Failure Modes, Effects and Diagnostic Analysis

Project:
644 HART Temperature Transmitter

Customer:

Rosemount Inc.
Chanhassen, Minnesota
USA

Contract No.: ROS 03/05-11US
Report No.: ROS 03/05-11 R001
Version V2, Revision R3.0, June 14, 2005
William M. Goble – John C. Grebe

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.
© All rights reserved.

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 644 HART Temperature Transmitter. 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 644 HART Temperature Transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 644 HART 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 device can be equipped with or without display.

The 644 HART Temperature Transmitter is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0. The Rosemount Models 644H and 644R are designed for use in critical applications where the loss of the temperature points may be detrimental. Each Model 644 transmitter provides both a 4–20 mA output and a digital HART® signal. Combined with a temperature-sensing device, the 644 Hart transmitter becomes a temperature sensor assembly.

The failure rates for the 644 HART Temperature Transmitter (T/C configuration) are as follows:

$\lambda^{H} = 26 * 10^{-9}$ failures per hour

$\lambda^{L} = 297 * 10^{-9}$ failures per hour

$\lambda^{DU} = 72 * 10^{-9}$ failures per hour

Table 1 lists the failure rates for 644 HART Temperature Transmitter (T/C configuration) according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 1: Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}^{*}	λ_{dd}	λ_{du}	SFF
Low trip	297 FIT	110 FIT	26 FIT	72 FIT	85.7%
High trip	26 FIT	110 FIT	297 FIT	72 FIT	85.7%

(*Note that the SU category includes failures that do not cause a spurious trip)

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

A user of the 644 HART 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 for different configurations is presented in section 4.5 along with all assumptions.

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

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include any software assessment.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition, this option includes an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 1.

This document shall describe the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 644 HART Temperature Transmitter. From these failure rates, the safe failure fraction (SFF) and example PFD_{AVG} values are calculated.

2 Project management

2.1 *exida.com*

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

2.2 Roles of the parties involved

Rosemount Inc. Manufacturer of the 644 HART Temperature Transmitter

exida.com Project leader of the FMEDA

Rosemount Inc. contracted ***exida.com*** in May 2003 with the FMEDA and PFD_{AVG} calculation of the above-mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91 & FMD-97, RAC 1991, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center. Statistical compilation of failure mode distributions for a wide range of components
[N3]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center. Statistical compilation of failure rate data, incl. mechanical and electrical sensors
[N4]	SN 29500	Failure rates of components
[N5]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N6]	Telcordia (Bellcore) Failure rate database and models	Statistical compilation of failure rate data over a wide range of applications along with models for estimating failure rates as a function of the application.
[N7]	Safety Equipment Reliability Handbook, 2003	exida.com L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N8]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods

2.4 Reference documents

2.4.1 Documentation provided by the customer

D1	00644-6100	Electronic Schematic
D2	00809-0100-4728	Reference Manual, Rev HA, Dec. 2002
D3	644 Citadel Software revision history	644 Software revision history
D4	644 Headmount HW Change history of first Citadel Produced Design	644 Hardware revision history
D5	644_Shipments&Failures_032005	644 shipments & failures data

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA spreadsheet.xls	Failure rate calculations, 644 HART Temperature Transmitter, August 27, 2003
[R2]	FMEDA Rosemount 644 V230.doc, June 14, 2005	FMEDA report, 644 HART Temperature Transmitter, V2, R2.0 (this report)
[R3]	Field Failure Analysis 644.xls, May 27, 2005	exida 644 Field Failure Analysis summary spreadsheet

3 Product Description

The 644 HART 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 device can be equipped with or without display.

The 644 HART Temperature Transmitter is classified as a Type B[2] device according to IEC61508, having a hardware fault tolerance of 0.

The Rosemount Models 644H and 644R are designed for use in critical applications where the loss of the temperature points may be detrimental. Each Model 644 transmitter provides both a 4–20 mA output and a digital HART® signal. Combined with a temperature sensing device, the 644 Hart transmitter becomes a temperature sensor assembly. This is also indicated in the following figure.

