TÜV AUSTRIA ITALIA - Blu Solutions s.r.l.

C.F. - P. IVA IT02217380423
Cap. Soc. i.v. EUR 10.000,00
R.I. Ancona REA n. 170070
A socio unico, soggetta a controllo e coordinamento di:
TÜV AUSTRIA HOLDING AG
Deutschstrasse 10,
A-1230, Vienna, Austria

Sede legale:
Via del Commercio, 6/A
60030 Monte Roberto (AN)
T: +39 0731 22781
F: +39 0731 227806
E: info@tuvaustriaitalia.com
tuvaustriaitalia@legalmail.it
W: www.tuvaustriaitalia.com
Codice SdI M5UXCR1

Sede operativa:
Via dell'Industria, 14
25030 Erbusco (BS)
T: +39 030 982 1049
F: +39 030 982 2253
E: info.bs@tuvaustriaitalia.com

Sede operativa:
Via Pasquale Romano, 25
72100 Brindisi (BR)
T: +39 347 597 0825
F: +39 030 982 2253
E: info.br@tuvaustriaitalia.com

TÜV ®

Report no.: TAI-FS-R-20-0087

SIL EVALUATION REPORT

IEC 61508-1/7:2010
IEC 61511-1:2016 + A1:2017
IEC 61511-2/3:2016

Mechanical partial stroke test device

DVG Automation S.p.A.
Via Gabriele Rossetti 2
I-29016 Cortemaggiore (PC)

Date: **2020-12-29**

Author
Carlo Tarantola

Signature

This document is only valid in its entirety, without any change.

INDEX

0 STATUS OF THE DOCUMENT

History: R 00: Initial release Date: 2020-12-29

Release status: Released to client

Author(s): Carlo Tarantola

1 PURPOSE AND SCOPE

This report summarizes the results of an analysis of suitability or use in a SIS for protective application of the DVG Automation mechanical partial stroke test device, and it includes:

- list of reference documents
- general description of the product
- safety function(s)
- procedure used for the analysis of suitability, including:
  - evaluation of the systematic failures, including functional tests
  - evaluation of the random HW failure rates of the product (λ values), including:
    - FMEA
    - Proven in use assessment
  - documentation for the final user
- results

The inspection of the further requirements defined in IEC 61508 and IEC 61511 and applicable product standards are not scope of this job.

NOTES:

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

2 REFERENCE DOCUMENTS

2.1 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

2.2 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.

3 INSPECTION DOCUMENTS

3.1 Documentation provided by the customer

No.	Reference	Title
[D1]	DVG Automation documents no. AAV_PS_1, AAV_PS_2	Schematic drawings
[D2]	DVG Automation document no. SCTD-TA-MPS-01 Rev. 1	Scheda tecnica per tronchetto special per PST meccanico
[D3]	DVG Automation document no. SCTD-CRMPS-01 Rev. 0	Linee guida per la verifica strutturale dei tronchetti per PST meccanico
[D4]	DVG Automation document no. SCTD-TR-MPS-01 Rev. 1	Rapporto di prova relativo a collaudi funzionali di tronchetti di PST meccanico
[D5]	DVG Automation document no. SM-MST-E002 Rev. 03	Service & operating manual

3.2 Documentation prepared by TÜV Austria

No.	Reference	Title
[R1]	20139 – TAI-FS-R-20-0087	FMEDA of DVG Automation mechanical partial stroke test device

4 ABBREVIATIONS, SYMBOLS AND DEFINITIONS

Term	Definition
β, β_D	Beta common cause factor
λ_D	Random hardware failure rate of dangerous failures
λ_{DD}	Random hardware failure rate of detected dangerous failures
λ_{DU}	Random hardware failure rate of undetected dangerous failures
λ_S	Random hardware failure rate of safe failures
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
PST	Partial stroke test
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
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)

NOTES:

- Symbols and abbreviations that can be used in the report are listed in the above table.
- For definitions, standard [N1] (in particular, Part 4) applies.

5 PRODUCT DESCRIPTION

5.1 Scope of assessment

This report is related to the DVG Automation mechanical PST device model “Mechanical Stroke Test Device”.
There are two possible type of stub pipe for mechanical PST, differentiated mainly for the stub pipe operation:

- Closed: characterised by tubular stub pipe to which are welded the two coupling flanges, one with the actuator and the other with the valve. The mechanical PST pivot seat is welded to the main tubular
- Open: characterised by a stub pipe realised with a square-shaped or rectangular section bar where there are the holes for valve and actuator connections. The pivot seat is a separated component

5.2 Functioning principle

The keys connect the sleeves to the actuator.
The pivot, in normal condition, gives the milled part to the sleeves, allowing their complete rotation.
The pivot, in its front part, includes a milled seat to insert the mechanical PST activation key.
To put the system in the mechanical PST state, the operator shall insert the activation key in the pivot seat and rotate it 90° clockwise.
The pressers, entering in the respective seats on the pivot, allow the operator to recognise the two extreme positions of the pivot rotation.

