Failure Modes, Effects and Diagnostic Analysis

Project:
2051 Pressure Transmitter

Company:
Rosemount
Chanhassen, MN
USA

Contract Number: Q07/10-08r2
Report No.: Rosemount 07/10-08 R001
Version V1, Revision R1, April 29, 2008
Rudolf Chalupa

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 2051 Pressure Transmitter, hardware revision 1 and software revision 178. 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 2051. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

The 2051 is a pressure transmitter, or more accurately a series of pressure transmitters, utilizing either a capacitive (2051C) sensor in differential or gage modes or a resistive bridge (2051T) sensor in absolute or gage mode. The 2051C has dual interface diaphragms and can interface to a manifold; wherease the 2051T has a single process connection. Both transmitters are microprocessor-based and contain internal diagnostics as well as the ability to communicate via the HART digital protocol. For safety applications only the 4 to 20mA output is considered. Other outputs are not covered by this report.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the 2051.

Table 1 Version Overview

2051C	Capacitive Sensor, Differential or Gage
2051T	Resistive Bridge Sensor, Absolute or Gage

The 2051 is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the device 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 based on hardware architectural constraints.

The complete sensor subsystem, of which the 2051 is the sensor, will need to be evaluated to determine the Safe Failure Fraction.

The failure rates for the 2051 are listed in Table 2 and Table 3.

[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 Failure rates 2051C

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		0.0
Fail Dangerous Detected		227.9
Fail Detected (detected by internal diagnostics)	174.0	
Fail High (detected by logic solver)	31.0	
Fail Low (detected by logic solver)	22.9	
Fail Dangerous Undetected		46.4
Residual		63.4
Annunciation Undetected		6.3

Table 3 Failure rates 2051T

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		0.0
Fail Dangerous Detected		253.7
Fail Detected (detected by internal diagnostics)	194.9	
Fail High (detected by logic solver)	35.9	
Fail Low (detected by logic solver)	22.9	
Fail Dangerous Undetected		49.0
Residual		74.9
Annunciation Undetected		10.3

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

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

Table 4 lists the failure rates for the 2051 according to IEC 61508.

Table 4 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	**SFF**[3]
2051C	0 FIT	70 FIT	228 FIT	46 FIT	86.6%
2051T	0 FIT	85 FIT	254 FIT	49 FIT	87.4%

A user of the 2051 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 *exida* 7

2.2 Roles of the parties involved 7

2.3 Standards and Literature used 7

2.4 Reference documents 8

2.4.1 Documentation provided by Rosemount 8

2.4.2 Documentation generated by *exida* 8

3 Product Description 9

4 Failure Modes, Effects, and Diagnostic Analysis 10

4.1 Failure Categories description 10

4.2 Methodology – FMEDA, Failure Rates 11

4.2.1 FMEDA 11

4.2.2 Failure Rates 11

4.3 Assumptions 12

4.4 Results 12

5 Using the FMEDA Results 15

5.1 PFD_{AVG} Calculation 2051 15

6 Terms and Definitions 16

7 Status of the Document 17

7.1 Liability 17

7.2 Releases 17

7.3 Future Enhancements 17

7.4 Release Signatures 18

Appendix A Lifetime of Critical Components 19

Appendix B Proof tests to reveal dangerous undetected faults 20

B.1 Suggested Proof Test 20

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 hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 2051. 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 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

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

Rosemount	Manufacturer of the 2051
exida	Performed the hardware assessment according to Option 1 (see Section 1)

Rosemount contracted *exida* in October 2007 with the hardware assessment of the above-mentioned device.

