Safety Manual

A-Series Pressure Switch

Document: I&M009-10210
REV A - Release 4/19/2013

Table of Contents:

1 INTRODUCTION

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the A-Series pressure switch. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.1 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	State where solenoid valve is de-energized and spring is extended.
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	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Fail 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.

1.2 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.
PFDavg	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).

1.3 Product Support

Product support can be obtained from:

Ashcroft Inc., 250 East Main St., Stratford Ct. 06614

www.ashcroft.com

(203) 378-8281

1.4 Related Literature

Hardware Documents:

- Ashcroft A-Series Switch Installation, Operation and Maintenance Instructions

Guidelines/References:

- Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis, ISBN 1-55617-777-1, ISA
- Control System Safety Evaluation and Reliability, 2nd Edition, ISBN 1-55617-638-8, ISA
- Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISBN 1-55617-909-9, ISA

1.5 Reference Standards

Functional Safety

- IEC 61508: 2010 Functional safety of electrical/electronic/ programmable electronic safety-related systems
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety – Safety Instrumented Systems for the Process Industry Sector

2 DEVICE DESCRIPTION

The A-Series Pressure switch is an electrical switch which is actuated via inlet pressure. The switch will change state from normally closed (NC) to normally open (NO) as pressure increases. It will change state again from NO to NC as pressure decreases.

The switch is available in several configurations. The unit can be purchased as a factory set model (APS) where the switch point is set at the time of manufacture and is not adjustable, or a field adjustable model (APA) which can be adjusted by the end user. Each of these styles is available in a watertight housing or an explosion-proof housing. There are a variety of female or male pressure inlets available. There are also several electrical connectors available (18 awg wire leads, ½" conduit fitting, cable, spade terminals, Micro Din Form C connector). The switch can be purchased as a single-pole double throw switch (SPDT) or a double pole double throw switch (DPDT). Electrical ratings range from .1amps at 125Vdc to 5amps at 250Vdc depending on the type of switch ordered. Pressure ranges are available from -15psi through 7500psi with setpoints no greater than the maximum range of the product.

3 DESIGNING A SIF USING A MANUFACTURER PRODUCT

3.1 Safety Function

The A-Series switch will change states with changes in inlet pressure. Once an actuation pressure is achieved the switch will change state as described in Section 2 of this document. The designer of the SIF must consider if the alarm condition is on fall pressure or increasing pressure and adjust the switch accordingly. If a factory set switch is desired the product must be specified to change state at a predefined pressure and in the desired direction. When using the A-Series product with dual switches only one setpoint pressure can be used. That pressure will actuate both switches.

The A-Series switch 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.

3.2 Environmental limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the temperature limits labeled on the product, or the A-Series pressure switch datasheet available at www.Ashcroft.com.

3.3 Application limits

The materials of construction of an A-Series switch are specified in the Ashcroft A-Series pressure switch datasheet. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the A-Series pressure switch is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

3.4 Design Verification

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Ashcroft Inc. This report details all failure rates and failure modes as well as the expected lifetime.

The achieved Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) design must be verified by the designer via a calculation of PFDavg 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. The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the A-Series pressure switch and its failure rates.

When using an A-Series pressure switch in a redundant configuration, a common cause factor of at least 5% should be included in safety integrity calculations.

The failure rate data listed the FMEDA report is only valid for the useful life time of an A-Series pressure switch. 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.

3.5 SIL Capability

3.5.1 Systematic Integrity

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.

3.5.2 Random Integrity

The A-Series pressure switch is a Type A Device. Therefore based on the SFF between 60% and 90%, when the A-Series pressure switch is used in low trip applications, and as the only component in a final element subassembly, a design can meet SIL 2 @ HFT=0. When used in high trip applications the SFF is <60%; therefore the architectural constraints are SIL 1 @ HFT=0 & SIL 2 @ HFT=1.

When the element assembly consists of many components 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.

3.5.3 Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the A-Series pressure switch.

3.6 General Requirements

The system's response time shall be less than process safety time. The A-Series pressure switch will change state in less than 1 S under specified conditions.

All SIS components including the A-Series pressure switch must be operational before process start-up.

