Failure Modes, Effects and Diagnostic Analysis

Project:
248 temperature transmitter

Customer:

Rosemount Inc.
Chanhassen, Minnesota
USA

Contract No.: ROS 06/01-34
Report No.: ROS 06/01-34 R001
Version V1, Revision R1, April 3, 2006
John C. Grebe - Rachel Amkreutz

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

Management summary

This report summarizes the results of the hardware assessment carried out on the 248 temperature transmitter. The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA 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 and consequently the Safe Failure Fraction (SFF) is calculated for the device. The FMEDA that is described in this report concerns only the hardware of the 248 temperature transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

The 248 temperature transmitter is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable.

Table 1 lists the versions of the 248 temperature transmitter that have been considered for the hardware assessment.

Table 1 Version overview

248H	248 temperature transmitter, Headmount option
248R	248 temperature transmitter, Railmount option

The 248 temperature transmitter is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the device has a Safe Failure Fraction between 60% and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 1 as a single device.

The failure rates for the 248 temperature transmitter, Headmount option are listed in Table 2.

Table 2 Failure rates 248 temperature transmitter, Headmount option

Failure category		Failure rate (in FIT)			
		TC configuration		RTD configuration	
Fail Dangerous Detected			334		326
	Fail Detected (detected by int. diagnostics)	270		262	
	Fail High (detected by the logic solver)	42		42	
	Fail Low (detected by the logic solver)	22		22	
Fail Dangerous Undetected			66		64
No Effect			78		83
Annunciation Undetected			2		2

The failure rates for the 248 temperature transmitter, Railmount option are listed in Table 3.

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

Table 3 Failure rates 248 temperature transmitter, Railmount option

Failure category		Failure rate (in FIT)			
		TC configuration		RTD configuration	
Fail Dangerous Detected			335		327
	Fail Detected (detected by int. diagnostics)	271		263	
	Fail High (detected by the logic solver)	42		42	
	Fail Low (detected by the logic solver)	22		22	
Fail Dangerous Undetected			66		64
No Effect			78		83
Annunciation Undetected			2		2

Table 4 lists the failure rates for the 248 temperature transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 4 Failure rates and SFF according to IEC 61508

Device	λ_{sd}	λ_{su}[2]	λ_{dd}	λ_{du}	SFF
Headmount option, TC configuration	0 FIT	80 FIT	334 FIT	66 FIT	86.2%
Headmount option, RTD configuration	0 FIT	85 FIT	326 FIT	64 FIT	86.4%
Railmount option, TC configuration	0 FIT	80 FIT	335 FIT	66 FIT	86.2%
Railmount option, RTD configuration	0 FIT	85 FIT	327 FIT	64 FIT	86.5%

Combined with a temperature sensing element, the 248 temperature transmitter becomes a temperature sensor assembly, see section 5.1.

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

A user of the 248 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.

[2] It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

Table of Contents

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

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

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

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

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

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

Option 3: Full assessment according to IEC 61508

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

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

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) carried out on the 248 temperature transmitter. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

It shall be assessed whether the 248 temperature transmitter meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 1 subsystems according to IEC 61508.

2 Project management

2.1 *exida*

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 248 temperature transmitter
exida	Performed the hardware assessment according to Option 1 (see section 1)

Rosemount Inc. contracted *exida* in February 2006 with the hardware assessment of the above-mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	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 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
[N9]	IEC 60654-1: 1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

2.4 Reference documents

2.4.1 Documentation provided by Rosemount Inc.

[D1]	00248-1100, Rev AE, 04/25/2005	Schematic, 248 Electronics Board Headmount, Sheet 1 through 3
[D2]	00248-1104, Rev AA, 02/04/2005	Schematic, 248 Electronics Board Railmount, Sheet 1 through 3
[D3]	00248-1107, Rev AC, 11/07/2005	Schematic, 248 Railmount Terminal Block
[D4]	248 Hardware Software Rev Hist.doc, 2/20/2006	248 Hardware and Software Revision History
[D5]	248Sales&Returns.xls, 2/20/2006	248 Sales and Returns overview

