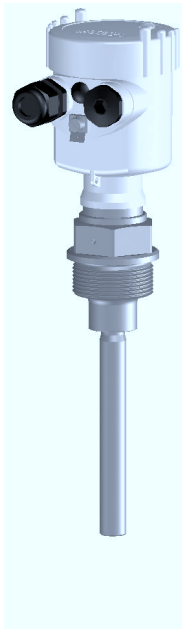


## Safety Manual

### VEGAVIB series 60

- NAMUR



Document ID:  
32005



Vibration

## Contents

### 1 Functional safety

1.1	General information . . . . .	3
1.2	Planning . . . . .	4
1.3	Adjustment instructions . . . . .	6
1.4	Setup. . . . .	7
1.5	Reaction during operation and in case of failure . . . . .	7
1.6	Recurring function test . . . . .	7
1.7	Safety-related characteristics . . . . .	9

### 2 Supplement

# 1 Functional safety

## 1.1 General information

**Scope**

This safety manual applies to measuring systems consisting of the vibrating level switch VEGAVIB series 60 with integrated electronics module VB60N:

**VEGAVIB 61, 62, 63, 65, 66, 67**

Valid hardware and software versions:

- Serial number of the electronics > 14642206
- Sensor software from Rev. 1.00

**Application area**

The measuring system can be implemented for level detection of bulk solids (powders and granulates) which meets the special requirements of safety technology.

This is possible up to SIL2 in a single channel architecture (1oo1D), and up to SIL3 in a multiple channel, redundant architecture.



**Note:**

With a special factory setting, the measuring system is also suitable for detection of solids in water (see "*Operating instructions manual*").

**SIL conformity**

The SIL conformity is confirmed by the verification documents in the appendix.

**Abbreviations, terms**

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD <sub>avg</sub>	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
$\lambda_{sd}$	Rate for safe detected failure
$\lambda_{su}$	Rate for safe undetected failure
$\lambda_{dd}$	Rate for dangerous detected failure
$\lambda_{du}$	Rate for dangerous undetected failure
DC <sub>S</sub>	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd}+\lambda_{su})$
DC <sub>D</sub>	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd}+\lambda_{du})$
FIT	Failure In Time (1 FIT = 1 failure/10 <sup>9</sup> h)
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure

MTTR	Mean Time To Repair
------	---------------------

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

### Relevant standards

- IEC 61508 (also available as DIN EN)
  - Functional safety of electrical/electronic/programmable electronic safety-related systems

### Safety requirements

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

Safety integrity level	Low demand mode	High demand mode
SIL	PFD <sub>avg</sub>	PFH
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	$\geq 10^{-2} \dots < 10^{-1}$	$\geq 10^{-6} \dots < 10^{-5}$

Safety integrity of hardware for safety-related subsystems of type B (IEC 61508-2, 7.4.3)

Safe failure fraction	Hardware fault tolerance		
	HFT = 0	HFT = 1	HFT = 2
SFF	HFT = 0	HFT = 1	HFT = 2
< 60 %	not permitted	SIL1	SIL2
60 % ... < 90 %	SIL1	SIL2	SIL3
90 % ... < 99 %	SIL2	SIL3	(SIL4)
$\geq 99$ %	SIL3	(SIL4)	(SIL4)

## 1.2 Planning

### Safety function

The safety function of this measuring system is the identification and signalling of the condition of the vibrating element.

A difference is made between the two conditions "covered" and "uncovered".

### Safe state

The safe state depends on the mode:

	Overflow protection (max. operation)	Dry run protection (min. operation)
Vibrating element in safe state	covered	uncovered
Output current in safe state	0.4 ... 1 mA	0.4 ... 1 mA
Failure current "fail low"	< 1 mA	< 1 mA
Failure current "fail high"	> 6.5 mA	> 6.5 mA

**Fault description**

A safe failure exists when the measuring system switches to the defined safe state or the fault mode without the process demanding it.

If the internal diagnostic system detects a failure, the measuring system goes into fault mode.

A dangerous undetected failure exists if the measuring system switches neither to the defined safe condition nor to the failure mode when the process requires it.

**Configuration of the processing unit**

If the measuring system delivers output currents of "fail low" or "fail high", it can be assumed that there is a malfunction.

