Failure Modes, Effects and Diagnostic Analysis

Project:
Trip Amplifier MTL5314

Customer:
MTL
Luton, Bedfordshire
United Kingdom

Contract No.: Q05/05-26
Report No.: MTL 05/05-26 R007
Version V1, Revision R1, August 15, 2006
Rachel Amkreutz - John C. Grebe

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management summary

This report summarizes the results of hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Trip Amplifier MTL5314. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety assessment per IEC 61508 of a device. From the FMEDA, a full set of failure rates is determined. For full functional safety assessment purposes all requirements of IEC 61508 must be considered.

The MTL5314 connects to a 2- or 3-wire 4 - 20mA transmitter or current source located in the hazardous area. It supplies one or two configurable alarm signals to the safe area via changeover relays. Each relay may be configured individually to signal an alarm condition (relay de-energized) when the input signal is greater than or less than a pre-set value.

It is assumed that one trip output is used in the safety instrumented function; the MTL5314 is set to trip on either a low input signal (Low Trip application) or a high input signal (High Trip application).

The Trip Amplifier MTL5314 is classified as a Type A[1] device, with a hardware fault tolerance of 0. The hardware assessment has shown that the MTL5314 has a Safe Failure Fraction between 60% and 90%, see table 2 of IEC 61508-2. The device therefore meets the hardware safety integrity requirements to be used as a single device in Safety Instrumented Functions up to SIL 2.

Table 1 lists the failure rates for the MTL5314.

Table 1 Failure rates MTL5314

Failure category	Failure rate (FIT)	
	Low Trip	High Trip
Fail Safe	156	151
Fail Dangerous Undetected	50	56
No Effect	165	165

Table 2 lists the failure rates for the Trip Amplifier MTL5314 according to IEC 61508.

Table 2 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}[2]	λ_{dd}	λ_{du}	SFF
MTL5314, Low Trip	0 FIT	321 FIT	0 FIT	50 FIT	86.5%
MTL5314, High Trip	0 FIT	316 FIT	0 FIT	56 FIT	85.0%

The failure rates are valid for the useful lifetime of the product; see Appendix A Useful life.

A user of the Trip Amplifier MTL5314 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).

[1] Type A subsystem: “Non-Complex” subsystem with well-defined failure modes, see 7.4.3.1.2 of IEC 61508-2.

[2] Note that the SU category includes failures that do not cause a spurious trip

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 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 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 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. In addition, this option includes an assessment of the proven-in-use documentation of the device 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 may help justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices when combined with plant specific proven-in-use records.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment 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 assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment by *exida* in the form of the Failure Modes, Effects and Diagnostic Analysis of the Trip Amplifier MTL5314. From this, failure rates example PFD_{AVG} values are calculated.

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

The assessment does not include any calculations for proving intrinsic safety.

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 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail 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

MTL	Manufacturer of the Trip Amplifier MTL5314
exida	Performed the hardware assessment according to Option 1 (see section 1)

MTL contracted *exida* in June 2005 with the FMEDA of the above mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91, RAC, 1991	Failure Mode / Mechanism Distributions, Reliability Analysis Center.
[N3]	FMD-97, RAC, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center.
[N4]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center.
[N5]	SN 29500	Failure rates of components
[N6]	Telcordia, SR-332, Issue 1	Reliability Prediction Procedure for Electronic Equipment
[N7]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N8]	Safety Equipment Reliability Handbook, 2003	exida.com L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N9]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods
[N10]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

2.4 Reference documents

2.4.1 Documentation provided by MTL

[D1]	TC5314-1/1, Issue 1	Schematic Drawing, MTL5314 Trip Amplifier
[D2]	MTL5314.pdf, June 2004	Product Data Sheet MTL5314 Trip Amplifier

2.4.2 Documentation generated by *exida*

[R1]	MTL 5314 One Trip Output.xls	Failure Modes, Effects and Diagnostic Analysis, MTL5314 – One Trip Output
[R2]	MTL 5314 Common Components.xls	Failure Modes, Effects and Diagnostic Analysis, MTL5314 – Common Components
[R3]	MTL 5314 Summary Sheet.xls	Failure Modes, Effects and Diagnostic Analysis, MTL5314 - Summary
[R4]	MTL 05-05-26 R007 V1 R1 FMEDA 5314.doc, 8/15/2006	FMEDA report, Trip Amplifier MTL5314 (this report)

3 Product Description

The Failure Modes, Effects and Diagnostic Analysis (FMEDA) is performed for the Trip Amplifier MTL5314.

The MTL5314 connects to a 2- or 3-wire 4 - 20mA transmitter or current source located in the hazardous area. It supplies one or two configurable alarm signals to the safe area via changeover relays. Each relay may be configured individually to signal an alarm condition (relay de-energized) when the input signal is greater than or less than a pre-set value.

It is assumed that one trip output is used in the safety instrumented function; the MTL5314 is set to trip on either a low input signal (Low Trip application) or a high input signal (High Trip application).

In addition, the MTL5314 can be connected in series to the hazardous-area side of an MTL5042 4/20mA repeater power supply (or equivalent device) to provide two trip alarm outputs direct from the transmitter signal.

The Trip Amplifier MTL5314 is classified as a Type A[3] device according to IEC 61508. The hardware fault tolerance of the device is 0.

