Failure Modes, Effects and Diagnostic Analysis

Project:
644 4-20mA / HART Temperature Transmitter

Company:
Rosemount Inc.
(an Emerson Process Management company)
Shakopee, MN
USA

Contract Number: Q13/10-107
Report No.: ROS 11/02-058 R001
Version V2, Revision R2, January 23, 2015
Griff Francis

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 644 4-20mA / HART Temperature Transmitter, hardware revision 1 and software revision 1.1.X. 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 are determined. The FMEDA that is described in this report concerns only the hardware of the 644 Temperature Transmitter. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 644 Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. This analysis includes the optional T1 transient protector. The transmitter can be equipped with or without display.

The 644 Temperature Transmitter is classified as a Type B device according to IEC61508, having a hardware fault tolerance of 0.

The 644 Temperature Transmitter together with a temperature-sensing element becomes a temperature sensor assembly. When using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing element must be considered. This is discussed in detail in Section 5.1 and Appendix B. Failure rates for the 644 Temperature Assembly when using thermocouples in a low stress environment are listed in Table 1. The dual sensing element mode assumes PV is S1, S2 or first good and drift alert is set to alarm.

Table 1 Version Overview

Failure category	Failure rate (in FITs)			
	Single T/C mode		**Dual T/C mode Drift Alert = Alarm**	
Fail High (detected by the logic solver)	31		31	
Fail Low (detected by the logic solver)	426		440	
Fail detected (int. diag.)*	398		412	
Fail low (inherently)	28		28	
Fail Dangerous Undetected	44		39	
No Effect	124		128	
Annunciation Undetected	12		12	
Safe Failure Fraction	91.3%		92.4%	

* These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High, these failures would need to be added to the Fail High failure category.

Failure rates for the 644 Temperature Assembly when using RTDs in a low stress environment are listed in Table 1. The dual sensing element mode assumes PV is S1, S2 or first good and drift alert is set to alarm.

Table 2 Failure rates 644 Temperature Transmitter using RTDs

Failure category		Failure rate (in FITs)			
		Single 4-wire RTD mode		**Dual 3-wire RTD mode, Drift Alert = Alarm**	
Fail High (detected by the logic solver)		31		31	
Fail Low (detected by the logic solver)		330		347	
	Fail detected (int. diag.)*	302		319	
	Fail low (inherently)	28		28	
Fail Dangerous Undetected		36		31	
No Effect		119		123	
Annunciation Undetected		12		12	
Safe Failure Fraction		90.9%		92.5%	

*These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High, these failures would need to be added to the Fail High failure category.

The failure rates are valid for the useful lifetime of the transmitter, see Appendix A.

A user of the 644 Temperature Transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

Table of Contents

1 Purpose and Scope

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 644 Temperature Transmitter. From this, failure rates and example PFD_{avg} values may be calculated.

The information in this report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

An FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and 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 global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

2.2 Roles of the parties involved

Rosemount Inc. Manufacturer of the 644 Temperature Transmitter

exida Performed the hardware assessment

Rosemount Inc. contracted *exida* in February 2012 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: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	exida LLC, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	EMCR Handbook, 2011 Update	exida LLC, Electrical & Mechanical Component Reliability Handbook, 2011 Update
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	exida LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[D1]	00644-7401, Rev AB, 10/13/11	Terminal Cap Assembly 644
[D2]	00644-6411, Rev AF, 7/27/11	Module Assembly 664R
[D3]	00644-7100, Rev AC, 5 Mar 2012	Schematic, 644 Electronics Board Headmount
[D4]	00644-7110, Rev 01, 5/3//11	Schematic, 644 Hart and Fieldbus Transient Protector, T1 Option
[D5]	Fault Injection List 644T_27Mar2012_results.xls, 28 Mar 2012	644 Fault Injection Test Results
[D6]	Fault_Injection_Test_Details.doc, 28 Mar 2012	644 Fault Injection Test Result Details
[D7]	644 Next Generation Transmitter Safety Integrity Requirements Specification Revision: A.4, 2 Nov 2011	644 Safety Integrity Requirements Specification
[D8]	644NG Diagnostic Design.doc	644 Diagnostics Design, attached to 27 Oct 2011 e-mail from Corey Wolf (Rosemount)
[D9]	00644-7600, Rev AB, 11 Oct 2011	Temperature Transmitter Hub Assembly 644, includes hardware revision history
[D10]	644_vdd.htm	software release notes/version description document, shows released software drawing number
[D11]	00644-7300, Rev AA, 9 Apr 2012	644 HART Software Revision Drawing, associates software release drawing (dash #) with NE-53 software revision

