Failure Modes, Effects and Diagnostic Analysis

Project:
One Series SAFETY TRANSMITTER

Company:
United Electric Controls
Watertown, MA
USA

Contract Number: Q04/04-001
Report No.: UE 12/10-073 R001
Version V2, Revision R2, April 11, 2014
Rudolf Chalupa

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

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the One Series SAFETY TRANSMITTER, hardware and software revision per section 2.5.1. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the SAFETY TRANSMITTER. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The One Series SAFETY TRANSMITTER is a smart device which senses temperature or pressure and provides a 4-20mA and/or solid state relay outputs. It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. The SAFETY TRANSMITTER also provides an “I Am Working” output as well as a switch status output which echoes the state of the relay output.

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

Table 1 Version Overview

Pressure Current IAW	Pressure input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is monitored.
Temperature Current IAW	Temperature input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is monitored
Pressure Current no IAW	Pressure input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is not monitored.
Temperature Current no IAW	Temperature input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is not monitored
Pressure Relay IAW	Pressure input; the de-energize-to-trip relay output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.
Temperature Relay IAW	Temperature input; the de-energize-to-trip relay output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.
Pressure Status IAW	Pressure input; the de-energize-to-trip status output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.
Temperature Status IAW	Temperature input; the de-energize-to-trip status output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.

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

The analysis shows that the has a Safe Failure Fraction between 90% and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

The failure rates for the SAFETY TRANSMITTER are listed in Table 2 - Table 9.

Table 2 Failure rates SAFETY TRANSMITTER Pressure Current IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		76
Fail Dangerous Detected		3429
Fail Detected (detected by internal diagnostics)	3391	
Fail High (detected by logic solver)	16	
Fail Low (detected by logic solver)	22	
Fail Dangerous Undetected		42
No Effect		331
Annunciation Undetected		24

Table 3 Failure rates SAFETY TRANSMITTER Temperature Current IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		76
Fail Dangerous Detected		3442
Fail Detected (detected by internal diagnostics)	3408	
Fail High (detected by logic solver)	15	
Fail Low (detected by logic solver)	19	
Fail Dangerous Undetected		42
No Effect		330
Annunciation Undetected		24

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

Table 4 Failure rates SAFETY TRANSMITTER Pressure Current no IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		78
Fail Dangerous Detected		3400
Fail Detected (detected by internal diagnostics)	3363	
Fail High (detected by logic solver)	17	
Fail Low (detected by logic solver)	20	
Fail Dangerous Undetected		48
No Effect		331
Annunciation Undetected		53

Table 5 Failure rates SAFETY TRANSMITTER Temperature Current no IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		76
Fail Dangerous Detected		3409
Fail Detected (detected by internal diagnostics)	3375	
Fail High (detected by logic solver)	15	
Fail Low (detected by logic solver)	19	
Fail Dangerous Undetected		45
No Effect		331
Annunciation Undetected		52

Table 6 Failure rates SAFETY TRANSMITTER Pressure Relay IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1711
Fail Safe Undetected	76
Fail Dangerous Detected	1700
Fail Dangerous Undetected	80
No Effect	297
Annunciation Detected	44
Annunciation Undetected	26

Table 7 Failure rates SAFETY TRANSMITTER Temperature Relay IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1711
Fail Safe Undetected	76
Fail Dangerous Detected	1719
Fail Dangerous Undetected	80
No Effect	297
Annunciation Detected	44
Annunciation Undetected	26

Table 8 Failure rates SAFETY TRANSMITTER Pressure Status IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1666
Fail Safe Undetected	106
Fail Dangerous Detected	1690
Fail Dangerous Undetected	46
No Effect	333
Annunciation Detected	28
Annunciation Undetected	25

Table 9 Failure rates SAFETY TRANSMITTER Temperature Status IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1668
Fail Safe Undetected	106
Fail Dangerous Detected	1710
Fail Dangerous Undetected	46
No Effect	335
Annunciation Detected	28
Annunciation Undetected	25

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

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

Table 10 lists the failure rates for the SAFETY TRANSMITTER according to IEC 61508, ed2, 2010.

