Safety Integrity Level (SIL)
Safety Manual
3/2 & 5/2 Single Acting and 5/2 Dual Coil (fail last) – including overrides.

IOM: TECHUK-101		**Revision:** 2	
Prepared By: S. Hayes	**Date:** 10/21/14	**Drafting Work Order:** 25101	**ECN:** 13819
Reviewed By: E. Barroso	**Date:** 7/7/22	**Approved By:** M. Patel	**Date:** 7/13/22

Description of Product

The Westlock Falcon range of pneumatic/solenoid pilot operated valves designed for being directly mounted onto Westlock Control Monitors can utilize either
3/2 or 5/2 spring return or 5/2 dual coil (stay put) valve actions in either direct acting valves for use as either pilot operator or as standalone valves.

Table of Contents

1. Purpose and Scope.

This document provides an overview of the user responsibilities for installation, operation and maintenance of the PRODUCT in order to maintain the designed Safety Integrity Level. Items that will be addressed are proof testing, repair and replacement of the product, lifetime, environmental and application limits.

2. Device Safety Function.

When de-energized, the Falcon Solenoid Pilot Valve moves to its fail-safe position. Depending on the solenoid specified Normally Closed (NC) or Normally Open (NO), the valve will supply actuation air / gas or vent the actuation air / gas depending on the piping of the installation. Please note that the solenoid pilot valve must be piped to the actuator in accordance with the recommendation and allowable desired function.

The valve is intended to be part of final element subsystem as defined per IEC 61508 and the achieved SIL level of the designed function must be verified by the designer.

3. Design Verification.

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_{avg} considering redundant architectures, 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 a Falcon solenoid in a redundant configuration, a common cause factor of 5% should be included in safety integrity calculations.

The product has met manufacturer 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.

3.1 Random Integrity.

The solenoid valve is a Type A Device. Therefore when used as the only component in a final element sub-assembly, a design can meet SIL 3 @ HFT=1 and SIL 2 @HFT=0 [SFC1]

Using the PRODUCT.

4 Setup and Installation.

No special installation is required in addition to the standard installation practices outlined in the Installation & Operation Manual that is supplied with every product.

4.1 Proof test.

The objective of proof testing is to detect failures within the PRODUCT that are not detected by diagnostics. Of main concern are undetected failures that prevent the safety-instrumented function from performing its intended function.

The frequency of proof testing, or the proof test interval, is to be determined in reliability calculations for the safety instrumented functions for which the PRODUCT is applied. The proof tests must be performed more frequently or as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

A field proof-test is to be carried out annually as a minimum.

4.2 Repair and replacement.

The Falcon valve can only be repaired when using the correct repair kit available from Westlock Controls. Please contact the sales office quoting the works order number as indicated on the wiring diagram of the original Control Monitor.

No special tools are required to refurbish pneumatic seals. All servicing should only be undertaken by suitably qualified engineers.

Any failures that are detected and that compromise functional safety should be reported to the QA Supervisor / Senior engineer at Westlock Controls.

4.3 Warranty Statement.

Westlock Controls provides a full warranty for all its products against defects in workmanship or materials of construction, subject to handling, storage, installation and operation within the stated parameters of the product. This warranty applies for 1 year from the date of dispatch from Westlock Controls. If, during this warranty period, the product is found by Westlock Controls to be defective then Westlock Controls will provide either a free of charge repair or replacement, depending on the preference of the customer. Westlock Controls warranty obligations are limited to those liabilities stated above irrespective of the cause.

4.4 Reliability data and lifetime limit.

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Westlock Controls. This report details all failure rates and failure modes, common cause factors for applications with redundant devices and the expected lifetime of the PRODUCT.

- In respect of the failure mode (insufficient actuation air / gas), the demonstration (by means of field and test data) of >75% safe failure [SFC2] fraction which makes it suitable for SIL 2 application when used in a simplex mode, without redundancy.
- In respect of the failure mode (failure to exhaust actuation air / gas), the demonstration (by means of field and test data) of >90% safe failure fraction which makes it suitable for SIL 3 application when used in a simplex mode, without redundancy.
- The reliability data listed the FMEDA report is only valid for the useful life time of the PRODUCT. The failure rates of the PRODUCT may increase sometime after this 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.

4.5 Environmental limits.

The environmental limits of the PRODUCT are specified in the respective catalogue and Installation and Maintenance Instructions. The designer of a SIF must check that the product is rated for use within the expected environmental limits.

4.6 Application limits.

The assumption of a high pressure/cycle annual proof- test and of refurbishment after 1 million operations.

A life time limit of 5 million cycles.
Temperature range of –40 to +80 degrees Celsius and a maximum working pressure of 10 bar.

Work Medium: Dry clean compressed air to ANSI/ISA S7.0.01-1996 (max 40 micron particle size).

A minimum of 1 operation per month is required to ensure free movement.

