Failure Modes, Effects and Diagnostic Analysis

Project:
Honeywell Temperature Transmitter STT650 with 4-20 mA Output

Company:
Honeywell International Inc.
Field Products
512 Virginia Drive
Fort Washington, PA 19034
USA

Contract Number: Q14/09-200
Report No.: HON 14/09-200 R001
Version V1, Revision R1, November 30, 2014
Loren Stewart

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 Honeywell Temperature Transmitter STT650 with 4-20 mA Output for temperature sensors, voltage signals, resistance-type sensors and potentiometers, with software revision V1.1 and hardware revision per the referred diagrams (see section 2.4.1). 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 Temperature Transmitter STT650 with 4-20 mA Output. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Temperature Transmitter STT650 with 4-20 mA Output is an isolated two-wire 4-20mA device used in many different industries for both control and safety applications. Combined with a temperature sensing device, the Temperature Transmitter STT650 with 4-20 mA Output becomes a temperature sensor assembly.

The transmitter operates with a 2-wire system. The same wires are used for the operating voltage (depending on the transmitter) and the output signal (4-20 mA) including HART® protocol.

Table 1 gives an overview of the version that was considered in the FMEDA of the Temperature Transmitter STT650 with 4-20 mA Output.

Table 1 Version Overview

Option 1	Temperature transmitter, head or rail mounted – (Standard, ATEX, FM, CSA)

The Temperature Transmitter STT650 with 4-20 mA Output is classified as a component of a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

Assuming that the application program in the connected safety logic solver is configured to detect under-range and over-range failures of the 4..20 mA output signal, and does not automatically trip on these failures; these failures have been classified as dangerous detected failures. For these applications the following tables show the worst-case failure rates according to IEC 61508:2010 2nd edition for the Temperature Transmitter STT650 with 4-20 mA Output (considering one input and one output being part of the safety function) when used with RTD or Thermocouple sensor types.

The failure rate data used for this analysis has a high confidence level and meets the exida criteria for Route 2_H. See Section 5.3. Therefore the Temperature Transmitter STT650 with 4-20 mA Output meets the hardware architectural constraints for up to up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) as a single device when the listed failure rates are used.

The failure rates for the Temperature Transmitter STT650 with 4-20 mA Output are listed in Table 2.

[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 2 Failure rates Temperature Transmitter STT650 with 4-20 mA Output

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		0
Fail Dangerous Detected		215
Fail Detected (detected by internal diagnostics)	148	
Fail High (detected by logic solver)	16	
Fail Low (detected by logic solver)	51	
Fail Dangerous Undetected		91
No Effect		149
Annunciation Undetected		2

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 random events, such as unexpected use, see section 4.2.2.

Table 2 lists the failure rates for the Temperature Transmitter STT650 with 4-20 mA Output according to IEC 61508, ed2, 2010.

A user of the Temperature Transmitter STT650 with 4-20 mA Output can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Temperature Transmitter STT650 with 4-20 mA Output. From this, failure rates and example PFD_{avg} values may be calculated.

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

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

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

Roles of the parties involved:

Honeywell International Inc.	Supplier of the Temperature Transmitter STT650 with 4-20 mA Output
exida	Performed the hardware assessment

Honeywell International Inc. contracted *exida* in September 2014 with the hardware assessment of the above-mentioned device.

2.2 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, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd 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. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

[N7]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9
[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.3 *exida* tools used

[T1]	Tool Version 1.1.7	FMEDA Tool

2.4 Reference documents

2.4.1 Documentation provided for Honeywell International Inc.

[D1]	6337Auk.pdf	Datasheet "6337A - 2-WIRE TRANSMITTER WITH HART® PROTOCOL"; 6337AY101-UK (1207)
[D2]	6337Duk.pdf	Datasheet "6337D - 2-WIRE TRANSMITTER WITH HART® PROTOCOL"; 6337AY101-UK (1207)
[D3]	6337A2A_BOM.xls 6337A2B_BOM.xls	Parts list
[D4]	6335-1-01-PDF.pdf	6335-1-01 schematic of 16.11.07
[D5]	6337 FMEDA v.1.xls	FMEDA dated 22.02.12
[D6]	6337 FMEDA RTD V1.xls	FMEDA dated 10.07.14
[D7]	6337 FMEDA TC V1.xls	FMEDA dated 10.07.14

