



IEC 61508 Functional Safety Assessment

Project:

FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P,
FP06P, FP10P and FP15 Series Solenoid and Interface Valves

Customer:

Bifold Fluidpower Ltd.
Chadderton, Greater Manchester
United Kingdom

Contract No.: Q21-03-178

Report No.: BIF 17/05-128 R002

Version V1, Revision R3, May 26, 2021

Ted Stewart



Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the following Series of Solenoid and Interface Valves:

- FP01, FP02, FP03, FP04, FP05 and FP15 Hydraulic Solenoid Valves
- FP02 and FP05G Gas Service Solenoid Valves
- FP03P, FP06P and FP10P Pneumatic Solenoid Valves
- FP15 & FP15E Low- and High-Pressure Pilot Interface Valves

Models included in this analysis are devices with a single Solenoid (up to 10W) including the Spring Return Manual Override, Detented Manual Override and the Manual Override Cover Assembly.

Only De-energize to Trip applications have been evaluated.

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* 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.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3 for mechanical components. A full IEC 61508 Safety Case was prepared using the *exida* Safety Case tool as the primary audit tool. Hardware 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 FP01, FP02, FP03, FP04, FP05, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid & Interface Valves were found to meet the Systematic Capability requirements of IEC 61508 for up to SC 3 (SIL 3 Capable)

The FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves were found to meet the Random Capability requirements for a Type A device of SIL 2@HFT=0, SIL 3@HFT=1 for all models using Route 2_H.



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





Table of Contents

Management Summary	2
1 Purpose and Scope	6
1.1 Tools and Methods used for the assessment	6
2 Project Management.....	7
2.1 <i>exida</i>	7
2.2 Roles of the parties involved	7
2.3 Standards and Literature used	7
2.4 Reference documents	7
2.4.1 Documentation provided by Bifold Fluidpower Ltd.	7
2.4.2 Documentation generated by <i>exida</i>	10
2.5 Assessment Approach	10
3 Product Description	12
4 IEC 61508 Functional Safety Assessment.....	14
4.1 Methodology	14
4.2 Assessment level	14
5 Results of the IEC 61508 Functional Surveillance Safety Assessment	15
5.1 Lifecycle Activities and Fault Avoidance Measures	15
5.1.1 Functional Safety Management	15
5.1.2 Safety Requirements Specification and Architecture Design.....	16
5.1.3 Hardware Design.....	16
5.1.4 Validation.....	16
5.1.5 Verification.....	17
5.1.6 Proven in Use.....	17
5.1.7 Modifications	17
5.1.8 User documentation.....	17
5.2 Hardware Assessment	18
6 2020 IEC 61508 Functional Safety Surveillance Audit.....	19
6.1 Roles of the parties involved	19
6.2 Surveillance Methodology	19
6.3 Surveillance Results.....	20
6.3.1 Procedure Changes.....	20
6.3.2 Engineering Changes	20
6.3.3 Impact Analysis	20
6.3.4 Field History	20
6.3.5 Safety Manual Review	20
6.3.6 FMEDA Update	20
6.3.7 Evaluate use of certificate and/or certification mark	20



6.3.8 Previous Recommendations	20
7 Terms and Definitions.....	21
8 Status of the Document	22
8.1 Liability	22
8.2 Version History.....	22
8.3 Future Enhancements	22
8.4 Release Signatures.....	22



1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the following Series of Solenoid and Interface Valves:

- FP01, FP02, FP03, FP04, FP05 and FP15 Hydraulic Solenoid Valves
- FP02G and FP05G Gas Service Solenoid Valves
- FP03P, FP06P and FP10P Pneumatic Solenoid Valves
- FP15 & FP15E Low- and High-Pressure Pilot Interface 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 [R5]).



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.

2.2 Roles of the parties involved

Bifold Fluidpower Ltd. Manufacturer of the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves

exida Performed the hardware assessment

exida Performed the IEC 61508 Functional Safety Assessment

Bifold Fluidpower Ltd. originally contracted *exida* in 2006 with the IEC 61508 Functional Safety Assessment of the above-mentioned devices.

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

Documents highlighted in grey below have been revised during the latest surveillance audit.

