File No.TCF1-BTLT-SIL

FUNCTIONAL SAFETY ASSESSMENT REPORT

Of BALL VALVES for ZHEJIANG BOTELI TECHNOLOGY CO., LTD.

Date of issue 08 Sep 2017

Ente Certificazione Macchine Srl

Via Cà Bella 243 – 40053 Valsamoggia (BO) - ITALY

☎ +39 051 6705141 ⧖ +39 051 6705156 ✉ info@entecerma.it ◔ www.entecerma.it

Contents

1. INTRODUCTION

1.1 Objective of the present document

This present document constitutes the final assessment report of all the series of Ball Valves listed in the chapter 2 developed by ZHEJIANG BOTELI TECHNOLOGY CO., LTD.

It presents in details all the functional safety assessment activity results according to the standard IEC 61508 applied to a SIL certification.

This report is only intended to support certification of the above product and products that are generically similar, i.e., the ball valve design is similar for all sizes of valve, and only materials are changed to suite different process applications. Ball valve include Floating Ball valve and Trunnion Ball valve.

This report contains the identified non compliances (if existing) and the assessment synthesis.

1.2 Document update and revision

This document is updated frequently during the assessment process by the assessment responsible.

1.3 Glossary

1.3.1 Acronyms

Acronym	**Signification**
CCF	Common Cause Failure
HFT	Hardware Fault Tolerance
IEC	International Electronic Committee
MTTR	Mean Time To Repair

PE	Programmable Electronic
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
RAMS	Reliability Availability Maintainability Safety
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specification

Table 1: Acronyms

1.3.2 Definitions

Term	**Definitions**
Conformity assessment	Proofs and demonstrations analysis activities in order to check the fulfilment of a reference document's requirements (NF EN ISO 9000, 2000 version).
Certification	Certification is an activity by which an independent recognized body gives a written insurance that a product, a process or a service is in accordance with specific requirements (AFNOR). Activity realized by ECM.
Client	Refers to the company that conceives, or conceives and manufactures the product according to the applicable requirements of the IEC 61508 standard.

Safety dossier	Set of documents linked to the functional safety of a product. Including Safety Plan, Safety Report et all the safety demonstrations required.
Final element	Part of the safety instrumented system which implements the physical action to achieve a safe state
Safety Integrity Level (SIL)	Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

Table 2: Definitions

1.4 References

R[01] Standard IEC 61508 : Part 1 to 7 - Edition 2

R[02] Contract

R[03] SIL product list

R[04] Catalog of Ball valve product.

2. ASSESSMENT SCOPE

2.1 Technical perimeter

The assessment and certification focus on the ball valves in followed table. All the ball valves associated with this assessment are all mature products and have been in the manufacturing phase for many years. The relevant lifecycle and management system assessment therefore applies to all relevant ongoing activities (including design modifications). This is reasonable, especially when considering that the devices qualify with the criteria for Type A components (IEC 61508-2, clause 7.4.3.1.2).

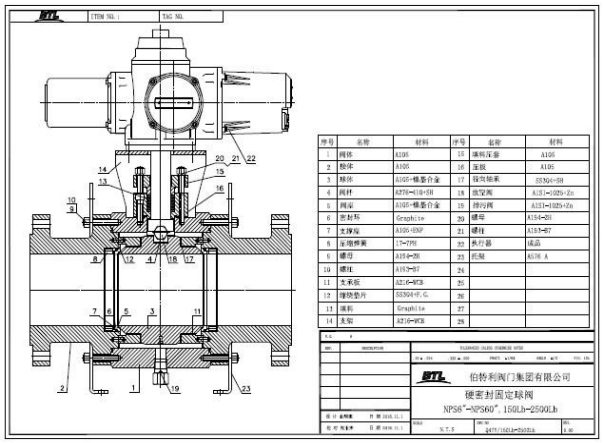
Product	name included
valve	Floating Ball valve
	Trunnion Ball valve

