Safety Manual

VEGAMET 391

4 … 20 mA-Steuergerät

Mit SIL-Qualifikation

Document ID: 40888

Inhaltsverzeichnis

Redaktionsstand: 2022-07-05

40888-DE-220705

1 Dokumentensprache

DE	Das vorliegende *Safety Manual* für Funktionale Sicherheit ist verfügbar in den Sprachen Deutsch, Englisch, Französisch und Russisch.
EN	The current *Safety Manual* for Functional Safety is available in German, English, French and Russian language.
FR	Le présent *Safety Manual* de sécurité fonctionnelle est disponible dans les langues suivantes: allemand, anglais, français et russe.
RU	Данное руководство по функциональной безопасности *Safety Manual* имеется на немецком, английском, французском и русском языках.

40888-DE-220705

2 Geltungsbereich

2.1 Geräteausführung

Dieses Sicherheitshandbuch gilt für das Steuergerät
VEGAMET 391 mit SIL-Qualifikation

Gültige Version:

- ab Hardwareversion 1.0.0
- ab Softwareversion 1.0.0

2.2 Anwendungsbereich

Das Steuergerät kann in Kombination mit einem 4 … 20 mA-Messumformer zur Messung von Füllstand, Grenzstand und anderen Prozessgrößen als Messsystem in einer sicherheitsrelevanten Schutzfunktion gemäß IEC 61508 in den Betriebsarten *low demand mode* und *high demand mode* eingesetzt werden:

Aufgrund der systematischen Eignung SC2 ist dies möglich bis:

- SIL2 in einkanaliger Architektur
- SIL3 in mehrkanaliger Architektur nur mit diversitärer Redundanz

Hierzu sind folgende Schnittstellen verwendbar:

- Sensoreingang: 4 … 20 mA mit Messumformerspeisung
- Relaisausgang: Relais 3 und 4, NO-Kontakt[1)]
- Stromausgang: 4 … 20 mA

SIL

Nicht zulässig für sicherheitsrelevante Anwendungen:

- Digitaleingänge 1 und 2
- Relaisausgänge 1 und 2
- Vorhandene Kommunikationsschnittstellen (z. B. HART, USB)

2.3 SIL-Konformität

Die SIL-Konformität wurde durch *exida* Certification LLC nach IEC 61508 unabhängig beurteilt und zertifiziert.[2)]

1) NO = Normal Open
2) Nachweisdokumente siehe "Anhang"

3 Projektierung

3.1 Sicherheitsfunktion

Der vom Steuergerät gespeiste Messumformer erzeugt ein der Prozessgröße proportionales Signal zwischen 3,8 und 20,5 mA.

Sicherheitsfunktion Relaisausgang
Abhängig von diesem analogen Signal und den eingestellten Schaltpunkten werden ein oder zwei Relais zur Grenzwertüberwachung geschaltet.

Sicherheitsfunktion Stromausgang
Weiterhin kann dieses analoge Signal einer nachgeschalteten Auswerteeinheit (z. B. SSPS) zugeführt werden. Die dort eingestellten Schaltpunkte können zur Grenzwertüberwachung benutzt werden.

Sicherheitstoleranz

Wird vom internen Diagnosesystem eine durch Hardware-Fehler verursachte Messwertverfälschung von mehr als 2 % entdeckt, so werden die Ausgangssignale auf den Zustand Störung gesetzt.

Dies muss bei der Auslegung der Sicherheitsfunktion berücksichtigt werden.

3.2 Sicherer Zustand

Sicherer Zustand Relaisausgang
Der sichere Zustand am Relaisausgang ist der geöffnete Schließerkontakt. Für die Sicherheitsfunktion darf deshalb nur der Schließerkontakt (NO-Kontakt) verwendet werden (Ruhestromprinzip).

Sicherer Zustand Stromausgang
Der sichere Zustand des Stromausganges ist abhängig von der Betriebsart und von der am Sensor eingestellten Kennlinie.

