

# Safety Manual

## VEGAPULS 6X

Zweileiter 4 ... 20 mA/HART

Mit SIL-Qualifikation



Document ID: 66494



# VEGA

## Inhaltsverzeichnis

<b>1</b>	<b>Dokumentensprache .....</b>	<b>3</b>
<b>2</b>	<b>Geltungsbereich.....</b>	<b>4</b>
2.1	Geräteausführung .....	4
2.2	Anwendungsbereich.....	4
2.3	SIL-Konformität .....	4
<b>3</b>	<b>Projektierung.....</b>	<b>5</b>
3.1	Sicherheitsfunktion.....	5
3.2	Sicherer Zustand.....	5
3.3	Voraussetzungen zum Betrieb.....	5
<b>4</b>	<b>Sicherheitstechnische Kennzahlen.....</b>	<b>7</b>
4.1	Kennzahlen gemäß IEC 61508 für Füllstandmessung.....	7
4.2	Kennzahlen gemäß ISO 13849-1 für Füllstandmessung .....	7
4.3	Ergänzende Informationen .....	8
<b>5</b>	<b>In Betrieb nehmen.....</b>	<b>10</b>
5.1	Allgemein .....	10
5.2	Geräteparametrierung.....	10
<b>6</b>	<b>Diagnose und Service .....</b>	<b>12</b>
6.1	Verhalten bei Ausfall.....	12
6.2	Reparatur .....	12
<b>7</b>	<b>Wiederholungsprüfung .....</b>	<b>13</b>
7.1	Allgemein .....	13
7.2	Prüfung 1: Ohne Überprüfung der Prozessgröße .....	13
7.3	Prüfung 2: Mit Überprüfung der Prozessgröße .....	14
<b>8</b>	<b>Anhang A: Prüfprotokoll.....</b>	<b>16</b>
<b>9</b>	<b>Anhang B: Begriffsdefinitionen .....</b>	<b>17</b>

## 1 Dokumentensprache

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

## 2 Geltungsbereich

### 2.1 Geräteausführung

Dieses Sicherheitshandbuch gilt für den Radarsensor

#### VEGAPULS 6X

Elektroniktypen:

- Zweileiter 4 ... 20 mA/HART
- Zweileiter 4 ... 20 mA/HART mit Überspannungsschutz

Jeweils mit Funktionaler Sicherheit SIL (IEC 61508)

Gültige Versionen:

- ab HW Ver 1.0.0
- ab SW Ver 1.1.0



Für sicherheitsrelevante Applikationen sind folgende Ausführungen ausgeschlossen:

### 2.2 Anwendungsbereich

Der Radarsensor kann in einem sicherheitsbezogenen System gemäß IEC 61508 in den Betriebsarten *low demand mode* oder *high demand mode* zur Messung folgender Prozessgrößen eingesetzt werden:

- Füllstandmessung von Flüssigkeiten und Schüttgütern

Aufgrund der systematischen Eignung SC3 ist dies möglich bis:

- SIL2 in einkanaliger Architektur
- SIL3 in mehrkanaliger Architektur

Zur Ausgabe des Messwertes ist folgende Schnittstelle verwendbar:

- Stromausgang: 4 ... 20 mA



Folgende Schnittstellen sind ausschließlich zur Parametrierung und zur informativen Nutzung zulässig:

- HART
- Anzeige- und Bedienmodul PLICSCOM (auch via Bluetooth)
- VEGACONNECT (auch via Bluetooth)
- Stromausgang II<sup>1)</sup>

### 2.3 SIL-Konformität

Die SIL-Konformität wurde durch TÜV NORD CERT nach IEC 61508:2010 (Ed.2) unabhängig beurteilt und zertifiziert (Nachweisdokumente siehe "Anhang").



Das Zertifikat ist für alle Geräte, die vor Ablauf der Gültigkeit des Zertifikates in Verkehr gebracht werden, über die gesamte Produktlebensdauer gültig!

