

# Safety Manual

## VEGACAP Serie 60

Zweileiter



Document ID: 31813



**VEGA**

## Inhaltsverzeichnis

<b>1 Funktionale Sicherheit .....</b>	<b>3</b>
1.1 Allgemein .....	3
1.2 Projektierung .....	4
1.3 Einstellhinweise.....	6
1.4 Inbetriebnahme .....	6
1.5 Verhalten im Betrieb und bei Störungen .....	6
1.6 Wiederkehrender Funktionstest .....	7
1.7 Sicherheitstechnische Kennzahlen .....	7
<b>2 Anhang.....</b>	<b>10</b>

# 1 Funktionale Sicherheit

## 1.1 Allgemein

### Geltungsbereich

Dieses Sicherheitshandbuch gilt für Messsysteme, bestehend aus dem kapazitiven Grenzscharter der Serie VEGACAP 60 mit eingebautem Elektronikeinsatz CP60Z:

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

Gültige Hardware- und Softwareversionen:

- Seriennummer der Elektronik > 14678431
- Sensorsoftware ab Rev. 1.01

### Anwendungsbereich

Das Messsystem kann zur Grenzstanderfassung von Flüssigkeiten und Schüttgütern, welche den besonderen Anforderungen der Sicherheitstechnik genügt, eingesetzt werden.

Aufgrund der systematischen Eignung SC3 ist dies möglich bis:

- SIL2 in einkanaliger Architektur
- SIL3 in mehrkanaliger Architektur



Der Einsatz des Messsystems mit einem montierten Schwimmer zur sicherheitsrelevanten Öl-/Wasser-Detektion ist ausgeschlossen.

### SIL-Konformität

Die SIL-Konformität wird durch die Nachweisdokumente im Anhang belegt.

### Abkürzungen, Begriffe

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PF <sub>D 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

Weitere Abkürzungen und Begriffe sind in der IEC 61508-4 benannt.

- IEC 61508 (auch als DIN EN verfügbar)

### Relevante Normen

- Functional safety of electrical/electronic/programmable electronic safety-related systems

**Sicherheitsanforderungen**

Ausfallgrenzwerte für eine Sicherheitsfunktion, abhängig von der SIL-Klasse (IEC 61508-1, 7.6.2)

Sicherheits-Integritäts-Level	Betriebsart mit niedriger Anforderungsrate	Betriebsart mit hoher Anforderungsrate
SIL	PFD <sub>avg</sub>	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	$\geq 10^2 \dots < 10^1$	$\geq 10^{-6} \dots < 10^{-5}$

Sicherheitsintegrität der Hardware für sicherheitsbezogene Teilsysteme vom Typ B (IEC 61508-2, 7.4.3)

Anteil ungefährlicher Ausfälle	Fehlertoleranz der Hardware		
	HFT = 0	HFT = 1	HFT = 2
SFF < 60 %	nicht erlaubt	SIL1	SIL2
60 % ... < 90 %	SIL1	SIL2	SIL3
90 % ... < 99 %	SIL2	SIL3	(SIL4)
$\geq 99$ %	SIL3	(SIL4)	(SIL4)

**1.2 Projektierung**

**Sicherheitsfunktion**

Das Messsystem erzeugt an seinem Stromausgang ein dem Füllstand entsprechendes Signal zwischen 3,8 mA und 20,5 mA.

Dieses analoge Signal wird einer nachgeschalteten Auswerteinheit zugeführt, um folgende Zustände zu überwachen:

- Überschreiten eines vorgegebenen Füllstandes
- Unterschreiten eines vorgegebenen Füllstandes

Beim Erreichen des an der Auswerteinheit eingestellten Schaltpunktes wird ein Signal ausgegeben.