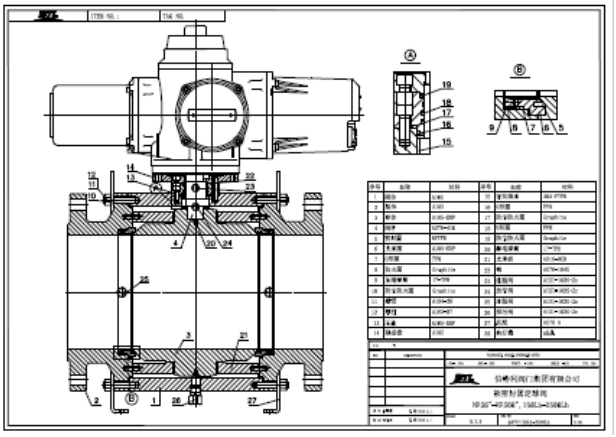
Note: Software is not part of the assessment scope, thus no compliancy assessment regarding the requirements of IEC 61508-3 has been done.

The valves are actuated thanks to an automatic actuator. Those actuators allow leading automatically to the safe state in case of safety instrumented systems operation or in

case of failure. Hence wheel and manual valves that are only manually activated are excluded from the present certificate and the present assessment report.

Here are typical presentations of ball valve:





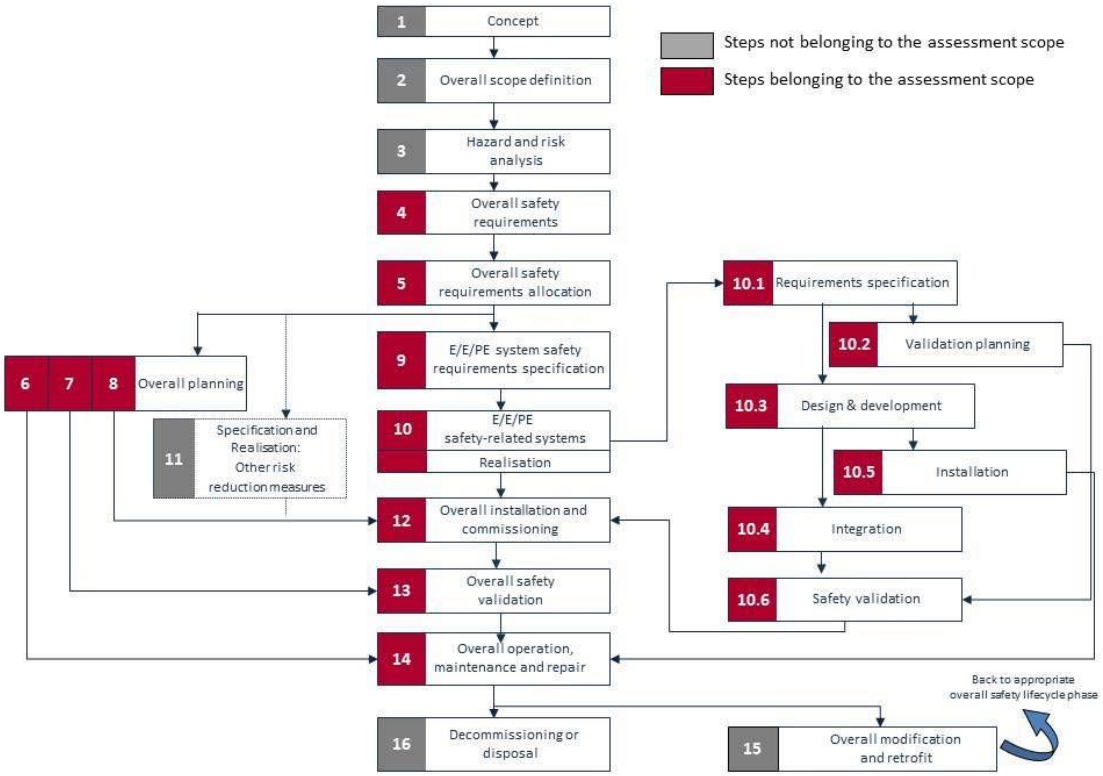
The description of ball valve can be found in the Safety Requirement Specification and Design and Development Files. The safety functions of ball valve are to open and to close on demand.

