Failure Modes, Effects and Diagnostic Analysis

Project:
FP15 & FP15E Low and High Pressure Pilot Interface Valves

Company:
Bifold Fluidpower Ltd.
Chadderton, Greater Manchester
UK

Contract Number: Q23/09-025
Report No.: BIF 16/10-005 R005
Version V1, Revision R6, November 14, 2023
Oluwatobi Falomo

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 FP15 & FP15E Low and High Pressure Pilot Interface Valves. 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 FP15 and FP15E Interface Valves. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

FP15 and FP15E Low Pressure Interface Valves take a low pressure (up to 10 bar) Pilot pressure signal to control the flow of a high pressure (up to 690 bar for the Hydraulic models and 150 bar for Gas models) hydraulic/gas line that typically is connected to a final control elements valve actuator. Similarly, the FP15 and FP15E High Pressure Interface Valves take a high pressure (up to 690 bar) signal to control the flow. This analysis is for the case where the safety function is when the pilot pressure is vented, the interface valve moves to the normally closed state and the Service port is opened to the Tank port.

Table 1 gives an overview of the different versions that were considered in this FMEDA of the FP15 and FP15E.

Table 1 Version Overview

FP15 and FP15E	3 Port, 2 Position Normally Closed/Open, Low or High Pressure Pilot Interface Valve, Hydraulic or Gas Service
FP15 and FP15E	3 Port, 2 Position Normally Closed/Open, Low or High Pressure Pilot Interface Valve, Hydraulic or Gas Service, with PVST

The FP15 and FP15E are classified as devices that are part of a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. See Section 5.2. Therefore, the FP15 and FP15E 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 final element, the architectural constraints will need to be evaluated per Route 1_H.

Based on the assumptions listed in 4.3, the failure rates for the FP15 and FP15E 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 FP15 and FP15E can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

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

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the FP15 and FP15E. 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, 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

Bifold Fluidpower Ltd.	Manufacturer of the FP15 and FP15E
exida	Performed the hardware assessment

Bifold Fluidpower Ltd. contracted *exida* in October 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]	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)
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[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,	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	http://www.exida.com/Resources/Whitepapers/random-versus-systematic-failures-issues-and-solutions
[N10]	Bukowski, J.V. and Chastain-Knight, D., April 2016	Assessing Safety Culture via the Site Safety Index™, Proceedings of the AIChE 12th Global Congress on Process Safety, GCPS2016, TX: Houston
[N11]	Bukowski, J.V. and Stewart, L.L., April 2016	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
[N12]	Criteria for the Application of IEC 61508:2010 Route 2H, December 2016	*exida* White Paper, Sellersville, PA www.exida.com
[N13]	Goble, W.M. and Brombacher, A.C., November 1999, Vol. 66, No. 2	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.

2.4 Reference documents

2.4.1 Documentation provided by Bifold Fluidpower Ltd.

[D1]	A1106, Rev 1, 18-Oct-12	FP15E/L1/04/32/X-MSO-03 Assy Dwg
[D2]	A1121, Rev 0, 13-Dec-12	FP15/H2/06/22/X3MSO Assy Dwg
[D3]	A1501, Rev 0, 1-Sep-16	FP15/L1A/04/32/X-G Assy Dwg
[D4]	fp15_fp15e, Jan 2013	FP15 Interface Valves, Product Brochure
[D5]	A1043, Rev 1	FP15/L1/04/22/X-H2S-03 Assy Dwg
[D6]	A1120, Rev 1	FP15/L1/0X/32/X-03 Assy Dwg
[D7]	A1138, Rev 0	FP15E/L2/04/32/X-NO-03 Assy Dwg
[D8]	A1256, Rev 0	FP15/H1A/M/22/X – NO Assy Dwg

