Failure Modes, Effects and Diagnostic Analysis

Project:

Surge protective devices
TERMITRAB complete multistage pluggable

Customer:

PHOENIX CONTACT GmbH & Co. KG
Blomberg
Germany

Contract No.: Phoenix Contact 16**/**06-072

Report No.: Phoenix Contact 16/06-072 R022

Version V2, Revision R1, November 2018

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the surge protective devices TERMITRAB complete multistage pluggable in the versions listed in the drawings referenced in section 2.5.1. Table 1 gives an overview of the different configurations that belong to the considered surge protective devices TERMITRAB complete multistage pluggable.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Only the described configurations were analyzed. All other possible variants or electronics are not covered by this report.

Surge protective devices are not considered to be elements according to IEC 61508-4 section 3.4.5 as they are not performing one or more element safety functions. Therefore there is no need to calculate a SFF (Safe Failure Fraction). Only the interference on safety functions needs to be considered. This interference is expressed in a contribution to the overall PFD_{AVG} / PFH.

The failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook ([N3]) for Profile 1 [1].

Table 1: Configuration overview

TTC-6P-1x2-…DC-UT-I TTC-6P-1x2-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for one 2-wire floating signal circuit. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-1x2-F-…DC-UT-I TTC-6P-1x2-F-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for one 2-wire floating signal circuit. Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-1x2-F-M-…DC-UT-I TTC-6P-1x2-F-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for one 2-wire floating signal circuit. Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-1x2-M-…DC-UT-I TTC-6P-1x2-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for one 2-wire floating signal circuit. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.

[1] See Appendix 3 for further details on the selected profile.

TTC-6P-2x1-…DC-UT-I TTC-6P-2x1-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for two signal circuits with common reference potential. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-2x1-F-…DC-UT-I TTC-6P-2x1-F-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for two signal circuits with common reference potential. Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-2x1-F-M-…DC-UT-I TTC-6P-2x1-F-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for two signal circuits with common reference potential. Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-2x1-M-…DC-UT-I TTC-6P-2x1-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for two signal circuits with common reference potential. Nominal voltages: 12 VDC, 24 VDC, 48 VDC.
TTC-6P-2-HC-…DC-UT-I TTC-6P-2-HC-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for one 2-wire floating signal circuit with high nominal current. Nominal voltages: 24 VDC.
TTC-6P-2-HC-M-…DC-UT-I TTC-6P-2-HC-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for one 2-wire floating signal circuit with high nominal current. Nominal voltages: 24 VDC.
TTC-6P-3-HF-M-…DC-UT-I TTC-6P-3-HF-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for three signal circuits including common reference potential. For HF applications and telecommunication interfaces without supply voltage (up to 90 Mbit/s). Nominal voltages: 12 VDC, 24 VDC.

TTC-6P-3-HF-F-M-…DC-UT-I TTC-6P-3-HF-F-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for three signal circuits including common reference potential. For HF applications and telecommunication interfaces without supply voltage (up to 90 Mbit/s). Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC.
TTC-6P-2xTVSD-…DC-UT-I TTC-6P-2xTVSD-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for two signal circuits with common reference potential. Nominal voltages: 12 VDC, 24 VDC.
TTC-6P-2xTVSD-M-…DC-UT-I TTC-6P-2xTVSD-M-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for two signal circuits with common reference potential. Nominal voltages: 12 VDC, 24 VDC.
TTC-6P-2-…-DC-UT-I TTC-6P-2-…-DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for one two-wire impedance-sensitive signal circuit. Nominal voltages: 24 VDC.
TTC-6P-2-M-…-DC-UT-I TTC-6P-2-M-…-DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for one two-wire impedance-sensitive signal circuit. Nominal voltages: 24 VDC.
TTC-6P-1x2-M-EX-…DC-UT-I TTC-6P-1x2-M-EX-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for one 2-wire floating Ex-i signal circuit. Nominal voltages: 24 VDC.
TTC-6P-2x1-M-EX-…DC-UT-I TTC-6P-2x1-M-EX-…DC-UT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for two Ex-i signal circuits with common reference potential. Nominal voltages: 24 VDC.

TTC-6P-3-HF-F-M-EX-…DC-UT-I TTC-6P-3-HF-F-M-EX-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element with integrated maintenance disconnector for one 3-wire Ex-i signal circuit including common reference potential. For HF applications. Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC.
TTC-6P-1x2-EX-…DC-UT-I TTC-6P-1x2-EX-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for one 2-wire floating Ex-I signal circuit. Nominal voltages: 24 VDC.
TTC-6P-3-HF-…DC-UT-I TTC-6P-3-HF-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for three signal circuits including common reference potential. For HF applications and telecommunication interfaces without supply voltage (up to 90 Mbit/s). Nominal voltages: 12 VDC, 24 VDC.
TTC-6P-3-HF-F-…DC-UT-I TTC-6P-3-HF-F-…DC-PT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for three signal circuits including common reference potential. For HF applications and telecommunication interfaces without supply voltage (up to 90 Mbit/s). Indirect grounding via gas-filled surge arrester. Nominal voltages: 12 VDC, 24 VDC.
TTC-6P-3-…DC-UT-I TTC-6P-3-…DC-PT-I TTC-6P-3-EX-24DC-UT-I	Surge protection device TTC multistage pluggable, consisting of protection plug with integrated status indicator and base element for three equal signal circuits. Indirect grounding via gas-filled surge arrester. Nominal voltages: 5 VDC, 24 VDC.

The following tables show how the above stated requirements are fulfilled.

Table 2: TTC-6P-1x2-…-I – Failure rates [2]

	exida Profile 1	
	Analysis 1 [3]	Analysis 2 [4]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.4	2.4
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	10.4	6.9
Total failure rate (interfering with SIF)	12.8	12.8

Table 3: TTC-6P-1x2-F-… -I – Failure rates [2]

	exida Profile 1	
	Analysis 1 [3]	Analysis 2 [4]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.6	1.6
Fail Dangerous Detected (λ_{DD})	0	5.1
Fail Dangerous Undetected (λ_{DU})	9.9	4.8
Total failure rate (interfering with SIF)	11.5	11.5

[2] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[3] Analysis 1 represents a worst-case analysis.

[4] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 4: TTC-6P-1x2-F-M-… -I – Failure rates [5]

	exida Profile 1	
	Analysis 1 [6]	Analysis 2 [7]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.1	2.1
Fail Dangerous Detected (λ_{DD})	0	5.1
Fail Dangerous Undetected (λ_{DU})	9.9	4.8
Total failure rate (interfering with SIF)	12.0	12.0

Table 5: TTC-6P-1x2-M-…-I – Failure rates [5]

	exida Profile 1	
	Analysis 1 [6]	Analysis 2 [7]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.9	2.9
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	10.4	6.9
Total failure rate (interfering with SIF)	13.3	13.3

[5] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[6] Analysis 1 represents a worst-case analysis.

[7] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 6: TTC-6P-2x1-…-I – Failure rates [8]

	exida Profile 1	
	Analysis 1 [9]	Analysis 2 [10]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.6	1.6
Fail Dangerous Detected (λ_{DD})	0	4.8
Fail Dangerous Undetected (λ_{DU})	7.8	3.0
Total failure rate (interfering with SIF)	9.4	9.4

Table 7: TTC-6P-2x1-F-…-I – Failure rates [8]

	exida Profile 1	
	Analysis 1 [9]	Analysis 2 [10]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.6	1.6
Fail Dangerous Detected (λ_{DD})	0	4.8
Fail Dangerous Undetected (λ_{DU})	8.8	4.0
Total failure rate (interfering with SIF)	10.4	10.4

[8] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[9] Analysis 1 represents a worst-case analysis.

[10] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 8: TTC-6P-2x1-F-M-…-I – Failure rates [11]

	exida Profile 1	
	Analysis 1 [12]	Analysis 2 [13]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.9	1.9
Fail Dangerous Detected (λ_{DD})	0	4.8
Fail Dangerous Undetected (λ_{DU})	8.8	4.0
Total failure rate (interfering with SIF)	10.7	10.7

Table 9: TTC-6P-2x1-M-…-I and TTC-6P-2x1-M-EX-…-I – Failure rates [11]

	exida Profile 1	
	Analysis 1 [12]	Analysis 2 [13]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.9	1.9
Fail Dangerous Detected (λ_{DD})	0	4.8
Fail Dangerous Undetected (λ_{DU})	7.8	3.0
Total failure rate (interfering with SIF)	9.7	9.7

[11] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[12] Analysis 1 represents a worst-case analysis.