	Überwachung oberer Grenzwert	**Überwachung unterer Grenzwert**
Steigende Kennlinie: 4 mA = 0 %; 20 mA = 100 %	Ausgangsstrom > Schaltpunkt -334 µA	Ausgangsstrom < Schaltpunkt +334 µA
Fallende Kennlinie: 20 mA = 0 % 4 mA = 100 %	Ausgangsstrom < Schaltpunkt +334 µA	Ausgangsstrom > Schaltpunkt -334 µA

Ausgangssignale im Störmode

Relaisausgang
- Schließerkontakt ist geöffnet

Stromausgang
- "fail low" ≤ 3,6 mA
- "fail high" > 21 mA

3.3 Voraussetzungen zum Betrieb

Hinweise und Einschränkungen

- Es ist auf einen anwendungsgemäßen Einsatz des Messsystems zu achten. Die anwendungsspezifischen Grenzen sind einzuhalten
- Die Spezifikationen laut Angaben der Betriebsanleitung, insbesondere die Strombelastung der Ausgangskreise, sind innerhalb der genannten Grenzen zu halten
- Zur Vermeidung des Verschweißens der Relaiskontakte sind diese durch eine externe Sicherung, die bei 60 % der maximalen Kontaktstrombelastung auslöst, abzusichern
- Vorhandene Kommunikationsschnittstellen (z. B. HART, USB) werden nicht zur Übermittlung des sicherheitsrelevanten Messwertes benützt
- Es sind die Hinweise in Kapitel "*Sicherheitstechnische Kennzahlen*", Abschnitt "*Ergänzende Informationen*" zu beachten
- Alle Bestandteile der Messkette müssen dem vorgesehenen "*Safety Integrity Level (SIL)*" entsprechen

4 Sicherheitstechnische Kennzahlen

4.1 Allgemeine Kennzahlen für alle Applikationen

Kenngröße gemäß IEC 61508	Wert
Safety Integrity Level	SIL2
Hardwarefehlertoleranz	HFT = 0
Gerätetyp	Typ B
Betriebsart	Low demand mode/High demand mode
MTTR	8 h
MTBF = MTTF + MTTR [3]	0,38 x 10^6 h (44 Jahre)
Diagnosetestintervall[4]	< 4 min
Anforderungsrate	> 50 h

4.2 Spezifische Kennzahlen für Applikation 1

Ein Relaisausgang

Ein Relais zur Ansteuerung eines Aktors für die Überwachung eines Grenzwertes (z. B. Überfüllsicherung oder Trockenlaufschutz).

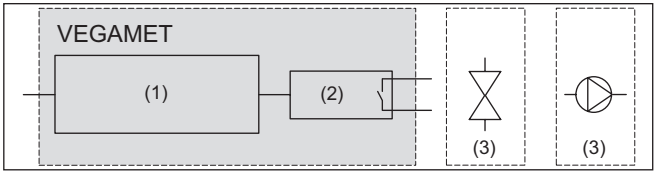

Abb. 1: Struktur der Applikation

1 Stromeingang und Auswertelektronik
2 Relais 3 oder Relais 4
3 Aktor

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0 FIT	716 FIT	0 FIT	24 FIT	96 %	94 %

PFD_{AVG}	0,0254 x 10^{-2}	(T1 = 1 Jahr)
PFD_{AVG}	0,0342 x 10^{-2}	(T1 = 2 Jahre)
PFD_{AVG}	0,0604 x 10^{-2}	(T1 = 5 Jahre)
PFH	0,0238 x 10^{-6} 1/h	

4.3 Spezifische Kennzahlen für Applikation 2

Zwei Relaisausgänge

Zwei Relais zur Ansteuerung von zwei Aktoren für die Überwachung von zwei Grenzwerten (z. B. Bereichsüberwachung).

[3] MTBF: Einschließlich Fehlern, die außerhalb der Sicherheitsfunktion liegen
[4] Zeit, in der alle internen Diagnosen mindestens einmal ausgeführt werden.