<sup>1)</sup> Nur bei Geräteausführung mit Zusatzelektronik "Zweileiter 4 ... 20 mA/HART plus zweiter Stromausgang 4 ... 20 mA".

### 3 Projektierung

#### 3.1 Sicherheitsfunktion

**Sicherheitsfunktion**

Der Sensor erzeugt an seinem Stromausgang ein der Prozessgröße entsprechendes Signal zwischen 3,8 mA und 20,5 mA. Dieses analoge Signal wird einem nachgeschalteten Auswertesystem zugeführt, um folgende Zustände zu überwachen:

- Überschreiten eines definierten Grenzwertes der Prozessgröße
- Unterschreiten eines definierten Grenzwertes der Prozessgröße
- Überwachung eines definierten Bereiches der Prozessgröße

**Sicherheitstoleranz**

Bei der Auslegung der Sicherheitsfunktion müssen bezüglich Toleranzen folgende Aspekte betrachtet werden:

- Aufgrund von unerkannten Ausfällen kann im Bereich von 3,8 mA und 20,5 mA ein falsches Ausgangssignal entstehen, das vom realen Messwert um bis zu 2 % abweicht
- Aufgrund von speziellen Applikationsbedingungen können erhöhte Messabweichungen entstehen (siehe Technische Daten in der Betriebsanleitung)

#### 3.2 Sicherer Zustand

**Sicherer Zustand**

Der sichere Zustand des Stromausganges ist abhängig von der Sicherheitsfunktion (Überwachung oberer/unterer Grenzwert) und von der am Sensor eingestellten Kennlinie.

Kennlinie	Überwachung oberer Grenzwert	Überwachung unterer Grenzwert
4 ... 20 mA	Ausgangsstrom $\geq$ Schalterpunkt	Ausgangsstrom $\leq$ Schalterpunkt
20 ... 4 mA	Ausgangsstrom $\leq$ Schalterpunkt	Ausgangsstrom $\geq$ Schalterpunkt

**Ausfallsignale bei Funktionsstörung**

Mögliche Fehlerströme:

- $\leq 3,6$  mA ("fail low")
- $> 21$  mA ("fail high")

#### 3.3 Voraussetzungen zum Betrieb

**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 laut Angaben der Betriebsanleitung, insbesondere die Strombelastung der Ausgangskreise, sind innerhalb der genannten Grenzen zu halten
- 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 Kennzahlen gemäß IEC 61508 für Füllstandmessung

VEGAPULS 6X

Kenngröße	Wert
Safety Integrity Level	SIL2 in einkanaliger Architektur SIL3 in mehrkanaliger Architektur <sup>2)</sup>
Hardwarefehler toleranz	HFT = 0
Gerätetyp	Typ B
Betriebsart	Low demand mode, High demand mode
SFF	> 90 %
MTBF <sup>3)</sup>	0,37 x 10 <sup>8</sup> h (42 Jahre)
Diagnostestintervall <sup>4)</sup>	< 30 min

#### Ausfallraten

$\lambda_{SD}$	$\lambda_{SU}$	$\lambda_{DD}$	$\lambda_{DU}$	$\lambda_H$	$\lambda_L$	$\lambda_{AD}$
179 FIT	158 FIT	895 FIT	45 FIT	10 FIT	324 FIT	67 FIT

PFD <sub>AVG</sub>	0,028 x 10 <sup>-2</sup>	(T1 = 1 Jahr)
PFD <sub>AVG</sub>	0,046 x 10 <sup>-2</sup>	(T1 = 2 Jahre)
PFD <sub>AVG</sub>	0,102 x 10 <sup>-2</sup>	(T1 = 5 Jahre)
PFH	0,045 x 10 <sup>-6</sup> 1/h	

#### Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart <sup>5)</sup>	Verbleibende Ausfallrate gefährbringender, unerkannter Ausfälle	PTC
Prüfung 1	16 FIT	65 %
Prüfung 2a	2 FIT	96 %
Prüfung 2b	6 FIT	86 %
Prüfung 2c	11 FIT	74 %

### 4.2 Kennzahlen gemäß ISO 13849-1 für Füllstandmessung

Der Messumformer wurde unter Anwendung von Prinzipien hergestellt und verifiziert, die seine Eignung und Zuverlässigkeit für sicherheitsbezogene Anwendungen zeigen. Somit ist er als "*bewährtes Bauteil*" nach DIN EN ISO 13849-1 zu betrachten.

