ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Italia

COMPLIANCE

with IEC EN 61508

Certificate No.: C – IS – 722163906 Rev.1

CERTIFICATE OWNER: **OMC S.p.A.**
20060 – Cassina de Pecchi (MI) - Italy

WE HEREWITH CONFIRM THAT

VALVES AND ACTUATORS

MEET THE SIL REQUIREMENTS DETAILED IN THE ANNEXED TABLES

FOR THE SAFETY FUNCTIONS:

"Close when required. In case of to Close Safety Function, valve leakage must be within limit values agreed with the Customer" FOR VALVES

and

"Proper valve acting when required" FOR ACTUATORS.

Examination result:	**The above reported valves and actuators were found to meet the standard defined requirements of the safety levels detailed in the following table (T – IS – 722163906) according to IEC EN 61508, under fulfillment of the conditions listed in the Report R-IS-722163906 Rev.1 dated April, 02nd 2018 in its currently valid version, on which this Certificate is based**
Examination parameters:	**Construction/Functional characteristics and reliability and availability parameters of the above valves and actuators**
Official Report No.:	**R-IS-722163906 Rev.1**
Expiry Date	**May, 01st 2021**

IT IS TO BE INTENDED THAT THE ABOVE OFFICIAL REPORT AND ITS ANNEXES ARE AN INTEGRAL PART OF THIS DOCUMENT

Reference Standard **IEC EN 61508:2010 Part 2, 4, 6, 7**

Sesto San Giovanni, August, 03rd 2018

TÜV Italia Srl Industrie Service
TÜV SÜD
Italia

TÜV ITALIA Srl
Industry Service Division
Director

Paolo Marcone

SUMMARY TABLE
T – IS – 722163906

E/EE/EP safety-related system (final element)	**Valves and actuators produced by OMC S.p.A.**		
System type	Type A		
Item	*Two-port valve*	*Three-port valve*	*Actuator*
Systematic Capability	*SC3*		
Safety Function Definition	*Close when required. In case of to Close Safety Function, valve leakage must be within limit values agreed with the Customer*		*Proper valve acting when required*
Max SIL [(1)]	**SIL3**	**SIL3**	**SIL3**
λ_{TOT}	8,232E-08	1,837E-07	2,998E-08
λ_{SD}	5,563E-10	1,241E-09	9,191E-09
λ_{SU}	3,383E-09	7,550E-09	1,015E-08
$\lambda_{DD,PST}$ [(2)]	2,642E-09	5,897E-09	6,578E-09
$\lambda_{DU,FPT}$	9,882E-09	2,206E-08	4,602E-09
β and β_D factor	10%	10%	10%
MTTR	8 h	8 h	8 h
Hardware Safety Integrity	Route 2_H	Route 2_H	Route 2_H
Systematic Safety Integrity	Route 2_S	Route 2_S	Route 2_S

Remarks
(1) The Safety Integrity Level (SIL) of the entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering the redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with the minimum hardware fault tolerance (HFT) requirements.
(2) Considering an automatic Partial Stroke Testing

SIL classification according to Standards IEC EN 61508:2010 (Chapters: 2, 4, 6, 7) for valves and actuators produced by OMC S.p.A.

TÜV Italia Srl Industrie Service
Italia

Italia

Scegli la certezza.

Aggiungi valore.

OFFICIAL REPORT	R – IS – 722163906 REV.1
OMC S.P.A.	

TECHNICAL REPORT FOR SIL CLASSIFICATION ACCORDING TO THE IEC 61508 FOR VALVES AND ACTUATORS PRODUCED BY OMC S.P.A.

Date	TÜV ITALIA Srl	Location
May, 02nd 2018		Sesto San Giovanni
Prepared by		**Approved by**
Industry Service Division Engineer		Industry Service Division Functional Safety Engineer
Francesco Zadra		*Alberto Macchi*

TÜV ITALIA S.R.L.
TÜV SÜD Group

Direzione e Sede Amministrativa:
Via Giosuè Carducci, 125 edificio 23
20099 Sesto San Giovanni (MI)
Sede legale: Via Mauro Macchi, 27 20124 Milano
Società Unipersonale,
soggetta al controllo e al coordinamento di
TÜV SÜD AG

Telefono: +39 02 24130.1
Telefax: +39 02 24130.399

www.tuv.it

Registro delle imprese di Milano
n. iscrizione e Cod. Fisc. 08922920155
R.E.A.: 1255140 - P. IVA 02055510966
Cod. Identificazione CEE IT 02055510966
Capitale sociale : Euro 500.000 int. Vers.

SUMMARY

The aim of the study described in the present document consists in the analysis of the reliability and architectural/functional characteristics of the Two-port and Three-port type Valves and Actuators produced by OMC S.p.A. (from now OMC). The results are summarized in the following table:

Table 1 – SIL classification according to Standards IEC EN 61508 (Chapters: 2, 4, 6, 7) for Valves and Actuators produced by OMC S.p.A.

E/EE/EP safety-related system (final element)	**Valves and Actuators produced by OMC S.p.A.**		
System type	Type A		
Item	*Two-port Valves*	*Three-port Valves*	*Actuators*
Systematic Capability	*SC3*		
Safety Function Definition	*Close when required. In case of to Close Safety Function, valve leakage must be within limit values agreed with the Customer*		*Proper valve acting when required*
Max SIL(1)	**SIL3**	**SIL3**	**SIL3**
λ_{TOT}	8,232E-08	1,837E-07	2,998E-08
λ_{SD}	5,563E-10	1,241E-09	9,191E-09
λ_{SU}	3,383E-09	7,550E-09	1,015E-08
$\lambda_{DD,PST}$(2)	2,642E-09	5,897E-09	6,578E-09
$\lambda_{DU,FPT}$	9,882E-09	2,206E-08	4,062E-09
β and β_D factor	10%	10%	10%
MTTR	8 h	8 h	8 h
Hardware Safety Integrity	Route 2_H	Route 2_H	Route 2_H
Systematic Safety Integrity	Route 2_S	Route 2_S	Route 2_S

Remarks

(1) The Safety Integrity Level (SIL) of the entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering the redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with the minimum hardware fault tolerance (HFT) requirements.

