Failure Modes, Effects and Diagnostic Analysis

Project:
InSight II Flame Scanner

Company:
FIREYE
Derry, New Hampshire
USA

Contract Number: Q08/04-57
Report No.: FIR 08/04-57 R001
Version V2, Revision R4, March 15, 2010
Rudolf Chalupa

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the InSight II Flame Scanner; Version as per 2.4.1. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the InSight II. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The FIREYE InSight II Flame Scanner is a microprocessor-based flame scanner utilizing solid state infrared (IR) and ultraviolet (UV) sensors. The FIREYE InSight II flame scanner incorporates a 4-20 mA output for each of the sensors, two internal flame relays, and an alarm relay. Each of the flame relays can be programmed to trip on any combination of thresholds of the two sensors. The report also assumes the alarm relay is connected to a system which will annunciate a detected alarm condition.

The InSight II is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0.

The InSight II is a flexible product and can be configured in a variety of ways. The analysis is for a configuration in which the InSight II opens one flame relay when both the IR and UV sensors indicate loss of flame and the alarm relay is connected to an annunciation means.

The analysis shows that the typical configurations of the device have a Safe Failure Fraction greater than 99% and therefore may be used up to SIL 3 as a single device based on hardware architectural constraints.

The failure rates for the InSight II are listed in Table 1.

Table 1 Failure rates InSight II

Failure category	Failure rate (in FITs)
	InSight II IR and UV
Fail Safe Detected	271.2
Fail Safe Undetected	568.9
Fail Dangerous Detected	12.3
Fail Dangerous Undetected	6.2
Residual	145.3
Annunciation Detected	18.6
Annunciation Undetected	12.1

These failure rates are valid for the useful lifetime of the product, see Appendix A.

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

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

Table 2 lists the failure rates for the InSight II according to IEC 61508.

Table 2 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[2]	λ_{DD}	λ_{DU}	SFF
InSight II IR and UV	290 FIT	726 FIT	12 FIT	6 FIT	99.4%

A user of the InSight II can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.4 along with all assumptions.

Table of Contents

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 per 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 1.

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the InSight II. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a sensor subsystem meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

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, safety lifecycle 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.

2.2 Roles of the parties involved

FIREYE Manufacturer of the InSight II

exida Performed the hardware assessment according to Option 1 (see Section 1)

FIREYE contracted *exida* in February 2010 with the hardware assessment of the above-mentioned device.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	exida L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N3]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	exida L.L.C, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N4]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN 1-55617-636-8. Reference on FMEDA methods
[N5]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N6]	Goble, W.M. and Cheddie, H., 2005	Safety Instrumented Systems Verification, Practical Probabilistic Calculations, ISA, ISBN 1-55617-909-X

2.4 Reference documents

2.4.1 Documentation provided by FIREYE

[D1]	Doc # 75-5901, REV NR3	Diagram, Insight 2 Board Interconnection
[D2]	Doc # 75-5911, Rev 5, January 23, 2008	Schematic Drawing, Insight 2 Sensor
[D3]	Doc # 75-5921, Rev 3, January 23, 2008	Schematic Drawing, Insight 2 Supply & I/O
[D4]	Doc # 75-5923, Rev 2, February 8, 2008	Schematic Drawing, Insight II Terminal Board
[D5]	Doc # 75-5924, Rev 1, August 21, 2008	Schematic Drawing, Insight 2 Display Board
[D6]	Doc # 75-5925, Rev 4, February 20, 2008	Schematic Drawing, Insight 2 CPU Board
[D7]	Doc # 75-5936, Rev 3, January 23, 2008	Schematic Drawing, Insight 2 Relay and Comm. Board
[D8]	Doc # 105-4456, Rev H, August 27, 2008	Insight 2 Scanner Software Specification
[D9]	Doc # 75-6108, Rev 1, February 16, 2010	Schematic Drawing, Insight 2 IR Sensor

