

Safety Manual

PROTRAC Serie 30

Vierleiter 4 ... 20 mA/HART

Mit SIL-Qualifikation



Document ID: 49354



VEGA

Inhaltsverzeichnis

1	Dokumentensprache	3
2	Geltungsbereich.....	4
2.1	Geräteausführung	4
2.2	Anwendungsbereich.....	4
2.3	SIL-Konformität	5
3	Projektierung.....	6
3.1	Sicherheitsfunktion.....	6
3.2	Sicherer Zustand.....	6
3.3	Voraussetzungen zum Betrieb.....	7
3.4	Systemeinschränkungen.....	7
3.5	Wasser-/Luft-Kühlung	7
4	Sicherheitstechnische Kennzahlen.....	8
4.1	Kennzahlen gemäß IEC 61508 für alle Applikationen.....	8
4.2	Kennzahlen gemäß IEC 61508 für die Applikationen zur Grenzstanderfassung.....	8
4.3	Kennzahlen gemäß IEC 61508 für die Applikationen zur Füllstandmessung.....	10
4.4	Kennzahlen gemäß ISO 13849-1	12
4.5	Ergänzende Informationen	12
5	In Betrieb nehmen.....	14
5.1	Allgemein	14
5.2	Geräteparametrierung.....	14
6	Diagnose und Service	16
6.1	Verhalten bei Ausfällen.....	16
6.2	Meldungen bei Funktionsstörung	16
6.3	Reparatur	16
7	Wiederholungsprüfung	17
7.1	Allgemein	17
7.2	Prüfung 1: Für Betriebsart Grenzstanderfassung	17
7.3	Prüfung 2: Für Betriebsart Füllstandmessung	18
8	Anhang A: Prüfprotokoll.....	19
9	Anhang B: Begriffsdefinitionen	20
10	Anhang C: SIL-Konformität	21

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 folgende radiometrische Messumformer:

- **POINTRAC 31** Vierleiter 8/16 mA/HART
- **MINITRAC 31, 32** Vierleiter 4 ... 20 mA/HART
- **SOLITRAC 31** Vierleiter 4 ... 20 mA/HART
- **FIBERTRAC 31, 32** Vierleiter 4 ... 20 mA/HART

Gültige Versionen:

- ab Hardwareversion 1.0.6
- ab Softwareversion 1.8.0

SIL Der FIBERTRAC 31 und 32 darf nur mit einer Detektorlänge von maximal 1,5 m verwendet werden!

SIL Der Strahlenschutzbehälter war nicht Gegenstand der Zertifizierung des Gerätes!

2.2 Anwendungsbereich

Die Messumformer können zur Grenzstanderfassung oder Füllstandmessung von Flüssigkeiten und Schüttgütern in einem sicherheitsinstrumentierten System 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 einer einkanaligen Architektur
- SIL3 in einer mehrkanaligen Architektur mit diversitärer Redundanz

Hierzu sind folgende Schnittstellen verwendbar:

Grenzstanderfassung

- Relaisausgang: NO-Kontakt¹⁾
- Stromausgang: 8/16 mA
- Stromausgang 4 ... 20 mA, wenn der Grenzwert in einem nachgeschalteten Auswertsystem festgelegt wird

Füllstandmessung

- Stromausgang: 4 ... 20 mA

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

- HART
- Anzeige- und Bedienmodul PLICSCOM (auch via Bluetooth)
- VEGACONNECT

¹⁾ NO = Normal Open

2.3 SIL-Konformität

Die SIL-Konformität wurde durch *exida* Certification S.A. nach IEC 61508 unabhängig beurteilt und zertifiziert.²⁾

²⁾ Nachweisdokumente siehe Anhang

3 Projektierung

3.1 Sicherheitsfunktion

Sicherheitsfunktion Grenzstanderfassung

Der Messumformer detektiert einen festgelegten Grenzstand und meldet den erkannten Zustand an seinem Relaisausgang mit Kontakt geöffnet/geschlossen oder an seinem Stromausgang mit 8 mA/16 mA.

