Failure Modes, Effects and Diagnostic Analysis

Project:

Surge protective devices
PLUGTRAB PT

Customer:

PHOENIX CONTACT GmbH & Co. KG
Blomberg
Germany

Contract No.: Phoenix Contact 14/09-007

Report No.: Phoenix Contact 14/09-007 R020

Version V2, Revision R1, March 2016

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the surge protective devices PLUGTRAB PT 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 PLUGTRAB PT.

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 a 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 ([N2]) for Profile 1 [1].

Table 1: Configuration overview

PT 2x2-…DC/AC	Protective plug PT with protective circuit for two 2-core floating signal circuits; nominal voltages: 5 VDC, 12 VDC, 24 VDC, 12 VAC and 24 VAC; HART compatible. Available with base element directly connected to the mounting or connected via gas discharge tube with the mounting.
PT 1x2-…DC/AC	Protective plug PT with protective circuit for one 2-core floating signal circuits; nominal voltages: 5 VDC, 12 VDC, 24 VDC, 12 VAC and 24 VAC; HART compatible. Available with base element directly connected to the mounting or connected via gas discharge tube with the mounting.
PT 4-…DC/AC	Protective plug PT with protective circuit for a 4-core floating signal circuit; nominal voltages: 5 VDC, 12 VDC, 24 VDC and 24 VAC. Available with base element directly connected to the mounting or connected via gas discharge tube with the mounting.
PT 3-…DC	Protective plug PT with protective circuit for two signal wires with common mode voltage coarse and fine protection to ground and additional fine protection between the two signal wires; nominal voltage: 24 VDC. Available with base element directly connected to the mounting.
PT 4-F	Protective plug PT with coarse protection for four signal lines grounded on one side. Available with base element directly connected to the mounting.

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

PT 5-HF-…DC	Surge voltage protection device for normal mode voltage coarse and fine protection for four floating signal wires and ground in IT, common mode voltage coarse protection to ground/earth; nominal voltages: 5 VDC, 12 VDC and 24 VDC. Available with base element directly connected to the mounting or connected via gas discharge tube with the mounting.
PT 3-HF-…DC / PT 3-PB	Surge voltage protection device for normal mode voltage coarse and fine protection for two floating signal wires and ground in IT, common mode voltage coarse protection to ground/earth; nominal voltages: 5 VDC and 12 VDC. Available with base element directly connected to the mounting or connected via gas discharge tube with the mounting.
PT 2-TELE	Surge voltage protection device, consisting of plug and base element, for protecting a double wire from analog and digital telecommunications interfaces (VDSL up to 50 Mbps). Available with base element directly connected to the mounting.

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

Table 2: Summary for PT 2x2-…DC/AC-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	26	26
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**3328 years**	**3328 years**

[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 3: Summary for PT 2x2-…DC/AC-ST and BE+F – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	46	46
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**2102 years**	**2102 years**

[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 4: Summary for PT 1x2-…DC/AC-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	26	26
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**3328 years**	**3328 years**

[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 5: Summary for PT 1x2-…DC/AC-ST and BE+F – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	46	46
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**2102 years**	**2102 years**

[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 6: Summary for PT 4-…DC/AC-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**6.8**	**6.8**
Fail Dangerous Detected ($_{DD}$)	**0**	**12.9**
Fail Dangerous Undetected ($_{DU}$)	**15.6**	**2.7**
No effect	51	51
No part	0	0
Total failure rate (interfering with safety function)	**22.4 FIT**	**22.4 FIT**
MTBF	**1562 years**	**1562 years**

[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 7: Summary for PT 4-…DC/AC-ST and BE+F – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**6.8**	**6.8**
Fail Dangerous Detected ($_{DD}$)	**0**	**12.9**
Fail Dangerous Undetected ($_{DU}$)	**15.6**	**2.7**
No effect	71	71
No part	0	0
Total failure rate (interfering with safety function)	**22.4 FIT**	**22.4 FIT**
MTBF	**1226 years**	**1226 years**

[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 8: Summary for PT 4-F-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.5**	**2.5**
Fail Dangerous Detected ($_{DD}$)	**0**	**1.4**
Fail Dangerous Undetected ($_{DU}$)	**2.4**	**1.0**
No effect	21	21
No part	0	0
Total failure rate (interfering with safety function)	**4.9 FIT**	**4.9 FIT**
MTBF	**4408 years**	**4408 years**

