ASCO®
Redundant Control System

Safety Manual for Safety Integrated Systems

exida®
SIL 3 Capable

TABLE OF CONTENTS

1 Introduction

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing an ASCO Redundant Control System, RCS. 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 the solenoid valve is de-energized and spring is extended.
- **Fail Safe Failure** - Failure which causes the valve to go to the defined fail-safe state without a demand from the process.
- **Fail 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).
- **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 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.
- **MTTFS** - Mean Time To Fail Spurious
- **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. An 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:
ASCO Customer Support / Technical Support.
160 Park Ave.
Florham Park NJ 07932, USA

support@ascovalve.com
Tel. (800) 524-1023 or (973) 966-2000
Fax. (973) 966-2628

1.4 Related Literature

- Hardware Documents: ASCO RCS Operation Guide # V9512, V9709, V9957, V9958, and V9959.
- 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: 2000 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 RCS Device Description

The RCS is an electro-mechanical and pneumatic system consisting of a set of two (2) or three (3) solenoid operated valves and possibly one (1) pneumatically operated valve. The valves are interconnected to allow different architectures for the control of pneumatically actuated block valves. It provides diagnostic components to verify the state of the devices as well as enabling online testing of the devices. These components are pressure or proximity switches monitoring the pneumatic pressures at critical points of the RCS assembly. In addition to the switches, an Automated Diagnostic Test, ADT, can be implemented in a safety rated logic solver (not included). The ADT provides the diagnostics necessary to achieve the safety ratings of the RCS. Alternatively, the Diagnostic Test can be initiated manually. Manually initiated tests are very effective. However, these tests cannot be considered automatic diagnostics in the sense of IEC 61508/IEC 61511.

Depending on the protected process, the safety action of the block valve can either be spring return open or spring return close. The spring forced block valve actuator will receive air supply to move the block valve to the safe state (NO) or the spring forced block valve actuator will be vented to move the block valve to the safe state (NC). The piston type actuator will receive air to one side and be vented on the opposite side to move the block valve to the safe state (DA). To account for these three action types, three different RCS versions are available for safety applications:

- Normally Closed (NC)
- Normally Open (NO)
- Double Acting (DA)

The NC version is used to vent air from a spring-forced actuator if the solenoids are de-energized, the NO version is used to supply air to a spring-forced actuator if the solenoids are de-energized. Both versions differ only in the air duct routing within the manifold that connects the valves and the external ports.
The selection of the version has direct impact on the probability of failure on demand of the entire safety instrumented function since the loss of instrument air for a NO RCS will inhibit the safety action of the block valve and decrease safety integrity.

www.emerson.com

The selection of the NO/NC version is based on the spring forced state of the controlled actuator. Most safety applications will require that the vented state (spring forced position) of the block valve actuator be the safe state; however, exceptions may require the pressurized state (not spring forced position) of the block valve actuator be the safe state. In this case, additional requirements to ensure the integrity and availability of all energy sources will be called for.

The Double Acting version is used with a piston type block actuator. The "safe" state of the process valve must be determined. The Double Acting RCS will control air to the side of the process valve actuating cylinder that will drive the process valve to the "safe" state and vent the opposite side of the process valve actuating cylinder in the same operation.

The RCS is available in a 1oo1 simplex, 1oo1 Hot Standby (HS), 2oo2 Normally Open (NO) & Normally Closed (NC), 2oo2 Double Acting (DA) and 2oo3 Normally Closed (NC) configuration. This manual covers the use of the RCS in all modes.

In this safety manual, the signals to the RCS are defined in de-energized-to-safe configuration. In the case of a 2oo2 configuration, at least one of the two solenoid operated valves in the RCS has to be energized to prevent the block valve from moving to the safe state. In a 2oo3 configuration at least two (2) solenoid operated valves in the RCS must be energized to prevent the valve from moving to the safe state.

The switches have both normally open and normally closed contacts to provide indication of valve state. Truth Tables contained in this manual provide status of the normally open contacts during various states.

3 Designing a Safety Instrumented Function using an ASCO RCS

3.1 Safety Function

When de-energized, the ASCO RCS moves to its fail-safe position. Depending on the version specified, Normally Closed (NC) or Normally Open (NO), the RCS will supply air or vent air depending on the piping of the installation. The Double Acting RCS, when de-energized, will supply air to one side of the cylinder and vent the opposite side of the cylinder at the same time.

As defined in IEC 61508, the RCS is intended to be a part of the final element subsystem 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.

Temperature: The RCS shall be mounted such that the internal temperature within the enclosure does not exceed the specified temperature limits shown in the unit's I&M.

3.3 Application limits

The application limits of an ASCO RCS are specified in the user manual, I&M:
- I&M V9512: 1oo1 and 2oo2 Aluminum with Pressure Switches
- I&M V9709: 1oo1 and 2oo2 Stainless steel with Pressure Switches.
- I&M V9957: 2oo2 Aluminum with Proximity Switches
- I&M V9958: 2oo3 Aluminum without diagnostics.
- I&M V9959: 2oo3 Aluminum with Proximity Switches

It is especially important that the designer checks for material compatibility considering on-site chemical contaminants and air supply conditions. If the RCS 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 ASCO Valves, Inc. Refer to the appropriate FMEDA report for all failure rates and the expected useful lifetime.
- 1oo1 Simplex, 1oo1 Hot Standby, 2oo2 with Pressure Switches (ASC 08-12-44)
- 1oo1 Simplex, 1oo1 Hot Standby, 2oo2 with Proximity Switches (ASC 15-04-065)
- 1oo1 Simplex, 1oo1 Hot Standby, 2oo2 with Stainless Steel construction (ASC 14-09-018)
- 2oo2, 2oo3 redundant with Pressure or Proximity switches (ASC 20-02-115)

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 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. The Exida exSILentia® tool is recommended for this purpose as it contains accurate models for the RCS and its failure rates.

When using an ASCO RCS in a redundant configuration, a common cause factor of 5% should be included in safety integrity calculations.

The failure rate data listed in the FMEDA report is only valid for the useful lifetime of an ASCO Solenoid. 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

This product has met manufacturer design process requirements for 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 RCS is a Type A Device.

The failure rate data used for the FMEDA meets the *exida* criteria for Route 2_H (See FMEDA report Section 5.1). Therefore, the Redundant Control System can be classified as a 2_H device when the listed failure rates are used. When 2_H 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) per Route 2_H. If Route 2_H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1_H.

When the final element assembly consists of many components (RCS, quick exhaust valve, actuator, isolation 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.

3.5.3 Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the RCS.

www.emerson.com

3.6 Connection of the RCS to the SIS Logic-solver

The RCS is connected to the safety rated logic solver which is actively performing the safety function as well as automatic diagnostics designed to diagnose potentially dangerous failures within the RCS. The isolating valves solenoid control power shall be supplied by the safety rated logic solver via the safety function output. Connections must be made according to the instructions supplied by the safety rated logic solver.

The output rating of the I/O module shall meet or exceed the electrical specifications of the valve solenoid:

Table 1 - Solenoid Specifications

Table 1.1 - Solenoid Specifications, Direct Current				
Wattage	Voltage (DC)	Min. Pull In (mA)	Drop Out (mA)	Coil Resistance @ 20°C, +-10% (Ohms)
1.4W	12	84	13.9	102
	24	42	7.0	410
	48	21	3.6	1640
	120	9	1.5	10,000

Table 1.2 - Solenoid Specifications, Alternating Current				
Wattage	Voltage (AC)	VA Holding	VA Inrush	Coil Resistance @ 20°C, +-10% (Ohms)
10.1W	120/60-110/50	25	50	85
	230/50-240/50			450

If the safety rated logic solver output module provides line-integrity testing by pulse tests or other means, the impedance range applicable for this test shall be within the RCS solenoid impedance.

If connected to a passive input module (a module that provides only the switching but not the switching energy), the external power supply shall meet all pertinent electrical safety requirements specified by the safety rated logic solver (i.e. IEC 61010).

The input rating of the I/O module shall meet the electrical specifications of the switches:

Construction		Pressure Switch		Proximity Switch
		Gold Contacts	Silver Contacts	Palladium Silver
Electrical Rating	DC	1A Resistive @28VDC 0.5A Inductive @28VDC	5A Resistive @28VDC 3A Inductive @28VDC 0.5A Resistive @125VDC	3A Resistive @ 24VDC
	AC	1A @125VAC	5A @ 125VAC or 250VAC	4A @120VAC 2A @240VAC

Table 2- Switch Specifications

NOTE: IEC 61508 requires de-rating, and the actual switch loads need to be less than the listed specifications.

