



IEC 61508 Functional Safety Assessment

Project:

GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor,
350800 Sensor, and 3500/33 Relay Card

Customer:

GE Optimization & Control / Bently Nevada
Minden, NV
USA

Contract No.: Q08/01-54

Report No.: GE 08-01-54 R002

Version V1, Revision R1, December 19, 2008

Iwan van Beurden

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:

GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card

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

- *exida-certification* assessed the development process used by GE Optimization & Control / Bently Nevada 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. A full IEC 61508 Safety Case was prepared, using the *exida SafetyCaseDB™* 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 GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card 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 GE Optimization & Control / Bently Nevada	5
2.4.2 Documentation generated by <i>exida-certification</i>	7
3 Product Description.....	8
3.1 Scope of Analysis.....	9
4 IEC 61508 Functional Safety Assessment.....	11
4.1 Methodology	11
4.2 Assessment level	11
5 Results of the IEC 61508 Functional Safety Assessment.....	12
5.1 Lifecycle Activities and Fault Avoidance Measures	12
5.1.1 Functional Safety Management.....	12
5.1.2 Safety Requirements Specification and Architecture Design	13
5.1.3 Hardware Design.....	13
5.1.4 Software (Firmware) Design.....	13
5.1.5 Validation.....	14
5.1.6 Verification.....	14
5.1.7 Modifications	14
5.1.8 User documentation	15
5.2 Hardware Assessment.....	15
6 Terms and Definitions	17
7 Status of the document	18
7.1 Liability	18
7.2 Releases	18
7.3 Future Enhancements.....	18
7.4 Release Signatures.....	18



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 GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card.



2 Project management

2.1 exida

exida is one of the world's leading 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 partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

exida-certification is the market leader for IEC 61508 certification for industrial control products.

2.2 Roles of the parties involved

GE Optimization & Control / Bently Nevada

Manufacturer of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card

exida-consulting

Provided services to support GE Optimization & Control / Bently Nevada during the development of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card.

exida-certification

Performed the IEC 61508 Functional Safety Assessment according to option 3 (see section 1)

GE Optimization & Control / Bently Nevada contracted *exida* in January of 2008 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.

[N1]	IEC 61508 (Parts 1 - 7): 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
------	----------------------------------	----------------------------------------------------------------------------------------------

2.4 Reference documents

2.4.1 Documentation provided by GE Optimization & Control / Bently Nevada

[D1]	Safety Case	GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card Safety Case
[D2]	283090, Rev NC	3500/63 Haz Gas Functional Safety Management Plan
[D3]	EMS System Screenshot	Intranet based Employee Management System, recording of training plans & records of individuals
[D4]	151762, Rev AD	Parts Release Process
[D5]	162643, Rev H	Safety Program Management Guideline

[D6]	181517, Rev NC	Component Derating Guidelines
[D7]	EEDI-170, Rev 1.0	Product Safety Process Instructions
[D8]	SPS-PSSQM-0420, Rev 2.2	Quality Procedure: Supplier Approval / Outsourcing standard
[D9]	RTM, Rev NC, 12/12/08	Requirements Traceability Matrix
[D10]	283091, Rev C	Functional Safety Requirements for 3500 Hazardous Gas Detection / Protection System
[D11]	e-mail 09/03/08	Safety Requirements Review Minutes, e-mail exchange between Dave Saarem and Brian Gilbert
[D12]	132384, Rev D	3500 Designers Guide
[D13]	167574, Rev NC	3500 6-Channel Firmware Maintenance Manual
[D14]	165868, Rev NC	Firmware Development Methodology
[D15]	Main.c	Sample code file
[D16]	State transition diagrams	Architecture design, collection of state transition diagrams Calibration State Diagram Calibration Steps Calibration SW Map LEL Limits Process Flow Diagram Stat ADC Interrupt Stat Alarm Process Stat Alarm Validation Stat HG Cal Stat HG Cal2 Stat Interrupt Vector Stat main Stat Mon Runtime Stat Mon Status Stat Powerup Selftest Stat SCI Service Stat Update Neuron State Diagram
[D17]	165052, Rev C	Third Party Review Methodology
[D18]	SPLINT test results	SPLINT test results, static source code analysis results
[D19]	Toll gate review	Toll gate review checklists Tollgate 1 checklist Tollgate 2 checklist Tollgate 3 checklist Tollgate 4 checklist Tollgate 5 checklist Tollgate 6 checklist

