



Failure Modes, Effects and Diagnostic Analysis

Project:
8800D Vortex Flowmeter

Customer:
Rosemount
Chanhassen, MN
USA

Contract No.: ROS 06/03-34
Report No.: ROS 06/03-34 R001
Version V1, Revision R2, July 20, 2006
John Grebe - Rudolf Chalupa

Management summary

This report summarizes the results of the hardware assessment of the 8800D Vortex 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 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 8800D, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 8800D is a two-wire 4 – 20 mA smart device. 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. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable.

Table 1 lists the versions of the 8800D that have been considered for the hardware assessment.

Table 1 Version overview

1	8800D
2	8800D with MTA option (temperature probe)

The 8800D is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the 8800D has a safe failure fraction between 60% and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 1 as a single device.

The failure rates for the 8800D Vortex Flowmeter are listed in Table 2.

Table 2 Failure rates 8800D

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	571
Fail Detected (detected by internal diagnostics)	414
Fail High (detected by the logic solver)	47
Fail Low (detected by the logic solver)	110
Fail Dangerous Undetected	126
No Effect	183
Annunciation Undetected	5

The failure rates for the 8800D Vortex Flowmeter with MTA option are listed in Table 3.

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



Table 3 Failure rates 8800D with MTA option

Failure category	Failure rate (in FIT)
Fail Dangerous Detected	1104
Fail Detected (detected by internal diagnostics)	947
Fail High (detected by the logic solver)	47
Fail Low (detected by the logic solver)	110
Fail Dangerous Undetected	160
No Effect	205
Annunciation Undetected	6

Table 4 lists the failure rates for the 8800D 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 according to IEC 61508 (worst-case assumption).

Table 4 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}^2	λ_{dd}	λ_{du}	SFF
8800D	0 FIT	188 FIT	571 FIT	126 FIT	85.8%
8800D with MTA option	0 FIT	211 FIT	1104 FIT	160 FIT	89.2%

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

A user of the 8800D Vortex 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 4.4 along with all assumptions.

² 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

Management summary	2
1 Purpose and Scope	5
2 Project management.....	6
2.1 <i>exida</i>	6
2.2 Roles of the parties involved.....	6
2.3 Standards / Literature used.....	6
2.4 Reference documents.....	7
2.4.1 Documentation provided by Rosemount	7
2.4.2 Documentation generated by <i>exida</i>	7
3 Product Description.....	8
4 Failure Modes, Effects, and Diagnostics Analysis	9
4.1 Description of the failure categories.....	9
4.2 Methodology – FMEDA, Failure rates	10
4.2.1 FMEDA.....	10
4.2.2 Failure rates	10
4.3 Assumptions	10
4.4 Results	12
5 Using the FMEDA results.....	14
5.1 PFD_{AVG} calculation for 8800D	14
6 Terms and Definitions	15
7 Status of the document.....	16
7.1 Liability.....	16
7.2 Releases	16
7.3 Future Enhancements.....	16
7.4 Release Signatures.....	16
Appendix A: Lifetime of critical components	17
Appendix B Proof test to reveal dangerous undetected faults	18
B.1 Suggested proof test.....	18



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 DIN V VDE 0801, 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}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and 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 is an assessment by *exida* according to the relevant functional safety standard(s) like DIN V VDE 0801, 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}). In addition, this option includes an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This option for pre-existing (programmable electronic) devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of 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 DIN V VDE 0801, 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 is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) carried out on the 8800D Vortex Flowmeter. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

It shall be assessed whether the 8800D meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 1 subsystems according to IEC 61508.



2.4 Reference documents

2.4.1 Documentation provided by Rosemount

[D1]	08800-0001, Rev AV, 01/23/2006	Schematic Drawing, Vortex Flowmeter, Final Assembly
[D2]	08800-0300, Rev AC, 04/18/2006	Schematic Drawing, Temp Probe/Connector Assembly
[D3]	08800-5660, Rev AH, 06/02/2005	Schematic Drawing, Housing, Electronics, Die Cast, Mach, Painted
[D4]	08800-7606, Rev AF, 12/12/2005	Schematic Diagram, Vortex Terminal Board
[D5]	08800-7609, Rev AA, 10/15/1997	Schematic Diagram, Vortex LCD Board
[D6]	08800-7700, Rev AF, 02/28/2006	Schematic Drawing, Phoenix Vortex Sensor Board
[D7]	08800-7703, Rev AH, 08/02/2005	Schematic Drawing, Phoenix Output Board
[D8]	00813-0100-4004, Rev BA, March 2006	Product Data Sheet, Rosemount 8800D Series Vortex Flowmeter
[D9]	00809-0100-4004, Rev AA, April 2006	Preliminary Reference Manual, Rosemount 8800D Series Smart Vortex Flowmeter
[D10]	8800D_Support_Slides.ppt, 05/02/2006	8800D FMEDA Support Material
[D11]	MV Vortex.ppt	8800D Photographs

