Safety Manual

Mechanically actuated valves, direct operated solenoid valves, pneumatically operated valves and pilot operated solenoid valves

HAFNER Pneumatika Kft.
Halászi
Hungary

Version V1, Revision R1, November 2016

Content

1 Introduction

This Safety Manual provides information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the mechanically actuated valves, direct operated solenoid valves, pneumatically operated valves and pilot operated solenoid valves. This manual provides necessary requirements for meeting the IEC 61508 or IEC 61511 functional safety standards.

1.1 Terms and Abbreviations

Safety	Freedom from unacceptable risk of harm
Functional Safety	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment / machinery / plant / apparatus under control of the system
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition
Safety Assessment	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems
Fail-Safe State	State where solenoid valve is de-energized and spring is extended.
Fail Safe	Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic stroke testing.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic stroke testing.
Fail Annunciation Undetected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic.
Fail Annunciation Detected	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication.
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.

1.2 Acronyms

FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance
MOC	Management of Change. These are specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFDavg	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIF	Safety Instrumented Function, a set of equipment intended to reduce the risk due to a specific hazard (a safety loop).
SIL	Safety Integrity Level, discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest.
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

1.3 Product Support

Product support can be obtained from:

HAFNER Pneumatika Kft.

H-9228 Halászi, Püski út 3.

Tel.: +36-96-573-012

E-Mail: ertekesites@hafner-pneumatika.com

1.4 Related Literature

Hardware Documents:

- Solenoid Valves Installation, Operation and Maintenance Instructions for the directional control valves of the HAFNER Pneumatika Kft.

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: 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 Device Description

2.1 Mechanically actuated valves

Hafner is offering a wide range of mechanically actuated valves. The valves become actuated either by stem, roller lever or roller lever with idle return. 3/2-way and 5/2-way versions with mechanical spring reset to basic position are available. Valves are available with port size M5, pif 4 mm, G 1/8" as well as G ¼" and offer between 115 l/min up to 1.250 l/min air-flow.

2.2 Direct operated solenoid valves

Hafner is offering a wide range of direct operated solenoid valves. 2-way and 3-way versions with mechanic spring are available. Valves are available with port size M5 up to G 1/4" and offer between 30 l/min up to 200 l/min air-flow. Valves are available with banjo-screw, as in-line version, for manifold assembly and as modular system. Standard solenoid operators are 230V/50Hz, 110V/50Hz, 24V/50Hz, 48V=, 24V=, 12V=.

2.3 Pneumatically operated valves

Hafner is offering a wide range of pneumatically operated valves. 2-way, 3-way and 5-way versions with pneumatic spring, mechanic spring as well as double pilot versions are available. Valves are available with port size M5 up to G ¾" and offer between 180l/min up to 6.000 l/min air-flow. Valves are available as in-line version, with NAMUR-interface and for manifold assembly.

2.4 Pilot operated solenoid valves

Hafner is offering a wide range of pilot operated solenoid valves. 2-way, 3-way and 5-way versions with pneumatic spring, combined spring as well as dual coil versions are available. Valves are available with port size M5 up to G ¾" and offer between 230 l/min up to 6.000 l/min air-flow. Valves are available as in-line version, with NAMUR-interface, for manifold assembly and for valve terminals. Standard solenoid operators are 230V/50Hz, 110V/50Hz, 24V/50Hz, 48V=, 24V=, 12V=

3 Designing a SIF using a HAFNER Pneumatika Kft. Solenoid valves

3.1 Safety Function

When de-energized, the actuator moves the Solenoid valves to their fail-safe position. Depending on the version specified Fail – Closed or Fail - Open, the Solenoid valves will rotate the valve plug to close off the flow path through the valve body or open the flow path through the valve body.

The Solenoid valves is intended to be part of final element subsystem as defined per IEC 61508 and the achieved SIL level of the designed function must be verified by the designer.

3.2 Environmental limits

The designer of a SIF must check that the product is rated for use within the expected environmental limits. Refer to the HAFNER Pneumatika Kft. Solenoid Valves Installation, Operation and Maintenance Instructions for environmental limits.