2.4.1 Documentation provided by Bifold Fluidpower Ltd.

Doc ID	Generic Document Name	Project Document Name	Version	Date
D001	Quality Manual	Management System Manual	11	3/22/2021
D003	Overall Development Process	02-2-01 Design and Development.docx	3	03/18/2018
D003b	Design and Development Procedure	02-2-01 Design and Development.docx	3	03/18/2018
D004	Configuration Management Process	QCDR - Documents & Records.pdf	1	1/16/2012
D004b	Configuration Management Process	02-3-04 - Creating-amending-deleting kits.doc	1	5/08/2014
D005	Field Failure Reporting Procedure	04-3-08 Customer Returns Procedure	1	05/13/2016



D006	Field Return Procedure	04-3-08 Customer Returns Procedure	1	05/13/2016
D007	Manufacturer Qualification Procedure	04-2-14 SQA MANUAL.pdf	53	03/18/2021
D008	Part Selection Procedure	02-2-01 Design and Development.docx	3	03/18/2018
D010	Quality Management System (QMS) Documentation Change Procedure	04-2-02 - Control of Documents & Records.pdf	7	03/16/2021
D012	Non-Conformance Reporting procedure	04-2-05 - Control of Non-Conforming Product.pdf	5	01/09/2018
D013	Corrective Action Procedure	04-2-06 - Corrective & Preventative Actions.pdf	4	05/10/2019
D016	Action Item List Tracking Procedure	02-2-01 Design and Development.docx	3	03/18/2018
D019	Customer Notification Procedure	04-3-05 Customer Escalation Procedure.pdf	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	8	
D023c	Change Order Example	CO1508.pdf	2	6/9/2014
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	
D026	FSM Plan or Development Plan	02-2-01 Design and Development.docx	3	03/18/2018
D026b	FP15 Pilot Operated FSM Plan or Development Plan	FP15 - Design File Summary.pdf		18-Jun-2015
D030	Shipment Records 2014-2017	Field Returns vs deliveries 2014 to 2017 - Exida.xlsx		16-Oct-2017
D031	Field Returns Records 2014-2017	Field Returns vs deliveries 2014 to 2017 - Exida.xlsx		16-Oct-2017
D033	Training Procedure	BMC18.8 [Training].doc	18.8	
D034	Skills Matrix	Sil - Technical Skills Matrix.pdf	2	10/20/2010
D036b	3rd Party Assessment	FP1x_Assessment - signed.pdf		6/28/2005
D040	Product Requirements Specification FP05G 150 bar	FP05G 150 bar Gas Service Qualification Specification_Rev 0.doc	0	
D040b	Data Sheet FP05G	FP05G_S1_M_32_NC_S_77A-24D_57.pdf	15/0	2013
D040c	Product Requirements Specification FP05G 210 bar	FP05G 210 bar Gas Service Qualification Specification_Rev 1.doc	1	28-Nov-13
D040d	Product Brochure FP01	05 - FP01 Solenoid.pdf	6	23-Feb-05
D040e	Product Brochure FP06P-FP10P-FP12P	09 - FP06P-FP10P-FP12P.pdf	7	7-Apr-05



D040f	Product Brochure FP15	06 - FP15 Solenoid.pdf	4	Feb 2007
D040g	Product Catalog FP 02, FP03, FP04 & FP05	FP02 FP03 FP04 FP05 Catalogue BFD10 Oct 10.pdf		1-Oct-10
D040h	FP15 Pilot Operated Product Requirements Specification	12 - FP15 Interface Pilot (January 2013).pdf		Jan 2015
D069	Validation Test Plan	02-2-02 Factory Acceptance Testing.docx	1	5/15/2014
D074	Validation Test Results FP05G	DP0036 - DC-QR21 - FP05G Low Pressure Pilot Proof and Function Test 01-1....pdf		11/1/2012
D074b	Validation Test Results FP05G	DP0036 - DC-QR21 - FP05G High Pressure Pilot Proof and Function Test 01-....pdf		11/1/2012
D074c	Validation Test Results FP05G	DP0036 - DC-QR21 - Test notes 210 bar 20k Endurance Test 23-08-13.pdf		8/23/2013
D074d	FP15 Pilot Operated Validation Test Results	FP15-L2-127 mod report.pdf		21-Jan-2005
D074e	FP15 Pilot Operated Pressure Qualification Test Results	DC-QR - Qualification Pressure Test Data FP15 1035 Bar.pdf		22-Jul-2009
D075	Environmental Test Results FP05G	DP0036 - DC-QR21 - Test notes high temp.pdf		10/8/2013
D075b	Environmental Test Results FP05G	DP0036 - DC-QR21 - Test notes low temp.pdf		10/8/2013
D078	Operation / Maintenance Manual Mechanical Operators FP06P, FP10P and FP12P	FP OIM, July 05.doc	1	7/1/2005
D078b	Operation / Maintenance Manual Mechanical Operators FP02, FP03, FP04 & FP05	OP0143_3.pdf	3	4/28/2021
D078c	Operation / Maintenance Manual Mechanical Operators FP02G & FP05G	OP0179_0.pdf	0	2/11/2014
D078d	Operation / Maintenance Manual Mechanical Operators FP03P	OPB0009_0.pdf		
D078e	Operation / Maintenance Manual Mechanical Operators FP10P	OPB0026_1.pdf	1	
D078f	Operation / Maintenance Manual Mechanical Operators FP06P	OPB0027_3.pdf	1	
D078g	Operation / Maintenance Manual Mechanical Operators FP01	OP0113_3.pdf	2	10/22/2009



