





Report: Failure Mode Effects Analysis and Systematic Capability Analysis

Company: Pneumax S.p.A. Project: regulators and filter-regulators Steel Line series

	Writers	Approved
Names	M.Cencio	P.Capellini
Document	TC1233/18/PC/mc	
Date	20/12/2018 R0	
Signatures		



Bureau Veritas Italia S.p.A. viale Monza 347, 20126 Milano
Tel. 02 270911 www.bureauveritas.it



Move Forward with Confidence

1. INTRODUCTION.....	3
2. REFERENCES & GLOSSARY	7
3. PRESENTATION OF PNEUMAX PRODUCTS	8
4. METHODOLOGY FOLLOWED BY BUREAU VERITAS.....	9
5. LIFETIME OF COMPONENTS.....	10
6. PROOF TESTS.....	11
7. SYSTEMATIC CAPABILITY ASSESSMENT	12

Record of revisions

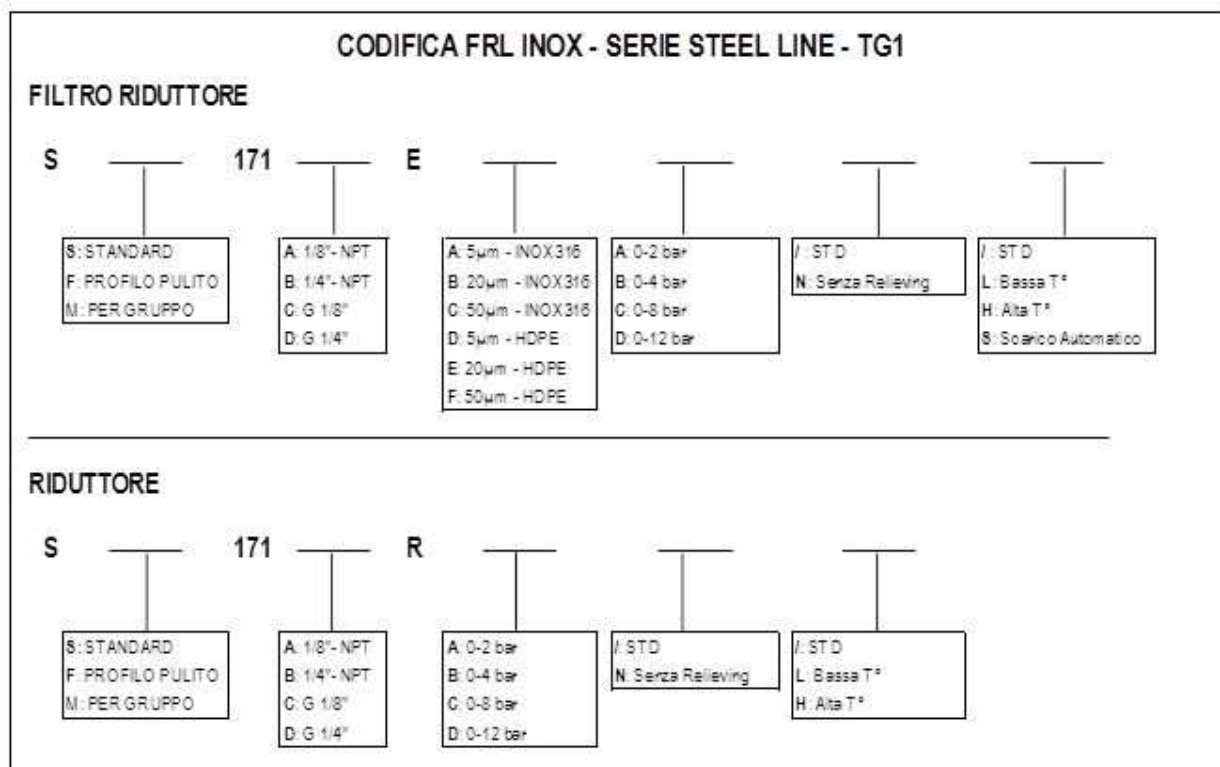
Revision	Date	Description
0	20 Dec. 2018	First release