User shall verify that the A-Series pressure switch is suitable for use in safety applications by confirming the A-Series pressure switch's nameplate is properly marked.

Personnel performing maintenance and testing on the A-Series pressure switch shall be competent to do so.

Results from the proof tests shall be recorded and reviewed periodically.

The useful life of the A-Series pressure switch is discussed in the Failure Modes, Effects and Diagnostic Analysis Report for the A-Series pressure switch.

4 INSTALLATION AND COMMISSIONING

4.1 Installation

The A-Series pressure switch must be installed per standard practices outlined in the Installation Manual.

The environment must be checked to verify that environmental conditions do not exceed the ratings.

The A-Series pressure switch must be accessible for physical inspection.

4.2 Physical Location and Placement

The A-Series pressure switch shall be accessible with sufficient room for pressure and electrical connections and shall allow manual proof testing.

The A-Series pressure switch shall be mounted in a low vibration environment. If excessive vibration can be expected special precautions shall be taken to ensure the integrity of pneumatic connectors or the vibration should be reduced using appropriate damping mounts.

4.3 Pressure Connections

It is the responsibility of the designer of the SIF to ensure that the pressure tubing and connections used when installing the switch are rated for the operating pressure of the system, and do not restrict the pressure to the switch.

5 OPERATION AND MAINTENANCE

5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within an Ashcroft Switch that are not detected by any automatic diagnostics of the system. 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 an Ashcroft Switch is applied. The proof tests must be performed more frequently than or as frequently as specified in the calculation in order to maintain the required safety integrity of the safety instrumented function.

The following proof test is recommended. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to Ashcroft.

Table1: Recommended Proof Test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Adjust pressure to the switch and verify that switch trips under designed conditions.
3	Inspect the A-Series pressure switch for any visible damage or contamination. Note that the white housing vent is still in place. (A missing vent plug is indication of a possible pressure leak in the switch)
4	Record any failures in your company's SIF inspection database.
5	Remove the bypass and otherwise restore normal operation.

This test will detect >90% of possible DU failures in the A-Series pressure switch.

The person(s) performing the proof test of an A-Series pressure switch should be trained in SIS operations, including bypass procedures, switch maintenance and company Management of Change procedures. No special tools are required.

5.2 Repair and replacement

An A-Series switch is adjustable (APA version only) but is not repairable. If a failure has occurred the switch must be replaced. The person(s) replacing an A-Series pressure switch should be trained in SIS operations, including bypass procedures, switch maintenance and company Management of Change procedures.

5.3 Useful Life

The useful life of the A-Series pressure switch is 10 to 15 years, or 10,000 cycles

5.4 MANUFACTURER Notification

Any failures that are detected and that compromise functional safety should be reported to Ashcroft. Please contact Ashcroft customer service.

6 START-UP CHECKLIST

The following checklist may be used as a guide to employ the A-Series pressure switch in a safety critical SIF compliant to IEC61508.

#	Activity	Result	Verified	
			By	Date
	Design			
	Target Safety Integrity Level and PFDavg determined			
	Correct valve mode chosen (Fail-closed, Fail-open)			
	Design decision documented			
	Pneumatic compatibility and suitability verified			
	SIS logic solver requirements for valve tests defined and documented			
	Routing of pneumatic connections determined			
	SIS logic solver requirements for partial stroke tests defined and documented			
	Design formally reviewed and suitability formally assessed			
	Implementation			
	Physical location appropriate			
	Pneumatic connections appropriate and according to applicable codes			
	SIS logic solver valve actuation test implemented			
	Maintenance instructions for proof test released			
	Verification and test plan released			
	Implementation formally reviewed and suitability formally assessed			

#	Activity	Result	Verified	
			By	Date
	Verification and Testing			
	Electrical connections verified and tested			
	Pneumatic connection verified and tested			
	SIS logic solver valve actuation test verified			
	Safety loop function verified			
	Safety loop timing measured			
	Bypass function tested			
	Verification and test results formally reviewed and suitability formally assessed			
	Maintenance			
	Tubing blockage / partial blockage tested			
	Safety loop function tested			