Table 10 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF[3]
Pressure Current IAW	0	76	3429	42	98.8%
Temperature Current IAW	0	76	3442	42	98.8%
Pressure Current no IAW	0	78	3400	48	98.6%
Temperature Current no IAW	0	76	3409	45	98.7%
Pressure Relay IAW	1755	76	1700	80	97.8%
Temperature Relay IAW	1755	76	1719	80	97.8%
Pressure Status IAW	1694	106	1690	46	98.7%
Temperature Status IAW	1696	106	1710	46	98.7%

A user of the SAFETY 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 no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

[3] Safe Failure Fraction if needed, is to be calculated on an element level

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the SAFETY TRANSMITTER. From this, failure rates and example PFD_{AVG} values may be calculated.

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

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

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

United Electric Controls	Manufacturer of the SAFETY TRANSMITTER
exida	Performed the hardware assessment
United Electric Controls	contracted *exida* in October 2012 with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

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

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3nd Edition, 2012	exida LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3nd Edition, 2012	exida LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	exida LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

2.4 *exida* tools used

[T1]	7.1.18	FMEDA Tool
[T2]	3.0.9.888	exSILentia

2.5 Reference documents

2.5.1 Documentation provided by United Electric Controls

[D1]	Doc # SR113028.D2.5, Rev B, 2012-12-26	System Architecture Description
[D2]	Doc # SR113028.D3.2, Rev A, 2013-06-17	Circuit Descriptions
[D3]	Doc # SR113028.D4.2, Rev C Draft, undated	Software Architecture Description
[D4]	Doc # 6247-691, Rev E, 2013-06-10	Schematic Drawing, Main Board
[D5]	Doc # 6247-692, Rev E, 2013-07-01	Schematic Drawing, Relay Board
[D6]	SR#113028.D3.8, 2013-11-12	Fault Injection Test Report

2.5.2 Documentation generated by *exida*

[R1]	UE1S Main Board Pressure Current IAW 2014-04-04.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Pressure Input, Current Output, IAW monitored
[R2]	UE1S Main Board Pressure Current No IAW 2014-04-04.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Pressure Input, Current Output, IAW not monitored
[R3]	UE1S Main Board Pressure Discrete IAW 2014-04-03.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Pressure Input Relay Output, IAW monitored
[R4]	UE1S Main Board Pressure Status IAW 2014-04-03.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Pressure Input Status Output, IAW monitored
[R5]	UE1S Main Board Temperature Current IAW 2014-04-03.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Temperature Input Current Output, IAW monitored
[R6]	UE1S Main Board Temperature Current No IAW 2014-04-02.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Temperature Input Current Output, IAW not monitored
[R7]	UE1S Main Board	Failure Modes, Effects, and Diagnostic Analysis – SAFETY

	Temperature Discrete IAW 2014-04-03.efm	TRANSMITTER Main Board, Temperature Input, Relay Output, IAW monitored
[R8]	UE1S Main Board Temperature Status IAW 2014-04-04.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Main Board, Temperature Input, Status Output, IAW monitored
[R9]	UE1S Relay Board Current IAW 2014-04-02.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Relay Board, Current Output, IAW monitored
[R10]	UE1S Relay Board Current No IAW 2014-04-02.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Relay Board, Current Output, IAW not monitored
[R11]	UE1S Relay Board Discrete IAW 2014-02-02.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Relay Board, Relay Output
[R12]	UE1S Relay Board Status IAW 2014-02-02.efm	Failure Modes, Effects, and Diagnostic Analysis – SAFETY TRANSMITTER Relay Board, Status Output
[R13]	UE1S Summary 2014-04-04.xls	Failure Modes, Effects, and Diagnostic Analysis - Summary –SAFETY TRANSMITTER
[R14]	UE 12-10-073 R001 V2 R2 One Series SAFETY TRANSMITTER FMEDA Report.doc, 04/11/2014	FMEDA report, SAFETY TRANSMITTER (this report)

3 Product Description

The One Series SAFETY TRANSMITTER is a smart device which senses temperature or pressure and provides a 4-20mA and/or solid state relay outputs. It contains self-diagnostics and is programmed to send its output to a specified failure state upon internal detection of a failure. The SAFETY TRANSMITTER provides an “I Am Working” output as well as a switch status output which echoes the state of the relay output.