If the safety rated logic solver input module requires line-end devices for open wire / short circuit wire protection, these devices shall be mounted at the terminal block of the RCS according to the logic-solver manufacturer's instructions.

If the logic-solver input module provides line-integrity testing by pulse tests or other means the impedance range applicable for this test shall be within the RCS pressure switch impedance.

3.7 General Requirements

- The system's response time shall be less than process safety time. The RCS will switch between two states in less than 500 ms.

- All SIS components including the RCS must be operational before process start-up.
- The ADT shall be run at least once per month or ten times within the expected hazard demand interval, whichever comes first. The ADT may be run as often as desired and is recommended every 24 hours.
- The user shall verify that the RCS is suitable for use in safety applications by confirming that the RCS nameplate is properly marked.
- The programming used to implement the ADT shall not be modified without the accomplishment of an impact analysis by a competent safety engineer.
- Personnel performing maintenance and testing on the RCS shall be competent to do so.
- Results from the ADT manually initiated tests, and proof tests shall be recorded and reviewed periodically.
  The useful life of the RCS is discussed in the Failure Modes, Effects and Diagnostic Analysis Report for the RCS.

4 <u>Installation and Commissioning</u>

4.1 Installation

- The ASCO Solenoid valve must be installed per standard installation practices outlined in the Installation Manual.
- The environment must be checked to verify that environmental conditions do not exceed the ratings.
- The ASCO Solenoid must be accessible for physical inspection.

4.2 Physical Location and Placement

- The RCS shall be accessible with sufficient room for cabling and pneumatic connections and shall allow manual proof testing of the bypass function.
- Pneumatic piping to the block valve shall be kept as short and straight as possible to minimize the airflow restrictions and potential clogging of the exhaust line. Long or kinked pneumatic tubes may also increase the block valve closure time.
- The Breather/Vent valve shall be accessible and should be inspected for obstruction during manual proof testing.
- The RCS shall be mounted in a low vibration environment. If excessive vibration is expected, special precautions shall be taken to ensure the integrity of electrical and pneumatic connectors or the vibration should be reduced using appropriate damping mounts.

4.3 Electrical Connections

- The device requires external electrical connections. The energy for actuating the isolating valves is provided by the control signal lines. The RCS device is available in the following control signal configurations: 12 VDC, 24 VDC, 48VDC, 120 VDC, 120/60-110/50 VAC or 230/50-240/50 VAC.
- All wirings shall provide sufficient electrical isolation between adjacent signal lines and between signal lines and ground.
- Stranded 16 to 18 AWG (or equivalent gauge and flexibility) shall be used.
- It is recommended that conduit sealant be used to prevent condensation from entering the enclosure and, in Class 1 Div. 2 conditions will prevent hazardous gasses and vapors from migrating through the conduit to the control room or open ignition source.
- Wiring shall be according to the National Electrical Code (ANSI-NFPA 70) or other applicable local codes.
- The terminal clamps are designed for one wire only; DO NOT attempt to terminate multiple wires into one terminal.
- Strip the wires to the recommended length appropriate for the termination block.
- Ensure all wire strands are fully inserted into the terminal block and no shorts between adjacent wires on the terminal block are possible.
- Use care when running signal wiring near to, or crossing conduit or wiring that supplies power to motors, solenoids, lighting, horns, bells, etc. Sufficient electrical isolation and shielding against electromagnetic interference from items in the vicinity of the cable run shall be provided.
- AC power wiring should be run in a separate conduit from DC power. All power wiring to and from the RCS should be in a grounded conduit. Outdoor cable runs shall be protected against lightning strike.

- The RCS shall be connected to a high-quality instrument grade ground with #14 AWG or heavier wire. A grounding stud is provided on the inside and outside of the enclosure.

4.4 Pneumatic Connections

- Recommended piping for the inlet and outlet pneumatic connections to the RCS is 1/2" stainless steel or PVC tubing. The length of tubing between the RCS and the block valve shall be kept as short as possible and free of kinks.
- Only dry instrument air filtered to 40-micron level or better shall be used.

- The Process air pressure shall be:
  - For 1oo1 and 2oo2 with Pressure Switches: 21 kPa – 1034 kPa (3 psi - 150 psi).
  - For 1oo1, 2oo2 and 2oo3 with Proximity Switches: 0 kPa – 1034 kPa (0 psi – 150 psi)
- The Pilot air pressure should be 275 kPa - 1034 kPa (40 psi -150 psi).
- The process air capacity shall be sufficient to move the pneumatically actuated bypass valve within the required time.
- The RCS has a Cv of greater than 2.0.

5 RCS Block Diagram

5.1 1oo1HS, 2oo2 Normally Closed with Pressure Switches

Figure 1 shows the simplified block diagram of the 1oo1HS and 2oo2 devices in Normally Closed configuration with Pressure switches. SOV1 and SOV2 are solenoid operated valves; B/P 3 is a key-lock or lever controlled pneumatically actuated valve, and PS1, PS2 and PS3 are pressure switches. The bypass valve is used to apply pneumatic supply directly through the bypass valve to the block valve actuator forcing it to remain in the normal condition (not safe state, maintenance override), while isolating and venting solenoid-operated valves 1 and 2 and all three pressure switches.

Figure 1 - RCS 1oo1HS, 2oo2 Normally Closed Configuration (Safe State) with Pressure Switches

The airflow in Figure 1 is depicted in the safe state of the RCS. In this state, both solenoids are de-energized resulting in the venting of air from the block valve actuator, allowing the spring return actuator to move the block valve to the safe state.

5.2 1oo1HS, 2oo2 Normally Open with Pressure Switches

Figure 2 shows the simplified block diagram of the 1oo1HS and 2oo2 devices in Normally Open configuration with Pressure switches. SOV1 and SOV2 are solenoid operated valves; B/P 3 is a key-lock or lever controlled pneumatically actuated valve, and PS1, PS2 and PS3 are pressure switches. Both SOV1 and SOV2 must remain de-energized to allow the block valve to remain in the safe state position. The bypass valve can be used to block the pneumatic supply directly forcing it to be vented while isolating solenoid-operated valves 1 and 2 and all three pressure switches.
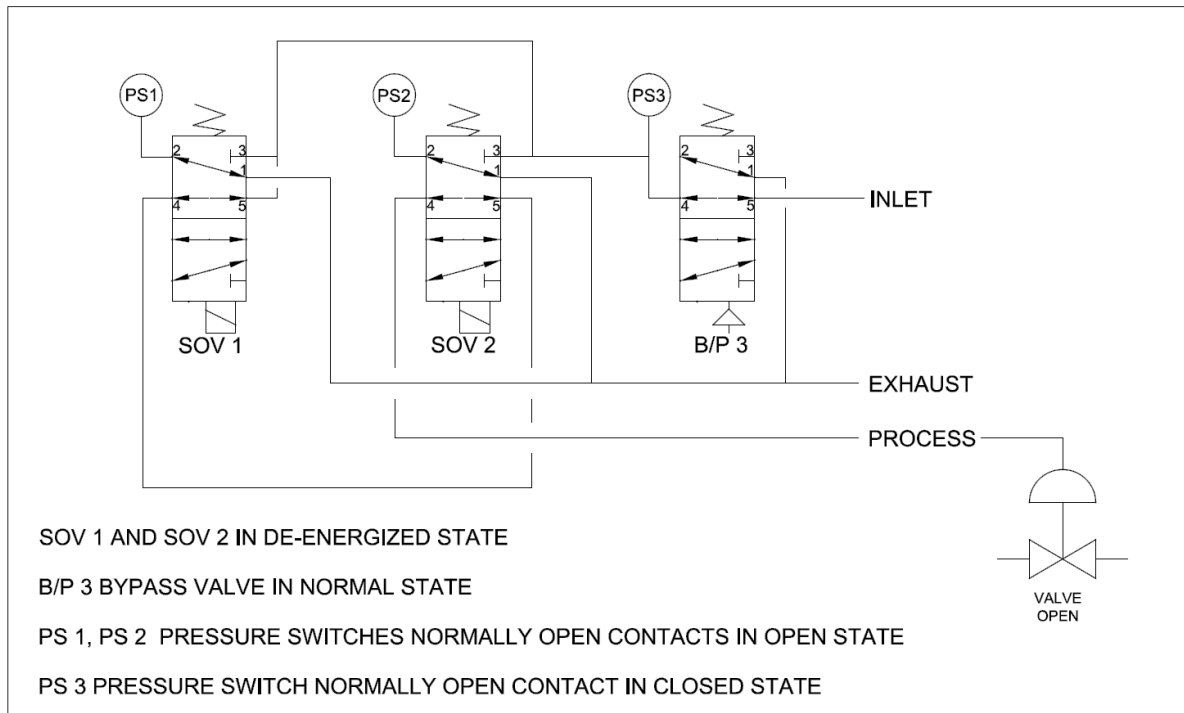
Figure 2 – RCS 1oo1HS, 2oo2 Normally Open Configuration (Safe State) with Pressure Switches

In Figure 2, The airflow is depicted in the safe state of the RCS. In this state, both solenoids are de-energized resulting in the supply of air to the block valve actuator, overcoming the spring return in the actuator to move the block valve to the safe state.