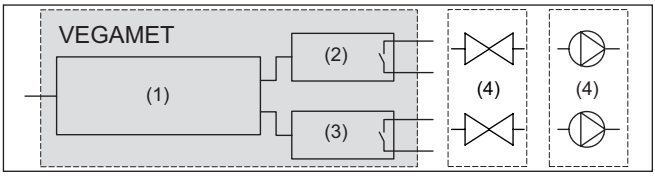

Abb. 2: Struktur der Applikation

1 Stromeingang und Auswertelektronik
2 Relais 3
3 Relais 4
4 Aktoren

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0 FIT	758 FIT	0 FIT	25 FIT	96 %	94 %

PFD_{AVG}	0,0271 x 10^{-2}	(T1 = 1 Jahr)
PFD_{AVG}	0,0364 x 10^{-2}	(T1 = 2 Jahre)
PFD_{AVG}	0,0643 x 10^{-2}	(T1 = 5 Jahre)
PFH	0,0253 x 10^{-6} 1/h	

4.4 Spezifische Kennzahlen für Applikation 3

Stromausgang

Ein Stromausgang zur Ansteuerung einer nachgeschalteten Auswerteinheit (z. B. SSPS).

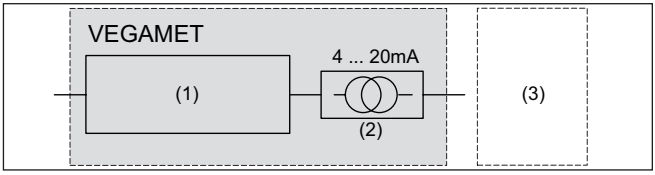

Abb. 3: Struktur der Applikation

1 Stromeingang und Auswertelektronik
2 Stromausgang
3 Nachgeschaltete Auswerteinheit

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0 FIT	0 FIT	860 FIT	23 FIT	97 %	97 %

PFD_{AVG}	0,0276 x 10^{-2}	(T1 = 1 Jahr)
PFD_{AVG}	0,0357 x 10^{-2}	(T1 = 2 Jahre)
PFD_{AVG}	0,0599 x 10^{-2}	(T1 = 5 Jahre)
PFH	0,0227 x 10^{-6} 1/h	

40888-DE-220705

4.5 Kennzahlen gemäß ISO 13849-1

Abgeleitet von den sicherheitstechnischen Kennzahlen ergeben sich gemäß ISO 13849-1 (Maschinensicherheit) folgende Kennzahlen:[5)]

Kenngröße gemäß ISO 13849-1	Wert für Applikation 1	Wert für Applikation 2	Wert für Applikation 3
$MTTF_d$	243 Jahre	236 Jahre	129 Jahre
DC	94 %	94 %	97 %
Performance Level	4,68 x 10^{-7} 1/h	4,83 x 10^{-7} 1/h	8,83 x 10^{-7} 1/h

4.6 Ergänzende Informationen

Ermittlung der Ausfallraten

Die Ausfallraten des Gerätes wurden durch eine FMEDA nach IEC 61508 ermittelt. Den Berechnungen sind Ausfallraten der Bauelemente nach **exida Profile 1** mit folgenden Daten zugrunde gelegt:

Profile according to IEC 60654-1	B2
Ambient Temperature (Average, external)	30 °C
Ambient Temperature (Mean, in Box)	60 °C
Temperature Cycle	5 °C/365 Tage

Annahmen der FMEDA

- Die Ausfallraten sind konstant. Hierbei ist auf die nutzbare Gebrauchsdauer der Bauelemente gemäß IEC 61508-2 zu achten.
- Mehrfachausfälle sind nicht betrachtet
- Abnützung von mechanischen Teilen sind nicht betrachtet
- Ausfallraten von externen Stromversorgungen sind nicht mit einberechnet
- Die Umweltbedingungen entsprechen einer durchschnittlichen industriellen Umgebung
- Zur Vermeidung des Verschweißens der Relaiskontakte sind diese durch eine externe Sicherung abgesichert

Berechnung von PFD_{AVG}

Die oben angegebenen Werte für PFD_{AVG} wurden für eine 1oo1-Architektur folgendermaßen berechnet:

$$PFD_{AVG} = \frac{PTC \times \lambda_{DU} \times T1}{2} + \lambda_{DD} \times MTTR + \frac{(1 - PTC) \times \lambda_{DU} \times LT}{2}$$

Verwendete Parameter:

- T1 = Proof Test Interval
- PTC (Applikation 1 & 2) = 84 %
- PTC (Applikation 3) = 81 %
- LT = 10 Jahre
- MTTR = 8 h

Randbedingungen bezüglich Messumformer

Der verwendete Messumformer muss einen Störstrom ausgeben, wenn er mit einer Spannung außerhalb seines spezifizierten Spannungsbereichs versorgt wird.

