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

HAW569

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	HAW569-AA2B		HAW569-DA2B		HAW569-CB2C	
	1)	2)	1)	2)	1)	2)
HFT	0	0	0	0	0	0
Device type	A	A	A	A	A	A
SFF [3]	> 78%	> 93%	> 78%	> 93%	> 84%	> 87%
λ_{SD}	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT
λ_{SU}	21 FIT	21 FIT	20 FIT	20 FIT	118 FIT	118 FIT
λ_{DD}	0 FIT	4 FIT	0 FIT	4 FIT	0 FIT	4 FIT
λ_{DU}	6 FIT	2 FIT	6 FIT	2 FIT	21 FIT	17 FIT
λ_{Total}	27 FIT	27 FIT	26 FIT	26 FIT	139 FIT	139 FIT
MTBF/years	2408	2408	2434	2434	821	821

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

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

HAW569

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

Bestelloption	HAW569-AA2B		HAW569-DA2B		HAW569-CB2C	
	1)	2)	1)	2)	1)	2)
HFT	0	0	0	0	0	0
Gerätetyp	A	A	A	A	A	A
SFF [3]	> 78%	> 93%	> 78%	> 93%	> 84%	> 87%
λ_{SD}	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT	0 FIT
λ_{SU}	21 FIT	21 FIT	20 FIT	20 FIT	118 FIT	118 FIT
λ_{DD}	0 FIT	4 FIT	0 FIT	4 FIT	0 FIT	4 FIT
λ_{DU}	6 FIT	2 FIT	6 FIT	2 FIT	21 FIT	17 FIT
λ_{Total}	27 FIT	27 FIT	26 FIT	26 FIT	139 FIT	139 FIT
MTBF/Jahre	2408	2408	2434	2434	821	821

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 arresters HAW569

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

Contract No.: 10/12-034
Report No.: 10/12-034 R055
Version V1, Revision R0; February 2011
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the surge arresters HAW569 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 arresters HAW569.

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) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Configuration overview

HAW569-AA2B	For 4-20 mA interfaces with thread M20 x 1.5 (inside/outside). Option of direct, indirect or no shield earthing. Max. continuous operating voltage U_C: 24.5 VAC / 34.8 VDC
HAW569-DA2B	Surge arrester for protecting intrinsically safe circuits and bus systems. Low-capacitance, energy-coordinated protective circuit with insulation resistance > 500 V to earth. Max. continuous operating voltage U_C: 24.5 VAC / 34.8 VDC
HAW569-CB2C	Flameproof surge arrester for use in potentially explosive atmospheres for combined protection of measuring circuits and power supplies. Protection of data side (measuring circuit) Max. continuous operating voltage U_C: 22.6 VAC / 32 VDC Protection of power side (power supply) Max. continuous operating voltage U_C: 255 VAC

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 2.

The surge arresters HAW569 are considered to be Type A[1] subsystems with a hardware fault tolerance of 0.

The following tables [2] 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.

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

Table 2: HAW569-AA2B – Failure rates

	exida Profile 2	
	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	21	21
Total failure rate (safety function)	**27 FIT**	**27 FIT**
SFF [5]	**78%**	**93%**
MTBF	**2408 years**	**2408 years**
SIL AC [6]	**SIL2**	**SIL3**

[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: HAW569-DA2B – Failure rates

	exida Profile 2	
	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})	**20**	**20**
Fail safe undetected	2	2
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	21	21
Total failure rate (safety function)	**26 FIT**	**26 FIT**
SFF [9]	**78%**	**93%**
MTBF	**2434 years**	**2434 years**
SIL AC [10]	**SIL2**	**SIL3**

[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: HAW569-CB2C – Failure rates

	exida Profile 2	
	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})	**118**	**118**
Fail safe undetected	80	80
No effect	38	38
Fail Dangerous Detected (λ_{DD})	**0**	**4**
Fail dangerous detected	0	4
Fail Dangerous Undetected (λ_{DU})	**21**	**17**
Fail dangerous undetected	21	17
No part	20	20
Total failure rate (safety function)	**139 FIT**	**139 FIT**
SFF [13]	**84%**	**87%**
MTBF	**821 years**	**821 years**
SIL AC [14]	**SIL2**	**SIL2**

A user of the surge arresters HAW569 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 4.4.3 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 arresters HAW569 (see Appendix 2).

[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.