2.4.2 Documentation generated by *exida*

[R1]	Fireye InSight II - common 03092010.efm, March 9, 2010	Failure Modes, Effects, and Diagnostic Analysis – InSight II Common Sections
[R2]	Fireye InSight II - Fault Relay Output path 03092010.efm, March 9, 2010	Failure Modes, Effects, and Diagnostic Analysis – InSight II Fault Relay Output Path
[R3]	Fireye InSight II - IR signal path 03092010.efm, March 9, 2010	Failure Modes, Effects, and Diagnostic Analysis – InSight II Infrared Detector Signal Path
[R4]	Fireye InSight II - One Flame Relay Output path 03092010.efm, March 9, 2010	Failure Modes, Effects, and Diagnostic Analysis – InSight II Single Flame Relay Output Path
[R5]	Fireye InSight II - uV signal path 03092010.efm, March 9, 2010	Failure Modes, Effects, and Diagnostic Analysis – InSight II Ultraviolet Detector Signal Path
[R6]	Insight II FMEDA Summary 030920101.xls, March 10, 2010	Failure Modes, Effects, and Diagnostic Analysis Summary – InSight II
[R7]	SUMMARY OF FIREYE RELAY REVIEW MEETING.doc, March 8, 2010	Summary of Conclusions – Fireye Relay Review Meeting
[R8]	FIR 08-04-57 R001 V2 R4 Insight II.doc, 03/15/2010	FMEDA report, InSight II (this report)

3 Product Description

The FIREYE InSight II flame scanner is a microprocessor-based flame scanner utilizing solid state infrared (IR) and ultraviolet (UV) sensors. The FIREYE InSight II flame scanner incorporates a 4-20 mA output for each of the sensors, two internal flame relays, and an alarm relay. Each of the flame relays can be programmed to trip on any combination of thresholds of the two sensors. The configuration assumed for this report is one flame relay tripping on loss of flame detected by both sensors. The report also assumes the alarm relay is connected to a system which will annunciate a detected alarm condition.

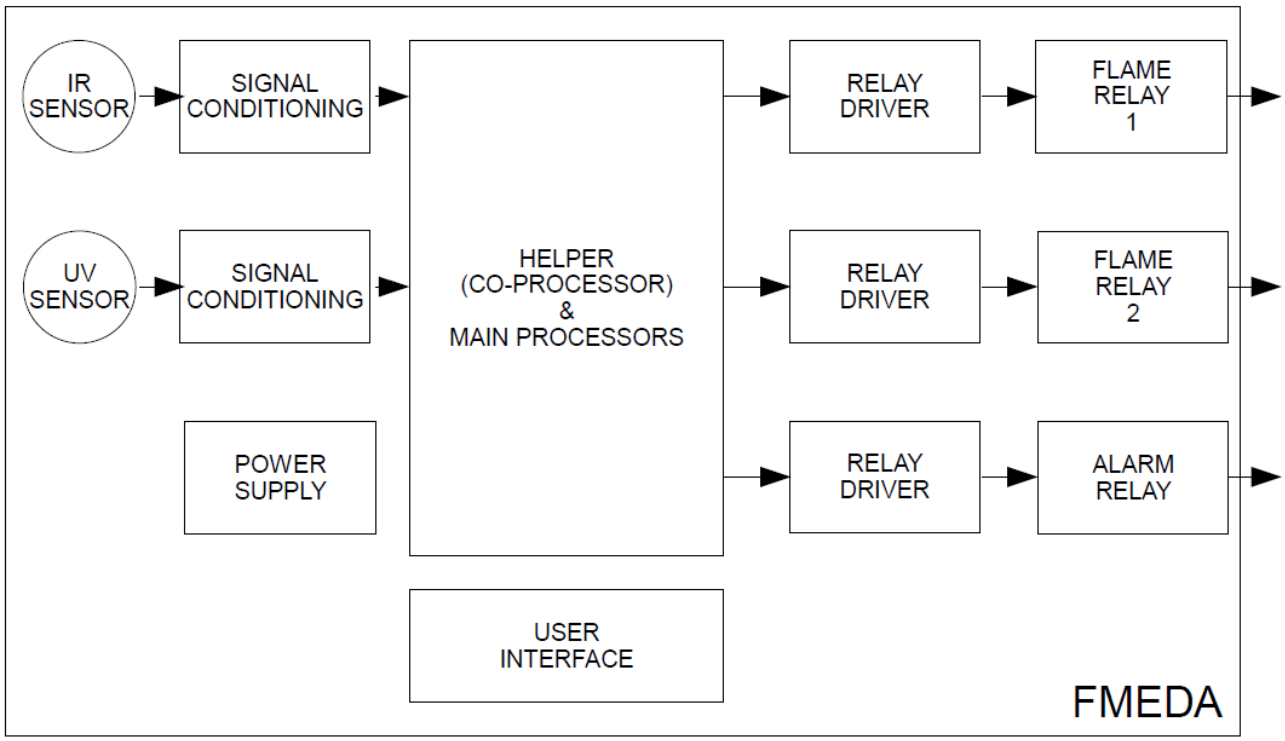


Figure 1 InSight II, Parts included in the FMEDA

The InSight II is classified as a Type B[2] device according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from FIREYE and is documented in [R1]- [R8].

4.1 Failure Categories description

In order to judge the failure behavior of the InSight II, the following definitions for the failure of the device were considered.