Sicherheitsfunktion Füll- standmessung

Der Messumformer erzeugt an seinem Stromausgang ein dem Füllstand entsprechendes Signal zwischen 3,8 mA und 20,5 mA. Dieses analoge Signal wird einem nachgeschalteten Auswertsystem zugeführt, um folgende Zustände zu überwachen:

- Überschreiten eines vorgegebenen Füllstandes
- Unterschreiten eines vorgegebenen Füllstandes
- Überwachung eines Füllstandbereiches (Einschränkungen siehe Kapitel "Kennzahlen für die Applikationen zur Füllstandmessung")

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 Grenz- standerfassung

Sicherer Zustand Relaisausgang

Der sichere Zustand des Ausganges ist unabhängig von der Betriebsart, definitionsgemäß der stromlose Zustand der Relais (Ruhestromprinzip).

Für sicherheitsrelevante Anwendungen darf deshalb nur der NO-Kontakt verwendet werden.

Sicherer Zustand Stromausgang

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

	Überfüllsicherung	Trockenlaufschutz
Füllstand	unbedeckt (hohe Zählrate)	bedeckt (niedrige Zählrate)
Relaisausgang	NO-Kontakt offen (stromlos)	NO-Kontakt offen (stromlos)
Stromausgang: 8/16 mA	8 mA $\pm 2\%$	16 mA $\pm 2\%$
Stromausgang: 16/8 mA	16 mA $\pm 2\%$	8 mA $\pm 2\%$

Sicherer Zustand Füllstandmessung

Sicherer Zustand Stromausgang

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

Kennlinie	Überwachung oberer Grenzwert	Überwachung unterer Grenzwert
4 ... 20 mA	Ausgangsstrom > Schaltpunkt	Ausgangsstrom < Schaltpunkt
20 ... 4 mA	Ausgangsstrom < Schaltpunkt	Ausgangsstrom > Schaltpunkt

Ausfallsignale bei Funktionsstörung

Relaisausgang

- NO-Kontakt offen

Stromausgang

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

Hinweise und Einschränkungen

3.3 Voraussetzungen zum Betrieb

- 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 benutzt
- 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



In der Betriebsart Trockenlaufschutz muss am Strahlenschutzbehälter die Schaltstellung EIN fixiert sein!

3.4 Systemeinschränkungen



Es gibt mehrere Faktoren, welche aufgrund des Messprinzips das Messergebnis beeinflussen. Diese Faktoren müssen berücksichtigt werden, um die Anforderungen an das Gerät bezüglich Stabilität und Nichtwiederholbarkeit zu erfüllen. Entsprechende Hinweise sind in der Betriebsanleitung in Kapitel "*Produktbeschreibung*" angegeben.

3.5 Wasser-/Luft-Kühlung



Ist zur Einhaltung der spezifizierten Betriebstemperatur eine Wasser-/Luft-Kühlung erforderlich, so ist diese Kühleinrichtung Bestandteil der Sicherheitsfunktion und muss entsprechend überwacht werden, z. B. durch einen SIL-qualifizierten Temperatursensor.

Es sind die Hinweise der Betriebsanleitung bezüglich Montage und Durchflussskennwerte zu beachten.

4 Sicherheitstechnische Kennzahlen

4.1 Kennzahlen gemäß IEC 61508 für alle Applikationen

Kenngröße gemäß IEC 61508	Wert
Safety Integrity Level	SIL2 in einkanaliger Architektur SIL3 in mehrkanaliger Architektur ³⁾
Hardwarefehlertoleranz	HFT = 0
Gerätetyp	Typ B
Betriebsart	Low demand mode, High demand mode
SFF	> 90 %
MTTR	8 h
MTBF ⁴⁾	0,39 x 10 ⁶ h (45 Jahre)
Diagnostestintervall ⁵⁾	< 10 min
Fehlerreaktionszeit ⁶⁾	10 s

4.2 Kennzahlen gemäß IEC 61508 für die Applikationen zur Grenzstanderfassung

Relaisausgang

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

Mögliche Geräteausführungen:

- POINTRAC 31
- MINITRAC 31, 32
- SOLITRAC 31
- FIBERTRAC 31, 32

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
458 FIT	1097 FIT	123 FIT	0 FIT	0 FIT	24 FIT	30 FIT

PFD _{AVG}	0,102 x 10 ⁻²	(T1 = 1 Jahr)
PFD _{AVG}	0,150 x 10 ⁻²	(T1 = 2 Jahre)
PFD _{AVG}	0,295 x 10 ⁻²	(T1 = 5 Jahre)
PFH	0,123 x 10 ⁻⁶ 1/h	

³⁾ Nur diversitäre Redundanz möglich, da Gerätesoftware SIL2.
⁴⁾ Bezieht sich nur auf Ausfälle bezüglich der Sicherheitsfunktion.
⁵⁾ Zeit, in der alle internen Diagnosen mindestens einmal ausgeführt werden.
⁶⁾ Zeit zwischen Ausfallerkennung und Ausgabe des Ausfallsignales.

