Failure Modes, Effects and Diagnostic Analysis

Project:
FP01, FP02, FP03, FP04, FP05, FP02G, FP05G,
FP03P, FP06P, FP10P and FP15 Solenoid Valves

Company:
Bifold Fluidpower Ltd.
Chadderton, Greater Manchester
UK

Contract Number: Q23/09-025
Report No.: BIF 17/05-128 R001
Version V1, Revision R6, January 12, 2024
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 FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Solenoid 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 FP Solenoid Valves. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

Table 1 gives an overview of the different versions and options that were considered in this FMEDA of the FP Solenoid Valves.

Note: the SIF designer is responsible for determining if any Latching and/or Override functions that a Valve may have is suitable for the application. The end user qualified personnel are responsible for determining if it is safe to manually Latch/Unlatch or Override the Valves position.

Table 1 Version Overview

FP01, FP02, FP03, FP04 and FP05	3 Port, 2 Position Normally Closed/Open Direct-Acting Hydraulic Solenoid Valves, De-Energize to Trip (DTT) Applications
FP02G and FP05G	3 Port, 2 Position Normally Closed/Open Solenoid Valve for Gas Service, De-Energize to Trip (DTT) Applications
FP03P, FP06P and FP10P	3 Port, 2 Position Normally Closed/Open Direct-Acting Pneumatic Solenoid Valves, De-Energize to Trip (DTT) Applications
FP15	3 Port, 2 Position Normally Closed/Open 2 Stage Hydraulic Solenoid Valve, De-Energize to Trip (DTT) Applications
Options Included for the above Models:	Single Type 74, 77 and 78 or Type 58 Solenoid Operator DC or AC (Wiring Option 1) Coil power up to 10W Up to 690 Bar Max Working Pressure Spring Return and Detented Manual Override

The FP Solenoid Valves 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 FP Solenoid Valves 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 FP Solenoid Valves are listed in section 4.4.

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

---

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

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

A user of the FP Solenoid Valves 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 FP Solenoid Valves. 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

Bifold Fluidpower Ltd.   Manufacturer of the FP Solenoid Valves

exida   Performed the hardware assessment

Bifold Fluidpower Ltd. 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]	Mechanical Component Reliability Handbook, 4th Edition, 2016	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2016 (pending publication, not publicly 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]	0-SC0003, Rev 9, 07-Apr-17	Type 27 & 77 Exd Solenoid Operator Assy Dwg
[D2]	0-SC0004, Rev 0, 22-Apr-09	Solenoid Lid Options Assy Dwg
[D3]	0-SC0008, Rev 1, 29-Mar-11	Override Cover Assy Assy Dwg
[D4]	A0897, Rev 2, 13-Dec-11	FP01/SX/M/32/NC/X-7X Assy Dwg
[D5]	A1406, Rev 0, 19-Jan-16	FP0X/XX/M/32/X-04 Assy Dwg
[D6]	0-GA0326, Rev 1, 5-Jul-11	Type 58 Solenoid Assy Dwg
[D7]	BFD87, Nov 2013	Model FP01 Solenoid Valves, Product Brochure
[D8]	0-GA0186, Rev 1, 17-Jun-09	FP06P-S1-M7-32-NC-X-XX-01 Assy Dwg
[D9]	0-GA0268, Rev 0, 26-Apr-10	FP10P-S1-04-32-NU-X-XX-02 Assy Dwg
[D10]	A0994, Rev 3, 28-Nov-13	FP05 Gas Service Assy Dwg
[D11]	A0463, Rev 1, 4-Nov-08	FP15/SX/0X/32/X - 97X Assy Dwg
[D12]	OPB.0034, Rev 3, 9-May-16	Type 58 Series Solenoid Operator, Installation Manual
[D13]	A1205, Rev 0, 8-Nov-13	FP02 Gas Service Assy Dwg
[D14]	06 - FP15 Solenoid.pdf	Brochure, Solenoid Valve Model FP15
[D15]	09 - FP06P-FP10P-FP12P.pdf	Brochure, Direct Acting Solenoid Valve Models FP06P, FP10P & FP12P