The processing unit must therefore interpret such currents as a malfunction and output a suitable fault signal.

If this is not the case, the corresponding portions of the failure rates must be assigned to the dangerous failures. The stated values in chapter "Safety-relevant characteristics" can thus worsen.

The processing unit must correspond to the SIL level of the measurement chain.

The adjustment of the operation mode on the NAMUR amplifier according to IEC 60947-5-6 has to be selected in such a way, that its switching output at an input current < 1,2 mA is in a safe position.

**Low demand mode**

If the demand rate is only once a year, then the measuring system can be used as safety-relevant subsystem in "low demand mode" (IEC 61508-4, 3.5.12).

If the ratio of the internal diagnostics test rate of the measuring system to the demand rate exceeds the value 100, the measuring system can be treated as if it is executing a safety function in the mode with low demand rate (IEC 61508-2, 7.4.3.2.5).

An associated characteristic is the value  $PFD_{avg}$  (average Probability of dangerous Failure on Demand). It is dependent on the test interval  $T_{Proof}$  between the function tests of the protective function.

Number values see chapter "Safety-related characteristics".

**High demand mode**

If the "low demand rate" does not apply, the measuring system should be used as a safety-relevant subsystem in the mode "high demand mode" (IEC 61508-4, 3.5.12).

The fault tolerance time of the complete system must be higher than the sum of the reaction times or the diagnostics test periods of all components in the safety-related measurement chain.

An associated characteristic is the value PFH (failure rate).

Number values see chapter "Safety-related characteristics".

**Assumptions**

The following assumptions form the basis for the implementation of FMEDA:

- Failure rates are constant, wear of the mechanical parts is not taken into account
- Failure rates of external power supplies are not taken into account
- Multiple errors are not taken into account
- The average ambient temperature during the operating time is 40 °C (104 °F)
- The environmental conditions correspond to an average industrial environment
- The lifetime of the components is around 8 to 12 years (IEC 61508-2, 7.4.7.4, remark 3)
- The repair time (exchange of the measuring system) after a nondangerous malfunction is eight hours (MTTR = 8 h)
- The processing unit can interpret "fail low" and "fail high" failures as a disruption and trigger a suitable error message
- The scanning interval of a connected control and processing unit is max. 1 hour, in order to react to dangerous, detectable errors
- Existing communication interfaces (e. g. HART, I<sup>2</sup>C-Bus) are not used for transmission of safety-relevant information

**General instructions and restrictions**

The measuring system should be used appropriately taking pressure, temperature, density and chemical properties of the medium into account.

The user-specific limits must be complied with. The specifications of the operating instructions manual must not be exceeded.

Keep in mind when using as dry run protection:

- Avoid buildup on the vibrating system (probably shorter proof test intervals will be necessary)
- Fork version: avoid granulate size of the medium > 15 mm (0.6 in)

**1.3 Adjustment instructions****Adjustment elements**

Since the plant conditions influence the safety of the measuring system, the adjustment elements must be set according to the application:

- Potentiometer for switching point adaptation

- DIL switch for mode adjustment

The function of the adjustment elements is described in the operating instructions manual.

## 1.4 Setup

### Mounting and installation

Take note of the mounting and installation instructions of the operating instructions manual.

In the setup procedure, a check of the safety function by means of an initial filling is recommended.

## 1.5 Reaction during operation and in case of failure

### Operation and interference

The adjustment elements or device parameters must not be modified during operation.

If modifications have to be made during operation, carefully observe the safety functions.

Fault signals that may appear are described in the appropriate operating instructions manual.

If faults or error messages are detected, the entire measuring system must be shut down and the process held in a safe state by other measures.

The exchange of the electronics is simple and described in the operating instructions manual. Note the instructions for parameter adjustment and setup.

If due to a detected failure the electronics or the complete sensor is exchanged, the manufacturer must be informed (incl. a fault description).

## 1.6 Recurring function test

### Reason

The recurring function test is testing the safety function and to find out possible undetected, dangerous failures. The functional capability of the measuring system has to be tested in adequate time intervals. It is up to the user's responsibility to select the kind of testing. The time intervals are subject to the  $PFD_{avg}$ -value according to the chart and diagram in section "*Safety-relevant characteristics*".

