HAUBER ELEKTRONIK

Sicherheitshandbuch SIL3

Schwingungsüberwachung

Typ 663

SIL3 PL-d *

Standard

Zone 1 & 21

Zone 2 & 21

* Die Hardware, der Schwingungsüberwachung Typ 663, wurde mittels der FMEDA durch die Firma Exida geprüft. Die Ergebnisse der FMEDA erfüllen die Kriterien nach SIL2, SIL3 und PL-d.

Ausgabe: 06.05.2015

Deutsch

Sicherheitshandbuch

Schwingungsüberwachung
Typ 663

Standard
Zone-1-21
Zone-2-22

Achtung !
Vor Inbetriebnahme des Produktes muss das Sicherheitshandbuch und die Betriebsanleitung vollständig gelesen und verstanden werden!

Alle Rechte, auch die der Übersetzung, vorbehalten.
Änderungen vorbehalten.

Bei Fragen wenden Sie sich bitte an die Firma:

HAUBER-Elektronik GmbH
Fabrikstraße 6
D-72622 Nürtingen
Germany
Tel.: +49 (0)7022 / 21750-0
Fax: +49 (0)7022 / 21750-50
info@hauber-elektronik.de
www.hauber-elektronik.de

Inhaltsverzeichnis

1. Geltungsbereich 4

2. Einsatzbereich 4

3. SIL-Konformität / Abkürzungen, Begriffe 4

4. Relevante Normen 5

5. Sicherheitsanforderungen 5

6. Projektierung 6

7. Montage und Installation 7

8. Verhalten im Betrieb und bei Störungen 7

9. Wiederholungsprüfung [TProof] 7

10. Nutzungsdauer 7

11. Sicherheitstechnische Kennzahlen 8-9

12. Management Summary 10-13

1 Geltungsbereich

Das vorliegende Sicherheitshandbuch der Schwingungsüberwachung Typ 663 gilt für die Varianten: Standard, Zone-1-21 und Zone-2-22.
Die Funktionalität der Varianten ist identisch. Die Varianten Zone-1-21 und Zone-2-22 verfügen zusätzlich über Zertifizierungen und Kennzeichnungen, die den Einsatz in explosionsgefährdeten Bereichen zulassen.

2 Einsatzbereich

Die Schwingungsüberwachung Typ 663 wird zur Messung und Überwachung der absoluten Lagerschwingung an Maschinen in Anlehnung an die Norm DIN ISO 10816 eingesetzt. Als Messgröße dient dabei der Effektivwert der Schwinggeschwindigkeit.
Die Auswertung der Schwingungsamplitude erfolgt in zwei voneinander unabhängigen Kanälen. Eine Überschreitung des einstellbaren Schwingungsgrenzwertes wird an Relaisausgängen signalisiert. Diese können zur Generierung eines Vor- und eines Hauptalarms genutzt werden. Des Weiteren besitzt der Typ 663 einen analogen Stromausgang. Dieser liefert einen zur Schwingungsgröße proportionalen Gleichstrom von 4...20 mA.

Bei der Ermittlung der Sicherheitsfunktion, mittels der sicherheitstechnischen Kennzahlen nach den unter Punkt 4 benannten Normen im Sicherheitshandbuch, wurden explizit die Relaiskontakte der Schwingungsüberwachung Typ 663 bewertet bzw. berücksichtigt. Der Stromausgang 4...20 mA ist nicht sicherheitsrelevant ausgeführt.

3 SIL-Konformität / Abkürzungen, Begriffe

Die SIL-Konformität wird durch die Nachweisdokumente unter Punkt.13 belegt.

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
λ_{sd}	Rate for safe detected failure
λ_{su}	Rate for safe undetected failure
λ_{dd}	Rate for dangerous detected failure
λ_{du}	Rate for dangerous undetected failure
DC_S	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd}+\lambda_{su})$
DC_D	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd}+\lambda_{du})$
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
CAT	Category according to EN ISO 13849-1:2008

Weitere Abkürzungen und Begriffe sind in der IEC 61508-4 benannt.