[D16]	06 - FP15 Solenoid.pdf	Brochure, Solenoid Valve Model FP15
[D17]	A1885, Rev 0	FP0X/SX/M/32/SV/X/LCF Assy Dwg
[D18]	A1256, Rev 0	FP15/H1A/M/22/X – NO Assy Dwg
[D19]	A1881, Rev 0	FP0X/SX/M/32/NC/X/LCF Assy Dwg
[D20]	A1883, Rev 0	FP0X/SX/M/32/NO/X/LCF Assy Dwg
[D21]	A1043, Rev 1	FP15/L1/04/22/X-H2S-03 Assy Dwg
[D22]	A1120, Rev 1	FP15/L1/0X/32/X-03 Assy Dwg
[D23]	A1138, Rev 0	FP15E/L2/04/32/X-NO-03 Assy Dwg

2.4.2 Documentation generated by *exida*

[R1]	Bifold FP Solenoids FMEDA R2_3.xlsx, 14-Nov-2023	Failure Modes, Effects, and Diagnostic Analysis – FP Solenoid Valves (internal document)

3   Product Description

The Bifold Fluidpower Ltd. FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Solenoid Valves are three-way, 3 port / 2 position Solenoid operated Valves.

Table 2 gives an overview of the different versions and options that were considered in the FMEDA of the FP Solenoid Valves. Models included in this analysis are devices with a single Type 74, 77 and 78 or Type 58 Solenoid (up to 10W) with a DC Coil or AC Coil (Wiring Option 1). Only De-energize to Trip applications have been evaluated in this FMEDA. The failure rates in this report also include the optional Spring Return Manual Override, Detented Manual Override and the Manual Reset Cover Assembly.

Note: the SIF designer is responsible for determining if any Latching and/or Override functions that a Valve may have is suitable for the application. The end user qualified personnel are responsible for determining if it is safe to manually Latch/Unlatch or Override the Valves position.

Figure 1 Typical FP Solenoid Valves covered in this FMEDA

Table 2 Version Overview

FP01, FP02, FP03, FP04 and FP05	3 Port, 2 Position Normally Closed/Open Direct-Acting Hydraulic Solenoid Valves, De-Energize to Trip (DTT) Applications
FP02G and FP05G	3 Port, 2 Position Normally Closed/Open Solenoid Valve for Gas Service, De-Energize to Trip (DTT) Applications
FP03P, FP06P and FP10P	3 Port, 2 Position Normally Closed/Open Direct-Acting Pneumatic Solenoid Valves, De-Energize to Trip (DTT) Applications
FP15	3 Port, 2 Position Normally Closed/Open 2 Stage Hydraulic Solenoid Valve, De-Energize to Trip (DTT) Applications
Options Included for the above Models:	Single Type 74, 77 and 78 or Type 58 Solenoid Operator DC or AC (Wiring Option 1) Coil power up to 10W Up to 690 Bar Max Working Pressure Spring Return and Detented Manual Override

The FP Solenoid 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 FP Solenoid Valves, the following definitions for the failure of the device were considered.

Fail-Safe State:	State where the solenoid is de-energized and Service port pressure is released.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics, such as Partial Valve Stroke Testing.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics, such as Partial Valve Stroke Testing.
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
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 any of the numbers. External leakage failure rates should be reviewed for secondary safety and environmental issues.

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.

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 in each application. 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].

4.2.2 Failure rates

The accuracy of any FMEDA analysis depends upon the component reliability data as input to the process. Component data from consumer, transportation, military or telephone applications could generate failure rate data unsuitable for the process industries. The component data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] which were derived using over 350-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 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 FP Solenoid Valves.

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

- Failure rates are constant for the useful life period.

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

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

- Materials are compatible with the environmental and process conditions.

- 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 and operated 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 Valve is not included in these failure rates.

- Valves with Latching and/or Override options are only used in applications where the use of the Latching and/or 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 Demand 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 FP Solenoid Valves.

Table 3 thru Table 6 lists the failure rates for the FP Solenoid Valves 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 DTT Failure rates for Static Applications[3] with Good Maintenance Assumptions in FIT (SSI=2)

Device/Application/Configuration	λ_{SD}	λ_{SU}[4]	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT	0	179	0	137	450	193
FP03P, FP06P and FP10P; NC, DTT	0	142	0	104	270	199
FP15; NC, DTT	0	266	0	227	933	250
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT; with automated PVST	172	7	122	15	450	193
FP03P, FP06P and FP10P; NC, DTT; with automated PVST	135	7	92	12	270	199
FP15; NC, DTT; with automated PVST	258	8	203	24	933	250
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT	0	128	0	183	440	193
FP03P, FP06P and FP10P; NO, DTT	0	125	0	117	259	199
FP15; NO, DTT	0	163	0	325	938	251
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT; with automated PVST	122	6	163	20	440	193
FP03P, FP06P and FP10P; NO, DTT; with automated PVST	119	6	103	14	259	199
FP15; NO, DTT; with automated PVST	156	7	290	35	938	251

---

[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.

