exida®

Failure Modes, Effects and Diagnostic Analysis

Project:
ECHOTEL 961/962 Ultrasonic Single and Dual Point Level Switches

Company:
Magnetrol International, Inc.
Aurora, IL
USA

Contract Number: Q17/10-006
Report No.: MAG 17/10-006 R001
Version V2, Revision R0, August 17, 2018
Rudolf Chalupa

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 ECHOTEL 961/962 Ultrasonic Single and Dual Point Level Switches, hardware and software revision per Section 2.5.1. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the 961/962. For full functional safety certification purposes, all requirements of IEC 61508 must be considered.

ECHOTEL 961/962 Ultrasonic Single and Dual Point Level Switches utilize pulsed signal technology to detect high, low, or dual point level in a broad range of liquid media applications. Model 961 is a single point level switch. Model 962 is a dual point switch used as a level controller or to control pumps in an auto-fill or auto-empty mode.

Table 1 and Table 2 are an overview of the different versions that were considered in the FMEDA of the 961/962.

Table 1 Line Powered, Relay Output Version Overview

961 Dry Is Safe Redundant	961-2 or 961-7 Single Point Level Switch, Reported Dry Condition Is Safe, Redundant Relay Contacts
961 Wet Is Safe Redundant	961-2 or 961-7 Single Point Level Switch, Reported Wet Condition Is Safe, Redundant Relay Contacts
961 Dry Is Safe Non-redundant	961-2 or 961-7 Single Point Level Switch, Reported Dry Condition Is Safe, Non-redundant Relay Contacts
961 Wet Is Safe Non-redundant	961-2 or 961-7 Single Point Level Switch, Reported Wet Condition Is Safe, Non-redundant Relay Contacts
962 Dry Is Safe	962-2 or 962-7 Dual Point Level Switch, Reported Dry Condition Is Safe
962 Wet Is Safe	962-2 or 962-7 Dual Point Level Switch, Reported Wet Condition Is Safe

Table 2 Loop Powered, Current Shift Version Overview

961 Dry Is Safe	961-5 Single Point Level Switch, Reported Dry Condition Is Safe
961 Wet Is Safe	961-5 Single Point Level Switch, Reported Wet Condition Is Safe
962 Dry Is Safe	962-5 Dual Point Level Switch, Reported Dry Condition Is Safe
962 Wet Is Safe	962-5 Dual Point Level Switch, Reported Wet Condition Is Safe

The 961/962 is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

---

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

The failure rate data used for this analysis meet the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the 961/962 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.

Based on the assumptions listed in 4.3, the failure rates for the 961/962 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 250 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 961/962 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 961/962. 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

Magnetrol International, Inc.   Manufacturer of the 961/962, performed the hardware assessment.

exida   Reviewed the hardware assessment

Magnetrol International, Inc. contracted *exida* 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 *exida* tools used

[T1]	V7.1.18	*exida* FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by Magnetrol International, Inc.

[D1]	Doc # 51-646.5, 2017-04	Installation and Operating Manual, Model 961/962
[D2]	Doc # 51-646, Rev 4, 2015-12	Instruction Manual, Loop Powered
[D3]	Doc # 51-650, Rev 0, 2010-07	Safety Manual; Loop Powered
[D4]	Doc # 51-651.0, 2017-04	Safety Manual, 961/962 Relay Version
[D5]	Doc # 094-5047, Rev A, 2005-	Schematic Drawing, 961

	05	
[D6]	Doc # 094-5048, Rev C, 2017-09-12	ECHOTEL 961 LOGIC SCHEMATIC
[D7]	Doc # 094-5049, Rev E, 2016-12	ECHOTEL 961 POWER SCHEMATIC
[D8]	Doc # 094-5050, Rev C, 2006-10	Schematic Drawing, 962
[D9]	Doc # 094-5052, Rev J, 2017-11-20	ECHOTEL 962 LOGIC SCHEMATIC
[D10]	Doc # 094-5051, Rev E, 2017-02	ECHOTEL 962 POWER SCHEMATIC
[D11]	Doc # 030-3590, Rev N, 2015-08-06	PCB Assembly Drawing & Bill of Material, 961,962
[D12]	Doc # 030-3594, Rev H, 2017-03	ECHOTEL 962 POWER P.C. BOARD ASSEMBLY
[D13]	Model 961 Theory of Operation..docx, 2016-09-26	Theory of Operation
[D14]	961 HOUSING DRY IS SAFE.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Housing, Dry Is Safe
[D15]	961 HOUSING WET IS SAFE.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Housing, Wet Is Safe
[D16]	961 LOOP PC BOARD DRY IS SAFE.efm, 2013-06-26	Failure Modes, Effects, and Diagnostic Analysis - 961 Loop PCB, Dry Is Safe
[D17]	961 LOOP PC BOARD WET IS SAFE.efm, 2013-06-26	Failure Modes, Effects, and Diagnostic Analysis – 961 Loop PCB, Wet Is Safe
[D18]	961 LOOP PC BOARD DRY IS SAFEwithCorrections.efm, 2013-10-10	Failure Modes, Effects, and Diagnostic Analysis – 961 Loop PCB, Dry Is Safe
[D19]	961 LOOP PC BOARD WET IS SAFEwithCorrections.efm.efm, 2013-10-10	Failure Modes, Effects, and Diagnostic Analysis – 961 Loop PCB, Wet Is Safe
[D20]	961 logic DRY is SAFE-2017-09-19.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Logic, Dry Is Safe
[D21]	961 logic WET is SAFE-2017-09-19.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Logic, Wet Is Safe
[D22]	961 power DC-NON-RedundantContacts-2017-09-15.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Power, Non-Redundant Relay Contacts
[D23]	961 power DC-RedundantContacts-2017-09-15.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Power, Redundant Relay Contacts