2.3 Standards and 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, 2006	exida L.L.C, Electrical & Mechanical Component Reliability Handbook, 2006, ISBN 0-9727234-2-0
[N3]	Safety Equipment Reliability Handbook, 2nd Edition, 2005	exida L.L.C, Safety Equipment Reliability Handbook, Second Edition, 2005, ISBN 0-9727234-1-2
[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

[D1]	Doc # 03031-0581, Rev AG, February 1, 2008	Schematic Drawing, Microboard #5, 3051C
[D2]	Doc # 03031-0823, Rev AA, February 15, 2000	Schematic Drawing, Sensor Board, Saturn (2051C)
[D3]	Doc # 03031-0926, Rev AG, October 22, 2003	Schematic Drawing, Sensor, 3051TAC (2051T)
[D4]	Doc # 02051-4226, Rev AB, January 29, 2008	Schematic Drawing, 4-20mA Std. Terminal Block
[D5]	Doc # 02051-4229, Rev AB, February 1, 2008	Schematic Drawing, Transient, 4-20mA Terminal Block
[D6]	Doc # 02051-1001, Rev AA, January 18, 2008	Mechanical Assembly and Options, C/T FM and CSA Flameproof Configuration

2.4.2 Documentation generated by *exida*

[R1]	Rosemount 2051 Microboard.efm, March 11, 2008	Failure Modes, Effects, and Diagnostic Analysis – 2051 Microprocessor Board
[R2]	Rosemount 2051 Saturn Sensor (C).efm, March 11, 2008	Failure Modes, Effects, and Diagnostic Analysis – 2051 Saturn Sensor Board (2051C)
[R3]	Rosemount 2051 TAC Sensor (T).efm, March 11, 2008	Failure Modes, Effects, and Diagnostic Analysis – 2051 TAC Sensor Board (2051T)
[R4]	Rosemount 2051 Terminal block.efm, March 11, 2008	Failure Modes, Effects, and Diagnostic Analysis – 2051 Terminal Block
[R5]	Rosemount 2051 FMEDA Summary.xls, March 11, 2008	Failure Modes, Effects, and Diagnostic Analysis - Summary –2051
[R6]	Rosemount 07-10-08 FMEDA Report 2051 R001 V1 R1.doc, 04/29/2008	FMEDA report, 2051 (this report)

3 Product Description

The 2051 is a pressure transmitter, or more accurately a series of pressure transmitters, utilizing either a capacitive (2051C) sensor in differential or gage modes or a resistive bridge (2051T) sensor in absolute or gage mode. The 2051C has dual interface diaphragms and can interface to a manifold. The 2051T has a single process connection. Both transmitters are microprocessor based and contain internal diagnostics as well as the ability to communicate via the HART digital protocol.

For safety applications only the 4 to 20mA output is considered. Other outputs are not covered by this report.

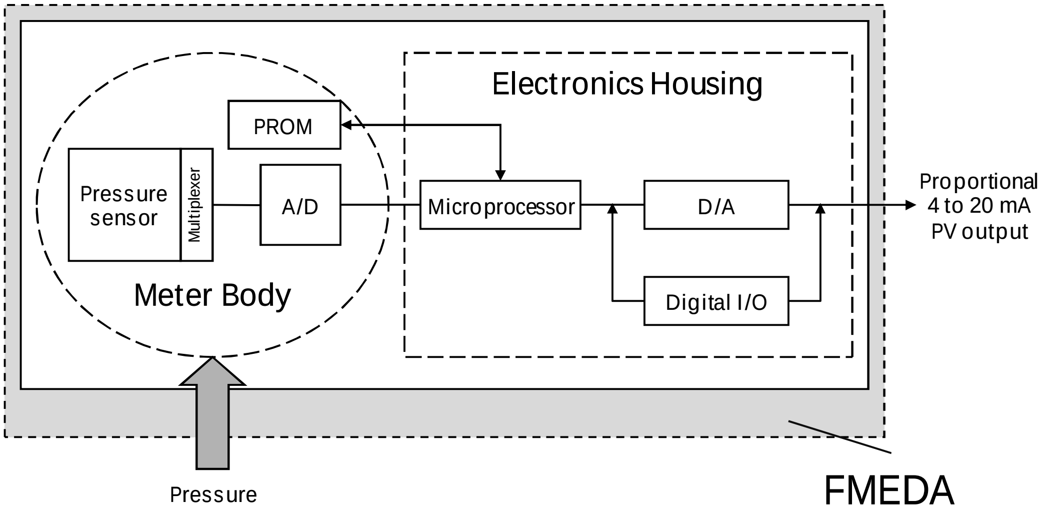

Figure 1 Parts included in the FMEDA - 2051 pressure transmitter

Table 5 gives an overview of the different versions that were considered in the FMEDA of the 2051.

