Failure Modes, Effects and Diagnostic Analysis

Project:
Netherlocks FAITH System PP-Series

Company:
Netherlocks Safety Systems B.V.
Alphen aan den Rijn,
Netherlands

Contract Number: Q09/09-47
Report No.: NET 09/09-47 R001
Version V1, Revision R2, January 27, 2010
Steven Close

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 Netherlocks FAITH System PP-Series. 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 Netherlocks FAITH System PP-Series. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Netherlocks Fail Action Integrity Test Handling (FAITH) system makes it possible to conduct a manually initiated partial valve stroke test on an ESD valve during normal operation by limiting the stroke of the valve-actuator combination to a fixed percentage. Any percentage of openings can be requested. The stroke is limited by the introduction of mechanical stops that are manually activated. The standard bracket and coupling between actuator and valve are replaced with the FAITH System PP-Series. The FAITH System PP-Series is protected from unauthorized use by a key that must be inserted to activate the stops. The FAITH System PP-Series is available with a single Lockpin or a dual Lockpin to match the torque developed by the actuator.

The FMEDA considers the FAITH System PP-Series a component of the valve-actuator combination. The FMEDA includes only failures that would impede valve-actuator operation under normal operating conditions. The FMEDA does not include failures that may occur while the FAITH System PP-Series is in the test mode unless they would subsequently interfere with the valve-actuator operation once the FAITH System PP-Series is returned to the normal operating mode.

The failure rates of the correct version of the FAITH System PP-Series must be added to the failure rates of the valve-actuator combination when determining the PFD_{AVG} and Safe Failure Fraction (SFF) for the final element. For applications with valve-actuator combinations that do not use an intermediate bracket and adapter shaft, use the 1 PIN or 2 PIN versions. For applications where the valve-actuator combinations employ an intermediate bracket and adapter shaft, use the “1 PIN w/out Adapters” or “2 PIN w/out Adapters” versions. It must also be noted that the FAITH system disables the safety instrumented function when in use and will cause a failure on demand if the demand occurs during the testing. Therefore the PFDavg calculation must account for the average test time per test interval and the increased probability of failure on demand must be added to the PFDavg calculated using the failure rates.

The FAITH System PP-Series is classified as a Type A[1] device according to IEC 61508, having a hardware fault tolerance of 0. The complete final element subsystem, of which a FAITH System PP-Series is a component of the final control element, will need to be evaluated to determine the Safe Failure Fraction. Note that failures in the actuator-valve detected by a manually initiated partial stroke test as done with the Netherlocks FAITH system are not counted as "detected" in a Safe Failure Fraction calculation as the SFF calculation assumes automatic testing done at least ten times within the expected demand interval.

[1] Type A device: “Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the FAITH System PP-Series.

Table 1 Version Overview

Application	Description
2 PIN FAITH	Used when existing valve-actuator do not require an intermediate bracket and adapter.
2 PIN FAITH W/out Adapters	Used when existing valve–actuator intermediate bracket and adapter are replaced by FAITH System.
1 PIN FAITH	Used when existing valve-actuator do not require an intermediate bracket and adapter.
1 PIN FAITH W/out Adapters	Used when existing valve–actuator intermediate bracket and adapter are replaced by FAITH System.

The failure rates for the Netherlocks FAITH System PP-Series are listed in Table 2.

Table 2 Failure rates Netherlocks FAITH System PP-Series

Failure Category	Failure Rate (FIT)			
	2 PIN	2 PIN w/out Adapters	1 PIN	1 PIN w/out Adapters
Fail Safe Detected	0	0	0	0
Fail Safe Undetected	0	0	0	0
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	54	15	43	4
Residual	83	39	52	7

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

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 3 lists the failure rates for Netherlocks FAITH System PP-Series according to IEC 61508.

Table 3 Failure rates according to IEC 61508.

Device	λ_{SD} (FIT)	λ_{SU}[2] (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	SFF[3]
2 PIN	0	83	0	54	--
2 PIN w/out adapters	0	39	0	15	
1 PIN	0	52	0	43	
1 PIN w/out adapters	0	7	0	4	

A user of Netherlocks FAITH System PP-Series 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] 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

[3] Safe Failure Fraction needs to be calculated on (sub)system level

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 Netherlocks FAITH System PP-Series. 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 final element 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 product certification and 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 global company 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

Netherlocks Safety Systems B.V.	Manufacturer of Netherlocks FAITH System PP-Series
exida	Performed the hardware assessment according to Option 1 (see Section 1)

Netherlocks Safety Systems B.V. contracted *exida* in September 2009 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 Netherlocks Safety Systems B.V.

