SIL – SM.017 Rev 1

Flow Line Pilot Valve

Compiled By : G. Elliott, Date: 01/11/2016

Bifold Group
Bifold
Bifold FluidPower
Bifold Subsea
Bifold Marshalsea

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Innovative and Reliable Valve & Pump Solutions

Contents

Terminology Definitions 3
Acronyms & Abbreviations 4

1. Introduction 5
   1.1 Scope 5
   1.2 Relevant Standards 5
   1.3 Other related documents and papers 5
2. Device Description 5
   2.1 Safety Function 5
   2.2 Environmental Limits 5
   2.3 Application Limits 5
   2.4 Design Verification 5
   2.5 SIL Capability 6
   2.5.1 Systematic Integrity 6
   2.5.2 Random Integrity 6

3. Installation & Commissioning 7
   3.1 Installation 8
   3.2 Proof testing 8
   3.3 Repair & Replacement 9
   3.4 Useful Life 9
   3.5 Reporting Concerns to Bifold 9

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Terminology Definitions:

Description	Explanation
Safety:	Freedom from unacceptable risk of harm
Functional Safety:	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment / machinery / plant / apparatus under control of the system.
Basic Safety:	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition.
Safety Assessment:	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems.
Fail-Safe State:	Single, Low (falling), NO : State where the valve is in the open position. Single, High (rising), NO : State where the valve is in the closed position. Single, Low (falling), NC : State where the valve is in the closed position. Single, High (rising), NC : State where ethe valve is in the open position. Twin : State where the valve is closed to supply pressure and open to vent.
Safe Failure	Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Dangerous Failure	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Dangerous Undetected Failure	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Dangerous Detected:	Failure that is dangerous but is detected by automatic stroke testing.
Fail Annunciation Undetected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
Fail Annunciation Detected:	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.
Fail No Effect:	Failure of a component that is part of the safety function but that has no effect on the safety function.
Low demand mode:	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Acronyms / Abbreviations

Acronym / Abbreviation	Description	Explanation
CCF	Common Cause Failure	A common cause failure is one in which a single failure or condition affects the operation of multiple devices that would otherwise be considered independent. Common cause failures can result in the SIS failing to function when there is a process demand.
FITS	Failures in Time	The number of failures that can be expected in one billion (10^9) device-hours of operation.
FMEDA	Failure Modes, Effects & Diagnostics Analysis	A method of assessing a hardware device in order to predict failure rates and hence determine the applicable SFF.
HFT	Hardware Fault Tolerance	Ability of a functional device to continue to perform a required function when faults or errors are prevailing.
LOPA	Layers of Protection Analysis	LOPA is a methodology for hazard evaluation and risk assessment.
MTBF	Mean Time Between Failures	Mean time Between Failures. (1/ λ).
MTTR	Mean Time To Repair	Mean time between the occurrence of an error in a unit or system and its repair.
OIM	Operation & Installation Manual	Information on correct installation, maintenance and testing.
PFD	Probability of Failure on Demand	Probability of failures for a safety function on demand
PFDavg	Average Probability of Failure on Demand	Average Probability of failures for a safety function on demand
PTI	Proof Test Interval	The time between diagnostic testing or Partial Stroke Testing.
SIL	Safety Integrity Level	The international standard IEC61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for the failure of a safety function. The higher the SIL level the lower the probability that they will not perform the required safety function
SFF	Safe Failure Fraction	The proportion of non-hazardous failures.
λ	Failure Rate	Failure Rate – the ratio of the total number of failures in a given time period
λD	Dangerous Failure Rate	Failure Rate of Dangerous failures (per hour).
λDD	Dangerous Detected Failure rate	Failure Rate of Dangerous failures detected by diagnostic testing (per hour).
λDU	Dangerous Undetected Failure Rate	Failure Rate of Dangerous failures Undetected by diagnostic testing (per hour).
λS	Safe Failure Rate	Failure Rate of Safe failures (per hour).

1. Introduction

1.1 Purpose & Scope

This manual provides the results of a functional safety assessment by Exida Consulting in accordance with IEC61508: ed2: 2010.

The results of this provides the safety instrumentation engineer with the required failure data as per IEC61508 / IEC 61511, and confidence that sufficient attention has been given to systematic failures during the development of the device.

1.2 Relevant Standards

IEC 61508 (Parts 1 – 7) Ed2: 2010 - Functional Safety of Electrical /Electronic/Programmable Electronic Safety-Related Systems.

1.3 Other Related documents and papers

Exida FMEDA Report : BIF 16-10-005 R002 V1R1FMEDA Report PSV5

.Device	Document ID	Document Type
PSV5A / PSV5E	OP0131	Operating & Installation Manual
PSV5A / PSV5E	17 - Flowline Pilot (PSV5A, PSV5E)	Product Catalogue

2. Device Description

The PSV5 valve is designed to switch a low pressure (pneumatic/gas/mineral oil) logic signal at a pre-set flowline pressure (Natural Gas / Crude Oil). Different diameter sensing pistons realise the different switching pressure ranges. The PSV5 can be supplied as a single unit or as a double unit on a common manifold block.

Single Configuration

A single sensing valve set up to trip the main valve on either a rise or a fall in system pressure.

(Trip High, Rising): A single unit will monitor the system pressure, and trip out if the pressure exceeds the pre-determined set point.

(Trip Low, Falling): A single unit will monitor the system pressure, and trip out if the pressure falls below the pre-determined set point.

