



IEC 61508 Functional Safety Assessment

Project:

Mine Safety Appliances Ultima XA, Ultima XE, and Ultima XIR Gas Monitors
(4-20mA output)

Customer:

Mine Safety Appliances
Cranberry Township, PA
USA

Contract No.: Q08/03-14

Report No.: MSA 08-03-14 R006

Version V1, Revision R1, March 2, 2009

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:

Mine Safety Appliances Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA output)

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

- *exida-certification* assessed the development process used by Mine Safety Appliances 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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) for Oxygen, Catalytic Combustible, and IR Gas applications were found to meet the requirements of SIL 2, single use (HFT = 0).

The MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) for applications including the toxic gas sensors were found to meet the requirements of SIL 1, single use (HFT = 0) and SIL 2, redundant use (HFT = 1).

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 Mine Safety Appliances	5
2.4.2 Documentation generated by <i>exida-certification</i>	7
3 Product Description.....	8
3.1 Ultima XA and Ultima XE Series Gas Monitors.....	8
3.2 Ultima XIR Infrared Gas Detector	8
3.3 Scope of Analysis.....	9
4 IEC 61508 Functional Safety Assessment.....	10
4.1 Methodology	10
4.2 Assessment level	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	12
5.1.3 Hardware Design.....	12
5.1.4 Software (Firmware) Design.....	12
5.1.5 Validation.....	13
5.1.6 Verification.....	13
5.1.7 Modifications	13
5.1.8 User documentation	14
5.2 Hardware Assessment.....	14
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

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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output).



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

Mine Safety Appliances

Manufacturer of the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output)

exida-consulting

Provided services to support Mine Safety Appliances during the development of the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output).

exida-certification

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

Mine Safety Appliances 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.

[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 Mine Safety Appliances

[D1]	Safety Case	MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) Safety Case
[D2]	NPD	Mine Safety Appliances New Product Development Process, 3D Define, Design, Deliver
[D3]	MSA 08/03-13 R002, V1R3; 1/30/2009	Ultima X Functional Safety Management Plan
[D4]	CAT-F, Rev 2, 03/07/2007	NA Competance, Awareness, and Training Process Flow Map (CAT-F)

[D5]	CAT-P, Rev 1; 4/23/2008	NA Competence, Awareness, and Training Process (CAT-P)
[D6]	MGR-04, Rev 8; 8/18/2006	Document Change and ECO Generation (MGR-04)
[D7]	NPD(1)-08, Rev 1; 4/8/2008	Identification and Qualification of Key Suppliers (NPD(1)-08)
[D8]	NPD(1)-09, Rev 4; 4/11/2008	Preliminary Design Review/Product Reviews ()
[D9]	SRS checklist, Rev NA, 1/28/2009	Ultima X Completed Safety Requirements Checklist
[D10]	MSA 08/03-14 R001, V1R2, 06-Feb-09	Ultima X Gas Monitor SRS
[D11]	Ultima X Main Module– Safety Discussion According to EN 50271, Rev NA; 1/20/2006	Safety Discussion According to EN50271 UltimaX Main Module
[D12]	Ultima X Sensor Modules – Safety Discussion According to EN 50271, Rev NA; 11/18/2004	Safety Discussion According to EN50271 UltimaX Sensor Modules
[D13]	Flowchart Ultima X Main, Rev 4.0; 11/1/2005	Main Assembly Flow Chart
[D14]	Flowchart Ultima X Sensor, Rev 1.5; 11/1/2004	Sensor Module Flowchart
[D15]	IEC 61508 Tables, Rev NA, 2/29/2008	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 Mine Safety Appliances meets each of the requirements
[D16]	MSA 08/03-14 R004, V1R1; 2/5/2009	Ultima X Validation Test Specification and Plan
[D17]	MSA 04/11-09 R004, V2R2; 2/3/2009	Ultima XA Series Gas Monitors Failure Modes Effects and Diagnostic Analysis
[D18]	MSA 04/11-09 R001, V2R2; 2/3/2009	Ultima XE Series Gas Monitors Failure Modes, Effects and Diagnostic Analysis
[D19]	MSA 04/11-09 R003, V2R2; 2/3/2009	Ultima XIR Failure Modes, Effects and Diagnostics Analysis
[D20]	10036101, Rev 3	Ultima X Series Gas Monitors Instruction Manual
[D21]	Excel spreadsheet, Rev NA	Ultima X Fault Injection Test Results
[D22]	Excel spreadsheet, NA; 1/8/2009	Module Test Results - Main Module
[D23]	Safety Requirements Specification Meeting Minutes , Rev NA; 1/13/2009	Safety Requirements Specification Review Meeting Minutes