4 Relevante Normen

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

ISO 13849-1 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006); German version EN ISO 13849-1:2008

5 Sicherheitsanforderungen

Ausfallgrenzwerte für eine Sicherheitsfunktion, abhängig von der SILKlasse (IEC 61508-1, 7.6.2)

Sicherheits-Integritäts-Level	**Betriebsart mit niedriger Anforderungsrate**	**Betriebsart mit hoher Anforderungsrate**
SIL	**PFD_{avg}**	**PFD_{avg}**
4	$\geqslant 10^{-5}$ ... < 10^{-4}	$\geqslant 10^{-9}$ ... < 10^{-8}
3	$\geqslant 10^{-4}$ ... < 10^{-3}	$\geqslant 10^{-8}$ ... < 10^{-7}
2	$\geqslant 10^{-3}$ ... < 10^{-2}	$\geqslant 10^{-7}$ ... < 10^{-6}
1	$\geqslant 10^{-2}$ ... < 10^{-1}	$\geqslant 10^{-6}$ ... < 10^{-5}

Anteil ungefährlicher Ausfälle	**Fehlertoleranz der Hardware für sicherheitsbezogene Teilsysteme vom Typ A (IEC 61508-2, 7.4.3)**		
SFF	**HFT = 0**	**HFT = 1**	**HFT = 2**
< 60 %	SIL1	SIL2	SIL3
60 % ... < 90 %	SIL2	SIL3	
90 % ... < 99 %	SIL3		
⩾ 99 %	SIL3		

6 Projektierung

Sicherheitsfunktion
Die Sicherheitsfunktion dieser Schwingungsüberwachung ist das Erkennen einer Überschreitung der Schwingungsgrenzwerte und das Melden einer überhöhten Schwingung mittels der Relaiskontakte. Die beiden Grenzwerte dienen als Vor- und Hauptalarm.

Bei der Ermittlung der Sicherheitsfunktion, mittels der sicherheitstechnischen Kennzahlen nach den unter Punkt 4 benannten Normen, wurden explizit die Relaiskontakte der Schwingungsüberwachung Typ 663 bewertet bzw. berücksichtigt.

Sicherer Zustand
Der sichere Zustand ist dann gewährleistet, wenn der oder die Schwingungsgrenzwerte nicht überschritten sind. Hierbei ist die Justierung der Schwingungsgrenzwerte entscheidend.
Der Betreiber muss seine anlagenspezifischen Schwingungsgrenzwerte justieren.
Die Vorgehensweise der Justierung ist in der Betriebsanleitung beschrieben.

Beschreibung der Ausfallkategorien
Um das Ausfallverhalten der Schwingungsüberwachung zu beurteilen, wurden die folgenden Definitionen für den Ausfall der Vorrichtung betrachtet.

Fail-Safe State
Auf einen Fehlerzustand wird durch den Wechsel in einen sicheren Zustand reagiert (fail safe state).

Safe Failure ($\lambda sd + \lambda su$)
Ein ungefährlicher Ausfall (S) liegt vor, wenn das Messsystem ohne Anforderung des Prozesses in den definierten sicheren Zustand oder in den Störmodus wechselt.

Dangerous Failure ($\lambda dd + \lambda du$)
Ein gefährlicher Ausfall (D) liegt generell dann vor, wenn das Messsystem in einen gefährlichen oder funktionsunfähigen Zustand versetzt wird.

Dangerous Detected Failure (λdd)
Ein gefährlicher entdeckter Ausfall (dangerous detected failure) liegt vor, wenn das Messsystem bei einer Anforderung des Prozesses in den definierten sicheren Zustand oder in den Störmodus wechselt.

Dangerous Undetected Failure (λdu):
Ein gefährlicher unentdeckter Ausfall (dangerous undetected failure) liegt vor, wenn das Messsystem bei einer Anforderung des Prozesses weder in den definierten sicheren Zustand, noch in den Störmodus wechselt.

Definition Störmodus:
Der Störmodus entspricht dem Alarmbetriebszustand der Relais.

7 Montage und Installation

Es sind die Montage- und Installationshinweise der Betriebsanleitung zu beachten.
Im Rahmen der Inbetriebnahme, muss die Sicherheitsfunktion mittels der Testfunktion „Self Check“ überprüft werden. Hierbei muss die Einstellung der Grenzwerte so gewählt werden, dass die Sicherheitsfunktion auslöst, bevor es zu einem Schaden an der Anlage kommt.

