SAFETY MANUAL FOR SWITCHING VALVE S3

STC-SM-SW

5					
4					
3					
2	Formal Revision	23/09/2019	CM	GC	DMDC
1	First Issue	24/03/2016	CM	GC	DMDC
No.	DESCRIPTION	DATA	ISSUE Technical Dept.	VERIFIED Quality Dept.	APPROVED General Mngr.
REVISIONS					

SUMMARY

0 INTRODUCTION

Purpose of this Safety Manual, written in compliance with IEC 61508-2, Annex D, is to give all the necessary information to the system integrator for a correct use of the product in Safety Instrumented Systems for SIL classified applications.

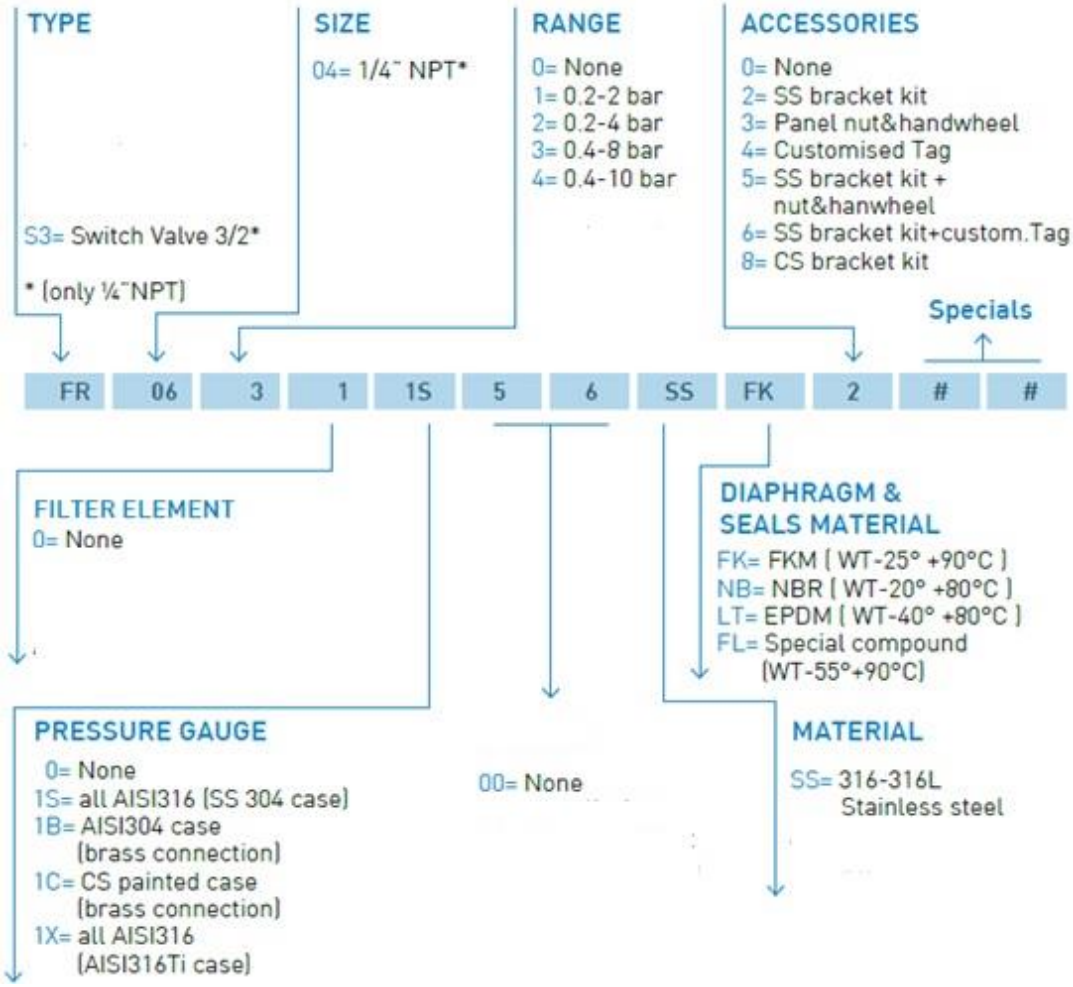
1 SAFETY FUNCTION SPECIFICATION

The Safety Functions for three-way Switching Valve used in safety-related services duties can be defined as follow:

When the signal pressure goes below the set value (regulated via the internal spring), the switching valve commutates, closing the pressure supply line and discharging the cylinder chamber of the actuator to the exhaust, or piloting a downstream power valve which performs the discharging of the cylinder chamber to the exhaust.

