Failure Modes, Effects and Diagnostic Analysis

Project:

Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter

Customer:

Magnetrol International

Downers Grove, IL

USA

Contract No.: MAG 05/06-13

Report No.: MAG 05/06-13 R001

Version V1, Revision R1, October 6, 2005

John C. Grebe - Rachel Amkreutz

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter. 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 Eclipse Enhanced Model 705, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The Eclipse Enhanced Model 705 is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low upon internal detection of a failure. The self-diagnostics have been confirmed using fault injection tests. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The unit is externally powered from 24 Volts DC. Table 1 lists the versions of the Eclipse Enhanced Model 705 that have been considered for the hardware assessment.

Table 1 Version overview

1	Eclipse Enhanced Model 705, 705-510*-***
2	Eclipse Enhanced Model 705, 705-51A*-***

The Eclipse Enhanced Model 705 is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0. The analysis shows that models 705-510*-*** have a safe failure fraction between 60 and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 1 as a single device. The analysis shows that models 705-51A*-*** have a safe failure fraction between 90 and 99% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 2 as a single device.

The failure rates for the Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter, models 705-510*-*** are listed in Table 2.

Table 2 Failure rates Eclipse Enhanced Model 705, 705-510*-*

Failure category		**Failure rate (in FIT)**	
Fail Dangerous Detected			567
	Fail Detected (detected by internal diagnostics)	405	
	Fail High (detected by the logic solver)	21	
	Fail Low (detected by the logic solver)	141	
Fail Dangerous Undetected			183
No Effect			393
Annunciation Undetected			38

The failure rates for the Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter, models 705-51A*-*** are listed in Table 3.

[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 3 Failure rates Eclipse Enhanced Model 705, 705-51A*-***

Failure category		Failure rate (in FIT)	
Fail Dangerous Detected			650
	Fail Detected (detected by internal diagnostics)	488	
	Fail High (detected by the logic solver)	21	
	Fail Low (detected by the logic solver)	141	
Fail Dangerous Undetected			106
No Effect			393
Annunciation Undetected			31

Table 4 lists the failure rates for the Eclipse Enhanced Model 705 according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 4 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}[2]	λ_{dd}	λ_{du}	SFF
Eclipse Enhanced Model 705, 705-510*-***	0 FIT	431 FIT	567 FIT	183 FIT	84.5%
Eclipse Enhanced Model 705, 705-51A*-***	0 FIT	424 FIT	650 FIT	106 FIT	91.0%

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

A user of the Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter 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 “no effect” 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 of Contents

Management summary 2

1 Purpose and Scope 5

2 Project management 6

2.1 *exida* 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 Magnetrol International 7

2.4.2 Documentation generated by *exida* 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 10

4.2.1 FMEDA 10

4.2.2 Failure rates 10

4.3 Assumptions 10

4.4 Results 12

5 Using the FMEDA results 14

5.1 PFD_{AVG} calculation Eclipse Enhanced Model 705 14

6 Terms and Definitions 15

7 Status of the document 16

7.1 Liability 16

7.2 Releases 16

7.3 Future Enhancements 16

7.4 Release Signatures 16

Appendix A: Lifetime of critical components 17

Appendix B Proof test to reveal dangerous undetected faults 18

B.1 Suggested proof test 18

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like DIN V VDE 0801, 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}).

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 include an assessment of the development process.

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

Option 2 is an assessment by *exida* 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 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}). 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* 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 hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) carried out on the Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

It shall be assessed whether the Eclipse Enhanced Model 705 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints for SIL 1 sub-systems (705-510*-***), respectively SIL 2 subsystems (705-51A*-***) according to IEC 61508.

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 150 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV 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.