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart (Siehe Abschnitt "Wiederholungsprüfung")	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 1	12 FIT	90 %

Stromausgang

Stromausgang 8/16 mA oder 4 ... 20 mA zur Ansteuerung eines nachgeschalteten Auswertsystems (z. B. SSPS) für die Überwachung eines Grenzwertes (z. B. Überfüllsicherung oder Trockenlaufschutz).

Mögliche Geräteausführungen:

- POINTRAC 31
- MINITRAC 31, 32
- SOLITRAC 31
- FIBERTRAC 31, 32

Single or Master device

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
123 FIT	1413 FIT	125 FIT	12 FIT	71 FIT	86 FIT	11 FIT

PFD _{AVG}	0,105 x 10 ⁻²	(T1 = 1 Jahr)
PFD _{AVG}	0,154 x 10 ⁻²	(T1 = 2 Jahre)
PFD _{AVG}	0,302 x 10 ⁻²	(T1 = 5 Jahre)
PFH	0,125 x 10 ⁻⁶ 1/h	

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart (Siehe Abschnitt "Wiederholungsprüfung")	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 1	13 FIT	90 %

Stromausgang im Summierungsbetrieb

Stromausgang 4 ... 20 mA zur Ansteuerung eines nachgeschalteten Auswertsystems (z. B. SSPS) für die Überwachung eines Grenzwertes (z. B. Überfüllsicherung oder Trockenlaufschutz).

Mögliche Geräteausführungen mit N Slaves:⁷⁾

- SOLITRAC 31 Master + Slave(s)
- FIBERTRAC 31, 32 Master + Slave(s)

Slave

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
123 FIT	1372 FIT	120 FIT	0 FIT	0 FIT	19 FIT	2 FIT

Master + 1 Slave

λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
246 FIT	2785 FIT	245 FIT	12 FIT	71 FIT	105 FIT	13 FIT

⁷⁾ Für N Slaves: $\lambda_X = \lambda_{X \text{ Master}} + N \cdot \lambda_{X \text{ Slave}}$

PFD _{AVG}	$0,206 \times 10^{-2}$	(T1 = 1 Jahr)
PFD _{AVG}	$0,303 \times 10^{-2}$	(T1 = 2 Jahre)
PFH	$0,245 \times 10^{-6}$ 1/h	

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart (Siehe Abschnitt "Wiederholungsprüfung")	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 1	25 FIT	90 %

Master + 2 Slaves

λ_s	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
368 FIT	4157 FIT	365 FIT	12 FIT	71 FIT	125 FIT	16 FIT

PFD _{AVG}	$0,307 \times 10^{-2}$	(T1 = 1 Jahr)
PFH	$0,365 \times 10^{-6}$ 1/h	

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart (Siehe Abschnitt "Wiederholungsprüfung")	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 1	37 FIT	90 %

4.3 Kennzahlen gemäß IEC 61508 für die Applikationen zur Füllstandmessung**Stromausgang**

Stromausgang 4 ... 20 mA zur Ansteuerung eines nachgeschalteten Auswertsystems (z. B. SSPS) für die Überwachung eines Füllstandbereichs.

Mögliche Geräteausführungen:

- MINITRAC 31, 32
- SOLITRAC 31
- FIBERTRAC 31, 32

Single or Master device

λ_s	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	1507 FIT	154 FIT	12 FIT	71 FIT	86 FIT	11 FIT

PFD _{AVG}	$0,129 \times 10^{-2}$	(T1 = 1 Jahr)
PFD _{AVG}	$0,190 \times 10^{-2}$	(T1 = 2 Jahre)
PFD _{AVG}	$0,371 \times 10^{-2}$	(T1 = 5 Jahre)
PFH	$0,154 \times 10^{-6}$ 1/h	

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart ⁸⁾	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 2	15 FIT	90 %

Stromausgang im Summierungsbetrieb

Stromausgang 4 ... 20 mA zur Ansteuerung eines nachgeschalteten Auswertsystems (z. B. SSPS) für die Überwachung eines Füllstandbereichs.

