Failure Modes, Effects and Diagnostic Analysis

Project:
Series 100 and 120 Switches

Company:
United Electric Controls Company
Watertown, MA
USA

Contract Number: Q20/06-043
Report No.: UEC 16/02-130 R001
Version V1, Revision R4, June 29, 2020
Loren Stewart

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Series 100 and 120 Switches. 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 100 and 120 switches. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 100 Series pressure and differential pressure switches are activated when a bellows, diaphragm or piston sensor responds to a pressure change. This response, at a pre-determined set point, actuates a single snap-acting switch, converting the pressure signal into an electrical signal.

The 100 Series temperature switch utilizes either a liquid filled sensing stem (immersion stem, direct mounting) or liquid filled sensing bulb (bulb & capillary, remote mounting) to detect a temperature change. The response at a pre-determined set point actuates a SPDT snap-acting microswitch, converting the temperature signal into an electrical signal.

The 120 Series pressure and differential pressure switches are actuated when a bellows, diaphragm or piston sensor responds to a pressure change. This response at a pre-determined set point(s) actuates a SPDT, DPDT or dual SPDT snap-acting microswitch(es), which convert the pressure signal into an electrical signal.

The 120 Series temperature switch utilizes either a liquid filled sensing stem (immersion stem, direct mounting) or liquid filled sensing bulb (bulb & capillary, remote mounting) to detect a temperature change. The response at a pre-determined set point(s), actuates a SPDT, dual SPDT, or DPDT snap-acting micro switch(es), converting the temperature signal into an electrical signal.

Table 1 gives an overview of the different versions that were considered in this FMEDA of the Series 100 and 120 switches.

Table 1 Version Overview

Option 1	100 Series Pressure / Vacuum, Single Switch – High Trip
Option 2	100 Series Pressure / Vacuum, Single Switch – Low Trip
Option 3	100 Series Differential, Single Switch – High Trip
Option 4	100 Series Differential, Single Switch – Low Trip
Option 5	100 Series Temperature, Single Switch - High Trip
Option 6	100 Series Temperature, Single Switch – Low Trip
Option 7	100 Series Pressure / Vacuum, Dual Switch – High Trip
Option 8	100 Series Pressure / Vacuum, Dual Switch – Low Trip
Option 9	100 Series Differential, Dual Switch – High Trip
Option 10	100 Series Differential, Dual Switch – Low Trip
Option 11	100 Series Temperature, Dual Switch – High Trip
Option 12	100 Series Temperature, Dual Switch – Low Trip
Option 13	120 Series Pressure / Vacuum, Single Switch – High Trip
Option 14	120 Series Pressure / Vacuum, Single Switch – Low Trip
Option 15	120 Series Differential, Single Switch – High Trip
Option 16	120 Series Differential, Single Switch – Low Trip
Option 17	120 Series Temperature, Single Switch - High Trip
Option 18	120 Series Temperature, Single Switch – Low Trip
Option 19	120 Series Pressure / Vacuum, Dual Switch – High Trip
Option 20	120 Series Pressure / Vacuum, Dual Switch – Low Trip
Option 21	120 Series Differential, Dual Switch – High Trip
Option 22	120 Series Differential, Dual Switch – Low Trip
Option 23	120 Series Temperature, Dual Switch – High Trip
Option 24	120 Series Temperature, Dual Switch – Low Trip

The Series 100 and 120 switches are classified as Type A[1] elements according to IEC 61508, having a hardware fault tolerance of 0.

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

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. See Section 5.2. Therefore, the Series 100 and 120 switches can be classified as a 2_H device when the listed failure rates are used. When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H. If Route 2_H is not applicable for the entire sensor element, the architectural constraints will need to be evaluated per Route 1_H.

The failure rates for the Series 100 and 120 switches 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 do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

A user of the Series 100 and 120 switches can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Series 100 and 120 switches. From this, failure rates and example PFD_{avg} values may be calculated.

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

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, cybersecurity, and availability. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

United Electric Controls Company	Manufacturer of the Series 100 and 120 switches
exida	Performed the hardware assessment

United Electric Controls Company contracted *exida* in May 2016 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, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 4th Edition, 2016	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2016 (pending publication, not publically available at the time of this report)
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M., 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9

[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N10]	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.
[N11]	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.
[N12]	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.
[N13]	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.