5.3 1oo1HS, 2oo2 Normally Closed with Proximity Switches

Figure 3 shows the simplified block diagram of the 1oo1HS and 2oo2 devices in Normally Closed configuration with proximity switches. SOV1 and SOV2 are solenoid operated valves; B/P 3 is a key-lock or lever controlled pneumatically actuated valve, and PS1, PS2 and PS3 are proximity switches. The bypass valve is used to apply pneumatic supply directly through the bypass valve to the block valve actuator forcing it to remain in the normal condition (not safe state, maintenance override), while isolating and venting solenoid-operated valves 1 and 2, changing the state of the proximity switches.

EXHAUST

SOV 1   SOV 2   B/P 3

INLET

PS1   PS2   PS3

PROCESS

SOV 1 AND SOV 2 IN DE-ENERGIZED STATE

B/P 3 BYPASS VALVE IN NORMAL STATE

PS 1, PS 2 AND PS 3 PROXIMITY SWITCHES
NORMALLY OPEN CONTACTS IN CLOSED STATE
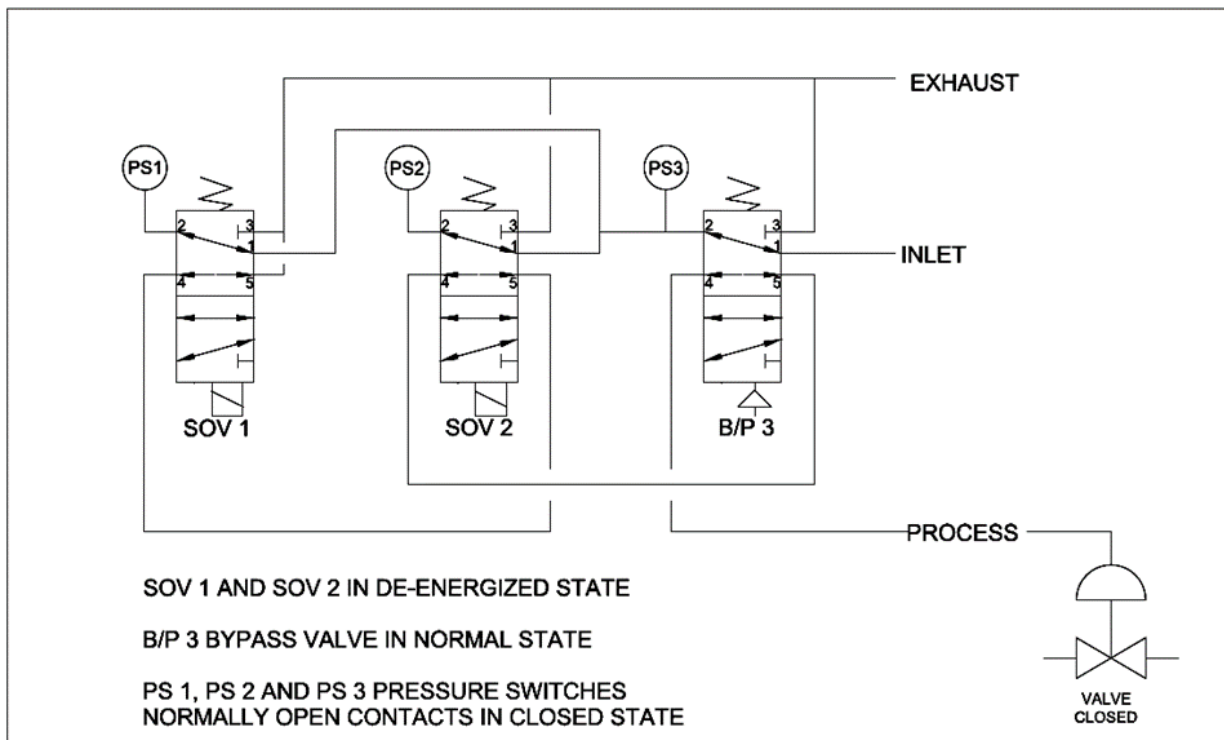
VALVE
CLOSED

Figure 3 – RCS 1oo1HS, 2oo2 Normally Closed Configuration (Safe State) with Proximity Switches

The airflow in Figure 3 is depicted in the safe state of the RCS. In this state, both solenoids are de-energized resulting in the venting of air from the block valve actuator, allowing the spring return actuator to move the block valve to the safe state.

5.4 1oo1HS, 2oo2 Normally Open with Proximity Switches

Figure 4 shows the simplified block diagram of the 1oo1HS and 2oo2 devices in Normally Open configuration with Proximity switches. SOV1 and SOV2 are solenoid operated valves; B/P 3 is a key-lock or lever controlled pneumatically actuated valve, and PS1, PS2 and PS3 are proximity switches. Both SOV1 and SOV2 must remain de-energized to allow the block valve to remain in the safe state position. The bypass valve can be used to block the pneumatic supply directly forcing it to be vented while isolating solenoid-operated valves 1 and 2 and all three proximity switches.
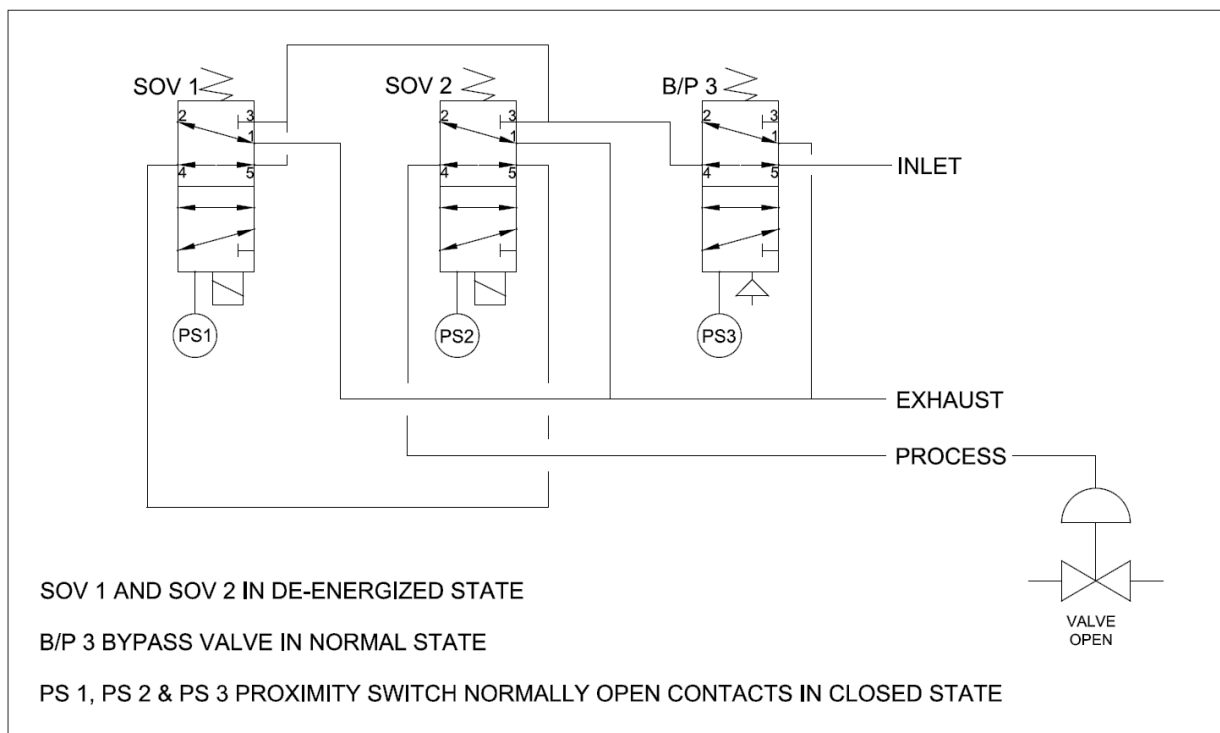