[5)] Die ISO 13849-1 war nicht Gegenstand der Zertifizierung des Gerätes.

Randbedingungen bezüglich Konfiguration der Auswerteinheit

Eine nachgeschaltete Steuer- und Auswerteinheit muss folgende Eigenschaften bieten:

- Die Ausfallsignale des Messsystems werden nach dem Ruhestromprinzip beurteilt
- "*fail low*"- und "*fail high*"-Signale werden als Störung interpretiert, worauf der sichere Zustand eingenommen werden muss!

Ist dies nicht der Fall, so müssen die entsprechenden Anteile der Ausfallraten den gefährlichen Ausfällen zugeordnet und die in Kapitel "*Sicherheitstechnische Kennzahlen*" genannten Werte neu ermittelt werden!

Mehrkanalige Architektur

In mehrkanaligen Systemen für SIL3-Anwendungen darf dieses Messsystem nur mit diversitärer Redundanz eingesetzt werden.

Die sicherheitstechnischen Kennzahlen sind speziell für die gewählte Struktur der Messkette anhand der angegebenen Ausfallraten zu berechnen. Dabei ist ein geeigneter Common Cause Faktor (CCF) zu berücksichtigen (siehe IEC 61508-6, Anhang D).

5 Inbetriebnahme

5.1 Geräteparametrierung

Hilfsmittel

Zur Parametrierung der Sicherheitsfunktion sind folgende Bedieneinheiten zulässig:

- Die integrierte Anzeige- und Bedieneinheit zur Vor-Ort-Bedienung
- Der zum VEGAMET 391 passende DTM in Verbindung mit einer Bediensoftware nach dem FDT/DTM-Standard, z. B. PACTware
- Bitte beachten Sie, dass die DTM Collection 06/2011 oder eine neuere Version erforderlich ist.

Die Vorgehensweise der Parametrierung ist in der Betriebsanleitung beschrieben.

SIL Die Änderung sicherheitsrelevanter Parameter ist nur bei aktiver Verbindung zum Gerät möglich (Online-Modus).

Sicherheitsrelevante Parameter

Zum Schutz gegen ungewollte bzw. unbefugte Bedienung müssen die eingestellten Parameter gegen unbeabsichtigten Zugriff geschützt werden. Aus diesem Grund wird das Gerät im verriegelten Zustand ausgeliefert. Die PIN im Auslieferungszustand lautet "0000".

Dem Gerät liegt bei Lieferung eine Übersicht bei, die alle sicherheitsrelevanten Parameter und deren Wert im Auslieferungszustand auflistet. Anhand der Seriennummer steht diese Liste auch über "www.vega.com", "*Suche*" zum Download zur Verfügung.

Sichere Parametrierung

Um bei der Parametrierung mit nicht sicherer Bedienumgebung mögliche Fehler zu vermeiden bzw. aufzudecken, wird ein Verifizierungsverfahren angewandt, das es ermöglicht, die sicherheitsrelevanten Parameter zu überprüfen.

Folgende Schritte werden bei der Parametrierung durchlaufen:

- Bedienung freigeben
- Parameter ändern
- Bedienung sperren und geänderte Parameter verifizieren

Der genaue Ablauf ist in der Betriebsanleitung beschrieben.

Mit der Bediensoftware können die aktuellen sicherheitsrelevanten Parameter ausgedruckt bzw. gespeichert werden. Diese Funktion ist jedoch nur bei aktiver Verbindung des Gerätes zur Bediensoftware (Online-Modus) möglich.

SIL Das Gerät wird im verriegelten Zustand ausgeliefert!

SIL Zur Verifizierung werden ausschließlich die geänderten sicherheitsrelevanten Parameter dargestellt. Die Verifizierungstexte werden entweder in Deutsch oder bei allen anderen Menüsprachen in Englisch zur Verfügung gestellt.