[D24]	961 Probe DRY is SAFE 2017-09-14.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Probe, Dry Is Safe
[D25]	961 Probe WET is SAFE 2017-09-14.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Probe, Wet Is Safe
[D26]	Echotel_961 Relay SIL Summary2017-09-19.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary – 961
[D27]	Echotel_961 Loop SIL Summary.xlsx, 2016-09-26	Failure Modes, Effects, and Diagnostic Analysis - Summary, Echotel 961
[D28]	Echotel_961 Loop SIL SummaryWithCorrections.xlsx , 2016-10-10	Failure Modes, Effects, and Diagnostic Analysis - Summary, Echotel 961
[D29]	962 logic DRY is SAFE-2017-09-19.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Logic, Dry Is Safe
[D30]	962 logic WET is SAFE-2017-09-19.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Logic, Wet Is Safe
[D31]	962 power DC-2017-09-15.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Power
[D32]	962 Probe DRY is SAFE 2017-09-15.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Probe, Dry Is Safe
[D33]	962 Probe WET is SAFE 2017-09-15.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Probe, Wet Is Safe
[D34]	962 LOOP PC BOARD DRY IS SAFE DELAY IS SAFE.efm, 2013-07-25	Failure Modes, Effects, and Diagnostic Analysis – 962 Loop PCB, Dry Is Safe
[D35]	962 LOOP PC BOARD WET IS SAFE DELAY IS SAFE.efm.efm, 2013-07-25	Failure Modes, Effects, and Diagnostic Analysis – 962 Loop PCB, Wet Is Safe
[D36]	962 LOOP PC BOARD DRY IS SAFE DELAY IS SAFEwithCorrections.efm, 2013-10-10	Failure Modes, Effects, and Diagnostic Analysis – 962 Loop PCB, Dry Is Safe
[D37]	962 LOOP PC BOARD WET IS SAFE DELAY IS SAFEwithCorrections.efm, 2013-10-10	Failure Modes, Effects, and Diagnostic Analysis – 962 Loop PCB, Wet Is Safe
[D38]	Echotel-962 Loop SIL Summary.xlsx, 2016-09-26	Failure Modes, Effects, and Diagnostic Analysis - Summary, Echotel 962
[D39]	Echotel-962 Loop SIL SummaryWithCorrections.xlsx , 2016-10-10	Failure Modes, Effects, and Diagnostic Analysis - Summary, Echotel 962
[D40]	Echotel_962 Relay SIL Summary2017-09-19.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary – 962
[D41]	961 FMEDA REVIEW	Failure Modes, Effects, and Diagnostic Analysis - Review

	NOTESwithComments.docx, 2016-10-10	Notes –961/962

2.5.2 Documentation generated by *exida*

[R1]	961 logic DRY is SAFE-2017-10-31.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Logic, Dry Is Safe
[R2]	961 logic WET is SAFE-2017-10-31.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Logic, Wet Is Safe
[R3]	961 power DC-NON-RedundantContacts-2017-10-31.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Power, Non-Redundant Relay Contacts
[R4]	961 power DC-RedundantContacts-2017-10-31.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Power, Redundant Relay Contacts
[R5]	961 Probe DRY is SAFE 2017-10-31.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Probe, Dry Is Safe
[R6]	961 Probe WET is SAFE 2017-10-31.efm	Failure Modes, Effects, and Diagnostic Analysis – 961 Probe, Wet Is Safe
[R7]	Echotel_961 Relay SIL Summary2017-10-31.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary – 961
[R8]	962 logic DRY is SAFE-2017-11-02.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Logic, Dry Is Safe
[R9]	962 logic WET is SAFE-2017-11-02.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Logic, Wet Is Safe
[R10]	962 power DC-2017-11-01.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Power
[R11]	962 Probe DRY is SAFE 2017-11-01.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Probe, Dry Is Safe
[R12]	962 Probe WET is SAFE 2017-11-01.efm	Failure Modes, Effects, and Diagnostic Analysis – 962 Probe, Wet Is Safe
[R13]	Echotel_962 Relay SIL Summary2017-11-02.xlsx	Failure Modes, Effects, and Diagnostic Analysis - Summary – 962
[R14]	961 HOUSING DRY IS SAFE RPC 2016-10-03.xls	FMEDA, 961 Housing, Dry Is Safe (Loop)
[R15]	961 HOUSING WET IS SAFE RPC 2016-10-03.xls	FMEDA, 961 Housing, Wet Is Safe (Loop)
[R16]	961 LOOP PC BOARD DRY IS SAFE RPC 2016-10-03.xls	FMEDA, 961 Loop PCB, Dry Is Safe
[R17]	961 FMEDA REVIEW NOTES.docx, 2016-10-04	Failure Modes, Effects, and Diagnostic Analysis - Review Notes –961/962 (Loop)

3   Product Description

ECHOTEL 961/962 Ultrasonic Single and Dual Point Level Switches utilize pulsed signal technology to detect high, low, or dual point level in a broad range of liquid media applications. Model 961 is a single point level switch. Model 962 is a dual point switch used as a level controller or to control pumps in an auto-fill or auto-empty mode.

961/962 switches utilize ultrasonic energy to detect the presence or absence of liquid in a single or dual point transducer. Ultrasonic contact level technology uses high frequency sound waves that are easily transmitted across a transducer gap in the presence of a liquid media, but are attenuated when the gap is dry. Model 961/962 switches use an ultrasonic frequency of 2 MHz to perform this liquid level measurement in a wide variety of process media and application conditions.