2.2 Roles of the parties involved

Magnetrol International	Manufacturer of the Eclipse Enhanced Model 705
exida	Project leader of the FMEDA

Magnetrol International contracted *exida* in August 2005 with the review of the FMEDA and PFD_{AVG} calculation of the above-mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 1999	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	exida 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

2.4 Reference documents

2.4.1 Documentation provided by Magnetrol International

[D1]	EM705 REV 1 fmeda summary.xls, 07/08/2005	Failure Modes, Effects, and Diagnostic Analysis - Summary
[D2]	fmeda0309145001RC0507 07SIL1.xls, 7/7/2005	Failure Modes, Effects, and Diagnostic Analysis - EM705 HART Digital Board SIL 1
[D3]	fmeda0309149001RC0507 08BSIL1.xls, 7/8/2005	Failure Modes, Effects, and Diagnostic Analysis - Enchanced Model 705 Analog Board Rev C SIL 1
[D4]	fmeda0309151001_050512 SIL1.xls, 05/12/2005	Failure Modes, Effects, and Diagnostic Analysis - EM705 HART Wiring Board
[D5]	rptSILFaults050707.doc, 07/07/2005	Eclipse 705 3.x FMEDA SIL 1 and SIL 2 Diagnostic Methods
[D6]	Bulletin 57-101.11, August 2005	Eclipse® Enhanced Model 705 Guided Wave Radar Level Transmitter, Sales Literature
[D7]	rpt7053pxinjection0509 27.doc, 09/27/2005	705 3.X FMEDA Fault Injection Test Summary

2.4.2 Documentation generated by *exida*

[R1]	Mag 05-06-13 R001 V1 R1 FMEDA EM 705 Eclipse.doc	FMEDA report, Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter

3 Product Description

The Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter is a loop-powered, 24 VDC level transmitter, based on Guided Wave Radar (GWR) technology. For safety instrumented systems usage it is assumed that the 4 – 20mA output is used as the primary safety variable. The analog output meets NAMUR NE 43 (3.8mA to 20.5mA usable). The transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either low or high upon internal detection of a failure (output state is programmable). The device can be equipped with or without display. Table 5 lists the versions of the Eclipse Enhanced Model 705 that have been considered for the hardware assessment.

Table 5 Version overview

1	Eclipse Enhanced Model 705, 705-510*-***
2	Eclipse Enhanced Model 705, 705-51A*-***

Guided Wave Radar is based upon the principle of TDR (Time Domain Reflectometry). TDR utilizes pulses of electromagnetic energy transmitted down a probe. When a pulse reaches a surface that has a higher dielectric than the air/vapor in which it is traveling, the pulse is reflected. An ultra high-speed timing circuit precisely measures the transit time and provides an accurate level measurement.

Choosing the proper Guided Wave Radar (GWR) probe is the most important decision in the application process. The probe configuration establishes fundamental performance characteristics. Coaxial, twin element (rod or cable), and single element (rod or cable) are the three basic configurations. The probe for use with the Eclipse Enhanced Model 705 should be selected as appropriate for the application. Careful selection of probe design and materials for a specific application will minimize media build-up on the probe.

The Eclipse Enhanced Model 705 is classified as a Type B[3] device 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 documentation obtained from Magnetrol International and is documented in [D1] through [D5]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level. This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the Eclipse Enhanced Model 705, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as state where the output exceeds the user defined threshold.
Fail Safe	Failure that causes the module / (sub)system 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 deviates the measured input state or the actual output by more than 2% of span and that leaves the output within active scale (includes frozen output).
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, or a connected logic solver.
Fail High	Failure that causes the output signal to go to the maximum output current (> 21.5mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.6mA)
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, depending on the application, a Fail High or a Fail Low can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified.

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 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* in this FMEDA is from a proprietary component failure rate database derived using the Telcordia failure rate database/models, the SN29500 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 Eclipse Enhanced Model 705.

- 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 HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the safety logic solver is configured to detect under-range (Fail Low) and over-range (Fail High) failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- Probe is selected and installed per the requirements of the application.

- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
    - IEC 60654-1, Class C with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- External power supply failure rates are not included.