[D20]	IEC 61508 Tables	IEC 61508 Tables, document shows all tables from IEC 61508 Annex A and B from part 2 and part 3 along with a description as to how GE Optimization & Control / Bently Nevada meets each of the requirements
[D21]	SMCKLST	Safety Manual Checklist
[D22]	GE 08-01-54r2 R001 V1 R3 3500-63	3500/63 Hazardous Gas Detection System Failure Modes, Effects and Diagnostics Analysis (FMEDA)
[D23]	159707, Rev B	C++ Language Coding Standard
[D24]	163179, Rev A	Test results for the 3500/60 Temperature Monitor system test plan.
[D25]	3021960	FM Approval report 3500 Monitoring System with 3500/63 Catalytic Gas Detector
[D26]	3027470	FM Approval report Alternate Remote Sensor for 3500/63 Catalytic Gas Detector
[D27]	166024, Rev B	3500 System Test Plan 163179-XX
[D28]	177490, Rev NC	Automated Test Tool Instruction
[D29]	166848-01, Rev. M	3500 Operations and Maintenance Manual including Safety Manual
[D30]	156233, Rev AR	Product Change Process
[D31]	146090, Rev S	Blank EC Form
[D32]	Impact Analysis Template	Impact Analysis Guideline for Changes (Modifications)
[D33]	Current Test, Rev NC	Test for current draw check on Haz Gaz Monitor

2.4.2 Documentation generated by *exida-certification*

[R1]	GE 08-01-54 R002 V1R1 IEC 61508 Assessment 3500_63, 350800, 3500_33, December 19, 2008	IEC 61508 Functional Safety Assessment for GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card (This document)
------	----------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3 Product Description

The GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card together form a Hazardous Gas Detection System. The 350800 Hazardous Gas Sensor (with or without housing) utilizes a continuous diffusion, catalytic bead technology. The 6-channel 3500/63 Hazardous Gas Monitor is suitable for both simplex and redundant (TMR) 3500 Rack configurations. The 3500/63 provides 4-20mA outputs or can include 3500/33 relay module(s) that the user can program to change state, enabling shutdown of machines or processes and audible and/or visible alarms to protect both human life and machine assets.

Figure 1 shows an overview of the main parts of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card that are included in the mA Output Assembly.

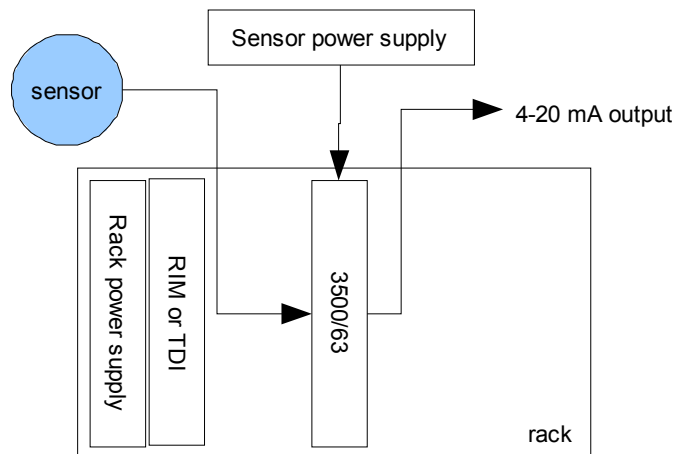


Figure 1 3500/63 Hazardous Gas Detection System mA Output Assembly

Figure 2 shows an overview of the main parts of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card that are included in the Relay Output Assembly.