**Sicherer Zustand**

Der sichere Zustand ist abhängig von der Betriebsart:

	Überlaufschutz (Max.-Betrieb)	Trockenlaufschutz (Min.-Betrieb)
Sicherer Zustand	Überschreiten des Schaltpunktes	Unterschreiten des Schaltpunktes
Ausgangsstrom im sicheren Zustand	> Schaltpunkt (-3 %)	< Schaltpunkt (+3 %)
Störstrom "fail low"	< 2,3 mA	< 2,3 mA
Störstrom "fail high"	> 23,5 mA	> 23,5 mA

31813-DE-181129

Die Stromtoleranz  $\pm 3\%$  bezieht sich auf den vollen Messbereich von 16 mA.

**Fehlerbeschreibung**

Ein ungefährlicher Ausfall (safe failure) liegt vor, wenn das Messsystem ohne Anforderung des Prozesses in den definierten sicheren Zustand oder in den Störmodus wechselt.

Erkennt das interne Diagnosesystem einen Fehler, so wechselt das Messsystem in den Störmodus.

Ein gefährlicher unentdeckter Ausfall (dangerous undetected failure) liegt vor, wenn das Messsystem bei einer Anforderung des Prozesses weder in den definierten sicheren Zustand, noch in den Störmodus wechselt.

**Konfiguration der Auswerteinheit**

Liefert das Messsystem Ausgangsströme von "fail low" oder "fail high", so muss davon ausgegangen werden, dass eine Störung vorliegt.

Die Auswerteinheit muss deshalb solche Ströme als Störung interpretieren und eine geeignete Störmeldung ausgeben.

Ist dies nicht der Fall, so müssen die entsprechenden Anteile der Ausfallraten den gefährlichen Ausfällen zugeordnet werden. Somit können sich die genannten Zahlenwerte in Kapitel "Sicherheitstechnische Kennzahlen" verschlechtern.

Die Auswerteinheit muss dem SIL-Level der Messkette entsprechen.

**Betriebsart mit niedriger Anforderungsrate**

Beträgt die Anforderungsrate nicht mehr als einmal pro Jahr, so darf das Messsystem als sicherheitsrelevantes Teilsystem in der Betriebsart "low demand mode" eingesetzt werden (IEC 61508-4, 3.5.12).

Wenn das Verhältnis der internen Diagnosetrate des Messsystems zur Anforderungsrate den Wert 100 überschreitet, kann das Messsystem so behandelt werden, als wenn es eine Sicherheitsfunktion in der Betriebsart mit niedriger Anforderungsrate ausführt (IEC 61508-2, 7.4.3.2.5).

Zugehörige Kenngröße ist der Wert  $PFD_{avg}$  (average Probability of dangerous Failure on Demand). Der Wert ist abhängig vom Prüfintervall  $T_{Proof}$  zwischen den Funktionstests der Schutzfunktion.

Zahlenwerte siehe Kapitel "Sicherheitstechnische Kennzahlen".

**Betriebsart mit hoher Anforderungsrate**

Trifft "Betriebsart mit niedriger Anforderungsrate" nicht zu, so ist das Messsystem als sicherheitsrelevantes Teilsystem in der Betriebsart "high demand mode" einzusetzen (IEC 61508-4, 3.5.12).

Die Fehlertoleranzzeit des Gesamtsystems muss dabei größer sein als die Summe der Reaktionszeiten bzw. der Diagnosetestdauern aller Komponenten der Sicherheitsmesskette.

Zugehörige Kenngröße ist der Wert PFH (Ausfallrate).

Zahlenwerte siehe Kapitel "Sicherheitstechnische Kennzahlen".