In the closed stub pipe version, the screws, leaning alternatively against the pivot rear part, mechanically limit the pivot excursion preventing the overrun.

In the open stub pipe version, the milling on the pivot rear part leans alternatively against the sides of the milling realised in the end flange: in this way the excursion is mechanically limited preventing the overrun.

Further information is included in [D2].

5.3 Architecture

The product has a 1oo1 architecture.

5.4 Classification

The product can be classified as Type A device according to [N1].
The application is “Low Demand Mode”.

6 SAFETY FUNCTION(S)

The product has not a specific safety function for itself, but it is integrated in an actuator which can be used as an element for Safety Instrumented Systems.

The safety function of the actuator can be defined as follows:

a. *When an unsafe condition is detected in a plant by a process sensor, the controller, via the control panel, drives the actuator to close the quarter-turn valve; or*
b. *When an unsafe condition is detected in a plant by a process sensor, the controller, via the control panel, drives the actuator to open the quarter-turn valve.*

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

The assessment covers the suitability for use of the DVG Automation mechanical partial stroke test device model “Mechanical Stroke Test Device” connected to an actuator used in a Safety Instrumented System for protective application with the above safety function.

7 ASSESSMENT PROCEDURE

The procedure used for the analysis of suitability includes:

- Evaluation of the systematic failures, including functional tests
- Evaluation of the random HW failure rates of the product (λ values), including:
  - FMEA
  - Proven in use assessment
- Assessment of the documentation for the final user

8 EVALUATION OF SYSTEMATIC FAILURES

The evaluation of systematic failures is assessed evaluating the application of adequate techniques and measures to control and avoid systematic failures.
The tables in IEC 61508-2 (for HW) are reproduced and reviewed, in respect to the product subject to assessment, evaluating their level of application.
Evidence is 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.
In particular:

- The general techniques and measures used by DVG Automation to control and avoid the occurrence of systematic failures are assessed, considering the existing SIL certification of DVG Automation actuators
- The avoidance and control of systematic failures via design is assessed (see documents [D1] – [D3])
- HW tests are performed (see document [D4]), to demonstrate the correctness of the design
- The completeness of the information for the final user is assessed (see document [D5])

Assessed documents:
[D1]–[D5] and related documents.

9 RANDOM HARDWARE FAILURE RATES

9.1 Procedure

The determination of random failure rates is performed with a Failure Modes, Effects and Diagnostic Analysis (FMEDA), integrated with field feedback.
The FMEDA is based on the documentation (drawings with components lists) provided by the manufacturer and is documented in [R1].
A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different components failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. A FMEDA is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, no effect) in the safety models.

The estimation is performed following the procedure described below:

1. FMEDA of the product
2. Classification of failures (see the failure categories in subclause 9.3 of the present document)
3. Evaluation of λ values

Furthermore, a “proven-in-use” demonstration of the device is performed, according to IEC 61508-2, parr. 7.4.10.1–7.4.10.7, and the approach of par. 7.4.4.3.3.

9.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis:

- Failure rates are considered constant for the lifetime of the product.
- Failure rates and failure modes are taken from databases [N3]–[N7].
- A single component failure fails the entire product, except for redundant configurations.
- 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.
- Diagnostic methods considered: Partial Stroke Test, Full Stroke Test.
- 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.
- The “rate” of systematic failures is controlled and minimised by the management of the safety lifecycle of the product.
- The installation, commissioning, operational and maintenance instruction are correctly applied by the final customer.
- The stress levels considered are average for an industrial environment (Oil & Gas industry – ground fixed).

9.3 Description of the failure categories

In order to judge the failure behaviour of the subsystem, the following definitions for the failure are considered:

Failure Type	Failure definition according to [N1]
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
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
No Effect	Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function
No Part	Failure of a component that plays no part in implementing 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.

9.4 Determination of numerical values

FMEDA

The FMEDA is performed according to the following procedure:

a. complete definition of the product;
b. identification of all potential items and their failure modes;
c. evaluation of each potential failure mode in terms of end system effect;
d. identification of the failure detection methods and compensating provisions for each failure mode (if possible);
e. association of a Failure Category to each failure mode.
f. association of a Failure Rate / Failure Distribution to each item / Failure Mode.

