

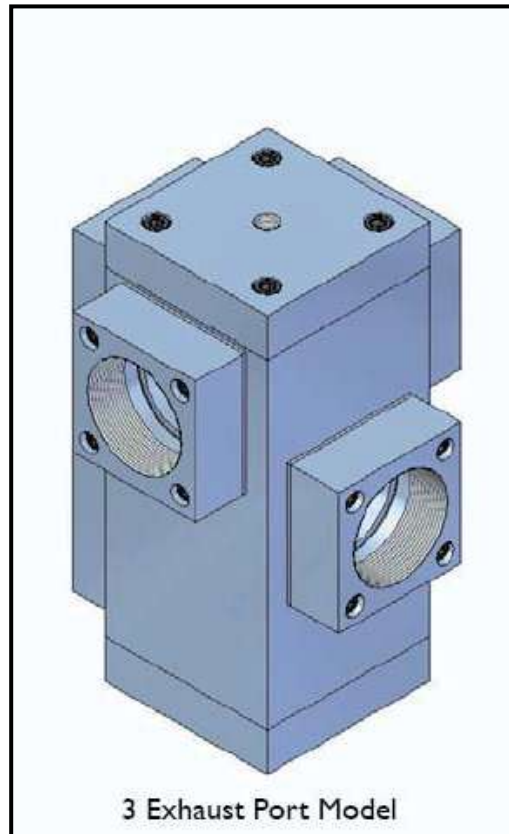
SIL – SM.0007 Rev: 4



PPV - Pneumatic Pilot Valve

Compiled By : G. Elliott,

Date: 8/14/2014



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 |

Terminology Definitions:

| Description | Explanation |
|-------------------------------------|--|
| <i>Safety:</i> | Freedom from unacceptable risk of harm |
| <i>Functional Safety:</i> | 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. |
| <i>Basic Safety:</i> | 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. |
| <i>Safety Assessment:</i> | The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems. |
| <i>Fail-Safe State:</i> | State where solenoid valve is de-energized and spring is extended. |
| <i>Safe Failure</i> | Failure that causes the valve to go to the defined fail-safe state without a demand from the process. |
| <i>Dangerous Failure</i> | Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state). |
| <i>Dangerous Undetected Failure</i> | Failure that is dangerous and that is not being diagnosed by automatic stroke testing. |
| <i>Dangerous Detected:</i> | Failure that is dangerous but is detected by automatic stroke testing. |
| <i>Fail Annunciation Undetected</i> | 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. |
| <i>Fail Annunciation Detected:</i> | 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. |
| <i>Fail No Effect:</i> | Failure of a component that is part of the safety function but that has no effect on the safety function. |
| <i>Low demand mode:</i> | Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency. |

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. ($1/\lambda$). |
| 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 |
| PFD _{avg} | 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 |
| λ_D | Dangerous Failure Rate | Failure Rate of Dangerous failures (per hour). |
| λ_{DD} | Dangerous Detected Failure rate | Failure Rate of Dangerous failures detected by diagnostic testing (per hour). |
| λ_{DU} | Dangerous Undetected Failure Rate | Failure Rate of Dangerous failures Undetected by diagnostic testing (per hour). |
| λ_s | 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 of the Bifold Pneumatic Pilot Valve Series (PPV), 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 09-10-25 R003 V2R1 FMEDA

| Device | Document ID | Document Type |
|--------------------|-----------------------------------|---------------------------------|
| PPV 24 & 32 Series | | Data Sheet |
| PPV 24 & 32 Series | OPB0032 | Operating & Installation Manual |
| PPV 24 & 32 Series | 10 - SPR & PPV Catalogue 20_06_13 | Product Catalogue |

2. Device Description

Bifold Fluidpower's PPV series poppet valves are positively sealed, for low pressure applications up to 10 bar (145 psi). This range of SIL 3 rated 1 1/2" and 2" valves offers the highest flow available in the market and satisfies the demands of exceedingly large swept volume and/or fast acting valve actuators controlling pipeline ESD, process plant, or similar valve applications. PPV Valves are available as 1, 2 or 3 port exhaust units offering exceptional versatility and flow.

Manufactured from 316L grade stainless steel the valves are suited for offshore and other corrosive atmospheres. Materials can be certified compliant to NACE MR-01-75 rendering the valves suitable for sour gas media. Low temperature elastomer seals are also available for arctic service applications.

2.1 Safety Function

When de-energised (signal removed), the valve moves to its fail-safe position. The valve will operate to close off the flow path through the valve body, and divert it to tank / exhaust.

The PPV - Pneumatic Pilot Valves 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 10 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 PFD_{average} 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 PPV - Pneumatic 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.

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.

| λ_{sd} | λ_{su} | λ_{dd} | λ_{du} | $SFF\% = 1 - \frac{\lambda_{du}}{(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du})}$ | λ_{sd} | λ_{su} | λ_{dd} | λ_{du} | $SFF\% = 1 - \frac{\lambda_{du}}{(\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du})}$ |
|---|----------------|----------------|----------------|--|---|----------------|----------------|----------------|--|
| Please refer to the Exida FMEDA report for specific Lambda Values | | | | | Please refer to the Exida FMEDA report for specific Lambda Values | | | | |

2.5.2 Random Integrity

The valve is a **Type A Device**.

Therefore, based on the SFF between 60% and 90%, when the valve is used as the only component in a final element subassembly, a design can meet SIL 2 @ 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.

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 Device 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 parts 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. This test will detect of the possible DU failures of the PPV - Pneumatic Pilot Valve, when PVST is not being performed.

| Step | Action |
|------|--|
| 1 | Bypass the safety function and take appropriate action to avoid a false trip |
| 2 | Send a signal to the device to perform a full stroke and verify that this is achieved. |
| 3 | Inspect the device for any visible damage or contamination. |
| 4 | Remove the bypass otherwise restore normal operation. |

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 valve 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 useful lifetime of the PPV - Pneumatic Pilot Valve is 20 years or 20,000 cycles - whichever occurs first.

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.