SIL Declaration of Conformity

FMEDA including SFF determination according to IEC 61508

Endress+Hauser Wetzer GmbH+Co. KG, Obere Wank 1, 87484 Nesselwang

declares as manufacturer, that the hardware assessment of surge arrester

HAW562

according to IEC 61508 has provided following parameters, which can be applied for calculating the functional safety of systems with used surge arresters.

Order code	HAW562-AAA		HAW562-AAB HAW562-AAC		HAW562-AAD		HAW562-8DA		HAW562-AAE	
	1)	2)	1)	2)	1)	2)	1)	2)	1)	2)
HFT	0	0	0	0	0	0	0	0	0	0
Device type	A	A	A	A	A	A	A	A	A	A
SFF 3)	> 78%	> 92%	-	-	> 76%	> 76%	> 85%	> 94%	> 78%	> 94%
λ_{SD}	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT
λ_{SU}	21 FIT	21 FIT	2 FIT	2 FIT	29 FIT	29 FIT	57 FIT	57 FIT	41 FIT	41 FIT
λ_{DD}	0 FIT	4 FIT	0 FIT	0.4 FIT	0 FIT	4 FIT	0 FIT	6 FIT	0 FIT	8 FIT
λ_{DU}	6 FIT	2 FIT	10 FIT	9.6 FIT	14 FIT	10 FIT	10 FIT	4 FIT	11 FIT	3 FIT
λ_{Total}	27 FIT	27 FIT	12 FIT	12 FIT	43 FIT	43 FIT	67 FIT	67 FIT	52 FIT	52 FIT
MTBF/years	4182	4182	-	-	2636	2636	1696	1696	2221	2221

1) Analysis 1 represents a worst-case analysis.
2) 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.
3) 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.

Nesselwang, 19.05.2011

Endress+Hauser Wetzer GmbH+Co.KG

Wilfried Meissner
Geschäftsführer

Endress+Hauser
People for Process Automation

SIL-Konformitätserklärung

FMEDA einschließlich SFF-Bestimmung nach IEC 61508

Endress+Hauser Wetzer GmbH+Co. KG, Obere Wank 1, 87484 Nesselwang

erklärt als Hersteller, dass die Hardware-Bewertung des Überspannungsschutzes

HAW562

nach IEC 61508 folgende Parameter ergeben hat, welche zur Berechnung der funktionalen Sicherheit von Systemen mit eingesetzten Überspannungsschutzgeräten verwendet werden können.

Bestelloption	HAW562-AAA		HAW562-AAB HAW562-AAC		HAW562-AAD		HAW562-8DA		HAW562-AAE	
	1)	2)	1)	2)	1)	2)	1)	2)	1)	2)
HFT	0	0	0	0	0	0	0	0	0	0
Gerätetyp	A	A	A	A	A	A	A	A	A	A
SFF 3)	> 78%	> 92%	-	-	> 67%	> 76%	> 85%	> 94%	> 78%	> 94%
λ_{SD}	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT
λ_{SU}	21 FIT	21 FIT	2 FIT	2 FIT	29 FIT	29 FIT	57 FIT	57 FIT	41 FIT	41 FIT
λ_{DD}	0 FIT	4 FIT	0 FIT	0.4 FIT	0 FIT	4 FIT	0 FIT	6 FIT	0 FIT	8 FIT
λ_{DU}	6 FIT	2 FIT	10 FIT	9.6 FIT	14 FIT	10 FIT	10 FIT	4 FIT	11 FIT	3 FIT
λ_{Total}	27 FIT	27 FIT	12 FIT	12 FIT	43 FIT	43 FIT	67 FIT	67 FIT	52 FIT	52 FIT
MTBF/Jahre	4182	4182	-	-	2636	2636	1696	1696	2221	2221

1) Analyse 1 ist eine Analyse des ungünstigsten Falls
2) Bei Analyse 2 wird angenommen, dass Leitungskurzschlüsse gegen Erde erkannt werden können oder keine Auswirkungen haben.
3) Das komplette Sensor- oder Aktorteilsystem muss ausgewertet werden, um den Gesamtanteil sicherer Ausfälle (Safe Failure Fraction) zu bestimmen. Die angegebene Zahl dient nur als Referenz.

Nesselwang, 19.05.2011

Endress+Hauser Wetzer GmbH+Co.KG

Wilfried Meissner
Geschäftsführer

Failure Modes, Effects and Diagnostic Analysis

Project:
Surge protective devices HAW562

Customer:
Endress+Hauser Wetzer GmbH+Co KG
Nesselwang
Germany

Contract No.: 10/12-079
Report No.: 10/12-079 R053
Version V1, Revision R0; March 2011

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the surge protective devices HAW562 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 HAW562.

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 HAW562

HAW562-AAA	Combined lightning current and surge arrester module 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
HAW562-AAD	Combined lightning current and surge arrester module 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
HAW562-8DA	Combined lightning current and surge arrester module for protecting 1 pair in intrinsically safe circuits and bus systems, available with direct or indirect shield earthing; Max. continuous operating voltage U_C: 23.3 VAC / 33 VDC
HAW562-AAE	Combined lightning current and surge arrester module for protecting 2 lines with common signal ground in Prosonic systems; Max. continuous operating voltage U_C: line 4: 15 VDC, line 2: 180 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 HAW562 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.

[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.

Table 2: HAW562-AAA – Failure rates [2]

	exida Profile 1	
	Analysis 1 [3]	Analysis 2 [4]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail safe 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 [5]	**78%**	**92%**
MTBF	**4182 years**	**4182 years**

SIL AC [6]	**SIL2**	**SIL3**

[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.

[5] 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.

[6] 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: HAW562-AAD – Failure rates

	exida Profile 1	
	Analysis 1 [7]	Analysis 2 [8]
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 [9]	**67%**	**76%**
MTBF	**2636 years**	**2636 years**

SIL AC [10]	**SIL2**	**SIL2**

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

[8] 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.

[9] 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.

[10] 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: HAW562-8DA – Failure rates

	exida Profile 1	
	Analysis 1 [11]	Analysis 2 [12]
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})	**57**	**57**
Fail safe undetected	3	3
No effect	54	54
Fail Dangerous Detected (λ_{DD})	**0**	**6**
Fail dangerous detected	0	6
Fail Dangerous Undetected (λ_{DU})	**10**	**4**
Fail dangerous undetected	10	4
No part	1	1

Total failure rate (safety function)	**67 FIT**	**67 FIT**
SFF [13]	**85%**	**94%**
MTBF	**1696 years**	**1696 years**

SIL AC [14]	**SIL2**	**SIL3**

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

[12] 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.

[13] 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.

[14] 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: HAW562-AAE – Failure rates

	exida Profile 1	
	Analysis 1 [15]	Analysis 2 [16]
Failure category	**Failure rates (in FIT)**	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail safe detected	0	0
Fail Safe Undetected (λ_{SU})	**41**	**41**
Fail safe undetected	4	4
No effect	37	37
Fail Dangerous Detected (λ_{DD})	**0**	**8**
Fail dangerous detected	0	8
Fail Dangerous Undetected (λ_{DU})	**11**	**3**
Fail dangerous undetected	11	3
No part	1	1

Total failure rate (safety function)	**52 FIT**	**52 FIT**
SFF [17]	**78%**	**94%**
MTBF	**2221 years**	**2221 years**

SIL AC [18]	**SIL2**	**SIL3**

A user of the surge protective devices HAW562 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 HAW562 (see Appendix 2).

[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.

[17] 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.

[18] 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.