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

Device/Application/Configuration	λ_{SD}	λ_{SU}[6]	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT	0	36	0	274	440	193
FP03P, FP06P and FP10P; NC, ETT	0	30	0	212	259	199
FP15; NC, ETT	0	106	0	381	938	251
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT; with automated PVST	29	7	257	17	440	193
FP03P, FP06P and FP10P; NC, ETT; with automated PVST	23	7	199	13	259	199
FP15; NC, ETT; with automated PVST	95	11	356	25	938	251
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT	0	104	0	207	440	193
FP03P, FP06P and FP10P; NO, ETT	0	72	0	170	259	199
FP15; NO, ETT	0	157	0	335	933	251
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT; with automated PVST	98	6	191	15	440	193
FP03P, FP06P and FP10P; NO, ETT; with automated PVST	66	6	158	12	259	199
FP15; NO, ETT; with automated PVST	150	7	307	28	933	251

---

[5] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[6] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

Table 5 DTT Failure rates for Dynamic Applications[7] with Good Maintenance Assumptions in FIT (SSI=2)

Device/Application/Configuration	λ_{SD}	λ_{SU}[8]	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT	0	181	0	90	475	203
FP03P, FP06P and FP10P; NC, DTT	0	145	0	75	281	214
FP15; NC, DTT	0	273	0	147	994	271
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT; with automated PVST	174	7	79	11	475	203
FP03P, FP06P and FP10P; NC, DTT; with automated PVST	138	7	66	9	281	214
FP15; NC, DTT; with automated PVST	264	9	130	17	994	271
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT	0	127	0	140	463	193
FP03P, FP06P and FP10P; NO, DTT	0	127	0	89	268	214
FP15; NO, DTT	0	162	0	249	987	261
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT; with automated PVST	121	6	124	16	463	193
FP03P, FP06P and FP10P; NO, DTT; with automated PVST	121	6	78	11	268	214
FP15; NO, DTT; with automated PVST	155	7	222	27	987	261

---

[7] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.
[8] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

Table 6 ETT Failure rates for Dynamic Applications[9] with Good Maintenance Assumptions in FIT (SSI=2)

Device/Application/Configuration	λ_{SD}	λ_{SU}[10]	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT	0	36	0	231	463	193
FP03P, FP06P and FP10P; NC, ETT	0	31	0	185	269	214
FP15; NC, ETT	0	107	0	304	987	261
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT; with automated PVST	28	8	218	13	463	193
FP03P, FP06P and FP10P; NC, ETT; with automated PVST	24	7	175	10	269	214
FP15; NC, ETT; with automated PVST	96	11	286	18	987	261
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT	0	107	0	160	463	193
FP03P, FP06P and FP10P; NC, ETT	0	75	0	141	269	214
FP15; NO, ETT	0	161	0	254	982	261
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT; with automated PVST	101	6	150	10	463	193
FP03P, FP06P and FP10P; NO, ETT; with automated PVST	69	6	132	9	269	214
FP15; NO, ETT; with automated PVST	154	7	234	20	982	261

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.

---

[9] Dynamic Application failure rates may be used if the device moves at least once every 200 hours.
[10] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.

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

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

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 FP Solenoid Valves 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 FP Solenoid Valves 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 12 and Table 14 lists the failure rates for the FP Solenoid Valves according to IEC 61508 with a Site Safety Index (SSI) of 4 (perfect site maintenance practices). This data should not be used for SIL verification and is provided only for comparison with other analysis than has assumed perfect maintenance. See Appendix E for an explanation of SSI.

5 Using the FMEDA Results

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

5.1 PFD$_{avg}$ calculation FP Solenoid Valves

Using the failure rate data displayed in Table 3, section 4.4, and the failure rate data for the associated element devices, an average 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 FP Solenoid Valves are listed in Appendix B.2. 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 FP Solenoid Valves 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 undertaking 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.

