IEC 61508 Functional Safety Assessment

Project:

D-ESD Valve Controller

Customer:

Topworx, Inc.

Louisville, Kentucky

USA

Contract Number: Q13/08-108

Report No.: EPM 13/08-108 R002

Version V1, Revision R4, May 30, 2014

Loren Stewart

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

© All rights reserved.

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the Topworx D-ESD Valve Controller

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

- *exida* assessed the development process used by Topworx, Inc. by an on-site audit and creation of a safety case against the requirements of IEC 61508.
- *exida* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to ensure that the FMEDA analysis was complete.
- *exida* reviewed the manufacturing quality system in use at Topworx.

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* SafetyCase 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 Topworx D-ESD Valve Controller was found to meet the Systematic Capability requirements of IEC 61508 for up to SC 3 (SIL 3 Capable).

The Topworx D-ESD Valve Controller meets the Random Capability requirements for a Type A device with the hardware architectural constraints per Route1$_H$ for SIL3 when automatic Partial Valve Stroke Testing is applied to the entire final element. The Safe Failure Fraction (SFF) must be determined for the entire final element per Route 1$_H$.

The D-ESD Valve Controller was found to meet the Random Capability requirements per Route 2$_H$. When 2$_H$ data is used for all of the associated devices in the final element, the final element meets the hardware architectural constraints per Route 2$_H$

The PFD$_{AVG}$ and architectural constraint requirements of the standard must be verified for each element of the safety function.

Manufacturing sites are located in Shenzhen, China; Szekesfehervar Berenyi U, Hungary and Kentucky, USA. Design control is retained in the Kentucky Facility.

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

Table of Contents

Management Summary 2

1 Purpose and Scope 4

2 Project Management 5

2.1 *exida* 5

2.2 Roles of the parties involved 5

2.3 Standards and literature used 5

2.4 Reference documents 5

2.4.1 Documentation provided by Topworx Inc. 5

2.4.2 Documentation generated by *exida* 7

3 Product Description 8

4 IEC 61508 Functional Safety Assessment 10

4.1 Methodology 10

4.2 Assessment level 10

5 Results of the IEC 61508 Functional Safety Assessment 11

5.1 Open Issues 11

5.2 Lifecycle Activities and Fault Avoidance Measures 11

5.2.1 Functional Safety Management 11

5.2.2 Safety Requirements Specification and Architecture Design 12

5.2.3 Hardware Design 12

5.2.4 Validation 12

5.2.5 Verification 12

5.2.6 Proven In Use 13

5.2.7 Modifications 13

5.2.8 User documentation 13

5.3 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 Topworx, Inc. D-ESD Valve Controller by *exida* according to the requirements of IEC 61508: ed2, 2010.

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.

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 and availability with over 300 years of cumulative experience in functional safety. 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 the largest process equipment database of failure rates and failure modes with over 60 billion unit operating hours.

2.2 Roles of the parties involved

Topworx, Inc.	Manufacturer of the D-ESD Valve Controller
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment

Topworx contracted *exida* in November 2013 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): ed 2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Topworx, Inc.

[D1]	Quality Manual	Quality Policy Manual.pdf	6	6/14/2013
[D2]	Overall Development Process	PRO-1.0 R16 06-14-13.pdf	16	6/14/2013
[D3]	Development Process Form	Master PPD Template.xls	14	9/6/2013
[D4]	Field Return Procedure	PRO-6.0 R15 03-12-12.pdf	15	3/12/2012
[D5]	Manufacturer Qualification Procedure	PRO-3.0 R18 06-14-13.pdf	16	6/14/2013
[D6]	Approved Supplier List	Approved Supplier List.xls		
[D7]	Quality Management System (QMS) Documentation Change Procedure	PRO-5.0 R20 06-14-13.pdf	20	6/14/2013
[D8]	Impact Analysis Template	Functional Safety Impact Analysis Report.pdf	1	3/12/14
[D9]	Engineering Change Form	ECO Form.pdf	45	