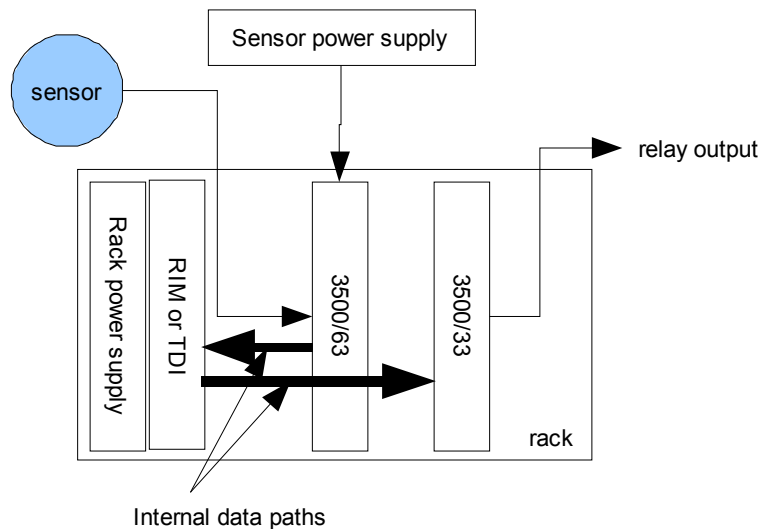


Figure 2 3500/63 Hazardous Gas Detection System Relay Output Arrangement

Table 1 gives an overview of the different versions that were considered in the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card assessment.

Table 1 Version Overview

Current Output	Sensor to 4-20mA output on 3500/63 module
Relay Output	Sensor to 3500/63 module to relay output on 3500/33 relay module

The GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

3.1 Scope of Analysis

The following were considered in this analysis:

Product: 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card

Options: 4-20mA output and Relay output

The critical documents needed to produce these parts are type coded as APE (Approvals Engineering) documents. This ensures that whenever a critical document changes, the release of the document goes through approvals engineering. The following is an overview of the critical documents, schematics, firmware files, etc., for the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card.

¹ Type B device: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.



Table 2 GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card Critical Drawings

Catalog Number	Part Number	Component/Dwg Description	Drawing Type	Drawing No.	Dwg Rev
3500/63	163179-04	6-ch monitor module	Schematic	166020	B
			Component layout	166021	A
			Overall Assy	166174	NC
	164895-01	3500 Catalytic Bead ET I/O	Component layout	164895	A
			Schematic	164896	D
	164578-01	3500 Catalytic Bead IT I/O	Component layout	164578	C
			Schematic	164579	G
	165962-02	3500/6x Microprocessor Odd	Image File Odd	167396	N
	165962-01	3500/6x Microprocessor Even	Image File Even	167397	N
	166848-01	User Manual, 3500/63	Manual	166848	M
3500/33	149986-01	3500 16-Ch Relay Monitor Module	Component layout	162266	NC
			Schematic	162267	NC
			Overall Assy	162268	NC
	149992-01	3500 16-Ch Relay I/O	Component layout	162269	NC
			Schematic	162270	NC
			Overall Assy	162271	NC
			16-ch Relay Firmware	Image File Even	161482
350800	350800-01-XXX-XX	Hazardous Gas Sensor	Overall Assy	350800	B
3500/05	138945-01	3500 Standard Rack Backplane	Component layout	141814	A
			Schematic	141815	A
			Trace layout	141816	A
	144464-01	3500 1/2 Rack Backplane	Component layout	145112	NC
			Schematic	145111	NC
	138953-01	3500 Bulkhead Backplane	Component layout	141403	A
Schematic			141404	B	
Trace layout			141405	B	

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from GE Optimization & Control / Bently Nevada and is documented in [D1].

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 Software HAZOP report

The review of the development procedures is described in section 5.1. The review of the product design is described in section 5.2.

4.2 Assessment level

The GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card 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 (SIL 2) according to IEC 61508.



5 Results of the IEC 61508 Functional Safety Assessment

exida-certification assessed the development process used by GE Optimization & Control / Bently Nevada during the product development against the objectives of IEC 61508 parts 1, 2, and 3, see [D1]. The development of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card was done prior to the establishing of this IEC 61508 SIL 2 compliant development process. Consequently for the evaluation of systematic fault avoidance measures actual measures used and operating experience where considered in addition to documented artifacts identifying potential systematic weaknesses in the current design. The Safety Case was updated with project specific design documents. Future modifications to the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card must be made per the IEC 61508 SIL 2 compliant development process.