[D1]	F-0142_00, A3	Faith, 2-Pin, Drawing & Bill of material 2 PIN Faith, 2 pages
[D2]	F-0142_03, A3	Bracket Assembly, Assembly Drawing
[D3]	F-0142_18, A2	Adaptor, Part Drawing
[D4]	F-0142_00, A3	Faith, 2-Pin, Drawing & Bill of material 2 PIN Faith, 2 pages
[D5]	N/A	Sample Quotation, Sample Quotation
[D6]	F-0148_00, A3	Faith, 1 Pin, Drawing & Bill of material 1 PIN Faith, 2 pages
[D7]	F-0148_03, A4	Bracket Assembly, Assembly Drawing
[D8]	F-0148_11, A3	Lockpin, Part Drawing
[D9]	F-0148_15, A3	Lever, Part Drawing
[D10]	F-0148_18, A3	Adapter, Part Drawing
[D11]	F-0148_00, A3	Faith, 1 Pin, Drawing & Bill of material 1 PIN Faith, 2 pages

2.4.2 Documentation generated by *exida*

[R1]	NET_Q090947_FAITH_FMEDA_r1.xls	Failure Modes, Effects, and Diagnostic Analysis – FAITH System PP-Series
[R2]	NET_Q090947_FAITH_FMEDA_R001 _V1R2.doc, 01/27/2010	FMEDA report, FAITH System PP-Series (this report)

3 Product Description

The Netherlocks Fail Action Integrity Test Handling (FAITH) system makes it possible to conduct a manually initiated partial valve stroke test on an ESD valve during normal operation by limiting the stroke of the valve-actuator combination to a fixed percentage. Any percentage of openings can be requested. The stroke is limited by the introduction of mechanical stops that are manually activated. The standard bracket and coupling between actuator and valve are replaced with the FAITH System PP-Series. The FAITH System PP-Series is protected from unauthorized use by a key that must be inserted to activate the stops. The FAITH System PP-Series is available with a single Lockpin or a dual Lockpin to match the torque developed by the actuator. The FAITH System PP-Series is available with or without a shaft Adapter.

The FMEDA considers the FAITH System PP-Series a component of the valve-actuator combination. The FMEDA includes only failures that would impede valve-actuator operation under normal operating conditions. The FMEDA does not include failures that may occur while the FAITH System PP-Series is in the test mode unless they would subsequently interfere with the valve-actuator operation once the FAITH System PP-Series is returned to the normal operating mode. The failure rates of the correct version FAITH System PP-Series must be added to the failure rates of the valve-actuator combination when determining the PFD_{AVG} and Safe Failure Fraction (SFF) for the final element. It must also be noted that the FAITH system disables the safety instrumented function when in use and will cause a failure on demand if the demand occurs during the testing. Therefore the PFDavg calculation must account for the average test time per test interval and the increased probability of failure on demand must be added to the PFDavg calculated using the failure rates.

The FAITH System PP-Series is classified as a Type A[4] device according to IEC 61508, having a hardware fault tolerance of 0. The complete final element subsystem, of which a FAITH System PP-Series is a component of the final control element, will need to be evaluated to determine the Safe Failure Fraction.

[4] Type A device: “Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2.

Figure 1 show the FAITH System PP-Series and depicts the boundaries of the FMEDA.

Figure 1 FAITH System PP-Series with two Lockpins

Netherlocks FAITH System PP-Series is classified as a Type A[5] device according to IEC 61508, having a hardware fault tolerance of 0.

[5] Type A device: "Non-Complex" subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2.

Table 4 gives an overview of the different versions that were considered in the FMEDA of the FAITH System PP-Series.

Table 4 Version Overview

Application	Description
2 PIN FAITH	Used when valve-actuator do not require an intermediate bracket and adapter.
2 PIN FAITH w/out Intermediate Bracket and Adapter	Used when existing valve–actuator intermediate bracket and adapter are replaced by FAITH System.
1 PIN FAITH	Used when valve-actuator do not require an intermediate bracket and adapter.
1 PIN FAITH w/out Intermediate Bracket and Adapter	Used when existing valve–actuator intermediate bracket and adapter are replaced by FAITH System.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from Netherlocks Safety Systems B.V. and is documented in [R1].

4.1 Failure Categories description

In order to judge the failure behavior of Netherlocks FAITH System PP-Series, the following definitions for the failure of the devices were considered.

Fail-Safe State	State where the valve is closed or open depending on the safety function of the final element subsystem.
Fail Safe	Failure that causes the valve device to go to the defined fail-safe state without a demand from the process.
Fail Safe Undetected	Failure that is safe and that is not being diagnosed by automatic diagnostics.
Fail Safe Detected	Failure that is safe and is detected by automatic diagnostics.
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, such as partial valve stroke testing.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics, such as partial valve stroke testing.
Residual	Failure of a component that is part of the safety function but that has no effect on the safety function.

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.

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 Profile 3, see Table 5. 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 5 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 Netherlocks FAITH System PP-Series.

