Failure Modes, Effects and Diagnostic Analysis

Project:
Rosemount Smart Wireless THUM Adapter

Company:
Rosemount, Inc.
Chanhassen, MN
USA

Contract Number: Q09/10-03
Report No.: ROS 09/10-03 R001
Version V1, Revision R3, November 11, 2009
John 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 hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Rosemount Smart Wireless THUM Adapter. The Smart Wireless THUM adapter is a device that can be added to any two or four-wire HART device, and it allows wireless access to HART measurement and diagnostic information.

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 non-interference FMEDA that is described in this report concerns only the potential interference of hardware of the THUM Adapter with its associated HART device since the THUMB Adapter does not perform any activities that are part of a Safety Instrumented Function (SIF).

For safety instrumented systems usage it is assumed that the 4 – 20 mA input or output of the connected HART device is used as the primary safety variable and the information transmitted through the THUM Adapter is not relied upon by any SIF. Therefore, this FMEDA only covers potential failure modes of the THUM Adapter that can impact the 4 – 20 mA output from the connected HART device. Other failure modes that only impact the correct operation of the THUM Adapter and the Wireless HART data are not included in the data provided by this report. Only the potential for interference with the analog primary variable of the associate HART device and not its function or location in the circuit determines whether or not a particular failure mode of a component is included.

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

Table 1 Version Overview

THUM Adapter	Rosemount Smart Wireless THUM™ Adapter

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

As the THUM Adapter is connected in series with the 4 – 20 mA loop and also includes a HART communications connection to the opposite side of the HART device, it is capable of resulting in the following types of interfering failure modes:

- Fail Low where the 4 - 20 mA loop current levels are 0 mA (open circuit) or limited to be below to the under-range or low alarm output current(typically ≤ 3.75 mA)
- Fail High where the 4 - 20 mA loop current levels are higher than the over-range or high alarm output current (typically ≥ 21.75 mA)
- Fail Dangerous Undetected where the 4 – 20 mA signal may be impacted (higher or lower) than 0.1% (as this would add to the worse case safety accuracy of the attached device)

The interfering failure rates for the THUM Adapter are listed in Table 2.

[1] Type A device: “Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2

Table 2 Interfering Failure rates THUM Adapter

Failure Category	Failure Rate (FIT)	
Fail Dangerous Detected		11.4
Fail High (detected by logic solver)	1.4	
Fail Low (detected by logic solver)	10.0	
Fail Dangerous Undetected		0.3

Table 3 lists the interfering failure rates for the THUM Adapter according to IEC 61508.

Table 3 Interfering Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
THUM Adapter	0 FIT	0 FIT	11.4 FIT	0.3 FIT

The user of the THUM Adapter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) by adding these failure rates to the failure rates of the wired device to which it is attached to determine total subsystem failure rates. These are then used to proceed with calculations. It is recommended that an engineering tool like the exida exSILentia® be used for this purpose. A table of failure rates is presented in section 4.4 along with all assumptions.

Table of Contents

Management Summary 2
1 Purpose and Scope 5
2 Project Management 6
2.1 *exida* 6
2.2 Roles of the parties involved 6
2.3 Standards and Literature used 6
2.4 Reference documents 7
2.4.1 Documentation provided by Rosemount, Inc. 7
2.4.2 Documentation generated by *exida* 7
3 Product Description 8
4 Failure Modes, Effects, and Diagnostic Analysis 9
4.1 Failure Categories description 9
4.2 Methodology – FMEDA, Failure Rates 9
4.2.1 FMEDA 9
4.2.2 Failure Rates 9
4.3 Assumptions 10
4.4 Results 11
5 Using the FMEDA Results 12
6 Terms and Definitions 13
7 Status of the Document 14
7.1 Liability 14
7.2 Releases 14
7.3 Future Enhancements 14
7.4 Release Signatures 15
Appendix A Lifetime of Critical Components 16
Appendix B Proof tests to reveal dangerous undetected faults 17

1 Purpose and Scope

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

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

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

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

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

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

2 Project Management

2.1 *exida*

exida is one of the world's leading certification and knowledge companies specializing in automation system safety and availability with over 300 man 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* has offices around the world. *exida* offers product functional safety and security certification, training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Rosemount, Inc.	Manufacturer of the THUM Adapter
exida	Performed the hardware assessment according to Option 1 (see Section 1)

