IEC 61508 Functional Safety Assessment

Project:

A, B, D & T Series Pressure Switch

Customer:

Ashcroft Inc.

Stratford, CT

USA

Contract Number: Q23/01-193

Report No.: ASH 16-02-007 R002

Version V3, Revision R1, June 2, 2023

Casimir Musa

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the A, B, D & T Series Pressure Switch

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

- *exida* assessed the development process used by Ashcroft 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* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Ashcroft.

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 Ashcroft Inc. A, B, D & T Series Pressure Switch 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 A, B, D & T Series Pressure Switch can be used in a high or low demand safety related system in a manner where the PFH/ PFD_{avg} meets the requirements of table 2 or table 3 of IEC 61508-1.

The assessment of the FMEDA also shows that the A, B, D & T Series Pressure Switch 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 A, B, D & T Series Pressure Switch 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.


exida
CERTIFIED
IEC 61508
SIL 3 CAPABLE

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Ashcroft Inc.: A, B, D & T Series Pressure Switch

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 out 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 Ashcroft Inc..

All assessment steps were continuously documented by *exida* (see [R1] to [R6])

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 500 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 350 billion hours of field failure data.

2.2 Roles of the parties involved

Ashcroft Inc.	Manufacturer of the A, B, D & T Series Pressure Switch
exida	Performed the hardware assessment
exida	Performed the IEC 61508 Functional Safety Assessment per the accredited *exida* scheme.

Ashcroft contracted *exida* in 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

Note: Documents listed below have been reviewed and confirmed to be the latest revisions during this surveillance audit. Items highlighted in Grey have been revised since the last audit.

2.4.1 Documentation provided by Ashcroft Inc.

Doc ID	Generic Document Name	Project Document Name	Rev	Date
D001	Quality Manual	QSM	18	28-Feb-2022
D003	Overall Development Process	EOP 1 O, Product Development	T	22-Jul-2022
D004b	Configuration Management Process – Template	EOP1-CMP, Configuration Management Plan	1	07-Jul-2016
D005	Field Failure Reporting Procedure	QAOP 6 Customer Complaints	C	18-Aug-2014

D005b	Field Failure Reporting Procedure – Issuing RMAs	050-RET-002, Issuing RMA Inside Sales.pdf	E	3/29.2017
D005c	Field Failure Reporting Procedure – Entering Comments in RMAs	050-RET-003, Entering Comments in RMAs	D	29-Mar-2017
D005d	Field Failure Reporting Procedure – Receipt of RMAs	050-RET-004, Receipt of RMA	G	24-Jan-2019
D005e	Field Failure Reporting Procedure – Returns process Roles	050-RET-100, Return Process Roles & Responsibilities	D	30-Aug-2018
D006	Field Return Procedure	QAOP 23 Returned Goods	D	18-Mar-2022
D007	Manufacturer Qualification Procedure	POP 2 Supplier Selection	G	28-May-2015
D008	Part Selection Procedure	QAOP 20 Control of Age Sensitive Material	G	09-May-2022
D009	Part/Products Qualification Procedure	QAOP 21 First Article Approval	J	02-Mar-2022
D010	Quality Management System (QMS) Documentation Change Procedure	ADMOP 1, Operating Procedure Control	H	28-Jan-2022
D011	Control of Design Records	EOP 17, Engineering Documentation Requirements	L	31-Aug-2016
D012	Non-Conformance Reporting procedure	MOP 5 Non-conforming Matl	K	01-Apr-2022
D013	Corrective Action Procedure	ADMOP 4, Corrective & Preventive Action	N	19-May-2021
D013b	Sample Corrective Action Report	CAR 150415	EM	15-Apr-2015
D015	Internal Audit Procedure	ADMOP 3 Internal Audits	I	21-May-2021
D016b	Action Item List Tracking Procedure	EOP1-ACT Action Item List Template v1.2.	1.3	21-Feb-2021
D017	Training Procedure	ADMOP 2, Training	O	27-Apr-2021
D018	Test Equipment Calibration Procedure	QAOP 4, Cont of Dim Meas Inst & Equip	S	06-Dec-2021
D019	Customer Notification Procedure	QAOP 27, Customer Notification Procedure	D	22-Feb-2022
D020	Management Review Process	ADMOP 6, Mngt Review	H	22-Feb-2022
D023	Modification Procedure	EOP 2 , Dwg Changes Releases	X	15-Nov-2022
D23b	Impact Analysis Template	EOP1-IAR TK	1.3	21-Jun-2022