<sup>2)</sup> Homogene Redundanz möglich, da systematische Eignung SC3.

<sup>3)</sup> Einschließlich Fehlern, die außerhalb der Sicherheitsfunktion liegen.

<sup>4)</sup> Zeit, in der alle internen Diagnosen mindestens einmal ausgeführt werden.

<sup>5)</sup> Siehe Abschnitt "Wiederholungsprüfung".

Abgeleitet von den sicherheitstechnischen Kennzahlen ergeben sich gemäß ISO 13849-1 (Sicherheit von Maschinen) folgende Kennzahlen:<sup>6)</sup>

## VEGAPULS 6X

Kenngröße	Wert
MTTF <sub>d</sub>	87 Jahre
DC	mittel
PFH <sub>D</sub>	0,045 x 10 <sup>-6</sup> 1/h

### 4.3 Ergänzende Informationen

#### Ermittlung der Ausfallraten

Die Ausfallraten des Gerätes wurden durch eine FMEDA nach IEC 61508 ermittelt. Den Berechnungen sind Ausfallraten der Bauelemente nach **SN 29500** zugrunde gelegt.

Alle Zahlenwerte beziehen sich auf eine mittlere Umgebungstemperatur während der Betriebszeit von 40 °C (104 °F). Für höhere Temperaturen sollten die Werte korrigiert werden:

- Dauereinsatztemperatur > 50 °C (122 °F) um Faktor 1,5
- Dauereinsatztemperatur > 60 °C (140 °F) um Faktor 2,3

Ähnliche Faktoren gelten, wenn häufige Temperaturschwankungen zu erwarten sind.

#### 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
- Abnutzung von mechanischen Teilen sind nicht betrachtet
- Ausfallraten von externen Stromversorgungen sind nicht mit einberechnet
- Die Umweltbedingungen entsprechen einer durchschnittlichen industriellen Umgebung

#### Berechnung von PFD<sub>AVG</sub>

Die oben angegebenen Werte für PFD<sub>AVG</sub> 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 = 96 %
- LT = 10 Jahre
- MTTR = 8 h

#### 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!

<sup>6)</sup> Die ISO 13849-1 war nicht Gegenstand der Zertifizierung des Gerätes.



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**

Aufgrund der systematischen Eignung SC3 darf dieses Gerät in mehrkanaligen Systemen bis SIL3 auch mit homogener 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 In Betrieb nehmen

### 5.1 Allgemein

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

**SIL** Die Inbetriebnahme mit Anfahren muss unter gleichen Prozessbedingungen durchgeführt werden, welche im späteren Betrieb zu erwarten sind. Ändern sich die Prozessbedingungen ist vom Betreiber zu entscheiden, ob eine erneute Inbetriebnahme erforderlich ist.

### 5.2 Geräteparametrierung

**Hilfsmittel** Zur Parametrierung der Sicherheitsfunktion sind folgende Bedieneinheiten zulässig:

- Anzeige- und Bedienmodul
- Der zum VEGAPULS 6X passende DTM in Verbindung mit einer Bediensoftware nach dem FDT/DTM-Standard, z. B. PACTware
- Die zum VEGAPULS 6X passende Gerätebeschreibung EDD

Die Vorgehensweise der Parametrierung ist in der Betriebsanleitung beschrieben.

**SIL** Bei vorhandener Bluetooth-Funktion ist auch eine drahtlose Verbindung möglich.

**SIL** Die Dokumentation der Geräteeinstellungen kann nur mit der Vollversion der DTM-Collection erfolgen.

### 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 gesperrten Zustand ausgeliefert.

Der Gerätecode wird der Gerätedokumentation beigelegt.

