

Safety Manual

VEGAWAVE Serie 60

- Transistor (NPN/PNP)



Document ID:
32365



Vibration

Inhaltsverzeichnis

1 Funktionale Sicherheit

| | | |
|-----|--|---|
| 1.1 | Allgemein | 3 |
| 1.2 | Projektierung | 4 |
| 1.3 | Einstellhinweise | 6 |
| 1.4 | Inbetriebnahme | 7 |
| 1.5 | Verhalten im Betrieb und bei Störungen | 7 |
| 1.6 | Wiederkehrender Funktionstest | 7 |
| 1.7 | Sicherheitstechnische Kennzahlen | 8 |

2 Anhang

1 Funktionale Sicherheit

1.1 Allgemein

Geltungsbereich

Dieses Sicherheitshandbuch gilt für Messsysteme, bestehend aus dem Vibrationsgrenzscharter VEGAWAVE Serie 60 mit eingebautem Elektronikeinsatz WE60T:

VEGAWAVE 61, 62, 63

Gültige Hardware- und Softwareversionen:

- Seriennummer der Elektronik > 14190006
- Sensorsoftware ab Rev. 1.03

Einsatzbereich

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

In einer einkanaligen Architektur (1oo1D) ist dies bis SIL2 und in einer mehrkanaligen, redundanten Architektur bis SIL3 möglich.



Hinweis:

Mit einem speziellen Abgleich ab Werk ist das Messsystem auch zur Detektion von Feststoffen in Wasser geeignet (siehe "Betriebsanleitung").

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 (auch als DIN EN verfügbar)
 - 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 _{avg} | 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 ungefährl-cher 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

Die Sicherheitsfunktion dieses Messsystems ist das Erkennen und die Meldung des Zustandes des Schwingelements.

Es wird zwischen den beiden Zuständen "bedeckt" und "unbedeckt" unterschieden.

Sicherer Zustand

Der sichere Zustand ist abhängig von der Betriebsart:

| | Überlaufschutz (Max.-Betrieb) | Trockenlaufschutz (Min.-Betrieb) |
|------------------------------------|-------------------------------|----------------------------------|
| Schwingelement im sicheren Zustand | bedeckt | unbedeckt |
| Ausgangskreis im sicheren Zustand | stromlos | stromlos |

Der sichere Zustand des Messsystems ist der abgeschaltete Zustand (Ruhestromprinzip):

- C-Elektronik: Kontaktloser Schalter offen
- R-Elektronik: Relaisausgang stromlos
- T-Elektronik: Transistorausgang nicht leitend

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 Auswertereinheit

Die Auswertereinheit muss den Ausgangskreis des Messsystems unter Beachtung des Ruhestromprinzips auswerten.

Die Auswertereinheit 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.

Zahlenwert 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 Diagnosedauern aller Komponenten der Sicherheitsmesskette.

Zugehörige Kenngröße ist der Wert PFH (Ausfallrate).

Zahlenwert 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 beurteilt den Ausgangskreis des Messsystems nach dem Ruhestromprinzip
- Das Abtastintervall einer angeschlossenen Steuer- und Auswerteinheit beträgt max. 1 Stunde, um auf gefährliche erkennbare Ausfälle zu reagieren
- Vorhandene Kommunikationsschnittstellen (z. B. HART, I²C-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 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:

- Anhaftung von Füllgut am Schwingsystem vermeiden (möglichst sind kleinere Proofest-Intervalle notwendig)
- Gabelversion: Korngröße des Füllgutes > 15 mm (0.6 in) vermeiden

1.3 Einstellhinweise

Bedienelemente

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

- Potentiometer zur Schaltpunktanpassung
- DIL-Schalter zur Betriebsartenumschaltung

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

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.

In der zweikanaligen Architektur (1oo2D) gilt dies getrennt für beide Kanäle.

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 Bauelementenausfallraten 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 im Kapitel "*Projektion*" 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

| | Überlaufschutz (Max.-Betrieb) | Trockenlaufschutz (Min.-Betrieb) |
|--------------------|--------------------------------------|---|
| λ_{sd} | 0 FIT | 0 FIT |
| λ_{su} | 487 FIT | 466 FIT |
| λ_{dd} | 124 FIT | 135 FIT |
| λ_{du} | 30 FIT | 40 FIT |
| DC _S | 0 % | 0 % |
| DC _D | 81 % | 77 % |
| MTBF = MTTF + MTTR | 1,52 x 10 ⁶ h | 1,52 x 10 ⁶ h |

Fehlerreaktionszeit

| | |
|-------------------|------------|
| Diagnosetestdauer | < 100 sek. |
|-------------------|------------|

Einkanalige Architektur (1oo1D)

