

Failure Modes, Effects and Diagnostic Analysis

Project:
Surge protective devices BLITZDUCTOR® BXT

Customer:

DEHN SE + Co KG
Neumarkt
Germany

Contract No.: DEHN 09/04-20

Report No.: DEHN 09/04-20 R001

Version V5, Revision R1; May 2020

Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights on the format of this technical report reserved.

Management summary

This report summarizes the results of the hardware assessment carried out on the surge protective devices BLITZDUCTOR® BXT in the versions listed in the drawings referenced in section 2.4.1. Table 1 gives an overview of the different configurations that belong to the considered surge protective devices BLITZDUCTOR® BXT.

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.

Table 1: Configuration overview BLITZDUCTOR® BXT

BXT ML4 B 180	4-pole lightning current arrester module with LifeCheck monitoring function. For use in connection with downstream surge arresters -type2P1 or combined lightning current and surge arresters with a lower or equal voltage level; max. continuous operating voltage U_C: 130 VAC / 180 VDC
BXT ML4 BE 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML4 BE 12	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BXT ML4 BE 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML4 BE 36	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 31 VAC / 45 VDC
BXT ML4 BE 48	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BXT ML4 BE 60	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 49.5 VAC / 70 VDC
BXT ML4 BE 180	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BXT ML4 BD 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML4 BD 12	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC

BXT ML4 BD 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML4 BD 48	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BXT ML4 BD 60	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 49.5 VAC / 70 VDC
BXT ML4 BD 180	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BXT ML4 BC 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting max. 4 earth-potential-free single lines with common reference potential; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML4 BC 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting max. 4 earth-potential-free single lines with common reference potential; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML4 BE C 12	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with protective diode circuit at the input, current loops (TTY) and opto-coupler inputs; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BXT ML4 BE C 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs of balanced interfaces with protective diode circuit at the input, current loops (TTY) and opto-coupler inputs; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML4 BE HF 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 4 single lines with common reference potential as well as high-frequency transmissions without electrical isolation; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML4 BD HF 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs in high-frequency bus systems or video transmission systems; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML4 BD HF 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 pairs in high-frequency bus systems or video transmission systems; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML4 MY 250	Surge arrester module with LifeCheck monitoring function for protecting 4 lines of stranded signal interfaces up to 250 VAC; max. continuous operating voltage U_C: 250 VAC / 320 VDC
BXTU ML4 BD 0-180	Combined SPD module with actiVsense and LifeCheck technology for protecting 2 pairs of balanced interfaces which are galvanically isolated. Can be used for all voltages in the range from 0 to 180V. Automatically detects the operating voltage of the wanted signal and optimally adjusts the voltage protection level to the currently applied signal voltage.
BXT ML4 BD EX 24	Surge arrester module with LifeCheck function for protecting 2 pairs in intrinsically safe circuits and bus systems; max. continuous operating voltage U_C: 23 VAC / 33 VDC

BXT ML4 BC EX 24	Surge arrester module with LifeCheck function for protecting up to 4 earth-potential-free single lines with common reference potential in intrinsically safe circuits; max. continuous operating voltage U_C: 23 VAC / 33 VDC
BXT ML2 B 180	2-pole lightning current arrester module with LifeCheck monitoring function and shield earthing for use in nearly all applications. For use in connection with downstream surge arresters type 2P1 or combined lightning current and surge arresters with a lower or equal voltage level; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BXT ML2 BE S 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML2 BE S 12	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BXT ML2 BE S 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML2 BE S 36	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 31 VAC / 45 VDC
BXT ML2 BE S 48	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BXT ML2 BD S 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair of balanced interfaces with electrical isolation, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML2 BD S 12	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair of balanced interfaces with electrical isolation, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BXT ML2 BD S 24	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair of balanced interfaces with electrical isolation, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML2 BD S 48	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair of balanced interfaces with electrical isolation, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BXT ML2 BD 180	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BXT ML2 BE HFS 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair in high-frequency transmissions without electrical isolation; available with direct or indirect shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML2 BD HFS 5	Combined lightning current and surge arrester module with LifeCheck monitoring function for protecting 1 pair in high-frequency bus systems or video transmission systems, available with direct or indirect shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC

BXT ML2 BD DL S 15	LifeCheck-equipped combined SPD module for protecting 1 pair of balanced and galvanically isolated interfaces, which particularly fulfils the requirements of Dupline buses, direct or indirect shield earthing; max. continuous operating voltage U_C: 12 VAC / 17 VDC
BXTU ML2 BD S 0-180	Combined SPD module with actiVsense and LifeCheck technology for protecting 1 pair of balanced interfaces which are galvanically isolated. Direct or indirect shield earthing. For all voltages in the range from 0 to 180V. Automatically detects the operating voltage of the wanted signal and optimally adapts the voltage protection level to the signal voltage currently applied.
BXT ML2 BD HF EX 6	Surge arrester module with LifeCheck monitoring for protecting 1 pair of balanced, high frequency bus systems in intrinsically safe circuits; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BXT ML2 BD S EX 24	Surge arrester module with LifeCheck monitoring for protecting 1 pair of balanced lines in intrinsically safe measuring circuits and bus systems; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BXT ML2 MY E 110	Surge arrester module with LifeCheck monitoring for protecting 1 pair of signal lines; max. continuous operating voltage line-line U_C: 120 VAC / 170 VDC max. continuous operating voltage line-PG U_C: 60 VAC / 85 VDC
BXT ML2 MY 250	Surge arrester module with LifeCheck monitoring for protecting 1 pair of signal lines; max. continuous operating voltage line-line U_C: 500 VAC / 620 VDC max. continuous operating voltage line-PG U_C: 250 VAC / 320 VDC
BXT M2 BD E EX 24	Surge arrester module without LifeCheck monitoring for protecting 1 pair of intrinsically safe measuring circuits and bus systems; max. continuous operating voltage U_C: 25.4 VAC / 36 VDC
BXT M2 BD S EX 24	Surge arrester module without LifeCheck monitoring for protecting 1 pair of intrinsically safe measuring circuits and bus systems; max. continuous operating voltage U_C: 25.4 VAC / 36 VDC
BXT ML4 MY 110	Surge arrester module with LifeCheck monitoring for protecting 2 pairs of signal lines; max. continuous operating voltage line-line U_C: 120 VAC / 170 VDC max. continuous operating voltage line-PG U_C: 60 VAC / 85 VDC
BXT ML4 BPD 24	Surge arrester module with LifeCheck feature for protecting two pairs in 24 VDC systems. Can also be used to protect earthed negative poles. Integrated PTC resistors allow to reliably reset the arrester after the system circuit has been affected by short-circuit currents up to 40 A.
BXT M2 BD HC5A 24 BXT M2 BD HC5A 24 CN	Space-saving combined arrester module for protecting one pair in 24 VDC systems of floating balanced interfaces. Module is adapted to the controller of motor-driven actuators with starting and operating currents up to 5 A.
BXT ML2 MVG 250	Surge arrester module with LifeCheck monitoring function for protecting 2 lines of stranded signal interfaces up to 250 VAC. Leakage-current-free circuit design. max. continuous operating voltage U_C: 250 VAC / 320 VDC

For safety applications only the described configurations were considered. 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 & Mechanical Component Reliability Handbook for Profile 1.

The following tables show how the above stated requirements are fulfilled under worst-case assumptions.

Table 2: BXT ML2 B 180 and BXT ML4 B 180 – Failure rates [1]

	***exida* Profile 1**	
	Analysis 1 [2]	**Analysis 2 [3]**
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**1**
Fail Dangerous Undetected (λ_{DU})	**3**	**2**
No effect	18	18
No part	1	1
Total failure rate (safety function)	**6 FIT**	**6 FIT**
MTBF	**4698 years**	**4698 years**

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

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

[3] 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: BXT ML2(4) BD *, BXT ML2 BD DL S 15, BXT ML2 BD S * – Failure rates

	exida Profile 1	
	Analysis 1 [4]	**Analysis 2** [5]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**6**	**2**
No effect	18	18
No part	1	1
Total failure rate (safety function)	**9 FIT**	**9 FIT**
MTBF	**4182 years**	**4182 years**

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

[5] 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: BXT ML2 BD HF EX 6 – Failure rates

	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**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**1**
Fail Dangerous Undetected (λ_{DU})	**16**	**15**
No effect	26	26
No part	21	21
Total failure rate (safety function)	**18 FIT**	**18 FIT**
MTBF	**1770 years**	**1770 years**

[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 5: BXT ML2 BD HFS 5, BXT ML4 BD HF * – Failure rates

	exida Profile 1	
	Analysis 1 [8]	Analysis 2 [9]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**14**	**10**
No effect	26	26
No part	1	1
Total failure rate (safety function)	**17 FIT**	**17 FIT**
MTBF	**2636 years**	**2636 years**

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

[9] 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: BXT ML2 BE HFS 5, BXT ML4 BE HF 5 – Failure rates

	exida Profile 1	
	Analysis 1 [10]	**Analysis 2** [11]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**8**
Fail Dangerous Undetected (λ_{DU})	**18**	**10**
No effect	30	30
No part	1	1
Total failure rate (safety function)	**21 FIT**	**21 FIT**
MTBF	**2225 years**	**2225 years**

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

[11] 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: BXT ML2 BE S *, BXT ML4 BE *, BXT ML4 BC * – Failure rates