It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the valves are used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

4.7 Functional Safety Policy.

The Quality Manual emphasises that capability with respect of functional safety, is a specific design capability within Westlock Controls. Some contracts will relate to safety-related applications. Some developments will specifically target safety-integrity conformance as a design requirement.

For these instances the provisions of International Standard IEC 61508 (and related guidance) shall be met by the Westlock Controls quality management system.

4.8 Product Safety Engineer.

Any failures that are detected and that compromise functional safety should be reported to the QA Supervisor / Senior engineer who is responsible for all aspects of functional safety.

4.9 Competencies.

Westlock Controls shall maintain a "safety-related competence register" containing profiles of those individuals eligible to carry out functional safety assessment and design tasks. Periodically the senior management and Safety/ Engineering Supervisor will review the list.

5. Terms and Abbreviations.

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	The state where the solenoid is de-energized and its return spring holds the pilot in the closed position.
Fail Safe	Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	(DU) Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Fail Dangerous Detected	(DD) Failure that is dangerous but is detected by automatic stroke testing
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 one per year and no greater than twice the proof test frequency.

Further definitions of terms used for safety techniques and measures and the description of safety related systems are given in IEC 61508-4.

5.1 **Acronyms.**

FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance
MOC	Management of Change: These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIF	Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
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).

6. Product Construction.

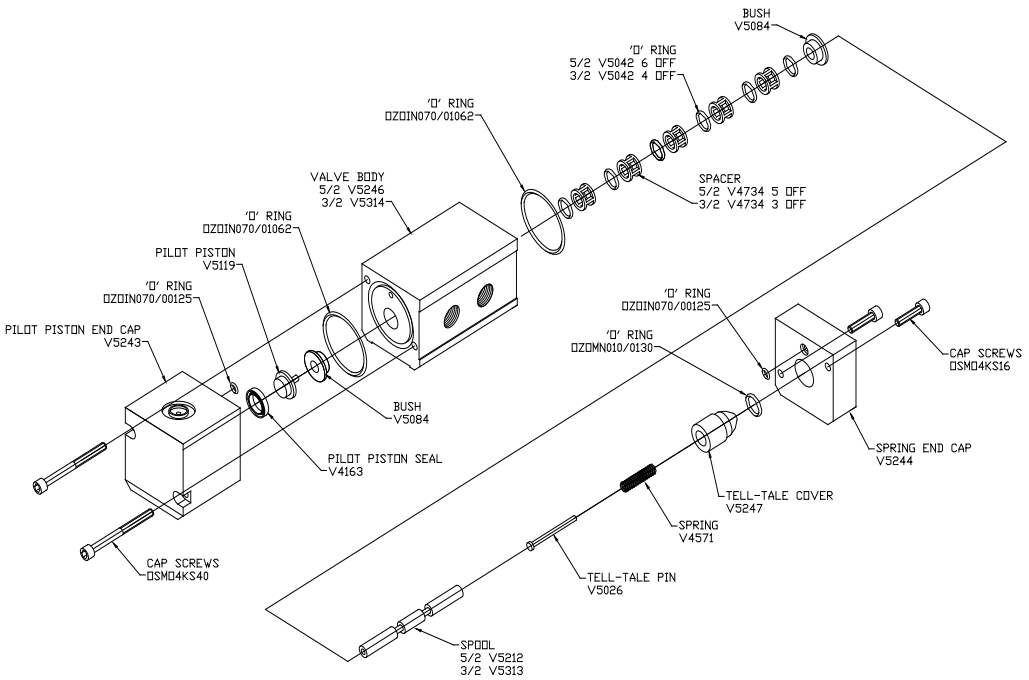
The valve typically comprises of:-

- A spring end cap made of anodised aluminium (Dural) or stainless steel.
- A body unit made of anodised aluminium (Dural) or stainless steel.
- A Pilot end cap made of anodised aluminium (Dural) or stainless steel.
- The spool is made from Hard Anodised Aluminium PTFE impregnated or stainless steel.

