Management Summary

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

FP100 Valve Assembly - VA1077

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 creation of a detailed safety case against the requirements of IEC 61508.

- exida reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

The functional safety assessment was performed to the requirements of IEC 61508, SIL 2. A full IEC 61508 Safety Case was prepared, using the exida SafetyCaseDB™ 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 VA1077 Valve Assembly was found to meet the Systematic Capability requirements of IEC 61508 for up to SC 2 (SIL 2 Capable)

The VA1077 Valve Assembly was found to meet the Random Capability requirements for a Type A device of SIL 2@HFT=0 using Route 2„.

The manufacturer will be entitled to use the Functional Safety Logos.
# Table of Contents

Management Summary ................................................................................................... 2

1 Purpose and Scope ................................................................................................... 4

2 Project Management .................................................................................................. 5
   2.1 *exida* ................................................................................................................ 5
   2.2 Roles of the parties involved ............................................................................... 5
   2.3 Standards and Literature used .......................................................................... 5
   2.4 Reference documents......................................................................................... 5
       2.4.1 Documentation provided by Bifold Fluidpower Ltd. ........................................ 5
       2.4.2 Documentation generated by *exida* ............................................................. 6

3 Product Description ................................................................................................. 7

4 IEC 61508 Functional Safety Assessment .................................................................. 8
   4.1 Methodology ....................................................................................................... 8
   4.2 Assessment level ................................................................................................. 8

5 Results of the IEC 61508 Functional Safety Assessment .......................................... 9
   5.1 Lifecycle Activities and Fault Avoidance Measures .......................................... 9
       5.1.1 Functional Safety Management ................................................................... 9
       5.1.2 Safety Requirements Specification and Architecture Design ...................... 10
       5.1.3 Hardware Design ....................................................................................... 10
       5.1.4 Validation .................................................................................................. 10
       5.1.5 Verification ................................................................................................ 11
       5.1.6 Proven In Use ........................................................................................... 11
       5.1.7 Modifications ............................................................................................ 11
       5.1.8 User documentation .................................................................................. 11
   5.2 Hardware Assessment ......................................................................................... 12

6 Terms and Definitions ............................................................................................. 13

7 Status of the Document .......................................................................................... 14
   7.1 Liability ............................................................................................................. 14
   7.2 Releases ............................................................................................................. 14
   7.3 Future Enhancements ....................................................................................... 14
   7.4 Release Signatures ............................................................................................. 14
1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the FP100 Valve Assembly - VA1077 by exida according to the requirements of IEC 61508: ed2, 2010.

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.
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 300 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 the largest process equipment database of failure rates and failure modes with over 60 billion unit operating hours.

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 FP100 Valve Assembly - VA1077
exida Performed the hardware assessment
exida Performed the IEC 61508 Functional Safety Assessment

Bifold Fluidpower Ltd. contracted exida in 2012 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

2.4.1 Documentation provided by Bifold Fluidpower Ltd.

| [D2] | A0474, Rev 0, 5/19/98 | Pot1/X Assembly Drawing |
| [D3] | A0211, Rev 1, 5/2/01 | Cartridge Check Valve - 690 BAR Assembly Drawing |
| [D4] | VA1034, 0, 1/25/12 | Adaptor Manifold Assy, General Arrangement Drawing and BOM |
| [D5] | VA1077, Rev 2, 8/1/12 | FP100 Assy + Double FP01 NC+SV Pilots, General Arrangement Drawing and BOM |
| [D6] | A0897, Rev 0, 2/1/10 | FP01/SX/M/32/NC/X-7X Assembly Drawing |
| [D7] | 0-GA0156, Rev 0, 9/15/08 | Solenoid Operator Assembly Drawing |
| [D8] | BOM VA1077 | BOM for VA1077 Assembly |
2.4.2 Documentation generated by exida

<table>
<thead>
<tr>
<th>[R1]</th>
<th>Bifold VA1077 FMEDA R1.xls, 5/30/2013</th>
<th>Failure Modes, Effects and Diagnostic Analysis,- FP100 Valve Assembly - VA1077 (internal document)</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R2]</td>
<td>BIF Q12/11-114 R001 V1R2, 8/6/2013</td>
<td>FMEDA report - FP100 Valve Assembly - VA1077</td>
</tr>
<tr>
<td>[R3]</td>
<td>Bifold Safety Case.esc</td>
<td>Bifold FP100 Valve Assembly - VA1077 IEC 61508 Compliance SafetyCaseDB (internal database)</td>
</tr>
<tr>
<td>[R4]</td>
<td>PIU Bifold VA1077-FP100 R3.xls</td>
<td>Proven In Use analysis (internal document)</td>
</tr>
<tr>
<td>[R5]</td>
<td>BIF 12-11-114 R002 V1R1 IEC 61508 Assessment.doc, 8/16/2013</td>
<td>IEC 61508 Functional Safety Assessment for FP100 Valve Assembly - VA1077 (This document)</td>
</tr>
</tbody>
</table>
3 Product Description

The Bifold Fluidpower Ltd. FP100 Valve Assembly - VA1077 is a specially configured Valve Assembly with built-in redundancy of the Solenoid valves, to control the supply and return of fluid from a hydraulic actuator. It is designed for use in hazardous and corrosive environments.