© *exida*
T-126 V3,R5

BIF 17-05-128 R001 V1R6 FMEDA Report FP Solenoid Valves.docx
exida 80 N. Main St, Sellersville, PA 18960   Page 20 of 37

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 (1×10^{-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 Version History

Note: This report supersedes all previous versions of report BIF 06/01-17 R001

Contract Number	Report Number	Revision Notes
Q23/09-025	BIF 17/05-128 R001 V1, R6	Updated version overview, Added type 74 and 78, January 12, 2024, TBF
Q23/09-025	BIF 17/05-128 R001 V1, R5	Added NO failure rates, November 13, 2023, TBF
Q22/11-167	BIF 17/05-128 R001 V1, R4	Added ETT failure rates, July 13, 2023, REG
Q21/03-178	BIF 17/05-128 R001 V1, R3	Analyzed stainless steel gauze filter; GPS
Q17/05-128	BIF 17/05-128 R001 V1, R2	Added FP02G, October 13, 2017
Q17/05-128	BIF 17/05-128 R001 V1, R1	Updated FMEDA analysis and added Dynamic failure rates

Reviewer: V1, R5: Bob Gavin, *exida*, November 14, 2023
Status: Released, November 14, 2023

7.3 Future enhancements

At request of client.

7.4   Release signatures

_____
Oluwatobi Falomo, Safety Engineer

_____
Robert Gavin III, MSME, CFSE,
Senior Safety Engineer

Appendix A   Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2.2) this only applies provided that the useful lifetime[11] 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 FP Solenoid Valves 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 10 years is expected for the FP Solenoid Valves.

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.

---

[11] 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 7. Refer to the tables in B.2 for the Proof Test Coverages.

Table 7 Suggested Proof Test – FP Solenoid Valves

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the signal to De-energize the Solenoid and 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 Control Valve as well as the rest of the final control element.
3.	Inspect the Solenoid Valve for any leaks, visible damage or contamination
4.	Re-store the original input to the Solenoid 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 Final Element Valve must be confirmed. To confirm the effectiveness of the test both the travel of the 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 8 and in Table 9 for Dynamic Applications.

Table 8 Proof Test Results – Static Applications FP Solenoid Valves

Device / Application	$\lambda_{DU}PT^{12}$ (FIT)	Proof Test Coverage	
		No PVST	with PVST
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; DTT	9.6	93%	36%
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; ETT	11	96%	36%
FP03P, FP06P and FP10P; DTT	6.6	94%	45%
FP03P, FP06P and FP10P; ETT	7.7	96%	41%
FP15; DTT	15	93%	38%
FP15; ETT	17	96%	33%

Table 9 Proof Test Results – Dynamic Applications FP Solenoid Valves

Device / Application	$\lambda_{DU}PT^{13}$ (FIT)	Proof Test Coverage	
		No PVST	with PVST
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; DTT	5.1	94%	54%
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; ETT	6.6	97%	50%
FP03P, FP06P and FP10P; DTT	3.6	95%	60%
FP03P, FP06P and FP10P; ETT	4.7	97%	54%
FP15; DTT	7.2	95%	58%
FP15; ETT	8.8	97%	50%

---

[12] $\lambda_{DU}PT$ = Dangerous undetected failure rate after performing the recommended proof test.

[13] $\lambda_{DU}PT$ = Dangerous undetected failure rate after performing the recommended proof test.

Appendix C *exida* Environmental Profiles

Table 10 *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[14]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[15]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[16]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[17]	G2	G3	G3	G3	G3	Compatible Material
Surge[18]						
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[19]						
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)[20]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

---

[14] Humidity rating per IEC 60068-2-3
[15] Shock rating per IEC 60068-2-27
[16] Vibration rating per IEC 60068-2-6
[17] Chemical Corrosion rating per ISA 71.04
[18] Surge rating per IEC 61000-4-5
[19] EMI Susceptibility rating per IEC 61000-4-3
[20] ESD (Air) rating per IEC 61000-4-2

© *exida*
T-126 V3,R5

BIF 17-05-128 R001 V1R6 FMEDA Report FP Solenoid Valves.docx
exida 80 N. Main St, Sellersville, PA 18960   Page 28 of 37

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 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 the 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).