D026	FSM Plan Series B	List of Personnel Responsible for the B Series Switches.		8/16/2014
D26b	FSM Plan Series A	Stage 2 Evaluation Team Assignment.doc		7/14/2011
D26c	FSM Plan Series A	Team Charter for A Series Switch Project.xls		1/7/2011
D030	Shipment Records	A & B Series Switch Return Data 2023.xlsx		5/2023
D031	Field Returns Records	A & B Series Switch Return Data 2023.xlsx		5/2023
D032	Job Descriptions and Competency Levels	Job Descriptions and Competency Levels		Folder
D033	Training Record	Dept 905 Training		1/9/2013
D034	Skills Matrix	Copy of Competency Matrix Rev C 1-14-2016.xlsx		
D036	ISO 900x Cert or equivalent	ISO 900x Cert		Folder
D039	Management Review Record	Ashcroft Mgmt Review		12/15/2011
D040	Safety Requirements Specification	datasheet-b-series.pdf	Rev J	21-Oct-2022
D040b	Safety Requirements Specification	datasheet-b-series-temp.pdf	Rev J	21-Oct-2022
D040c	Safety Requirements Specification	datasheet_b_series_press_diff.pdf	Rev J	21-Oct-2022
D40d	Safety Requirements Specification	A-Series Spec 10-23-2012.xls	Rev E	
D40e	Safety Requirements Specification	A-Series Spec-Scope.ppt		7/14/2011
D053	Design Review Record	Design_Review_Records		Folder
D054	Verification Results	A-Series Verification Results		Folder
D069	Validation Test Plan	B Series Sil – High Pressure Test Plan.pdf	A	
D069b	Validation Test Plan	A Series Test Plan		1/25/2011
D071	Environmental Test Plan	B Series SIL – Test Plan Requirements.pdf		
D074	Validation Test Results	B Series Sil – High Pressure Test Plan.pdf	A	
D074b	Validation Test Results	A-Series Product Performance Report.docx.docx		1/30/2012
D075	Environmental Test Results	B Series SIL – Test Plan Requirements.pdf		

D075b	Environmental Test Results	13-192 A Series Switch Conduit Temp Test Report.pdf		4/11/2013
D078	Operation / Maintenance Manual	I&M009-10010-10-00 250-2367D.pdf		
D078b	Operation / Maintenance Manual	manual-B400XG6-B700XG6-SnapAct.pdf		01-Jul-2007
D078c	Operation / Maintenance Manual	manual-D0230-D700-LR-DifControl.pdf		01-Dec-2007
D078d	Operation / Maintenance Manual	manual-pressure-switch-B400-B700-SnapAct.pdf		01-Dec-2015
D078e	Operation / Maintenance Manual	manual-pressure-switch-b400-XGR-SnapAction.pdf		01-Apr-2006
D078f	Operation / Maintenance Manual	manual-pressure-switch-D0230-D700-DP-Switch.pdf		01-Dec-2007
D078g	Operation / Maintenance Manual	manual-pressure-switch-T400-T700.pdf	Rev A	24-Mar-2017
D078h	Operation / Maintenance Manual	I&M009-10046 manual-pressure-explosion_switches_a_n7.pdf	Rev D	03-May-2021
D078i	Operation / Maintenance Manual	I&M009-10045 manual-pressure-switches-A-N4-WTI.pdf	Rev F	22-Feb-2023
D079	Safety Manual	I&M900-10253 B-series Pressure Switch Safety Manual	A	24-Mar-2017
D079b	Safety Manual	I&M009-10210 manual-pressure-switches-A-N4-EXP-Safety.pdf	Rev A	19-Apr-2013
D088	Impact Analysis Record	B Series Sil – High Pressure Test Plan.pdf	A	
D088b	Impact Analysis Record	B Series SIL – Test Plan Requirements.pdf		
D088c	Impact Analysis Records	Series A Impact_Analysis_Records		Folder
D089	Impact Analysis Records	IAR-13390 A Series Impact Analysis	A	12/5/2022
D090	Impact Analysis Records	IATP-13390 A Series Impact Analysis Test Plan and Report	Rev 1	12/6/2022
D091	Impact Analysis Records	IAR-13389 A Series Impact Analysis	A	12/5/2022
D092	Impact Analysis Records	IATP-13389 A Series Impact Analysis Test Plan and Report	Rev 1	12/6/2022
D093	A Series Calibration Procedure	196-A-113, APS Calibration	C	7/17/2015
D094	A Series Calibration Procedure	196-A-113B, APA Calibration	B	7/17/2015

D095	Calibration Report	196-046, Calibration Report (XCA4)	H	4/5/2013
D096	B4 Assembly & Calibration Procedure	196-B-400, B4 Switch Calibration & Assembly	C	9/22/2020
D097	Calibration Record	Example Certified Calibration Chart -30390038		5/8/2023
D098	Calibration Record	Master Calibration Record - 0424		
D099	Test Equipment Calibration Procedure	QAOP 5 Cont of Pres Tem & Elec Mea Std	Q	12/11/2021
D100	Design Review	N4 - Design Changes		
D101	Design Review	A-Series Watertight Assembly Drawing - 50C411	P	11/22/2022
D102	Design Review	A-Series Explosion-Proof Assembly Drawing - 50C412	E	4/7/2021

