Safety Manual for Fisher™ DSV1000 Valves

Purpose

This safety manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Fisher DSV1000 valve.

⚠ WARNING

This instruction manual supplement is not intended to be used as a stand-alone document. It must be used in conjunction with the following manual:

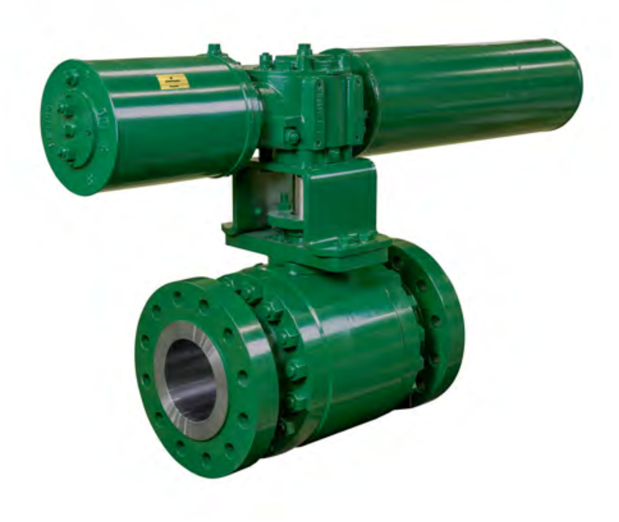
Fisher DSV1000 Full-Bore Ball Valves Instruction Manual (D104727X012)

Failure to use this instruction manual supplement in conjunction with the above referenced manual could result in personal injury or property damage. If you have any questions regarding these instructions or need assistance in obtaining any of these documents, contact your Emerson sales office.

Introduction

This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

Figure 1. Fisher DSV1000 Valve



DSV1000 WITH G-SERIES ACTUATOR

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 injury 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 the facts - of the safety achieved by safety-related systems.

Fail-Safe State: State where valve actuator 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.

Acronyms

FMEDA: Failure Modes, Effects and Diagnostic Analysis

HFT: Hardware Fault Tolerance

MOC: Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.

PFD_{AVG}: Average Probability of Failure on Demand

SFF: Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.

SIF: Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).

SIL: Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.

SIS: Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

Related Literature

Hardware Documents:

Bulletin:

51.3:DSV1000, Fisher DSV1000 Full-Bore Ball Valve: D104724X012

Instruction Manual:

Fisher DSV1000 Full-Bore Ball Valve: D104727X0012

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

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

Product Description

Fisher DSV1000 valve (figure 1) is used in Safety Instrumented System (SIS) service. These valves connect to a variety of rotary-shaft actuators. Fisher DSV1000 is designed to meet international standards for pressure and temperature ratings. Fisher DSV1000 valves move to a designated safe state when called upon to perform the required safety function. They are typically used with other interface components (valve actuator and positioner or solenoid valve) to provide a final element subsystem for a Safety Instrumented Function (SIF).

Designing a SIF Using Fisher DSV1000 Valve

Safety Function

When the valve's actuator is de-energized, the actuator and valve shall move to its fail-safe position. Depending on which configuration is specified fail–closed or fail-open, the actuator will rotate the valve ball to close off the flow path through the valve body or open the flow path through the valve body.

The DSV1000 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.

Pressure, Temperature, and Environmental Limits

The designer of a SIF must check that the product is rated for use within the expected pressure, temperature, and environmental limits. Refer to the DSV1000 valve product bulletin (D104724X012) for these environmental limits.

Application Limits

The materials of construction of DSV1000 valves are specified in the DSV1000 product bulletin (D104724X012). A range of materials are available for various applications. The serial card will indicate what the materials of construction are for a given valve. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and environmental conditions. If the DSV1000 valve is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

Diagnostic Response Time

The DSV1000 valve does not perform any automatic diagnostic functions by itself and therefore it has no diagnostic response time of its own. However, automatic diagnostics of the final control subsystem may be performed such as Partial Valve Stroke Testing (PVST). This typically will exercise the valve over a small percentage of its normal travel without adversely affecting the flow through the valve. If any failures of this PVST are automatically detected and annunciated, the diagnostic response time will be the PVST interval time. The PVST must be performed 10 times more often than an expected demand in order for credit to be given for this test.

Design Verification

A detailed FMEDA report is available from Emerson. This report details all failure rates and failure modes as well as the expected lifetime.

The achieved SIL of an entire SIF design must be verified by the designer via a calculation of PFD_{AVG} 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 HFT requirements.

When using a DSV1000 valve in a redundant configuration, a common cause factor of at least 5% should be included in the Safety Integrity calculations. This value is dependent on the level of common cause training and maintenance in use at the end user's facility.