[D10]	Engineering Change Form	Engineering Change Order R46.pdf	46	3/13/14
[D11]	FSM Plan or Development Plan	PRO-0.5 Business Management Plan R15 06-14-13.pdf	15	6/14/2013
[D12]	FS Organization Chart	Functional Safety Organizational Chart.pdf		
[D13]	FS Policy	Functional Safety Policy.pdf		1/09/12
[D14]	Shipment Records	Topworx ESD-series shipments.pdf		2/24/14
[D15]	Field Returns Records	Coil & Spool Application failures.pdf		2/24/14
[D16]	Field Returns Records	Coil Failures.pdf		2/24/14
[D17]	Field Returns Records	Spool failures.pdf		2/24/14
[D18]	Firmware Engineer Job Description	FIRMWARE ENGINEER Job Description 2012.pdf		2012
[D19]	Manager, Technical Service Job Description	Manager, Technical Service Job Description ACTIVE.DOCX		7/8/2013
[D20]	Quality Manager Job description	Quality Manager JD FY12 - EXTERNAL.DOC		7/3/1905
[D21]	Manufacturing Engineering Supervisor Job Description	Manufacturing Engineering Supervisor 2013.doc		7/5/1905
[D22]	Valvetop & Wireless Product Manager	Manager, Valvetop & Wireless Product Manager Job Description ACTIVE.DOCX		7/5/1905
[D23]	Manufacturing Engineer Supervisor Job Description	Manufacturing Engineering Supervisor 2013.doc		7/5/1905
[D24]	Training Record	Functional Safety Training Evidense.pdf		5/18/2012
[D25]	People Development	PRO-2.0 R16 06-14-13.pdf	16	6/14/2013
[D26]	Training Record	R&D Lab Engineer Training Checklist.doc		
[D27]	Skills Matrix	PRO-0.5 R15 06-14-13.pdf	15	6/14/2013
[D28]	ISO 900x Cert or equivalent	Lloyd's Register - ISO Certificate.pdf		3/1/2012
[D29]	Lifecycle and Functional Safety Management Report (SIRA)	Lifecycle & Functional Safety Management Report.pdf	1	5/25/2012
[D30]	SIRA Functional Safety Certification	SIRA FSP 08002-03 - Functional Safety Certificate - ESD Valve Controller.pdf	3	6/12/2012
[D31]	SIRA Functional Safety Certificate	Sira FSP 08002-04_markup.pdf		8/12/2013
[D32]	List of Design Tools	Inventor, Autocad, ANSIS, EMAG - 7 years		
[D33]	Safety Requirements Specification	ES-04513-1 - Safety Requirement Specification.pdf	1	pending
[D34]	Requirements Traceability Matrix	D-Series Standards.pdf		
[D35]	Validation Test Plan	ESD Conventional Test Report.pdf		5/17/2007

[D36]	Validation Test Plan	OPS-DXP-610 Testing (rev 14) 4_26_10.xlsx	14	
[D37]	Validation Test Plan	Tester_schematic_ver2.pdf	2	
[D38]	Validation Test Plan	TOPWORX D-Series Seat Leak Tester D-sub External wirelist.pdf		10/5/2011
[D39]	Validation Test Plan Review Record	Shop Routing Example.pdf		
[D40]	Environmental Test Plan	Validation Test Plan ESD CONV.xls		4/16/2007
[D41]	SIRA Functional Safety Certificate	Sira FSP 08002-04_markup.pdf		8/12/2013
[D42]	Name of Change Request Tracking System	Manual Tracking by ECO Coordinator		
[D43]	Validation Test Results	Validation Test Plan Results.doc	2	3/6/2008
[D44]	Validation Test Results	640-PST.doc		10/19/07
[D45]	Validation Test Results	644 Hot Cold Test.doc		10/15/07
[D46]	Validation Test Results	Validation Test Plan Results.doc		3/6/08
[D47]	Operation / Maintenance Manual	ES-00936-1 ESD IOM.pdf	14	
[D48]	Operation / Maintenance Manual	ES-00043-1 - Replacement Instructions.pdf	4	
[D49]	Operation / Maintenance Manual	tmp_DXP-ES1GN4B1A2T.pdf		
[D50]	Operation / Maintenance Manual	Operations and Maintenance manual for D-series Tester.docx	xxx	Dec-11
[D51]	Safety Manual	ESD IOM.pdf		
[D52]	Business Case Template	Business Case ESD-PST.pdf		
[D53]	Business Case Template	ES-00449-1.pdf		
[D54]	Pricing Guide and part naming	Leak_ladder_diag_VER3.pdf	19	1-Oct-13
[D55]	Electrical Diagram	CALIBRATION MASTER LIST - D-Series Line.pdf	3	
[D56]	Quality Manual	PRO-1.0 R16 06-14-13.pdf	6	6/14/2013
[D57]	Overall Development Process	Master PPD Template.xls	16	6/14/2013

