Failure Modes, Effects and Diagnostic Analysis

Project:
Series 12 Switch

Company:
United Electric Controls
Watertown, MA
USA

Contract Number: Q20/06-041
Report No.: UEC 20/06-041 R001
Version V1, Revision R1, November 20, 2020
Brad Hitchcock

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 Series 12 Switch. 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 Series 12 Switch. For full functional safety certification purposes, all requirements of IEC 61508 must be considered.

At the heart of the 12 Series is a Belleville spring assembly. The spring is a small conical washer that transfers motion to a hermetically sealed 1 or 5 amp microswitch. Its 'snap-action' provides fast, positive contact transfer. The Belleville spring 'snaps over' when pressure is applied and 'snaps back' upon pressure release.

The 12 series models include a pressure switch, differential pressure switch, local access temperature switch, and remote access temperature switch. Specifications for these switches are shown on Table 2.

There are single switch and dual switch configurations. The dual switch configurations can be wired in series or in parallel. When wired in series the safety function architecture is 2oo2. When wired in parallel the safety function architecture is 1oo2.

The safety function of the Series 12 Switch is to send a signal when a designated pressure or temperature set point is reached. This set point can be either a low trip or high trip application.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Series 12 Switch.

Table 1 Version Overview

Pressure Model	Sensor Type: 2-9; P0-P4; P6-P9; W1-W4 Pressure: 3 to 12,500 psi
Differential Pressure Model	Sensor Type: K1-5 Pressure: 0.3 to 15 psi
Temperature Model – Local Access	Sensor Type: L1-L2 Includes Bellows Assembly Temperature: 0 to 425°F
Temperature Model – Remote Access	Sensor Type: R1-R4 Includes Thermal Assembly Temperature: -130 to 650°F

The Series 12 Switch is classified as a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H (see Section 5.2). Therefore, the Series 12 Switch meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

[1] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

Based on the assumptions listed in 4.3, the failure rates for the Series 12 Switch 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 Series 12 Switch 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).

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 Series 12 Switch. 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

United Electric Controls	Manufacturer of the Series 12 Switch
exida	Performed the hardware assessment

United Electric Controls contracted *exida* in September 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™, April 2016	Bukowski, J.V. and Chastain-Knight, D., Assessing Safety Culture via the Site Safety Index™, 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 Reference documents

2.4.1 Documentation provided by United Electric Controls

[D1]	12-B-10	Product Catalog
[D2]	M-13972, Rev F, 17-Jun-10	12 Series Models P6 to P9 Drawings
[D3]	DIFF PRESSURE BOM, 10-Nov-20	Bill of Materials - Differential Pressure Model
[D4]	M-13966, 17-Jun-10	12 Series Diff. Press. K1-K3 Drawing
[D5]	6291-325, Rev B, 01-May-15	Diff'l Diaphragm Ass'y (3.5 Piston) Drawing
[D6]	M-13965, Rev F, 17-Jun-10	12 Series Remote Temperature Drawing
[D7]	REMOTE TEMPERATURE BOM, 10-Nov-20	Bill of Materials - Temp Model Remote Access
[D8]	A-6291-301, Rev F, 08-Apr-11	Diaphragm Assy - Temp Model
[D9]	M-13982, Rev C, 19-Feb-13	12 Series Local Mount Temperature Drawing
[D10]	LOCAL TEMP MOUNT BOM, 10-Nov-20	Bill of Materials - Temp Model Local Access
[D11]	A-6259-803, Rev F, 30-Oct-15	Dual Switch Drawing

2.4.2 Documentation generated by *exida*

[R1]	Pressure Model FMEDA.xls, Rev 1, 16-Nov-20	Failure Modes, Effects, and Diagnostic Analysis – Series 12 Switch, Pressure
[R2]	Differential Pressure Model FMEDA.xls, Rev 1, 16-Nov-20	Failure Modes, Effects, and Diagnostic Analysis – Series 12 Switch, Differential
[R3]	Local Access Temperature Model FMEDA.xls, Rev 1, 16-Nov-20	Failure Modes, Effects, and Diagnostic Analysis – Series 12 Switch, Temperature, Local
[R4]	Remote Access Temperature Model FMEDA.xls, Rev 1, 16-Nov-20	Failure Modes, Effects, and Diagnostic Analysis – Series 12 Switch, Temperature, Remote
[R5]	FMEDA_Summary.xls, Rev 1, 17-Nov-20	Failure Modes, Effects, and Diagnostic Analysis - Summary –Series 12 Switch
[R6]	UEC 20-06-041 R001 V1R1 12 Series FMEDA Report	FMEDA Report - Series 12 Switch (This document)