4.4 Results

Using reliability data extracted from the exida component reliability database the following failure rates resulted from the Eclipse Enhanced Model 705 FMEDA. The results include failure of the probe. It is assumed that the probe was selected appropriately for the intended application. Table 6 lists the failure rates for the models 705-510*-*** of the Eclipse Enhanced Model 705.

Table 6 Failure rates Eclipse Enhanced Model 705, 705-510*-*

Failure category		Failure rate (in FIT)	
Fail Dangerous Detected			567
	Fail Detected (detected by internal diagnostics)	405	
	Fail High (detected by the logic solver)	21	
	Fail Low (detected by the logic solver)	141	
Fail Dangerous Undetected			183
No Effect			393
Annunciation Undetected			38

Table 7 lists the failure rates for models 705-51A*-*** of the Eclipse Enhanced Model 705.

Table 7 Failure rates Eclipse Enhanced Model 705, 705-51A*-*

Failure category		Failure rate (in FIT)	
Fail Dangerous Detected			650
	Fail Detected (detected by internal diagnostics)	488	
	Fail High (detected by the logic solver)	21	
	Fail Low (detected by the logic solver)	141	
Fail Dangerous Undetected			106
No Effect			393
Annunciation Undetected			31

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the Eclipse Enhanced Model 705 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. This is reflected in 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 8 Safe Failure Fraction of the Eclipse Enhanced Model 705

Device	SFF
Eclipse Enhanced Model 705, 705-510*-***	84.5%
Eclipse Enhanced Model 705, 705-51A*-***	91.0%

The failure rates that are derived from the FMEDA for the Eclipse Enhanced Model 705 are in a format different from the IEC 61508 format. Table 9 lists the failure rates for Eclipse Enhanced Model 705 according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 9 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	SFF
Eclipse Enhanced Model 705, 705-510*-***	0 FIT	431 FIT	567 FIT	183 FIT	84.5%
Eclipse Enhanced Model 705, 705-51A*-***	0 FIT	424 FIT	650 FIT	106 FIT	91.0%

The architectural constraint type for Eclipse Enhanced Model 705 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] It is important to realize that the “no effect” 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 Eclipse Enhanced Model 705

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter. The failure rate data used in this calculation is displayed in section 4.4.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} value for a single Eclipse Enhanced Model 705 with a proof test interval of 1 year equals 8.06E-04 (705-510*-***) and 4.69E-04 (705-51A*-***) respectively.