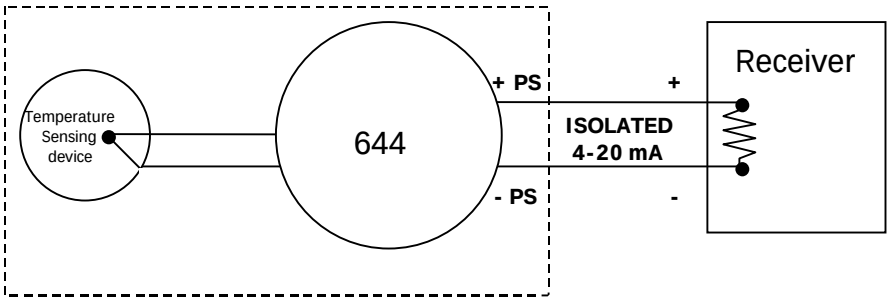


Figure 1 644 HART Temperature Transmitter

The temperature sensing devices that can be connected to the 644 HART Temperature Transmitter are listed underneath.

- 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 two different input sensor configurations of the 644 Hart transmitter, i.e. RTD and thermocouple. Estimates have been made of the temperature sensing device failure rates given the ability of the 644 Hart temperature transmitter to detect several failure modes of the temperature sensing device.

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

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Rosemount Inc. and is documented in [R1] and [R2]. 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 system level.

4.1 Description of the failure categories

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

Fail-Safe State	State where output exceeds the user defined threshold.
Fail Safe	Failure that causes the module / (sub)system 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, output saturate high or high alarm value (>21mA).
Fail Low	Failure that causes the output signal to go to the minimum output current, output saturate low or low alarm value (≤ 3.6, 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 [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High or a Fail Low can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as either safe or dangerous.

The Annunciation Undetected failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with 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) 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.com*** in this FMEDA is from a proprietary component failure rate database derived using the Telcordia (N6) failure rate database/models, the SN29500 (N4) failure rate database and other sources. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 644 HART Temperature Transmitter with 4..20 mA output, 2-wire.

- 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 Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
    - IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

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 < 3.6mA (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 > 21.5mA (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 2 represents the under-range and over-range detection capability of the connected logic solver.

Table 2 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.com component reliability database the following failure rates resulted from the 644 HART Temperature Transmitter FMEDA.

Table 3 Failure rates 644 (T/C configuration)

Failure category				Failure rate (in FITs)
Fail High (detected by the logic solver)				26
Fail Low (detected by the logic solver)				297
	Fail detected (int. diag.)	274		
	Fail low (inherently)	23		
Fail Dangerous Undetected				72
No Effect				101
Annunciation Undetected				9

Table 4 Failure rates 644 (RTD configuration)

Failure category				Failure rate (in FITs)
Fail High (detected by the logic solver)				26
Fail Low (detected by the logic solver)				290
	Fail detected (int. diag.)	267		
	Fail low (inherently)	23		
Fail Dangerous Undetected				70
No Effect				105
Annunciation Undetected				9

It is assumed that upon the detection of a failure the output will be sent downscale, all detected failure categories are sub-categories of the fail low failure category.

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the 644 HART Temperature Transmitter should be calculated. The SFF is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. As both the Fail High and Fail Low failure categories are assumed to be detected by the logic solver (regardless of the fact if their effect is safe or dangerous), the Safe Failure Fraction can be calculated independently of the 644 HART Temperature Transmitter application.

This is reflected in the following formula for SFF:

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

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

Table 5 Safe Failure Fraction of 644 HART Temperature Transmitter

644 HART Temperature Transmitter	SFF
644 HART Temperature Transmitter (T/C configuration)	85.74%
644 HART Temperature Transmitter (RTD configuration)	86.00%

The architectural constraint type for 644 HART 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

5.1 Temperature sensing devices

The 644 HART Temperature Transmitter together with a temperature-sensing device becomes a temperature sensor. 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 thermocouples and RTDs are listed in the following table.

Table 6 Typical failure rates thermocouples and RTDs

Temperature Sensing Device	Failure rate (in FITs)
Thermocouple low stress environment	5,000.00
Thermocouple high stress environment	20,000.00
RTD low stress environment	2,000.00
RTD high stress environment	8,000.00

5.1.1 644 HART 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 the following table when close-coupled thermocouples are supplied with the 644 HART Temperature Transmitter. The drift failure mode is primarily due to T/C aging. The 644 HART Temperature Transmitter will detect a thermocouple burnout failure and drive it’s output to the specified failure state.