(2) Considering an automatic Partial Stroke Testing

REVISIONS

Revision	Date	Description
0	26/04/2018	Draft
1	02/05/2018	Official

ABBREVIATIONS AND SYMBOLS

CCF	Common Cause Failure
DC	Diagnostic Coverage
DD	Dangerous Detectable
DU	Dangerous Undetectable
DD,PST	Dangerous Detectable by means of Partial Stroke Testing
DU,FPT	Dangerous Undetectable, detectable by means of Full Proof Testing
NE	No Effect
E/E/EP	Electrical, Electronic, Programmable Electronic
FMEDA	Failure Modes Effects and Diagnostic Analysis
FPT	Full Proof Test
PFD	Probability of Failure per Demand
PST	Partial Stroke Test
HFT	Hardware Fault Tolerance
SD	Safe Detectable
SIF	Safety Instrumented Function
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SU	Safe Undetectable

REFERENCES

[1]	International Standard IEC EN 61508:2010 – Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 2, 4, 6, 7
[2]	OREDA 2015 database (SINTEF Norway - Offshore Reliability Data 6th edition)

INDEX

1 INTRODUCTION AND AIM OF THE STUDY

The aim of the study described in the present document consists of the analysis of the reliability and architectural/functional characteristics of Valves and Actuators produced by OMC, in order to:

- perform an accurate assessment of the maximum applicable SIL, according to Standard IEC 61508:2010 (Chapters: 2, 4, 6, 7) [1],
- support the related *Compliance Report to IEC EN 61508* (named C-IS-722163906*)* issued by TÜV Italia.

It is worth noticing that the Standards IEC EN 61508 foresees a methodological approach at level of complete Safety Life Cycle for the design, development, commissioning, operation & maintenance, and decommissioning of complete Safety Instrumented Systems (SISs) of E/E/EP type. In this perspective, it is important to remark that the present study:

- is restricted, in terms of battery limits, to a single and elementary component (a Valve and an Actuator), anyway suitable for use as a Final Element in a Safety Instrumented System of E/E/EP type;
- is limited, in terms of phase of assessment, to the phase of validation of the maximum level of claimable SIL downstream the completion of the related design step (included as part of Phase 10 of IEC EN 61508).

In the following Table 2, the main data about the company OMC S.p.A. are showed:

Company	OMC S.p.A.
Site	Via Galileo Galilei 18 20060, Cassina de Pecchi (MI) Italy
Web Site	http://www.omcvalves.com
Certifications	The Company has a Quality Management System according to the requirements of ISO 9001-2008.Test facilities are available in house and non-destructive testing is performed.
Reliability field data collection	The Company applies a recording of claims of failures from field returns compliant with ISO 9001, through completion of dedicated non-conformity reports.

Table 2 - Main information about OMC S.p.A.

The analysis has been referred and restricted to the following specific typologies of components:

- Two-port Valves (series Air-D, VL10, VD10, KD10, KD20, KD30, RD10, KA10, KA20, KA30, RA10);
- Three-port Valves (series TD10, TM10 AD10, AM10);

- Actuators (series AP23, AP28, AP29, AP34, AP35, AP36, AP37, AP43, AP44, AP45, AP46, AP47, AP48, AP60, AP61, AL23, AL28, AL29, AL34, AL35, AL36, AL37, AL43, AL44, AL45, AR085, AR100, AR120, AR150, AR205, AR265).

The document is structured according to the following sections:

Chapter 2 Review of the requirements concerning the probabilistic and architectural/functional aspects reported in the Standard IEC EN 61508:2010

Chapter 3 Description of the systems object of the analysis and of the safety function which is evaluated for SIL

Chapter 4 Description of all steps of the analysis necessary for the evaluation of the reliability and architectural/functional parameters to classify the SIL

Chapter 5 Summary of the results with compliance declaration.

2 IEC 61508 PROBABILISTIC AND ARCHITECTURAL REQUIREMENTS

The Standard IEC EN 61508 [1] reports a standard procedure of assessment and analysis aimed to verify and classify the safety features of E/E/EP systems (Electrical, Electronic and Programmable Electronic), introducing the SIL concept (Safety Integrity Level).

It is essential to underline that the SIL concept, according to Standard IEC EN 61508:2010, is not strictly and solely related to the system/sub-system/component, but to a specific Safety Instrumented Function (SIF) that the system/sub-system/component carries out.

The evaluation of the highest SIL that can be assigned to a system/sub-system/component, takes place throughout an accurate examination of the complete and correct compliance with both hardware safety integrity requirements and systematic safety integrity requirements.

2.1 Hardware safety integrity requirements

The Standard IEC 61508:2010 establishes for safety systems the hardware safety integrity requirements comprising the following:

- architectural constraints on hardware safety integrity,
- requirements for quantifying the effect of random failures.

2.1.1 Architectural constraints

The highest safety integrity level that can be claimed for a safety function is limited by the hardware safety integrity constraints which shall be achieved by implementing one of two possible routes:

- Route 1_H based on hardware fault tolerance and safe failure fraction concepts;
- **Route 2_H based on component reliability data from feedback from end users, increased confidence levels and hardware fault tolerance for specified safety integrity levels.**

2.1.2 Random hardware failure requirements

For each safety function, a reliability prediction has to be performed using the appropriate techniques. The results shall be compared to the target failure measure.

The following aspects have to be considered in the analysis:

- The architecture
- The failure rates
- The common cause failures
- The diagnostic coverage of the diagnostic test,
- The proof tests interval and coverage,
- The repair time for detected failures,
- The effect of random human error,
- The modelling methods used.

2.2 Systematic safety integrity requirements

The Standard IEC 61508:2010 establishes for safety systems the systematic safety integrity or systematic capability requirements which determines the potential for systematic faults of that element to lead to a failure of the safety function.

