Failure Modes, Effects and Diagnostic Analysis

Project:

Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac

Customer:

MTL
Luton, Bedfordshire
United Kingdom

Contract No.: Q05/05-26
Report No.: MTL 05/05-26 R003
Version V1, Revision R3, September 19, 2006
Rachel Amkreutz - John C. Grebe

Management summary

This report summarizes the results of hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac. 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.

With the MTL5012, a switch or proximity detector located in a hazardous area can control a safe-area solid-state output. With the MTL5015, two switches or proximity detectors located in a hazardous area can each control a safe-area solid-state output. The FMEDA applies to either channel of the MTL5015, used in a single safety function.

With the MTL5017, two switches or proximity detectors located in a hazardous area can each control a safe-area load (relay output). The FMEDA applies to either channel of the MTL5017, used in a single safety function. With the MTL5011B, a switch or proximity detector located in a hazardous area can control a safe-area load (relay output). With the MTL5014, a switch or proximity detector located in a hazardous area can control two safe-area loads (two relay outputs). For safety purposes it is assumed that channel 1 is used.

With the MTL5018 and MTL5018ac, two switches or proximity detectors located in a hazardous area can each control a safe-area load (two relay outputs). The FMEDA applies to either channel of the MTL5018 and MTL5018ac, used in a single safety function.

The two channels of the MTL5015, MTL5017, MTL5018 and MTL5018ac may be used in separate safety functions if due regard is taken of the possibility of common failures.

The Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac are classified as Type A[1] devices, with a hardware fault tolerance of 0. The hardware assessment has shown that the devices have a Safe Failure Fraction between 60% and 90% or higher, see table 2 of IEC 61508-2. The devices therefore meet the hardware safety integrity requirements to be used as single devices in Safety Instrumented Functions up to SIL 2.

Table 1 lists the failure rates for the MTL5017 when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 1 Failure rates MTL5017

Failure category	Failure rate (FIT)	
	MTL5017 Normal	MTL5017 Phase reversal
Fail Safe	89	89
Fail Dangerous Undetected	22	21
No Effect	112	112
Annunciation Undetected	11	11

Table 2 lists the failure rates for the MTL5012 and MTL5015 when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

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

Table 2 Failure rates MTL5012 and MTL5015

Failure category	Failure rate (FIT)			
	MTL5012 Normal	MTL5012 Phase reversal	MTL5015 Normal	MTL5015 Phase reversal
Fail Safe	98	95	103	100
Fail Dangerous Undetected	27	29	27	29
No Effect	151	151	161	161
Annunciation Undetected	4	4	4	4

Table 3 lists the failure rates for the MTL5011B and MTL5014 when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 3 Failure rates MTL5011B and MTL5014

Failure category	Failure rate (FIT)			
	MTL5011B Normal	MTL5011B Phase reversal	MTL5014 Normal	MTL5014 Phase reversal
Fail Safe	108	106	106	104
Fail Dangerous Undetected	30	32	30	32
No Effect	115	115	113	113
Annunciation Undetected	4	4	4	4

Table 4 lists the failure rates for the MTL5018 and MTL5018ac when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 4 Failure rates MTL5018 and MTL5018ac

Failure category	Failure rate (FIT)			
	MTL5018 Normal	MTL5018 Phase reversal	MTL5018ac Normal	MTL5018ac Phase reversal
Fail Safe	110	108	108	106
Fail Dangerous Undetected	30	32	41	43
No Effect	121	121	143	143
Annunciation Undetected	4	4	4	4

Table 5 lists the failure rates for the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac according to IEC 61508. It is assumed that the probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

Table 5 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su} [2]	λ_{dd}	λ_{du}	SFF
MTL5017, normal mode	0 FIT	212 FIT	0 FIT	22 FIT	90.8%
MTL5017, phase reversal mode	0 FIT	212 FIT	0 FIT	21 FIT	90.9%
MTL5012, normal mode	0 FIT	253 FIT	0 FIT	27 FIT	90.5%
MTL5012, phase reversal mode	0 FIT	250 FIT	0 FIT	29 FIT	89.5%
MTL5015, normal mode	0 FIT	268 FIT	0 FIT	27 FIT	91.0%
MTL5015, phase reversal mode	0 FIT	265 FIT	0 FIT	29 FIT	90.1%
MTL5011B, normal mode	0 FIT	227 FIT	0 FIT	30 FIT	88.2%
MTL5011B, phase reversal mode	0 FIT	225 FIT	0 FIT	32 FIT	87.5%
MTL5014, normal mode	0 FIT	223 FIT	0 FIT	30 FIT	88.2%
MTL5014, phase reversal mode	0 FIT	221 FIT	0 FIT	32 FIT	87.4%
MTL5018, normal mode	0 FIT	235 FIT	0 FIT	30 FIT	88.6%
MTL5018, phase reversal mode	0 FIT	233 FIT	0 FIT	32 FIT	87.9%
MTL5018ac, normal mode	0 FIT	255 FIT	0 FIT	41 FIT	86.4%
MTL5018ac, phase reversal mode	0 FIT	253 FIT	0 FIT	43 FIT	85.7%

