
[R2]	Field failure analysis Micro Motion 1700_2700.xls, October 4, 2004	exida field failure analysis summary spreadsheet to calculate failure rates based on field experience

3 Proven In Use Assessment

The functional safety standard IEC 61508 has specific requirements with regard to Proven In Use considerations for existing products. It is the interpretation of exida that in order for a product to be considered Proven In Use, that product will need to meet those specific proven in use requirements as well as all modification process requirements. These requirements are listed in both IEC 61508-2 and IEC 61508-3. Note that the modification process will be assessed as part of the IEC 61508 certification and is therefore outside of the scope of this report.

The relevant requirements and their reference are listed in this section. For each requirement an argument is provided why the Micro Motion MVD 1700/2700 Flow Transmitter meets this requirement.

3.1 IEC 61508 Proven In Use requirements

3.1.1 IEC 61508-2 Clause 7.4.7.6

"A previously developed subsystem shall only be regarded as proven in use when it has a clearly restricted functionality and when there is adequate documentary evidence which is based on the previous use of a specific configuration of the subsystem (during which time all failures have been formally recorded, see 7.4.7.10), and which takes into account any additional analysis or testing, as required (see 7.4.7.8). The documentary evidence shall demonstrate that the likelihood of any failure of the subsystem (due to random hardware and systematic faults) in the E/E/PE safety-related system is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved."

For a device to be considered proven-in-use the volume of operating experience needs to be considered. For the Micro Motion MVD 1700/2700 Flow Transmitter this information is obtained from the Operation Experience and Warranty Information [D1].

The Micro Motion MVD 1700/2700 Flow Transmitter was first introduced in July 2001. In this time period there have been no significant revisions or changes to the design.

The operating experience and warranty information [D1] indicates that the total number of shipped units during this time period is approximately 51,431. For failure rates calculated on the basis of field returns only the hours recorded during the warranty period of the manufacturer are used, since this is the only time frame when failures can be expected to be reported. It must be assumed that all failures after the warranty period are not reported to the manufacturer.

Micro Motion calculated estimated operational hours [D1] as:

Operation Hours = 332,266,320 hrs

These operating hours are considered to be sufficient taking into account the medium complexity of the sub-system and the use in SIL 3 safety functions.

The operating experience and warranty information [D1] indicates that two field failure studies were performed. Returns in the period July 2001 to July 2002 and returns in the period July 2003 to July 2004 were analyzed. In the July 2001 to July 2002 period 82 units were returned. From these 82 units 14 failures were clearly systematic failures, guide pin damage. Since the first study this problem was solved by creating more robust guide pins. Consequently a worst case assessment concludes that 68 random hardware failures were discovered in the July 2001 to July 2002 period. The second field failure study from July 2003 to July 2004 reports only 14 failures. This shows a clear trend of decreasing number of field failures, which is to be expected when the bathtub curve (failure rate as a function of time) is considered. Therefore a worst case assumption would be to assume that in the July 2002 to July 2003 period the same amount of field failures is reported as in the initial July 2001 to July 2002 period. Consequently it is concluded that a total of 150 (=68+68+14) field failures are reported.

There is no evidence that all devices are returned when a failure occurs within the warranty period. Therefore it is to be assumed that only 70% of failures are returned per exida criteria [N3]. This leads to the following number of estimated failures for the Micro Motion MVD 1700/2700 Flow Transmitter.

Estimated failures = 150 / 0.7 = 215 failures

From this information, an overall failure rate for the Mirco Motion MVD 1700/2700 Flow Transmitter can be calculated. The failure rate point estimate yields 6.47E-07 [1/hr]. IEC 61508 requires the calculation of a 70% upper confidence limit for the failure rate. Given the data above the 70% upper confidence limit for the failure rate equals 6.73E-07 [1/hr].

This information must be compared to the information obtained from a Failure Modes, Effects and Diagnostic Analysis of the product. The failure rates calculated from the field data must be less than the failure rates obtained from the FMEDA. If the field failure rate is larger this is an indication of serious systematic design issues.

The FMEDA shows that the Micro Motion MVD 1700/2700 Flow Transmitter has a failure rate of over 2.00E-06 [1/hr] for various flow transmitter configurations. This excludes the No Effect failures since these will not cause a failure of the product and therefore will not result in the return of the product. Based on the 70% upper confidence limits that are calculated, it is considered that the MVD 1700/2700 Flow Transmitter meets this requirement.