The transducer uses a pair of piezoelectric crystals that are encapsulated in epoxy at the tip of the transducer. The crystals are made of a ceramic material that vibrates at a given frequency when subjected to an applied voltage. The transmit crystal converts the applied voltage from the electronics into an ultrasonic signal. When liquid is present in the gap, the receive crystal senses the ultrasonic signal from the transmit crystal and converts it back to an electrical signal. This signal is sent to the electronics to indicate the presence of liquid in the transducer gap. When there is no liquid present, the ultrasonic signal is attenuated and is not detected by the receive crystal.

Model 961

Model 962

Figure 1 961/962, Parts included in the FMEDA

Table 3 and Table 4 give an overview of the different versions that were considered in the FMEDA of the 961/962.

Table 3 Line Powered, Relay Output Version Overview

961 Dry Is Safe Redundant	961-2 or 961-7 Single Point Level Switch, Reported Dry Condition Is Safe, Redundant Relay Contacts
961 Wet Is Safe Redundant	961-2 or 961-7 Single Point Level Switch, Reported Wet Condition Is Safe, Redundant Relay Contacts
961 Dry Is Safe Non-redundant	961-2 or 961-7 Single Point Level Switch, Reported Dry Condition Is Safe, Non-redundant Relay Contacts
961 Wet Is Safe Non-redundant	961-2 or 961-7 Single Point Level Switch, Reported Wet Condition Is Safe, Non-redundant Relay Contacts
962 Dry Is Safe	962-2 or 962-7 Dual Point Level Switch, Reported Dry Condition Is Safe
962 Wet Is Safe	962-2 or 962-7 Dual Point Level Switch, Reported Wet Condition Is Safe

Table 4 Loop Powered, Current Shift Version Overview

961 Dry Is Safe	961-5 Single Point Level Switch, Reported Dry Condition Is Safe
961 Wet Is Safe	961-5 Single Point Level Switch, Reported Wet Condition Is Safe
962 Dry Is Safe	962-5 Dual Point Level Switch, Reported Dry Condition Is Safe
962 Wet Is Safe	962-5 Dual Point Level Switch, Reported Wet Condition Is Safe

The 961/962 is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

---

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

4   Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis review was performed based on the documentation in section 2.5.1 and is documented in 2.5.2.

4.1   Failure categories description

In order to judge the failure behavior of the 961/962, the following definitions for the failure of the device were considered.

Fail-Safe State - Relay	State where the fault relay is de-energized.
Fail-Safe State - Loop	Failure that deviates the process signal or the actual output by more than 2% of span, drifts toward the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected - Relay	Failure that causes the output signal to go to the predefined alarm state (fault relay de-energized).
Fail Detected - Loop	Failure that causes the output signal to go to the predefined alarm state (3.6 or 22 mA, user selectable).
Fail Dangerous - Relay	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 - Loop	Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics.
Fail High – Loop only	Failure that causes the output signal to go to the over-range or high alarm output current (> 21 mA).
Fail Low – Loop only	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.6 mA).
Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in IEC 61508 in order to provide a complete set of data needed for design optimization.

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 250 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 2 as this was judged to be the best fit for the product and application information submitted by Magnetrol International, Inc.. 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 961/962.

- The worst-case assumption of a series system is made. Therefore, only a single component failure will fail the entire 961/962 and propagation of failures is not relevant.

- Failure rates are constant for the useful life period.

- Any product component that cannot influence the safety function (feedback immune) is excluded. All components that are part of the safety function including those needed for normal operation are included in the analysis.

- The stress levels are specified in the *exida* Profile used for the analysis are limited by the manufacturer's published ratings.

- Practical fault insertion tests have been used when applicable to demonstrate the correctness of the FMEDA results.

- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function on the Loop Powered Current Shift version.

- Materials are compatible with process conditions.

- The device is installed and operated per manufacturer's instructions.

- External power supply failure rates are not included.

- Worst-case internal fault detection time is 10 seconds.

4.4 Application specific restrictions for Loop Powered, Current Shift version

The following application specific restrictions are applicable to the 961/962 and have been considered during the Failure Modes, Effects, and Diagnostic Analysis of the 961/962. These restrictions shall be included in the safety manual for the 961/962.

- The safety function must be designed so that it will operate correctly with the 961/962 set to maximum delay.

4.5 Line Powered, Relay Output Version Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 961/962 FMEDA.

Table 5 - Table 10 list the failure rates for the 961/962 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 5: 961 Dry Is Safe Redundant Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	258
Fail Safe Undetected	186
Fail Dangerous Detected	28
Fail Dangerous Undetected	30
Annunciation Detected	5
Annunciation Undetected	26

Table 6: 961 Wet Is Safe Redundant Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	10
Fail Safe Undetected	165
Fail Dangerous Detected	275
Fail Dangerous Undetected	50
Annunciation Detected	5
Annunciation Undetected	30

Table 7: 961 Dry Is Safe Non-redundant Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	258
Fail Safe Undetected	199
Fail Dangerous Detected	28
Fail Dangerous Undetected	55
Annunciation Detected	5
Annunciation Undetected	24

Table 8: 961 Wet Is Safe Non-redundant Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	10
Fail Safe Undetected	178
Fail Dangerous Detected	275
Fail Dangerous Undetected	76
Annunciation Detected	5
Annunciation Undetected	28

Table 9: 962 Dry Is Safe Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	447
Fail Safe Undetected	226
Fail Dangerous Detected	39
Fail Dangerous Undetected	60
Annunciation Detected	4
Annunciation Undetected	32

Table 10: 962 Wet Is Safe Failure rates with Good Maintenance Assumptions in FIT @ SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	20
Fail Safe Undetected	186
Fail Dangerous Detected	466
Fail Dangerous Undetected	96
Annunciation Detected	4
Annunciation Undetected	32

Table 11 lists the failure rates for the 961/962 according to IEC 61508.