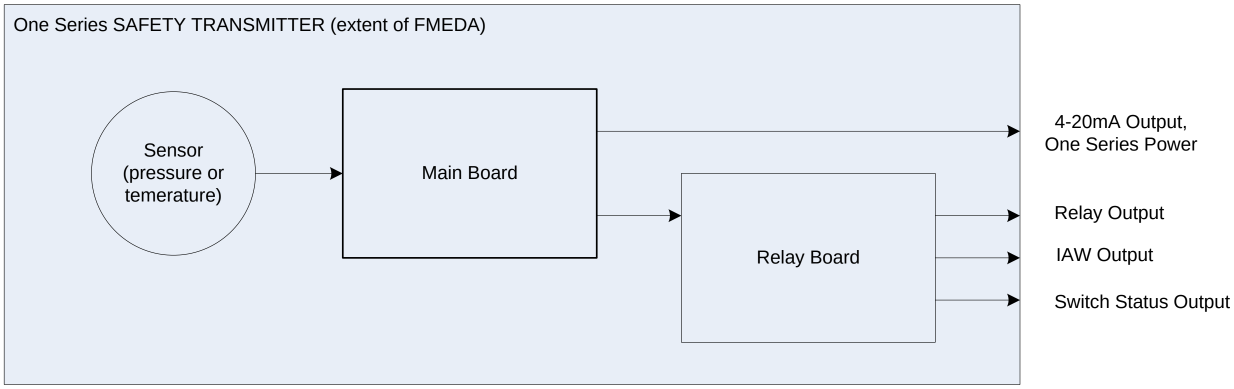

One Series SAFETY TRANSMITTER (extent of FMEDA)
Sensor (pressure or temerature)
Main Board
Relay Board
4-20mA Output, One Series Power
Relay Output
IAW Output
Switch Status Output

Figure 1 SAFETY TRANSMITTER, Parts included in the FMEDA

Table 11 gives an overview of the different versions that were considered in the FMEDA of the SAFETY TRANSMITTER.

Table 11 Version Overview

Pressure Current IAW	Pressure input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is monitored.
Temperature Current IAW	Temperature input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is monitored
Pressure Current no IAW	Pressure input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is not monitored.
Temperature Current no IAW	Temperature input; the externally energized 4-20mA current loop supplies the safety variable to a logic solver. The IAW output is not monitored
Pressure Relay IAW	Pressure input; the de-energize-to-trip relay output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.
Temperature Relay IAW	Temperature input; the de-energize-to-trip relay output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.
Pressure Status IAW	Pressure input; the de-energize-to-trip status output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.
Temperature Status IAW	Temperature input; the de-energize-to-trip status output provides the safety variable to a logic solver or directly to the final element. The IAW output is monitored.

The SAFETY TRANSMITTER is classified as a Type B[4] element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis as performed based on the documentation obtained from United Electric Controls and is documented in [R1] - [R13].

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, see Fault Injection Test Report [D6]..

4.1 Failure categories description

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

Fail-Safe State
Failure that deviates the process signal or the actual output by more than 3% of span, drifts toward the user defined threshold (Trip Point) and that leaves the output within active scale.

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

Fail Detected
Failure that causes the output signal to go to the predefined alarm state (3.7 mA).

Fail Dangerous
Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

Transmitter
Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within active scale.

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

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

Fail High
Failure that causes the output signal to go to the over-range or high alarm output current (> 21 mA).

Fail Low
Failure that causes the output signal to go to the under-range or low alarm output current(< 3.8 mA).

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

Annunciation Detected
Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.

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

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation needed when Route 2H failure data is not available.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which was derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations.

The rates were chosen to match *exida* Profile 2, see Appendix C. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by United Electric Controls. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

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

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

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its "useful life". 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 such as *exida* SILStat^{TM} 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 SAFETY TRANSMITTER.