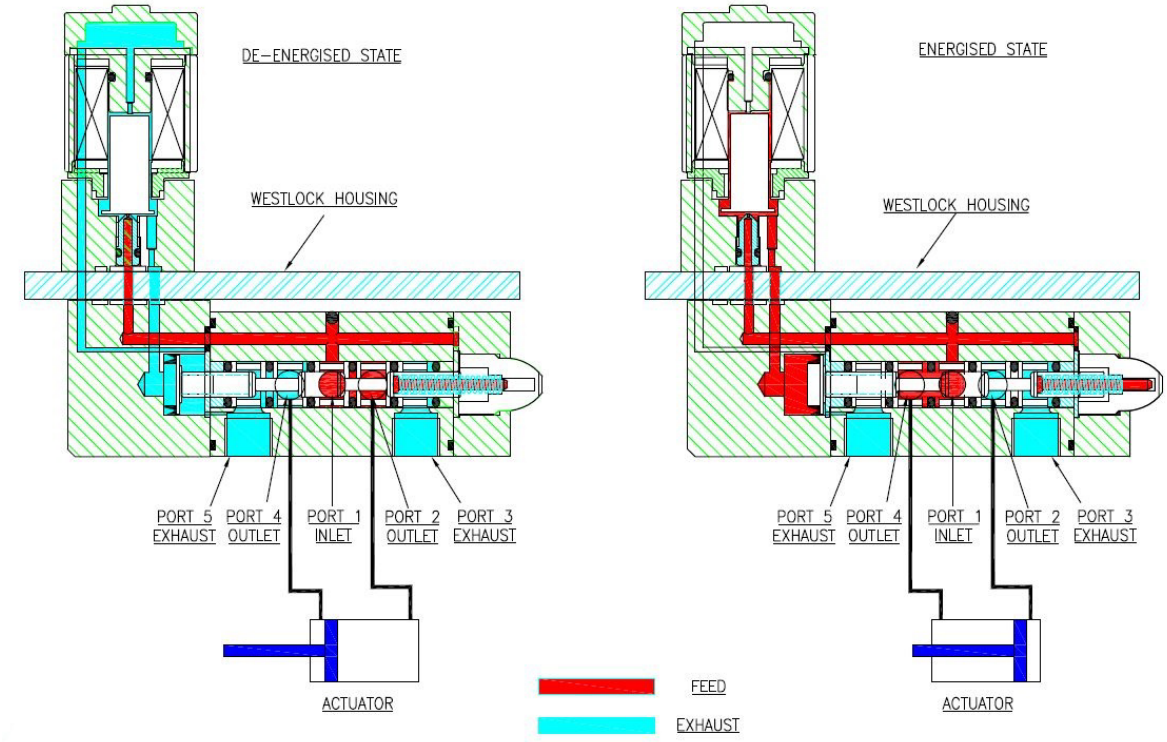
The basic design of a pneumatic pilot valve is shown below. It can be seen that the spring is located at the opposite end from the pilot piston and sits inside the spool. The pilot piston is located in the pilot end cap chamber it is connected to the spool by means of a tolerance fit. The spool along with the pilot piston and the spring are held in place by the seals and spacers and are guided by the brass bushes located at either end of the body. 4 stainless steel screws hold it all together.

The air supply is piped in to the pilot end cap through the coil, when the coil is energised the air pushes the piston to the edge of the chamber in turn pushing the spool along which in turn compresses the spring. When the coil is switched off the air supply is stopped and the spring pushes the spool and the pilot piston back.

Illustration of a typical valve arrangement



Typical Sectional Arrangement of Pilot Operated Spool Valve



De-energised position, the spool and pilot piston are forced against the inner face of the pilot end cap by the compression spring, pressurised air enters the valve body at port 1 and exits through port 2.

Energised position, pressurised air enters the pilot end cap, which forces the pilot piston and spool to move until final rest position, pressurised air enters the valve body at port 1 and exits through port 3.

Valve body allows pressurised air to flow through the inlet and outlet ports, provides support for the pilot piston, spool, spacers, bushes, springs and seals.

Spool oscillates within the valve body and allows pressurised air to flows through the inlet and outlet ports. Provides location for the pilot piston.

Pilot piston is located at the end of the spool and provides support and location for the pilot piston seal.

Pilot piston seal is located and secured to the pilot piston, when pressurised, airflows from the pilot piston end cap through drillings into the chamber and movement of the pilot piston takes place.

Spacer allows pressurised air to flow through the inlet and outlet ports, provides accurate positioning of `O` ring seals within the valve body.

Seals prevent air leakage within the valve body, withstand temperature range of –40 to +80 degrees Celsius and a pressure of 10 bar maximum.

Bushes provide bearing support for the spool.

Spring provides force on the spool (energised state), when the valve is de-energised, movement of the spool takes place.

Pilot piston end cap is secured to the valve body, provides support and location for the pilot piston, bearing bush and allows pressurised air to flow through drilling into the chamber.

Spring end cap is secured to the valve body, provides support and location for the spring and bearing bushes.

7. Product Support.

EUA

Westlock Controls.
280 North Midland Ave. - Saddle Brook, NJ 07663
Tel: (201) 794-7650 •Fax: (201) 794-0913

E-mail: westlockinfo@westlockcontrols.com
Internet http://www.westlockcontrols.com

8. Related Literature.

A full range of Installation and Maintenance manuals (IOM) are available for all Falcon solenoid valve combinations and are included in the relevant Control Monitor IOM documents.
They can be obtained free of charge by contacting Westlock Controls as indicated above.

9. Reference Standards.

Functional Safety – A straightforward guide to applying IEC61508 and related standards.

IEC 61508:2010 Functional Safety of electrical/electronic/programmable electronic safety-related systems.

ANSI/ISA 84.00.01-2004(IEC 61511Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector.