IEC 61508 and ISO 13849 Functional Safety Assessment

Project:

Precision Sensors W Series Pressure Switch

Customer:

Precision Sensors

Milford, Connecticut

USA

Contract Number: Q19/02/138

Report No.: 002

Version V1, Revision R1, January 7, 2020

Brad Hitchcock

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 and ISO 13849 carried out on the W Series Pressure Switch.

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

- *exida* assessed the development process used by Precision Sensors through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508 and ISO 13849. The investigation was executed using subsets of the IEC 61508 and ISO 13849 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 Precision Sensors.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 3 and ISO 13849: ed3, 2015, PL e for mechanical and electrical components. A full IEC 61508 and ISO 13849 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 Precision Sensors W Series Pressure Switch development project, complies with the relevant safety management requirements of IEC 61508 SIL 3, **SC 3 (SIL 3 Capable) as well as ISO 13849 PL e (PL e capable).**

The assessment of the FMEDA, done to the requirements of IEC 61508 and ISO 13849, has shown that the Precision Sensors W Series Pressure Switch can be used in a high demand safety related system in a manner where the PFH is within the allowed range for up to SIL 2 according to table 3 of IEC 61508-1 and PL d according to ISO 13849-1..

The assessment of the FMEDA also shows that the Precision Sensors W Series Pressure Switch meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 / PL d safety function (with HFT = 0) or a SIL 3 / PL e safety function (with HFT = 1).

This means that the Precision Sensors W Series Pressure Switch is capable for use in SIL 3 / PL e 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 3.1 of this document.

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

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Precision Sensors W Series Pressure Switch by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010 and ISO 13849, ed3, 2015.

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 / ISO 13849 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 and ISO 13849.

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 Precision Sensors.

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 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

Precision Sensors	Manufacturer of the Precision Sensors W Series Pressure Switch
exida	Performed the hardware assessment
exida	Performed the IEC 61508 and ISO 13849 Functional Safety Assessment per the accredited *exida* scheme.

Precision Sensors contracted *exida* in October 2019 for the IEC 61508 and ISO 13849 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
[N2]	ISO 13849 Part 1: 2015	Safety of Machinery – Safety-Related Parts of Control Systems

2.4 Reference documents

2.4.1 Documentation provided by Precision Sensors

[D1]	QAM 010 / 17-017, Sep 11, 2017	Quality Assurance Manual
[D2]	SOP 7.3, Rev A, Sep 26, 2011	Design and Development
[D3]	W.I.3.1 S&C, Rev A, Nov 7, 2008	Type 1 Development Program - Semiconductor & Commercial
[D4]	W.I. 3.2, Rev F, March 24, 2016	Type 2 Development Program
[D5]	SOP 4.2.3, Rev B, Sept. 27, 2019	Control of Documents
[D6]	ES12, Rev H, July 13, 2015	Engineering Document / Change Control
[D7]	ES17, Rev -, Dec 18, 2003	Configuration Management
[D8]	WI 8.3, Rev ORG, Sept. 2, 2005	Completion of Discrepant Material Report (DMR)
[D9]	Letter CPAR RMR, Dec 11, 2019	RMA Log
[D10]	SOP 7.4, Rev K, Aug 31, 2019	Purchasing
[D11]	W.I. 5.1, Rev A, Sep 19, 2003	Document Change Notice (DCN)
[D12]	SOP 8.3, Rev I, Sep 26, 2019	Control of Nonconforming Product
[D13]	SOP 8.5.2, Rev D, Sep 01, 2015	Corrective Action
[D14]	SOP 8.5.3, Rev A, Dec 10, 2012	Preventative Action
[D15]	WI 21.6, Rev ORG, May 9, 2000	Customer Notification (Customers, FAA, Government)
[D16]	Engineering Form #546, Nov 2019	Impact Analysis Template
[D17]	W.I.3.1 S&C, Rev A, Nov 7, 2008	Type 1 Development Program - Semiconductor & Commercial
[D18]	W.I. 3.2, Rev F, March 24, 2016	Type 2 Development Program
[D19]	PIU Analysis.xlsx	Shipment Records
[D20]	99-1583-05_United_Electric_Controls.pdf	ISO 900x Cert or equivalent
[D21]	W Series Product Specifications, Dec 30, 2019	Safety Requirements Specification
[D22]	EM342, Rev -, Oct 19, 2016	FMEA/MTBF: P48W-138
[D23]	D608B, Dec 11 2018	W Series 1MPa Design Pressure and Burst Pressure Validation
[D24]	TP 346, Oct 2, 2018	E36W-42 – Test Sheet
[D25]	TP 346, May 14, 2019	E36W-42 – Test Sheet
[D26]	TP 346, July 26, 2019	E36W-L30 – Test Sheet
[D27]	TP 344, November 29, 2018	PV48W-68 – Test Sheet

[D28]	W Series Installation and Maintenance Instructions, Dec 12, 2019	Operation / Maintenance Manual
[D29]	Safety Manual W Series Pressure Switch, Dec 30, 2019	Safety Manual

2.4.2 Documentation generated by *exida*

[R1]	PRS 19-02-138 R001 V1R2 W Series FMEDA Report	1 FMEDA report, W Series
[R2]	PRS 19-02-138 R002 V1R2 W Series Assessment Report	IEC 61508 Site Audit Report, Precision Sensors
[R3]	Precision Sensors Final Safety Case	IEC 61508 SafetyCaseDB for Precision Sensors W Series Pressure Switch

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508 and ISO 13849.

The assessment was planned by *exida* and agreed upon by Precision Sensors.