SOV 1   SOV 2   B/P 3

INLET

PS1   PS2   PS3

EXHAUST

PROCESS

SOV 1 AND SOV 2 IN DE-ENERGIZED STATE

B/P 3 BYPASS VALVE IN NORMAL STATE

PS 1, PS 2 & PS 3 PROXIMITY SWITCH NORMALLY OPEN CONTACTS IN CLOSED STATE
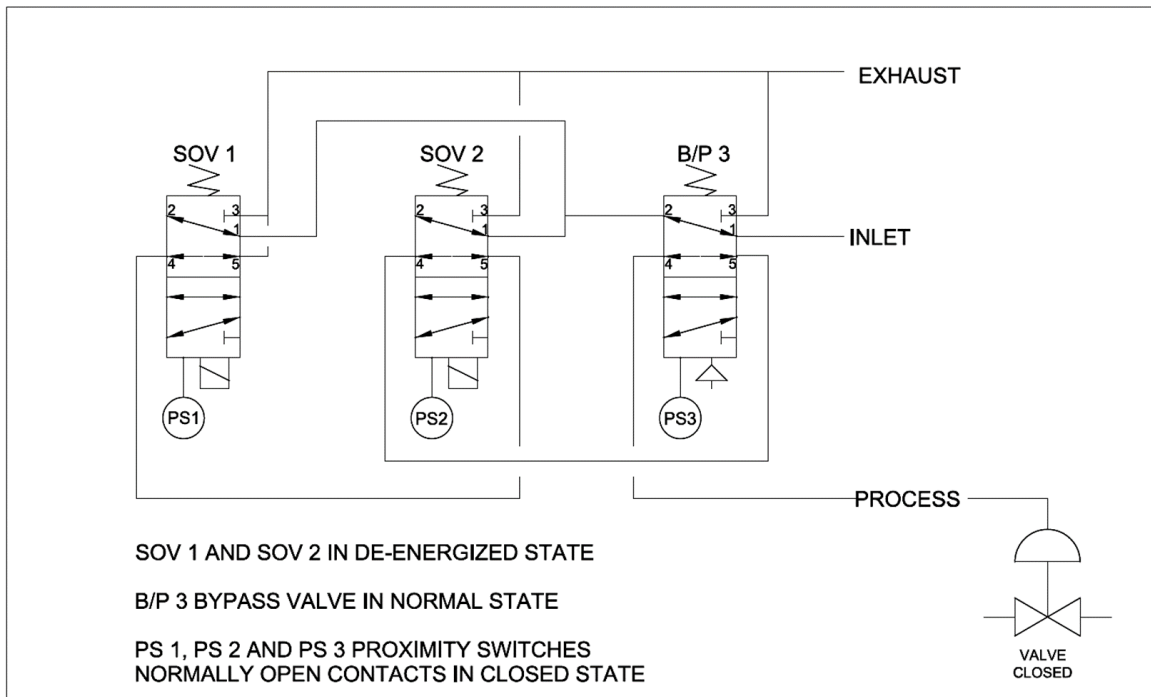
VALVE
OPEN

Figure 4 – RCS 1oo1HS, 2oo2 Normally Open Configuration (Safe State) with Proximity Switches

In Figure 4, The airflow is depicted in the safe state of the RCS. In this state, both solenoids are de-energized resulting in the supply of air to the block valve actuator, overcoming the spring return in the actuator to move the block valve to the safe state

5.5 2oo2 Double Acting with Pressure Switches

Depending on the protected process, the safety action of the 2oo2 Double Acting will direct the air supply to either side of the block actuator. Figure 6 shows the simplified block diagram of the device in the safe mode in the De-energized to Trip (DTT) configuration and using proximity switched for diagnostics.
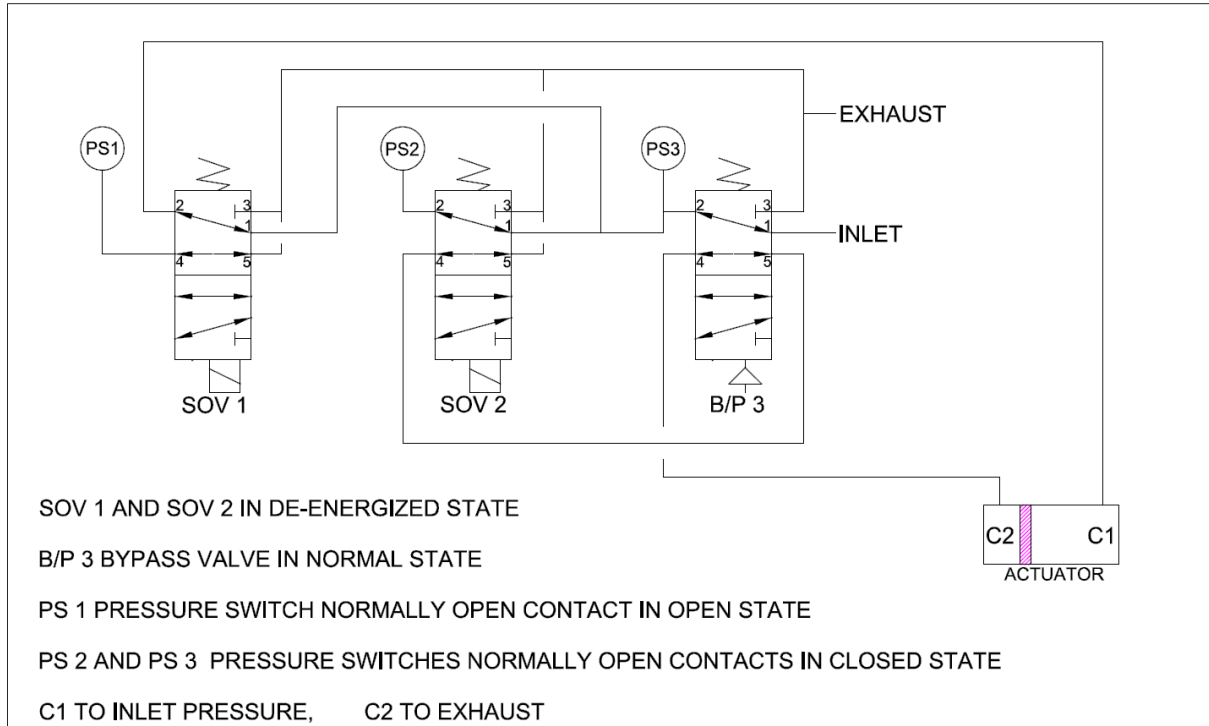
Figure 5 – RCS 2oo2 Double Acting Configuration (Safe State) with Pressure Switches

5.6 2oo2 Double Acting with Proximity Switches

Depending on the protected process, the safety action of the 2oo2 Double Acting will direct the air supply to either side of the block actuator. Figure 6 shows the simplified block diagram of the device in the safe mode in the De-energized to Trip (DTT) configuration and using proximity switched for diagnostics.

www.emerson.com
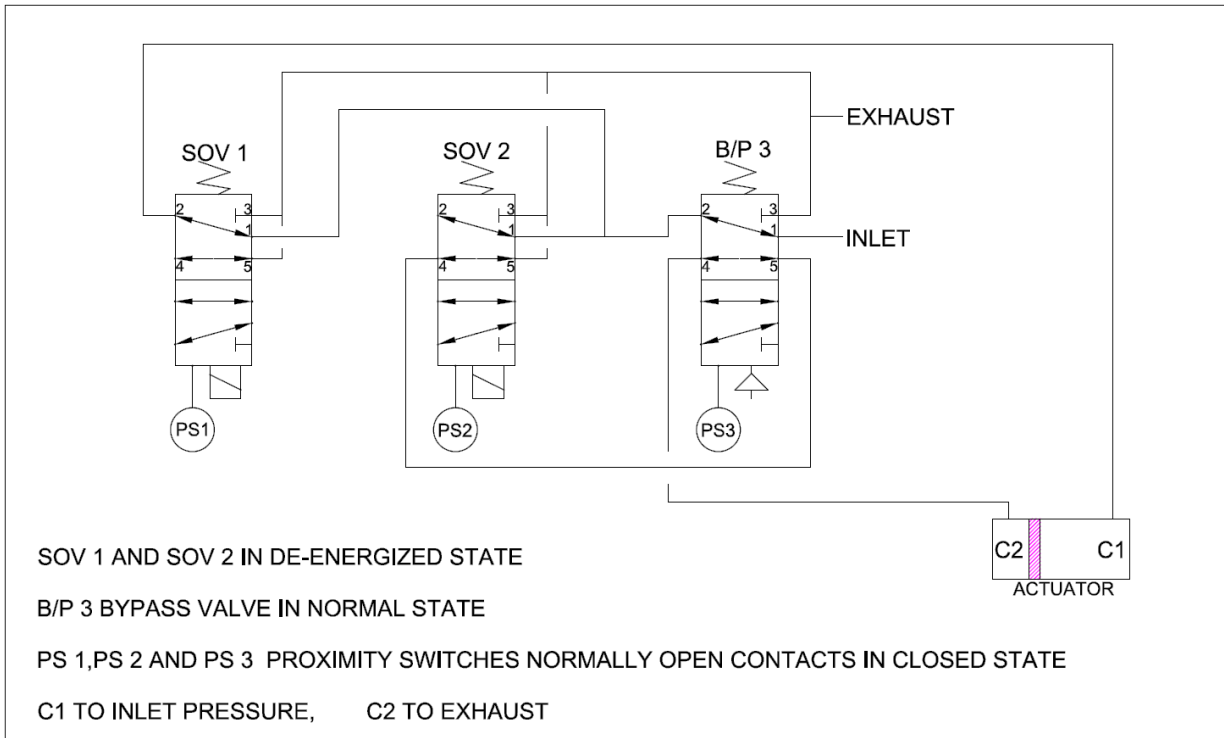
Figure 6 – RCS 2oo2 with Proximity Switches, Double Acting Configuration (Safe State)

