IEC 61508 Functional Safety Assessment

Project:
Acoustic Detector Analog Output

Customer:
Detector Electronics Corp.
Minneapolis, MN
USA

Contract No.: Q12/01-022
Report No.: DET12/01-022 R001
Version V1, Revision R1, July 31, 2013
Dave Butler
Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the Acoustic Detector Analog Output.

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

- **exida** assessed the development process used by Detector Electronics Corp. through an audit and creation of a detailed safety case against the requirements of IEC 61508.

- **exida** reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

- **exida** reviewed the manufacturing quality system in use at Detector Electronics Corp.

The functional safety assessment was performed to the requirements of IEC 61508: ed2, 2010, SIL 2. A full IEC 61508 Safety Case was prepared, using the **exida** SafetyCaseWB tool, and used as the primary audit tool. Hardware and software 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 by the following statements:

**The Acoustic Detector Analog Output was found to meet the requirements of SIL 2. 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

Management Summary ........................................................................................................... 2

1 Purpose and Scope ................................................................................................................ 4

2 Project management .............................................................................................................. 5
   2.1 exida ................................................................................................................................. 5
   2.2 Roles of the parties involved ............................................................................................. 5
   2.3 Standards / Literature used ............................................................................................... 5
   2.4 Reference documents ......................................................................................................... 5
       2.4.1 Documentation provided by Detector Electronics Corp. ............................................ 5
       2.4.2 Documentation generated by exida ........................................................................... 7

3 Product Description ............................................................................................................... 8

4 IEC 61508 Functional Safety Assessment ............................................................................. 9
   4.1 Methodology ..................................................................................................................... 9
   4.2 Assessment level .............................................................................................................. 9
   4.3 Product Modifications ..................................................................................................... 10

5 Results of the IEC 61508 Functional Safety Assessment .................................................... 11
   5.1 Lifecycle Activities and Fault Avoidance Measures ......................................................... 11
       5.1.1 Functional Safety Management ............................................................................... 11
       5.1.2 Safety Requirements Specification and Architecture Design .................................. 11
       5.1.3 Hardware Design ..................................................................................................... 12
       5.1.4 Software (Firmware) Design ..................................................................................... 12
       5.1.5 Validation .................................................................................................................. 12
       5.1.6 Verification ................................................................................................................. 13
       5.1.7 Modifications ........................................................................................................... 13
       5.1.8 User Documentation ................................................................................................. 14
   5.2 Hardware Assessment ...................................................................................................... 15

6 Terms and Definitions ......................................................................................................... 16

7 Status of the document ........................................................................................................ 17
   7.1 Liability ............................................................................................................................ 17
   7.2 Releases ............................................................................................................................ 17
   7.3 Future Enhancements ...................................................................................................... 17
   7.4 Release Signatures ......................................................................................................... 17
1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Detector Electronics Corp.:

- Acoustic Detector Analog Output (consists of one Model AC100 Sensor and one Model ATX10 Transmitter)

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

The results of this assessment 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

Detector Electronics Corp.  Manufacturer of the Acoustic Detector Analog Output

exida  Performed the hardware assessment

exida  Performed the IEC 61508 Functional Safety Assessment

Detector Electronics Corp. contracted exida with 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.

<table>
<thead>
<tr>
<th>N1</th>
<th>IEC 61508 (Parts 1 - 7): 2010</th>
<th>Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems</th>
</tr>
</thead>
</table>