Twin Configuration

A Twin unit comprises two separate sensing valves on a common manifold, each sensing the system pressure, to trip the main valve on both a rise and a fall in system pressure.

(Trip High, Rising) One sensing valve will trip the valve if the supply pressure exceeds the pre-determined (High) set point.

(Trip Low, Falling): The other sensing valve will trip the valve if the supply pressure falls below the pre-determined set point.

2.1 Safety Function

In the even of a trip, the control pressure is vented.

The PSV5A / PSV5E are designed to be part of a final element subsystem as defined by IEC61508 and the achieved SIL level of the designed function must be verified by the system designer.

2.2 Environmental Limits

The designer of a SIF must verify that the product is rated for use within the expected environmental limits.

For SIL rated valves the minimum operating temperature is Arctic Service Option to -50°C.

Refer to Bifold Product Catalogue for more information.

2.3 Application Limits

The materials of construction are specified in the various Bifold Catalogues and Data Sheets.
Maximum Operating Pressure is up to 700 Bar.

2.4 Design Verification

A Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report has been carried out independently by Exida.com and is available from Bifold on request.
The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFDaverage considering architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

When using the Flow Line Pilot Valve in a redundant configuration, a common cause factor of 10% should be included in safety integrity calculations.
The failure rate data listed the FMEDA report is only valid for the useful life time of a valve.
The failure rates will increase sometime after this time period.
Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

2.5 SIL Capability

2.5.1 Systematic Integrity

The product has met manufacturers design process requirements of **Safety Integrity Level SIL 3.**

These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without “prior use” justification by end user or diverse technology redundancy in the design.

2.5.2 Random Integrity

The Flow Line Pilot Valve is classified as a device that is part of a TYPE A element according to IEC 61508, Having a hardware fault tolerance (HFT) of 0. If the SFF of the subsystem is >90%, and the PFDavg < 10^{-3}, the design can meet SIL 3 @ HFT=0.

When the final element assembly consists of many components (Solenoid Valve, quick exhaust valve, etc.) the SIL must be verified for the entire assembly using failure rates from all components.
This analysis must account for any hardware fault tolerance and architecture constraints.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the Route 1H approach according to 7.4.4.2 of IEC 61508 or the Route 2H approach according to 7.4.4.3 of IEC 61508.

The Route 1H approach involves calculating the Safe Failure Fraction for the entire element.

The Route 2H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The Flow Line Pilot Valve meets the exida criteria for Route 2H; therefore, the PSV5A / PSV5E can be classified as a 2H device. When 2H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1). If Route 2H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1H.

3.0 Installation and Commissioning

3.1 Installation

The device must be installed per standard practices outlined in the Installation Manual. The environment must be checked to ensure that environmental conditions do not exceed the ratings.

The device must be accessible for physical inspection.

3.2 Proof Testing

The System should be subjected to a full test at least once every 12 months (or more frequently based on the desired PFDavg calculations – Ref Section 2.4). This would normally be conducted as part of a proof test or partial stroke test for the actuator under control. Partial stroke testing of the Safety Instrumented Function (SIF) must provide a full test of the device.

According to section 7.4.3.2.2 f) of IEC61508-2, proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

3.2.1 Suggested Proof Test

The suggested proof test consists of a full stroke of the device, as described in the table below.

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip
2	Interrupt or change the flowline signal to the PSV5 to confirm that the PSV5 trips at the specified set point
3	Restore the flowline pressure to the PSV5 and inspect for any leaks, visible damage or contamination and confirm that the normal operating state was achieved.
4	Remove the bypass otherwise restore normal operation.

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

3.3 Repair and Replacement

Repair procedures must be implemented as per the Operation, Installation and Maintenance Manual for the device.

The SIL rating of the device will be voided if the repair is not performed with Genuine Bifold parts and serviced by a competent person.

3.4 Useful Lifetime for the Device.

The Product lifetime of the Flow Line Pilot Valve is 20 Years. (Provided the device is maintained in accordance with the Bifold Operation, Installation & Maintenance Manual). This implies a useful life of 10 years.

3.5 Reporting Concerns to Bifold

All faults to be reported to Bifold for recording purposes, by contacting the Quality Department at the supplying facility listed at the bottom of the page. All defective devices must be returned to Bifold for investigation and rectification by the Manufacturer. A Valve Return and Service Report form (VRSR) – available upon request, from the supplying facility - (Contact details at the foot of this page) must be completed and returned with the device.

Bifold Group Ltd,
Head Office,
Greenside Way,
Middleton,
Manchester M24 1SW.
Tel: +44 (0) 161 345 4777
Fax: +44 (0) 161 345 4780
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Marshalsea Hydraulics Ltd
Marshalsea House,
Venture Way,
Priorswood Industrial Estate,
Taunton, Somerset, TA2 8DE. UK.
Tel: +44 (0) 1823 331081
Fax: +44 (0) 1823 323382
Email: info@marshalsea.co.uk
Web: www.bifold.co.uk

USA Office
Bifold Fluidpower Ltd
11490 Westheimer,
Suite 850,
Houston, TX 77077.
Tel: +1 (713) 783 4253
Fax: +1(713) 783 0067
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk

Singapore Office
Bifold Fluidpower Ltd
Toa Payoh Industrial Park,
Block 1002, Lorong 8 #07-1475,
Singapore 3109075
Tel: +65 6735 1323
Fax: +65 6735 1367
Email: marketing@bifold.co.uk
Web: www.bifold.co.uk