2 CONFIGURATION OF THE PRODUCT

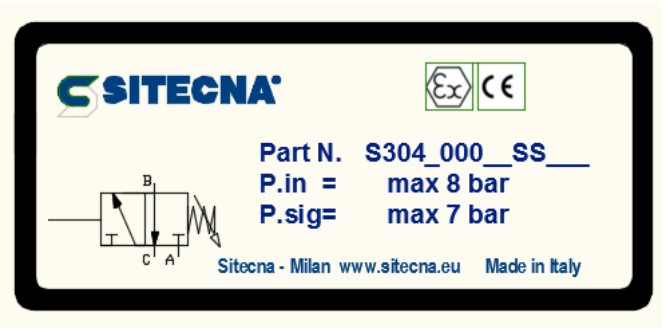
The product is named and coded as follow:



For the setting procedure please see the IOM.
The set point of the Switching Valve is modifiable with via an adjusting screw(See IOM Switching Valve). In option has a “Anti-tamper system” to avoid unauthorized modifications of the set point. This option is mandatory for safety related applications.

3 SERVICE CONDITION LIMITATIONS (LIMITATION OF USE)

The service condition limitations (Max Inlet Pressure 8 bar and range of temperature -20°C + 80°C), the type of material, range regulation and dimension are included on valve label (see the sample below).
Special Material (FVMQ -55°C – FKM +90°C)



Also, we have a “TRACE NUMBER” for the material traceability

4 EXPECTED LIFETIME

Valves lifetime strongly depends on operating conditions and on materials of construction. As a general rule, the customer selects the main materials of construction.

For normal service conditions, the expected lifetime can be considered an average of 20 years.

The above value is valid only if prescriptions in paragraph 6 of this manual are respected.

5 FAILURE MODES AND ESTIMATED FAILURE RATES

Configuration	Safety function	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_{S} [1/h]
S3 - No PST	De-Energise-To-Trip	1,14E-08	0,00E+00	1,05E-07
S3 - With PST	De-Energise-To-Trip	1,14E-10	1,13E-08	1,05E-07

Failure modes and estimated failure rates

NOTES:

1. No internal diagnostics is included in the device.
2. The failure rates are guaranteed:
    a. For the service conditions listed in par. 3
    b. For the expected lifetime declared in par. 4
    c. Considering the periodic test and maintenance included in par. 6

The failure rates are determined performing a FMEDA based on the failure rates of components taken from industrial databases (NPRD-2016/FMD97/2016, EXIDA E&MCRH and NSWC-2011), integrated with field feedback using the Bayesian statistical approach mentioned in IEC 61508-2 Par. 7.4.4.3.3.

The system for reporting failures is based on field feedback from end users, with:

- Identification of the claim/failure
- Root cause analysis to identify cause and responsibility of the failure
- Identification of the possible effect of the failure on the Safety Function
- Classification of the failure considering the failure categories of IEC 61508-2 (Safe, Dangerous, No Effect)

Customer Service, Quality and Technical Department are responsible for the procedure, according to the respective role.

6 PERIODIC TEST AND MAINTENANCE REQUIREMENTS

6.1 General

Please consider that the information in this paragraph are relevant only in regards of Reliability Tests; please refer to the Maintenance and Instructions Manual for detailed information about product maintenance, handling and storage

Tests may be carried out to increase the system reliability.
"On site" tests depend on Project/Plant facilities/requirements; however, a functional test must be executed on site, before Valve usage.