Die Basiswerte der Parameter sind in der Betriebsanleitung aufgelistet. Bei Auslieferung mit einer kundenspezifischen Parametrierung, wird dem Gerät eine Liste mit den zur Basiseinstellung unterschiedlichen Werten beigelegt.

Anhand der Seriennummer steht diese Liste auch über "[www.vega.com](http://www.vega.com)", "*Gerätesuche (Seriennummer)*" zum Download zur Verfügung.

### Sichere Parametrierung

Um bei der Parametrierung mit nicht sicherer Bedienungsumgebung 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.



Bei vorhandener Bluetooth-Funktion ist auch eine drahtlose Verbindung möglich.



Das Gerät wird im gesperrten Zustand ausgeliefert!



Zur Verifizierung werden alle geänderten sicherheitsrelevanten und nicht sicherheitsrelevanten Parameter dargestellt.

Die Verifizierungstexte werden entweder in Deutsch oder bei allen anderen Menüsprachen in Englisch zur Verfügung gestellt.

#### Unsicherer Gerätezustand



##### Warnung:

Ist die Bedienung freigegeben, so muss die Sicherheitsfunktion als unsicher betrachtet werden. Dies gilt solange, bis die Parameter verifiziert wurden und die Bedienung wieder gesperrt ist. Wird der Ablauf der Parametrierung nicht vollständig durchgeführt, so sind die in der Betriebsanleitung beschriebenen Gerätezustände zu beachten.

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

#### Gerätereset



##### Warnung:

Wird ein Reset auf "*Werkseinstellung*" durchgeführt, so müssen alle sicherheitsrelevanten Parameter überprüft bzw. neu eingestellt werden.

## 6 Diagnose und Service

### 6.1 Verhalten bei Ausfall

#### Interne Diagnosen

Das Gerät wird permanent durch ein internes Diagnosesystem überwacht. Wird eine Funktionsstörung erkannt, so wird am sicherheitsrelevanten Ausgang ein Ausfallsignal ausgegeben (siehe Abschnitt "Sicherer Zustand").

Das Diagnosetestintervall ist in Kapitel "Sicherheitstechnische Kennzahlen" angegeben.

#### Fehlermeldungen bei Funktionsstörung

Je nach Fehlerart wird eine entsprechend kodierte Fehlermeldung ausgegeben. Die Fehlermeldungen sind in der Betriebsanleitung aufgelistet.



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

Das Auftreten eines Ausfalls ist dem Hersteller zu melden (inklusive Fehlerbeschreibung und der Angabe ob es sich um einen gefahrbringenden, unerkannten Ausfall handelt). Das Gerät ist zur Untersuchung an den Hersteller zurückzusenden.

### 6.2 Reparatur

#### Elektroniktausch

Die Vorgehensweise ist in der Betriebsanleitung "Elektroniktausch" beschrieben. Es sind die Hinweise zur Parametrierung und Inbetriebnahme zu beachten.

#### Softwareupdate

Die Vorgehensweise ist in der Betriebsanleitung beschrieben. Es sind die Hinweise zur Parametrierung und Inbetriebnahme zu beachten.

## 7 Wiederholungsprüfung

### 7.1 Allgemein

#### Zielsetzung

Um mögliche gefahrbringende, unerkannte Ausfälle zu erkennen, muss in angemessenen Zeitabständen die Sicherheitsfunktion durch eine Wiederholungsprüfung überprüft werden. 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").

Zur Dokumentation dieser Tests kann das Prüfprotokoll im Anhang verwendet werden.

Verläuft einer der Tests negativ, so 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.

#### Vorbereitung

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

#### Assistent

Sie haben die Möglichkeit die Wiederholungsprüfung über den Assistenten im DTM oder der App durchzuführen.

#### 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 Prüfung 1: Ohne Überprüfung der Prozessgröße

#### Bedingungen

- Gerät verbleibt im eingebauten Zustand
- Ausgangssignal entspricht der zugeordneten Prozessgröße
- Gerätestatus im Menü Diagnose: "OK"

#### Ablauf:

Neustart durchführen (den Prüfling für mindestens 10 Sekunden von der Spannungsversorgung trennen + 1 Minute warten) und anschließend erneut das Ausgangssignal auf Übereinstimmung mit der zugeordneten Prozessgröße vergleichen.