Note: The valve can be used with a manual wheel; in this case, assessment and certification regarding IEC 61508 are not applicable.

2.2 Certification limits

The objective of BOTELI TECHNOLOGY is to obtain a SIL3 Capable certification of the ball valves in 1oo2 configuration.

The current assessment does not cover all the requirements of the IEC 61508 standard.



The ball valves are generic products that could be used in a complete safety loop. Chapters 1, 2, 3, 11, 14, 15 and 16 are not included in the area of assessment and fall under the responsibility of the final client.

2.3 Safety functions description

The safety function of the valves is defined as below:

To open or close on demand as the requirement of the system

2.4 Assessed documents

Each Series ball valves' Catalog, design consideration, user manual, maintains manual have been assessed.

3. CALCULATION ASSESSMENT

The objective of this paragraph is to verify that figured goals (PFD/PFH) and the safe failure rate are compliant with IEC 61508 requirements.

3.1 Field experience analysis

ECM requires information, according to the IEC 61508 standard, for reliability computations from the field experience. There are given here under:

at least 10 devices in different applications;

documentation of all changes about safety and impact analysis on safety;

unchanged specification;

10 million operation time in hours (with energy); and

at least two years' experience.

The field experience study is based on the BOTELI TECHNOLOGY commitment.

As a result, the field experience is available on ball valves sold since 2007. ECM assesses the proven in use data. BOTELI TECHNOLOGY supplies enough operating hours. BOTELI TECHNOLOGY fulfills requirements about 3 years' experience and more than 1000 devices in different applications.

ECM has assessed the field experience data and BOTELI TECHNOLOGY presents its results in FMEA & Field Experience & PFD calculation.

3.2 IEC 61508 requirements

3.2.1 Demand Mode

The hardware requirements compliancy is assessed according to the Failure Modes Effects and Diagnostic Analysis of the system. The safety function shall respect the following requirements according to Standard IEC 61508: Part 1 to 7 - Edition 2 [R01]:

Safety integrity level **(SIL)**	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)**
1	10^{-2} δ PFD < 10^{-1}	10^{-6} δ PFH < 10^{-5}
2	10^{-3} δ PFD < 10^{-2}	10^{-7} δ PFH < 10^{-6}
3	10^{-4} δ PFD < 10^{-3}	10^{-8} δ PFH < 10^{-7}
4	PFD < 10^{-4}	PFH < 10^{-8}

Low demand, High demand or continuous modes are defined in the standard, Part 4, §3.5.16:

"Way in which a safety function operates, which may be either

– low demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year; or

– high demand mode: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year; or

– Continuous mode: where the safety function retains the EUC in a safe state as part of normal operation."

Regarding this definition, BOTELI TECHNOLOGY specifies that ball valves shall be used in Low demand mode.

3.2.2 Product Type

Type A and type B are defined in the standard, Part 2, §7.4.4:

– An element can be regarded as type A if, for the components required to achieve the safety function

a) The failure modes of all constituent components are well defined; and

b) The behaviour of the element under fault conditions can be completely determined;

c) There is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

– An element shall be regarded as type B if, for the components required to achieve the safety function,

a) The failure mode of at least one constituent component is not well defined; or

b) The behaviour of the element under fault conditions cannot be completely determined; or

c) There is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures.

èThis requirement of type A is met by ball valves;

3.2.3 Systematic failures

The systematic failures are “related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors”.

è Systematic failures of ball valves have been considered covered by BOTELI TECHNOLOGY

process.

3.2.4 Failure rates and PFD calculation

A Failure Modes and Effect Analysis has been realized to determine:

The effects of different component failure modes,

What could reduce the occurrence of failure,

Failure modes of each component of the PRODUCT,

If a failure mode is safety related or not,

The proportion of each detected dangerous failure,

An estimation of each failure rates associated to failure mode.

ECM performed an assessment of the client’s FMEA and its dangerous failure rate detection distributions.

4. ASSESSMENT ACTIVITIES RESULTS ACCORDING TO THE IEC 61508 STANDARD

The results identified hereunder are a synthesis of the activities led by ECM in the frame of this assessment.