	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})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**7**
Fail Dangerous Undetected (λ_{DU})	**9**	**2**
No effect	18	18
No part	1	1
Total failure rate (safety function)	**12 FIT**	**12 FIT**
MTBF	**3768 years**	**3768 years**

[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 8: BXT ML4 BC EX 24 – Failure rates

	exida Profile 1	
	Analysis 1 [14]	**Analysis 2** [15]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**8**
Fail Dangerous Undetected (λ_{DU})	**11**	**3**
No effect	36	36
No part	1	1
Total failure rate (safety function)	**14 FIT**	**14 FIT**
MTBF	**2269 years**	**2269 years**

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

[15] 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: BXT ML4 BD EX 24, BXT M2 BD E EX 24, BXT M(L)2 BD S EX 24 – Failure rates

	exida Profile 1	
	Analysis 1 [16]	Analysis 2 [17]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**6**
Fail Dangerous Undetected (λ_{DU})	**10**	**4**
No effect	54	54
No part	1	1
Total failure rate (safety function)	**13 FIT**	**13 FIT**
MTBF	**1696 years**	**1696 years**

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

[17] 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: BXT ML4 BE C * – Failure rates**

	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})	**4**	**4**
Fail Dangerous Detected (λ_{DD})	**0**	**9**
Fail Dangerous Undetected (λ_{DU})	**12**	**3**
No effect	19	19
No part	1	1
Total failure rate (safety function)	**16 FIT**	**16 FIT**
MTBF	**3252 years**	**3252 years**

[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 11: BXT ML2(4) MY 250, BXT ML2(4) MY E 110 – Failure rates

	exida Profile 1	
	Analysis 1 [20]	**Analysis 2** [21]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**0.4**
Fail Dangerous Undetected (λ_{DU})	**10**	**9.6**
No effect	18	18
No part	1	1
Total failure rate (safety function)	**12 FIT**	**12 FIT**
MTBF	**3743 years**	**3743 years**

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

[21] 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: BXTU ML2 BD S 0-180 and BXTU ML4 BD 0-180 – Failure rates

	exida Profile 1	
	Analysis 1 [22]	**Analysis 2** [23]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**7**
Fail Dangerous Undetected (λ_{DU})	**42**	**35**
No effect	48	48
No part	20	20
Total failure rate (safety function)	**44 FIT**	**44 FIT**
MTBF	**1026 years**	**1026 years**

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

[23] 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: BXT ML4 BPD 24 – Failure rates

	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})	**8**	**8**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**9**	**5**
No effect	18	18
No part	1	1
Total failure rate (safety function)	**17 FIT**	**17 FIT**
MTBF	**3216 years**	**3216 years**

[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 14: BXT M2 BD HC5A 24 (CN) – Failure rates

	exida Profile 1	
	Analysis 1 [26]	**Analysis 2** [27]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**11**	**7**
No effect	55	55
No part	1	1
Total failure rate (safety function)	**13 FIT**	**13 FIT**
MTBF	**1686 years**	**1686 years**

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

[27] 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 15: BXT ML2 MVG 250 – Failure rates

	exida Profile 1	
	Analysis 1 [28]	**Analysis 2** [29]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**0.4**
Fail Dangerous Undetected (λ_{DU})	**12**	**11.6**
No effect	36	36
No part	1	1
Total failure rate (safety function)	**14 FIT**	**14 FIT**
MTBF	**2261 years**	**2261 years**

The failure rates are valid for the useful life of the surge protective devices BLITZDUCTOR® BXT (see Appendix 2).

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

[29] 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.

Management summary 2
1 Purpose and Scope 21
2 Project management 22
2.1 *exida* 22
2.2 Roles of the parties involved 22
2.3 Standards / Literature used 22
2.4 Reference documents 22
2.4.1 Documentation provided by the customer 22
2.4.2 Documentation generated by *exida* 24
3 Description of the analyzed devices 26
4 Failure Modes, Effects, and Diagnostic Analysis 37
4.1 Description of the failure categories 37
4.2 Methodology – FMEDA, Failure rates 38
4.2.1 FMEDA 38
4.2.2 Failure rates 38
4.3 Assumptions 39
4.4 Results 39
4.4.1 BXT ML2 B 180 and BXT ML4 B 180 40
4.4.2 BXT ML2(4) BD *, BXT ML2 BD DL S 15 and BXT ML2 BD S * 41
4.4.3 BXT ML2 BD HF EX 6 42
4.4.4 BXT ML2 BD HFS 5 and BXT ML4 BD HF * 43
4.4.5 BXT ML2 BE HFS 5 and BXT ML4 BE HF 5 44
4.4.6 BXT ML2 BE S *, BXT ML4 BE * and BXT ML4 BC * 45
4.4.7 BXT ML4 BC EX 24 46
4.4.8 BXT ML4 BD EX 24, BXT M2 BD E EX 24 and BXT M(L)2 BD S EX 24 47
4.4.9 BXT ML4 BE C *** 48
4.4.10 BXT ML2(4) MY 250 and BXT ML2(4) MY E 110 49
4.4.11 BXTU ML2 BD S 0-180 and BXTU ML4 BD 0-180 50
4.4.12 BXT ML4 BPD 24 51
4.4.13 BXT M2 BD HC5A 24 (CN) 52
4.4.14 BXT ML2 MVG 250 53
5 Using the FMEDA results 54
5.1 Example PFD_{AVG} / PFH calculation 54
6 Terms and Definitions 57
7 Status of the document 58
7.1 Liability 58
7.2 Releases 59
7.3 Release Signatures 59
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test 60
Appendix 1.1: Proof test to detect dangerous undetected faults 60
Appendix 2: Impact of lifetime of critical components on the failure rate 61
Appendix 3: *exida* Environmental Profiles 62

1 Purpose and Scope

This document shall describe the results of hardware assessment according to IEC 61508 carried out on the surge protective devices BLITZDUCTOR® BXT in the versions listed in the drawings referenced in section 2.4.1. Table 1 gives an overview of the different configurations that belong to the considered surge protective devices BLITZDUCTOR® BXT.

The FMEDA builds the basis for an evaluation whether a sensor or final element subsystem, including the surge protective devices BLITZDUCTOR® BXT 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, availability, and cybersecurity with over 500-person years of cumulative experience in functional safety, alarm management, and cybersecurity. Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project-oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508.

2.2 Roles of the parties involved

DEHN SE + Co KG	Manufacturer of the surge protective devices BLITZDUCTOR® BXT.
exida	Performed the hardware assessment.

DEHN SE + Co KG contracted *exida* in March 2020 with the update and extension of the FMEDAs for 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
[N2]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	Schaltplaene und Stuecklisten BXT an Exida wg SIL.pdf	Overview of the BXT devices with circuit diagrams and parts lists
[D2]	Technical description LifeCheck.pdf	Description of LifeCheck function Blitzductor CT MLC
[D3]	Explosionszeichnungen BXT BSP.pdf	Circuit diagram "Basisunterteil BXT" 1008562.102 PR01 of 10.08.06 Circuit diagram "Basisunterteil BXT WCO" 1209040.000 PR01 of 13.05.09

[D4]	Schaltbilder Basisteile.pdf	Circuit diagram “Basisteil BXT BAS WECO EX” 920 302 of 27.02.09 Circuit diagram “Basisteil BXT BAS” 920 300 of 27.02.09 Circuit diagram “Basisteil BXT BAS EX” 920 301 of 27.02.09
[D5]	SLP 920226.pdf	Circuit diagram / parts list “Blitzductor BXT ML2 BE S 36” SLP 920 226 of 12.07.11
[D6]	SLP 920280.pdf	Circuit diagram / parts list “Blitzductor BXT ML2 BD S EX 24” SLP 920 280 of 19.07.11
[D7]	SLP 920288.pdf	Circuit diagram / parts list “Blitzductor BXT ML2 MY E 110” SLP 920 288 of 03.04.12
[D8]	SLP 920289.pdf	Circuit diagram / parts list “Blitzductor BXT ML2 MY 250” SLP 920 289 of 24.08.10
[D9]	SLP 920382.pdf	Circuit diagram / parts list “Blitzductor BXT M2 BD E EX 24” SLP 920 382 of 18.08.09
[D10]	SLP 920383.pdf	Circuit diagram / parts list “Blitzductor BXT M2 BD S EX 24” SLP 920 383 of 18.08.09
[D11]	SLP 920388.pdf	Circuit diagram / parts list “Blitzductor BXT ML4 MY 110” SLP 920 388 of 03.04.12
[D12]	920226.pdf	Datasheet “BLITZDUCTOR® BXT ML2 BE S 36”
[D13]	920280.pdf	Datasheet “BLITZDUCTOR® BXT ML2 BD S EX 24”
[D14]	920288.pdf	Datasheet “BLITZDUCTOR® BXT ML2 MY E 110”
[D15]	920289.pdf	Datasheet “BLITZDUCTOR® BXT ML2 MY 250”
[D16]	920382.pdf	Datasheet “BLITZDUCTOR® BXT M2 BD E EX 24”
[D17]	920383.pdf	Datasheet “BLITZDUCTOR® BXT M2 BD S EX 24”
[D18]	920388.pdf	Datasheet “BLITZDUCTOR® BXT ML4 MY 110”
[D19]	920314.pdf	Datasheet “BLITZDUCTOR® BXT ML4 BPD 24
[D20]	Schaltbild_BXT ML4 BPD 24.pdf	Circuit diagram / parts list “Blitzductor BXT ML4 BPD 24” SLP 920 314 of 22.01.15
[D21]	SLP 920297 BXT M2 BD HC5A CN.pdf	Circuit diagram “BXT M2 BD HC5A 24 CN” of 10.02.2016
[D22]	SLP 920290.pdf	Circuit diagram “BXT ML2 MVG 250” SLP 920 290 of 30.10.2019

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.