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

Additional results displayed in figure:

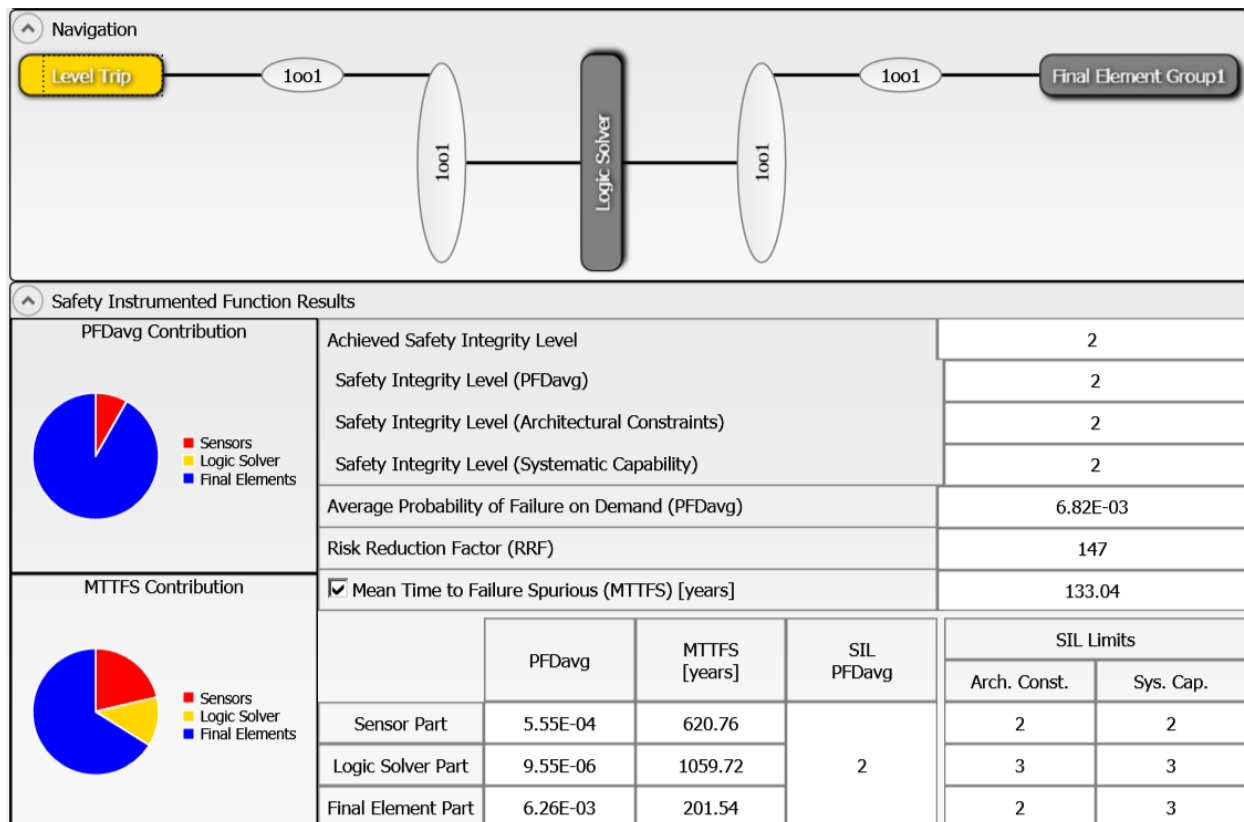| Achieved Safety Integrity Level	2
Safety Integrity Level (PFDavg)	2
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	6.82E-03
Risk Reduction Factor (RRF)	147
Mean Time to Failure Spurious (MTTFS)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

Figure 2: exSILentia results for idealistic variables

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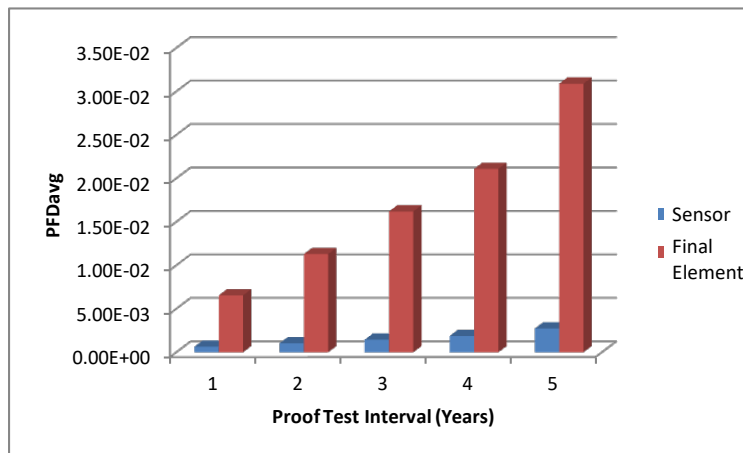

