IEC 61508 Functional Safety Assessment

Project:
D-ESD Valve Controller

Customer:
Topworx, Inc.
Louisville, Kentucky
USA

Contract Number: Q17/01-120
Report No.: EPM 13/08-108 R002
Version V3, Revision R1, March 31, 2017
Steven Close

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 Route 1_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.

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 Topworx, Inc. D-ESD Valve Controller by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010. 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.

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* agreed with Topworx, 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 and availability with over 400 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 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

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.

Topworx contracted *exida* in July 2015 for the IEC 61508 Functional Safety Assessment of the Go Switch Redesign of the D-ESD Valve Controller.

Topworx contracted *exida* in September 2015 for the IEC 61508 Functional Safety Assessment of the 3rd Party Solenoid Design of the D-ESD Valve Controller.

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.

Doc ID	Generic Document Name	Project Document Name	Version	Date
D001	Quality Manual	Quality Policy Manual.pdf	18	6/15/2016
D003	Overall Development Process	PRO-1.0 R18 06-17-16.pdf	18	6/17/2016
D003b	Development Process Form	Master PPD Template.xls	15	6/8/2016
D004	Configuration Management Process	PRO-1.0 R18 06-17-16.pdf	18	6/17/2016

D005	Field Failure Reporting Procedure	PRO-6.0 R17 12-01-16.pdf	17	12/1/2016
D006	Field Return Procedure	PRO-6.0 R17 12-01-16.pdf	17	12/1/2016
D007	Manufacturer Qualification Procedure	PRO-3.0 R21 05-06-16.pdf	21	5/6/2016
D007b	Sourcing From Approved Vendors	PRO-3.0 R21 05-06-16.pdf	21	5/6/2016
D007c	Approved Supplier List	Approved Supplier List.xls		
D008	Part Selection Procedure	PRO-1.0 R18 06-17-16.pdf	18	6/17/2016
D010	Quality Management System (QMS) Documentation Change Procedure	PRO-5.0 R23 12-07-16.pdf	23	12/7/2016
D012	Non-Conformance Reporting procedure	PRO-6.0 R17 12-01-16.pdf	17	12/1/2016
D013	Non-Conformance Reporting procedure	PRO-6.0 R17 12-01-16.pdf	17	12/1/2016
D016	Action Item List Tracking Procedure	PRO-1.0 R18 06-17-16.pdf	18	6/17/2016
D019	Customer Notification Procedure	PRO-6.0 R17 12-01-16.pdf	17	12/1/2016
D023	Modification Procedure	PRO-1.0 R18 06-17-16.pdf	18	6/17/2016
D023b	Impact Analysis Template	Functional Safety Impact Analysis Report.pdf		
D023c	Engineering Change Form	ECO Form.pdf		
D023d	Engineering Change Form	Engineering Change Order R46.pdf		
D023e	Go Switch Modification Impact Analysis	ES -05425-1 TopWorx Impact Analysis Report for ESD Re-Design.pdf	01	11/19/2015
D026	FSM Plan or Development Plan	PRO-0.5 Business Management Plan R15 06-14-13.pdf	15	6/14/2013
D026b	FS Organization Chart	Functional Safety Organizational Chart.pdf		
D026c	FS Policy	Functional Safety Policy.pdf		
D027	Configuration Management Plan	PRO-1.0 R18 06-17-16.pdf	18	6/17/2016
D030	Shipment Records	Topworx ESD-series shipments.pdf		
D031	Field Returns Records	Coil & Spool Application failures.pdf		
D031b	Field Returns Records	Coil Failures.pdf		
D031c	Field Returns Records	Spool failures.pdf		
D032	Firmware Engineer Job Description	FIRMWARE ENGINEER Job Description 2012.pdf		2012

