Failure Modes, Effects and Diagnostic Analysis

Project:
Surge protective devices BLITZDUCTOR® BSP

Customer:

DEHN + SÖHNE GmbH + Co. KG.
Neumarkt
Germany

Contract No.: DEHN 09/04-20

Report No.: DEHN 09/04-20 R002

Version V2, Revision R0; November 2009

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the surge protective devices BLITZDUCTOR® BSP 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® BSP.

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® BSP

BSP M4 BE 5	Combined lightning current and surge arrester module 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
BSP M4 BE 12	Combined lightning current and surge arrester module 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
BSP M4 BE 24	Combined lightning current and surge arrester module 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
BSP M4 BE 48	Combined lightning current and surge arrester module 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
BSP M4 BE 60	Combined lightning current and surge arrester module 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
BSP M4 BE 180	Combined lightning current and surge arrester module for protecting 4 single lines with common reference potential as well as unbalanced interfaces; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BSP M4 BD 5	Combined lightning current and surge arrester module for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BSP M4 BD 12	Combined lightning current and surge arrester module for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BSP M4 BD 24	Combined lightning current and surge arrester module for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BSP M4 BD 48	Combined lightning current and surge arrester module for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BSP M4 BD 60	Combined lightning current and surge arrester module for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 49.5 VAC / 70 VDC
BSP M4 BD 180	Combined lightning current and surge arrester module for protecting 2 pairs of balanced interfaces with electrical isolation; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BSP M4 BE HF 5	Combined lightning current and surge arrester module 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

BSP M4 BD HF 5	Combined lightning current and surge arrester module for protecting 2 pairs in high-frequency bus systems or video transmission systems; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BSP M2 BE 5	Combined lightning current and surge arrester module for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BSP M2 BE 12	Combined lightning current and surge arrester module for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct shield earthing; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BSP M2 BE 24	Combined lightning current and surge arrester module for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct shield earthing; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BSP M2 BE 48	Combined lightning current and surge arrester module for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct shield earthing; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BSP M2 BE 60	Combined lightning current and surge arrester module for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct shield earthing; max. continuous operating voltage U_C: 49.5 VAC / 70 VDC
BSP M2 BE 180	Combined lightning current and surge arrester module for protecting 2 single lines with common reference potential as well as unbalanced interfaces, available with direct shield earthing; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BSP M2 BD 5	Combined lightning current and surge arrester module for protecting 1 pair of balanced interfaces with electrical isolation, available with direct shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BSP M2 BD 12	Combined lightning current and surge arrester module for protecting 1 pair of balanced interfaces with electrical isolation, available with direct shield earthing; max. continuous operating voltage U_C: 10.6 VAC / 15 VDC
BSP M2 BD 24	Combined lightning current and surge arrester module for protecting 1 pair of balanced interfaces with electrical isolation, available with direct shield earthing; max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
BSP M2 BD 48	Combined lightning current and surge arrester module for protecting 1 pair of balanced interfaces with electrical isolation, available with direct shield earthing; max. continuous operating voltage U_C: 38.1 VAC / 54 VDC
BSP M2 BD 60	Combined lightning current and surge arrester module for protecting 1 pair of balanced interfaces with electrical isolation, available with direct shield earthing; max. continuous operating voltage U_C: 49.5 VAC / 70 VDC
BSP M2 BD 180	Combined lightning current and surge arrester module for protecting 1 pair of balanced interfaces with electrical isolation, available with direct shield earthing; max. continuous operating voltage U_C: 127 VAC / 180 VDC
BSP M2 BE HF 5	Combined lightning current and surge arrester module for protecting 1 pair in high-frequency transmissions without electrical isolation; available with direct shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC
BSP M2 BD HF 5	Combined lightning current and surge arrester module for protecting 1 pair in high-frequency bus systems or video transmission systems, available with direct shield earthing; max. continuous operating voltage U_C: 4.2 VAC / 6 VDC

For safety applications only the described configurations were considered. All other possible variants or electronics are not covered by this report.

The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 1.

The surge protective devices BLITZDUCTOR® BSP are considered to be Type A[1] subsystems with a hardware fault tolerance of 0.

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

Table 2: BSP M2(4) BD * – Failure rates

	***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 detected	0	0
Fail Safe Undetected (λ_{SU})	**21**	**21**
Fail safe undetected	3	3
No effect	18	18
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail dangerous detected	0	4
Fail Dangerous Undetected (λ_{DU})	**6**	**2**
Fail dangerous undetected	6	2
No part	1	1

Total failure rate (safety function)	**27 FIT**	**27 FIT**
SFF [4]	**78.2%**	**92.8%**
MTBF	**4182 years**	**4182 years**

SIL AC [5]	**SIL2**	**SIL3**

[1] Type A subsystem: "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

[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.

[4] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[5] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. See also previous footnote.

Table 3: BSP M2 BD HF 5 and BSP M4 BD HF 5 – 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 detected	0	0
Fail Safe Undetected (λ_{SU})	**29**	**29**
Fail safe undetected	3	3
No effect	26	26
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail dangerous detected	0	4
Fail Dangerous Undetected (λ_{DU})	**14**	**10**
Fail dangerous undetected	14	10
No part	1	1

Total failure rate (safety function)	**43 FIT**	**43 FIT**
SFF [8]	**67.7%**	**76.8%**
MTBF	**2636 years**	**2636 years**

SIL AC [9]	**SIL2**	**SIL2**

[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.

[8] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. See also previous footnote.

Table 4: BSP M2 BE HF 5 and BSP M4 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 detected	0	0
Fail Safe Undetected (λ_{SU})	**33**	**33**
Fail safe undetected	3	3
No effect	30	30
Fail Dangerous Detected (λ_{DD})	**0**	**8**
Fail dangerous detected	0	8
Fail Dangerous Undetected (λ_{DU})	**18**	**10**
Fail dangerous undetected	18	10
No part	1	1

Total failure rate (safety function)	**51 FIT**	**51 FIT**
SFF [12]	**64.9%**	**80.4%**
MTBF	**2225 years**	**2225 years**

SIL AC [13]	**SIL2**	**SIL2**

[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.

[12] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[13] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. See also previous footnote.

Table 5: BSP M2(4) BE * – 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 detected	0	0
Fail Safe Undetected (λ_{SU})	**21**	**21**
Fail safe undetected	3	3
No effect	18	18
Fail Dangerous Detected (λ_{DD})	**0**	**7**
Fail dangerous detected	0	7
Fail Dangerous Undetected (λ_{DU})	**9**	**2**
Fail dangerous undetected	9	2
No part	1	1
Total failure rate (safety function)	**30 FIT**	**30 FIT**
SFF [16]	**71.4%**	**93.0%**
MTBF	**3768 years**	**3768 years**
SIL AC [17]	**SIL2**	**SIL3**

A user of the surge protective devices BLITZDUCTOR® BSP can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 4.4.1 to 4.4.4 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508:2000. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

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

[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.

[16] The complete sensor or final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[17] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. See also previous footnote.