Table 7 Typical failure mode distributions for thermocouples

Temperature Sensing Device	Percentage
Open Circuit (Burn-out)	95%
Wire Short (Temperature measurement in error)	1%
Drift (Temperature measurement in error)	4%

A complete temperature sensor assembly consisting of 644 HART Temperature Transmitter and a closely coupled thermocouple supplied with the 644 HART 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 HART Temperature Transmitter is programmed to drive it’s output low on detected failure, the failure rate contribution for the thermocouple in a low stress environment is:

- λ^{L} = (5000) * (0.95) = 4750 FITs
- λ^{DU} = (5000) * (0.05) = 250 FITs

The failure rate contribution of the 644 HART Temperature Transmitter when used with a thermocouple is:

- λ^{L} = 297 FITs
- λ^{H} = 26 FITs
- λ^{DU} = 72 FITs

When these failure rates are added, the total for the temperature sensor subsystem is:

- λ^{L} = 4750 + 297 = 5047 FITs
- λ^{H} = 26 FITs
- λ^{DU} = 250 + 72 = 322 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 94.0%.

5.1.2 644 HART 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 (2/3 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 obtained from a manufacturer are shown in Table 8. The 644 HART Temperature Transmitter will detect open circuit and short circuit RTD failures and drive it's output to the specified failure state.

Table 8 Typical failure mode distributions for RTDs (low stress)

RTD Failure Modes – Close coupled device	Percentage
Open Circuit	70%
Short Circuit	29%
Drift (Temperature measurement in error)	1%

A complete temperature sensor assembly consisting of 644 HART Temperature Transmitter and a closely coupled, cushioned 4-wire RTD (low stress) supplied with the 644 HART 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 HART 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} = (2000) * (0.70 + 0.29) = 1980 FITs
- λ^{DU} = (2000) * (0.01) = 20 FITs

The failure rate contribution of the 644 HART Temperature Transmitter when used with an RTD is:

- λ^{L} = 290 FITs
- λ^{H} = 26 FITs
- λ^{DU} = 70 FITs

When these failure rates are added, the total for the temperature sensor subsystem is:

- λ^{L} = 1980 + 290 = 2270 FITs
- λ^{H} = 26 FITs
- λ^{DU} = 20 + 70 = 90 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 96.2%.

5.2 Converting failure rates to IEC 61508 format

The failure rates that are derived from the FMEDA for the 644 HART 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 HART 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 HART 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, 644 with 4-wire RTD, the following would then be the case:

$\lambda^{H} = \lambda^{DD}$ = 26 * 10^{-9} failures per hour

$\lambda^{L} = \lambda^{SD}$ = 2270 * 10^{-9} failures per hour

λ^{DU} = 90 * 10^{-9} failures per hour

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.com equipment database that is part of the online SIL verification tool, SILver.

Furthermore the No Effect failures and Annuncation Undetected failure are classified as Safe Undetected failures according to IEC 61508. Note that these failures will not affect system reliability or safety, and should not be included in spurious trip calculations.

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

5.3 PFD_{AVG} calculation 644 HART Temperature Transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 644 HART Temperature Transmitter with 4-wire RTD. The failure rate data used in this calculation is displayed in section 4.5.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 2. As shown in the figure the PFD_{AVG} value for a single 644 HART Temperature Transmitter with 4-wire RTD with a proof test interval of 1 year equals 3.94E-04.

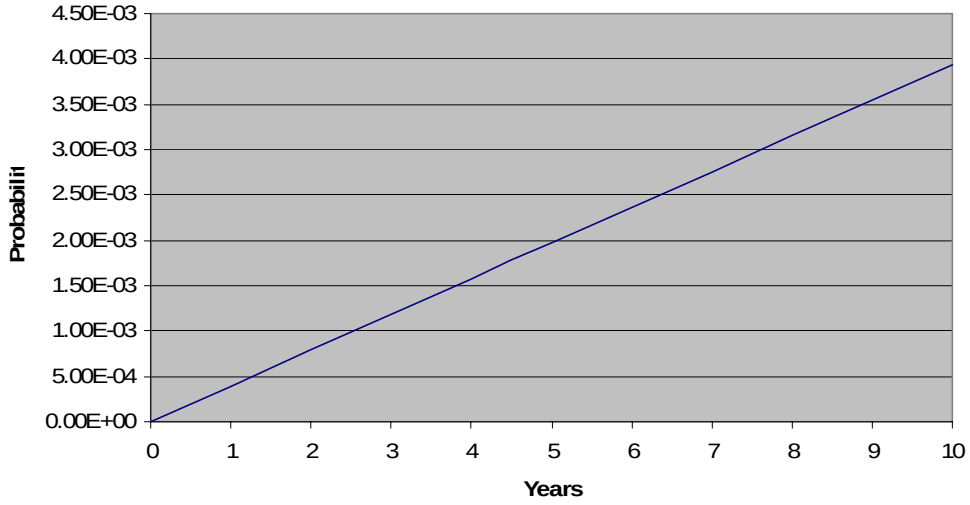


Figure 2: $PFD_{AVG}(t)$ 644 HART Temperature Transmitter

For SIL 1 applications, the PFD_{AVG} value needs to be between 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 644 HART Temperature Transmitter is equal to 0.4% 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
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	"Non-Complex" component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	"Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

exida.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. ***exida.com*** accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

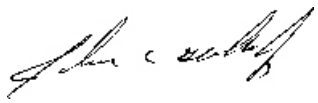
7.2 Releases

Version:	V2	
Revision:	R3.0	
Version History:	V0, R1.0:	Initial version; June 2003
	V1, R1.0:	Released to client
	V2, R1.0:	Updated format; August 28, 2003
	V2, R2.0:	Added appendices; May 27, 2005
	V2, R3.0:	Correction Table 11; June 14, 2005
Authors:	William M. Goble – John C. Grebe	
Review:	V1, R1.0:	Client, WMG
	V2, R1.0:	Rachel Amkreutz (exida), August 28, 2003
	V2, R2.0:	Randy Paschke (Rosemount); June 13, 2005
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures



John C. Grebe, Partner

Dr. William M. Goble, Principal Partner

Appendix A: Lifetime of critical components

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 9 shows which electrolytic capacitors are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 9: Useful lifetime of electrolytic capacitors contributing to λ

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

As there are no aluminium 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. According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. According to section 7.4.7.4 note 3 of IEC 61508 experiences have shown that the useful lifetime often lies within a range of 8 to 12 years for transmitters.

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 FMEDA can be detected during proof testing.

B.1 Proof test 1

Proof test 1 consists of an analog output Loop Test, as described in Table 10. 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 72% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 10 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

B.1 Proof test 2

The alternative proof test consists of the following steps, see Table 11. 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 97% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 11 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.
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

Appendix C: 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 12 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
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

Item	X_{SF}	Y_{SF}	Example	Score
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
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

Item	X_{SF}	Y_{SF}	Example	Score
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 D: Review of operating experience

For the Rosemount 644 temperature transmitter with hardware version 27 and software version 5.6.4, a review of proven-in-use documentation was performed. Design changes between hardware version 25, software version 5.6.1 and hardware version 27, software version 5.6.4 (current product) to the 644 temperature transmitter are extensively documented, see [D3], [D4].

The review focused on the volume of operating experience and number of returned units (see [R3], [D3], [D4], and [D5]).

Since the last major HW revision in 2002, the following operating experience exists:

644: *over 400 million hours of operation in a wide range of applications*

Failure rates, calculated on the basis of returns for Factory Analysis, shows field failure rates that are below the failure rates predicted by the Failure Modes, Effects and Diagnostic Analysis (FMEDA). No systematic problems were identified based on the review of the return data.

Since 2002, there have been three software revisions:

5.6.2 in 2002

5.6.3 in 2003

5.6.4 in 2004

None of these software revisions modified the behavior of the transmitter in a significant way for functional safety.

A separate assessment has been performed of the quality management, configuration management and modification systems within the Rosemount development department. All development and modification procedures have been independently certified and are compliant with IEC 61508 up to SIL 3. Units shipped back for Factory Analysis undergo a root cause analysis and results are documented and checked for systematic problems.