Failure Modes, Effects and Diagnostic Analysis

Project:
BXS Pilot & Mechanical Valve

Company:
Bifold Fluidpower Ltd.
Chadderton, Greater Manchester
United Kingdom

Contract Number: Q22/08-077
Report No.: BIF 13/09-019 R001
Version V3, Revision R1, November 22, 2022
Ted Stewart

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the BXS Pilot & Mechanical Valve. 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 BXS Pilot & Mechanical Valve. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The BXS Pilot & Mechanical Valves analyzed include an Integrated Pilot Valve, 3/2 and 5/2 spool valve bodies and 17 available operators. Operators are design to be used in either the primary and/or secondary position. When the operator in the primary position is energized the pilot valve is in its normal operating mode. The safe state is with the primary operator de-energized and the secondary operator energized or providing mechanical return force.

The Integrated Pilot Valve (IPV) is the interface between the Solenoid and the Primary Operator. It is designed to provide pressure to the Primary Operator when the associated solenoid is energized. When the associated solenoid is de-energized the IPV vents the pressure in the Primary Operator.

The associated solenoid is not included in this analysis.

When used in a functional safety application, the complete valve assembly must be operated automatically.

Note: the SIF designer is responsible for determining if the Latching and/or Override functions are 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

Figure 1 in Section 3 shows the arrangement of the valve body and the two operator positions.

Table 1 gives an overview of the valve bodies and operators that were considered in the FMEDA of the BXS Pilot & Mechanical Valve. The analysis was conducted both with and without partial Valve Stroke Testing (PVST).

Table 1 Component Overview

Part Number	Description
IPV3-S1-M20-32-NC-AL	IPV Integrated Pilot Valve
BX-SUB1-04-04-3XX-V-01	3/2 Valve
BX-SUB1-04-04-5XX-V-01	5/2 Valve
BX-SUBX-E1-X-01	E1 Internal Pilot Inline
BX-SUBX-E2-X-01	E2 Internal Pilot Inline
BX-SUBX-P1-X-01	P1 Standard Air Pilot
BX-SUBX-P2-X-01	P2 Side Air Pilot
BX-SUBX-P9-X-01	Air Latch Pilot Operator
BX-SUBX-M7-01	M7 Plunger
BX-SUBX-M13-01	M13 Roller Cam Ball
BX-SUBX-00-01	00 Spring Return
BX-SUBX-02-01	02 Spring Return
BX-SUBX-M3-X-01	M3 Push / Pull Button
BX-SUBX-M15-X-01	M15 Pull Button Spring Return
BX-SUBX-M16-X-01	M16 Pull Button Spring Return with Latch
BX-SUBX-M17-X-01	M17 Pull Button Spring Return Padlockable

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. See Section 0. Therefore, the BXS Pilot & Mechanical Valve 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.

The architectural constraints for the entire final element will need to be evaluated per Route 1_H

The failure rates for the BXS Pilot & Mechanical Valve are listed in section 4.4.

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

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

A user of the BXS Pilot & Mechanical Valve can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system

(SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the BXS Pilot & Mechanical Valve. 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.

An FMEDA is part of 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 BXS Pilot & Mechanical Valve
exida	Performed the hardware assessment
Bifold Fluidpower Ltd.	originally contracted *exida* in August 2013 with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3rd & 4th Edition	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third & Fourth Edition, (4th edition is pending publication, not publically available at the time of this report)
[N3]	Mechanical Component Reliability Handbook, 3rd & 4th Edition	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third & Fourth Edition, (4th edition is pending publication, not publically available at the time of this report)
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

[N7]	O'Brien, C. & Bredemeyer, L., 2009	*exida* LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9
[N8]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers
[N9]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design
[N10]	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 *exida* tools used