D032b	Manager, Technical Service Job Description	Manager, Technical Service Job Description ACTIVE.DOCX		7/8/2013
D032c	Quality Manager Job description	Quality Manager JD FY12 - EXTERNAL.DOC		7/3/1905
D032d	Manufacturing Engineering Supervisor Job Description	Manufacturing Engineering Supervisor 2013.doc		7/5/1905
D032e	Valvetop & Wireless Product Manager	Manager, Valvetop & Wireless Product Manager Job Description ACTIVE.DOCX		7/5/1905
D032f	Manufacturing Engineer Supervisor Job Description	Manufacturing Engineering Supervisor 2013.doc		7/5/1905
D033	Training Record	Functional Safety Training Evidense.pdf		5/18/2012
D033b	People Development	PRO-2.0 R17 11-25-14.pdf	17	11/25/2014
D033c	Training Record	R&D Lab Engineer Training Checklist.doc		
D034	Skills Matrix	PRO-0.5 R17 06-14-16.pdf	17	6/14/2016
D036	ISO 900x Cert or equivalent	Lloyd's Register - ISO Certificate.pdf		3/1/2012
D036b	Lifecycle and Functionl Safety Management Report (SIRA)	Lifecycle & Functional Safety Management Report.pdf	1	5/25/2012
D036c	SIRA Functional Safety Certification	SIRA FSP 08002-03 - Functional Safety Certificate - ESD Valve Controller.pdf	3	6/12/2012
D036d	SIRA Functional Safety Certificate	Sira FSP 08002-04_markup.pdf		8/12/2013
D036e	ISO 900x Cert or equivalent	Shenzhen Manufacturing Site ISO Cert		1/28/2015
D036f	ISO 900x Cert or equivalent	Szekes ISO Cert		3/1/2012
D036g	ISO 900x Cert or equivalent	Fisher Controls International LLC ISO 9001:2008		10/18/2015
D038	List of Design Tools	Inventor, Autocad, ANSIS, EMAG - 7 years		
D040	Go Switch Redesign Schematics	ES-05078-1_DRAFT_REV B.pdf	B	pending
D040b	Go Switch Redesign Product Specifications	ES-05422-1 Product Specifications for D-ESD Re-Design Assembly.pdf	01	11/25/2015
D040c	3rd Part Solenoid Diagram	CERT-ES-05424-1.pdf	1	11/25/2015
D040d	3rd Part Solenoid Explanation	ES-05423-1 Product Identifiers for Third Party Solenoid.doc	1	10/22/2015

D040e	Safety Requirements Specification Redesign	ES-05421-1 Specific Product Identifiers for D-ESD Product Variants.pdf	01	11/25/2015
D040f	Safety Requirements Specification	ES-05421-1 Specific Product Identifiers for D-ESD Product Variants.pdf	1	2/28/2015
D055	FMEDA Report	EPM 14-08-108_R001 V1R1_FMEDA Topworx.pdf		
D056b	Requirements Traceability Matrix	D-Series Standards.pdf		
D069	Validation Test Plan	ESD Conventional Test Report.pdf		5/17/2007
D069b	Validation Test Plan	OPS-DXP-610 Testing (rev 14) 4_26_10.xlsx	14	
D069c	Validation Test Plan	Tester_schematic_ver2.pdf		
D069d	Validation Test Plan	TOPWORX D-Series Seat Leak Tester D-sub External wirelist.pdf		10/5/2011
D069e	Go Switch Re-design Prototype Functional Validation Test Plan	ESD RE-Design Prototype Functional Template.xlsx		9/15/2006
D070	Validation Test Plan Review Record	Shop Routing Example.pdf		
D071	Environmental Test Plan	Validation Test Plan ESD CONV.xls		4/16/2007
D071b	Go Switch Re-Design Environmental Test Plan	Validation Test Plan for ESD Re-Design Exida.xls		4/16/2007
D072	SIRA Functional Safety Certificate	Sira FSP 08002-04_markup.pdf		8/12/2013
D073	Name of Change Request Tracking System	Manual Tracking by ECO Coordinator		
D074	Validation Test Results	Validation Test Plan Results.doc		3/6/2008
D074b	Validation Test Results	640-PST.doc		10/19/2007
D074c	Validation Test Results	644 Hot Cold Test.doc		10/15/2007
D074d	Validation Test Results	Validation Test Plan Results.doc		
D074e	Validation Functional Test Results GO Switch Redesign	1293.pdf		7/13/2015
D074f	Validation Storage Temperature Test Results GO Switch Redesign	1294.pdf		7/30/2015
D074g	Validation Functional Results GO Switch Redesign	1305.pdf		8/28/2015
D074h	Validation Temperature Cycle Tests GO Switch Redesign	1295.pdf		8/28/2015