2.4 Reference documents

2.4.1 Documentation provided by Detector Electronics Corp.

<table>
<thead>
<tr>
<th>ID</th>
<th>Project Document</th>
<th>Ver.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>D001</td>
<td>POL Quality Management System Manual 99-1117 AF-2687.doc</td>
<td>AF</td>
<td></td>
</tr>
<tr>
<td>D003</td>
<td>POL Product Development Procedure F-82.doc</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>D004</td>
<td>PRC Software Configuration Management A-236.doc</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>D006</td>
<td>WRK RMI Request Procedure C-3080.doc</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D006b</td>
<td>DEC RMI Request Form.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D007</td>
<td>POL Supplier Selection, Evaluation and Management G-72.docx</td>
<td>G</td>
<td></td>
</tr>
<tr>
<td>D010</td>
<td>POL ECO Process H-80.doc</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td>D012</td>
<td>POL Nonconforming Product-Deviation C-49.doc</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D013</td>
<td>POL Corrective Action And Preventive Action D-95.doc</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Project Document</td>
<td>Ver.</td>
<td>Date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------</td>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>D016</td>
<td>PRC Product Software Issue Tracking A-237.doc</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>D019</td>
<td>POL Product Life Cycle Management B-132.doc</td>
<td>B</td>
<td></td>
</tr>
<tr>
<td>D019b</td>
<td>POL Product Recall &amp; Field Update Procedure C-136.doc</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>D021</td>
<td>PRC Software Development D-85.docx</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>D023b</td>
<td>TMP Impact Analysis Template A-3144.doc</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>D026</td>
<td>Acoustic_v-01_FSM_2013FEB.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D032</td>
<td>AC100 Training Plan 1.3.pdf</td>
<td>1.3</td>
<td>7/9/2013</td>
</tr>
<tr>
<td>D036</td>
<td>ISO 9001_2011_11.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D040</td>
<td>Acoustic Detector_v.001_SRS_2013JUL11.pdf</td>
<td></td>
<td>7/11/2013</td>
</tr>
<tr>
<td>D045</td>
<td>Arch Spec AC100 Acoustic Detector - 300331-001 - v1.1.pdf</td>
<td>v1.1</td>
<td>3/8/2013</td>
</tr>
<tr>
<td>D047</td>
<td>AcousticDetectorSchematics.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D051</td>
<td>AC100_SDS_19Jul13_0105.doc</td>
<td>A 1.05</td>
<td>7/1/2013</td>
</tr>
<tr>
<td>D053b</td>
<td>AC100 Software Review 9_21_2010.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D053c</td>
<td>IS Design Discussion.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D058</td>
<td>ATX10 Code Review 071913.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D059</td>
<td>Acoustic Fault Injection List_Test data, v01, 2013FEB20.xlsx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D060</td>
<td>300179 SW Style Guide Rev B.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D061</td>
<td>std.lnt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D062</td>
<td>ATX10_LINT.TXT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D066</td>
<td>ATX10 Module Test Results_0002.docx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D069</td>
<td>AC100, ATX10 Validation Test Plan_v001, 2013JUL31.pdf</td>
<td>1</td>
<td>7/31/2013</td>
</tr>
<tr>
<td>D074</td>
<td>Acoustic Validation Test Results, v-01, 2013JUL19.xlsx</td>
<td>v-01</td>
<td>7/19/2013</td>
</tr>
<tr>
<td>D074b</td>
<td>Acoustic FW Changes Summary, v-01, 2013MAR03.docx</td>
<td>v-01</td>
<td>3/3/2013</td>
</tr>
<tr>
<td>D078</td>
<td>95-8657-2.2 (AC100_ATX10).pdf</td>
<td>2.2</td>
<td></td>
</tr>
<tr>
<td>D079</td>
<td>95-8658-1.2 (AC100_ATX10 Safety), 2013JUN28.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D086b</td>
<td>Software Tools HAZOP, Acoustic, v-01, 2013JUL17.docx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D087</td>
<td>011353-001_B.mot.sha1; 012385-001_A.ldr.sha1;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D088</td>
<td>IAF, AC100, ATX10_Initial, 2013FEB, Ver1.0.docx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D089</td>
<td>Detronics Acoustic Detector project SW Hazop Report Update.docx</td>
<td></td>
<td>7/10/2013</td>
</tr>
<tr>
<td>D091</td>
<td>SIL Checklist, Acoustic V-001, Initial, 2012APR.pdf</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 2.4.2 Documentation generated by *exida*