2.4.2 Documentation generated by *exida*

[R1]	FMEDA_V7_BXT_ML2_B_180_V0R1.efm of 03.08.09
[R2]	FMEDA_V7_BXT_ML2_BD_180_V0R1.efm of 03.08.09
[R3]	FMEDA_V7_BXT_ML2_BD_DL_S_15_V0R1.efm of 03.08.09
[R4]	FMEDA_V7_BXT_ML2_BD_HF_EX_6_V0R1.efm of 03.08.09
[R5]	FMEDA_V7_BXT_ML2_BD_HFS_5_V0R1.efm of 03.08.09
[R6]	FMEDA_V7_BXT_ML2_BD_S_5-12-24-48_V0R1.efm of 03.08.09
[R7]	FMEDA_V7_BXT_ML2_BE_HFS_5_V0R1.efm of 03.08.09
[R8]	FMEDA_V7_BXT_ML2_BE_S_5-12-24-48_V0R1.efm of 03.08.09
[R9]	FMEDA_V7_BXT_ML4_B_180_V0R1.efm of 03.08.09
[R10]	FMEDA_V7_BXT_ML4_BC_5-24_V0R1.efm of 03.08.09
[R11]	FMEDA_V7_BXT_ML4_BC_EX_24_V0R1.efm of 03.08.09
[R12]	FMEDA_V7_BXT_ML4_BD_5-12-24-48-60-180_V0R1.efm of 03.08.09
[R13]	FMEDA_V7_BXT_ML4_BD_EX_24_V0R1.efm of 03.08.09
[R14]	FMEDA_V7_BXT_ML4_BD_HF_5-24_V0R1.efm of 03.08.09
[R15]	FMEDA_V7_BXT_ML4_BE_5-12-24-36-48-60-180_V0R1.efm of 03.08.09
[R16]	FMEDA_V7_BXT_ML4_BE_C_12-24_V0R1.efm of 03.08.09
[R17]	FMEDA_V7_BXT_ML4_BE_HF_5_V0R1.efm of 03.08.09
[R18]	FMEDA_V7_BXT_ML4_MY_250_V0R1.efm of 03.08.09
[R19]	FMEDA_V7_BXTU_ML2_BD_0-180_V0R1.efm of 03.08.09
[R20]	FMEDA_V7_BXTU_ML4_BD_0-180_V0R1.efm of 03.08.09
[R21]	FMEDA_V7_BXT_ML2_B_180_w_ED_V0R1.efm of 12.11.09
[R22]	FMEDA_V7_BXT_ML2_BD_180_w_ED_V0R1.efm of 12.11.09
[R23]	FMEDA_V7_BXT_ML2_BD_DL_S_15_w_ED_V0R1.efm of 12.11.09
[R24]	FMEDA_V7_BXT_ML2_BD_HF_EX_6_w_ED_V0R1.efm of 12.11.09
[R25]	FMEDA_V7_BXT_ML2_BD_HFS_5_w_ED_V0R1.efm of 12.11.09
[R26]	FMEDA_V7_BXT_ML2_BD_S_5-12-24-48_w_ED_V0R1.efm of 12.11.09
[R27]	FMEDA_V7_BXT_ML2_BE_HFS_5_w_ED_V0R1.efm of 12.11.09
[R28]	FMEDA_V7_BXT_ML2_BE_S_5-12-24-48_w_ED_V0R1.efm of 12.11.09
[R29]	FMEDA_V7_BXT_ML4_B_180_w_ED_V0R1.efm of 12.11.09
[R30]	FMEDA_V7_BXT_ML4_BC_5-24_w_ED_V0R1.efm of 12.11.09
[R31]	FMEDA_V7_BXT_ML4_BC_EX_24_w_ED_V0R1.efm of 12.11.09
[R32]	FMEDA_V7_BXT_ML4_BD_5-12-24-48-60-180_w_ED_V0R1.efm of 12.11.09
[R33]	FMEDA_V7_BXT_ML4_BD_EX_24_w_ED_V0R1.efm of 12.11.09
[R34]	FMEDA_V7_BXT_ML4_BD_HF_5-24_w_ED_V0R1.efm of 12.11.09
[R35]	FMEDA_V7_BXT_ML4_BE_5-12-24-36-48-60-180_w_ED_V0R1.efm of 12.11.09
[R36]	FMEDA_V7_BXT_ML4_BE_C_12-24_w_ED_V0R1.efm of 12.11.09

[R37]	FMEDA_V7_BXT_ML4_BE_HF_5_w_ED_V0R1.efm of 12.11.09
[R38]	FMEDA_V7_BXT_ML4_MY_250_w_ED_V0R1.efm of 12.11.09
[R39]	FMEDA_V7_BXTU_ML2_BD_0-180_w_ED_V0R1.efm of 12.11.09
[R40]	FMEDA_V7_BXTU_ML4_BD_0-180_w_ED_V0R1.efm of 12.11.09
[R41]	FMEDA_V8_BXT_M2_BD_E_EX_24_V0R1.efm of 23.04.13
[R42]	FMEDA_V8_BXT_M2_BD_E_EX_24_w_ED_V0R1.efm of 23.04.13
[R43]	FMEDA_V8_BXT_M2_BD_S_EX_24_V0R1.efm of 23.04.13
[R44]	FMEDA_V8_BXT_M2_BD_S_EX_24_w_ED_V0R1.efm of 23.04.13
[R45]	FMEDA_V8_BXT_ML2_BD_S_EX_24_V0R1.efm of 23.04.13
[R46]	FMEDA_V8_BXT_ML2_BD_S_EX_24_w_ED_V0R1.efm of 23.04.13
[R47]	FMEDA_V8_BXT_ML2_BE_S_36_V0R1.efm of 23.04.13
[R48]	FMEDA_V8_BXT_ML2_BE_S_36_w_ED_V0R1.efm of 23.04.13
[R49]	FMEDA_V8_BXT_ML2_MY_250_V0R1.efm of 23.04.13
[R50]	FMEDA_V8_BXT_ML2_MY_250_w_ED_V0R1.efm of 23.04.13
[R51]	FMEDA_V8_BXT_ML2_MY_E_110_V0R1.efm of 23.04.13
[R52]	FMEDA_V8_BXT_ML2_MY_E_110_w_ED_V0R1.efm of 23.04.13
[R53]	FMEDA_V8_BXT_ML4_MY_110_V0R1.efm of 23.04.13
[R54]	FMEDA_V8_BXT_ML4_MY_110_w_ED_V0R1.efm of 23.04.13
[R55]	FMEDA_V8_BXT_ML4_BPD_24_V0R1.efm of 30.09.15
[R56]	FMEDA_V8_BXT_ML4_BPD_24_w_ED_V0R1.efm of 30.09.15
[R57]	FMEDA_V8_BXT_M2_BD_HC5A_24_CN_V0R1.efm of 21.06.2016
[R58]	FMEDA_V8_BXT_M2_BD_HC5A_24_CN_w_ED_V0R1.efm of 21.06.2016
[R59]	FMEDA_V8_BXT_ML2_MVG_250.efm of 14.05.2020
[R60]	FMEDA_V8_BXT_ML2_MVG_250_w_ED.efm of 14.05.2020

3 Description of the analyzed devices

BLITZDUCTOR® BXT are pluggable multi pole universal lightning current and surge arresters for DIN rail mounting in measuring and control circuits, bus systems, alarm systems and telecommunication systems which are subject to maximum availability requirements.

LifeCheck allows quick and easy testing of surge Protective Devices (SPD) without removing the module. Being integrated into the SPD modules, LifeCheck continually monitors the operating state of the SPD. Just like an early warning system, LifeCheck detects potential electrical or thermal overloads on the protection components.

The portable DEHNrecord LC reading device can read out the LifeCheck operating state in a second by means of non-contact RFID technology and shows when the SPD module was tested last time.

The FMEDA of the surge protective devices BLITZDUCTOR® BXT has been carried out on the parts indicated in Figure 1 to Figure 28.