Unsicherer Gerätezustand

⚠ **Warnung:**
Ist das Gerät entriegelt, so muss die Sicherheitsfunktion als unsicher betrachtet werden. Dies gilt solange, bis die Parametrierung ordnungsgemäß abgeschlossen wurde.

Gegebenenfalls müssen andere Maßnahmen ergriffen werden, um die Sicherheitsfunktion aufrecht zu erhalten.

Unvollständiger Ablauf der Geräteparametrierung

Warnung:
Wenn der beschriebene Ablauf der Parametrierung nicht vollständig durchlaufen wird (z. B. durch Abbruch oder Stromausfall), so bleibt das Gerät im unsicheren und unverriegelten Gerätezustand.

Gerätereset

Warnung:
Bei einem Reset auf Basiseinstellung werden alle sicherheitsrelevanten Parameter auf Werkseinstellung zurückgesetzt. Danach müssen alle sicherheitsrelevanten Parameter überprüft bzw. neu eingestellt werden.

5.2 Montage und Installation

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

Im Rahmen der Inbetriebnahme wird empfohlen, z. B. anhand einer Erstbefüllung oder durch Simulation des Eingangssignales die Sicherheitsfunktion zu überprüfen. Hierzu kann auch die in Kapitel "*Wiederkehrender Funktionstest*" beschriebene Vorgehensweise verwendet werden.

6 Verhalten im Betrieb und bei Störungen

6.1 Allgemein

Das Verhalten im Betrieb und bei Störung sowie das entsprechende Ausfallsignal sind in der Betriebsanleitung beschrieben.

Das Auftreten eines gefahrbringenden, unerkannten Ausfalls ist dem Hersteller zu melden (inklusive einer Fehlerbeschreibung).

6.2 Verhalten im Fehlerfall

Interne Diagnosen

Das Gerät wird permanent durch ein internes Diagnosesystem überwacht. Wird eine Funktionsstörung erkannt, so wechseln die entsprechenden Ausgangssignale in den sicheren Zustand (siehe Abschnitt "*Sicherer Zustand*").

Dieser Zustand wird für mindestens 5 Sekunden beibehalten. Wird kein Fehler mehr erkannt, so wird die Sicherheitsfunktion wieder korrekt ausgeführt.

Das Diagnosetestintervall ist in Kapitel "*Sicherheitstechnische Kennzahlen*" angegeben.

Fehlerreaktionszeit sicherheitsrelevanter Ausfallsignale

Je nach Fehlerart wird ein entsprechendes Ausfallsignal mit folgender Reaktionszeit ausgegeben:

Ausfallsignal im Betrieb	Reaktionszeit
E012 Hardwarefehler Sensoreingang	< 1 min
E014 Leitungskurzschluss Sensoreingang	< 5 s
E015 Leitungsbruch Sensoreingang	< 5 s
E034 EEPROM-CRC-Fehler	< 2 s
E035 Programmspeicher-CRC-Fehler	< 1 min
E037 RAM defekt	< 4 min
E040 Hardware defekt	< 4 min
E080 Microcontroller defekt	< 4 min
E113 Hardwarefehler Stromausgang	< 1 min
E117 Pumpe meldet Störung	Parametrierbar
E125 Geräteelektroniktemperatur	1 h

Ausfallsignal beim Parametrieren	Reaktionszeit
E017 Abgleichspanne zu gering	< 5 s
E021 Skalierspanne zu gering	< 5 s
E062 Pulswertigkeit zu klein	< 5 s
E110 Relaisschaltpunkte: Spanne zu klein	< 5 s
E111 Relaisschaltpunkte vertauscht	< 5 s
E115 Verhalten bei Störung fehlerhaft	< 5 s
E116 Ausgangsbetriebsart fehlerhaft	< 5 s

7 Wiederkehrender Funktionstest

7.1 Allgemein

Der wiederkehrende Funktionstest (*Proof Test*) dient dazu, die Sicherheitsfunktion zu überprüfen, um mögliche gefährliche, unentdeckte Fehler zu erkennen. 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} (siehe Kapitel "*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.

Zur Dokumentation der Funktionstests kann das Prüfprotokoll im Anhang verwendet werden.

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.