The requirements for systematic safety integrity can be met by achieving one of the following compliance routes:

Route 1_S: compliance with the requirements for the avoidance of systematic faults and the requirements for the control of systematic faults, or

Route 2_S: compliance with the requirements for evidence that the equipment is proven in use, or

Route 3_S (pre-existing software elements only): compliance with the requirements of IEC 61508-3, 7.4.2.12.

OMC provided the analysis of systematic failures for Valves and Actuators according to the tables t A15-A17 and B1-B5 of the Standard IEC 61508-2, attesting a Systematic Capability SC3 (see annex 6).

2.3 Probabilistic requirements

The Standard IEC EN 61508:2010 establishes for safety systems the probabilistic requirements reported in the following table in order to classify the highest applicable SIL levels.

Table 3 - Safety Integrity Level: categories of probabilistic targets for E/E/PE safety systems operating either in "low demand mode" or "high demand or continuous mode"

SAFETY INTEGRITY LEVEL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

A safety system (or sub-system or component) is classified by the Standard IEC 61508 as:

- "*low demand mode"* type, when the expected intervention frequency is not higher than one operation per year, or anyway, not higher than the frequency of the inspection/proof tests foreseen for the system.
- "*high demand or continuous mode of operation*" type, when the operation mode is either continuous or discontinuous with expected frequencies higher than those characterising the prior category.

2.4 Architectural/functional requirements

In order to support an effective design process of a safety system, the Standard IEC EN 61508 merges the above mentioned probabilistic requirements with the architectural/functional constrains, in order to consistently take into account the complexity level of the system too.

According to this approach (route 2_H), a correct hardware safety integrity can be achieved as a function the "Hardware Fault Tolerance".

A system characterised by a Hardware Fault Tolerance equal to N means that N+1 contemporary failures must occur to trigger the loss of the safety function: therefore it is a parameter able to take into account the redundancy levels characterising the system under examination. By determining such parameter, any other measures that could prevent or mitigate the failure effect/effects must not be considered (i.e. diagnostics).

The Standard IEC EN 61508 moreover considers two system/sub-system categories: type A and type B.

A system/sub-system can be regarded as type A, whether the following requirements are fulfilled:

a. all failure modes of all equipping components are well known;

b. the behaviour of the system under faulty condition can be fully and comprehensively determined;

c. there is a sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failure are met.

The subsystem is regarded as type B if not all of the criteria listed above are met. Typical examples of type A devices are switch, solenoids, and relays. Type B devices are microprocessor based or devices with complex custom logic.

2.5 Additional discussion about the concept of "detection" and related issues

Concerning the concept of "*detection*" and related issues, the following discussion can be made on the basis of the several, distributed and often not completely aligned definitions along the standard of reference:

- the Standard IEC EN 61508-4 (section 3.8.8) defines as "*detected*" any failure that can be revealed *"by diagnostic tests, but also proof tests, operator intervention (for example physical inspection and manual tests) or through normal operation*";
- no specific definition of "*diagnostic test*" is clearly reported in the standards, but it can be derived by definitions of "*diagnostic coverage*" (IEC 61508-4, section 3.8.6) and "*diagnostic test interval*" (IEC 61508-4, section 3.8.7): these definitions seems to lead to the definition of "*diagnostic test*" as an automated and online test, performed within time intervals at least a magnitude less than the expected demand rate of the SIF of interest;
- the definition of "*proof test*" can be retrieved in IEC EN 61508-4 (section 3.8.5), where it can be read that it is "*a periodic test performed to detect failures in a safety-related systems so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition*". In the same definition it is also underlined that "*for the full proof test to be effective, it will be necessary to detect 100% of all dangerous failures*".

On the basis of the previous statements and definitions taken from the reference Standard, the following methodological approach can be defined concerning the consideration of "*detection*" capability and related parameters:

- Diagnostic tests and all types of periodical proof test, able to relieve dangerous undetected failures, must be taken into account (together with related time intervals) in the determination of the PFD for the SIF under examination (see next sections for analytical details).

3 SYSTEM DESCRIPTION

3.1 Valves and Actuators

General specifications of the models of Valves and Actuators produced by OMC are reported in the following tables.

Table 4 – General description of Valves produced by OMC

Series	Description	Flange type
Air-D	Globe two-port	EN (DIN-UNI…)
VL10	Globe two-port	EN (DIN-UNI…)
VD10	Globe two-port	EN (DIN-UNI…)
KD10	Globe two-port	EN (DIN-UNI…)
KD20	Globe two-port	EN (DIN-UNI…)
KD30	Globe two-port	EN (DIN-UNI…)
RD10	Globe two-port	EN (DIN-UNI…)
TD10	Three-port deviating	EN (DIN-UNI…)
TM10	Three-port mixing	EN (DIN-UNI…)
KA10	Globe two-port	ANSI
KA20	Globe two-port	ANSI
KA30	Globe two-port	ANSI
RA10	Globe two-port	ANSI
AD10	Three-port deviating	ANSI
AM10	Three-port mixing	ANSI

Table 5 – General description of Actuators produced by OMC

Series	Description
AP23	Integral yoke actuator
AP28	Integral yoke actuator
AP29	Integral yoke actuator
AP34	Integral yoke actuator
AP35	Integral yoke actuator
AP36	Integral yoke actuator
AP37	Integral yoke actuator
AP43	Integral yoke actuator
AP44	Integral yoke actuator

AP45	Integral yoke actuator
AP46	Integral yoke actuator
AP47	Integral yoke actuator
AP48	Integral yoke actuator
AP60	Integral yoke actuator
AP61	Integral yoke actuator
AL23	Pillar yoke actuator
AL28	Pillar yoke actuator
AL29	Pillar yoke actuator
AL34	Pillar yoke actuator
AL35	Pillar yoke actuator
AL36	Pillar yoke actuator
AL37	Pillar yoke actuator
AL43	Pillar yoke actuator
AL44	Pillar yoke actuator
AL45	Pillar yoke actuator
AR085	Quick change actuator
AR100	Quick change actuator
AR120	Quick change actuator
AR150	Quick change actuator
AR205	Quick change actuator
AR265	Quick change actuator

3.2 Specific safety function subjected to SIL classification

The safety function for the Valves indicated in the previous paragraph, for which the SIL classification according to Standard IEC EN 61508:2010 has been carried out in the present study, is defined as follows:

"Close when required. In case of to Close Safety Function, valve leakage must be within limit values agreed with the Customer".

