



Failure Modes, Effects and Diagnostic Analysis

Project:
SD & TP Surge Suppressors

Company:
MTL Surge Technologies
West Melbourne, FL
USA

Contract Number: Q07/11-12
Report No.: AS 07/11-12 R001
Version V1, Revision R3, January 31, 2008
Rudolf Chalupa

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 SD & TP Surge Suppressors, hardware revisions as described in Section 2.4.1. 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 SD & TP Series. For full functional safety certification purposes all requirements of IEC 61508 will be considered.

The SD & TP Surge Suppressors are designed to reduce the impact of external electrical events on a process control system; this increases the system's reliability.

The SD series surge suppressors are designed to be located at the logic solver. The loop wiring between the sensor/final element and the logic solver passes through the SD surge suppressor; various models have various combinations of series fuses, inductors, and resistors in addition to shunt components.

The TP series surge suppressors are designed for installation at the transmitter or final element. They are connected in parallel with the associated device, thus introducing no series resistance into the wiring.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the SD & TP Series.

Table 1 Version Overview

SD07, SD16, SD32, SD55	Series Surge Suppressor, Inductor, With Fuse
SD07R, SD16R, SD32R, SD55R	Series Surge Suppressor, Resistor, No Fuse
SD07X, SD16X, SD32X, SD55X	Series Surge Suppressor, Inductor, No Fuse
SD07R3	Series Surge Suppressor, 3 Wire, Resistor, No Fuse
SD16R3, SD32R3, SD55R3	Series Surge Suppressor, 3 Wire, Resistor, No Fuse
SD07T3	Series Surge Suppressor, 3 Wire, Inductor/Resistor, No Fuse
SD16T3, SD32T3, SD55T3	Series Surge Suppressor, 3 Wire, Inductor/Resistor, No Fuse
SD07X3	Series Surge Suppressor, 3 Wire, Inductor, No Fuse
SD16X3, SD32X3, SD55X3	Series Surge Suppressor, 3 Wire, Inductor, No Fuse
SDRTD	Series Surge Suppressor, 3 Wire, Inductor, No Fuse, Optimized for 3-Wire RTD
TP24/7	Parallel Surge Suppressor, 24 + 7 Volt
TP32	Parallel Surge Suppressor, 32 Volt
TP48 2W+G	Parallel Surge Suppressor, 48 Volt, 2 Wire Plus Ground
TP48 3W+G	Parallel Surge Suppressor, 48 Volt, 3 Wire Plus Ground
TP48 4W+G	Parallel Surge Suppressor, 48 Volt, 4 Wire Plus Ground

The SD & TP Series are classified as Type A¹ devices according to IEC 61508, having a hardware fault tolerance of 0.

The analysis shows that the device has 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 2 as a single device based on hardware architectural constraints.

The complete final element subsystem, of which the SD & TP Series is an element, will need to be evaluated to determine the Safe Failure Fraction.

The failure rates for the SD & TP Series are listed in Table 2 to Table 12.

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

Table 2 Failure rates SD07, SD16, SD32, SD55

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	23.9
Fail Dangerous Detected	14.5
Fail Dangerous Undetected	1.5
Residual Effect	51.4

Table 3 Failure rates SD07R, SD16R, SD32R, SD55R

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	14.3
Fail Dangerous Detected	14.5
Fail Dangerous Undetected	1.5
Residual Effect	31.5

Table 4 Failure rates SD07X, SD16X, SD32X, SD55X

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	14.9
Fail Dangerous Detected	14.5
Fail Dangerous Undetected	1.5
Residual Effect	32.4

Table 5 Failure rates SD07R3, SD07T3, SD07X3

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	22.0
Fail Dangerous Detected	20.1
Fail Dangerous Undetected	6.9
Residual Effect	51.3

Table 6 Failure rates SD16R3, SD16T3, SD16X3, SD32R3, SD32T3, SD32X3, SD55R3, SD55T3, SD55X3

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	22.0
Fail Dangerous Detected	17.8
Fail Dangerous Undetected	5.9
Residual Effect	49.9

Table 7 Failure rates SDRTD

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	21.1
Fail Dangerous Detected	20.1
Fail Dangerous Undetected	9.0
Residual Effect	50.1

Table 8 Failure rates TP24/7

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	11.4
Fail Dangerous Undetected	6.4
Residual Effect	42.9

Table 9 Failure rates TP32

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	12.1
Fail Dangerous Undetected	5.4
Residual Effect	22.9

Table 10 Failure rates TP48 2W+G

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	7.6
Fail Dangerous Undetected	3.5
Residual Effect	20.1

Table 11 Failure rates TP48 3W+G

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	15.1
Fail Dangerous Undetected	7.0
Residual Effect	40.2

Table 12 Failure rates TP48 4W+G

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	15.1
Fail Dangerous Undetected	7.0
Residual Effect	40.2

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 13 lists the failure rates for the SD & TP Series according to IEC 61508.

Table 13 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}^2	λ_{DD}	λ_{DU}	SFF ³
SD07, SD16, SD32, SD55	0 FIT	75 FIT	15 FIT	2 FIT	-
SD07R, SD16R, SD32R, SD55R	0 FIT	46 FIT	15 FIT	2 FIT	-
SD07X, SD16X, SD32X, SD55X	0 FIT	47 FIT	15 FIT	2 FIT	-
SD07R3, SD07T3, SD07X3	0 FIT	73 FIT	20 FIT	7 FIT	-
SD16R3, SD16T3, SD16X3, SD32R3, SD32T3, SD32X3, SD55R3, SD55T3, SD55X3	0 FIT	72 FIT	18 FIT	6 FIT	-
SDRTD	0 FIT	71 FIT	20 FIT	9 FIT	-
TP24/7	0 FIT	43 FIT	11 FIT	6 FIT	-
TP32	0 FIT	23 FIT	12 FIT	5 FIT	-
TP48 2W+G	0 FIT	20 FIT	8 FIT	4 FIT	-
TP48 3W+G	0 FIT	40 FIT	15 FIT	7 FIT	-
TP48 4W+G	0 FIT	40 FIT	15 FIT	7 FIT	-

A user of the SD & TP 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 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

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

Table of Contents

Management Summary	2
1 Purpose and Scope.....	9
2 Project Management	10
2.1 <i>exida</i>	10
2.2 Roles of the parties involved	10
2.3 Standards and Literature used.....	10
2.4 Reference documents.....	11
2.4.1 Documentation provided by MTL Surge Technologies	11
2.4.2 Documentation generated by <i>exida</i>	11
3 Product Description	13
4 Failure Modes, Effects, and Diagnostic Analysis.....	15
4.1 Failure Categories description.....	15
4.2 Methodology – FMEDA, Failure Rates.....	16
4.2.1 FMEDA	16
4.2.2 Failure Rates.....	16
4.3 Assumptions	16
4.4 Results.....	17
5 Using the FMEDA Results.....	22
5.1 PFD _{AVG} Calculation SD & TP Series	22
6 Terms and Definitions	23
7 Status of the Document.....	24
7.1 Liability.....	24
7.2 Releases.....	24
7.3 Future Enhancements.....	24
7.4 Release Signatures.....	25
Appendix A Lifetime of Critical Components.....	26
Appendix B Proof tests to reveal dangerous undetected faults	27
B.1 Suggested Proof Test	27

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 the SD & TP 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 sensor or 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 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 like TÜV and manufacturers, *exida* is a partnership 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

MTL Surge Technologies Manufacturer of the SD & TP Series

exida Performed the hardware assessment according to Option 1 (see Section 1)