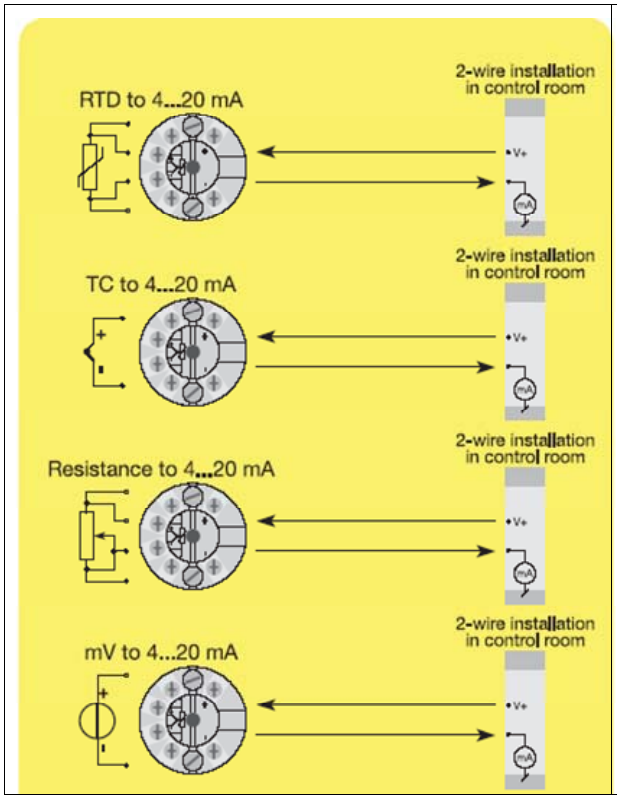
2.4.2 Documentation generated by *exida*

[R1]	PRetop 5337 FMEDA RTD V2 - exida.xls, Rev @	Failure Modes, Effects, and Diagnostic Analysis – Temperature Transmitter STT650 with 4-20 mA Output
[R2]	PRetop 5337 FMEDA TC V2 - exida.xls, Rev 1	Failure Modes, Effects, and Diagnostic Analysis – Temperature Transmitter STT650 with 4-20 mA Output
[R3]	PRetop 6337 FMEDA RTD V2 - exida.xls	Failure Modes, Effects, and Diagnostic Analysis -– Temperature Transmitter STT650 with 4-20 mA Output
[R4]	PRetop 6337 FMEDA TC V2 - exida.xls	Failure Modes, Effects, and Diagnostic Analysis -– Temperature Transmitter STT650 with 4-20 mA Output
[R5]	Calculations for FMEDA Report_30Nov2014.xls	Calculations for FMEDA Report

3 Product Description

The Temperature Transmitter STT650 with 4-20 mA Output is an isolated two-wire 4-20mA device used in many different industries for both control and safety applications. Combined with a temperature sensing device, the Temperature Transmitter STT650 with 4-20 mA Output becomes a temperature sensor assembly. It can be considered to be a Type B element with a hardware fault tolerance of 0.

The transmitter operates with a 2-wire system. The same wires are used for the operating voltage (depending on the transmitter) and the output signal (4-20 mA) including HART® protocol. This is also indicated in the following figure.



The temperature sensing devices that can be connected to the Temperature Transmitter STT650 with 4-20 mA Output are:

- 2-, 3- and 4-wire RTD
- Thermocouple
- 2-, 3- and 4-wire resistance
- mV input

Figure 1 Input configurations of Temperature Transmitter STT650 with 4-20 mA Output,

Table 3 gives an overview of the version that was considered in the FMEDA of the Temperature Transmitter STT650 with 4-20 mA Output.

Table 3 Version Overview

Option 1	Temperature transmitter, head or rail mounted – (Standard, ATEX, FM, CSA)

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.4.1 and is documented in section 2.4.2.