While, for the Actuators:

"Proper valve acting when required".

In order to correctly comprehend such safety function, some considerations must be pointed out:

- the battery limits considered in the analysis are the ones determined by components of typologies of the actuators considered in the analysis, as reported in the attached technical documentation and mentioned in the previous § 3.1;
- the defined safety function complies with the battery limits defined in the previous point. The SIL classification has been focused on the switching on demand (open to closed) of the valves and on the acting of the proper valve when required for the actuator, regardless to the higher level effects that the switching can involve in the complex system enclosing the Valve or the Actuator itself, whose design characteristics are outside the scope of the present study;
- since installation and use modes of Valves and Actuators in the complex systems cannot be known in advance, but considering the above mentioned function as strictly associated to emergency/safety interventions inside the overall plant with very low expected frequencies, the analysis has referred to a "low demand mode" of operation;
- the analysis has considered the pneumatic and/or mechanical failure modes able to prevent the correct and complete switching of Valves and Actuators: therefore any failure cause lying outside the battery limits of the Valves and Actuators has not been considered (for example, air supply to pressurise/release the pistons has been considered as always correctly available).

Boundary limits of a system for SIL classification scope represent the interface between the item to be considered and its surroundings. Safety Functions shall be defined within these boundary selections. See following figure to identify the boundary limits considered for the scope. Valves and Actuators have been considered as single devices (1oo1).

4 ANALYSIS OF THE SYSTEM ACCORDING TO THE STANDARD IEC EN 61508

4.1 Estimation of reliability data

IEC EN 61508-2 indicates that input reliability data can be estimated either using component failure data from a recognised industry source or (preferable) from experience of the previous use of the subsystem in a similar environment. In particular, reliability data have to be characterised by a single-sided lower confidence limit of at least 90% (see IEC EN 61508-2, sections 7.4.7.4÷9).

In order to evaluate the basic reliability parameters, statistical evaluations have been performed in the study, on the basis of the approaches suggested by one of the most important reliability database in the oil and petrochemical field, that is OREDA [2].

OREDA foresees two methods for the simplified statistical treatment of data coming from field use and from functional/fatigue tests: statistical approach for cases without failure occurrence and statistical approach for cases with failure occurrence. They are based on a statistical analysis approach based on the χ^2 distribution, also mentioned and suggested by EN 61511-2 (section 11.9.2, last paragraph).

It is important to remark how both methodologies are based upon the assumption that the examined components lie in the useful period of the their life cycle and, therefore, their relevant failure rates can be considered as not-time depending and failures characterised by an exponential distribution.

According to TÜV procedure, as reported in the following §§ 4.1.1 and 4.1.2, with the aim to evaluate the reliability data of the Valves and Actuators, both data provided by the functional/fatigue tests performed by OMC and data obtained by the field experience concerning the population of Valves and Actuators produced and traded by OMC in the period from 2007 to 2017, have been employed.

Concerning the probabilistic analysis section, the exigency by TÜV of treating both data from the field and functional/fatigue tests is motivated by the following two considerations:

- data from the field are considered the primary source of data, as they can supply a very high statistical sample in terms of systems and related operational application and, above all, they are representative of components used in real environmental and operational conditions: due to the considerable economic value of the Valves and Actuators object of the analysis and thanks to the warranty and quality policy adopted by OMC, it can be stated with good confidence that, in general, any failure affecting the Valve and Actuator functionality is claimed by the final Clients.
- the functional/fatigue tests are considered as a fundamental and complementary set of statistical data, as they can supply a very high statistical sample in terms of cycles of application of the Safety Function even if, being performed within a controlled and protected environment, they could not be completely representative of the environmental conditions in which the Valves and Actuators object of the analysis will actually work (i.e. external pipeline, extreme environmental conditions, etc.). In addition, it can be stated that Valves and Actuators in their actual low demand safety application will definitely perform a number of operation during their lifecycle that is widely lower in comparison with the amount of cycles that are performed during a Functional Fatigue test.

Following the previous considerations, the statistical treatment of both sources of data is essential and mandatory, being anyway the first source of data the reference for the estimation of Failure Rates and PFDs at the basis of max claimable SIL classification. The second source of data is used only to confirm (if possible) the highest level of SIL reached by means of the field data: in fact, although functional/fatigue tests can provide a large statistical basis in terms of number of cycles, usually they are performed on a

very small number of components, that cannot be considered completely representative of the whole population under analysis and cannot represent an adequate statistical sample.

4.1.1 Failure rate and PFD estimation by means of functional/fatigue tests

A Two-port Valve and an Actuator have been subjected to functional/fatigue tests.

The complete functional/fatigue tests reports, that also include data about tests, are reported in Annex 2. Although the functional/fatigue tests don't cover the whole range of different versions of Valves and Actuators, the variety of typologies and especially the high number of cycles can be assumed as an adequate sample in order to statistically represent the whole family of Valves and Actuators.

In addition, due to the wide variety of possible solutions, with reference to the foreseen Valves and Actuators, Two-port Valve and an Actuator have been assumed as representative of the whole families.

- Valve DN50,
- Actuator AP28RD.

This approach can be considered reasonably acceptable due to the high fraction of Valves and Actuators commercialised with this configuration and to the approach of analysis highly conservative in terms of probabilistic assumptions.

Each test consists of a wide amount of pressurisation and release cycles (open to closed & closed to open), with the control of the structural, mechanical and torque wrench of the Valves and Actuators under examination.

Such tests, consisting of actuations on demand, have represented the basis for the estimation of a representative value of PFD concerning the families, to be compared with the values reported in Table 3 referred to the "low demand mode of operation".

As indicated in the functional/fatigue tests report in Annex 2, tests did not outcome any functional anomaly. The statistical method has been therefore applied for cases without failures occurrence exposed in previous paragraphs, in order to estimate the representative values of PFD.