Mögliche Geräteausführungen mit N Slaves:⁹⁾

- SOLITRAC 31 Master + Slave(s)
- FIBERTRAC 31, 32 Master + Slave(s)

Slave

λ_s	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	1466 FIT	149 FIT	0 FIT	0 FIT	19 FIT	2 FIT

Master + 1 Slave

λ_s	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	2973 FIT	302 FIT	12 FIT	71 FIT	105 FIT	13 FIT

PFD _{AVG}	$0,254 \times 10^{-2}$	(T1 = 1 Jahr)
PFD _{AVG}	$0,373 \times 10^{-2}$	(T1 = 2 Jahre)
PFH	$0,302 \times 10^{-6} \text{ 1/h}$	

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart ¹⁰⁾	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 2	30 FIT	90 %

Master + 2 Slaves

λ_s	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
0 FIT	4439 FIT	451 FIT	12 FIT	71 FIT	125 FIT	16 FIT

PFD _{AVG}	$0,379 \times 10^{-2}$	(T1 = 1 Jahr)
PFH	$0,451 \times 10^{-6} \text{ 1/h}$	

⁸⁾ Siehe Abschnitt "Wiederholungsprüfung".

⁹⁾ Für N Slaves: $\lambda_x = \lambda_{x \text{ Master}} + N \cdot \lambda_{x \text{ Slave}}$

¹⁰⁾ Siehe Abschnitt "Wiederholungsprüfung".

Deckungsgrad bei der Wiederholungsprüfung (PTC)

Prüfungsart ¹¹⁾	Verbleibende gefährliche unerkannte Ausfälle	PTC
Prüfung 2	45 FIT	90 %

4.4 Kennzahlen gemäß ISO 13849-1

Abgeleitet von den sicherheitstechnischen Kennzahlen ergeben sich gemäß ISO 13849-1 (Maschinensicherheit) folgende Kennzahlen:¹²⁾

Grenzstanderfassung

Applikation	MTTFd	DC	Performance Level
Relaisausgang	91 Jahre	90 %	1,23 x 10 ⁻⁷ 1/h
Stromausgang	66 Jahre	93 %	1,25 x 10 ⁻⁷ 1/h
Summierungsbetrieb mit 1 Slave	35 Jahre	92 %	2,45 x 10 ⁻⁷ 1/h
Summierungsbetrieb mit 2 Slaves	24 Jahre	92 %	3,65 x 10 ⁻⁷ 1/h

Füllstandmessung

Applikation	MTTFd	DC	Performance Level
Stromausgang	62 Jahre	92 %	1,54 x 10 ⁻⁷ 1/h
Summierungsbetrieb mit 1 Slave	33 Jahre	91 %	3,02 x 10 ⁻⁷ 1/h
Summierungsbetrieb mit 2 Slaves	22 Jahre	91 %	4,51 x 10 ⁻⁷ 1/h

4.5 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 1,3
- Dauereinsatztemperatur > 60 °C (140 °F) um Faktor 2,5

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

¹¹⁾ Siehe Abschnitt "Wiederholungsprüfung".

¹²⁾ Die ISO 13849-1 war nicht Gegenstand der Zertifizierung des Gerätes.

- 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 = 90 %
- LT = 10 Jahre
- $MTTR$ = 8 h

Randbedingungen bezüglich Konfiguration der Auswertereinheit

Eine nachgeschaltete Steuer- und Auswertereinheit 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 In Betrieb nehmen

5.1 Allgemein

Montage und Installation

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

Die Inbetriebnahme muss unter Prozessbedingungen erfolgen.

5.2 Geräteparametrierung

Hilfsmittel

Zur Parametrierung der Sicherheitsfunktion sind folgende Bedieneinheiten zulässig:

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

Die Vorgehensweise der Parametrierung ist in der Betriebsanleitung beschrieben.



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. Die PIN im Auslieferungszustand lautet "0000".

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", "*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 verriegelten 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 Geräte- zustand



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.

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

Unvollständiger Ablauf der Geräte- parametrierung



Warnung:

Wenn der beschriebene Ablauf der Parametrierung nicht vollständig durchlaufen wird (z. B. durch Abbruch oder Stromausfall), so bleibt das Gerät im Zustand "unverriegelt".

Gerätereset



Warnung:

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

6 Diagnose und Service

6.1 Verhalten bei Ausfällen

Interne Diagnosen

Das Gerät wird permanent durch ein internes Diagnosesystem überwacht. Wird eine Funktionsstörung erkannt, so wird dies durch entsprechende Ausfallsignale angezeigt (siehe Abschnitt "*Sicherer Zustand*").

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



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

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

6.2 Meldungen bei Funktionsstörung

Meldungen bei Funktionsstörung

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

Auflösung der Funktionsstörung

Bezüglich der Auflösung der Funktionsstörung werden folgende Verhaltensweisen unterschieden:

- Funktionsstörungen aufgrund eines Bedienfehlers (z. B. Kommunikationsprobleme, falscher Abgleich, usw.), werden unmittelbar nach dessen Bereinigung aufgelöst.
- Funktionsstörungen aufgrund eines Hardwareausfalls können in der Regel nur durch einen manuellen Neustart aufgelöst werden. Wenn die Ausfallursache nicht mehr vorliegt, so wird die Sicherheitsfunktion wieder korrekt ausgeführt.
- Bei Hardwareausfällen "F041 Photomultiplierfehler" und "F045 Fehler am Stromausgang" wird die Funktionsstörung unmittelbar nach Bereinigung des Fehlers aufgelöst.
- Treten Ausfälle auf, die einen automatischen Neustart zur Folge haben, bleibt das Gerät nach Wiederanlauf mindestens 5 Sekunden im Zustand Funktionsstörung. Wird kein Ausfall mehr erkannt, so wird die Sicherheitsfunktion wieder korrekt ausgeführt.

6.3 Reparatur

Elektroniktausch

Ein Austausch der Elektronik darf nur von VEGA-Service-Technikern oder von Fachpersonal durchgeführt werden, welches bei VEGA entsprechend geschult wurde (z. B. VEGA-Vertriebspartner).

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

Softwareupdate

Ein Softwareupdate darf durch den Anwender vorgenommen werden. 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

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: Für Betriebsart Grenzstanderfassung

Bedingungen

- Gerät im eingebauten Zustand
- Ausgangssignal entspricht dem Prozessdruck oder dem Füllstand
- Gerätestatus im Menü Diagnose: "OK"

Ablauf

1. Prozessbedingungen in den Zustand versetzen, so dass die Strahlung am Sensor möglichst hoch ist
2. Messwert auf Korrektheit überprüfen
3. Strahlungsquelle(n) schließen
4. Messwert auf Korrektheit überprüfen
5. Strahlungsquelle(n) öffnen
6. Messwert auf Korrektheit überprüfen
7. Normaler Messbetrieb wieder aufnehmen

Erwartetes Ergebnis

- zu 1: Füllstand unterhalb des Sensors
- zu 2: Schaltzustand meldet unbedeckt
- zu 4: Schaltzustand meldet bedeckt
- zu 6: wie Punkt 2

Deckungsgrad der PrüfungSiehe *Sicherheitstechnische Kennzahlen***7.3 Prüfung 2: Für Betriebsart Füllstandmessung****Bedingungen**

- Gerät im eingebauten Zustand
- Ausgangssignal entspricht dem Prozessdruck oder dem Füllstand
- Gerätestatus im Menü Diagnose: "OK"

Ablauf

1. Prozessbedingungen in den Zustand versetzen, so dass die Strahlung am Sensor möglichst hoch ist
2. Messwert auf Korrektheit überprüfen
3. Strahlungsquelle(n) schließen
4. Messwert auf Korrektheit überprüfen
5. Strahlungsquelle(n) öffnen
6. Messwert auf Korrektheit überprüfen
7. Normaler Messbetrieb wieder aufnehmen

Erwartetes Ergebnis

- zu 1: Füllstand unterhalb 50 %
- zu 2: Messwert entspricht dem Füllstand
- zu 4: Gerät zeigt voll an
- zu 6: wie Punkt 2

Deckungsgrad der PrüfungSiehe *Sicherheitstechnische Kennzahlen*

8 Anhang A: Prüfprotokoll

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

Testgrund		Testumfang	
(...)	Inbetriebnahme	(...)	Prüfung 1
(...)	Wiederholungsprüfung	(...)	Prüfung 2