4.1 Failure categories description

In order to judge the failure behavior of the Temperature Transmitter STT650 with 4-20 mA Output, 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 2% 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 Dangerous	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 (< 3.6 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 2_H failure data is not available.

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

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

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which was derived using over 100 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 2, see Appendix C. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Honeywell International Inc.. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

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

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

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

The user of these numbers is responsible for determining their applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

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

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Temperature Transmitter STT650 with 4-20 mA Output.

- Only a single component failure will fail the entire Temperature Transmitter STT650 with 4-20 mA Output.
- 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 operational errors are site specific and therefore are not 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 HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- 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 5 minutes.
- Only the described HW and SW versions are used for safety applications.
- The device is operated in the low demand mode of operation.
- Only the 4..20mA current output is used for safety applications.
- The application program in the safety logic solver is configured to detect under-range and over-range failures of the 4..20 mA output signal, and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Temperature Transmitter STT650 with 4-20 mA Output FMEDA.

Table 4 Failure rates Temperature Transmitter STT650 with 4-20 mA Output

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		0
Fail Dangerous Detected		215
Fail Detected (detected by internal diagnostics)	148	
Fail High (detected by logic solver)	16	
Fail Low (detected by logic solver)	51	
Fail Dangerous Undetected		91
No Effect		149
Annunciation Undetected		2

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

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508 (See Section 5.3).

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.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore the Temperature Transmitter STT650 with 4-20 mA Output meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) as a single device when the listed failure rates are used.

5 Using the FMEDA Results

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

5.1 Temperature sensing devices

The Temperature Transmitter STT650 with 4-20 mA Output together with a temperature-sensing device becomes a temperature sensor assembly. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered. Typical failure rates for close-coupled thermocouples and RTDs are listed in Table 5.

Table 5 Typical failure rates close-coupled thermocouples and RTDs

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

5.1.1 Temperature Transmitter STT650 with 4-20 mA Output with thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 6 when close-coupled thermocouples are supplied with the Temperature Transmitter STT650 with 4-20 mA Output. The drift failure mode is primarily due to T/C aging. The Temperature Transmitter STT650 with 4-20 mA Output will detect a thermocouple burnout failure and drive the analog output to the specified failure state.

Table 6 Typical failure mode distributions for thermocouples

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

A complete temperature sensor assembly consisting of Temperature Transmitter STT650 with 4-20 mA Output and a closely coupled thermocouple supplied with the Temperature Transmitter STT650 with 4-20 mA Output 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 Temperature Transmitter STT650 with 4-20 mA Output is programmed to drive its output to the specified failure state on detected failures of the thermocouple, the failure rate contribution for the thermocouple in a low stress environment is:

λ_{SU}= (100) * (0.005) = 0.5 FIT

λ_{DD} = (100) * (0.95) = 95 FIT

λ_{DU} = (100) * (0.045) = 4.5 FIT

The total for the temperature sensor assembly with the Temperature Transmitter STT650 with 4-20 mA Output is:

λ_{SU} = 0.5 + 0 = 0.5 FIT

λ_{DD} = 95 + 215 = 310 FIT

λ_{DU} = 4.5 + 91 = 95.5 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions.

5.1.2 Temperature Transmitter STT650 with 4-20 mA Output with 4-wire 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. Typical failure rate distributions are shown in Table 7. The Temperature Transmitter STT650 with 4-20 mA Output will detect open circuit and short circuit RTD failures and drive its output to the alarm state on detected failures of the RTD.

Table 7 Failure mode distribution for 4-wire RTD, low stress environment

RTD Failure Modes – Close-coupled device	Percentage
Open Circuit	83%
Short Circuit	5%
Drift (Temperature measurement in error) (50% Safe; 50% Dangerous)	12%

A complete temperature sensor assembly consisting of Temperature Transmitter STT650 with 4-20 mA Output and a closely coupled, cushioned 4-wire RTD supplied with the Temperature Transmitter STT650 with 4-20 mA Output 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 Temperature Transmitter STT650 with 4-20 mA Output is programmed to drive its output to the alarm state on detected failures of the RTD, the failure rate contribution for a close-coupled 4-wire RTD in a low stress environment is:

λ_{SU} = (50) * (0.06) = 3 FIT

λ_{DD} = (50) * (0.83 + 0.05) = 44 FIT

λ_{DU} = (50) * (0.06) = 3 FIT

The total for the temperature sensor assembly with the Temperature Transmitter STT650 with 4-20 mA Output is:

λ_{SU} = 3 + 0 = 3 FIT

λ_{DD} = 44 + 215 = 259 FIT

λ_{DU} = 3 + 91 = 94 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions.