D074i	Validation Operating Temperature Tests GO Switch Redesign	1295.pdf		8/28/2015
D078	Operation / Maintenance Manual	ES-00936-1 ESD IOM.pdf	17	
D078b	Operation / Maintenance Manual	ES-00043-1 - Replacement Instructions.pdf	4	
D078c	Operation / Maintenance Manual	tmp_DXP-ES1GN4B1A2T.pdf		
D078d	Operation / Maintenance Manual	Operations and Maintenance manual for D-series Tester.docx	xxx	Dec-11
D079c	Safety Manual	ES-05481-1 ESD Re-Design Safety Manual.doc	01	11/25/2015
D083	EPM 17-01-120 D-ESD PIU	PIU Analysis		3/15/2016
D089	Business Case Template	Business Case.xls		
D089b	Business Case Template	Business Case ESD-PST.pdf		
D090	Pricing Guide and part naming	ES-00449-1.pdf		1-Oct-13
D091	Electrical Diag	Leak_ladder_diag_VER3.pdf	3.00	
D092	Calibration Master List	CALIBRATION MASTER LIST - D-Series Line.pdf		

Note: Documents highlighted in gray were reviewed as part of the Go Switch and 3rd Party Solenoid redesigns.

2.4.2 Documentation generated by *exida*

[R1]	EPM 13-08-108 R002 V2R1 FMEDA report, November 24, 2015.	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 V4 Topworx SafetyCase	IEC 61508 SafetyCaseWB for Topworx D-ESD Valve Controller
[R4]	EPM 13-08-108 R002 V3R1 Topworx D-ESD Assessment.doc, August 25, 2016	IEC 61508 Functional Safety Assessment, Topworx, Inc. Topworx D-ESD Valve Controller (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 Topworx, Inc..

The following IEC 61508 objectives were subject to detailed auditing at Topworx, 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 architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
    - Integration and fault insertion test strategy
- Hardware-related operation, installation and maintenance requirements

3 Product Description

The 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). The FMEDA addresses the ESD function as the PVST function was determined to be non-interfering. The PVST function can be automatically initiated; therefore, credit was given for PVST as a diagnostic. The D-ESD Valve Controller is an actuator 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 function is de-energize to trip. The D-ESD Valve Controller is not a standalone element. In order to perform the final element safety function, the D-ESD Valve Controller must be used with spring return actuator and valve.

The following cube assemblies are included in the assessment:

Model Designation	Description	Cube Assembly
DXP/S-ESXXXXXXXXYX	Integrated Solenoid	ES-00921-1
DXP/S-ESXXXXXXXXYXZZZZ	Integrated Solenoid	ES-05078-1
DXP/S-ESXXXXX000YX	3rd Party Solenoid	ES-00921-1
DXP/S-ESXXXXX000YXZZZZ	3rd Party Solenoid	ES-05078-1

The main difference in the cube design is the mating with different switch technologies. The design of the safety function is the same for either cube.

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

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

A configuration that uses a 3rd party solenoid is also available. 3rd party solenoids selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall meet the requirements of IEC 61511, 1st Edition, paragraph 11.5.2.

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	Integral solenoid, single acting, spring return actuator application
Option 2	Integral solenoid, single acting, spring return actuator application with PVST
Option 3	3rd Party Solenoid, spring return actuator application
Option 4	3rd Party Solenoid, 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].

