Safety Manual

VEGAVIB series 60

Two-wire

Document ID: 32006

Contents

1 Functional safety **3**
1.1 General information 3
1.2 Planning 4
1.3 Adjustment instructions 6
1.4 Setup 6
1.5 Reaction during operation and in case of failure 6
1.6 Recurring function test 7
1.7 Safety-related characteristics 8

2 Supplement **11**

Editing status: 2018-11-29

32006-EN-181129

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 VB60Z:

VEGAVIB 61, 62, 63

Valid hardware and software versions:

- Serial number of the electronics > 14215176
- Sensor software from Rev. 1.03

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.

Due to the systematic capability SC3 this is possible up to:

- SIL2 in single-channel architecture
- SIL3 in multiple channel 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_{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 stated in IEC 61508-4.

Relevant standards

- IEC 61508 (also available as DIN EN)

32006-EN-181129

– 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_{avg}**	**PFH**
4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

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

Safe failure fraction	Hardware fault tolerance		
SFF	**HFT = 0**	**HFT = 1**	**HFT = 2**
< 60 %	not permitted	SIL1	SIL2
60 % … < 90 %	SIL1	SIL2	SIL3
90 % … < 99 %	SIL2	SIL3	(SIL4)
≥ 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 if mode switch on the sensor is set to "**max.**"	12.5 … 23.5 mA	2.3 … 11.5 mA
Output current in safe state if mode switch on the sensor is set to "**min.**"	2.3 … 11.5 mA	12.5 … 23.5 mA
Failure current "fail low"	< 2.3 mA	< 2.3 mA
Failure current "fail high"	> 23.5 mA	> 23.5 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 state 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.

If a VEGATOR 636 is used for processing, the mode switch on the sensor must be set to "*max.*".

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 an non-dangerous 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^2C-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 in 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.

32006-EN-181129

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 failuress. The functional capability of the measuring system has to be tested in adequate time intervals. It is up to the user's responsibility to selct 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 a multiple channel architecture this applies separately to each channel.

Simple function test

If the conditions of the following instructions are applicable, a simple function test can be triggered by interrupting the voltage supply for at least two seconds.

This can be the case through:

- Manual interruption of the supply cable
- Interruption of the supply cable through a connected control (SPLC)
- Pushing the **Test key** on a connected signal conditioning instrument (you can find suitable signal conditioning instruments in chapter "*Technical data*" of the operating instructions).

Note:
Conditions for the simple function test:

- A mechanical damage of the vibrating element as well as corrosion are excluded.
- Buildup on the vibrating element which can cause a considerable damping of the vibrating frequency is excluded.
- This test can be carried out only if the vibrating element is uncovered.

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

Mode switch on the sensor to "**max.**"

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
λ_{sd}	49 FIT	39 FIT
λ_{su}	387 FIT	352 FIT
λ_{dd}	163 FIT	182 FIT
λ_{du}	18 FIT	43 FIT
DC_S	11 %	10 %
DC_D	90 %	81 %
MTBF = MTTF + MTTR	1.59×10^6 h	1.59×10^6 h

Mode switch on the sensor to "**min.**"

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
λ_{sd}	39 FIT	45 FIT
λ_{su}	373 FIT	361 FIT
λ_{dd}	168 FIT	173 FIT
λ_{du}	36 FIT	37 FIT
DC_S	9 %	11 %
DC_D	82 %	82 %
MTBF = MTTF + MTTR	1.59×10^6 h	1.59×10^6 h

32006-EN-181129

Fault reaction time

Diagnosis test period	< 100 sec.

Single channel architecture

Specific characteristics

SIL	SIL2
HFT	0
Instrument type	Type B

Mode switch on the sensor to "**max.**"

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
SFF	97 %	93 %
PFD_{avg}		
T_{Proof} = 1 year	$< 0.008 \times 10^{-2}$	$< 0.019 \times 10^{-2}$
T_{Proof} = 5 years	$< 0.039 \times 10^{-2}$	$< 0.093 \times 10^{-2}$
T_{Proof} = 10 years	$< 0.077 \times 10^{-2}$	$< 0.186 \times 10^{-2}$
PFH	$< 0.018 \times 10^{-6}$/h	$< 0.043 \times 10^{-6}$/h

Mode switch on the sensor to "**min.**"

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
SFF	94 %	94 %
PFD_{avg}		
T_{Proof} = 1 year	$< 0.016 \times 10^{-2}$	$< 0.016 \times 10^{-2}$
T_{Proof} = 5 years	$< 0.078 \times 10^{-2}$	$< 0.081 \times 10^{-2}$
T_{Proof} = 10 years	$< 0.156 \times 10^{-2}$	$< 0.162 \times 10^{-2}$
PFH	$< 0.036 \times 10^{-6}$/h	$< 0.037 \times 10^{-6}$/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.

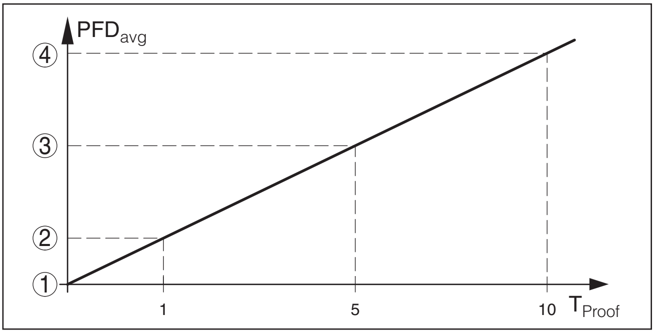

Fig. 1: Chronological sequence of PFD_{avg} (figures see above charts)

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

The manufacturer
may use the mark:

Revision 2.0 February 24, 2015

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証

VEGA 100981C P0011 C001

exida hereby confirms that the:

VEGAVIB / VEGAWAVE 60 Level Switch
Output C, R,T, N, Z

VEGA Grieshaber KG
Schiltach - Germany

Has been assessed per the relevant requirements of:

IEC 61508 : 2000 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; SIL 3 @ HFT = 1; Route 1_H

PFD_{AVG} and Architecture Constraints
must be verified for each application

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

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

VEGAVIB / VEGAWAVE 60 Level Switch

Certificate / Certificat / Zertifikat / 合格証

VEGA 100981C P0011 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; SIL 3 @ HFT = 1; Route 1_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic 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 stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

Versions:

See listing in the assessment report

IEC 61508 Failure Rates

Model	Fail-Safe state	λ_{SD}	λ_{SU}	λ_{DD}	λ_{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 (failures / 10^9 hours)

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, 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 element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: VEGA 03/05-08 R005 V3R2

Safety Manuals: VEGAVIB / VEGAWAVE 60:
C: 32002 / 32363 R: 32003 / 32364 T: 32004 / 32365
N: 32005 / 32366 Z: 32006 / 32367

Page 2 of 2

exida

64 N Main St
Sellersville, PA 18960

T-002, V3R8

32006-EN-181129

32006-EN-181129

Printing date:

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.
Subject to change without prior notice

32006-EN-181129

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
www.vega.com