- Only a single component failure will fail the entire SAFETY TRANSMITTER.
- 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.
- Failures caused by maintenance capability are site specific and therefore cannot be included.
- 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.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed per manufacturer's instructions.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is 6 seconds.

4.4 Results

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

Table 12 Failure rates SAFETY TRANSMITTER Pressure Current IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		76
Fail Dangerous Detected		3429
Fail Detected (detected by internal diagnostics)	3391	
Fail High (detected by logic solver)	16	
Fail Low (detected by logic solver)	22	
Fail Dangerous Undetected		42
No Effect		331
Annunciation Undetected		24

Table 13 Failure rates SAFETY TRANSMITTER Temperature Current IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		76
Fail Dangerous Detected		3442
Fail Detected (detected by internal diagnostics)	3408	
Fail High (detected by logic solver)	15	
Fail Low (detected by logic solver)	19	
Fail Dangerous Undetected		42
No Effect		330
Annunciation Undetected		24

Table 14 Failure rates SAFETY TRANSMITTER Pressure Current no IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		78
Fail Dangerous Detected		3400
Fail Detected (detected by internal diagnostics)	3363	
Fail High (detected by logic solver)	17	
Fail Low (detected by logic solver)	20	
Fail Dangerous Undetected		48
No Effect		331
Annunciation Undetected		53

Table 15 Failure rates SAFETY TRANSMITTER Temperature Current no IAW

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		76
Fail Dangerous Detected		3409
Fail Detected (detected by internal diagnostics)	3375	
Fail High (detected by logic solver)	15	
Fail Low (detected by logic solver)	19	
Fail Dangerous Undetected		45
No Effect		331
Annunciation Undetected		52

Table 16 Failure rates SAFETY TRANSMITTER Pressure Relay IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1711
Fail Safe Undetected	76
Fail Dangerous Detected	1700
Fail Dangerous Undetected	80
No Effect	297
Annunciation Detected	44
Annunciation Undetected	26

Table 17 Failure rates SAFETY TRANSMITTER Temperature Relay IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1711
Fail Safe Undetected	76
Fail Dangerous Detected	1719
Fail Dangerous Undetected	80
No Effect	297
Annunciation Detected	44
Annunciation Undetected	26

Table 18 Failure rates SAFETY TRANSMITTER Pressure Status IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1666
Fail Safe Undetected	106
Fail Dangerous Detected	1690
Fail Dangerous Undetected	46
No Effect	333
Annunciation Detected	28
Annunciation Undetected	25

Table 19 Failure rates SAFETY TRANSMITTER Temperature Status IAW

Failure Category	Failure Rate (FIT)
Fail Safe Detected	1668
Fail Safe Undetected	106
Fail Dangerous Detected	1710
Fail Dangerous Undetected	46
No Effect	335
Annunciation Detected	28
Annunciation Undetected	25

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

Table 20 lists the failure rates for the SAFETY TRANSMITTER according to IEC 61508.

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

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

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

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$\mathrm{SFF} = (\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg})/(\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg} + \Sigma\lambda_{DU} \text{ avg })$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$\mathrm{SFF} = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$

Where:

$\lambda_{S\,=}$ Fail Safe
$\lambda_{DD\,=}$ Fail Dangerous Detected
$\lambda_{DU=}$ Fail Dangerous Undetected

Table 20 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	SFF[6]
Pressure Current IAW	0	76	3429	42	98.8%
Temperature Current IAW	0	76	3442	42	98.8%
Pressure Current no IAW	0	78	3400	48	98.6%
Temperature Current no IAW	0	76	3409	45	98.7%
Pressure Relay IAW	1755	76	1700	80	97.8%
Temperature Relay IAW	1755	76	1719	80	97.8%
Pressure Status IAW	1694	106	1690	46	98.7%
Temperature Status IAW	1696	106	1710	46	98.7%

[5] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

[6] Safe Failure Fraction if needed, is to be calculated on an element level

5 Using the FMEDA Results

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

5.1 Impulse line clogging

The transmitter can be connected to the process using impulse lines; depending on the application, the analysis needs to account for clogging of the impulse lines. The SAFETY TRANSMITTER failure rates that are displayed in section 4.4 are failure rates that reflect the situation where the transmitter is used in clean service. Clean service indicates that failure rates due to clogging of the impulse line are not counted. For applications other than clean service, the user must estimate the failure rate for the clogged impulse line and add this failure rate to the SAFETY TRANSMITTER failure rates. Note that the SAFETY TRANSMITTER has plugged port detection; this should be taken into account when estimating the failure rate.

