# IEC 61508 Functional Safety Assessment

Project:
Quick Exhaust Valves

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

Contract No.: Q18/02-353
Report No.: BIF 15/03-004 R002
Version V3, Revision R1, May 31, 2018
Steven Close

## Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the following Bifold Quick Exhaust Valves:

Models included in this analysis are devices with a single Solenoid (up to 10W) and without manual overrides or reset options. 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 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 3. 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 Quick Exhaust Valves were found to meet the Systematic Capability requirements of IEC 61508 for up to SC 3 (SIL 3 Capable)**

**The QEV 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

# 1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the following Bifold Quick Exhaust Valves:

**Table 1 Version overview**

| Model No. | Description |
|---|---|
| S06-QEV: | 1/4" NPT |
| AS06-QEV: | 1/4" NPT Arctic Service |
| S06-QEV-K6: | QEV BSPP PORTS |
| AS06-QEV-K6: | QEV BSPP PORTS Arctic Service |
| | |
| AS09-QEV-K6: | 3/8" BSPP QEV Arctic Service |
| AS09-QEV: | 3/8" NPT QEV Arctic service |
| S09-QEV: | 3/8"NPT QEV |
| S09-QEV-K6 | 3/8" BSPP QEV |
| | |
| ASE12-QEV: | 1/2" NPT QEV Arctic Service (Economy Body) |
| AS12-QEV-K6: | 1/2" BSPP QEV Arctic Service |
| AS12-QEV: | 1/2" NPT Arctic Service |
| S12-QEV: | 1/2" NPT QEV |
| | |
| S19-QEV | 3/4" NPT QEV |
| S19-QEV-K6 | 3/4" BSPP QEV |
| AS19-QEV | 3/4" NPT QEV Arctic Service |
| | |
| S25-QEV | 1" NPT QEV |
| S25-QEV-K6 | 1" BSPP QEV |
| AS25-QEV | 1" NPT QEV Arctic Service |
| | |
| QEV15 | ¼" to ½" NPT Hydraulic Service |
| QEV50 | ½" NPT Hydraulic Service |

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.

## 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.

All assessment steps were continuously documented by *exida* (see [R1] to [R3]).

# 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 250 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 Quick Exhaust Valves |
| *exida* | Performed the hardware assessment |
| *exida* | Performed the IEC 61508 Functional Safety Assessment |

## 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.

| Doc ID | Generic Document Name | Project Document Name | Version | Date |
|---|---|---|---|---|
| D001 | Quality Manual | Quality Manual- v6.pdf | 6 | 3/27/2017 |
| D003 | Overall Development Process | 02-2-01 Design and Development.docx | 2 | 12/21/2015 |
| D003b | Design and Development Procedure | 02-2-01 Design and Development.docx | 2 | 12/21/2015 |

| | | | | |
|---|---|---|---|---|
| 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 | 1/16/2012 |
| D005 | Field Failure Reporting Procedure | 04-3-08 Valve Returns.pdf | 1 | 5/6/2014 |
| D006 | Field Return Procedure | QD 026 Valve Returns.pdf | 1 | 4/14/2009 |
| D007 | Manufacturer Qualification Procedure | SQA MANUAL.pdf | 4 | Apr-14 |
| D008 | Part Selection Procedure | 02-2-01 Design and Development.docx | 2 | 12/21/2015 |
| D010 | Quality Management System (QMS) Documentation Change Procedure | 04-2-02 - Control of Documents & Records.pdf | 5 | 6/23/2016 |
| D012 | Non-Conformance Reporting procedure | 04-2-05 - Control of Non Conforming Product.pdf | 4 | 1/5/2016 |
| D013 | Corrective Action Procedure | 04-2-06 - Corrective & Preventative Actions.pdf | 2 | 8/15/2014 |
| D016 | Action Item List Tracking Procedure | 02-2-01 Design and Development.docx | 2 | 12/21/2015 |
| D019 | Customer Notification Procedure | 02-3-05 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 | 8 | |
| D026 | FSM Plan or Development Plan | 02-2-01 Design and Development.docx | 2 | 12/21/2015 |
| D026b | QEV Hydraulic Development Plan | QEV Development Plan.pdf | 0 | 9/23/2004 |
| D030 | Shipment Records | Pneumatic QEV Sales.xlsx | | 5/25/2018 |
| D033 | Training Procedure | BCM18.8 [Training].DOC | 18.8 | |
| D034 | Skills Matrix | SIL - Technical Skills Matrix SM.002.pdf | 2 | 5/8/2015 |
| D036 | ISO 900x Cert or equivalent | ISO9001 Cert 2015-2018.pdf | 1 | 8/10/2014 |
| D040 | Product Requirements Specification QEV | Catalogue 19a - QEV Quick Exhaust Valves March 2013.pdf | 0 | 1-Mar |
| D040b | Product Requirements Specification QEV | Models to be Certified Document Matrix.xlsx | 0 | 2-Mar |
| D040c | QEV Hydraulic Design Brief | QEV50 Design Brief.pdf | 0 | 31-Aug |
| D041 | QEV Hydraulic Final Design Review | QEV - Final Design Review.pdf | | 12/6/2004 |
| D041b | QEV Hydraulic Design Review Minutes | QEV Design Review Minutes.pdf | | 9/22/2004 |
| D069 | Validation Test Plan | 02-2-02 Factory Acceptance Testing.docx | 1 | 5/15/2014 |