In the following Table 6, on the basis of the functional/fatigue tests performed for the different categories of Valves and Actuators, the number of samples and the amount of cycles, PFD values provided by the methodological approach have been reported.

Table 6 – PFD for a Two-port Valve and an Actuator resulting from functional/fatigue tests

Item	n. cycles	Confidence %	PFD_{inf}	PFD_{mean}	PFD_{sup}
Two-port Valve DN50	1800	90	7,282E-07	1,852E-04	7,114E-04
Actuator AP28RD	1800	90	7,282E-07	1,852E-04	7,114E-04

As it can be seen in the table above reported, the representative value of PFD for the Valves and Actuators have been characterised by the following conservative hypotheses:

- the uncertainty range of the failure rate representative for each size class has been evaluated with reference to a confidence level conservatively equal to 90%;

- within the uncertainty range for each selected type of Valves and Actuators, the PFD value corresponding to the 95-th percentile (PFD_{UP}), that is to say the worst one in probabilistic terms, has been considered.

The estimated PFD for the Valves and Actuators, with reference to the "low demand mode of operation" from a strictly probabilistic point of view, could be adequate to support a classification for the safety function up to the SIL 3 category.

4.1.2 Failure rate and PFD estimation by means of data from the field

By means of the information about the quantities of Valves and Actuators produced and traded by OMC in the period from 2007 to 2017 and the field return data due to failures, an estimation of the failure rate can be made.

With regard to the tables reported in Annex 2 and declared by OMC, a total reference time of more than 1.300.000.000 hours for the Valves and of more than 1.300.000.000 hours for the Actuators (calendar time) can be considered, during which some components have been returned in fault conditions (failure able to prevent the carrying out of the safety function, not due to external causes, like human error).

By means of the statistical approaches for cases without failures reported in the previous paragraphs, an estimation of the failure rates relevant to the Valves and Actuators has been carried out.

Table 7 – Failure rate for Valves and Actuators by means of data from field

Item	q*h	n. of faults	confidence %	λ_{low} [h^{-1}]	λ_{mean} [h^{-1}]	λ_{up} [h^{-1}]
Two-port Valves	1.157.191.620	79	90	5,614E-08	6,827E-08	8,232E-08
Three-port Valves	164.600.400	21	90	8,549E-08	1,276E-07	1,837E-07
Actuators	1.357.226.220	30	90	1,591E-08	2,210E-08	2,998E-08

As it can be seen in Table 7, the calculation has been characterised by the following conservative hypothesis:

- the uncertainty range of the failure rate representative for each size class has been evaluated with reference to a confidence level conservatively equal to 90%;
- within the uncertainty range for each size class, the failure rate corresponding to the 95-th percentile (λ_{UP}), that is to say the worst one in probabilistic terms, has been considered.

Since the operating mode of the Valves and Actuators according to the Standard IEC 61508 is "low demand mode operation", the reference statistical parameter is the PFD, provided by the following formula (adapted from IEC EN 61508):

$$\text{PFD} = \lambda_{DD,PST} \cdot MTTR + \lambda_{DU,FPT}\left(\frac{1}{2}\theta_{FPT} + MRT\right)$$

which has validity for the hypothesis (generally widely accomplished) of $\lambda t < 0{,}1$ and $\theta >> MRT$, and in which:

$\lambda_{DD,PST}$ = cumulative failure rate related to dangerous failure modes that can be detected by means of Partial Stroke Testing, with characteristics of diagnostics according to the interpretation of IEC EN 61508;

$\lambda_{DU,FPT}$ = cumulative failure rate related to dangerous failure modes that can be detected by means of Full Proof Testing, with characteristics of diagnostics according to the interpretation of IEC EN 61508;

λ_{NE} = cumulative failure rate related to failure modes that have no effect on the safety function;

θ_{PST} = time interval between two consecutive Partial Stroke Tests (expressed in hours);

θ_{FPT} = time interval between two consecutive Full Proof Tests (expressed in hours);

MRT = Mean Repair Time (expressed in hours);

MTTR = Mean Time To Restoration (expressed in hours) = θ_{PST} + *MRT*.

Assuming the following alternatives:

- time intervals for the execution of Full Functional Proof Tests in a range from 1 month (730 hours) up to three years (26.280 hours), considered by TÜV as the maximum acceptable time interval for Full Functional Proof Test for devices implementing safety related functions,
- time intervals for the execution of Partial Stroke Tests in a range from 1 month (730 hours) and 1 year (8760 hours),

the resulting values of PFD, with reference to the “low demand mode of operation” for the Valves and Actuators are distributed as in the following tables.

Table 8 – PFD values for different inspection/proof test intervals - Valves

Full Proof Test Interval [months]	Two-port Valves											
36	1,319E-04	1,338E-04	1,357E-04	1,377E-04	1,396E-04	1,415E-04	1,435E-04	1,454E-04	1,473E-04	1,492E-04	1,512E-04	1,531E-04
33	1,211E-04	1,230E-04	1,249E-04	1,268E-04	1,288E-04	1,307E-04	1,326E-04	1,346E-04	1,365E-04	1,384E-04	1,403E-04	1,423E-04
30	1,102E-04	1,122E-04	1,141E-04	1,160E-04	1,180E-04	1,199E-04	1,218E-04	1,237E-04	1,257E-04	1,276E-04	1,295E-04	1,315E-04
27	9,942E-05	1,013E-04	1,033E-04	1,052E-04	1,071E-04	1,091E-04	1,110E-04	1,129E-04	1,148E-04	1,168E-04	1,187E-04	1,206E-04
24	8,860E-05	9,053E-05	9,245E-05	9,438E-05	9,631E-05	9,824E-05	1,002E-04	1,021E-04	1,040E-04	1,060E-04	1,079E-04	1,098E-04
21	7,778E-05	7,970E-05	8,163E-05	8,356E-05	8,549E-05	8,742E-05	8,935E-05	9,128E-05	9,321E-05	9,514E-05	9,706E-05	9,899E-05
18	6,695E-05	6,888E-05	7,081E-05	7,274E-05	7,467E-05	7,660E-05	7,853E-05	8,046E-05	8,239E-05	8,431E-05	8,624E-05	8,817E-05
15	5,613E-05	5,806E-05	5,999E-05	6,192E-05	6,385E-05	6,578E-05	6,771E-05	6,964E-05	7,156E-05	7,349E-05	7,542E-05	7,735E-05
12	4,531E-05	4,724E-05	4,917E-05	5,110E-05	5,303E-05	5,496E-05	5,689E-05	5,881E-05	6,074E-05	6,267E-05	6,460E-05	6,653E-05
9	3,449E-05	3,642E-05	3,835E-05	4,028E-05	4,221E-05	4,414E-05	4,607E-05	4,799E-05	4,992E-05	-	-	-
6	2,367E-05	2,560E-05	2,753E-05	2,946E-05	3,139E-05	3,332E-05	-	-	-	-	-	-
3	1,285E-05	1,478E-05	1,671E-05	-	-	-	-	-	-	-	-	-
	1	2	3	4	5	6	7	8	9	10	11	12
	Partial Stroke Test Interval [months]											

