



Failure Modes, Effects and Diagnostic Analysis

Project:
InSight Type 95IR/95UV/95DS Flame Scanners

Customer:
FIREYE
Derry, New Hampshire
USA

Contract No.: FIR 04/08-21
Report No.: FIR 04/08-21 R002
Version V1, Revision R3, December 23, 2010
John C. Grebe – Rachel Amkreutz

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the InSight Type 95IR/95UV/95DS Flame Scanners. 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 Type 95IR/95UV/95DS Flame Scanners. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The FIREYE InSight Type 95IR/95UV/95DS Flame Scanners are microprocessor based flame scanners utilizing a solid state infrared (IR), or ultraviolet (UV), or dual (IR and UV) flame detection sensors. Outputs are provided for flame switch, fault relay and 4 to 20mA flame strength monitoring. The InSight Type 95IR/95UV/95DS Flame Scanners are powered by 24Vdc.

The InSight Type 95IR/95UV/95DS Flame Scanners are classified as Type B¹ devices according to IEC61508, having a hardware fault tolerance of 0. The analysis shows that the flame scanners have a Safe Failure Fraction greater than 99%.

Failure rates for the InSight Type 95IR/95UV/95DS Standard Model S1 Flame Scanners are listed in Table 1.

Table 1 Failure rates InSight Type 95IR/95UV/95DS Standard Model S1 – Flame relay output

Failure category	Failure rate (in FITs)		
	InSight Type 95IR	InSight Type 95UV	InSight Type 95DS
Fail Safe Detected	95	95	95
Fail Safe Undetected	305	311	336
Fail Dangerous Detected	467	467	520
Fail Dangerous Undetected	5	5	5
No Effect	250	251	287
Annunciation Undetected	16	12	16
Safe Failure Fraction	99.6%	99.6%	99.6%

Failure rates for the InSight Type 95IR/95UV/95DS Expanded Model S2 Flame Scanners are listed in Table 2.

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

Table 2 Failure rates InSight Type 95IR/95UV/95DS Expanded Model S2 – Flame relay output

Failure category	Failure rate (in FITs)		
	InSight Type 95IR	InSight Type 95UV	InSight Type 95DS
Fail Safe Detected	95	95	95
Fail Safe Undetected	327	333	358
Fail Dangerous Detected	467	467	520
Fail Dangerous Undetected	5	5	5
No Effect	255	256	292
Annunciation Undetected	16	12	16
Safe Failure Fraction	99.6%	99.6%	99.6%

The failure rates are valid for the useful lifetime of the InSight Type 95IR/95UV/95DS Flame Scanners, see Appendix A.

Table 3 lists the failure rates according to IEC 61508 for the InSight Type 95IR/95UV/95DS Flame Scanners.

Table 3: Failure rates according to IEC 61508

Failure Categories	λ^{SD}	λ^{SU2}	λ^{DD}	λ^{DU}	SFF
Standard Model S1, Type 95IR – Flame relay output	95 FIT	571 FIT	467 FIT	5 FIT	99.6%
Standard Model S1, Type 95UV – Flame relay output	95 FIT	574 FIT	467 FIT	5 FIT	99.6%
Standard Model S1, Type 95DS – Flame relay output	95 FIT	639 FIT	520 FIT	5 FIT	99.6%
Expanded Model S2, Type 95IR – Flame relay output	95 FIT	598 FIT	467 FIT	5 FIT	99.6%
Expanded Model S2, Type 95UV – Flame relay output	95 FIT	601 FIT	467 FIT	5 FIT	99.6%
Expanded Model S2, Type 95DS – Flame relay output	95 FIT	666 FIT	520 FIT	5 FIT	99.6%

A user of the InSight Type 95IR/95UV/95DS Flame Scanners 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.