The failure rate data listed in the FMEDA report is only valid for the useful lifetime of a DSV1000 valve. The failure rates will increase after this time period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the useful lifetime may yield results that are too optimistic, i.e. the calculated Safety Integrity Level will not be achieved.

SIL Capability

Systematic Integrity

Figure 2. exida SIL 3 Capable

The product has met manufacturer design process requirements of IEC 61508 Safety Integrity Level 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A SIF designed with this product must not be used at a SIL level higher than stated without “prior use” justification by the end user or diverse technology redundancy in the design.

Random Integrity

The DSV1000 valve is classified as a Type A device according to IEC 61508, having a hardware fault tolerance of 0. The complete final element subsystem, with a Fisher valve as the final control element, will need to be evaluated to determine the Safe Failure Fraction of the subsystem. If the SFF for the entire final element subsystem is between 60% and 90%, a design can meet SIL 2 @ HFT=0.

Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the DSV1000 valve.

Connection of the Fisher DSV1000 Valve to the SIS Logic solver

The final element subsystem (consisting of a positioner, actuator, and DSV1000 valve) is connected to the safety rated logic solver which is actively performing the Safety Function as well as any automatic diagnostics designed to diagnose potentially dangerous failures within the DSV1000 valve, actuator and any other final element components, (i.e. Partial Valve Stroke Test).

General Requirements

The system's response time shall be less than process safety time. The final control element subsystem needs to be sized properly to assure that the response time is less than the required process safety time. The DSV1000 valve will move to its safe state in less than the required SIF's safety time under the specified conditions.

All SIS components including the DSV1000 valve must be operational before process start-up. The user shall verify that the DSV1000 valve is suitable for use in safety applications.

Personnel performing maintenance and testing on the DSV1000 valve shall be competent to do so.

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

The useful life of the DSV1000 valve is discussed in the Failure Modes, Effects and Diagnostic Analysis Report for the Fisher DSV1000 valve.

Installation and Commissioning

Installation

The Fisher DSV1000 valve must be installed per standard practices outlined in the appropriate instruction manual.

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

The DSV1000 valve must be accessible for physical inspection.

Physical Location and Placement

The Fisher DSV1000 valve shall be accessible with sufficient room for the actuator, pneumatic connections, and any other components of the final control element. Provisions shall be made to allow for manual proof testing.

Pneumatic piping to the actuator shall be kept as short and straight as possible to minimize the airflow restrictions and potential clogging. Long or kinked pneumatic tubes may also increase the valve closure time.

The DSV1000 valve 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.

Operation and Maintenance

Suggested Proof Test

The objective of proof testing is to detect failures within a DSV1000 valve 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 a DSV1000 valve 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 proof test shown in table 1 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 Emerson Automation Solutions. The suggested proof test consists of a full stroke of the DSV1000 valve.

The person(s) performing the proof test of a DSV1000 valve should be trained in SIS operations, including bypass procedures, valve maintenance and company Management of Change procedures. No special tools are required.

Table 1. Recommended Full Stroke Proof Test

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Interrupt or change the signal/supply to the actuator to force the actuator and valve to perform a full stroke to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time.
3	Restore the supply/signal to the actuator and confirm that the normal operating state was achieved.
4	Inspect the DSV1000 valve and the other final control element components for any leaks, visible damage or contamination.
5	Record the test results and any failures in your company's SIF inspection database.
6	Remove the bypass and restore normal operation.

Repair and Replacement

Repair procedures in the appropriate valve instruction manual must be followed.

Manufacturer Notification

Any failures that are detected and that compromise functional safety should be reported to Emerson. Please contact your Emerson sales office.

Appendix A

Sample Startup Checklist

This appendix provides a Sample Start-up Checklist for a Fisher DSV1000 valve. A start-up checklist will provide guidance during the final control element's employment.

Start Up Checklist

The following checklist may be used as a guide to employ the DSV1000 valve in a safety critical SIF compliant to IEC61508.

#	Activity	Result	Verified	
			By	**Date**
	Design			
	Target Safety Integrity Level and PFD$_{AVG}$ 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			
	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			

Neither Emerson, Emerson Automation Solutions, nor any of their affiliated entities assumes responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use, and maintenance of any product remains solely with the purchaser and end user.

Fisher is a mark owned by one of the companies in the Emerson Automation Solutions business unit of Emerson Electric Co. Emerson Automation Solutions, Emerson, and the Emerson logo are trademarks and service marks of Emerson Electric Co. All other marks are the property of their respective owners.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available upon request. We reserve the right to modify or improve the designs or specifications of such products at any time without notice.

Emerson Automation Solutions
Marshalltown, Iowa 50158 USA
Sorocaba, 18087 Brazil
Cernay, 68700 France
Dubai, United Arab Emirates
Singapore 128461 Singapore

www.Fisher.com

EMERSON