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

A user of the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac 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).

[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 Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac. 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 Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac
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]	TC5015-1/2, Issue 2	Schematic Drawing, MTL5015 Switch/Proximity Detector Interface Unit
[D2]	TC5012-1/1, Issue 1	Schematic Drawing, MTL5012 Switch/Proximity Detector Interface Unit
[D3]	TC5017-1/3, Issue 3	Schematic Drawing, MTL5017 Switch/Proximity Detector Interface Unit
[D4]	TC5011-31/4, Issue 4	Schematic Drawing, MTL5011B Switch/Proximity Detector Interface Unit
[D5]	TC5014-1/1, Issue 1	Schematic Drawing, MTL5014 Switch/Proximity Detector Interface Unit
[D6]	TC5018-1/5, Issue 5	Schematic Drawing, MTL5018 Switch/Proximity Detector Interface Unit
[D7]	MTLI/DTS50-018-01/02	Schematic Drawing, MTL5018ac Switch/Proximity Detector Interface Unit
[D8]	MTL5011B.pdf, June 2004	Product Data Sheet MTL5011B Switch/Proximity Detector
[D9]	MTL5012.pdf, June 2004	Product Data Sheet MTL5012 Switch/Proximity Detector
[D10]	MTL5014.pdf, June 2004	Product Data Sheet MTL5014 Switch/Proximity Detector
[D11]	MTL5015.pdf, June 2004	Product Data Sheet MTL5015 Switch/Proximity Detector
[D12]	MTL5017.pdf, June 2004	Product Data Sheet MTL5017 Switch/Proximity Detector
[D13]	MTL5018.pdf, June 2004	Product Data Sheet MTL5018 Switch/Proximity Detector
[D14]	MTL5018ac.pdf, June 2004	Product Data Sheet MTL5018ac Switch/Proximity Detector

2.4.2 Documentation generated by *exida*

[R1]	4044D Fault Injection List.xls, 06/15/05	Fault Injection List, MTL Repeater Power Supplies 4044(D)
[R2]	MTL 5017 Common Power.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5017 – common power
[R3]	MTL 5017 One Input to Output.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5017 – one input to one output
[R4]	MTL 5017One Channel cross interference.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5017 – one channel cross interference
[R5]	MTL 5017 Summary Sheet.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5017 – Summary
[R6]	MTL 5015 5012 Common Power.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5012 and MTL5015 – common power
[R7]	MTL 5015 5012 One Input to Output.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5012 and MTL5015 – one input to one output

[R8]	MTL 5015 One Channel cross interference.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5015 – one channel cross interference
[R9]	MTL 5015 5012 Summary Sheet.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5012 and MTL5015 - Summary
[R10]	MTL 5011 Null Channel interference.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5011B - Null Channel interference
[R11]	MTL 5014 Input to Output.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5014 – input to output
[R12]	MTL 5018 5011 One Input to Output.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5018 and MTL5011B – one input to one output
[R13]	MTL 5018 5014 5011 Common Power.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5018, MTL5014 and MTL5011B – common power
[R14]	MTL 5018 One Channel cross interference.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5018– one channel cross interference
[R15]	MTL 5018ac Common Power.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5018ac – common power
[R16]	MTL 5018ac One Input to Output.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL 5018ac – one input to one output
[R17]	MTL 5018 5018ac 5014 5011 Summary Sheet.xls, 07/07/2006	Failure Modes, Effects and Diagnostic Analysis, MTL5018, MTL5018ac, MTL5014, and MTL5011B – Summary
[R18]	MTL 05-05-26 R003 V1 R3 FMEDA 5011B - 5018.doc, 9/19/2006	FMEDA report, Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac (this report)

3 Product Description

The Failure Modes, Effects and Diagnostic Analysis (FMEDA) is performed for the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac.