Werkzeuge

- Geeignetes kalibriertes Strommessgerät (Genauigkeit besser ±0,1 mA)
- Geeignetes kalibriertes Widerstandsmessgerät
- Gegebenenfalls Simulator für Sensorstrom (passive Stromquelle)

Vorbereitung

- Sicherheitsfunktion feststellen (Betriebsart, Schaltpunkte)
- Bei Bedarf Gerät aus der Sicherheitskette entfernen und Sicherheitsfunktion anderweitig aufrechterhalten

Unsicherer Gerätezustand

Warnung:
Während des Funktionstests muss die Sicherheitsfunktion als unsicher betrachtet werden. Es ist zu berücksichtigen, dass der Funktionstest Auswirkungen auf nachgeschaltete Geräte hat.

Gegebenenfalls müssen andere Maßnahmen ergriffen werden, um die Sicherheitsfunktion aufrecht zu erhalten.

Nach Abschluss des Funktionstests muss der für die Sicherheitsfunktion spezifizierte Zustand wieder hergestellt werden.

7.2 Test Applikation 1 - Ein Relaisausgang

Ablauf für Betriebsart Überfüllsicherung

1. Sensorstrom unterhalb des unteren Relaisschaltpunktes "Lo" einstellen
2. Sensorstrom unmittelbar oberhalb des oberen Relaisschaltpunktes "Hi" einstellen

Ablauf für Betriebsart Trockenlaufschutz

1. Sensorstrom oberhalb des oberen Relaisschaltpunktes "Hi" einstellen
2. Sensorstrom unmittelbar unterhalb des unteren Relaisschaltpunktes "Lo" einstellen

40888-DE-220705

Erwartetes Ergebnis

Verwendeter SIL-Relaiskontakt muss bei Punkt 1 geschlossen und bei Punkt 2 innerhalb der Sicherheitstoleranz (+334 µA) geöffnet sein.

Deckungsgrad der Prüfung

PTC = 84 %

7.3 Test Applikation 2 - Zwei Relaisausgänge für Bereichsüberwachung

Ablauf

1. Mindestens drei Werte des Sensorstromes innerhalb der Bereichsgrenzen einstellen
2. Sensorstrom unmittelbar oberhalb des oberen Relaisschaltpunktes "Hi" für die obere Bereichsgrenze einstellen
3. Sensorstrom unmittelbar unterhalb des unteren Relaisschaltpunktes "Lo" für die untere Bereichsgrenze einstellen

Erwartetes Ergebnis

Punkt 1: Beide SIL-Relaiskontakte müssen geschlossen sein.

Punkt 2: Der SIL-Relaiskontakt für die Überwachung der oberen Bereichsgrenze muss innerhalb der Sicherheitstoleranz (+334 µA) geöffnet sein.

Punkt 3: Der SIL-Relaiskontakt für die Überwachung der unteren Bereichsgrenze muss innerhalb der Sicherheitstoleranz (+334 µA) geöffnet sein.

Deckungsgrad der Prüfung

PTC = 84 %

7.4 Test Applikation 3 - Stromausgang

Ablauf

Mindestens fünf Werte des Sensorstromes innerhalb des Messbereiches einstellen.

Erwartetes Ergebnis

Alle gemessenen Stromausgangswerte weichen um weniger als 2 % (+334 µA) vom erwarteten Ausgangsstrom ab.

Deckungsgrad der Prüfung

PTC = 81 %

8 Anhang A: Prüfprotokoll Funktionstest

Identifikation	
Firma/Prüfer	
Anlage/Geräte-TAG	
Messstellen-TAG	
Gerätetyp/Bestellcode	
Geräte-Seriennummer	
Datum Inbetriebnahme	
Datum letzter Funktionstest	

Eingestellte Geräteparameter der Sicherheitsfunktion		
Verwendete sicherheitsrelevante Ausgänge	**O** Relais 3 **O** Relais 4 **O** Stromausgang	
Eingestellte Betriebsart Relais 3	**O** Überfüllsicherung **O** Trockenlaufschutz	
Eingestellter oberer Schaltpunkt Relais 3 "Hi"	mA	
Eingestellter unterer Schaltpunkt Relais 3 "Lo"	mA	
Eingestellte Betriebsart Relais 4	**O** Überfüllsicherung **O** Trockenlaufschutz	
Eingestellter oberer Schaltpunkt Relais 4 "Hi"	mA	
Eingestellter unterer Schaltpunkt Relais 4 "Lo"	mA	