With high demand rate, a recurring function test is not requested in IEC 61508. The functional efficiency of the measuring system is demonstrated by the frequent use of the system. In double channel architectures it is a good idea to verify the effect of the redundancy through recurring function tests at appropriate intervals.

**Implementation**

Please carry out the test in such a way, that the correct safety function in combination with all components is granted. This is granted by the control of the response height during a filling process. If a filling up to the response height is not practicable, the measuring system has to be responded by an appropriate simulation of the level or the physical measuring effect.

The methods and procedures used during the tests must be stated and their suitability must be specified. The tests must be documented.

If the function test proves negative, the entire measuring system must be switched out of service and the process held in a safe state by means of other measures.

In the double channel architecture (1oo2D) this applies separately to both channels.

**Function test in mode overfill protection**

If the measuring system is used as overfill protection, the proof of the function is ensured by a simple function test which can be triggered and monitored manually or by a connected control system.

This function test is triggered by an interruption of the supply cable for at least two seconds. Then a special warm-up reaction of the current output is carried out which must be recorded.

The test procedure is described in detail in the operating instructions manual.

**Simulation key:**

Pushing the simulation key simulates line break between sensor and processing unit.

**Note:**

This test can be carried out only if the vibrating element is uncovered.

**Function test of connected instruments**

The function of connected instruments can be checked in the "max." and "min." modes with the "**Simulation key**". The test procedure is described in detail in the operating instructions manual.

**Note:**

For this test, take note of the condition of the vibrating element:

- Mode "*max.*": Vibrating element "*uncovered*"
- Mode "*min.*": Vibrating element "*covered*"

## 1.7 Safety-related characteristics

### Basics

The failure rates of the electronics, the mechanical parts of the transmitter as well as the process fitting are determined by an FMEDA according to IEC 61508. The calculations are based on component failure rates according to SN 29500. All values refer to an average ambient temperature during the operating time of 40 °C (104 °F).

For a higher average temperature of 60 °C (140 °F), the failure rates should be multiplied by a factor of 2.5. A similar factor applies if frequent temperature fluctuations are expected.

The calculations are also based on the specifications stated in chapter "Planning".

### Service life

After 8 to 12 years, the failure rates of the electronic components will increase, whereby the derived PFD and PFH values will deteriorate (IEC 61508-2, 7.4.7.4, note 3).

### Failure rates

	Overflow protection (max. operation)	Dry run protection (min. operation)
$\lambda_{sd}$	12 FIT	36 FIT
$\lambda_{su}$	160 FIT	155 FIT
$\lambda_{dd}$	390 FIT	366 FIT
$\lambda_{du}$	47 FIT	52 FIT
DC <sub>S</sub>	7 %	19 %
DC <sub>D</sub>	89 %	88 %
MTBF = MTTF + MTTR	1.56 x 10 <sup>6</sup> h	1.56 x 10 <sup>6</sup> h

### Fault reaction time

Diagnosis test period	< 100 sec.
-----------------------	------------

### Single channel architecture (1oo1D)

### Specific characteristics

SIL	SIL2
HFT	0
Instrument type	Type B

	Overflow protection (max. operation)	Dry run protection (min. operation)
<b>SFF</b>	92 %	91 %
<b>PFD<sub>avg</sub></b>		
T <sub>Proof</sub> = 1 year	< 0.021 x 10 <sup>-2</sup>	< 0.023 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 5 years	< 0.104 x 10 <sup>-2</sup>	< 0.114 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 10 years	< 0.207 x 10 <sup>-2</sup>	< 0.228 x 10 <sup>-2</sup>

	Overflow protection (max. operation)	Dry run protection (min. operation)
<b>PFH</b>	$< 0.047 \times 10^{-6}/h$	$< 0.052 \times 10^{-6}/h$

### Time-dependent process of $PFD_{avg}$

The chronological sequence of  $PFD_{avg}$  is nearly linear to the operating time over a period up to 10 years. The above values apply only to the  $T_{Proof}$  interval after which a recurring function test must be carried out.