2.4.2 Documentation generated by *exida*

[R1]	248 Temp Transmitter sheet 1 of 3.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, Sheet 1 (internal document)
[R2]	248 Temp Transmitter sheet 2 of 3.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, Sheet 2 (internal document)
[R3]	248 Temp Transmitter TC Portion of sheet 3 of 3.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, TC Portion of sheet 3 of 3 (internal document)
[R4]	248 Temp Transmitter 3 Wire RTD Portion of sheet 3 of 3.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, 3 Wire RTD Portion of sheet 3 of 3 (internal document)
[R5]	248 Temp Transmitter Common Portion of sheet 3 of 3.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, Common Portion of sheet 3 of 3 (internal document)
[R6]	248 Temp Transmitter adder for pannel mount.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, adder for pannel mount (internal document)
[R7]	248 Temp Transmitter Summary.xls, 03/06/2006	Failure Modes, Effects, and Diagnostic Analysis, 248 temperature transmitter, Summary (internal document)
[R8]	Field failure analysis Rosemount 248.xls, 03/29/2006	Field Failure Analysis 248 temperature transmitter (internal document)
[R9]	ROS 06-01-34 R001 V1 R1 FMEDA 248.doc, 4/3/2006	FMEDA report, 248 temperature transmitter (this report)

3 Product Description

The 248 temperature transmitter is a two-wire, smart device. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. The transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either low or high upon internal detection of a failure (output state is programmable).

The FMEDA has been performed for two different options of the 248 temperature transmitter. Table 5 lists the versions of the 248 temperature transmitter that have been considered for the hardware assessment.

Table 5 Version overview

248H	248 temperature transmitter, Headmount option
248R	248 temperature transmitter, Railmount option

The 248R attaches directly to a wall or a DIN rail. The 248H installs in a connection head or universal head mounted directly on a sensor assembly or apart from a sensor assembly using a universal head. The 248H can also mount to a DIN rail using an optional mounting clip.

The 248 temperature transmitter is classified as a Type B[3] device according to IEC 61508, having a hardware fault tolerance of 0. Combined with a temperature sensing device, the 248 temperature transmitter becomes a temperature sensor assembly.

The temperature sensing devices than can be connected to the 248 temperature transmitter are listed below:

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

Section 5.1 explains in more detail how to combine the failure rates for the transmitter and a sensing device.

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

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on documentation obtained from Rosemount Inc. and is documented in [R1] through [R7]. This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the 248 temperature transmitter, the following definitions for the failure of the product were considered.

Fail-Safe State
The fail-safe state is defined as state where the 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 (includes frozen output).

Fail Dangerous Undetected
Failure that is dangerous and that is not being diagnosed by internal diagnostics.

Fail Dangerous Detected
Failure that is dangerous but is detected by internal diagnostics, or a connected logic solver.

Fail High
Failure that causes the output signal to go to the maximum output current (> 21.5mA)

Fail Low
Failure that causes the output signal to go to the minimum output current (< 3.6mA)

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

Annunciation Undetected
Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High or a Fail Low can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified.

The Annunciation Undetected failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508, Edition 2000 [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* in this FMEDA is from a proprietary component failure rate database derived using the Telcordia failure rate database/models, the SN29500 failure rate database and other sources. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 248 temperature transmitter.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The application program in the safety logic solver is configured to detect under-range (Fail Low) and over-range (Fail High) failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- The HART protocol is only used for setup, calibration, and diagnostic purposes; not for safety critical operation.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
    - IEC 60654-1, Class C with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- External power supply failure rates are not included.

4.4 Results

Using reliability data extracted from the exida component reliability database the following failure rates resulted from the 248 temperature transmitter FMEDA. Table 6 lists the failure rates for the 248 temperature transmitter, Headmount option.

Table 6 Failure rates 248 temperature transmitter, Headmount option

Failure category		Failure rate (in FIT)			
		TC configuration		RTD configuration	
Fail Dangerous Detected			334		326
	Fail Detected (detected by int. diagnostics)	270		262	
	Fail High (detected by the logic solver)	42		42	
	Fail Low (detected by the logic solver)	22		22	
Fail Dangerous Undetected			66		64
No Effect			78		83
Annunciation Undetected			2		2

Table 7 lists the failure rates for the 248 temperature transmitter, Railmount option.

