Safety Manual

VEGACAP series 60

Transistor (NPN/PNP)

Document ID: 31815

Contents

Editing status: 2018-11-29

1 Functional safety

1.1 General information

Scope

This safety manual applies to measuring systems consisting of the capacitive level switch VEGACAP series 60 with integrated electronics module CP60T:

VEGACAP 62, 63, 64, 65, 66, 69

Valid hardware and software versions:

- Serial number of the electronics > 14701856
- Sensor software from Rev. 1.01

Application area

The measuring system can be implemented for level detection of liquids and solids which meet the specific 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

SIL The use of the measuring system with a mounted float for safety-relevant oil/water detection is not permitted.

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)

- 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 is such that in case of the process requirement "*Reaching the determined switching point*" the output circuit changes condition.

Overflow protection:

When exceeding the switching point, change to condition "**Level exceeded**"

Dry run protection:

When falling below the switching point, change to condition "**Falling below level**"

Safe state

The safe state depends on the mode:

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
Safe state	Exceeding the switching point	Falling below the switching point
Output circuit in safe state	currentless	currentless

The safe state of the measuring system is the switched-off status (idle current principle):

- R electronics: relay output deenergised
- T electronics: transistor output non-conductive

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

The processing unit must evaluate the output circuit of the measuring system under the conditions of the quiescent current principle.

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 evaluates the output circuit of the measuring system according to the idle current principle.

- 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 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 measuring range selection
- 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.

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

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
λ_{sd}	0 FIT	0 FIT
λ_{su}	395 FIT	397 FIT
λ_{dd}	115 FIT	115 FIT

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
λ_{du}	35 FIT	33 FIT
DC_S	0 %	0 %
DC_D	76 %	77 %
MTBF = MTTF + MTTR	1.74 x 10^6 h	1.74 x 10^6 h

Fault reaction time

Diagnosis test period	< 360 sek.

Specific characteristics

Single channel architecture

SIL	SIL2
HFT	0
Instrument type	Type B

	Overflow protection (max. operation)	**Dry run protection (min. operation)**
SFF	94 %	94 %
PFD_{avg}		
T_{Proof} = 1 year	< 0.015 x 10^{-2}	< 0.015 x 10^{-2}
T_{Proof} = 5 years	< 0.077 x 10^{-2}	< 0.073 x 10^{-2}
T_{Proof} = 10 years	< 0.153 x 10^{-2}	< 0.145 x 10^{-2}
PFH	< 0.035 x 10^{-6}/h	< 0.033 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.

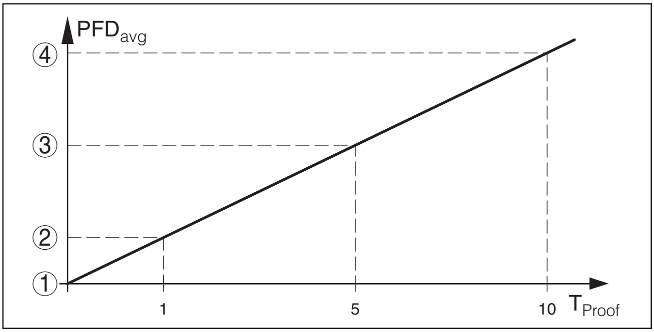


Fig. 1: Chronological sequence of PFD_{avg} (figures see above charts)

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.

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 C002

exida hereby confirms that the:

VEGACAP 60 Level Switch
Output R,T, 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