5.7 2oo3 Normally Closed without Diagnostics

Figure 7 shows the simplified block diagram of the 2oo3 in Normally Closed without diagnostics. SOV1, SOV2 and SOV3 are solenoid operated valves. This version does not present a bypass valve to isolate and vent the solenoid-operated valves 1, 2 and 3.

The airflow in Figure 7 is depicted in the safe state of the RCS. In this state, the three (3) solenoids are de-energized resulting in the venting of air from the block valve actuator, allowing the spring return actuator to move the block valve to the safe state.
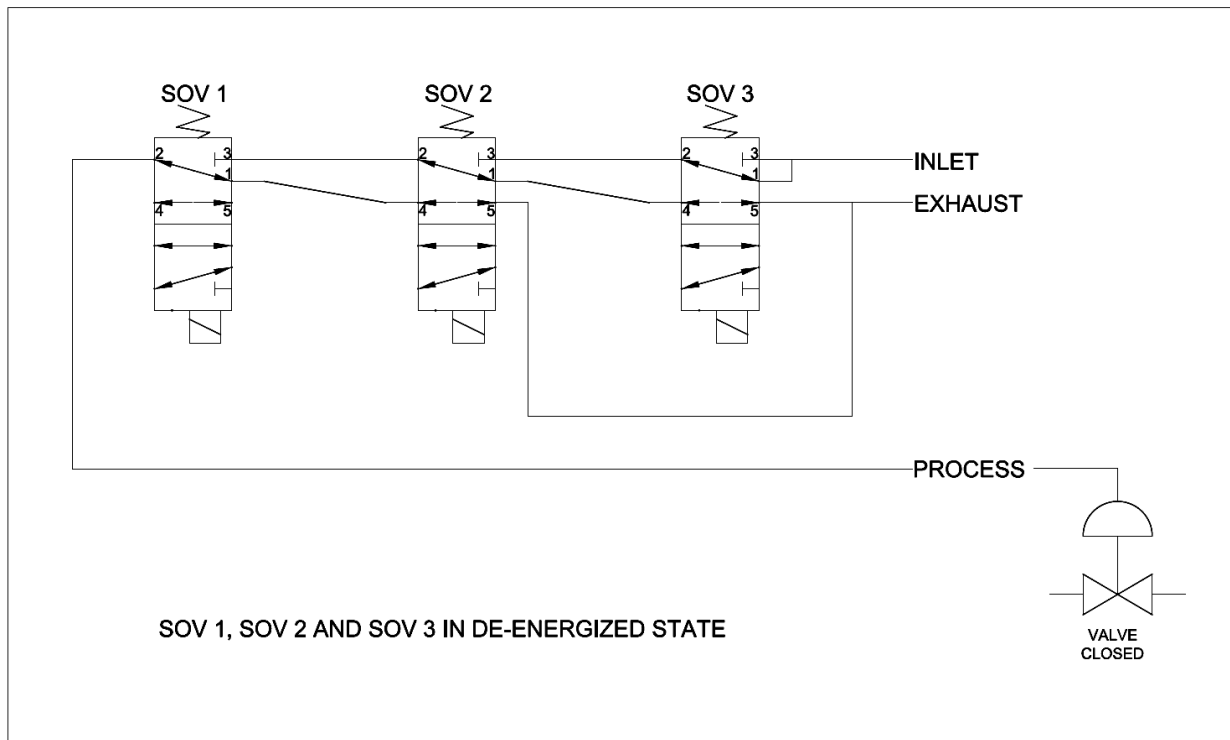
Figure 7 – RCS 2oo3 Normally Closed Configuration (Safe State) without Diagnostics

In this configuration, it is required to have at two (2) solenoids energized to provide pneumatic supply and allow the pressure to overcome the spring return actuator to move the block valve to the normal or degraded state (not safe state).

5.8 2oo3 Normally Closed with Proximity Switches

Figure 8 shows the simplified block diagram of the 2oo3 in Normally Closed with proximity switches. SOV1, SOV2 and SOV3 are solenoid operated valves; B/P 4 is a key-lock or lever controlled pneumatically actuated valve; and PS1, PS2 PS3 and PS4 are proximity switches. The bypass valve is used to apply pneumatic supply directly through the bypass valve to the block valve actuator forcing it to remain in the normal condition (not safe state, maintenance override), while isolating and venting solenoid-operated valves 1, 2 and 3, changing the state of the proximity switches.

The airflow in Figure 8 is depicted in the safe state of the RCS. In this state, the three (3) solenoids are de-energized resulting in the venting of air from the block valve actuator, allowing the spring return actuator to move the block valve to the safe state.
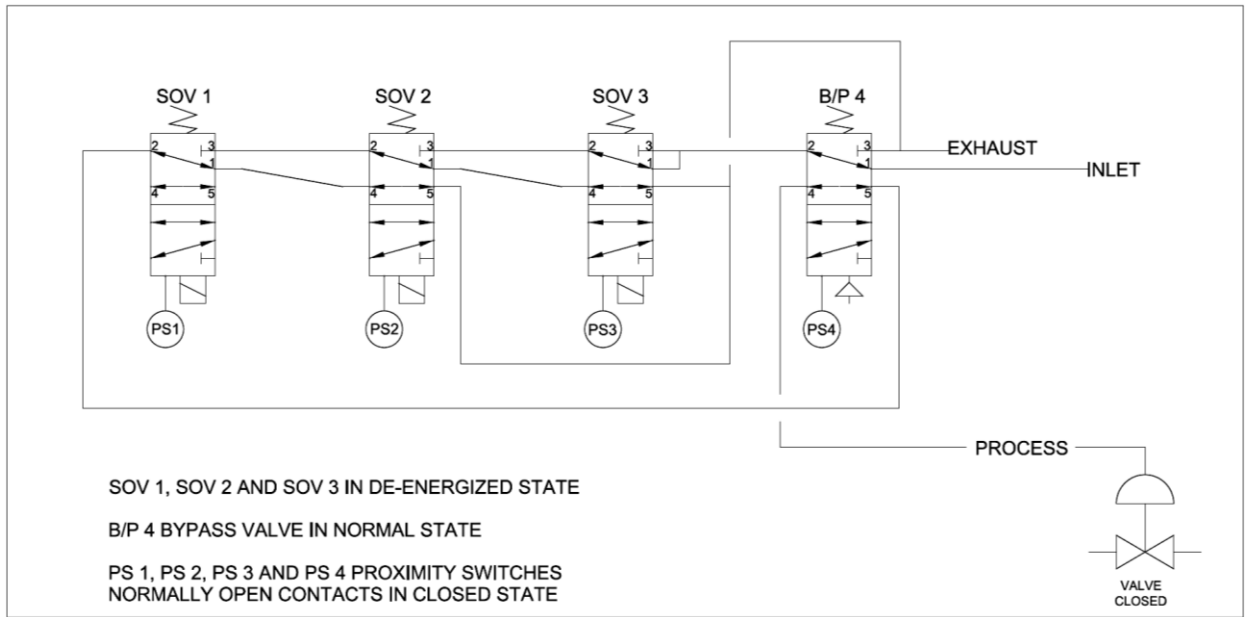
Figure 8 – RCS 2oo3 with Proximity Switches, Normally Closed Configuration (Safe State)

6 RCS Operation and Truth Tables

In the truth tables for all possible device states it can be noticed the following color code:
- Highlighted in light gray is the state when the RCS unit is in a legal mode (safe state) other than the standard running conditions.
- Dark gray indicates an illegal state.