2.4.2 Documentation generated by *exida*

[R1]	Bifold FP15E FMEDA R4.xls, 12-Oct-17	Failure Modes, Effects, and Diagnostic Analysis – FP15 and FP15E (internal document)
[R2]	Bifold FP15E-Hyd QEV ETT_NO FMEDA R1.xls, 14-Nov-23	Failure Modes, Effects, and Diagnostic Analysis – FP15 and FP15E – ETT and NO Failure Modes (internal document)
[R3]	BIF 16/10-005 R005, V1R6, 14-Nov-23	FMEDA report, FP15 & FP15E Low and High Pressure Pilot Interface Valves (this report)

3 Product Description

The FP15 and FP15E Low Pressure Interface Valves take a low pressure (up to 10 bar) Pilot pressure signal to control the flow of a high pressure (up to 690 bar for the Hydraulic models and 150 bar for Gas models) hydraulic/gas line that typically is connected to a final control elements valve actuator. Similarly, the FP15 and FP15E High Pressure Interface Valves take a high pressure (up to 690 bar) signal to control the flow.

These valves are available in a variety of configurations. Included in this analysis are ¼” and ⅜” body ported models, 3 port 2 position Normally Closed, different O-Ring materials and an optional Manual Screw down Override. This analysis is for the case where the safety function is when the pilot pressure is vented, the interface valve moves to the normally closed state and the Service port is opened to the Tank port.

Note: the SIF designer is responsible for determining if the optional Override functions are suitable for the application. The end user qualified personnel are responsible for determining if it is safe to manually Override the Valves position.

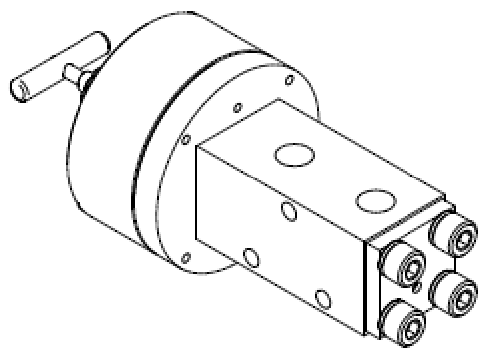


Figure 1 Typical FP15 and FP15E covered in this FMEDA,

Table 2 gives an overview of the different versions that were considered in the FMEDA of the FP15 and FP15E.

Table 2 Version Overview

FP15 and FP15E	3 Port, 2 Position Normally Closed, Low or High Pressure Pilot Interface Valve, Hydraulic or Gas Service
FP15 and FP15E	3 Port, 2 Position Normally Closed, Low or High Pressure Pilot Interface Valve, Hydraulic or Gas Service with PVST

The FP15 and FP15E valves are classified as devices that are part of a Type A[2] element according to IEC 61508, having a hardware fault tolerance of 0.

[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 FP15 and FP15E, the following definitions for the failure of the device were considered.

Fail-Safe State:	State where the Pilot pressure is de-energized and the valve moves to the normally closed state where the Service port is vented to the Tank port.
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).
Valve	Failure that prevents the valve from moving to the defined fail-safe state within the normal time span.
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.
External Leakage	Failure that causes gas, hydraulic fluids or operating media to leak outside of the valve; External Leakage is not considered part of the safety function and therefore this failure rate is not included in the Safe Failure Fraction calculation.

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.

External leakage failure rates do not directly contribute to the reliability of the device but should be reviewed for secondary safety and environmental issues.

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 was 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 5 (Offshore Equipment) as this was judged to be the best fit for the product and application information submitted by Bifold Fluidpower Ltd.. 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 ([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 the 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 FP15 and FP15E.

- A single component failure will fail the entire FP15 and FP15E, therefore propagation of failures is not relevant.
- Failure rates are constant; wear-out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.

