Safety Manual

VEGACAL Serie 60

Zweileiter 4 … 20 mA/HART

Document ID: 35593

Inhaltsverzeichnis

1 Funktionale Sicherheit 3
1.1 Allgemein 3
1.2 Projektierung 4
1.3 Geräteparametrierung 6
1.4 Inbetriebnahme 7
1.5 Verhalten im Betrieb und bei Störungen 8
1.6 Wiederkehrender Funktionstest 8
1.7 Sicherheitstechnische Kennzahlen 9

2 Anhang 11

Redaktionsstand: 2018-11-29

35593-DE-181129

1 Funktionale Sicherheit

1.1 Allgemein

Geltungsbereich

Dieses Sicherheitshandbuch gilt für Messsysteme, bestehend aus dem kapazitiven Füllstandsensor VEGACAL Serie 60 in der Ausführung Zweileiter 4 … 20 mA/HART:

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

Gültige Hardware- und Softwareversionen:

- Seriennummer der Elektronik > 14557661
- Sensorsoftware ab Rev. 1.01

Anwendungsbereich

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

Aufgrund der Betriebsbewährtheit ist dies in einer einkanaligen Architektur bis SIL2 und in einer mehrkanaligen, diversitär redundanten Architektur bis SIL3 möglich.

Der Einsatz des Messsystems in einer mehrkanaligen, homogen redundanten Architektur 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
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

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

Relevante Normen

- 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

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_{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	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

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

Anteil ungefährlicher Ausfälle	Fehlertoleranz der Hardware		
SFF	**HFT = 0**	**HFT = 1 (0)**	**HFT = 2**
< 60 %	nicht erlaubt	SIL1	SIL2
60 % … < 90 %	SIL1	SIL2	SIL3
90 % … < 99 %	SIL2	SIL3	(SIL4)
≥ 99 %	SIL3	(SIL4)	(SIL4)

Betriebsbewährtheit

Nach IEC 61511-1, Abschnitt 11.4.4 kann für betriebsbewährte Teilsysteme die Fehlertoleranz HFT um eins reduziert werden, wenn folgende Bedingungen erfüllt sind:

- Das Gerät ist betriebsbewährt
- Am Gerät können nur prozessrelevante Parameter geändert werden (z. B. Messbereich, Stromausgang bei Störung …)
- Die Veränderung dieser prozessrelevanten Parameter ist geschützt (z. B. Passwort, …)
- Die Sicherheitsfunktion erfordert kleiner SIL4

Die Beurteilung des Änderungswesens war Bestandteil des Nachweises der Betriebsbewährtheit.

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:

	Überwachung oberer Füllstand	**Überwachung unterer Füllstand**
Sicherer Zustand	Überschreiten des Schaltpunktes	Unterschreiten des Schaltpunktes
Ausgangsstrom im sicheren Zustand	> Schaltpunkt (-2 %)	< Schaltpunkt (+2 %)
Störstrom "fail low"	< 3,6 mA	< 3,6 mA
Störstrom "fail high"	> 21,5 mA	> 21,5 mA

Die Stromtoleranz ±2 % bezieht sich auf den Abgleich von 0 … 120 pF (siehe Betriebsanleitung).

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 Diagnosetestrate 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, Abnützung 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^2C-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 Geräteparametrierung

Bedientools

Da die Anlagenbedingungen Einfluss auf die Funktionssicherheit des Messsystems haben, sind die Geräteparameter entsprechend der Anwendung einzustellen.

Als Hilfsmittel hierfür sind zulässig:

- Der zum VEGACAL passende DTM in Verbindung mit einer Bediensoftware nach dem FDT/DTM-Standard, z. B. PACTware

35593-DE-181129

- Anzeige- und Bedienmodul

Hinweis:
Bitte beachten Sie, dass die DTM Collection 10/2005 oder eine neuere Version benutzt werden muss.

Messstelle einrichten

Wurde das Messsystem nicht speziell für den Einsatz in sicherheitsinstrumentierten Systemen (SIS) bestellt, so muss in der Bediensoftware in der Menüebene "*Grundstellung*" der Parameter "*Sensor nach SIL*" angewählt werden. Wird das Anzeige- und Bedienmodul verwendet, so muss in der Menüebene "*Service*" der Parameter "*SIL*" aktiviert werden.