<table>
<thead>
<tr>
<th>ID</th>
<th>Project Document</th>
<th>Ver.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>D091b</td>
<td>Acoustic V-01 Final Review Meeting Minutes_2013MAR.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D092</td>
<td>097-RPT.CAL.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D093</td>
<td>Detronics AC100 Transcribed-ScannedNotes from WMG visit in Jan 2013.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D094</td>
<td>Acoustic Initial v-01 SIL Serena_Approval Report, 2013MAR07.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D095</td>
<td>Code Examples ATX10.txt</td>
<td>7/19/2013</td>
<td></td>
</tr>
<tr>
<td>D096</td>
<td>ATX10 source package.bmp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D097</td>
<td>Compiler Validation ATX10, 2013JUL17.docx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D097b</td>
<td>ValidationOfCompliance-EWARM-441a.pdf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D098</td>
<td>Compiler Validation AC100, 2013JUL17.docx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D099</td>
<td>AC100 FW Specs_v-01_2013JUL24.pdf</td>
<td>v-01</td>
<td>7/24/2013</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Project Document</th>
<th>Ver.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>[R1]</td>
<td>DET Leak Detector Safety Case IEC61508 V1R4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[R2]</td>
<td>DET 12-01-022 R001 V1 R1 Assessment Report.doc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[R3]</td>
<td>DET 11-09-046 R001 V1 R1 AC100 FMEDA Report.pdf</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[R1]: DET Leak Detector Safety Case IEC61508 V1R4

[R2]: IEC 61508 Functional Safety Assessment for Acoustic Detector Analog Output (This document)

[R3]: FMEDA Report for the Acoustic Detector Analog Output
3 Product Description

The Acoustic Detector Analog Output, as its name implies, identifies gas leaks by detecting and interpreting their acoustic signature. It consists of two modules, the AC100 proper and the ATX10. The AC100 contains the detector, an acoustic sounder to enable Acoustic Integrity testing, signal conditioning circuitry, and a digital signal processor which determines if a leak has been detected. The AC100 communicates with the ATX 10, which communicates the state of the overall system to the outside world via a current output and/or digital link. Only the current output is part of the safety function.

![Diagram of AC100 and ATX10](image)

The AC100 is classified as a Type B element according to IEC 61508, having a hardware fault tolerance of 0.

**Defined Operational States:**

The normal state is defined as:
- The current output properly represents the defined acoustic signal within the safety accuracy limits;
- The current output responds to changes in the defined acoustic signal within the worst case safety response time;
- Normal limits for the 4-20mA current loop are defined as a 4-20mA output signal that corresponds to a pre-defined acoustic condition ranging from normal to full alarm.

The fault state is defined as:
- The current output is \(\leq 3.6\)mA to indicate fault.

The warm-up state is defined as:
- The current output = 3.0mA within the safety accuracy limits during the warm-up period.

**The Acoustic Detector SIL approved firmware is listed below (see section 4.3 for modification constraints):**
- 011353-001 Rev B, v1.00 (ATX10) and higher
- 012385-001 Rev A, v1.72 (AC100) and higher

**The Acoustic Detector SIL approved hardware is listed below (see section 4.3 for modification constraints):**
- 010611_002, Rev B and higher
- 011006_002, Rev A and higher
- 011366_002, Rev B and higher
4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Detector Electronics Corp. and is documented in the safety case database [R1].

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software 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).

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

- Product design
  - Hardware architecture and failure behavior, documented in a FMEDA
  - Software architecture and failure behavior, documented in a Software Criticality and HAZOP report

The review of the development procedures and documentation is described in section 5.1, Lifecycle Activities and Fault Avoidance Measures. The review of the product design is described in section 5.2, Hardware Assessment.

4.2 Assessment level

The Acoustic Detector Analog Output has been assessed per IEC 61508 to the following levels:

- Systematic Safety Integrity: SIL 2 capable
• Random Safety Integrity: PFD_{AVG} and Architectural Constraints must be verified for each application.

The development procedures were assessed as suitable for use in applications with a maximum Safety Integrity Level of SIL 2 according to IEC 61508.