Table 11 961/962 Failure rates with Good Maintenance Assumptions in FIT @ SSI=2 according to IEC 61508

Application/Device/Configuration	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}
961 Dry Is Safe Redundant	263	186	28	30
961 Wet Is Safe Redundant	15	165	275	50
961 Dry Is Safe Non-redundant	263	199	28	55
961 Wet Is Safe Non-redundant	15	178	275	76
962 Dry Is Safe	451	226	39	60
962 Wet Is Safe	24	186	466	96

---

[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.

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

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

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (see Section 5.2).

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 meet the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the 961/962 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 961/962 is B. 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 26 lists the failure rates for the 961/962 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 that has assumed perfect maintenance. See Appendix E for an explanation of SSI.

4.6 Loop Powered, Current Shift Version Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the 961/962 FMEDA.

Table 12 Failure rates 961 Dry Is Safe

Failure Category		Failure Rate (FIT)
Fail Safe Undetected		38
Fail Dangerous Detected		234
Fail Detected (detected by internal diagnostics)	190	
Fail High (detected by logic solver)	18	
Fail Low (detected by logic solver)	26	
Fail Dangerous Undetected		10
No Effect		118
Annunciation Undetected		15

Table 13 Failure rates 961 Wet Is Safe

Failure Category		Failure Rate (FIT)
Fail Safe Undetected		20
Fail Dangerous Detected		234
Fail Detected (detected by internal diagnostics)	190	
Fail High (detected by logic solver)	18	
Fail Low (detected by logic solver)	26	
Fail Dangerous Undetected		27
No Effect		118
Annunciation Undetected		15

Table 14 Failure rates 962 Dry Is Safe

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		64
Fail Dangerous Detected		426
Fail Detected (detected by internal diagnostics)	373	
Fail High (detected by logic solver)	22	
Fail Low (detected by logic solver)	31	
Fail Dangerous Undetected		10
No Effect		124
Annunciation Undetected		7

Table 15 Failure rates 962 Wet Is Safe

Failure Category	Failure Rate (FIT)	
Fail Safe Undetected		26
Fail Dangerous Detected		426
Fail Detected (detected by internal diagnostics)	373	
Fail High (detected by logic solver)	22	
Fail Low (detected by logic solver)	31	
Fail Dangerous Undetected		47
No Effect		124
Annunciation Undetected		7

Table 16 lists the failure rates for the 961/962 according to IEC 61508.

Table 16 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}
961 Dry Is Safe	0	38	234	10
961 Wet Is Safe	0	20	234	27
962 Dry Is Safe	0	64	426	10
962 Wet Is Safe	0	26	426	47

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

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

According to IEC 61508-2 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2, or the approach according to IEC 61511:2016 which is based on 2_H (see Section 5.2).

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 meet the *exida* criteria for Route 2_H which is more stringent than IEC 61508. Therefore, the 961/962 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 961/962 is B. 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.

---

[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.

5 Using the FMEDA Results

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

5.1 PFD$_{avg}$ calculation 961/962

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 22 and Table 23.

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 (1×10^{-9} failures per hour)

FMEDA — Failure Mode Effect and Diagnostic Analysis

HFT — Hardware Fault Tolerance

PFD_{avg} — Average Probability of Failure on Demand

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

SIF — Safety Instrumented Function

SIL — Safety Integrity Level

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

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
Q17/10-006	MAG 17/10-006 R001 V2 R0	Updated to included Loop Powered (MAG 16/08-078 R001 V1R4) to this report
Q17/10-006	MAG 17/10-006 R001 V1 R4	Added model idnetifiers
Q17/10-006	MAG 17/10-006 R001 V1 R3	Updated 962 logic schematic information
Q17/10-006	MAG 17/10-006 R001 V1 R2	Updated per client feedback
Q17/10-006	MAG 17/10-006 R001 V1 R1	Released
Q17/10-006	MAG 17/10-006 R001 V0 R1	Initial draft

Updated by Ted Stewart 8/14/2018

Reviewer: Rudolf Chalupa, *exida*, 2018-08-15

Status: Released, 11/8/2017

7.3 Future enhancements

At request of client.

7.4   Release signatures

Rudolf P. Chalupa, CFSE, Senior Safety Engineer

Ted E. Stewart, CFSP
Program Development & Compliance Manager

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[5] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

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

Table 17 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) – Aluminum electrolytic, non-solid electrolyte	Approx. 90,000 hours

It is the responsibility of the end user to maintain and operate the 961/962 per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

The limiting factors with regard to the useful lifetime of the system are the aluminum electrolytic capacitors. Therefore, the useful is predicted to be 10 years.

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

When plant/site experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant/site 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   Line Powered, Relay Output Version Suggested Proof Test

The suggested proof test for the 961/962 is described in Table 18 and Table 19 . Refer to the table in B.3 for the Proof Test Coverages

Table 18 Suggested Proof Test – 961 Relay

Step	Proof Test, Echotel Model 961 Relay
	(Refer to the Model 961 installation and operation manual and the SIL Safety Manual. Note the charts in the section labeled "Model 961 Line-Powered Configuration" of the I & O Manual.)
1	Bypass the PLC or take other action to avoid a false trip.
2	Inspect the Unit in detail outside and inside for physical damage or evidence of environmental or process leaks.
	a. Inspect the exterior of the Unit housing. If there is any evidence of physical damage that may impact the integrity of the housing and the environmental protection, the unit should be repaired or replaced.
	b. Inspect the interior of the Unit. Any evidence of moisture, from process or environment, is an indication of housing damage, and the unit should be repaired or replaced.
3	Observe and record the settings of the HI/LOW and INDEPENDENT/JOINT (I/J) DIP switches, the LED indicators, Relay contact conditions and Sensor GAP condition (WET or DRY).
	If the FAULT LED is lighted or the MALF LED is OFF, diagnose the fault and repair or replace the unit.
	Confirm proper operation of the unit: WET/DRY GAP condition and WET LED; LEVEL LED and relay operation.
	a. Press LEVEL TEST push button and confirm Relay Contacts and LEVEL LED change state. Release the button and unit returns to proper operation based on the GAP condition and switch settings.
	b. Change HI/LOW DIP switch position. Confirm LED & Relay change state. Observe the time delay from change of DIP switch until LED and Relay contacts change. Delay is set by Time Delay Pot, so delay may be as long as 10 seconds. Change HI/LOW DIP switch back to original setting and confirm proper operation, after the delay.
	c. Press MALF TEST push button and confirm: FAULT LED lights, MALF and WET LEDs goes OFF and MALF Relay contacts go to the de-energized state. Release button. Confirm unit returns to normal operation.