Rosemount, Inc. contracted *exida* in September 2009 with the hardware assessment of the above-mentioned device.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	exida L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	exida L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	Goble, W.M. and Cheddie, H., 2005	Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISA, ISBN 1-55617-909-X

2.4 Reference documents

2.4.1 Documentation provided by Rosemount, Inc.

[D1]	775-3203.pdf	Schematic, SCHEMATIC, THUM DIGITAL BOARD, Drawing No. 00775-3203, Rev. AE
[D2]	775-3200.pdf	Schematic, SCHEMATIC, THUM REGULATOR BOARD, Drawing No. 00775-3200, Rev. AF
[D3]	00809-0100-4075_AA_ screen.pdf	Reference Manual, Smart Wireless THUM, Drawing No. 00809-0100-4075, Rev. AA, September 2009

2.4.2 Documentation generated by *exida*

[R1]	Rosemount Thum HART Interference Only.efm	Failure Modes, Effects, and Diagnostic Analysis – THUM Adapter
[R2]	ROS 09-10-03 R001 V0 R0 FMEDA Thum Wireless Adapter.doc, 11/11/2009	FMEDA report, THUM Adapter (this report)

3 Product Description

The Smart Wireless THUM adapter is a device that can be added to any two or four-wire HART device, and it allows wireless access to HART measurement and diagnostic information. With simple HART configuration, the THUM transmits the HART information from the sub-device into the WirelessHART network.

The THUM Adapter is connected to a powered 4–20 mA loop, powering itself by scavenging power. The THUM Adapter causes a voltage drop across the loop that is linear from 2.25 volts at 3.5 mA to 1.2 volts at 25 mA, and is not expected to effect the 4–20mA signal on the loop during normal operation or transmitter fault conditions.

For safety instrumented systems usage it is assumed that the 4 – 20 mA input or output of the connected HART device is used as the primary safety variable and the information transmitted through the THUM Adapter is not relied upon by any SIF. Therefore, this FMEDA only covers potential failure modes of the THUM Adapter that can impact the 4 – 20 mA output from the connected HART device. Other failure modes that only impact the correct operation of the THUM Adapter and the Wireless HART data are not included in the data provided by this report. Only the potential for interference with the analog primary variable of the associate HART device and not its function or location in the circuit determines whether or not a particular failure mode of a component is included.

As the THUM Adapter is connected in series with the 4 – 20 mA loop and also includes a HART communications connection to the opposite side of the HART device, it is capable of resulting in the following types of interfering failure modes:

- Fail Low where the 4 - 20 mA loop current levels are 0 mA (open circuit) or limited to be below to the under-range or low alarm output current(typically ≤ 3.75 mA)
- Fail High where the 4 - 20 mA loop current levels are higher than the over-range or high alarm output current (typically ≥ 21.75 mA)
- Fail Dangerous Undetected where the 4 – 20 mA signal may be impacted (higher or lower) than 0.1% (as this would add to the worse case safety accuracy of the attached device)

Table 4 gives an overview of the different versions that were considered in the FMEDA of the THUM Adapter.

Table 4 Version Overview

THUM Adapter	Rosemount Smart Wireless THUM™ Adapter

The THUM Adapter for interference purposes is classified as a Type A[3] device according to IEC 61508, having a hardware fault tolerance of 0.

[3] Type A device: “Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Rosemount, Inc. and is documented in [D1] through [D3].

4.1 Failure Categories description

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

Fail Dangerous Undetected	Failure that deviates the measured input state or the actual output by more than 0.1% of span and that leaves the output within active scale
Fail High	Failure that causes the output signal of the attached device to go to the over-range or high alarm output current (≥ 21.75 mA)
Fail Low	Failure that causes the output signal of the attached device to go to the under-range or low alarm output current(≤ 3.75 mA)

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected.

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.

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

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

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook which was derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 2, see Table 5. 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.

