Technical Report – SIL Assessment

SUBJECT:	***Technical Report – SIL Assessment***
TÜV NORD Italia JOB No.	***PS-20059-20-L-01***

Customer:	**Pneumax S.p.A.**
Manufacturer:	**Pneumax S.p.A.** **Via Archimede 57 – 20129 Milano (MI)**
Type of product:	**Volume booster series SA17, SS17**
Revision detail:	**Rev. 0 Initial release**

Written by: TÜV NORD Italia Inspector

Approved by: TÜV NORD Italia Inspector

Table of contents

I Abbreviations and definitions

Term	Meaning
β, β_D	Beta common cause factor
λ_{BB}	"Black Box" Failure rate – Literature data
λ_D	Failure rate of dangerous failures
λ_{DD}	Failure rate of detected dangerous failures
λ_{DU}	Failure rate of undetected dangerous failures
λ_{NE}	Failure rate of no effect failures
λ_S	Failure rate of safe failures
λ_{SS}	"Steady State" Failure rate – Final value
DC	Diagnostic coverage
FMEDA	Failure modes, effects and diagnostic analysis
HFT	Hardware fault tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year
MRT	Mean repair time
PFD	Probability of failure on demand
PFD_{AVG}	Average probability of failure on demand
PFH	Probability of failure per hour
PST	Partial stroke test
PTC	Proof test coverage
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SLC	Safety lifecycle
SRS	Safety requirements specification
TI	Test interval for proof test (full stroke)
TI_D (TI_{PS})	Test interval for diagnostic test (partial stroke)
Type A	"Non-complex" element (using only discrete components to implement the safety function)
Type B	"Complex" element (using also micro controllers or programmable logic to implement the safety function)

For definitions, standard IEC 61508 (in particular Part 4) applies.

II References

a. Standards

No.	Reference	Title
[N1]	IEC 61508:2010 Part 1–7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
[N2]	IEC 61511-1:2016 + A1:2017 IEC 61511:2016 Part 2–3	Functional Safety – Safety Instrumented Systems for the process industry sector

NOTES:

- [N2] is mentioned only because in Part 1, par. 1, letter c) and related figures 2 and 3, it makes reference to [N1] as reference standard for manufacturers and suppliers of devices.

b. Databases

No.	Reference	Title
[N3]	RiAC NPRD-2016	Non electronic Parts Reliability Data
[N4]	RiAC FMD-97/2013	Failure Modes/Mechanism Distributions
[N5]	NSWC	Handbook of Reliability Prediction Procedures for Mechanical Equipment
[N6]	Exida	Safety Equipment Reliability Handbook
[N7]	OREDA	Offshore Reliability Data

NOTES:

- For databases, where there is no indication of the publishing date it means that the reference is the latest edition.

c. Assessment documents

No.	Reference	Title
Planning		
[D1]	Pneumax document no. P-002-MA Rev. 0	Functional safety management plan
Specification		
[D2]	Pneumax documents no. P-005-P Rev. 0	Safety requirements specification
Design		
[D3]	Pneumax documents no. P-006-P Rev. 0	Safety concept
[D4]	Pneumax Folder	Sectional drawings with component list
[D5]	Pneumax document no. P-007-P Rev. 0	HW systematic failure estimation
[D6]	Pneumax document no. P-007-P Rev. 0	Common cause failure estimation
[D7]	Pneumax documents no. P-010-P Rev. 0	Random failure analysis
Verification and validation		
[D8]	Pneumax document no. P-008-P Rev. 0	Safety validation plan
[D9]	Pneumax document no. P-009-P Rev. 0	Safety validation report
[D10]	Pneumax internal document	Products database
[D11]	Pneumax internal document	Failure database
Manuals		
[D12]	Pneumax document no. TX204006/IST Rev. 0	IOM manual
[D13]	Pneumax document no. P-001-MA Rev. 0	Safety manual

NOTES:

- Specific documents mentioned in [D1]–[D13] (e.g. individual Test Reports referenced in [D9]) are not explicitly mentioned in the above list.