		d. Adjust the Time Delay Pot to maximum delay, fully clock-wise up to 20 turns. Change HI/LOW DIP switch position and observe the time delay from change of DIP switch until LED and Relays change. Confirm delay ≥ 10 seconds. Change HI/LOW DIP switch back to original setting and confirm ≥ 10 seconds delay. Adjust the Time Delay Pot to minimum delay, fully counter-clock-wise ~20 turns. Change HI/LOW DIP switch position and observe the time delay. Confirm delay ≤ 1 seconds. Change HI/LOW DIP switch back to original setting and confirm minimum delay.
4		When possible moving the process level will provide a more complete proof test.
		Confirm proper operation of the unit: WET/DRY GAP condition, WET LED and relay operation.
		a. Move the process level and confirm the GAP condition has changed. Confirm proper operation of the unit: WET/DRY GAP condition and corresponding LED and Relay contacts state.
		b. Return process level to original state. Confirm proper operation of the unit: WET/DRY GAP condition and corresponding LED and Relay contacts state.
		c. If unit fails the tests of steps 4.a or 4.b proceed to step 5.
		d. Adjust the Time Delay Pot to the original setting. Use HI/LOW DIP switch (as described in step 3.b) to confirm that delay is returned to original setting.
		e. Proceed to step 6.
5		If the unit under test fails to respond to process level changes remove the unit from the process and bench test.
		a. Remove the unit from the process. Inspect the ultrasound transducer for evidence of damage or coating buildup. Fouling on the transducer surface may interfere with normal operation. If heavy fouling is evident, it is suggested to service the transducer more frequently.
		b. Clean the ultrasonic transducer, especially in the area of the sensor GAP.
		c. Perform a bench test per the steps of section 4. When possible, it is best to use the actual process material, because material properties affect the ultrasonic performance. Confirm proper unit operation: WET/DRY GAP condition; LEDs and Relay contacts state.
		d. If unit passes the tests of steps 5.c, return to the process installation and repeat the tests of step 4.
		e. If the unit fails re-test in the process, it must be replaced.
6		Proof test is complete. Restore loop to full operation.

Table 19 Suggested Proof Test – 962 Relay

Step	Proof Test, Echotel Model 962 Relay
	(Refer to the Model 962 installation and operation manual and the SIL Safety Manual. Note the charts in the section labeled "Model 962 Line-powered Configuration" of the I & O Manual.)
1	Bypass the PLC or take other action to avoid a false trip.
2	Inspect the Unit in detail outside and inside for physical damage or evidence of environmental or process leaks.
	a. Inspect the exterior of the Unit housing. If there is any evidence of physical damage that may impact the integrity of the housing and the environmental protection, the unit should be repaired or replaced.
	b. Inspect the interior of the Unit. Any evidence of moisture, from process or environment, is an indication of housing damage, and the unit should be repaired or replaced.
3	Observe and record the settings of the HI/LOW and PUMP CONTROL/LEVEL CONTROL (PC/LC) DIP switches, the LED indicators, Relay contact conditions and Sensor GAP condition (WET or DRY).
	If the FAULT LED is lighted or the MALF LED is OFF, diagnose the fault and repair or replace the unit.
	Confirm proper operation of the unit: WET/DRY GAP condition for each GAP; UPPER LED and relay operation; and LOWER LED and relay operation.
	a. Press LEVEL TEST push button and confirm both UPPER and LOWER Relay Contacts change state, and LEDs also change. Release the button and unit returns to proper operation based on the GAP condition and switch settings.
	b. Change HI/LOW DIP switch position. Confirm LEDs & Relays change state. Observe the time delay from change of DIP switch until LEDs and Relay contacts change. Delay is set by Time Delay Pot, so delay may be as long as 10 seconds. Change HI/LOW DIP switch back to original setting and confirm proper operation, after the delay.
	c. Press MALF TEST push button and confirm: FAULT LED lights, All other LEDs goes OFF, and all Relay contacts go to the de-energized state. Release button. Confirm unit returns to normal operation.
	d. Adjust the Time Delay Pot to maximum delay, fully clock-wise up to 20 turns. Change HI/LOW DIP switch position and observe the time delay from change of DIP switch until LED and Relays change. Confirm delay ≥ 10 seconds. Change HI/LOW DIP switch back to original setting and confirm ≥ 10 seconds delay. Adjust the Time Delay Pot to minimum delay, fully counter-clock-wise ~20 turns. Change HI/LOW DIP switch position and observe the time delay. Confirm delay ≤ 1 seconds. Change HI/LOW DIP switch back to original setting and confirm minimum delay.
4	When possible moving the process level will provide a more complete proof