Full Proof Test Interval [months]	Three-port Valves											
36	2,943E-04	2,986E-04	3,029E-04	3,072E-04	3,116E-04	3,159E-04	3,202E-04	3,245E-04	3,288E-04	3,331E-04	3,374E-04	3,417E-04
33	2,702E-04	2,745E-04	2,788E-04	2,831E-04	2,874E-04	2,917E-04	2,960E-04	3,003E-04	3,046E-04	3,089E-04	3,132E-04	3,175E-04
30	2,460E-04	2,503E-04	2,546E-04	2,589E-04	2,633E-04	2,676E-04	2,719E-04	2,762E-04	2,805E-04	2,848E-04	2,891E-04	2,934E-04
27	2,219E-04	2,262E-04	2,305E-04	2,348E-04	2,391E-04	2,434E-04	2,477E-04	2,520E-04	2,563E-04	2,606E-04	2,649E-04	2,692E-04
24	1,977E-04	2,020E-04	2,063E-04	2,106E-04	2,150E-04	2,193E-04	2,236E-04	2,279E-04	2,322E-04	2,365E-04	2,408E-04	2,451E-04
21	1,736E-04	1,779E-04	1,822E-04	1,865E-04	1,908E-04	1,951E-04	1,994E-04	2,037E-04	2,080E-04	2,123E-04	2,166E-04	2,209E-04
18	1,494E-04	1,537E-04	1,580E-04	1,623E-04	1,667E-04	1,710E-04	1,753E-04	1,796E-04	1,839E-04	1,882E-04	1,925E-04	1,968E-04
15	1,253E-04	1,296E-04	1,339E-04	1,382E-04	1,425E-04	1,468E-04	1,511E-04	1,554E-04	1,597E-04	1,640E-04	1,683E-04	1,726E-04
12	1,011E-04	1,054E-04	1,097E-04	1,140E-04	1,183E-04	1,227E-04	1,270E-04	1,313E-04	1,356E-04	1,399E-04	1,442E-04	1,485E-04
9	7,698E-05	8,128E-05	8,559E-05	8,989E-05	9,420E-05	9,850E-05	1,028E-04	1,071E-04	1,114E-04	-	-	-
6	5,283E-05	5,713E-05	6,144E-05	6,574E-05	7,005E-05	7,435E-05	-	-	-	-	-	-
3	2,868E-05	3,298E-05	3,729E-05	-	-	-	-	-	-	-	-	-
	1	2	3	4	5	6	7	8	9	10	11	12
	Partial Stroke Test Interval [months]											

Legend			
SIL 4	SIL 3	SIL 2	SIL 1

Table 9 – PFD values for different inspection/proof test intervals - Actuators

Full Proof Test Interval [months]	Actuators											
36	5,826E-05	6,307E-05	6,787E-05	7,267E-05	7,747E-05	8,227E-05	8,708E-05	9,188E-05	9,668E-05	1,015E-04	1,063E-04	1,111E-04
33	5,382E-05	5,862E-05	6,342E-05	6,822E-05	7,302E-05	7,783E-05	8,263E-05	8,743E-05	9,223E-05	9,704E-05	1,018E-04	1,066E-04
30	4,937E-05	5,417E-05	5,897E-05	6,377E-05	6,858E-05	7,338E-05	7,818E-05	8,298E-05	8,779E-05	9,259E-05	9,739E-05	1,022E-04
27	4,492E-05	4,972E-05	5,452E-05	5,933E-05	6,413E-05	6,893E-05	7,373E-05	7,854E-05	8,334E-05	8,814E-05	9,294E-05	9,774E-05
24	4,047E-05	4,527E-05	5,008E-05	5,488E-05	5,968E-05	6,448E-05	6,929E-05	7,409E-05	7,889E-05	8,369E-05	8,849E-05	9,330E-05
21	3,602E-05	4,083E-05	4,563E-05	5,043E-05	5,523E-05	6,003E-05	6,484E-05	6,964E-05	7,444E-05	7,924E-05	8,405E-05	8,885E-05
18	3,158E-05	3,638E-05	4,118E-05	4,598E-05	5,078E-05	5,559E-05	6,039E-05	6,519E-05	6,999E-05	7,480E-05	7,960E-05	8,440E-05
15	2,713E-05	3,193E-05	3,673E-05	4,153E-05	4,634E-05	5,114E-05	5,594E-05	6,074E-05	6,555E-05	7,035E-05	7,515E-05	7,995E-05
12	2,268E-05	2,748E-05	3,228E-05	3,709E-05	4,189E-05	4,669E-05	5,149E-05	5,630E-05	6,110E-05	6,590E-05	7,070E-05	7,550E-05
9	1,823E-05	2,303E-05	2,784E-05	3,264E-05	3,744E-05	4,224E-05	4,704E-05	5,185E-05	5,665E-05	-	-	-
6	1,378E-05	1,859E-05	2,339E-05	2,819E-05	3,299E-05	3,779E-05	-	-	-	-	-	-
3	9,335E-06	1,414E-05	1,894E-05	-	-	-	-	-	-	-	-	-
	1	2	3	4	5	6	7	8	9	10	11	12
	Partial Stroke Test Interval [months]											

Legend			
SIL 4	SIL 3	SIL 2	SIL 1

The following information can be extracted with regard to the considered safety function:

- for all the classes here above, a SIL 3 classification can be fully achieved for a wide range of combinations of Partial Stroke Tests and Full Proof Tests.