Figure 3: PFD$_{avg}$ versus Proof Test Interval

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

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

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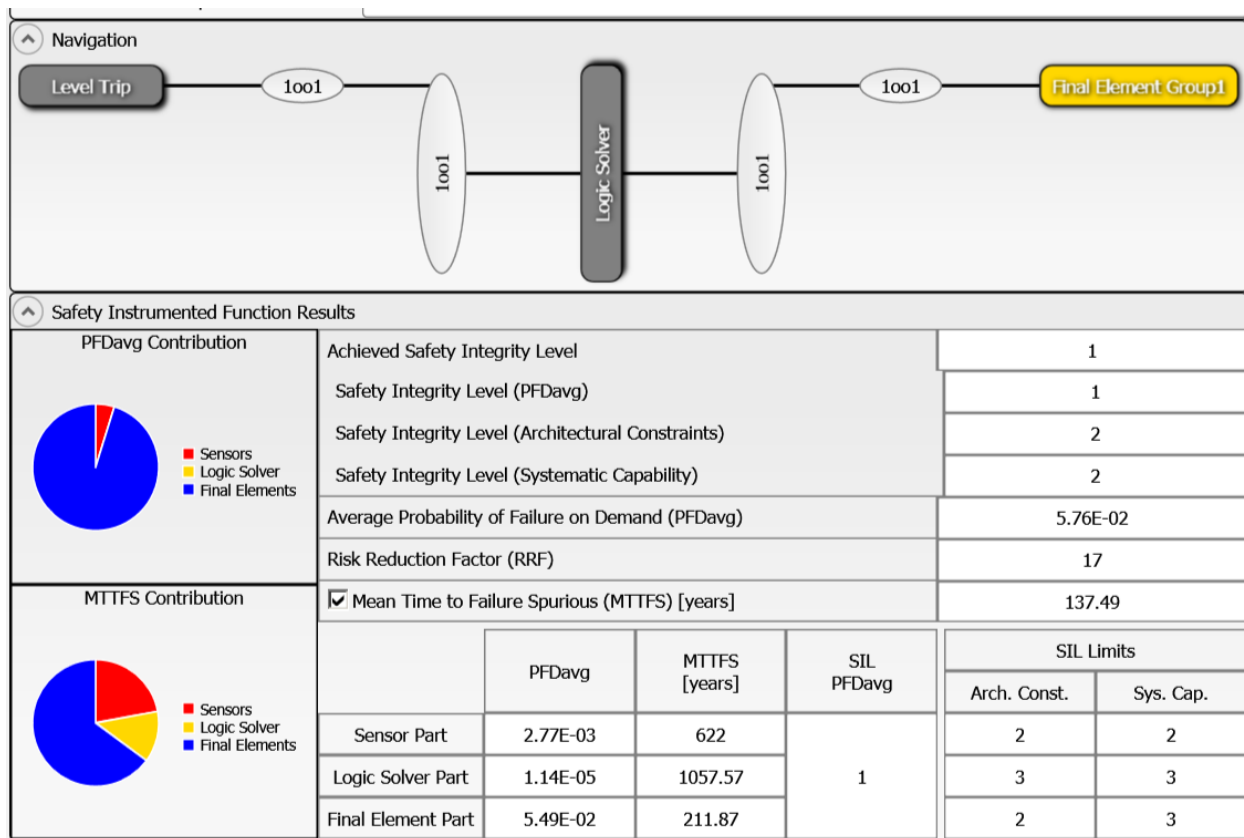
Figure 4: exSILentia results with realistic variables

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

Appendix E   Site Safety Index

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

E.1   Site Safety Index Profiles

The SSI is a number from 0 – 4 which is an indication of the level of site activities and practices that contribute to the safety performance of SIF's on the site. Table 11 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 11 *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.

