# IEC 61508 Functional Safety Assessment

Project:

LESV - Flow Sensor

Customer:

Woodward Industrial Controls

Fort Collins, CO

USA

Contract Number: Q13/04-021

Report No.: WOO Q13-04-021 R001

Version V0, Revision R1, November 26, 2013

Chris O'Brien

## Management summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the LESV - Flow Sensor

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

- *exida* assessed the development process used by Woodward Industrial Controls 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 Woodward.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 2 for mechanical components. A full IEC 61508 Safety Case was prepared using the *exida* SafetyCaseWB™ 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.

Some areas of improvement were identified in the design process and the design procedures were upgraded during the project. However because of the low complexity of the products and the proven in use design, Woodward was able to demonstrate that the objectives of the standard have been met.

The results of the Functional Safety Assessment can be summarized as:

**The Woodward LESV - Flow Sensor were found to meet the requirements of IEC 61508 for up to SIL 2 (SIL 2 Capable). 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 Woodward Industrial Controls:

- LESV – Flow Sensor

by *exida* according to the requirements of IEC 61508: ed2, 2010.

The results of this provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

# 2 Project management

## 2.1 *exida*

*exida* is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

## 2.2 Roles of the parties involved

| | |
|---|---|
| Woodward Industrial Controls | Manufacturer of the LESV - Flow Sensor |
| *exida* | Performed the hardware assessment |
| *exida* | Performed the IEC 61508 Functional Safety Assessment according. |

Woodward contracted *exida* in June 2013 for the IEC 61508 Functional Safety Assessment of the above mentioned devices.

## 2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

| | | |
|---|---|---|
| [N1] | IEC 61508 (Parts 1 - 7): 2010 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems |

## 2.4 Reference documents

### 2.4.1 Documentation provided by Woodward Industrial Controls

| | | |
|---|---|---|
| [D1] | 1-QCI-00001, Rev 3; 4/8/2013 | Quality Manual |
| [D2] | Project Tool Artifact; 9/23/2013 | LESV – Flow Sensor Project Plan |
| [D3] | 2-07-2599, Rev 13; 4/2/2013 | One Woodward Product Life Cycle (PLC) Process |
| [D4] | 4-30-266, Rev 14; 2/26/2013 | Engineering Change Request Procedure |
| [D5] | 3-QCI-00074, Rev 2; 4/25/2011 | Global Corrective Action Committee and Corrective Action Board Process Procedures |
| [D6] | 3-14-3710, Rev 7; 12/14/2011 | Investigation of Customer Product |
| [D7] | 3-06-3016, Rev 7; 5/23/2013 | Supplier Approval Process |
| [D8] | 2-QCI-00194, Rev 3; 11/12/2010 | Document and Date Control |
| [D9] | 3-QCI-00381, Rev 5; 1/3/2013 | Business Disciplines Documentation Changes |

| | | |
|---|---|---|
| [D10] | 2-QCI-00192, Rev 4; 2/14/2013 | Non-Conforming Product Control System |
| [D11] | 2-QCI-00155, Rev 5; 6/30/2012 | Corrective and Preventive Action |
| [D12] | 2-QCI-00377, Rev 3; 1/21/2013 | Internal Quality Audits |
| [D13] | Project Tool Artifact; 9/23/2013 | Action Item Register |
| [D14] | 3-11-0001, Rev 6; 9/20/2010 | Woodward Calibration Program |
| [D15] | 3-QCI-00197, Rev 4; 5/7/21013 | Management Review |
| [D16] | 3-09-3762, Rev 4; 11/29/2011 | EC Risk Assessment Tool |
| [D17] | Sample; 3/29/2013 | Completed Engineering Change Risk Assessment Tool Form |
| [D18] | 74 300 3411; 6/30/2011 | ISO Certificate |
| [D19] | Project Tool Artifact; 9/23/2013 | Safety Requirement Specification |
| [D20] | 397A7650, Rev A; 3/27/2012 | Customer Functional Specification |
| [D21] | 402A1600, Rev A; 4/20/2012 | Customer Ordering Specification |
| [D22] | Project Artifact; 9/23/2013 | Design File |
| [D23] | Product Performances Compliance Matrix, Rev A; 2/22/2012 | Requirements Traceability Matrix |
| [D24] | 123415R001, Rev 3 | Validation Test Plan |
| [D25] | 123415R008, Rev 2 | Validation Test Results |
| [D26] | 123415R004, Rev 4 | Production Test Requirements |
| [D27] | TSP-14205, Rev H | Production Test Results |
| [D28] | Project Artifact; 9/23/13 | Shipment Records |
| [D29] | B26762, Rev C; 11/25/2013 | LESV – Flow Sensor Safety Manual |

