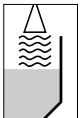


## Safety Manual

### VEGAPULS series 60

4 ... 20 mA/HART



## Contents

### 1 Functional safety

1.1	In general . . . . .	3
1.2	Planning . . . . .	5
1.3	Instrument parameter adjustment . . . . .	7
1.4	Setup . . . . .	9
1.5	Reaction during operation and in case of failure	9
1.6	Recurring function test . . . . .	9
1.7	Safety-related characteristics . . . . .	10

# 1 Functional safety

## 1.1 In general

**Scope**

This safety manual applies to measuring systems consisting of the VEGAPULS series 60 radar sensor in two-wire and four-wire versions 4 ... 20 mA/HART:

**VEGAPULS 61, 62, 63, 65, 66, 67, 68**

Valid hardware and software versions:

	Serial number of the electronics	Sensor software
VEGAPULS 61, 62, 63, 65, 66	>13978716	from rev. 3.22
VEGAPULS 61, 62, 63 with increased sensitivity	>14165303	from rev. 3.25
VEGAPULS 67, 68	>14165303	from rev. 3.25

**Area of application**

The measuring system can be used for level measurement of liquids and solids which meet the specific requirements of the safety technology.

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

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

**SIL conformity**

The SIL declaration of conformity can be downloaded from our homepage in the Internet.

**Abbreviations, terms**

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

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
$\lambda_{sd}$	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
$DC_S$	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

**Relevant standards**

- IEC 61508 (also available as DIN EN)
  - 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		
	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)

**Proven in use**

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

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

The assessment of the modification management was part of the proof for "Proven in use".

**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 outputted.

**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 is present when the measuring system switches to the defined safe state or the fault mode without the process demanding it.

	<p>If the internal diagnosis system detects a failure, the measuring system goes into fault mode.</p>
	<p>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.</p>
<b>Configuration of the processing unit</b>	<p>If the measuring system delivers output currents of "<i>fail low</i>" or "<i>fail high</i>", it can be assumed that there is a malfunction.</p> <p>The processing unit must therefore interpret such currents as a malfunction and output a suitable fault signal.</p> <p>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 "<i>Safety-relevant characteristics</i>" can thus worsen.</p>
	<p>The processing unit must correspond to the SIL level of the measurement chain.</p>
<b>Low demand mode</b>	<p>If the demand rate is only once a year, then the measuring system can be used as safety-relevant subsystem in "<i>low demand mode</i>" (IEC 61508-4, 3.5.12).</p> <p>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).</p> <p>An associated characteristic is the value <math>PFD_{avg}</math> (average Probability of dangerous Failure on Demand). It is dependent on the test interval <math>T_{Proof}</math> between the function tests of the protective function.</p>
	<p>Number values see chapter "<i>Safety-related characteristics</i>".</p>
<b>High demand mode</b>	<p>If the "<i>low demand rate</i>" does not apply, the measuring system as safety-relevant subsystem in "<i>high demand mode</i>" should be used (IEC 61508-4, 3.5.12).</p> <p>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.</p>
	<p>An associated characteristic is the value PFH (failure rate).</p>
	<p>Number values see chapter "<i>Safety-related characteristics</i>".</p>

**Assumptions**

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

- 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 errors 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, dielectric value and chemical properties of the medium into account.

Instructions to critical process and vessel situations are described in the operating instructions manual.

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

### 1.3 Instrument parameter adjustment

**Adjustment tools**

Since the plant conditions influence the safety of the measuring system, the instrument parameters must be set according to the application.

The following tools are allowed:

- the DTM suitable for VEGAPULS in conjunction with an adjustment software according to the FDT/DTM standard, e.g. PACTware™
- Indicating and adjustment module