Eingestellte Geräteparameter der Sicherheitsfunktion		
Isotop	(...) Cs-137 (...) Co-60	
Verwendete sicherheitsrelevante Ausgänge	(...) Relaisausgang (...) Stromausgang	
Eingestellte Betriebsart	(...) Grenzstanderfassung Überfüllsicherung (...) Grenzstanderfassung Trockenlaufschutz (...) Füllstandmessung	
Detektorlänge	mm	
Grenzstanderfassung: eingestellter Abgleich "unbedeckt"	ct/s	
Grenzstanderfassung: eingestellter Abgleich "bedeckt"	ct/s	
Füllstandmessung: maximaler Prozesswert		
Füllstandmessung: minimaler Prozesswert		

Testergebnis			
Testschritt	Zustand Relais	Ausgangsstrom	Testergebnis
		mA	
		mA	
		mA	
		mA	
		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

SIL Manufacturer declaration, NE130: Form B.1

Manufacturer		
VEGA Grieshaber KG Am Hohenstein 113, D-77761 Schiltach, Germany		VEGA Americas, Inc. 4241 Aliendorf Drive, Cincinnati, Ohio 45209, USA
General		
Device designation and permissible types	PROTRAC Series 30	
	POINTRAC 31 8/16 mA/HART - Four-wire with SIL qualification PT31.***I/L/S***** MINITRAC 31, 32 4 ... 20 mA/HART - Four-wire with SIL qualification MT31/32.***I/L/S**** SOLITRAC 31 4 ... 20 mA/HART - Four-wire with SIL qualification ST31.***I/L/S***** FIBERTRAC 31, 32 4 ... 20 mA/HART - Four-wire with SIL qualification FT31/32.***I/L/S*****	
Safety-related output signal	4...20 mA or 8/16 mA and/or Relay	
Fault current	Current output: ≥ 21 mA; $\leq 3,6$ mA; Relay output: NO contact open	
Process variable / function	Point level detection or level measurement In addition with slave sensor in summation mode	
Safety function(s)	- MIN/MAX limit detection - Range measurement	
Device type acc. to IEC 61508-2	☐ Type A ☒ Type B	
Operating mode	☒ Low Demand Mode ☒ High Demand or Continuous Mode	
Valid Hardware-Version	$\geq 1.0.6$	
Valid Software-Version	$\geq 1.8.0$	
Safety manual	Document ID: 49354	
Type of evaluation (check only one box)	☒ Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3 ☐ Evaluation of "Prior use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3 ☐ Evaluation of HW/SW field data to verify „prior use" acc. to IEC 61511 ☐ Evaluation by FMEDA acc. to IEC61508-2 for devices without software	
Evaluation through (incl. certificate no.)	exida.com -Excellence in Dependable Automation GmbH, VEGA 1202050C P0011 C004	
Test documents	Development documents	Test reports Data sheets
Safety Integrity		
Systematic Capability (SC)	☒ SC2 for SIL2 ☐ SC3 for SIL3	
Hardware Safety Integrity	Single-channel use (HFT=0) ☒ SIL2 capable ☐ SIL3 capable Multi-channel use (HFT $\geq$ 1) ☐ SIL2 capable ☒ SIL3 capable	
FMEDA	Version: POINTRAC 31, 32; MINITRAC 31, 32; SOLITRAC 31; FIBERTRAC 31, 32	
	Relay	Current output
Safety function(s)	MIN / MAX	MIN / MAX
λ_{DU} (FIT = Failure In Time / 10^9 h)	123 FIT	125 FIT
λ_{DO}	1097 FIT	1413 FIT
λ_{SU}	364 FIT	29 FIT

SIL Manufacturer declaration, NE130: Form B.1

λ_{SD}	94 FIT	94 FIT
SFF (Safe Failure Fraction)	> 90 %	> 90 %
PTC (Proof Test Coverage)	Test 1: 90%, with checking the process value	Test 1: 90%, with checking the process value
FMEDA data source	SN 29500	