5.2 $\mathrm{PFD}_{\mathrm{AVG}}$ calculation SAFETY TRANSMITTER

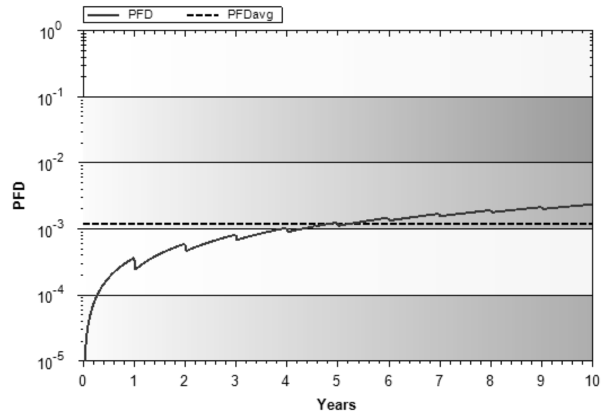
An average Probability of Failure on Demand ($\mathrm{PFD}_{\mathrm{AVG}}$) calculation is performed for a single (1oo1) SAFETY TRANSMITTER with *exida's* exSILentia tool. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. Table 21 lists the proof test coverage (see Appendix B) used for the various configurations as well as the results when the proof test interval equals 1 year.

Table 21 Sample $\mathrm{PFD}_{\mathrm{AVG}}$ Results

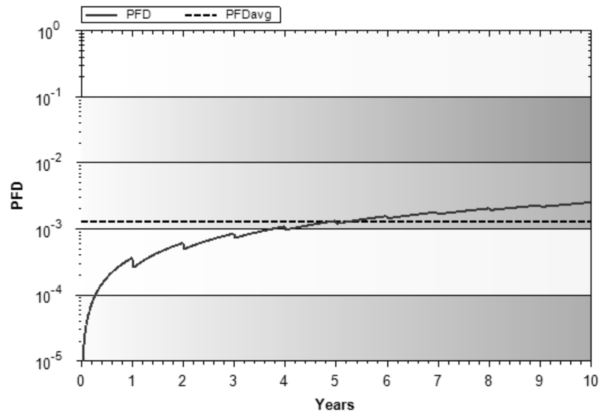
Device	Proof Test Coverage	$\mathrm{PFD}_{\mathrm{AVG}}$	% of SIL 2 Range
Pressure Current IAW	40%	1.19E-03	12%
Temperature Current IAW	35%	1.27E-03	13%
Pressure Current no IAW	47%	1.23E-03	12%
Temperature Current no IAW	40%	1.28E-03	13%
Pressure Relay IAW	71%	1.36E-03	14%
Temperature Relay IAW	71%	1.36E-03	14%
Pressure Status IAW	49%	1.14E-03	11%
Temperature Status IAW	49%	1.19E-03	12%

The resulting $\mathrm{PFD}_{\mathrm{AVG}}$ Graphs generated from the exSILentia tool for a proof test of 1 year are displayed in Figure 2.