² Note that these include failures that will not affect system reliability or safety

Table of Contents

Management summary	2
1 Purpose and Scope	5
2 Project management.....	6
2.1 <i>exida.com</i>	6
2.2 Roles of the parties involved	6
2.3 Standards / Literature used	6
2.4 Reference documents	7
2.4.1 Documentation provided by the customer.....	7
2.4.2 Documentation generated by <i>exida.com</i>	7
3 Product Description.....	8
4 Failure Modes, Effects, and Diagnostics Analysis	9
4.1 Description of the failure categories	9
4.2 Methodology – FMEDA, Failure rates.....	9
4.2.1 FMEDA.....	9
4.2.2 Failure rates.....	10
4.3 Assumptions	10
4.4 Results.....	11
4.5 Results in IEC 61508 format.....	13
5 Example PFD _{AVG} calculation InSight Standard Model S1, Type 95DS	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
Appendix A: Lifetime of critical components	18
Appendix B: Proof tests to reveal dangerous undetected faults	19
B.1 Suggested Proof Test	19

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.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of an FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not contain any software assessment.

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

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition, this option includes an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of 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.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, 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 is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 1.

This document shall describe the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the InSight Type 95IR/95UV/95DS Flame Scanners. From these failure rates, the Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

2 Project management

2.1 *exida.com*

exida is one of the world's leading product certification and knowledge companies specializing in automation system safety, availability and cyber-security with over 300 years of cumulative experience in automation systems. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global corporation 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 Type 95IR/95UV/95DS Flame Scanners
exida.com Project leader of the FMEDA

FIREYE contracted *exida.com* in October 2004 with the FMEDA and PFD_{AVG} calculation of the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91 & FMD-97, RAC 1991, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center. Statistical compilation of failure mode distributions for a wide range of components
[N3]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center. Statistical compilation of failure rate data, incl. mechanical and electrical sensors
[N4]	SN 29500	Failure rates of components
[N5]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N6]	Telcordia (Bellcore) Failure rate database and models	Statistical compilation of failure rate data over a wide range of applications along with models for estimating failure rates as a function of the application.
[N7]	Safety Equipment Reliability Handbook, 2003	<i>exida.com</i> L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N8]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods
[N9]	IEC 60654-1: 1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	75-4869, Rev 5, 02/06/06	Schematic, I/O Bd
[D2]	75-4870, Rev 6, 04/20/07	Schematic, CPU Bd
[D3]	75-5540, Rev 4, 04/20/07	Schematic, Sensor Bd.
[D4]	75-4873, Rev 5, 06/27/06	Schematic, Filter Bd.
[D5]	127-3340, Rev 4, 06/27/06	Parts list for 61-6913
[D6]	127-3530, Rev 1, 04/20/07	Parts list for 61-6947
[D7]	127-3409, Rev 4, 04/20/07	Parts list for 61-7106
[D8]	127-3341, Rev 2, 02/06/06	Parts list for 61-6909
[D9]	CU-95.pdf, 08/26/08	Type 95IR/95UV/95DS Model S1, S2 Integrated Flame Scanner with Internal Flame Relay, product literature
[D10]	127-3541, Rev 3, 07/08/09	Parts list for 61-6948 (display)

2.4.2 Documentation generated by *exida.com*

[R1]	InSight - 4-20mA Output.xls, 11/30/04	FMEDA, InSight Type 95IR/95UV/95DS Flame Scanners, 4-20mA Output (exida internal document)
[R2]	InSight - Common.xls, 11/30/04	FMEDA, InSight Type 95IR/95UV/95DS Flame Scanners, Common (exida internal document)
[R3]	InSight - Relay Output.xls, 11/30/04	FMEDA, InSight Type 95IR/95UV/95DS Flame Scanners, Relay Output (exida internal document)
[R4]	InSight - IR Sensor.xls, 11/30/04	FMEDA, InSight Type 95IR/95UV/95DS Flame Scanners, IR Sensor (exida internal document)
[R5]	InSight - UV Sensor.xls, 11/30/04	FMEDA, InSight Type 95IR/95UV/95DS Flame Scanners, UV Sensor (exida internal document)
[R6]	InSight Summary.xls, 11/29/04	FMEDA, InSight Type 95IR/95UV/95DS Flame Scanners, Failure Rate Summary (exida internal document)
[R7]	FIR 04-08-21 R002 V1 R3 Insight FMEDA Report.doc, 12/20/2010	FMEDA report, InSight Type 95IR/95UV/95DS Flame Scanners (this report)

3 Product Description

This report documents the results of the Failure Modes, Effects and Diagnostics Analysis performed for the InSight Type 95IR/95UV/95DS Flame Scanners. The FIREYE InSight Type 95IR, 95UV, and 95DS flame scanners are used to detect the presence or absence of a target flame in single or multi-burner application.

