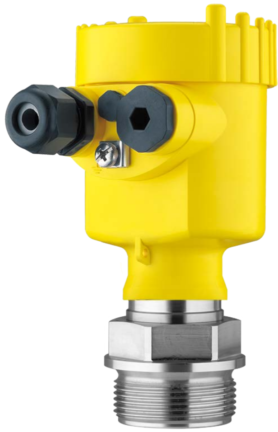
Safety Manual

VEGAPULS 6X

Two-wire 4 … 20 mA/HART

With SIL qualification



Document ID: 66494

VEGA

Contents

Editing status: 2022-06-28

1 Document language

DE	Das vorliegende *Safety Manual* für Funktionale Sicherheit ist verfügbar in den Sprachen Deutsch, Englisch, Französisch und Russisch.
EN	The current *Safety Manual* for Functional Safety is available in German, English, French and Russian language.
FR	Le présent *Safety Manual* de sécurité fonctionnelle est disponible dans les langues suivantes: allemand, anglais, français et russe.
RU	Данное руководство по функциональной безопасности *Safety Manual* имеется на немецком, английском, французском и русском языках.

2 Scope

2.1 Instrument version

This safety manual applies to radar sensor

VEGAPULS 6X

Electronics types:

- Two-wire 4 … 20 mA/HART
- Two-wire 4 … 20 mA/HART with overvoltage arrester

Each with functional safety SIL (IEC 61508)

Valid versions:

- from HW Ver 1.0.0
- from SW Ver 1.1.0

SIL The following versions are excluded from safety-relevant applications:

2.2 Application area

The radar sensor can be used in a safety-related system according to IEC 61508 in the modes *low demand mode* or *high demand mode* for the measurement of the following process variables:

- Level measurement of liquids and bulk solids

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

- SIL2 in single-channel architecture
- SIL3 in multiple channel architecture

The following interface can be used to output the measured value:

- Current output: 4 … 20 mA

SIL The following interfaces are only permitted for parameter adjustment and for informative use:

- HART
- Display and adjustment module PLICSCOM (also via Bluetooth)
- VEGACONNECT (also via Bluetooth)
- Current output II [1)]

2.3 SIL conformity

The SIL confirmity was judged and certified independently by *TÜV NORD CERT* according to IEC 61508:2010 (Ed.2) (verification documents see " *Supplement*").

SIL The certificate is valid for the entire service life of all instruments that were sold before the certificate expired!

66494-EN-220712

[1)] Only with instrument version with supplementary electronics "Two-wire 4 … 20 mA/HART plus additional current output 4 … 20 mA".

3 Planning

3.1 Safety function

Safety function

The sensor generates on its current output a signal between 3.8 mA and 20.5 mA corresponding to the process variable. This analogue signal is fed to a connected processing system to monitor the following conditions:

- Exceeding a defined limit value of the process variable
- Falling below a defined limit value of the process variable
- Monitoring of a defined range of the process variable

Safety tolerance

For the design of the safety function, the following aspects must be taken into account with regard to the tolerances:

- Due to undetected failures in the range between 3.8 mA and 20.5 mA, an incorrect output signal can be generated which deviates from the real measured value by up to 2 %
- Due to the special application conditions, increased measurement deviations can be caused (see Technical data in the operating instructions)

3.2 Safe state

Safe state

The safe state of the current output depends on the safety function (monitoring upper/lower limit) and on the characteristics set on the sensor.

Characteristics	Monitoring upper limit value	Monitoring lower limit value
4 … 20 mA	Output current ≥ Switching point	Output current ≤ Switching point
20 … 4 mA	Output current ≤ Switching point	Output current ≥ Switching point

Fault signals in case of malfunction

Possible fault currents:

- ≤ 3.6 mA ("fail low")
- > 21 mA ("fail high")

3.3 Prerequisites for operation

Instructions and restrictions

- The measuring system should be used appropriately taking pressure, temperature, density and chemical properties of the medium into account. The application-specific limits must be observed.
- The specifications according to the operating instructions manual, particularly the current load on the output circuits, must be kept within the specified limits
- Existing communication interfaces (e. g. HART, USB) are not used for transmission of the safety-relevant measured value
- The instructions in chapter " *Safety-related characteristics*", paragraph " *Supplementary information*" must be noted
- All parts of the measuring chain must correspond to the planned " *Safety Integrity Level (SIL)*"

