



IEC 61508 Functional Safety Assessment

Project:

Series 364 3 Way/2 Position Solenoid Valves

Customer:

ASCO, L.P.

Florham Park, NJ

USA

Contract Number: Q15/01-030

Report No.: ASC 15/01-030 R001

Version V1, Revision R2, July 25, 2018

Loren Stewart

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the Series 364 3 Way/2 Position Solenoid Valves

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

- *exida* assessed the development process used by ASCO 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* reviewed and assessed the detailed Failure Modes, Effects, and Diagnostic Analyses (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at ASCO.

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 ASCO Series 364 3 Way/2 Position Solenoid Valves development project, complies with the relevant safety management requirements of IEC 61508 SIL3, **SC 3 (SIL 3 Capable)**.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the Series 364 3 Way/2 Position Solenoid Valves 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 SIL2 (HFT = 0) according to table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the Series 364 3 Way/2 Position Solenoid Valves meets 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 Series 364 3 Way/2 Position Solenoid Valves are capable for use in SIL3 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	5
1.1	Tools and Methods used for the assessment	5
2	Project Management.....	6
2.1	<i>exida</i>	6
2.2	Roles of the parties involved	6
2.3	Standards and literature used	6
2.4	Reference documents	6
2.4.1	Documentation provided by ASCO	6
2.4.2	Documentation generated by <i>exida</i>	7
2.5	Assessment Approach	7
3	Product Descriptions.....	9
4	IEC 61508 Functional Safety Assessment Scheme.....	10
4.1	Methodology	10
4.2	Assessment level	10
5	Results of the IEC 61508 Functional Safety Assessment.....	11
5.1	Lifecycle Activities and Fault Avoidance Measures	11
5.1.1	Functional Safety Management	11
5.1.2	Safety Requirements Specification and Architecture Design.....	12
5.1.3	Hardware Design.....	12
5.1.4	Validation.....	12
5.1.5	Verification.....	13
5.1.6	Modifications	13
5.1.7	User documentation.....	13
5.2	Hardware Assessment	13
6	Terms and Definitions.....	15
7	Status of the Document	16
7.1	Liability	16
7.2	Releases	16
7.3	Future Enhancements.....	16
7.4	Release Signatures.....	16



1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the ASCO:

- Series 364 3 Way/2 Position Solenoid Valves

by *exida* according to the 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 by ASCO.

All assessment steps were continuously documented by *exida* (see [R1] to [R2])



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, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world’s top reliability and safety experts from manufacturers, operators and assessment organizations, exida is a global corporation with offices around the world. exida offers training, coaching, project oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. exida maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

ASCO, L.P. Manufacturer of the Series 364

exida Performed the IEC 61508 Functional Safety Assessment

ASCO contracted exida in January 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 ASCO

[D1]	Quality Manual	QUALITY MANUAL REV E WHOLE.pdf
[D2]	Overall Development Process	NPD2.5-001.pdf
[D3]	Overall Development Process	NPD2-005.pdf
[D4]	Overall Development Process	NPD2-006.pdf
[D5]	Field Return Procedure	MP-I-129.pdf
[D6]	Non-Conformance Reporting procedure	MP-I-121.pdf
[D7]	Customer Notification Procedure	Sample Safety Notice.doc
[D8]	Modification Procedure	GBP-007.pdf
[D9]	Verification Plan	EDP-148.pdf
[D10]	Training Record	Sample Training Class Attendance.pdf

[D11]	ISO 900x Cert or equivalent	FP_ISO_cert_2018.pdf
[D12]	Product Catalog Data Sheet	asco-series-364-ss-spool-valves-solenoid-catalog.pdf
[D13]	Safety Manual	V9629, Rev 8, 9-Mar-2018
[D14]	Engineering Change Documentation	ECR 23811.pdf
[D15]	Impact Analysis Record	8314-8316-8320_IMPACT_ANALYSIS-002a.pdf
[D16]	Competency procedures/records, example	ASCO_DMDO_Results_final 5-27-2004.pdf
[D17]	Marketing Data Sheet Outline	Marketing Data Sheet – Outline (MDS)
[D18]	Marketing Data Sheet example, reviewed on-site	MDS Example
[D19]	Technical Specification Sheet template	Technical Specification Sheet (TSS), Template, Rev C; 1/2/02
[D20]	Verification Results	NPD100031-1-QTP-8364.pdf
[D21]	Safety Requirements Specification	NPD 100031-1 Gate 5 and 6 - Charter.pdf
[D22]	Validation Test Plan	QC-ER-003.pdf
[D23]	Validation Test Plan	ELP-161.pdf
[D24]	List of Diagnostics for FMEDA	364_SS_Spool_Valves_NonSolenoid.pdf
[D25]	List of Diagnostics for FMEDA	364_SS_Spool_Valves_Solenoid_R2.pdf
[D26]	ASCO FMEDA Report	516115-R03-25July2018.doc