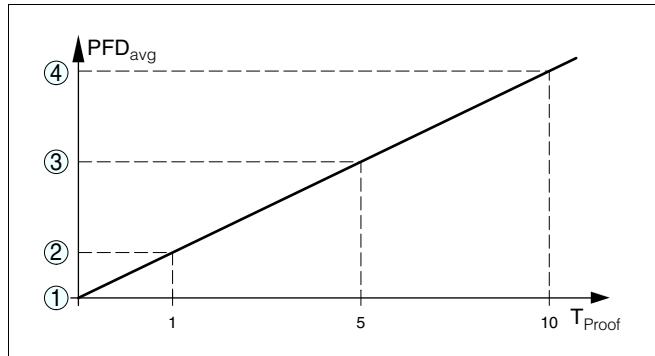


Fig. 1: Chronological sequence of  $PFD_{avg}$  (figures see above charts)

- 1  $PFD_{avg} = 0$
- 2  $PFD_{avg}$  after 1 year
- 3  $PFD_{avg}$  after 5 years
- 4  $PFD_{avg}$  after 10 years

### Multiple channel architecture

#### Specific characteristics

If the measuring system is used in a multiple channel architecture, the safety-relevant characteristics of the selected structure of the meas. chain must be calculated specifically for the selected application according to the above failure rates.

A suitable Common Cause Factor must be taken into account.

2 Supplement



CERTIFICATE

VEGA 100981C P0011 C001.1



exida Certification S.A. hereby confirms that the

**VEGAVIB / VEGAWAVE 60 Level Switch**

Output C, R, T, N, Z

Product Version: See listing in assessment report

**VEGA Grieshaber KG**

Schiltach, Germany

Has been assessed per the relevant requirements of

**IEC 61508:2000**

Parts 1 - 3, and meets requirements providing a level of integrity to

**Systematic Integrity : SIL 3 Capable**

**Random Integrity : SIL 2 @ HFT=0  
SIL 3 @ HFT=1**

**Safety function**

The VEGAVIB / VEGAWAVE 60 will de-energize its output (C,R,T,N) or set current (Z) to fail-safe output when a level goes above (or below) the trip point within the safety accuracy.

**Application Restrictions**

The unit must be properly designed and validated in a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor

Certifying Assessor

Date: 11 Jan 2011

exida Certification SA, Nyon, Switzerland



CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証



## Systematic Integrity: SIL 3 Capable

### SIL 3 Capability

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement.

Random Integrity: SIL 2 @ HFT=0  
SIL 3 @ HFT=1

### Summary for the VEGAVIB / VEGAWAVE 60 Level Switch:

#### Type B device

IEC 61508 failure rates in FIT ( $\lambda = 10^{-9}/h$ )

Model	Fail-Safe state	$\lambda_{SD}$	$\lambda_{SU}$	$\lambda_{DD}$	$\lambda_{DU}$
C Max / High trip	Out De-energized	0	506	124	41
C Min / Low trip	Out De-energized	0	481	135	56
R Max / High trip	Out De-energized	0	586	124	27
R Min / Low trip	Out De-energized	0	565	135	37
T Max / High trip	Out De-energized	0	487	124	30
T Min / Low trip	Out De-energized	0	466	135	40
N Max / High trip	Out < 1.0 mA	12	160	390	47
N Min / Low trip	Out < 1.0 mA	36	155	366	52
Z Max / High trip	Out > 12.5 mA	49	387	163	18
Z Min / Low trip	Out < 11.5 mA	39	352	182	43

All failure rates are given in FIT =  $10^{-9}/h$

### SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH /  $PFH_{AVG}$  considering the architecture, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

### The following documents are mandatory part of this certificate:

VEGA 03/05-08 R005 V3R1 Assessment Report

Safety manuals VEGAVIB / VEGAWAVE 60, all with versions:

C: 32002 / 32363      R: 32003 / 32364      T: 32004 / 32365

N: 32005 / 32366      Z: 32006 / 32367

The holder of this certificate  
may use this mark.

exida Certification SA, Nyon, Switzerland

info@exidacert.ch

Page 2 (2)



CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証









Printing date:

VEGA Grieshaber KG  
Am Hohenstein 113  
77761 Schiltach  
Germany  
Phone +49 7836 50-0  
Fax +49 7836 50-201  
E-mail: [info@de.vega.com](mailto:info@de.vega.com)  
[www.vega.com](http://www.vega.com)



All statements concerning scope of delivery, application, practical use and operating conditions of the sensors and processing systems correspond to the information available at the time of printing.

© VEGA Grieshaber KG, Schiltach/Germany 2011