1. Introduction

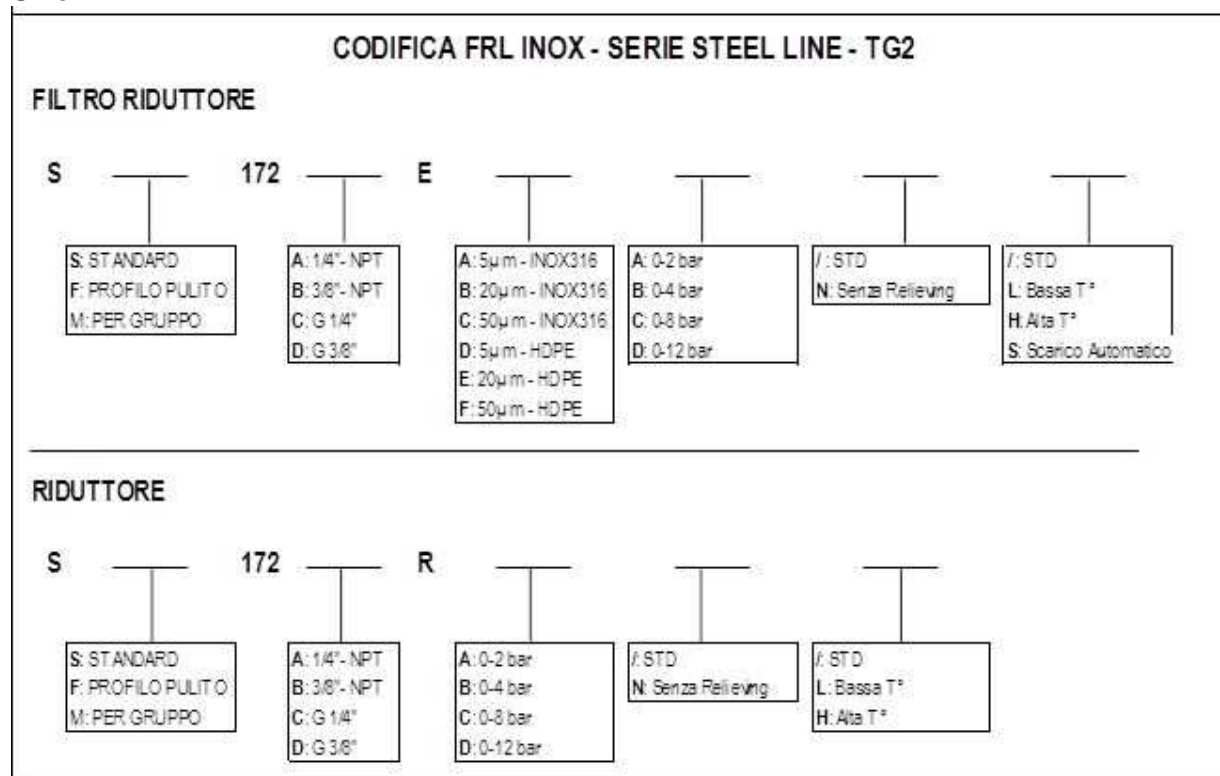
In this report are reported the results of the item assessment carried out to study the achievement of the PNEUMAX pressure reducers and filter-reducers of the performance required to be implemented in a final element of a safety related system projected and built to meet the IEC 61508 and IEC 61511 requirements.

This report concerns only the hardware below described PNEUMAX item listed in the STEEL LINE series treated in this report:

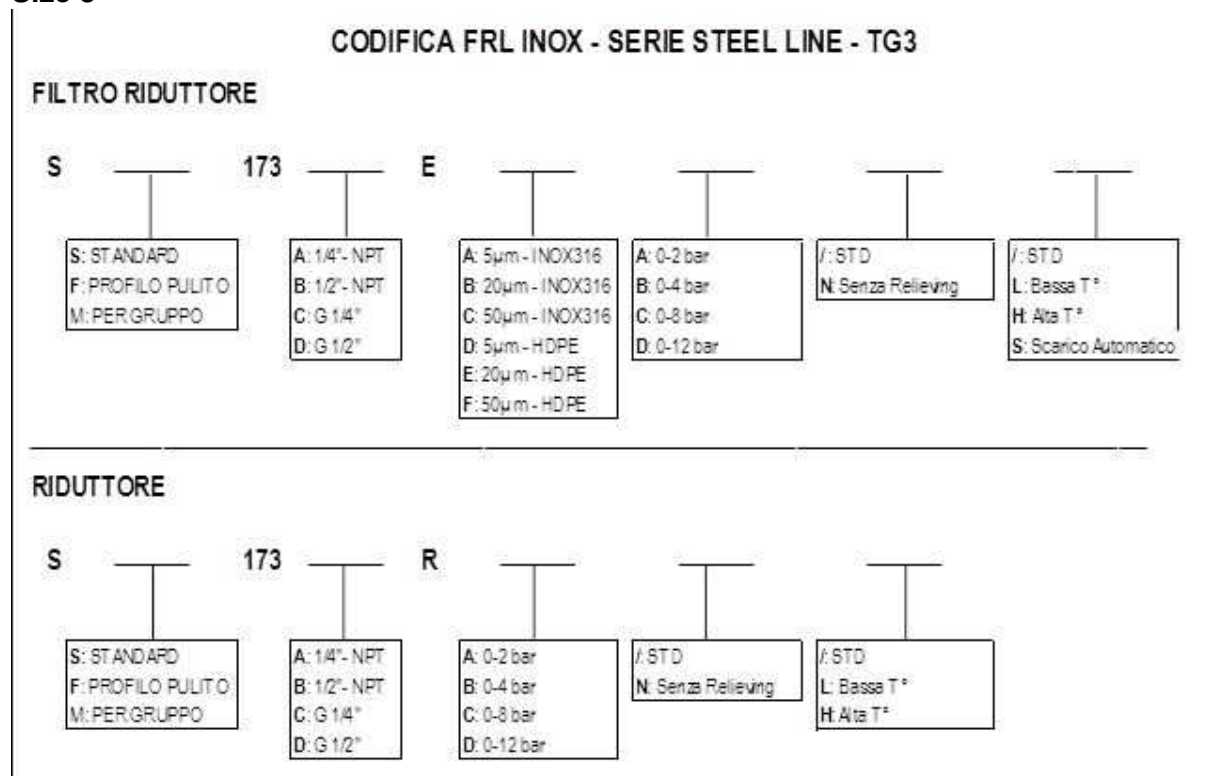
Size 1



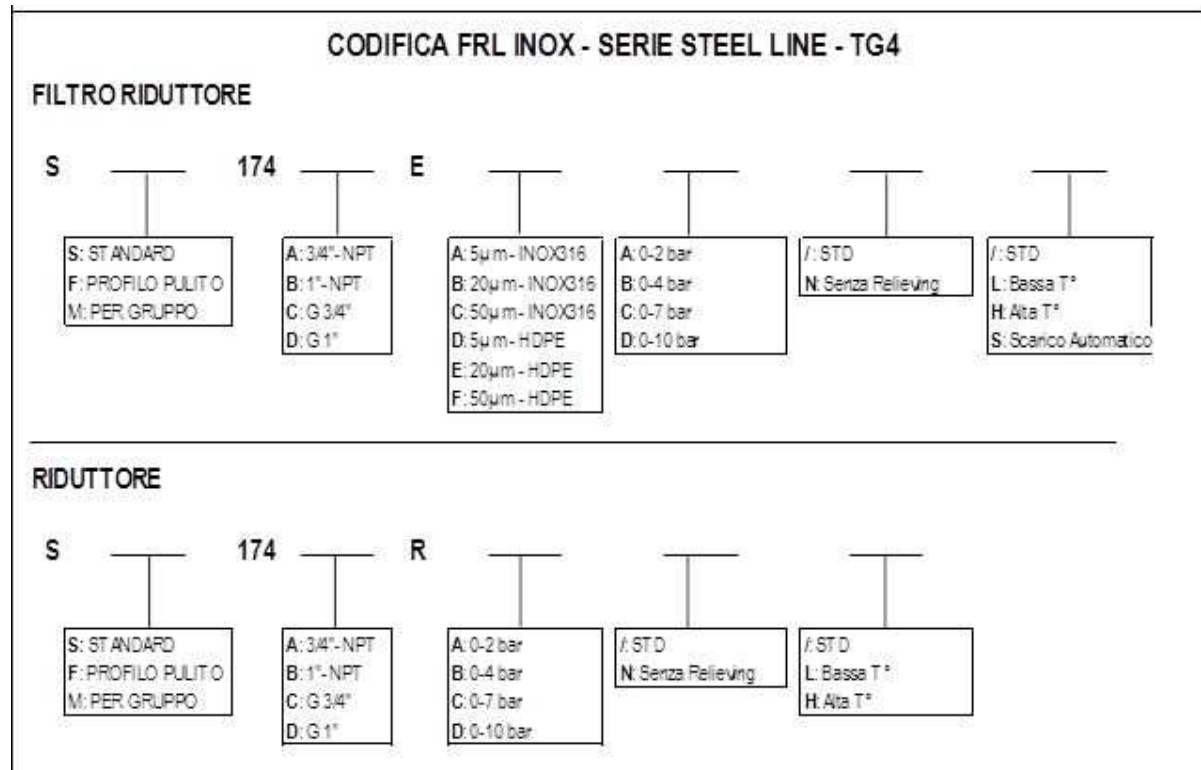
Size 2



Size 3



Size 4



For a full description and features refer to the PNEUMAX data sheet. All the internal and external parts are made up of inox AISI 316L steel as per standard NACE MR0175/ ISO 15156-1.

These elements are classified as Type A element according to IEC 61508, having a hardware fault tolerance of 0. The complete subsystem of which each of these item represents an element, will need to be evaluated to determine the Safe failure fraction.

A user of these equipment can utilize the failure rate reported in this document in a model of a safety instrumented function (SIF) to determine suitability for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

The purpose of this project is a hardware assessment according to IEC 61508. The hardware assessment consists of a FMEDA to determine the fault behaviour and the failure rates of the device, which are then used to calculate the Probability of failure on Demand (PFD) and the Safe failure fraction (SFF).

The information in this report can be used to evaluate whether a final element subsystem meets the average Probability of failure on demand requirements and architectural constraints requirements per IEC 61511 and IEC 61508.

According to manufacturer policy, no reliability tests were performed to confirm consistency with FMEDA outcomes, so the user is encouraged to adjust equipment failure rate for duty.

2. References & Glossary

2.1 Standard References

[1]	EN/IEC 61508 standard: Part 1 – 2nd edition Part 2 – 2nd edition Part 3 – 2nd edition Part 4 – 2nd edition Part 5 – 2nd edition Part 6 – 2nd edition Part 7 – 2nd edition
[2]	EN/IEC 61511 standard: Part 1 – 2nd edition Part 2 – 2nd edition Part 3 – 2nd edition