III Summary

This report is related to the assessment according to standards:

IEC 61508-1/7:2010

for the following products:

volume booster series SA17, SS17

1. Introduction

This report is related to the assessment according to standards:

IEC 61508-1/7:2010

for the following products:

volume booster series SA17, SS17

The assessment covers the following aspects:

- Management of Functional Safety / Functional Safety Planning
- Safety Requirements Specification
- Design:
  - Quantifiable aspects:
    - Random Failure Rates, DC, SFF, PFD_{AVG}
    - β Factors
    - MRT
    - PTC
    - Architectural Constraints
  - Non quantifiable aspects:
    - Behaviour of the safety function under fault conditions
    - Safety related SW
    - Systematic failures (Systematic Capability)
    - Behaviour under environmental conditions
- Verification and Validation
- Information for Use
- Modification

The report includes:

- List of reference documents
- Description of the safety function(s)
- Description of the product(s) subject to the assessment
- Assessment procedure
- Assessment of all the above mentioned aspects
- Summary of results

NOTES:

- The results of this report can be used for the assessment of a complete Safety Instrumented System.

2. Safety function(s)

The safety function is defined as follows:

1. *<u>De-energize-to-trip operation</u> (to discharge a chamber of a single acting or double acting pneumatic actuator): when the pressure on the signal port goes to zero, the booster allows the discharge of the cylinder chamber to the exhaust, and the actuator goes towards the safety position.*
2. *<u>Energize-to-trip operation</u> (to charge a chamber of a double acting pneumatic actuator): when the pressure on the signal port goes to the system operating pressure (2,5 barg), the booster allows the air supply to reach the cylinder chamber of the actuator, which goes to the safety position, until the equalisation between the output pressure and the signal pressure, when the three ports (IN, OUT, EXHAUST) are not in communication, and the chamber of the actuator remains pressurised.*

In the following paragraphs, the safety functions are simply mentioned numbered **1** and **2,** meaning**:**
1. De-energize-to-trip operation
2. Energize-to-trip operation

The assessment covers the above safety function(s).

3. Product description

3.1 Scope of certification and exclusions

The products subject to certification are volume boosters series SA17, SS17.

The assessment refers to the volume boosters only.

Detailed information are included in point 3.5 and [D3], [D4], [D12], [D13].

3.2 Architecture

The product has a single channel configuration, HFT=0.

3.3 Classification

The product can be classified as Type A device according to [N1], for use in Low Demand Mode applications.

NOTES:

- The classification refers to the volume booster itself. The classification remains Type A even in case the complete valve-actuator assembly is equipped with a (non-interfering) PST device, according to the definition included in [N1] Part 2, par. 7.4.4.1.2.