3.1.2 IEC 61508-2 Clause 7.4.7.7

"The documentary evidence required by 7.4.7.6 shall demonstrate that the previous conditions of use (see note) of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/E/PE safety-related system, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved.

NOTE The conditions of use (operational profile) include all the factors which may influence the likelihood of systematic faults in the hardware and software of the subsystem. For example, environment, modes of use, functions performed, configuration, interfaces to other systems, operating system, translator, human factors."

The updated MVD 1700/2700 Flow Transmitter will be used in similar applications and similar environments under similar environmental conditions as the existing MVD 1700/2700 Flow Transmitter. Consequently as the conditions of use are identical this requirement is met.

3.1.3 IEC 61508-2 Clause 7.4.7.8

"When there is any difference between the previous conditions of use and those which will be experienced in the E/E/PE safety-related system, then any such difference(s) shall be identified and there shall be an explicit demonstration, using a combination of appropriate analytical methods and testing, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved."

There is no difference between the previous conditions of use for the MVD 1700/2700 Flow Transmitter and the expected conditions of use for the updated MVD 1700/2700 Flow Transmitter. Therefore this requirement is met.

3.1.4 IEC 61508-2 Clause 7.4.7.9

"The documentary evidence required by 7.4.7.6 shall establish that the extent of previous use of the specific configuration of the subsystem (in terms of operational hours), is sufficient to support the claimed rates of failure on a statistical basis. As a minimum, sufficient operational time is required to establish the claimed failure rate data to a single-sided lower confidence limit of at least 70 % (see IEC 61508-7, annex D and IEEE 352). An operational time of any individual subsystem of less than one year shall not be considered as part of the total operational time in the statistical analysis (see note).

NOTE The necessary time, in terms of operational hours, required to establish the claimed rates of failure may result from the operation of a number of identical subsystems, provided that failures from all the subsystems have been effectively detected and reported (see 7.4.7.10). If, for example, 100 subsystems each work fault-free for 10,000 h, then the total time of fault-free operation may be considered as 1,000,000 h. In this case, each subsystem has been in use for over a year and the operation therefore counts towards the total number of operational hours considered."

For a failure rate the lower confidence limit the standard refers to is impractical, an upper confidence limit should be considered.

The calculated operational hours for the MVD 1700/2700 Flow Transmitter are *332,266,320*. These operating hours are considered to be sufficient taking into account the medium complexity of the sub-system and the use in SIL 3 safety functions only. A single sided upper confidence limit of 70% is calculated for the failure rate derived from the field failure data of the MVD 1700/2700 Flow Transmitter. As a result this requirement is met.

3.1.5 IEC 61508-2 Clause 7.4.7.10

"Only previous operation where all failures of the subsystem have been effectively detected and reported (for example, when failure data has been collected in accordance with the recommendations of IEC 60300-3-2) shall be taken into account when determining whether the above requirements (7.4.7.6 to 7.4.7.9) have been met."

Assuming 100% failure reporting is unrealistic irrespective of the failure data reporting and collection methods utilized. Consequently in the Proven In Use failure rate calculation it is assumed that only a percentage of the actual failures is reported during the warranty period. This percentage is 70%. Based on this assumption it is argued that this requirement is met.

3.1.6 IEC 61508-2 Clause 7.4.7.11

"The following factors shall be taken into account when determining whether or not the above requirements (7.4.7.6 to 7.4.7.9) have been met, in terms of both the coverage and degree of detail of the available information (see also 4.1 of IEC 61508-1):

a) the complexity of the subsystem;

b) the contribution made by the subsystem to the risk reduction;

c) the consequence associated with a failure of the subsystem;

d) the novelty of design."

Each of the factors listed in this clause have been considered in the above requirements. Consequently the MVD 1700/2700 Flow Transmitter Proven In Use considerations meet this requirement.

3.1.7 IEC 61508-2 Clause 7.4.7.12

"The application of a "proven-in-use" safety-related subsystem in the E/E/PE safety related system should be restricted to those functions and interfaces of the subsystem which meet the relevant requirements (see 7.4.7.6 to 7.4.7.10).

