Safety Manual

VEGACAL series 60

Two-wire 4 … 20 mA/HART

Document ID: 35593

Contents

Editing status: 2018-11-29

35593-EN-181129

1 Functional safety

1.1 General information

Scope

This safety manual applies for measuring systems consisting of the capacitive sensor VEGACAL series 60 in the version two-wire 4 … 20 mA/HART:

VEGACAL 62, 63, 64, 65, 66, 69

Valid hardware and software versions:

- Serial number of the electronics > 14557661
- Sensor software from Rev. 1.01

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, implemention 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_{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
  - 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	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
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 (0)**	**HFT = 2**
< 60 %	not permitted	SIL1	SIL2
60 % … < 90 %	SIL1	SIL2	SIL3
90 % … < 99 %	SIL2	SIL3	(SIL4)
≥ 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 (-2 %)	< Switching point (+2 %)
Failure current "fail low"	< 3.6 mA	< 3.6 mA
Failure current "fail high"	> 21.5 mA	> 21.5 mA

The current tolerance ±2 % refers to the adjustment of 0 … 120 pF (see operating instructions manuals).

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 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, dielectric value 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 rod or cable breakage (probably smaller proof test intervals will be necessary)

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 VEGACAL 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.

Create a measurement loop

If the measuring system has not been ordered especially for applications in safety-instrumented systems (SIS), the parameter "*Sensor according to SIL*" must be selected in the adjustment sofware in the menu level "*Basic setting*". If the display and adjustment module

is used, the parameter "*SIL*" must be activated in the menu level "*Service*".

Reaction when malfunctions occur

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 independently 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 display and adjustment module

Access by means of HART handheld or similar equipment 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.

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.

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.

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:

λ_{sd}	0 FIT
λ_{su}	212 FIT
λ_{dd}	458 FIT
λ_{du}	208 FIT
DC_S	0 %
DC_D	68 %
MTBF = MTTF + MTTR	0.93 x 10^6 h

Fault reaction time

E013 (no measured value available)	< 10 sek.
E036/E037 (no executable sensor software)	< 1 h

Specific characteristics

Single channel architecture

SIL	SIL2
HFT	0
Instrument type	Type B

Applies to overfill and dry run protection:

SFF	76 %
PFD_{avg} T_{Proof} = 1 year T_{Proof} = 5 years	 < 0.091 x 10^{-2} < 0.182 x 10^{-2}
PFH	< 0.208 x 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.

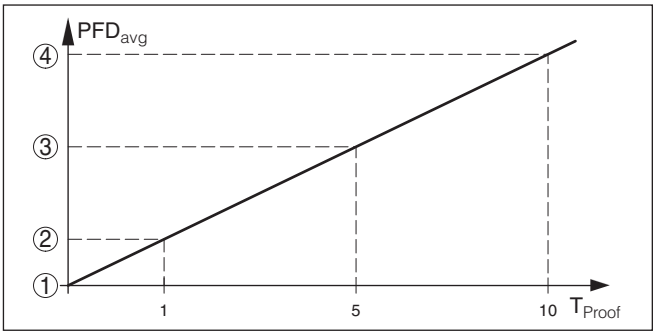

Fig. 1: Chronological sequence of PFD$_{avg}$ (figures see above charts)

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.

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

2 Supplement

35593-EN-181129

Konformitätserklärung
Declaration of conformity
Déclaration de conformité

IEC 61508 / IEC 61511

VEGA Grieshaber KG,
Am Hohenstein 113,
77761 Schiltach / Germany

erklärt als Hersteller, dass die kapazitiven Füllstandsensoren der Produktfamilie

declares as manufacturer, that the capacitive level sensors of the product family

déclare en tant que fabricant que les capteurs de niveau capacitifs de la famille

VEGACAL 62, 63, 64, 65, 66, 69

4 ... 20 mA/HART

entsprechend der IEC 61511-1, Abschnitt 11.4.4 („Betriebsbewährtheit") für den Einsatz in sicherheitsinstrumentierten Systemen (SIS) als Untersystem bis **SIL2** geeignet sind.
Die Sicherheitstechnischen Kennzahlen sowie die Sicherheitshinweise im „Safety Manual" sind zu beachten.
Die Beurteilung des Änderungswesens war Bestandteil des Nachweises der Betriebsbewährtheit.

according to IEC 61511-1, section 11.4.4 ("proven in use")
are suitable as a subsystem until **SIL2** in safety instrumented systems (SIS).
The safety related characteristics as well as the safety instructions in the "Safety Manual" must be considered.
The assessment of the modification management was part of the proof for "proven in use".

conviennent à une utilisation dans les systèmes instrumentés de sécurité (SIS) comme sous-système jusqu'à **SIL2** suivant la norme IEC 61511-1, paragraphe 11.4.4 ("validé en utilisation").
Les caractéristiques techniques relatives à la sécurité ainsi que les consignes de sécurité stipulées dans le „Safety Manual" sont à respecter.
L'évaluation du service de modifications a fait partie de la preuve de la validité en utilisation.

Schiltach, 18 Februar 2009

J. Fehrenbach

Josef Fehrenbach
R&D Director

Printing date:

35593-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