		test.
		Confirm proper operation of the unit: WET/DRY GAP condition for each GAP; UPPER LED and relay operation; and LOWER LED and relay operation.
		a. Move the process level and confirm the GAP condition has changed. Confirm proper operation of the unit: WET/DRY GAP condition and corresponding LED and Relay contacts state. Continue to move process level in order to test three possible states; 1. Both GAPS DRY 2. One GAP WET 3. BOTH GAPS WET.
		b. Change the PUMP CONTROL / LEVEL CONTROL (PC/LC) DIP switch position. Repeat the test of step 4.a to test all 3 possible GAP states and confirm expected operation. Return the PC/LC DIP to the original position.
		c. If unit fails the tests of steps 4.a or 4.b proceed to step 5.
		d. Adjust the Time Delay Pot to the original setting. Use HI/LOW DIP switch (as described in step 2.e) to confirm that delay is returned to original setting.
		e. Proceed to step 6.
5		If the unit under test fails to respond to process level changes remove the unit from the process and bench test.
		a. Remove the unit from the process. Inspect the ultrasound transducer for evidence of damage or coating buildup. Fouling on the transducer surface may interfere with normal operation. If heavy fouling is evident, it is suggested to service the transducer more frequently.
		b. Clean the ultrasonic transducer, especially in the area of the sensor GAP.
		c. Perform a bench test per the steps of section 4. When possible, it is best to use the actual process material, because material properties affect the ultrasonic performance. Confirm proper unit operation: WET/DRY GAP condition; LEDs and Relay contacts state.
		d. If unit passes the tests of steps 5.c, return to the process installation and repeat the tests of step 4.
		e. If the unit fails re-test in the process, it must be replaced.
6		Proof test is complete. Restore loop to full operation.

B.2   Loop Powered, Current Shift Version Suggested Proof Test

The suggested proof test for the 961/962 is described below. Refer to the table in B.3 for the Proof Test Coverages

Table 20 Suggested Proof Test, 961 Loop

Step	Proof Test, Echotel Model 961 Loop
	(Refer to the Model 961 installation and operation manual and the SIL Safety Manual. Note the chart in the High/Low Dip Switch section of the I & O Manual.)
1	Bypass the PLC or take other action to avoid a false trip.
2	Inspect the Unit in detail outside and inside for physical damage or evidence of environmental or process leaks.
	a. Inspect the exterior of the Unit housing. If there is any evidence of physical damage that may impact the integrity of the housing and the environmental protection, the unit should be repaired or replaced.
	b. Inspect the interior of the Unit. Any evidence of moisture, from process or environment, is an indication of housing damage, and the unit should be repaired or replaced.
3	Observe and record the settings of the HI/LOW and 22/3.6 DIP switches, the LED indicators, Loop Current and Sensor GAP condition (WET or DRY).
	If the FAULT LED is lighted, diagnose the fault and repair or replace the unit.
	Confirm proper operation of the unit: WET/DRY GAP condition; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.
	a. Press LOOP TEST push button and confirm change; 8mA >> 16mA or 16mA >> 8mA. Release the button and unit returns to proper operation.
	b. Change HI/LOW DIP switch position. Confirm both LED & Loop Current change state; 8mA >> 16mA or 16mA >> 8mA. Observe and record the time delay from change of DIP switch until LED and Loop current change. Delay is set by Time Delay Pot, so the delay may take somewhere around 10 seconds. Change HI/LOW DIP switch back to original setting and confirm proper operation, after the delay.
	c. Press FAULT TEST push button and confirm: FAULT LED lights; Loop current ≥ 22mA or ≤ 3.6mA based on 22/3.6 switch. Release button.
	d. Change the 22/3.6 DIP switch position. Press FAULT TEST push button and confirm: FAULT LED lights; Loop current ≥ 22mA or ≤ 3.6mA as expected. Release push button. Return 22/3.6 switch to original setting.

		e. Adjust the Time Delay Pot to maximum delay, fully clock-wise up to 25 turns. Change HI/LOW DIP switch position and observe the time delay from change of DIP switch until LED and Loop current change. Confirm delay is ~10 seconds. Change HI/LOW DIP switch back to original setting and confirm ~10 seconds delay. Adjust the Time Delay Pot to minimum delay, fully counter-clock-wise ~25 turns. Change HI/LOW DIP switch position and observe the time delay. Confirm delay ≤ 1 second. Change HI/LOW DIP switch back to original setting and confirm minimum delay.
4	When possible moving the process level will provide a more complete proof test.	
	Confirm proper operation of the unit: WET/DRY GAP condition; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.	
	a. Move the process level and confirm the GAP condition has changed. Confirm proper operation of the unit: WET/DRY GAP condition; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.	
	b. Move the process level and confirm the GAP condition has returned to orginal state. Confirm proper operation of the unit: WET/DRY GAP condition; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.	
	c. If unit fails the tests of steps 4.a or 4.b proceed to step 5.	
	d. Adjust the Time Delay Pot to the original setting recorded in step 3b. Use HI/LOW DIP switch (just as you did in step 3b) to confirm that delay is returned to original setting.	
	e. Proceed to step 6.	
5	If the unit under test fails to respond to process level changes remove the unit from the process and bench test.	
	a. Remove the unit from the process. Inspect the ultrasound transducer for evidence of damage or coating buildup. Fouling on the transducer surface may interfere with normal operation. If heavy fouling is evident, it is suggested to service the transducer more frequently.	
	b. Clean the ultrasonic transducer, especially in the area of the sensor GAP.	
	c. Perform a bench test per the steps of section 4. When possible, it is best to use the actual process material, because material properties affect the ultrasonic performance. Confirm proper unit operation: WET/DRY GAP condition; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.	
	d. If unit passes the tests of steps 5.c, return to the process installation and repeat the tests of step 4.	
	e. If the unit fails re-test in the process, it must be replaced.	
6	Proof test is complete. Restore loop to full operation.	

