IEC 61508 Functional Safety Assessment

Project:
VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves

Customer:
Bifold Fluidpower Ltd
Chadderton, Manchester
United Kingdom

Contract No.: Q20-05-039
Report No.: BIF 09/10-25 R003
Version V4, Revision R1, July 31, 2020
Ted Stewart

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the:

VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves

The functional safety assessment performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Bifold Fluidpower Ltd through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team. *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Bifold Fluidpower Ltd

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3. A full IEC 61508 Safety Case was prepared, using the *exida* SafetyCase™ tool, and used as the primary audit tool. Hardware and software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also, the user documentation (safety manual) was reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The Bifold VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves were found to meet the Systematic Capability requirements of IEC 61508 for up to SC 3 (SIL 3 Capable)

The VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves were found to meet the Random Capability requirements for a Type A device of SIL 2 @HFT=0 , SIL3 @HFT=1 using Route 2_H.

The manufacturer will be entitled to use the Functional Safety Logos.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Bifold Fluidpower Ltd.

- VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves

by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010.

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

The results of this provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with Bifold Fluidpower Ltd.

All assessment steps were continuously documented by *exida* (see [R1] to [R6]).

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 and availability with over 500 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 350 billion hours of field failure data.

exida is the market leader for IEC 61508 certification for currently active marketed products.

2.2 Roles of the parties involved

Bifold Fluidpower Ltd	Manufacturer of the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment

Bifold Fluidpower Ltd originally contracted *exida* in 2009 with the IEC 61508 Functional Safety 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 (Parts 1 - 7): ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

Note: Documents highlighted in gray, in this section, were reviewed and updated during the 2020 surveillance audit.

2.4.1 Documentation provided by Bifold Fluidpower Ltd

Doc ID	Generic Document Name	Project Document Name and Link	Version	Date
D001	Quality Manual	Bifold Quality Manual	9	1/21/2019
D003	Overall Development Process	02-2-01 Design and Development.docx	3	3/18/2018
D004	Configuration Management Process	QGA - General Assembly.pdf	5	6/23/2016
D004b	Configuration Management Process	02-3-04 - Creating-amending-deleting kits.doc	1	5/8/2014
D006	Field Return Procedure	04-3-08 Valve Returns.pdf	1	5/13/2016
D007	Manufacturer Qualification Procedure	04-2-14; SQA MANUAL.pdf	45	4/29/2020
D008	Part Selection Procedure	02-2-01 Design and Development.docx	3	3/18/2018
D010	Quality Management System (QMS) Documentation Change Procedure	04-2-02 - Control of Documents & Records.pdf	6	10/12/2017
D012	Non-Conformance Reporting procedure	04-2-05 - Control of Non-Conforming Product.pdf	5	1/9/2018
D013	Corrective Action Procedure	04-2-06 - Corrective & Preventative Actions.pdf	4	5/10/2019
D019	Customer Notification Procedure	04-3-05 Customer Escalation Procedure	3	4/1/2015
D023	Modification Procedure	02-3-02 Modification Control - Change Orders.docx	2	6/9/2014
D023b	Impact Analysis Template	DOCUMENT CHANGE ORDER.docx		12/18/2014
D023c	Modification Change Order Example	CO3356.pdf		8/24/2016
D023d	Impact Analysis Procedure	TD 011 - Change Order Impact Analysis Proc.pdf	3	10/2/2011
D023e	Change order form	DOCUMENT CHANGE ORDER.docx	9	
D26b	Responsibility Plan	DP0053 – DC-QR14_2-Responsibility Plan	2	6/15/2017
D031	Field Returns Records	Sales Data VBP-HIPEX-PPV.xlsx		5/1/2014
D034	Skills Matrix	Sil - Technical Skills Matrix.pdf	3	
D040	Safety Requirements Specification	VBP Catalog.pdf	BFD03/9	Nov-16

D040b	Safety Requirements Specification	DC/QR21 Product Specification & Operating Requirements	1	3/2009
D069	Validation Test Plan	02-2-02 Factory Acceptance Testing.docx	1	5/15/2014
D078	Operation / Maintenance Manual Mechanical Operators	OPB0024 IOM VBP	2	3/1/2017
D079e	SM.0006_13	VBP-Volume Booster & HIPEX Safety Manual	13	12/13/2019
D079f	SM.0007_4 PPV	PPV Valve Safety Manual	4	8/14/2014
D081	Engineering Change Documentation	CO3781.pdf		9/22/2017
D088	Impact Analysis Record	CO3781.pdf		9/22/2017