[3] Type A subsystem: "Non-Complex" subsystem with well-defined failure modes, for details see 7.4.3.1.2 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the information received from MTL and is documented in [R1] through [R3]. 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 Trip Amplifier MTL5314, the following definitions for the failure of the product were considered.

Fail-Safe State
The fail-safe state is defined as the output being de-energized.

Fail Safe
Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.

Fail Dangerous Undetected
Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

Fail No Effect
Failure of a component that is part of the safety function but that has no effect on the safety function.

The No Effect failurea are provided for those who wish to do more detailed reliability modeling than required by IEC 61508. In IEC 61508, Edition 2000, the No Effect 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 Trip Amplifier MTL5314.

- 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 stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HDBK-217F. Alternatively, the assumed environment is similar 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 40ºC. Humidity levels are assumed within manufacturer’s rating.
- External power supply failure rates are not included.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- One trip output is used in the safety instrumented function.

4.4 Results

Using reliability data extracted from the *exida* component reliability database the following failure rates resulted from the Trip Amplifier MTL5314 FMEDA.

Table 3 Failure rates MTL5314

Failure category	Failure rate (FIT)	
	Low Trip	High Trip
Fail Safe	156	151
Fail Dangerous Undetected	50	56
No Effect	165	165

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 Trip Amplifier MTL5314 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 IEC 61508 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 4 lists the failure rates for the Trip Amplifier MTL5314 according to IEC 61508, including the Safe Failure Fraction.

Table 4 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}[4]	λ_{dd}	λ_{du}	SFF
MTL5314, Low Trip	0 FIT	321 FIT	0 FIT	50 FIT	86.5%
MTL5314, High Trip	0 FIT	316 FIT	0 FIT	56 FIT	85.0%

The Trip Amplifier MTL5314 are classified as Type A devices according to IEC 61508. The hardware fault tolerance of the devices is 0. The SFF and required SIL of the Safety Instrumented Function 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] Note that the SU category includes failures that do not cause a spurious trip

5 Using the FMEDA results

5.1 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) MTL5314. 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. The PFD_{AVG} for a single MTL5314, with a proof test interval of 1 year equals 2.19E-04 (Low Trip), respectively 2.45E-04 (High Trip).

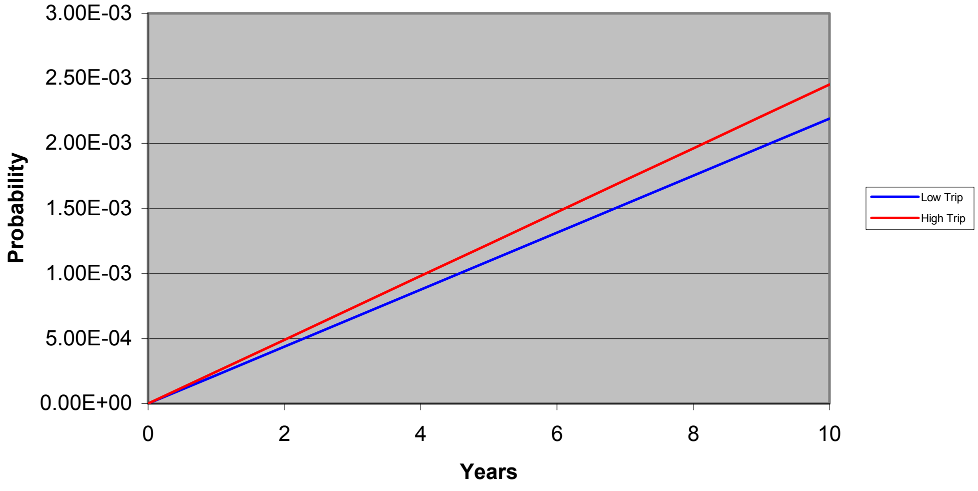

Figure 1: PFD_{AVG}(t) MTL5023, normal mode of operation

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. An accurate, IEC 61508 approved tool should be used for this, e.g. the *exida* SILver tool, part of the exSILentia tool set.

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 MTL5314 is approximately equal to 2.2% (Low Trip), respectively 2.5% (High Trip) 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 subsystem	“Non-Complex” subsystem (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B subsystem	“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:	V1, R1:	Released to MTL; August 15, 2006
	V0, R1:	Draft; August 2, 2006
Authors:	Rachel Amkreutz - John C. Grebe	
Review:	V0, R1:	John C. Grebe (exida); August 14, 2006
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

William M Goble

Dr. William M. Goble, Principal Partner

John C. Grebe, Partner

Rachel Amkreutz, Safety Engineer

Appendix A Useful life

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 4.3) this only applies provided that the useful lifetime[5] 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, electrolytic 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 5 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 5: Useful lifetime of electrolytic capacitors contributing to λ_{du}

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

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

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

[5] 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 FMEDA can be detected during proof testing.

B.1 Suggested proof test

A suggested proof test is described in Table 6. This test will detect approximately 99% of possible DU failures in the Trip Amplifier MTL5314.

Table 6 Steps for Proof Test

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip.
2.	Provide an appropriate input signal to the Trip Amplifier MTL5314 to de-energize the output and verify that the output(s) are de-energized.
3.	Restore the loop to full operation.
4.	Remove the bypass from the safety PLC or otherwise restore normal operation.