Durch Simulation des oberen und unteren Fehlerstromes können nachgeschaltete Geräte auf korrektes Ansprechen der Sicherheitsfunktion geprüft werden.

1. Oberer Strom > 20 mA simulieren und Stromausgang überprüfen (Test Leitungswiderstand)

2. Unterer Fehlerstrom  $\leq 3,6$  mA simulieren und Stromausgang überprüfen (Test Ruheströme)

**Erwartetes Ergebnis**

Ausgangssignal entspricht der zugeordneten Prozessgröße  
 Schritt 1: Ausgangssignal entspricht  $> 20$  mA  
 Schritt 2: Ausgangssignal entspricht  $\leq 3,6$  mA

**Deckungsgrad der Prüfung**

Siehe *Sicherheitstechnische Kennzahlen*

Zusätzlich zum Diagnosedeckungsgrad für gefährliche Fehler ( $DC_D$ ) von 96,6 % der internen Diagnosen, werden durch diese Wiederholungsprüfung ca. 65 % der restlichen gefährlichen unerkannten Ausfälle aufgedeckt. Dies gibt einen gesamten Diagnosedeckungsgrad von 98,7 %.

**7.3 Prüfung 2: Mit Überprüfung der Prozessgröße****Bedingungen**

- Gerät verbleibt im eingebauten Zustand
- Ausgangssignal entspricht der zugeordneten Prozessgröße
- Gerätestatus im Menü Diagnose: "OK"

**Prüfung 2a: Anfahren der Sicherheitsfunktion****Ablauf**

1. Neustart durchführen (den Prüfling für mindestens 10 Sekunden von der Spannungsversorgung trennen + 1 Minute warten) und anschließend erneut das Ausgangssignal auf Übereinstimmung mit der zugeordneten Prozessgröße vergleichen
2. Referenzmessung bei 0 % - 50 % - 100 % des abgeglichenen Füllstandes in der Verwendung (4 mA - 12 mA - 20 mA)

**Erwartetes Ergebnis**

Schritt 1: Ausgangssignal entspricht der zugeordneten Prozessgröße  
 Schritt 2: Ausgangssignale entsprechen dem Füllstand

**Deckungsgrad der Prüfung**

Siehe *Sicherheitstechnische Kennzahlen*

Zusätzlich zum Diagnosedeckungsgrad für gefährliche Fehler ( $DC_D$ ) von 96,67 % der internen Diagnosen, werden durch diese Wiederholungsprüfung ca. 96 % der restlichen gefährlichen unerkannten Ausfälle aufgedeckt. Dies gibt einen gesamten Diagnosedeckungsgrad von 99,8 %.

**Prüfung 2b: Anfahren von Bereichen + Simulation Stromausgang****Ablauf**

1. Neustart durchführen (den Prüfling für mindestens 10 Sekunden von der Spannungsversorgung trennen + 1 Minute warten) und anschließend erneut das Ausgangssignal auf Übereinstimmung mit der zugeordneten Prozessgröße vergleichen
2. Referenzmessung bei 0 ... 10 % - 50 % - 90 ... 100 % des abgeglichenen Füllstandes in der Verwendung (4 ... 5,6 mA - 12 mA - 18,4 ... 20 mA)

3. Durch Simulation des oberen und unteren Fehlerstromes können nachgeschaltete Geräte auf korrektes Ansprechen der Sicherheitsfunktion geprüft werden.