3.4 Drawings and parts lists

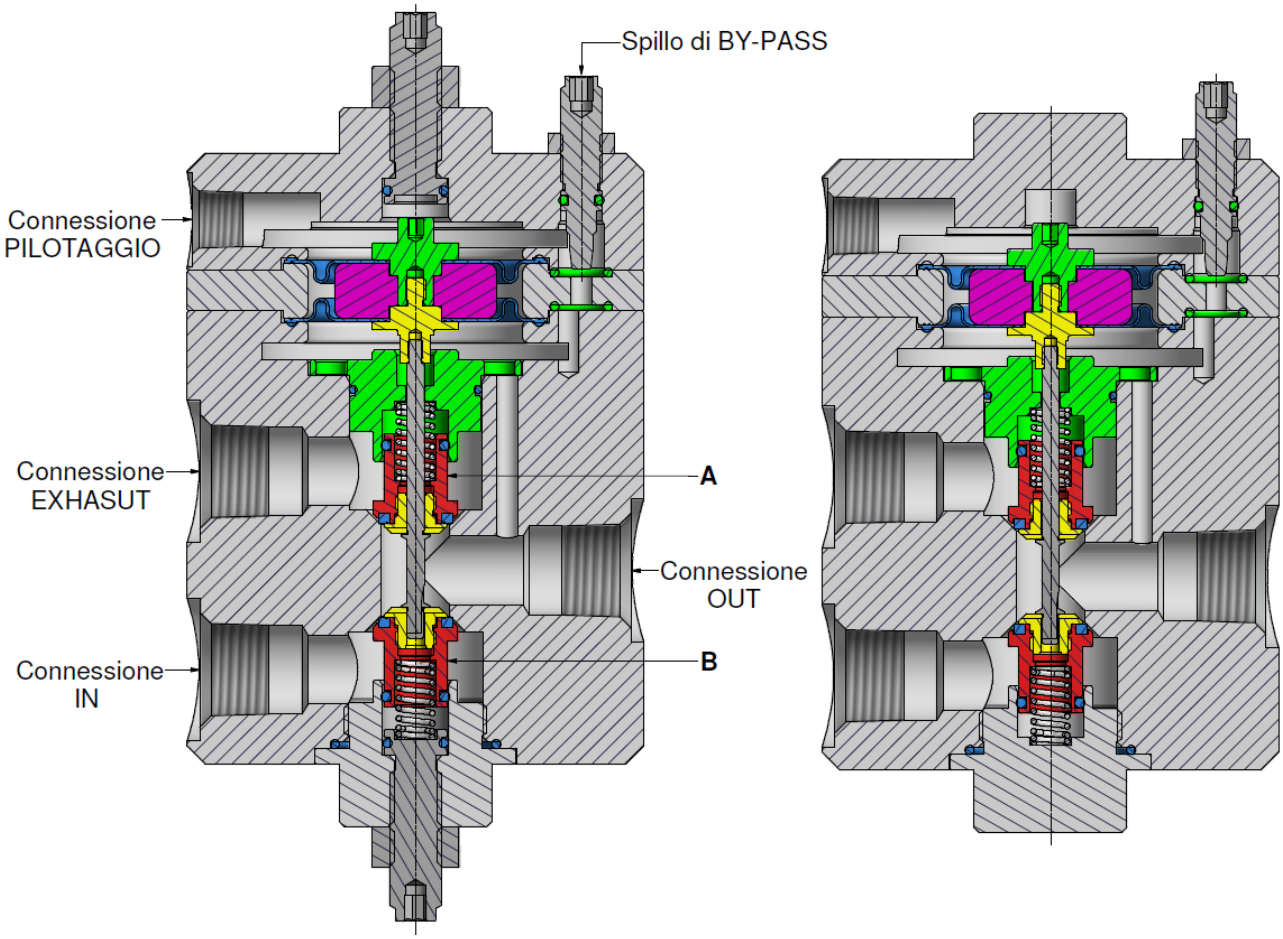
Drawings and parts lists are included in [D4].

3.5 Details of design and functioning

In the oil & gas sector the device is called volume booster or flow amplifier.
The device converts a low flow pressure signal (pilot) into a high flow output signal with a 1:1 ratio between pilot pressure and output pressure. The high volumetric output flow reduces the response and adjustment times of the actuator connected to it.
The device in the basic version is equipped with a bypass pin, which connects the pilot chamber with the outlet chamber. This, in addition to determining the opening times of the main shutter, regulates the sensitivity of the device to changes in the value of the pilot signal.

The product is also supplied in versions with flow regulator in port 1, in port 3 or on both ports. All of the above can be translated into a high flow pilot regulator, with the addition of the bypass pin functionality, and of the flow regulation devices on ports 1 and 3.
The device is pneumatically powered from the IN port. When a pilot pressure signal from 2 to 10 bar is applied on the pilot port, the main valve assembly opens the lower shutter B (IN side) to allow the passage of a high volumetric flow from the inlet port main IN to the OUT port.
When the outlet pressure equals the pilot pressure, the main valve moves to the rest position, (situation in section) and this position is maintained until there is a change in the pilot pressure or in the outlet pressure.
If the system detects that the outlet pressure value is higher than the pilot pressure, the main valve assembly opens the upper shutter A (exhaust side) to release the excess pressure. If the system detects that the outlet pressure is too low, the main valve opens to reload the system at the correct pressure.
The pilot / output pressure ratio is 1:1.

Figure 1: Volume booster principle set-up



Further information is included in [D3] and [D4].

4. Assessment procedure

The basis for the certification is provided by the assessment of the following phases:

1. Management of functional safety / Functional safety planning
2. Safety requirements specification
3. Design:
    a. quantifiable aspects: random failure rates, DC, SFF, PFD_{AVG}; β factors; MRT; PTC; architectural constraints
    b. non-quantifiable aspects: behaviour of the safety function under fault conditions; safety-related software; systematic failures (Systematic Capability); behaviour under environmental conditions
4. Verification and validation
5. Information for use
6. Modification

5. Management of functional safety

5.1 Management of functional safety / Functional safety planning

A functional safety audit of the management systems and of the functional safety planning is conducted to document and highlight that the development of the product under consideration is compliant with [N1].