### 2.4.2 Documentation generated by *exida*

| | | |
|---|---|---|
| [R1] | WOO 12-03-036 R001 V1R3 FMEDA LESV – Sensor; 11/20/2013 | FMEDA report, LESV - Flow Sensor |
| [R2] | PIU Analysis; 11/23/13 | Proven in Use Analysis |
| [R3] | Q13-04-021 Safety Case WB-61508 v1.5.2 V1R2; 11/25/2013 | IEC 61508 Safety Case WB for LESV - Flow Sensor |
| [R4] | WOO Q13-04-021 R001 V1R1 LESV - Flow Sensor IEC 61508 Assessment Report; 11/26/2013 | IEC 61508 Functional Safety Assessment, Woodward Industrial Controls LESV - Flow Sensor (this report) |

# 3 Product Descriptions

The LESV - Flow Sensor provides position feedback of the valve plug position. Accurate valve position feedback can be used one of the inputs to calculate the flow through an LESV. An accurate feedback device such as the MTS Tempsonics position sensor must be used in order to produce the position signal. The logic solver must be programmed to read the valve plug position and calculate the flow rate through the valve.

The Safety Function of the LESV - Flow Sensor shall be to provide valve plug position feedback within the measurement safety accuracy.

# 4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Woodward Industrial Controls 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. The review of the product design is described in section 5.3.

## 4.2 Assessment level

The LESV - Flow Sensor has been assessed per IEC 61508 to the following levels:

- SIL 2 capability

The development procedures have been assessed as suitable for use in applications with a maximum Safety Integrity Level of 2 (SIL2) according to IEC 61508.

## 4.3 Product Modifications

Woodward Industrial Controls may make modifications to this product as needed. Modifications shall be classified into two types:

Type 1 Modification: Changes requiring re-certification, which includes the re-design of safety functions or safety integrity functions.

Type 2 Modification: Changes allowed to be made by Woodward Industrial Controls provided that:

- A competent person from Woodward Industrial Controls, appointed and agreed with *exida*, judges and approves the modifications. Terry Mize is currently approved by *exida* to fulfill this role.
- The modification documentation listed below is submitted prior to a renewal of the certification to *exida* for review of 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

# 5 Results of the IEC 61508 Functional Safety Assessment

*exida* assessed the development process used by Woodward Industrial Controls for these products against the objectives of IEC 61508 parts 1 - 7. The assessment was done on-site at the Fort Collins, CO facility on September 23, 2013 and documented in the SafetyCase [R3].

## 5.1 Open Issues

The overall process is strong and elements of the designs have extensive proven field experience, sufficient for SIL 2 capability. Some areas of improvement were identified in the design process and some of the design procedures and forms were upgraded during the project. All of the improvements were evaluated and included in the final version of the SafetyCase.

## 5.2 Lifecycle Activities and Fault Avoidance Measures

Woodward Industrial Controls has a defined product lifecycle process in place. This is documented in the One Woodward Product Life Cycle (PLC) Process [D3]. The PLC is a phase and gate roadmap for complete product life cycle management. The process includes cross-functional tasks and management approvals. Phases contain the deliverables, activities, and tasks required at specific points in the process. Gates contain business and technical hurdles, checklists, and activities that must be completed before the project can move to the next phase.

The PLC has three main phases; Technology/Platform Development Process, Product Development Process, and Production Process. The Woodward Product Development System (WPDS) is a project documentation file system that is used to track and manage all projects. A documented modification process is also covered in the Engineering Change Request Procedure [D4]. 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 2 work scope of the development team. The result of the assessment can be summarized by the following observations:

**The audited Woodward Industrial Controls design and development process complies with the relevant managerial requirements of IEC 61508 SIL 2.**

### 5.2.1 Functional Safety Management

<u>FSM Planning</u>

Woodward Industrial Controls has a defined process in place for product design and development. Required activities are specified along with review and approval requirements. A project specific plan is created for every project and captured in WPDS. The project plan for the LESV - Flow Sensor [D2] was reviewed and found to be sufficient. The modification process is covered by Engineering Change Request Procedure. This process and the procedures referenced therein fulfill the requirements of IEC 61508 with respect to functional safety management for a product with simple complexity and well defined safety functionality.