2.4.2 Documentation generated by *exida*

[R1]	BIF 091025_FMEDA_r2, 5/7/2014	Failure Modes, Effects and Diagnostic Analysis - Bifold VBP Series Volume Boosters and HIPEX Valve (internal document)
[R2]	Bifold VBP Q09-10-25r2 FMEDA R3, 5/13/2014	Failure Modes, Effects and Diagnostic Analysis, VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves (internal document)
[R3]	BIF 091025 VBP FMEDA R002 V2R1, 5/21/2014	FMEDA report- VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves (internal document)
[R4]	BIF 091025_VBP_FMEDA R001 V2R2, 5/21/2014	FMEDA report - Bifold VBP Series Volume Boosters and HIPEX Valve
[R5]	BIF Q14-03-083 Bifold Volume Booster	Bifold VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves IEC 61508 Compliance SafetyCase (internal database)
[R6]	Q20-05-039 PIU2017-2020.xls	Proven In Use Analysis – VBP-PPV

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed upon by Bifold Fluidpower Ltd.

The following IEC 61508 objectives were subject to detailed auditing at Bifold Fluidpower Ltd:

- FSM planning, including

- Safety Life Cycle definition
    - Scope of the FSM activities
    - Documentation
    - Activities and Responsibilities (Training and competence)
    - Configuration management
    - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
- Hardware-related operation, installation and maintenance requirements

3 Product Description

The VBP Volume Boosters convert a low volume pressure signal into a 1:1 ratio high volume output. It is specifically designed for both modulating and On - Off pilot pressure signals. When a low volume pilot pressure signal of 2 to 10 bar g is applied to the sensing port, the main valve assembly opens to allow high volume flow from the main inlet port to the outlet port. When the sensing assembly detects that the outlet pressure is equal to the pilot pressure, the main valve moves to the 'all ports blocked' rest position and will remain in this position until there is a change in the pilot pressure or outlet pressure. If the sensing head detects that the outlet is higher than the pilot pressure, the high flow exhaust opens to vent the excess pressure. If the sensing head detects that the outlet pressure is too low, the main valve opens to recharge the system to the correct 1:1 ratio pressure. For functional safety applications, only the on-off mode of operation is considered.

The PPV Pilot Valves allow a low volume pressure signal to control a high-volume output. When a low volume pilot pressure signal is applied to the pilot port, the main valve assembly opens to allow high volume flow from the main inlet port to the outlet port. These valves are generally used to control pneumatic flow to and from an actuator, or to dump large volumes of air. Two Valve configurations were considered in this evaluation, a Normally Closed (NC or Block Before Bleed – BBB) and a Normally Universal (NU or Block After Bleed – BAB).

The HIPEX Valves is a quick exhaust valve designed for the purpose of providing a high-volume exhaust capability. With pilot pressure applied to the pilot port the input port is blocked. When the pilot pressure is released the input port if connected to a high-volume capacity exhaust port. The input is also fed back against the pilot pressure. This enables the HIPEC Valve to also serve as a pressure relief valve. If the input pressure exceeds the pilot pressure the input port will open exhausting the input pressure until it is once again equal to the pilot pressure. The FMEDA only considered the quick exhaust function of VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves.

Table 1 Version overview gives an overview of the valve bodies and operators that were considered in the assessment of the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves.

Table 1 Version overview

Port Size	Description
½ & 1 inch	Standard Volume Booster – VBP-8 and VBP-16 Series
½ & 1 inch	Filter Volume Booster – VBP-16 Series
½ & 1 inch	HIPEX Valve - HIPEX-8 and HIPEX-16 Series
1½ & 2 inch	Standard Volume Booster – VBP-24 and VBP-32 Series
1½ & 2 inch	Pneumatic Pilot Valve – PPV-24 and PPV-32 Series
1½ & 2 inch	HIPEX Valve – HIPEX-24 and HIPEX-32 Series

The VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves are classified as a Type A[1] devices according to IEC 61508, having a hardware fault tolerance of 0.

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Bifold Fluidpower Ltd and is documented in the SafetyCase [R5].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software development (if applicable) and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software. The assessment also includes a review of existing manufacturing quality procedures to ensure compliance to the quality requirements of IEC 61508.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
    - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
    - Specification process, techniques and documentation
    - Design process, techniques and documentation, including tools used
    - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
    - Verification activities and documentation
    - Modification process and documentation
    - Installation, operation, and maintenance requirements, including user documentation
    - Manufacturing Quality System
- Product design
    - Hardware architecture and failure behavior, documented in a FMEDA

The review of the development procedures is described in section 5.1. The review of the product design is described in section 5.2.