2.4.2 Documentation generated by *exida*

[R1]	ASCO 364 FMEDA Review R2.xlsx	Series 364 FMEDA reviews summary
[R2]	Q15-01-030 ASCO 364 SafetyCase	IEC 61508 SafetyCaseWB for Series 364 3 Way/2 Position Solenoid Valves
[R3]	ASC 15/01-030 R001, 25-Jul-2018	IEC 61508 Functional Safety Assessment, ASCO Series 364 3 Way/2 Position Solenoid Valves (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 to by ASCO.

The following IEC 61508 objectives were subject to detailed auditing at ASCO:

- FSM planning, including
 - Scope of the FSM activities



- Documentation
- Activities and Responsibilities (Training and competence)
- Configuration management
- Tools
- Safety Requirement Specification
- Change and modification management
- Hardware architecture design - process, techniques and documentation
- Hardware-related operation, installation and maintenance requirements

3 Product Descriptions

The 364 3 Way/2 Position Solenoid Valves are pilot operated general service solenoid valves. These solenoids are intended for use on clean, dry air inert gas, or sweet dry natural gas filtered to 40 micron or better.

The 364 Valves feature 316L Stainless Steel valve materials. Valve sizes included in this assessment are 1/4" NPT port sizes. Also included are the JS2D junction box and coils option.

Table 1 gives an overview of the different versions that were considered in the FMEDAs and assessment of the 364 3 Way/2 Position Solenoid Valves.

Table 1 Version overview 364 3 Way/2 Position Solenoid Valves

Type	Function and Safe Mode Considered	Configuration	
		NC	NO
SOV	Single Solenoid Valve, DTT	✓	✓
	Single Solenoid Valve, ETT	✓	✓
	Double Solenoid Valve, ETT	User Config.	
	Latching Palm Button, Single Solenoid Valve, DTT	✓	N/A
Non-SOV	Pilot Operated / Spring Return, DTT	✓	✓
	Pilot Operated / Spring Return, ETT	✓	✓
	Double Pilot, Air Operated (with Detent), ETT	User Config.	
	Palm Operated / Air Return, ETT	✓	N/A
	Palm Operated / Air Return, Manual Trip (MT)	✓	N/A
	Pilot Operated / Spring Return, Latching, DTT	✓	N/A
	Pilot Operated / Spring Return, Latching, ETT	✓	N/A
	Remote Pilot, Latching Non Indicating, DTT	✓	N/A
	Remote Pilot, Latching Non Indicating, Remote Pilot Trip	✓	N/A
	Specialized Application: NON Latching Indicating, DTT	✓	N/A
Button Operated / Spring Return, Manual Trip (MT)	✓	✓	

The Series 364 Valves are classified as a component of a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by ASCO 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 [R2].

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 Series 364 3 Way/2 Position Solenoid Valves have 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 (SIL3) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by ASCO for these products against the objectives of IEC 61508 parts 1 - 7. The assessment was done on the Florham Park, NJ facility on March 28, 2016 and documented in the SafetyCase [R2].

5.1 Lifecycle Activities and Fault Avoidance Measures

ASCO has a 7-phase staged-gate process in place for product development with specific deliverables, reviews and approvals at each gate. This is documented in NPD2.5-001 [D2]. The same process is used for modifications. This process and procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management. No software is part of the design and therefore any requirements specific from IEC 61508 to software and software development do not apply.

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 defined product lifecycle process was modified as a result of the audit which showed some areas for improvement. However, given the simple nature of the safety function and the extensive proven field experience for existing products ASCO was able to demonstrate that the objectives of the standard have been met. The result of the assessment can be summarized by the following observations:

The audited ASCO design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

FSM Planning

ASCO has a defined process in place for product design and development. Required activities are specified along with review and approval requirements. This is primarily documented in NPD2.5-001. Templates and sample documents were reviewed and found to be sufficient. The modification process is covered by the same procedure. This process and the procedures referenced therein fulfill the requirements of IEC 61508 with respect to functional safety management for a product with simple complexity and well defined safety functionality.

Version Control

NPD2.5-001 requires that all documents be under document control. Use of this to control revisions was evident during the audit.