2.4.2 Documentation generated by *exida*

[R1]	ASH Q12-07-077 R001 V2R1 A-Series FMEDA Report	FMEDA Report, A-Series Pressure Switch
[R2]	ASH 16-02-007 R001 V1R2 B-Series FMEDA Report	FMEDA Report, B-D-T Series Pressure Switches
[R3]	ASH 16-02-007 r1 Series A, B, D & T Pressure Switch Safety Case.xlsm	IEC 61508 SafetyCaseDB for A, B, D & T Series Pressure Switch
[R4]	ASH 15-09-123 V2R1 IEC 61508 SafetyCaseWB - E2 Pressure Transducer.xxlsm	IEC 61508 Ashcroft Baseline SafetyCase
[R5]	ASH 23-01-193 ABDT Switches PM Workbook	2023 Surveillance Audit Project Management Workbook
[R6]	ASH 23-02-193 FFA Switches ABDT	2020 – 2023 Field Failure Analysis (Internal Document)

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 Ashcroft Inc..

The following IEC 61508 objectives were subject to detailed auditing at Ashcroft 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 Descriptions

The A, B, D & T Series Pressure Switch are externally mounted to pressure applications to activate (or deactivate) at a pre-determined pressure. The pressurized media enters the product by means of a process connection.

The A, B, D & T Series Pressure Switch are actuated via a pressure input at a pressure fitting. These fittings can vary in size and type of thread or connection based on the needs of the end user. The media can be liquid or gas and the activation pressure can be set from -30” Hg vacuum up to 7500 psi depending on the product configuration. Once the pressurized media enters the pressure fitting it is sensed by the actuator seal. This actuator seal varies based on seal type and desired pressure range.

The Temperature Switches (T) utilize a gas filled thermal well to provide the pressure to operate the switch(s).

The setpoint for the A, B, D & T Series Pressure Switch can be either factory set or field adjustable.

Both single and dual switches are available. When dual switches are used in a non-redundant application the failure rates for a single switch are applicable.

The safety function of the A, B, D & T Series Pressure Switch is to de-energize the associated circuit on a trip. The de-energized switch position is with the NC switch contact open on a high pressure trip and with the NO switch contact open on a low pressure trip.

Table 1 Model Overview

Model	Description
A N4	Miniature Watertight Pressure Switch
A N7	Explosion Proof Pressure Switch
B400	Pressure Switch Watertight Enclosure
B700	Pressure Switch plosion-Proof Enclosure
D400	Differential Pressure Switch Watertight Enclosure
D700	Differential Pressure Switch plosion-Proof Enclosure
T400	Temperature Pressure Switch Watertight Enclosure
T700	Temperature Pressure Switch Explosion-Proof Enclosure

Figure 1(a) ***B-D-T Series Pressure Switch***

Figure 1(b) ***A-Series Pressure Switch***

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Ashcroft 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 [R5].

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 A, B, D & T Series Pressure Switch 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 Ashcroft Inc. for these products against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 see [N1]. The development of the A, B, D & T Series Pressure Switch was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Ashcroft Inc. has a defined product lifecycle process in place. This is documented in the Quality Management System Manual [D001] and various Quality Procedures. A documented modification process is also covered in EOP 2 [D023]. 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 the *exida* certification scheme which includes subsets of 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 Ashcroft Inc. design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3 .

5.1.1 Functional Safety Management

The switches manufactured by Ashcroft are not built for inventory. These switches are built-to-order. The basic designs are standardized, but each order can have trim and materials variations or specific customer requested configurations.

FSM Planning

Ashcroft 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 EOP 1 [D003]. Templates and sample documents were reviewed and found to be sufficient. The modification process is covered by EOP 2 [D023]. 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

ADMOP 1 [D010] requires that all documents be under document control. Use of this to control revisions was evident during the audit.

