I&M V9642

ASCO®

Manual Reset Valves used in Safety Instrumented Systems

Operating Manual in accordance with IEC 61508

exida® SIL 3 Capable

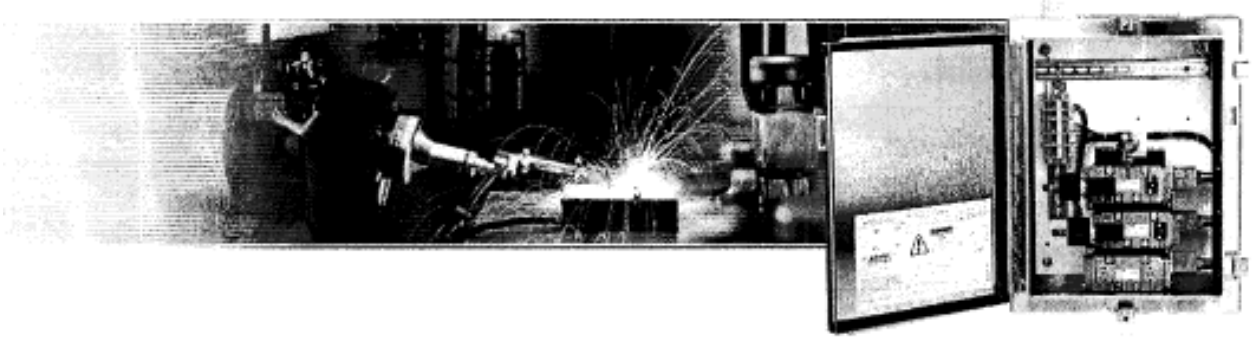


Table of Contents

1 Introduction

This Operating Manual provides the necessary information to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing an ASCO Manual Reset Valve. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.1 Terms and Abbreviations

- **Process Valve** — Any valve that is used to control the flow of media being used in a process. For the purpose of this document, this is usually a 2-way valve whose movement is being controlled by an actuator and pilot valve.
- **Pilot Valve** — A 3-way or 4-way valve that is used to send or remove pressurized media to and from an actuator for the opening and closing of a process valve.
- **Direct Acting** — Refers to a solenoid valve's main orifice that is opened and closed as a direct result of the solenoid valve's electromagnetic movement when the coil is energized and de-energized.
- **Indirect Acting** — Refers to a solenoid valve's main orifice that is opened and closed as a result of fluid flow being directed from the electromagnetic 3-way solenoid pilot.
- **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 twice the proof test frequency.
- **Tamper Proof** — Type of Manual Reset Valve where moving the handle while the valve is in its tripped state will not cause the actuator/process valve to shift.
- **High shock** — Type of Manual Reset Valve where once tripped, the lever may be cycled causing the valve discs to open and close.

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**.**
- **MRV** — Manual Reset Valve
- **NVR** — No Voltage Release. Type of valve where the pilot valve solenoid must be energized while the handle is raised manually to latch the operator in the "up" (latched) position. Upon loss of voltage, the latch is tripped returning the operator to the "down" (unlatched) position.
- **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).
- **TSO** — Electrically tripped. Type of valve where the pilot valve solenoid must be de-energized while the handle is raised manually to latch the operator in the "up" (latched) position. Upon energizing the pilot valve solenoid, the latch is tripped returning the operator to the "down" (unlatched) position.

2 Designing a Safety Instrumented Function (SIF) using an ASCO Manual Reset Valve

2.1 Safety Function

The ASCO NVR Manual Reset Valve moves to its fail-safe position when de-energized. The valve in the "up" (latched) position will supply the fluid media or vent the fluid media depending on the piping of the installation, then switch when tripped into the "down" (unlatched) position.

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.

2.2 Environmental limits

The environmental limits of each valve assembly are specified in the product's respective catalog and Installation & Maintenance Instructions. The designer of a SIF must check that the product is rated for use within the expected environmental limits.

2.3 Application limits

The application limits of an ASCO MRV are specified in the products' respective catalog and Installation & Maintenance Instructions. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the valve is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

2.4 Design Verification

- A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from ASCO Numatics. 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 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. The Exida exSILentia tool is recommended for this work.
- When using an ASCO MRV 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 life time of an ASCO MRV. The failure rates will increase sometime after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

2.5 SIL Capability

2.5.1 Systematic Integrity

The product has met 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.