Then, with reference to the overall table of PFD results, requirement can be defined for the execution of a program of Partial Stroke Testing with time interval not higher than 12 months AND of Full Functional Proof Testing with time interval not higher than 36 months.

4.2 Architectural/functional analysis

4.2.1 FMEDA Analysis

The FMEDA analysis has been carried out in order to identify any possible weak point of the systems object of the study. Such objective has been reached by carrying out a systematic and documented examination of all possible failure modes and identifying their local and system effects and the possible preventive and compensating measures in order to mitigate them. The detail of information at single failure mode level is moreover of fundamental importance in order to support the considerations relevant to the architectural/functional aspects mentioned in the previous § 2.4.

The main general assumption for the performing of the FMEDA analysis are the following:

- the considered failure effects refers to the worst case scenario;
- the analysis is performed under the general hypothesis of single failure: the effects related to a generic failure mode must be assessed with regard to the case in which no other failure takes place with reference both to the same component and to the overall system. This assumption has a fundamental importance in order to highlight any criticality of the system in its design configuration.

In this specific case, it is important to remark that it is not possible to know the functionality and the architecture of the overall complex system in which the considered item will be installed and working. By this reason, the qualitative criticality assessment is limited to the possible worst effects at single Valve or Actuator level, without any considerations at system level (out of scope for the present analysis).

The meaning of each field of the FMEDA table is defined as follows:

Item	Definition of the considered component
Function	Short description of the function performed by the considered item
Failure mode	The mode or form in which the examined failure appears (failure modes have been identified on the basis of information coming from the OREDA database [2])
Failure cause	The triggering condition
Failure rate (item)	Overall failure rate for the component (safe + dangerous) [h^{-1}]
Allocation index (%)	Percentage factor of splitting for the failure rate over the different foreseen failure modes

Failure classification	Classification of the failure mode regarding the considered safety function calculation in absence of diagnostic tests or implementation of other effective detection measures: S: safe failure; D: dangerous failure;
Failure rate	Failure rate related to a specific failure mode [h^{-1}]
Local effects	The worst possible effects of the related failure mode at local level
System effects	The worst possible effects of the related failure mode upon the functionality of the component
MRT	Mean Repair Time
MTTR	Mean Time To Restoration
On-line / Off-line repair	Indication whether maintenance task regarding the considered failure mode is carried out on-line (without removing the item from the process line) or off-line
Failure detection by diagnostic tests or self-detection	Indication of possible detection by diagnostic tests (if any) or indication of possible symptoms in the associated process leading to immediate detection (self-detectable failure mode)
Failure detection by proof tests	Indication of possible detection by periodical proof tests or other means that can be assimilated to diagnostic (see previous § 2.5)
	Classification of the failure mode in terms of impact on the identified SIF and in terms of detection: NE: no effect; DU: dangerous undetected; SU: safe undetected; SD/DD: safe/dangerous detected by diagnostic tests and/or self-detectable; DD,PST: dangerous detected with Partial Stroke Testing; DU,FPT: dangerous undetected with periodical Full Proof Testing.
Notes	Any additional remark

The percentage allocation at the basis of the study has been carried out, firstly, on the basis of the percentage weights deduced, for the reference failure modes of the correspondent type of equipment (a Valve or an Actuator) from the OREDA database: a further modification process has been applied in order to adapt the allocation to the specificity of the valves object of the analysis, taking into account the basic percentage distributions of the recorded claims from field returns, and allocating other detailed failure modes proportionally according to indications from OREDA. In particular, claims from field returns have been considered as primary source, because they are representative of real working conditions. On the other hand, data from OREDA are considered as necessary and complementary because all the possible failure modes are included, since it is possible that claims from field returns do not cover all possible failure modes. See column “notes” in the FMEDA for further details.

For the Valves and Actuators object of the analysis the following failure modes have been considered, starting from OREDA:

DOP - Delayed Operation

ELP - External Leakage - Process medium

FTC - Fail to Close on demand

FTO - Fail to Open on demand

FTR - Fail to Regulate

INL - Internal Leakage

LCP - Valve Leakage in Closed Position

OTH - Other Critical Failures

SER - Minor in-service problems

SPO - Spurious Operation

STD - Structural Deficiency

UNK - Unknown

The complete FMEDA analysis for the Valves and Actuators has been reported in Annex 3.

4.2.2 Mean Repair Time

FMEDA analysis allows to systematically assign values of Mean Repair Time with regard to all possible reference failure modes of the Valves and Actuators.

Regarding MRT, following considerations must be pointed out:

- MRT has been assumed as the time necessary to replace the failed item with a spare, in order to correctly evaluate the availability of the Valves and Actuators in the overall system, for all failure modes requiring an "*off-line*" repair;
- MRT has been assumed equal to the actual time necessary to repair on line the failed item, without removing it from the process line, for all failure modes requiring an "*on line*" repair.

According to the above mentioned assumptions and to partial MRT values depicted in FMEDA, MRT for the Valves and Actuators, results to be:

$$MRT = \frac{\sum_i MRT_i * \lambda_i}{\sum_i \lambda_i}$$

Where:

MRT_i = MRT related to the i-th failure mode;

λ_i = failure rate related to the i-th failure mode;

Table 10 – MRT values for different types of Pneumatic Rotary Actuators Scotch Yoke HD-type

Item	MRT [h]
Two-port Valves	8
Three-port Valves	8
Actuators	8

Due to the low value identified, a conservative value of 8 hours for all classes will be assumed.