Training, Competency recording

ADMOP 1 [D017] requires that each department supervisor shall assure that training is provided for all personnel so they understand and are able to perform their job tasks satisfactorily The procedures and records were examined and found up-to-date and sufficient. Ashcroft 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

For the A, B, D & T Series Pressure Switch, the simple primary functionality of the switch is the same as the safety functionality of the product. Therefore, no special Safety Requirements Specification was needed. The normal functional requirements were sufficient. As the A, B, D & T Series Pressure Switch designs are simple and are based upon standard designs with extensive field history, no semi-formal methods are 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 EOP 1, [D003] which includes a flowchart of the design process. The design process contains 5 Stage Gates. Activities and deliverables are defined for each stage. Each stage is signed off before proceeding to the next stage. Stage Gate signoffs and meeting notes were submitted in evidence. Items from **IEC 61508-2, Table B.2** include observance of guidelines and standards, 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 in [D069] which lists the tests to be performed. Testing covers environmental conditions such as temperature extremes, shock and vibration. A test report [D074] is created to document test results. The report includes product description, test setups, and test results. As the A, B, D & T Series Pressure Switch are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The A, B, D & T Series Pressure Switch 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 carried out during Stage Gate 3 of EOP-1. 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 Ashcroft A, B, D & T Series Pressure Switch. Shipment records were used to determine that the A, B, D & T Series Pressure Switch have >300 million hours in use 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 Drawing Changes and Releases procedure, EOP 2, [D023 Engineering changes are processed and tracked in the Engineering Central suite of the Enovia web-based software. 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.

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

- As part of the *exida* scheme a surveillance audit is conducted every 3 years. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.
    - List of all anomalies reported
    - List of all modifications completed
    - Safety impact analysis which shall indicate with respect to the modification:
        - The initiating problem (e.g. results of root cause analysis)
        - The effect on the product / system
        - The elements/components that are subject to the modification
        - The extent of any re-testing
    - List of modified documentation
    - Regression test plans

This meets SIL 3.

5.1.8 User documentation

Ashcroft 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 (A, B, D & T Series Pressure Switch 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 A, B, D & T Series Pressure Switch Failure Modes, Effects, and Diagnostic Analysis's were performed by *exida*. These are documented in [R1] & [R2].

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 reports [R1] & [R2]. Tables in the FMEDA report list these failure rates for the A, B, D & T Series Pressure Switch 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 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2.

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 61508-2.

The failure rate data used for this analysis meets the *exida* criteria for Route 2_H. Therefore, the A, B, D & T Series Pressure Switch 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.

Note, as the A, B, D & T Series Pressure Switch are only one part of a (sub)system, the SFF should be calculated for the entire final element combination.

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 A, B, D & T Series Pressure Switch can meet the hardware requirements of IEC 61508, 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 2023 IEC 61508 Functional Safety Surveillance Audit

6.1 Roles of the parties involved

Ashcroft Inc.	Manufacturer of the A, B, D & T Series Pressure Switch
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Ashcroft Inc. contracted *exida* in May 2023 to perform the surveillance audit for the above A, B, D & T Series Pressure Switch. A surveillance audit was recently completed for the Ashcroft Inc. process, so this assessment was limited to a product specific review.

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 any of the changes could affect the safety function of the A, B, D & T Series Pressure Switch.
- 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.

6.3 Surveillance Results

6.3.1 Procedure Changes

There were no significant (to functional safety) changes to the procedures during the previous certification period.

6.3.2 Engineering Changes

exida reviewed two engineering changes to these products, and they were found to not impact functional safety. The changes were revalidated, and the results were found to be within the acceptable ranges.

6.3.3 Impact Analysis

There were no safety-related design changes during the previous certification period.

6.3.4 Field History

The field histories of these products were analyzed and found to be consistent with the failure rates predicted by the FMEDA.

6.3.5 Safety Manual

The safety manuals were not modified since the last assessment, so it is still compliant with the relevant requirements of IEC 61508.

6.3.6 FMEDA Update

There were no updates to the FMEDA during the previous certification period.

6.3.7 Previous Recommendations

There were no previous recommendations to be assessed at this audit.

6.4 Surveillance Audit Conclusion

The result of the Surveillance Audit Assessment can be summarized by the following observations:
The Ashcroft Inc. A, B, D & T Series Pressure Switch continue to meet the relevant requirements of IEC 61508:2010 for SIL 2 @ HFT = 0 (SIL 3 @ HFT=1) in low demand applications based on the initial assessment and considering:

- field failure history

- Updated process documents

-Engineering Changes

This conclusion is supported by the updated Safety Case and other certification documents.

7 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

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 Version History

Contract Number	Report Number	Revision Notes
Q16/02-007	ASH 16/02-007 R002 V0, R1	Draft
Q16/02-007	ASH 16/02-007 R002 V1, R1	Release
Q19/07-029	ASH 16/02-007 R002 V2, R1	Added Series A to the Series B, D & T Assessment Report
Q23/01-193	ASH 16/02-007 R002 V3, R1	Updated per Surveillance audit; 6/2/2023 - CAM

Reviewer: Bob Gavin, exida, 6/2/2023

Status: Released, 6/2/2023

8.3 Future Enhancements

At request of client.

8.4 Release Signatures

Casimir Musa, CFSP, Evaluating Assessor

Rober Gavin III, MSME, CFSE, Senior Safety Engineer, Certifying Assessor