Failure Modes, Effects and Diagnostic Analysis

Project:
Yokogawa YTA710 & YTA610 Temperature Transmitter

Company:
Yokogawa Electric Corporation
Musashino-shi, Tokyo
Japan

Contract Number: Q20/01-064
Report No.: YEC 15/10-041 R001
Version V4, Revision R7,May 19, 2022
Takao Kajitani

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 Yokogawa YTA710 & YTA610 Temperature Transmitter, hardware version S1 and software version R1.03.01 and R1.04.01. 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 YTA710 & YTA610 Temperature Transmitter. For full functional safety certification purposes, all requirements of IEC 61508 must be considered.

YTA710 & YTA610 Temperature Transmitter are two-wire smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4-20 mA output is used as the primary safety variable. The transmitter can communicate via HART (or Yokogawa proprietary BRAIN) communications that are superimposed on the current signal. These communications are not required for safety functionality and are considered interference free.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the YTA710 & YTA610 Temperature Transmitter.

Table 1 Version Overview

Option 1	YTA710 & YTA610 Temperature Transmitter, single TC configuration
Option 2	YTA710 & YTA610 Temperature Transmitter, single RTD configuration

The YTA710 & YTA610 Temperature 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 YTA710 & YTA610 Temperature Transmitter 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.

Based on the assumptions listed in 4.3, the failure rates for the YTA710 & YTA610 Temperature Transmitter are listed in section 4.4.

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

The failure rates listed in this report are based on over 350 billion unit operating hours of process industry field failure data. The failure rate predictions reflect realistic failures and include site specific failures due to human events for the specified Site Safety Index (SSI), see section 4.2.2.

A user of the YTA710 & YTA610 Temperature Transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

---

[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 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 YTA710 & YTA610 Temperature Transmitter. From this, failure rates for each failure mode/category, useful life, and proof test coverage are determined.

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.

A 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, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

Yokogawa Electric Corporation	Manufacturer of the YTA710 & YTA610 Temperature Transmitter
exida	Performed the hardware assessment

Yokogawa Electric Corporation contracted *exida* in January 2020 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, 4th Edition, 2017	*exida* LLC, Electrical Component Reliability Handbook, Fourth Edition, 2017
[N3]	Mechanical Component Reliability Handbook, 4th Edition, 2017	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2017
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. 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]	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
[N7]	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

[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N9]	Random versus Systematic – Issues and Solutions, September 2016	Goble, W.M., Bukowski, J.V., and Stewart, L.L., Random versus Systematic – Issues and Solutions, exida White Paper, PA: Sellersville, www.exida.com/resources/whitepapers, September 2016.
[N10]	Assessing Safety Culture via the Site Safety Index^{TM}, April 2016	Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index^{TM}, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston, April 2016.
[N11]	Quantifying the Impacts of Human Factors on Functional Safety, April 2016	Bukowski, J.V. and Stewart, L.L., Quantifying the Impacts of Human Factors on Functional Safety, Proceedings of the 12th Global Congress on Process Safety, AIChE 2016 Spring Meeting, NY: New York, April 2016.
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	Criteria for the Application of IEC 61508:2010 Route 2H, exida White Paper, PA: Sellersville, www.exida.com, December 2016.
[N13]	Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, November 1999	Goble, W.M. and Brombacher, A.C., Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999.
[N14]	FMEDA – Accurate Product Failure Metrics, June 2015	Grebe, J. and Goble W.M., FMEDA – Accurate Product Failure Metrics, www.exida.com, June 2015.

2.4 *exida* tools used

[T1]	V7.1.17	*exida* FMEDA Tool
[T2]	V4.3.0.4922	exSILentia

2.5 Reference documents

2.5.1 Documentation provided by Yokogawa Electric Corporation

[D1]	GS01C50G01-01EN.pdf 22nd Edition, Oct. 2019	YTA710 General Specifications
[D2]	GS01C50H01-01EN.pdf 16th Edition, Oct.2019	YTA610 General Specifications
[D3]	STR-CMNPF_TX-MB005 Rev5	YTA710 and YTA610 presentation with model selection guide, specifications, PCB interconnections, explanation of Function Blocks
[D4]	STR-CMNPF_TX-NB002 Rev0	YTA710 and YTA610 Architecture some sections translated, includes block diagram, data flow diagrams and diagnostic functions