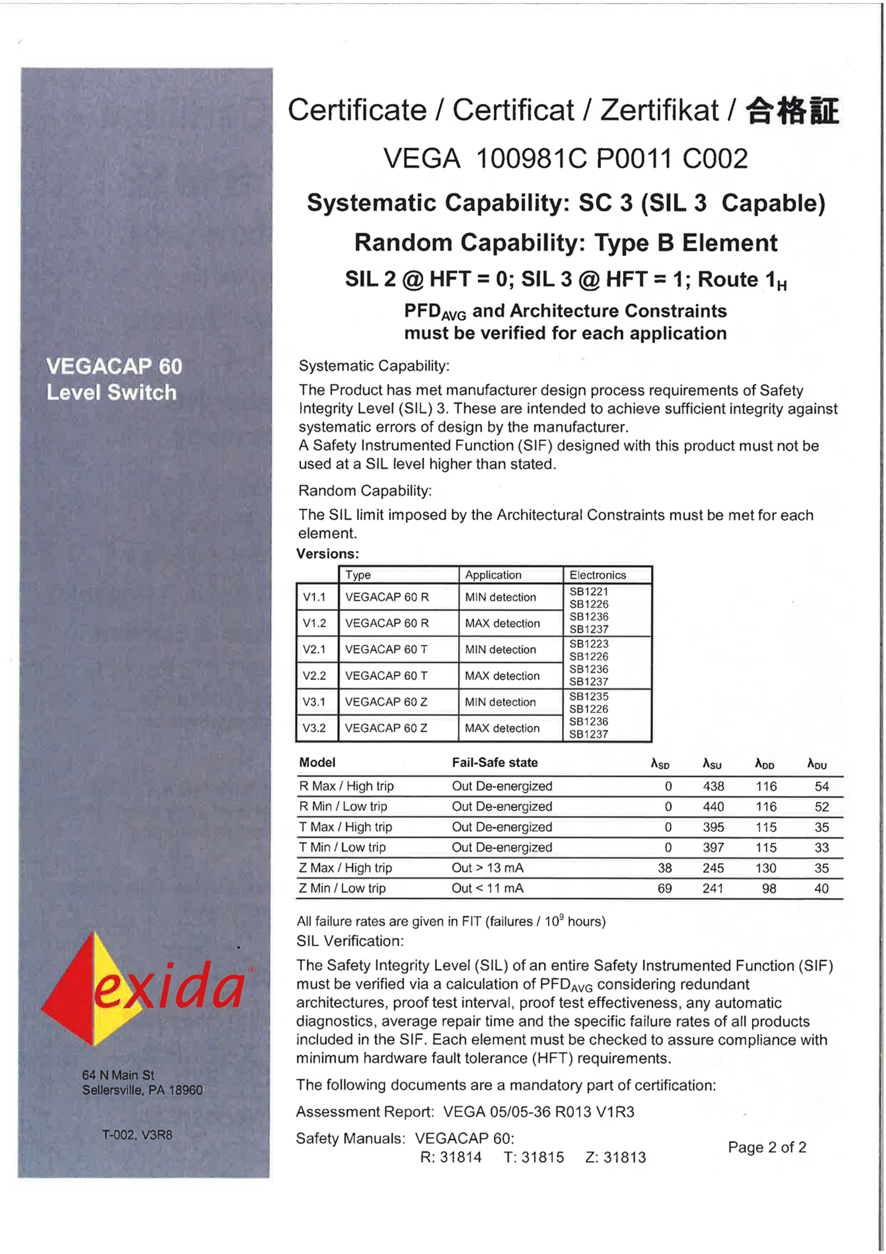
Safety Function:
The VEGACAP 60 will de-energize its output (R & T) or set current (Z) to fail-safe output when the level goes above (or below) the trip point within the stated safety accuracy.

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



VEGACAP 60
Level Switch

Certificate / Certificat / Zertifikat / 合格証

VEGA 100981C P0011 C002

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:

	Type	Application	Electronics
V1.1	VEGACAP 60 R	MIN detection	SB1221 SB1226 SB1236 SB1237
V1.2	VEGACAP 60 R	MAX detection	
V2.1	VEGACAP 60 T	MIN detection	SB1223 SB1226 SB1236 SB1237
V2.2	VEGACAP 60 T	MAX detection	
V3.1	VEGACAP 60 Z	MIN detection	SB1235 SB1226 SB1236 SB1237
V3.2	VEGACAP 60 Z	MAX detection	

Model	**Fail-Safe state**	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
R Max / High trip	Out De-energized	0	438	116	54
R Min / Low trip	Out De-energized	0	440	116	52
T Max / High trip	Out De-energized	0	395	115	35
T Min / Low trip	Out De-energized	0	397	115	33
Z Max / High trip	Out > 13 mA	38	245	130	35
Z Min / Low trip	Out < 11 mA	69	241	98	40

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 05/05-36 R013 V1R3

Safety Manuals: VEGACAP 60:
R: 31814 T: 31815 Z: 31813

exida
64 N Main St
Sellersville, PA 18960

T-002, V3R8

Page 2 of 2

Printing date:

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