4.3 Product Modifications

Detector Electronics Corp. 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 Detector Electronics Corp. provided that:

• A competent person from Detector Electronics Corp., appointed and agreed with exida, judges and approves the modifications. A Compliance Engineer 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 with respect to the modifications made.
  
  o List of all anomalies reported
  o List of all modifications completed
  o 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
  o List of modified documentation
  o Regression test plans
5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Detector Electronics Corp. during the product development against the objectives of IEC 61508 parts 1, 2, and 3, see [N1]. The development of the Acoustic Detector Analog Output was done per this IEC 61508 SIL 2 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Detector Electronics Corp. has an IEC 61508 compliant development process as assessed during this IEC 61508 certification. This compliant development process is documented in [N1]. This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for product 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 development process complies with the relevant managerial requirements of IEC 61508 SIL 2.

5.1.1 Functional Safety Management

FSM Planning
The functional safety management of this Detector Electronics Corp. product’s development is governed by [D026], which is a template for a Functional Safety Management Plan, containing boilerplate procedures for certain required actions. It also contains structure and format so that the plan can be tailored and adapted to the particular project on which it is used. The Functional Safety Management Plan defines all of the tasks that must be done to ensure functional safety as well as the person(s) responsible for each task. These processes and the procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management.

Version Control
All documents are under version control as required by [D004].

Training, Competency recording
Competency is ensured by the creation of a competency and training matrix for the project [D032]. The matrix lists all of those on the project who are working on any of the phases of the safety lifecycle. Specific competencies for each person are listed on the matrix which is reviewed by the project manager. Any deficiencies are then addressed by updating the matrix with required training for the project.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D003], a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. For the Acoustic Detector Analog Output, the requirements specification [D040] contains a system overview section, a System Safety Strategy section, and one or more sections containing the safety requirements for the product. During the assessment, exida reviewed the content of the specification for completeness per the requirements of IEC 61508.
Requirements are tracked throughout the development process by the creation of a series of traceability matrices which are included in [D069]. The system requirements are broken down into derived hardware and software requirements which include specific safety requirements. Traceability matrices show how the safety requirements map to and from the derived requirements and validation tests.

Requirements from IEC 61508-2, Table B.1 that have been met by Detector Electronics Corp. include project management, documentation, structured specification, inspection of the specification, and checklists.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D003]. The hardware design process includes creating a hardware architecture specification, a peer review of this specification, creating a detailed design, a peer review of the detailed design, component selection, detailed drawings and schematics, a Failure Modes, Effects and Diagnostic Analysis (FMEDA), electrical unit testing, fault injection testing, and hardware verification tests.

Requirements from IEC 61508-2, Table B.2 that have been met by Detector Electronics Corp. include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, checklists, semi-formal methods, computer aided design tools and inspection of the specification. This is also documented in [R01]. This meets the requirements of SIL 2.

5.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D021]. The software design process includes software architecture design and peer review, detailed design and peer review, code reviews, static source code analysis and unit testing.

Requirements from IEC 61508-3, Table A.2 that have been met by Detector Electronics Corp. include modular approach, structured diagrammatic methods, time-triggered architecture design.

Requirements from IEC 61508-3, Table A.3 that have been met by Detector Electronics Corp. include suitable programming language, strongly typed programming language, and tools and translators: increased confidence from use.

Requirements from IEC 61508-3, Table A.4 that have been met by Detector Electronics Corp. include structured and semi-formal methods, modular approach, design and coding standards and structured programming.

This is also documented in [R01]. This meets the requirements of SIL 2.

5.1.5 Validation

Validation Testing is done via a set of documented tests. The validation tests are traceable to the Safety Requirements Specification [D040], in the validation test plan [D069]. The traceability matrices show that all safety requirements have been validated by one or more tests. In addition to standard Test Specification Documents, third party testing is included as part of the validation testing. All non-conformities are documented in a change request and procedures are in place for corrective actions to be taken when tests fail as documented in [D003].
Requirements from IEC 61508-2, Table B.5 that have been met by Detector Electronics Corp. include functional testing, functional testing under environmental conditions, interference surge immunity testing, fault insertion testing, project management, documentation, expanded functional testing and black-box testing.

Requirements from IEC 61508-3, Table A.7 that have been met by Detector Electronics Corp. include functional and black box testing.

[R01] documents more details on how each of these requirements has been met. This meets SIL 2.