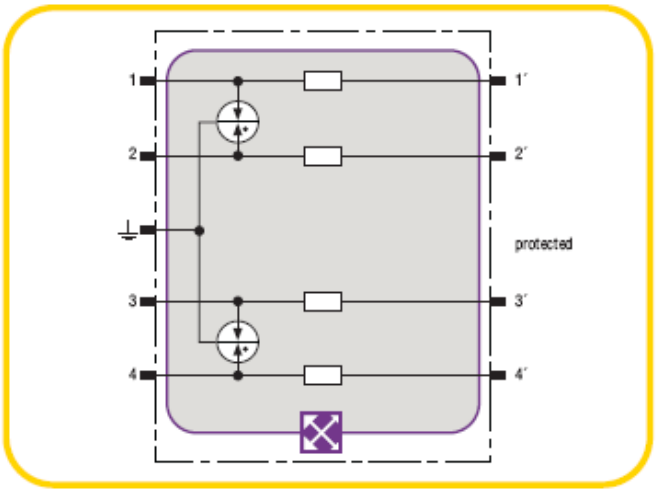


Figure 1: Block diagram of the surge protective device BXT ML4 B *

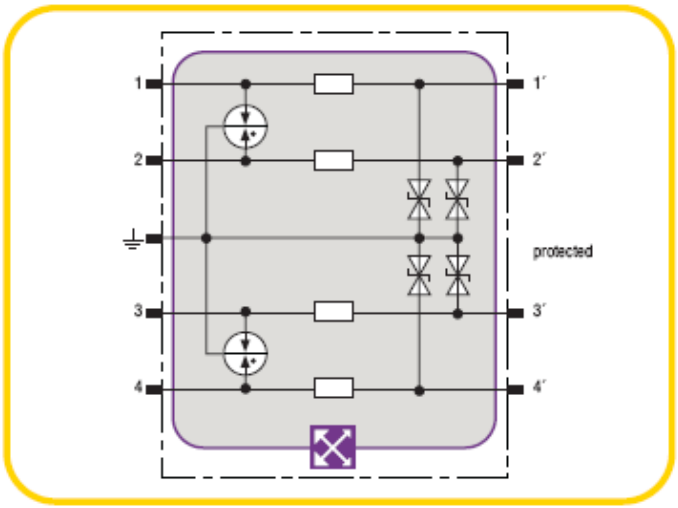


Figure 2: Block diagram of the surge protective device BXT ML4 BE *

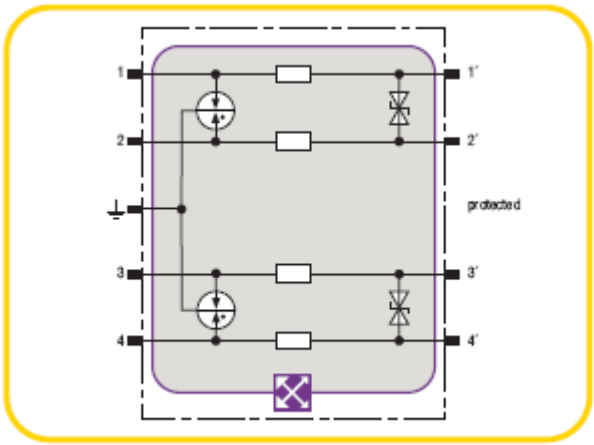


Figure 3: Block diagram of the surge protective device BXT ML4 BD *

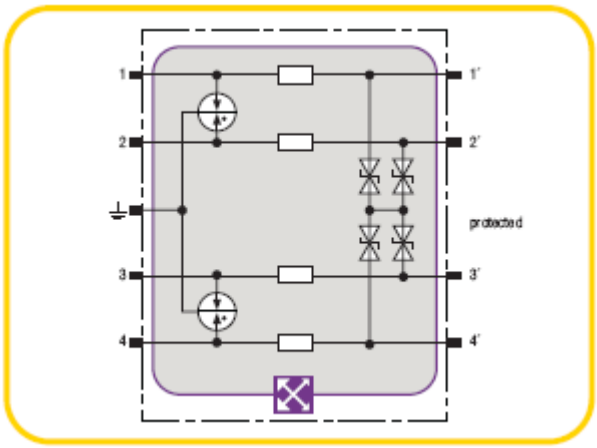


Figure 4: Block diagram of the surge protective device BXT ML4 BC *

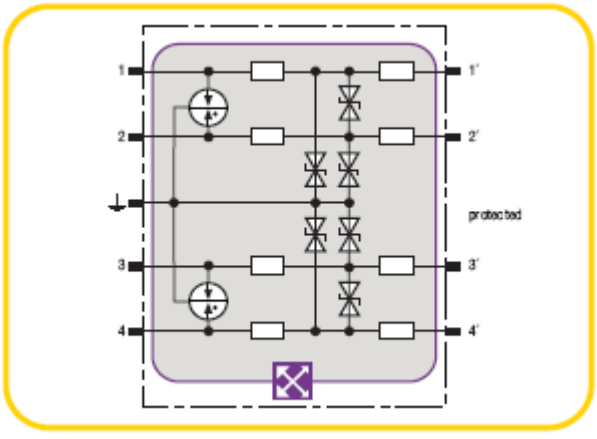


Figure 5: Block diagram of the surge protective device BXT ML4 BE C *

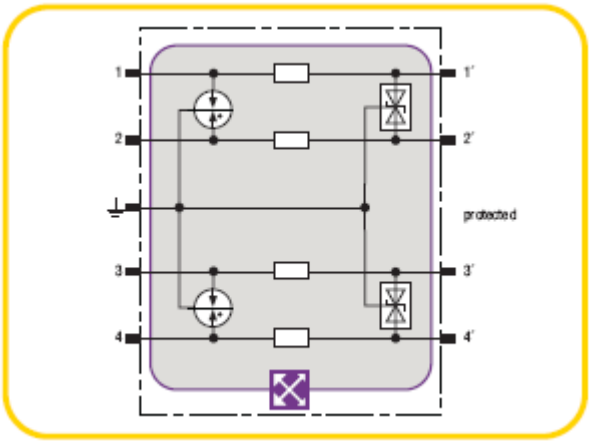


Figure 6: Block diagram of the surge protective device BXT ML4 BE HF **

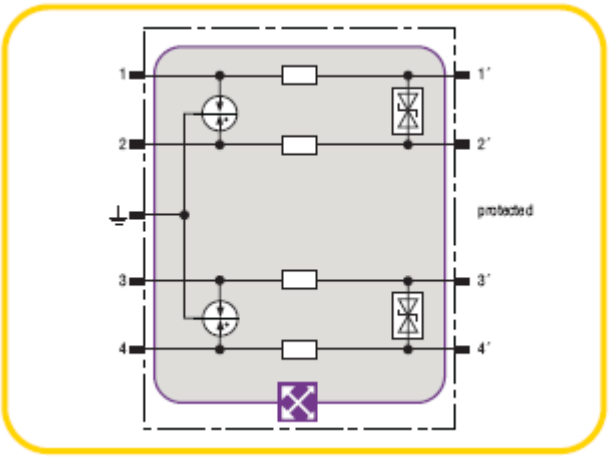


Figure 7: Block diagram of the surge protective device BXT ML4 BD HF **

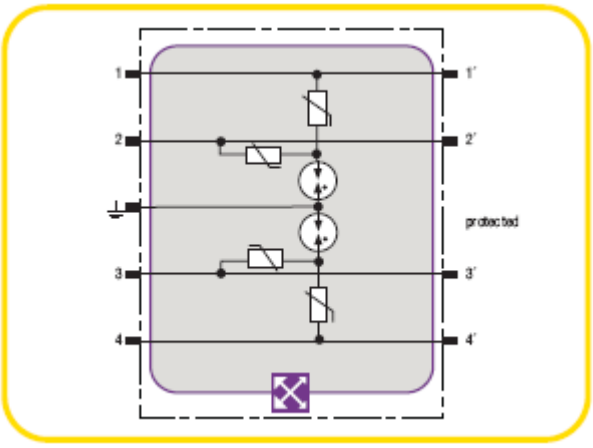


Figure 8: Block diagram of the surge protective device BXT ML4 MY 250

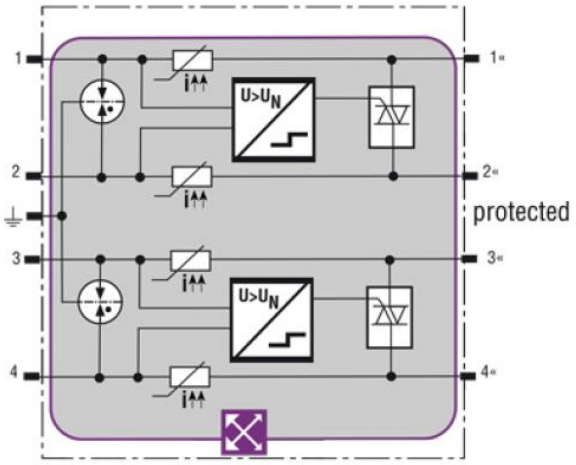


Figure 9: Block diagram of the surge protective device BXTU ML4 BD 0-180

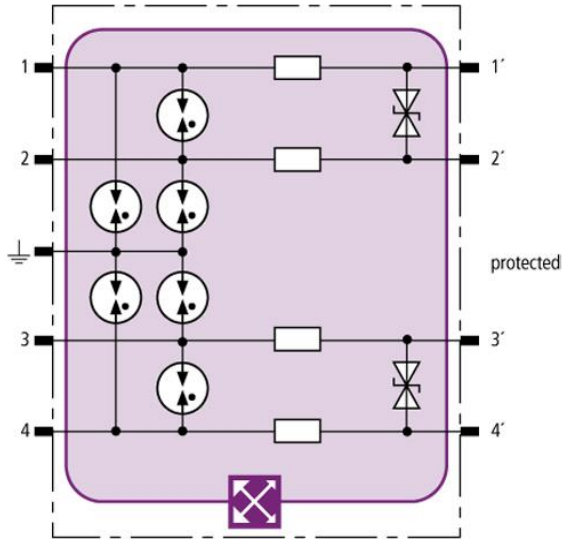


Figure 10: Block diagram of the surge protective device BXT ML4 BD EX 24

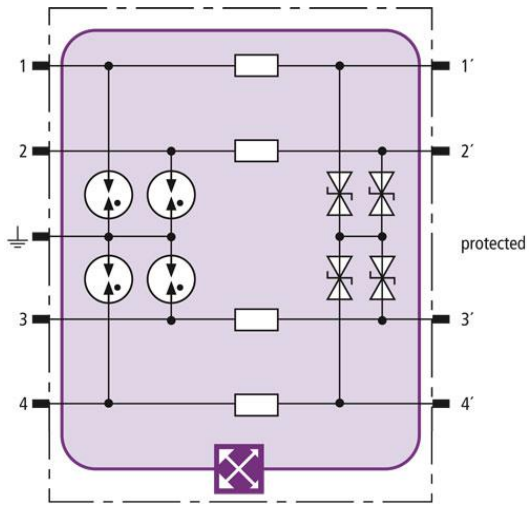