Fail-Safe State	State where the flame relay that is part of the safety function is de-energized
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state.
Fail Dangerous	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2000, the Residual failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

4.2 Methodology – FMEDA, Failure Rates

4.2.1 FMEDA

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.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure Rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook which was derived using field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match exida Environmental Profile 3, see Table 3. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

Table 3 exida Environmental Profiles

EXIDA ENVIRONMENTAL PROFILE		GENERAL DESCRIPTION	PROFILE PER IEC 60654-1	AMBIENT TEMPERATURE [°C]		TEMP CYCLE [°C / 365 DAYS]
				AVERAGE (EXTERNAL)	MEAN (INSIDE BOX)	
1	Cabinet Mounted Equipment	Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings	B2	30	60	5
2	Low Power /Mechanical Field Products	Mechanical / low power electrical (two-wire) field products have minimal self heating and are subjected to daily temperature swings	C3	25	30	25
3	General Field Equipment	General (four-wire) field products may have moderate self heating and are subjected to daily temperature swings	C3	25	45	25
4	Unprotected Mechanical Field Products	Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation.	D1	25	30	35

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the InSight II.

- Only a single component failure will fail the entire InSight II
- Failure rates are constant, wear-out mechanisms are not included
- Propagation of failures is not relevant
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded
- The stress levels are average for an industrial environment and can be compared to the exida Environmental Profile 3 with temperature limits within the manufacturer’s rating. Other environmental characteristics are assumed to be within manufacturer’s rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics
- Materials are compatible with process conditions
- The device is installed per manufacturer’s instructions
- External power supply failure rates are not included
- Worst-case internal fault detection time is less than one minute

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the InSight II FMEDA..

The InSight II is a flexible product and can be configured in a variety of ways. The analysis is for a configuration in which the InSight II opens one flame relay when both the IR and UV sensors indicate loss of flame and the alarm relay is connected to an annunciation means.

Table 4 Failure rates InSight II

Failure category	Failure rate (in FITs)
	InSight II IR and UV
Fail Safe Detected	271.2
Fail Safe Undetected	568.9
Fail Dangerous Detected	12.3
Fail Dangerous Undetected	6.2
Residual	145.3
Annunciation Detected	18.6
Annunciation Undetected	12.1

These failure rates are valid for the useful lifetime of the product, see Appendix A.

Table 5 lists the failure rates for the InSight II according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However as the InSight II is only one part of a (sub)system, the SFF should be calculated for the entire sensor combination. The Safe Failure Fraction is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. This is reflected in the following formulas for SFF: $SFF = 1 - \lambda_{DU} / \lambda_{TOTAL}$

Table 5 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	SFF
InSight II IR and UV	290 FIT	726 FIT	12 FIT	6 FIT	99.4%

The architectural constraint type for the InSight II is B. The hardware fault tolerance of the device is 0. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

[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

5 Using the FMEDA Results

5.1 PFD_{AVG} Calculation InSight II

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) InSight II. The failure rate data used in this calculation are displayed above. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. For the proof test a proof test coverage of 67% has been assumed, see Appendix A.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 2. As shown in the graph the PFD_{AVG} value for a single InSight II IR and UV, with a proof test interval of 1 year equals 1.05E-04.