[D5]	FD1-F9221GA Rev0	Schematic- Arrester Board
[D6]	FD1-F9221EA Rev0	Schematic- Filter Board
[D7]	FD1-F9221AA Rev0	Schematic- Indicator (HMI) Board
[D8]	FD1-F9221BA Rev1	Schematic- Main Board
[D9]	FD1-F9221DA Rev1	Schematic- Temperature Board
[D10]	FD1-F9221FA Rev0	Schematic- Terminal Board
[D11]	FE1-F9221GA Rev1	Bill of Materials- Arrestor Board
[D12]	FE1-F9221EA Rev1	Bill of Materials- Filter Board
[D13]	FE1-F9221AA Rev1	Bill of Materials- Indicator (HMI) Board
[D14]	FE1-F9221BA Rev1	Bill of Materials- Main Board
[D15]	FE1-F9221DA Rev1	Bill of Materials- Temperature Board
[D16]	FE1-F9221FA Rev1	Bill of Materials- Terminal Board
[D17]	STR-CMNPF_TX-MB005_YTA710_YTA610_共通部機能仕様書_5.pdf, 30 Sep 2016	Functional Specification, some sections translated, section 11 is Self-Diagnostics
[D18]	YTA710 Fault_Injection_Plan-Result_28Jan2016.xls	Fault Injection Test Result
[D19]	STR-CMNPF_TX-MB005_YTA710_YTA610_共通部機能仕様書_6.doc	YTA710 & YTA610 presentation with model selection guide, specifications, PCB interconnections, explanation of Function Blocks and Self Diagnostic
[D20]	STR-CMNPF_TX-OC006_YTA710_Main_Assy_ROMのCRCチェックに関する検証計画報告書.pdf	Fault Injection Plan-Result
[D21]	STR-CMNPF_TX-MB002_rev1	YTA710 & YTA610 Architecture some sections translated, includes block diagram, data flow diagrams and diagnostic functions
[D22]	FD1-F9221EAからの変更内容.pdf,	Modified Contents from FD1-F9221EA
[D23]	FD1-F9221ED_Rev0.pdf, 15 January 2020	Schematic- SMART FILTER ASSY
[D24]	FE1-F9221EA_Rev4.pdf, 15 Jan. 2020	Bill of Materials- Filter Board
[D25]	FE1-F9221ED_Rev0.pdf 15 Jan. 2020	Bill of Materials- Filter Board
[D26]	STR-CMNPF_TX-MB005_YTA710_YTA610_共通部機能仕様書_9.pdf, 2 April 2019	YTA710 & YTA610 Functional Specification
[D27]	FE1-F9221AA_Rev3	Bill of Materials- Indicator (HMI) Board
[D28]	FE1-F9221BA_Rev2	Bill of Materials- Main Board
[D29]	FE1-F9221DA_Rev2	Bill of Materials- Temperature Board

2.5.2 Documentation generated by *exida*

[R1]	YTA710_CPU&mA_15Nov2015.efm, V1R1, 15 Nov 2015	Failure Modes, Effects, and Diagnostic Analysis – YTA710 & YTA610 Temperature Transmitter, CPU, mA Output, Common Sensor and Indicator Circuitry
[R2]	YTA710_RTD_15Nov2015.efm, V1R1, 15 Nov 2015	Failure Modes, Effects, and Diagnostic Analysis – YTA710 & YTA610 Temperature Transmitter, 1 RTD channel
[R3]	YTA710_TC_CJC_15Nov2015.efm, V1R1, 15 Nov 2015	Failure Modes, Effects, and Diagnostic Analysis – YTA710 & YTA610 Temperature Transmitter, 1 thermocouple channel with cold junction compensation
[R4]	YTA710 Temp Xmtr FMEDA Summary RPC 2016-04-11.xlsx, 11 Apr 2016	Failure Modes, Effects, and Diagnostic Analysis - Summary –YTA710 & YTA610 Temperature Transmitter, Summary
[R5]	YTA710 Fault_Injection_Plan_28Jan2016.xls	Fault Injection Test Plan
[R6]	YEC 15-10-041 R001 V3R4 FMEDA YTA710.doc	FMEDA report for YTA710 Temperature Transmitter
[R7]	YEC 15-10-041 R001 V3R7 FMEDA YTA710.doc	FMEDA report for YTA710 Temperature Transmitter
[R8]	YEC 15-10-041 R002 V1R3 FMEDA YTA610.doc	FMEDA report for YTA610 Temperature Transmitter
[R9]	YEC 15-10-041 R002 V1R6 FMEDA YTA610.doc	FMEDA report for YTA610 Temperature Transmitter
[R10]	YEC 20-01-064 YTA710_610 Revised Design FMEDA V1R3.nefm.xlsx, February 26, 2021	Failure Modes, Effects, and Diagnostic Analysis for Revised Design – YTA710 & YTA610 Temperature Transmitter, 1 thermocouple channel with cold junction compensation and 1 RTD channel.
[R11]	YEC 15-10-041 R001 V4R7 FMEDA YTA710 and YTA610.docx May 19, 2022	FMEDA report for YTA710 & YTA610 Temperature Transmitter. (This Document)