2.4.2 Documentation generated by *exida*

[R1]	644NG TT and sensing devices Rev AB.xls	Failure rate calculations Summary, 644 Temperature Transmitter, August 2012
[R2]	644NG Temp Transmitter part 1 of 3 Rev AB.xls	Failure rate calculations, 644 Temperature Transmitter, April 2012
[R3]	644NG Temp Transmitter part 2 of 3 Rev AB.xls	Failure rate calculations, 644 Temperature Transmitter, April 2012
[R4]	644NG Temp Transmitter Common Portion of part 3 of 3 Rev AB.xls	Failure rate calculations Common Portion, 644 Temperature Transmitter, April 2012
[R5]	644NG Temp Transmitter TC Portion of Rev AB.xls	Failure rate calculations T/C Portion, 644 Temperature Transmitter, April 2012
[R6]	644NG Temp Transmitter Dual TC Portion of Rev AB.xls	Failure rate calculations Dual T/C, 644 Temperature Transmitter, April 2012
[R7]	644NG Temp Transmitter 3 Wire RTD Portion of Rev AB.xls	Failure rate calculations 3 Wire RTD, 644 Temperature Transmitter, April 2012
[R8]	644NG Temp Transmitter Dual 3 Wire RTD Portion of Rev AB.xls	Failure rate calculations Dual 3 Wire RTD, 644 Temperature Transmitter, April 2012

3 Product Description

This report documents the results of the Failure Modes, Effects and Diagnostics Analysis performed for the 644 Temperature Transmitter with Hardware version 1 and Device Label SW REV 1.1.X. The 644 Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The transmitter can be equipped with or without display.

The 644 Temperature Transmitter is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0. Combined with one or two temperature sensing elements, the 644 transmitter becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 644 Temperature Transmitter are:

- 2-, 3-, and 4-wire RTD
- Thermocouple
- Millivolt input (–10 to 100mV)
- 2-, 3-, and 4-wire Ohm input (0 to 2000Ω)

The FMEDA has been performed for different input sensing element configurations of the 644 transmitter, i.e. 3-wire RTD, 4-wire RTD, and thermocouple. Estimates have been made of the temperature sensing element failure rates given the ability of the 644 transmitter to detect several failure modes of the temperature sensing element.

644 HART SIS Capabilities and Options

- Single or Dual sensor inputs for RTD, Thermocouple, mV and Ohm
- DIN A Head mount and Field mount transmitters
- SIL3 Capable: IEC 61508 certified by an accredited 3rd party agency for use in safety instrumented systems up to SIL 3 [Minimum requirement of single use (1oo1) for SIL 2 and redundant use (1oo2) for SIL 3]
- LCD display
- Enhanced display with Local Operator Interface
- Integral Transient Protection
- Diagnostic Suite
- Enhanced accuracy and stability
- Transmitter-Sensor Matching with Callendar Van Dusen constants

[1] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation received from Rosemount Inc. and is documented in [R1] through [R8]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on a system level [D5] and [D6].

4.1 Failure categories description

In order to judge the failure behavior of the 644 Temperature Transmitter, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the process reaches a safe situation. Depending on the application the fail-safe state is defined as the output going to fail low or fail high.
Fail Safe	Failure that causes the transmitter to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 2% of span and that leaves the output within active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (> 20.9 mA, output saturate high) or high alarm (>21 mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.7 mA, output saturate low) or low alarm (3.5, 3.75 mA)
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 IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation needed when Route 2_H failure data is not available.

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 automatic diagnostic 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 Handbooks [N2] which was derived using over 100 billion unit operational hours of 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 *exida* Profile 2, see Appendix D. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Rosemount Inc.. 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 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 wearout 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. *exida* Environmental Profiles listing expected stress levels can be found in Appendix D. 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.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 644 Temperature Transmitter with 4..20 mA output.

- 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 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.
- The stress levels are average for an industrial environment and can be compared to the exida Profile 2 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- External power supply failure rates are not included.
- The device is installed per manufacturer's instructions.
- Worst-case internal fault detection time is <1 hour.

4.4 Behavior of the Safety Logic Solver

Depending on the application, the following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value below a predefined low set value. A current < 3.75mA (Fail Low) is below the specified trip-point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 21mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by a connected logic solver. The PLC Detection Behavior in Table 3 represents the under-range and over-range detection capability of the connected logic solver.

Table 3 Application example

Application	PLC Detection Behavior	λ_{low}	λ_{high}
Low trip	< 4mA	= λ_{sd}	= λ_{du}
Low trip	> 20mA	= λ_{su}	= λ_{dd}
Low trip	< 4mA and > 20mA	= λ_{sd}	= λ_{dd}
Low trip	-	= λ_{su}	= λ_{du}
High trip	< 4mA	= λ_{dd}	= λ_{su}
High trip	> 20mA	= λ_{du}	= λ_{sd}
High trip	< 4mA and > 20mA	= λ_{dd}	= λ_{sd}
High trip	-	= λ_{du}	= λ_{su}

In this analysis it is assumed that the logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

4.5 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 644 Temperature Transmitter FMEDA.