The complete FMEDA is included in document [R1].

Classification of failures

Each single failure mode was classified, in document [R1], according to the description of the failure categories included in subclause 9.3 of the present document.

9.5 "Proven-in-use" assessment

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, using a checklist compiled by the manufacturer, included in document [R1].
Evidence is identified for each specific point.
The failure rates derived from the FMEDA are integrated with field feedback, using the approach of IEC 61508-2, par. 7.4.4.3.3.

10 INFORMATION FOR USE

The information for use (document [D5]) is examined.
In particular, the following points are assessed:

- Completeness of the document, concerning the correct performing of PST
- Inclusion of the relevant information for the management of the PST, as “”bypass” of the Safety Function (with reference in particular to the requirements of [N2])

Assessment result:

1. The information for use are complete, concerning the correct performing of PST
2. The information for use includes all the relevant information for the management of the PST, as “”bypass” of the Safety Function (with reference in particular to the requirements of [N2]).

The examinations conducted do not reveal any cause for objection in terms of safety.

Assessed documents:
[D5].

11 OVERALL RESULT

The analysis gives the following results.

1. Random failure rates (considering the Safety Function performed by the actuator)[1]:

Safety action	λ_D [1/h]	$\lambda_{DD(PS)}$ [1/h]
Open / Close on demand	1,14E-08	1,02E-08

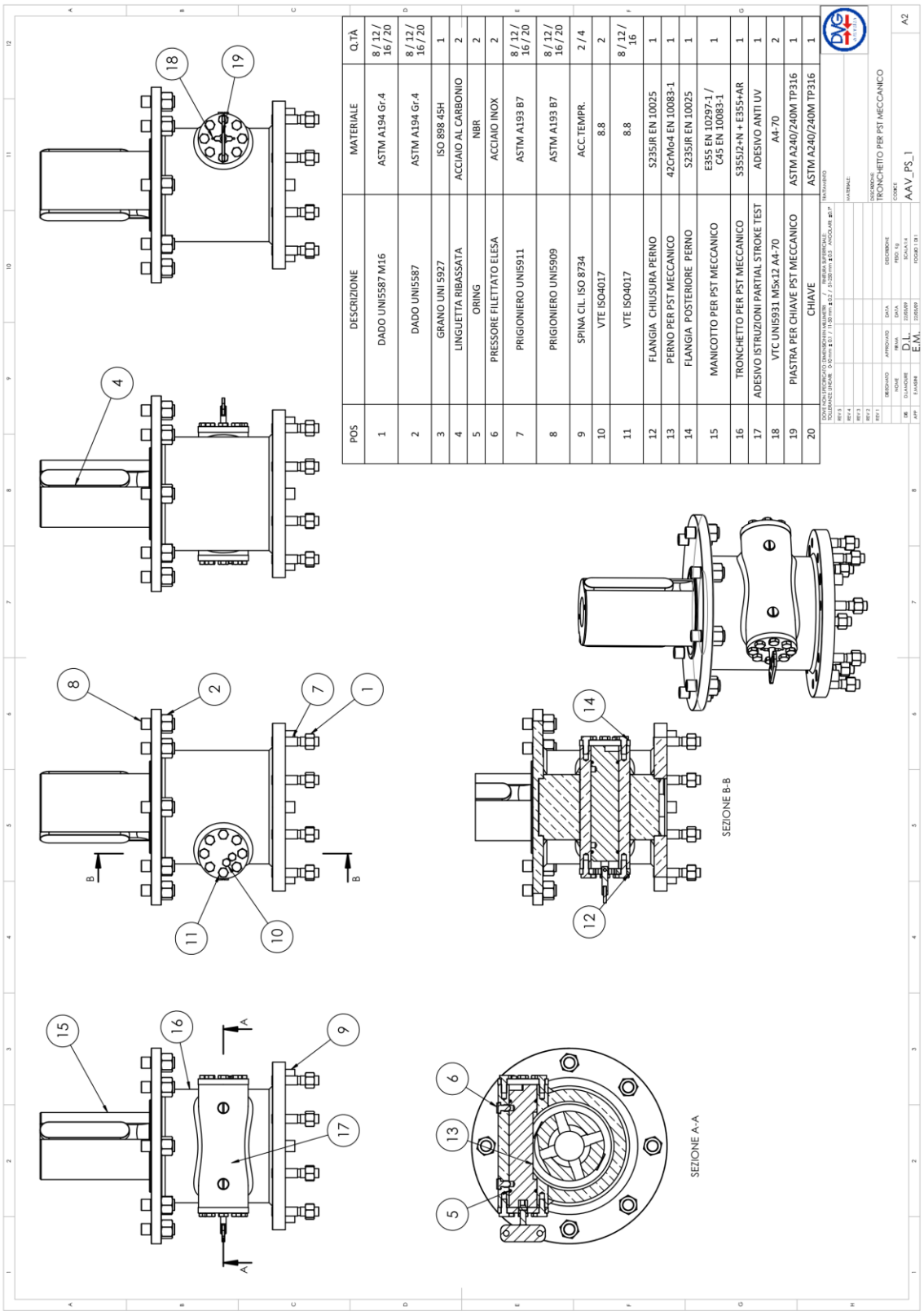
2. Systematic failures
   The techniques and measures used to control and avoid the occurrence of systematic failures are adequate, up to a SIL 3 value.