Table 21 Suggested Proof Test, 962 Loop

Step	Proof Test, Echotel Model 962 Loop
	(Refer to the Model 962 installation and operation manual and the SIL Safety Manual. Note the chart in the High/Low Dip Switch section of the I & O Manual.)
1	Bypass the PLC or take other action to avoid a false trip.
2	Inspect the Unit in detail outside and inside for physical damage or evidence of environmental or process leaks.
	a. Inspect the exterior of the Unit housing. If there is any evidence of physical damage that may impact the integrity of the housing and the environmental protection, the unit should be repaired or replaced.
	b. Inspect the interior of the Unit. Any evidence of moisture, from process or environment, is an indication of housing damage, and the unit should be repaired or replaced.
3	Observe and record the settings of the HI/LOW and 22/3.6 DIP switches, the LED indicators, Loop Current and Sensor GAP conditions (WET or DRY
	If the FAULT condition is indicated by loop current and LED indicators all OFF, diagnose the fault and repair or replace the unit.
	Confirm proper operation of the unit: WET/DRY GAP conditions; 8mA LED, 12mA or 16mA LED is lighted; Loop current = 8mA +/- 1mA, 12mA +/- 1mA or 16mA +/- 1 mA.
	a. Press LOOP TEST push button and confirm change; 8mA >> 12mA, 12mA >> 16mA or 16mA >> 8mA . Release the button and unit returns to proper operation.
	b. Change HI/LOW DIP switch position. Confirm both LED & Loop Current change state; 8mA >> 16mA or 16mA >> 8mA. Note that 12mA will stay at 12mA with the switch change. Observe and record the time delay from change of DIP switch until LED and Loop current change. Delay is set by Time Delay Pot, so the delay may take somewhere around 10 seconds. Press LOOP TEST push button and confirm change; 8mA >> 12mA, 12mA >> 16mA or 16mA >> 8mA. Release the button and unit returns to proper operation. Change HI/LOW DIP switch back to original setting and confirm proper operation, after the delay.
	c. Press FAULT TEST push button and confirm: all LEDs go OFF; Loop current ≥ 22mA or ≤ 3.6mA based on 22/3.6 switch. Release button.
	d. Change the 22/3.6 DIP switch position. Press FAULT TEST push button and confirm: all LEDs go OFF; Loop current ≥ 22mA or ≤ 3.6mA as expected. Release push button. Return 22/3.6 switch to original setting.

		e. Adjust the Time Delay Pot to maximum delay, fully clock-wise up to 25 turns. Change HI/LOW DIP switch position and observe the time delay from change of DIP switch until LED and Loop current change. Confirm delay is ~10 seconds. Change HI/LOW DIP switch back to original setting and confirm ~10 seconds delay. Adjust the Time Delay Pot to minimum delay, fully counter-clock-wise ~25 turns. Change HI/LOW DIP switch position and observe the time delay. Confirm delay ≤ 1 second. Change HI/LOW DIP switch back to original setting and confirm minimum delay.
	4	Move the process level to achieve three possible states: 1. both GAPs DRY, 2. one GAP DRY & one GAP WET, 3. Both GAPs WET. This test confirms operation with all GAP states.
		Confirm proper operation of the unit: WET/DRY GAP conditions; 8mA LED, 12mA or 16mA LED is lighted; Loop current = 8mA +/- 1mA, 12mA +/- 1mA or 16mA +/- 1 mA.
		a. Move the process level to achieve state 1. Both GAPS DRY. Confirm proper operation of the unit: WET/DRY GAP conditions; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.
		b. Move the process level to achieve state 2. one GAP DRY and one GAP WET. Confirm proper operation of the unit: WET/DRY GAP conditions; 12mA LED is lighted; Loop current = 12mA +/- 1mA.
		c. Move the process level to achieve state 3. Both GAPS WET. Confirm proper operation of the unit: WET/DRY GAP conditions; 8mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA or 16mA +/- 1 mA.
		c. If unit fails the tests of steps 4.a 4.b or 4.c proceed to step 5.
		d. Adjust the Time Delay Pot to the original setting recorded in step 3b. Use HI/LOW DIP switch (just as you did in step 3b) to confirm that delay is returned to original setting.
		e. Proceed to step 6.
	5	If the unit under test fails to respond to process level changes remove the unit from the process and bench test.
		a. Remove the unit from the process. Inspect the ultrasound transducer for evidence of damage or coating buildup. Fouling on the transducer surface may interfere with normal operation. If heavy fouling is evident, it is suggested to service the transducer more frequently.
		b. Clean the ultrasonic transducer, especially in the area of the sensor GAPs.
		c. Perform a bench test per the steps of section 4. When possible, it is best to use the actual process material, because material properties affect the ultrasonic performance. Confirm proper unit operation: WET/DRY GAP conditions; 8mA LED, 12mA LED or 16mA LED is lighted; Loop current = 8mA +/- 1mA, 12ma +/- 1mA or 16mA +/- 1 mA.

	d. If unit passes the tests of steps 5.c, return to the process installation and repeat the tests of step 4.
	e. If the unit fails re-test in the process, it must be replaced.
6	Proof test is complete. Restore loop to full operation.

B.3   Proof Test Coverage

The Proof Test Coverages for the various product configurations is given in Table 22 and Table 23.

Table 22 Proof Test Coverage – 961/962 Line Powered, Relay Output Version

Device	λ_{DU}PT (FIT)[6]	Proof Test Coverage
961 Dry Is Safe Redundant	30	87%
961 Wet Is Safe Redundant	50	78%
961 Dry Is Safe Non-redundant	55	93%
961 Wet Is Safe Non-redundant	76	84%
962 Dry Is Safe	60	75%
962 Wet Is Safe	96	72%

Table 23 Proof Test Coverage – 961/962 Loop Powered, Current Shift Version

Device	λ_{DU}PT (FIT)[6]	Proof Test Coverage
961 Dry Is Safe	10	20%
961 Wet Is Safe	27	63%
962 Dry Is Safe	10	70%
962 Wet Is Safe	47	87%

---

[6] This is the failure rate remaining after the proof test.