Verhalten bei Störung

Die Parametrierung des Störstroms beeinflusst die sicherheitstechnischen Kennzahlen. Für sicherheitsrelevante Anwendungen sind deshalb nur folgende Störströme zulässig:

- fail low = < 3,6 mA (Defaultwert)
- fail high = 22 mA

Dämpfung des Ausgangssignals

Die Dämpfung des Ausgangssignals muss an die Prozesssicherheitszeit angepasst werden.

Unzulässige Betriebsarten

Die Messwertübertragung mittels HART-Signal, sowie die Betriebsart HART-Multidrop ist nicht zulässig.

Überprüfungsmöglichkeiten

Die Wirksamkeit der eingestellten Parameter muss in geeigneter Weise überprüft werden.

- Nach dem Anschluss des Gerätes springt am Ende der Einschaltphase das Ausgangssignal auf den eingestellten Störstrom
- In der Betriebsart "*Simulation*" kann der Signalstrom unabhängig vom aktuellen Füllstand simuliert werden

Zugangsverriegelung

Zum Schutz gegen ungewollte bzw. unbefugte Veränderungen müssen die eingestellten Parameter gegen unbeachsichtigten Zugriff geschützt werden:

- In der Bediensoftware den Passwortschutz aktivieren
- Am Anzeige- und Bedienmodul die PIN aktivieren

Der Zugang mittels HART-Handheld o. ä. ist nicht zulässig.

Der Schutz vor ungewollter bzw. unbefugter Bedienung kann zum Beispiel durch Versiegelung des Gehäusedeckels erfolgen.

Vorsicht:
Nach dem Rücksetzen der Werte durch einen Reset müssen alle Parameter überprüft bzw. neu eingestellt werden.

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

Begründung

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_{avg}-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.

Durchführung

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.

35593-DE-181129

In einer mehrkanaligen Architektur gilt dies getrennt für jeden Kanal.

1.7 Sicherheitstechnische Kennzahlen

Grundlagen

Die Ausfallraten der Elektronik, der mechanischen Teile des Messwertaufnehmers, sowie des Prozessanschlusses wurden durch eine FMEDA nach IEC 61508 ermittelt. Den Berechnungen sind Bauelementeausfallraten nach SN 29500 zugrunde gelegt. Alle Zahlenwerte beziehen sich auf eine mittlere Umgebungstempertur 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 "*Projektierung*" 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

Gilt für Überlaufschutz und Trockenlaufschutz:

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

Fehlerreaktionszeit

E013 (kein Messwert vorhanden)	< 10 sek.
E036/E037 (keine lauffähige Sensorsoftware)	< 1 h

Spezifische Kennzahlen

Einkanalige Architektur

SIL	SIL2
HFT	0
Gerätetyp	Typ B

Gilt für Überlaufschutz und Trockenlaufschutz:

SFF	76 %
PFD_{avg} T_{Proof} = 1 Jahr T_{Proof} = 5 Jahre	 < 0,091 x 10^{-2} < 0,182 x 10^{-2}
PFH	< 0,208 x 10^{-6}/h

Zeitabhängiger Verlauf von PFD_{avg}

Der zeitliche Verlauf von PFD_{avg} verhält sich im Zeitraum bis 10 Jahren annähernd linear zur Betriebszeit. Die oben genannten Werte gelten nur für das T_{Proof}-Intervall, nach dem ein wiederkehrender Funktionstest durchgeführt werden muss.

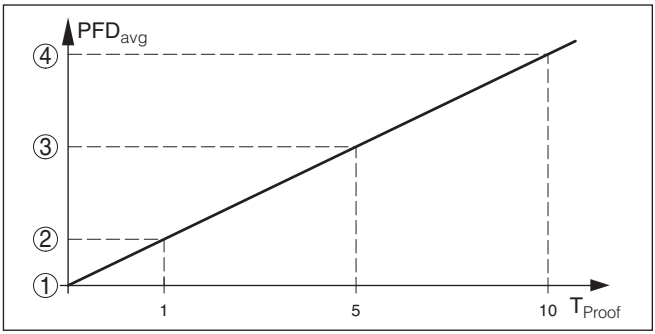

Abb. 1: Zeitabhängiger Verlauf von PFD_{avg} (Zahlenwerte siehe oben dargestellte Tabellen)

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.

Das Messsystem darf nur in einer diversitär redundanten Architektur eingesetzt werden!

2 Anhang

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

35593-DE-181129

Druckdatum:

VEGA

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

35593-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
www.vega.com