[T1]	Version 3.1.2.867	exSILentia

2.5 Reference documents

2.5.1 Documentation provided by Bifold Fluidpower Ltd.

[D1]	GA0432, Rev 0, 10/17/2012	3/2 Valve Assembly Drawing
[D2]	GA0433, Rev 0, 10/17/2012	5/2 Valve Assembly Drawing
[D3]	GA0452, Rev 0, 11/8/2012	E1 Internal Pilot Drawing
[D4]	GA0459, Rev 0, 11/8/2012	P1 Standard Air Pilot Drawing
[D5]	GA0453, Rev 0, 11/8/2012	E2 Internal Pilot Inline
[D6]	GA0445, Rev 0, 11/8/2012	P2 Side Air Pilot
[D7]	GA0443, Rev 0, 11/7/2012	00 Spring Return
[D8]	GA0449, Rev 0, 11/8/2012	M7 Plunger

[D9]	GA0450, Rev 0, 11/8/2012	M15 Pull Button Spring Return
[D10]	GA0451, Rev 0, 11/8/2012	M16 Pull Button Spring Return with Latch
[D11]	GA0505, Rev 0, 3/7/2013	M17 Pull Button Spring Return - Padlockable
[D12]	GA0384, Rev 2, 4/6/2012	Integrated Pilot Valve
[D13]	BXS-40-04-P1-32-NU-IND	02 Spring Return
[D14]	GA0444, Rev 1, 11/08/2012	P9 General Arrangement
[D15]	GA0467, Rev 0, 11/09/2012	M3 General Arrangement

2.5.2 Documentation generated by *exida*

[R1]	BIF 13-07-019_BXS FMEDA r1.xls, 10/18/2016	Failure Modes, Effects, and Diagnostic Analysis – BXS Pilot & Mechanical Valve

3 Product Description

The BXS Pilot & Mechanical Valves analyzed include an Integrated Pilot Valve, 3/2 and 5/2 spool valve bodies and 17 available operators. Operators are design to be used in either the primary and/or secondary position. When the operator in the primary position is energized the pilot valve is in its normal operating mode. The safe state is with the primary operator de-energized and the secondary operator energized or providing mechanical return force.

The Integrated Pilot Valve (IPV) is the interface between the Solenoid and the Primary Operator. It is designed to provide pressure to the Primary Operator when the associated solenoid is energized. When the associated solenoid is de-energized the IPV vents the pressure in the Primary Operator.

The associated solenoid is not included in this analysis.

When used in a functional safety application, the complete valve assembly must be operated automatically. Manual overrides must be secured such that they cannot be operated accidently or by unqualified personnel.

Figure 1 shows the arrangement of the valve body and operators.

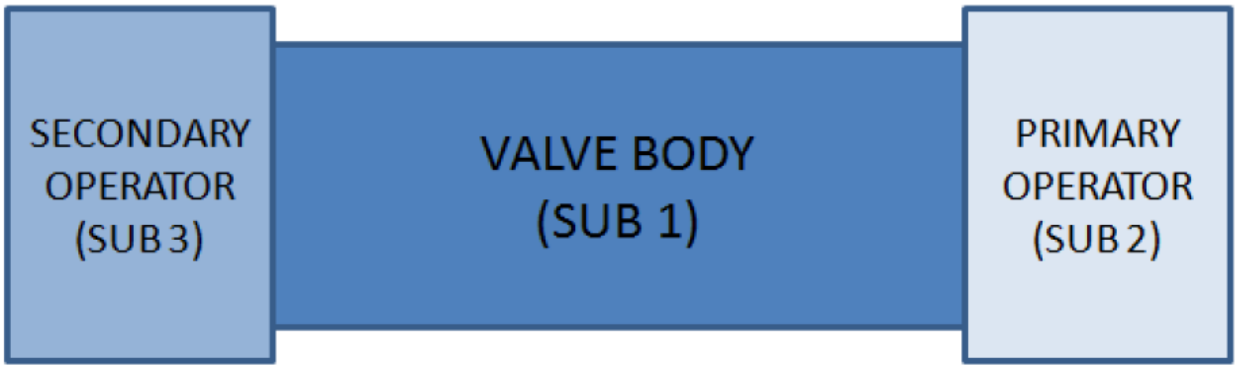


Figure 1 BXS Pilot & Mechanical Valve arrangement showing the layout of valve body and operators.

