



IEC 61508 Functional Safety Assessment

Project:

Pointwatch Eclipse Gas Detector - Models PIRECL and HC200

Customer:

Det-Tronics
Minneapolis, MN
USA

Contract No.: Q09/02-04

Report No.: DET 09-02-04 R002

Version V1, Revision R1, April 15, 2009

Michael Medoff

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

© All rights reserved.

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the:

Pointwatch Eclipse Gas Detector - Models PIRECL and HC200

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

- *exida-certification* assessed the development process used by Det-Tronics through an audit and creation of a detailed safety case against the requirements of IEC 61508.
- *exida-certification* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

The functional safety assessment was performed to the requirements of IEC 61508, SIL 2. All documents referenced in section 2.4.1 were reviewed and form the basis of this assessment.

The results of the Functional Safety Assessment can be summarized by the following statements:

The Pointwatch Eclipse Gas Detector was found to meet the requirements of SIL 2, single use (HFT = 0).

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 <i>exida</i>	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 Det-Tronics	5
2.4.2 Documentation generated by <i>exida</i>	6
3 Product Description.....	7
4 IEC 61508 Functional Safety Assessment.....	8
4.1 Methodology	8
4.2 Assessment level	9
5 Results of the IEC 61508 Functional Safety Assessment	10
5.1 Lifecycle Activities and Fault Avoidance Measures	10
5.1.1 Functional Safety Management.....	10
5.1.2 Safety Requirements Specification and Architecture Design	10
5.1.3 Hardware Design.....	11
5.1.4 Validation.....	11
5.1.5 Verification.....	11
5.1.6 Modifications	12
5.1.7 User documentation	12
5.2 Hardware Assessment.....	13
Terms and Definitions.....	14
6 Status of the document	15
6.1 Liability	15
6.2 Releases	15
6.3 Future Enhancements.....	15
6.4 Release Signatures.....	15



1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option 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.

This assessment shall be done according to option 3.

This document shall describe the results of the IEC 61508 functional safety assessment of the Pointwatch Eclipse Gas Detector - Models PIRECL and HC200.



[D7]	701-018/2004T, 3/17/2005, V1.0	TUV Certification Report of the Eclipse Gas Detector – Model PIRECL
[D8]	300182-001, 12/8/2004, Rev. C	Eclipse Product Specification
[D9]	GOP 313, 11/15/2004	Software Development Process
[D10]	PIRECL_v.001_VC, 4/15/2005	Completed Phase Verification Checklists for Model PIRECL Hydrocarbon Infrared Gas Detector
[D11]	DET 04/02-24 R001, 1/25/2005, V1R1	Model PIRECL Pointwatch Eclipse IR Gas Detector FMEDA Report
[D12]	DET 04/02-24 R006, 8/23/2004, V1R1.0	Proven-in-Use Assessment for PIRECL Pointwatch Eclipse IR Gas Detector
[D13]	PIRECL Project Record, 3/6/2005	Test plan and results for hardware verification testing including those required for CE Mark
[D14]	F30049-003, 6/6/07	PAF (Project Authorization Form)
[D15]	GOP 301, 2/14/01	Engineering Assistance Request (EAR) Procedure (GOP 301).
[D16]	GOP 308, 1/23/07	Product Approval Process (GOP 308)
[D17]	GOP 421, 12/12/02	Procedure 421: Corrective Action and Preventive Action
[D18]	GOP 911, 11/14/00	Product Recall Procedure (GOP 911)
[D19]	RWTUV Fault Injection Tests, 1/19/2005	Fault Injection test results.
[D20]	DET 07-04-17 R002, V1R1, 7/13/2007	IEC 61508 Functional Safety Assessment, Det-Tronics Eclipse Gas Detector - Model PIRECL
[D21]	DET 09-02-04 R001, V1R1, 3/23/09	Proven-in-Use Assessment for PIRECL Pointwatch Eclipse IR Gas Detector

2.4.2 Documentation generated by *exida*

[R1]	DET 09-02-04 R002 V1R1 IEC 61508 Assessment.doc, April 15, 2009	IEC 61508 Functional Safety Assessment, Pointwatch Eclipse Gas Detector - Models PIRECL and HC200 (this report)
------	---	---



3 Product Description

The Pointwatch Eclipse™ Models PIRECL and HC200 is a diffusion-based, infrared combustible gas detector that provides continuous, fixed monitoring of flammable hydrocarbon gases from 0 to 100% Lower Explosive Limit (LEL). Standard device outputs include an electrically isolated 4 to 20 mA signal with HART communication protocol, and RS-485 serial communication. Serial communication protocols supported include MODBUS and ASCII.

It is ideally suited for protection of challenging on/offshore oil and gas facilities and other downstream hydrocarbon applications, the PointWatch Eclipse is globally certified for use in Class I, Divisions 1 and 2, and Zone 1 hazardous areas. In addition, the stainless steel construction, sapphire optics, and modular design all combine to deliver industrial grade hardness along with easy installation and the lowest cost of ownership available.