FMEDA	Version with slave sensor consisting of a combination of SOLITRAC 31 Master + Slave; FIBERTRAC 31, 32 Master + Slave		
	Slave	Master + 1 Slave	Master + 2 Slaves
Safety function(s)	MIN / MAX	MIN / MAX	MIN / MAX
λ_{DU} (FIT = Failure In Time / 10^9 h)	120 FIT	245 FIT	365 FIT
λ_{DD}	1372 FIT	2785 FIT	4157 FIT
λ_{SU}	62 FIT	90 FIT	152 FIT
λ_{SD}	61 FIT	155 FIT	216 FIT
SFF (Safe Failure Fraction)		> 90 %	> 90 %
PTC (Proof Test Coverage)		Test 1: 90% ¹⁾	Test 1: 90% ¹⁾
	¹⁾ Test 1 with checking the process value		
FMEDA data source	SN 29500		

FMEDA	Version: MINITRAC 31, 32; SOLITRAC 31; FIBERTRAC 31, 32 Current output
Safety function(s)	Range
λ_{DU} (FIT = Failure In Time / 10^9 h)	154 FIT
λ_{DD}	1507 FIT
λ_{SU}	0 FIT
λ_{SD}	0 FIT
SFF (Safe Failure Fraction)	> 90 %
PTC (Proof Test Coverage)	Test 1: 90%, with checking the process value
FMEDA data source	SN 29500

FMEDA	Version with slave sensor consisting of a combination of SOLITRAC 31 Master + Slave; FIBERTRAC 31, 32 Master + Slave		
	Slave	Master + 1 Slave	Master + 2 Slaves
Safety function(s)	Range	Range	Range
λ_{DU} (FIT = Failure In Time / 10^9 h)	149 FIT	302 FIT	451 FIT
λ_{DD}	1466 FIT	2973 FIT	4439 FIT
λ_{SU}	0 FIT	0 FIT	0 FIT
λ_{SD}	0 FIT	0 FIT	0 FIT
SFF (Safe Failure Fraction)		> 90 %	> 90 %
PTC (Proof Test Coverage)		Test 1: 90% ¹⁾	Test 1: 90% ¹⁾
	¹⁾ Test 1 with checking the process value		
FMEDA data source	SN 29500		

Declaration	
☒	Our internal company quality management system ensures information on safety-related systematic faults which become evident in the future.



The manufacturer
may use the mark:



Revision 2.3 August 19, 2019
Surveillance Audit Due
September 1, 2021



ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat Zertifikat / 合格証

VEGA 1202050C P0011 C004

exida hereby confirms that the:

Radiation-based Transmitters PROTRAC 30 Series

**VEGA Grieshaber KG
Schiltach - Germany**

Have been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; Route 1_H

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

Safety Function:

The PROTRAC 30 Series Transmitter will measure the level of the process material 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

PROTRAC 30 Series
Transmitter



80 N Main St
Sellersville, PA 18960

T-013, V3R7

Certificate / Certificat / Zertifikat / 合格証

VEGA 1202050C P0011 C004

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT = 0; Route 1_H

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

Systematic Capability:

These Products have 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 these products 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:

Applications with continuous level measurement and level limit detection of liquids and bulk solids.
Hardware version 1.0.6 and Software version 2.1.0

Single or Master devices:

- C1 – Point Level PT31, MT31, MT32 using relay output (MIN/MAX)
- C2 – Point Level PT31, MT31, MT32 using 8/16mA current output (MIN/MAX)
- C3 – Level MT31, MT32, FT31/32, ST31 (short) using 4...20mA current output (MIN/MAX/RANGE)
- C4 – Level FT31/32, ST31 (long) using 4...20mA current output (MIN/MAX)

Slave devices:

- C5 – Level FT31/32, ST31 (short scintillator) (MIN/MAX/RANGE)
- C6 – Level FT31/32, ST31 (long scintillator) (MIN/MAX)

Configuration	λ_S	λ_{DD}	λ_{DU}	λ_H	λ_L	λ_{AD}	λ_{AU}
C1: MIN/MAX limit detection	458	1097	123	0	0	24	30
C2, C3, C4: MIN/MAX limit detection	123	1413	125	12	71	86	11
C3: Range measurement	0	1507	154	12	71	86	11
C5: Range measurement	0	1466	149	0	0	19	2
C5, C6: MIN/MAX limit detection	123	1372	120	0	0	19	2
C3 with 2 slaves, C5: RANGE measurement	0	4439	451	12	71	125	16
C4 with 2 slaves C6: MIN/MAX limit detection	368	4157	365	12	71	125	16

All failure rates are given in FIT (failures / 10⁹ 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.