Figure 2 shows the BXS Pilot & Mechanical Valve with the IPV and solenoid operator.

Note: The solenoid operator is not included in this analysis.

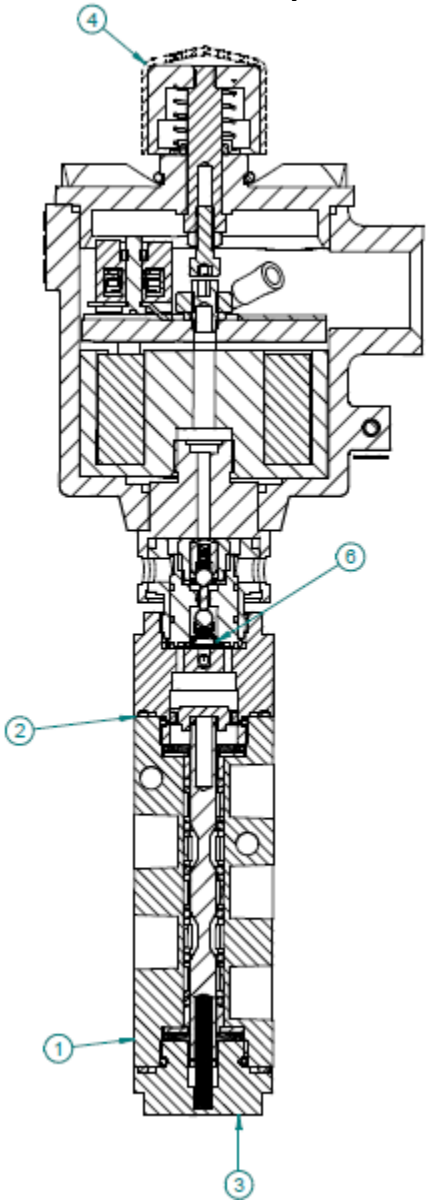


Figure 2: #1 5/2 Valve Assembly; #2 SUB2 – E1 Int Pilot; #3 SUB3 – Spring; #4 Solenoid Operator; #6 IPV

Table 2 gives an overview of the different versions that were considered in the FMEDA of the BXS Pilot & Mechanical Valve.

Table 2 Component Overview

Part Number	Description
IPV3-S1-M20-32-NC-AL	IPV Integrated Pilot Valve
BX-SUB1-04-04-3XX-V-01	3/2 Valve
BX-SUB1-04-04-5XX-V-01	5/2 Valve
BX-SUBX-E1-X-01	E1 Internal Pilot Inline
BX-SUBX-E2-X-01	E2 Internal Pilot Inline
BX-SUBX-P1-X-01	P1 Standard Air Pilot
BX-SUBX-P2-X-01	P2 Side Air Pilot
BX-SUBX-P9-X-01	Air Latch Pilot Operator
BX-SUBX-M7-01	M7 Plunger
BX-SUBX-M13-01	M13 Roller Cam Ball
BX-SUBX-00-01	00 Spring Return
BX-SUBX-02-01	02 Spring Return
BX-SUBX-M3-X-01	M3 Push / Pull Button
BX-SUBX-M15-X-01	M15 Pull Button Spring Return
BX-SUBX-M16-X-01	M16 Pull Button Spring Return with Latch
BX-SUBX-M17-X-01	M17 Pull Button Spring Return Padlockable

The BXS Pilot & Mechanical Valve is classified as a component of a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis as performed based on the documentation in section 2.5.1and is documented in [R1].

4.1 Failure categories description

In order to judge the failure behavior of the BXS Pilot & Mechanical Valve, the following definitions for the failure of the device were considered.

Fail-Safe State

Solenoid Valve	State where the primary operator solenoid is de-energized and the secondary operator is energized or provides mechanical return force.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics 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 process fluids 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 2H failure data is not available.

External leakage failure rates do not directly contribute to the reliability of a component 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, fail high, fail low, etc.) 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 failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which was derived using over twenty billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 3, see Appendix C. The *exida* profile chosen 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.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. 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. 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.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the BXS Pilot & Mechanical Valve.