Assessment result:
The documentation structure and the structure of the functional safety management system are adequately documented.
The audit, interviews and document reviews conducted have shown that the requirements laid down in [N1] with respect to functional safety management are fulfilled, with particular reference to:

- Organisation and responsibilities
- Competence of personnel
- Procedures used and documentation issued for each applicable phase of the SLC
- Techniques/measures used for each phase of the SLC

The following existing Company Quality Certifications have been considered:

- EN ISO 9001:2015

Assessed documents:
[D1] and related documents.

5.2 Safety requirements specification

The SRS [D2] is assessed with respect to its consistency and completeness in a comparison with the applicable requirements of [N1] Part 1, par. 7.10.

Assessment result:
The audit revealed that the SRS completely describes the safety function(s) to be implemented, in terms of functional and safety requirements.

Assessed documents:
[D2].

6. Design

6.1 Quantifiable aspects

6.1.1 Random failure rates, DC, SFF, PFD_{AVG}

6.1.1.1 Procedure

The determination of random failure rates is performed with a Failure Modes, Effects and Diagnostic Analysis (FMEDA), integrated with field feedback (documented in [D11]), according to [N1] Part 2 par. 7.4.4.3.3, using the Bayesian approach.

The procedure used for the determination of random hardware failures is the following:

1. FMEDA of the product, with classification of failure modes
2. Evaluation of λ_{BB} values (literature data)
3. Evaluation of field feedback
4. Integration between literature data and field feedback, using the Bayesian approach
5. Determination of λ_{SS} values (final value)

The FMEDA is based on the documentation (drawings with components lists) provided by the manufacturer, and the other design documentation referenced in par. II, and is documented in [D7].

The FMEDA includes the following information:

Item	**Meaning**
Position	Position of the component on the drawing
Component	Description of the component
Function	Function of the component
Quantity	No. of components which have the same function
Local Architecture	Local redundancy of the component (if any), to perform the specific function
Beta Factor	Parameter used in case of local redundancy
Failure rate	Total failure rate of the single component – Taken from the databases referenced in par. II.
Total failure rate	Total failure rate, considering the values of Quantity and Beta Factor
Failure Mode	Failure Mode taken from the databases referenced in par. II.
Failure Distribution	% of the total failure rate allocated to the specific failure mode
Mode failure rate	Failure rate of the specific failure mode
Effect	Effect of the failure mode on the safety function(s)
SIL Classification	Failure category according to [N1]. See par. 6.1.1.2 for details.
Diagnostics	Diagnostic test (internal or external) able to detect the specific failure mode
DC	Diagnostic Coverage of the identified diagnostic test
λ_S, λ_{DD}, λ_{DU}, λ_{NE}	Failure rate of the failure mode, for the specific failure category

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 [N1]

Furthermore, the requirements in [N1] Part 2, par. 7.4.10.1–7.4.10.7 are assessed and considered fulfilled (as detailed in [D7]), as:

- the product has a restricted and specified functionality and is designed to perform specified safety functions
- the product has an adequate documentary evidence (including extensive operating experience and results of suitability analysis and testing), sufficient to claim the declared failure rates
- the company has an effective system for reporting failures, as above described

6.1.1.2 Description of the failure categories

The following table lists:

- The failure types considered in the assessment
- The failure definition according to [N1]
- For each failure type, examples of failures considered for the specific product

Failure Type	Failure definition according to [N1]	Examples for the specific product
Safe	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a. results in the spurious operation of the safety function; or b. increases the probability of the spurious operation of the safety function	De-energize to trip case: • Structural breakage of mechanical components which can generate spurious trips • Leakage of O-rings which can generate spurious trips Energize to trip case: • None
Dangerous	Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that: a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode); or b. decreases the probability that the safety function operates correctly when required	• Binding / sticking of components involved in the safety function • Breakage of components involved in the safety function
No Effect	Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function	• Superficial score / dent of structural components • Negligible leakage
No Part	Failure of a component that plays no part in implementing the safety function	• Failure of components not involved in the safety function

NOTES:

1. According to definitions 3.6.13 and 3.6.14 of [N1] Part 4, the no part and no effect failures are not used for SFF calculations.
2. According to definitions 3.6.8, 3.6.13, 3.6.14 of [N1] Part 4, the safe, no part and no effect failures do not contribute to PFD_{AVG} calculations.