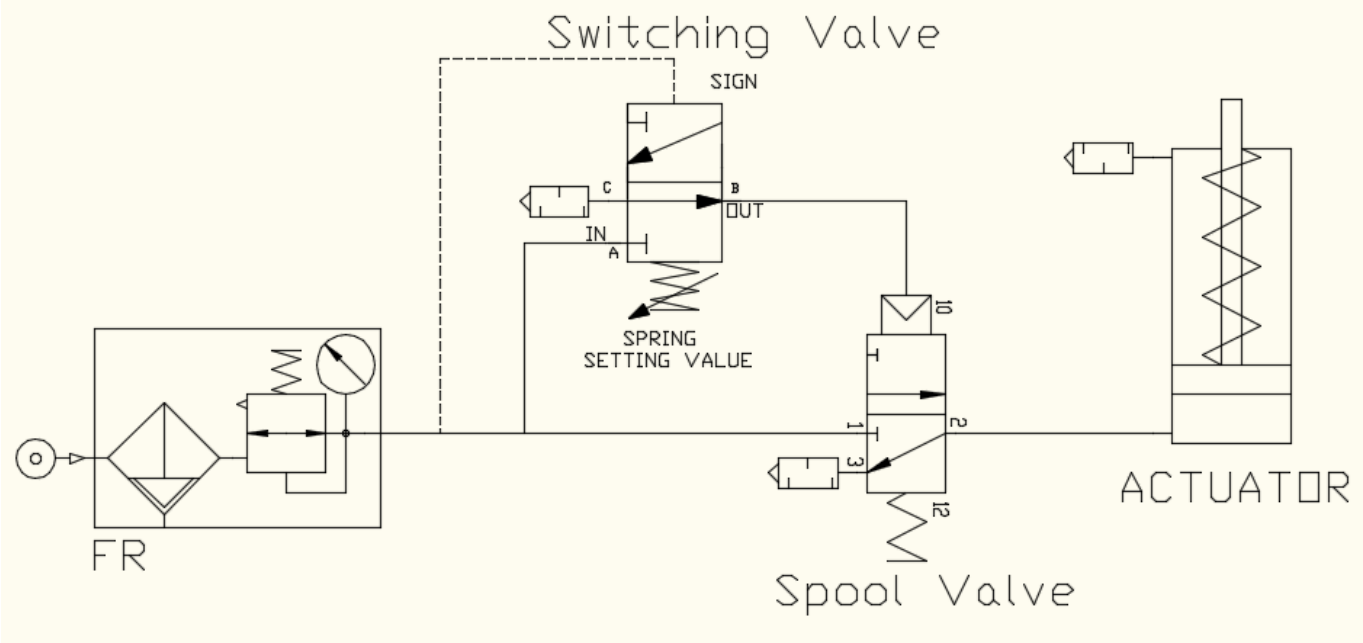
6.2 Full Stroke + Leak Test

The "Full Stroke + Leak Test" ("On line") must be performed to satisfy the PFD_{AVG} (average probability of failure on demand) value.
The test frequencies will be defined from the final integrator in relation to the defined SIL level to achieve.

The following parameters can be verified:

- Correct performing of open – close and test regulation pressure;
- Internal Leakage.

Procedure for Full Stroke Test



- Supply the air in the "Signal Port" and in the "Inlet Port" of the Switch Valve "S3" and increase the pressure in the "Signal Port" above the setting pressure level adjusted on the valve "S3" through the screw;
- Verify the correct functionality of the actuator;
- Decrease the pressure in the "Signal Port" and verify the air exit of the "EXH port" of the Switch Valve "S3" and verify the actuator returns in initial position;

Procedure for Leak Test On Line

- Pressurize the Switch Valve increasing the pressure until 8 bar;
- Verify if there are pressure leak.

Considering the application of the above described Full Stroke + Leak Test procedure, the "Test Coverage" can be considered 100%.

6.3 Partial Stroke Test

- The Partial Stroke Test on the ESD assembly results in full stroke on the S3.

6.4 Periodic Maintenance

The periodic maintenance is described in section 8 of the IOM Manual.

7 CLASSIFICATION

The device is classified Type A according to IEC 61508-2.

8 ARCHITECTURAL CONSTRAINTS

For the evaluation of the conformity to the requirement of Hardware safety integrity architectural constraints of the standard IEC 61508, both Route 1_H and Route 2_H are used.

Route 1_H
- The device has a single channel configuration, HFT=0
- SFF (without external diagnostic tests): 90,15%
- SFF (with external diagnostic tests): 99%

Route 2_H
The application of Route 2_H ("proven in use approach") is evaluated according paragraphs 7.4.10.1÷7.4.10.7 of IEC 61508-2,. Evidence was identified for each specific point.
As the device is classified as "Type A", no requirements for SFF are given for Route 2_H.

Conclusion
The device can be used in single channel configuration up to SIL 3.

9 MEAN REPAIR TIME

The Mean Repair Time (MRT) is:
- Substitution = 30 min
- Repair using the spare part kit = 120 min

The MRT considered is the Technical Mean Repair Time, i.e., it takes in consideration availability of skilled personnel and adequate tools.

10 COMMON CAUSE FACTORS

The product has a single channel configuration, HFT=0.
The β factors can be used when performing PFD_{AVG} calculations for redundant architectures.
The Common Cause factors, relevant when the product is used in redundant configuration, are:

$\beta=\beta_D=0,05$

NOTES:

- The above value is the value for 1oo2 architecture. The values for other architectures shall be calculated according to IEC 61508 Part 6, Table D.5.
- The above value is calculated in the hypothesis of redundancy without diversity

11 SYSTEMATIC CAPABILITY

The systematic capability of the device is 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)