SAFETY MANUAL

SOLENOID VALVES

3/2 – 5/2

SIZE ¼” ½”

AND ACCESSORIES

Data Revisione Rev. Date	Revisione numero Rev. Number	Redattore Compiler
03/01/2017	00	C. Brembati
14/01/2022	01	C. Brembati

Emesso Issue	Verificato Verified	Approvato Approved
Lurano 03/01/2017	Lurano 03/01/2018	Lurano 03/01/2017
C. Brembati	M. Cencio	G. Resmini

INDEX

1 Introduction

1.1 Scope and purpose of the Safety Manual

This safety manual provides the information necessary to design, install, verify and maintain a Safety Instrumented Function (SIF) utilizing the Steel Line Solenoid Valves and Accessories. This manual provides necessary requirements to enable the integration of the Steel Line Solenoid Valves and Accessories when showing compliance with the IEC 61508 or IEC 61511 functional safety standards.
This Safety Manual indicates all assumptions that have been made on the usage of these valves.
If the assumptions cannot be met by the application, the SIL capability of the Steel Line Solenoid Valves and Accessories may be adversely.

The safety function used in Steel Line Solenoid Valves and Accessories is defined as follows:
a. When an unsafe condition is detected in a plant by a process sensor, the controller, via the control panel, de-energize the solenoid valve which vents the load air port (2) via the exhaust port (3);
b. When an unsafe condition is detected in a plant by a process sensor, the controller, via the control panel, drives to energize a solenoid valve, and providing air to the load;

The choice of the safety function to be implemented is responsibility of the system integrator.

1.2 Skill level required

System design, installation and commissioning, and repair and maintenance shall be carried out by suitably qualified personnel.
For the installation / repair / maintenance, the manufacturer must provide a Use and Maintenance Manual.

1.3 Product Support & Service

Please refer to the PNEUMAX Quality and Technical Offices.

1.4 Related Documents

Valves datasheet and drawing

Use and Maintenance Manuals

1.5 Reference standards

IEC 61508-1÷7: 2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
IEC 60654-1:1993-02, second edition, Industrial-process measurement and control equipment – Operating conditions

1.6 Terms, abbreviations and acronyms

Safety - Freedom from unacceptable risk of harm.
BPCS - Basic Process Control System - a system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1.
Fail-safe State - State where solenoid valve is de-energized and spring is extended.
Fail Annunciation Detected - 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 Undetected - 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 Dangerous (λ_D) - Failure that does not respond to a demand from the process (i.e. being unable to go to the fail-safe state).
Fail Dangerous Detected (λ_{DD}) - Failure that is dangerous but is detected as part of partial valve stroke testing.
Fail Dangerous Undetected (λ_{DU}) - Failure that is dangerous and that is not detected as part of partial valve 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.
Fail Safe – (λ_S) Failure that causes the valve to go to the defined fail-safe state without a demand from the process.
Fail Safe Detected (λ_{SD}) - Failure that is safe and is detected as part of partial valve stroke testing.
Fail Safe Undetected (λ_{SU}) - Failure that is safe and that is not detected as part of partial valve stroke testing.
FMEDA - Failure Modes, Effects and Diagnostics Analysis.
Functional safety - Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers.
HFT - Hardware Fault Tolerance.
Low demand - Mode of operation, where the frequency of demands for operation made on a safety related system is no greater than twice the proof test frequency.
MOC - Management Of Change - specific procedures often done when performing any work activities in compliance with government regulatory authorities.
PFD_{AVG} - Average Probability of Failure on Demand.
PVST - Partial Valve Stroke Test.

SFF - Safe Failure Fraction - fraction of the overall random failure rate of a device that results in either a safe failure or a detected dangerous failure.

SIF - Safety Instrumented Function - safety function with a specified SIL, which is necessary to achieve functional safety. Typically, a set of equipment intended to reduce the risk due to a specified hazard (a safety loop).

SIL - Safety Integrity Level - discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest level of safety integrity; SIL 1 has the lowest.