[13] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 10: TTC-6P-2-HC-…-I – Failure rates [14]

	exida Profile 1	
	Analysis 1 [15]	Analysis 2 [16]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.4	2.4
Fail Dangerous Detected (λ_{DD})	0	2.5
Fail Dangerous Undetected (λ_{DU})	4.8	2.3
Total failure rate (interfering with SIF)	7.2	7.2

Table 11: TTC-6P-2-HC-M-…-I – Failure rates [14]

	exida Profile 1	
	Analysis 1 [15]	Analysis 2 [16]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.9	2.9
Fail Dangerous Detected (λ_{DD})	0	2.5
Fail Dangerous Undetected (λ_{DU})	4.8	2.3
Total failure rate (interfering with SIF)	7.7	7.7

[14] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[15] Analysis 1 represents a worst-case analysis.

[16] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 12: TTC-6P-3-HF-M-…-I – Failure rates [17]

	exida Profile 1	
	Analysis 1 [18]	Analysis 2 [19]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.9	2.9
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	26.6	23.1
Total failure rate (interfering with SIF)	29.5	29.5

Table 13: TTC-6P-3-HF-F-M-…-I and TTC-6P-3-HF-F-M-EX-…-I – Failure rates [17]

	exida Profile 1	
	Analysis 1 [18]	Analysis 2 [19]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.1	2.1
Fail Dangerous Detected (λ_{DD})	0	20.2
Fail Dangerous Undetected (λ_{DU})	26.1	5.9
Total failure rate (interfering with SIF)	28.2	28.2

[17] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[18] Analysis 1 represents a worst-case analysis.

[19] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 14: TTC-6P-2xTVSD-…-I – Failure rates [20]

	exida Profile 1	
	Analysis 1 [21]	Analysis 2 [22]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.6	1.6
Fail Dangerous Detected (λ_{DD})	0	3.8
Fail Dangerous Undetected (λ_{DU})	4.0	0.2
Total failure rate (interfering with SIF)	5.6	5.6

Table 15: TTC-6P-2xTVSD-M-…-I – Failure rates [20]

	exida Profile 1	
	Analysis 1 [21]	Analysis 2 [22]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.9	1.9
Fail Dangerous Detected (λ_{DD})	0	3.8
Fail Dangerous Undetected (λ_{DU})	4.0	0.2
Total failure rate (interfering with SIF)	5.9	5.9

[20] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[21] Analysis 1 represents a worst-case analysis.

[22] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 16: TTC-6P-2-…-I – Failure rates [23]

	exida Profile 1	
	Analysis 1 [24]	Analysis 2 [25]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.4	2.4
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	6.8	3.3
Total failure rate (interfering with SIF)	9.2	9.2

Table 17: TTC-6P-2-M-…-I – Failure rates [23]

	exida Profile 1	
	Analysis 1 [24]	Analysis 2 [25]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.9	2.9
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	6.8	3.3
Total failure rate (interfering with SIF)	9.7	9.7

[23] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[24] Analysis 1 represents a worst-case analysis.

[25] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 18: TTC-6P-1x2-M-EX-…-I – Failure rates [26]

	exida Profile 1	
	Analysis 1 [27]	Analysis 2 [28]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.9	2.9
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	10.4	6.9
Total failure rate (interfering with SIF)	13.3	13.3

Table 19: TTC-6P-1x2-EX-…-I – Failure rates [26]

	exida Profile 1	
	Analysis 1 [27]	Analysis 2 [28]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.4	2.4
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	10.4	6.9
Total failure rate (interfering with SIF)	12.8	12.8

[26] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[27] Analysis 1 represents a worst-case analysis.

[28] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 20: TTC-6P-3-HF-…-I – Failure rates [29]

	exida Profile 1	
	Analysis 1 [30]	Analysis 2 [31]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	2.4	2.4
Fail Dangerous Detected (λ_{DD})	0	3.5
Fail Dangerous Undetected (λ_{DU})	26.6	23.1
Total failure rate (interfering with SIF)	29.0	29.0

Table 21: TTC-6P-3-HF-F-…-I – Failure rates [29]

	exida Profile 1	
	Analysis 1 [30]	Analysis 2 [31]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0	0
Fail Safe Undetected (λ_{SU})	1.6	1.6
Fail Dangerous Detected (λ_{DD})	0	20.2
Fail Dangerous Undetected (λ_{DU})	26.1	5.9
Total failure rate (interfering with SIF)	27.7	27.7

[29] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[30] Analysis 1 represents a worst-case analysis.

[31] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table 22: TTC-6P-3-…DC-…-I – Failure rates [32]

	exida Profile 1	
	Analysis 1 [33]	Analysis 2 [34]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**7.6**
Fail Dangerous Undetected (λ_{DU})	**24.0**	**16.4**
Total failure rate (interfering with SIF)	**26.4**	**26.4**

The failure rates are valid for the useful life of the surge protective devices TERMITRAB complete multistage pluggable (see Appendix 2).

[32] It is assumed that complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.

[33] Analysis 1 represents a worst-case analysis.

[34] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

Table of Contents

1 Purpose and Scope

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the surge protective devices TERMITRAB complete multistage pluggable in the versions listed in the drawings referenced in section 2.5.1. Table 1 gives an overview of the different configurations that belong to the considered surge protective devices TERMITRAB complete multistage pluggable.

The FMEDA builds the basis for an evaluation whether a final element subsystem, including the surge protective devices TERMITRAB complete multistage pluggable meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per Hour (PFH) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety or the correct functioning of the surge protective device.

2 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 400 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, 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

PHOENIX CONTACT GmbH & Co. KG	Manufacturer of the surge protective devices TERMITRAB complete multistage pluggable.
exida	Performed the hardware assessment.

PHOENIX CONTACT GmbH & Co. KG contracted *exida* in June 2016 and March 2018 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 61508-2:2010	Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/ programmable electronic safety related systems
[N2]	IEC 61508-4:2010	Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 4: Definitions and abbreviations
[N3]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0

2.4 *exida* tools used

[T1]	SILcal V8.0.14	FMEDA Tool
[T2]	exSILentia V3.7.1.1119	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	SIL- FMEDA-Bericht TTC_Mehrstufig_plug_R01_V00.pdf	Safety considerations for TERMITRAB complete multistage pluggable including parts lists and circuit diagrams; R01.V00 of 20.09.2018

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.5.2 Documentation generated by *exida*

[R1]	FMEDA_TTC-6P-1x2-...-I_V1R0.efm of 13.10.2016
[R2]	FMEDA_TTC-6P-1x2-...-I_w_ED_V1R0.efm of 13.10.2016
[R3]	FMEDA_TTC-6P-1x2-F-...-I_V1R0.efm of 13.10.2016
[R4]	FMEDA_TTC-6P-1x2-F-...-I_w_ED_V1R0.efm of 13.10.2016
[R5]	FMEDA_TTC-6P-1x2-F-M-...-I_V1R0.efm of 13.10.2016
[R6]	FMEDA_TTC-6P-1x2-F-M-...-I_w_ED_V1R0.efm of 13.10.2016
[R7]	FMEDA_TTC-6P-1x2-M-...-I_V1R0.efm of 13.10.2016
[R8]	FMEDA_TTC-6P-1x2-M-...-I_w_ED_V1R0.efm of 13.10.2016
[R9]	FMEDA_TTC-6P-1x2-M-EX-...-I_V1R0.efm of 13.10.2016
[R10]	FMEDA_TTC-6P-1x2-M-EX-...-I_w_ED_V1R0.efm of 13.10.2016
[R11]	FMEDA_TTC-6P-2-...-I_V1R0.efm of 13.10.2016
[R12]	FMEDA_TTC-6P-2-...-I_w_ED_V1R0.efm of 13.10.2016
[R13]	FMEDA_TTC-6P-2-HC-...-I_V1R0.efm of 13.10.2016
[R14]	FMEDA_TTC-6P-2-HC-...-I_w_ED_V1R0.efm of 13.10.2016
[R15]	FMEDA_TTC-6P-2-HC-M-...-I_V1R0.efm of 13.10.2016
[R16]	FMEDA_TTC-6P-2-HC-M-...-I_w_ED_V1R0.efm of 13.10.2016
[R17]	FMEDA_TTC-6P-2-M-...-I_V1R0.efm of 13.10.2016
[R18]	FMEDA_TTC-6P-2-M-...-I_w_ED_V1R0.efm of 13.10.2016
[R19]	FMEDA_TTC-6P-2x1-...-I_V1R0.efm of 13.10.2016
[R20]	FMEDA_TTC-6P-2x1-...-I_w_ED_V1R0.efm of 13.10.2016
[R21]	FMEDA_TTC-6P-2x1-F-...-I_V1R1.efm of 13.10.2016
[R22]	FMEDA_TTC-6P-2x1-F-...-I_w_ED_V1R1.efm of 13.10.2016
[R23]	FMEDA_TTC-6P-2x1-F-M-...-I_V1R0.efm of 13.10.2016
[R24]	FMEDA_TTC-6P-2x1-F-M-...-I_w_ED_V1R0.efm of 13.10.2016
[R25]	FMEDA_TTC-6P-2x1-M-...-I_&_TTC-6P-2x1-M-EX-...-I_V1R0.efm of 13.10.2016
[R26]	FMEDA_TTC-6P-2x1-M-...-I_&_TTC-6P-2x1-M-EX-...-I_w_ED_V1R0.efm of 13.10.2016

[R27]	FMEDA_TTC-6P-2xTVSD-...-I_V1R0.efm of 13.10.2016
[R28]	FMEDA_TTC-6P-2xTVSD-...-I_w_ED_V1R0.efm of 13.10.2016
[R29]	FMEDA_TTC-6P-2xTVSD-M-...-I_V1R0.efm of 13.10.2016
[R30]	FMEDA_TTC-6P-2xTVSD-M-...-I_w_ED_V1R0.efm of 13.10.2016
[R31]	FMEDA_TTC-6P-3-HF-F-M-...-I_&_TTC-6P-3-HF-F-M-EX-...-I _V1R0.efm of 13.10.2016
[R32]	FMEDA_TTC-6P-3-HF-F-M-...-I_&_TTC-6P-3-HF-F-M-EX-...-I _w_ED_V1R1.efm of 14.11.2016
[R33]	FMEDA_TTC-6P-3-HF-M-...-I _V1R0.efm of 13.10.2016
[R34]	FMEDA_TTC-6P-3-HF-M-...-I _w_ED_V1R0.efm of 13.10.2016
[R35]	FMEDA_TTC-6P-1x2-EX-...-I_V1R0.efm of 26.10.2018
[R36]	FMEDA_TTC-6P-1x2-EX-...-I_w_ED_V1R0.efm of 26.10.2018
[R37]	FMEDA_TTC-6P-3-...DC-...-I _V1R0.efm of 26.10.2018
[R38]	FMEDA_TTC-6P-3-...DC-...-I_w_ED_V1R0.efm of 26.10.2018
[R39]	FMEDA_TTC-6P-3-HF-...-I _V1R0.efm of 26.10.2018
[R40]	FMEDA_TTC-6P-3-HF-...-I_w_ED_V1R0.efm of 26.10.2018
[R41]	FMEDA_TTC-6P-3-HF-F-...-I _V1R0.efm of 26.10.2018
[R42]	FMEDA_TTC-6P-3-HF-F-...-I_w_ED_V1R0.efm of 26.10.2018

3 Description of the analyzed devices

The FMEDA of the surge protective devices TERMITRAB complete multistage pluggable has been carried out on the parts indicated in the following figures.

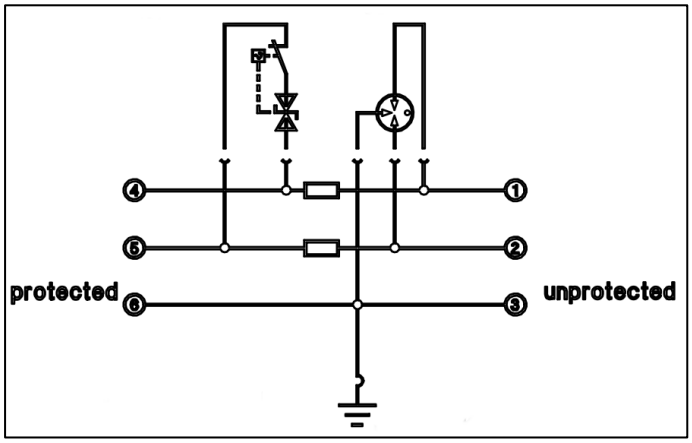


Figure 1: Circuit diagram of TTC-6P-1x2-…-I

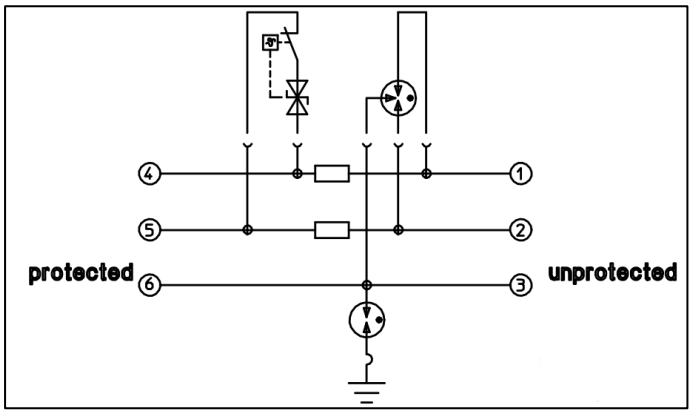


Figure 2: Circuit diagram of TTC-6P-1x2-F-…-I

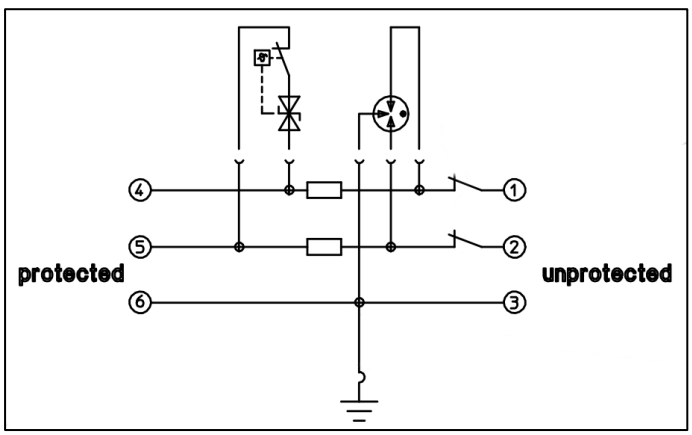


Figure 3: Circuit diagram of TTC-6P-1x2-M-…-I

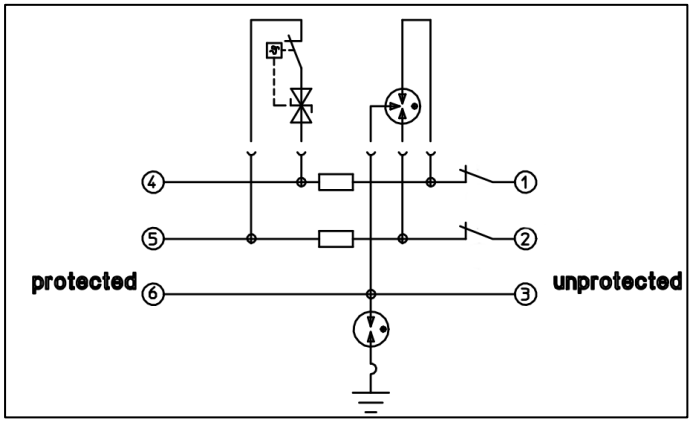


Figure 4: Circuit diagram of TTC-6P-1x2-F-M-…-I

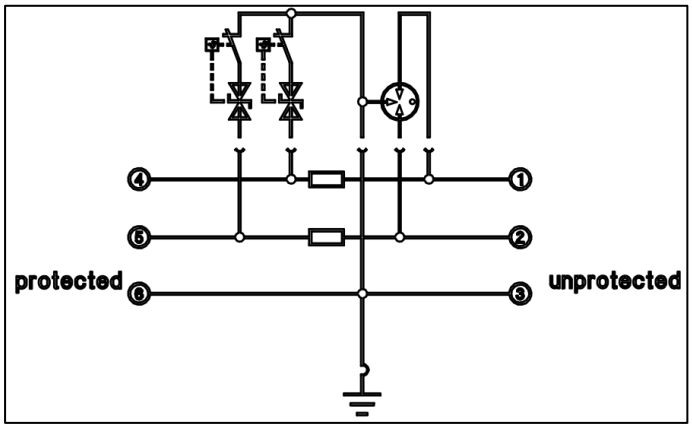


Figure 5: Circuit diagram of TTC-6P-2x1-…-I

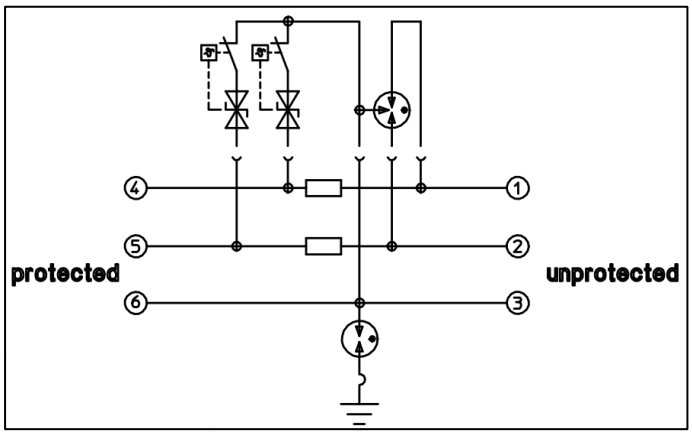


Figure 6: Circuit diagram of TTC-6P-2x1-F-…-I

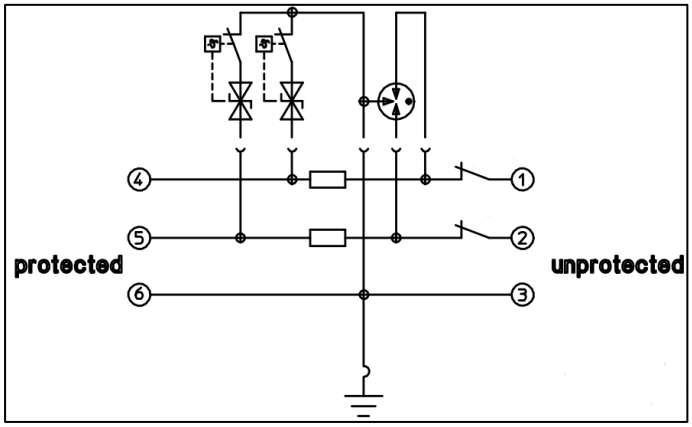


Figure 7: Circuit diagram of TTC-6P-2x1-M-…-I

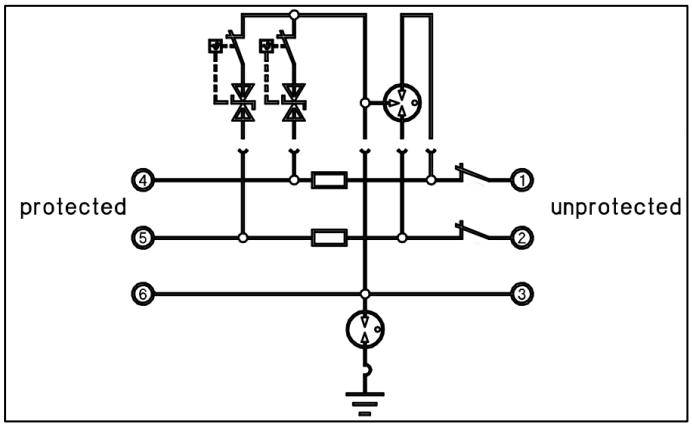


Figure 8: Circuit diagram of TTC-6P-2x1-F-M-…-I

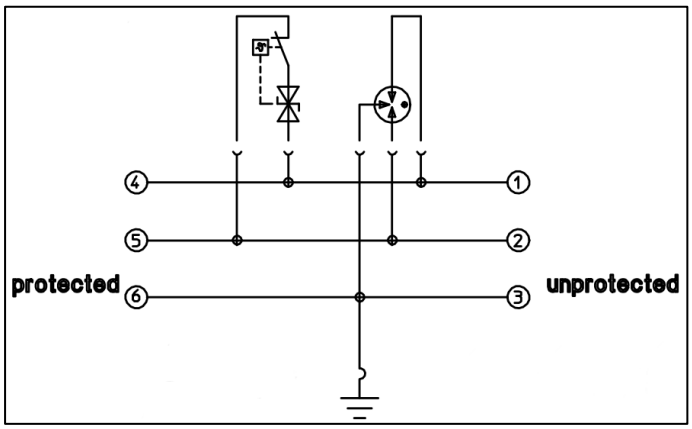


Figure 9: Circuit diagram of TTC-6P-2-HC-…-I

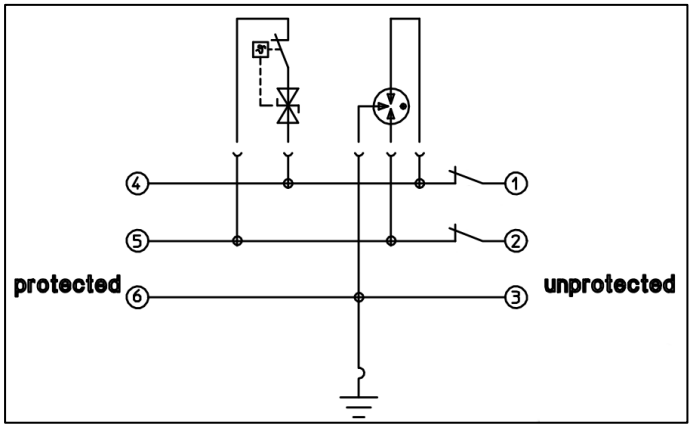


Figure 10: Circuit diagram of TTC-6P-2-HC-M-…-I

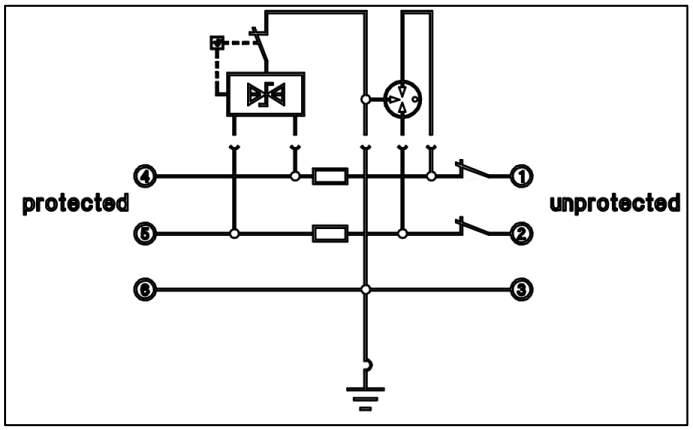


Figure 11: Circuit diagram of TTC-6P-3-HF-M-…-I

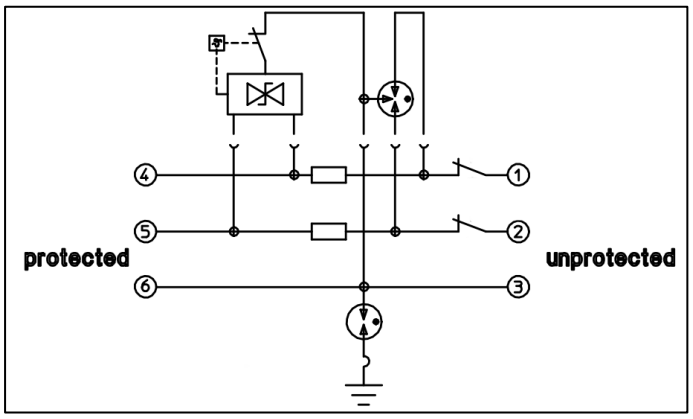


Figure 12: Circuit diagram of TTC-6P-3-HF-F-M-…-I

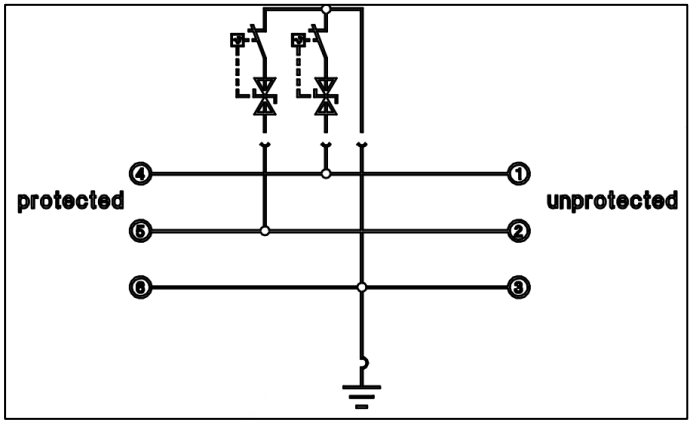


Figure 13: Circuit diagram of TTC-6P-2xTVSD-…-I

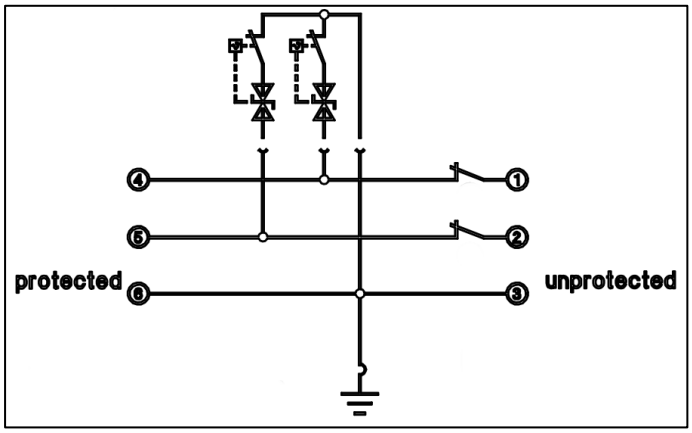


Figure 14: Circuit diagram of TTC-6P-2xTVSD-M-…-I

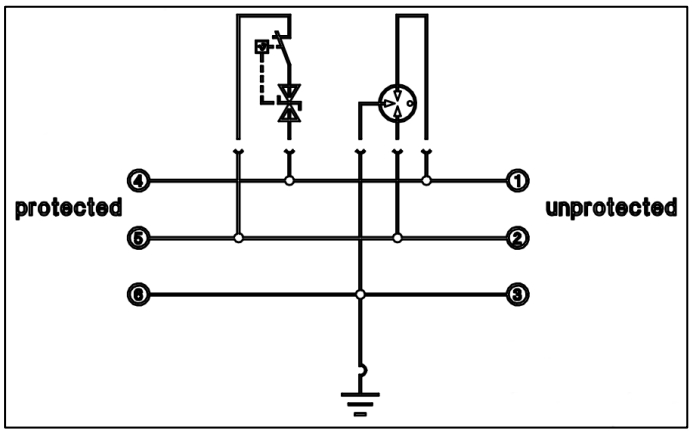


Figure 15: Circuit diagram of TTC-6P-2-…-I

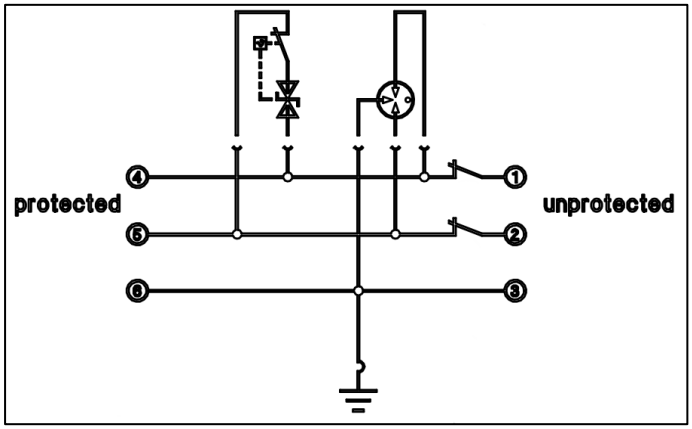


Figure 16: Circuit diagram of TTC-6P-2-M-…-I

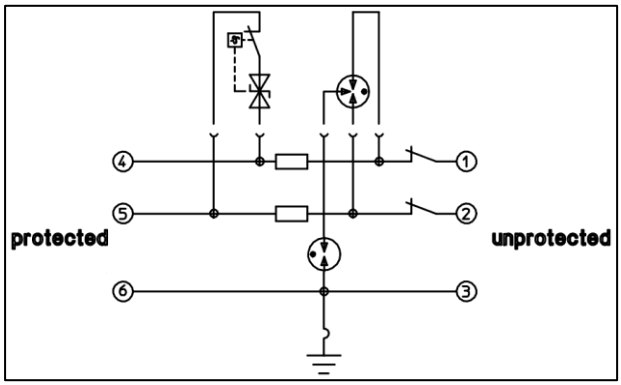


Figure 17: Circuit diagram of TTC-6P-1x2-M-EX-…-I

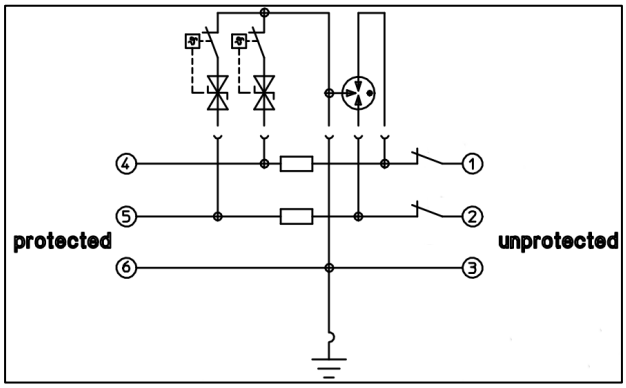


Figure 18: Circuit diagram of TTC-6P-2x1-M-EX-…-I

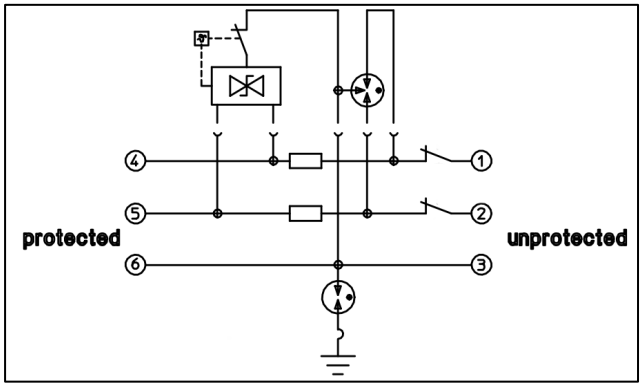


Figure 19: Circuit diagram of TTC-6P-3-HF-F-M-EX-…-I

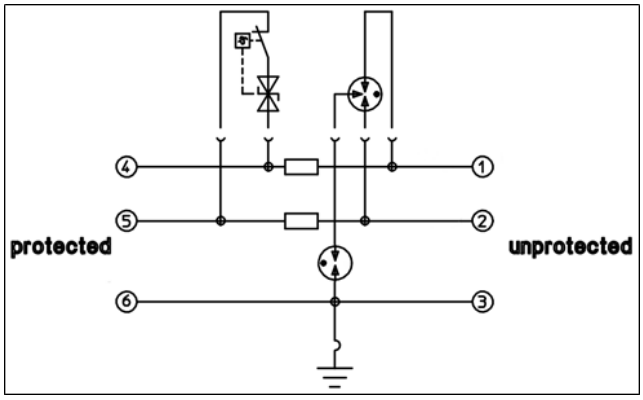


Figure 20: Circuit diagram of TTC-6P-1x2-EX-…-I

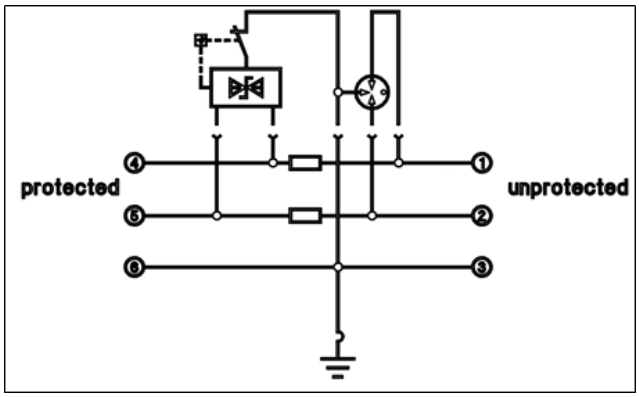


Figure 21: Circuit diagram of TTC-6P-3-HF-…-I

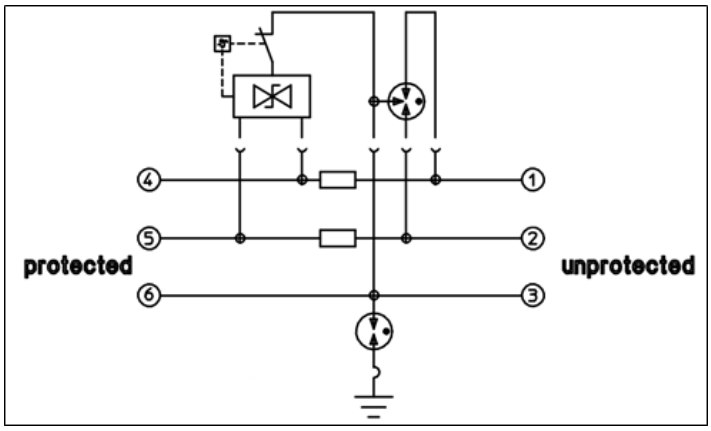


Figure 22: Circuit diagram of TTC-6P-3-HF-F-…-I

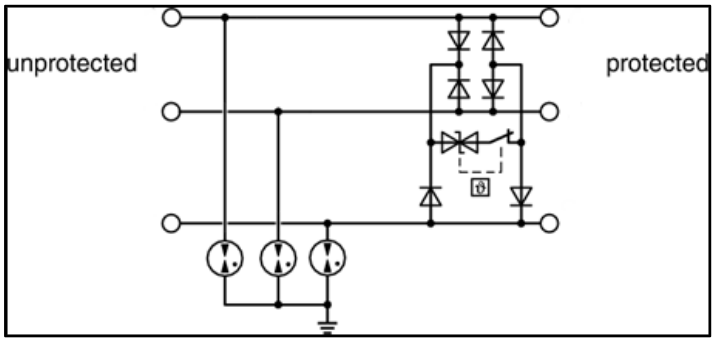


Figure 23: Circuit diagram of TTC-6P-3-…DC-…-I

The following two figures Figure 24 and Figure 25 show how the surge protective devices (SPD) can be connected to other devices. All considered surge protective devices can be used with analog or binary devices.

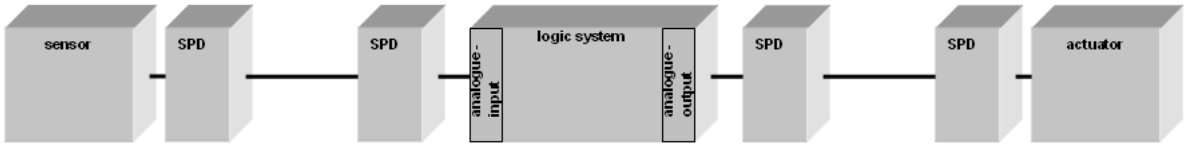


Figure 24: Connection with analog devices

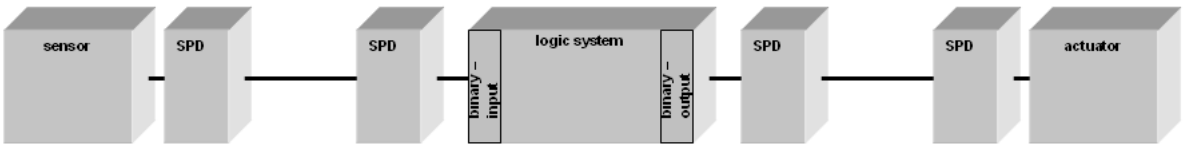


Figure 25: Connection with binary devices

Figure 26 shows how faults of the surge protective devices on the actuator side can be detected. On the sensor side faults can be detected by the safety PLC via an out of range check as the input signal will be outside the allowed range of 4-20mA or 2-10V in case of line short circuits and short circuits to GND.

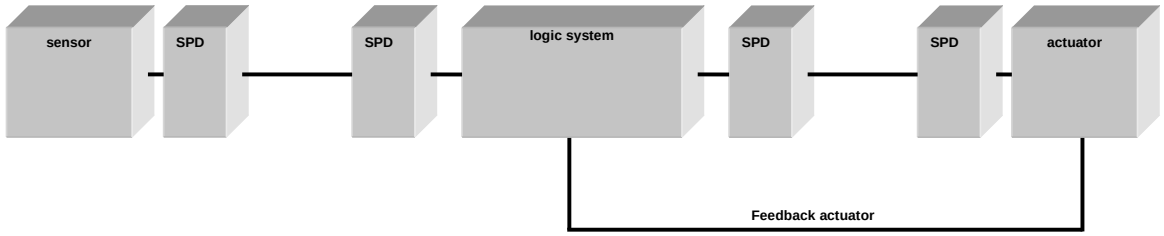


Figure 26: Connection for fault detection

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with PHOENIX CONTACT GmbH & Co. KG and is documented in [R1] to [R42]. Failures have been classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the surge protective devices TERMITRAB complete multistage pluggable, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output corresponding to the fail-safe output specified for the individual safety function. A dangerous failure is therefore a failure that does not correspond to the input signal of the SPD and therefore leads to a corrupted analog or binary output signal.
Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU).
Dangerous Detected	Failure that is dangerous but is detected by external diagnostics (DD).
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.
No part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

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 Modes, Effects, and Diagnostic Analysis) is a 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 the Electrical Component Reliability Handbook ([N3]) which was derived using over ten billion unit operational hours of 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 *exida* Profile 1. 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 or physical abuse.

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”.

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 such as *exida* SILStat™ 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 surge protective devices TERMITRAB complete multistage pluggable.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.
- The device is installed per manufacturer's instructions.
- The device is used within its specified limits.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- For safety applications only the described configurations are considered.
- In case of multiple channel devices only one channel is part of the considered safety function. If multiple channels are used in a safety function then the given failure rates need to be multiplied by the number of used channels.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) is 24 hours.
- Devices using differential transmission mode and which are decoupled from earth via GDT, don´t have any connected potential on terminal 3 and 6. In case of connected potential to terminal 3 or 6, the dangerous undetected failure rate (λ_{DU}) of the equivalent article without decoupling from earth shall be used.

4.4 Results

For the calculation the following has to be noted:

λ_{total} consists of the sum of all component failure rates. This means:

$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

4.4.1 TTC-6P-1x2-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-1x2-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [35]	**Analysis 2** [36]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**10.4**	**6.9**
Total failure rate (interfering with SIF)	**12.8**	**12.8**
No effect	25.7	25.7
No part	0	0

[35] Analysis 1 represents a worst-case analysis.

[36] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.2 TTC-6P-1x2-F-… -I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-1x2-F-… -I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [37]	**Analysis 2** [38]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.6**	**1.6**
Fail Dangerous Detected (λ_{DD})	**0**	**5.1**
Fail Dangerous Undetected (λ_{DU})	**9.9**	**4.8**
Total failure rate (interfering with SIF)	**11.5**	**11.5**
No effect	44.5	44.5
No part	0	0

[37] Analysis 1 represents a worst-case analysis.

[38] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.3 TTC-6P-1x2-F-M-… -I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-1x2-F-M-… -I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [39]	**Analysis 2** [40]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.1**	**2.1**
Fail Dangerous Detected (λ_{DD})	**0**	**5.1**
Fail Dangerous Undetected (λ_{DU})	**9.9**	**4.8**
Total failure rate (interfering with SIF)	**12.0**	**12.0**
No effect	44.5	44.5
No part	0	0

[39] Analysis 1 represents a worst-case analysis.

[40] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.4 TTC-6P-1x2-M-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-1x2-M-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [41]	**Analysis 2** [42]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.9**	**2.9**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**10.4**	**6.9**
Total failure rate (interfering with SIF)	**13.3**	**13.3**
No effect	25.7	25.7
No part	0	0

[41] Analysis 1 represents a worst-case analysis.

[42] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.5 TTC-6P-2x1-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2x1-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [43]	**Analysis 2** [44]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.6**	**1.6**
Fail Dangerous Detected (λ_{DD})	**0**	**4.8**
Fail Dangerous Undetected (λ_{DU})	**7.8**	**3.0**
Total failure rate (interfering with SIF)	**9.4**	**9.4**
No effect	24.2	24.2
No part	0	0

[43] Analysis 1 represents a worst-case analysis.

[44] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.6 TTC-6P-2x1-F-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2x1-F-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [45]	**Analysis 2** [46]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.6**	**1.6**
Fail Dangerous Detected (λ_{DD})	**0**	**4.8**
Fail Dangerous Undetected (λ_{DU})	**8.8**	**4.0**
Total failure rate (interfering with SIF)	**10.4**	**10.4**
No effect	43.2	43.2
No part	0	0

[45] Analysis 1 represents a worst-case analysis.

[46] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.7 TTC-6P-2x1-F-M-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2x1-F-M-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [47]	**Analysis 2** [48]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.9**	**1.9**
Fail Dangerous Detected (λ_{DD})	**0**	**4.8**
Fail Dangerous Undetected (λ_{DU})	**8.8**	**4.0**
Total failure rate (interfering with SIF)	**10.7**	**10.7**
No effect	43.2	43.2
No part	0	0

[47] Analysis 1 represents a worst-case analysis.

[48] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.8 TTC-6P-2x1-M-…-I and TTC-6P-2x1-M-EX-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2x1-M-…-I and TTC-6P-2x1-M-EX-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [49]	**Analysis 2** [50]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.9**	**1.9**
Fail Dangerous Detected (λ_{DD})	**0**	**4.8**
Fail Dangerous Undetected (λ_{DU})	**7.8**	**3.0**
Total failure rate (interfering with SIF)	**9.7**	**9.7**
No effect	24.2	24.2
No part	0	0

[49] Analysis 1 represents a worst-case analysis.

[50] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.9 TTC-6P-2-HC-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2-HC-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [51]	**Analysis 2** [52]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**2.5**
Fail Dangerous Undetected (λ_{DU})	**4.8**	**2.3**
Total failure rate (interfering with SIF)	**7.2**	**7.2**
No effect	66.8	66.8
No part	0	0

[51] Analysis 1 represents a worst-case analysis.

[52] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.10 TTC-6P-2-HC-M-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2-HC-M-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [53]	**Analysis 2** [54]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.9**	**2.9**
Fail Dangerous Detected (λ_{DD})	**0**	**2.5**
Fail Dangerous Undetected (λ_{DU})	**4.8**	**2.3**
Total failure rate (interfering with SIF)	**7.7**	**7.7**
No effect	66.8	66.8
No part	0	0

[53] Analysis 1 represents a worst-case analysis.

[54] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.11 TTC-6P-3-HF-M-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-3-HF-M-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [55]	**Analysis 2** [56]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.9**	**2.9**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**26.6**	**23.1**
Total failure rate (interfering with SIF)	**29.5**	**29.5**
No effect	26.6	26.6
No part	0	0

[55] Analysis 1 represents a worst-case analysis.

[56] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.12 TTC-6P-3-HF-F-M-…-I and TTC-6P-3-HF-F-M-EX-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-3-HF-F-M-…-I and TTC-6P-3-HF-F-M-EX-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [57]	**Analysis 2** [58]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.1**	**2.1**
Fail Dangerous Detected (λ_{DD})	**0**	**20.2**
Fail Dangerous Undetected (λ_{DU})	**26.1**	**5.9**
Total failure rate (interfering with SIF)	**28.2**	**28.2**
No effect	45.4	45.4
No part	0	0

[57] Analysis 1 represents a worst-case analysis.

[58] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.13 TTC-6P-2xTVSD-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2xTVSD-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [59]	**Analysis 2** [60]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.6**	**1.6**
Fail Dangerous Detected (λ_{DD})	**0**	**3.8**
Fail Dangerous Undetected (λ_{DU})	**4.0**	**0.2**
Total failure rate (interfering with SIF)	**5.6**	**5.6**
No effect	6.2	6.2
No part	0	0

[59] Analysis 1 represents a worst-case analysis.

[60] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.14 TTC-6P-2xTVSD-M-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2xTVSD-M-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [61]	**Analysis 2** [62]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.9**	**1.9**
Fail Dangerous Detected (λ_{DD})	**0**	**3.8**
Fail Dangerous Undetected (λ_{DU})	**4.0**	**0.2**
Total failure rate (interfering with SIF)	**5.9**	**5.9**
No effect	6.2	6.2
No part	0	0

[61] Analysis 1 represents a worst-case analysis.

[62] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.15 TTC-6P-2-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [63]	**Analysis 2** [64]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**6.8**	**3.3**
Total failure rate (interfering with SIF)	**9.2**	**9.2**
No effect	25.7	25.7
No part	0	0

[63] Analysis 1 represents a worst-case analysis.

[64] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.16 TTC-6P-2-M-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-2-M-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [65]	**Analysis 2** [66]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.9**	**2.9**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**6.8**	**3.3**
Total failure rate (interfering with SIF)	**9.7**	**9.7**
No effect	25.7	25.7
No part	0	0

[65] Analysis 1 represents a worst-case analysis.

[66] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.17 TTC-6P-1x2-M-EX-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-1x2-M-EX-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [67]	**Analysis 2** [68]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.9**	**2.9**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**10.4**	**6.9**
Total failure rate (interfering with SIF)	**13.3**	**13.3**
No effect	45.7	45.7
No part	0	0

[67] Analysis 1 represents a worst-case analysis.

[68] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.18 TTC-6P-1x2-EX-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-1x2-EX-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [69]	**Analysis 2** [70]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**10.4**	**6.9**
Total failure rate (interfering with SIF)	**12.8**	**12.8**
No effect	45.7	45.7
No part	0	0

[69] Analysis 1 represents a worst-case analysis.

[70] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.19 TTC-6P-3-HF-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-3-HF-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [71]	**Analysis 2** [72]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**3.5**
Fail Dangerous Undetected (λ_{DU})	**26.6**	**23.1**
Total failure rate (interfering with SIF)	**29.0**	**29.0**
No effect	26.6	26.6
No part	0	0

[71] Analysis 1 represents a worst-case analysis.

[72] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.20 TTC-6P-3-HF-F-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-3-HF-F-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [73]	**Analysis 2** [74]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**1.6**	**1.6**
Fail Dangerous Detected (λ_{DD})	**0**	**20.2**
Fail Dangerous Undetected (λ_{DU})	**26.1**	**5.9**
Total failure rate (interfering with SIF)	**27.7**	**27.7**
No effect	45.4	45.4
No part	0	0

[73] Analysis 1 represents a worst-case analysis.

[74] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

4.4.21 TTC-6P-3-…DC-…-I

The FMEDA carried out on the surge protective devices TERMITRAB complete multistage pluggable TTC-6P-3-…DC-…-I leads under the assumptions described in section 4.3 and the definitions given in section 4.1 to the following failure rates.

	***exida* Profile 1**	
	Analysis 1 [75]	**Analysis 2** [76]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2.4**	**2.4**
Fail Dangerous Detected (λ_{DD})	**0**	**7.6**
Fail Dangerous Undetected (λ_{DU})	**24.0**	**16.4**
Total failure rate (interfering with SIF)	**26.4**	**26.4**
No effect	65.6	65.6
No part	0	0

[75] Analysis 1 represents a worst-case analysis.

[76] Analysis 2 represents an analysis with the assumption that line short circuits and short circuits to GND are detectable or do not have an effect.

5 Using the FMEDA results

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. The following section describes how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} / PFH calculation

The following 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).

