SAFETY MANUAL
FOR VOLUME BOOSTERS
VB04
VB06
VB08
VB12
VB16

STC-SM-VB

5					
4					
3					
2					
1	Formal Revision	17/09/2019	CM	GC	DMDC
0	First Issue	10/05/2016	CM	GC	DMDC
No.	**DESCRIPTION**	**DATA**	**ISSUE Technical Dept.**	**VERIFIED Quality Dept.**	**APPROVED General Mngr.**
REVISIONS					

SUMMARY

0 INTRODUCTION 3

1 SAFETY FUNCTION SPECIFICATION.....3

2 CONFIGURATION OF THE PRODUCT 3

3 SERVICE CONDITION LIMITATIONS (LIMITATION OF USE) 4

4 EXPECTED LIFETIME 4

5 FAILURE MODES AND ESTIMATED FAILURE RATES 4

6 CUSTOMER SERVICE, QUALITY AND TECHNICAL DEPARTMENT ARE RESPONSIBLE FOR THE PROCEDURE, ACCORDING TO THE RESPECTIVE ROLEPERIODIC TEST AND MAINTENANCE REQUIREMENTS 5

7 CLASSIFICATION.....7

8 ARCHITECTURAL CONSTRAINTS 7

9 MEAN REPAIR TIME 7

10 COMMON CAUSE FACTORS 7

11 SYSTEMATIC CAPABILITY 8

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 Volume Booster used in safety-related services duties can be defined as follow :

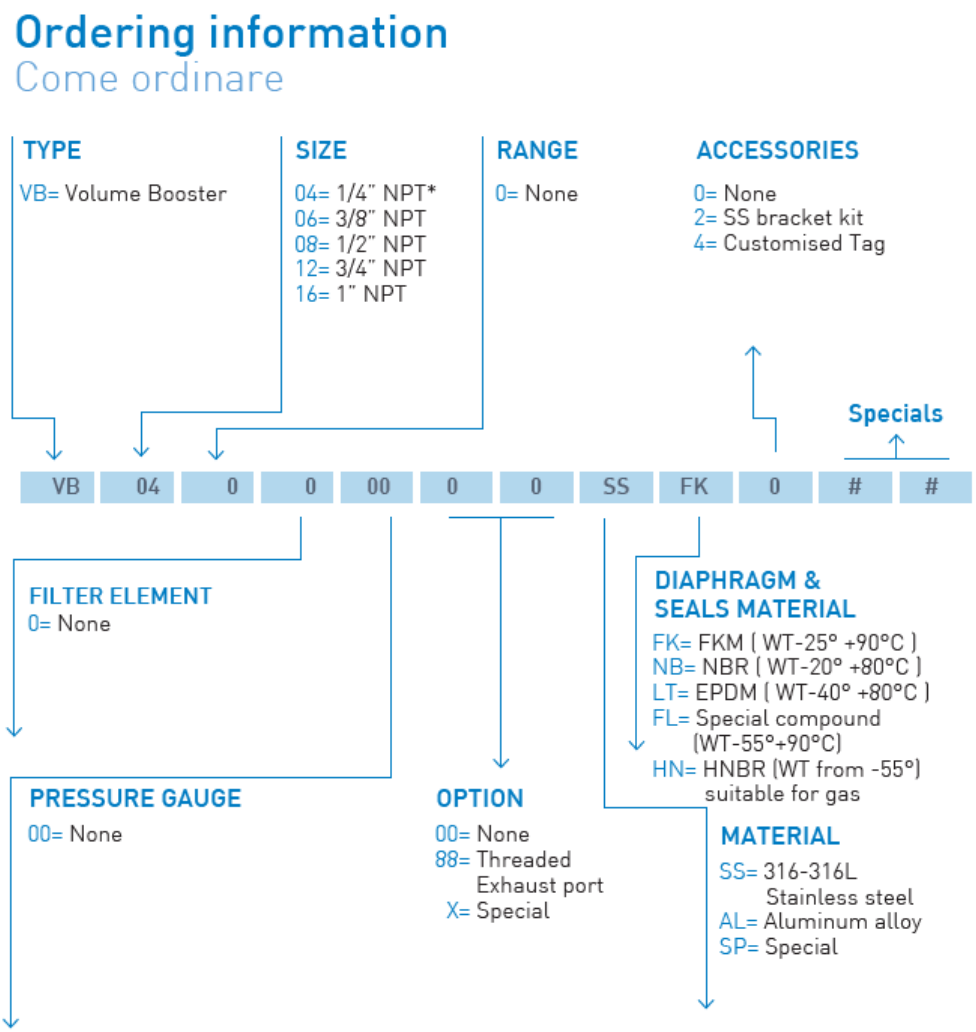
De-energize-to-trip operation (to discharge a chamber of a single acting or double acting actuator): when the pressure on the Signal port goes to zero, the Volume Booster stops the air supply to the cylinder chamber of the actuator which goes to the safety position.