[D24]	Ultima X Safety Manual Checklist, Rev NA; 1/29/2009	Completed Safety Manual Checklist
[D25]	FSM Plan Meeting Minutes, Rev NA; 1/30/2009	FSM Plan Review Meeting Minutes
[D26]	Ultima X software design review Checklist, Rev NA; 2/2/2009	Completed Software Design Review Checklist
[D27]	Ultima X Sensor, Rev NA; 2/4/2009	Module Test Results - Sensor Module
[D28]	Architecture Design Checklist, Rev NA; 1/28/2009	Completed System Architecture Design Checklist
[D29]	Attachment 1 of NPD 07/02, Rev 8.05.0000; 7/2/2008	Programming Guidelines (Source Code Standard)
[D30]	10100751, Rev 0	Ultima X Series Gas Monitors Safety Manual
[D31]	Excel spreadsheet, NA	Module Test Results - XiR / IRIS module
[D32]	PCLINT_UltimaX.zip	PC Lint output
[D33]	Validation Test Specification and Plan Meeting Minutes, 02/09/2009	Validation Test Spec Review
[D34]	Word document	Ultima X Flow Control Justification
[D35]	CCS-04, Rev 0; 11/1/2007	Product Concern Report Process
[D36]	Ultima X Rev 7 EMI Verification, Rev NA; 1/12/2006	EMC Test Results
[D37]	IAT, Rev NA; 5/5/2008	Impact Analysis Template
[D38]	MGR-12, Rev 0; 8/10/2007	Potential Safety Issue Response Guidelines
[D39]	NPD(3)-04, Rev 1; 4/14/2008	Production Readiness Review
[D40]	RTMX	Safety Requirements Traceability Matrix
[D41]	VTRES	Validation Test Results

2.4.2 Documentation generated by *exida-certification*

[R1]	MSA 08-03-14 R006 V1R1 IEC 61508 Assessment Ultima XA, XE, XIR, March 2, 2009	IEC 61508 Functional Safety Assessment for Mine Safety Appliances Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA output) (this document)
------	---	---

3 Product Description

3.1 Ultima XA and Ultima XE Series Gas Monitors

The Ultima XA and Ultima XE Series Gas Monitors are microprocessor-based transmitter providing continuous monitoring of combustible and toxic gases and oxygen deficiency. They utilize catalytic or electrochemical detection methods.

The Ultima XA and Ultima XE Series Gas Monitors operate in diffusion mode, with factory-calibrated sensors ready to perform immediately after installation. As with all gas monitors, Ultima XA and Ultima XE Series Gas Monitors must be calibrated periodically with the gas of interest to ensure proper operation.

Two applications of the Ultima XA and Ultima XE Series Gas Monitors have been reviewed for the FMEDA:

1. The Ultima XA and Ultima XE Series Gas Monitors are used in environments where combustible or toxic gas is not constantly present, i.e. for long periods of more than 24 hours (toxic, and catalytic measurement), or for applications where deviations from normal atmosphere concentrations are monitored (oxygen measurement)
2. The Ultima XA and Ultima XE Series Gas Monitors are used in applications where the previous assumptions do not apply.

The Ultima XA and Ultima XE Series Gas Monitors are used in either two-wire or three-wire mode of operation. For safety instrumented systems usage it is assumed that the 4 – 20 mA output or the relay output is used as the primary safety variable. The Ultima XA and Ultima XE Series Gas Monitors are classified as Type B¹ devices according to IEC 61508, having a hardware fault tolerance of 0.

As with all gas monitors of this type, high levels of, or long exposure to, certain compounds in the tested atmosphere could contaminate the sensors. In atmospheres where Ultima XA and Ultima XE Series Gas Monitors may be exposed to such materials, calibration must be performed frequently to ensure that operation is dependable and display indications are accurate. The only absolute method to ensure proper operation of Ultima XA and Ultima XE Series Gas Monitors is to check it with a known concentration of the gas for which it has been calibrated. Consequently, calibration checks must be included as part of the routine inspection of the system.

3.2 Ultima XIR Infrared Gas Detector

The Ultima XIR Infrared Gas Detector is a microprocessor-based, infrared point gas detector for continuous monitoring of combustible gases and vapors. It can operate in high-gas and low-oxygen environments. The Ultima XIR Infrared Gas Detector operation is based on dual wavelength, heated-optics technology, providing definitive compensation for temperature, humidity and aging effects. The IR technology offers long-term stability, eliminating the need for frequent calibrations.