3 Product Description

At the heart of the 12 Series is a Belleville spring assembly. The spring is a small conical washer that transfers motion to a hermetically sealed 1 or 5 amp microswitch. Its 'snap-action' provides fast, positive contact transfer. The Belleville spring 'snaps over' when pressure is applied and 'snaps back' upon pressure release.

The 12 series models include a pressure switch, differential pressure switch, local access temperature switch, and remote access temperature switch. Specifications for these switches are shown on Table 2.

There are single switch and dual switch configurations. The dual switch configurations can be wired in series or in parallel. When wired in series the safety function architecture is 2oo2. When wired in parallel the safety function architecture is 1oo2.

The safety function of the Series 12 Switch is to send a signal when a designated pressure or temperature set point is reached. This set point can be either a low trip or high trip application.

Figure 1 Series 12 Switch, Parts included in the FMEDA

Table 2 gives an overview of the different versions that were considered in the FMEDA of the Series 12 Switch.

Table 2 Version Overview

Pressure Model	Sensor Type: 2-9; P0-P4; P6-P9; W1-W4 Pressure: 3 to 12,500 psi
Differential Pressure Model	Sensor Type: K1-5 Pressure: 0.3 to 15 psi
Temperature Model – Local Access	Sensor Type: L1-L2 Includes Bellows Assembly Temperature: 0 to 425°F
Temperature Model – Remote Access	Sensor Type: R1-R4 Includes Thermal Assembly Temperature: -130 to 650°F

The Series 12 Switch is classified as a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

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 [R1] to [R6][R5].

4.1 Failure categories description

In order to judge the failure behavior of the Series 12 Switch, the following definitions for the failure of the device were considered.

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

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 static 3 as this was judged to be the best fit for the product and application information submitted by United Electric Controls. It is expected that the actual number of field failures 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 Series 12 Switch.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Series 12 Switch 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.
- Materials are compatible with process conditions.
- The device is installed and operated per manufacturer's instructions.
- External power supply failure rates are not included.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the Series 12 Switch FMEDA.

Table 3 and Table 4 lists the failure rates for the Series 12 Switch 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 for Static Applications[2] with Good Maintenance Assumptions in FIT @ SSI=2

Model – Switch Type	Trip	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	#
Pressure -Single Switch	High	0	45	0	141	193
	Low	0	67	0	119	194
Pressure - Dual Switch, Series	High	0	29	0	199	197
	Low	0	53	0	175	197
Pressure - Dual Switch, Parallel	High	0	64	0	88	197
	Low	0	83	0	69	197
Differential Pressure – Single Switch	High	0	169	0	300	427
	Low	0	227	0	245	427
Differential Pressure – Dual Switch, Series	High	0	152	0	359	430
	Low	0	212	0	302	430
Differential Pressure – Dual Switch, Parallel	High	0	187	0	248	430
	Low	0	243	0	195	430
Temp, Local Access – Single Switch	High	0	34	0	270	42
	Low	0	79	0	215	42
Temp, Local Access– Dual Switch, Series	High	0	17	0	329	45
	Low	0	64	0	272	45
Temp, Local Access – Dual Switch, Parallel	High	0	52	0	218	45
	Low	0	95	0	165	45
Temp, Remote Access– Single Switch	High	0	21	0	178	62
	Low	0	99	0	99	58
Temp, Remote Access– Dual Switch, Series	High	0	4	0	236	65
	Low	0	84	0	155	61
Temp, Remote Access– Dual Switch, Parallel	High	0	39	0	125	65
	Low	0	115	0	49	61

[2] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[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.