Table 7 Failure rates 248 temperature transmitter, Railmount option

Failure category		Failure rate (in FIT)			
		TC configuration		RTD configuration	
Fail Dangerous Detected			335		327
	Fail Detected (detected by int. diagnostics)	271		263	
	Fail High (detected by the logic solver)	42		42	
	Fail Low (detected by the logic solver)	22		22	
Fail Dangerous Undetected			66		64
No Effect			78		83
Annunciation Undetected			2		2

The failure rates that are derived from the FMEDA for the 248 temperature transmitter are in a format different from the IEC 61508 format. Table 8 lists the failure rates for 248 temperature transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

According to IEC 61508 [N1], also the Safe Failure Fraction (SFF) of the 248 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. This is reflected in the following formula for SFF:

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

Note that according to IEC 61508 definition the No Effect and Annunciation Undetected failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

Table 8 Failure rates and SFF according to IEC 61508

Device	λ_{sd}	λ_{su}[4]	λ_{dd}	λ_{du}	**SFF**
Headmount option, TC configuration	0 FIT	80 FIT	334 FIT	66 FIT	86.2%
Headmount option, RTD configuration	0 FIT	85 FIT	326 FIT	64 FIT	86.4%
Railmount option, TC configuration	0 FIT	80 FIT	335 FIT	66 FIT	86.2%
Railmount option, RTD configuration	0 FIT	85 FIT	327 FIT	64 FIT	86.5%

The architectural constraint type for 248 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.

[4] It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

5 Using the FMEDA results

5.1 Temperature sensing devices

The 248 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 thermocouples and RTDs are listed in the following table.

Table 9 Typical failure rates thermocouples and RTDs

Temperature Sensing Device	Failure rate (in FIT)
Thermocouple low stress environment	5,000
Thermocouple high stress environment	20,000
RTD low stress environment	2,000
RTD high stress environment	8,000

5.1.1 248 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 248 temperature transmitter. The drift failure mode is primarily due to T/C aging. The 248 temperature transmitter will detect a thermocouple burnout failure and drive the analog output to the specified failure state.

Table 10 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 248 temperature transmitter and a closely coupled thermocouple supplied with the 248 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 248 temperature transmitter is programmed to drive its output either high or low on detected failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

- λ^{DD} = (5000) * (0.95) = 4750 FIT
- λ^{DU} = (5000) * (0.05) = 250 FIT

The total for the temperature sensor assembly with the 248 temperature transmitter, Headmount option, is:

- λ^{DD} = 4750 + 334 = 5084 FIT
- λ^{DU} = 250 + 66 = 316 FIT

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 assembly is 94.2%.

5.1.2 248 temperature transmitter with RTD

The failure mode distribution for an RTD also depends on the application with 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 11. The 248 temperature transmitter will detect open circuit and short circuit RTD failures and drive its output either high or low on detected failures of the RTD.

Table 11 Typical failure mode distributions for 4-wire RTD, low stress environment

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 248 temperature transmitter and a closely coupled, cushioned 4-wire RTD supplied with the 248 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 248 temperature transmitter is programmed to drive its output either high or low on detected failures of the RTD, the failure rate contribution for a close-coupled 4-wire RTD in a low stress environment is:

- λ^{DD} = (2000) * (0.70 + 0.29) = 1980 FIT
- λ^{DU} = (2000) * (0.01) = 20 FIT

The total for the temperature sensor assembly with the 248 temperature transmitter, Headmount option, is:

- λ^{DD} = 1980 + 326 = 2306 FIT
- λ^{DU} = 20 + 64 = 84 FIT

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 96.6%.

5.2 PFD_{AVG} calculation 248 temperature transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 248 temperature transmitter, Headmount option with 4-wire RTD. The failure rate data used in this calculation is displayed in section 4.4 and 5.1.2.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} value for a single 248 temperature transmitter, Headmount option with 4-wire RTD with a proof test interval of 1 year equals 3.86E-04.