6.1 1oo1HS Normally Closed

Figures 1 and 3 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is blocking the inlet air supply and venting the block valve actuator (normally closed operation). This configuration is most commonly used in safety applications since a loss of electrical or pneumatic energy will result in the safe state of the block valve.

In the 1oo1HS, Normally Closed Mode, only one solenoid is on-line during normal operation. A spurious failure of the online solenoid is indicated by the pressure or proximity switch state associated with the on-line solenoid. The response to the detected failure is to energize the second solenoid to maintain air supply to the block valve, reducing the potential for spurious trips.

The truth table for the 1oo1HS Normally Closed with Pressure Switches is presented in Table 3.

State	State Type	Valve Position			Valve Pressure Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Degraded	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
3	Normal	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	Air Supply
4	Normal	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Air Supply
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply
6	Illegal	Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply
7	Illegal	De-Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply
8	Illegal	Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply

Table 3 – Truth Table for 1oo1HS Normally Closed with Pressure Switches – De-Energized to trip

I&M V 9535 DA

www.emerson.com

The truth table for the 1oo1HS Normally Closed with Proximity Switches is presented in Table 4.

State	State Type	Valve Position			Valve Proximity Sensor/Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Degraded	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
3	Normal	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	Air Supply
4	Normal	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Air Supply
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
6	Illegal	Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
7	Illegal	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
8	Illegal	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply

Table 4 – Truth Table for 1oo1HS Normally Closed with Proximity Switches – De-Energized to trip

The normal operating state of the device is state number 3 (SOV1 de-energized only) or state number 4 (SOV2 de-energized only). If the logic-solver responds to a safety demand, it de-energizes SOV1 and SOV2 and causes the inlet air supply to be blocked off and venting the block valve actuator. This in turn will cause the block valve to move to the safe state. The safe state of the RCS is therefore state 2.

6.2 1oo1HS Normally Open

Figures 2 and 4 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is supplying air to the block valve actuator, hence the expression normally open.

This configuration is characterized by supplying air to the block valve if the solenoids are de-energized. To put the protected process into the safe state, pneumatic energy is necessary. Therefore, this configuration should only be used in rare cases such as when:
- the activation of the system is mitigating an existing hazard
- the unintentional or spurious activation of the system is a hazard itself

Examples of such applications are fire & gas systems, emergency cooling and deluge systems, or flare control systems.

Additionally, restrictions to secure the integrity of the air supply may apply:
- At least two independent air sources or an air storage device such as an accumulator shall be used. These sources must provide emergency air for a safe process shutdown, for a time span required by the application.
- Each air source must be provided with pressure integrity monitoring through a safety critical input read back into the safety rated logic solver. Any air supply failure shall lead to an alarm.

The truth table for 1oo1HS Normally Open using Pressure Switches is shown in Table 5.

State	State Type	Valve Position			Valve Pressure Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Degraded	Energized	Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
2	Safe	De-Energized	De-Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
3	Normal	De-Energized	Energized	Normal	Open (False)	Closed (True)	Closed (True)	Vented
4	Normal	Energized	De-Energized	Normal	Closed (True)	Open (False)	Closed (True)	Vented
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented
6	Illegal	Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented
7	Illegal	De-Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented
8	Illegal	Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented

Table 5 – Truth Table for 1oo1HS Normally Open with Pressure Switches – De-Energized to trip

I&M V 9535_DA

www.emerson.com

The truth table for 1oo1HS Normally Open using Proximity Switches is shown in Table 6.

State	State Type	Valve Position			Valve Proximity Sensor/Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Degraded	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
3	Normal	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	Air Supply
4	Normal	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Air Supply
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
6	Illegal	Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
7	Illegal	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
8	Illegal	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply

Table 6 – 1oo1HS Normally Open with Proximity Switches – De-Energized to trip

The normal operating state of the device is state number 3 (SOV1 de-energized only) or state number 4 (SOV2 de-energized only). If the logic-solver responds to a safety demand, it de-energizes SOV1 resulting in the supply of air to the block valve actuator, overcoming the spring return in the actuator. This in turn will cause the block valve to move to the safe state. The safe state of the RCS is therefore state 2.

6.3 2oo2 Normally Closed

Figures 1 and 3 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is blocking the inlet air supply and venting the block valve actuator (normally closed operation). This configuration is most commonly used in safety applications since a loss of electrical or pneumatic energy will result in the safe state of the block valve.

In the 2oo2 Normally Closed Mode, both solenoids are on-line during normal operation. A spurious failure of either solenoid is indicated by the pressure or proximity switch state associated with that solenoid. The second solenoid will maintain air supply to the block valve, reducing the potential for spurious trips.

The truth table for the 2oo2 Normally Closed with Pressure Switches is shown in Table 7.

State	State Type	Valve Position			Valve Pressure Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Normal	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
3	Degraded	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	Air Supply
4	Degraded	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Air Supply
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply
6	Illegal	Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply
7	Illegal	De-Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply
8	Illegal	Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Air Supply

Table 7 – Truth Table for 2oo2 Normally Closed with Pressure Switches – De-Energized to trip

The truth table for the 2oo2 Normally Closed with Proximity Switches is shown in Table 8.

State	State Type	Valve Position			Valve Proximity Sensor/Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Normal	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
3	Degraded	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	Air Supply
4	Degraded	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Air Supply
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
6	Illegal	Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
7	Illegal	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
8	Illegal	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply

Table 8 – Truth Table for 2oo2 Normally Closed with Proximity Switches – De-Energized to trip

The normal operating state of the device is state number 1 (both SOV's are energized open). If the logic-solver responds to a safety demand, it de-energizes both SOV1 and SOV2, and causes the inlet air supply to be blocked off and venting the block valve actuator. This in turn will cause the block valve to move to the safe state. The safe state of the RCS is therefore state 2.

6.4 2oo2 Normally Open

Figures 2 and 4 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is supplying air to the block valve actuator, hence the expression normally open.

This configuration is characterized by supplying air to the block valve if the solenoids are de-energized. To put the protected process into the safe state, pneumatic energy is necessary. Therefore, this configuration should only be used in rare cases such as when:

- The activation of the system is mitigating an existing hazard
- The unintentional or spurious activation of the system is a hazard itself

Examples of such applications are fire & gas systems, emergency cooling and deluge systems, or flare control systems.

Additionally, restrictions to secure the integrity of the air supply may apply:

- At least two independent air sources or an air storage device such as an accumulator shall be used. These sources must provide emergency air for a safe process shutdown, for a time span required by the application.
- Each air source must be provided with pressure integrity monitoring through a safety critical input read back into the safety rated logic solver. Any air supply failure shall lead to an alarm.

The truth table for the 2oo2 Normally Open with Pressure Switches is shown in Table 9.

State	State Type	Valve Position			Valve Pressure Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Normal	Energized	Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
2	Safe	De-Energized	De-Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
3	Degraded	De-Energized	Energized	Normal	Open (False)	Closed (True)	Closed (True)	Vented
4	Degraded	Energized	De-Energized	Normal	Closed (True)	Open (False)	Closed (True)	Vented
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented
6	Illegal	Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented
7	Illegal	De-Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented
8	Illegal	Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	Vented

Table 9 – Truth Table for 2oo2 Normally Open with Pressure Switches – De-Energized to trip

The truth table for the 2oo2 Normally Open with Proximity Switches is shown in Table 10.

State	State Type	Valve Position			Valve Proximity Sensor/Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Normal	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Vented
3	Degraded	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	Air Supply
4	Degraded	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Air Supply
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
6	Illegal	Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
7	Illegal	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply
8	Illegal	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	Air Supply

Table 10 – Truth Table for 2oo2 Normally Open with Proximity Switches – De-Energized to trip

The normal operating state of the device is state number 1 (both SOV's energized open). If the logic solver responds to a safety demand, it de-energizes both SOV1 and SOV2 resulting in the supply of air to the block valve actuator, overcoming the spring return in the actuator. This in turn will cause the block valve to move to the safe state. The safe state of the RCS is therefore state 2.

6.5 2oo2 Double Acting

The Double Acting RCS must be used with a safe last state actuator valve package.