Table 5 Version Overview

2051C	Capacitive Sensor, Differential or Gage
2051T	Resistive Bridge Sensor, Absolute or Gage

The 2051 is classified as a Type B[4] 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 Diagnostic Analysis was performed based on the documentation obtained from Rosemount and is documented in [R1] - [R6].

4.1 Failure Categories description

In order to judge the failure behavior of the 2051, the following definitions for the failure of the device were considered.

Fail-Safe State
State where the output exceeds the user defined threshold

Fail Safe
Failure that causes the device to go to the defined fail-safe state without a demand from the process.

Fail Detected
Failure that causes the output signal to go to the predefined alarm state (>21.6 mA).

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 automatic diagnostics

Fail Dangerous Detected
Failure that is dangerous but is detected by automatic diagnostics

Fail High
Failure that causes the output signal to go to the over-range or high alarm output current (>21.6mA)

Fail Low
Failure that causes the output signal to go to the under-range or low alarm output current(<3.4 mA)

Residual
Failure of a component that is part of the safety function but that has no effect on the safety function.

Annunciation Detected
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 detected by internal diagnostics.

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 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. 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 2051.

- Only a single component failure will fail the entire 2051
- 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 C3 (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
- 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 40ºC. 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.
- Worst-case internal fault detection time is 1 hour.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 2051 FMEDA.

Table 6 Failure rates 2051C

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		0.0
Fail Dangerous Detected		227.9
Fail Detected (detected by internal diagnostics)	174.0	
Fail High (detected by logic solver)	31.0	
Fail Low (detected by logic solver)	22.9	
Fail Dangerous Undetected		46.4
Residual		63.4
Annunciation Undetected		6.3

Table 7 Failure rates 2051T

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		0.0
Fail Dangerous Detected		253.7
Fail Detected (detected by internal diagnostics)	194.9	
Fail High (detected by logic solver)	35.9	
Fail Low (detected by logic solver)	22.9	
Fail Dangerous Undetected		49.0
Residual		74.9
Annunciation Undetected		10.3

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

Table 8 lists the failure rates for the 2051 according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However, as the 2051 may only be one part of a (sub)system, the SFF should be calculated for the entire sensor combination. The Safe Failure Fraction 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 formulas for SFF: SFF = 1 - $\lambda_{DU} / \lambda_{TOTAL}$

Table 8 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF[6]
2051C	0 FIT	70 FIT	228 FIT	46 FIT	86.6%
2051T	0 FIT	85 FIT	254 FIT	49 FIT	87.4%

The architectural constraint type for the 2051 is B. The hardware fault tolerance of the device is 0. 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 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

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 PFD$_{AVG}$ Calculation 2051

An average Probability of Failure on Demand (PFD$_{AVG}$) calculation is performed for a single (1oo1) 2051. 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 graph the PFD$_{AVG}$ value for a single 2051C, with a proof test interval of 1 year equals 2.04E-04. The PFD$_{AVG}$ value for a single 2051T, with a proof test interval of 1 year equals 2.17E-04.