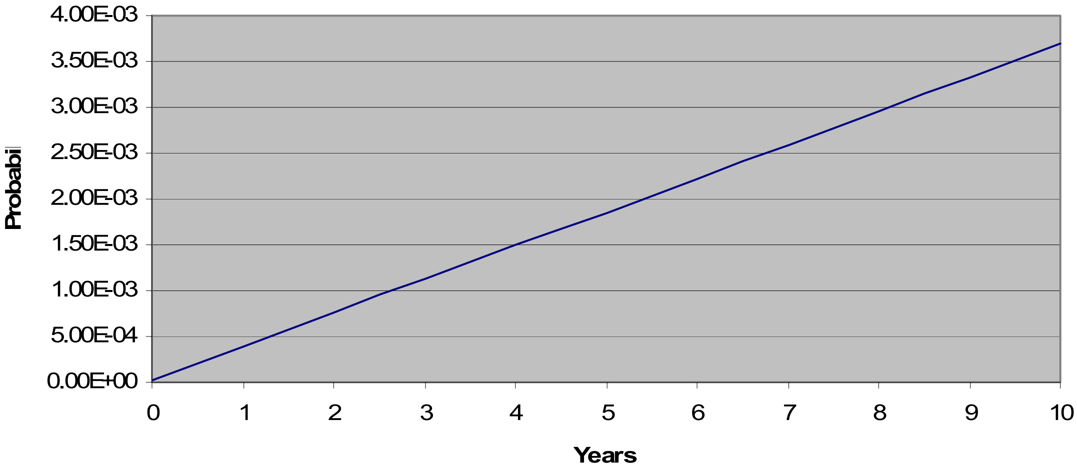

Figure 1 $PFD_{AVG}(t)$ 248 temperature transmitter

For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of the 248 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
RTD	Resistance Temperature Detector
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	“Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” subsystem (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

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

7.2 Releases

Version:	V1	
Revision:	R1	
Version History:	V1, R1:	Released to Rosemount Inc.; April 3, 2006
	V0, R1:	Draft; March 29, 2006
Authors:	John C. Grebe - Rachel Amkreutz	
Review:	V0, R1:	Randy Paschke (Rosemount); April 2, 2006
	V0, R1:	John Grebe (exida); March 29, 2006
Release status:	Released to Rosemount Inc.	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

William M Goble

Dr. William M. Goble, Principal Partner

John C. Grebe, Partner

Ir. Rachel Amkreutz, Safety Engineer

Appendix A: Lifetime of critical components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime[5] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

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

Table 12 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 12 Useful lifetime of electrolytic capacitors contributing to λ_{du}

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

As there are no aluminum electrolytic capacitors used, the tantalum electrolytic capacitors are the limiting factors with regard to the useful lifetime of the 248 temperature transmitter. The tantalum electrolytic capacitors that are used in the 248 temperature transmitter have an estimated useful lifetime of about 50 years.

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

[5] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B Proof test to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

B.1 Suggested Proof Test

A suggested proof test consists of an analog output loop test, as described in Table 13. This test will detect approximately 60% of possible DU failures in the 248 temperature transmitter, and 90% of the simple sensing element DU failures. This would mean a Proof Test Coverage of approximately 67% for the overall sensor assembly, assuming a single close-coupled 4-wire RTD is used.

Table 13 Steps for Proof Test

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 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 Alternative Proof Test

An alternative proof test consists of the following steps, as described in Table 14. This test will detect approximately 90% of possible DU failures in the 248 temperature transmitter, and 99% of the simple sensing element DU failures. This would mean a Proof Test Coverage of approximately 94% for the overall sensor assembly, assuming a single close-coupled 4-wire RTD is used.

Table 14 Steps for Alternative Proof Test

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; verify that the mA output corresponds to the temperature input value.
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 - redundant transmitter configuration

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 248 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 15 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	Design 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	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 248 temperature transmitter with hardware version Rev 4 and software revision 5.2.1, a review of proven-in-use documentation was performed. Design changes between the initial version of the product and hardware version Rev 4 and software revision 5.2.1 (current product) to the 248 temperature transmitter are documented, see [D4].

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

Since the 248 temperature transmitter was introduced to the market in 2003, the following operating experience exists:

248 temperature transmitter:	*> 300 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 2003, there have been two software revisions:

5.1.2 in April 2004

5.2.1 in July 2005

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

A separate assessment has previously been performed of the quality management, configuration management and modification systems within the Rosemount Inc. 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.