The InSight 95IR (infrared flame sensor), 95UV (ultraviolet flame sensor), and 95DS (Dual flame sensors) scanners measure the amplitude of the modulations (the flame “flicker”) that occur within the targeted flame. During the scanner set-up procedure, the modulation frequency that yields the best flame ON/OFF discrimination is selected. The appropriate modulation frequency and sensor gain is either manually selected (S1 models), or automatically selected with manual override capability (S2 models). The InSight scanners are each available in two models differentiated by feature levels.

- Standard Model S1, which has three choices of modulation frequency, adjustable sensor gain, adjustable flame relay ON/OFF thresholds, 4-20 mA analog signal strength output, fault relay, and two selectable programmable files to store setpoints (for two different fuels or firing rates).
- Expanded Model S2, which adds automatic programming (AutoTune) with manual override capability, 21 choices of flame flicker frequency, a total of four selectable programmable files to store setpoints, plus adds remote communication capability via Fireeye Windows 95/98/NT user software.

All FIREYE InSight scanner models are powered by 24 Vdc and contain electronic self-checking (no mechanical shutter required).

- The FLAME RELAY is energized (and its normally open contacts close) when the signal strength is at or above the programmed flame ON threshold. The flame relay is de-energized when the signal strength is at or below the programmed flame OFF threshold. The flame relay contact circuit will also open upon a power interruption or the detection of an internal fault (see below).
- The FAULT RELAY is energized when the scanner is powered (24 vdc) and when the scanner has successfully passed all internal self-checking routines. The Fault relay is de-energized if there is a power interruption to the scanner or if the scanner has detected an internal fault. A normally open (fault relay) contact is wired in series with the flame relay contact (internally), and a normally closed contact is available for alarm indication.

The InSight Type 95IR/95UV/95DS Flame Scanners are classified as Type B³ devices according to IEC61508, having a hardware fault tolerance of 0.

³ Type B component: “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 Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation received from FIREYE and is documented in [R1] through [R6].

4.1 Description of the failure categories

In order to judge the failure behavior of the InSight Type 95IR/95UV/95DS Flame Scanners, the following definitions for the failure of the product were considered.

InSight Type 95IR/95UV/95DS Flame Scanners with Flame relay output

Fail-Safe State	State where flame relay is de-energized
Fail Safe	Failure that causes the flame scanner to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	Failure that prevents the flame scanner from going to the defined fail-safe state when a demand occurs and that leaves the flame relay energized.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics.
Fail No Effect	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 [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that Fail High or Fail Low failures may be detected or undetected depending on the programming of the logic solver.

The Annunciation Undetected failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected 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.

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.

An 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) 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.com* in this FMEDA is from a proprietary component failure rate database derived using the Telcordia [N6] failure rate database/models, the SN29500 [N4] failure rate database and other sources. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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 Type 95IR/95UV/95DS Flame Scanners.

- Only a single component failure will fail the entire product
- 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 application program in the logic solver is constructed in such a way that the Fault Relay is recognized as a diagnostic function.
- The stress levels are average for an industrial environment and can be compared to IEC 60654-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

4.4 Results

Using reliability data extracted from the exida.com component reliability database the following failure rates resulted from the InSight Type 95IR/95UV/95DS Flame Scanners FMEDA.

Table 4 Failure rates InSight Type 95IR/95UV/95DS Standard Model S1 – Flame relay output

Failure category	Failure rate (in FITs)		
	InSight Type 95IR	InSight Type 95UV	InSight Type 95DS
Fail Safe Detected	95	95	95
Fail Safe Undetected	305	311	336
Fail Dangerous Detected	467	467	520
Fail Dangerous Undetected	5	5	5
No Effect	250	251	287
Annunciation Undetected	16	12	16

Table 5 Failure rates InSight Type 95IR/95UV/95DS Expanded Model S2 – Flame relay output

Failure category	Failure rate (in FITs)		
	InSight Type 95IR	InSight Type 95UV	InSight Type 95DS
Fail Safe Detected	95	95	95
Fail Safe Undetected	327	333	358
Fail Dangerous Detected	467	467	520
Fail Dangerous Undetected	5	5	5
No Effect	255	256	292
Annunciation Undetected	16	12	16

The failure rates as displayed above are the same failure rates as stored in the exida.com equipment database that is part of the online SIL verification tool, SILver.