- Failures caused by the operational / maintenance culture are site specific and modeled by the Site Safety index (SSI). Failure rates are presented for an average realistic level (SSI=2) and for comparison purposes at an ideal level, SSI=4.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 5 (Offshore Equipment) with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Materials are compatible with the environmental and process conditions.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- Clean and filtered hydraulic fluid is used per the manufacturer's recommendations and requirements.
- The device is installed per the manufacturer's instructions.
- Breakage or plugging of air / hydraulic inlet and outlet lines has not been included in the analysis.
- Loss of the Air Pressure supply is not included in these failure rates.
- Loss of the hydraulic supply pressure due to causes outside of the device is not included in these failure rates.
- Valves with Override options are only used in applications where the use of the Override will not put the system in a dangerous condition.
- In order to claim diagnostic coverage for Partial Valve Stroke Testing it is automatically performed at a rate at least ten times faster than the Proof Test frequency.
- Partial Valve Stroke Testing of the Safety Instrumented Function provides a full cycle test of the solenoid/pilot valve. In cases where this is not true, another method must be used to perform a full Valve cycle during automated diagnostics in order to use the PVST numbers.
- Partial Valve Stroke Testing of the final element includes position detection from actuator top mounted position sensors, typical of quarter turn installations.
- Worst-case internal fault detection time is the PVST test interval time.

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 FP15 and FP15E.

Table 3 and Table 4 lists the failure rates for the FP15 and FP15E 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	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}	#	E
FP15 & FP15E NC, DTT	0	129	0	141	694	395
FP15 & FP15E NC, DTT with PVST	124	5	127	14	694	395
FP15 & FP15E NC, ETT	0	27	0	242	694	395
FP15 & FP15E NO, ETT	0	56	0	209	710	395
FP15 & FP15E NC, ETT with PVST	24	3	225	17	694	395
FP15 & FP15E NO, ETT with PVST	12	44	195	14	710	395

Table 4 Failure rates for Dynamic Applications[5] with Good Maintenance Assumptions in FIT (SSI=2)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
FP15 & FP15E NC, DTT	0	142	0	79	799	424
FP15 & FP15E NC, DTT with PVST	136	6	71	8	799	424
FP15 & FP15E NC, ETT	0	28	0	195	799	424
FP15 & FP15E NC, ETT with PVST	25	3	183	12	799	424

Where:

λ_{SD} = Fail Safe Detected

λ_{SU} = Fail Safe Undetected

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

= No Effect Failures

E = External Leaks

As the External Leak failure rates are a subset of the No Effect failure rates, the total No Effect failure rate is the sum of the listed No Effect and External Leak rates. External leakage failure rates do not directly contribute to the reliability of the device but should be reviewed for secondary safety and environmental issues.

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, 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.

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

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 FP15 and FP15E 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.

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 FP15 and FP15E 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 and Table 10 lists the failure rates for the FP15 and FP15E 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.

5 Using the FMEDA Results

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

5.1 PFD_{avg} calculation FP15 and FP15E

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 final 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 final 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 final element and the proof test coverage for the final 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 FP15 and FP15E are listed in Table 6. This is combined with the dangerous failure rates after proof test for other devices in the final element to establish the proof test coverage for the final element.

When performing Partial Valve Stroke Testing at regular intervals, the FP15 and FP15E contributes less to the overall PFD_{avg} of the Safety Instrumented Function.

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.
Element	A collection of devices that perform an element safety function such as a final element consisting of a logic solver interface, actuator and valve.
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, R6:	Added Normally Open application failure rates; November 14, 2023
	V1, R5:	Added ETT application failure rates; July 13, 2023
	V1, R4:	Added Gas Service models; October 13, 2017
	V1, R3:	Added Dynamic failure rate data; October 6, 2017
	V1, R2:	Added High Pressure Pilot models; October 26, 2016
	V1, R1:	Released to Bifold Fluidpower Ltd.; October 25, 2016
	V0, R1:	Draft; October 21, 2016
Author(s):	Oluwatobi Falomo	
Review:	V1, R6:	Robert Gavin (*exida*); November 29, 2023
	V1, R5:	Steven Close (*exida*); July 13, 2023
	V1, R3:	Steven Close (*exida*); October 10, 2017
	V0, R1:	Steven Close (*exida*); October 24, 2016
Release Status:	Released to Bifold Fluidpower Ltd.	

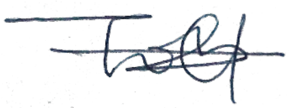
7.3 Future enhancements

At request of client.