8 Verhalten im Betrieb und bei Störungen

Die Einstellelemente bzw. Geräteparameter sollten während dem Betrieb nicht verändert werden. Bei Veränderungen der Einstellelemente bzw. Geräteparameter während dem Betrieb, muss die Sicherheit der Anlage durch den Betreiber gewährleistet sein! Auftretende Störungen sind in der Fehlertabelle der Betriebsanleitung beschrieben. Bei festgestellten Fehlern muss die gesamte Schwingungsüberwachung außer Betrieb genommen und der Prozess durch andere Maßnahmen im sicheren Zustand gehalten werden. Ein Austausch der Schwingungsüberwachung ist in der Betriebsanleitung beschrieben.

9 Wiederholungsprüfung [TProof]

Nach IEC 61508-4, Abschnitt 3.5.8 wird TProof definiert als wiederkehrende Prüfung zur Aufdeckung von Ausfällen in einem sicherheitsbezogenen System.

Der wiederkehrende Funktionstest dient dazu, die Sicherheitsfunktion zu überprüfen, um mögliche, nicht erkennbare gefährliche Fehler aufzudecken. Die Funktionsfähigkeit der Schwingungsüberwachung ist deshalb in angemessenen Zeitabständen zu prüfen. Es liegt in der Verantwortung des Betreibers, die Art der Überprüfung zu wählen. Die Zeitabstände richten sich nach der Häufigkeit der zu erwartenden Inanspruchnahme der Schwingungsüberwachung in der Praxis. Hierbei sollte der Testintervall der Testfunktion „Self Check“ 1% der zu erwartenden Inanspruchnahme sein.

Beispiel:
Geht man davon aus, dass die Schwingungsüberwachung alle 365 Tage einen kritischen Fehler einer Anlage erkennt, sollte der Zeitabstand der Testintervall zwischen 3...4 Tagen liegen.

Die Prüfung ist so durchzuführen, dass die einwandfreie Sicherheitsfunktion im Zusammenwirken aller Komponenten nachgewiesen wird. Die bei den Tests verwendeten Methoden und Verfahren müssen benannt und deren Eignungsgrad spezifiziert werden. Die Prüfungen sind zu dokumentieren. Verläuft der Funktionstest negativ, muss das gesamte Messsystem außer Betrieb genommen werden und der Prozess durch andere Maßnahmen im sicheren Zustand gehalten werden.

Bei Anwendung der in der Schwingungsüberwachung bereitgestellten Testfunktion „Self Check“, kann die Schwingungsüberwachung selbst in der Kategorie CAT2 Architektur als Eingabeinheit genutzt werden.

Die allg. Beschreibung und die Funktionsweise des „Self Check“, finden Sie in der Betriebsanleitung unter dem Punkt 15 Selbsttest.

10 Nutzungsdauer

Die Nutzungsdauer des Messsystems liegt bei 10 Jahren.

11 Sicherheitstechnische Kennzahlen

Die Ausfallraten der Elektronik, der mechanischen Teile der Schwingungsüberwachung, sowie des Prozessanschlusses wurden durch eine FMEDA nach IEC 61508 ermittelt. Den Berechnungen sind Bauelementeausfallraten nach SN 29500 zugrunde gelegt. Alle Zahlenwerte beziehen sich auf eine mittlere Umgebungstempertur während der Betriebszeit von 40°C. Für eine höhere durchschnittliche Temperatur von 60°C sollten die Ausfallraten erfahrungsgemäß mit einem Faktor von 2,5 multipliziert werden. Ein ähnlicher Faktor gilt, wenn häufige Temperaturschwankungen (täglich >15°C) zu erwarten sind.
Die Berechnungen stützen sich weiterhin auf die im Kapitel "Projektierung" genannten Hinweise.

Table 1: IEC 61508-2010 failure rates during normal operation with self-test

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**75**
Fail Dangerous Detected (λ_{DD})	**85**
Fail Dangerous Detected (λ_{DD})	64
Fail Annunciation Detected (λ_{AD})	21
Fail Dangerous Undetected (λ_{DU})	**9**
Fail Annunciation Undetected (λ_{AU})	1
No effect	206
No part	39
Total failure rate (safety function)	**169**
SFF [2]	**94%**
SIL AC [3]	**SIL3**
PFH	**9.0E-09 1/h**

Safety metrics according to ISO 13849-1:

$MTTF_d$ (years)	**1563**
DC	**90%**
Category (CAT)	**CAT2**

The user of the Vibration Control can initiate a self-test of the system, which can find several errors and check the basic safety function. During continuous operation, this self-test cannot be applied. The user of the system is responsible to apply the self-test in adequate intervals. If no self-test can be applied during continuous operation, the values according to Table 2 are valid.