4 Safety-related characteristics

4.1 Characteristics in accordance with IEC 61508 for level measurement

VEGAPULS 6X

Parameter	**Value**
Safety Integrity Level	SIL2 in single-channel architecture SIL3 in multiple channel architecture [2]
Hardware fault tolerance	HFT = 0
Instrument type	Type B
Mode	Low demand mode, High demand mode
SFF	> 90 %
MTBF [3]	0.37 x 10^6 h (42 years)
Diagnostic test interval [4]	< 30 min

Failure rates

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}
179 FIT	158 FIT	895 FIT	45 FIT	10 FIT	324 FIT	67 FIT

PFD_{AVG}	0.028 x 10^{-2}	(T1 = 1 year)
PFD_{AVG}	0.046 x 10^{-2}	(T1 = 2 years)
PFD_{AVG}	0.102 x 10^{-2}	(T1 = 5 years)
PFH	0.045 x 10^{-6} 1/h	

Proof Test Coverag (PTC)

Test type [5]	**Remaining failure rate of dangerous undetected failures**	**PTC**
Test 1	16 FIT	65 %
Test 2a	2 FIT	96 %
Test 2b	6 FIT	86 %
Test 2c	11 FIT	74 %

4.2 Characteristics in accordance with ISO 13849-1 for level measurement

The transmitter has been manufactured and verified using principles that demonstrate its suitability and reliability for safety-related applications. It can therefore be considered a " *proven component*" according to DIN EN ISO 13849-1.

[2] Homogeneous redundancy possible, because systematic capability SC3.
[3] Including errors outside the safety function.
[4] Time during which all internal diagnoses are carried out at least once.
[5] See section "Proof test".

66494-EN-220712

Derived from the safety-related characteristics, the following figures result according to ISO 13849-1 (safety of machinery): [6)]

VEGAPULS 6X

Parameter	**Value**
$MTTF_d$	87 years
DC	Average
PFH_D	0.045 x 10^{-6} 1/h

4.3 Supplementary information

Determination of the failure rates

The failure rates of the instruments were determined by an FMEDA according to IEC 61508. The calculations are based on failure rates of the components according to **SN 29500**:

All figures refer to an average ambient temperature of 40 °C (104 °F) during the operating time. For higher temperatures, the values should be corrected:

- Continuous application temperature > 50 °C (122 °F) by factor 1.5
- Continuous application temperature > 60 °C (140 °F) by factor 2.3

Similar factors apply if frequent temperature fluctations are expected.

Assumptions of the FMEDA

- The failure rates are constant. Take note of the useful service life of the components according to IEC 61508-2.
- Multiple failures are not taken into account
- Wear on mechanical parts is not taken into account
- Failure rates of external power supplies are not taken into account
- The environmental conditions correspond to an average industrial environment

Calculation of PFD_{AVG}

The values for PFD_{AVG} specified above were calculated as follows for a 1oo1 architecture:

$$PFD_{AVG} = \frac{PTC \times \lambda_{DU} \times T1}{2} + \lambda_{DD} \times MTTR + \frac{(1 - PTC) \times \lambda_{DU} \times LT}{2}$$

Parameters used:

- T1 = Proof Test Interval
- PTC = 96 %
- LT = 10 years
- MTTR = 8 h

Boundary conditions relating to the configuration of the processing unit

A connected control and processing unit must have the following properties:

- The failure signals of the measuring system are judged according to the idle current principle
- " *fail low*" and " *fail high*" signals are interpreted as a failure, whereupon the safe state must be taken on

6) ISO 13849-1 was not part of the certification of the instrument.

If this is not the case, the respective percentages of the failure rates must be assigned to the dangerous failures and the values stated in chapter *Safety-related characteristics*" redetermined!

Multiple channel architecture

Due to the systematic capability SC3, this instrument can also be used in multiple channel systems up to SIL3, also with a homogeneously redundant configuration.

The safety-related characteristics must be calculated especially for the selected structure of the measuring chain using the stated failure rates. In doing this, a suitable Common Cause Factor (CCF) must be considered (see IEC 61508-6, appendix D).

5 Setup

5.1 General information

Mounting and installation

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

SIL Setup with controlling the level must be carried out under the same process conditions that are to be expected in later operation. If the process conditions change, the operator must decide whether a new setup is necessary.

5.2 Instrument parameter adjustment

Tools

The following adjustment units are permitted for parameterization of the safety function:

- Display and adjustment module
- The DTM suitable for VEGAPULS 6X in conjunction with an adjustment software according to the FDT/DTM standard, e. g. PACTware
- The device description EDD suitable for VEGAPULS 6X

The parameter adjustment is described in the operating instructions manual.

SIL Wireless connection is also possible with existing Bluetooth function.

