Failure Modes, Effects and Diagnostic Analysis

Project:

Rosemount Corporation 8732E Electromagnetic Flowmeter

Customer:

Rosemount Corporation
Eden Prairie, MN
USA

Contract No.: Rosemount Q06/11-25
Report No.: Rosemount 06-11-25 R001
Version V1, Revision R1, May 4, 2007
Rudolf Chalupa

Management summary

This report summarizes the results of the hardware assessment of the 8732E Electromagnetic Flowmeter. The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification of a device per IEC 61508. 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 8732E Flowmeter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 8732E Flowmeter is a four-wire 4 – 20 mA smart device used to measure process flow. The 8732E Flowmeter contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable.

The 8732E Flowmeter is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the transmitter has a safe failure fraction between 60 and 90%[2] (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 1as a single device in safety applications.

The failure rates for the 8732E Electromagnetic Flowmeter are listed in Table 1 and Table 2.

Table 1 Failure rates 8732E Flowmeter with AC Power

Failure category		Failure rate (in FIT)	
Fail Safe Undetected			31
Fail Dangerous Detected			916
	Fail Detected (detected by internal diagnostics)	788	
	Fail High (detected by the logic solver)	17	
	Fail Low (detected by the logic solver)	111	
Fail Dangerous Undetected			309
No Effect			240
Annunciation Undetected			13

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

[2] Provided that 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.

Table 2 Failure rates 8732E Flowmeter with DC Power

Failure category		Failure rate (in FIT)	
Fail Safe Undetected			31
Fail Dangerous Detected			910
	Fail Detected (detected by internal diagnostics)	778	
	Fail High (detected by the logic solver)	17	
	Fail Low (detected by the logic solver)	115	
Fail Dangerous Undetected			306
No Effect			243
Annunciation Undetected			13

Table 3 lists the failure rates for the 8732E Flowmeter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents. It is assumed that the probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

Table 3 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su} [3]	λ_{dd}	λ_{du}	SFF
8732E Flowmeter with AC Power	0 FIT	284 FIT	916 FIT	309 FIT	79.5%
8732E Flowmeter with DC Power	0 FIT	287 FIT	910 FIT	306 FIT	79.6%

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

A user of the 8732E Electromagnetic Flowmeter 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 along with all assumptions.

[3] It is important to realize that the “no effect” 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

Table of Contents

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 according to 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 hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 8732E Electromagnetic Flowmeter. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a sensor subsystem, including the 8732E Electromagnetic Flowmeter, meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508.

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 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety 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

Rosemount Corporation	Manufacturer of the 8732E Flowmeter
exida	Performed the hardware assessment per Option 1 (see Section 1)

Rosemount Corporation contracted *exida* in February 2007 for the FMEDA of the 8732E Flowmeter.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical and Mechanical Component Handbook, exida, 2006	Electrical and Mechanical Component Handbook
[N3]	Safety Equipment Reliability Handbook, 2003	exida L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[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

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Corporation

[D1]	08732-0810.pdf	Schematic Drawing, 8732 RFI Suppression, Rev. AA, 07/13/06
[D2]	08732-0820.pdf	Schematic, 8732E Magmeter DSP Board, Rev. AE, 01/03/07
[D3]	08732-0823.pdf	Schematic, 8732E Magmeter Power Supply/Coil Drive, Rev. AC, 12/06/06
[D4]	08705-0003 Final Assembly Drawing.pdf	1.5 – 4 In. Flanged Meter Final Assembly, Rev. AU, 1/11/07
[D5]	08705-0145 Electrode Drawing.pdf	Electrode, 3 – 36 In.,Rev. AW, 4/21/06
[D6]	08705-2500 Lined Weldment Drawing.pdf	Lined Weldment, 1.5 – 4.0 In., Rev. BC, 12/4/06
[D7]	08705-3034 Coil Drawing.pdf	Coil Set, Rev. AC, 3/31/06

2.4.2 Documentation generated by *exida*

[R1]	Rosemount 06-11-25 R001 V0 R2 FMEDA MagMeter.doc, 05/04/2007	FMEDA report, 8732E Electromagnetic Flowmeter (this report)
[R2]	8732E Magmeter Summary.xls, 03/22/2007	Failure Modes, Effects, and Diagnostic Analysis – 8732E Flowmeter Summary
[R3]	8732E AC Power.xls, 03/22/2007	Failure Modes, Effects, and Diagnostic Analysis – 8732E Flowmeter AC Power Circuit
[R4]	8732E DC Power.xls, 03/22/2007	Failure Modes, Effects, and Diagnostic Analysis – 8732E Flowmeter DC Power Circuit
[R5]	8732E Coil Drive.xls, 03/22/2007	Failure Modes, Effects, and Diagnostic Analysis – 8732E Flowmeter Coil Drive Circuit
[R6]	8732E DSP Board.xls, 03/22/2007	Failure Modes, Effects, and Diagnostic Analysis – 8732E Electromagnetic Flowmeter Main (DSP) Circuit

3 Product Description

The Rosemount Corporation 8732E Electromagnetic Flowmeter is a four-wire, 4 – 20 mA smart device used in many different industries. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low, upon internal detection of a failure.