3 Product Description

YTA710 & YTA610 Temperature Transmitter is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 - 20 mA output is used as the primary safety variable. The transmitter can communicate via HART (or Yokogawa proprietary BRAIN) communications that are superimposed on the current signal. These communications are not required for safety functionality and are considered interference free.

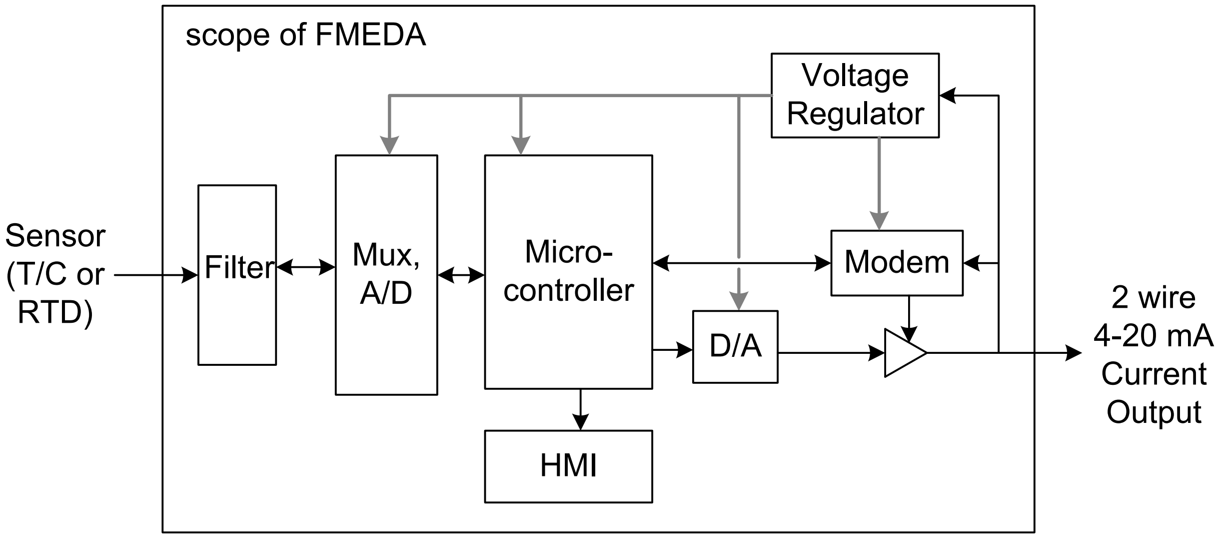


Figure 1 YTA710 & YTA610 Temperature Transmitter, Parts included in the FMEDA

Table 2 gives an overview of the different versions that were considered in the FMEDA of the YTA710 & YTA610 Temperature Transmitter.

Table 2 Version Overview

Option 1	YTA710 & YTA610 Temperature Transmitter, single TC configuration
Option 2	YTA710 & YTA610 Temperature Transmitter, single RTD configuration

The YTA710 & YTA610 Temperature Transmitter is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

---

[2] 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 was performed based on the documentation in section 2.5.1 and is documented in [R10] and [R11].

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. Refer to Fault Injection Test Result [D18].

4.1 Failure categories description

In order to judge the failure behavior of the YTA710 & YTA610 Temperature 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 10% of span, drifts toward the user defined threshold (Trip Point) and that leaves the output within the 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, user selectable, 3.6mA or 21.6mA.
Fail Dangerous	Failure that deviates the process signal or the actual output by more than 10% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within the 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 in order to provide a complete set of data needed for design optimization.

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.

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is a failure rate prediction technique based on a study of design strength versus operational profile stress. It combines design FMEA techniques with extensions 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 failure mode category [N13, N14].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N3] which were derived using over 350 billion unit operational hours of process industry field failure data from multiple sources and failure data formulas from international standards. The component failure rates are provided for each applicable operational profile and application, see Appendix C. The *exida* profile chosen for this FMEDA was < Profile 2> as this was judged to be the best fit for the product and application information submitted by Yokogawa Electric Corporation. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

The failure rates are predicted for a Site Safety Index of SSI=2 [N10, N11] as this level of operation is common in the process industries. Failure rate predictions for other SSI levels are included in the exSILentia® tool from exida.