2.4 Reference documents

2.4.1 Documentation provided by United Electric Controls Company

[D1]	IMP100-11	Instruction Manual 100 Series
[D2]	IMP100-06	Instruction Manual 100 Series
[D3]	IMP120-17	Instruction Manual 120 Series
[D4]	IMT120-11	Instruction Manual 120 Series
[D5]	Various	Series 100 Temperature drawings and BOMs
[D6]	Various	Series 100 Differential drawings and BOMs
[D7]	Various	Series 100 Vacuum and Compound drawings and BOMs
[D8]	Various	Series 120 Temperature drawings and BOMs
[D9]	Various	Series 120 Differential drawings and BOMs
[D10]	Various	Series 120 Vacuum and Compound drawings and BOMs

2.4.2 Documentation generated by *exida*

[R1]	United Electric FMEDA 100 Series R4.xls, Rev 4, 21-Feb-17	Failure Modes, Effects, and Diagnostic Analysis – Series 100 Switches (internal document)
[R2]	United Electric FMEDA 120 Series-R5.xls, Rev 6, 27-Jun-20	Failure Modes, Effects, and Diagnostic Analysis – Series 120 Switches (internal document)
[R3]	UEC 16/02-130 R001, V1R4, 29-Jun-20	FMEDA report, Series 100 and 120 Switches (this report)

3 Product Description

The 100 Series pressure and differential pressure switches are activated when a bellows, diaphragm or piston sensor responds to a pressure change. This response, at a pre-determined set point, actuates a single snap-acting switch, converting the pressure signal into an electrical signal. Included are the H100 and H100K Series.

The 100 Series temperature switch utilizes either a liquid filled sensing stem (immersion stem, direct mounting) or liquid filled sensing bulb (bulb & capillary, remote mounting) to detect a temperature change. The response at a pre-determined set point actuates a SPDT snap-acting microswitch, converting the temperature signal into an electrical signal. Included are the B100, C100, E100 and F100 Series.

The 120 Series pressure and differential pressure switches are actuated when a bellows, diaphragm or piston sensor responds to a pressure change. This response at a pre-determined set point(s) actuates a SPDT, DPDT or dual SPDT snap-acting microswitch(es), which convert the pressure signal into an electrical signal. Included are the J120, H121, H122, J120K, H121K and H122K Series.

The 120 Series temperature switch utilizes either a liquid filled sensing stem (immersion stem, direct mounting) or liquid filled sensing bulb (bulb & capillary, remote mounting) to detect a temperature change. The response at a pre-determined set point(s), actuates a SPDT, dual SPDT, or DPDT snap-acting micro switch(es), converting the temperature signal into an electrical signal. Included are the B121, B122, C120, E121, E122 and F120 Series.

Figure 1 Typical Series 100 and 120 switches covered in this FMEDA

Table 2 gives an overview of the different versions that were considered in the FMEDA of the Series 100 and 120 switches.

Table 2 Version Overview

Option 1	100 Series Pressure / Vacuum, Single Switch – High Trip
Option 2	100 Series Pressure / Vacuum, Single Switch – Low Trip
Option 3	100 Series Differential, Single Switch – High Trip
Option 4	100 Series Differential, Single Switch – Low Trip
Option 5	100 Series Temperature, Single Switch - High Trip
Option 6	100 Series Temperature, Single Switch – Low Trip
Option 7	100 Series Pressure / Vacuum, Dual Switch – High Trip
Option 8	100 Series Pressure / Vacuum, Dual Switch – Low Trip
Option 9	100 Series Differential, Dual Switch – High Trip
Option 10	100 Series Differential, Dual Switch – Low Trip
Option 11	100 Series Temperature, Dual Switch – High Trip
Option 12	100 Series Temperature, Dual Switch – Low Trip
Option 13	120 Series Pressure / Vacuum, Single Switch – High Trip
Option 14	120 Series Pressure / Vacuum, Single Switch – Low Trip
Option 15	120 Series Differential, Single Switch – High Trip
Option 16	120 Series Differential, Single Switch – Low Trip
Option 17	120 Series Temperature, Single Switch - High Trip
Option 18	120 Series Temperature, Single Switch – Low Trip
Option 19	120 Series Pressure / Vacuum, Dual Switch – High Trip
Option 20	120 Series Pressure / Vacuum, Dual Switch – Low Trip
Option 21	120 Series Differential, Dual Switch – High Trip
Option 22	120 Series Differential, Dual Switch – Low Trip
Option 23	120 Series Temperature, Dual Switch – High Trip
Option 24	120 Series Temperature, Dual Switch – Low Trip

The Series 100 and 120 switches are classified as Type A[2] elements according to IEC 61508, having a hardware fault tolerance of 0.

Note: If a 100 or 120 has Dual Switches and only one of them is being used for the safety function, then the Single Switch failure rates should be used.

[2] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 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 listed in section 2.4.1 and is documented in [R1].

4.1 Failure categories description

In order to judge the failure behavior of the Series 100 and 120 switches, 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, such as Partial Valve Stroke Testing.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics, such as Partial Valve Stroke Testing.
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 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore, they are not used for the Safe Failure Fraction calculation needed when Route 2_H failure data is not available.

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

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

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

4.2.2 Failure rates

The 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 [N2] which were derived using over 250 billion unit operational hours of process industry field failure data from multiple sources and failure data from various databases. 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 3 (General Field Equipment) as this was judged to be the best fit for the product and application information submitted by United Electric Controls Company. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

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 ([N11] & [N12]) 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 100 and 120 switches.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire Series 100 and 120 switches, 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 limited by the manufacturer's published ratings.
- Materials are compatible with the environmental and process conditions.
- The device is installed per the 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 FMEDA analysis of the Series 100 and 120 switches.

Table 3 lists the failure rates for the Series 100 and 120 switches according to IEC 61508 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[3] with Good Maintenance Assumptions in FIT (SSI=2)

Application/Device/Configuration	Trip	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}	#
100 Series Pressure / Vacuum, Single Switch	High	0	74	0	152	84
	Low	0	39	0	191	79
100 Series Differential, Single Switch	High	0	114	0	180	221
	Low	0	61	0	239	215
100 Series Temperature, Single Switch	High	0	74	0	190	149
	Low	0	114	0	154	144
100 Series Pressure / Vacuum, Dual Switch	High	0	97	0	105	81
	Low	0	62	0	140	79
100 Series Differential, Dual Switch	High	0	137	0	133	218
	Low	0	83	0	188	215
100 Series Temperature, Dual Switch	High	0	97	0	143	145
	Low	0	137	0	104	144
120 Series Pressure / Vacuum, Single Switch	High	0	122	0	242	288
	Low	0	86	0	293	284
120 Series Differential, Single Switch	High	0	142	0	270	407
	Low	0	90	0	339	402
120 Series Temperature, Single Switch	High	0	122	0	263	250
	Low	0	121	0	279	246
120 Series Pressure / Vacuum, Dual Switch	High	0	144	0	195	284
	Low	0	109	0	243	284
120 Series Differential, Dual Switch	High	0	164	0	224	404
	Low	0	112	0	289	402
120 Series Temperature, Dual Switch	High	0	144	0	216	247
	Low	0	144	0	228	246

[3] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[4] 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.

Note that the Dual Switch numbers are for when the two set of switch contacts are wired in series for when an Open contact is the Safe state or the switches are wired in parallel for when a Closed contact is the Safe state.

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 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508 (See Section 5.2).

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.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the Series 100 and 120 switches meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) when the listed failure rates from Table 3 are used.

If Route 2_H is not applicable for all devices that constitute the entire element, the architectural constraints will need to be evaluated per Route 1_H.

The architectural constraint type for the Series 100 and 120 switches 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 9 lists the failure rates for the Series 100 and 120 switches 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 sections describe how to apply the results of the FMEDA.

5.1 PFD_{avg} calculation Series 100 and 120 switches

Using the failure rate data displayed in, Table 3 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 entire sensor 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 which may be incorrect. Therefore, the use of pre-calculated PFDavg 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 the sensor element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates for all the devices in the sensor element and the proof test coverage for the sensor element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test and the dangerous failure rate after proof test for the Series 100 and 120 switches are listed in Appendix B. This is combined with the dangerous failure rates after proof test for other devices in the sensor element to establish the proof test coverage for the sensor element.

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 of its components have been installed in the field for one year or more; and

3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and

4. failure definitions, especially "random" vs. "systematic" are checked by *exida*; and

5. every component used in an FMEDA meets the above criteria.

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

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
Device	A device is something that is part of an element; but, cannot perform an element safety function on its own.
Dynamic Applications	The movement interval of the final element device is less than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.
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
High demand Mode	Mode, where the demand interval for operation made on a safety-related system is less than twice the proof test interval.
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
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.
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
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).
SSI	Site Safety Index (See Appendix E)

Static Applications	The movement interval of the final element device is greater than 200 hours. Movement may be accomplished by PVST, full stroke proof testing or a demand on the system.
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 exida compiled field failure data and 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 Releases

Version History: V1, R4: Added hermetically sealed switches to Series 120; June 29, 2020

V1, R3: Added C100 models and revised redundant Dual Switch failure rates; February 17, 2017

V1, R2: Revised failure rates per updated analysis; January 30, 2017

V1, R1: Update models; 1/9/17

V0, R1: Draft; 1/8/17

Author(s): Loren Stewart

Review: V0, R1: Ted Stewart (*exida*); 1/8/17

Release Status: Released to United Electric Controls Company

7.3 Future enhancements

At request of client.

7.4 Release signatures

Loren Stewart, CFSP, Safety Engineer

Ted Stewart, CFSP, Safety Engineer

Appendix A Lifetime of Critical Components

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

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[5] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

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

It is the responsibility of the end user to maintain and operate the Series 100 and 120 switches 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 100 and 120 switches.

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 normal switch/mechanical parts is > 100,000 full scale cycles or 10 years, whichever results in the shortest lifetime. The useful lifetime of the hermetic switches is > 10,000 full scale cycles or 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.

[5] 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 consists of a calibration check, see Table 4.

Table 4 Suggested Proof Test – Series 100 and 120 switches

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 5 through Table 6.

Table 5 Suggested Proof Test – Series 100 Switches

Device – Single or Dual Switch		λ_{DU}PT (FIT)	Proof Test Coverage
Pressure / Vacuum	High Trip	6	95%
	Low Trip	14	92%
Differential	High Trip	9	94%
	Low Trip	18	92%
Temperature	High Trip	7	96%
	Low Trip	14	90%

Table 6 Suggested Proof Test – Series 120 Switches

Device – Single or Dual Switch		λ_{DU}PT (FIT)	Proof Test Coverage
Pressure / Vacuum	High Trip	13	94%
	Low Trip	37	85%
Differential	High Trip	15	93%
	Low Trip	40	86%
Temperature	High Trip	13	94%
	Low Trip	37	84%

Appendix C *exida* Environmental Profiles

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

[6] Humidity rating per IEC 60068-2-3
[7] Shock rating per IEC 60068-2-27
[8] Vibration rating per IEC 60068-2-6
[9] Chemical Corrosion rating per ISA 71.04
[10] Surge rating per IEC 61000-4-5
[11] EMI Susceptibility rating per IEC 61000-4-3
[12] ESD (Air) rating per IEC 61000-4-2

Appendix D Determining Safety Integrity Level

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

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

These are:
A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;
B. Architecture Constraints (minimum redundancy requirements) are met; and
C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

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

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

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

A Probability of Failure on Demand (PFD_{avg}) 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 250 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 (Figure 2).

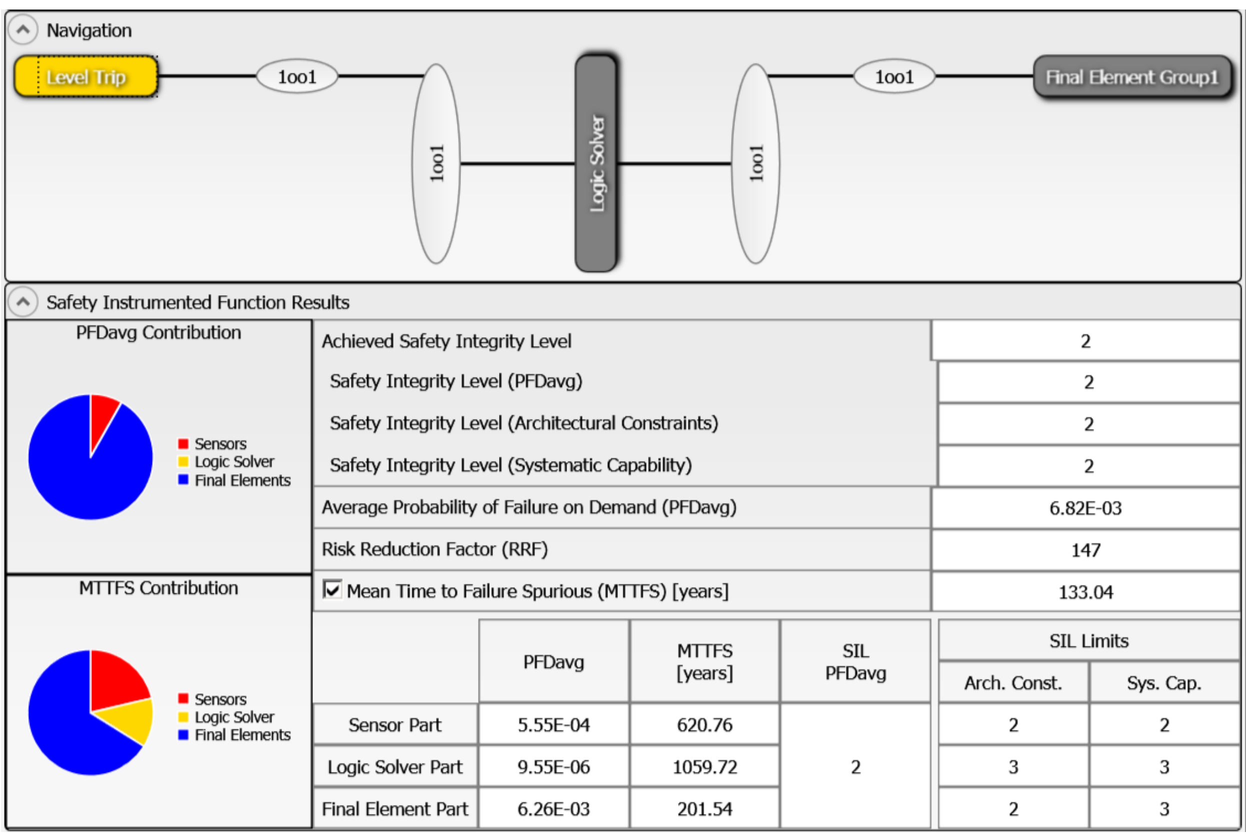

Figure 2: exSILentia results for idealistic variables.

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

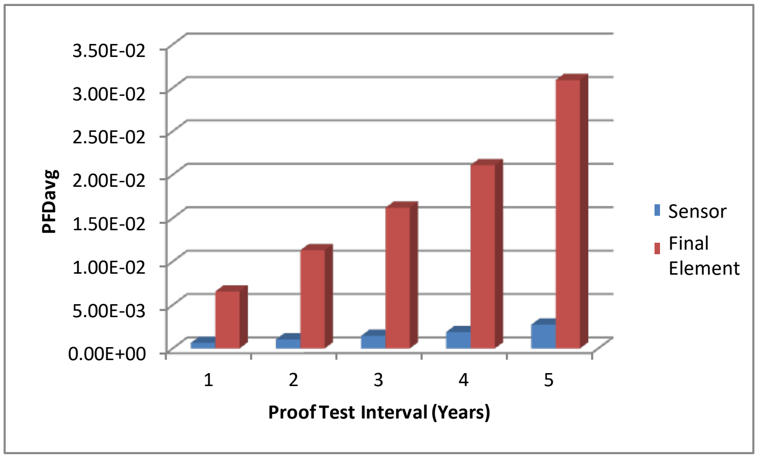

Figure 3: PFD_{avg} versus Proof Test Interval

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 of 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).