It is assumed that the 4 – 20 mA output is used as the primary safety variable. All other output variants are not covered by this report.

The 8732E Flowmeter is classified as a Type B[4] device according to IEC 61508, having a hardware fault tolerance of 0.

[4] Type B component: "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 Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by exida and is documented in [R1] through [R6]. This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the 8732E Flowmeter, the following definitions for the failure of the product were considered by Rosemount Corporation.

Fail-Safe State	The fail-safe state is defined as state where the output exceeds the user defined threshold.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 2% of span away from the fail-safe state and output remains in the active range.
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 which cause the output signal to go to the predefined alarm state.
Fail Safe Undetected	Failure that deviates the output toward the fail-safe state but is undetected by internal diagnostics.
Fail Safe Detected	Failure that deviates the output toward the fail-safe state but is detected by internal diagnostics which cause the output signal to go to the predefined alarm state.
Fail High	Failure that forces the output signal to go to the maximum output current (> 20.4mA).
Fail Low	Failure that forces the output signal to go to the minimum output current (< 4mA).
Fail Detected	Failure that causes the output to go to the predefined alarm state and that is detected by a connected logic solver.
Fail No Effect	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 a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High, a Fail Low, or Fail Detected failure can either 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.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected 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.

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 under 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. 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) 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 are from the exida proprietary component failure rate database. 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 C3. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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 8732E Flowmeter.

- Only a single component failure will fail the entire product
- 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 application program in the safety logic solver is configured to detect under-range (Fail Low), over-range (Fail High) and Fail Detected failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs and the diagnostic coverage provided by the online diagnostics.
- Transmitter is installed per the instructions and the requirements of the application.

- The stress levels are average for an industrial environment and can be compared To IEC 60654-1, Class C3 with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 30C. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

4.4 Results

The FMEDA described in [R1] – [R6] carried out by exida on the 8732E Flowmeter and under the assumptions described in section 4.3 leads to the following failure rates.

Table 4 and Table 5 list the failure rates for the 8732E Flowmeter.

Table 4 Failure rates 8732E Flowmeter with AC Power

Failure category		Failure rate (in FIT)	
Fail Safe Undetected			31
Fail Dangerous Detected			916
	Fail Detected (detected by internal diagnostics)	788	
	Fail High (detected by the logic solver)	17	
	Fail Low (detected by the logic solver)	111	
Fail Dangerous Undetected			309
No Effect			240
Annunciation Undetected			13

Table 5 Failure rates 8732E Flowmeter with DC Power

Failure category		Failure rate (in FIT)	
Fail Safe Undetected			31
Fail Dangerous Detected			910
	Fail Detected (detected by internal diagnostics)	778	
	Fail High (detected by the logic solver)	17	
	Fail Low (detected by the logic solver)	115	
Fail Dangerous Undetected			306
No Effect			243
Annunciation Undetected			13

The failure rates that are derived from the FMEDA for the 8732E Flowmeter are in a format different from the IEC 61508 format. Table 6 lists the failure rates for 8732E Flowmeter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of a sensor subsystem, including the 8732E Flowmeter, should be calculated. The SFF is the fraction of the overall failure rate of a subsystem that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formula for SFF:

$SFF = 1 - \lambda_{du} / \lambda_{total}$

Note that according to IEC61508 definition the No Effect and Annunciation Undetected failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

Table 6 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su} [5]	λ_{dd}	λ_{du}	SFF
8732E Flowmeter with AC Power	0 FIT	284 FIT	916 FIT	309 FIT	79.5%
8732E Flowmeter with DC Power	0 FIT	287 FIT	910 FIT	306 FIT	79.6%

The architectural constraint type for 8732E Flowmeter 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] It is important to realize that the “no effect” 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

5 Using the FMEDA results

5.1 Example PFD_{AVG} calculation for 8732E Flowmeter

An example average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 8732E Electromagnetic Flowmeter. The failure rate data used in this calculation is displayed in section 4.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} value for a single 8732E Flowmeter with AC power with a proof test interval of 12 months equals 1.36E-03. The PFD_{AVG} value for a single 8732E Flowmeter with DC power with a proof test interval of 12 months equals 1.35E-03.