3.3 Application limits

The materials of construction of a Solenoid valves are specified in the HAFNER Pneumatika Kft. Solenoid Valves Installation, Operation and Maintenance Instructions. It is especially important that the designer check for material compatibility considering on-site chemical contaminants and air supply conditions. If the Solenoid valves are 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 HAFNER Pneumatika Kft.. 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 architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements. The exida exSILentia® tool is recommended for this purpose as it contains accurate models for the Solenoid valves and their failure rates.

When using Solenoid valves in a redundant configuration, a common cause factor of at least 5% should be included in safety integrity calculations.

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

3.5 SIL Capability

3.5.1 Systematic Integrity

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

3.5.2 Random Integrity

When the final element assembly consists of many components (Solenoid valves, actuator, solenoid, quick exhaust 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 Solenoid valves.

3.6 Connection of the Solenoid valves to the SIS Logic-solver

The Solenoid valves are 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 Solenoid valves and the final element valve, (i.e. partial valve stroke test).

3.7 General Requirements

The system’s response time shall be less than process safety time. The Solenoid valves will move to its safe state in not more than 50 ms under specified conditions.

All SIS components including the Solenoid valves must be operational before process start-up.

User shall verify that the Solenoid valves are suitable for use in safety applications by confirming the Solenoid valves nameplates are properly marked.

Personnel performing maintenance and testing on the Solenoid valves shall be competent to do so.

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

The useful life of the Solenoid valves is discussed in the Failure Modes, Effects and Diagnostic Analysis Report for the Solenoid valves.

4 Installation and Commissioning

4.1 Installation

The Solenoid valves valve must be installed per standard practices outlined in the HAFNER Pneumatika Kft. Solenoid Valves Installation, Operation and Maintenance Instructions.

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

The Solenoid valves must be accessible for physical inspection.

4.2 Physical Location and Placement

The Solenoid valves shall be accessible with sufficient room for pneumatic connections and shall allow manual proof testing.

Pneumatic piping to the valve 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 Solenoid valves shall be mounted in a low vibration environment. If excessive vibration can be expected special precautions shall be taken to ensure the integrity of pneumatic connectors or the vibration should be reduced using appropriate damping mounts.

4.3 Pneumatic Connections

Recommended piping for the inlet and outlet pneumatic connections to the Solenoid valves is 1/2" stainless steel or PVC tubing. The length of tubing for the Solenoid valves shall be kept as short as possible and free of kinks.

The pressurized air filtering, pressure, and air quality are specified in the HAFNER Pneumatika Kft. Solenoid Valves Installation, Operation and Maintenance Instructions

The process air capacity shall be sufficient to move the valve within the required time.

5 Operation and Maintenance

5.1 Proof test without automatic testing

The objective of proof testing is to detect failures within a HAFNER Pneumatika Kft. 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 d, is to be determined in reliability calculations for the safety-instrumented functions for which an HAFNER Pneumatika Kft. 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 following proof test is recommended. The results of the proof test should be recorded and any failures that are detected and that compromise functional safety should be reported to HAFNER Pneumatika Kft.. The suggested proof test consists of a full stroke of the Solenoid valves.

Step	Action
1	Bypass the safety function and take appropriate action to avoid a false trip
2	Inspect the device for any visible damage, corrosion or contamination.
3	De-energize / de-activate the valve and verify that the connected actuator is moved into its safe position and that this is achieved within the appropriate time.
4	Remove the bypass and otherwise restore normal operation
5	Record any failures in your company's SIF inspection database

Table1: Recommended Proof Test

For the test to be effective the movement of the valve must be confirmed. To confirm the effectiveness of the test both the travel of the valve and slew rate must be monitored and compared to expected results to validate the testing.

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

5.2 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 Solenoid valves 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.

5.3 Repair and replacement

Repair procedures in the Solenoid Valves Installation, Operation and Maintenance Instructions must be followed.

5.4 Useful Life

The useful life of the Solenoid valves is approximately 10 years for the mechanical parts. For the Solenoid coil this time 10 6 years for power <2W and 3 years for power >2W.

5.5 MANUFACTURER Notification

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

6 Status of the document

6.1 Releases

Version History:	V0, R1:	Draft 2016-09-22
	V1, R0:	Updated after review 2016-10-31
	V1, R1:	Released version 2016-11-08

Release status: Released