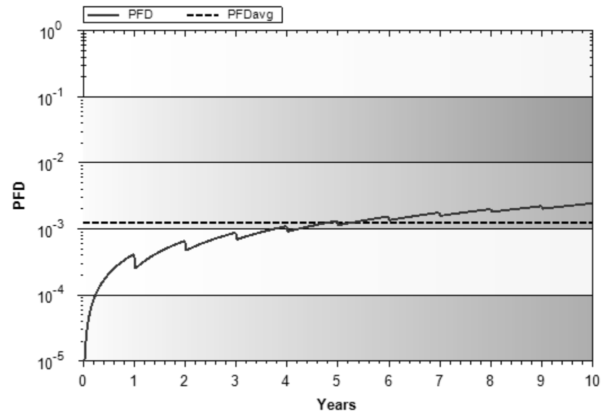
Sensor Group 1: Pressure Current IAW



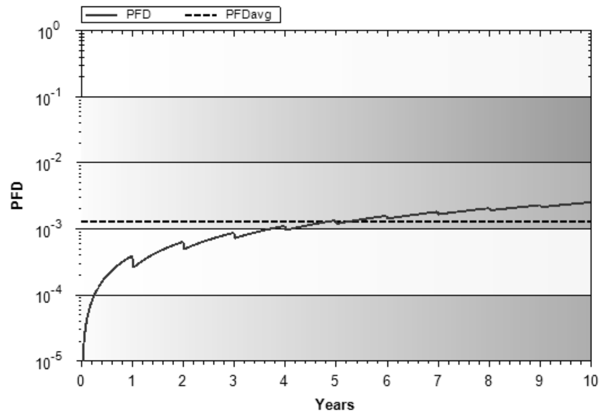
Sensor Group 1: Temperature Current IAW



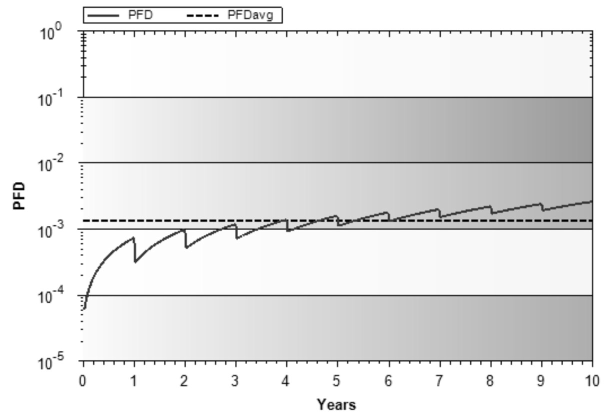
Sensor Group 1: Pressure Current no IAW



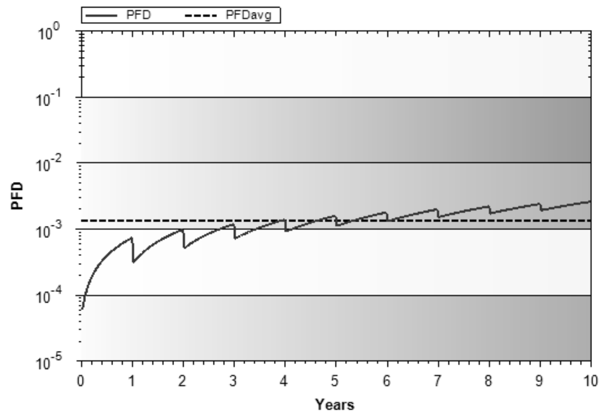
Sensor Group 1: Temperature Current no IAW