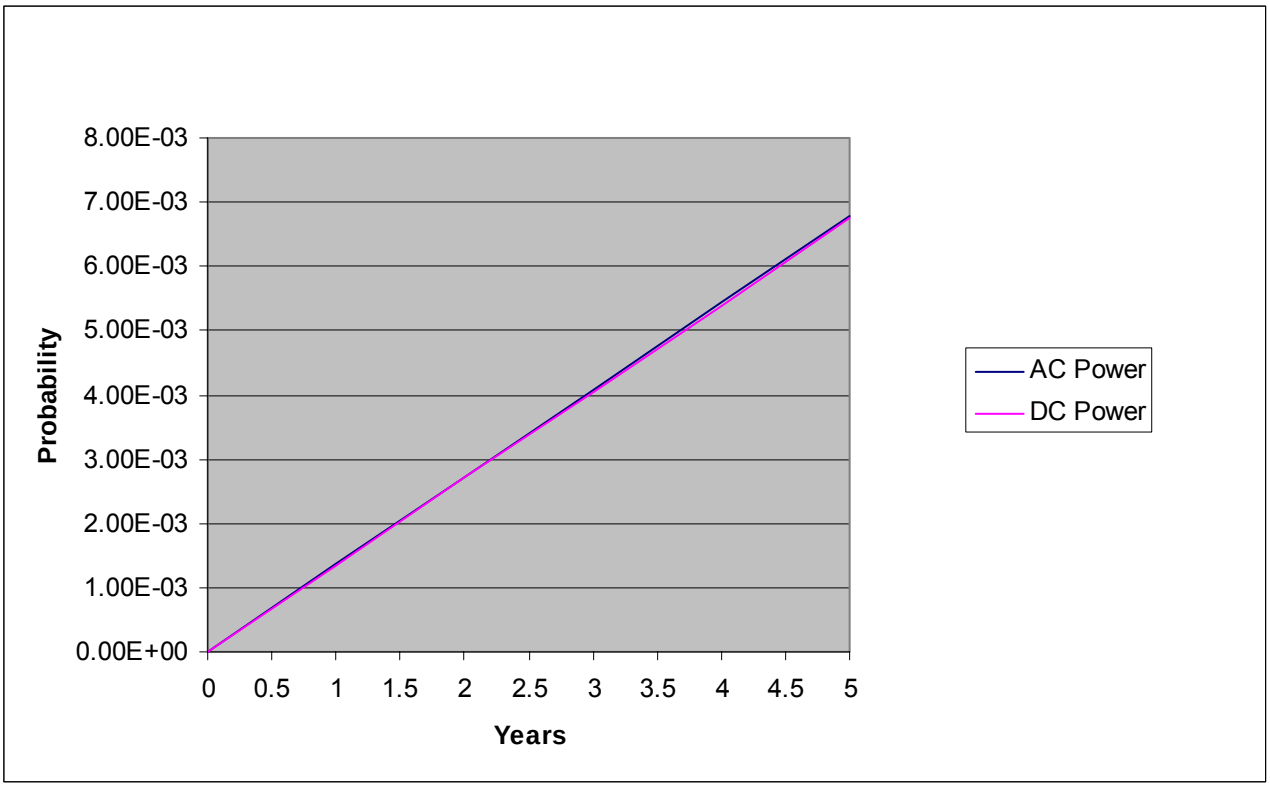


Figure 1 $PFD_{AVG}(t)$ 8732E Flowmeter

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF), considering the appropriate parameters such as proof test interval.

For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, the PFD_{AVG} for a 12 month Proof Test Interval of the 8732E Flowmeter with AC Power or with DC Power is equal to 1.4% of the range, allowing it to be used as a single device in safety applications.

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 Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
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 twice the proof test frequency.
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" subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	"Complex" subsystem (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

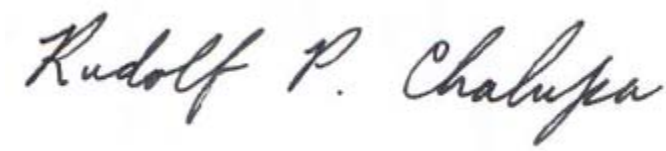
Version:	V1
Revision:	R1
Version History:	V1, R1: released to client, Rudolf Chalupa, May 4, 2007
	V0, R1: Draft; March 28, 2007
Authors:	Rudolf Chalupa
Review:	V0, R1: William Goble, May 3, 2007
Release status:	released to client

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Dr. William M. Goble, Principal Partner



Rudolf Chalupa

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 (see section 4.3) this only applies provided that the useful lifetime[6] 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 component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. 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 7 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 7 Useful lifetime of electrolytic components contributing to λ_{du}

Type	Useful life at 40°C
Capacitor (electrolytic) - Aluminum electrolytic, non-solid electrolyte	Approx. 90000 Hours[7]

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[6] 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.

[7] The operating temperature has a direct impact on this time. Therefore a small increase in the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.

Appendix B Proof test 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 FMEDA can be detected during proof testing.

B.1 Suggested proof test

A suggested proof test is described in Table 8. This test will detect approximately 84.5% of possible DU failures in the 8732E Flowmeter.

Table 8 Steps for Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Use HART communications to retrieve any diagnostics and take appropriate action.
3.	Use HART connection to run and review off-line diagnostics: • Flow simulator • Coil voltage and current monitoring • Forced analog output and readback of low alarm, high alarm, 4mA, 12mA, 20mA
4.	Use HART communications to read primary variable flow rate information (at moderate flow rate) and verify reasonability against independent flow rate estimation data.
5.	Return unit to normal operation
6.	Remove the bypass from the safety PLC or otherwise restore normal operation.