

Safety Manual

- Sonden VA40 ... ZG7 mit integriertem Umformer UVA im Gehäuse AS80
- Sonden VA40 ... ZG10 mit integriertem Umformer UVA im Gehäuse AS80
- Messrohre VA Di ... ZG1 mit integriertem Umformer UVA im Gehäuse AS80 oder AS102

- Sonden VA40 ... ZG8 Ex-d mit integriertem Umformer UVA-Ex-d im druckfest gekapselten Gehäuse Ex-d
- Sonden VA40 ... ZG9 Ex-d mit integriertem Umformer UVA-Ex-d im druckfest gekapselten Gehäuse Ex-d
- Messrohre VA Di ... ZG1 Ex-d mit integriertem Umformer UVA-Ex-d im druckfest gekapselten Gehäuse Ex-d



VA40 ... ZG7 + VA40 ... ZG10 (PVDF)



VA40 ... ZG8 Ex-d + VA40 ... ZG9 Ex-d



VA DI ... ZG1



VA DI ... ZG1 Ex-d

Inhaltsverzeichnis

- 1 Sicherheitssymbole**
- 2 Betriebssicherheit**
- 3 Planung / Auslegung**
 - 3.1 Einsatz im Ex-Bereich
 - 3.2 Auswahl des Einbauorts
 - 3.3 Sicherheitsbezogene Systeme gem. IEC 61508
SIL 1, SIL 2 und SIL 2/SC3
- 4 Lieferumfang**
- 5 Normenkonformität**
- 6 Begriffsbestimmungen und Abkürzungen**
- 7 Sicherheitstechnisches System (SIS)**
- 8 Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFD_{avg})**
- 9 Sicherheitsintegrität der Hardware**
- 10 Inbetriebnahme**
- 11 Verhalten im Betrieb und bei Störung**
- 12 Wiederkehrende Prüfungen des Strömungsmessgeräts**
 - 12.1 Sicherheitsüberprüfung
 - 12.2 Funktionsprüfung
- 13 Reparaturen**
- 14 Sicherheitstechnische Kenngrößen**
- 15 Konformitätsbescheinigung (Certificate of Compliance)**

1 Sicherheitssymbole



Warnung! Bei Nichtbeachtung der Anweisung kann es zu schweren Personen- und Sachschäden kommen!



Wichtiger Hinweis! Bei Nichtbeachtung kann es zu einer Beschädigung des Gerätes oder zu Einschränkungen der Gerätefunktion führen!

2 Betriebssicherheit



Alle im Folgenden beschriebenen Schritte dürfen nur von dafür qualifiziertem Fachpersonal vorgenommen werden!

Vor dem Auspacken des Gerätes Bedienungsanleitung sorgfältig lesen!

Nur bei bestimmungsgemäßer Handhabung des Gerätes ist ein sicherer Betrieb möglich. Nicht sachgemäßer Umgang kann zu schweren Personen- und Sachschäden führen.

Das Safety Manual hat nur in Verbindung mit der Bedienungsanleitung und bei Ex-Geräten zusätzlich nur in Verbindung mit der Betriebsanleitung des entsprechenden Gerätes Gültigkeit.

3 Planung / Auslegung



3.1 Einsatz im Ex-Bereich

Im Falle des Einsatzes in explosionsgefährdeten Bereichen dürfen nur dafür zugelassene Geräte zum Einsatz kommen. Hierbei ist besonders die Betriebsanleitung UVA-Ex-d zu beachten.



3.2 Auswahl des Einbauortes

Der Einbauort muss sorgfältig ausgewählt werden, damit die Messgenauigkeit des Gerätes optimal genutzt werden kann. Bitte beachten Sie dazu die Hinweise in der Bedienungsanleitung.



3.3 Sicherheitsbezogene Systeme gem. IEC 61508 SIL 1, SIL 2 und SIL 2/SC3 (SIL 3 in 1oo2 Architektur)

Voraussetzungen:

- Der Betriebsmode des Gerätes ist der „Low Demand Mode“ (Betriebsart mit niedriger Anforderungsrate)
- Die Analogausgangswerte ≥ 21 mA und $\leq 3,6$ mA werden von der nachfolgenden Steuerung als Fehlerfall diagnostiziert, der Prozess geht in den sicheren Zustand.
- Sicherheitsfunktionen können nicht mit dem Digitalausgang realisiert werden, da über den Digitalausgang keine Fehlerdiagnose erfolgen kann.
- Eine Messwertabweichung von weniger als 10 % vom Messwert hat keine Auswirkung auf die Sicherheitsfunktion.
- Die Funktionsfähigkeit des Geräts muss durch Wiederholungsprüfungen in regelmäßigen Zeitabständen geprüft werden.