© *exida*
T-126 V3,R5

BIF 17-05-128 R001 V1R6 FMEDA Report FP Solenoid Valves.docx
exida 80 N. Main St, Sellersville, PA 18960   Page 33 of 37

E.2 Site Safety Index Failure Rates – FP Solenoid Valves

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 12 thru

Table 15 lists the failure rates for the FP Solenoid Valves according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal maintenance practices).

Table 12 DTT Failure rates for Static Applications[21] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}[22]	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT	0	107	0	69	270	110
FP03P, FP06P and FP10P; NC, DTT	0	85	0	52	162	119
FP15; NC, DTT	0	160	0	114	560	151
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT; with automated PVST	103	4	61	8	270	110
FP03P, FP06P and FP10P; NC, DTT; with automated PVST	81	4	46	6	162	119
FP15; NC, DTT; with automated PVST	155	5	102	12	560	151
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT	0	77	0	110	264	116
FP03P, FP06P and FP10P; NO, DTT	0	75	0	70	155	119
FP15; NO, DTT	0	98	0	195	563	151
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT; with automated PVST	73	4	98	12	264	116

---

[21] Static Application failure rates are applicable if the device is static for a period of more than 200 hours.
[22] 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.

	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
FP03P, FP06P and FP10P; NO, DTT; with automated PVST	71	4	62	8	155	119
FP15; NO, DTT; with automated PVST	94	4	174	21	563	151

Table 13 ETT Failure rates for Static Applications[23] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}[24]	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT	0	22	0	137	264	110
FP03P, FP06P and FP10P; NC, ETT	0	18	0	106	155	119
FP15; NC, ETT	0	64	0	191	563	151
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT; with automated PVST	18	4	128	9	264	110
FP03P, FP06P and FP10P; NC, ETT; with automated PVST	14	4	99	7	155	119
FP15; NC, ETT; with automated PVST	57	7	178	13	563	151
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT	0	62	0	124	264	116
FP03P, FP06P and FP10P; NO, ETT	0	43	0	102	155	119
FP15; NO, ETT	0	94	0	201	560	151
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT; with automated PVST	59	4	115	9	264	116
FP03P, FP06P and FP10P; NO, ETT; with automated PVST	40	4	95	7	155	119
FP15; NO, ETT; with automated PVST	90	4	184	17	560	151

---

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

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

Table 14 DTT Failure rates for Dynamic Applications[25] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT	0	109	0	45	285	116
FP03P, FP06P and FP10P; NC, DTT	0	87	0	38	169	128
FP15; NC, DTT	0	164	0	74	596	157
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, DTT; with automated PVST	105	4	39	6	285	116
FP03P, FP06P and FP10P; NC, DTT; with automated PVST	83	4	33	5	169	128
FP15; NC, DTT; with automated PVST	159	5	65	9	596	157
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT	0	76	0	84	278	116
FP03P, FP06P and FP10P; NO, DTT	0	76	0	53	161	128
FP15; NO, DTT	0	97	0	149	592	157
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, DTT; with automated PVST	73	4	74	10	278	116
FP03P, FP06P and FP10P; NO, DTT; with automated PVST	73	4	47	7	161	128
FP15; NO, DTT; with automated PVST	93	4	133	16	592	157

---

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

Table 15 ETT Failure rates for Dynamic Applications[26] with Ideal Maintenance Assumption in FIT (SSI=4)

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	E
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT	0	71	0	75	278	116
FP03P, FP06P and FP10P; NC, ETT	0	68	0	52	161	128
FP15; NC, ETT	0	114	0	111	592	157
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NC, ETT; with automated PVST	66	5	68	7	278	116
FP03P, FP06P and FP10P; NC, ETT; with automated PVST	63	5	47	5	161	128
FP15; NC, ETT; with automated PVST	107	7	102	9	592	157
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT	0	64	0	96	278	116
FP03P, FP06P and FP10P; NO, ETT	0	45	0	85	161	128
FP15; NO, ETT	0	97	0	152	589	157
FP01, FP02, FP03, FP04, FP05, FP02G and FP05G; NO, ETT; with automated PVST	61	4	90	6	278	116
FP03P, FP06P and FP10P; NO, ETT; with automated PVST	41	4	79	5	161	128
FP15; NO, ETT; with automated PVST	92	4	140	12	589	157

---

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

© *exida*   BIF 17-05-128 R001 V1R6 FMEDA Report FP Solenoid Valves.docx
T-126 V3,R5   *exida* 80 N. Main St, Sellersville, PA 18960   Page 37 of 37