IEC 61508 Functional Safety Assessment

Project:
C-Series and T-Series Ball Valves

Customer:
MOGAS Industries, Inc.

Contract Number: Q16/10-021
Report No.: MOG 16-10-021 R003
Version V1, Revision R1, December 22, 2016
Chris O'Brien

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the:

- MOGAS C- Series Floating Ball Valve
- MOGAS T-Series Trunnion Ball Valve

The functional safety assessment performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by MOGAS Industries, Inc. through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* assessed the manufacturing quality system in use at MOGAS by an on-site audit and creation of a detailed safety case against the requirements of IEC 61508 of the Houston, TX facility.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3 for mechanical components. A full IEC 61508 Safety Case was prepared using the *exida* Safety Case tool as the primary audit tool. Hardware process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also the user documentation (safety manual) was reviewed.

The results of the Functional Safety Assessment can be summarized as:

The audited development process as tailored and implemented by the MOGAS Industries, Inc. C-Series and T-Series development project, complies with the relevant safety management requirements of IEC 61508 SIL 3, **SC 3 (SIL 3 Capable).**

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the C-Series and T-Series can be used in a low demand safety related system in a manor where the PFD_{avg} is within the allowed range for up to SIL 2 (HFT = 0) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the C-Series and T-Series can meet the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the C-Series and T-Series is capable for use in SIL 3 applications in Low DEMAND mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3 of this document.

The manufacturer will be entitled to use the Functional Safety Logo.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the MOGAS Industries, Inc. C-Series and T-Series Ball Valves by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010.

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

The results of this provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* and agreed to with MOGAS Industries, Inc..

All assessment steps were continuously documented by *exida* (see [R1] to [R3])

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, cybersecurity and availability. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data..

2.2 Roles of the parties involved

MOGAS Industries, Inc.	Manufacturer of the C-Series and T-Series Ball Valves
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment.

MOGAS contracted *exida* in August 2016 for the IEC 61508 Functional Safety Assessment of the above mentioned devices.

2.3 Standards and literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508 (Parts 1 - 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by MOGAS

[D1]	QA-01; Rev M; 4-Sep-16	Quality Assurance Manual
[D2]	QAP-1001; Rev B; 16-Oct-13	Supplier Approval & Qualification Process
[D3]	QAP-1002; Rev A; 15-Oct-13	Post Inspection and Labeling
[D4]	QAP-1003; Rev C; 6-Feb-14	Preferred Supplier Qualification Program
[D5]	QAP-1004; Rev B; 24-Feb-14	Management of Change
[D6]	QAP-1005; Rev A; 24-Feb-14	Risk Assessment and Management Plan
[D7]	QAP-1007; Rev H; 17-Oct-02	Certifications Statement
[D8]	QAP-1008; Rev C; 26-Jun-14	Legal Requirements
[D9]	QAP-1009; Rev A; 30-Jul-15	Calibration Supplier Approval Process
[D10]	QAP-1011; Rev A; 30-Jun-16	German AS 2000 HP0 Certified Machine Shops
[D11]	QMS-01-02; Rev G; 21-Feb-14	Competence, Training, and Awareness

[D12]	NPDP-01; Rev 0; 24-Mar-16	R&D New Product Development Process
[D13]	ESP-006; Rev H; 22-Dec-16	ECN Database Procedure
[D14]	RD-NPDP Form 1-1; Rev 0; Dec-16	Marketing Requirements Document
[D15]	RD-NPDP Form 2-1; Rev 0; Dec-16	Validation Test Plan
[D16]	ESP-006B; Rev A	Impact Analysis Form
[D17]	ESI-6121; Rev B; Jan-09	C-Series IOM
[D18]	ESI-6142; Rev A; 22-Oct-15	IOM for Flexstream Tortuous Path Rotary Control Technology
[D19]	Safety Manual; Dec-16	C-Series Safety Manual
[D20]	Safety Manual; Dec-16	T- Series Safety Manual
[D21]	SB-1006	Example Service bulletin
[D22]	ESD-4316; Rev E; 10-Jul-14	Trunnion Ball Valves T-Series for Flexstream Control Valves
[D23]	EST-1130; Rev B; 18-Jun-14	Valve/Actuator Assembly Testing to Meet API 6D

2.4.2 Documentation generated by *exida*

[R1]	MOG 16-10-021 R001 V1R1, 16-Dec-16	FMEDA report, C-Series Floating Ball Valves
[R2]	MOG 16-10-021 R002 V1R1, 19-Dec-16	FMEDA report, T-Series Trunnion Ball Valves
[R3]	MOG 16-10-021 Safety Case IEC 61508; 19-Dec-16	Safety Case (internal document)
[R4]	MOG 16-10-021 R003 V1R1 61508 Assessment C and T Series Ball Valves, 22-Dec-16	IEC 61508 Functional Safety Assessment, MOGAS C-Series and T-Series (this report)

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed upon by MOGAS Industries, Inc..