5.1.6 Verification

Verification activities are built into the standard development process as defined in [D003]. Verification activities include the following: Fault Injection Testing, static source code analysis, module testing, integration testing, FMEDA, peer reviews and both hardware and software unit testing. In addition, safety verification checklists are filled out for each phase of the safety lifecycle. This meets the requirements of IEC 61508 SIL 2.

Requirements from IEC 61508-2, Table B.3 that have been met by Detector Electronics Corp. include functional testing, project management, documentation, and black-box testing.

Requirements from IEC 61508-3, Table A.5 that have been met by Detector Electronics Corp. include dynamic analysis and testing, data recording and analysis, functional and black box testing, and test management and automation tools.

Requirements from IEC 61508-3, Table A.6 that have been met by Detector Electronics Corp. include functional and black box testing.

Requirements from IEC 61508-3, Table A.9 that have been met include static analysis and dynamic analysis and testing.

[R01] documents more details on how each of these requirements has been met. This meets the requirements of SIL 2.

5.1.7 Modifications

Modifications are done per the Detector Electronics Corp.'s change management process as documented in [D004] and [D026]. Impact analyses are performed for all changes once the product is released for integration testing. The results of the impact analysis are used in determining whether to approve the change. The standard development process as defined in [D003] is then followed to make the change. The handling of hazardous field incidents and customer notifications is governed by [D078] and [D079]. This procedure includes identification of the problem, analysis of the problem, identification of the solution, and communication of the solution to the field. This meets the requirements of IEC 61508 SIL 2.

Requirements from IEC 61508-3, Table A.8 that have been met by the Detector Electronics Corp. modification process include impact analysis, reverify changed software modules, reverify affected software modules, revalidate complete system or regression validation, software configuration management and data recording and analysis.
5.1.8 User Documentation

Detector Electronics Corp. created a safety manual for the Acoustic Detector Analog Output [D079] which addresses all relevant operation and maintenance requirements from IEC 61508. This safety manual [D079] was assessed by exida, and is considered to be in compliance with the requirements of IEC 61508.

Requirements from IEC 61508-2, Table B.4 that have been met by Detector Electronics Corp. include operation and maintenance instructions, maintenance friendliness, project management, documentation, and limited operation possibilities.

[R01] documents more details on how each of these requirements has been met. This meets the requirements for SIL 2.
5.2 Hardware Assessment

To evaluate the hardware design of the Acoustic Detector Analog Output, a Failure Modes, Effects, and Diagnostic Analysis was performed by exida for each component in the system. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D059], and as part of the IEC 61508 assessment.

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.

These results must be considered in combination with PFD\textsubscript{AVG} of other devices of a Safety Instrumented Function (SIF), in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD\textsubscript{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF, using the failure rates published in the FMEDA Report.
## 6 Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault tolerance</td>
<td>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)</td>
</tr>
<tr>
<td>FIT</td>
<td>Failure In Time (1x10^-9 failures per hour)</td>
</tr>
<tr>
<td>FMEDA</td>
<td>Failure Mode Effect and Diagnostic Analysis</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>Low demand mode</td>
<td>Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.</td>
</tr>
<tr>
<td>PFD_avg</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>PFH</td>
<td>Probability of dangerous Failure per Hour</td>
</tr>
<tr>
<td>SFF</td>
<td>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.</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>SIS</td>
<td>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).</td>
</tr>
<tr>
<td>HART</td>
<td>Highway Addressable Remote Transducer</td>
</tr>
<tr>
<td>AI</td>
<td>Analog Input</td>
</tr>
<tr>
<td>AO</td>
<td>Analog Output</td>
</tr>
<tr>
<td>Type A element</td>
<td>“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2</td>
</tr>
<tr>
<td>Type B element</td>
<td>“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2</td>
</tr>
</tbody>
</table>
7 Status of the document

7.1 Liability

_exida_ prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. _exida_ accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version: V1
Revision: R1
Version History: V1, R1: Released the client manufacturer-reviewed version.
V0, R1: Fixed some review issues.
V0, R0: Initial version for draft review.
Authors: Dave Butler
Review: V0, R0: Griff Francis
Release status: Released

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

John C. Yozallinas, CFSE – Senior Safety Engineer

David E. Butler, CFSE – Safety Engineer