4.2 Assessment Level

The VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves have been assessed per IEC 61508 to the following levels:

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

- Systematic Capability SC 3 (SIL 3 capability) as the design documentation analysis justified that this device is suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3) according to IEC 61508.
- Architecture Constraint limitations of SIL 2 for a single device using Route 2_H or if the SFF for the complete final element is >60% using Route 1_H.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Bifold Fluidpower Ltd for this development against the objectives of IEC 61508 parts 1 and 2. This assessment was performed remotely and is documented in the SafetyCase [R5].

The current development process is fully compliant with IEC 61508. The existing design documentation and additional documented safety analysis shows the design integrity. The SafetyCase was created with project specific design documents. Future modifications to the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves must be made per the IEC 61508 SIL 3 compliant development process.

5.1 Lifecycle Activities and Fault Avoidance Measures

Bifold Fluidpower Ltd has a defined product lifecycle process in place. This is documented in company procedures 02-2-01, Design and Development. These are also part of Bifold's Quality Management System which is ISO 9001 approved. No software is part of the design and therefore any requirements specific from IEC 61508 related to software and software development do not apply.

The assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for product design and development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 2 work scope of the development team. The defined product lifecycle process was modified as a result of a previous audit which showed some areas for improvement. However, given the simple nature of the safety function and the extensive proven field experience for existing products Bifold Fluidpower Ltd was able to demonstrate that the objectives of the standard have been met. The result of the assessment can be summarized by the following observations:

The audited Bifold Fluidpower Ltd development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

FSM Planning

Bifold Fluidpower Ltd has a defined process in place for product design and development. Required activities are specified along with review and approval requirements. This is primarily documented in 02-2-01, Design and Development. Templates, forms and sample documents are provided. The same process is used for modifications. This process and procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management for a product with simple complexity and well-defined safety functionality.

Version Control

Bifold Fluidpower Ltd Procedure 04-2-02 requires that all documents be version controlled. Document revisions were evident during the audit.

Training, Competency recording

Personnel training records are kept per standard quality procedures. BOP 4.1 states that the Technical Director is responsible for ensuring that only qualified personnel and/or Subcontractors are used to perform the design and development tasks. Bifold Fluidpower Ltd hired *exida* to provide analysis, training and supplemental functional safety expertise. Bifold Fluidpower Ltd hired *exida* to be the independent assessor per IEC 61508.

5.1.2 Safety Requirements Specification and Architecture Design

For the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves, the simple safety functionality is the primary functionality of the product (Close / Open the final Control Valve). Therefore, no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the Valve Assembly design is relatively simple and is based upon standard designs with extensive field history, no semi-formal methods are needed. General design and testing methodology is documented and required as referenced in [D003], and [D069]. This meets SIL 3.

Requirements from IEC 61508-2, Table B.1 that have been met by Bifold Fluidpower Ltd include project management, documentation, structured specification, review of the specification, and checklists. This meets the requirements of SIL 3.

5.1.3 Hardware Design

The design process is documented in [D003]. Items from IEC 61508-2, Table B.2 include observance of guidelines and standards (PED, API NACE, ATEX), project management, documentation (design outputs are documented per Procedure 02-2-01), structured design, modularization, use of well-tried components, and computer-aided design tools. This meets SIL 3.

5.1.4 Validation

Validation Testing is done via a documented plan [D069] created that links to the product's requirements specifications and includes compliance testing per application and agency standards. Bifold Fluidpower Ltd also maintains requirements for factor acceptance testing [D069c] that are used to validate their designs. As the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves perform only one Safety Function, which is extensively tested under various conditions during validation testing.

Items from IEC 61508-2, Table B.3 include functional testing, project management, documentation, and black-box testing (for the considered devices this is similar to functional testing). Field experience and statistical testing via regression testing are not applicable. This meets SIL 3.

Items from IEC 61508-2, Table B.5 included functional testing and functional testing under environmental conditions, project management, documentation, failure analysis (analysis on products that failed), expanded functional testing, black-box testing, and fault insertion testing. This meets SIL 3.

5.1.5 Verification

The development and verification activities are also defined in 02-02-01. Design reviews [D053] are conducted at critical phases of the project to verify that the design is capable of meeting the design requirements. For each design phase the objectives are stated, the required input and output documents are specified and necessary review activities are determined. Verification activities also included a design FMEA and review, a third party FMEDA, and other reviews of the tests and test results. The results of these activities were documented and reviewed. This meets SIL 2.

5.1.6 Proven In Use

A surveillance audit was concluded in July of 2020. The audit covered the Design Fault avoidance techniques listed above and a Proven in Use evaluation on the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves. Shipment records were used to determine that the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves have >100 million hours in use and they have demonstrated a field failure rate less than the failure rates indicated in the FMEDA reports. This meets the requirements for Proven In Use for SIL 3.