**Annahmen**

Bei der Durchführung der FMEDA wurden folgende Annahmen zugrunde gelegt:

- Ausfallraten sind konstant, Abnutzung der mechanischen Teile sind nicht betrachtet
- Ausfallraten von externen Stromversorgungen sind nicht mit einberechnet
- Mehrfachfehler sind nicht betrachtet
- Die mittlere Umgebungstemperatur während der Betriebszeit beträgt 40 °C (104 °F)
- Die Umweltbedingungen entsprechen einer durchschnittlichen industriellen Umgebung
- Die Gebrauchsdauer der Bauteile liegt im Bereich von 8 bis 12 Jahren (IEC 61508-2, 7.4.7.4, Anmerkung 3)
- Die Reparaturzeit (Austausch des Messsystems) nach einem ungefährlichen Ausfall beträgt acht Stunden (MTTR = 8 h)
- Die Auswerteinheit kann "fail low"- und "fail high"-Ausfälle als Störung interpretieren und eine geeignete Störmeldung ausgeben
- Das Abtastintervall einer angeschlossenen Steuer- und Auswerteinheit beträgt max. 1 Stunde, um auf gefährliche erkennbare Ausfälle zu reagieren
- Vorhandene Kommunikationsschnittstellen (z. B. HART, I<sup>2</sup>C-Bus) werden nicht zur Übermittlung sicherheitsrelevanter Informationen benützt

### Allgemeine Hinweise und Einschränkungen

Es ist auf einen anwendungsgemäßen Einsatz des Messsystems unter Berücksichtigung von Druck, Temperatur, Dichte, Dielektrizitätszahl und chemische Eigenschaften des Mediums zu achten.

Die anwendungsspezifischen Grenzen sind einzuhalten. Die Spezifikationen der Betriebsanleitung dürfen nicht überschritten werden.

Beim Einsatz als Trockenlaufschutz ist zu beachten:

- Stab- bzw. Seilbruch vermeiden (möglicherweise sind kleinere Prooftest-Intervalle erforderlich)

### 1.3 Einstellhinweise

#### Bedienelemente

Da die Anlagenbedingungen Einfluss auf die Funktionssicherheit des Messsystems haben, sind die Bedienelemente entsprechend der Anwendung einzustellen:

- DIL-Schalter zur Messbereichsauswahl

Die Funktion der Bedienelemente ist in der Betriebsanleitung beschrieben.

### 1.4 Inbetriebnahme

#### Montage und Installation

Es sind die Montage- und Installationshinweise der Betriebsanleitung zu beachten.

Im Rahmen der Inbetriebnahme wird empfohlen, anhand einer Erstbefüllung die Sicherheitsfunktion zu überprüfen.

### 1.5 Verhalten im Betrieb und bei Störungen

#### Betrieb und Störung

Die Einstellelemente bzw. Geräteparameter dürfen im Betrieb nicht verändert werden.

Bei Veränderungen im Betrieb sind die Sicherheitsfunktionen zu beachten.

Auftretende Störmeldungen sind in der Betriebsanleitung beschrieben.

Bei festgestellten Fehlern oder Störmeldungen muss das gesamte Messsystem außer Betrieb genommen und der Prozess durch andere Maßnahmen im sicheren Zustand gehalten werden.

Ein Austausch der Elektronik ist einfach möglich und in der Betriebsanleitung beschrieben. Dabei sind die Hinweise zur Parametrierung und Inbetriebnahme zu beachten.

Werden aufgrund eines festgestellten Fehlers die Elektronik oder der gesamte Sensor ausgetauscht, so ist dies dem Hersteller zu melden (inklusive einer Fehlerbeschreibung).

## 1.6 Wiederkehrender Funktionstest

Der wiederkehrende Funktionstest dient dazu, die Sicherheitsfunktion zu überprüfen, um mögliche, nicht erkennbare gefährliche Fehler aufzudecken. Die Funktionsfähigkeit des Messsystems ist deshalb in angemessenen Zeitabständen zu prüfen. Es liegt in der Verantwortung des Betreibers, die Art der Überprüfung zu wählen. Die Zeitabstände richten sich nach dem in Anspruch genommenen PFD<sub>avg</sub>-Wert laut Tabelle und Diagramm im Abschnitt "*Sicherheitstechnische Kennzahlen*".