- Only a single component failure will fail the entire BXS Pilot & Mechanical Valve.
- 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 maintenance capability are site specific and therefore cannot be included.

- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 3 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- Materials are compatible with process conditions.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- The device is installed per manufacturer's instructions.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- Partial Valve Stroke Testing is performed at a rate at least ten times faster than the expected demand rate on the associated valve actuator combination.
- Partial Valve Stroke Testing will stroke the pilot valve through full travel.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is the Partial Valve Stroke Test interval or the Proof test interval in hours.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the BXS Pilot & Mechanical Valve FMEDA.

Table 3 and Table 4 lists the failure rates for the BXS Pilot & Mechanical Valve 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 BXS Pilot & Mechanical Valve without PVST (FIT)

Device Description	Position	λ_{SD}[2]	λ_{SU}[3]	λ_{DD}[4]	λ_{DU}[5]	λ_{NE}[6]	λ_{EL}[7]
IPV Integrated Pilot Valve	--	0	65	0	49	194	0
3/2 Valve	1	0	51	0	155	299	366
5/2 Valve	1	0	51	0	217	593	366
E1 Internal Pilot Inline	2	0	63	0	28	133	14
E2 Internal Pilot Inline	2	0	85	0	28	132	70
P1 Standard Air Pilot	2	0	57	0	28	133	0
P2 Side Air Pilot	2	0	85	0	28	132	70
P9 Air Latch Pilot Operator	2	0	106	0	26	168	0
M7 Plunger	2	0	3	0	14	4	0
M13 Roller Cam Ball	2	0	3	0	14	4	0
00 Spring Return	3	0	0	0	4	10	0
02 Spring Return	3	0	0	0	4	10	0
E1 Internal Pilot Inline	3	0	0	0	90	133	14
E2 Internal Pilot Inline	3	0	0	0	113	132	70
P1 Standard Air Pilot	3	0	0	0	84	133	0
P2 Side Air Pilot	3	0	0	0	113	132	70
M7 Plunger	3	0	0	0	17	4	0
M13 Roller Cam Ball	3	0	0	0	17	4	0
M3 Push / Pull Button	3	0	3	0	17	43	0
M15 Pull Button Spring Return	3	0	0	0	38	2	0

[2] Safe Detected Failure Rate
[3] Safe Undetected Failure Rate
[4] Dangerous Detected Failure Rate
[5] Dangerous Undetected Failure Rate
[6] No Effect Failure Rate
[7] External Leak Failure Rate

M16 Pull Button Spring Return with Latch	3	0	0	0	38	2	0
M17 Pull Button Spring Return Padlockable	3	0	0	0	38	2	0

Table 4 Failure rates BXS Pilot & Mechanical Valve with PVST (FIT)

Device Description	Position	λ_{SD}	λ_{SU}[8]	λ_{DD}	λ_{DU}	λ_{NE}	λ_{EL}
IPV Integrated Pilot Valve	--	64	1	46	3	194	0
3/2 Valve	1	50	1	140	15	299	366
5/2 Valve	1	50	1	195	21	593	366
E1 Internal Pilot Inline	2	62	1	25	3	133	14
E2 Internal Pilot Inline	2	84	1	25	3	132	70
P1 Standard Air Pilot	2	56	1	25	3	133	0
P2 Side Air Pilot	2	84	1	25	3	132	70
P9 Air Latch Pilot Operator	2	105	1	15	11	168	0
M7 Plunger	2	3	0	13	1	4	0
M13 Roller Cam Ball	2	3	0	13	1	4	0
00 Spring Return	3	0	0	3	1	10	0
02 Spring Return	3	0	0	3	1	10	0
E1 Internal Pilot Inline	3	0	0	87	3	133	14
E2 Internal Pilot Inline	3	0	0	109	4	132	70
P1 Standard Air Pilot	3	0	0	81	3	133	0
P2 Side Air Pilot	3	0	0	109	4	132	70
M3 Push / Pull Button	3	3	0	10	7	43	0
M7 Plunger	3	0	0	16	1	4	0
M13 Roller Cam Ball	3	0	0	16	1	4	0
M15 Pull Button Spring Return	3	0	0	36	2	2	0
M16 Pull Button Spring Return with Latch	3	0	0	36	2	2	0
M17 Pull Button Spring Return Padlockable	3	0	0	36	2	2	0

[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.