Figure 11: Block diagram of the surge protective device BXT ML4 BC EX 24

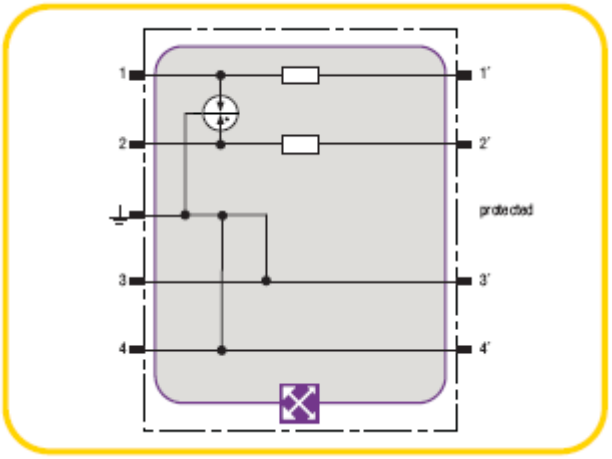


Figure 12: Block diagram of the surge protective device BXT ML2 B *

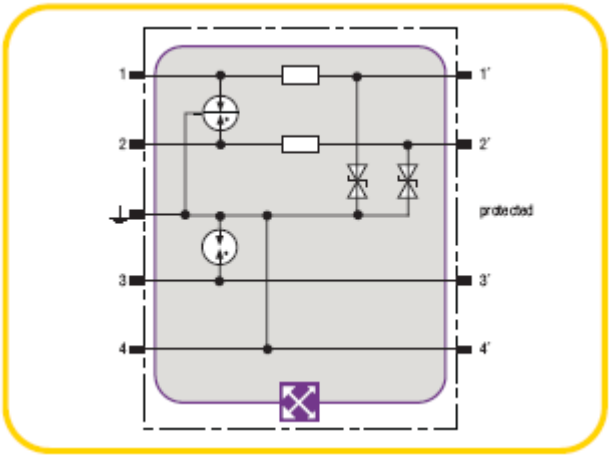


Figure 13: Block diagram of the surge protective device BXT ML2 BE S *

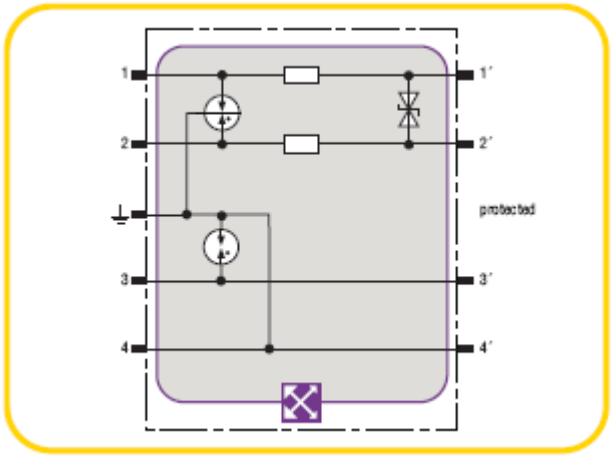


Figure 14: Block diagram of the surge protective device BXT ML2 BD S *

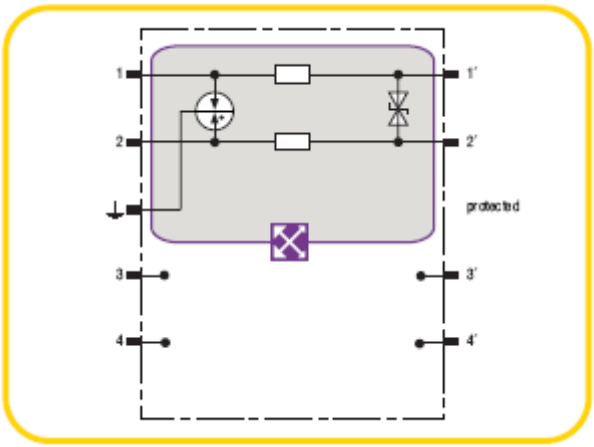


Figure 15: Block diagram of the surge protective device BXT ML2 BD 180

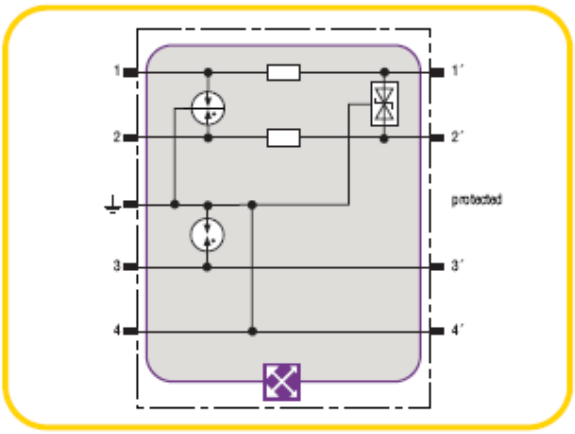


Figure 16: Block diagram of the surge protective device BXT ML2 BE HFS 5

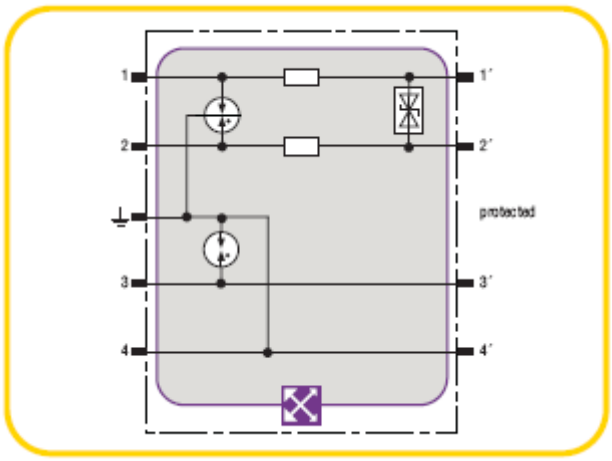


Figure 17: Block diagram of the surge protective device BXT ML2 BD HFS 5

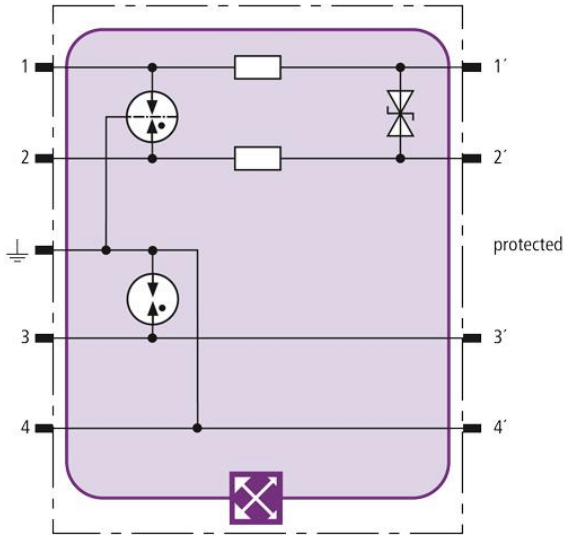


Figure 18: Block diagram of the surge protective device BXT ML2 BD DL S 15

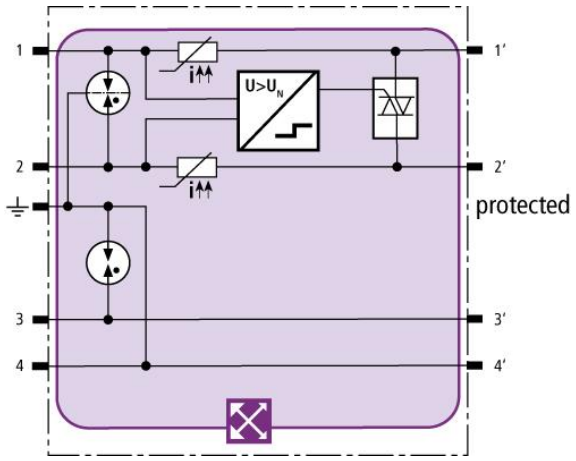


Figure 19: Block diagram of the surge protective device BXTU ML2 BD S 0-180

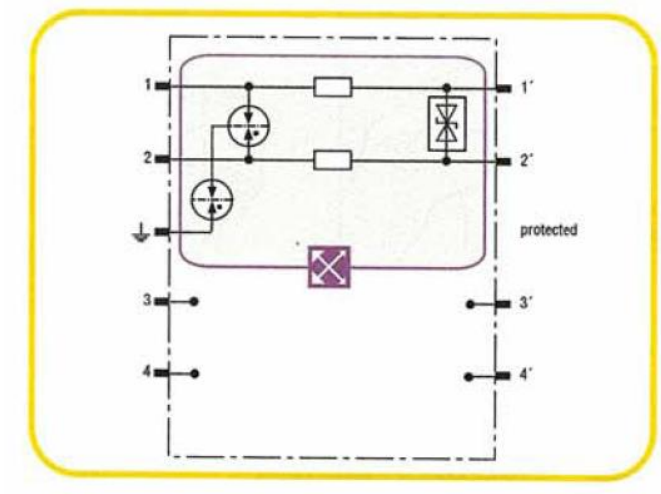


Figure 20: Block diagram of the surge protective device BXT ML2 BD HF EX 6

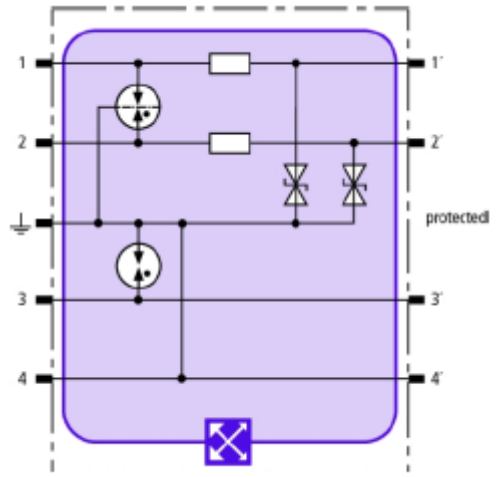


Figure 21: Block diagram of the surge protective device BXT ML2 BE S 36