Table 4 Failure rates 644 Temperature Transmitter (T/C configuration)

Failure category		Failure rate (in FITs)			
		Single T/C mode		Dual T/C mode	
Fail High (detected by the logic solver)			31		31
Fail Low (detected by the logic solver)			331		340
	Fail detected (int. diag.)[2]	303		312	
	Fail low (inherently)	28		28	
Fail Dangerous Undetected			39		39
No Effect			124		128
Annunciation Undetected			12		12

Table 5 Failure rates 644 Temperature Transmitter (RTD configuration)

Failure category	Failure rate (in FITs)

[2] These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High Alarm, these failures would need to be added to the Fail High failure category.

		Single RTD mode		Dual RTD mode (3-wire RTD)	
Fail High (detected by the logic solver)			31		31
Fail Low (detected by the logic solver)			286		299
	Fail detected (int. diag.)[3]	258		271	
	Fail low (inherently)	28		28	
Fail Dangerous Undetected			30		31
No Effect			119		123
Annunciation Undetected			12		12

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

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508 (See Section 5.4).

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

If Route 2_H is not applicable for the 644 Temperature Transmitter, the architectural constraints will need to be evaluated per Route 1_H.

Note that according to IEC61508:2010 definition the No Effect and Annunciation Undetected failures are not included in the total failure rate and therefore are not part of the Safe Failure Fraction calculation.

Table 6 Failure rates according to IEC 61508 in FIT

644 Temperature Transmitter	SFF
644, Single T/C mode	90.4%
644, Dual T/C mode	90.5%
644, Single RTD mode	91.3%
644, Dual RTD mode	91.5%

The architectural constraint type for 644 Temperature Transmitter is B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

5 Using the FMEDA Results

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

5.1 Temperature sensing devices

The 644 Temperature Transmitter together with a temperature-sensing device becomes a temperature sensor assembly. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered. Typical failure rates for close-coupled thermocouples and RTDs are listed in Table 7.

Table 7 Typical failure rates close-coupled thermocouples and RTDs

Temperature Sensing Device	Failure rate (FIT)
Thermocouple low stress environment	100
Thermocouple high stress environment	2,000
4-wire RTD low stress environment	50
4-wire RTD high stress environment	1,000

The following sections give examples on how to combine the temperature-sensing element failure rates and the transmitter failures. The examples given are for PV (Process Value) set to represent Sensor 1 or Sensor 2 when using a single sensor, either T/C or RTD. More information on how to combine temperature-sensing element failure rates and transmitter failure rates for other configurations, including the use of dual sensing-elements is given in Appendix B.

5.1.1 644 Temperature Transmitter with thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 8 when close-coupled thermocouples are supplied with the 644 Temperature Transmitter. The drift failure mode is primarily due to T/C aging. The 644 Temperature Transmitter will detect a thermocouple burnout failure and drive the analog output to the specified failure state.

Table 8 Typical failure mode distributions for thermocouples

TC Failure Modes – Close-coupled device	Percentage
Open Circuit (Burn-out)	95%
Wire Short (Temperature measurement in error)	4%
Drift (Temperature measurement in error)(50% Safe; 50% Dangerous)	1%

A complete temperature sensor assembly consisting of 644 Temperature Transmitter and a closely coupled thermocouple supplied with the 644 Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the 644 Temperature Transmitter is programmed to drive its output to the specified failure state on detected failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

- λ^{L} = (100) * (0.95) = 95 FITs
- λ^{DU} = (100) * (0.05) = 5 FITs

When these failure rates are added to the failure rates of the 644 Temperature Transmitter, single T/C mode (see Table 4), the total for the temperature sensor subsystem is:

- λ^{L} = 95 + 331 = 426 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 5 + 39 = 44 FITs

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. For these circumstances, the Safe Failure Fraction of this temperature sensor subsystem is 91.3%.

5.1.2 644 Temperature Transmitter with RTD

The failure mode distribution for an RTD also depends on application with the key variables being stress level, RTD wire length and RTD type (3-wire or 4-wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions are shown in Table 9. The 644 Temperature Transmitter will detect open circuit and short circuit RTD failures and drive its output to the specified failure state.

Table 9 Typical failure mode distributions for 3-Wire and 4-Wire RTDs in a Low Stress environment or using a cushioned sensor construction

RTD Failure Modes – Close coupled element	Percentage	
	3-wire RTD	4-wire RTD
Open Circuit	79%	83%
Short Circuit	3%	5%
Drift (Temperature measurement in error)	18%	12%

A complete temperature sensor assembly consisting of 644 Temperature Transmitter and a closely coupled, cushioned 4-wire RTD supplied with the 644 Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 4-wire RTD in a low stress environment is:

- λ^{L} = (50) * (0.83 + 0.05) = 44 FITs

- λ^{DU} = (50) * (0.12) = 6 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, single RTD mode (see Table 5), the total for the temperature sensor subsystem is:

- λ^{L} = 44 + 286 = 330 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 6 + 30 = 36 FITs

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. The Safe Failure Fraction for this temperature subsystem, given the assumptions, is 90.9%.