7.4 Release signatures

Steven Close, Senior Safety Engineer

Robert Gavin III, MSME, CFSE,
Senior Safety Engineer



Oluwatobi Falomo, 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[6] 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 FP15 and FP15E per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

A major factor influencing the useful life is the air quality / quality of the hydraulic oil used.

Based on general field failure data a useful life period of approximately 15 years is expected for the FP15 and FP15E.

For high demand mode applications, the useful lifetime is limited by the number of cycles. The useful lifetime is > 10,000 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.

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

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The suggested Proof Test consists of a full stroke of the associated device, see Table 5. Refer to the table in B.2 for the Proof Test Coverages.

Table 5 Suggested Proof Test – FP15 and FP15E

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the air supply/input to the Interface Valve to force the Actuator/ Valve assembly to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time. Note:-This tests for all failures that could prevent the functioning of the Interface Valve as well as the rest of the final control element.
3.	Inspect the Valve for any leaks, visible damage or contamination
4.	Re-store the original air supply/input to the Interface Valve and confirm that the normal operating state was achieved.
5.	Remove the bypass and otherwise restore normal operation.

For the test to be effective the movement of the Valve must be confirmed. To confirm the effectiveness of the test both the travel of the Final Element Valve and slew rate must be monitored and compared to expected results to validate the testing.

B.2 Proof Test Coverage

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

Table 6 Proof Test Results – FP15 and FP15E

Device / Application	λ_{DU}PT[7] (FIT)	Proof Test Coverage	
		No PVST	with PVST
FP15 and FP15E Low or High Pressure Pilot, DTT, Static	3.7	97%	74%
FP15 and FP15E Low or High Pressure Pilot, DTT, Dynamic	1.4	98%	83%
FP15 and FP15E Low or High Pressure Pilot, ETT, Static	4.8	98%	72%
FP15 and FP15E Low or High Pressure Pilot, ETT, Dynamic	2.6	98%	78%

[7] **λ_{DU}PT** = Dangerous undetected failure rate after performing the recommended proof test.

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[8]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[9]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[10]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[11]	G2	G3	G3	G3	G3	Compatible Material
Surge[12]						
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[13]						
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)[14]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

---

8 Humidity rating per IEC 60068-2-3
9 Shock rating per IEC 60068-2-27
10 Vibration rating per IEC 60068-2-6
11 Chemical Corrosion rating per ISA 71.04
12 Surge rating per IEC 61000-4-5
13 EMI Susceptibility rating per IEC 61000-4-3
14 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}) must be done based on a number of variables including:

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

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

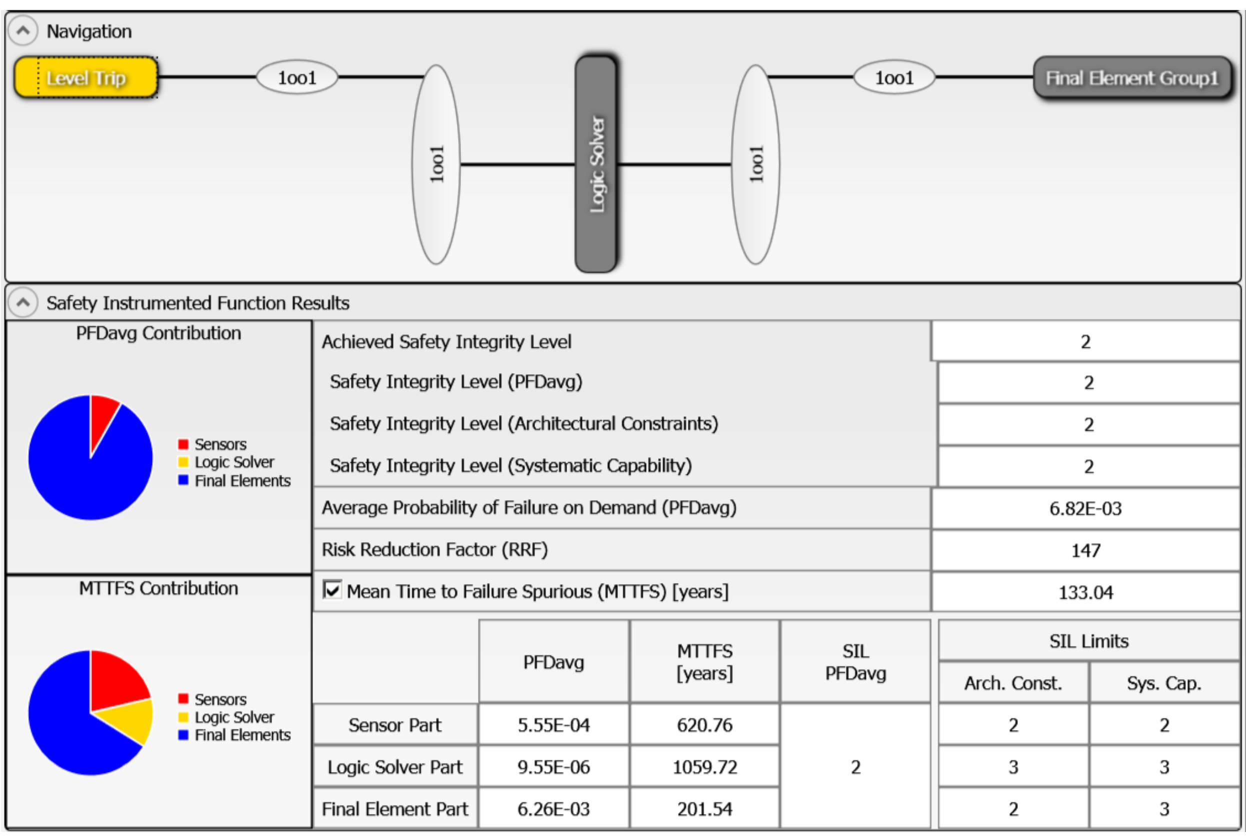
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic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

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

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

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

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



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

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

Figure 2: exSILentia results for idealistic variables.