Eclipse is a point type, combustible gas detector capable of detecting many types of gases including methane, ethane, propane, butane, ethylene, and propylene. Although a separate 24VDC nominal power supply to power the unit is required an isolated, two-wire, 4 to 20 mA current loop is provided for connection to the optional display unit, personal computer or DCS. The device will be certified for use in SIL 2 safety integrity functions in a 1oo1 safety architecture.

The detector operates on a principle known as infrared absorption, where combustible hydrocarbon gases or vapors absorb light in the infra-red region. A beam of modulated light from an incandescent source, running at 4 Hz is projected on a dual infrared detector. Interference filters placed in front of the detector makes each half of the detector respond to a specific band of infrared energy. The reference wavelength is unaffected by combustible gases, while the active wavelength is strongly absorbed by the gas. The ratio of active and reference wavelengths are computed to determine the concentration of gas present in the path.

Two alarm levels are provided via relay outputs, high and low, both can be set from 5 to 60% LEL, latching or non-latching. A 3% LEL dead band is provided to prevent excessive toggling with changing gas levels. Alarm configuration can be done with the HART or Modbus interfaces.

Eclipse monitors for many types of faults on an ongoing basis including power supply voltages and memory errors. Faults are annunciated via both the 4-20mA loop and Fault Relay. Additional details are available through the digital communications interfaces.

Three digital communication protocols are supported, HART, Modbus RTU, and ASCII. HART communications allows the unit to be configured with the use of a Rosemount 275 handheld communicator. Modbus is intended for factory configuration and communication with the Eagle Quantum System.

4 to 20 milli-amp version:

The system comprises of an Eclipse field device wired to a safety rated controller. The signal from the field device to the controller is a 4 to 20 milli-amp signal. . See figure 1 for an example layout.

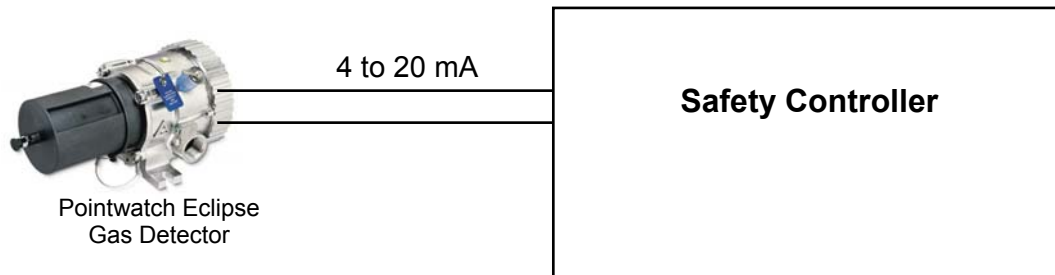


Figure1 – Eclipse - 4 – 20mA communication

3.1 Scope of Analysis

The following were considered in this analysis:

Hardware: Part Number 007168-xxx Serial Numbers 06JANxxxxxx or later

CPU Firmware: Part Number 007228-001 Revision C or D or
Part Number 007455-001 Revision A or B

Reference Drawings:

DWG, DESIGN REFERENCE ECLIPSE (PIRECL) “FM”, 007262-001, Rev. L and higher

DWG, DESIGN REFERENCE ECLIPSE (PIRECL) “DEMKO”, 007263-001, Rev. L and higher

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Det-Tronics and is documented in this section.

4.1 Methodology

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
 - 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
- Evidence that the equipment is proven-in-use
 - Analysis of field failure rates to ensure that no systematic faults exist in the product.

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 Pointwatch Eclipse Gas Detector - Models PIRECL and HC200 has been assessed per IEC 61508 to the following levels:

- SIL 2 capability, single use (Hardware Fault Tolerance = 0)

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



5 Results of the IEC 61508 Functional Safety Assessment

exida-certification assessed the development process used by Det-Tronics during the EQP Safety System IEC 61508 certification against the objectives of IEC 61508 parts 1, 2, and 3, see [D1]. The development of the Pointwatch Eclipse Gas Detector - Models PIRECL and HC200 modules was done per this IEC 61508 SIL 2 compliant development process. The Safety Case created for the EQP Safety System was updated with Pointwatch Eclipse design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Det-Tronics has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D4] and [D9].

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the Det-Tronics 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 Det-Tronics 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 any EQP Safety System development is governed by General Operating Procedure (GOP) 305 [D4]. For each development Det-Tronics creates a Functional Safety Management Plan, see [D1], with specific deliverables, reviews and approvals. This process 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 documented in [D9]. Design drawings and documents are also under version control. Det-Tronics uses CVS for its version control.