Energize-to-trip operation (to charge a chamber of a double acting actuator): when the pressure on the Signal port goes to the system operating pressure necessary to move the actuator, the Volume Booster allows the air supply to reach the cylinder chamber of the actuator, which goes to the safety position.

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

2 CONFIGURATION OF THE PRODUCT

The product is named and coded as follow:



3 SERVICE CONDITION LIMITATIONS (LIMITATION OF USE)

The service condition limitations (Max Inlet Pressure 10bar), the material of membrane that define the temperature range, are included on valve label (see the sample below).

Furthermore, the device is identified with a “TRACE NUMBER” for the material traceability

NOTE for Energize-to-trip operation:
All the requirements of IEC 61511-1 par. 11.2.11 shall be met.
For this reason, as a pressure switch or pressure transmitter mounted downstream the Volume Booster or upstream the Volume Booster (signal line) would be ineffective, the corresponding tubing connections’ length shall be reduced at a minimum.

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]
VB - No PST	De-Energise-To-Trip	1,12E-08	0,00E+00	5,18E-08
VB - With PST	De-Energise-To-Trip	1,12E-10	1,11E-08	5,18E-08
VB - No PST	Energise-To-Trip	8,92E-08	0,00E+00	0,00E+00
VB - With PST	Energise-To-Trip	8,92E-10	8,83E-08	0,00E+00

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)

6 Customer Service, Quality and Technical Department are responsible for the procedure, according to the respective rolePERIODIC 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

The "Full Stroke" ("On line") must be performed to satisfy the PFD_{AVG} (average probability of failure on demand) value.
The described procedure is the one used for the Full Stroke of the ESD assembly witch includes the Volume Booster
The test frequencies will be defined from the final integrator in relation to the defined SIL level to achieve.

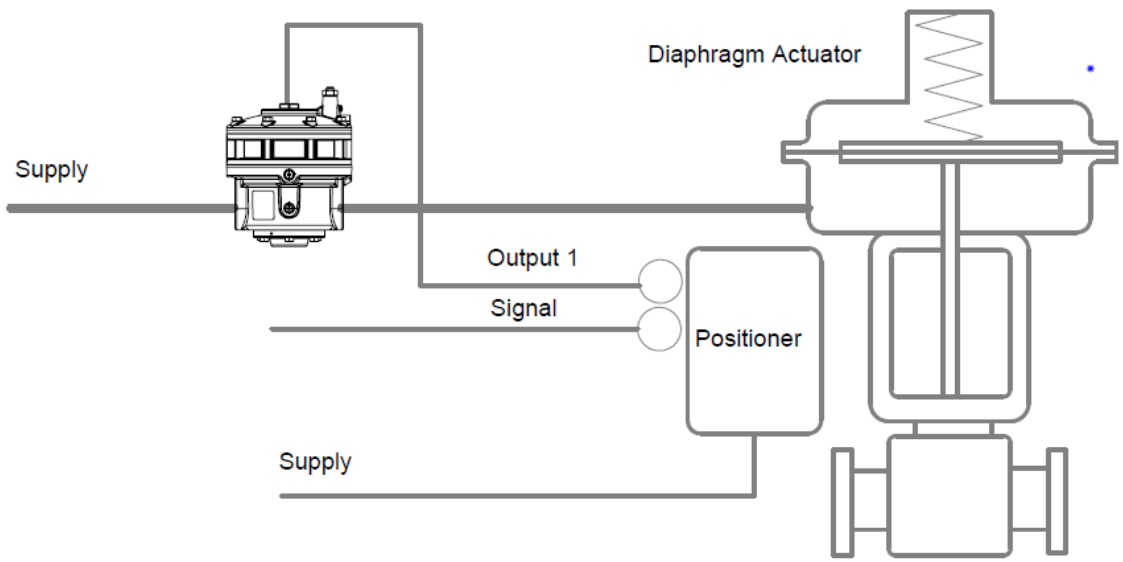
The following parameters can be verified:

- Correct performing of open – close manoeuvre of the ESD assembly;
- Pressure measurement downstream the VB if suitable means are present in the plant.