Table 4 Failure rates for Dynamic Applications[4] with Good Maintenance Assumptions in FIT @ SSI=2

Model – Switch Type	Trip	λ_{SD}	λ_{SU}[5]	λ_{DD}	λ_{DU}	#
Pressure -Single Switch	High	0	46	0	123	209
	Low	0	70	0	99	209
Pressure - Dual Switch, Series	High	0	29	0	182	212
	Low	0	55	0	156	212
Pressure - Dual Switch, Parallel	High	0	64	0	71	212
	Low	0	86	0	49	212
Differential Pressure – Single Switch	High	0	174	0	302	427
	Low	0	240	0	235	427
Differential Pressure – Dual Switch, Series	High	0	158	0	360	430
	Low	0	226	0	292	430
Differential Pressure – Dual Switch, Parallel	High	0	192	0	249	430
	Low	0	256	0	185	430
Temp, Local Access – Single Switch	High	0	34	0	261	49
	Low	0	80	0	215	49
Temp, Local Access– Dual Switch, Series	High	0	17	0	320	53
	Low	0	65	0	271	53
Temp, Local Access – Dual Switch, Parallel	High	0	52	0	209	53
	Low	0	96	0	165	53
Temp, Remote Access– Single Switch	High	0	21	0	168	70
	Low	0	105	0	85	70
Temp, Remote Access– Dual Switch, Series	High	0	4	0	227	73
	Low	0	90	0	141	73
Temp, Remote Access– Dual Switch, Parallel	High	0	39	0	116	73
	Low	0	121	0	35	73

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.

[4] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.

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

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 5.2).

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.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H which is more stringent than IEC 61508-2. Therefore, the Series 12 Switch meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates are used.

The architectural constraint type for the Series 12 Switch is A. The hardware fault tolerance of the device is 0. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

Table 10 and Table 11 lists the failure rates for the Series 12 Switch 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 PFD_{avg} calculation Series 12 Switch

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 6.

5.2 *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.
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
PVST	Partial Valve Stroke Test - It is assumed that Partial Valve Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequently than the proof test; therefore, the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption, the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Severe Service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

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

Due to future potential changes in the standards, 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 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, contact the product vendor to verify the current validity of the results.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q20/06-041	UEC 20/06-041 R001 V1, R1	Initial Release

Reviewer: Steve Close, exida, 20-Nov-20

Status: Released, 20-Nov-20

7.3 Future enhancements

At request of client.

7.4 Release signatures

Brad Hitchcock, Safety Engineer, CFSP

Steven Close, 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 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[6] 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.

It is the responsibility of the end user to maintain and operate the Series 12 Switch per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

Based on general field failure data a useful life period of approximately 10 years is expected for the Series 12 Switch.

For high demand mode applications, the useful lifetime of the switch / mechanical parts is limited by the number of cycles. The useful lifetime of the switch / mechanical parts is > 100,000 full scale cycles 10 years, whichever results in the shortest lifetime.

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

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

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 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 for the Series 12 Switch is described in Table 5. Refer to the table in B.2 for the Proof Test Coverages

Table 5 Suggested Proof Test – Series 12 Switch

Step	Action
1.	Take appropriate action to avoid a false trip.
2.	Inspect the device for any visible damage, corrosion or contamination.
3.	Increase the pressure/temperature to reach the increasing set point value and verify that the electric signal proceeds into the safe state.
4.	Lower the pressure/temperature to reach the decreasing set point value and verify that the electric signal returns to the normal state.
5.	Repeat steps 3 and 4 twice or more to evaluate the average set point value and repeatability.
6.	Restore the connection to full operation.
7.	Restore normal operation.

B.2 Proof Test Coverage

The Proof Test Coverage for the various product configurations is given in Table 6.

