

Safety Manual

Vibration Control

Type 663

SIL2 PL - d



Standard



Zone-1-21 



Zone-2-22 

Safety Manual

Vibration Control Type 663

Standard
Zone-1-21
Zone-2-22

Achtung !

Before Start-Up Procedure the Safety Manual must be read and understood!

All rights, including translation, reserved.
Changes reserved.

Should any question arise, please contact:

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

Table of Contents

1. Scope	4
2. Field of Application	4
3. SIL-Conformity / Abbreviations, Terms.....	4
4. Relevant Standards	5
5. Safety Requirements	5
6. Project Planning	6
7. Assembly and Installation.....	7
8. Behaviour in Operation and in Disorders.....	7
9. Recurrent Testing [TProof]	7
10. Useful Life.....	7
11. Safety Indicators.....	8
12. SIL-Declaration of Conformity	9
13. Management Summary	10-13

1 Scope

The present Safety Manual of the Vibration Control Type 663 is applicable for the variants: Standard, Zone-1-21 and Zone-2-22. The functionality of the variants is identical. In addition the variants Zone-1-21 and Zone-2-22 have certifications and labellings, that allow operation in explosion endangered areas.

2 Field of Application

The Vibration Control Type 663 ist applied for measurement and control of machines absolute bearing vibration, referring to DIN ISO 10816. Measurement parameter is the root mean square (rms) of the vibration velocity. The evaluation takes place in two channels independent from each other. An exceeding of the adjustable Limit Value is signalled via relay outputs. This can be used to generate a pre- and a main alarm.

In addition the Type 663 has an analogue current output. This delivers a direct current from 4...20 mA proportional to the vibration amplitude.

3 SIL-Conformity / Abbreviations, Terms

SIL-Conformity is proofed by documents; see chap. 13.

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

Further abbreviations and terms are named in IEC 61508-4.

4 Relevant Standards

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

IEC 61511-1 Functional safety - safety instrumented systems for the process industry sector

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 Safety Requirements

Failure limit for a safety function, depending on the SIL class (IEC 61508-1, 7.6.2)

Safety-Integrity-Level	Operating Mode with low Requirement Rate	Operating Mode with high Requirement Rate
SIL	PFD _{avg}	PFD _{avg}
4	$\geq 10^{-5} \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-4} \dots < 10^{-3}$	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-3} \dots < 10^{-2}$	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$

Safe Failure Fraction	Hardware Fault Tolerance for safety related Subsystems Type 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		
$\geq 99 \%$	SIL3		

6 Project Planning

Safety Function

The safety function of this vibration control is the detection of exceeding vibration limits and the report of excessive vibration via relay contacts. The two limit values serve as pre- and mainalarm.

Safe Condition

Safe condition is ensured then, if one or two limit values are not exceeded. The operator has to adjust his plant-specific vibration limits. The procedure of adjusting is described in the operating manual.

Description of the Failure Categories

To evaluate the failure behavior, the following definitions for the device failure were considered:

Fail-Safe State

A failure condition will be responded by a change into a safe condition (fail safe state).

Safe Failure ($\lambda_{sd} + \lambda_{su}$)

There is a safe failure if, without a request of the process, the measuring system changes into the defined safe state or into the failure mode.

Dangerous Failure ($\lambda_{dd} + \lambda_{du}$)

Generally there is a dangerous failure if the measuring system is put into a dangerous or inoperable condition.

Dangerous Detected Failure (λ_{dd})

There is a dangerous detected failure if, on a request of the process, the measuring system changes into the defined safe state or into the failure mode.

Dangerous Undetected Failure (λ_{du}):

There is a dangerous undetected failure if, on a request of the process, the measuring system neither changes into the defined safe condition nor into the failure mode.

7 Assembly and Installation

Note the assembly- and installation instructions in the operating manual. As part of the commissioning it is recommended to check the safety function by the testfunction "Self Check".

8 Behaviour in Operation and in Disorders

During operation the adjustable elements or device parameters shall not be changed.

If the adjustable elements or device parameters are changed during operation, nevertheless the safety of the plant must be guaranteed!

Occurring errors are described in the fault table of the operating manual. If errors are detected the whole vibration control has to be taken out of service and the process has to be kept in a safe condition by other measures. A replacement of the vibration control is described in the operating manual.

9 Recurrent Testing [TProof]

According to IEC 61508-4, Sec. 3.5.8, TProof is defined as recurrent Testing for the detection of failures in a safety-related system.

The recurrent function test is used to check the safety function, to uncover possible, not identified errors.

Therefore the operating ability has to be checked in reasonable intervals.

It is the responsibility of the operator to choose the kind of verification. The intervals are according to the expected frequency of utilization of the vibration control in practice. Here the test intervall of the test function "Self Check" should be 1 % of the expected utilization.

Example:

Assuming that the vibration control detects one critical error every 365 days, the intervall of testing should be 3...4 days.

The test shall be performed so that the perfect safety function in interaction of all components is proved. The test methods and procedures have to be named and the suitability level specified.

The tests must be documented. If the test is negative, the whole measuring system has to be taken out of service and the process has to be kept in a safe condition by other measures.

10 Useful Life

The useful life of the measuring system is 10...15 years.

11 Safety Indicators

The failure rates of electronics, mechanical parts of the vibration control as well as the process connection were determined by an FMEDA, according to IEC 61508.

The calculations are based on component-failure rates, according to SN 29500.

All numerical values refer to an average ambient temperature of 40° C during operation. For a higher average ambient temperature of 60° C, experience has shown that the failure rates should be multiplied by a factor 2,5. There is a similar value if frequent temperature fluctuations are expected (> 15° C a day) . The calculations base on the references in Chapter "Project Planning".

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.

PFD_{AVG} Werte

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
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.

12 SIL-Declaration of Conformity



SIL-Declaration of Conformity

Functional Safety of a Vibration Control, according to IEC 61508/IEC 61511

We **HAUBER-Elektronik GmbH**
Fabrikstraße 6
D-72622 Nürtingen

declare as manufacturer, that the

Vibration Control Type 663

is suitable for use in a safety-relevant application up to and including SIL3, according to IEC 61511"1 und IEC 61508, if the installation is compliant to the Safety Manual and the safety instructions are followed.

The vibration control is corresponding to a Type A element, according to IEC 61508.

The study revealed the following values:

- | | |
|--|--------|
| ☐ Failure rates for | |
| o total failures (λ_{SU}) | 75 FIT |
| o safe failures (λ_{SD}) | 0 FIT |
| o dangerous undetected failures (λ_{DU}) | 9 FIT |
| o dangerous detected failures (λ_{DD}) | 85 FIT |

It follows:

- | | |
|--|----------------------------|
| ☐ the proportion of safe failures (SFF) | 94% |
| ☐ SIL (Safety level) | SIL3 |
| ☐ PFH | 9.0E"09 1/h |
| ☐ PFD _{AVG} | 4,04E"05 (T[Proof] 1 year) |

Nürtingen, 31.05.2012

HAUBER"Elektronik GmbH

Tobias Bronkal
Managing director

13 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 40°C. 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 A¹ 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.