**Note:**

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

- Create a measurement loop** In the adjustment software, the parameter "*Sensor according to SIL*" must be selected in the menu level "*Basic adjustment*".  
If the indicating and adjustment module is used, the parameter "*SIL*" must be activated in the menu level "*Service*".
- Reaction in case of failure** The parameter adjustment of the interference current influences the safety-related characteristics. For safety-relevant applications only the following interference currents are permitted:
- fail low = <3.6 mA (default value)
  - fail high = 22 mA
- Damping of the output signal** The damping of the output signal must be adapted to the process safety time.
- Inadmissible modes** Measured value transmission via HART signal as well as HART multidrop mode is not permitted.
- Inspection possibilities** The effectivity of the set parameters must be checked in a suitable way.
- After connecting the instrument, the output signal jumps to the set interference current (at the end of the switch on phase)
  - In mode "*Simulation*", the signal current can be simulated independent of the actual level
- Access locking** To avoid unwanted or unauthorized modification, the set parameters must be protected against unintentional access:
- activate the password protection in the adjustment software
  - Activate the PIN on the indicating and adjustment module
- The access by means of HART handheld or similar is not permitted.
- Protecting against unintentional or unauthorized adjustment can be done, e.g. by sealing the housing cover.

**Caution:**

After a reset of the values, all parameters must be checked or readjusted.

**Mounting and installation****1.4 Setup**

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**

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.

An exchange of the electronics is easily possible and is described in the operating instructions manual.

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****In general**

The recurring function test is used to check the safety function, to detect possible non-detectable dangerous faults. The function of the measuring system must be checked in adequate intervals.

The operator is responsible for choosing the type of check. The time intervals depend on the selected  $PFD_{avg}$  value according to chart and diagram in paragraph "*Safety-related characteristics*".

With high demand rate, a recurring function test is not requested in IEC 61508. The function 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 redundancy through recurring function tests at appropriate intervals.

The test must be carried out in a way that verifies the flawless operation of the safety functions in conjunction with all system components.

This is ensured by a controlled reaching of the response height during filling. If filling up to the response height is not possible, then a response of the measuring system must be triggered by a suitable 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.

## 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
$\lambda_{su}$	461 FIT
$\lambda_{dd}$	1129 FIT
$\lambda_{du}$	358 FIT
DC <sub>S</sub>	0 %

DC <sub>D</sub>	75 %
MTBF = MTTF + MTTR	0.45x10 <sup>6</sup> h

**Fault reaction time**

**VEGAPULS 61, 62, 63**

E013 (no measured value available)	2 ... 20 min depending on the application
E042/E043 (hardware error)	<2 min
E036/E037 (no executable sensor software)	<25 h

**VEGAPULS 65, 66**

E013 (no measured value available)	2 ... 8 min depending on the application
E042/E043 (hardware error)	<2 min
E036/E037 (no executable sensor software)	<15 h

**VEGAPULS 68 and VEGAPULS 61, 62, 63 with increased sensitivity**

E013 (no measured value available)	2 ... 36 min depending on the application
E042/E043 (hardware error)	<4 min
E036/E037 (no executable sensor software)	<80 h

**Single channel architecture 1oo1D**

**Specific characteristics**

SIL	SIL2
HFT	0
Sensor type	Type B

**Applies to overflow and dry run protection:**

SFF	81 %
PFD <sub>avg</sub>	
T <sub>Proof</sub> = 1 year	<0.157x10 <sup>-2</sup>
T <sub>Proof</sub> = 5 years	<0.779x10 <sup>-2</sup>

PFH	$<0.358 \times 10^{-6}/h$
-----	---------------------------

**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.

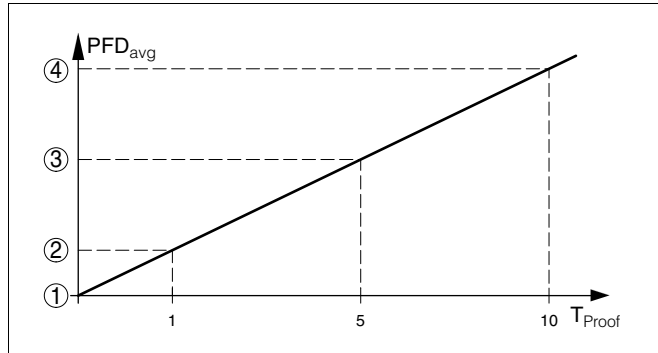


Fig. 1: Chronological sequence of  $PFD_{avg}$  (figures see above charts)

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

**Specific characteristics**

**Multiple channel architecture**

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!









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 2007