4 Lieferumfang

Bitte kontrollieren Sie den Lieferumfang gemäß der Auflistung im Technischen Blatt, das Sie mit der Geräteelieferung erhalten. Achten Sie hierbei auch auf mögliche Kleinteile (z. B. Schraubensatz, Dichtungen).

Für den Einsatz in 'Sicherheitsbezogenen Anwendungen (SIL 1, SIL 2 und SIL 3 in 1oo2 Architektur)' muss das Gerät mit **einem SIL-Logo am Elektronikgehäuse ausgestattet sein und im Technischen Blatt muss die SIL-Konformität bestätigt sein (siehe Lieferunterlagen zum Gerät).**

5 Normenkonformität

Für die Funktionale Sicherheit gelten zusätzlich folgende Normen:

DIN EN 61508 Teil 1 bis Teil 7:2010
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

DIN EN 61511 Teil 1 bis Teil 3:2016
Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie

Die Strömungsmessgeräte entsprechen der Norm DIN EN 61508 Teil 1 bis Teil 7 und dürfen in sicherheitstechnischen Systemen nach der Norm DIN EN 61511 Teil 1 bis Teil 3 eingesetzt werden.

6 Begriffsbestimmungen und Abkürzungen

Nachfolgend sind einige Begriffe erklärt:

deutsch	englisch	Erklärung
Funktionale Sicherheit	functional safety	bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion der sicherheitsbezogenen (Sub-)Systeme und externer Einrichtungen zur Risikominderung abhängt.
Sicherheits-Integritätslevel (SIL)	safety integrity level (SIL)	Er dient der Beurteilung elektrischer / elektronischer / programmierbar elektronischer (E/E/PE)-Systeme in Bezug auf die Zuverlässigkeit von Sicherheitsfunktionen. Aus dem angestrebten Level ergeben sich die sicherheitsgerichteten Konstruktionsprinzipien, die eingehalten werden müssen, damit das Risiko einer Fehlfunktion minimiert werden kann. SIL 4 = höchste Stufe, SIL 1 = niedrigste Stufe.
Sicherheitstechnisches System (SIS)	safety instrumented system (SIS)	Sicherheitstechnisches System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein SIS besteht aus Sensor(en), Logiksystem und Aktor(en).
Zeitspanne der Analyse	mission time	Zeitspanne der Fehlermöglichkeits- und Einflussanalyse
Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFDG/PFD _{avg})	average probability of failure on demand (PFDG/PFD _{avg})	gemittelte Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion bei Anforderung
Mittlere Wahrscheinlichkeit für die Auslösung eines störenden Fehlers (PFS _{avg})	average probability of causing a spurious trip of the process (PFS _{avg})	die gemittelte Wahrscheinlichkeit für die Auslösung eines störenden Fehlers im Prozess
Wahrscheinlichkeit für fehlerfreie Funktion (OK)	probability product is running without any failures (OK)	die Wahrscheinlichkeit für fehlerfreie Funktion
Fehlermöglichkeits- und Einflussanalyse (FMEA)	Failure Mode and Effects Analysis (FMEA)	FMEA: Fehlermöglichkeits- und Einflussanalyse
Betriebsart	mode of operation	- Betriebsart mit niedriger Anforderungsrate (low demand mode), wobei die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist - Betriebsart mit hoher Anforderungsrate oder Betriebsart mit kontinuierlicher Anforderung (high demand or continuous mode), wobei die Anforderungsrate an das sicherheitsbezogene System mehr als einmal pro Jahr beträgt oder größer als die doppelte Frequenz der Wiederholungsprüfung ist
Anteil ungefährlicher Fehler (SFF)	safe failure fraction (SFF)	Anteil der ungefährlichen Fehler bezogen auf die insgesamt möglichen Fehler
Fehlertoleranz der Hardware (HFT)	hardware fault tolerance (HFT)	Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern und Abweichungen weiter auszuführen
Fehler pro Zeiteinheit (FIT)	failure in time (FIT)	1 FIT = 1 Fehler pro 10 ⁹ Stunden
Ausfallrate (λ)	failure rate (λ)	Ausfallrate Kat. „sd“ =safe detected=sicher erkannt Ausfallrate Kat. „su“ =safe undetected=sicher unerkannt Ausfallrate Kat. „dd“ =dangerous detected=gefährlich erkannt Ausfallrate Kat. „du“ =danger. undetected=gefährl. unerkannt
Mittlere Dauer bis zum Ausfall (MTTF)	mean time to failure (MTTF)	Mittlere Dauer bis zum Ausfall. Kat. „s“ = safe = sicher, Kat. „d“ = dangerous = gefährlich