External leakage failure rates do not directly contribute to the reliability of the valve 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.

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. Therefore, the BXS Pilot & Mechanical Valve meets the hardware architectural constraints Route 2_H when used with other Route 2_H devices in an element 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 the entire final element, the architectural constraints will need to be evaluated per Route 1_H

As the BXS Pilot & Mechanical Valve is only one part of an element, the architectural constraints should be determined for the entire final element using either Route 1_H or Route 2_H.

5 Using the FMEDA Results

5.1 Air quality failures

The product failure rates that are listed in this report are failure rates that reflect the situation where the device is used with clean filtered air. Contamination from poor control air quality may affect the function or air flow in the device. For applications where these assumptions do not apply, the user must estimate the failure rates due to contaminated air and add this failure rate to the product failure rates.

5.2 PFD_{avg} calculation BXS Pilot & Mechanical Valve

Using the failure rate data displayed in 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 BXS Pilot & Mechanical Valve are listed in Table 5 and 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 BXS Pilot & Mechanical Valve contributes less to the overall PFD_{avg} of the Safety Instrumented Function.

5.3 *exida* Route 2_H Criteria

IEC 61508, ed2, 2010 describes the Route 2H alternative to Route 1H 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 2H, 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 on line internally by the device or, if specified, externally by another device without manual intervention.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
FIT	Failure in Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
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.
Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
SSI	Site Safety Index (See Appendix E)
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

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

Due to future potential changes in the standards, 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 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 and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q22-08-077	BIF 13-07-019 R001 V3R1	Update per customer comments; TES 11/22/2022
Q16-10-005	BIF 13-07-019 R001 V2R1	Added M3 & P9, October 25, 2016; GPS
Q13-07-019	BIF 13-07-019 R001 V1R1	Released to Bifold Fluidpower Ltd. Dec 20, 2013
Q13-07-019	BIF 13-07-019 R001 V0R1	Draft; November 22, 2013

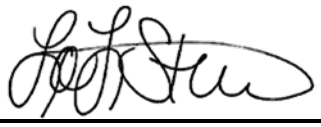
Original Author: Steven Close

Reviewer: Loren Stewart, 11/22/2022
Status: Released, 11/22/2022

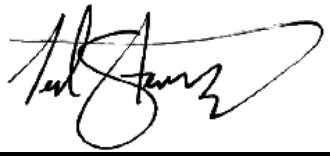
7.3 Future enhancements

At request of client.

7.4 Release signatures



Loren L. Stewart, CFSE, Senior Safety Engineer



Ted Stewart, CFSP, Safety Engineer

Steven Close, Senior Safety Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be 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[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 BXS Pilot & Mechanical 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.

Based on general field failure data a useful life period of approximately 10 years is expected for the BXS Pilot & Mechanical Valve. This will depend highly the associated solenoid valve.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant 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 proof test described in Table 5 is for an entire final element which would include a BXS Pilot & Mechanical Valve. It is assumed that the BXS Pilot & Mechanical Valve is able to perform the safety function properly if the final element reaches the safety state within the specified safety time. The suggested proof test consists of a full stroke of the final element actuator and valve, see Table 5.

Table 5 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	De-energize the BXS Pilot & Mechanical Valve to force the actuator and valve to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time.
3.	Return the BXS Pilot & Mechanical Valve to the energized state and inspect the final element for any leaks, visible damage or contamination and confirm that the normal operating state was achieved.
4.	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 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 product configurations is given in Table 6.