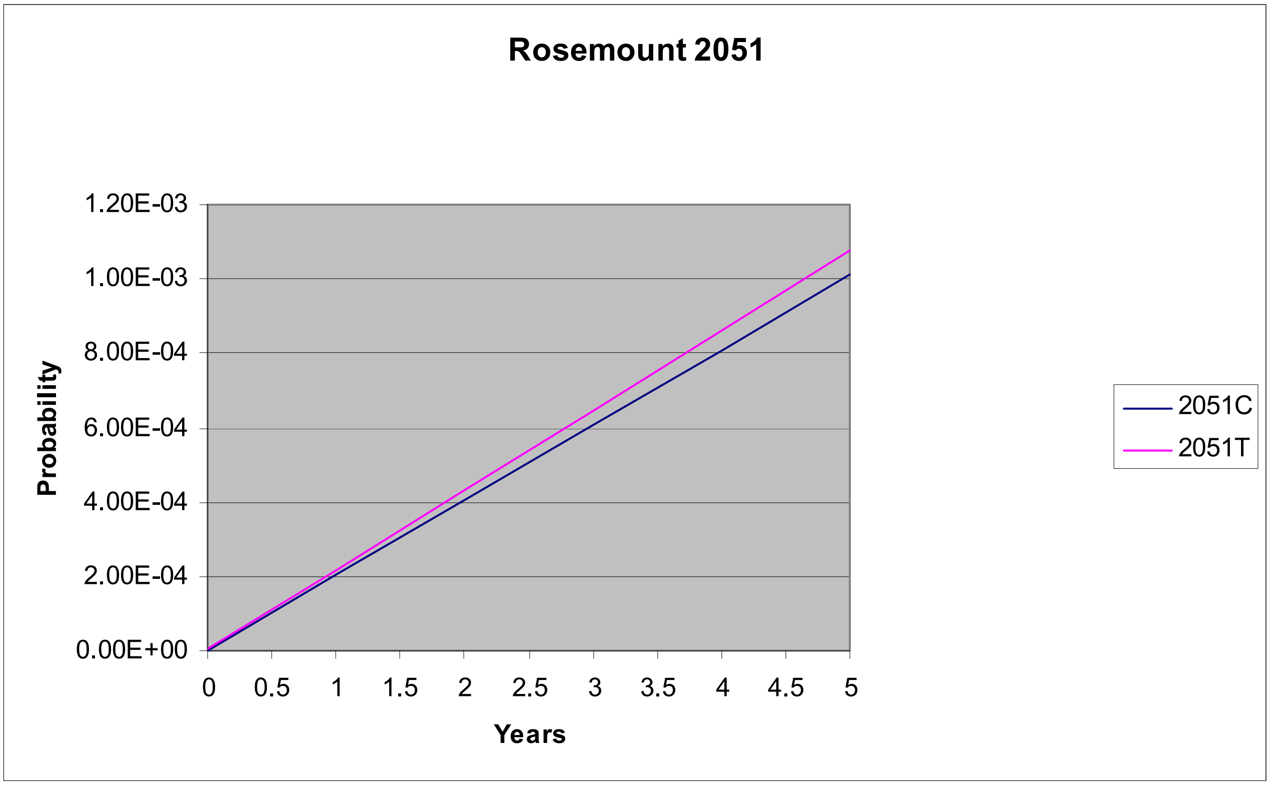

Figure 2: PFDavg vs. Time

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 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 1-year Proof Test Interval of the 2051C or 2051T is approximately equal to 0.2% 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 (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" component (using discrete elements); for details see 7.4.3.1.2 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:	V1	
Revision:	R1	
Version History:	V1, R1:	Released to Rosemount; April 29, 2008
	V0, R1:	Draft; April 1, 2008
Author(s):	Rudolf Chalupa	
Review:	V0, R1:	Rachel Amkreutz (exida); April 29, 2008
Release Status:	Released to Rosemount	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

William M Goble

Dr. William M. Goble, Principal Partner

Rudolf P. Chalupa

Rudolf P. Chalupa, Senior Safety Engineer

John C. Grebe Jr., Principal 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 4.2.2) this only applies provided that the useful lifetime[7] 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 17 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 components contributing to dangerous undetected failure rate

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

It is the responsibility of the end user to maintain and operate the 2051 per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

As there are no aluminum electrolytic capacitors used, the limiting factors with regard to the useful lifetime of the system are the Tantalum electrolytic capacitors. The Tantalum electrolytic capacitors 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.

[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 Suggested Proof Test

The suggested proof test consistist of the following steps, see Table xx. This test will detect > 99% of possible DU failures in the device.

Table 10 Suggested Proof Test – 2051 Pressure Transmitter

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Use HART communications to retrieve any diagnostics and take appropriate action.
3.	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].
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[9].
5.	Perform a two-point calibration[10] of the transmitter over the full working range.
6.	Remove the bypass and otherwise restore normal operation

[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.

[10] If the two-point calibration is performed with electrical instrumentation, this proof test will not detect any failures of the sensor