1oo2 SIL 3 durch homogene Redundanz, systematische Eignung (SC 3)	1oo2 SIL 3 by redundancy setup, systematic capability (SC 3)	Zwei identische Betriebsmittel sind für SIL 3 in der Architektur 1oo2 geeignet. Jedes Betriebsmittel kann die Sicherheitsfunktion ausführen
Diagnosedeckung (DC)	diagnostic coverage (DC)	Diagnosedeckung Kat. „s“ = safe = sicher Diagnosedeckung Kat. „d“ = dangerous = gefährlich

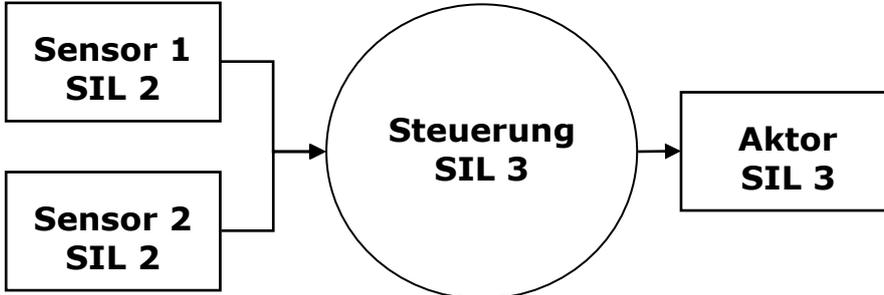
7 Sicherheitstechnisches System (SIS)

Ein sicherheitstechnisches System besteht üblicherweise aus den drei Teilsystemen Eingangsteilsystem (Sensor/-en), Logik-Teilsystem (SPS oder Leitsystem) und Ausgangs-Teilsystem (Stellgerät, Aktor). Die mittlere Wahrscheinlichkeit eines Ausfalls PFDG/PFD_{avg} bei Anforderung wird dabei üblicherweise wie folgt aufgeteilt:

Einkanaliges Sicherheitssystem (1oo1)



Mehrkanaliges Sicherheitssystem (1oo2)



8 Mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFD_{avg})

Diese Tabelle gibt den erreichbaren Sicherheits-Integritätslevel (SIL) in Abhängigkeit von der mittleren Wahrscheinlichkeit eines Ausfalls bei Anforderung wieder. Die angegebenen Ausfallgrenzen sind hierbei gültig für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate (low demand mode) betrieben wird.

Sicherheits-Integritätslevel (SIL)	PFD _{avg} mit niedriger Anforderungsrate (low demand mode)
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

9 Sicherheitsintegrität der Hardware

Diese Tabelle gibt den erreichbaren Sicherheits-Integritätslevel (SIL) für Typ B Geräte (nach IEC61508-2) in Abhängigkeit vom Anteil der ungefährlichen Ausfälle (SFF) und der Fehlertoleranz der Hardware (HFT) an:

Anteil ungefährlicher Fehler (SFF)	Fehlertoleranz der Hardware (HFT)		
	0	1 (0)*	2
< 60%	nicht erlaubt	SIL 1	SIL 2
60% bis < 90%	SIL 1	SIL 2	SIL 3
90% bis < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

* Mit Nachweis der Betriebsbewährung nach IEC/EN 61511 für SIL 1 bis SIL 3

Die zertifizierten Betriebsmittel entsprechen SIL 2 mit einer systematischen Kapazität von SC3 nach IEC 61508 route 2. Einsatz entsprechend IEC 61511 für SIL 1 und SIL 2 in 1oo1 und für SIL3 in 1oo2 Konfigurationen.

10 Inbetriebnahme

Die Inbetriebnahme des Strömungsmessgeräts ist in der jeweiligen Bedienungsanleitung für das Gerät beschrieben. Bei Anwendungen für den Einsatz im Ex-Bereich ist zusätzlich die jeweilige Betriebsanleitung für das Gerät zu beachten.

11 Verhalten im Betrieb und bei Störung

Das Verhalten im Betrieb und bei Störungen ist in der jeweiligen Bedienungsanleitung für das Gerät beschrieben.

12 Wiederkehrende Prüfungen des Strömungsmessgeräts

12.1 Sicherheitsüberprüfungen

Gemäß IEC 61508/61511 ist die Sicherheitsfunktion des gesamten Sicherheitskreises regelmäßig zu überprüfen. Die hierfür notwendigen Testintervalle werden bei der Berechnung des jeweiligen Sicherheitskreises bestimmt.