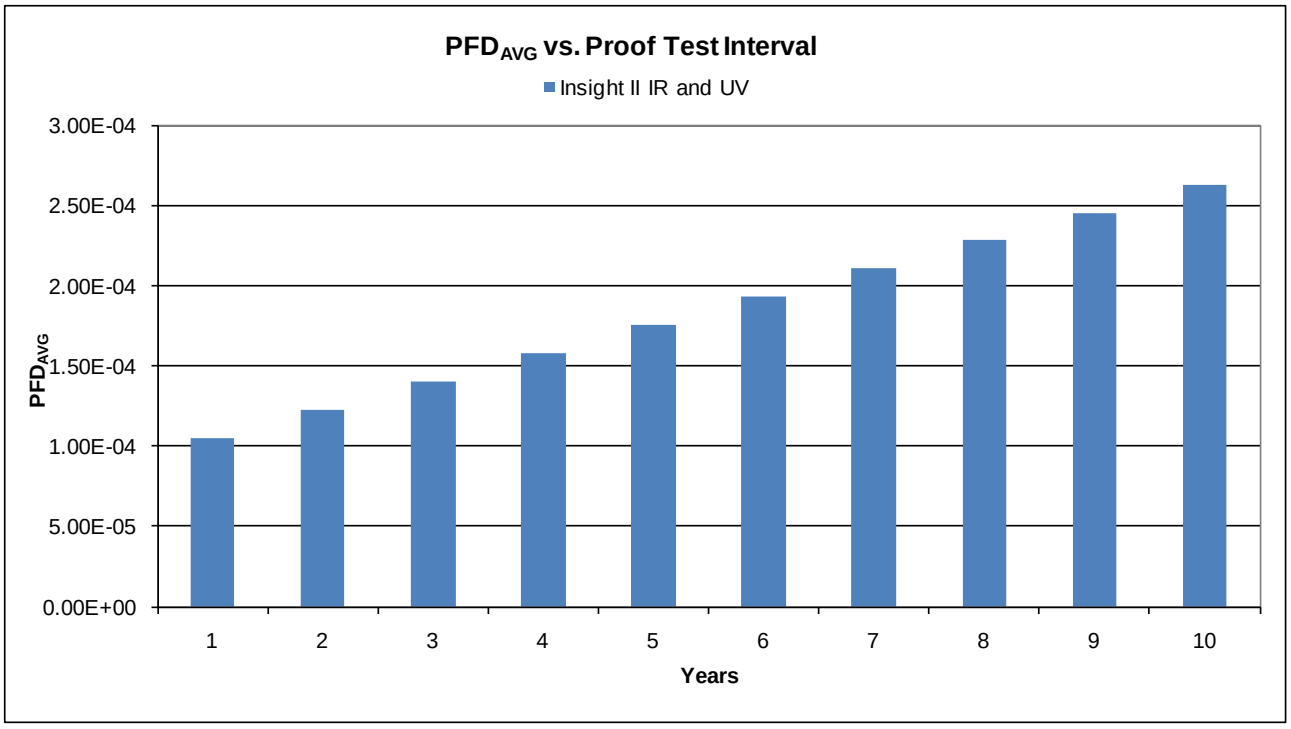


Figure 2: PFDavg vs. time, Insight II

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

For SIL 3 applications, the PFD_{AVG} value needs to be $\geq 10^{-4}$ and $< 10^{-3}$. This means that for a SIL 3 application, the PFD_{AVG} for a 1-year Proof Test Interval of the InSight II IR and UV is approximately equal to 10.5% of the range.

These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Definitions

FIT	Failure In Time (1x10-9 failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the 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
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 component	“Non-Complex” component (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” component (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 FMEDA 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.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

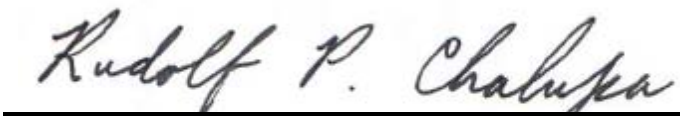
Version:	V2	
Revision:	R4	
Version History:	V2, R4:	Updated block diagram, March 15, 2010
	V2, R3	Updated per client feedback, March 15, 2010
	V2, R2	Updated per internal feedback, March 12, 2010
	V2, R1	New FMEDA, consolidated models, March 11, 2010
	V1, R1.1:	Updated data presentation, October 28, 2008
	V1, R1:	Released to FIREYE; October 27, 2008
	V0, R2:	Sample configurations; October 27, 2008
	V0, R1:	Draft; October 15, 2008
Author(s):	Rudolf Chalupa	
Review:	V0, R2:	Rachel Amkreutz (exida); October 27, 2008
Release Status:	Released to FIREYE	

7.3 Future Enhancements

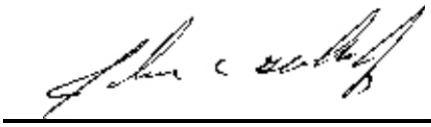
At request of client.

7.4 Release Signatures

Dr. William M. Goble, Principal Partner



Rudolf P. Chalupa, Senior Safety Engineer



John C. Grebe Jr., Principal Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[4] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 17 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 6 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) – Aluminum electrolytic, non-solid electrolyte	Approx. 90,000 hours

It is the responsibility of the end user to maintain and operate the InSight II per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

The limiting factors with regard to the useful lifetime of the system are the aluminum electrolytic capacitors. The aluminum electrolytic capacitors have an estimated useful lifetime of about 10 years.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[4] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B Proof tests to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The suggested proof test consists of a functional test of the scanner to test the flame relay(s) plus a power cycle to test the alarm relay, see Table 7. This test will detect ~ 67% of possible DU failures in the device.

Table 7 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Remove the flame or interrupt the path between the flame and scanner. Confirm flame relay operation. Restore the flame or flame path.
3.	Remove power to the flame scanner. Confirm alarm relay operation. Restore power to the scanner.
4.	Remove the bypass and otherwise restore normal operation