The following IEC 61508 and ISO 13849 objectives were subject to detailed auditing at Precision Sensors:

- FSM planning, including
  - Safety Life Cycle definition
  - Scope of the FSM activities
  - Documentation
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- 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
- Software and system related V&V activities including documentation, verification
- System Validation including hardware
- Hardware-related operation, installation and maintenance requirements

3 Product Descriptions

The safety function of the W Series Pressure Switch is to switch when a set point is reached.

Switches are designed specifically for equipment where cleanliness, reliability and performance are critical. This includes applications such as pressure and vacuum interlocks, atmospheric sensing for chamber door interlocks, gas delivery system alarms and shutdown, gas regulator failure alarm and absolute pressure sensing for process interlocks.

Operating temperatures range from 0°F to 130°F.

3.1 Version Numbers

This assessment is applicable to the following hardware versions of W Series Pressure Switch:

- P17
- P36
- P48
- E17
- E33
- E36
- E48
- PV36
- PV48

4 IEC 61508 / ISO 13849 Functional Safety Assessment Scheme

exida assessed the development process used by Precision Sensors for this development project against the objectives of the *exida* certification scheme which includes subsets of IEC 61508 and ISO 13849. The results of the assessment are documented in [R3].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508 and ISO 13849. 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 and ISO 13849.

As part of the IEC 61508 and ISO 13849 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 W Series Pressure Switch has been assessed per IEC 61508 and ISO 13849 to the following levels:

- SIL 3 capability
- PL e 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 and a maximum Performance level of e (PL e) according to ISO 13849.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Precision Sensors for these products against the objectives of the *exida* certification scheme which includes IEC 61508 parts and ISO 13849 [N1] and [N2]. The development of the W Series Pressure Switch was done per this IEC 61508 SIL 3 and ISO 13849 PL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Precision Sensors has a defined product lifecycle process in place. This is documented in the Quality Management System Manual [D1] and various Quality Procedures. Every customer job goes through the complete design process. 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 or ISO 13849 to software and software development do not apply.

The assessment investigated the compliance with IEC 61508 and ISO 13849 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 and ISO 13849 requirements tailored to the SIL 3 and PL e work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited Precision Sensors design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3 and ISO 13849 PL e **.**

5.1.1 Functional Safety Management

The pressure switches manufactured by Precision Sensors are not built for inventory. These pressure switches are built-to-order. The basic designs are standardized, but each order can have trim and materials variations or specific customer requested proof tests. Due to the specialized nature of each pressure switch, documentation that defines all of the requirements is generated for every order as part of the process.

FSM Planning

Precision Sensors 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 Engineering Standard ES12 [D6] and in greater detail in additional procedures. Templates and sample documents were reviews and found to be sufficient. The modification process is covered by also covered in [D6]. 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

SOP 4.2 [D5] requires that all documents be under document control. Use of this to control revisions was evident during the audit.

Training, Competency recording

The team members were reviewed by *exida* and the team is properly staffed. 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. Precision Sensors hired *exida* to be the independent assessor per IEC 61508 and ISO 13849 and to provide specific IEC 61508 / ISO 13849 knowledge.

5.1.2 Safety Requirements Specification and Architecture Design

For the Precision Sensors W Series Pressure Switch, the simple primary functionality of the pressure 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 W 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 / PL e.

5.1.3 Hardware Design

The design process is documented in the flowcharts shown in [D17] and [D18]. 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 / PL e.

5.1.4 Validation

Validation Testing is documented on form [D22] which is created for each order. The test plan includes testing per all standard and customer performance requirements. As the Precision Sensors W Series Pressure Switch are purely mechanical devices with a simple safety function, there is no separate integration testing necessary. The W 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 / PL e.

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 / PL e.

5.1.5 Verification

The development and verification activities are defined in [D22]. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 3 / PL e.

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 Precision Sensors W Series Pressure Switch. Shipment records were used to determine that the W Series have >30 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 / PL e.

5.1.7 Modifications

Modifications are initiated per Engineering Standard ES12 [D6]. 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 Precision Sensors may make modifications to this product as needed. or Since this was the initial assessment of Precision Sensors's modification procedure according to IEC 61508 and ISO 13849, it was expected that modifications to the product prior the assessment did not include a functional safety impact analysis. The modification process has been revised to include a functional safety impact analysis. The initial post assessment modification to the W Series Pressure Switch shall be audited by *exida* to confirm that a functional safety impact analysis was performed according to Precision Sensors' modification procedure.

- 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

Precision Sensors 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 (Precision Sensors W Series Pressure Switch perform well-defined actions) and operation only by skilled operators (operators familiar with type of switch, although this is partly the responsibility of the end-user). This meets SIL 3 / PL e.

5.2 Hardware Assessment

To evaluate the hardware design of the W Series Pressure Switch 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 Precision Sensors W 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 W 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 Precision Sensors W Series Pressure Switch are only one part of a (sub)system, the SFF should be calculated for the entire 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 element application. It is the end user's responsibility to confirm this for each particular application and to include all components of the element in the calculations.

The analysis shows that the design of the Precision Sensors W Series Pressure Switch can meet the hardware requirements of IEC 61508, SIL 3 for the W Series depending on the complete element design. The Hardware Fault Tolerance and PFD_{avg} requirements of IEC 61508 must be verified for each specific design.

6 Terms and Definitions

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

7 Status of the Document

7.1 Liability

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

7.2 Version History

Contract Number	Report Number	Revision Notes
Q19/02-138	R002 V1, R1	Initial Release

Reviewer: Steve Close, exida, 1/7/20

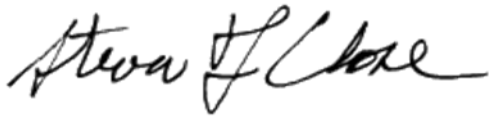
Status: Released, 1/7/20

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Brad Hitchcock, Safety Engineer, CFSP



Steven Close, Senior Safety Engineer