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the InSight Type 95IR/95UV/95DS Flame Scanners should be calculated. The SFF is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. The Safe Failure Fraction of the InSight Type 95IR/95UV/95DS Flame Scanners can be calculated using the following formula for SFF:

$$SFF = 1 - \lambda_{du} / \lambda_{total}$$

Note that according to IEC61508 definition the No Effect and Annunciation Undetected failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

Table 6 Safe Failure Fraction of InSight Type 95IR/95UV/95DS Flame Scanners

InSight Type 95IR/95UV/95DS Flame Scanners	SFF
Standard Model S1, Type 95IR – Flame relay output	99.6%
Standard Model S1, Type 95UV – Flame relay output	99.6%
Standard Model S1, Type 95DS – Flame relay output	99.6%
Expanded Model S2, Type 95IR – Flame relay output	99.6%
Expanded Model S2, Type 95UV – Flame relay output	99.6%
Expanded Model S2, Type 95DS – Flame relay output	99.6%

The architectural constraint type for InSight Type 95IR/95UV/95DS Flame Scanners is B. 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.

4.5 Results in IEC 61508 format

The failure rates that are derived from the FMEDA for the InSight Type 95IR/95UV/95DS Flame Scanners are in a format different from the IEC 61508 format. This section explains how the failure rates can be converted into the IEC 61508 format.

The No Effect failures and Annunciation Undetected failure are classified as Safe Undetected failures according to IEC 61508. Note that these failures will not affect system reliability or safety, and should not be included in spurious trip calculations.

Table 7 lists the IEC 61508 failure rates for the InSight Type 95IR/95UV/95DS Flame Scanners.

Table 7: Failure rates according to IEC 61508

Failure Categories	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	SFF
Standard Model S1, Type 95IR – Flame relay output	95 FIT	571 FIT	467 FIT	5 FIT	99.6%
Standard Model S1, Type 95UV – Flame relay output	95 FIT	574 FIT	467 FIT	5 FIT	99.6%
Standard Model S1, Type 95DS – Flame relay output	95 FIT	639 FIT	520 FIT	5 FIT	99.6%
Expanded Model S2, Type 95IR – Flame relay output	95 FIT	598 FIT	467 FIT	5 FIT	99.6%
Expanded Model S2, Type 95UV – Flame relay output	95 FIT	601 FIT	467 FIT	5 FIT	99.6%
Expanded Model S2, Type 95DS – Flame relay output	95 FIT	666 FIT	520 FIT	5 FIT	99.6%

5 Example PFD_{AVG} calculation InSight Standard Model S1, Type 95DS

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) architecture with *exida's* exSILentia tool⁴. The failure rate data used in this calculation is displayed in section 4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 24 hours. Table 8 lists the proof test coverage (see Appendix B) used as well as the results when the proof test interval equals 1 year.

Table 8 Sample PFD_{AVG} Results

Device	Proof Test Coverage	PFD _{AVG}	% of SIL 3 Range
InSight Standard Model S1, Type 95DS	60%	1.17E-04	11.7%

The resulting PFD_{AVG} Graph generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 1.