5.2 PFD_{avg} calculation Temperature Transmitter STT650 with 4-20 mA Output

Using the failure rate data displayed in section 4.4, and the failure rate data for the associated devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

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

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

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

5.3 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2_H alternative to Route 1_H architectural constraints. The standard states:
"based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to

- the amount of field feedback; and
- the exercise of **expert judgment**; and when needed
- the undertake of specific tests,

in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508, ed2, 2010 does not give detailed criteria for Route 2_H, *exida* has established the following:
1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" vs. "systematic" are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.

6 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type B element	"Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

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

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

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

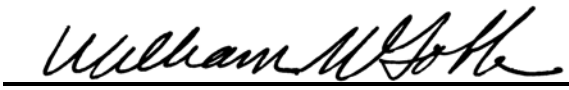
7.2 Releases

Version History:	V1, R1:	Released to Honeywell International Inc.; November 30, 2014
	V0, R1:	Draft; November 15, 2014
Author(s):	Loren Stewart	
Review:	V0, R1:	William Goble; November 15, 2014
Release Status:	Released to Honeywell International Inc.	

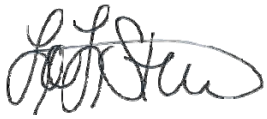
7.3 Future enhancements

At request of client.

7.4 Release signatures



Dr. William M. Goble, Principal Partner



Loren Stewart, Safety Engineer

Griff Francis, Senior Safety Engineer

Appendix A Lifetime of Critical Components

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[2] 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
Tantalum electrolytic (C40)	Approximately 500,000 hours (50 years)
Temperature sensor	According to manufacturer specification

It is the responsibility of the end user to maintain and operate the Temperature Transmitter STT650 with 4-20 mA Output per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

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

[2] 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 proof test described in Table 9 will detect 85% of possible DU failures in the Temperature Transmitter STT650 with 4-20 mA Output. The suggested transmitter proof test consists of a setting the output to the min and max, and a calibration check, see Table 9.

Table 9 Suggested Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate actions to avoid a false trip
2.	Perform a multi-point calibration of the temperature transmitter covering the applicable temperature range
3.	Apply an adequate input signal to reach the out of band high limit and the low limit. Verify that the diagnostic limit detection is successful in the logic solver.
4.	Restore the loop to full operation
5.	Remove the bypass from the safety PLC or otherwise restore normal operation

Appendix C *exida* Environmental Profiles

Table 10 *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[3]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[4]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[5]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[6]	G2	G3	G3	G3	G3	Compatible Material
Surge[7]						
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[8]						
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)[9]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[3] Humidity rating per IEC 60068-2-3
[4] Shock rating per IEC 60068-2-6
[5] Vibration rating per IEC 60770-1
[6] Chemical Corrosion rating per ISA 71.04
[7] Surge rating per IEC 61000-4-5
[8] EMI Susceptibility rating per IEC 6100-4-3
[9] ESD (Air) rating per IEC 61000-4-2