MTL Surge Technologies contracted *exida* in November 2007 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, 2006	<i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, 2006, ISBN 0-9727234-2-0
[N3]	Safety Equipment Reliability Handbook, 2nd Edition, 2005	<i>exida</i> L.L.C, Safety Equipment Reliability Handbook, Second Edition, 2005, ISBN 0-9727234-1-2
[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

2.4 Reference documents

2.4.1 Documentation provided by MTL Surge Technologies

[D1]	Doc # 901-100, Rev J, 2/21/2007	TP48 Series Specification
[D2]	Doc # 901-107, Rev J, 4/23/2007	SD Series Specification
[D3]	Doc # SKT0508, August 12, 2003	Schematic Drawing, SD***
[D4]	Doc # SKT0509, August 12, 2003	Schematic Drawing, SD 3-Wire
[D5]	Doc # SKT0806, November 28, 2007	Schematic Drawing, TP Series
[D6]	Doc # SPDSIL, September 19, 2003	White Paper, "SIL rating of surge protection devices used in analogue instrument systems"

2.4.2 Documentation generated by *exida*

[R1]	7V portion of TP24-7.efm, December 11, 2007	Failure Modes, Effects, and Diagnostic Analysis – SD & TP Series - 7V portion of TP24-7
[R2]	SD07R3 3-wire with series resistors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis – SD & TP Series - SD07R3 3-wire with series resistors and no removable fuses
[R3]	SD07X3 3-wire with series inductors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis – SD & TP Series - SD07X3 3-wire with series inductors and no removable fuses
[R4]	SDRTD 3-wire with series resistors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – SDXXX3 3-wire with series resistors and no removable fuses
[R5]	SDxx two lines with series inductors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – SDxx two lines with series inductors and no removable fuses
[R6]	SDxx two lines with series inductors and removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – SDxx two lines with series inductors and removable fuses
[R7]	SDxx two lines with series	Failure Modes, Effects, and Diagnostic Analysis -

	resistors and no removable fuses.efm, December 12, 2007	Summary –SD & TP Series – SDxx two lines with series resistors and no removable fuses
[R8]	SDxx two lines with series resistors and removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – SDxx two lines with series resistors and removable fuses
[R9]	SDxxR3 3-wire (except SD07R3) with series resistors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – SDxxR3 3-wire (except SD07R3) with series resistors and no removable fuses
[R10]	SDxxX3 3-wire (except SD07X3) with series inductors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – SDxxX3 3-wire (except SD07X3) with series inductors and no removable fuses
[R11]	TP32 for two active lines.efm, December 12, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – TP32 for two active lines
[R12]	TP48 for three active lines.efm, December 12, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – TP48 for three active lines
[R13]	TP48 for two active lines.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series – TP48 for two active lines
[R14]	xxx SDxxX3 3-wire with series inductors and no removable fuses.efm, December 4, 2007	Failure Modes, Effects, and Diagnostic Analysis - Summary –SD & TP Series –SDxxX3 3-wire with series inductors and no removable fuses
[R15]	AS 07-11-12 R001 V1 R3 SD TP.doc, 01/31/2008	FMEDA report, SD & TP Series (this report)

3 Product Description

The SD & TP Surge Suppressors are designed to reduce the impact of external electrical events on a process control system; this increases the system's reliability.

The SD series surge suppressors are designed to be located at the logic solver. The loop wiring between the sensor/final element and the logic solver passes through the SD surge suppressor; various models have various combinations of series fuses, inductors, and resistors in addition to shunt components.

The TP series surge suppressors are designed for installation at the transmitter or final element. They are connected in parallel with the associated device, thus introducing no series resistance into the wiring.

Table 14 gives an overview of the different versions that were considered in the FMEDA of the SD & TP Series.