Figures 5 and 6 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is supplying inlet air to C1 process and venting C2 process of the block valve actuator

In the 2oo2-Double Acting Mode, both solenoids are on-line during normal operation. A spurious failure of either solenoid is indicated by the pressure or proximity switch state associated with that solenoid. When SOV1 or SOV2 is energized by itself, the pressure across the block valve actuator is balanced. The block valve actuator does not change states.

The truth table for the 2oo2 Double acting with Pressure Switches is shown in Table 11:

State	State Type	Valve Position			Valve Pressure Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Normal	Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	C1 Vented C2 Air Supply
2	Safe	De-Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	C1 Air Supply C2 Vented
3	Degraded	De-Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	C1 Air Supply C2 Air Supply
4	Degraded	Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	C1 Vented C2 Vented
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	C1 Vented C2 Air Supply
6	Illegal	Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	C1 Vented C2 Air Supply
7	Illegal	De-Energized	Energized	Actuated	Open (False)	Open (False)	Open (False)	C1 Vented C2 Air Supply
8	Illegal	Energized	De-Energized	Actuated	Open (False)	Open (False)	Open (False)	C1 Vented C2 Air Supply

Table 11 – Truth Table for 2oo2 Double Acting with Pressure Switches

The truth table for the 2oo2 Double acting with Proximity Switches is shown in Table 12:

State	State Type	Valve Position			Valve Proximity Sensor/Switch Normally Open Contacts			Process/Outlet
		SOV1	SOV2	Bypass Valve	PS 1	PS 2	PS 3	
1	Normal	Energized	Energized	Normal	Open (False)	Open (False)	Closed (True)	C1 Vented C2 Air Supply
2	Safe	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	C1 Air Supply C2 Vented
3	Degraded	De-Energized	Energized	Normal	Closed (True)	Open (False)	Closed (True)	C1 Air Supply C2 Air Supply
4	Degraded	Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	C1 Vented C2 Vented
5	Maintenance Bypass	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	C1 Vented C2 Air Supply
6	Illegal	Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	C1 Vented C2 Air Supply
7	Illegal	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Open (False)	C1 Vented C2 Air Supply
8	Illegal	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Open (False)	C1 Vented C2 Air Supply

Table 12 – Truth Table for 2oo2 Double Acting with Proximity Switches

The normal operating state of the device is state number 1 (both SOV's are energized open). If the logic-solver responds to a safety demand, it de-energizes both SOV1 and SOV2, and causes the inlet air supply to be directed to C1 and vents C2 of the block valve actuator. This in turn will cause the block valve to move to the safe state. The safe state of the RCS is therefore state 2

6.6 2oo3 Normally Closed without Diagnostics

Figures 7 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is blocking the inlet air supply and venting the block valve actuator (normally closed operation). This configuration is most commonly used in safety applications since a loss of electrical or pneumatic energy will result in the safe state of the block valve.

In the 2oo3 Normally Closed Mode, the three (3) solenoids are on-line during normal operation. A spurious failure of only one (1) solenoid will not generate a spurious trip of the block valve as the other two solenoids will maintain air supply to the block valve, reducing the potential for spurious trips.

However, when at least two (2) solenoids present a spurious failure the block valve will be vented and move to the safe position.

The truth table for the 2oo3 Normally Closed without Diagnostics is shown in Table 13.

www.emerson.com

State	State Type	Valve Position			Process/Outlet
		SOV 1	SOV 2	SOV 3	
1	Normal	Energized	Energized	Energized	Air Supply
2	Safe	De-Energized	De-Energized	De-Energized	Vented
3	Degraded	De-Energized	Energized	Energized	Air Supply
4	Degraded	Energized	De-Energized	Energized	Air Supply
5	Degraded	Energized	Energized	De-Energized	Air Supply
6	Degraded	De-Energized	De-Energized	Energized	Vented
7	Degraded	De-Energized	Energized	De-Energized	Vented
8	Degraded	Energized	De-Energized	De-Energized	Vented

Table 13 – Truth Table for 2oo3 without Diagnostics – De-Energized to Trip

6.7 2oo3 Normally Closed with Proximity Switches

Figures 8 illustrates the pneumatic pathways for this configuration at the safe state condition (safety action). In this condition, the RCS is blocking the inlet air supply and venting the block valve actuator (normally closed operation). This configuration is most commonly used in safety applications since a loss of electrical or pneumatic energy will result in the safe state of the block valve.

In the 2oo3 Normally Closed Mode, the three (3) solenoids are on-line during normal operation. A spurious failure of only one (1) solenoid, indicated by its respective proximity switch, will not generate a spurious trip of the block valve as the other two solenoids will maintain air supply to the block valve, reducing the potential for spurious trips.

However, when at least two (2) solenoids present a spurious failure the block valve will be vented and move to the safe position.

The truth table for the 2oo3 Normally Closed with Proximity Switches is shown in Table 14.

State	State Type	Valve Position				Valve Poximity Sensor/Switch Normally Open Contacts				Process/Outlet
		SOV 1	SOV 2	SOV 3	Bypass Valve	PS 1	PS 2	PS 3	PS 4	
1	Normal	Energized	Energized	Energized	Normal	Open (False)	Open (False)	Open (False)	Closed (True)	Air Supply
2	Safe	De-Energized	De-Energized	De-Energized	Normal	Closed (True)	Closed (True)	Closed (True)	Closed (True)	Vented
3	Degraded	De-Energized	Energized	Energized	Normal	Closed (True)	Open (False)	Open (False)	Closed (True)	Air Supply
4	Degraded	Energized	De-Energized	Energized	Normal	Open (False)	Closed (True)	Open (False)	Closed (True)	Air Supply
5	Degraded	Energized	Energized	De-Energized	Normal	Open (False)	Open (False)	Closed (True)	Closed (True)	Air Supply
6	Degraded	De-Energized	De-Energized	Energized	Normal	Closed (True)	Closed (True)	Open (False)	Closed (True)	Vented
7	Degraded	De-Energized	Energized	De-Energized	Normal	Closed (True)	Open (False)	Closed (True)	Closed (True)	Vented
8	Degraded	Energized	De-Energized	De-Energized	Normal	Open (False)	Closed (True)	Closed (True)	Closed (True)	Vented
9	Maintenance Bypass	De-Energized	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
10	Illegal	Energized	Energized	Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
11	Illegal	De-Energized	Energized	Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
12	Illegal	Energized	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
13	Illegal	Energized	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
14	Illegal	De-Energized	De-Energized	Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
15	Illegal	De-Energized	Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply
16	Illegal	Energized	De-Energized	De-Energized	Actuated	Closed (True)	Closed (True)	Closed (True)	Open (False)	Air Supply

Table 14 – Truth Table for 2oo3 Normally Closed with Proximity Switches – De-Energized to Trip

7   RCS Maintenance

7.1   Operator Interface Options

The RCS is available with various interface and display options. These options provide local indication and feedback for plant personnel. There are several constraints related to these options.
- Any operator interface shall be implemented in a manner that has a predictable effect on the RCS and does not interfere with its safety function.
- Field modifications shall not be made to the internal wiring or pneumatic connections of the RCS.

7.2   Automated Diagnostic Test (ADT)

The RCS architecture alone is not sufficient to achieve the required diagnostic coverage for devices used in critical environments. The associated pressure or proximity switches will have to be used by the safety rated logic solver to:
- Verify the system transitions into the safe state if requested
- Detect illegal states of the system (refer to truth tables)
- Detect degraded state for the 1oo1HS configuration (refer to truth tables) or the degraded state for the 2oo2 and 2oo3 configuration (refer to truth tables)
- Detect the bypass (forced) state of the safety function (refer to truth tables).

In addition to the static detection of the system state and to enable the logic-solver to verify correct system state transition, the sensor information is used to implement a safety-critical test of the RCS function. These diagnostics also allow implementing a hot-standby switchover to SOV2 if SOV1 fails safe, however this function is NOT a safety function since it only reduces the spurious trip rate of the device.

For functional testing, the two (2) solenoids, in case of 2oo2 configuration, or the three (3) for the 2oo3, are brought on-line. Each solenoid is then de-energized individually with pressure or proximity switch confirmation of successful changing of state. No bypassing is required for functional testing. This means that the system is sequenced, from its normal operation, through the states:

- 2oo2: 1 > 3 >1 > 4 > 1
- 2oo3D: 1 > 3 > 1 > 4 > 1 > 5 > 1

The correct assertion of these states is verified by reading the switch transition. The safe state can be achieved at any time during the function test by de-energizing the digital outputs on the safety rated logic solver.

Refer to the relevant Truth table for the pressure and proximity switches for each of these states.