The user of these numbers is responsible for determining the failure rate 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. exida has detailed models available to make customized failure rate predictions. Contact exida.

Accurate plant specific data may be used to check validity of this failure rate data. 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 YTA710 & YTA610 Temperature Transmitter.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire YTA710 & YTA610 Temperature Transmitter and propagation of failures is not relevant.
- Failure rates are constant for the useful life period.
- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.

- The stress levels are specified in the *exida* Profile used for the analysis are limited by the manufacturer's published ratings.
- Practical fault insertion tests have been used when applicable to demonstrate the correctness of the FMEDA results.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed and operated per manufacturer's instructions.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is <1 hour.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the YTA710 & YTA610 Temperature Transmitter FMEDA.

Table 3 and table 4 lists the failure rates for the YTA710 & YTA610 Temperature Transmitter with a Site Safety Index (SSI) of 2 (good site maintenance practices). See Appendix E for an explanation of SSI and the failure rates for SSI of 4 (ideal maintenance practices).

Table 3 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2, for single TC configuration

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		40
Fail Dangerous Detected		794
Fail Detected (detected by internal diagnostics)	671	
Fail High (detected by logic solver)	57	
Fail Low (detected by logic solver)	66	
Fail Dangerous Undetected		63
No Effect		268
Annunciation Undetected		30

Table 4 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2, for single RTD configuration

Failure Category	**Failure Rate (FIT)**	
Fail Safe Undetected		36
Fail Dangerous Detected		759
Fail Detected (detected by internal diagnostics)	636	
Fail High (detected by logic solver)	57	
Fail Low (detected by logic solver)	66	
Fail Dangerous Undetected		53
No Effect		263
Annunciation Undetected		30

Table 5 lists the failure rates for the YTA710 & YTA610 Temperature Transmitter according to IEC 61508.

Table 5 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2 according to IEC 61508

Device/Configuration	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	**#**	**SFF**
YTA710 & YTA610 Temperature Transmitter, single TC configuration	-	40	794	63	268	93.0%
YTA710 & YTA610 Temperature Transmitter, single RTD configuration	-	36	759	53	263	93.8%

Where:

λ_{SD} = Fail Safe Detected
λ_{SU} = Fail Safe Undetected
λ_{DD} = Fail Dangerous Detected
λ_{DU} = Fail Dangerous Undetected
\# = No Effect Failures

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

According to IEC 61508-2 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 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (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 61508-2.

---

[3] 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.

The analysis shows that the YTA710 & YTA610 Temperature Transmitter 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.

Table 15 lists the failure rates for the YTA710 & YTA610 Temperature Transmitter according to IEC 61508 with a Site Safety Index (SSI) of 4 (perfect site maintenance practices). This data should not be used for SIL verification and is provided only for comparison with other analysis than has assumed perfect maintenance. See Appendix E for an explanation of SSI.

5 Using the FMEDA Results

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

5.1 Temperature sensing devices

The YTA710 & YTA610 Temperature Transmitter together with a temperature-sensing device becomes a temperature sensor assembly. Therefore, when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered. Typical failure rates for close-coupled thermocouples and RTDs are listed in Table 6.

Table 6 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 YTA710 & YTA610 Temperature Transmitter with thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 7 when close-coupled thermocouples are supplied with the YTA710 & YTA610 Temperature Transmitter. The drift failure mode is primarily due to T/C aging. The YTA710 & YTA610 Temperature Transmitter will detect a thermocouple burnout failure and drive the analog output to the specified failure state.

Table 7 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 YTA710 & YTA610 Temperature Transmitter and a closely coupled thermocouple supplied with the YTA710 & YTA610 Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the YTA710 & YTA610 Temperature Transmitter 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:

$\lambda_{SU}= (100) * (0.005) = 0.5$ FIT

$\lambda_{DD} = (100) * (0.95) = 95$ FIT

$\lambda_{DU} = (100) * (0.045) = 4.5$ FIT

The total for the temperature sensor assembly with the YTA710 & YTA610 Temperature Transmitter is:

λ_{SU} = 0.5 + 40 = 40.5 FIT

λ_{DD} = 95 + 794 = 889 FIT

λ_{DU} = 4.5 + 63 = 67.5 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. For these circumstances, the Safe Failure Fraction of this temperature sensor assembly is 93.2%.

5.1.2 YTA710 & YTA610 Temperature Transmitter 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 8. The YTA710 & YTA610 Temperature Transmitter will detect open circuit and short circuit RTD failures and drive its output to the alarm state on detected failures of the RTD.