| | | | | |
|---|---|---|---|---|
| D069b | Production Validation Test Plan | PCP.0035_0 Quick Exhaust & Shuttle Valve.pdf | 0 | 4/14/2015 |
| D069c | Production Validation Test Document Pack | BM41609 - Document Pack.pdf | 0 | 9/16/2015 |
| D069d | QEV Hydraulic Qualification Procedures | QEV Qualification Procedures.pdf | 0 | 9/15/2004 |
| D074 | QEV Hydraulic Flow Test Graph | QEV - Flow Test Graphs.pdf | | |
| D074c | QEV Hydraulic Pressure Test Plan | TP0050_0.pdf | 0 | 6/21/2006 |
| D075 | QEV Hydraulic Environmental Test Results QEV15/08/10/SA | TRTP0348_0 QEV15-08-10-SA.pdf | 0 | 10/27/2016 |
| D075b | QEV Hydraulic Environmental Test Results QEV15/08/10/V | TRTP0348_0 QEV15-08-10-V.pdf | 0 | 10/25/2016 |
| D075c | QEV Hydraulic Environmental Test Results QEV50/08/10/V | TRTP0348_0 QEV50-08-05-V.pdf | 0 | 10/28/2016 |
| D078 | Operation / Maintenance Manual Mechanical Operators QEV | OPB0002_0.pdf | 0 | |
| D078b | Catalog QEV | Catalogue 19a - QEV Quick Exhaust Valves March 2013.pdf | | 3/1/2013 |
| D078c | QEV Hydraulic Operation / Maintenance Manual QEV | OP0129_1.pdf | 1 | 7/1/2014 |
| D079 | Safety Manual QEV | SM.010_1 Pneumatic QEV Safety Manual.pdf | 1 | 8/19/2015 |
| D079b | QEV Hydraulic Safety Manual | SM.016_0 - Hydraulic QEV Safety Manual.pdf | 0 | 10/27/2016 |
| D081b | Change Order Form | DOCUMENT CHANGE ORDER.docx | 8 | |

| | | | | |
|---|---|---|---|---|
| D083 | PIU Analysis | BIF 15-03-004 PIU QEV.xls | R0 | 9/14/2025 |
| D083b | QEV Hydraulic PIU Analysis | Q16-10-005 QEV Hydraulic PIU.pdf | | 10/10/2016 |
| D088 | Impact Analysis Record | CO4028.pdf | | 4/27/2018 |
| D088b | Impact Analysis Record | CO4044.pdf | | 5/9/2018 |

Note: Documents highlighted in gray were evaluated as part of the assessment of the QEV15 & QEV 50 Hydraulic Valves

### 2.4.2 Documentation generated by *exida*

| | | |
|---|---|---|
| [R1] | Q16-10-005 R006 V1R1 Hydraulic QEV FMEDA Report.doc, 10/26/2016 | Failure Modes, Effects and Diagnostic Analysis, - QEV Hydraulic |
| [R2] | BIF Q15-03-004 V1 Safety Case QEV.xls10/20/2016 | Bifold Quick Exhaust Valves IEC 61508 Compliance SafetyCaseWB (internal database) |
| [R3] | BIF 15-03-004 PIU QEV.xls | PIU analysis, shipping, field return and modification listings 2010 to 2014. |
| [R4] | Q16-10-005 QEV Hydraulic PIU.xls | PIU analysis, shipping, field return QEV Hydraulic, 2012 to 2016. |
| [R5] | BIF 18-02-353 QEV PIU.xlsx | PIU analysis, shipping, field return QEV, 2014 to 2018. |

## 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
- Safety Requirement Specification

- Change and modification management
- Hardware design / probabilistic modeling
- Hardware V&V activities including documentation
- Hardware-related operation, installation and maintenance requirements

# 3 Product Description

The Bifold Fluidpower Ltd. Quick Exhaust Valves are designed to exhaust the output port quickly upon removal of the input signal.