Assessed points deal with risk analysis, safety function specification and their safety integrity in order to reach the required functional safety. Regarding Valves' design, only hardware development is considered according to the standard IEC 61508.

4.1 Transverse assessment of the organization (planning, project management, documentation)

This paragraph focuses on the pieces of information concerning project management, verification and functional safety assessment. Its first target is to assess whether they are correctly identified and documented.

Its second target is to verify the respect of the global safety life cycle. It is done by checking the outputs and their correspondence with the next phases' required inputs.

The "Safety Plan" highlights the product's functional safety construction strategy. All the participants in this project and their competencies are listed in Safety plan.

The whole documentation is listed in the Appendix 1. It includes the organization aspects, the plan of functional safety activities and the technical documentation.

A set of templates and guidelines which controls the common layout of documents exists. The basic properties as document name or number, revision and approval identification are defined in naming convention rules. The approbation management process is described on the procedures for IEC 61508 Compliance.

Procedures regarding the selection of suppliers are available.

Findings ensure that these activities have been realized in accordance with the IEC 61508 standard's recommendations.

The assessment activity leads to a positive conclusion concerning the fulfilment of the IEC 61508's organization requirements.

4.2 Safety demonstration assessment/ functional safety management

This paragraph aims to assess the functional safety management. It includes the respect of all safety life cycle requirements, all responsibilities of the people dealing with the functional safety and all activities that have to be done.

The BOTELI TECHNOLOGY documents regroup all the functional safety activities led by BOTELI TECHNOLOGY to ensure the objectives of safety concerning the valve project.

Periodic functional safety audits are realized by BOTELI TECHNOLOGY (internal audit) in order to analyze all modifications brought to the valves. There are planned at least every 1 year.

Qualitative system & hardware risk analysis have been done in FMEA & Field Experience & PFD calculation. The final safety requirements have been reported in the Safety requirement specification documents of each valve.

Quantitative analysis – led through PFD/PFH calculations & SFF – have been realized by BOTELI TECHNOLOGY and assessed by ECM and prove that each valve reaches the SIL 3 Capability quantitative target in 1oo2 configuration.(see FMEA & Field Experience & PFD calculation.

The assessment activity leads to a positive conclusion concerning the fulfilment of the standard's requirements.

4.3 V&V assessment

4.3.1 Verification and Validation plans

The target of this paragraph is to assess whether each step of the global safety life cycle has been the subject of verification plan requirement, and that the verification activities have been realized and documented according to the specifications of these same plans.

V&V plan set and organizes the system verification and validation activities.

The verification activities are related to the verification of methods used during different phases of the safety lifecycle given in the standards IEC 61508.

Verification activities have been planned in the safety plan in terms of time and resources (reviews activities, input and output documents) for each applicable phase of the safety life cycle.

Associated verifications are organized with:

Compliance matrix to the SRS (clause by clause),

The assessment activity leads to a positive conclusion concerning the verification activities (planning & realization).

Validation activities are correctly identified in the system validation plan.

All responsible should have been independent from the design team.

4.3.2 Traceability assessment

Ball valves have a very limited number of safety related product requirements. All requirements were kept in the Safety Requirement Specification. As all requirements are thoroughly verified and validated, this approach was considered to be appropriate, fulfilling the objectives of the standard. Moreover, the IEC 61508 requirement traceability has been realized by ECM during the assessment, for each requirement.

The assessment activity leads to a positive conclusion concerning the traceability process requirements.

ECM recommendation: A traceability matrix of all requirements of IEC 61508 should be realized by BOTELI TECHNOLOGY in order to prove the compliancy.

4.4 Maintenance assessment (modifications management, configuration management, installation, operation, decommissioning)

Commissioning, configuration, maintenance and exploitation activities are described in the “safety manual”.

Commissioning and maintenance of the valve must be done by qualified staff; according to requirements presented on the Safety manual.The valve’s user is responsible of the periodic test and maintenance recording.

BOTELI TECHNOLOGY is a supplier, and its responsibility ends by supplying the safety manual. BOTELI TECHNOLOGY only gives requirements for the installation and the maintenance of its valve through the Safety manual. Regarding the maintenance and functional safety, frequencies for proof tests are given in the Safety manual.