5.1 Lifecycle Activities and Fault Avoidance Measures

GE Optimization & Control / Bently Nevada has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D1]. Most of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card functionality was developed before this IEC 61508 compliant development process was in place, consequently the original development process and artifacts were considered and evaluated as suitable for some of the systematic fault avoidance measures.

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the Hazardous Gas Monitor, Sensor, and Relay Card 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 GE Optimization & Control / Bently Nevada 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 GE Optimization & Control / Bently Nevada Safety Instrumented Systems Product development is governed by document 162643 Safety Program Management Guideline [D5] and EEDI-170 Product Safety Process Instructions [D7]. EEDI-170 is part of a detailed tollgate development process within GE for New Product Introductions. It requires that GE Optimization & Control / Bently Nevada create a Functional Safety Management Plan [D2] which is specific for each development project. 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 documented in [D1] and required by EEDI-170 Product Safety Process Instructions [D7]. Design drawings and documents are also under version control. GE Optimization & Control / Bently Nevada uses a SAP based system for its version control.



Training, Competency recording

Personnel training records are kept in accordance with IEC 61508 requirements as documented in [D1] in the Employee Management System, an example is shown in [D3]. GE Optimization & Control / Bently Nevada hired *exida-certification* to be the independent assessor per IEC 61508.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D5], [D7], and [D2] a safety requirements specification (SRS) is created for all products that must meet IEC 61508 requirements. The requirements specification contains a scope and safety requirements section. For the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card, the Functional Safety Requirements [D10], 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. The relation between requirements, tests, etc. is documented in the Requirements Traceability Matrix [D9].

Requirements from **IEC 61508-2, Table B.1** that have been met by GE Optimization & Control / Bently Nevada include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, semi-formal methods and checklists. [D20] documents more details on how each of these requirements has been met. This meets the requirements of SIL 2.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D12][D10] and [D6]. The hardware design process includes component selection, detailed drawings and schematics, safety case documents for agency justification, a Failure Modes, Effects and Diagnostic Analysis (FMEDA), an architecture design review, the creating of prototypes, and hardware verification tests.

Requirements from **IEC 61508-2, Table B.2** that have been met by GE Optimization & Control / Bently Nevada 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, simulation, and inspection of the specification. This is also documented in [D20]. This meets the requirements of SIL 2.

5.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D12] and [D14]. The software design process includes architecture design through state transition diagrams [D16], detailed module design, design and critical code reviews [D17], static source code analysis [D18], and the creation of a firmware maintenance manual explaining the developed firmware for future modifications [D13].



Requirements from **IEC 61508-3, Table A.1 through A.5** that have been met by GE Optimization & Control / Bently Nevada 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, simulation, and inspection of the specification, selection of suitable programming language, use of a defined subset of the language, and others. This is also documented in [D20]. This meets the requirements of SIL 2.

5.1.5 Validation

Validation Testing is done via a set of documented tests (see [D2], [D5], and [D7]). The validation tests are traceable to the Safety Requirements Specification [D9] in the validation test plan [D24]. In addition to standard Test Specification Documents, third party testing may be included as part of agency approvals. As the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card consists of simple electrical devices with a straightforward safety function, integration testing has been limited to verifying that all diagnostics take the appropriate action when they find a problem (see [D1], [D2] for more details on this testing).

Procedures are in place for corrective actions to be taken when tests fail as documented in [D1] and [D7].

Requirements from **IEC 61508-2, Table B.3** that have been met by GE Optimization & Control / Bently Nevada include functional testing, project management, documentation, and black-box testing. Field experience and statistical testing via regression testing are not applicable. [D20] documents more details on how each of these requirements has been met. This meets the requirements of SIL 2.