The following IEC 61508 objectives were subject to detailed auditing at MOGAS Industries, Inc.:

- FSM planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation
  - Activities and Responsibilities (Training and competence)
  - Configuration management
- Safety Requirement Specification
- Change and modification management
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
- System Validation including hardware validation
- Hardware-related operation, installation and maintenance requirements

3 Product Descriptions

The C-Series and T-Series are an excellent choice in large bore isolation applications. Each ball and seat subassembly is mate-lapped by hand and put through a rigorous testing procedure to ensure its integrity.

The C-Series valve is available in full or reduced bore, ½ inch to 42 inches and in a wide variety of end connections.

Specifications:

Valve Sizes:	Valve Sizes ½" through 42"
Pressure Ratings:	ANSI Class 150 to ANSI Class 4500

The T-Series valve is available in full or reduced bore, 2 inch to 42 inches and in a wide variety of end connections.

Specifications:

Valve Sizes:	Valve Sizes 2" through 42"
Pressure Ratings:	ANSI Class 300 to ANSI Class 2500

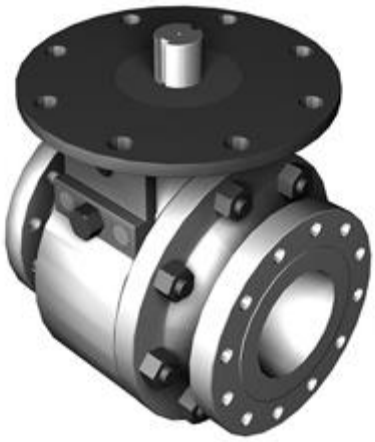

Figure 1 Typical C-Series covered in this Assessment

The MOGAS C-Series and T-Series are classified as devices that are part of a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0.

[1] Type A element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2, ed2, 2010.

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by MOGAS Industries, Inc. for this development project against the objectives of the *exida* certification scheme which includes subsets of IEC 61508 -1 to 3. The results of the assessment are documented in the Safety Case [R3].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software. The assessment also includes a review of existing manufacturing quality procedures to ensure compliance to the quality requirements of IEC 61508.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
  - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
  - Specification process, techniques and documentation
  - Design process, techniques and documentation, including tools used
  - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
  - Verification activities and documentation
  - Modification process and documentation
  - Installation, operation, and maintenance requirements, including user documentation
  - Manufacturing Quality System
- Product design
  - Hardware architecture and failure behavior, documented in a FMEDA

The review of the development procedures is described in section 5. The review of the product design is described in section 5.2.

4.2 Assessment level

The C-Series and T- Series Ball Valves has been assessed per IEC 61508 to the following levels:

- SIL 3 capability

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by MOGAS Industries, Inc. for these products against the objectives of IEC 61508 parts 1 - 7.

5.1 Lifecycle Activities and Fault Avoidance Measures

MOGAS Industries, Inc. has a 4-phase staged-gate process in place for product development with specific deliverables, reviews and approvals at each gate. This is documented in R&D New Product Development Process [D12]. No software is part of the design and therefore any specific requirements from IEC 61508 related to software and software development do not apply.

This functional safety assessment has shown that the process sufficiently meets the requirements of IEC 61508, SIL 3. The assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for product design and development. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited MOGAS Industries, Inc. design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

FSM Planning

MOGAS Industries, Inc. has a 4-phase staged-gate process in place for product development with specific deliverables, reviews and approvals at each gate. This is documented in R&D New Product Development Process. The R&D New Product Development Process meets the requirements of IEC 61508. Modifications are controlled under the ECN Database Procedure [D12] which calls out the requirements for changes to safety certified products.

Version Control

All documents as called out for in R&D New Product Development Process are under version control. Design drawings and documents are also under version control.

Training, Competency recording

Training and competency are controlled by the Competence, Training and Awareness procedure [D11]. Functional safety training has been conducted. Training records are maintained. MOGAS hired *exida* to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

5.1.2 Safety Requirements Specification and Architecture Design

During Phase 1 – Plan and Specify, the Market Requirements Document (MRD) [D14] is created. The MRD lists the market requirements for the product. The completion of the MRD is one of the required deliverables to move from Phase 1 – Plan and Specify, to Phase 2 - Develop. Once the MRD has been reviewed and the project accepted, engineering will begin detailed design.

During Phase 2 – Develop, the Bill of Material and a Validation Plan with be produced. As the valves are simple mechanical devices, there is no need for a separate architecture design phase. The MRD and FRD will indicate if the design is new or based on an existing design.

Requirements as specified in the MRD are tracked through all development phases.

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 actuator is simple and clearly defined there is no need for semi-formal 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.