2.4.2 Documentation generated by exida

[R1]	ROS 06-03-34 R001 V1 R2 FMEDA 8800D.doc, 07/20/2006	FMEDA report, 8800D Vortex Flowmeter (this report)
[R2]	8800D Vortex Common 052606.xls	Failure Modes, Effects, and Diagnostic Analysis – 8800D Common Circuitry
[R3]	8800D MTA Sensor 052606.xls	Failure Modes, Effects, and Diagnostic Analysis – 8800D MTA Sensor
[R4]	8800D Vortex Pulse Output.xls, 05/26/2006	Failure Modes, Effects, and Diagnostic Analysis – 8800D Pulse Output
[R5]	8800D Vortex Summary 052606.xls	Failure Modes, Effects, and Diagnostic Analysis – 8800D Summary



3 Product Description

The 8800D Vortex Flowmeter is a smart device providing flow measurement of gases, liquids, and steam. It features a non-clogging sensor and an all-welded body that requires no process seals and purges fugitive emissions. The 8800D features HART communications as well as a Foundations Fieldbus interface and an optional pulse output. The 8800D is available as a dual assembly (ordering code 8800DD) which consists of two independent flowmeters welded into a single unit. For the purposes of this report, each dual flowmeter having dual shedder bars is considered to consist of two independent units.

For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. Other outputs are not covered by this report. The pulse output is not recommended for safety applications. The analog output meets NAMUR NE 43 (3.8mA to 20.5mA usable). The system contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. Table 5 lists the models of the 8800D that have been considered for the hardware assessment.

Table 5 Version overview

1	8800D
2	8800D with MTA option (temperature probe)

The 8800D is classified as a Type B³ device according to IEC 61508, having a hardware fault tolerance of 0.

³ 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 based on the information received from Rosemount, see [D1] through [D11] and is documented in [R1] through [R5]. 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 8800D, the following definitions for the failure of the product were considered by Rosemount.

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 and that leaves the output within active scale.
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 or a connected logic solver.
Fail Detected	Failure that causes the output to go to the defined alarm state (either High or Low).
Fail High	Failure that causes the output signal to go to the maximum output current (> 21.5mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.6mA)
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 or a Fail Low 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.

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 is from the *exida* proprietary component failure rate database derived using the Telcordia failure rate database/models, the SN29500 failure rate database and other sources. 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 C. 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 8800D.

- 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 HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the safety logic solver is configured to detect under-range (Fail Low) and over-range (Fail High) failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.



- The 8800D is available as a dual assembly (ordering code 8800DD) which consists of two independent flowmeters welded into a single unit. For the purposes of this report, each dual flowmeter having dual shedder bars is considered to consist of two independent units. The data in this report can also be used to calculate a 1oo2 voting achieved by a Dual Vortex meter, constructed of two complete vortex meters: sensor, electronics, and shedder bar.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
 - IEC 60654-1, Class C with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- 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.
- External power supply failure rates are not included.

4.4 Results

The FMEDA carried out by exida on the 8800D under the assumptions described in section 4.3 leads to the following failure rates. Table 6 lists the failure rates for the 8800D.

Table 6 Failure rates 8800D

Failure category		Failure rate (in FIT)	
Fail Dangerous Detected		571	
	Fail Detected (detected by internal diagnostics)	414	
	Fail High (detected by the logic solver)	47	
	Fail Low (detected by the logic solver)	110	
Fail Dangerous Undetected		126	
No Effect		183	
Annunciation Undetected		5	

The failure rates for the 8800D Vortex Flowmeter with MTA option are listed in Table 7.

Table 7 Failure rates 8800D with MTA option

Failure category		Failure rate (in FIT)	
Fail Dangerous Detected		1104	
	Fail Detected (detected by internal diagnostics)	947	
	Fail High (detected by the logic solver)	47	
	Fail Low (detected by the logic solver)	110	
Fail Dangerous Undetected		160	
No Effect		205	
Annunciation Undetected		6	

The failure rates that are derived from the FMEDA for the 8800D are in a format different from the IEC 61508 format. Table 8 lists the failure rates for 8800D 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 the 8800D should be calculated. The SFF is the fraction of the overall failure rate of a device 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 8 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}^4	λ_{dd}	λ_{du}	SFF
8800D	0 FIT	188 FIT	571 FIT	126 FIT	85.8%
8800D with MTA option	0 FIT	211 FIT	1104 FIT	160 FIT	89.2%

The architectural constraint type for 8800D 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.

⁴ 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 PFD_{AVG} calculation for 8800D

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) 8800D Vortex Flowmeter. 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 1. As shown in the figure the PFD_{AVG} value for a single 8800D with a proof test interval of 1 year equals 5.56E-04. The PFD_{AVG} value for a single 8800D with MTA option with a proof test interval of 1 year equals 7.09E-04.