The product modification procedure is defined on the Nonconforming product control procedure and Correction prevention action procedure. The document modification is defined on the Document control procedure. And design modification procedure is defined on the Design & development of control procedure. Any modification leads to the verification and validation of each phase of safety function have been traced and meet require of standard.

Factory and Site Acceptance: Tests are planned for the validation of the product. There are realized according a FAT procedures, and all results are documented.

The Safety Manuals describes that if a failure occurs whereas it is not described on the manual, BOTELI TECHNOLOGY shall be in charge on the repair task. Then, an impact analysis is realized in order to update the document.

The assessment activity leads to a positive conclusion concerning the compliance toward maintenance requirements.

5. SYNTHESIS

5.1 Exported requirements reminder

Ball valves must be used respecting essential rules to maintain its SIL3 Capability properties in 1oo2 configuration. These rules are reminded hereunder.

The product's concerned version is reminded in part 3 of this present document.

Acceptable environment constraints are reminded in the SIL user's manual of the valve. The element shall always be verified before integration of the valve.

The following working conditions must be respected. Exported requirements are presented in the Safety manual.

The limits of working conditions strongly depend on the valve type and on materials of construction; operating limits of temperature and pressure of several specified valves are indicated in the following tables (detailed information could be found in safety manual):

Ball valves		
ball valve type	Min-Max T Range	Remark
Floating ball valve	-29-425℃	Depending on valve size/class/material
Trunnion ball valve	-29-120℃	Depending on valve size/class/material

The Safety Integrity Level and PFD/PFH of the safety function using the valves shall be calculated taking into account the characteristics of the whole system.

The mode of operation, used as a hypothesis for PFD calculation, is Low demand, which means less than 1 trip demand each year;

5.2 Conclusion

Ball valves are:

Type A elements

Suitable to be used in a safety loop SIL 2 in 1oo1 configuration:

Suitable to be used in a safety loop SIL 3 in 1oo2 configuration:

ECM assessment leads to the conclusion that Ball valves designed and manufactured by BOTELI TECHNOLOGY are compliant to a SIL 3 Capability IEC 61508 (Edition 2) if used in a 1oo2 configurations.

ECM recommendation: A traceability matrix of all requirements of IEC 61508 should be realized by BOTELI TECHNOLOGY in order to prove the compliancy.

This report remains valid 3 years, or until the next change of the system or configuration.

APPENDIX 1: ASSESSED DOCUMENT

Reference	Title	revision	date
SIL2017-001	Safety plan	B	23/8/2016
SIL2017-004	Safety Requirement Specification for Ball Valve	C	8/9/2016
SIL2017-005	V&V Plan	A	12/2015
SIL2017-008	Safety Manual for Ball Valve	B	23/8/2016
SF-FE003	Design and development files	A	25/5/2016
SIL2017-009	FMEA & Field Experience & PFD calculation	A	27/5/2016
P016	Non-conforming product control procedure	B	20/5/2015
P008	Correction prevention action procedure	B	20/5/2015
P002	Document control procedure	B	20/5/2015
P001	Design & Development Control Procedure	B	20/5/2015

APPENDIX 2: PFD ASSESSMENT

BOTELI calculations assessment

BOTELI TECHNOLOGY realizes PFD calculations according to the field experience of the valve
components. ECM has assessed these PFD calculations and presented the results.

Component Architecture	SIL Capabiility	Demand frequency	PFD
1oo1 Configuration	SIL 2	Low	3.12E-03
1oo2 Configuration	SIL 3	Low	2.95E-04

Safety Function	Failure Rate	Undetected Dangerous Failure Rate	Tests Intervals	MTTR
SF1	3.02E-07	2.79E-07	12 Months	24h
SF2	4.08E-07	3.14E-07	12 Months	24h

Conclusion of PFD calculation

According to BOTELI TECHNOLOGY's results, ECM has assessed Ball valves as SIL 3 Capable. The Ball valves are suitable to be used in a safety loop SIL 3 in 1oo2 configuration.