Appendix C *exida* Environmental Profiles

Table 24 *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	
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	N/A
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 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. See Figure 2.

Figure 2: exSILentia results for idealistic variables.

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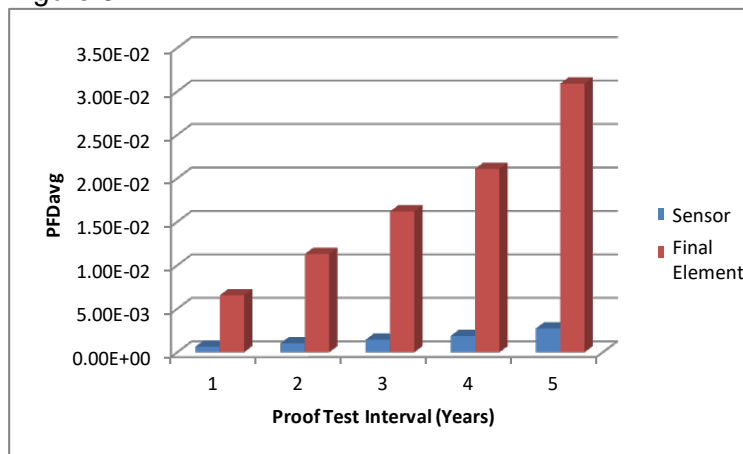

Figure 3 PFD$_{avg}$ versus Proof Test Interval.

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

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

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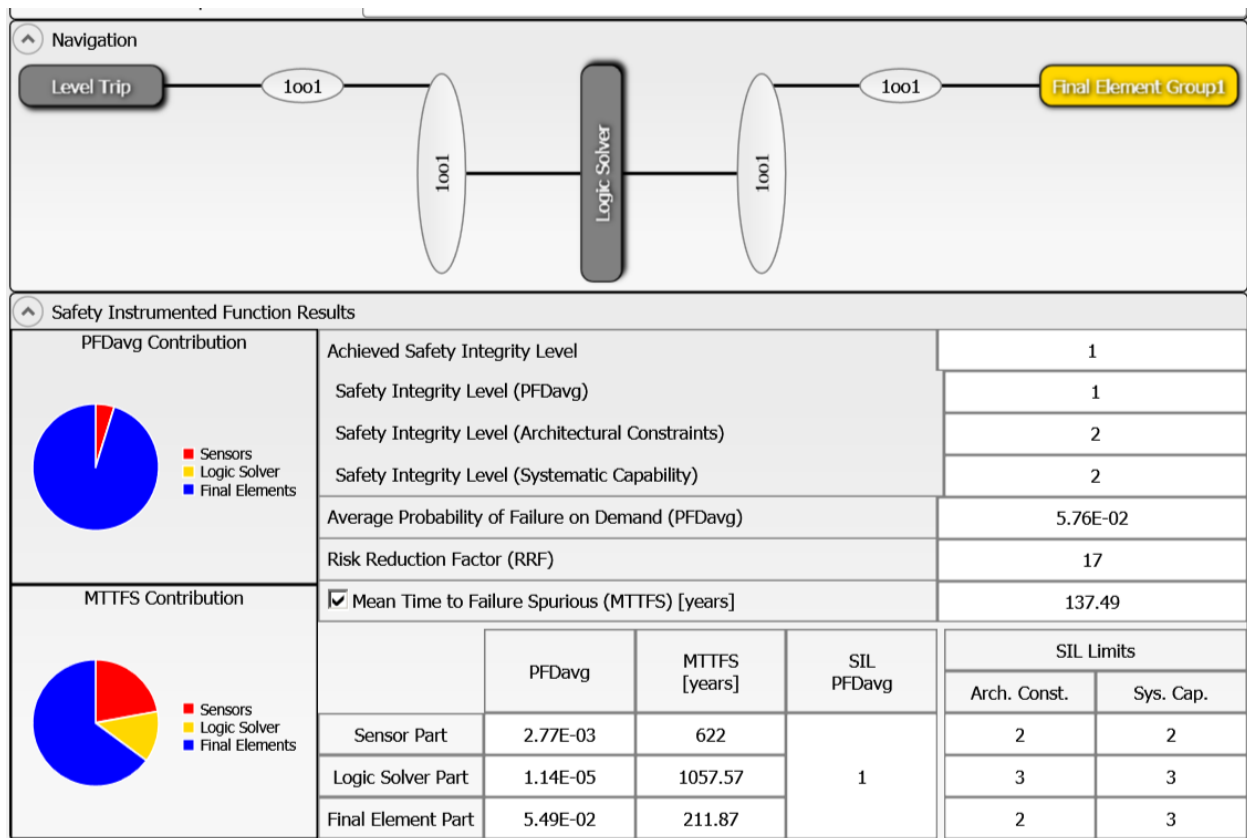
Figure 4: exSILentia results with realistic variables

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 25 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 25 *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 – 961/962

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 26 lists the failure rates for the Line Powered, Relay Output Version 961/962 according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 26 Failure rates with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
961 Dry Is Safe Redundant	237	167	25	27
961 Wet Is Safe Redundant	14	149	248	45
961 Dry Is Safe Non-redundant	237	179	25	50
961 Wet Is Safe Non-redundant	14	160	248	68
962 Dry Is Safe	406	203	35	54
962 Wet Is Safe	22	167	419	86

NOTE: The Loop Powered, Current Shift Version was not in scope or calculated @ SSI =4 for this project.