The functional testing is performed to detect potential undetected dangerous component failure within the device such as:

- SOV1 stuck in energized position
- SOV2 stuck in energized position
- SOV3 stuck in energized position
- Pressure switch 1 stuck in open or closed position
- Pressure switch 2 stuck in open or closed position
- Proximity switch 1 stuck in open or closed position
- Proximity switch 2 stuck in open or closed position
- Proximity switch 3 stuck in open or closed position
- Open bypass valve in combination with a defective pressure switch 3
- Open bypass valve in combination with a defective proximity switch 4

A potentially dangerous state of the bypass valve is detectable through pressure or proximity switch 3 (in 2oo2 configurations) or proximity switch 4 (in 2oo3 configuration).

In 2oo2, an open bypass valve will cause a transition of pressure or proximity switch 3 into a position disallowed in the normal state.

In 2oo3, an open bypass valve will cause a transition of proximity switch 4 into a position disallowed in the normal state.

When in Bypass mode, the detection mechanism for the SOV's will not provide the actual electrical state of the SOV's as no pressure is supplied to these valves (refer to Truth tables for additional details).

Since the position of the bypass valve is safety critical, the valve can be secured with a key switch. The key is removable in normal state (not bypassed) and should not be left inserted during normal operation to prevent inadvertent overrides.

Any failure detected by the ADT shall be annunciated by the safety rated logic solver.

7.2.1 State Verification Test

The correct state of all valves shall be verified and compared against the commanded state. The state tables in Section 6 of this manual can be used as a guide. This verification shall be performed periodically with a cycle time of ½ of the process safety time or less.

If any illegal states are detected, they shall be immediately annunciated. These states are excluded by design and the root cause for these faults cannot be determined or be contributed to a specific component. The RCS shall be repaired within 72 hours.

7.2.2 Valve Diagnostic Test

The ability of the logic solver to actuate the RCS shall be tested. This test shall sequence the SOV valves through the different states. The truth tables presented in **Section 6** represent the normal working conditions for the RCS configurations.

However, some critical functions of the RCS cannot be tested by the ADT. The failure analysis of the device has determined that the following failure modes will not be detected by the diagnostic test:

1. Blockage or partial blockage of the line between the actuator and the RCS (NC).
2. Blockage or partial blockage of the supply line between the pneumatic supply and the RCS (NO).
3. Electrical shorts between a pressure or proximity sensor and the associated valve solenoid at the termination block (if common ground is used for both signals and in NO mode)
4. Interruption of the Diagnostic Test

Items 1 and 2 are important since they entirely disable the actuating function of the RCS and are instantaneously dangerous. These faults however can be detected if a partial valve stroke test is implemented. Items 3 and 4 will not be instantaneously dangerous but will affect the diagnostic coverage or may induce a dangerous state if a second fault occurs.

These failure modes shall be tested manually in an interval longer than the diagnostic interval time, and often enough to reduce the probability of the system to be in an undetected dangerous state. Manual test with longer test intervals is commonly called proof test.

Items 1-4 shall be tested during the proof test of the SIF.

The manual tests of items 1, 2 and 3 can be substituted by automated tests if a partial stroke test of the block valve is implemented.

The following tables identify the defective valve / switch and the failure must be annunciated to initiate repair.

NOTE: All "Failure Verification" states of PS1, PS2, PS3, and PS4 in tables 15 through 21 are made with reference to the switch normally open contacts.

- **2oo2 Configurations**

State	Failure Verification	Defective Component
1	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 closed	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table 15 - 2oo2 (NC) with Pressure Switches - Defective Component Identification

State	Failure Verification	Defective Component
1	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 closed	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table 16 - 2oo2 (NC) with Proximity Switches - Defective Component Identification

www.emerson.com

State	Failure Verification	Defective Component
1	PS1 open	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 closed	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table 17 - 2oo2 (NO) with Pressure Switches - Defective Component Identification

State	Failure Verification	Defective Component
1	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 closed	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table18 - 2oo2 (NO) with Proximity Switches - Defective Component Identification

State	Failure Verification	Defective Component
1	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 open	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table 19 - 2oo2 (DA) with Pressure Switches - Defective Component Identification

State	Failure Verification	Defective Component
1	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 closed	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table 20 - 2oo2 (DA) with Proximity Switches - Defective Component Identification

- **2oo3 Configuration**

State	Failure Verification	Defective Component
1	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 closed	PS3 defective or SOV3 defective
	PS4 open	PS4 defective or bypass function active
	More than one signal mismatched	Fault not localizable
3	PS1 open	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 closed	PS3 defective or SOV3 defective
	PS4 open	PS4 defective or bypass function active
	More than one signal mismatched	Fault not localizable
4	PS1 closed	PS1 defective or SOV1 defective
	PS2 open	PS2 defective or SOV2 defective
	PS3 closed	PS3 defective or SOV3 defective
	PS4 open	PS4 defective or bypass function active
	More than one signal mismatched	Fault not localizable
5	PS1 closed	PS1 defective or SOV1 defective
	PS2 closed	PS2 defective or SOV2 defective
	PS3 open	PS3 defective or SOV3 defective
	PS4 open	PS4 defective or bypass function active
	More than one signal mismatched	Fault not localizable

Table 21 - 2oo3 Defective Component Identification

7.3 Manually Initiated Diagnostic Test

The manually initiated diagnostic test is identical to the ADT described in **7.2** except that instead of automatically initiating the diagnostic, operator action is required by means of pushing a push button. The diagnostics that are executed are identical, thus, the same outputs can be expected.

7.4 Proof Test without Automatic Testing

The objective of proof testing is to detect failures within an ASCO Solenoid 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 ASCO Solenoid 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.

The following proof test procedure is recommended. Any failures that are detected and that compromise functional safety should be reported to ASCO Valves, Inc.

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Perform an Automated Diagnostic Test (ADT) to confirm the proper functioning of the RCS.
3.	De-energize the RCS Solenoids to force the Actuator/Valve assembly to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time. Note:-This tests for all failures that could prevent the functioning of the Control Valve as well as the rest of the final control element.
4.	Inspect the RCS for any leaks, visible damage or contamination
5.	Re-store the RCS to normal operation and confirm that the normal operating state was achieved.
6.	Remove the bypass and otherwise restore normal operation.

Table 22 - Proof Test Procedure

This test will detect approximately 96% of possible DU failures without ADT, 33% with ADT. The person(s) performing the proof test of an ASCO Solenoid should be trained in SIS operations, including bypass procedures, solenoid maintenance and company Management of Change procedures. No special tools are required.

7.5 Proof Test with Automatic Partial Valve Stroke Testing

An automatic partial valve stroke testing scheme that performs a full stroke of the isolation valves in the RCS and measures valve movement timing will detect most potentially dangerous failure modes. It is recommended that a physical inspection (Step 2 from Table 1) be performed on a periodic basis with the time interval determined by plant conditions. A maximum inspection interval of five years is recommended.

7.6 Repair and replacement

Repair procedures must be followed. Please refer to the appropriate I&M per your specific construction:
- I&M V9512: 1oo1 and 2oo2 Aluminum with Pressure Switches
- I&M V9709: 1oo1 and 2oo2 Stainless steel with Pressure Switches.
- I&M V9957: 2oo2 Aluminum with Proximity Switches
- I&M V9958: 2oo3 without diagnostics.
- I&M V9959: 2oo3 Aluminum with Proximity Switches

7.7 ASCO Notification

Any failures that are detected and that compromise functional safety should be reported to ASCO Valves, Inc. Please contact ASCO Technical Support.

8 Status of the document

8.1 Releases
Version: R3
Revision: DA
Version History: V0, R3, DA
Release status: ECN 314141 Released on 07/21

Appendix A – SIS Checklist

The following checklist may be used as a guide to employ the RCS device 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 (NO/NC/DA)			
	Design decision documented			
	Electrical compatibility and suitability verified			
	Pneumatic compatibility and suitability verified			
	SIS logic solver requirements for valve tests defined and documented			
	Line monitoring requirements for SIS logic solver connection determined			
	Routing of electric and 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			
	Electrical connections appropriate and according to applicable codes			
	Pneumatic connections appropriate and according to applicable codes			
	SIS logic solver line-end devices installed (if applicable)			
	SIS logic solver state verification test implemented			
	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			
	Verification and Testing			
	Electrical connections verified and tested			
	Pneumatic connection verified and tested			
	SIS logic solver line-end devices tested			
	SIS logic solver state verification test verified			
	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			
	Enclosure vent inspected			
	Electrical connection inspected			
	Bypass function and pressure sensors tested			
	Safety loop function tested			