PFD_{AVG} Werte

T[Proof] = 1 year	**T[Proof] = 2 years**	**T[Proof] = 5 years**
PFD_{AVG} = 4,04E-05	PFD_{AVG} = 7,56E-05	PFD_{AVG} = 1,81E-04

[2] The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[3] 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 that all related IEC 61508 requirements are fulfilled.

zu 11 Sicherheitstechnische Kennzahlen

Table 2: IEC 61508-2010 failure rates during continuous operation

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**75**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{DD})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**73**

Fail Annunciation Undetected (λ_{AU})	22
No effect	205
No part	39

Total failure rate (safety function)	**148**

SFF [4]	**50%**
SIL AC [5]	**SIL1**
PFH	**7.3E-08 1/h**

Safety metrics according to ISO 13849-1:

$MTTF_d$ (years)	**1563**
DC	**0%**
Category (CAT)	**CAT 1**

The values shown above are valid, if no self-test can be applied during continuous operation.

[4] The complete 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 that all related IEC 61508 requirements are fulfilled.

12 Management Summary

Failure Modes, Effects and Diagnostic Analysis

Project:
Type 663 Vibration Control

Customer:
HAUBER-Elektronik GmbH
Nürtingen
Germany

Contract No.: Hauber Q11/09-058

Report No.: Hauber Q11/09-058 R001

Version V2, Revision R0; May 2012

Jan Hettenbach

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 Type 663 Vibration Control.

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.

For safety applications only the described device was considered. All other possible variants are not covered by this report.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500. This failure rate database is specified in the safety requirements specification from HAUBER-Elektronik GmbH for the Vibration Control.

The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

These failure rates are valid for the useful lifetime of the Vibration Control, see Appendix B.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.3.

The Vibration Control is classified as Type A [1] elements according to IEC 61508, having a hardware fault tolerance of 0.

It can only be used for low demand mode applications. The failure rates according to IEC 61508:2010 2nd edition for the Vibration Control (considering only the relay switching output being part of the safety function) are listed in the following table.

[1] Type A element: “Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

Table 1: IEC 61508-2010 failure rates during normal operation with self-test

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**75**
Fail Dangerous Detected (λ_{DD})	**85**
Fail Dangerous Detected (λ_{DD})	64
Fail Annunciation Detected (λ_{AD})	21
Fail Dangerous Undetected (λ_{DU})	**9**

Fail Annunciation Undetected (λ_{AU})	1
No effect	206
No part	39

Total failure rate (safety function)	**169**

SFF [2]	**94%**
SIL AC [3]	**SIL3**
PFH	**9.0E-09 1/h**

Safety metrics according to ISO 13849-1:

$MTTF_d$ (years)	**1563**
DC	**90%**
Category (CAT)	**CAT2**
Performance Level	**9.0E-09 1/h**

The user of the Vibration Control can initiate a self-test of the system, which can find several errors and check the basic safety function. During continuous operation, this self-test cannot be applied. The user of the system is responsible to apply the self-test in adequate intervals. If no self-test can be applied during continuous operation, the values according to Table 2 are valid.

[2] The complete subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[3] 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 that all related IEC 61508 requirements are fulfilled.

Table 2: IEC 61508-2010 failure rates during continuous operation

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**75**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Detected (λ_{DD})	0
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**73**
Fail Annunciation Undetected (λ_{AU})	22
No effect	205
No part	39
Total failure rate (safety function)	**148**
SFF [4]	**50%**
SIL AC [5]	**SIL1**
PFH	**7.3E-08 1/h**

Safety metrics according to ISO 13849-1:

$MTTF_d$ (years)	**1563**
DC	**0%**
Category (CAT)	**CAT 1**
Performance Level	**7.3E-08 1/h**

The values shown above are valid, if no self-test can be applied during continuous operation.

[4] The complete 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 that all related IEC 61508 requirements are fulfilled.