Table 6 Proof Test Coverage – Static Applications Series 12 Switch

Device		$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
Pressure -Single Switch	High Trip	8.8	94%
	Low Trip	6.4	95%
Pressure - Dual Switch, Series	High Trip	9.4	95%
	Low Trip	7.0	96%
Pressure - Dual Switch, Parallel	High Trip	8.3	91%
	Low Trip	5.9	91%
Differential Pressure – Single Switch	High Trip	25	92%
	Low Trip	19	92%
Differential Pressure – Dual Switch, Series	High Trip	25	93%
	Low Trip	20	93%
Differential Pressure – Dual Switch, Parallel	High Trip	24	90%
	Low Trip	19	90%
Temp, Local Access – Single Switch	High Trip	22	92%
	Low Trip	16	93%
Temp, Local Access– Dual Switch, Series	High Trip	22	93%
	Low Trip	17	94%
Temp, Local Access – Dual Switch, Parallel	High Trip	21	90%
	Low Trip	16	90%
Temp, Remote Access– Single Switch	High Trip	13	93%
	Low Trip	4.4	96%
Temp, Remote Access– Dual Switch, Series	High Trip	13	94%
	Low Trip	5.0	97%
Temp, Remote Access– Dual Switch, Parallel	High Trip	12	90%
	Low Trip	3.9	92%

Table 7 Proof Test Coverage – Dynamic Applications Series 12 Switch

Device		$\lambda_{DU}PT$ (FIT)	Proof Test Coverage
Pressure -Single Switch	High Trip	7.1	94%
	Low Trip	4.5	95%
Pressure - Dual Switch, Series	High Trip	7.7	96%
	Low Trip	5.0	97%
Pressure - Dual Switch, Parallel	High Trip	6.6	91%
	Low Trip	4.0	92%
Differential Pressure – Single Switch	High Trip	25	92%
	Low Trip	18	92%
Differential Pressure – Dual Switch, Series	High Trip	26	93%
	Low Trip	19	93%
Differential Pressure – Dual Switch, Parallel	High Trip	24	90%
	Low Trip	18	90%
Temp, Local Access – Single Switch	High Trip	21	92%
	Low Trip	16	93%
Temp, Local Access– Dual Switch, Series	High Trip	21	93%
	Low Trip	17	94%
Temp, Local Access – Dual Switch, Parallel	High Trip	20	90%
	Low Trip	16	90%
Temp, Remote Access– Single Switch	High Trip	12	93%
	Low Trip	3.0	96%
Temp, Remote Access– Dual Switch, Series	High Trip	12	95%
	Low Trip	3.6	97%
Temp, Remote Access– Dual Switch, Parallel	High Trip	11	91%
	Low Trip	2.5	93%

Appendix C *exida* Environmental Profiles

Table 8 *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[7]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[8]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[9]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[10]	G2	G3	G3	G3	G3	Compatible Material
Surge[11]						
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[12]						
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)[13]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[7] Humidity rating per IEC 60068-2-3
[8] Shock rating per IEC 60068-2-27
[9] Vibration rating per IEC 60068-2-6
[10] Chemical Corrosion rating per ISA 71.04
[11] Surge rating per IEC 61000-4-5
[12] EMI Susceptibility rating per IEC 61000-4-3
[13] 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™ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

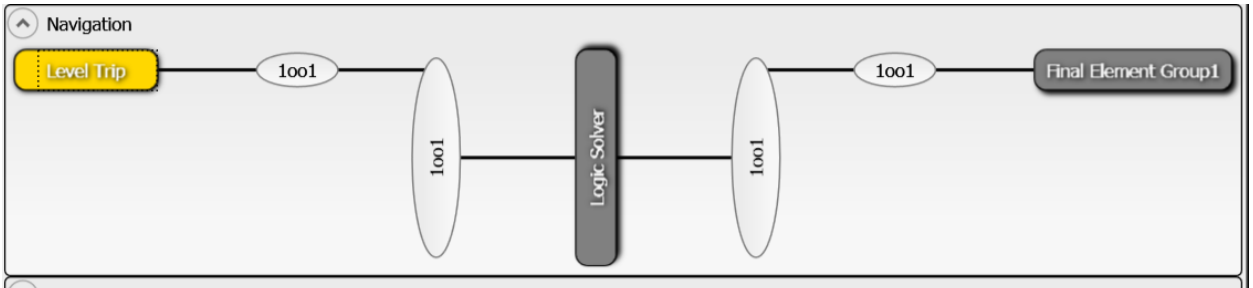
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic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

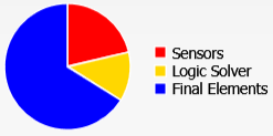
This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03. See Figure 2.