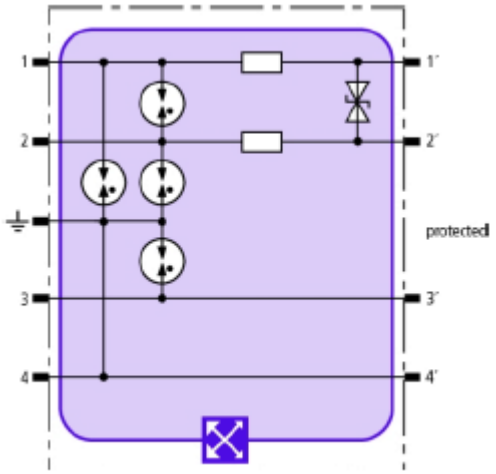


Figure 22: Block diagram of the surge protective device BXT ML2 BD S EX 24

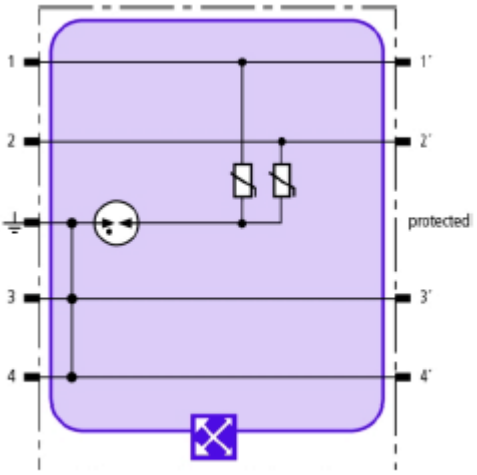


Figure 23: Block diagram of the surge protective device BXT ML2 MY E 110

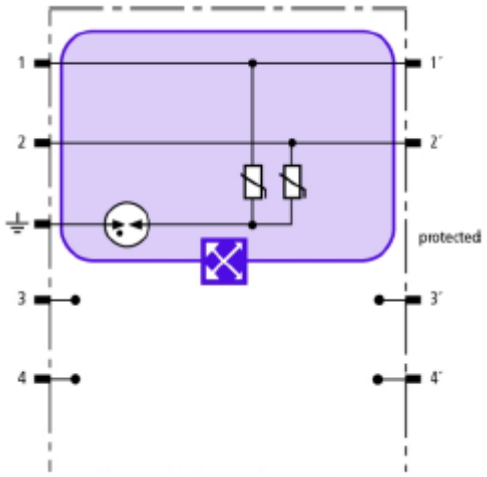


Figure 24: Block diagram of the surge protective device BXT ML2 MY 250

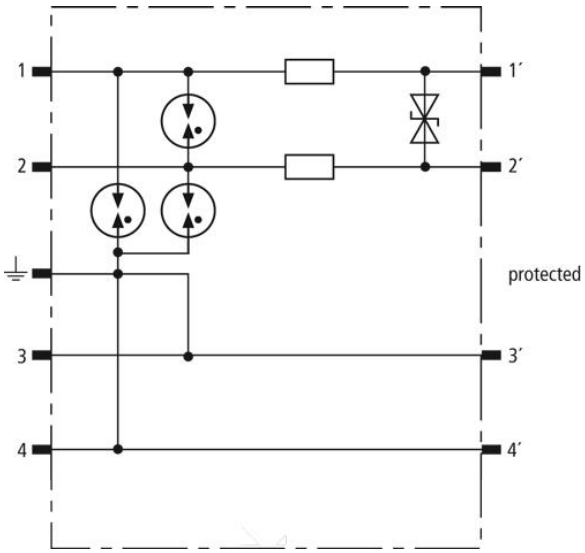


Figure 25: Block diagram of the surge protective device BXT M2 BD E EX 24

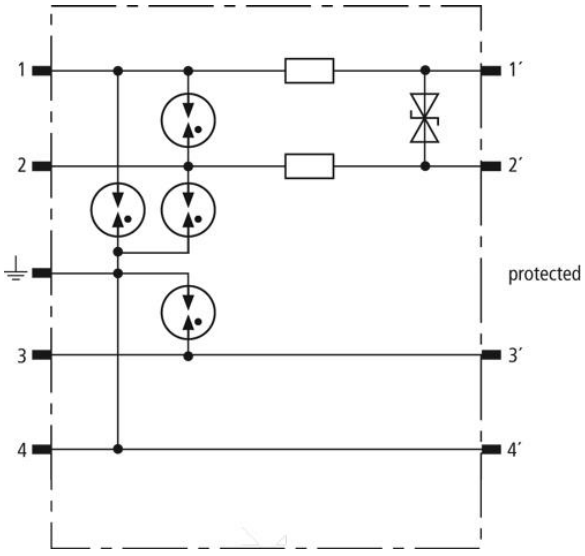


Figure 26: Block diagram of the surge protective device BXT M2 BD S EX 24

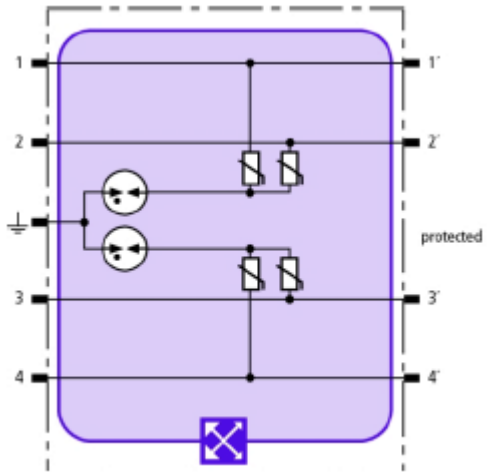


Figure 27: Block diagram of the surge protective device BXT ML4 MY 110

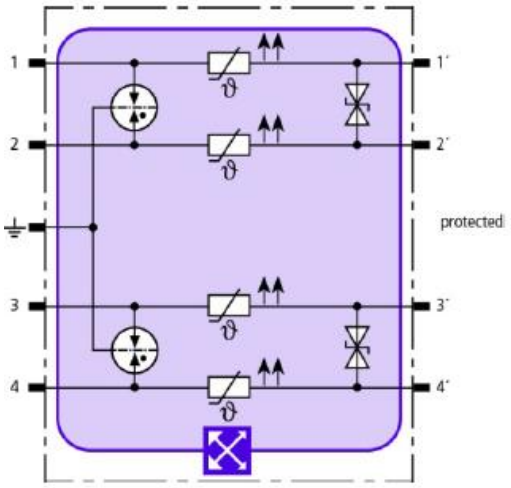


Figure 28: Block diagram of the surge protective device BXT ML4 BPD 24

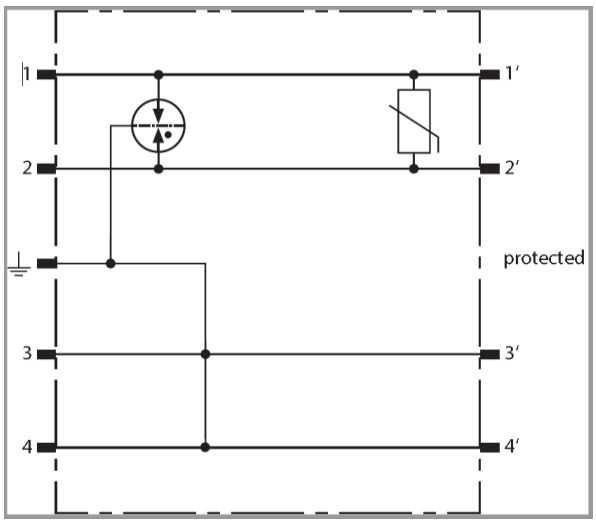


Figure 29: Block diagram of the surge protective device BXT M2 BD HC5A 24 (CN)

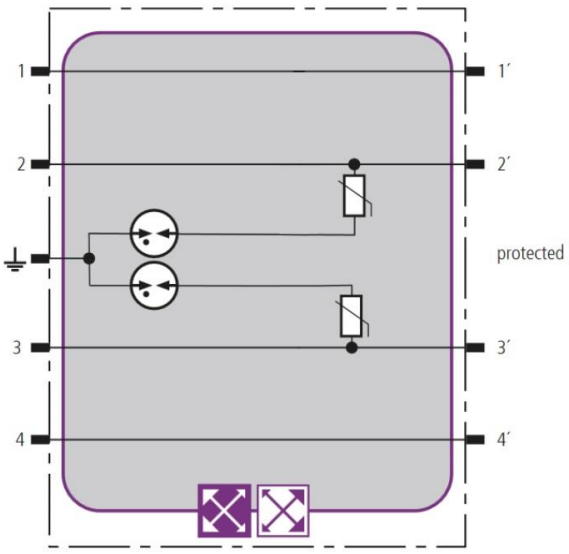


Figure 30: Block diagram of the surge protective device BXT ML2 MVG 250

The following Figure 31 shows how the surge protective devices can be connected to other devices. All considered surge protective devices can be used with analog or binary devices.