Table 14 Version Overview

SD07, SD16, SD32, SD55	Series Surge Suppressor, Inductor, With Fuse
SD07R, SD16R, SD32R, SD55R	Series Surge Suppressor, Resistor, No Fuse
SD07X, SD16X, SD32X, SD55X	Series Surge Suppressor, Inductor, No Fuse
SD07R3	Series Surge Suppressor, 3 Wire, Resistor, No Fuse
SD16R3, SD32R3, SD55R3	Series Surge Suppressor, 3 Wire, Resistor, No Fuse
SD07T3	Series Surge Suppressor, 3 Wire, Inductor/Resistor, No Fuse
SD16T3, SD32T3, SD55T3	Series Surge Suppressor, 3 Wire, Inductor/Resistor, No Fuse
SD07X3	Series Surge Suppressor, 3 Wire, Inductor, No Fuse
SD16X3, SD32X3, SD55X3	Series Surge Suppressor, 3 Wire, Inductor, No Fuse
SDRTD	Series Surge Suppressor, 3 Wire, Inductor, No Fuse, Optimized for 3-Wire RTD
TP24/7	Parallel Surge Suppressor, 24 + 7 Volt
TP32	Parallel Surge Suppressor, 32 Volt
TP48 2W+G	Parallel Surge Suppressor, 48 Volt, 2 Wire Plus Ground
TP48 3W+G	Parallel Surge Suppressor, 48 Volt, 3 Wire Plus Ground
TP48 4W+G	Parallel Surge Suppressor, 48 Volt, 4 Wire Plus Ground

The SD & TP Series are classified as Type A⁴ devices according to IEC 61508, having a hardware fault tolerance of 0.

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

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation obtained from MTL Surge Technologies and is documented in [R1] - [R15].

4.1 Failure Categories description

In order to judge the failure behavior of the SD & TP Series, the following definitions for the failure of the device were considered.

Fail-Safe State

Transmitter	State where the output exceeds the user defined threshold
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state.
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).
Transmitter	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
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current
Residual Effect	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 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.

Depending on the application, a Fail High or a Fail Low failure 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 as safe or dangerous, detected or undetected.

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 operating stress conditions typical of an industrial field environment similar to IEC 60654-1, Class D (Outdoor Locations). 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.

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 the SD & TP Series.

- Only a single component failure will fail the entire SD & TP 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 IEC 60654-1, Class C3 (outdoor location) 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 and the diagnostic coverage provided by the online diagnostics
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions
- The device is installed per manufacturer's instructions
- External power supply failure rates are not included
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C3 with an average temperature over a long period of time of 40°C. 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.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the SD & TP Series FMEDA.

Table 15 Failure rates SD07, SD16, SD32, SD55

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	23.9
Fail Dangerous Detected	14.5
Fail Dangerous Undetected	1.5
Residual Effect	51.4

Table 16 Failure rates SD07R, SD16R, SD32R, SD55R

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	14.3
Fail Dangerous Detected	14.5
Fail Dangerous Undetected	1.5
Residual Effect	31.5

Table 17 Failure rates SD07X, SD16X, SD32X, SD55X

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	14.9
Fail Dangerous Detected	14.5
Fail Dangerous Undetected	1.5
Residual Effect	32.4

Table 18 Failure rates SD07R3, SD07T3, SD07X3

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	22.0
Fail Dangerous Detected	20.1
Fail Dangerous Undetected	6.9
Residual Effect	51.3

Table 19 Failure rates SD16R3, SD16T3, SD16X3, SD32R3, SD32T3, SD32X3, SD55R3, SD55T3, SD55X3

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	22.0
Fail Dangerous Detected	17.8
Fail Dangerous Undetected	5.9
Residual Effect	49.9

Table 20 Failure rates SDRTD

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	21.1
Fail Dangerous Detected	20.1
Fail Dangerous Undetected	9.0
Residual Effect	50.1

Table 21 Failure rates TP24/7

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	11.4
Fail Dangerous Undetected	6.4
Residual Effect	42.9

Table 22 Failure rates TP32

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	12.1
Fail Dangerous Undetected	5.4
Residual Effect	22.9

Table 23 Failure rates TP48 2W+G

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	7.6
Fail Dangerous Undetected	3.5
Residual Effect	20.1

Table 24 Failure rates TP48 3W+G

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	15.1
Fail Dangerous Undetected	7.0
Residual Effect	40.2

Table 25 Failure rates TP48 4W+G

Failure Category	Failure Rate (FIT)
Fail Safe Undetected	0
Fail Dangerous Detected	15.1
Fail Dangerous Undetected	7.0
Residual Effect	40.2

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

Table 26 lists the failure rates for the SD & TP Series according to IEC 61508. According to IEC 61508 [N1], the Safe Failure Fraction of a (sub)system should be determined.