Spezifische Kennzahlen

| | |
|-----------|-------|
| SIL | SIL2 |
| HFT | 0 |
| Gerätetyp | Typ B |

| | Überlaufschutz (Max.-Betrieb) | Trockenlaufschutz (Min.-Betrieb) |
|-------------------------------|-------------------------------|----------------------------------|
| SFF | 95 % | 94 % |
| PFD_{avg} | | |
| T _{Proof} = 1 Jahr | < 0,013 x 10 ⁻² | < 0,018 x 10 ⁻² |
| T _{Proof} = 5 Jahre | < 0,066 x 10 ⁻² | < 0,088 x 10 ⁻² |
| T _{Proof} = 10 Jahre | < 0,131 x 10 ⁻² | < 0,177 x 10 ⁻² |
| PFH | < 0,03 x 10 ⁻⁶ /h | < 0,04 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.

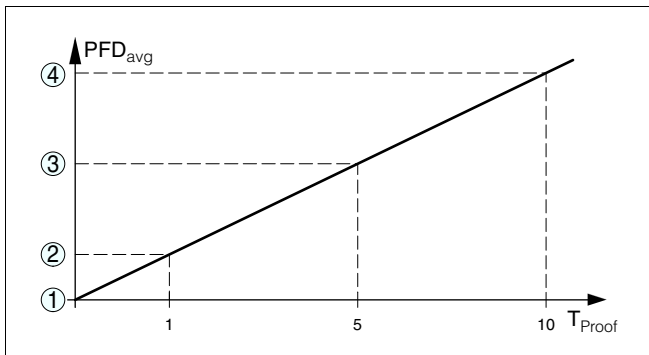


Abb. 1: Zeitabhängiger Verlauf von PFD_{avg} (Zahlenwerte siehe oben dargestellte Tabellen)

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

Spezifische Kennzahlen

Mehrkanalige Architektur

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



CERTIFICATE

VEGA 100981C P0011 C001.1



exida Certification S.A. hereby confirms that the

VEGAVIB / VEGAWAVE 60 Level Switch

Output C, R, T, N, Z

Product Version: See listing in assessment report

VEGA Grieshaber KG

Schiltach, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000

Parts 1 - 3, and meets requirements providing a level of integrity to

Systematic Integrity : SIL 3 Capable

Random Integrity : SIL 2 @ HFT=0
SIL 3 @ HFT=1

Safety function

The VEGAVIB / VEGAWAVE 60 will de-energize its output (C,R,T,N) or set current (Z) to fail-safe output when a level goes above (or below) the trip point within the safety accuracy.

Application Restrictions

The unit must be properly designed and validated in a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor

Certifying Assessor

Date: 11 Jan 2011

exida Certification SA, Nyon, Switzerland



CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証



Systematic Integrity: SIL 3 Capable

SIL 3 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 the statement.

Random Integrity: SIL 2 @ HFT=0
 SIL 3 @ HFT=1

Summary for the VEGAVIB / VEGAWAVE 60 Level Switch:

Type B device

IEC 61508 failure rates in FIT [$\approx 10^{-9}/h$]

| Model | Fail-Safe state | λ_{SD} | λ_{SU} | λ_{DD} | λ_{DU} |
|-------------------|------------------|----------------|----------------|----------------|----------------|
| C Max / High trip | Out De-energized | 0 | 506 | 124 | 41 |
| C Min / Low trip | Out De-energized | 0 | 481 | 135 | 56 |
| R Max / High trip | Out De-energized | 0 | 586 | 124 | 27 |
| R Min / Low trip | Out De-energized | 0 | 565 | 135 | 37 |
| T Max / High trip | Out De-energized | 0 | 487 | 124 | 30 |
| T Min / Low trip | Out De-energized | 0 | 466 | 135 | 40 |
| N Max / High trip | Out < 1.0 mA | 12 | 160 | 390 | 47 |
| N Min / Low trip | Out < 1.0 mA | 36 | 155 | 366 | 52 |
| Z Max / High trip | Out > 12.5 mA | 49 | 387 | 163 | 18 |
| Z Min / Low trip | Out < 11.5 mA | 39 | 352 | 182 | 43 |

All failure rates are given in FIT = $10^{-9}/h$

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH / $PF_{D,AVG}$ considering the architecture, 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 subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory part of this certificate:

VEGA 03/05-08 R005 V3R1 Assessment Report

Safety manuals VEGAVIB / VEGAWAVE 60, all with versions:

C: 32002 / 32363 R: 32003 / 32364 T: 32004 / 32365

N: 32005 / 32366 Z: 32006 / 32367

exida Certification SA, Nyon, Switzerland

info@exidacert.ch

Page 2 (2)

The holder of this certificate
may use this mark.



CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証



Druckdatum:

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



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

© VEGA Grieshaber KG, Schiltach/Germany 2011