4.2.3 Common Cause Failure

The Standard IEC EN 61508-6 Annex D indicates the approach of the β-factor model in order to assess the Common Cause Failure:

$$\lambda_{CCF} = \lambda_{DU} \cdot \beta + \lambda_{DD} \cdot \beta_D$$

Where:

λ_{CCF} = overall failure rate due to dangerous Common Cause Failures;

λ_{DU} = probability of dangerous undetected failure of a single channel;

β = common cause failure factor for undetectable dangerous fault, which is equal to the overall

β-factor that would be applicable in the absence of diagnostic testing;

λ_{DD} = probability of dangerous detected failure of a single channel;

β_D = common cause failure factor for detectable dangerous fault.

To estimate β and β_D, tables and checklists reported in the Standard IEC EN 61508-6 Annex D have to be applied. Several issues reported in these tables refer to aspects related to the overall Safety Loop System enclosing the Valves and Actuators object of the present study. These aspects concern operational/maintenance issues, architecture/redundancies/diversifications within the overall Safety Loop System, testing and commissioning aspects, experience and training of operators, environmental parameters, etc. As the most part of these issues is not under control of TÜV Italia, the β-factors have to be assumed equal to the worst values for sensors/final elements.

According to the Standard IEC EN 61508-6 Annex D, the maximum value that can be assessed for β or β_D for sensors/final elements is then equal to 10%.

4.2.4 Hardware Fault Tolerance

From the point of view of the Hardware Fault Tolerance parameter, according to technical indications provided by OMC, the system under analysis consists of several components in series and no redundancies are foreseen.

As already discussed in the previous chapters, several failure modes of the Valves and Actuators are critical from the point of view of the identified Safety Function.

By this reason, regarding the considered Safety Function, the Valves and Actuators are certainly characterised by the minimum level of Hardware Fault Tolerance, equal to 0.

Being the Valves and Actuators Type A systems, according to IEC EN 61508-2 7.4.4.3.1, the maximum SIL that can be allocated is SIL 2 for HFT = 0 and SIL 3 for HFT = 1, regardless to any other probabilistic or architectural/functional consideration.

4.3 Systematic safety integrity requirements

As mentioned in § 2, the SIL classification for a specific safety function must take into account systematic safety integrity constraints according to IEC EN 61508-2 7.4.2.

The systematic safety integrity evaluation has been performed according to the route 2_S as foreseen by the standard IEC EN 61508-2 7.4.10, in order to identify the highest safety integrity level that can be claimed for identified safety function. In particular, the following aspects have been considered:

- A specified functionality with an adequate documentary evidence of the failure collected in a database;
- Evidence that the dangerous failure rate has not been exceeded in previous use;
- Effectiveness of the system for reporting failure through statistical evidence;
- Low complexity of the element;
- The design is well established for many years;
- There are no elements that can affect the safety integrity of the element function and that are not covered by proven in use.

Furthermore the following requirements have to be considered for future applications:

- Any difference between the previous conditions of use and those that have been experienced will require an impact analysis on the differences in order to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required safety integrity level(s) of the safety function(s) that use the element is not affected.
- Any future modification of a proven in use element shall be evaluated according to IEC EN 61508-2 7.8.

4.4 SIL classification of the system

As mentioned in § 2, the SIL classification for a specific safety function must take into account both probabilistic aspects and functional/architectural issues.

Concerning the architectural/functional aspects (based on considerations relevant to Hardware Fault Tolerance), the following outcome has been obtained:

- With regard to the Safety Function, the Valves and Actuators object of the analysis, are compliant for a classification up to SIL 2, stated that a correct and adequate program of Partial Stroke Testing, executed by means of procedure and supported by technical devices able to assimilate them to diagnostic tests (see § 2.5) is foreseen.

With reference to probabilistic issues, the following results have been obtained:

- for all the items here above, a SIL 3 classification can be fully achieved for a wide range of combinations of Partial Stroke Tests and Full Proof Tests.

With reference to systematic safety integrity,

- for all the items here above, a SIL 3 classification can be fully achieved.

On the basis of all previous considerations, concerning both functional/architectural aspects and probabilistic evaluations, the Valves result to be compliant according to Standard IEC EN 61508:2010:

- up to SIL 2 classification with HFT = 0 and up to SIL3 with HFT = 1 with regard to Safety Function consisting of complete switching on demand (open to closed), with valve leakage within limit values agreed with the customer.

On the basis of all previous considerations, concerning both functional/architectural aspects and probabilistic evaluations, the Actuators result to be compliant according to Standard IEC EN 61508:2010:

- up to SIL 2 classification with HFT = 0 and up to SIL3 with HFT = 1 with regard to Safety Function consisting of acting of the proper valve when required.

5 CONCLUSIONS

The methodological approaches of analysis specified by IEC EN 61508:2010 have been fully implemented, carrying out an accurate assessment of correct and complete compliance with both reliability and architectural/functional requirements indicated by the Standards.

The safety function for which the SIL classification of the Valves has been carried out according to Standard IEC EN 61508, is the following:

"Close when required. In case of to Close Safety Function, valve leakage must be within limit values agreed with the Customer".

While, for the Actuators:

"Proper valve acting when required".

For the estimation of the reliability data, both data resulting from the functional/fatigue tests performed by OMC and field data related to the complete population of Valves and Actuators produced and traded by OMC in the period from 2007 to 2017 have been considered.

On the basis of both functional/architectural aspects and probabilistic evaluations, the Valves object of the analysis result to be compliant according to Standard IEC EN 61508 (Chapters: 2, 4, 6, 7)

- *up to SIL 2 classification with HFT = 0 and up to SIL3 with HFT = 1 with regard to Safety Function consisting of switching on demand (open to closed), with valve leakage within limit values agreed with the customer.*

On the basis of both functional/architectural aspects and probabilistic evaluations, the Actuators object of the analysis result to be compliant according to Standard IEC EN 61508 (Chapters: 2, 4, 6, 7)

- *up to SIL 2 classification with HFT = 0 and up to SIL3 with HFT = 1 with regard to Safety Function consisting of acting of the proper valve when required.*

6 DISCLAIMER

The present technical report is exclusively based on the documentation and information provided by OMC during the meetings or by mean of email communications.

The origin of this documentation, as well as the use of this report, is not under TÜV liability.