Testergebnis 1 Relaisausgänge

	Relaisausgang 3			**Relaisausgang 4**		
Schaltpunkt	**Gemessener Sensorstrom**	**Zustand Relais 3**	**Testergebnis**	**Gemessener Sensorstrom**	**Zustand Relais 4**	**Testergebnis**
"Hi“	mA			mA		
"Hi“	mA			mA		
"Hi“	mA			mA		
"Lo"	mA			mA		
"Lo"	mA			mA		
"Lo"	mA			mA		

Testergebnis 2 Stromausgang

Simulierter Sensorstrom		**Erwarteter Ausgangsstrom**	**Gemessener Ausgangsstrom**	**Testergebnis**
Sensorstrom 1	mA	mA	mA	
Sensorstrom 2	mA	mA	mA	
Sensorstrom 3	mA	mA	mA	

Simulierter Sensorstrom		Erwarteter Ausgangsstrom	Gemessener Ausgangsstrom	Testergebnis
Sensorstrom 4	mA	mA	mA	
Sensorstrom 5	mA	mA	mA	

Bestätigung

Datum: Unterschrift:

9 Anhang B: Begriffsdefinitionen

Abkürzungen

SIL	Safety Integrity Level (SIL1, SIL2, SIL3, SIL4)
SC	Systematic Capability (SC1, SC2, SC3, SC4)
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{AVG}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of a dangerous failure per hour (Ed.2)
FMEDA	Failure Mode, Effects and Diagnostics Analysis
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
λ_{SD}	Rate for safe detected failure
λ_{SU}	Rate for safe undetected failure
λ_S	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
λ_{DD}	Rate for dangerous detected failure
λ_{DU}	Rate for dangerous undetected failure
λ_H	Rate for failure, who causes a high output current (> 21 mA)
λ_L	Rate for failure, who causes a low output current (≤ 3.6 mA)
λ_{AD}	Rate for diagnostic failure (detected)
λ_{AU}	Rate for diagnostic failure (undetected)
DC	Diagnostic Coverage
PTC	Proof Test Coverage (Diagnostic coverage for manual proof tests)
T1	Proof Test Interval
LT	Useful Life Time
MTBF	Mean Time Between Failure = MTTF + MTTR
MTTF	Mean Time To Failure
MTTR	IEC 61508, Ed1: Mean Time To Repair IEC 61508, Ed2: Mean Time To Restoration
$MTTF_d$	Mean Time To dangerous Failure (ISO 13849-1)
PL	Performance Level (ISO 13849-1)

10 Anhang C: SIL-Konformität

The manufacturer may use the mark:

Revision 2.0 February 26, 2015

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat

Zertifikat / 合格証

VEGA 100183C P0011 C003

exida hereby confirms that the:

VEGAMET 391
Signal Conditioning Instrument

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 2 (SIL 2 Capable)

Random Capability: Type B Device

SIL 2 @ HFT = 0

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The VEGAMET 391 will read the analog input and control its output(s) in accordance to the parameter settings 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

40888-DE-220705

Certificate / Certificat / Zertifikat / 合格証

VEGA 100183C P0011 C003

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Device

SIL 2 @ HFT = 0

PFD_{AVG} and Architecture Constraints must be verified for each application

VEGAMET 391 Signal Conditioning Instrument

Systematic Capability:

The Product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. 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.

Configuration	λ_S	λ_{DD}	λ_{DU}
One relay output	716	0	24
Two relay outputs	758	0	25
Two relays in series connection	758	0	24
Current output	0	860	23
Current output and one relay	291	620	24

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 1001-83-R1-C R004 V1R2

Safety Manual: VEGAMET 391 40888

exida®

64 N Main St
Sellersville, PA 18960

T-062, V1R7

40888-DE-220705

Druckdatum:

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

40888-DE-220705

VEGA Grieshaber KG
Am Hohenstein 113
77761 Schiltach
Deutschland

Telefon +49 7836 50-0
E-Mail: info.de@vega.com
www.vega.com