D078h	FP15 Operation / Maintenance Manual	OP0131_0.pdf	15	4-Sep-2012
D079	Safety Manual FP02G & FP05G	SM.002_2 FP02G & FP05G - Gas Valve- Safety Manual.pdf	2	10/31/2017
D079b	Safety Manual Pneumatic FP Solenoid Valves	SM.001_5 FP Pneumatic Solenoid Valves.pdf	4	21-Feb-2018
D079e	Safety Manual Hydraulic FP Solenoid Valves	SM.004_4 Hydraulic Solenoid Valves- Safety Manual.pdf	4	30-Oct-2017
D079f	Safety Manual FP15 Interface Valve	SM.018_1 FP15 Interface Valve Safety Manual.pdf	1	30-Oct-2017
D081	Engineering Change Documentation 2008 to 2011	FP01-6-10-15 Design Changes 2.xlsx		6/31/2011
D081b	Change Order Form	DOCUMENT CHANGE ORDER.docx	8	
D088	Impact Analysis Record	CO3456.docx		1-Dec-2016
D089	Assembly & Test Procedure FP01	PI.0080		1/7/2008
D090	Assembly & Test Procedure FP10	PI.0110		5/23/2007
D091	Assembly & Test Procedure FP15	PI.0132		1/29/2008
D092	Design and Development Procedure	02-3-01 Creating New Drawings	1	05/21/2014
D093	Filter Test Request	QTR0114	1	4/9/2021
D094	Filter Test Request	QTR0117	1	4/16/2021

2.4.2 Documentation generated by *exida*

[R1]	BIF 17/05-128 R001 V1R3, May 26, 2021	FMEDA report - FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves
[R2]	BIF 16/10-005 R005 V1R4, 13-Oct-2017	FMEDA Report - FP15 & FP15E Low- and High-Pressure Pilot Interface Valves
[R3]	BIF Q14-06-031 V4 Safety Case FP Series, 5/28/2020	Bifold FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface Valves IEC 61508 Compliance SafetyCase (internal database)
[R4]	Q20-08-014 FP Series PIU 2017-2020	PIU analysis, shipping and field returns 2017-2020
[R5]	BIF Baseline_SC_R5	Bifold Baseline IEC 61508 Compliance SafetyCase

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

Table 1 gives an overview of the different versions and options that were considered in the assessment of the valves. Models included in this analysis are devices with a single Type 77 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 valve covered in this assessment



Table 1 Version Overview

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

The FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface Valves are classified as devices that are part of a Type A¹ 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 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 [R3] and [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 FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface Valves have been assessed per IEC 61508 to the following levels:

- Systematic Capability SC3 (SIL 3 capability) as the development procedures were assessed as 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) and SIL 3 for a single device where the SFF for the complete final element is >90% (if using Route 1_H).



5 Results of the IEC 61508 Functional Surveillance 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 during the surveillance audit in 2014 and is documented in the SafetyCase [R3] and [R5].