Requirements from **IEC 61508-2, Table B.5** that have been met by GE Optimization & Control / Bently Nevada include 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, see [D25] and [D26] for third party environmental testing executed specifically for hazardous gas measurement applications. [D20] documents more details on how each of these requirements has been met. This meets SIL 2.

5.1.6 Verification

The development and verification activities are defined in [D2], [D5], and [D7]. Verification activities include the following: Fault Injection Testing, Code Review per [D17], and FMEDA [D22]. Further verification activities are documented in [D2], [D5], and [D7] for new product development projects. Checklists are used as part of each tollgate review process and ensure completeness of the development deliverables [D19]. This meets the requirements of IEC 61508 SIL 2.

5.1.7 Modifications

Modifications are done per the GE Optimization & Control / Bently Nevada' IEC 61508 SIL 2 compliant development process as documented in [D1] and [D2], and governed by [D7]. Impact analyses are performed once the product is released for integration testing, typically at tollgate 5/6 [D32]. This meets the requirements of IEC 61508 SIL 2.



5.1.8 User documentation

GE Optimization & Control / Bently Nevada updated the user manual for the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card and incorporated the requirements for the Safety Manual, see [D29]. 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.

Requirements from IEC **61508-2, Table B.4** that have been met by GE Optimization & Control / Bently Nevada include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities, protection against operator mistakes, and operation only by skilled operators. [D20] 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 GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card, a Failure Modes, Effects, and Diagnostic Analysis was performed by exida consulting for each component in the system. This is documented in [D23]. The FMEDA was verified using Fault Injection Testing as part of the development 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. Table 3 lists these failure rates as reported in the FMEDA report for each of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card parts. Table 4 lists the combined failure rates for a single gas sensor input with mA output and a single gas sensor input with relay output. The failure rates are valid for the useful life of the devices.

Table 3 Failure rates according to IEC 61508 per Part

Device	λ_{sd}	λ_{su}^2	λ_{dd}	λ_{du}	SFF
350800 - gas sensor	0 FIT	38 FIT	2778 FIT	188 FIT	-
3500/63 - per gas sensor input	0 FIT	52 FIT	190 FIT	25 FIT	-
3500/63 - common to all gas sensor inputs	0 FIT	128 FIT	732 FIT	50 FIT	-
3500/63 - per mA output	0 FIT	3 FIT	104 FIT	10 FIT	-
3500/63 - common to all mA outputs	0 FIT	2 FIT	45 FIT	0 FIT	-
3500/33 - per relay output	0 FIT	90 FIT	0 FIT	26 FIT	-
3500/33 - common to all relay outputs	0 FIT	225 FIT	788 FIT	105 FIT	-

Table 4 Failure rates according to IEC 61508 for Specific Configuration

Hazardous Gas Monitor, Sensor, and Relay Card Configuration	λ_{sd}	λ_{su}^2	λ_{dd}	λ_{du}	SFF
Single gas sensor input, mA output	0 FIT	223 FIT	3849 FIT	273 FIT	93.7%
Single gas sensor input, relay output	0 FIT	533 FIT	4488 FIT	394 FIT	92.7%

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 [D22] lists the percentage that the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card uses of this budget. Considering a 90 day proof test interval, required for recalibration of hazardous gas sensor, the Hazardous Gas Monitor, Sensor, and Relay Card uses 3.3% of the PFD_{AVG} budget.

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 analysis shows that design of the GE Optimization & Control / Bently Nevada 3500/63 Hazardous Gas Monitor, 350800 Sensor, and 3500/33 Relay Card meets the hardware requirements of IEC 61508 SIL 2, single use (HFT = 0).

² It is important to realize that the “residual” 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

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 (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 twice the proof test frequency
OC	Optimization & Control
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).
TMR	Triple Modular Redundant
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



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: First Release; December 19, 2008

V0, R1: Internal Draft; November 26, 2008

Authors: Iwan van Beurden

Review: V0, R1: William M. Goble

Release status: First Release

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

A handwritten signature in black ink, appearing to read "Iwan van Beurden".

Iwan van Beurden, Director of Engineering

A handwritten signature in black ink, appearing to read "William M. Goble".

William M. Goble, Principal Partner