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



It uses an electronically modulated source of infrared energy and detectors that convert the infrared energy into electrical signals. Each detector is sensitive to a different range of wavelengths in the infrared portion of the spectrum. The microprocessor monitors the ratio of the detector signals and correlates this to a %LEL combustible reading.

The Ultima XIR Infrared Gas Detector is used in either two-wire or three-wire mode of operation. For safety instrumented systems usage it is assumed that the 4 – 20 mA output or the relay output is used as the primary safety variable. The Ultima XIR Infrared Gas Detector is classified as a Type B² device according to IEC 61508, having a hardware fault tolerance of 0.

3.3 Scope of Analysis

The following were considered in this analysis:

Product: MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output)

Options: 4-20mA output and Relay output

The associated hardware and software versions are:

Assembly	Hardware version	Software version
Pre-amp assembly	P/n 10028867 Rev. 9 P/n 10028865 Rev. 13 P/n 10028863 Rev. 4	Version 1.10
Main Display	P/n 10037124 Rev. 11 P/n 10028869 Rev. 11 P/n 10037122 Rev. 11 P/n 10037123 Rev. 11 P/n 10037125 Rev. 11	Version 1.3U
Ultima XIR	P/n 10033033 Rev. 4	Version 1.40
Oxygen Sensor	Rev 9	Rev 7
Catalytic Sensor	Rev 13	Rev 7
Toxic Sensor – standard	Rev 4	Rev 7
Toxic Sensor – high gain	Rev 4	Rev 7
Toxic Sensor – extended range	Rev 4	Rev 7

² Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Mine Safety Appliances 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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) have been assessed per IEC 61508 to the following levels:

- SIL 2 capability, single use (Hardware Fault Tolerance = 0) for Oxygen, Catalytic Combustible, and IR Gas applications
- SIL 2 capability, redundant use (Hardware Fault Tolerance = 1) for Toxic Gas applications

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 Mine Safety Appliances during the product development against the objectives of IEC 61508 parts 1, 2, and 3, see [D1]. The development of the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) 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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) must be made per the IEC 61508 SIL 2 compliant development process.

5.1 Lifecycle Activities and Fault Avoidance Measures

Mine Safety Appliances 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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) 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 Gas Monitors 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 Mine Safety Appliances 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 Mine Safety Appliances Safety Instrumented Systems Product development is governed by the 3D New Product Development Process [D2]. The 3D Define, Design, Deliver, New Product Development Process is of a detailed tollgate development process within MSA. It requires that Mine Safety Appliances create a Functional Safety Management Plan [D3] 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 MGR-04 Document Change and ECO Generation [D6]. Design drawings and documents are also under version control.



Training, Competency recording

Personnel training records are kept in accordance with IEC 61508 requirements as documented in [D1] in the Lotus Notes System as part of the PMP (Performance Management Process). This is also governed by [D4] and [D5]. Group managers have access to the review documents of all within their respective groups. Mine Safety Appliances hired *exida-certification* to be the independent assessor per IEC 61508.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D2] and [D3] 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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output), the Safety Requirements Specification [D10] has been reviewed by *exida-consulting* [D9], [D23]. 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 using the “house of reliability” approach. Derived requirements 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 [D40].

Requirements from **IEC 61508-2, Table B.1** that have been met by Mine Safety Appliances include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, semi-formal methods and checklists. [D15] 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 [D2] and [D3]. 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) [D17], [D18], and [D19], an architecture design review [D8], [D13] and [D14], the creating of prototypes, and hardware verification tests.

Requirements from **IEC 61508-2, Table B.2** that have been met by Mine Safety Appliances 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 [D15]. This meets the requirements of SIL 2.

5.1.4 Software (Firmware) Design

Software (firmware) design is done according to [D2] and [D3]. The software design process includes architecture design and review [D8], [D11], and [D12], detailed module design, design and critical code reviews, static source code analysis [D29] and [D31]. Since the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) was developed before the IEC 61508 compliant development process was in place additional firmware evaluations were done like the flow control justification [D34].



Requirements from **IEC 61508-3, Table A.1 through A.5** that have been met by Mine Safety Appliances 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 [D15]. This meets the requirements of SIL 2.

5.1.5 Validation

Validation Testing is done via a set of documented tests (see [D3], [D16] and [D41]). The validation tests are traceable to the Safety Requirements Specification [D10] in the validation test plan [D16]. In addition to standard Test Specification Documents, third party testing may be included as part of agency approvals. As the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) 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 [D3] and [D21] for more details on this testing). All non-conformities are documented in an automated tracking system called TracMSA.