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) surge protective device TERMITRAB complete multistage pluggable TTC-6P-1x2-F-…-I with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.4.2 for analysis 2. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 23 lists the results for different proof test intervals considering a proof test coverage of 99% (see Appendix 1.1).

Table 23: PFD_{AVG} / PFH values

T[Proof] = 1 year	T[Proof] = 5 years	PFH
PFD_{AVG} = 2.30E-05	PFD_{AVG} = 1.06E-04	PFH = 4.80E-09 1/h

For SIL3 the overall PFD_{AVG} shall be better than 1.00E-03 and the PFH shall be better than 1.00E-07 1/h. As the surge protective device is contributing to the entire safety function it should only consume a certain percentage of the allowed range. Assuming 5% of this range as a reasonable budget it should be better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively. The PFH value and the calculated PFD_{AVG} value for a proof test interval of 1 year are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 5% of the allowed range, i.e. to be better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively.

In order to check whether the above mentioned requirements (for identical assumptions) are fulfilled for a device listed in sections 4.4.1 to 4.4.17, the lambda λ_{DU} of the selected article must be below or equal to the values presented in Table 24 or Table 25, respectively.

Table 24: λ_{DU} limit for low demand mode applications

T[Proof]	Maximum allowed λ_{DU}	Budget of SIF for SIL 3
1 year	$\lambda_{DU} \leq$ 10 FIT	≈ 5%
1 year	$\lambda_{DU} \leq$ 20 FIT	≈ 10%
1 year	$\lambda_{DU} \leq$ 30 FIT	≈ 15%
0.5 years	$\lambda_{DU} \leq$ 18 FIT	≈ 5%
0.5 years	$\lambda_{DU} \leq$ 37 FIT	≈ 10%

Table 25: λ_{DU} limit for high demand mode applications

Maximum allowed λ_{DU}	Budget of SIF for SIL 3
$\lambda_{DU} \leq 5$ FIT	5%
$\lambda_{DU} \leq 10$ FIT	10%
$\lambda_{DU} \leq 15$ FIT	15%
$\lambda_{DU} \leq 20$ FIT	20%
$\lambda_{DU} \leq 25$ FIT	25%

The resulting PFD_{AVG} graph of the surge protective device TERMITRAB complete multistage pluggable TTC-6P-1x2-F-…-I generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 27.

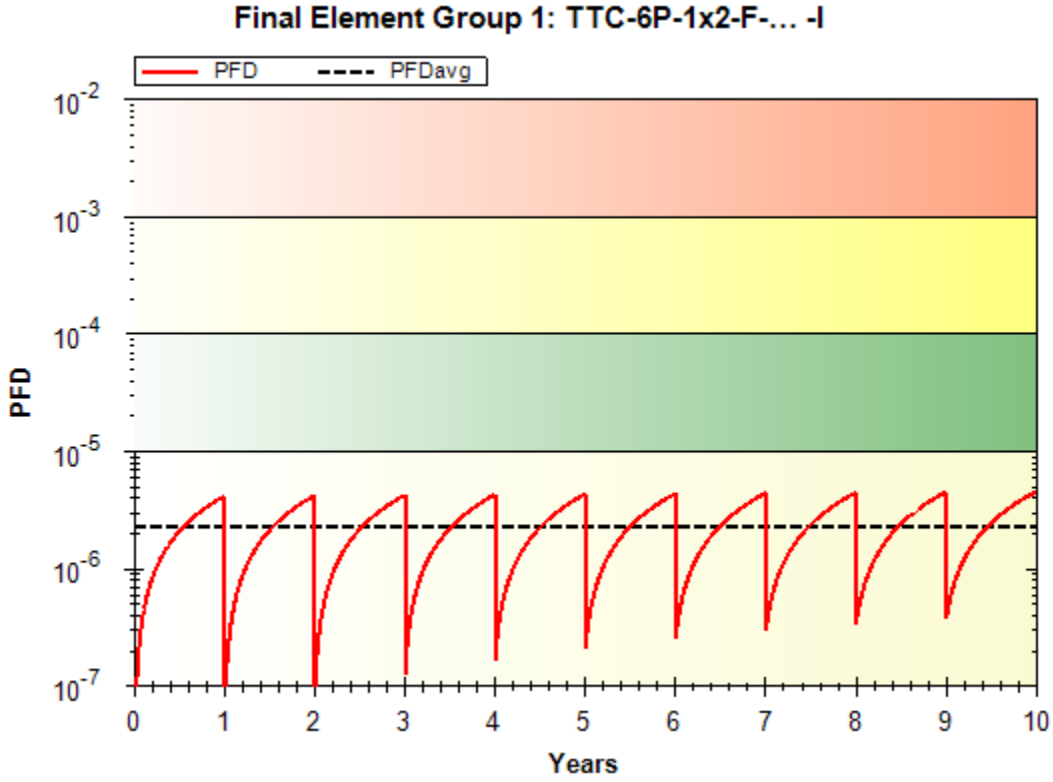


Figure 27: $PFD_{AVG}(t)$

An average Probability of Failure on Demand (PFD_{AVG}) calculation performed for homogenous redundant (1oo2) surge protective devices (according to analysis 2) considering a proof test coverage of 99% (see Appendix 1.1), a mission time of 10 years, a Mean Time To Restoration of 24 hours, a maintenance capability of 100% and a common cause factor of 10% would result in a PFD_{AVG} value for a one year proof test interval of 10% of the PFD_{AVG} value for 1oo1.

6 Terms and Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, 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.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTBF	Mean Time Between Failure
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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
SPD	Surge Protective Device
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares 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.

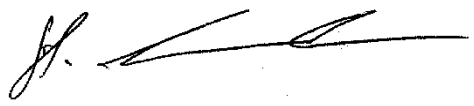
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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 History:	V2R1	Editorial changes; November 5, 2018
	V2R0	Additional devices added; October 29, 2018
	V1R1	Assumptions adjusted; November 15, 2016
	V1R0	Review comments incorporated; November 15, 2016
	V0R1	Initial version; October 28, 2016
Author:	Stephan Aschenbrenner	
Review:	V2R0	Stephan Seggebruch (PHOENIX CONTACT); November 5, 2018
	V1R0	Stephan Seggebruch (PHOENIX CONTACT); November 15, 2016
	V0R1	Stephan Seggebruch (PHOENIX CONTACT); November 7, 2016
		Dr. Cornelius Rieß (*exida*); November 4, 2016
Release status:	Released to PHOENIX CONTACT GmbH & Co. KG	

7.3 Release Signatures



Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

Dr. rer. nat. Cornelius Rieß, Senior Safety Engineer

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.5.2 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.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1: Proof test to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 26.

Table 26 Steps for a possible proof test

Step	Action
1	Bypass the connected safety device(s) or take other appropriate action to avoid a false trip
2	Force the surge protective devices TERMITRAB complete multistage pluggable to reach predefined output levels over the entire range and verify that the output behaves as expected.
3	Restore the loop to full operation
4	Remove the bypass from the connected safety device(s) or otherwise restore normal operation

This test will detect approximately 99% of possible “du” failures of the surge protective devices TERMITRAB complete multistage pluggable.

Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.9.5 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[77] 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.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

The surge protective devices TERMITRAB complete multistage pluggable do not contain components with reduced useful lifetime which are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation. Therefore there is no limiting factor to the useful lifetime.

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

[77] 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 3: *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30°C	25°C	25°C	5°C	25°C	25°C
Average Internal Temperature	60°C	30°C	45°C	5°C	45°C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5°C	25°C	25°C	0°C	25°C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5°C	40°C	40°C	2°C	40°C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[78]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[79]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[80]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[81]	G2	G3	G3	G3	G3	Compatible Material
Surge[82]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[83]						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)[84]	6kV	6kV	6kV	6kV	6kV	N/A

[78] Humidity rating per IEC 60068-2-3
[79] Shock rating per IEC 60068-2-27
[80] Vibration rating per IEC 60068-2-6
[81] Chemical Corrosion rating per ISA 71.04
[82] Surge rating per IEC 61000-4-5
[83] EMI Susceptibility rating per IEC 6100-4-3
[84] ESD (Air) rating per IEC 61000-4-2