Table 6 Proof Test Coverage – BXS Pilot & Mechanical Valve

Device	Application	No PVST	with PVST
3/2 Valve Body	All possible configurations	98%	81%
5/2 Valve Body	All possible configurations	98%	83%

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[12]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[13]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[14]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[15]	G2	G3	G3	G3	G3	Compatible Material
Surge[16]						
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[17]						
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)[18]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[12] Humidity rating per IEC 60068-2-3
[13] Shock rating per IEC 60068-2-6
[14] Vibration rating per IEC 60770-1
[15] Chemical Corrosion rating per ISA 71.04
[16] Surge rating per IEC 61000-4-5
[17] EMI Susceptibility rating per IEC 6100-4-3
[18] ESD (Air) rating per IEC 61000-4-2

Appendix D Determining Safety Integrity Level

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

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

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

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

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

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

A Probability of Failure on Demand (PFD_{avg}) must be done based on a number of variables including:

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

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 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.

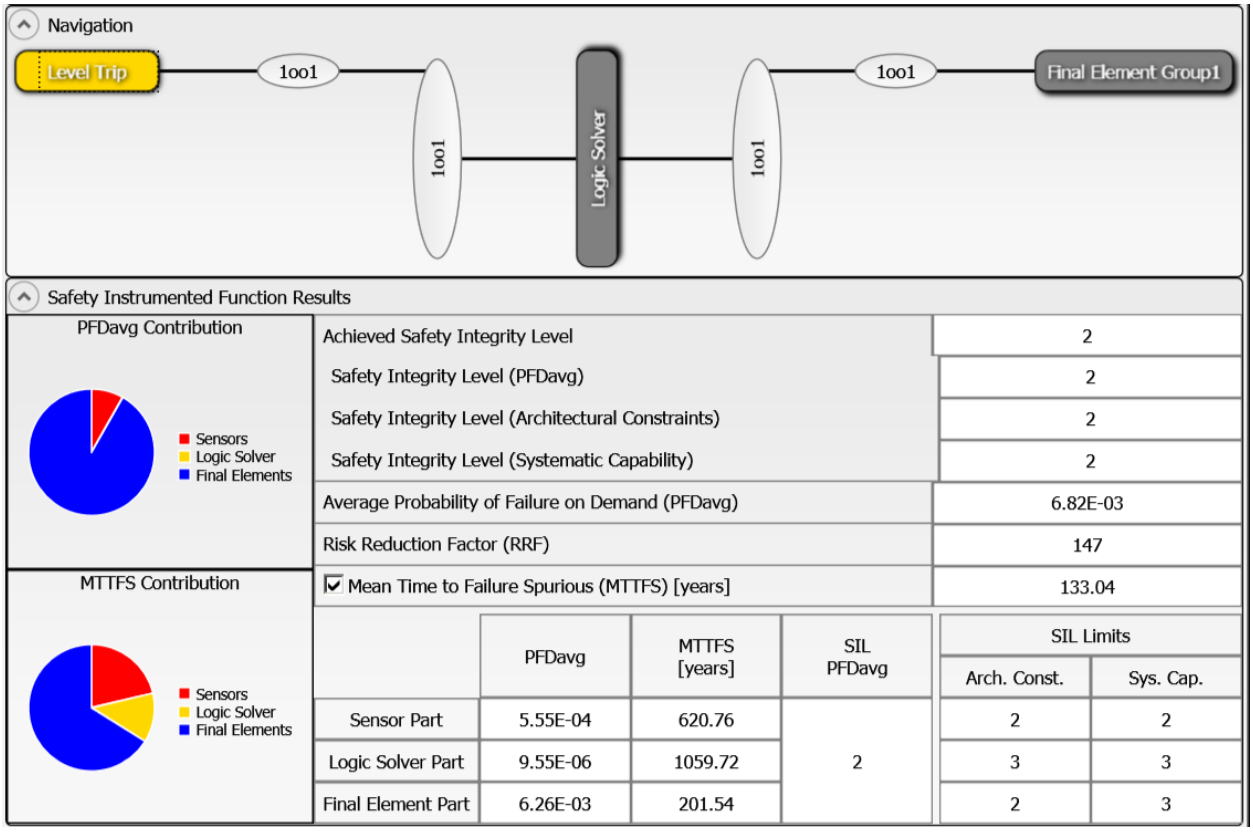
Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic 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 3).



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 3: 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 4.