2.2 Manufacturer References

- [3] Steel Line series catalogue and specification
- [4] TXSS171BEBD drawing for filter-regulator (dated 4/3/2016)
- [5] TXSS171BRD drawing for filter-regulator (dated 4/3/2016)
- [6] TXSS172BEBD drawing for filter-regulator (dated 4/3/2016)
- [7] TXSS172BRD drawing for filter-regulator (dated 4/3/2016)
- [8] TXSS173BEBD drawing for filter-regulator (dated 4/3/2016)
- [9] TXSS173BRD drawing for filter-regulator (dated 4/3/2016)
- [10] TXSS174BEBD drawing for filter-regulator (dated 4/3/2016)
- [11] TXSS175BRD drawing for filter-regulator (dated 4/3/2016)
- [12] ISO 9001-14001-18001 certificate No. CH 10-677 form SQS, valid until 2020-2-11
- [13] Safety manuals for the items
- [14] FMEDA calculations for the Steel Line items doc. No. FMEDA - TSXX17xBxD
- [15] Functional organization chart with SIL manager identification doc. No. V7ROS from Oct. 2017

2.3 Glossary

Acronym	Description
1oo1	1 out of 1 (MooN: M out of N)
1oo2	1 out of 2
DC	Diagnostic Coverage
FMEA	Failure Mode and Effects Analysis
FST	Full Stroke Test
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
PFD	Probability of Failure on Demand
PST	Partial Stroke Test
SIL	Safety Integrity Level
SFF	Safe Failure Fraction
TID	Diagnostic Test Interval
λ	Failure rate
λ_S	Safe Failure rate
λ_D	Dangerous Failure rate
λ_{DD}	Detected Dangerous Failure rate
λ_{DU}	Undetected Dangerous Failure rate
β	Fraction of undetected failures that have a common cause
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause

3. Presentation of PNEUMAX products

3.1 The Manufacturer

PNEUMAX S.p.A, is an Italian Company specialized in the production of pneumatic valves and component for use in manufacturing and oil & gas industries. The manufacturer is ISO 9001 certified company.