5.1.3 Hardware Design

The hardware design process is conducted in Phase 2 – Develop. The objective of this phase is to complete the physical design of the product. The main deliverable at the end of this phase is a physical prototype that is ready for detailed verification and validation testing. The MRD guides the work through this phase. During this phase a Validation and Test Plan is developed which provides the requirements for validation testing. A Preliminary Design Review is conducted during this phase as well. MOGAS Industries, Inc. has standards for documentation with specified output documents.

MOGAS Industries, Inc. uses SolidWorks as a development tool. Version numbers are listed and re-qualification is done when the tool vendor makes revisions.

Items from **IEC 61508-2, Table B.2** include observance of guidelines and standards project management, documentation (design outputs are documented per R&D New Product Development Process and other quality guidelines), structured design, modularization, use of well-tried components / materials, and computer-aided design tools. This meets SIL 3.

5.1.4 Validation

Validation Testing is done during Phase 3 – Validate. Validation is performed via a documented plan, the Validation and Test Plan [D15], written in the Develop Phase. As the C-Series and T-Series are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The C-Series and T- Series Ball Valves perform only 1 Safety Function, which is extensively tested under various conditions during validation testing.

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). Field experience and statistical testing via regression testing are not applicable. This meets SIL 3.

Items from IEC **61508-2, Table B.5** included functional testing and functional testing under environmental conditions, project management, documentation, failure analysis (analysis on products that failed), expanded functional testing, black-box testing, and fault insertion testing. This meets SIL 3.

5.1.5 Verification

The development and verification activities are defined in the R&D New Product Development Process for each phase the objectives are stated along with the required input and output documents and review activities. Design reviews are governed by this process. Per R&D New Product Development Process business viability, product requirements, and manufacturing capability are verified. All verification activities are documented. This meets SIL 3.

5.1.6 Modifications

Modifications are initiated per the ECN Database Procedure. The ECN Database Procedure requires that a Functional Safety engineer be present for all major changes and that an Impact Analysis be performed [D16]. If design changes are identified as a result of a design request, they are usually treated as a derived product and therefore the same general procedure is used for both new development and modifications. All design change requests are reviewed to determine if there is any negative impact on product safety. This review is done by both the assigned engineer and the appropriate engineering manager.

The modification process has been successfully assessed and audited, so MOGAS Industries, Inc. may make modifications to this product as needed

This meets SIL 3.

5.1.7 User documentation

MOGAS Industries, Inc. created the following user documentation: Installation, Operations and Maintenance manuals [D17] and [D18], and Safety Manuals [D19] and [D20]. The Safety Manuals was found to contain all of the required information given the simplicity of the products. The Safety Manual references the FMEDA report which is available and contains the required failure rates, failure modes, useful life, and suggested proof test information.

Items from IEC **61508-2, Table B.4** include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (C-Series and T-Series perform well-defined actions) and operation only by skilled operators (operators familiar with type of actuator, although this is partly the responsibility of the end-user). This meets SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the C-Series and T- Series Ball Valves a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida*. This is documented in [R1].

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) 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.

From the FMEDA, failure rates are derived for each important failure category. All failure rate analysis results and useful life limitations are listed in the FMEDA report [R1]. Tables in the FMEDA report list these failure rates for the C-Series and T-Series under a variety of applications. The failure rates listed are valid for the useful life of the devices.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore the C-Series and T- Series Ball Valves can be classified as a 2_H device. When 2_H data is used for all of the devices in an element, the element meets the hardware architectural constraints up to SIL 2 at HFT=0 (or SIL 3 @ HFT=1) per Route 2_H.

If Route 2_H is not applicable for the entire final element, the architectural constraints will need to be evaluated per Route 1_H.

These results must be considered in combination with PFD_{avg} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The architectural constraints requirements of IEC 61508-2, Table 2 also need to be evaluated for each final element application. It is the end users responsibility to confirm this for each particular application and to include all components of the final element in the calculations.

The analysis shows that the design of the C-Series and T-Series can meet the hardware requirements of IEC 61508, up to SIL 3 depending on the complete final element design. The Hardware Fault Tolerance and PFD_{avg} requirements of IEC 61508 must be verified for each specific design.

6 Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test It is assumed that the Partial Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Random Capability	The SIL limit imposed by the PFD_{avg} for each element.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares reports based on methods advocated in International standards. *exida* accepts no liability whatsoever for the use of this report or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version:	V1	
Revision:	R1	
Version History:	V1, R1:	Release; December 22, 2016
	V1, R0:	Draft; December 22, 2016
Authors:	Chris O'Brien	
Review:	V1, R0	Greg Sauk (*exida*); December 22, 2016
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Chris O'Brien, CFSE, Partner

Gregory Sauk, CFSE, Senior Safety Engineer