This assessment includes the redesign of the cube to accommodate Go Switches as well as the 3rd part solenoid design. This revised designs do not change the emergency shutdown function.

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 D001 and various Quality Procedures [D003-D023]. 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.

FSM Planning

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 [D001]. 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.

Version Control

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 [D040f]. 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 [D001]. 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 [D001]. 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 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. Since the execution of the safety function for the design that uses the ES-05078-1 is the same as the safety execution for the originally assessed design, the proven in use analysis is also applicable to the ES-05078-1 cube.

5.1.7 Modifications

Modifications are initiated per the Engineering Change Order procedure (section 1.3 of [D001]). 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 user's 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 2017 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Topworx, Inc.	Manufacturer of the D-ESD Valve Controller
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Topworx contracted *exida* in February 2017 to perform the surveillance audit for the above Topworx D-ESD Valve Controller. The surveillance audit was conducted remotely in February and March of 2017.

6.2 Surveillance Methodology

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

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if an of the changes could affect the safety function of the Topworx D-ESD Valve Controller.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the exida Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.

6.2.1 Surveillance Documentation generated by *exida*

[R5]	EPM 13-08-108_R001 V3R2_FMEDA_Topworx.pdf	FMEDA report, D-ESD Valve Controller
[R6]	EPM 13-08-108 R4 Topworx Safety Case.xlsm	IEC 61508 SafetyCaseDB for Topworx D-ESD Valve Controller

6.3 Surveillance Results

6.3.1 Procedure Changes

Changes to the documents highlighted in section 2.4.1 were reviewed and were found to be consistent with the requirements of IEC 61508.

6.3.2 Engineering Changes

A list of engineering changes was reviewed. It was determined that none of the changes affected the safety function of the D-ESD Valve Controller.

6.3.3 Impact Analysis

Not Applicable.

6.3.4 Field History

Shipping and warrantee field return data was reviewed. A failure rate analysis was performed based on the shipping and field return information. The failure rate of the D-ESD Valve Controller was determined to be consistent with the failure rates reported in the FMEDA analysis.

6.3.5 Safety Manual

The latest version of the safety manual, D079c was reviewed and was found to meet the requirements of IEC 61508 for a functional safety manual.

6.3.6 FMEDA Update

The FMEDA analysis was updated using the failure rate that will be published in edition 4 of the Mechanical Component Reliability Handbook. The revised FMEDA includes failure rates for both static and dynamic applications. Failure rates for Site Safety Index 2 & 4 were added to the FMEDA report. See the FMEDA report for an explanation of static and dynamic applications as well as the Site Safety Index.

6.3.7 Evaluate use of certificate and/or certification mark.

The use of the SIL certification and/or certification mark on the Topworx (http://www.emerson.com/en-us/automation/topworx) website was reviewed. The SIL certificate

appears in the Master Installation, Operation & Maintenance Manual is a section dedicated to emergency shutdown. This is consistent with the terms in the Certification Agreement.

6.3.8 Previous Recommendations

There were no recommendations from the last audit that are required for this audit.

7 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

8 Status of the Document

8.1 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.

8.2 Releases

Version History:	V3, R1:	Revised per surveillance audit, S. Close
	V2, R2:	Revised Safety Manual Number, S. Close. 8/25/2016
	V2, R1:	Added re-designed cube & 3rd party solenoid configurations, S. Close
	V1, R4:	Removed HFT references, S. Close May 5, 2014
	V1, R3:	Removed standalone reference. S. close
	V1, R2:	Included Topworx edits, April 8, 2014
	V1, R1:	First Release, March 31, 2014
	V0, R1:	Draft; March 31, 2014
Authors:	Steven Close	
Review:	V0, R1:	Gregory Sauk
Review:	V2, R1:	Ted Stewart
Review:	V3, R1:	Ted Stewart
Release status:	Released	

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Steven Close, Senior Safety Engineer

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