SIS - Safety Instrumented System - instrumented system used to implement on or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

2 Device Description

Model	SS1432C##01 - SS1232C##01 SS1132C##01 – SS3432C##01 SS14520##01 - SS12520##01 SS1152C##01 – SS3452C##01	Solenoid-Spring Valves 3/2 and 5/2 Monostable and Bistable
	SS1432C#### - SS1232C#### SS14520#### - SS12520####	Double Solenoid Valves 3/2 and 5/2 Monostable and Bistable
	SS1432C0401L - SS145200401L	Roller-Spring Valves 3/2 and 5/2 Monostable and Bistable
	SS1432C0001L - SS145200001L	Plunger-Spring Valves 3/2 and 5/2 Monostable and Bistable
	SS1232C1101L - SS1432C1101L SS125201101L - SS145201101L	Pneumatic-Spring Valves 3/2 and 5/2 Monostable and Bistable
	SS1232C1111L - SS1432C1111L SS125201111L - SS145201111L	Pneumatic-Pneumatic Valves 3/2 and 5/2 Monostable and Bistable
	SS1232C1114L - SS1432C1114L	Pneumatic-spring type valve self-locking and release by the operator 3/2
	SS1232CA114L - SS1432CA114L	Solenoid-spring type valve with self-locking and release by the operator 3/2
	SS1202SR# - SS1402SR# SS1102SR# - SS3402SR# -	Quick exhaust valves
	TXSS17#####	Filters and filter regulator.
Size	1/4" - 1/2" - 1” - 3/4”	
Body Material	AISI 316L	
Spool, Spring, Operator	AISI 316L	
Seals Material	FPM NBR for low temperatures (-50°C) standard.	

The models are designed to be used in a Safety Instrumented System for use **in Low Demand** application.

The valves are classified as **Type A** devices according to IEC 61508, having an hardware fault tolerance of 0 (**1oo1** architecture).

3 Designing a SIF Using the solenoid valves

3.1 Safety Function

When the valve is de-energized, the spool shall move to its safety position by means of the spring force.
The valves are 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 the SIF must check that the product is rated for use within the expected environmental limits, maximum working pressure and temperature. Refer to the valves datasheet for this information.

3.3 Application limits

The materials of construction of the valve are specified in the datasheet.
It is especially important that the designer of the SIF check for material compatibility considering on-site chemical contaminants and air (as appropriate) supply conditions. If the solenoid valves are used outside the application limits or with incompatible materials, the reliability data and predicted SIL capability becomes invalid.

3.4 Design Verification

A detailed Failure Modes, Effects and Diagnostics Analysis (FMEDA) report is available from the manufacturer for these products. This report details all failure rates and failure modes as well as expected lifetime of the product.
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 the architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failures rates of all equipment included in the SIF. Each subsystem must be checked to assure compliance with minimum Hardware Fault Tolerance (HFT) requirements. A suitable tool is recommended for this purpose.
When using the valves in a redundant configuration, a common cause factor b of 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 the valves. The failure rates will increase after this useful lifetime period has expired. 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 SIL will not be achieved.

3.5 SIL Capability

3.5.1 Systematic Integrity

The solenoid valves have met manufacturer design process requirements of SIL 3.

This systematic capability is guaranteed only if the user:
1. Use the device according to the instructions for use and to the present Manual
2. Use the device in the appropriate environment (limitation of use)

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 higher than the statement without “prior use” justification by the end user, or verification of diverse technology in the design.

3.5.2 Random Hardware Integrity

According to IEC 61508 the architectural constraints of an element must be determined. This has been done by following the 1H approach according to 7.4.4.2 of IEC 61508.

The 1H approach involves calculating the SFF for the entire element. Please refer to Table 2 of IEC 61508-2 for assessing the max SIL achievable by the solenoid valve, with respect to SFF and HFT.