Appendix D Determining Safety Integrity Level

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

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

These are:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

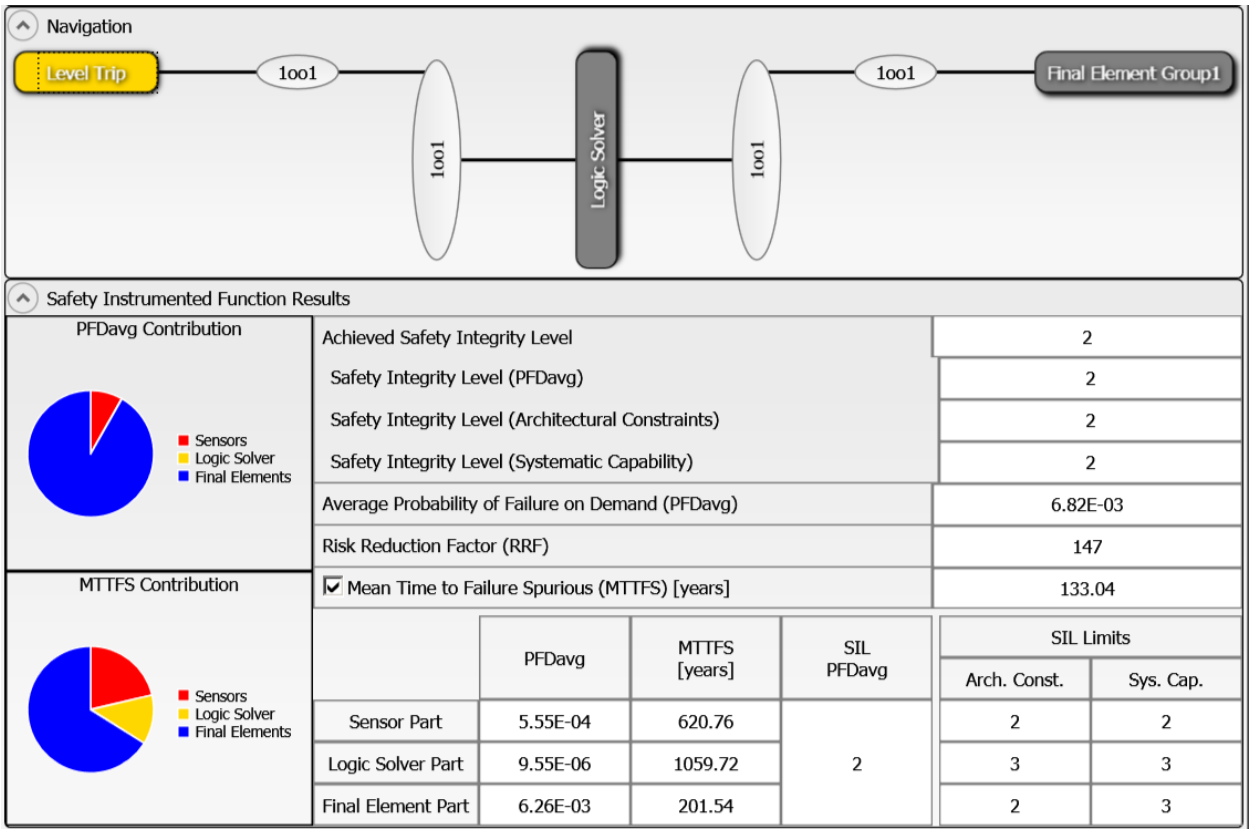


Figure 2: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 3.

