SIL Safety Manual for Type BM6X Slam Shut Valve

Figure 1. *Type BM6X Slam-Shut Valve*

Purpose

This safety manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Type BM6X slam shut valve.

Introduction

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

Terms and Abbreviations

Safety: Freedom from unacceptable risk.

Functional Safety: The ability of a system to carry out the actions necessary to achieve or 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 and 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:

Type BM6X slam shut valve Bulletin: **0016EN**

Type BM6X slam shut valve Instruction Manual:
Type BM6X 3”~12”: **0028EN**

Guidelines/References:

- Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis, ISBN 1-55617-777-1, 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

Device Description

The purpose of the Type BM6X slam shut device (see Figure 1) is to totally and rapidly cut the flow of gas when the inlet and/or outlet pressure in the system either exceeds or drops below set points. The Type BM6X is axial flow design and possible to fit in horizontal positions, and also possible in vertical position only with a flow direction from top to bottom.

Limit switch, Solenoid is option for device status transmitter and remote control.

Designing a SIF Using Type BM6X Slam Shut Valve

Safety Function

When the inlet and/or outlet pressure in the system either exceeds or drops below set points, the actuator and valve shall move to its fail-safe position. The valve plug will move to close off the flow path through the valve body.

The Type BM6X slam shut 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.

Environmental limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the Type BM6X slam shut valve product bulletin for environmental limits.

Application limits

The materials of construction of Type BM6X slam shut valve are specified in the product bulletin. 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 Type BM6X slam shut valve is used outside of the application limits or with incompatible materials, the reliability data provided becomes invalid.

Design Verification

A detailed FMEDA report is available from Emerson Process Management Regulator Technologies, Inc., (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 Type BM6X slam shut valve in a redundant configuration, a common cause factor of at least 5% should be included in the Safety Integrity calculations.

The failure rate data listed in the FMEDA report is only valid for the useful lifetime of a Type BM6X slam shut 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 SIL 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 Type BM6X slam shut valve is classified as Type A devices according to IEC 61508, having a hardware fault tolerance of 0. The failure rate data used for the analysis of the BM6X Series Slam Shut Valves meets the exida criteria for Route 2_H; therefore, BM6X Series Slam Shut Valves meets the hardware architectural constraints for up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) as a single device when the failure rates listed in the FMEDA report are used.

Safety Parameters

For detailed failure rate information refer to the Failure Modes, Effects and Diagnostic Analysis Report for the Type BM6X slam shut valve.

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 Type BM6X slam shut valve will move to its safe state in less than the required SIF’s safety time under the specified conditions.

All SIS components of Type BM6X slam shut valve must be operational before process start-up.

The user shall verify that the Type BM6X slam shut valve is suitable for use in safety applications.

Personnel performing maintenance and testing on the Type BM6X slam shut valve shall be competent to do so.

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

The useful life of the Type BM6X slam shut valve is discussed in the Failure Modes, Effects and Diagnostic Analysis Report.

Installation and Commissioning

Installation

The Type BM6X slam shut valve must be installed per standard practices outlined in the appropriate Instruction Manual.

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

The Type BM6X slam shut valve must be accessible for physical inspection.

Physical Location and Placement

The Type BM6X slam shut 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 Type BM6X slam shut 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 Type BM6X slam shut 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 Type BM6X slam shut 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.

Table 1. *Recommended Full Stroke Proof Test*

STEP	ACTION
1	Bypass the safety function and take appropriate action to avoid a false trip.
2	Change the sensor(s) pressure to simulate a trip and observe that the valve stroked to the Fail-Safe state and confirm that the Safe State was achieved and within the correct time. Remove the cover of the Slam Shut Device and inspect for damage or leakage of the valve.
3	Determine the codes and standards applicable to the valve installation and confirm that the valve internal leakage does not exceed the leakage specification.
4	Restore the process signal to the sensor and reset the valve. Check the valve for any leaks, visible damage or contamination and confirm that the normal operating state was achieved.
5	Remove the bypass and restore normal operation.

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™. The suggested proof test consists of a full stroke of the Type BM6X slam shut valve.

The person(s) performing the proof test of a Type BM6X slam shut valve should be trained in SIS operations, including bypass procedures, valve maintenance and company Management of Change procedures. No special tools are required.

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 local Sales Office.

Note

Emerson or any of their affiliated entities shall not assume responsibility for the selection, use or maintenance of any product. Responsibility for the selection, use and maintenance of any product remains with the purchaser and end user.

Industrial Regulators

Emerson Process Management
Regulator Technologies, Inc.

USA - Headquarters
McKinney, Texas 75070 USA
Tel: +1 800 558 5853
Outside U.S. +1 972 548 3574

Asia-Pacific
Shanghai 201206, China
Tel: +86 21 2892 9000

Europe
Bologna 40013, Italy
Tel: +39 051 419 0611

Middle East and Africa
Dubai, United Arab Emirates
Tel: +971 4811 8100

Natural Gas Technologies

Emerson Process Management
Regulator Technologies, Inc.

USA - Headquarters
McKinney, Texas 75070 USA
Tel: +1 800 558 5853
Outside U.S. +1 972 548 3574

Asia-Pacific
Singapore 128461, Singapore
Tel: +65 6770 8337

Europe
Bologna 40013, Italy
Tel: +39 051 419 0611
Chartres 28008, France
Tel: +33 2 37 33 47 00

Middle East and Africa
Dubai, United Arab Emirates
Tel: +971 4811 8100

TESCOM

Emerson Process Management
Tescom Corporation

USA - Headquarters
Elk River, Minnesota 55330-2445, USA
Tels: +1 763 241 3238
+1 800 447 1250

Europe
Selmsdorf 23923, Germany
Tel: +49 38823 31 287

Asia-Pacific
Shanghai 201206, China
Tel: +86 21 2892 9499

For further information visit www.tartarini-naturalgas.com