

# Safety Manual

## VEGASON series 60

Two-wire 4 ... 20 mA/HART

Four-wire 4 ... 20 mA/HART



Document ID: 32774



**VEGA**

## Contents

<b>1</b>	<b>Functional safety</b> .....	<b>3</b>
1.1	General information.....	3
1.2	Planning.....	4
1.3	Instrument parameter adjustment.....	6
1.4	Setup.....	7
1.5	Reaction during operation and in case of failure.....	7
1.6	Recurring function test.....	8
1.7	Safety-related characteristics.....	8
<b>2</b>	<b>Supplement</b> .....	<b>11</b>

# 1 Functional safety

## 1.1 General information

**Scope**

This safety manual applies to measuring systems consisting of VEGASON series 60 ultrasonic sensors in two and four-wire version - 4 ... 20 mA/HART:

**VEGASON 61, 62, 63**

Valid hardware and software versions:

- Serial number of the electronics > 14455153
- Sensor software from Rev. 3.26

**Application area**

The measuring system can be used for level measurement of liquids and solids that meets the special requirements of safety engineering. Due to the service-proven reliability, implementation is possible in a single channel architecture up to SIL2 and in a multi-channel, diversitary redundant architecture up to SIL3.

The use of the measuring system in a multiple channel, homogeneous redundant architecture is excluded.

**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
  - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511-1

- Functional safety - safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

## 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	$\geq 10^{-5} \dots < 10^{-4}$	$\geq 10^{-9} \dots < 10^{-8}$
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		
SFF	HFT = 0	HFT = 1 (0)	HFT = 2
< 60 %	not permitted	SIL1	SIL2
60 % ... < 90 %	SIL1	SIL2	SIL3
90 % ... < 99 %	SIL2	SIL3	(SIL4)
$\geq 99$ %	SIL3	(SIL4)	(SIL4)

## Service proven

According to IEC 61511-1, paragraph 11.4.4, the failure tolerance HFT can be reduced by one for service-proven subsystems if the following conditions are met:

- The instrument is service proven
- Only process-relevant parameters can be modified on the instrument (e. g. measuring range, current output in case of failure ...)
- These process-relevant parameters are protected (e.g. password, ...)
- The safety function requires less than SIL4

The assessment by change management staff was a part of the "service proven" verification.

## 1.2 Planning

### Safety function

The measuring system generates on the current output a signal between 3.8 mA and 20.5 mA corresponding to the level.

This analogue signal is transmitted to a connected processing unit to monitor the following conditions:

- Exceeding a preset level
- Falling below a preset level

When the switching point set on the processing unit is reached, a signal is output.

**Safe state**

The safe state depends on the mode:

	Monitoring upper level	Monitoring lower level
Safe state	Exceeding the switching point	Falling below the switching point
Output current in safe state	> Switching point (-1 %)	< Switching point (+1 %)
Failure current "fail low"	< 3.6 mA	< 3.6 mA
Failure current "fail high"	> 21.5 mA	> 21.5 mA

The current tolerance  $\pm 1\%$  refers to the full measuring range of 16 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.

**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  $PF_{D,avg}$  (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 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
- 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.

The following critical process and vessel situations can cause measurement errors:

- Buildup on the transducer
- Flat or sharp-edged obstacles
- False reflections when agitators are used
- Foam generation above the medium
- Different gases above the medium (particularly CO<sub>2</sub>)
- Strong temperature gradient above the medium

Probably smaller proof test intervals required!

### 1.3 Instrument parameter adjustment

### Adjustment tools

Since plant conditions influence the functional safety of the measuring system, the instrument parameters must be set in compliance with the application.


The following tools are allowed:

- The DTM suitable for VEGASON in conjunction with an adjustment software according to the FDT/DTM standard, e. g. PACTware
- Display and adjustment module



#### Note:

Make sure that DTM Collection 10/2005 or a newer version is used.