**Erwartetes Ergebnis** Schritt 1: Ausgangssignal entspricht der zugeordneten Prozessgröße  
 Schritt 2: Ausgangssignale entsprechen dem Füllstand  
 Schritt 3: Sicherheitsfunktion der nachgeschalteten Geräte spricht korrekt an

**Deckungsgrad der Prüfung** Siehe *Sicherheitstechnische Kennzahlen*  
 Zusätzlich zum Diagnosedeckungsgrad für gefährliche Fehler ( $DC_D$ ) von 96,67 % der internen Diagnosen, werden durch diese Wiederholungsprüfung ca. 86 % der restlichen gefährlichen unerkannten Ausfälle aufgedeckt. Dies gibt einen gesamten Diagnosedeckungsgrad von 99,5 %.

**Prüfung 2c: Anfahren von Bereichen**

**Ablauf**

1. Neustart durchführen (den Prüfling für mindestens 10 Sekunden von der Spannungsversorgung trennen + 1 Minute warten) und anschließend erneut das Ausgangssignal auf Übereinstimmung mit der zugeordneten Prozessgröße vergleichen
2. Referenzmessung bei 0 ... 10 % - 50 % - 90 ... 100 % des abgeglichenen Füllstandes in der Verwendung (4 ... 5,6 mA - 12 mA - 18,4 ... 20 mA)

**Erwartetes Ergebnis** Schritt 1: Ausgangssignal entspricht der zugeordneten Prozessgröße  
 Schritt 2: Ausgangssignale entsprechen dem Füllstand

**Deckungsgrad der Prüfung** Siehe *Sicherheitstechnische Kennzahlen*  
 Zusätzlich zum Diagnosedeckungsgrad für gefährliche Fehler ( $DC_D$ ) von 96,67 % der internen Diagnosen, werden durch diese Wiederholungsprüfung ca. 74 % der restlichen gefährlichen unerkannten Ausfälle aufgedeckt. Dies gibt einen gesamten Diagnosedeckungsgrad von 99,1 %.

## 8 Anhang A: Prüfprotokoll

Identifikation	
Firma/Prüfer	
Anlage/Geräte-TAG	
Messstellen-TAG	
Gerätetyp/Bestellcode	
Geräte-Seriennummer	
Datum Inbetriebnahme	
Datum letzte Wiederholungsprüfung	

Testgrund/Testumfang	
	Inbetriebnahme ohne Überprüfung der Prozessgröße
	Inbetriebnahme mit Überprüfung der Prozessgröße
	Wiederholungsprüfung ohne Überprüfung der Prozessgröße
	Wiederholungsprüfung mit Überprüfung der Prozessgröße

Betriebsart	
	Überwachung eines oberen Grenzwertes
	Überwachung eines unteren Grenzwertes
	Bereichsüberwachung

Eingestellte Parameter der Sicherheitsfunktion sind dokumentiert	
	Ja
	Nein

Testergebnis (falls erforderlich)				
Testpunkt	Prozessgröße <sup>7)</sup>	Erwarteter Messwert	Istwert	Testergebnis
Wert 1				
Wert 2				
Wert 3				
Wert 4				
Wert 5				

Bestätigung	
Datum:	Unterschrift:

<sup>7)</sup> z. B.: Grenzstand, Füllstand, Trennschicht, Druck, Durchfluss, Dichte



## 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 <sup>9</sup> h)
$\lambda_{SD}$	Rate for safe detected failure
$\lambda_{SU}$	Rate for safe undetected failure
$\lambda_S$	$\lambda_S = \lambda_{SD} + \lambda_{SU}$
$\lambda_{DD}$	Rate for dangerous detected failure
$\lambda_{DU}$	Rate for dangerous undetected failure
$\lambda_H$	Rate for failure, who causes a high output current (> 21 mA)
$\lambda_L$	Rate for failure, who causes a low output current ( $\leq 3.6$ mA)
$\lambda_{AD}$	Rate for diagnostic failure (detected)
$\lambda_{AU}$	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)



A large grid of graph paper for taking notes, consisting of 20 columns and 30 rows of small squares.

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 2022



66494-DE-220712

VEGA Grieshaber KG  
Am Hohenstein 113  
77761 Schiltach  
Deutschland

Telefon +49 7836 50-0  
E-Mail: [info.de@vega.com](mailto:info.de@vega.com)  
[www.vega.com](http://www.vega.com)