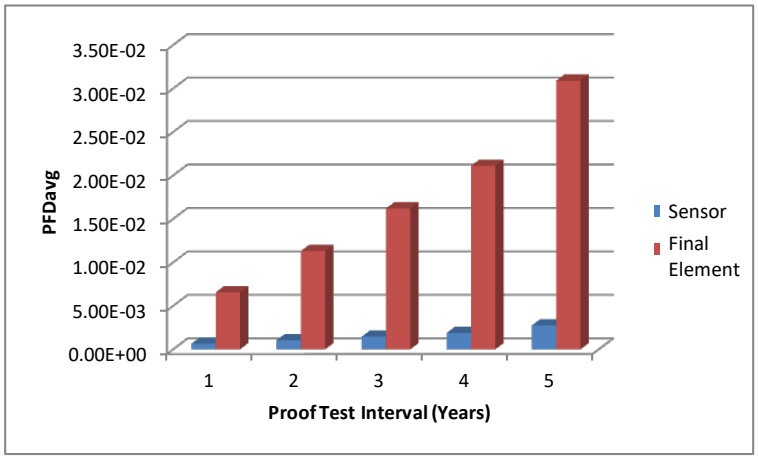


Figure 4: PFD_{avg} versus Proof Test Interval

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 5).

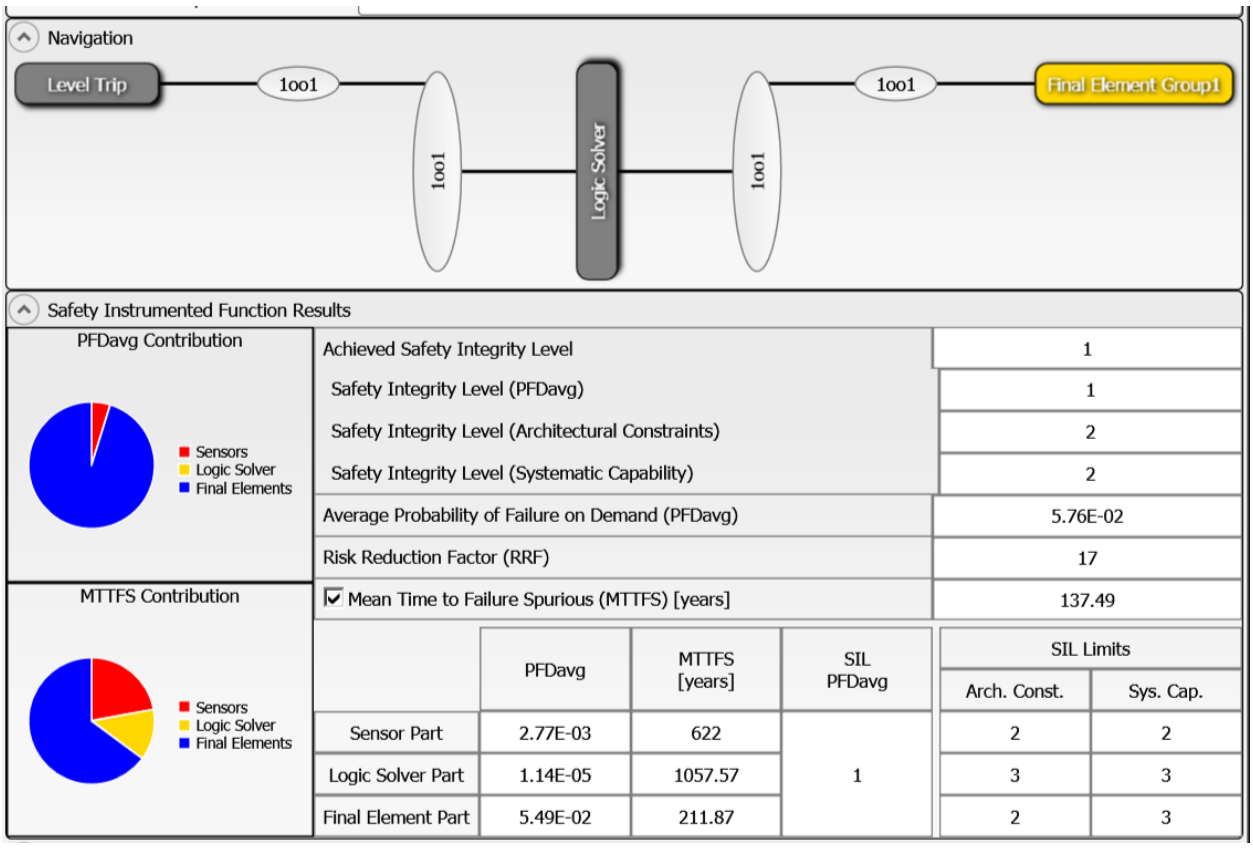


Figure 5: exSILentia results with realistic variables

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. 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 – BXS Pilot & Mechanical Valve

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 and Table 10 lists the failure rates for the BXS Pilot & Mechanical Valve according to IEC 61508 with a Site Safety Index (SSI) of 4 (ideal 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.

Table 9 Failure rates with Ideal Maintenance Assumption (SSI=4), without PVST in FIT

Device Description	Position	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{NE}	λ_{EL}
IPV Integrated Pilot Valve	--	0	39	0	25	116	0
3/2 Valve	1	0	31	0	78	179	220
5/2 Valve	1	0	31	0	109	356	220
E1 Internal Pilot Inline	2	0	38	0	14	80	8
E2 Internal Pilot Inline	2	0	51	0	14	79	42
P1 Standard Air Pilot	2	0	34	0	14	80	0
P2 Side Air Pilot	2	0	51	0	14	79	42
P9 Air Latch Pilot Operator	2	0	64	0	13	101	0
M7 Plunger	2	0	2	0	7	2	0
M13 Roller Cam Ball	2	0	2	0	7	2	0
00 Spring Return	3	0	0	0	2	6	0
02 Spring Return	3	0	0	0	2	6	0
E1 Internal Pilot Inline	3	0	0	0	45	80	8
E2 Internal Pilot Inline	3	0	0	0	57	79	42