<b>Create a measurement loop</b>	If the measuring system has not been ordered especially for applications in safety-instrumented systems (SIS), the parameter " <i>Sensor according to SIL</i> " must be selected in the adjustment software in the menu level " <i>Basic setting</i> ". If the display and adjustment module is used, the parameter " <i>SIL</i> " must be activated in the menu level " <i>Service</i> ".
<b>Reaction when malfunctions occur</b>	The parameter adjustment of the interference current influences the safety-related characteristics. For safety-relevant applications only the following interference currents are permitted: <ul style="list-style-type: none"> <li>● fail low = &lt;3.6 mA (default value)</li> <li>● fail high = 22 mA</li> </ul>
<b>Damping of the output signal</b>	The damping of the output signal must be adapted to the process safety time.
<b>Inadmissible modes</b>	Measured value transmission via HART signal as well as HART multidrop mode is not permitted.
<b>Inspection possibilities</b>	The effectivity of the set parameters must be checked in a suitable way. <ul style="list-style-type: none"> <li>● After connecting the instrument, the output signal jumps to the set interference current (at the end of the switch-on phase)</li> <li>● In mode "<i>Simulation</i>", the signal current can be simulated independently of the actual level</li> </ul>
<b>Access locking</b>	To avoid unwanted or unauthorized modification, the set parameters must be protected against unintentional access: <ul style="list-style-type: none"> <li>● Activate the password protection in the adjustment software</li> <li>● Activate the PIN on the display and adjustment module</li> </ul> <p>Access by means of HART handheld or similar equipment is not permitted.</p> <p>Protecting against unintentional or unauthorized adjustment can be done, e.g. by sealing the housing cover.</p> <p><b>Caution:</b>   After a reset of the values, all parameters must be checked or readjusted.</p>

## 1.4 Setup

<b>Mounting and installation</b>	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

<b>Operation and interference</b>	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  $PF_{avg}$ -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.

## 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**

Applies to overfill and dry run protection:

$\lambda_{sd}$	0 FIT
$\lambda_{su}$	458 FIT
$\lambda_{dd}$	668 FIT
$\lambda_{du}$	193 FIT
DC <sub>s</sub>	0 %
DC <sub>d</sub>	77 %
MTBF = MTTF + MTTR	0.6 x 10 <sup>6</sup> h

**Fault reaction time**

E013 (no measured value available)	
Application liquids	< 6 min
Application bulk solids	< 14 min
E013 (hardware error)	< 2 min
E036/E037 (no executable sensor software)	< 25 h

**Single channel architecture**

**Specific characteristics**

SIL	SIL2
HFT	0
Instrument type	Type B

Applies to overfill and dry run protection:

SFF	85 %
PFD <sub>avg</sub>	
T <sub>Proof</sub> = 1 year	< 0.085 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 5 years	< 0.423 x 10 <sup>-2</sup>
PFH	< 0.193 x 10 <sup>-6</sup> /h

**Time-dependent process of PFD<sub>avg</sub>**

The chronological sequence of PFD<sub>avg</sub> is nearly linear to the operating time over a period up to 10 years. The above values apply only to the T<sub>Proof</sub> interval after which a recurring function test must be carried out.

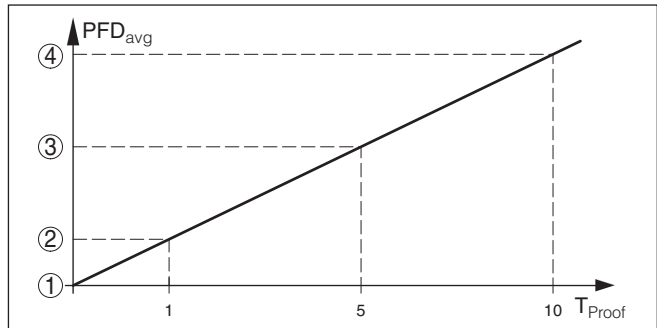


Fig. 1: Chronological sequence of  $PFD_{avg}$  (figures see above charts)

- 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.

The measuring system must only be used in a diversitary redundant architecture!

## 2 Supplement



## **FMEDA and Proven-in-use Assessment**

Project:

Ultrasonic transmitter VEGASON 60  
for continuous level measurement of liquids and solids

Customer:

**VEGA Grieshaber KG**  
Schiltach  
Germany

Contract No.: VEGA 06/03-33

Report No.: VEGA 06/03-33 R014

Version V1, Revision R0, October 2006

Stephan Aschenbrenner

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.