Training, Competency recording

Personnel training records are kept in accordance with IEC 61508 requirements and individual competencies are documented in [D1]. Det-Tronics hired *exida-certification* to be the independent assessor per IEC 61508.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D4], a safety requirements specification (SRS) is done for all products that must meet IEC 61508 certification. The requirements specification contains three major sections: Product Specific Safety Requirements, Product Specific Architecture, and Derived Safety requirements. For the PIRECL model, the SRS[D2], has been reviewed by *exida-consulting*. During the assessment, *exida-certification* 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 derived requirements, which map the requirements to the design, and by mapping requirements to appropriate validation tests in the validation test plan [D3]

Items from **IEC 61508-2, Table B.1** include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, and checklists. As the functions of the Pointwatch Eclipse are simple and clearly defined there is no need for semi-formal methods such as functional block diagrams. The application is considered when specifying the requirements; the devices may be required to meet specific applications standards. This meets SIL 2.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D4]. The hardware design process includes component selection, detailed drawings and schematics, a peer review of the design, an authorization review of the design, bench testing, unit testing, and fault injection testing. In addition, an engineering specification (see [D6]) is created for the product which contains technical specifications, safety characteristics, and characteristics of the design that are crucial to the safe and proper functioning of the product. As defined in section 7.4.2.2 the requirements for the avoidance of failures in the hardware design are not required because there is evidence that the PIRECL model is 'proven-in-use'.

The requirements of SIL 2 have been met in this area.

5.1.4 Validation

Validation Testing is done via a set of documented tests (see [D3]). The validation tests are traceable to the Safety Requirements Specification [D2] in the validation test plan [D3]. In addition to standard Test Specification Documents, third party testing may be included as part of agency approvals. As the Pointwatch Eclipse consists of simple electrical devices with a straightforward safety function, there is no separate integration testing necessary.

Procedures are in place for corrective actions to be taken when tests fail as documented in [D1].

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, Interference surge immunity testing, fault insertion testing, project management, documentation, static analysis, dynamic analysis, and failure analysis, expanded functional testing and black-box testing. This meets SIL 2.

5.1.5 Verification

The development and verification activities are defined in [D4] and [D9]. For each phase the objectives are stated, the process is described, and required input and output documents are included. Several checklists are included in [D4], including a checklist for each phase of the development process. Completed phase verification checklists are included in [D10].



5.1.6 Modifications

Modifications are done per the Det-Tronics IEC 61508 SIL 2 compliant development process as documented in [D4]. Consequently this meets SIL 2.

5.1.7 User documentation

Det-Tronics created a Safety Manual for the Pointwatch Eclipse, see [D5]. This safety manual was assessed by *exida-certification*. The final version is considered to be in compliance with the requirements of IEC 61508. The document includes all required reliability data and operations, maintenance, and proof test procedures.

Items from IEC **61508-2, Table B.4** include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities (the Pointwatch Eclipse performs well-defined actions) and operation only by skilled operators (operators familiar with type of devices, although this is partly the responsibility of the end-user). This meets SIL 2.

5.2 Hardware Assessment

To evaluate the hardware design of the Pointwatch Eclipse, a Failure Modes, Effects, and Diagnostic Analysis was performed by exida. This is documented in [D11]. The FMEDA was verified using Fault Injection Testing as part, see [D19].

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. Table 1 lists these failure rates as reported in the FMEDA reports. The failure rates are valid for the useful life of the devices.

Table 1 Failure rates according to IEC 61508

Failure Category	λ_{sd}	λ_{su}^1	λ_{dd}	λ_{du}	SFF
Eclipse-PIRECL IR Gas Detector, Analog Output	118 FIT	645 FIT	1537 FIT	123 FIT	94.6%
Eclipse-PIRECL IR Gas Detector, Relay Output	118 FIT	626 FIT	1322 FIT	132 FIT	94.0%

For low demand SIL 2 applications the PFD_{AVG} value of the Safety Instrumented Function needs to be $\geq 10^{-3}$ and $< 10^{-2}$. The FMEDA report, [D11], lists the percentage that the Pointwatch Eclipse uses of this budget. Considering a proof test is performed every year, the PIRECL model uses 5.5% of the PFD_{AVG} budget when the analog output is used and 5.9% of the PFD_{AVG} budget when the relay output is used.

These results must be considered in combination with PFD_{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_{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF.

The architectural constraints requirements of IEC 61508-2, Table 2 are also reviewed. The Safe Failure Fractions (SFF) for both Pointwatch Eclipse configurations are greater than 94%. Therefore the Pointwatch Eclipse can be used in SIL 2 applications, in simplex (single use) mode.

The analysis shows that design of the Pointwatch Eclipse meets the hardware requirements of IEC 61508 SIL 2, single use (HFT = 0).

¹ It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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).
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
Type A (sub)system	“Non-Complex” (sub)system (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B (sub)system	“Complex” (sub)system (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2



6 Status of the document

6.1 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.

6.2 Releases

Version: V1

Revision: R1

Version History: V0, R1: Internal Draft; March 27, 2009

V0, R2: Updated based on Internal Review; March 31, 2009

V1, R1 Added HC200 Model Number to report

Authors: Michael Medoff

Review: V0, R1: William M. Goble, March 31, 2009

Release status: Released to Customer

6.3 Future Enhancements

At request of client.

6.4 Release Signatures

A handwritten signature in black ink that reads "Michael Medoff".

Michael Medoff, Senior Safety Engineer

A handwritten signature in black ink that reads "William M. Goble".

Dr. William M. Goble, Principal Partner