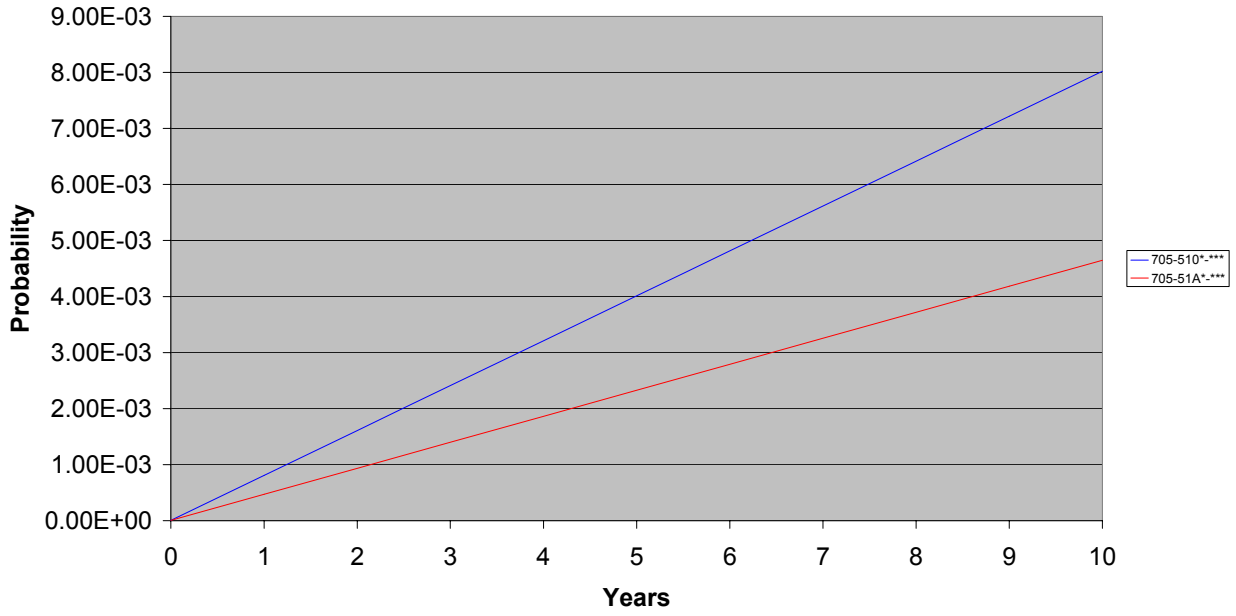

Figure 1 PFD_{AVG}(t) Eclipse Enhanced Model 705

For SIL 1 applications, the PFD_{AVG} value needs to be ≥ 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of the Eclipse Enhanced Model 705, 705-510*-*** is equal to 0.8% of the range. For SIL 2 applications, the PFD_{AVG} value needs to be ≥ 10^{-3} and < 10^{-2}. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval of the Eclipse Enhanced Model 705, 705-51A*-*** is equal to 4.7% 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 ($1x10^{-9}$ 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” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B component	“Complex” subsystem (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.

7.2 Releases

Version:	V1	
Revision:	R1	
Version History:	V0, R1:	Draft; September 2, 2005
	V0, R2:	Added 705-51A*-*** and review comments; September 29, 2005
	V1, R1:	Released to Magnetrol; September 29, 2005
Authors:	John C. Grebe - Rachel Amkreutz	
Review:	V0, R1:	John Benway (Magnetrol); September 28, 2005
	V0, R2:	John Benway (Magnetrol); October 1, 2005
Release status:	Released to Magnetrol International	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Dr. William M. Goble, Principal Partner

John C. Grebe, Partner

Ir. Rachel Amkreutz, Safety Engineer

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 that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 10 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 10 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

As there are no aluminum electrolytic capacitors used, the tantalum electrolytic capacitors are the limiting factors with regard to the useful lifetime of the system. The tantalum electrolytic capacitors that are used in the Eclipse Enhanced Model 705 have an estimated useful lifetime of about 50 years. According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. According to section 7.4.7.4 note 3 of IEC 61508 experiences have shown that the useful lifetime often lies within a range of 8 to 12 years for transmitters.

Appendix B Proof test 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

A suggested proof test is described in Table 11. This test will detect approximately 97% of possible DU failures in Model 705-510*-*** of the Eclipse Enhanced Model 705 Guided Wave Radar Level Transmitter. The test will detect approximately 94% of possible DU failures in Model 705-51A*-*** of the Eclipse Enhanced Model 705.

Table 11 Steps for Proof Test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. This tests for compliance voltage problems such as low loop power supply voltage or increased wiring resistance. This also tests for other possible failures in the current loop circuitry.
3	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures.
4	Remove level from the probe. The Status parameter should say “Dry Probe” and the level reading should be equal to value in the “Level Offset” parameter.
5	Perform a two point calibration check of the transmitter by applying level to two points on the probe and compare the transmitter display reading and the current level value to a known reference measurement.
6	If the calibration is correct the proof test is complete. Proceed to step 11.
7	If the calibration is incorrect, remove the transmitter and probe from the process. Inspect the probe for build-up or clogging. Clean the probe, if necessary. Perform a bench calibration check by shorting the probe at two points. Measure the level from the bottom of the probe to the points and compare to the transmitter display and current level readings.
8	If the calibration is off by more than 2%, call the factory for assistance.
9	If the calibration is correct, the proof test is complete. Proceed to step 10.
10	Re-install the probe and transmitter.
11	Restore the loop to full operation.
12	Remove the bypass from the safety PLC or otherwise restore normal operation