3.2 Product description

The items that are studied during this project are those referenced in Clause 1.

4. Methodology followed by Bureau Veritas

4.1 Failure Mode Effects Analysis

The assessment was performed based on the documentation obtained from the manufacturer. In order to assess the failure behaviour of the products the following failure of the devices were considered:

Safety function: each safety function is reported with the failure rates in Clause 4.3

Fail safe state: state according to the safety function.

Fail safe undetected: Failure that is safe and that is not being diagnosed by automatic diagnostics.

Fail Safe Detected: Failure that is safe and is detected by automatic diagnostic

Fail dangerous undetected: failure that is dangerous and is not being diagnosed by automatic diagnostics

Fail dangerous detected: failure that is dangerous but is detected by automatic diagnostics.

The failure that not affect the safety function (as per IEC 61508 Ed. 2) and the external leakage that is not considered part of the safety function are not treated in this assessment.

The methodology adopted is a systematic way to identify and evaluate the effects of different component failure mode, to determine what could eliminate or reduce the probability of failure. This methodology combines the FMEA techniques with the identification of the diagnostic techniques and the failure modes relevant to the safety instrumented system design.

The failure rates used in the assessment are derived from the EXIDA reliability database 2nd edition, which is derived using field failure data from multiple sources.

It is expected that the actual number of field failures due to random events will be less that the number predicted by these failure rates.

For product assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned.

Since the product is newly placed on the marked, PNEUMAX, together with end users, is incited to collect data from the field during the operational life for such equipment, so as to refine the analysis related to the failure rates.

It is assumed also that the equipment is maintained as per the requirements of IEC 61508 and IEC 61511 and a preventive maintenance program is in place. The selection of the equipment shall be done considering the material and technology suitable for the application in all modes of operation.

The user of the data reported in this document is responsible for determining their applicability to any particular environment, considering also eventually particular level of stress of the equipment that may lead to higher level of failures.

4.2 Assumptions

The following assumptions have been made during Failure Mode Effects Analysis:

- A single component failure will lead to the entire element failure
- Failure rate are constant, wear-out are not included
- A single failure at time is considered, a second failure due to the primary failure is considered the same failure
- Component that is not part of the safety function and not influence the safety function are excluded
- Environmental and stress conditions are assumed to be within manufacturer's rating
- Material are compatible with the process conditions
- The device is installed as per manufacturer's instructions (and correct flow direction)
- Partial stroke test not provided.
- The failure modes considered are the solely related to the element structure: failure of power supplies (electrical or pneumatic) have not been considered.

4.3 Results

Using reliability data extracted from the EXIDA 2nd edition database for generic equipment data, with failure rate and modes:

Table 11: **Filter-reducers**

Failure category	Failure rate (1/h)	
	λ_{su}	λ_{du}
Maintain outlet pressure ≤ setpoint	1,99E-07	3,33E-07

Data for calculation have been derived from FMEDA (see [14]).

The SIS designer has to calculate the Safe Failure Fraction that should be calculated for the entire final element combination, while the element is only one part of the subsystem.

The architecture constraint type for these element is A. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required as per IEC 61508 and IEC61511 requirements.

The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

5. Lifetime of components

According to section 7.4.9.5 of IEC 61508-2 the lifetime is important information that describes the operational time interval where the failure rate of the device is currently constant.

Although a constant failure rate is assumed by most probabilistic estimation methods this only applies provided that the useful lifetime of elements is not exceeded. Beyond their useful lifetime the results of most probabilistic calculation are therefore meaningless, as the probability of failure significantly increase with time.

Based on general field failure data a product life period of approximately 20 years is expected for the item treated in this report, if the components are renewed before the end of their useful life and the device is maintained as per manufacturer's instructions.

The assumption of a constant failure rate could be expected for a useful life period of 10 to 15 years or 10000 cycles that are however strongly dependent by the installation conditions that have to take in consideration from the SIS designer.

6. Proof tests

According to section 7.4.5.2 of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostics tests.

This means that it is necessary to specify how dangerous undetected faults can be detected during proof testing.