With the MTL5012, a switch or proximity detector located in a hazardous area can control a safe-area solid-state output. With the MTL5015, two switches or proximity detectors located in a hazardous area can each control a safe-area solid-state output. The FMEDA applies to either channel of the MTL5015, used in a single safety function. The two channels of the MTL5015 may be used in separate safety functions if due regard is taken of the possibility of common failures.

With the MTL5017, two switches or proximity detectors located in a hazardous area can each control a safe-area load (relay output). The FMEDA applies to either channel of the MTL5017, used in a single safety function. The two channels of the MTL5017 may be used in separate safety functions if due regard is taken of the possibility of common failures.

With the MTL5011B, a switch or proximity detector located in a hazardous area can control a safe-area load (relay output). With the MTL5014, a switch or proximity detector located in a hazardous area can control two safe-area loads (two relay outputs). For safety purposes it is assumed that channel 1 is used.

With the MTL5018 and MTL5018ac, two switches or proximity detectors located in a hazardous area can each control a safe-area load (two relay outputs). The FMEDA applies to either channel of the MTL5018 and MTL5018ac, used in a single safety function. The two channels of the MTL5018 and MTL5018ac may be used in separate safety functions if due regard is taken of the possibility of common failures.

For normal operation, the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac outputs are de-energized if <1.2mA in sensor circuit; outputs are energized if > 2.1mA in sensor circuit (see NAMUR and DIN 19234 standards for proximity detectors). A phase-reversal switch, located on top of the all products, allows an alarm signal to be signaled for either state of the sensors. All devices provide built-in line fault detection for broken or shorted lines.

The Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac are classified as a Type A[3] devices according to IEC 61508. The hardware fault tolerance of the devices 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 [R6] through [R9]. 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 Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac, 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.
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.

The No Effect and Annunciation Undetected failure 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 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 Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac.

- 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.
- The probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).
- Line fault monitoring is assumed to be active.
- The probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).
- For MTL5014, the channel 1 output is used for safety purposes.

4.4 Results

Using reliability data extracted from the *exida* component reliability database the following failure rates resulted from the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac FMEDA.

Table 6 lists the failure rates for the MTL5017 when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 6 Failure rates MTL5017

Failure category	Failure rate (FIT)	
	MTL5017 Normal	MTL5017 Phase reversal
Fail Safe	89	89
Fail Dangerous Undetected	22	21
No Effect	112	112
Annunciation Undetected	11	11

Table 7 lists the failure rates for the MTL5012 and MTL5015 when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 7 Failure rates MTL5012 and MTL5015

Failure category	Failure rate (FIT)			
	MTL5012 Normal	MTL5012 Phase reversal	MTL5015 Normal	MTL5015 Phase reversal
Fail Safe	98	95	103	100
Fail Dangerous Undetected	27	29	27	29
No Effect	151	151	161	161
Annunciation Undetected	4	4	4	4

Table 8 lists the failure rates for the MTL5011B and MTL5014 when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 8 Failure rates MTL5011B and MTL5014

Failure category	Failure rate (FIT)			
	MTL5011B Normal	MTL5011B Phase reversal	MTL5014 Normal	MTL5014 Phase reversal
Fail Safe	108	106	106	104
Fail Dangerous Undetected	30	32	30	32
No Effect	115	115	113	113
Annunciation Undetected	4	4	4	4

Table 9 lists the failure rates for the MTL5018 and MTL5018ac when used in normal mode of operation (trip on < 1.2mA in sensor circuit) and when used with phase reversal mode of operation (trip on > 2.1mA in sensor circuit).

Table 9 Failure rates MTL5018 and MTL5018ac

Failure category	Failure rate (FIT)			
	MTL5018 Normal	MTL5018 Phase reversal	MTL5018ac Normal	MTL5018ac Phase reversal
Fail Safe	110	108	108	106
Fail Dangerous Undetected	30	32	41	43
No Effect	121	121	143	143
Annunciation Undetected	4	4	4	4

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 Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac 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 10 lists the failure rates for the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac according to IEC 61508, including the Safe Failure Fraction.