Table 5 exida Environmental Profiles

EXIDA ENVIRONMENTAL PROFILE		GENERAL DESCRIPTION	PROFILE PER IEC 60654-1	AMBIENT TEMPERATURE [°C]		TEMP CYCLE [°C / 365 DAYS]
				AVERAGE (EXTERNAL)	MEAN (INSIDE BOX)	
1	Cabinet Mounted Equipment	Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings	B2	30	60	5
2	Low Power /Mechanical Field Products	Mechanical / low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings	C3	25	30	25
3	General Field Equipment	General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings	C3	25	45	25
4	Unprotected Mechanical Field Products	Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation.	D1	25	30	35

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however, should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

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

4.3 Assumptions

The following assumptions have been made during the interfering only Failure Modes, Effects, and Diagnostic Analysis of the THUM Adapter.

- Only a single component failure will fail the entire THUM Adapter
- Failure rates are constant, wear-out mechanisms are not included
- Propagation of failures is not relevant
- All components and failure modes that are not potentially interfering and cannot influence the safety function of the connected sub-device (feedback immune) are excluded

- 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.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics
- The HART protocol is not used 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 device is installed per manufacturer's instructions
- External power supply failure rates are not included

4.4 Results

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

The failure rates for the THUM are listed in Table 6.

Table 6 Interfering Failure rates THUM Adapter

Failure Category	Failure Rate (FIT)	
Fail Dangerous Detected		11.4
Fail High (detected by logic solver)	1.4	
Fail Low (detected by logic solver)	10.0	
Fail Dangerous Undetected		0.3

These failure rates are valid for the useful lifetime of the product, see Appendix A. Table 7lists the failure rates for the THUM Adapter according to IEC 61508.

Table 7 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF[5]
THUM Adapter	0 FIT	0 FIT	11.4 FIT	0.3 FIT	-

The architectural constraint type for the THUM Adapter is A. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

[5] Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

The results of this FMEDA are only useful when evaluated within the context of an actual SIF or at least in combination with the FMEDA failure rate data for a selected connected sub-device.

For use of the THUM Adapter on a connected sub-device that is part of a SIF, the Dangerous Undetected, Fail High and Fail Low failure rates for the THUM Adapter are added to failure rates fro the associated connected sub-device prior to the SFF or PFD_{AVG} calculations for the Safety Instrumented Function (SIF).

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The results must be considered in combination with PFD_{AVG} values of all other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Definitions

FIT	Failure In Time (1x10-9 failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	“Non-Complex” component (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

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

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

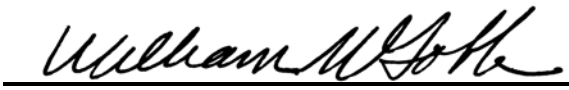
7.2 Releases

Version:	V1	
Revision:	R3	
Version History:	V0, R0:	Draft; August 27, 2009
	V1, R1:	Draft for client review, October 15, 2009
	V1, R2:	First Release, October 23, 2009
	V1, R3:	Addressed comments from client
Author(s):	John Grebe	
Review:	V0, R0:	William Goble
	V1, R1:	Rosemount
	V1, R2:	Rosemount
Release Status:	Released	

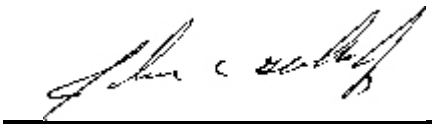
7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Dr. William M. Goble, Principal Partner



John C. Grebe Jr., Principal Engineer

Appendix A Lifetime of Critical Components

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[6] 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 8 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 8 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
No known potentially interfering component with limited lifetime	Approx. 50+ years

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

As there are no potentially interfering components with specific mechanisms that limit their useful lifetime the estimated useful lifetime is considered to be 50+ years.

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

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

Appendix B Proof tests to reveal dangerous undetected faults

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

No special proof test is needed to detect possible DU failures in the THUM. The simple suggested proof test is part of the transmitter test and can be performed with the THUM Adapter and its associated transmitter without need for removal from the process. This test will detect essentially 100% of possible DU interfering failures in the THUM device.

Table 9 Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Use HART communications to retrieve any diagnostics and take appropriate action.
3.	Use HART command to the transmitter attached to the THUM Adapter to go to the high alarm current output and verify that the analog current reaches that value[7].
4.	Send a HART command to the transmitter attached to the THUM Adapter to go to the low alarm current output and verify that the analog current reaches that value[8].
5.	Remove the bypass and otherwise restore normal operation

[7] This tests for compliance voltage problems such as the THUM Adapter consuming too much compliance voltage or a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

[8] This tests for possible leakage current related failures with the THUM Adapter.