6.1.1.3 Assumptions

The following assumptions are used for the evaluation of random hardware failures:

- Failure rates are considered constant for the lifetime (20 years, as stated in the Safety Manual [D13])
- Failure rates and failure modes in the FMEDA are taken from databases [N3]–[N7].
- A single component failure fails the entire product, except for redundant configurations. For β values used, see par. 6.1.2.
- Propagation of failures is considered not relevant, unless a clear propagation path is present: in this case, the failure is considered a single failure, with failure rate corresponding to the failure rate of the first failure.
- The components that are not part of the safety function and cannot influence the safety function are excluded from the evaluation.
- After a proof test, the product will be "as new". The PFD_{AVG} is calculated in the hypothesis of perfect proof test performed by trained, skilled and competent personnel. See also the remarks in par. 6.1.1.4.
- The "rate" of systematic failures is controlled and minimised by the management of the safety lifecycle of the system.
- The installation, commissioning, operational and maintenance instruction are correctly applied by the final customer.
- The stress levels considered are average for an industrial environment (ground fixed).

6.1.1.4 Determination of λ values, DC, SFF and PFD_{AVG}

λ values

The total random failure rates – λ values – are calculated from the FMEDA + field feedback.

Assessment result:
The results are included in the following table.

Configuration	Safety function	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_S [1/h]
Volume booster - No PST	1	9,20E-08	0,00E+00	1,65E-07
Volume booster - With PST	1	9,20E-10	9,11E-08	1,65E-07
Volume booster - No PST	2	1,84E-07	0,00E+00	≅0,00E+00
Volume booster - With PST	2	1,84E-09	1,82E-07	≅0,00E+00

NOTES:

- The results in the table are valid for all the configurations listed in par. 3
- For definitions of Safety Functions, see par. 2
- For the reason why λ_S=0, see par. 6.1.1.2
- The λ_S values are not divided in λ_{SD} and λ_{SU}, as this subdivision would have no relevance for any of the SIL parameters

Assessed documents:
[D7] and related documents.

DC

The product does not include internal diagnostics.
Diagnostic is only possible via external means, e.g. with a PST.
The procedure for the external diagnostic tests is described in the Safety Manual [D13].
The effect of an external diagnostic test is considered during the FMEDA, to discriminate between λ_{DD} and λ_{DU}.

Assessment result:
Considering the application of the described PST procedure, for all automatic methods indicated, the test coverage can be considered:

- ≥ 90%

In case of manual procedure, the test coverage shall take into account also the test imperfections and the reliability/competence of the operator.

NOTES:

- It the test is automatic, then the test coverage can also be considered as DC
- If the test is manual, then the test coverage can be considered as PTC, but cannot be considered as DC

Assessed documents:
[D3]–[D7], [D13]

SFF

The formula for SFF is the following:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D}$$

The value of SFF is calculated using the λ values resulting from the FMEDA + field feedback.

Assessment result:

- SFF (without external diagnostic tests):
  - DETT application: SFF≅64%
  - ETT application: SFF≅0%
- SFF (with external diagnostic tests): 99%

Assessed documents:
[D3]–[D7].

PFD_{AVG}

According to [N1], the following formula is used to estimate the PFD_{AVG} value:

$$PFD_{AVG} = \lambda_{DU} \cdot \left(\frac{TI}{2} + MRT\right) + \lambda_{DD} \cdot \left(\frac{TI_D}{2} + MRT\right)$$

As the PFD_{AVG} value depends also on the test intervals and on the PTC and the test coverage of external tests, which are not product-dependant quantities, the PFD_{AVG} values are not product relevant quantities, while λ values are.
Anyway, PFD_{AVG} values are calculated for a certain number of combination of test intervals.

Assessment result:
The results are given in the following tables.