Table 8 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 YTA710 & YTA610 Temperature Transmitter and a closely coupled, cushioned 4-wire RTD supplied with the YTA710 & YTA610 Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Assuming that the YTA710 & YTA610 Temperature Transmitter 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 YTA710 & YTA610 Temperature Transmitter is:

λ_{SU} = 3 + 36 = 39 FIT

λ_{DD} = 44 +759 = 803 FIT

λ_{DU} = 3 + 53 = 56 FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. The Safe Failure Fraction for this temperature element, given the assumptions, is 93.8%.

5.2 PFD_{avg} calculation YTA710 & YTA610 Temperature Transmitter

Using the failure rate data displayed in section 4.4, and the failure rate data for the associated element 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. 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 are listed in Table 12.

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 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" [N9] 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. [N12}

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
BRAIN	Broadband Radio Access for IP-based Networks, Yokogawa's digital protocol superimposed on a 4-20 mA signal
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.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
FIT	Failure in Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
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).
RTD	Resistance Temperature Detectors
TC	Thermocouple temperature sensing device
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, product design changes, 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 model number product at some future time. As a leader in the functional safety marketplace, *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, contact the product vendor to verify the current validity of the results.

7.2 Version History

Version History:	V4, R7:	Kaoru Sonoda, Correct 4.1, May 19, 2022
	V4, R6:	Kaoru Sonoda, Correct 5.1.1 and 5.1.2, September 1, 2021
	V4, R5:	Takao Kajitani, Update failure rate summary, March 18, 2021
	V4, R4:	Takao Kajitani, correct proof test coverage, 27, February 2020
	V4, R3:	Takao Kajitani, updated after customer review, 25, February 2020
	V4, R2:	Takao Kajitani, updated after internal review, 10, February 2020
	V4, R1:	Takao Kajitani, FMEDA for revised design and integrate YTA710 and YTA610 FMEDA report, 10, February 2020
	V3, R7:	Kiyoshi Takai, [D21] description, February 21, 2017
	V3, R6:	Kiyoshi Takai, add [D21] by customer review, February 21, 2017
	V3, R5:	Kiyoshi Takai, Revised FMEDA Report, February 20, 2017 Revised documents to sections 2.4.2 [D19]-[D20], added documents: 2.4.3 [R7]
	V3, R4:	Correct Document List, 15, November 2016
	V3, R3:	Update Document List, 11, November 2016
	V3, R2:	Update Document List, 08, November 2016
	V3, R1:	Release to Customer Review, 29, October 2016
	V2, R7:	This document number is corrected: From Q15-12-066 to Q15-10-041, 30 August 2016
	V2, R6:	Final Update Fault Injection Test Plan, 23 May 2016
	V2, R5:	Update Fault Injection Test Plan, 29 January 2016
	V2, R4:	Update Fault Injection Test Plan, 25 December 2015
	V2, R3:	Update customer reviewed, 22 December 2015
	V2, R2:	Release to customer, 14 December 2015
	V2, R1:	Updated Design modified, 18 Nov 2015

V1, R1: Released to Yokogawa Electric Corporation; 29 June 2015
V0, R1: Draft; 18 May 2015
Author(s): Takao Kajitani, Takao Kajitani
Review: V4, R5 Kaoru Sonoda (*exida*), March 18, 2021
V4, R1: Kaoru Sonoda (*exida*); 10 February 2020
V3, R1: Kaoru Sonoda (*exida*); 29 October 2016
V2, R1: Rudy Chalupa (*exida*); 9 December 2015
V0, R1: Rudy Chalupa (*exida*); 19 May 2015
Release Status: Released to Yokogawa Electric Corporation

7.3 Future enhancements

At request of client.

7.4 Release signatures

Rudolf P. Chalupa

Rudolf P. Chalupa, Senior Safety Engineer

Kiyoshi Takai

Kiyoshi Takai, Safety Engineer

Takao Kajitani

Takao Kajitani, Safety Engineer

Kaoru Sonoda, Certifying Assessor

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 determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the exida FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime[4] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

Table 9 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 9 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 YTA710 & YTA610 Temperature Transmitter per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

The limiting factors with regard to the useful lifetime of the system are the tantalum electrolytic capacitors. Therefore, the useful is predicted 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.

---

[4] 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 Abbreviated Proof Test

The suggested abbreviated proof test for the YTA710 & YTA610 Temperature Transmitter is described in Table 10. Refer to the table in B.3 for the Proof Test Coverages.

Table 10 Suggested Abbreviated Proof Test – YTA710 & YTA610 Temperature Transmitter

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Use HART or BRAIN communications to retrieve any diagnostics and take appropriate action.
3.	Send a HART or BRAIN command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value[5].
4.	Send a HART or BRAIN command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value[6].
5.	Remove the bypass and otherwise restore normal operation.

---

[5] This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.

[6] This tests for possible quiescent current related failures.

B.2 Suggested Extended Proof Test

The suggested extended proof test for the YTA710 & YTA610 Temperature Transmitter consists of a setting the output to the min and max, and a calibration check, see .

Table 11 Suggested Extended Proof Test – YTA710 & YTA610 Temperature Transmitter

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.	Send a HART command to the transmitter 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 to go to the low alarm current output and verify that the analog current reaches that value[8].
5.	Inspect the transmitter for any leaks, visible damage or contamination.
6.	Perform a two-point calibration[9] of the transmitter over the full working range.
7.	Remove the bypass and otherwise restore normal operation.

B.3 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 12.

Table 12 Proof Test Coverage – YTA710 & YTA610 Temperature Transmitter

Device	Application	Abbreviated Proof Test	Extended Proof Test
YTA710 & YTA610 Temperature Transmitter	single TC configuration	65.1%	84.1%
	single RTD configuration	67.9%	84.9%

---

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

[8] This tests for possible quiescent current related failures.

[9] 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 13 *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[10]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[11]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[12]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[13]	G2	G3	G3	G3	G3	Compatible Material
Surge[14]						
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[15]						
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)[16]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

---

[10] Humidity rating per IEC 60068-2-3

[11] Shock rating per IEC 60068-2-27

[12] Vibration rating per IEC 60068-2-6

[13] Chemical Corrosion rating per ISA 71.04

[14] Surge rating per IEC 61000-4-5

[15] EMI Susceptibility rating per IEC 61000-4-3

[16] 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) [N4] and [N7].

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 [N8].

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 350 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^{TM} software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

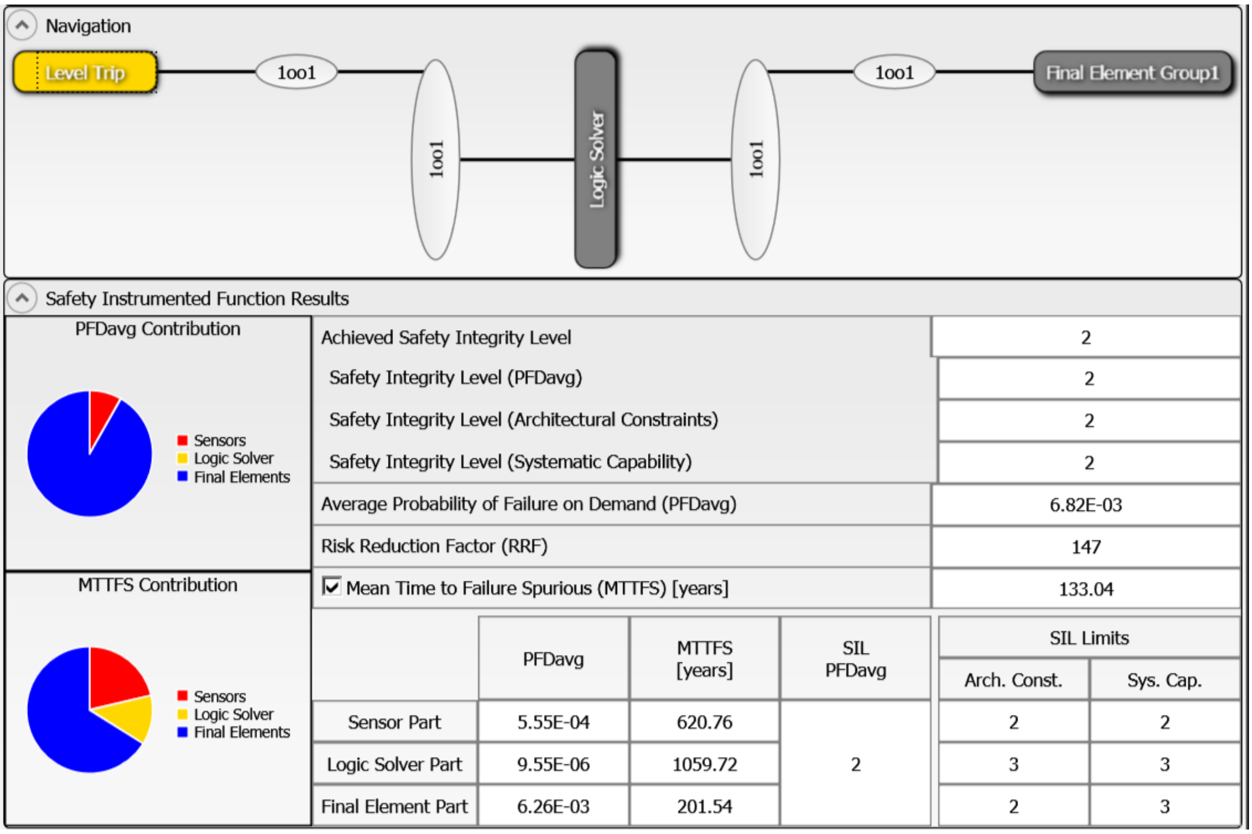
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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.



Achieved Safety Integrity Level	2
Safety Integrity Level (PFDavg)	2
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	6.82E-03
Risk Reduction Factor (RRF)	147
☑ Mean Time to Failure Spurious (MTTFS) [years]	133.04

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	5.55E-04	620.76	2	2	2
Logic Solver Part	9.55E-06	1059.72		3	3
Final Element Part	6.26E-03	201.54		2	3

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.

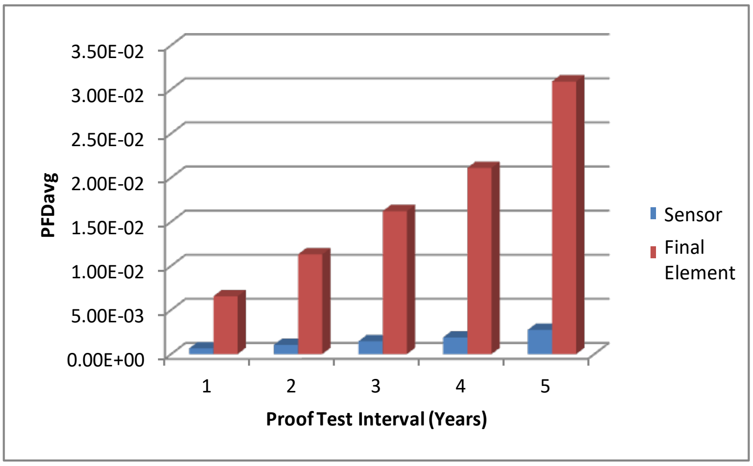
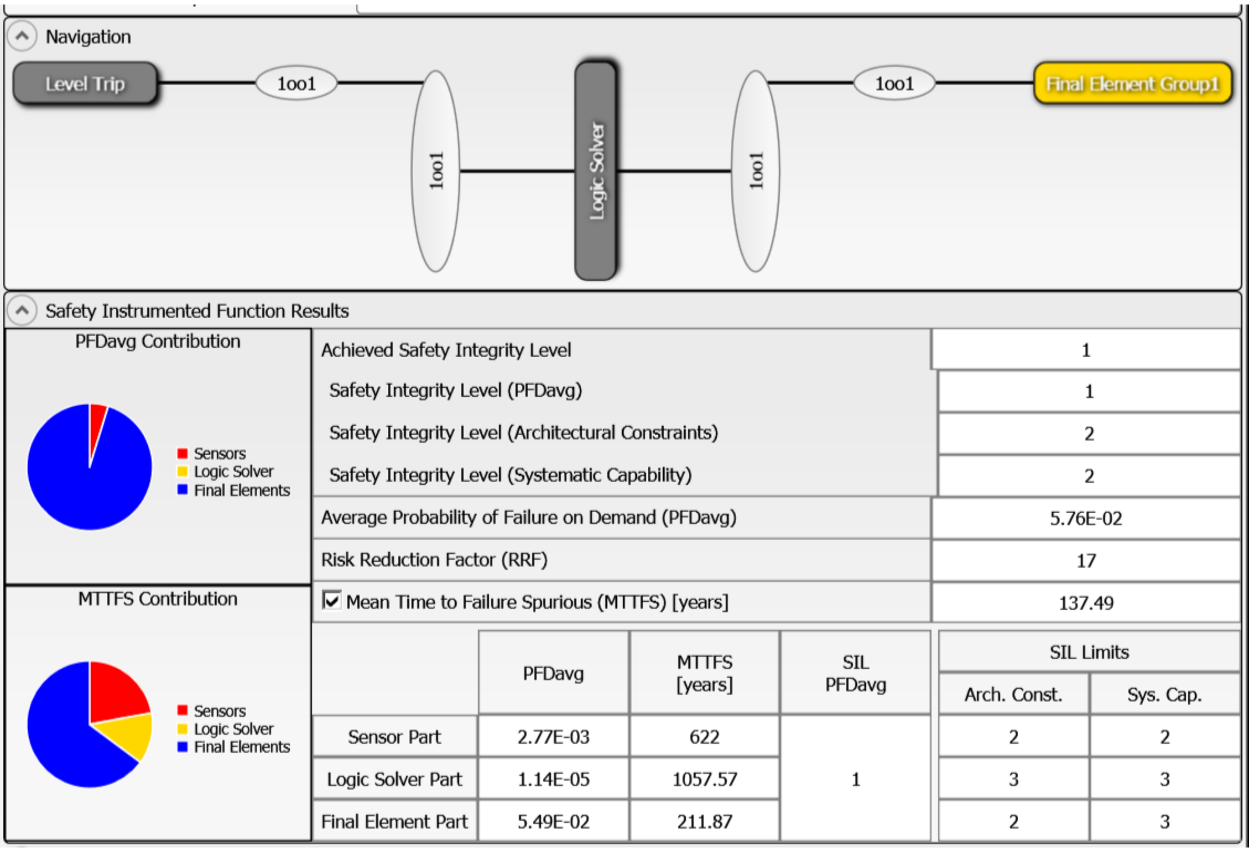


Figure 3 PFD$_{avg}$ versus Proof Test Interval.

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.

Appendix E Site Safety Index

Numerous field failure studies have shown that the failure rate for a specific device (same Manufacturer and Model number) will vary from site to site. The Site Safety Index (SSI) was created to account for these failure rates differences as well as other variables. The information in this appendix is intended to provide an overview of the Site Safety Index (SSI) model used by *exida* to compensate for site variables including device failure rates.

E.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 14 details the interpretation of each SSI level. Note that the levels mirror the levels of SIL assignment and that SSI 4 implies that all requirements of IEC 61508 and IEC 61511 are met at the site and therefore there is no degradation in safety performance due to any end-user activities or practices, i.e., that the product inherent safety performance is achieved.

Several factors have been identified thus far which impact the Site Safety Index (SSI). These include the quality of:

Commission Test
Safety Validation Test
Proof Test Procedures
Proof Test Documentation
Failure Diagnostic and Repair Procedures
Device Useful Life Tracking and Replacement Process
SIS Modification Procedures
SIS Decommissioning Procedures
and others

Table 14 *exida* Site Safety Index Profiles

Level	Description
SSI 4	Perfect - Repairs are always correctly performed, Testing is always done correctly and on schedule, equipment is always replaced before end of useful life, equipment is always selected according to the specified environmental limits and process compatible materials. Electrical power supplies are clean of transients and isolated, pneumatic supplies and hydraulic fluids are always kept clean, etc. Note: This level is generally considered not possible but retained in the model for comparison purposes.
SSI 3	Almost perfect - Repairs are correctly performed, Testing is done correctly and on schedule, equipment is normally selected based on the specified environmental limits and a good analysis of the process chemistry and compatible materials. Electrical power supplies are normally clean of transients and isolated, pneumatic supplies and hydraulic fluids are mostly kept clean, etc. Equipment is replaced before end of useful life, etc.
SSI 2	Good - Repairs are usually correctly performed, Testing is done correctly and mostly on schedule, most equipment is replaced before end of useful life, etc.
SSI 1	Medium – Many repairs are correctly performed, Testing is done and mostly on schedule, some equipment is replaced before end of useful life, etc.
SSI 0	None - Repairs are not always done, Testing is not done, equipment is not replaced until failure, etc.

E.2 Site Safety Index Failure Rates – YTA710 & YTA610 Temperature Transmitter

Failure rates of each individual device in the SIF are increased or decreased by a specific multiplier which is determined by the SSI value and the device itself. It is known that final elements are more likely to be negatively impacted by less than ideal end-user practices than are sensors or logic solvers. By increasing or decreasing device failure rates on an individual device basis, it is possible to more accurately account for the effects of site practices on safety performance.

Table 15 lists the failure rates for the YTA710 & YTA610 Temperature Transmitter according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 15 Failure rates with Ideal Maintenance Assumption in FIT (SSI=4)

Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	SFF
YTA710 & YTA610 Temperature Transmitter, single TC configuration	-	36	715	57	242	92.9%
YTA710 & YTA610 Temperature Transmitter, single RTD configuration	-	33	684	48	237	93.7%