- Only a single component failure will fail the entire FAITH System PP-Series.
- 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* 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.
- Materials are compatible with process conditions.
- The device is installed per manufacturer's instructions.
- Anaerobic adhesives are used during assembly of the FAITH System PP-Series to assure fasteners do not come loose under vibration.
- Applications requiring precise positioning of the valve may be effected due to the design of the adapter coupling.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the FAITH System PP-Series FMEDA.

Table 6 Failure rates for Netherlocks FAITH System PP-Series

Failure Category	Failure Rate (FIT)			
	2 PIN	2 PIN w/out Adapters	1 PIN	1 PIN w/out Adapters
Fail Safe Detected	0	0	0	0
Fail Safe Undetected	0	0	0	0
Fail Dangerous Detected	0	0	0	0
Fail Dangerous Undetected	54	15	43	4
Residual	83	39	52	7

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

Table 7 lists the failure rates for Netherlocks FAITH System PP-Series according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

As the FAITH System PP-Series is only one part of a (sub)system, the SFF should be calculated for the entire final element 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 - $\lambda_{DU} / \lambda_{TOTAL}$

Note that the Netherlocks FAITH system is a device used to facilitate a manual proof test and such manually obtained test results that detect final element subsystem failures do not impact the SFF calculation.

Table 7 Failure rates according to IEC 61508 Clean Service

Device	λ_{SD} (FIT)	λ_{SU}[6] (FIT)	λ_{DD} (FIT)	λ_{DU} (FIT)	SFF[7]
2 PIN	0	83	0	54	--
2 PIN w/out Adapters	0	39	0	15	
1 PIN	0	52	0	43	
1 PIN w/out Adapters	0	7	0	4	

The architectural constraint type for a FAITH System PP-Series is A. 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.

[6] 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

[7] Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

5.1 PFD_{AVG} Calculation FAITH System PP-Series

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) FAITH System PP-Series. The failure rate data used in this calculation is displayed in section 4.4. A mission time of 10 years has been assumed and a Mean Time To Restoration of 96 hours. Manual Proof Test Time of 1 hour is assumed. Table 8 lists the proof test coverage, Random PFD_{AVG}, and percent of SIL range for a FAITH System PP-Series when the proof test interval equals 1 year.

Test Time PFDavg is calculated using a ratio of average test time divided by the average test interval. For a test time of 1 hour and test interval of one year the result is (1 / 8760) = 1.14E-04.

For SIL 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. 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.

Table 8 Sample Results

Device	Proof Test Coverage	Random Failure PFD_{AVG}	Test Time PFD_{AVG}	Total PFDavg	% of SIL 2 Range	Random Failure PFD_{AVG} For 100% Proof Test Coverage[8]
2 PIN	43%	1.45E-03	1.14E-04	1.56E-03	15.6%	2.37E-04
2 PIN w/out Adapters	93%	1.07E-04	1.14E-04	2.21E-04	2.2%	6.57E-05
1 PIN	30%	1.37E-03	1.14E-04	1.48E-03	14.8%	1.88E-04
1 PIN w/out Adapters	99%	1.91E-05	1.14E-04	1.33E-04	1.3%	1.75E-05

[8] The PFD_{AVG} results are based on a simplified equation that assumes 100% Proof Test Coverage. These PFD_{AVG} results can be used for comparison with the PFD_{AVG} results of other products that also used the simplified PFD_{AVG} equation.

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 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 7.4.3.1.2 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
Severe service	Condition that exists when material through the valve has abrasive particles, as opposed to Clean Service where these particles are absent.
Proof Tests	See Appendix B

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:	V1	
Revision:	R2	
Version History:	V1, R2	Added 1 PIN & revised rates w/out adapters, S. Close Jan 19, 2010.
	V1, R1:	Released to Netherlocks Safety Systems B.V.; January 13, 2010
	V0, R1:	Draft; January 11, 2010
Author(s):		Steven Close
Review:	V0, R1:	Gregory Sauk (*exida*); January 12, 2010
	V1, R2:	William Goble (exida); January 26, 2010
Release Status:	Released to Netherlocks Safety Systems B.V.	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Steven Close, Safety Engineer

Dr. William M. Goble, Principal Partner

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[9] 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.

A useful life period of 10 to 15 years or 10,000 cycles is expected for the FAITH System PP-Series.

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

[9] 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 of a valve-actuator and FAITH system consists of a full stroke of the actuator and/or valve, see Table 9.

Table 9 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Interrupt or change the signal/supply to the actuator to force the actuator and valve to the Fail-Safe state and confirm that the Safe State was achieved and within the specified time.
3.	Re-store the supply/signal to the actuator and inspect for any visible damage or contamination and confirm that the normal operating state was achieved.
4.	Inspect the valve for any leaks, visible damage or contamination.
5.	Remove the bypass and otherwise restore normal operation.

For the test to be effective the movement of the valve must be confirmed. To confirm the effectiveness of the test both the travel of the valve and slew rate must be monitored and compared to expected results to validate the testing.