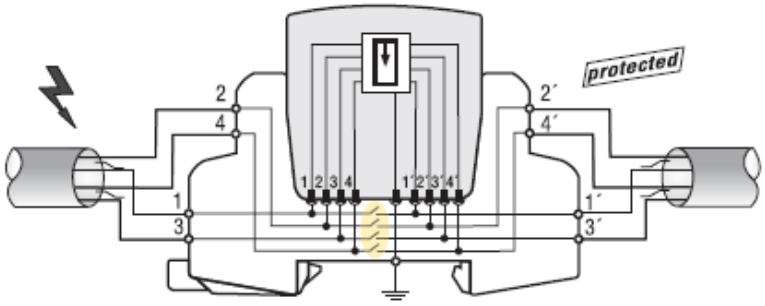


Figure 31: Connection diagram

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with DEHN SE + Co KG and is documented in [R1] to [R60]. 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 BLITZDUCTOR® BXT, 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 (when used with binary devices) or reaching the user defined threshold value (when used with analog devices).
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 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 and Mechanical 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 BLITZDUCTOR® BXT.

- 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.
- Complete practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA.
- 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.
- All modules are operated in the low demand mode of operation.
- The LifeCheck function is not part of the safety function and therefore not considered in this analysis.

4.4 Results

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

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

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

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

4.4.1 BXT ML2 B 180 and BXT ML4 B 180

The FMEDA carried out on the surge protective devices BXT ML2 B 180 and BXT ML4 B 180 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***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})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**1**
Fail Dangerous Undetected (λ_{DU})	**3**	**2**

No effect	18	18
No part	1	1

Total failure rate (safety function)	**6 FIT**	**6 FIT**

MTBF	**4698 years**	**4698 years**

[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.

4.4.2 BXT ML2(4) BD *, BXT ML2 BD DL S 15 and BXT ML2 BD S *

The FMEDA carried out on the surge protective devices BXT ML2(4) BD *, BXT ML2 BD DL S 15 and BXT ML2 BD S * leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [32]	**Analysis 2** [33]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**6**	**2**

No effect	18	18
No part	1	1

Total failure rate (safety function)	**9 FIT**	**9 FIT**

MTBF	**4182 years**	**4182 years**

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

[33] 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 BXT ML2 BD HF EX 6

The FMEDA carried out on the surge protective device BXT ML2 BD HF EX 6 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	exida Profile 1	
	Analysis 1 [34]	**Analysis 2** [35]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**1**
Fail Dangerous Undetected (λ_{DU})	**16**	**15**
No effect	26	26
No part	21	21
Total failure rate (safety function)	**18 FIT**	**18 FIT**
MTBF	**1770 years**	**1770 years**

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

[35] 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 BXT ML2 BD HFS 5 and BXT ML4 BD HF *

The FMEDA carried out on the surge protective devices BXT ML2 BD HFS 5 and BXT ML4 BD HF * leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [36]	**Analysis 2** [37]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**14**	**10**
No effect	26	26
No part	1	1
Total failure rate (safety function)	**17 FIT**	**17 FIT**
MTBF	**2636 years**	**2636 years**

[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.

4.4.5 BXT ML2 BE HFS 5 and BXT ML4 BE HF 5

The FMEDA carried out on the surge protective devices BXT ML2 BE HFS 5 and BXT ML4 BE HF 5 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [38]	**Analysis 2** [39]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**8**
Fail Dangerous Undetected (λ_{DU})	**18**	**10**
No effect	30	30
No part	1	1
Total failure rate (safety function)	**21 FIT**	**21 FIT**
MTBF	**2225 years**	**2225 years**

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

[39] 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 BXT ML2 BE S *, BXT ML4 BE * and BXT ML4 BC *

The FMEDA carried out on the surge protective devices BXT ML2 BE S *, BXT ML4 BE * and BXT ML4 BC * leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [40]	**Analysis 2** [41]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**7**
Fail Dangerous Undetected (λ_{DU})	**9**	**2**

No effect	19	19
No part	1	1

Total failure rate (safety function)	**12 FIT**	**12 FIT**

MTBF	**3768 years**	**3768 years**

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

[41] 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 BXT ML4 BC EX 24

The FMEDA carried out on the surge protective device BXT ML4 BC EX 24 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [42]	**Analysis 2** [43]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**8**
Fail Dangerous Undetected (λ_{DU})	**11**	**3**

No effect	36	36
No part	1	1

Total failure rate (safety function)	**14 FIT**	**14 FIT**

MTBF	**2269 years**	**2269 years**

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

[43] 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 BXT ML4 BD EX 24, BXT M2 BD E EX 24 and BXT M(L)2 BD S EX 24

The FMEDA carried out on the surge protective device BXT ML4 BD EX 24, BXT M2 BD E EX 24, BXT M2 BD S EX 24 and BXT ML2 BD S EX 24 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [44]	**Analysis 2** [45]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**3**	**3**
Fail Dangerous Detected (λ_{DD})	**0**	**6**
Fail Dangerous Undetected (λ_{DU})	**10**	**4**
No effect	54	54
No part	1	1
Total failure rate (safety function)	**13 FIT**	**13 FIT**
MTBF	**1696 years**	**1696 years**

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

[45] 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 BXT ML4 BE C ***

The FMEDA carried out on the surge protective devices BXT ML4 BE C *** leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	exida Profile 1	
	Analysis 1 [46]	**Analysis 2** [47]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**4**	**4**
Fail Dangerous Detected (λ_{DD})	**0**	**9**
Fail Dangerous Undetected (λ_{DU})	**12**	**3**
No effect	19	19
No part	1	1
Total failure rate (safety function)	**16 FIT**	**16 FIT**
MTBF	**3252 years**	**3252 years**

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

[47] 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 BXT ML2(4) MY 250 and BXT ML2(4) MY E 110

The FMEDA carried out on the surge protective device BXT ML4 MY 250, BXT ML2 MY 250, BXT ML2 MY E 110 and BXT ML4 MY 110 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [48]	**Analysis 2** [49]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**0.4**
Fail Dangerous Undetected (λ_{DU})	**10**	**9.6**

No effect	18	18
No part	1	1

Total failure rate (safety function)	**12 FIT**	**12 FIT**

MTBF	**3743 years**	**3743 years**

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

[49] 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 BXTU ML2 BD S 0-180 and BXTU ML4 BD 0-180

The FMEDA carried out on the surge protective devices BXTU ML2 BD S 0-180 and BXTU ML4 BD 0-180 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	exida Profile 1	
	Analysis 1 [50]	**Analysis 2** [51]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**7**
Fail Dangerous Undetected (λ_{DU})	**42**	**35**
No effect	48	48
No part	20	20
Total failure rate (safety function)	**44 FIT**	**44 FIT**
MTBF	**1026 years**	**1026 years**

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

[51] 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 BXT ML4 BPD 24

The FMEDA carried out on the surge protective devices BXT ML4 BPD 24 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	exida Profile 1	
	Analysis 1 [52]	**Analysis 2** [53]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**8**	**8**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**9**	**5**

No effect	18	18
No part	1	1

Total failure rate (safety function)	**17 FIT**	**17 FIT**

MTBF	**3216 years**	**3216 years**

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

[53] 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 BXT M2 BD HC5A 24 (CN)

The FMEDA carried out on the surge protective devices BXT M2 BD HC5A 24 (CN) leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	exida Profile 1	
	Analysis 1 [54]	**Analysis 2** [55]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail Dangerous Undetected (λ_{DU})	**11**	**7**
No effect	55	55
No part	1	1
Total failure rate (safety function)	**13 FIT**	**13 FIT**
MTBF	**1686 years**	**1686 years**

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

[55] 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 BXT ML2 MVG 250

The FMEDA carried out on the surge protective devices BXT ML2 MVG 250 leads under the assumptions described in sections 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

	***exida* Profile 1**	
	Analysis 1 [56]	**Analysis 2** [57]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**2**	**2**
Fail Dangerous Detected (λ_{DD})	**0**	**0.4**
Fail Dangerous Undetected (λ_{DU})	**12**	**11.6**
No effect	36	36
No part	1	1
Total failure rate (safety function)	**14 FIT**	**14 FIT**
MTBF	**2261 years**	**2261 years**

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

[57] 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} / PFH values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

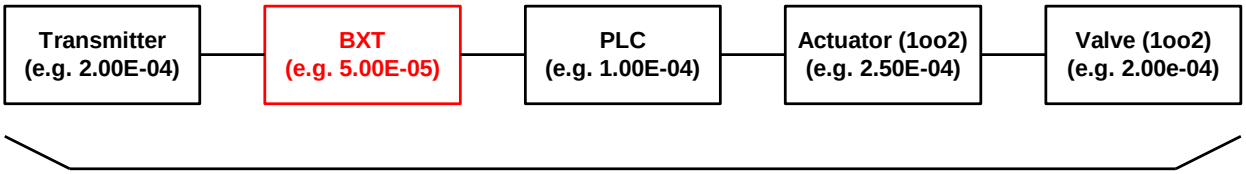
An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) surge protective device with *exida's* exSILentia tool. The failure rate data used in this calculation are displayed in sections 4.4.1 to 4.4.14 for analysis 2. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%.