3. Information for use
   - The information for use are complete, concerning the correct performing of PST
   - The information for use includes all the relevant information for the management of the PST, as “”bypass” of the Safety Function (with reference in particular to the requirements of [N2])

The assessment demonstrates the suitability for use of the DVG Automation mechanical partial stroke test device model “Mechanical Stroke Test Device”, connected to an actuator used in a Safety Instrumented System for protective application up to SIL 3, with the safety function defined in par. 6, when used according to the information for use [D5].

[1] Worst-case results considering the possible configurations of the mechanical PST device.

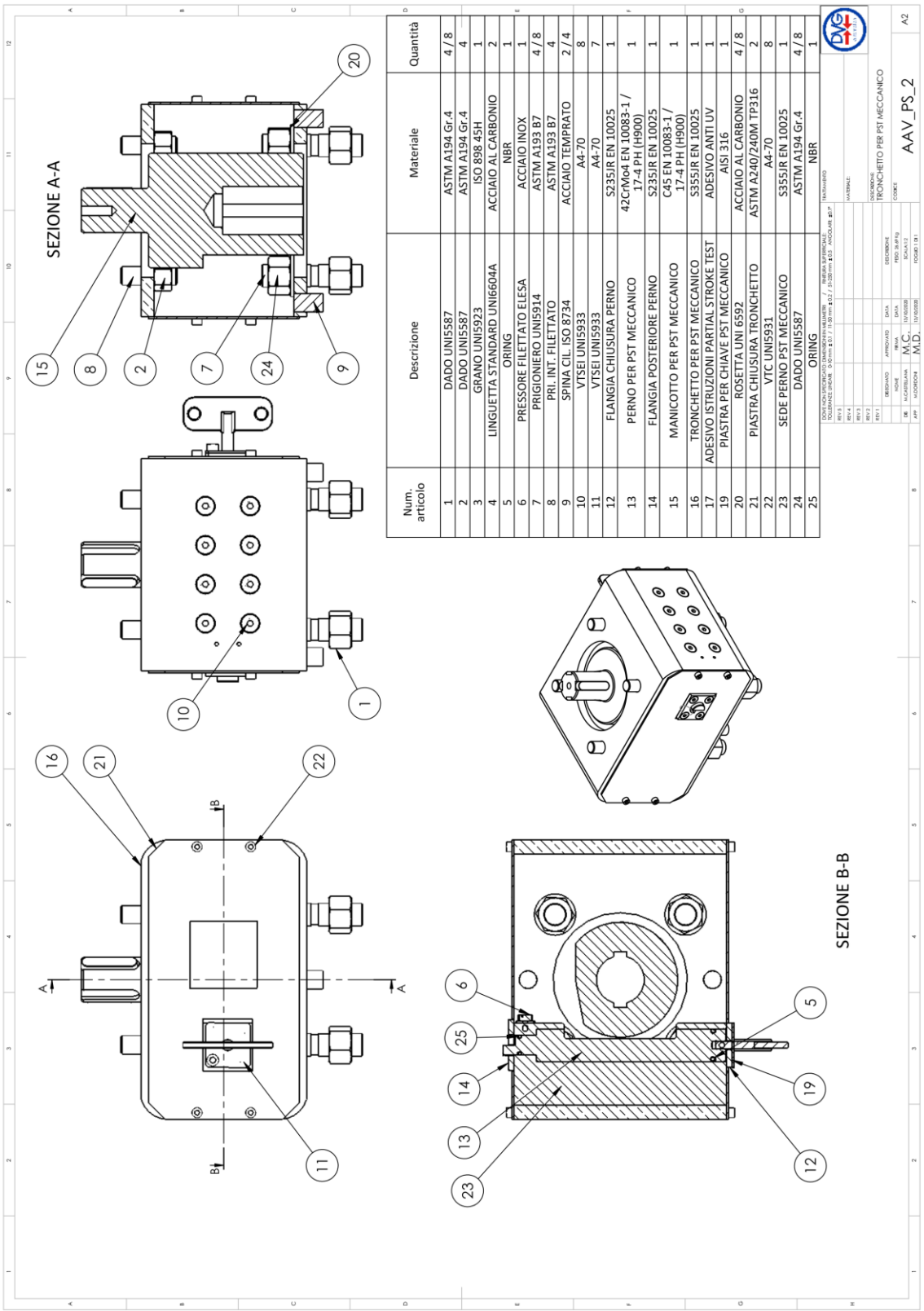
ANNEX A: DRAWINGS, PARTS LISTS



POS	DESCRIZIONE	MATERIALE	Q.TÀ
1	DADO UNI5587 M16	ASTM A194 Gr.4	8 / 12 / 16 / 20
2	DADO UNI5587	ASTM A194 Gr.4	8 / 12 / 16 / 20
3	GRANO UNI 5927	ISO 898 45H	1
4	LINGUETTA RIBASSATA	ACCIAIO AL CARBONIO	2
5	ORING	NBR	2
6	PRESSORE FILETTATO ELESA	ACCIAIO INOX	2
7	PRIGIONIERO UNI5911	ASTM A193 B7	8 / 12 / 16 / 20
8	PRIGIONIERO UNI5909	ASTM A193 B7	8 / 12 / 16 / 20
9	SPINA CIL. ISO 8734	ACC.TEMPR.	2 / 4
10	VTE ISO4017	8.8	2
11	VTE ISO4017	8.8	8 / 12 / 16
12	FLANGIA CHIUSURA PERNO	S235JR EN 10025	1
13	PERNO PER PST MECCANICO	42CrMo4 EN 10083-1	1
14	FLANGIA POSTERIORE PERNO	S235JR EN 10025	1