Safety Instrumented Function Results

PFDavg Contribution

MTTFS Contribution



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.

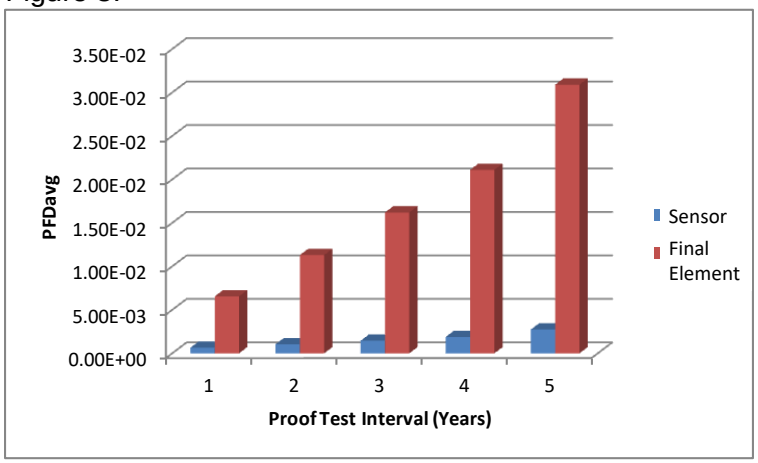


Figure 3 PFD_{avg} versus Proof Test Interval.

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).