Training, Competency recording

Personnel training records are kept per standard quality procedures. A competency plan was developed for the project [D16]. ASCO 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

The first step for any new development is the creation of a Marketing Data Sheet (MDS) [D18] by the Marketing Department. Once this has been reviewed and the project accepted, engineering will develop the project Technical Specification Sheet (TSS) [D19]. This captures in detail all the requirements for the devices, such as critical functions, performance targets etc. exida reviewed the content of the specification for completeness per the requirements of IEC 61508.

As the valves are simple electro-mechanical devices, there is no need for a separate architecture design phase. The MDS and TSS will indicate if the design is new or based on an existing design. Requirements as specified in the Technical Specification Sheet (TSS) are tracked through all development phases.

As the function of the valve 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 consists of two distinct phases: concept verification, and design and development. During concept verification all possible solutions are reviewed and the most promising is detailed. During this phase also the Qualification Test Plan and Agency Approval Plan is developed (equal to validation plan per IEC 61508). In the design and development phase, the design is further detailed and Qualification testing is performed on beta units. Per NPD2-005 [D3], a preliminary design review, an intermediate and final design review is conducted. ASCO has standards for documentation with specified output documents.

ASCO uses ProE and AutoCad as development tools. Version numbers should be listed and re-qualification should be done when the tool vendor makes revisions. Re-qualification test results should be documented and reviewed. ASCO confirmed in discussions during the on-site audit that tool re-qualification is performed.

Items from **IEC 61508-2, Table B.2** include observance of guidelines and standards, project management, documentation (design outputs are documented per NPD2.5-001 and other quality guidelines), structured design, modularization, use of well-tried components, and computer-aided design tools. This meets SIL 3.

5.1.4 Validation

Validation Testing is done via a documented plan, the Qualification Test Plan, written per the Technical Specification Sheet and includes compliance testing per application standards, through the Agency Approval Plan which is part of the QTP. The QTP is traceable to the TSS. As the Series 364 3 Way/2 Position Solenoid Valves are purely electro-mechanical devices with a simple safety function, there is no separate integration testing necessary. However, the solenoids do undergo several separate tests before valve body and solenoid are integrated; this is part of the Qualification Test Plan. The Series 364 3 Way/2 Position Solenoid 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 New Product Development Process for Platform Products, NPD2.5-001. For each phase the objectives are stated, as well as required input and output documents and review activities. Checklists are used for e.g. the review of the Marketing Data Sheet. Design reviews are governed by NPD2-005, Valve Engineering Design Review Process. Per NPD2.5-001, the following verification steps are defined: product idea review, concept definition review, feasibility review, design and development review, pilot run review, and introduction review. All verification activities are documented. This meets SIL 3.

5.1.6 Modifications

Modifications are done per the Engineering Change Notice procedure [D8]. A web-based system is in place to track ECNs. The ECN system allows to user to identify if a certified device is affected. Affected documents and/or drawings are also listed. If design changes are identified as a result of an ECN, 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. This meets SIL 3.

5.1.7 User documentation

ASCO creates the following user documentation: product catalog [D12] and a Safety Manual [D13]. The Safety Manual was found to contain all of the required information given the simplicity of the products. The Safety Manual references the FMEDA reports which are available and contain 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 (Series 364 3 Way/2 Position Solenoid Valves perform well-defined actions) and operation only by skilled operators (operators familiar with type of valve, 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 Series 364 3 Way/2 Position Solenoid Valves Failure Modes, Effects, and Diagnostic Analysis's were reviewed by *exida*. These are 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 [D26]. Tables in the FMEDA report list these failure rates for the Series 364 3 Way/2 Position Solenoid Valves 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 Series 364 3 Way/2 Position Solenoid 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 PFH/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 Series 364 3 Way/2 Position Solenoid Valves can meet the hardware requirements of IEC 61508, SIL 3 depending on the complete final element design. The Hardware Fault Tolerance and PFH/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
<i>exida</i> 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: R2

Version History: V1, R2: Added JS2D option and other minor updates, 25-Jul-2018 GPS

V1, R1: Minor edits and updates from Draft review, April 3, 2016

V0, R1: Draft; April 3, 2016

Authors: Loren Stewart

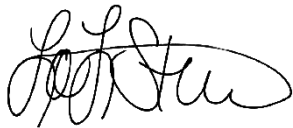
Review: V0, R1: Ted Stewart; April 3, 2016

Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

A handwritten signature in black ink, appearing to read "Loren Stewart".

Loren L. Stewart, CFSP, Senior Safety Engineer

A handwritten signature in black ink, appearing to read "Ted Stewart".

Ted E. Stewart, CFSP,
Program Development & Compliance Manager