32774-EN-181129



**Management summary**

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the ultrasonic transmitters VEGASON 60 with 4..20 mA HART® output and software version Rev. 3.26 of June 2005. The devices manufactured in the USA by the Ohmart / VEGA Corporation carry the same name and are identically constructed under comparable quality aspects. Table 1 gives an overview of the different types that belong to the considered ultrasonic transmitters VEGASON 60.

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.

**Table 1: Version overview**

Type	Ultrasonic pulse	Process connection	Remark
VEGASON 61	68 kHz	G1½ A of PVDF	
VEGASON 62	53 kHz	G2 A of PVDF	
VEGASON 63	37 kHz	Compression flange or mounting strap	Ex not available

For safety applications only the 4..20 mA 4-wire current output was considered. All other possible output variants or electronics are not covered by this report. The different devices can be equipped with or without display.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be  $\geq 1,00E-03$  to  $< 1,00E-02$  for SIL 2 safety functions. A generally accepted distribution of PFD<sub>AVG</sub> values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD<sub>AVG</sub> value is caused by the sensor part.

For a SIL 2 application operating in low demand mode the total PFD<sub>AVG</sub> value of the SIF should be smaller than  $1,00E-02$ , hence the maximum allowable PFD<sub>AVG</sub> value for the sensor part would then be  $3,50E-03$ .

The ultrasonic transmitters VEGASON 60 are considered to be Type B<sup>1</sup> components with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to  $< 90\%$  must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

As the ultrasonic transmitters VEGASON 60 are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the ultrasonic transmitters and their software was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% to  $< 90\%$ .

The proven-in-use investigation was based on field return data collected and analyzed by VEGA.

<sup>1</sup> Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.



According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6 the device is suitable to be used, as a single device, for SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

VEGA did a qualitative analysis of the mechanical parts of the ultrasonic transmitters VEGASON 60 (see [D9]). This analysis was used by *exida* to calculate the failure rates of the sensor elements using *exida's* experienced-based data compilation for the different components of the sensor elements (see [R1] and [R2]). The results of this quantitative analysis are part for the calculations described in sections 5.2 and 5.3.

Assuming that the application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled.

**Table 2: Summary for the worst case version – Failure rates <sup>2</sup>**

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	<b>668</b>
Fail dangerous detected (internal diagnostics or indirectly <sup>3</sup> )	320
Fail high (detected by the logic solver)	19
Fail low (detected by the logic solver)	329
Annunciation detected	0
Fail Dangerous Undetected	<b>193</b>
Fail dangerous undetected	191
Annunciation undetected	2
No Effect	<b>458</b>
Not part	<b>354</b>
MTBF = MTTF + MTTR	68 years

**Table 3: Summary for the worst case version – IEC 61508 Failure rates**

$\lambda_{SD}$	$\lambda_{SU}$ <sup>4</sup>	$\lambda_{DD}$	$\lambda_{DU}$	SFF	DC <sub>S</sub> <sup>5</sup>	DC <sub>D</sub> <sup>3</sup>
0 FIT	458 FIT	668 FIT	193 FIT	85%	0%	77%

**Table 4: Summary for the worst case version – PFD<sub>AVG</sub> values**

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD <sub>AVG</sub> = 8,47E-04	PFD <sub>AVG</sub> = 4,23E-03	PFD <sub>AVG</sub> = 8,43E-03



<sup>2</sup> It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

<sup>3</sup> "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

<sup>4</sup> Note that the SU category includes failures that do not cause a spurious trip

<sup>5</sup> DC means the diagnostic coverage (safe or dangerous) for the ultrasonic transmitters VEGASON 60 by the safety logic solver.



The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to  $3.50E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to  $3.50E-03$ .

The failure rates listed above do not include failures resulting from incorrect use of the ultrasonic transmitters VEGASON 60, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of  $40^{\circ}\text{C}$ . For a higher average temperature of  $60^{\circ}\text{C}$ , the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the ultrasonic transmitters VEGASON 60 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 for different operating conditions is presented in sections 5.2 to 5.3 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. 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 ultrasonic transmitters VEGASON 60 (see Appendix 3).

Printing date:

# VEGA

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

© VEGA Grieshaber KG, Schiltach/Germany 2018



32774-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](mailto:info.de@vega.com)  
[www.vega.com](http://www.vega.com)