SIL The documentation of the device settings is only possible with the full version of the DTM Collection.

Safety-relevant parameters

For protection against unwanted or unauthorzed adjustment, the set parameters must be protected against unauthorized access. For this reason, the instrument is shipped in locked condition.

The device code is attached to the device documentation.

The default values of the parameters are listed in the operating instructions. When shipped with customer-specific parameter settings, the instrument is accompanied by a list of the values differing from the default values.

By means of the serial number this list can also be downloaded at " www.vega.com", " *Instrument search (serial number)*".

Safe parameterization

To avoid or detect possible errors during parameter adjustment for unsafe operating environments, a verification procedure is used that allows the safety-relevant parameters to be checked.

Parameter adjustment proceeds according to the following steps:

- Unlock adjustment
- Change parameters
- Lock adjustment and verify modified parameters

The exact process is described in the operating instructions.

SIL Wireless connection is also possible with existing Bluetooth function.

SIL The instrument is shipped in blocked condition!

For verification, all modified, safety-relevant and non safety-relevant parameters are shown.

The verification texts are displayed either in German or, when any other menu language is used, in English.

Unsafe device status

Warning:
When adjustment is unlocked, the safety function must be considered as unreliable. This applies until the parameters are verified and the adjustment is locked again. If the parameter adjustment process is not carried out completely, the device statuses described in the operating instructions must be taken into consideration.

If necessary, you must take other measures to maintain the safety function.

Instrument reset

Warning:
In case a reset to " *Default setting*" is carried out, all safety-relevant parameters must be checked or set anew.

6 Diagnostics and servicing

6.1 Behaviour in case of failure

Internal diagnosis

The instrument permanently monitored by an internal diagnostic system. If a malfunction is detected, a fault signal will be output on the safety-relevant output (see section " *Safe status*").

The diagnosis interval is specified in chapter " *Safety-related characteristics*".

Error messages in case of malfunction

A fault message coded according to the type of fault is output. The fault messages are listed in the operating instructions.

SIL

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

The occurrence of a failure must be reported to the manufacturer (including a description of the fault and whether it is a dangerous, undetected failure). The device must be returned to the manufacturer for examination.

6.2 Repair

Electronics exchange

The procedure is described in the operating instructions manual " *Electronics exchange*". Note the instructions for parameter adjustment and setup.

Software update

The procedure is described in the operating instructions manual. Note the instructions for parameter adjustment and setup.

66494-EN-220712

7 Proof test

7.1 General information

Objective

To identify possible dangerous, undetected failures, the safety function must be checked by a proof test at adequate intervals. It is the user's responsibility to choose the type of testing. The time intervals are determined by the selected PFD_{AVG} (see chapter " *Safety-related characteristics*").

For documentation of these tests, the test protocol in the appendix can be used.

If one of the tests 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.

Preparation

- Determine safety function (mode, switching points)
- If necessary, remove the instruments from the safety chain and maintain the safety function by other means
- Provide an approved adjustment unit

Assistant

You have the option of performing the proof test with the assistant in the DTM or the app.

Unsafe device status

⚠ **Warning:**
During the function test, the safety function must be treated as unreliable. Take into account that the function test influences downstream connected devices.

If necessary, you must take other measures to maintain the safety function.

After the function test, the status specified for the safety function must be restored.

7.2 Test 1: Without checking the process variable

Conditions

- Device remains in the installed condition
- Output signal corresponds to the assigned process variable
- Device status in the menu Diagnosis: " *OK*"

Procedure:

Carry out a restart (disconnect the test object from the power supply for at least 10 seconds + wait 1 minute) and then compare the output signal again for compliance with the assigned process variable.

By simulating the upper and lower fault current, downstream devices can be tested for correct response of the safety function.

1. Simulate upper current > 20 mA and check current output (test line resistor)
2. Simulate lower fault current ≤ 3.6 mA and check current output (test quiescent currents)

Expected result

Output signal corresponds to the assigned process variable

Step 1: Output signal corresponds to > 20 mA

Step 2: Output signal corresponds to ≤ 3.6 mA

Proof Test Coverage

See *Safety-related characteristics*

In addition to the diagnostic coverage for dangerous errors (DC_D) of 96.6 % of the internal diagnoses, this proof test uncovers approx. 65 % of the remaining dangerous undetected failures. This gives a total diagnostic coverage of 98.7 %.