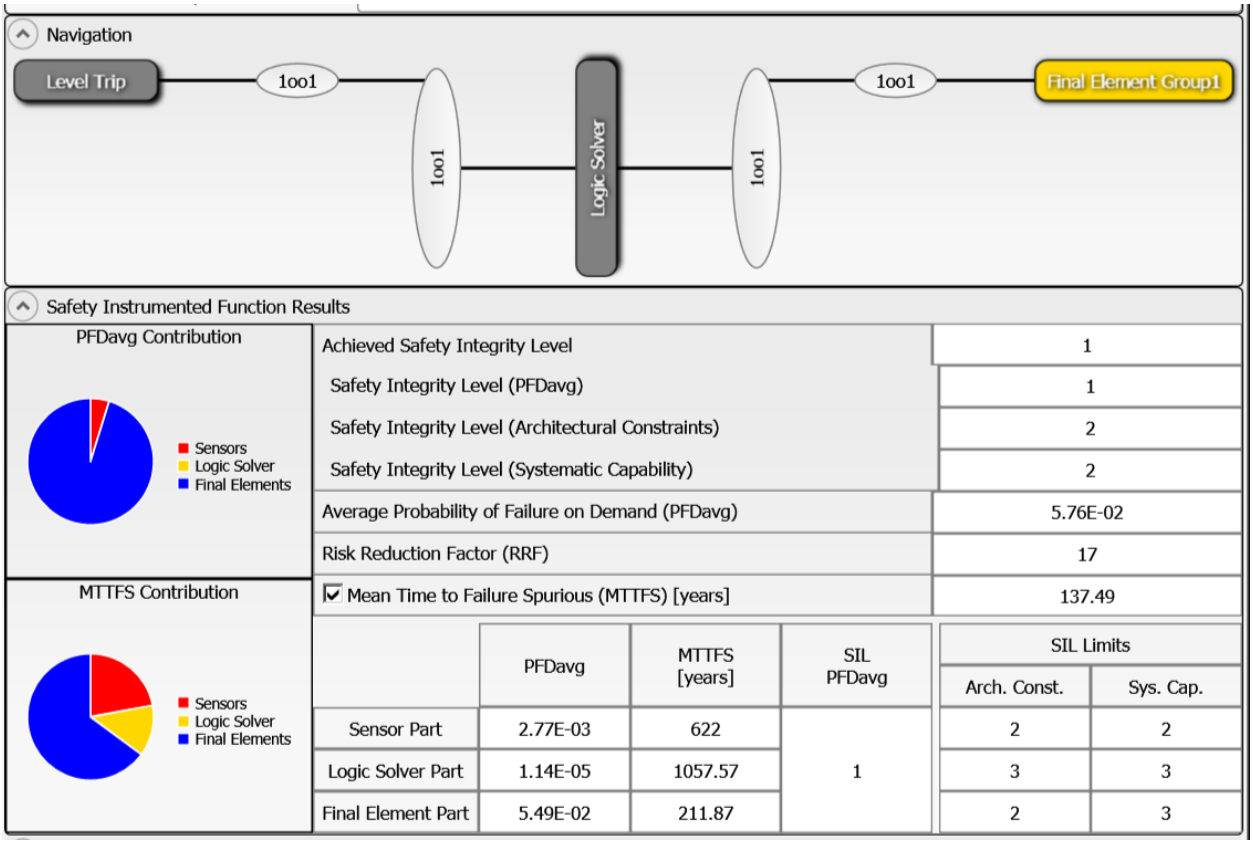


Figure 4: exSILentia results with realistic variables

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 9 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 9 *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 – Series 12 Switch

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 10 and Table 11 lists the failure rates for the Series 12 Switch according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 10 Failure rates for Static Applications with Ideal Maintenance Assumption in FIT (SSI=4)

Model – Switch Type	Trip	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#
Pressure -Single Switch	High	0	27	0	70	116
	Low	0	40	0	60	116
Pressure - Dual Switch, Series	High	0	17	0	99	118
	Low	0	32	0	88	118
Pressure - Dual Switch, Parallel	High	0	38	0	44	118
	Low	0	50	0	34	118
Differential Pressure – Single Switch	High	0	101	0	150	256
	Low	0	136	0	123	256
Differential Pressure – Dual Switch, Series	High	0	91	0	179	258
	Low	0	127	0	151	258
Differential Pressure – Dual Switch, Parallel	High	0	112	0	124	258
	Low	0	146	0	98	258
Temp, Local Access – Single Switch	High	0	20	0	135	25
	Low	0	47	0	108	25
Temp, Local Access– Dual Switch, Series	High	0	10	0	164	27
	Low	0	39	0	136	27
Temp, Local Access – Dual Switch, Parallel	High	0	31	0	109	27
	Low	0	57	0	83	27
Temp, Remote Access– Single Switch	High	0	13	0	89	37
	Low	0	59	0	49	35
Temp, Remote Access– Dual Switch, Series	High	0	3	0	118	39
	Low	0	51	0	77	36
Temp, Remote Access– Dual Switch, Parallel	High	0	24	0	63	39
	Low	0	69	0	24	36

Table 11 Failure rates for Dynamic Applications with Ideal Maintenance Assumption in FIT (SSI=4)

Model – Switch Type	Trip	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#
Pressure -Single Switch	High	0	27	0	62	126
	Low	0	42	0	50	126
Pressure - Dual Switch, Series	High	0	17	0	91	127
	Low	0	33	0	78	127
Pressure - Dual Switch, Parallel	High	0	38	0	35	127
	Low	0	51	0	25	127
Differential Pressure – Single Switch	High	0	104	0	151	256
	Low	0	144	0	118	256
Differential Pressure – Dual Switch, Series	High	0	95	0	180	258
	Low	0	136	0	146	258
Differential Pressure – Dual Switch, Parallel	High	0	115	0	125	258
	Low	0	154	0	93	258
Temp, Local Access – Single Switch	High	0	20	0	131	30
	Low	0	48	0	108	30
Temp, Local Access– Dual Switch, Series	High	0	10	0	160	32
	Low	0	39	0	136	32
Temp, Local Access – Dual Switch, Parallel	High	0	31	0	104	32
	Low	0	57	0	83	32
Temp, Remote Access– Single Switch	High	0	13	0	84	42
	Low	0	63	0	42	42
Temp, Remote Access– Dual Switch, Series	High	0	3	0	113	44
	Low	0	54	0	71	44
Temp, Remote Access– Dual Switch, Parallel	High	0	24	0	58	44
	Low	0	72	0	17	44