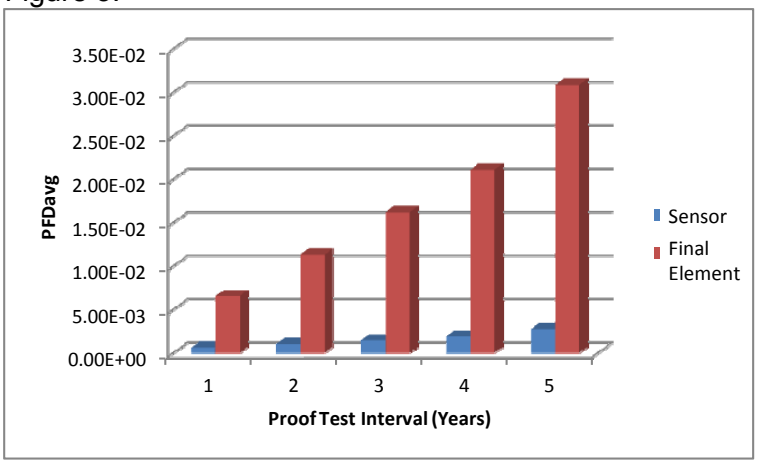
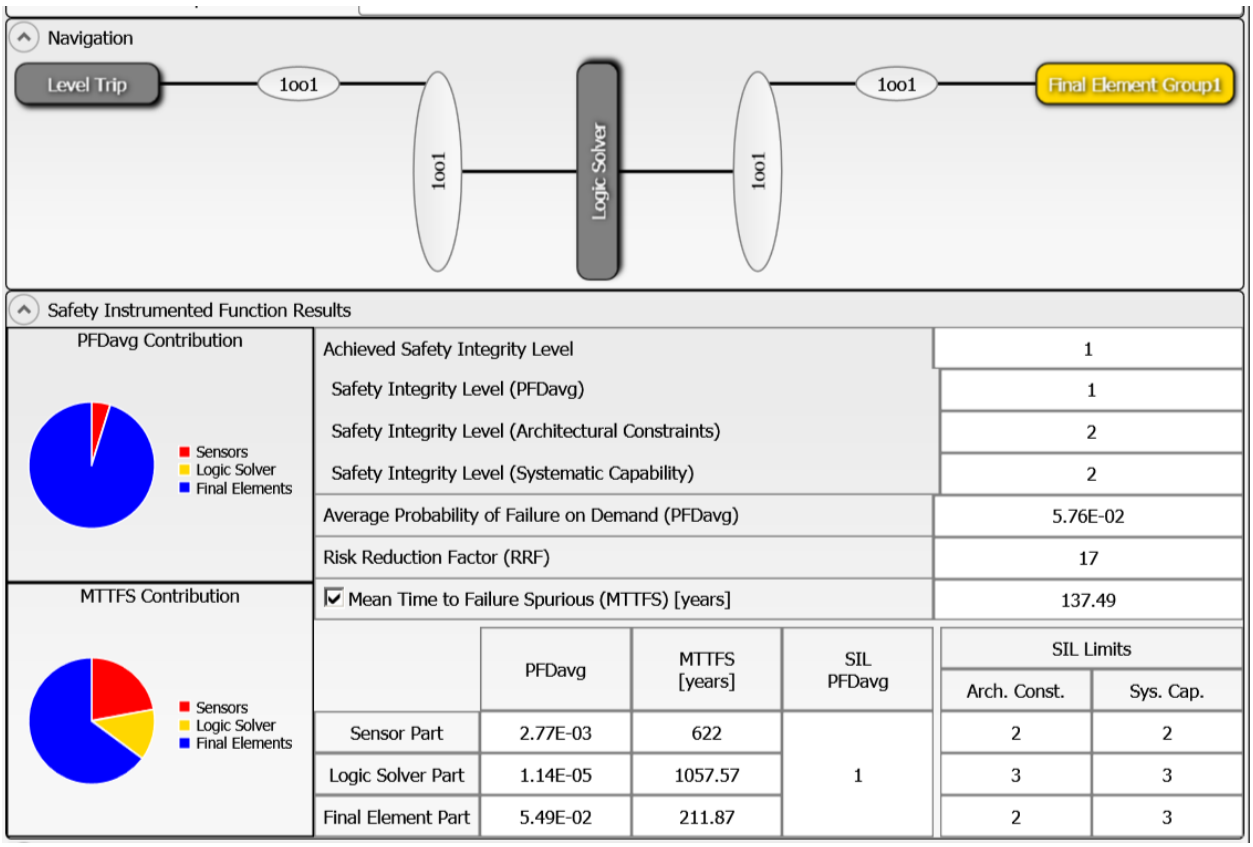


Figure 3 PFD_{avg} versus Proof Test Interval.

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

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

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 4).



Achieved Safety Integrity Level	1
Safety Integrity Level (PFDavg)	1
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	5.76E-02
Risk Reduction Factor (RRF)	17
☑ Mean Time to Failure Spurious (MTTFS) [years]	137.49

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	2.77E-03	622	1	2	2
Logic Solver Part	1.14E-05	1057.57		3	3
Final Element Part	5.49E-02	211.87		2	3

Figure 4: exSILentia results with realistic variables

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