5.2 Converting failure rates to IEC 61508 format

When The failure rates that are derived from the FMEDA for the 644 Temperature Transmitter are in a format different from the IEC 61508 format. This section will explain how the failure rates can be converted into the IEC 61508 format.

First of all, depending on the application, the high and low failure rates of the 644 Temperature Transmitter must be classified as either safe or dangerous. Assume an application where a safety action needs to be performed if the temperature drops below a certain level. The 644 Temperature Transmitter will therefore be configured with a low trip level. A low failure of the transmitter will cause the transmitter output to go through the low trip level. Consequently the transmitter will indicate that the safety action needs to be performed. Therefore a low failure can be classified as a safe failure for this application. A high failure on the other hand will cause the transmitter output to move away from the trip level and therefore not cause a trip. The failure will prevent the transmitter from indicating that the safety action needs to be performed and is therefore classified as a dangerous failure for this application.

Assuming that the logic solver can detect both over-range and under-range, a low failure can be classified as a safe detected failure and a high failure can be classified as a dangerous detected failure. For this application, assuming 644 Temperature Transmitter with single RTD, the following would then be the case:

$\lambda^{H} = \lambda^{DD}$ = 31 FITs

$\lambda^{L} = \lambda^{SD}$ = 330 FITs

λ^{DU} = 36 FITs

In a similar way the high and low failure rates can be classified as respectively safe detected and dangerous detected in case the application has a high trip level. The failure rates as displayed above are the same failure rates as stored in the exida equipment database that is part of the online SIL verification tool, SILver.

No Effect failures and Annunciation Undetected failures are not classified as Safe Undetected failures according to IEC 61508:2010.

λ^{SU} = 0 FITs

Note that the dangerous undetected failures will of course remain dangerous undetected.

Table 10 shows the failure rates according to IEC 61508 for this application, assuming 644 Temperature Transmitter with single RTD.

Table 10: Failure rates according to IEC 61508 – 644 with single RTD

Failure Categories	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
Low trip	330 FIT	0 FIT	31 FIT	36 FIT	91%
High trip	31 FIT	0 FIT	330 FIT	36 FIT	91%

5.3 PFD_{avg} calculation 644 Temperature Transmitter

Using the failure rate data displayed in section 4.5, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix F for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test are listed in Table 14 - Table 16.

6 Terms and Definitions

exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
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 demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic 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 element	"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	"Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 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 History:	V2, R2:	Updated per customer comments; TES 1/23/15
	V2, R1:	Updated Proof Test; TES 11/21/14
	V1, R2	changed product name on cover sheet, corrected PDFavg graph
	V1, R1:	updated with comments in 27 April 2012 e-mail, released to Rosemount; 15 May 2012
	V0, R1:	Initial version; 20 April 2012
Author(s):	Griff Francis	
Review:	V0, R1:	Todd Larson, Rosemount
	V0, R1:	William Goble, *exida*
Release Status:	RELEASED to Rosemount Inc.	

7.3 Future enhancements

At request of client.

7.4 Release signatures

Dr. William M. Goble, CFSE, Principal Partner

Griff Francis, Senior Safety Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 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[3] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

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

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

Table 11 Useful lifetime of electrolytic capacitors contributing to λ^{DU}

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

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.

[3] 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 Failure rates for various transmitter modes

This Appendix discusses in more detail how to combine the 644 Temperature Transmitter failure rates with sensing element failure rates and how to take credit for diagnostics provided by the transmitter on the sensing element (Drift Alert = Alarm).

Table 12 644 Temperature Transmitter modes

S1 Type	S2 Type	Suspend Non-PV Faults	Drift Alert[4]	Primary Variable (PV)	Calculation
T/C, 3 Wire RTD, 4 wire RTD	Disabled	X	N/A	S1	1
Disabled	T/C, 3 Wire RTD	X	N/A	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	S1	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	S1	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	S1	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	S1	2*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	S2	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	S2	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	Average	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	Average	4
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	Average	3*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	Average	4*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	First Good	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	First Good	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	First Good	1*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	First Good	2

* These modes represent “Hot back-up”. Using the calculation method as described will results in accurate numbers for PFD_{AVG}, but will overestimate the false trip rate. (The sensing elements are configured as a 2oo2 voting and will not alarm on a single sensor failure).