Sensor Group 1: Pressure Relay IAW



Sensor Group 1: Temperature Relay IAW



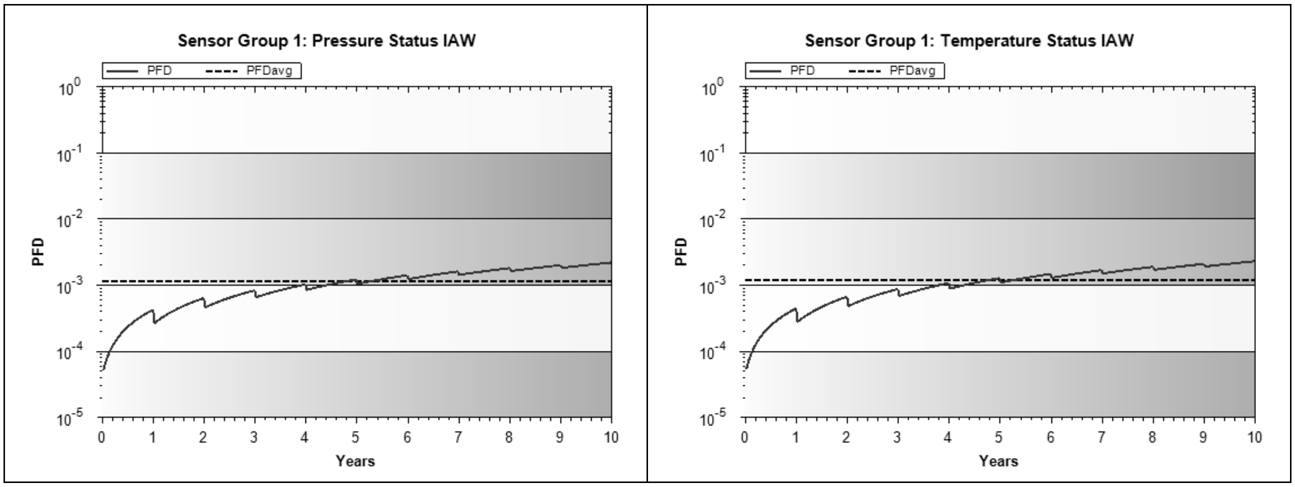


Figure 2 PFD$_{AVG}$ value for a single SAFETY TRANSMITTER with proof test interval of 1 year.

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.

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

6 Terms and Definitions

FIT — Failure In Time (1x10-9 failures per hour)

FMEDA — Failure Mode Effect and Diagnostic Analysis

HFT — Hardware Fault Tolerance

Low demand mode — Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.

Automatic Diagnostics — Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.

PFD_{AVG} — Average Probability of Failure on Demand

SFF — Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.

SIF — Safety Instrumented Function

SIL — Safety Integrity Level

SIS — Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

Type A element — “Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2

Type B element — “Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

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

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

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

7.2 Releases

Version:	V2
Revision:	R2
Version History:	V2, R2: corrected typos; updated fault injection test data; 2014-04-11
	V2, R1: Updated analysis per current hardware, added status output and unsupervised current output analyses, 2014-04-07
	V1, R2: Updated product name; 2013-10-18
	V1, R1: Released to United Electric Controls; 2013-07-24
	V0, R1: Draft; 2013-07-16
Author(s):	Rudolf Chalupa
Review:	V2, R1: John Yozallinas (exida); 2014-04-04
	V0, R1: Chris O'Brien (exida); 2013-07-19
Release Status:	Released to United Electric Controls

7.3 Future enhancements

At request of client.

7.4 Release signatures

Rudolf P. Chalupa

Rudolf P. Chalupa, Senior Safety Engineer

Ch O'B

Chris O’Brien, Partner

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[7] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

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

Table 17 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 22 Useful lifetime of components contributing to dangerous undetected failure rate

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

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

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

For high demand mode applications, the useful lifetime of the relay is limited by the number of cycles. The useful lifetime of the relay is > 100,000 full scale cycles or 8 to 10 years, whichever results in the shortest lifetime.

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

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

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The suggested transmitter proof test consists of a setting the output to the min and max, and a calibration check, see Table 23.

Table 23 Suggested Proof Test – Transmitter

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Inspect the transmitter for any leaks, visible damage or contamination.
3.	Verify proper operation of relay outputs.
4.	Perform a two-point calibration[8] of the transmitter over the full working range.
5.	Remove the bypass and otherwise restore normal operation.

B.2 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 24.

Table 24 Proof Test Coverage – SAFETY TRANSMITTER

Device	Proof Test Coverage
Pressure Current IAW	40%
Temperature Current IAW	35%
Pressure Current no IAW	47%
Temperature Current no IAW	40%
Pressure Relay IAW	71%
Temperature Relay IAW	71%
Pressure Status IAW	49%
Temperature Status IAW	49%

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

Appendix C *exida* Environmental Profiles

Table 25 *exida* Environmental Profiles

exida **Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[9]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[10]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[11]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[12]	G2	G3	G3	G3	G3	Compatible Material
Surge[13]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[14]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[15]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[9] Humidity rating per IEC 60068-2-3
[10] Shock rating per IEC 60068-2-6
[11] Vibration rating per IEC 60770-1
[12] Chemical Corrosion rating per ISA 71.04
[13] Surge rating per IEC 61000-4-5
[14] EMI Susceptibility rating per IEC 6100-4-3
[15] ESD (Air) rating per IEC 61000-4-2