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

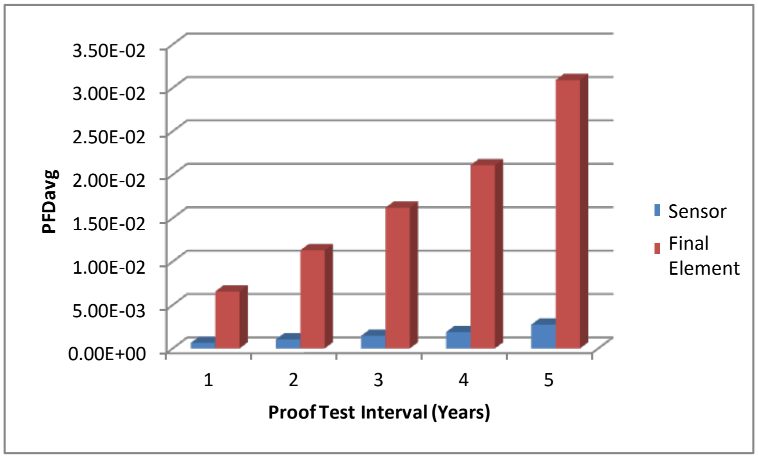
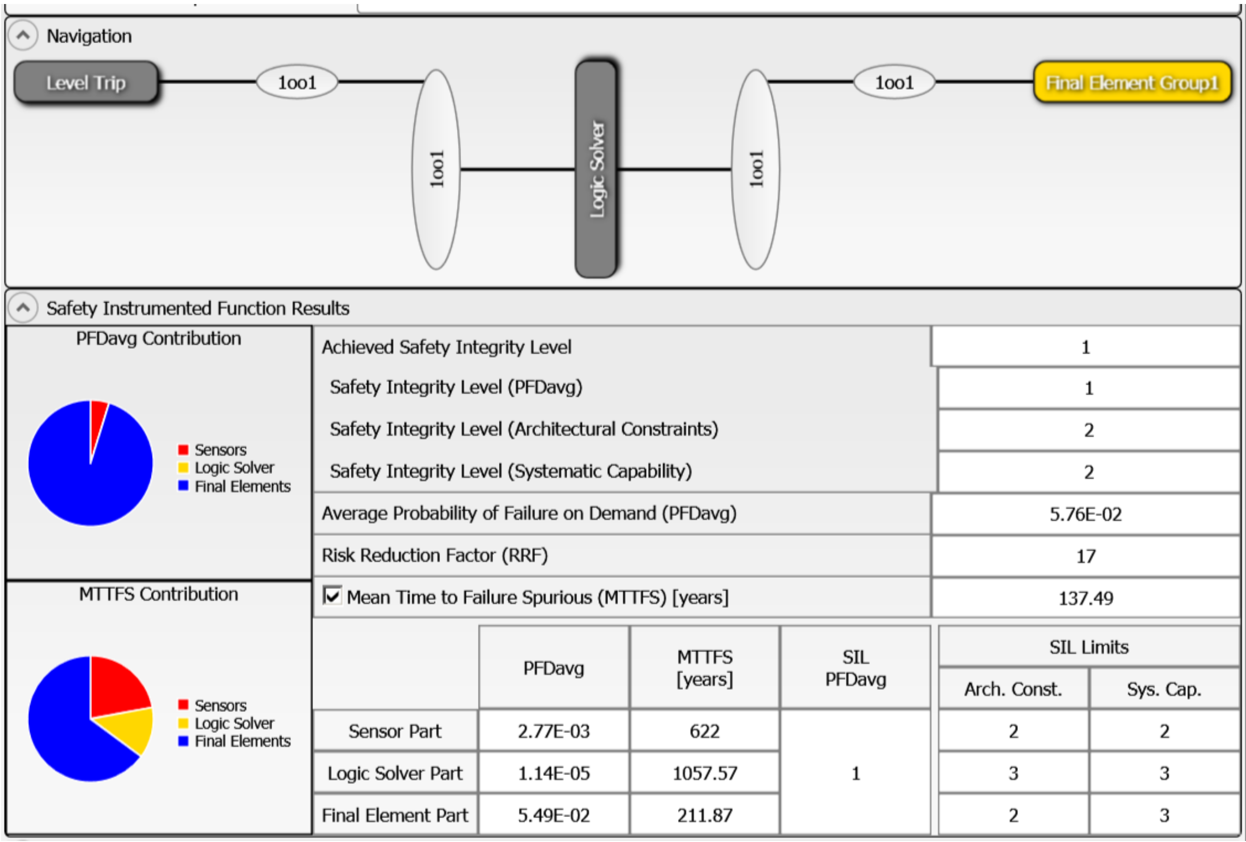


Figure 3: PFD_{avg} versus Proof Test Interval

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).



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

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

Figure 4: exSILentia results with realistic variables

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

Appendix E Site Safety Index

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

E.1 Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 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 – FP15 and FP15E

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 9 lists the failure rates for the FP15 and FP15E according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 9 Failure rates for Static Applications[15] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}[16]	λ_{DD}	λ_{DU}	#	E
FP15 & FP15E NC, DTT	0	77	0	71	416	237
FP15 & FP15E NC, DTT with PVST	74	3	64	7	416	237
FP15 & FP15E NC, ETT	0	16	0	121	416	237
FP15 & FP15E NO, ETT	0	34	0	105	426	237
FP15 & FP15E NC, ETT with PVST	14	2	112	9	416	237
FP15 & FP15E NO, ETT with PVST	7	26	98	7	426	237

Table 10 Failure rates for Dynamic Applications[17] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
FP15 & FP15E NC, DTT	0	85	0	40	479	254
FP15 & FP15E NC, DTT with PVST	81	4	36	4	479	254
FP15 & FP15E NC, ETT	0	17	0	98	479	254
FP15 & FP15E NC, ETT with PVST	15	2	92	6	479	254

[15] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[16] 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.
[17] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.