Procedures are in place for corrective actions to be taken when tests fail as documented in [D1] and [D3].

Requirements from **IEC 61508-2, Table B.3** that have been met by Mine Safety Appliances include functional testing, project management, documentation, and black-box testing. Field experience and statistical testing via regression testing are not applicable. [D15] 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 Mine Safety Appliances 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 [D36] for environmental testing executed specifically for hazardous gas measurement applications. [D15] 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 [D3]. Verification activities include the following: Fault Injection Testing [D21], static source code analysis per [D32], FMEDA [D17], [D18], and [D19], and module testing per [D22], [D27], and [D31]. Further verification activities are documented in [D2] for new product development projects and [D3]. Checklists are used as part of each tollgate review process and ensure completeness of the development deliverables [D25], [D26], [D28], [D33], and [D39]. This meets the requirements of IEC 61508 SIL 2.

5.1.7 Modifications

Modifications are done per the Mine Safety Appliances' IEC 61508 SIL 2 compliant development process as documented in [D1] and [D3]. Impact analyses are performed once the product is released for integration testing per the impact analysis template [D37]. Product concerns and customer notifications are governed by [D35] and [D38] respectively. Any customer complaints are handled by a designated team, customer solutions group. Past failure history is input to any new development to ensure appropriate feedback to the development team. This meets the requirements of IEC 61508 SIL 2.



5.1.8 User documentation

Mine Safety Appliances created a safety manual for the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) [D30] which addresses all Safety Manual requirements, see [D24]. 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. In addition to the safety manual an instruction manual exists, see [D20].

Requirements from IEC **61508-2, Table B.4** that have been met by Mine Safety Appliances 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. [D15] 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 MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output), a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida consulting* for each component in the system. This is documented in [D17], [D18], and [D19]. The FMEDA was verified using Fault Injection Testing [D21] 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 1, Table 2, and Table 3 list these failure rates as reported in the FMEDA report for each of the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output). The failure rates are valid for the useful life of the devices.

Table 1 Failure rates according to IEC 61508 Ultima XA Series Gas Monitors

Device	λ_{SD}	λ_{SU}^3	λ_{DD}	λ_{DU}	SFF
Ultima XA Series Gas Monitors, Oxygen, 4-20mA output	0 FIT	139 FIT	4956 FIT	459 FIT	91.8%
Ultima XA Series Gas Monitors, Toxic, 4-20mA output	0 FIT	151 FIT	3337 FIT	2103 FIT	62.7%
Ultima XA Series Gas Monitors, Catalytic, 4-20mA output	0 FIT	190 FIT	5029 FIT	435 FIT	92.4%

³ 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

Table 2 Failure rates according to IEC 61508 Ultima XE Series Gas Monitors

Device	λ_{SD}	λ_{SU}^3	λ_{DD}	λ_{DU}	SFF
Ultima XE Series Gas Monitors, Oxygen, 4-20mA output	0 FIT	139 FIT	4956 FIT	459 FIT	91.8%
Ultima XE Series Gas Monitors, Toxic, 4-20mA output	0 FIT	151 FIT	3337 FIT	2103 FIT	62.7%
Ultima XE Series Gas Monitors, Catalytic, 4-20mA output	0 FIT	190 FIT	5029 FIT	435 FIT	92.4%

Table 3 Failure rates according to IEC 61508 Ultima XIR Infrared Gas Detector

Device	λ_{SD}	λ_{SU}^3	λ_{DD}	λ_{DU}	SFF
Ultima XIR Infrared Gas Detector, 4-20mA output	0 FIT	369 FIT	862 FIT	98 FIT	92.6%

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 reports [D17], [D18], and [D19] lists the percentage that the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) uses of this budget. Considering a 1 year proof test interval, the Gas Monitors use a percentage of the PFD_{AVG} budget that is adequate enough to allow use in SIL 2 applications.

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 the design of the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) for Oxygen, Catalytic Combustible, and IR Gas applications meets the hardware requirements of IEC 61508 SIL 2, single use (HFT = 0).

The analysis shows that the design of the MSA Ultima XA, Ultima XE, and Ultima XIR Gas Monitors (4-20mA Output) for applications including the toxic gas sensors meets the hardware requirements of IEC 61508 SIL 1, single use (HFT = 0) and IEC 61508 SIL 2, redundant use (HFT = 1).

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
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).
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; March 2, 2009
V0, R1: Internal Draft; March 2, 2009
Authors: Iwan van Beurden
Review: V0, R1: Bill Goble (*exida*)
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