Calculation 1

Single Sensor configured, PV = S1 or PV = S2 or,

Dual Sensors configured, PV = S1, PV = S2 or PV = First Good and Drift Alert = disabled

[4] For purposes of safety validation, Drift Alert = Warning is considered the same as Drift Alert = disabled

Modeled as a series subsystem where failure occurs if either sensing element or transmitter fails. For such a system, failure rates are added. Use single mode failure rates for the 644 Temperature Transmitter and add sensing element failure rates (single element). This has been described in detail in sections 5.1.1 and 5.1.2.

Calculation 2

Dual Sensors configured, PV = S1 or PV = S2 or PV = First Good, and Drift Alert = alarm

Modeled as a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Use dual mode failure rates for the 644 Temperature Transmitter and add sensing element failure rates (single element). The sensing element failure rates should reflect the additional coverage on the drift failures (99%) provided by the Drift Alert.

Example: 644 with dual 3-wire RTDs

Table 13 Typical failure mode distributions for 3-wire RTDs, Low Stress environment / cushioned sensor

RTD Failure Modes – Close coupled element	Percentage
Open Circuit	79%
Short Circuit	3%
Drift (Temperature measurement in error)	18%

Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = (48) * (0.79 + 0.03 + 0.99·0.18) = 47.9 FITs
- λ^{DU} = (48) * (0.01·0.18) = 0.1 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, single RTD mode (see Table 5, second column), the total for the temperature sensor subsystem is:

- λ^{L} = 47.9 + 286 = 333.9 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 0.1 + 30 = 30.1 FITs

Calculation 3

Dual Sensors configured, PV = Average or PV = Differential mode, Drift Alert = disabled

Both sensing elements need to function. Use single mode failure rates for the 644 Temperature Transmitter (single mode failure rates are selected because Drift Alert = disabled) and add failure rates for both sensing elements.

Example: 644 with dual 3-wire RTDs

Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = 2 * ((48) * (0.79 + 0.03)) = 79 FITs
- λ^{DU} = 2 * ((48) * (0.18)) = 17 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, single RTD mode (see Table 5, first column), the total for the temperature sensor subsystem is:

- λ^{L} = 79 + 299 = 378 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 17 + 31 = 48 FITs

Calculation 4

Dual Sensors configured, PV = Average and Drift Alert = alarm

To obtain the overall failure rates of the sensor assembly, use the dual mode failure rates for the 644 Temperature Transmitter and add failure rates for both sensing elements. The sensing element failure rates should be adjusted to reflect the additional coverage on the drift failures (99%) provided by the Drift Alert.

Example: 644 with dual 3-wire RTDs

Assuming that the 644 Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = 2 * ((48 * (0.79 + 0.03 + 0.99·0.18)) = 95.8 FITs
- λ^{DU} = 2 * ((48 * (0.01·0.18)) = 0.2 FITs

When these failure rates are added to the failure rate of the 644 Temperature Transmitter, dual RTD mode (see Table 5, second column), the total for the temperature sensor subsystem is:

- λ^{L} = 95.8 + 299 = 394.8 FITs
- λ^{H} = 31 FITs
- λ^{DU} = 0.2 + 31 = 31.2 FITs

Appendix C Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic 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.

C.1 Partial Proof Test 1

Proof test 1 consists of an analog output Loop Test, as described in Table 14. This test will detect approximately 63% of possible DU failures in the transmitter and approximately 90% of the simple sensing element DU failures. This means a Proof Test Coverage of 67% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 14 Steps for Proof Test 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. 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.
3	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
4	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
5	Perform reasonability check on the sensor value(s) versus an independent estimate (i.e. from direct monitoring of BPCS value) to show current reading is good
6	Restore the loop to full operation
7	Remove the bypass from the safety PLC or otherwise restore normal operation

C.2 Comprehensive Proof Test 2

The alternative proof test consists of the following steps, as described in Table 15. This test will detect approximately 96% of possible DU failures in the transmitter and approximately 99% of the simple sensing element DU failures. This results in a Proof Test Coverage of 96% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 15 Steps for Proof Test 2

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Verify the measurement for two temperature points for Sensor 1. Verify the measurement for two temperature points for Sensor 2, if second sensor is present.
4	Perform reasonability check of the housing temperature
5	Restore the loop to full operation
6	Remove the bypass from the safety PLC or otherwise restore normal operation

C.3 Comprehensive Proof Test 3

The third proof test consists (as described in Table 16) of a comprehensive transmitter and a limited sensor proof test combination. This test will detect approximately 96% of possible DU failures in the transmitter and approximately 90% of the simple sensing element DU failures. This results in a Proof Test Coverage of 95% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 16 Steps for Proof Test 3

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform Proof Test 1
3	Connect calibrated sensor simulator in place of sensor 1
4	Verify safety accuracy of 2 temperature points inputs to transmitter.
5	If sensor 2 is used, repeat steps 3 and 4.
6	Restore sensor connections to transmitter.
7	Perform reasonability check of transmitter housing temperature.
8	Perform reasonability check on the sensor(s) values versus an independent estimate (i.e. from direct monitoring of BPCS value) to show current reading is acceptable.
9	Restore loop to full operation.
10	Remove the bypass from the safety PLC or otherwise restore normal operation