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

**Table 2 Version overview**

| Model No. | Description |
|---|---|
| S06-QEV: | 1/4" NPT |
| AS06-QEV: | 1/4" NPT Arctic Service |
| S06-QEV-K6: | QEV BSPP PORTS |
| AS06-QEV-K6: | QEV BSPP PORTS  Arctic Service |
| | |
| AS09-QEV-K6: | 3/8" BSPP QEV Arctic Service |
| AS09-QEV: | 3/8" NPT QEV Arctic service |
| S09-QEV: | 3/8"NPT QEV |
| S09-QEV-K6 | 3/8" BSPP QEV |
| | |
| ASE12-QEV: | 1/2" NPT QEV Arctic Service (Economy Body) |
| AS12-QEV-K6: | 1/2" BSPP QEV Arctic Service |
| AS12-QEV: | 1/2" NPT Arctic Service |
| S12-QEV: | 1/2" NPT QEV |
| | |
| S19-QEV | 3/4" NPT QEV |
| S19-QEV-K6 | 3/4" BSPP QEV |
| AS19-QEV | 3/4" NPT QEV Arctic Service |
| | |
| S25-QEV | 1" NPT QEV |
| S25-QEV-K6 | 1" BSPP QEV |
| AS25-QEV | 1" NPT QEV Arctic Service |
| | |
| QEV15 | ¼" to ½" NPT Hydraulic Service |
| QEV50 | ½" NPT Hydraulic Service |

The Quick Exhaust Valves 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 [R2].

## 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 Quick Exhaust 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 [R2].

The current development process is fully compliant with IEC 61508. However, portions of the QEV 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 QEV 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 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 QEV, 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 D89 to D91. 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 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 Quick Exhaust Valves are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The QEV perform only one Safety Function, which is extensively tested under various conditions during validation testing. See [D074], [D074c], [D075], [D075b] & [D075c].

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 Quick Exhaust Valves during the certification renewal activity. Shipment records from 2010 to 2015 were used to determine that the Bifold Quick Exhaust Valves have >900 million operating hours and they have demonstrated a field failure rate less than the failure rates indicated in the FMEDA reports. In addition, shipment records for the Hydraulic versions from 2012 to 2016 were used to determine that the hydraulic versions have >100 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.

The modification process has been successfully assessed and audited, so Bifold Fluidpower Ltd. may make modifications to this product as needed.

- As part of the *exida* scheme a surveillance audit is conducted every 3 years. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.
    - List of all anomalies reported
    - List of all modifications completed
    - Safety impact analysis which shall indicate with respect to the modification:
        - The initiating problem (e.g. results of root cause analysis)
        - The effect on the product / system
        - The elements/components that are subject to the modification
        - The extent of any re-testing
    - List of modified documentation
    - Regression test plans

### 5.1.8 User documentation

Bifold Fluidpower Ltd. has created a Safety Manual for the QEV, [D079]. The 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.

## 5.2 Hardware Assessment

To evaluate the hardware design of the QEV, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* Consulting for each component in the system. This is documented in [R1].

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 [R1].

Note, if the Bifold Quick Exhaust Valves 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 Quick Exhaust 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 Quick Exhaust 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 2018 IEC 61508 Functional Safety Surveillance Audit

## 6.1 Roles of the parties involved

| | |
|---|---|
| Bifold Fluidpower Ltd. | Manufacturer of the Quick Exhaust Valves. |
| *exida* | Performed the hardware assessment review |
| *exida* | Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme. |

## 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 Quick Exhaust 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 2.4.1 were reviewed and were found to be consistent with the requirements of IEC 61508.

### 6.3.2 Engineering Changes

Two engineering changes [D088] & [D088b] were reviewed. The changes were made to improve the manufacturing process. The changes were executed per the approved modification procedure[D023]

### 6.3.3 Impact Analysis

The review of the engineering changes also included a review of the impact on functional safety. The impact analysis [D088] & [D088b] was documented as part of the modification process.

### 6.3.4 Field History

The field histories from 2014 to 2018 for the Quick Exhaust Valves were analyzed and found to be consistent with the failure rates predicted by the FMEDA.

### 6.3.5 Safety Manual

The latest versions of the safety manuals were reviewed and were 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 Bifold Fluidpower Ltd. website was searched and no misleading or misuse of the certification or certification marks was found.

### 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 Releases

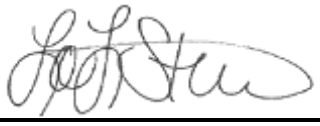
| | | |
|---|---|---|
| Version History: | V3, R1: | Recertification, May 31, 2018 |
| | V2, R1: | Added the QEV15 & QEV50 Hydraulic Valves. October 28, 2016 |
| | V1, R2: | Revised Tables 1 & 2, October 5, 2015 |
| | V1, R1: | Released, September 23, 2015 |
| | V0, R1: | Draft, S. Close |
| Authors: | Steven Close | |
| Review: | Ted Stewart | |
| Release status: | Released | |

## 8.3 Future Enhancements

At request of client.

## 8.4 Release Signatures

Steven F. Close, Safety Engineer



Loren L. Stewart, CFSE, Senior Safety Engineer