Type: Volume booster - No PST – Safety function: ***1***

Proof test interval (months)				
6	12	24	36	48
2,04E-04	4,05E-04	8,08E-04	1,21E-03	1,61E-03

Type: Volume booster - With PST – Safety function: ***1***

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	3,75E-05	3,95E-05	4,35E-05	4,76E-05	5,16E-05
	2	7,07E-05	7,27E-05	7,68E-05	8,08E-05	8,48E-05
	3	1,04E-04	1,06E-04	1,10E-04	1,14E-04	1,18E-04
	6		2,06E-04	2,10E-04	2,14E-04	2,18E-04
	9				3,14E-04	
	12			4,09E-04	4,13E-04	4,17E-04

Type: Volume booster - No PST – Safety function: ***2***

Proof test interval (months)				
6	12	24	36	48
4,08E-04	8,12E-04	1,62E-03	2,43E-03	3,23E-03

Type: Volume booster - With PST – Safety function: ***2***

		Proof test interval (months)				
		6	12	24	36	48
PST interval (months)	1	7,51E-05	7,91E-05	8,72E-05	9,53E-05	1,03E-04
	2	1,42E-04	1,46E-04	1,54E-04	1,62E-04	1,70E-04
	3	2,08E-04	2,12E-04	2,20E-04	2,28E-04	2,37E-04
	6		4,12E-04	4,20E-04	4,28E-04	4,36E-04
	9				6,28E-04	
	12			8,20E-04	8,28E-04	8,36E-04

NOTES:

- The above values of PFD_{AVG} are calculated for MRT=24 h and proof test coverage=100%. For other values of MRT, TI, TI_{PS} and/or non-perfect proof test, the PFD_{AVG} values must be re-calculated.
- The PFD_{AVG} values including partial stroke test are calculated considering the use of a commercial automatic partial stroking test system: for further details, see the Safety Manual.

The values in the above table are compatible with SIL 3.

Assessed documents:
[D7] and related documents.

6.1.2 *β factors*

The product has a single channel configuration, HFT=0.
The β factors can be used when performing PFD_{AVG} calculations for redundant architectures.

Assessment result:
The evaluation of Common Cause factors, relevant when the product is used in redundant configuration, is performed according to [N1], Part 6.
The result is:

- $\beta=\beta_D=0,05$

NOTES:

- The above value is the value for 1oo2 architecture. The values for other architectures shall be calculated according to [N1] Part 6, Table D.5.
- The above value is calculated in the hypothesis of redundancy without diversity

Assessed documents:
[D6].

6.1.3 *MRT*

The MRT is estimated taking in consideration the failure distribution and the estimated repair time for the main failure modes.

Assessment result:
The MRT is indicated in the following table.

Model / Configuration	MRT [h]
Volume booster	1

NOTE:

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

Assessed documents:
[D13].

6.1.4 *PTC*

The procedure for the Proof Test is described in the Safety Manual [D13].

Assessment result:
Considering the application of the described test procedure, the PTC, in case of automatic procedure, can reach values > 99%. It could be lower considering test procedure imperfections (e.g. non calibrated instrumentation, non-safety software functions used for the test).
In case of manual procedure, the test coverage shall take into account also the test imperfections and the reliability/competence of the operator.

Assessed documents:
[D13].

6.1.5 *Architectural constraints*

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

As the device is classified as "Type A", no requirements for SFF are given for Route 2_H.

Assessment result:

Configuration	Safety Function	Type	HFT	SFF[1]	Route 1_H	Route 2_H	Max. SIL according to architectural constraints
Volume booster - No PST	1	A	0	≅64%	Applied. For a type A element with 60%≤SFF<90%, Route 1_H results in a maximum claimable SIL equal to 2.	Applied. The application of Route 2_H results in a maximum claimable SIL equal to 2.	2
Volume booster - With PST				≥90%	Applied in case of performing of PST and assuming a PST coverage up to ≥90%. For a type A element with SFF≥90%, Route 1_H results in a maximum claimable SIL equal to 3.	Applied. The application of Route 2_H results in a maximum claimable SIL equal to 2.	2 / 3
Volume booster - No PST	2	A	0	≅0%	--	Applied. The application of Route 2_H results in a maximum claimable SIL equal to 2.	2
Volume booster - With PST				≥90%	Applied in case of performing of PST and assuming a PST coverage up to ≥90%. For a type A element with SFF≥90%, Route 1_H results in a maximum claimable SIL equal to 3.	Applied. The application of Route 2_H results in a maximum claimable SIL equal to 2.	2 / 3

The product 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

Assessed documents:
[D3]–[D7].