7.3 Test 2: With check of the process variable

Conditions

- Device remains in the installed condition
- Output signal corresponds to the assigned process variable
- Device status in the menu Diagnosis: " *OK*"

Test 2a: Starting the safety function

Procedure

1. Carry out a restart (disconnect the test object from the power supply for at least 10 seconds + wait 1 minute) and then compare the output signal again for compliance with the assigned process variable
2. Reference measurement at 0 % - 50 % - 100 % of the adjusted level in use (4 mA - 12 mA - 20 mA)

Expected result

Step 1: Output signal corresponds to the assigned process variable

Step 2: Output signals correspond to the level

Proof Test Coverage

See *Safety-related characteristics*

In addition to the diagnostic coverage for dangerous errors (DC_D) of 96.67 % of the internal diagnoses, this proof test uncovers approx. 96 % of the remaining dangerous undetected failures. This gives a total diagnostic coverage of 99.8 %.

Test 2b: Starting areas + simulation current output

Procedure

1. Carry out a restart (disconnect the test object from the power supply for at least 10 seconds + wait 1 minute) and then compare the output signal again for compliance with the assigned process variable
2. Reference measurement at 0 … 10 % - 50 % - 90 … 100 % of the adjusted level in use (4 … 5.6 mA - 12 mA - 18.4 … 20 mA)
3. By simulating the upper and lower fault current, downstream devices can be tested for correct response of the safety function.

Expected result

Step 1: Output signal corresponds to the assigned process variable

Step 2: Output signals correspond to the level

Step 3: Safety function of the downstream devices responds correctly

Proof Test Coverage

See *Safety-related characteristics*

In addition to the diagnostic coverage for dangerous errors (DC_D) of 96.67 % of the internal diagnoses, this proof test uncovers approx.

86 % of the remaining dangerous undetected failures. This gives a total diagnostic coverage of 99.5 %.

Test 2c: Starting areas

Procedure

1. Carry out a restart (disconnect the test object from the power supply for at least 10 seconds + wait 1 minute) and then compare the output signal again for compliance with the assigned process variable
2. Reference measurement at 0 … 10 % - 50 % - 90 … 100 % of the adjusted level in use (4 … 5.6 mA - 12 mA - 18.4 … 20 mA)

Expected result

Step 1: Output signal corresponds to the assigned process variable

Step 2: Output signals correspond to the level

Proof Test Coverage

See *Safety-related characteristics*

In addition to the diagnostic coverage for dangerous errors (DC_D) of 96.67 % of the internal diagnoses, this proof test uncovers approx. 74 % of the remaining dangerous undetected failures. This gives a total diagnostic coverage of 99.1 %.

8 Appendix A: Test report

Identification	
Company/Tester	
Plant/Instrument TAG	
Meas. loop TAG	
Instrument type/Order code	
Instrument serial number	
Date, setup	
Date of the last proof test	

Test reason/Test scope	
	Setup without checking the process variable
	Setup with check of the process variable
	Proof test without checking the process variable
	Proof test with check of the process variable

Mode	
	Monitoring of an upper limit value
	Monitoring a lower limit value
	Range monitoring

Adjusted parameters of the safety function are documented	
	Yes
	No

Test result (if necessary)				
Test point	**Process variable** [7]	**Expected measured value**	**Real value**	**Test result**
Value 1				
Value 2				
Value 3				
Value 4				
Value 5				

Confirmation	
Date:	Signature:

[7] e.g.: limit level, level, interface, pressure, flow, density

9 Appendix B: Term definitions

Abbreviations

SIL	Safety Integrity Level (SIL1, SIL2, SIL3, SIL4)
SC	Systematic Capability (SC1, SC2, SC3, SC4)
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{AVG}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of a dangerous failure per hour (Ed.2)
FMEDA	Failure Mode, Effects and Diagnostics Analysis
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
λ_S	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_H	Rate for failure, who causes a high output current (> 21 mA)
λ_L	Rate for failure, who causes a low output current (≤ 3.6 mA)
λ_{AD}	Rate for diagnostic failure (detected)
λ_{AU}	Rate for diagnostic failure (undetected)
DC	Diagnostic Coverage
PTC	Proof Test Coverage (Diagnostic coverage for manual proof tests)
T1	Proof Test Interval
LT	Useful Life Time
MTBF	Mean Time Between Failure = MTTF + MTTR
MTTF	Mean Time To Failure
MTTR	IEC 61508, Ed1: Mean Time To Repair IEC 61508, Ed2: Mean Time To Restoration
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

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

© VEGA Grieshaber KG, Schiltach/Germany 2022

66494-EN-220712

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Germany

Phone +49 7836 50-0
E-mail: info.de@vega.com
www.vega.com