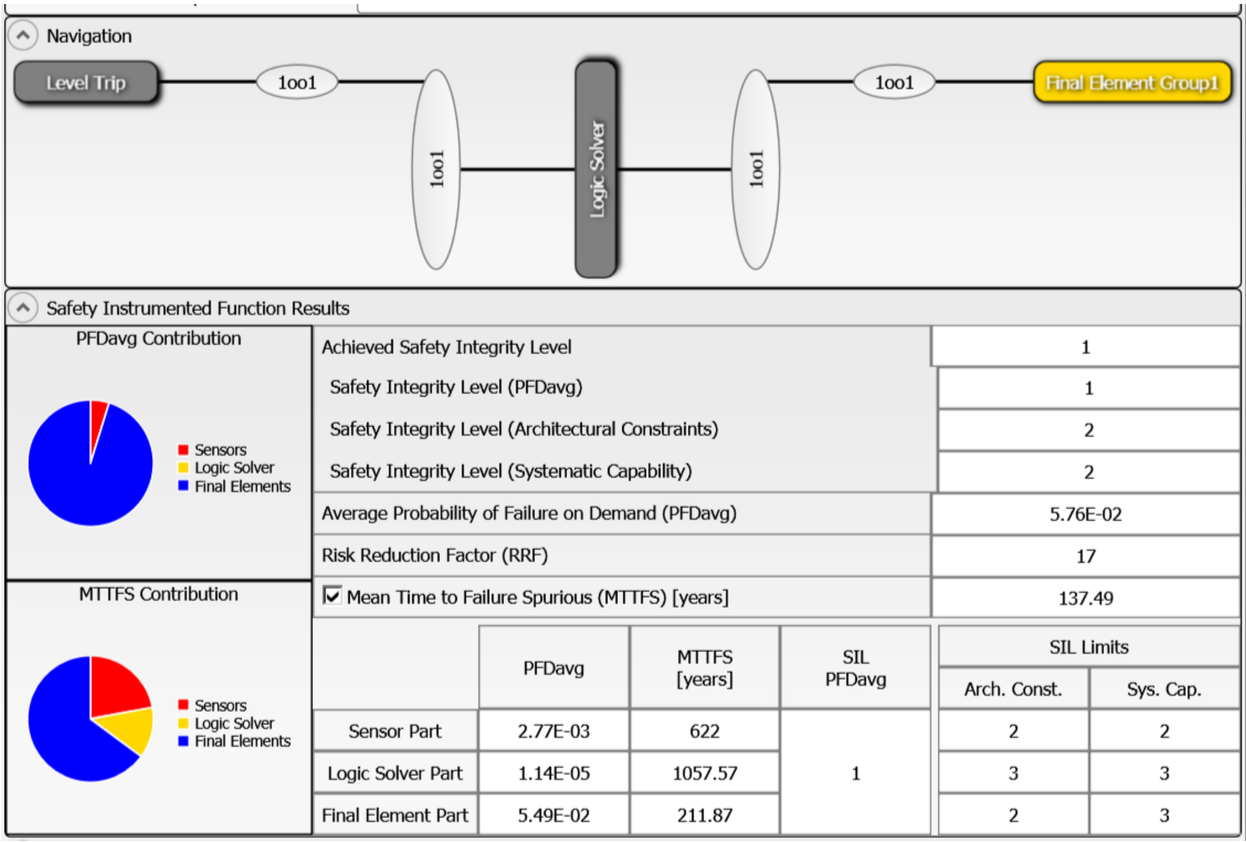

Figure 4: exSILentia results with realistic variables

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 8 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 8 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 100 and 120 switches

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 sensor 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 9 lists the failure rates for the Series 100 and 120 switches according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 9 Failure rates for Static Applications[13] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	Trip	λ_{SD}	λ_{SU}[14]	λ_{DD}	λ_{DU}	#
100 Series Pressure / Vacuum, Single Switch	High	0	44	0	76	50
	Low	0	23	0	96	47
100 Series Differential, Single Switch	High	0	68	0	90	133
	Low	0	37	0	120	129
100 Series Temperature, Single Switch	High	0	44	0	95	89
	Low	0	68	0	77	86
100 Series Pressure / Vacuum, Dual Switch	High	0	58	0	53	49
	Low	0	37	0	70	47
100 Series Differential, Dual Switch	High	0	82	0	67	131
	Low	0	50	0	94	129
100 Series Temperature, Dual Switch	High	0	58	0	72	87
	Low	0	82	0	52	86
120 Series Pressure / Vacuum, Single Switch	High	0	73	0	121	173
	Low	0	52	0	147	170
120 Series Differential, Single Switch	High	0	85	0	135	244
	Low	0	54	0	170	241
120 Series Temperature, Single Switch	High	0	73	0	132	150
	Low	0	73	0	140	148
120 Series Pressure / Vacuum, Dual Switch	High	0	86	0	98	170
	Low	0	65	0	122	170
120 Series Differential, Dual Switch	High	0	98	0	112	242
	Low	0	67	0	145	241
120 Series Temperature, Dual Switch	High	0	86	0	108	148
	Low	0	86	0	114	148

[13] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[14] 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.