Appendix D *exida* Environmental Profiles

Table 17 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[5]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[6]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[7]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[8]	G2	G3	G3	G3	G3	Compatible Material
Surge[9]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[10]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[11]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[5] Humidity rating per IEC 60068-2-3
[6] Shock rating per IEC 60068-2-6
[7] Vibration rating per IEC 60770-1
[8] Chemical Corrosion rating per ISA 71.04
[9] Surge rating per IEC 61000-4-5
[10] EMI Susceptibility rating per IEC 61000-4-3
[11] ESD (Air) rating per IEC 61000-4-2

Appendix E Common Cause for redundant transmitter configurations

A method for estimating the beta factor is provided in IEC 61508, part 6. This portion of the standard is only informative and other techniques may be used to estimate the beta factor. Based on the approach presented in IEC 61508 a series of questions are answered. Based on the total points scored for these questions, the beta factor number is determined from IEC61508-6 Table D.4.

Example – 2oo3 Temperature Transmitters

A design is being evaluated where three Rosemount 644 Temperature Transmitters are chosen. The transmitters are connected to a logic solver programmed to detect over-range and under-range currents as a diagnostic alarm. The process is not shutdown when an alarm occurs on one transmitter. The logic solver has a two out of three (2oo3) function block that votes to trip when two of the three transmitters indicate the need for a trip. Following the questions from the sensor portion of Table D.1 of IEC 61508, Part 6, the following results are obtained.

Table 18 Example version of Table D.1, Part 6 IEC 61508

Item	X_{SF}	Y_{SF}	Example	Score
Are all signal cables for the channels routed separately at all positions?	1.0	2.0	Not guaranteed	0.0
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	2.5	1.5	Transmitters are separate	4.0
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?	2.5	0.5	Transmitters are in different housings	3.0
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc.?	7.5		No – transmitters are identical	0.0
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?	5.5		No – transmitters are identical	0.0
Do the channels employ enhanced redundancy with MooN architecture, where N > M + 2?	2.0	0.5	No – 2oo3	0.0
Do the channels employ enhanced redundancy with MooN architecture, where N = M + 2?	1.0	0.5	No – 2oo3	0.0
Are separate test methods and people used for each channel during commissioning?	1.0	1.0	No - impractical	0.0
Is maintenance on each channel carried out by different people at different times?	2.5		No - impractical	0.0
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0.5	0.5	No cross channel information between transmitters	1.0
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	1.0	1.0	644 based on well proven design	2.0
Is there more than 5 years experience with the same hardware used in similar environments?	1.5	1.5	Extensive experience in process control	3.0

Item	X_{SF}	Y_{SF}	Example	Score
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1.5	0.5	Transient voltage and current protection provided	2.0
Are all devices/components conservatively rated? (for example, by a factor of 2 or more)	2.0		Design has conservative rating factors proven by field reliability	2.0
Have the results of the failure modes and effects analysis or fault tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3.0	FMEDA done by third party – exida. No common cause issues	3.0
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3.0	Design review is part of the development process. Results are always fed back into the design	3.0
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	Field failure feedback procedure reviewed by third party – exida. Results are fed back into the design.	4.0
Is there a written system of work which will ensure that all component failures (or degradations) are detected, the root causes established and other similar items are inspected for similar potential causes of failure?	0.5	1.5	Proof test procedures are provided but they cannot insure root cause failure analysis.	0.0
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	2.0	1.0	Procedures are not sufficient to ensure staggered maintenance.	0.0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.), intended to be independent of each other, must not be relocated?	0.5	0.5	MOC procedures require review of proposed changes, but relocation may inadvertently be done.	0.0
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.5	Repair is done by returning product to the factory, therefore this requirement is met.	2.0
Do the system diagnostic tests report failures to the level of a field-replaceable module?	1.0	1.0	Logic solver is programmed to detect current out of range and report the specific transmitter.	2.0
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures	2.0	3.0	Control system designers have not been trained.	0.0

Item	X_{SF}	Y_{SF}	Example	Score
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures	0.5	4.5	Maintenance personnel have not been trained.	0.0
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	A tool is required to open the transmitter therefore this requirement is met.	3.0
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	Environmental conditions are checked at installation.	4.0
Are all signal and power cables separate at all positions?	2.0	1.0	No	0.0
Has a system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	Rosemount has complete testing of all environmental stress variables and run-in during production testing.	20.0
Totals	23	37	S=X+Y	58

A score of 58 results in a beta factor of 5%. If the owner-operator of the plant would institute common cause training and more detailed maintenance procedures specifically oriented toward common cause defense, a score of greater than 70 could be obtained. Then the beta factor would be 2%.