The main proof test consists of a visual inspection of the filter-reducer, to check whether the main components providing the safety function are affected or not.

The actions could be (proof test suggested):

1. Bypass the element and take appropriate action to avoid a false trip
2. Remove the filter-reducer or the reducer from the line.
3. Dismount the element as per PNEUMAX instructions and inspect for any visible damage or contamination of main parts which provide the safety function (seal on the plunger, plunger, springs, diaphragm, stem, etc...)
4. Re-mount the element if no damages are present.
5. Restore the normal operation

7. Systematic Capability Assessment

7.1 Functional Safety Management

According EN ISO 9001, Pneumax possess a quality management system certified. Registration number CH-10677 issued by SQS on 2017-2-15 and valid until 2020-2-11.

The organizational chart (doc. V7ROS, dd. Oct. 2017) identifies the functional safety manager and its duties.

Planning

Procedures referenced inside the Project Quality Plan fulfil the requirements of IEC 61508 with respect to functional safety management.

Version Control

Design drawings and documents are also under version control.

Training, Competency recording

Personnel training records are kept per standard quality procedures. Pneumax hired BV to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

7.2 Safety Requirements Specification and Architecture Design

As the elements are simple pneumatic devices, there is no need for a separate architecture design phase. The Manufacturer Data Sheet included in the STEEL Line Catalogue and the user and safety manuals will indicate all the necessary provisions to be adopted and observed by the installer/end user.

Items from IEC 61508-2, Table B.1 include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, and inspection of the specification. As the function of the element is simple and clearly defined there is no need for semiformal methods such as functional block diagrams. The application is considered when specifying the requirements; the devices may be required to meet specific applications standards. This meets SIL 3.

7.3 Hardware Design

The hardware design process consists of two distinct phases: concept verification, and design and development. During concept verification all possible solutions are reviewed and the most promising is detailed.

Pneumax utilize CAD's as development tools. Version numbers should be listed and re-qualification should be done when the tool vendor makes revisions. Re-qualification test results should be documented and reviewed.

Items from IEC 61508-2, Table B.2 include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, and computer-aided design tools. This meets SIL 3.

7.4 Manufacturing

The Steel Line items which have been assessed are manufactured in an ISO 9001 certified facility. All units are functionally tested. Field returns are tracked and reviewed regularly to identify quality issues and performance issues. Customer feedback is solicited and reviewed to identify performance issues and opportunities for product improvements. This meets SIL 3.

7.5 Validation

Validation Testing is done via a documented plan, the Qualification Test Plan and includes compliance testing per application standards.

As the Steel Line Series of Item are purely pneumatic devices with a simple safety function, there is no separate integration testing necessary.

Procedures are in place for corrective actions to be taken when tests fail.

Items from IEC 61508-2, Table B.3 include functional testing, project management, documentation, and black-box testing (for the considered devices this is similar to functional testing). This meets SIL 3.

Items from IEC 61508-2, Table B.5 included functional testing and project management, documentation, failure analysis (analysis on products that failed), and expanded functional testing and black-box testing. Interference surge immunity testing is not applicable and fault insertion testing is not feasible for these devices. Instead a detailed FMEDA was performed. This meets SIL 3.

7.6 Modifications

Modifications are done per the related QSM procedures.

All design change requests are reviewed to determine if there is any negative impact on product safety. This review shall be done by both the assigned engineer and the appropriate SIL engineering manager. This meets SIL 3.

7.7 User documentation

Pneumax creates the following user documentation: product catalogue, drawings, and safety manual. Items from IEC 61508-2, Table B.4 include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (element performs well-defined action) and operation only by skilled operators (operators familiar with pneumatic elements, although this is partly the responsibility of the end-user). This meets SIL 3.

7.8 Hardware Assessment

To evaluate the hardware design of the item Series listed in Clause 1, a Failure Modes, Effects, and Diagnostic Analysis was performed by PNEUMAX. This is documented in doc [14], which is part of the item technical. BV reviewed the FMEDA for correctness and completeness.

7.9 Dependability Growth

PNEUMAX is suggested to provide continuous analysis on the equipment failure data (**particularly by means of product standards, e.g. ISO 19973 for B10 determination**) in order to refine the evaluation for the estimation of the target failure measure. The assessor reserves to revise the failure data accordingly, during future planned activities.