Table 16 and Table 17 list the results of all devices considering a proof test coverage of 99% (see Appendix 1.1) for the PFD_{AVG} calculation.

For SIL2 the overall PFD_{AVG} shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 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-04 or 5.00E-08 1/h, respectively for SIL2 and better than or equal to 5.00E-05 or 5.00E-09 1/h, respectively for SIL3. Figure 32 illustrates this on an example.



SIL2: PFD_{AVG} < 1.00E-02

SIL3: PFD_{AVG} < 1.00E-03

Example: PFD_{AVG} = 8.00E-04 < 1.00E-03

Figure 32: SIF example

Table 16 and Table 17 show that the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 / SIL 3 according to table 2 of IEC 61508-1 and their contribution to the SIL budget. Most of the devices fulfill the assumption to not claim more than 5% of the allowed range.

Table 16: PFD_{AVG}

Type	T[Proof] = 1 year	Percentage of SIL2	Percentage of SIL3
BXT ML2 B 180 ML4 B 180	PFD_{AVG} = 8.31E-06	≈ 0.1%	≈ 1%
BXT ML2(4) BD * BXT ML2 BD DL S 15 BXT ML2 BD S *	PFD_{AVG} = 9.21E-06	≈ 0.1%	≈ 1%
BXT ML2 BD HF EX 6	PFD_{AVG} = 6.88E-05	≈ 0.7%	≈ 7%
BXT ML2 BD HFS 5 BXT ML4 BD HF *	PFD_{AVG} = 4.74E-05	≈ 0.5%	≈ 5%
BXT ML2 BE HFS 5 BXT ML4 BE HF 5	PFD_{AVG} = 4.77E-05	≈ 0.5%	≈ 5%
BXT ML2 BE S * BXT ML4 BE * BXT ML4 BC *	PFD_{AVG} = 1.01E-05	≈ 0.1%	≈ 1%
BXT ML4 BC EX 24	PFD_{AVG} = 1.50E-05	≈ 0.2%	≈ 2%
BXT ML4 BD EX 24 BXT M2 BD E EX 24 BXT M(L)2 BD S EX 24	PFD_{AVG} = 1.89E-05	≈ 0.2%	≈ 2%
BXT ML4 BE C ***	PFD_{AVG} = 1.44E-05	≈ 0.1%	≈ 1%
BXT ML2(4) MY 250 BXT ML2(4) MY E 110	PFD_{AVG} = 4.59E-05	≈ 0.5%	≈ 5%
BXTU ML2 BD S 0-180 BXTU ML4 BD 0-180	PFD_{AVG} = 1.65E-04	≈ 1.7%	≈ 17%
BXT ML4 BPD 24	PFD_{AVG} = 2.48E-05	≈ 0.2%	≈ 2%
BXT M2 BD HC5A 24 BXT M2 BD HC5A 24 CN	PFD_{AVG} = 3.08E-05	≈ 0.3%	≈ 3%
BXT ML2 MVG 250	PFD_{AVG} = 5.53E-05	≈ 0.6%	≈ 6%

Table 17: PFH values

Type	PFH	Percentage of SIL2	Percentage of SIL3
BXT ML2 B 180 ML4 B 180	PFH = 1.73E-09 1/h	≈ 0.2%	≈ 2%
BXT ML2(4) BD * BXT ML2 BD DL S 15 BXT ML2 BD S *	PFH = 1.91E-09 1/h	≈ 0.2%	≈ 2%
BXT ML2 BD HF EX 6	PFH = 1.44E-08 1/h	≈ 1.4%	≈ 14%
BXT ML2 BD HFS 5 BXT ML4 BD HF *	PFH = 9.91E-09 1/h	≈ 1.0%	≈ 10%
BXT ML2 BE HFS 5 BXT ML4 BE HF 5	PFH = 9.95E-09 1/h	≈ 1.0%	≈ 10%
BXT ML2 BE S * BXT ML4 BE * BXT ML4 BC *	PFH = 2.09E-09 1/h	≈ 0.2%	≈ 2%
BXT ML4 BC EX 24	PFH = 3.10E-09 1/h	≈ 0.3%	≈ 3%
BXT ML4 BD EX 24 BXT M2 BD E EX 24 BXT M(L)2 BD S EX 24	PFH = 3.93E-09 1/h	≈ 0.4%	≈ 4%
BXT ML4 BE C ***	PFH = 2.89E-09 1/h	≈ 0.3%	≈ 3%
BXT ML2(4) MY 250 BXT ML2(4) MY E 110	PFH = 9.60E-09 1/h	≈ 1.0%	≈ 10%
BXTU ML2 BD S 0-180 BXTU ML4 BD 0-180	PFH = 3.44E-08 1/h	≈ 3.4%	≈ 34%
BXT ML4 BPD 24	PFH = 5.19E-09 1/h	≈ 0.5%	≈ 5%
BXT M2 BD HC5A 24 BXT M2 BD HC5A 24 CN	PFH = 6.44E-09 1/h	≈ 0.6%	≈ 6%
BXT ML2 MVG 250	PFH = 1.16E-08 1/h	≈ 1.2%	≈ 12%

The resulting PFD_{AVG} graph for a single (1oo1) surge protective device BXTU ML2 BD S 0-180 and BXTU ML4 BD 0-180 (representing the worst-case of all considered devices) generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 33.

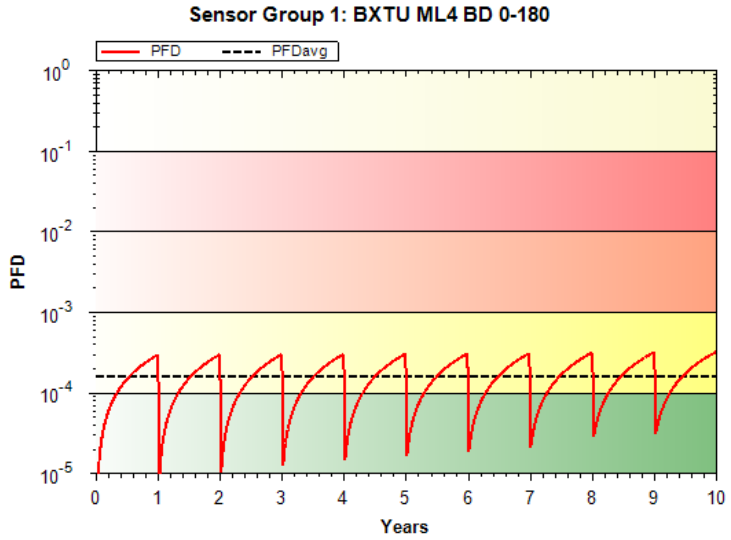


Figure 33: $PFD_{AVG}(t)$

6 Terms and Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
High demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
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
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.

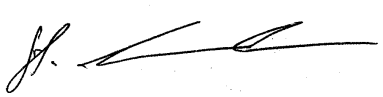
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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:	V5R1:	Device BXT ML2 MVG 250 added; May 14, 2020
	V5R0:	Device BXT M2 BD HC5A 24 (CN) added; June 29, 2016
	V4R0:	Device BXT ML4 BPD 24 added; October 5, 2015
	V3R0:	Devices added and report updated to IEC 61508:2010 (2nd edition); September 23, 2013
	V2R1:	Naming corrected; November 18, 2009
	V2R0:	Additional analysis included; November 13, 2009
	V1R0:	Review comments incorporated and report split into R001 and R002; October 12, 2009
	V0R1:	Initial version; September 25, 2009
Author:	Stephan Aschenbrenner	
Review:	V2R0:	Thomas J. Weiß (DEHN); November 17, 2009
	V0R1:	Rachel Amkreutz (*exida*); September 28, 2009
		Josef Birkl (DEHN); October 10, 2009
Release status:	Released to DEHN SE + Co KG	

7.3 Release Signatures



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



Rachel Amkreutz, 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 18.

Table 18 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 BLITZDUCTOR® BXT to reach predefined output signals 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 BLITZDUCTOR® BXT.

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[58] 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 BLITZDUCTOR® BXT 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.

[58] 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[59]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[60]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[61]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[62]	G2	G3	G3	G3	G3	Compatible Material
Surge[63]						
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[64]						
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)[65]	6kV	6kV	6kV	6kV	6kV	N/A

[59] Humidity rating per IEC 60068-2-3
[60] Shock rating per IEC 60068-2-27
[61] Vibration rating per IEC 60068-2-6
[62] Chemical Corrosion rating per ISA 71.04
[63] Surge rating per IEC 61000-4-5
[64] EMI Susceptibility rating per IEC 6100-4-3
[65] ESD (Air) rating per IEC 61000-4-2