Note that the diagnostic coverage for the transmitter is not being considered. Additional points can be obtained when diagnostics are taken into account. However this assumes that a shutdown occurs whenever any diagnostic alarm occurs. In the process industries this could even create dangerous conditions. Therefore the practice of automatic shutdown on a diagnostic fault is rarely implemented. IEC 61508, Part 6 has a specific note addressing this issue. The note states:

> *"NOTE 5 In the process industries, it is unlikely to be feasible to shut down the EUC when a fault is detected within the diagnostic test interval as described in table D.2. This methodology should not be interpreted as a requirement for process plants to be shut down when such faults are detected. However, if a shut down is not implemented, no reduction in the b-factor can be gained by the use of diagnostic tests for the programmable electronics. In some industries, a shut down may be feasible within the described time. In these cases, a non-zero value of Z may be used."*

In this example, automatic shutdown on diagnostic fault was not implemented so no credit for diagnostics was taken.

Appendix F Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). The numbers used in the examples are not for the product described in this report.

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N5] and [N8].

These are:

A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;

B. Architecture Constraints (minimum redundancy requirements) are met; and

C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N9].

C. Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD_{avg}) calculation must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restore (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03. See Figure 1.

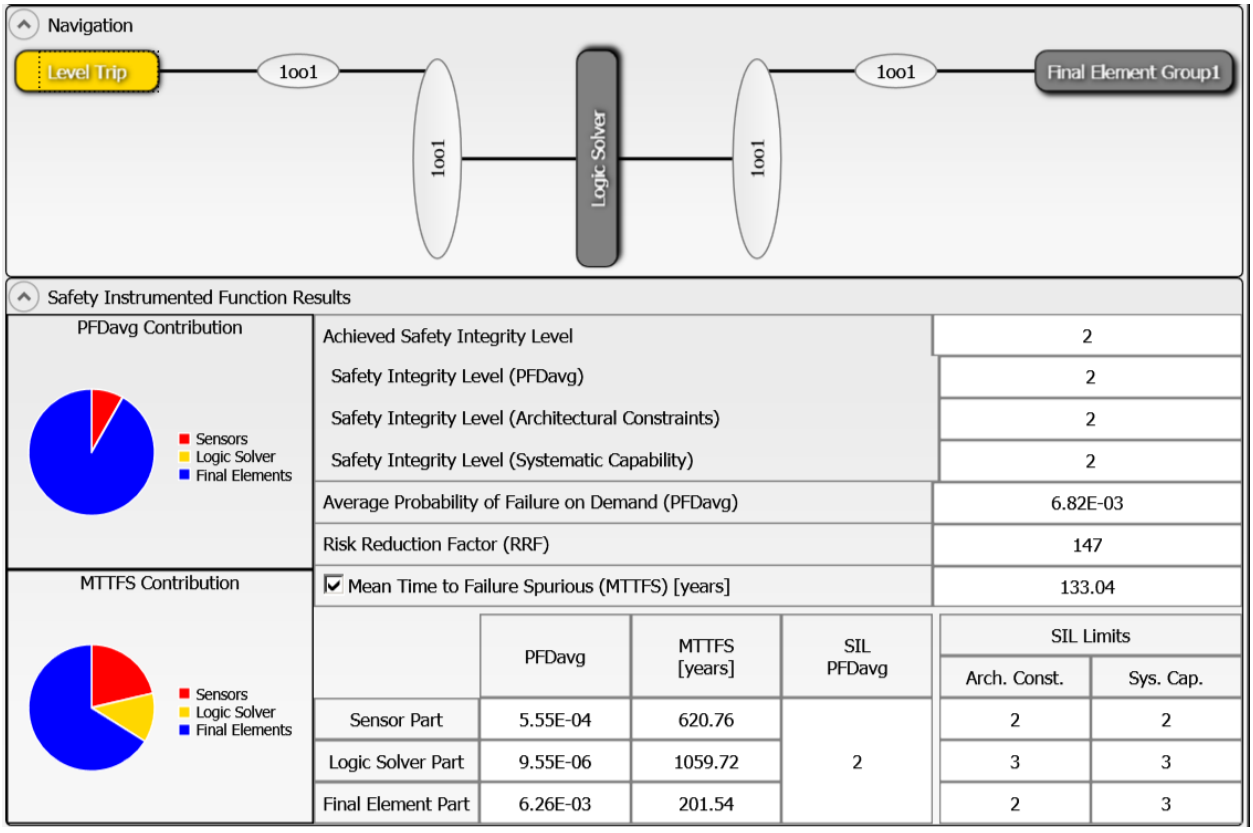

Figure 1: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 2.