The current development process is fully compliant with IEC 61508. However, portions of the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves were developed prior to the establishment of this IEC 61508 SIL 3 compliant development process. Consequently, for the evaluation of systematic fault avoidance measures, proven in use claims were also considered in addition to the existing design documentation and additional documented safety analysis which showed the design integrity. The SafetyCase was created with project specific design documents. Future modifications to the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 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 the Quality Manual and in the Design and Development Procedure 02-2-01. These are also part of Bifold's Quality Management System which is ISO 9001 approved. The same process is used for modifications. 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 3 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 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 documented in procedure 02-2-01. Templates, forms and sample documents are provided. The process used for modifications is procedure 02-3-02. 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. Procedures QCDR and 02-2-04 require that all design documents be version controlled. Document revisions were evident during the audit.



Procedure 04-2-02 Describes the Control of Documents and Records. Quality documents are classified as levels 1, 2 & 3. Level 1 & 2 are the high-level documents and company operating procedures. Level 3 includes Process Instructions and work instructions. All quality documents are version controlled. Document revisions were evident during the audit.

Training, Competency recording

Personnel training records are kept per standard quality procedures. BMC 18 states that the Quality Manger and Heads of Department are responsible for ensuring that only qualified personnel and are used to perform the design and development tasks. Bifold Fluidpower Ltd. hired *exida* Consulting 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 FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves, the simple safety functionality is the primary functionality of the product (Close / Open Valve). Therefore, no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the valve designs are relatively simple and are 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, D007 and D089 to D091. 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-trying components, and computer-aided design tools. This meets SIL 3.

5.1.4 Validation

Validation Testing is done via a documented plan created that links to the product's requirements specifications and also includes compliance testing per application and agency standards. Bifold also maintains a set of standard tests per D069 that are used to validate their designs. As the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface Valves are purely electro-mechanical devices with a simple safety function, there is no separate integration testing necessary. The FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 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 procedure 02-2-01. 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 3.

5.1.6 Proven in Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was carried out on the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Valves during the certification renewal activity. Shipment records from July 2008 to April 2011 were used to determine that the Bifold FP Series Valves have >800 million operating hours 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. All changes receive an impact analysis which is documented as part of form DC/QR3. This meets the requirements of IEC 61508 SIL 3.

Modifications were reviewed as part of a certification renewal activity.

5.1.8 User documentation

Bifold Fluidpower Ltd. has created Safety Manuals for the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves, see D079 to D079g. These safety manuals were assessed by *exida*. They 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.



5.2 Hardware Assessment

To evaluate the hardware design of the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Valves, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* Consulting for each component in the system. 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 [R1] and [R2].

Note, if the Bifold FP Series Valve is only one part 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 user's 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, all of the reviewed FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface Valves meet the Route 2_H hardware architectural constraints for up to SIL 2 at HFT=0 when the listed failure rates are used, and SIL 3 applications with a HFT=1.

The analysis shows that design of the Bifold FP Solenoid and Interface 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 FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface 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* to perform the surveillance audit for the FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series Solenoid and Interface 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 FP01, FP02, FP03, FP04, FP05, FP02G, FP05G, FP03P, FP06P, FP10P and FP15 Series 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

Procedure changes were reviewed and found to be consistent with the requirements of IEC 61508:2010.

6.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period. Several Change Orders were reviewed and were found to be consistent with the previously audited modification procedure [D023].

6.3.3 Impact Analysis

An impact analyses is performed on every change order. Several were reviewed and were found to be consistent with the requirements of IEC 61508:2010.

6.3.4 Field History

The field histories [D030 & D031] of these products during the surveillance period were analyzed and found to be consistent with the failure rates predicted by the FMEDA.

6.3.5 Safety Manual Review

The safety manuals were reviewed and found to be compliant with IEC 61508:2010.

6.3.6 FMEDA Update

The FMEDA's and reports [R2 & R4] were 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.
<i>exida</i> 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
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
Q21-03-178	BIF 17/05-128 R002 V2, R2	Analyzed stainless steel gauze filter; GPS
Q20-08-014	BIF 17/05-128 R002 V2, R1	2020 Surveillance audit update; TES 11/13/2020
Q17-05-128	BIF 17/05-128 R002 V1, R2	Revised 2.4.1 Document List
Q17-05-128	BIF 17/05-128 R002 V1, R1	Supersedes all BIF 06/01-17 R002 Assessment Reports. Revised per 2017 surveillance audit.

Reviewer: Greg Sauk, *exida*, May 26, 2021

Status: Released, May 26, 2021

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Ted E. Stewart, CFSP, *exida*CSP
Program Development & Compliance Manager

Gregory Sauk, CFSE, Senior Safety Engineer