Bei hoher Anforderungsrate ist in der IEC 61508 kein wiederkehrender Funktionstest vorgesehen. Ein Nachweis der Funktionstüchtigkeit wird hier in der häufigeren Inanspruchnahme des Messsystems gesehen. In zweikanaligen Architekturen ist es jedoch sinnvoll, die Wirkung der Redundanz durch wiederkehrende Funktionstests in angemessenen Zeitabständen nachzuweisen.

Die Prüfung ist so durchzuführen, dass die einwandfreie Sicherheitsfunktion im Zusammenwirken aller Komponenten nachgewiesen wird. Dies ist bei einem Anfahren der Ansprechhöhe im Rahmen einer Befüllung gewährleistet. Wenn eine Befüllung bis zur Ansprechhöhe nicht praktikabel ist, so ist das Messsystem durch geeignete Simulation des Füllstandes oder des physikalischen Messeffekts zum Ansprechen zu bringen.

Die bei den Tests verwendeten Methoden und Verfahren müssen benannt und deren Eignungsgrad spezifiziert werden. Die Prüfungen sind zu dokumentieren.

Verläuft der Funktionstest negativ, muss das gesamte Messsystem außer Betrieb genommen werden und der Prozess durch andere Maßnahmen im sicheren Zustand gehalten werden.

In einer mehrkanaligen Architektur gilt dies getrennt für jeden Kanal.

## 1.7 Sicherheitstechnische Kennzahlen

Die Ausfallraten der Elektronik, der mechanischen Teile des Messwertaufnehmers, sowie des Prozessanschlusses wurden durch eine FMEDA nach IEC 61508 ermittelt. Den Berechnungen sind Bauele-

### Begründung

### Durchführung

### Grundlagen

menteausfallraten nach SN 29500 zugrunde gelegt. Alle Zahlenwerte beziehen sich auf eine mittlere Umgebungstemperatur während der Betriebszeit von 40 °C (104 °F).

Für eine höhere durchschnittliche Temperatur von 60 °C (140 °F) sollten die Ausfallraten erfahrungsgemäß mit einem Faktor von 2,5 multipliziert werden. Ein ähnlicher Faktor gilt, wenn häufige Temperaturschwankungen zu erwarten sind.

Die Berechnungen stützen sich weiterhin auf die in Kapitel "Projekti-rung" genannten Hinweise.

**Nutzungsdauer**

Nach 8 bis 12 Jahren werden sich die Ausfallraten der elektronischen Bauelemente vergrößern, wodurch sich die daraus abgeleiteten PFD- und PFH-Werte verschlechtern (IEC 61508-2, 7.4.7.4, Anmerkung 3).

**Ausfallraten**

	<b>Überlaufschutz (Max.-Betrieb)</b>	<b>Trockenlaufschutz (Min.-Betrieb)</b>
$\lambda_{sd}$	38 FIT	69 FIT
$\lambda_{su}$	245 FIT	241 FIT
$\lambda_{dd}$	130 FIT	98 FIT
$\lambda_{du}$	35 FIT	40 FIT
DC <sub>S</sub>	13 %	22 %
DC <sub>D</sub>	78 %	71 %
MTBF = MTTF + MTTR	1,97 x 10 <sup>6</sup> h	1,97 x 10 <sup>6</sup> h

**Fehlerreaktionszeit**

Diagnosetestdauer	< 360 sek.
-------------------	------------

**Einkanalige Architektur**

**Spezifische Kennzahlen**

SIL	SIL2
HFT	0
Gerätetyp	Typ B

	<b>Überlaufschutz (Max.-Betrieb)</b>	<b>Trockenlaufschutz (Min.-Betrieb)</b>
<b>SFF</b>	92 %	91 %
<b>PFD<sub>avg</sub></b>		
T <sub>Proof</sub> = 1 Jahr	< 0,016 x 10 <sup>-2</sup>	< 0,018 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 5 Jahre	< 0,078 x 10 <sup>-2</sup>	< 0,088 x 10 <sup>-2</sup>
T <sub>Proof</sub> = 10 Jahre	< 0,155 x 10 <sup>-2</sup>	< 0,177 x 10 <sup>-2</sup>
<b>PFH</b>	< 0,035 x 10 <sup>-6</sup> /h	< 0,04 x 10 <sup>-6</sup> /h