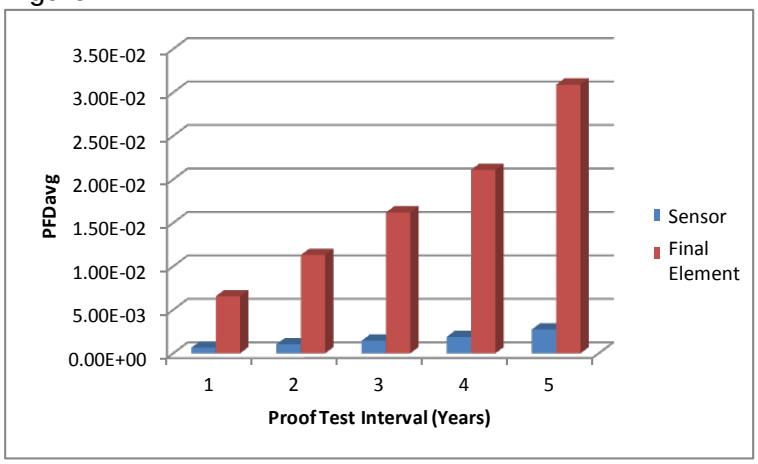

Figure 2 PFD_{avg} versus Proof Test Interval.

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 3).

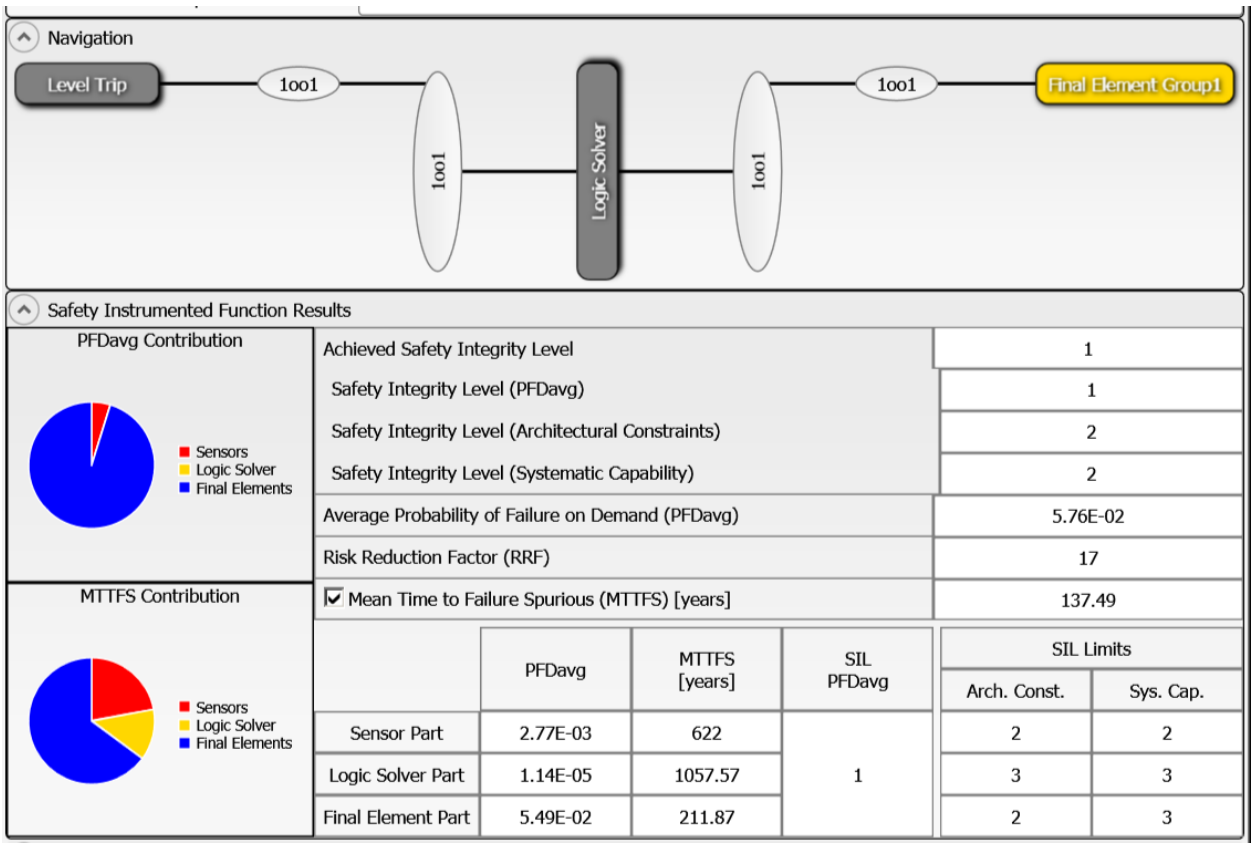

Figure 3: exSILentia results with realistic variables

It is clear that PFD_{avg} results can change an entire SIL level or more when all critical variables are not used.