Table 1 gives an overview of the different versions that were considered in the FMEDA and IEC 61508 assessments of the VA1077. Only De-energize to Trip applications have been evaluated.

Table 1 Version overview

<table>
<thead>
<tr>
<th>Device</th>
<th>Description / Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA1077 Assembly</td>
<td>VA1077 Assembly, 2oo2 Solenoid DTT Application</td>
</tr>
<tr>
<td>VA1077 Assembly</td>
<td>VA1077 Assembly, 2oo2 Solenoid DTT Application w/PVST</td>
</tr>
</tbody>
</table>

The FP100 Valve Assembly - VA1077 are classified as a Type A\(^1\) devices 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].

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 FP100 Valve Assembly - VA1077 have been assessed per IEC 61508 to the following levels:

- Systematic Capability SC 2 (SIL 2 capability) as the Proven In Use analysis justified that this device is suitable for use in applications with a maximum Safety Integrity Level of 2 (SIL 2) 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 on-site and is documented in the SafetyCase [R3].

The current development process is fully compliant with IEC 61508. However, portions of the VA1077 Valve Assembly were developed prior to the establishment of this IEC 61508 SIL 2 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 VA1077 Valve Assembly must be made per the IEC 61508 SIL 2 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 BCM04 and BOP 4.1. 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 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 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 2.

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 BCM04 [D13] and BOP 4.1 [D14]. 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 TD 001 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 VA1077 Valve Assembly, 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 [D12] and [D18] to [D19]. This meets SIL 2.

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 2.

5.1.3 Hardware Design
The design process is documented in [D12] to [D14]. 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 TD 001 [D12]), structured design, modularization, use of well-tried components, and computer-aided design tools. This meets SIL 2.

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 (documented in DC/QR17) that are used to validate their designs. As the FP100 Valve Assembly - VA1077 are purely electro-mechanical devices with a simple safety function, there is no separate integration testing necessary. The VA1077 Valve Assembly performs 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 2.

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 2.
5.1.5 Verification

The development and verification activities are also defined in BCM04 and BOP 4.1 ([D13] and [D14]). 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

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was carried out on the FP100 Valve Assembly - VA1077 during the certification activity. Shipment records from 2008 to 2012 were used to determine that the sub assembly components of the VA1077 have >3 million operating hours and that they have demonstrated a field failure rate in line with the failure rates indicated in the FMEDA reports. This meets the requirements for Proven In Use for SIL 2.

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 and documented per the Change Order Impact Analysis procedure TD 011. This meets the requirements of IEC 61508 SIL 2.

5.1.8 User documentation

Bifold Fluidpower Ltd. has created a Safety Manual for the VA1077 Valve Assembly, see [D22]. 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 2.
5.2 Hardware Assessment

To evaluate the hardware design of the VA1077 Valve Assembly, a Failure Modes, Effects, and Diagnostic Analysis was performed by exida 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 report [R2].

Note, as the VA1077 is only one component of a final element, the SFF must be calculated for the entire final element combination if following the Route 1\textsubscript{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\textsubscript{H}. Therefore the reviewed FP100 Valve Assembly - VA1077 meets the Route 2\textsubscript{H} hardware architectural constraints for up to SIL 2 at HFT=0 when the listed failure rates are used.

The analysis shows that design of the VA1077 can meet the hardware requirements of IEC 61508, SIL 2 depending on the complete final element design. The Hardware Fault Tolerance, PFDAVG, and Safe Failure Fraction (when not following Route 2\textsubscript{H}) requirements of the IEC 61508 must be verified for each specific design.
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 2H 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
7 Status of the Document

7.1 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.

7.2 Releases

Version: V1
Revision: R1
Version History: V1, R1: Released; August 16, 2013
V0, R1: Draft; August 8, 2013
Authors: Gregory Sauk
Review: Steven Close; August 16, 2013
Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

______________________________
Gregory Sauk, CFSE, Senior Safety Engineer

______________________________
Steven Close, Senior Safety Engineer