2.4.2 Documentation generated by *exida*

[R1]	EPM 13-08-108 R002 V1R4 FMEDA report, April 9, 2014	FMEDA report, D-ESD Valve Controller
[R2]	Q13-08-108 EPM D-ESD V1R1 PIU Spreadsheet.xls	IEC 61508 Site Audit Report, Topworx, Inc.
[R3]	EPM 13-08-108 V3 Topworx SafetyCase	IEC 61508 SafetyCaseWB for Topworx D-ESD Valve Controller
[R4]	EPM 13-08-108 R002 V1R4 Topworx D-ESD Assessment, May 5, 2014	IEC 61508 Functional Safety Assessment, Topworx, Inc. Topworx D-ESD Valve Controller (this report)

3 Product Description

The Topworx D-ESD Valve Controller provides two functions. It can be used to automatically or manually initiate a Partial Valve Stroke Test (PVST) as well as an Emergency Shutdown Function (ESD). This assessment only addresses the ESD function as the Safety Function. The PVST function was determined to be non-interfering. Since the PVST function can be automatically initiated, credit was given for PVST as a diagnostic in the FMEDA analysis for that version.

The Topworx D-ESD Valve Controller is a top mounted device that consists of a housing that contains an ESD module, proximity switches, and a solenoid pilot. Mounted external to the enclosure is a 5 port 2 position spool valve. The spool valve is driven by the solenoid pilot. The ESD functions is de-energize to trip. The Topworx D-ESD Valve Controller is not a standalone device. In order to perform the safety function the Topworx D-ESD Valve Controller must be used with spring return actuator and valve.

This assessment is applicable to Topworx D-ESD Valve Controllers using the following solenoid pilots:

- SMC Series SY100
- Amisco 15mm Series
- ASCO 302 Series

Figure 1 Typical Topworx D-ESD Valve Controller covered in this assessment,

Table 1 gives an overview of the different versions that were considered in the FMEDA of the Topworx D-ESD Valve Controller.

Table 1 Version Overview

Option 1	Single acting, spring return actuator application
Option 2	Single acting, spring return actuator application with PVST

The Topworx D-ESD Valve Controller is classified as a component 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

The IEC 61508 Functional Safety Assessment was performed based on the information received from Topworx, Inc. and is documented in this report.

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 5.1. The review of the product design is described in section 5.2.

4.2 Assessment level

The Topworx D-ESD Valve Controller has been assessed per IEC 61508 to the following level:

- Systematic Capability SC3 (SIL 3 capability) as the development procedures were 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 Topworx, Inc. for these products against the objectives of IEC 61508 parts 1 - 7. The assessment was done on-site at the Louisville, Kentucky facility on February 24-25, 2014 and documented in the SafetyCase [R3].