15	MANICOTTO PER PST MECCANICO	E355 EN 10297-1 / C45 EN 10083-1	1
16	TRONCHETTO PER PST MECCANICO	S355J2+N + E355+AR	1
17	ADESIVO ISTRUZIONI PARTIAL STROKE TEST	ADESIVO ANTI UV	1
18	VTC UNI5931 M5x12 A4-70	A4-70	2
19	PIASTRA PER CHIAVE PST MECCANICO	ASTM A240/240M TP316	1
20	CHIAVE	ASTM A240/240M TP316	1

SEZIONE B-B

SEZIONE A-A



Num. articolo	Descrizione	Materiale	Quantità
1	DADO UNI5587	ASTM A194 Gr.4	4 / 8
2	DADO UNI5587	ASTM A194 Gr.4	4
3	GRANO UNI5923	ISO 898 45H	1
4	LINGUETTA STANDARD UNI6604A	ACCIAIO AL CARBONIO	2
5	ORING	NBR	1
6	PRESSORE FILETTATO ELESA	ACCIAIO INOX	1
7	PRIGIONIERO UNI5914	ASTM A193 B7	4 / 8
8	PRI. INT. FILETTATO	ASTM A193 B7	4
9	SPINA CIL. ISO 8734	ACCIAIO TEMPRATO	2 / 4
10	VTSEI UNI5933	A4-70	8
11	VTSEI UNI5933	A4-70	7
12	FLANGIA CHIUSURA PERNO	S235JR EN 10025	1
13	PERNO PER PST MECCANICO	42CrMo4 EN 10083-1 / 17-4 PH (H900)	1
14	FLANGIA POSTERIORE PERNO	S235JR EN 10025	1
15	MANICOTTO PER PST MECCANICO	C45 EN 10083-1 / 17-4 PH (H900)	1
16	TRONCHETTO PER PST MECCANICO	S355JR EN 10025	1
17	ADESIVO ISTRUZIONI PARTIAL STROKE TEST	ADESIVO ANTI UV	1
19	PIASTRA PER CHIAVE PST MECCANICO	AISI 316	1
20	ROSETTA UNI 6592	ACCIAIO AL CARBONIO	4 / 8
21	PIASTRA CHIUSURA TRONCHETTO	ASTM A240/240M TP316	2
22	VTC UNI5931	A4-70	8
23	SEDE PERNO PST MECCANICO	S355JR EN 10025	1
24	DADO UNI5587	ASTM A194 Gr.4	4 / 8
25	ORING	NBR	1

DESCRIZIONE: TRONCHETTO PER PST MECCANICO
CODICE: AAV_PS_2
A2