Table 10 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su} [4]	λ_{dd}	λ_{du}	SFF
MTL5017, normal mode	0 FIT	212 FIT	0 FIT	22 FIT	90.8%
MTL5017, phase reversal mode	0 FIT	212 FIT	0 FIT	21 FIT	90.9%
MTL5012, normal mode	0 FIT	253 FIT	0 FIT	27 FIT	90.5%
MTL5012, phase reversal mode	0 FIT	250 FIT	0 FIT	29 FIT	89.5%
MTL5015, normal mode	0 FIT	268 FIT	0 FIT	27 FIT	91.0%
MTL5015, phase reversal mode	0 FIT	265 FIT	0 FIT	29 FIT	90.1%
MTL5011B, normal mode	0 FIT	227 FIT	0 FIT	30 FIT	88.2%
MTL5011B, phase reversal mode	0 FIT	225 FIT	0 FIT	32 FIT	87.5%
MTL5014, normal mode	0 FIT	223 FIT	0 FIT	30 FIT	88.2%
MTL5014, phase reversal mode	0 FIT	221 FIT	0 FIT	32 FIT	87.4%

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

Device	λ_{sd}	λ_{su}[4]	λ_{dd}	λ_{du}	SFF
MTL5018, normal mode	0 FIT	235 FIT	0 FIT	30 FIT	88.6%
MTL5018, phase reversal mode	0 FIT	233 FIT	0 FIT	32 FIT	87.9%
MTL5018ac, normal mode	0 FIT	255 FIT	0 FIT	41 FIT	86.4%
MTL5018ac, phase reversal mode	0 FIT	253 FIT	0 FIT	43 FIT	85.7%

The Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac 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.

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) MTL5011B, Normal mode of operation. 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 MTL5011B, with a proof test interval of 1 year equals 1.31E-04.

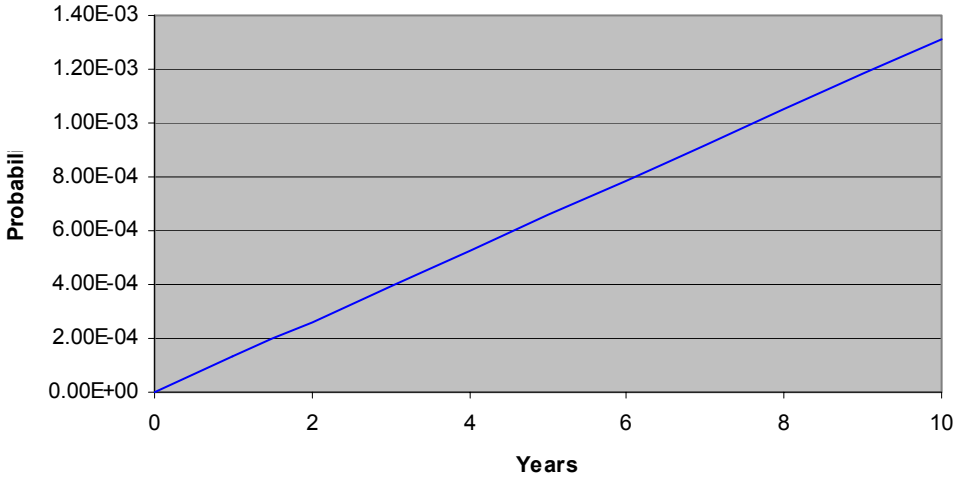


Figure 1: PFD_{AVG}(t) MTL5011B, Normal mode of operation

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 MTL5011B is approximately equal to 1.3% 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

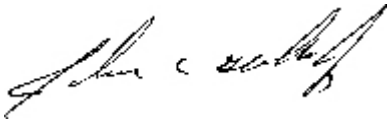
Version:	V1	
Revision:	R3	
Version History:	V1, R3:	Updated references (MTL5011B); September 19, 2006
	V1, R2:	Updated reference (MTL5011B); September 6, 2006
	V1, R1:	Released to MTL; July 18, 2006
	V0, R1:	Draft; July 14, 2006
Authors:	Rachel Amkreutz - John C. Grebe	
Review:	V0, R1:	John C. Grebe (exida); July 18, 2006
	V1, R1:	Barry Lytollis (MTL); September 4, 2006
	V1, R2:	Barry Lytollis (MTL); September 11, 2006
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

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 11 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 11: 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 12. This test will detect approximately 99% of possible DU failures in the Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac.

Table 12 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 Switch/Proximity Detector Interface Units MTL5011B, MTL5012, MTL5014, MTL5015, MTL5017, MTL5018, and MTL5018ac to de-energize the output and verify that the output(s) are de-energized. For MTL5015, MTL5017, MTL5018 and MTL5018ac, test each input separately and verify that the outputs of the specific input behave as expected and that there are no unexpected responses on the other outputs.
3.	Restore the loop to full operation.
4.	Remove the bypass from the safety PLC or otherwise restore normal operation.