5.1 Lifecycle Activities and Fault Avoidance Measures

Topworx, Inc. has a defined product lifecycle process in place. This is documented in the Quality Management System Manual [D1] and various Quality Procedures [D2-D8]. A documented modification process is also covered in the Quality Manual. 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 Topworx, Inc. 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 Topworx, Inc. design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

The Valve Controllers manufactured by Topworx are not built for inventory. These Controllers are built-to-order. The basic designs are standardized, but each order can have specific customer requests. Due to the specialized nature of each Controller, documentation that defines all of the requirements is generated for every order as part of the process.

<u>FSM Planning</u>

Topworx, Inc. 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 their Quality Management System Manual [D1]. Templates and sample documents were reviews and found to be sufficient. The modification process is covered by PRO-1.0 R16 06-14-13. 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.

<u>Version Control</u>

PRO-1.0 R16 06-14-13, sections 1.2 and 5.1 requires that all documents be under document control. Use of this to control revisions was evident during the audit.

Training, Competency recording

PRO-2.0 R16 06-14-13 requires the Human Resource department to maintain training records of education, experience, training and qualifications for all personnel. Department heads are responsible for identifying and providing the training needs for their department as well as proficiency evaluations. The procedures and records were examined and found up-to-date and sufficient. Topworx 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 safety requirement specification for the Topworx D-ESD Valve Controller is documented in ES-04513-1 [D33]. As the Topworx D-ESD Valve Controller designs are simple and are based upon standard designs with extensive field history, only a semi-formal method is needed. General Design and testing methodology is documented and required as part of the design process. This meets SIL 3.

5.1.3 Hardware Design

The design process is documented in Section 1.0 of [D1]. Items from **IEC 61508-2, Table B.2** include observance of guidelines and standards, (API, PED, ATEX) project management, documentation (design outputs are documented per quality procedures), 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 documented on form Validation Test Plan Results Template which is created for each order. The test plan includes testing per all standard and customer performance requirements. As the Topworx D-ESD Valve Controller's safety function is simple, there is no separate integration testing necessary. The Topworx D-ESD Valve Controller performs 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 Section 1.0 of [D1]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3.

5.1.6 Proven In Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was carried out on the Topworx Topworx D-ESD Valve Controller. Shipment records were used to determine that the D-ESD Valve Controllers have >10 million field unit operating hours and they have demonstrated a field failure rate less than the failure rates indicated in the FMEDA reports. This meets the requirements for Proven In Use for SIL 3.

5.1.7 Modifications

Modifications are initiated per the Engineering Change Order procedure (section 1.3 of [D1]). All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process. This meets SIL 3.

5.1.8 User documentation

Topworx, Inc. creates the following user documentation: product catalogs and a Safety Manual. 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 (Topworx D-ESD Valve Controllers 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 Topworx D-ESD Valve Controller Failure Modes, Effects, and Diagnostic Analysis's were performed 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 [R1]. Tables in the FMEDA report list these failure rates for the Topworx D-ESD Valve Controller under a variety of applications. The failure rates listed are valid for the useful life of the devices.

Note, as the Topworx D-ESD Valve Controller is only one part of the final element of a safety instrumented function, architectural constraints shall be calculated for the entire final element using Route 1_H or Route 2_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 Topworx D-ESD Valve Controller can meet the hardware requirements of IEC 61508, SIL 3 depending on the complete final element design. The Hardware Fault Tolerance, $PFD_{AVG,}$ and Safe Failure Fraction (when not following Route 2_H) requirements of IEC 61508 must be verified for each specific design.

6 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
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 Architectural Constraints 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	Measure of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL.
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:	R4	
Version History:	V1, R4:	Removed HFT references, S. Close May 30, 2014
	V1, R3:	Removed standalone refence. S. close
	V1, R2:	Included Topworx edits, April 8, 2014
	V1, R1:	First Release, March 31, 2014
	V0, R1:	Draft; March 31, 2014
Authors:	Loren Stewart	
Review:	V0, R1:	Gregory Sauk
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Loren L. Stewart, CFSP, Safety Engineer

Gregory Sauk, CFSE, Senior Safety Engineer