WARNING: the SFF for the entire subsystem shall be evaluated, after having designed the complete loop, in order to satisfy the architectural constraints and the target failure measure!

The solenoid valves are classified as a device that is part of a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

The solenoid valves can be classified as a 1H device when the failure rates listed in the FMEDA report are used for the Design Verification calculations. When 1H 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 1H.

When the final element assembly consists of several components additional to SBF / SBT ball valve, the SIL must be verified for the entire assembly using the failure rates of all components. This analysis must account for architectural constraints by comparing both SFF and HFT with IEC61508-2.

3.5.3 Safety Parameters

For detailed failure rate information refer to the FMEDA report for the solenoid valves. The failure rates and modes are derived from the following data source:
"EXIDA - Electrical & Mechanical Component Reliability Handbook (2nd Ed-2008), with environmental profile B2 as per IEC 60654-1."
See relevant certificates for λ_{SU} and λ_{DU} values according with the safety function.

3.6 Connection of the Valve to the SIS Logic Solver

The solenoid valves should be assembled with an actuator and logic solver where all components are safety rated.
The safety rated logic solver shall actively perform the safety function as well as automatic diagnostics (if any) designed to diagnose potentially dangerous failures within the valves.

3.7 General Requirements

The system and function response time shall be less than the process safety time. The solenoid valve will move to its defined safe state in less than this time with relation to the specific hazard scenario.
The response time of a solenoid pilot valve will vary by design. The factors that affect response time are pilot valve orifice size, operating pressure, size of actuator, torque required to open and close process valve, and distance between pilot valve and actuator.
All SIS components including the solenoid valves must be operational before process start-up.
The User shall verify that the valve is suitable for use in safety applications by confirming the nameplate and model number is properly marked.
Personnel performing maintenance and testing on the solenoid valves shall first be assessed as being competent to do so. Results from periodic proof tests shall be recorded and periodically reviewed.
The solenoid valves shall not be operated beyond the useful lifetime as listed in paragraph 5.3 without undergoing overhaul or replacement.

4 Installation & Commissioning

4.1 Installation

The solenoid valves must be installed per the standard practices outlined in the Use and Maintenance Manual.
The environment must be checked to verify that environmental conditions do not exceed the ratings.
The 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 shall allow for manual proof testing to take place.
The valves shall be mounted in a low vibration environment. If excessive vibration can be expected then special precautions shall be taken to ensure the integrity of pneumatic connectors or the vibration should be reduced using appropriate damping mounts.

5 Operation & Maintenance

5.1 Proof Test requirement

During operation, a low demand mode SIF must be proof tested. The objective of proof testing is to detect failures within the equipment in the SIF that are not detected by any automatic diagnostics of the system. Of main concern are undetected failures that prevent the SIF from performing its function.
Periodic proof tests shall take place at the frequency (or interval) defined by a SIL verification calculation. The proof tests must be performed more frequently than (or as frequently as) specified in the SIL verification calculation in order to maintain the required safety integrity of the overall SIF. Results from periodic proof tests and partial valve stroke tests (if any) shall be recorded and periodically reviewed.

5.2 Repair and replacement

Repair procedures specified in the Use and Maintenance Manual must be followed. The MRT to be considered is 24 hours. The MRT considered is the technical mean repair time, i.e. it takes in consideration availability of skilled personnel, adequate tool and spare parts.

5.3 Useful life

Based on general field failure data and a low demand mode of operation, a useful life period of approximately 5 to 10 years is expected for the solenoid valve.

5.4 Notification of failures

In case of malfunction of the system or SIF, the solenoid valve shall be put out of operation and the process shall be kept in a safe state by other measures.

Please remember that: the detection of a faulty state of the item, by means of proof testing, shall be treated as stated in 7.4.8.2 of IEC 61508-2:2010 or, alternatively, 11.3 of IEC 61551-1.

PNEUMAX must be informed when the solenoid valves are required to be replaced due to failure. The occurred failure shall be documented and reported to PNEUMAX Quality & Technical representatives.