5.1.7 Modifications

Any Modifications must go through Bifold's Engineering Change procedure which is initiated with a Change Request Form (DC/QR3). All changes are first reviewed and if approved, the work follows the normal design process. An impact analysis is performed on every change order and documented per form (DC/QR3). This meets the requirements of IEC 61508 SIL 3

During the surveillance audit in 2020 the modifications to the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves were reviewed. It was determined that the modifications were carried out per the Engineering Change Procedure and that an impact analysis was performed. See [D081].

5.1.8 User documentation

Bifold Fluidpower Ltd has created a Safety Manual for the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves, see [D079]. This safety manual was assessed by *exida*. It contained all required information given the simplicity of the products. The FMEDA reports are available and they contain failure rate, failure mode, useful life and suggested proof test information. The combination of the Safety Manual and the FMEDA's are considered to be in compliance with the requirements of IEC 61508.

Requirements from IEC 61508-2, Table B.4 that have been met by Bifold Fluidpower Ltd include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (the products perform well-defined actions) and operation only by skilled operators (operators familiar with type of valve, although this is partly the responsibility of the end-user). This meets the requirements for SIL 3.

The latest versions of the safety manuals for the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves were reviewed as part of the 2020 surveillance audit. The manuals were in compliance with the requirements of IEC 61508

5.2 Hardware Assessment

To evaluate the hardware design of the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves, two Failure Modes, Effects, and Diagnostic Analysis were performed by *exida* for each component in the products. This is documented in [R1] and [R2].

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. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA failure rates are derived for each important failure category. All failure rate analysis results and useful life limitations are listed in the FMEDA reports [R3] and [R4].

Note, as the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves are only one component of a final element, the SFF must be calculated for the entire final element combination if following the Route 1_H hardware architectural constraints. It is the end users' responsibility to confirm this for each particular application and to include all components of the final element in the calculations.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore, the reviewed VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves meets the Route 2_H hardware architectural constraints for up to SIL 2 at HFT=0 when the listed failure rates are used.

The analysis shows that designs of the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves can meet the hardware requirements of IEC 61508, SIL 3 depending on the complete final element design. The Hardware Fault Tolerance, PFD_{AVG}, and Safe Failure Fraction (when not following Route 2_H) requirements of the IEC 61508 must be verified for each specific design.

6 2020 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Bifold Fluidpower Ltd	Manufacturer of the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Bifold Fluidpower Ltd contracted *exida* in 2020 to perform the surveillance audit for the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves. The surveillance audit was conducted remotely.

6.2 Surveillance Methodology

As part of the IEC 61508 functional safety surveillance audit the following aspects have been reviewed:

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if any of the changes could affect the safety function of the VBP Volume Boosters, PPV Pilot Valves and HIPEX Valves.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the exida Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

6.3 Surveillance Results

6.3.1 Procedure Changes

Changes to the Procedures highlighted in gray in section 2.4.1 were reviewed and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period. One minor modification [D081] was reviewed and all documentation was found to be acceptable.

6.3.3 Impact Analysis

The impact analysis for the modification mentioned in 6.3.2 was reviewed and found to be consistent with the requirements of IEC 61508:2010.

6.3.4 Field History

The field histories during the surveillance period were analyzed and found to be consistent with the failure rates predicted by the FMEDA.

6.3.5 Safety Manual

The updated safety manual [D079e] was reviewed and found to be compliant with IEC 61508:2010.

6.3.6 FMEDA Update

The FMEDA was not updated as part of this project.

6.3.7 Evaluate use of certificate and/or certification mark

The certification mark is appropriately displayed on the Bifold Fluidpower Ltd Website.

6.3.8 Previous Recommendations

There were no previous recommendations to be assessed at this audit.

7 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.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
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 the Partial Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent 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.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2

8 Status of the Document

8.1 Liability

exida prepares reports based on methods advocated in International standards. *exida* accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

8.2 Version History

Contract Number	Report Number	Revision Notes
Q20-05-039	BIF 09-10-25 R003 V4R1	Revised per 2020 Surveillance audit, TES
Q17-05-126	BIF 09-10-25 R003 V3R1	Revised per 2017 Surveillance audit, S. Close
Q17-01-083	BIF 09-10-25 R003 V2R2	Added VBP-04, 06 & 12, S. Close
Q14-03-083	BIF 09-10-25 R003 V2R1	Revised per Surveillance audit, S. Close
Q14-03-083	BIF 09-10-25 R003 V1R1	Draft

Reviewer: Loren Stewart, *exida*, 7/31/2020

Status: Released, 7/31/2020

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Ted E. Stewart, CFSP, exidaCSP
Program Development & Compliance Manager

Loren L. Stewart, CFSE, Senior Safety Engineer