[1] The performing of PST has been taken into account when evaluating the Safe Failure Fraction.

6.2 Non-quantifiable aspects

6.2.1 Behaviour of the safety function under fault conditions

As written in par. 6.1.1.4, the product does not include internal diagnostics.
Diagnostic is only be possible via external means, e.g. with a PST.

Assessment result:
The behaviour of the safety functions under fault condition is evaluated with the FMEDA, and is described in [D7].
See also paragraph 6.1.1.4 for details.

Assessed documents:
[D3]–[D9], [D13].

6.2.2 Safety-related software

No SW is used to implement the safety function.

6.2.3 Systematic failures (Systematic Capability)

The systematic capability is assessed using Route 1_S, evaluating the application of adequate techniques and measures to control and avoid systematic failures (Tables A.15–A.17 and B.1–B.5 of [N1] Part 2).
Evidence was identified for each technique/method used.

Assessment result:
The techniques and measures used to control and avoid the occurrence of systematic failures are adequate up to a SIL 3 value.
The audit, interviews and document reviews have shown that the requirements laid down in [N1] with respect to systematic failures are fulfilled, with particular reference to:

- Organisational measures: project management, documentation structure, information for use, etc.
- Technical measures: safety design, correct choice of components, test planning and reports, etc.

HW tests and analysis are performed (see [D8]–[D9] and related documents) to assess the functional and integrity requirements. The following analysis and tests are planned and documented:

- Normal functional tests (production tests)
- Extended and worst case analyses and tests
- Failure analysis and tests:
  - Random failure analysis
  - Systematic failure analysis
  - Common cause analysis
  - Fault insertion tests
- Environmental tests

The existing tests have been considered for the assessment.

Assessed documents:
[D5], [D8]–[D9] and related documents.

6.2.4 Behaviour under environmental conditions

The behaviour in environmental conditions is assessed evaluating the results of adequate environmental tests.

Assessment result:
Functional tests in the relevant extreme environmental conditions are performed.
The tests in environmental conditions do not impact the functional safety of the product.

Assessed documents:
[D8]–[D9] and [D12]–[D13].

7. Verification and validation

The verification and validation activities performed by the manufacturer using review, analysis and tests, are assessed.

Assessment result:
After each design phase, a verification activity is performed by the manufacturer to check that the requirements of the specific phase are fulfilled.
The verification and validation activities cover the following:

- Design review
- Design calculations
- Normal functional tests
- Extended and worst case analyses and tests
- Failure analysis and tests
- Environmental tests

Assessed documents:
[D1] and related documents, [D8]–[D9] and related documents.

8. Information for use

The assessment covers:

- the installation, operation and maintenance instructions (IOM Manual)
- the particular instructions required by Annex D of [N1] Part 2 (Safety Manual)

Assessment result:
The relevant instructions for the installation, operation and maintenance of the product are included in the IOM manual [D12].
The Safety Manual [D13] includes all the information required by [N1] Part 2, Annex D.

Assessed documents:
[D12]–[D13].

9. Modification

Procedures for modification activity are described in specific documents, referenced in [D1].

10. Summary of results

The analysis gives the results summarised in the following table.

Configuration	Safety function	λ_{DU} [1/h]	λ_{DD} [1/h]	λ_S [1/h]	Systematic Capability	Max. SIL according to Architectural Constraints
Volume booster - No PST	1	9,20E-08	0,00E+00	1,65E-07	3	2
Volume booster - With PST	1	9,20E-10	9,11E-08	1,65E-07	3	3
Volume booster - No PST	2	1,84E-07	0,00E+00	≅0,00E+00	3	2
Volume booster - With PST	2	1,84E-09	1,82E-07	≅0,00E+00	3	3

NOTES:

- The results in the table are valid for all the configurations listed in par. 3.
- For definitions of Safety Functions, see par. 2
- The λ_S values are not divided in λ_{SD} and λ_{SU}, as this subdivision would have no relevance for any of the SIL parameters
- The product 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
- For further details, make reference to the Safety Manual [D13]

The results of this report can be used for the assessment of a complete Safety Instrumented System.