**Zeitabhängiger Verlauf von PFD<sub>avg</sub>**

Der zeitliche Verlauf von PFD<sub>avg</sub> verhält sich im Zeitraum bis 10 Jahren annähernd linear zur Betriebszeit. Die oben genannten Werte gelten nur für das T<sub>Proof</sub>-Intervall, nach dem ein wiederkehrender Funktions-test durchgeführt werden muss.

31813-DE-181129



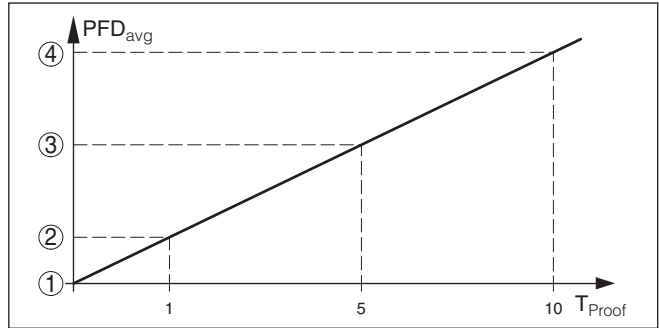


Abb. 1: Zeitabhängiger Verlauf von  $PFD_{avg}$  (Zahlenwerte siehe oben dargestellte Tabellen)

- 1  $PFD_{avg} = 0$
- 2  $PFD_{avg}$  nach 1 Jahr
- 3  $PFD_{avg}$  nach 5 Jahren
- 4  $PFD_{avg}$  nach 10 Jahren

**Mehrkanalige Architektur**

**Spezifische Kennzahlen**

Wird das Messsystem in einer mehrkanaligen Architektur eingesetzt, so sind die sicherheitstechnischen Kennzahlen der gewählten Struktur der Messkette anhand der oben angegebenen Ausfallraten speziell für die gewählte Applikation zu berechnen.

Es ist ein geeigneter Common Cause Faktor zu berücksichtigen.

## 2 Anhang



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<sub>H</sub>**

**PFD<sub>AVG</sub> 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



64 N Main St  
Sellersville, PA 18960

T-002, V3R8

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<sub>H</sub>**

**PFDAVG 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	SB1223 SB1226 SB1236 SB1237
V2.1	VEGACAP 60 T	MIN detection	SB1235 SB1226 SB1236 SB1237
V2.2	VEGACAP 60 T	MAX detection	SB1235 SB1226 SB1236 SB1237
V3.1	VEGACAP 60 Z	MIN detection	SB1235 SB1226 SB1236 SB1237
V3.2	VEGACAP 60 Z	MAX detection	SB1235 SB1226 SB1236 SB1237

Model	Fail-Safe state	$\lambda_{SD}$	$\lambda_{SU}$	$\lambda_{DD}$	$\lambda_{DU}$
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<sup>9</sup> hours)

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFDAVG 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

Page 2 of 2

Druckdatum:

# VEGA

Die Angaben über Lieferumfang, Anwendung, Einsatz und Betriebsbedingungen der Sensoren und Auswertsysteme entsprechen den zum Zeitpunkt der Drucklegung vorhandenen Kenntnissen.  
Änderungen vorbehalten

© VEGA Grieshaber KG, Schiltach/Germany 2018



31813-DE-181129

VEGA Grieshaber KG  
Am Hohenstein 113  
77761 Schiltach  
Deutschland

Telefon +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)