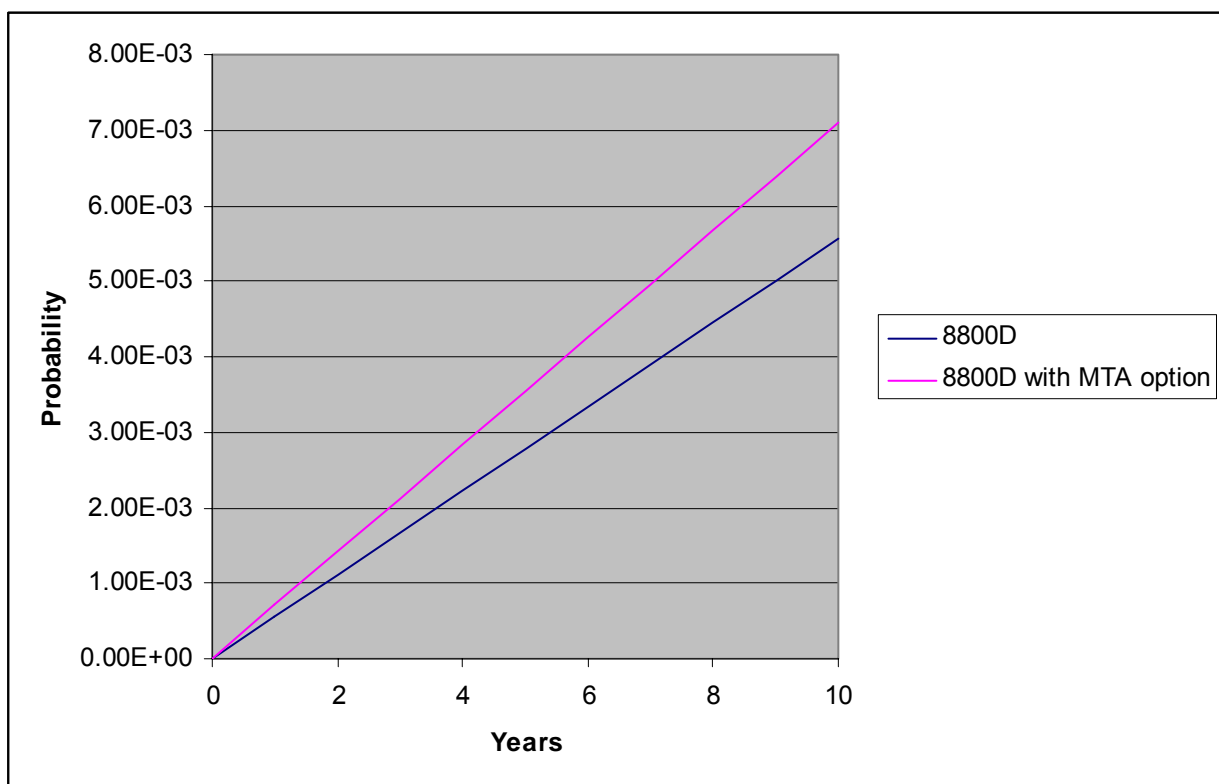


Figure 1 PFD_{AVG}(t) 8800D

For SIL 1 applications, the PFD_{AVG} value needs to be $\geq 10^{-2}$ and $< 10^{-1}$. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of the 8800D is equal to 0.6% of the range. Under the same conditions the PFD_{AVG} for a 1-year Proof Test Interval of the 8800D with MTA option is equal to 0.7% 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 Definitions

FIT	Failure In Time (1×10^{-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.
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.

7.2 Releases

Version: V0
Revision: R1
Version History: V1, R2 Added clarification for dual flowmeter assemblies, July 20, 2006
V1, R1 Updated per RA review, released; May 31, 2006
V0, R2 Updated proof test per JCG comments; May 31, 2006
V0, R1: Draft; May 26, 2006
Authors: John Grebe - Rudolf Chalupa
Review: V0, R1: John C. Grebe (*exida*); May 31, 2006
V0, R2: Rachel Amkreutz (*exida*); May 31, 2006
Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Handwritten signature of William M. Goble in black ink.

Dr. William M. Goble, Principal Partner

Handwritten signature of John C. Grebe in black ink.

John C. Grebe, Partner

Handwritten signature of Rudolf P. Chalupa in black ink.

Rudolf Chalupa, 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 (see section 4.3) this only applies provided that the useful lifetime⁵ 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 9 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 9 Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours

As there are no aluminum electrolytic capacitors used, the tantalum electrolytic capacitors are the limiting factors with regard to the useful lifetime of the system. The tantalum electrolytic capacitors that are used in the 8800D have an estimated useful lifetime of about 50 years.

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

⁵ 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 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 10. This test will detect approximately 82% of possible DU failures in the 8800D.

Table 10 Steps for Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Connect a HART communicator to the flowmeter. Connect a current measuring device into the loop. (The safety PLC can be used for this purpose if it can display the current while bypassing the 8800D in the logic solver.)
3.	Use the HART communicator to force the output current to 22.6mA and ensure this is measured at the output.
4.	Use the HART communicator to force the output current to 12mA and ensure this is measured at the output.
5.	Use the HART communicator to force the output current to 3.6mA and ensure this is measured at the output. Remove the output current force. Remove the HART communicator.
6.	Ensure that with no flow the output is 4mA.
7.	Provide flow through the Flowmeter; ensure that the current output corresponds to the flow. (Reasonability check)
8.	Restore the loop to full operation.
9.	Remove the bypass from the safety PLC or otherwise restore normal operation.