2.5.2 Random Integrity

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

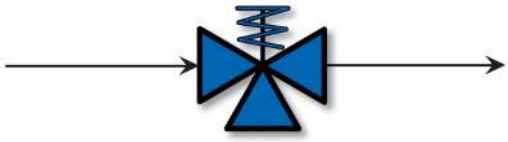
When the final element assembly consists of many components (solenoid valve, quick exhaust valve, actuator, isolation valve, etc.) the SIL must be verified for the entire assembly using failure rates from all components. This analysis must account for any hardware fault tolerance and architecture constraints.

3 Installation and Commissioning

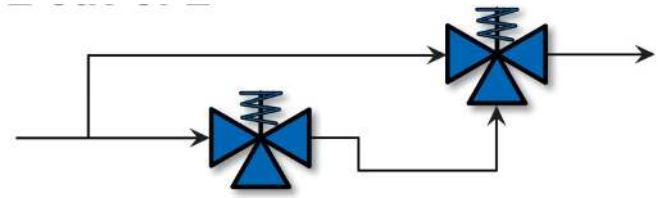
3.1 Installation

- The ASCO Manual Reset 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.
- Instrument Air Filtration: These solenoids are intended for use on clean, dry air or inert gas filtered to 50 microns or better. To prevent freezing, the dew point of the media should be at least 18℉ (10℃) below the minimum temperature to which any portion of the clean air or gas system could be exposed. Instrument air in compliance with ANSI/ISA Standard S7.3-1975 (R1981) exceeds the above requirements and is, therefore, an acceptable medium for these valves.
- Typical 3-way pilot valve piping configurations:

a. 1 out-of 1 – This is the most common pilot valve configuration used.



b. 2 out-of 2 – This is commonly used for high availability applications. In the case that one solenoid valve was to spuriously trip, the second solenoid valve still maintains the position of the actuator/process valve at its operating state. Both solenoid valves must close in order to shift the actuator/process valve to its non-operating state.



3.2 Response Time

The response time of an MRV valve will vary by design. It is the responsibility of the end user to use a pilot valve that delivers the correct opening and closing time of the process valve required for the application.

4 Operation and Maintenance

4.1 Proof testing

The objective of proof testing is to detect failures within an ASCO MRV 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 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. Any failures that are detected and that compromise functional safety should be reported to ASCO Valve.

Table 1

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip, following company Management of Change (MOC) procedures.
2	Inspect the external parts of the MRV for dirty or clogged ports and other physical damage. Do not attempt disassembly of the valve.
3	For NVR: De-energize the solenoid coil. Observe that the lever arm drops into the unlatched closed position and flow through the valve shifts. Energize the solenoid of the valve and lift the lever arm up into the latched position. The lever arm should remain in the up position while the solenoid is energized. For TSO: Energize the solenoid coil. Observe that the lever arm drops into the unlatched closed position and flow through the valve shifts. De-energize the solenoid and lift the lever arm up into the latched position. The latch arm should remain in the up position while the solenoid is de-energized.
4	Inspect the valve for dirt, corrosion or excessive moisture. Clean if necessary and take corrective action to properly clean the air supply. This is done to avoid incipient failures due to dirty air.
5	Record any failures in your company's SIF inspection database. Restore the loop to full operation.
6	Remove the bypass from the safety PLC or otherwise restore normal operation

This test will detect approximately 99% of possible DU failures in the solenoid valve (Proof Test Coverage).

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.

4.2 Repair and replacement

According to section 7.4.7.4 of IEC 61508-2 a useful lifetime based on experience, should be assumed. General field knowledge suggests that most solenoid valves have a useful life of 3 to 10 years. It is the responsibility of the end user to establish a preventive maintenance process to replace all solenoid valves before the end of the useful life.

4.3 ASCO Notification

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

5 ASCO Solenoid Pilot Valves Covered

3/2 Tamper Proof and 3/2 High Shock Manual Reset Valves have been evaluated per IEC 61508 parts 1 and 2 and covered under this document.

6 Status of the document

6.1 Releases

Revision:	(initial release)
ECN Number:	217357
Release status:	V9642 Initial Release on TBD