However as the SD & TP Series is only one part of a (sub)system, the SFF should be calculated for the entire sensor / logic / 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: $SFF = 1 - \lambda_{DU} / \lambda_{TOTAL}$

Table 26 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}^5	λ_{DD}	λ_{DU}	SFF ⁶
SD07, SD16, SD32, SD55	0 FIT	75 FIT	15 FIT	2 FIT	-
SD07R, SD16R, SD32R, SD55R	0 FIT	46 FIT	15 FIT	2 FIT	-
SD07X, SD16X, SD32X, SD55X	0 FIT	47 FIT	15 FIT	2 FIT	-
SD07R3, SD07T3, SD07X3	0 FIT	73 FIT	20 FIT	7 FIT	-
SD16R3, SD16T3, SD16X3, SD32R3, SD32T3, SD32X3, SD55R3, SD55T3, SD55X3	0 FIT	72 FIT	18 FIT	6 FIT	-
SDRTD	0 FIT	71 FIT	20 FIT	9 FIT	-
TP24/7	0 FIT	43 FIT	11 FIT	6 FIT	-
TP32	0 FIT	23 FIT	12 FIT	5 FIT	-
TP48 2W+G	0 FIT	20 FIT	8 FIT	4 FIT	-
TP48 3W+G	0 FIT	40 FIT	15 FIT	7 FIT	-
TP48 4W+G	0 FIT	40 FIT	15 FIT	7 FIT	-

The architectural constraint type for the SD & TP 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.

⁵ It is important to realize that the Residual 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

⁶ Safe Failure Fraction needs to be calculated on (sub)system level

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 PFD_{AVG} Calculation SD & TP Series

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1001) SD & TP Series model SD07X. 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 graph the PFD_{AVG} value for a single SD & TP Series model SD07X with a proof test interval of 1 year equals 6.69E-06.