[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 9: Summary for PT 3-…DC-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.1**	**2.1**
Fail Dangerous Detected ($_{DD}$)	**0**	**6.5**
Fail Dangerous Undetected ($_{DU}$)	**8.2**	**1.7**
No effect	25	25
No part	0	0
Total failure rate (interfering with safety function)	**10.3 FIT**	**10.3 FIT**
MTBF	**3271 years**	**3271 years**

[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 10: Summary for PT 3-HF-…DC-ST / PT 3-PB-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	30	30
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**2751 years**	**2751 years**

[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 11: Summary for PT 3-HF-…DC-ST / PT 3-PB-ST and BE+F – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	50	50
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**1856 years**	**1856 years**

[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 12: Summary for PT 5-HF-…DC-ST and BE – 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	30	30
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**2751 years**	**2751 years**

[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 13: Summary for PT 5-HF-…DC-ST and BE+F – Failure rates [35]

	exida Profile 1	
	Analysis 1 [36]	**Analysis 2 [37]**
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	50	50
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**1856 years**	**1856 years**

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

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

[37] 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: Summary for PT 2-TELE-ST and BE – Failure rates [38]

	exida Profile 1	
	Analysis 1 [39]	**Analysis 2 [40]**
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**4.3**
Fail Dangerous Undetected ($_{DU}$)	**8.7**	**4.4**
No effect	37	37
No part	0	0
Total failure rate (interfering with safety function)	**11.4 FIT**	**11.4 FIT**
MTBF	**2363 years**	**2363 years**

The failure rates are valid for the useful life of the surge protective devices PLUGTRAB PT (see Appendix 2).

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

[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.

Table of Contents

Management summary 2
1 Purpose and Scope 18
2 Project management 19
2.1 *exida* 19
2.2 Roles of the parties involved 19
2.3 Standards / Literature used 19
2.4 *exida* tools used 19
2.5 Reference documents 20
2.5.1 Documentation provided by the customer 20
2.5.2 Documentation generated by *exida* 20
3 Description of the analyzed devices 21
4 Failure Modes, Effects, and Diagnostic Analysis 25
4.1 Description of the failure categories 25
4.2 Methodology – FMEDA, Failure rates 26
4.2.1 FMEDA 26
4.2.2 Failure rates 26
4.3 Assumptions 27
4.4 Results 27
4.4.1 PT 2x2-…DC/AC-ST and BE 28
4.4.2 PT 2x2-…DC/AC-ST and BE+F 29
4.4.3 PT 1x2-…DC/AC-ST and BE 30
4.4.4 PT 1x2-…DC/AC-ST and BE+F 31
4.4.5 PT 4-…DC/AC-ST and BE 32
4.4.6 PT 4-…DC/AC-ST and BE+F 33
4.4.7 PT 4-F-ST and BE 34
4.4.8 PT 3-…DC-ST and BE 35
4.4.9 PT 3-HF-…DC-ST / PT 3-PB-ST and BE 36
4.4.10 PT 3-HF-…DC-ST / PT 3-PB-ST and BE+F 37
4.4.11 PT 5-HF-…DC-ST and BE 38
4.4.12 PT 5-HF-…DC-ST and BE+F 39
4.4.13 PT 2-TELE-ST and BE 40
5 Using the FMEDA results 41
5.1 Example PFD_{AVG} / PFH calculation 41
6 Terms and Definitions 42
7 Status of the document 43
7.1 Liability 43
7.2 Releases 43
7.3 Release Signatures 43
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test 44
Appendix 1.1: Proof test to detect dangerous undetected faults 44

Appendix 2: Impact of lifetime of critical components on the failure rate 45
Appendix 3: *exida* Environmental Profiles 46

1 Purpose and Scope

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the surge protective devices PLUGTRAB PT 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 PLUGTRAB PT.

The FMEDA builds the basis for an evaluation whether a sensor or final element subsystem, including the surge protective devices PLUGTRAB PT 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 devices.

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 300 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 PLUGTRAB PT.
exida	Performed the hardware assessment.

PHOENIX CONTACT GmbH & Co. KG contracted *exida* in February 2016 with the extension and update of this report.

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
[N2]	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 V8.0.12	FMEDA Tool
[T2]	exSILentia V3.3.0.906	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	SIL- FMEDA-Bericht PT2x2, PT1x2, PT4, PT3_R02_V01.docx	Safety considerations for PLUGTRAB PT including parts lists and circuit diagrams; 29.03.2016

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_V8_PT 1x2-…DC_AC_V1R0.efm of 09.09.2014
[R2]	FMEDA_V8_PT 1x2-…DC_AC_w_ED_V1R0.efm of 29.09.2014
[R3]	FMEDA_V8_PT 1x2-…DC_AC+F_V1R0.efm of 12.09.2014
[R4]	FMEDA_V8_PT 1x2-…DC_AC+F_w_ED_V1R0.efm of 29.09.2014
[R5]	FMEDA_V8_PT 2x2-…DC_AC_V1R0.efm of 09.09.2014
[R6]	FMEDA_V8_PT 2x2-…DC_AC_w_ED_V1R0.efm of 29.09.2014
[R7]	FMEDA_V8_PT 2x2-…DC_AC+F_V1R0.efm of 12.09.2014
[R8]	FMEDA_V8_PT 2x2-…DC_AC+F_w_ED_V1R0.efm of 29.09.2014
[R9]	FMEDA_V8_PT 3...DC_V1R1.efm of 15.09.2014
[R10]	FMEDA_V8_PT 3...DC_w_ED_V1R1.efm of 29.09.2014
[R11]	FMEDA_V8_PT 4...DC_V1R0.efm of 09.09.2014
[R12]	FMEDA_V8_PT 4...DC_w_ED_V1R0.efm of 29.09.2014
[R13]	FMEDA_V8_PT 4...DC+F_V1R1.efm of 15.09.2014
[R14]	FMEDA_V8_PT 4...DC+F_w_ED_V1R1.efm of 29.09.2014
[R15]	FMEDA_V8_PT 4+F_V1R0.efm of 09.09.2014
[R16]	FMEDA_V8_PT 4+F_w_ED_V1R0.efm of 29.09.2014
[R17]	FMEDA_V8_PT 3HF_PT 3PB_V1R1.efm of 24.03.2016
[R18]	FMEDA_V8_PT 3HF_PT 3PB_w_ED_V1R1.efm of 24.03.2016
[R19]	FMEDA_V8_PT 3HF_PT 3PB+F_V1R1.efm of 24.03.2016
[R20]	FMEDA_V8_PT 3HF_PT 3PB+F_w_ED_V1R1.efm of 24.03.2016
[R21]	FMEDA_V8_PT 5HF_V1R1.efm of 24.03.2016
[R22]	FMEDA_V8_PT 5HF_w_ED_V1R1.efm of 24.03.2016
[R23]	FMEDA_V8_PT 5HF+F_V1R1.efm of 24.03.2016
[R24]	FMEDA_V8_PT 5HF+F_w_ED_V1R1.efm of 24.03.2016
[R25]	FMEDA_V8_PT2-TELE_V1R1.efm of 24.03.2016
[R26]	FMEDA_V8_PT2-TELE_w_ED_V1R1.efm of 24.03.2016

3 Description of the analyzed devices

The FMEDA of the surge protective devices PLUGTRAB PT has been carried out on the parts indicated in Figure 1 to Figure 8.

PT 2x2-…DC/AC is a surge voltage protection device for two separate floating signal circuits. A fine protection element guarantees a low voltage threshold in conjunction with fast response between the corresponding cores. The high surge arresting capacity is achieved by using gas-filled surge voltage arresters from each wire to the common reference potential. PT 2x2…-ST is installed together with the PT 2x2-BE or the PT 2x2+F-BE base element.

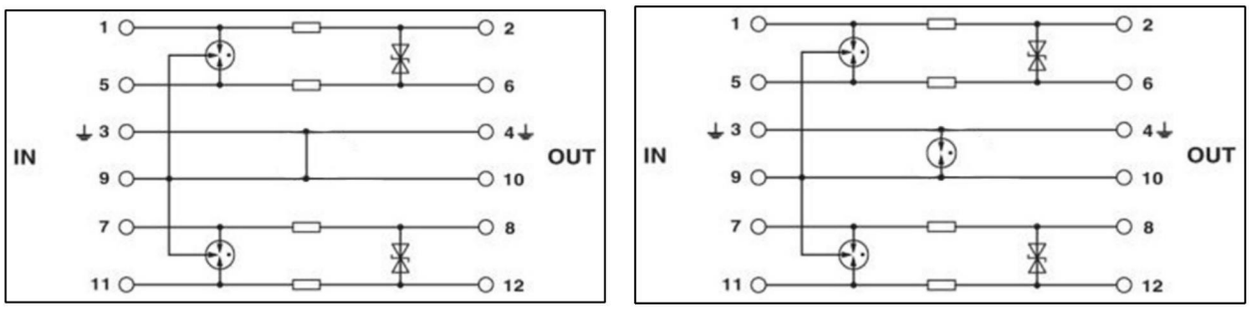


Figure 1: Block diagram of the surge protective device PT 2x2-…DC/AC

PT 1x2-…DC/AC is a surge voltage protection device for one floating signal circuit. A fine protection element guarantees a low voltage threshold in conjunction with fast response between the corresponding cores. The high surge arresting capacity is achieved by using gas-filled surge voltage arresters from each wire to the common reference potential. PT 1x2…-ST is installed together with the PT 1x2-BE or the PT 1x2+F-BE base element.

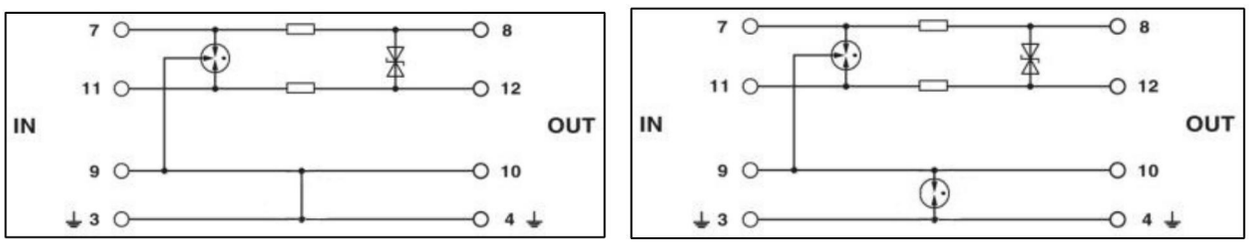


Figure 2: Block diagram of the surge protective device PT 1x2-…DC/AC

PT 4-…DC/AC is a surge voltage protection device for two, three or four-conductor signal circuits. By arranging suppressor diodes between all the signal wires, fine protection between them is achieved together with fast response. The use of gas-filled surge voltage arresters from each wire to the common reference potential guarantees the high surge arresting capacity. PT 4…-ST is installed together with the PT 4-BE or the PT 4+F-BE base element.

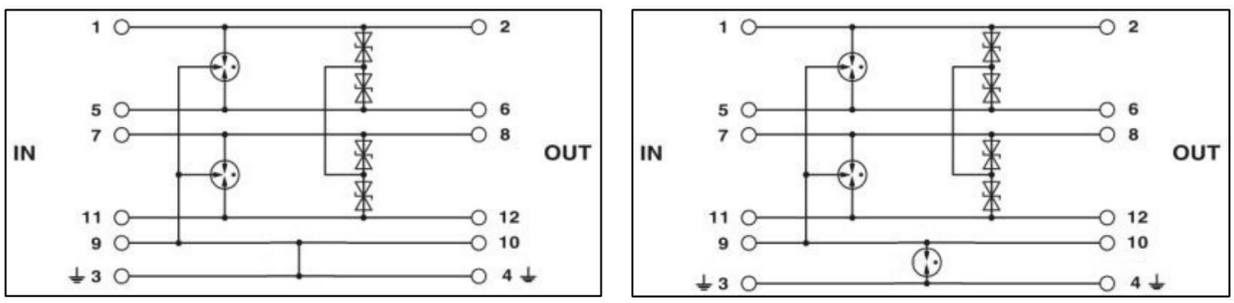


Figure 3: Block diagram of the surge protective device PT 4-…DC/AC

PT 3-HF-…DC and PT 3-PB are surge voltage protection devices for normal mode voltage coarse and fine protection for two floating signal wires and ground in IT, common mode voltage coarse protection to ground/earth. PT 3-HF…-ST and PT 3-PB-ST are installed together with the PT 1x2-BE or the PT 1x2+F-BE base element.

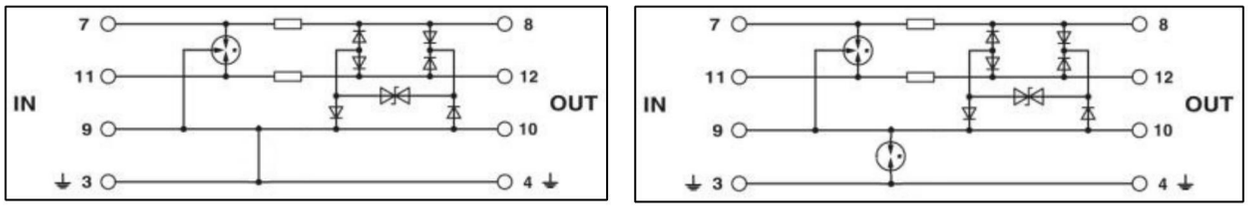


Figure 4: Block diagram of the surge protective device PT 3-HF-…DC and PT 3-PB

PT 5-HF-…DC is a surge voltage protection device for normal mode voltage coarse and fine protection for four floating signal wires and ground in IT, common mode voltage coarse protection to ground/earth.PT 5-HF…-ST is installed together with the PT 2x2-BE or the PT 2x2+F-BE base element.

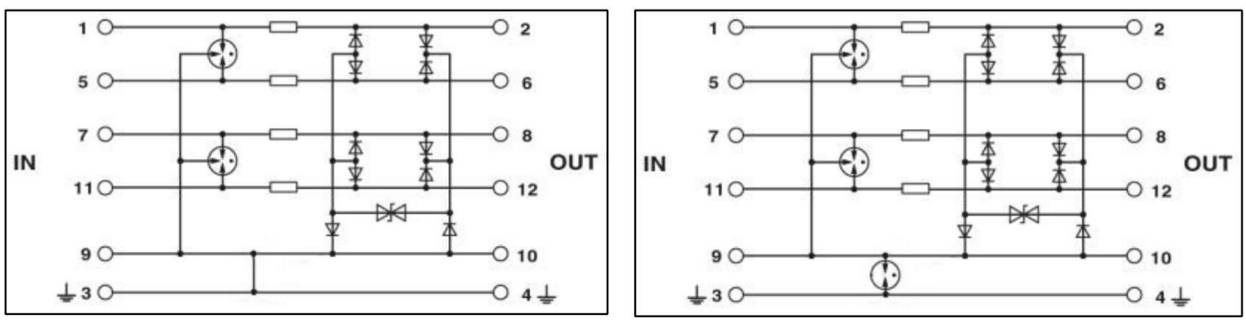


Figure 5: Block diagram of the surge protective device PT 5-HF-…DC

PT 2-TELE is a surge voltage protection device, consisting of plug and base element, for protecting a double wire from analog and digital telecommunications interfaces (VDSL up to 50 Mbps). PT 2-TELE-ST is installed together with the PT 1x2-BE base element.

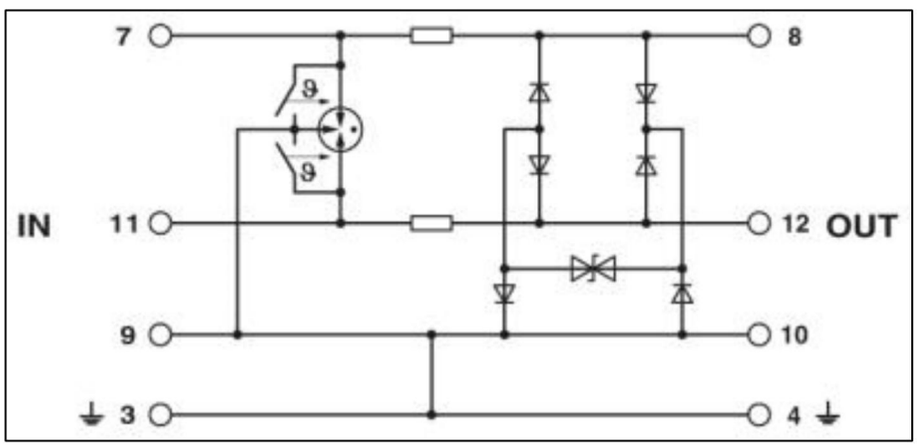


Figure 6: Block diagram of the surge protective device PT 2-TELE

PT 4-F is a surge voltage protection device for four signal wires with common reference potential. The high surge arresting capacity is achieved by using gas-filled surge voltage arresters from each wire to the common reference potential. PT 4-F-ST is installed together with the PT 4-BE base element, which ground the reference potential.

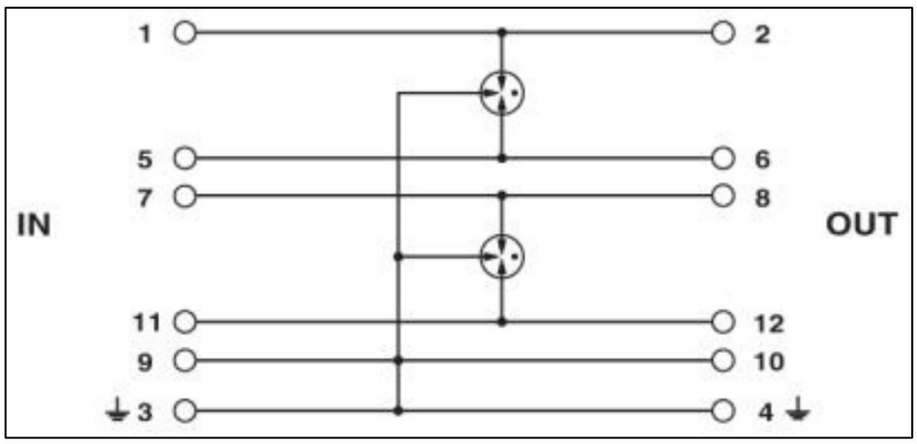


Figure 7: Block diagram of the surge protective device PT 4-F

PT 3-…DC is a surge voltage protection device for two signal wires with common reference potential. Three fine protection elements guarantee a low voltage threshold in conjunction with fast response between the corresponding wires. The high surge arresting capacity is achieved by using gas-filled surge voltage arresters from each wire to the common reference potential. PT 3…-ST is installed together with the PT 3-1R2-BE base element, which ground the reference potential.

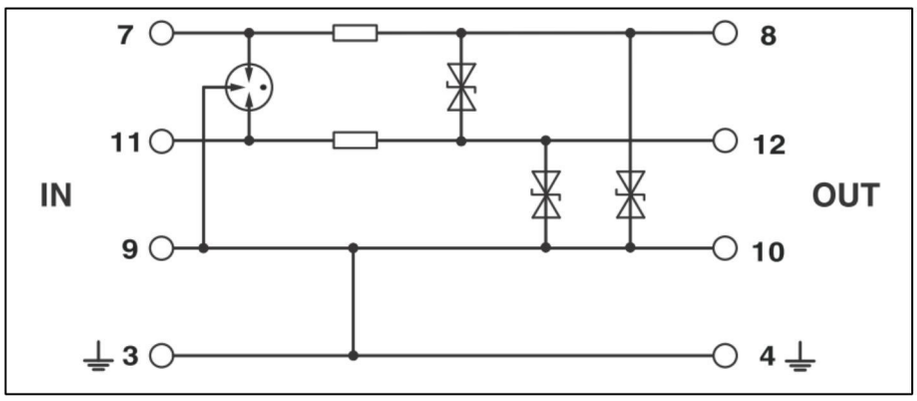


Figure 8: Block diagram of the surge protective device PT 3-…DC

The following two figures Figure 9 and Figure 10 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.

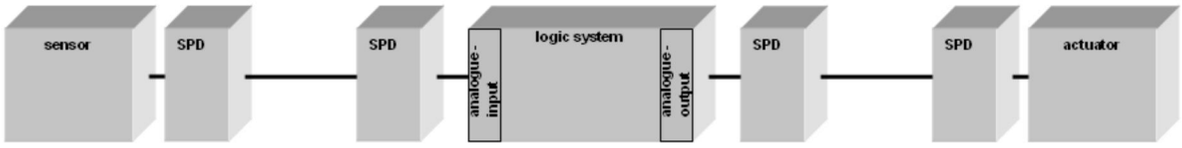


Figure 9: Connection with analog devices

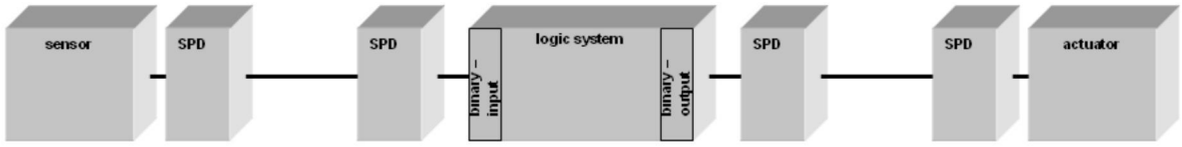


Figure 10: Connection with binary devices

Figure 11 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.

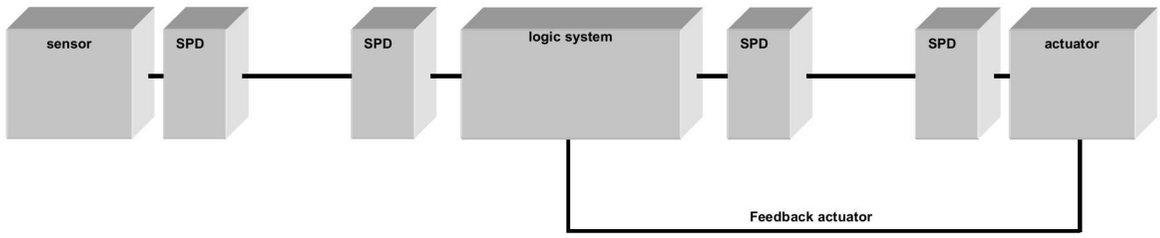


Figure 11: Connection for fault detection

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 [R26]. 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 PLUGTRAB PT, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized or reaching the user defined threshold value or the predefined alarm state.
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 ([N2]) 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 PLUGTRAB PT.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.

4.4 Results

For the calculation the following has to be noted:

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

$_{total} = {}_{SD} + {}_{SU} + {}_{DD} + {}_{DU}$

MTBF = MTTF + MTTR = (1 / ($_{total} + {}_{no\ effect} + {}_{no\ part}$)) + 24 h

4.4.1 PT 2x2-…DC/AC-ST and BE

The FMEDA carried out on the surge protective devices PT 2x2-…DC/AC-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	26	26
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**3328 years**	**3328 years**

[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.

4.4.2 PT 2x2-…DC/AC-ST and BE+F

The FMEDA carried out on the surge protective devices PT 2x2-…DC/AC-ST and BE+F 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	46	46
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**2102 years**	**2102 years**

[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.

4.4.3 PT 1x2-…DC/AC-ST and BE

The FMEDA carried out on the surge protective devices PT 1x2-…DC/AC-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	26	26
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**3328 years**	**3328 years**

[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.

4.4.4 PT 1x2-…DC/AC-ST and BE+F

The FMEDA carried out on the surge protective devices PT 1x2-…DC/AC-ST and BE+F 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**5.8**	**1.9**
No effect	46	46
No part	0	0
Total failure rate (interfering with safety function)	**8.5 FIT**	**8.5 FIT**
MTBF	**2102 years**	**2102 years**

[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.

4.4.5 PT 4-…DC/AC-ST and BE

The FMEDA carried out on the surge protective devices PT 4-…DC/AC-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**6.8**	**6.8**
Fail Dangerous Detected ($_{DD}$)	**0**	**12.9**
Fail Dangerous Undetected ($_{DU}$)	**15.6**	**2.7**
No effect	51	51
No part	0	0
Total failure rate (interfering with safety function)	**22.4 FIT**	**22.4 FIT**
MTBF	**1562 years**	**1562 years**

[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.

4.4.6 PT 4-…DC/AC-ST and BE+F

The FMEDA carried out on the surge protective devices PT 4-…DC/AC-ST and BE+F 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**6.8**	**6.8**
Fail Dangerous Detected ($_{DD}$)	**0**	**12.9**
Fail Dangerous Undetected ($_{DU}$)	**15.6**	**2.7**
No effect	71	71
No part	0	0
Total failure rate (interfering with safety function)	**22.4 FIT**	**22.4 FIT**
MTBF	**1226 years**	**1226 years**

[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.

4.4.7 PT 4-F-ST and BE

The FMEDA carried out on the surge protective devices PT 4-F-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.5**	**2.5**
Fail Dangerous Detected ($_{DD}$)	**0**	**1.4**
Fail Dangerous Undetected ($_{DU}$)	**2.4**	**1.0**
No effect	21	21
No part	0	0
Total failure rate (interfering with safety function)	**4.9 FIT**	**4.9 FIT**
MTBF	**4408 years**	**4408 years**

[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.

4.4.8 PT 3-…DC-ST and BE

The FMEDA carried out on the surge protective devices PT 3-…DC-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.1**	**2.1**
Fail Dangerous Detected ($_{DD}$)	**0**	**6.5**
Fail Dangerous Undetected ($_{DU}$)	**8.2**	**1.7**
No effect	25	25
No part	0	0
Total failure rate (interfering with safety function)	**10.3 FIT**	**10.3 FIT**
MTBF	**3271 years**	**3271 years**

[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.

4.4.9 PT 3-HF-…DC-ST / PT 3-PB-ST and BE

The FMEDA carried out on the surge protective devices PT 3-HF-…DC-ST / PT 3-PB-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	30	30
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**2751 years**	**2751 years**

[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.

4.4.10 PT 3-HF-…DC-ST / PT 3-PB-ST and BE+F

The FMEDA carried out on the surge protective devices PT 3-HF-…DC-ST / PT 3-PB-ST and BE+F 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	50	50
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**1856 years**	**1856 years**

[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.

4.4.11 PT 5-HF-…DC-ST and BE

The FMEDA carried out on the surge protective devices PT 5-HF-…DC-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	30	30
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**2751 years**	**2751 years**

[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.

4.4.12 PT 5-HF-…DC-ST and BE+F

The FMEDA carried out on the surge protective devices PT 5-HF-…DC-ST and BE+F 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**3.9**
Fail Dangerous Undetected ($_{DU}$)	**8.4**	**4.5**
No effect	50	50
No part	0	0
Total failure rate (interfering with safety function)	**11.1 FIT**	**11.1 FIT**
MTBF	**1856 years**	**1856 years**

[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.

4.4.13 PT 2-TELE-ST and BE

The FMEDA carried out on the surge protective devices PT 2-TELE-ST and BE 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 ($_{SD}$)	**0**	**0**
Fail Safe Undetected ($_{SU}$)	**2.7**	**2.7**
Fail Dangerous Detected ($_{DD}$)	**0**	**4.3**
Fail Dangerous Undetected ($_{DU}$)	**8.7**	**4.4**
No effect	37	37
No part	0	0
Total failure rate (interfering with safety function)	**11.4 FIT**	**11.4 FIT**
MTBF	**2363 years**	**2363 years**

[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.

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 PT 3(5)-HF…DC (representing the worst-case of all considered devices) with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in section 4.4.9 to 4.4.12 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 15 lists the results for different proof test intervals considering a proof test coverage of 99% (see Appendix 1.1).

Table 15: PFD_{AVG} / PFH values

T[Proof] = 1 year	T[Proof] = 5 years	PFH
PFD_{AVG} = 2.16E-05	PFD_{AVG} = 9.98E-05	PFH = 4.51E-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 devices are contributing to the entire safety function they should only consume a certain percentage of the allowed range. Assuming 5% of this range as a reasonable budget they 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.

The resulting PFD_{AVG} graph generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 12.

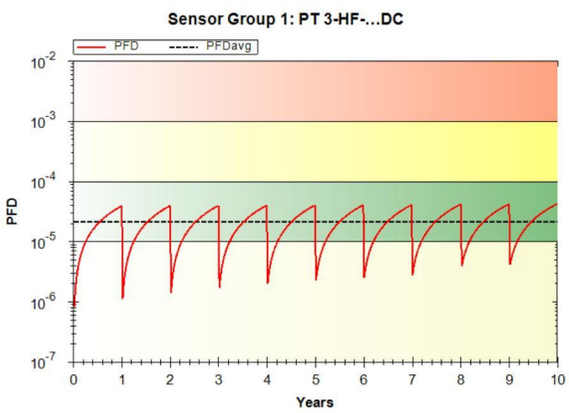


Figure 12: $PFD_{AVG}(t)$

An average Probability of Failure on Demand (PFD_{AVG}) calculation performed for 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 of 2.16E-06 for a one year proof test interval.

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.

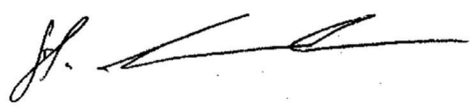
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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.

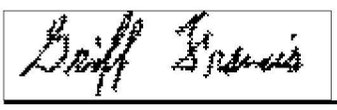
7.2 Releases

Version History:	V2R1:	Editorial changes; March 30, 2016
	V2R0:	Additional devices added; March 30, 2016
	V1R0:	Review comments incorporated; October 28, 2014
	V0R1:	Initial version; October 24, 2014
Author:	Stephan Aschenbrenner	
Review:	V0R1:	Stephan Seggebruch (PHOENIX CONTACT); October 27, 2014
		Griff Francis (*exida*); October 27, 2014
Release status:	Released to PHOENIX CONTACT GmbH & Co. KG	

7.3 Release Signatures



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



Griff Francis, 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 16.

Table 16 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 PLUGTRAB PT 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 PLUGTRAB PT.

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[67] 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 PLUGTRAB PT 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.

[67] 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	30C	25C	25C	5C	25C	25C
Average Internal Temperature	60C	30C	45C	5C	45C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5C	25C	25C	0C	25C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5C	40C	40C	2C	40C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[68]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[69]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[70]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[71]	G2	G3	G3	G3	G3	Compatible Material
Surge[72]						
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[73]						
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)[74]	6kV	6kV	6kV	6kV	6kV	N/A

[68] Humidity rating per IEC 60068-2-3
[69] Shock rating per IEC 60068-2-27
[70] Vibration rating per IEC 60068-2-6
[71] Chemical Corrosion rating per ISA 71.04
[72] Surge rating per IEC 61000-4-5
[73] EMI Susceptibility rating per IEC 6100-4-3
[74] ESD (Air) rating per IEC 61000-4-2