Procedure for Full Stroke Test

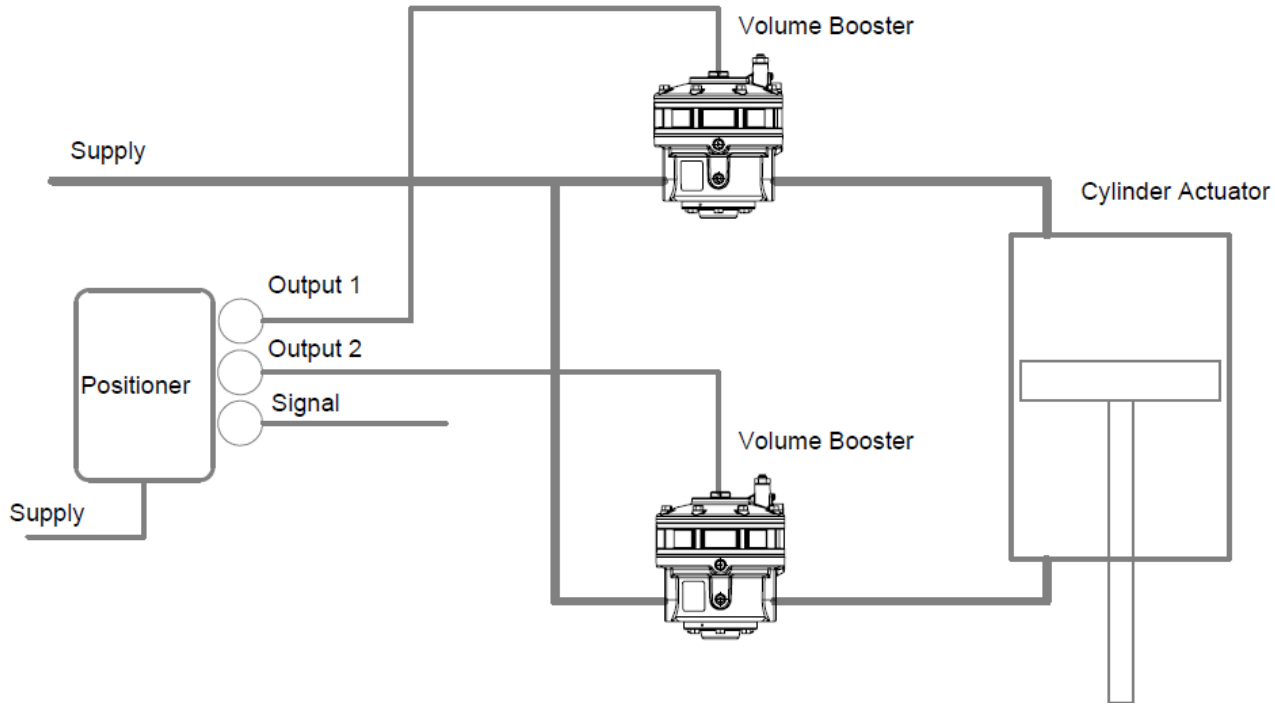
SINGLE ACTING ACTUATOR

1. Move the valve clearly away from the fail-safe position (e.g. set point at 50 % in control valves or to the operating position of on/off valves).
2. De-energize (e.g. 0 bar signal) the inputs at the connected devices (positioner, solenoid valve etc.).
3. Check the effect:
   Does the valve move to the fail-safe position within the required time?



DOUBLE ACTING ACTUATOR

1. Move the valve clearly away from the fail-safe position (e.g. set point at 50 % in control valves or to the operating position of on/off valves).
2. De-energize (e.g. 0 bar signal) the inputs at the connected devices (positioner, solenoid valve etc.) of a Volume Booster.
3. Energize (e.g. increase a pressure signal) the inputs at the connected devices (positioner, solenoid valve etc.) of a second Volume Booster.
4. Check the effect:
   Verify if the valve moving correctly and does the valve move to the fail-safe position within the required time?



Considering the application of the above described Full Stroke Test, the “Test Coverage” can be considered >99%.

6.3 Partial Stroke Test

- The Partial Stroke Test on the ESD assembly results in full stroke on the VB. So a partial stroke test done with manual or automatic procedure with PST device, gives as a result on the VB the same test coverage reached with the Full Stroke Test.

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):
  - DETT application: SFF=82,19%
  - ETT application: SFF=0%
- 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 2 without external diagnostic tests
  - up to SIL 3 considering external diagnostic tests
- double 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)