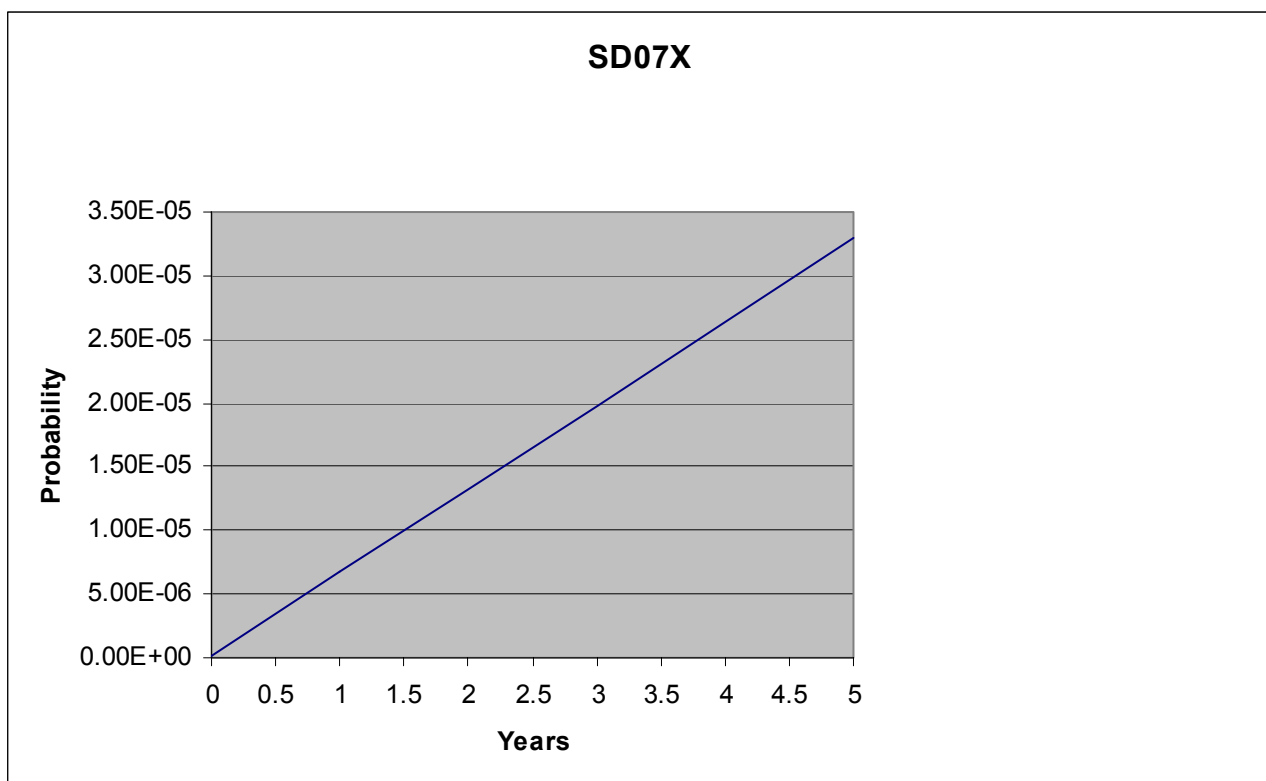


Figure 1: PFDavg vs. Time

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.

For SIL 2 applications, the PFD_{AVG} value needs to be $\geq 10^{-3}$ and $< 10^{-2}$. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval of an SD07X is less than 0.1% 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 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

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: R3

Version History: V1, R3 Updated model descriptions per client feedback, January 31, 2008
V1, R2 Client name updated per client request, December 17, 2007
V1, R1: Released to MTL Surge Technologies; December 13, 2007
V0, R2 Consolidated models per review, December 13, 2007
V0, R1: Draft; December 12, 2007

Author(s): Rudolf Chalupa

Review: V0, R1: William Goble (*exida*); December 12, 2007

Release Status: Released to MTL Surge Technologies

7.3 Future Enhancements

At request of client.

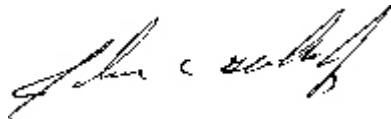
7.4 Release Signatures

A handwritten signature in black ink, appearing to read "William M. Goble", written in a cursive style.

Dr. William M. Goble, Principal Partner

A handwritten signature in black ink, appearing to read "Rudolf P. Chalupa", written in a cursive style.

Rudolf P. Chalupa, Senior Safety Engineer

A handwritten signature in black ink, appearing to read "John C. Grebe Jr.", written in a cursive style.

John C. Grebe Jr., Principal Engineer

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 lifetime⁷ 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.

It is the responsibility of the end user to maintain and operate the SD & TP Series per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

The limiting factors with regard to the useful lifetime of the system are the surge suppressing components (avalanche diode, diac, gas discharge tube, varistor), which have an estimated useful lifetime of about 50 years. This assumes that these components will not be stressed beyond their ratings by applied surges.

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

⁷ 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 consists of a proof test of the associated field device. Note that this proof test will only indicate that the SD & TP Series associated with the field device does not interfere with the operation of that device; it does NOT test whether the surge suppressing capabilities of the SD & TP Series are intact.

Table 27 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Perform a proof test of the field device protected by this SD & TP Series surge suppressor.
3.	Remove the bypass and otherwise restore normal operation