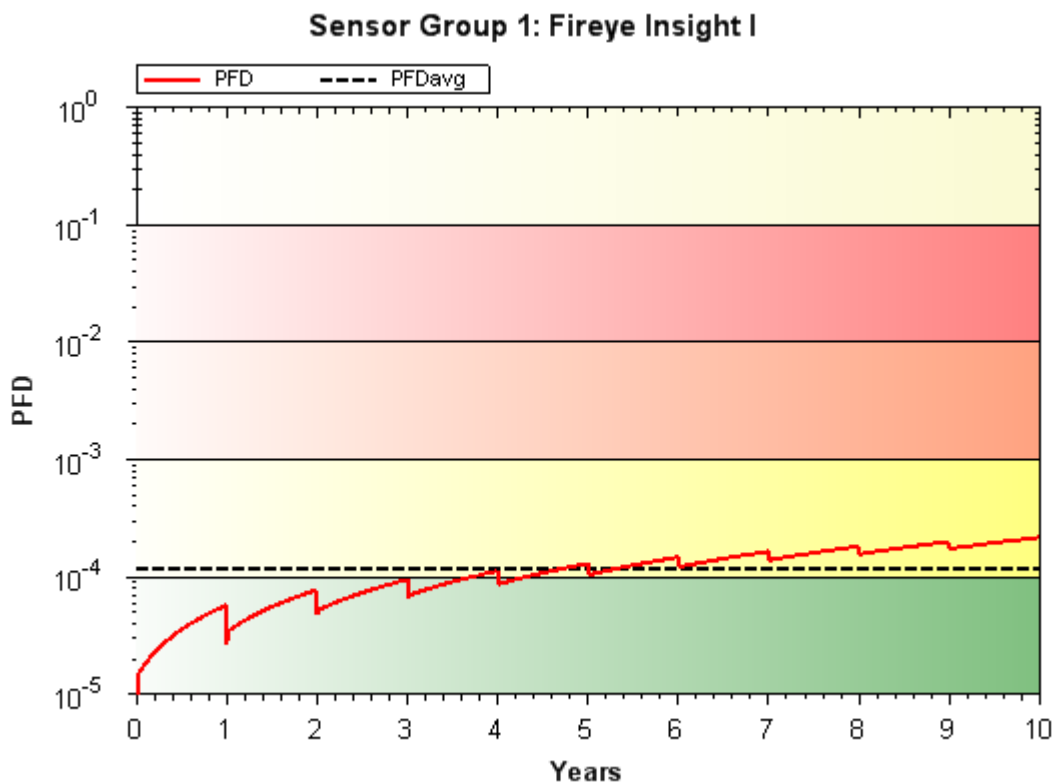


Figure 1: PFD_{AVG} InSight Standard Model S1, Type 95DS

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.

⁴ V3.0.0.670 of *exida's* exSILentia was used to generate the PFD_{AVG} values and Graphs.



For SIL 3 applications, the PFD_{AVG} value for a safety function needs to be $< 10^{-3}$. This means that for a SIL 3 application, the PFD_{AVG} for a 1-year Proof Test Interval of the InSight Type 95IR/95UV/95DS Flame Scanners with flame relay output is equal to 11.7% 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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
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 7.4.3.1.3 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.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* 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: R3

Version History: V1, R3: Reviewed updated documents, updated Section 2.4.1, R. Chalupa, December 22, 2010

V1, R2: Updated with newer standard test; eliminated references to analog output, R. Chalupa, December 20, 2010

V1, R1: Released to FIREYE, December 1, 2004

V0, R1: Draft; November 30, 2004

Authors: John C. Grebe – Rachel Amkreutz

Review: V1, R2: William Goble (*exida*), December 20, 2010

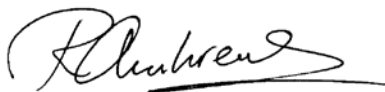
V0, R1: Rachel Amkreutz (*exida.com*); November 30, 2004

Release status: Released

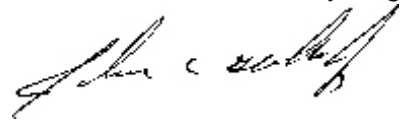
7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Ir. Rachel Amkreutz, Safety Engineer



John C. Grebe Jr., Principal Engineer



Dr. William M. Goble, Principal Partner

Appendix A: Lifetime of critical components

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime 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 component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 9 shows which electrolytic capacitors are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 9: Useful lifetime of electrolytic capacitors contributing to λ^{DU}

Type	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500 000 hours
Capacitor (electrolytic) – Aluminum electrolytic, non-solid electrolyte	Approx. 90 000 hours

As the capacitors are the limiting factor with regard to the useful life of the flame scanner, the useful lifetime should be limited to 10 years.

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 FMEDA can be detected during proof testing.

B.1 Suggested Proof Test

The suggested proof test described in Table 10 will detect approximately 60% of possible DU failures in the Insight I.

Table 10 Suggested Proof Test – Insight I

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Interrupt power to the Insight I.
3.	Verify that the output relay and fault relay are open.
4.	Restore power to the Insight I.
5.	Remove the flame or interrupt the path between the flame and the Insight I
6.	Verify that the output relay opens.
7.	Remove the bypass and otherwise restore normal operation