<u>Version Control</u>

The Document and Date Control [D8] procedure requires that all documents be under document control. Use of this to control revisions was evident during the audit.

Training, Competency recording

The WDPS Deliverable lists the key personnel assigned to projects. Smart Loading is used to level load projects with personnel. The Project Management Office (PMO) is responsible for assigning personnel to projects. The Human Resource department maintains training records of 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. Woodward hired *exida* to be the independent assessor per IEC 61508 and to provide specific IEC 61508 knowledge.

### 5.2.2 Safety Requirements Specification and Architecture Design

For the LESV - Flow Sensor, the Safety Requirement Specification is part of the product specification. The product requirements specification is maintained in DOORS. The product requirements specification [D19] was examined and found to be up-to-date and sufficient. The product requirements specification was derived from the Customer Functional Specification [D20]. Adherence to the functional specification was confirmed through the Requirements Traceability Matrix [D23]. This meets SIL 2.

### 5.2.3 Hardware Design

The design process is documented in Product Development Process of the PLC. 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 2.

### 5.2.4 Validation

Validation Testing is documented in the Validation Test Results [D25]. The validation testing was performed on the LESV – Flow Sensor integrated with a position sensor. The validation testing included performance and environmental testing. In addition to the validation testing, Production Testing [D26], [D27] is performed on the LESV – Flow Sensor with the position feedback sensor to validate the integrated sensor element meets the requirements. The LESV - Flow Sensor 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 2.

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 2.

### 5.2.5 Verification

The development and verification activities are defined LESV – Flow Sensor Project Plan. For each design phase the objectives are stated, required input and output documents and review activities. This meets SIL 2.

### 5.2.6 Proven In Use

In addition to the Design Fault avoidance techniques listed above, a Proven in Use [R2] evaluation was carried out on the some of the components utilized in the LESV - Flow Sensor. Shipment records [D28] for other valve designs that use these components were used to determine that these components have >10 million operating hours. This supports the requirements for Proven In Use for SIL 2.

### 5.2.7 Modifications

Modifications are initiated per the Engineering Change Request Procedure. All changes are first reviewed and analyzed for impact before being approved by means of the EC Risk Assessment Tool [D16]. Measures are in place to verify and validate the change are developed following the normal design process. This meets SIL 2.

### 5.2.8 User documentation

Woodward Industrial Controls creates the following user documentation: product catalogs and an Installation and Operations Manual (IOM). The IOM contains a chapter on Safety Management [D29]. The Safety Management chapter 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 (LESV - Flow Sensor 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 2.

## 5.3 Hardware Assessment

To evaluate the hardware design of the LESV - Flow Sensor 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]. The FMEDA report list these failure rates for the LESV - Flow Sensor. The failure rates listed are valid for the useful life of the devices.

Note, as the LESV - Flow Sensor is 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 users responsibility to confirm this for each particular application and to include all components of the final element in the calculations.

**The analysis shows that the design of the LESV - Flow Sensor can meet the hardware requirements of IEC 61508, SIL 2 and SIL 2 for the LESV - Flow Sensor depending on the complete sensor element design. The Hardware Fault Tolerance, $PFD_{AVG}$, and Safe Failure Fraction requirements of IEC 61508 must be verified for each specific design.**

# 6 Terms and Definitions

| | |
|---|---|
| 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 |
| 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). |
| Type A element | "Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2 |
| Type B element | "Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2 |

# 7 Status of the Document

## 7.1 Liability

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

## 7.2 Releases

| | | |
|---|---|---|
| Version: | V0 | |
| Revision: | R1 | |
| Version History: | V1, R1: | Released, November 26, 2013 |
| | V0, R1: | Draft; November 20, 2013 |
| Authors: | Chris O'Brien | |
| Review: | V0, R1: | Griff Francis; November 22, 2013 |
| Release status: | Released | |

## 7.3 Future Enhancements

At request of client.

## 7.4 Release Signatures

Chris O'Brien, CFSE, Partner

Griff Francis, Senior Safety Engineer