NOTE The measures 7.4.7.4 to 7.4.7.12 are also applicable for subsystems which contain software. In this case it has to be assured that the subsystem performs in its safety related application only that function for which evidence of the required safety integrity is given. See also 7.4.2.11 of IEC 61508-3."

The MVD 1700/2700 Flow Transmitter will only be used as a Proven In Use considered device when all requirements above have been met. Consequently the MVD 1700/2700 Flow Transmitter Proven In Use considerations meet this requirement.

4 Terms and Definitions

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
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.
MVD	MultiVariable Digital
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).
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

5 Status of the document

5.1 Liability

exida.com prepares PIU Assessment reports based on methods advocated in International standards. Usage and failure reports are obtained from the manufacturer. *exida.com* 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.

5.2 Releases

Version:	V1	
Revision:	R1	
Version History:	V0, R1:	Internal Draft; October 4, 2004
	V1, R1:	First Release; October 4, 2004
Authors:	William M. Goble - Iwan van Beurden	
Review:	William M. Goble	
Release status:	First Release	

5.3 Future Enhancements

At request of client.

5.4 Release Signatures

Ir. Iwan van Beurden, Senior Safety Engineer

Dr. William M. Goble, Principal Partner

Appendix A *exida* Key Proven In Use Criteria

This appendix displays the key proven in use criteria that are used by exida during a proven in use assessment to determine if for a particular device proven in use can be claimed.

A.1 Time In Use

- A product must be shipping for one year without any revisions or changes

  OR

- A product must be shipping for two years without any significant revisions or changes

A.2 Hours In Use

- 30,000,000 hours of estimated usage in a minimum of 10 different applications with stress conditions equal to or above average conditions of the application.
- Estimation rules
  - Installation dates, not shipment dates, shall be used for usage estimation. If installation dates are not available, it shall be assumed that installation occurs six months after shipment.
  - If the product has a wearout mechanism, it shall be assumed that all units operate no longer than the useful life period. It shall further be assumed that no wearout failures are reported to the manufacturer.

A.3 Failure Rate Calculation

Failure rates calculated on the basis of field returns shall use only hours recorded during the warranty period of the manufacturer. It shall be assumed that all failures after the warranty period are not reported to the manufacturer. A confidence interval of 70% shall be assumed per IEC 61508.

Without evidence to the contrary it shall be assumed that only 50% of the failed units are returned during the warranty period and that 0% are returned after warranty.

A.4 Failure Data Comparison

An FMEDA must be performed by or reviewed by *exida*. The failure rate calculated from field data must be less than the failure rate obtained by exida FMEDA techniques. If the field failure rate is larger this is an indication of serious systematic design issues and no proven in use report shall be issued.

In addition, the FMEDA results must show a Safe Failure Fraction greater than 80% (excluding thermocouples and RTDs). The FMEDA must be verified by fault insertion testing.

A.5 Safety Manual

The manufacturer must produce a safety manual meeting the requirements of IEC 61508 and this must be reviewed by exida before any proven in use report is issued.

Note: Since this Proven in Use Report is part of an IEC 61508 certification process the safety manual is one of the documents assessed during the eventual audit. As this Proven In Use Report will not be distributed to customers this criteria has not been assessed during the Proven In Use assessment.

A.6 Quality System

A.6.1 ISO9000 or better

The manufacturer must have an ISO 9000 (or better) certified quality system that covers all manufacturing operations and field failure returns.

A.6.2 Field Failure Return Procedures

Field failure return procedures must require that statistics be maintained on all field returns. When a trend is indicated by the statistics, the trend must be analyzed for root cause failure. The root cause failure reports must be communicated to those responsible for product improvement and a corrective action system must be in place to assure that corrective action is taken.

A.6.3 Version / Modification Control

The manufacturer must have a detailed version control system that identifies all changes and revisions. The product must be marked with sufficient information to allow the user to identify each revision. The modification requirements of IEC 61508 must be met.

A.6.4 Development Process

A process gap analysis must be performed per IEC 61508. For products that were first installed within the last two years, the process must meet SIL1 requirements. For products that were first installed more than two years ago, the modification process must meet all requirements for IEC 61508 SIL2.

Note: Since this Proven in Use Report is part of an IEC 61508 certification process the development process is part of the eventual audit. In this particular case the Micro Motion development process will be assessed as part of the IEC 61508 certification project. As this Proven In Use Report will not be distributed to customers this criteria has not been assessed during the Proven In Use assessment.