P1 Standard Air Pilot	3	0	0	0	42	80	0
P2 Side Air Pilot	3	0	0	0	57	79	42
M7 Plunger	3	0	0	0	9	26	0
M13 Roller Cam Ball	3	0	0	0	9	2	0
M3 Push / Pull Button	3	0	0	0	9	2	0
M15 Pull Button Spring Return	3	0	0	0	19	1	0

M16 Pull Button Spring Return with Latch	3	0	0	0	19	1	0
M17 Pull Button Spring Return Padlockable	3	0	0	0	19	1	0

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

Device Description	Position	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{NE}	λ_{EL}
IPV Integrated Pilot Valve	--	38	1	23	2	116	0
3/2 Valve	1	30	1	70	8	179	220
5/2 Valve	1	30	1	98	11	356	220
E1 Internal Pilot Inline	2	37	1	13	2	80	8
E2 Internal Pilot Inline	2	50	1	13	2	79	42
P1 Standard Air Pilot	2	34	1	13	2	80	0
P2 Side Air Pilot	2	50	1	13	2	79	42
P9 Air Latch Pilot Operator	2	63	1	8	6	101	0
M7 Plunger	2	2	0	7	1	2	0
M13 Roller Cam Ball	2	2	0	7	1	2	0
00 Spring Return	3	0	0	2	0	6	0
02 Spring Return	3	0	0	2	0	6	0
E1 Internal Pilot Inline	3	0	0	44	2	80	8
E2 Internal Pilot Inline	3	0	0	55	2	79	42
P1 Standard Air Pilot	3	0	0	41	2	80	0
P2 Side Air Pilot	3	0	0	55	2	79	42
M7 Plunger	3	0	0	5	4	26	0
M13 Roller Cam Ball	3	0	0	8	1	2	0
M3 Push / Pull Button	3	0	0	8	1	2	0
M15 Pull Button Spring Return	3	0	0	18	1	1	0
M16 Pull Button Spring Return with Latch	3	0	0	18	1	1	0
M17 Pull Button Spring Return Padlockable	3	0	0	18	1	1	0