12.2 Funktionsprüfung

Die ordnungsgemäße Funktionsfähigkeit des Strömungsmessgeräts ist regelmäßig mindestens alle 5 Jahre zu überprüfen. Die Überprüfung kann nur durch den Hersteller durchgeführt werden. Bei ungünstigen Prozessbedingungen können kürzere Prüfintervalle durch den Betreiber festgelegt werden.

13 Reparaturen

Defekte Geräte sollten unter Angabe der genauen Störung bzw. Ursache an die Reparaturabteilung der Firma Höntzsch GmbH & Co. KG gesandt werden.

14 Sicherheitstechnische Kenngrößen

Auszug aus dem Prüfbericht Nr. 2266.465.1 Version 1 (Reliability Study – Vortex Sensors)

Properties:

Device Type: B

Mode of operation: low demand mode

Hardware fault tolerance: 0

Table 1 - Results FMEDA at +55 °C

Properties	VA40 ... ZG7 VA40 ... ZG10 VA40 ... ZG8 Ex-d VA40 ... ZG9 Ex-d VA Di ... ZG1 VA Di ... ZG1 Ex-d		
	FMEDA	Proven In Use	90% Confidence
Safe failure rate	248	40	62
Safe detected failure rate	0	n.a.	n.a.
Safe undetected failure rate	248	n.a.	n.a.
Dangerous failure rate	56	5.7	18
Dangerous detected failure rate	34	n.a.	n.a.
Dangerous undetected failure rate	22	n.a.	n.a.
DC	61%	n.a.	n.a.
Safe failure fraction	93%	n.a.	n.a.
MTTFd [years]	1768		

Notes:

Failure rates are in FIT 10⁻⁹/h.

Confidence interval according to IEC 61508 route 2h.

IEC 61508 requires a minimum DC of 60% for Type B products for route 2h, 2s.

Table 2 - Results PFDG Calculations (1oo1)

Years	VA40 ... ZG7 VA40 ... ZG10 VA40 ... ZG8 Ex-d VA40 ... ZG9 Ex-d VA Di ... ZG1 VA Di ... ZG1 Ex-d				
	1	2	5	10	20
PFDG	9.8E-05	1.95E-04	4.9E-04	9.7E-04	2E-03
%SIL 2	1%	2%	5%	10%	20%
PFSavg			9.7E-05		

MRT, MTTR 8h

Table 3 -Results PFDG Calculations (1oo2)

	VA40 ... ZG7 VA40 ... ZG10 VA40 ... ZG8 Ex-d VA40 ... ZG9 Ex-d VA Di ... ZG1 VA Di ... ZG1 Ex-d				
Years	1	2	5	10	20
PFDG	5.7E-06	1.12E-05	2.77E-05	5.52E-05	1.10E-04
%SIL 2	1%	2%	5%	10%	20%

MRT, MTTR 72h, β 5% (common cause)

Summary results

The proven in use analysis demonstrates that the hardware of the Vortex Sensors VA40 ... ZG7/ZG10/ZG8/ZG9 and VA Di ... ZG1/Ex-d are corresponding with SIL 2 safety properties according to IEC 61508, route 2h and route 2s SIL 3 in 1oo2 configuration.

15



Certificate of compliance
Product



Holder Höntzsch GmbH, Waiblingen, Germany

Compliant Item Vortex Sensors VA40 ... ZG7 and VA40 ... ZG8
Vortex Sensors VA Di...ZG1 and VA Di...ZG1 Ex-d

Basis of Certification IEC 61508:2010

Certification Include(s) Safety requirements specification
 Hardware requirements
 Reliability requirements
 Software requirements
 Basic safety
 User documentation

Functional Safety Data

Safety function: See report
Mode: Low demand
Type: B
HFT: 0
Hardware compliance route: 2_H
Systematic compliance route: 2_S
Systematic capability: SC3
Failure rates (FIT): SD=0, SU=248, DD=34, DU=22
Safe failure fraction: 93%
Diagnostic coverage: 61%
Fit for use up to: SIL 3
Fit for use up to: STL 5

Certification Results Risknowlogy certifies that the above Compliant Item meets the requirements of the Basis of Certification for the selected assessment(s). The Risknowlogy report 2266.465.1 are an integral part of this certificate.

Certificate Number 2266.465.2

Issue Date 2019-06-09

Expiry Date After modification of Compliant Item

A handwritten signature in blue ink, appearing to read 'Michel Houtermans'.

Certifier Dr. Michel Houtermans



www.risknowlogy.com

Höntzsch GmbH & Co. KG
Gottlieb-Daimler-Straße 37
D-71334 Waiblingen
Telefon +49 7151 / 17 16-0
E-Mail info@hoentzsch.com
Internet www.hoentzsch.com

Änderungen vorbehalten