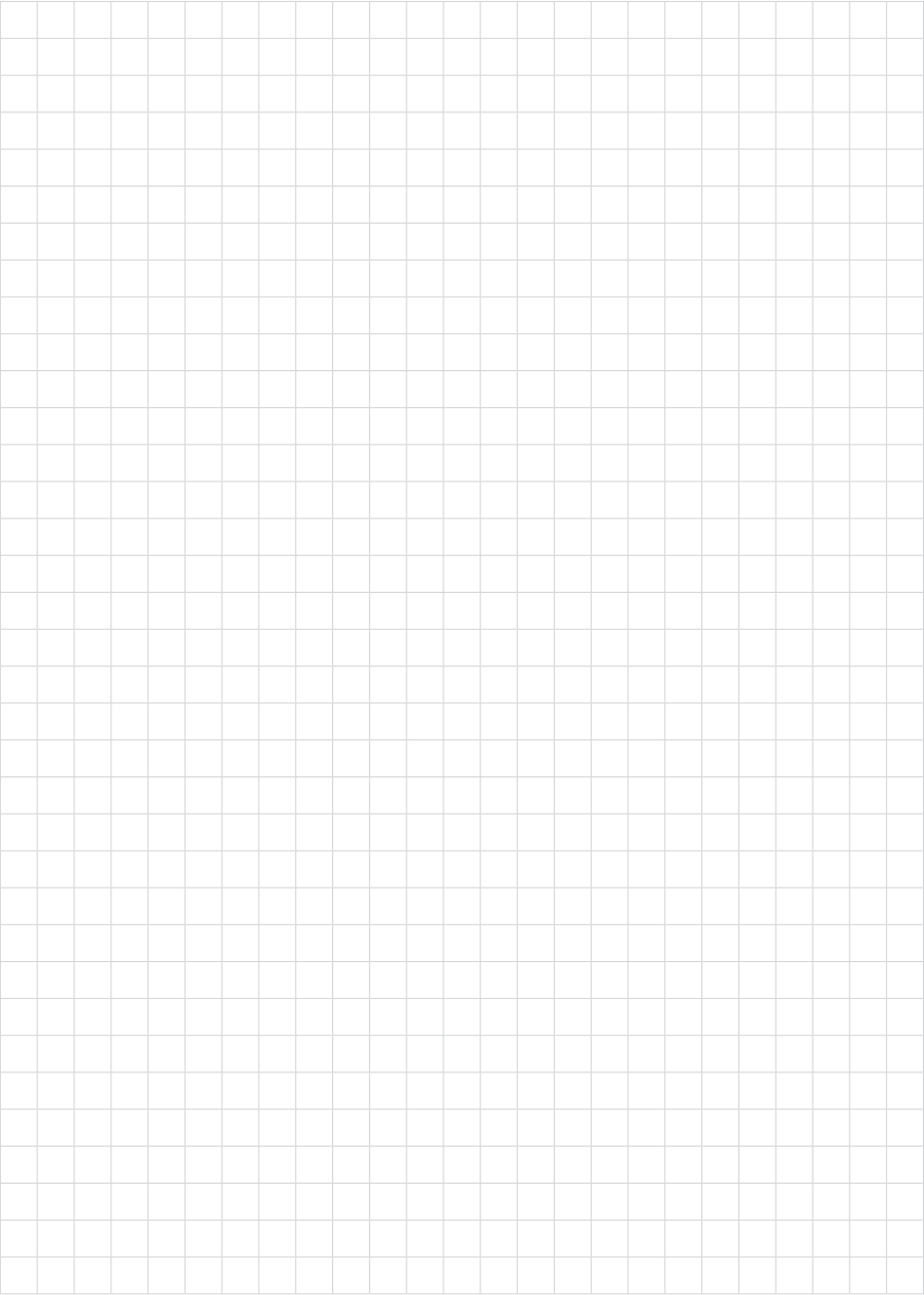
The following documents are a mandatory part of certification:

Assessment Report: VEGA 1202-050-C R008 V1R4

Safety Manual: PROTRAC 30 Series 49354

Page 2 of 2

49354-DE-190820



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 2019



49354-DE-190820

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