KROHNE

Safety Manual
OPTISWITCH Serie 5000

- Zweileiter

Document
ID: 32750

Schwebekörper-Durchflussmessgeräte
Wirbelfrequenz-Durchflussmessgeräte
Durchflusskontrollgeräte
Magnetisch-Induktive Durchflussmessgeräte
Ultraschall-Durchflussmessgeräte
Masse-Durchflussmessgeräte
Füllstand-Messgeräte
Kommunikationstechnik
Engineering-Systeme & -Lösungen
Schaltgeräte, Zähler, Anzeiger und Schreiber
Energie
Druck und Temperatur

Inhaltsverzeichnis

1 Funktionale Sicherheit

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

Redaktionsstand: 2013-11-13

32750-DE-131113

1 Funktionale Sicherheit

1.1 Allgemein

Geltungsbereich

Dieses Sicherheitshandbuch gilt für Messsysteme, bestehend aus dem Vibrationsgrenzschalter OPTISWITCH Serie 5000 mit Elektronikeinsatz SWE60Z:

OPTISWITCH 5100 C, 5150 C, 5200 C, 5250 C

Hinweis:
Bei Geräten mit emaillierter Gabel ist der Elektronikeinsatz SWE60Z.E oder SWE60Z.E1 erforderlich.

Einsatzbereich

Das Messsystem kann zur Grenzstanderfassung von Flüssigkeiten, welche den besonderen Anforderungen der Sicherheitstechnik genügt, eingesetzt werden.

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

SIL-Konformität

Die SIL-Konformitätserklärung können Sie im Internet auf unserer Homepage herunterladen.

Abkürzungen, Begriffe

SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
SFF	Safe Failure Fraction
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Probability of a dangerous Failure per Hour
FMEDA	Failure Mode, Effects and Diagnostics Analysis
λ_{sd}	Rate for safe detected failure
λ_{su}	Rate for safe undetected failure
λ_{dd}	Rate for dangerous detected failure
λ_{du}	Rate for dangerous undetected failure
DC_S	Diagnostic Coverage of safe failures; $DC_S = \lambda_{sd}/(\lambda_{sd}+\lambda_{su})$
DC_D	Diagnostic Coverage of dangerous failures; $DC_D = \lambda_{dd}/(\lambda_{dd}+\lambda_{du})$
FIT	Failure In Time (1 FIT = 1 failure/10^9 h)
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair

Weitere Abkürzungen und Begriffe sind in der IEC 61508-4 benannt.

Relevante Normen

- IEC 61508
  - Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511-1
  - Functional safety - safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements

Sicherheitsanforderungen

Ausfallgrenzwerte für eine Sicherheitsfunktion, abhängig von der SIL-Klasse (IEC 61508-1, 7.6.2)

Sicherheits-Integritäts-Level	**Betriebsart mit niedriger Anforderungsrate**	**Betriebsart mit hoher Anforderungsrate**
SIL	**PFD_{avg}**	**PFH**
4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Sicherheitsintegrität der Hardware für sicherheitsbezogene Teilsysteme vom Typ A (IEC 61508-2, 7.4.3)

Anteil ungefährlicher Ausfälle	Fehlertoleranz der Hardware		
SFF	**HFT = 0**	**HFT = 1**	**HFT = 2**
< 60 %	SIL1	SIL1	SIL3
60 % … < 90 %	SIL2	SIL3	(SIL4)
90 % … < 99 %	SIL3	(SIL4)	(SIL4)
≥ 99 %	SIL3	(SIL4)	(SIL4)

Betriebsbewährtheit

Nach IEC 61511-1, Abschnitt 11.4.4 kann für betriebsbewährte Teilsysteme die Fehlertoleranz HFT um eins reduziert werden, wenn folgende Bedingungen erfüllt sind:

- Das Gerät ist betriebsbewährt
- Am Gerät können nur prozessrelevante Parameter geändert werden (z. B. Messbereich, Stromausgang bei Störung …)
- Die Veränderung dieser prozessrelevanten Parameter ist geschützt (z. B. Passwort, …)
- Die Sicherheitsfunktion erfordert kleiner SIL4

Die Beurteilung des Änderungswesens war Bestandteil des Nachweises der Betriebsbewährtheit.

1.2 Projektierung

Sicherheitsfunktion

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

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

Sicherer Zustand

Der sichere Zustand ist abhängig von der Betriebsart:

	Überlaufschutz (Max.-Betrieb)	**Trockenlaufschutz (Min.-Betrieb)**
Schwingelement im sicheren Zustand	bedeckt	unbedeckt
Ausgangsstrom im sicheren Zustand	12,5 … 23,5 mA	2,3 … 11,5 mA
Störstrom "fail low"	< 2,3 mA	< 2,3 mA

	Überlaufschutz (Max.-Betrieb)	Trockenlaufschutz (Min.-Betrieb)
Störstrom "fail high"	> 23,5 mA	> 23,5 mA

Fehlerbeschreibung

Ein ungefährlicher Ausfall (safe failure) liegt vor, wenn das Messsystem ohne Anforderung des Prozesses in den definierten sicheren Zustand oder in den Störmodus wechselt.

Ein gefährlicher unentdeckter Ausfall (dangerous undetected failure) liegt vor, wenn das Messsystem bei einer Anforderung des Prozesses weder in den definierten sicheren Zustand, noch in den Störmodus wechselt.

Konfiguration der Auswerteinheit

Liefert das Messsystem Ausgangsströme von "*fail low*" oder "*fail high*", so muss davon ausgegangen werden, dass eine Störung vorliegt.

Die Auswerteinheit muss deshalb solche Ströme als Störung interpretieren und eine geeignete Störmeldung ausgeben.

Ist dies nicht der Fall, so müssen die entsprechenden Anteile der Ausfallraten den gefährlichen Ausfällen zugeordnet werden. Somit können sich die genannten Zahlenwerte im Kapitel "*Sicherheitstechnische Kennzahlen*" verschlechtern.

Die Auswerteinheit muss dem SIL-Level der Messkette entsprechen.

Betriebsart mit niedriger Anforderungsrate

Beträgt die Anforderungsrate nicht mehr als einmal pro Jahr, so darf das Messsystem als sicherheitsrelevantes Teilsystem in der Betriebsart "*low demand mode*" eingesetzt werden (IEC 61508-4, 3.5.12).

Wenn das Verhältnis der internen Diagnosetestrate des Messsystems zur Anforderungsrate den Wert 100 überschreitet, kann das Messsystem so behandelt werden, als wenn es eine Sicherheitsfunktion in der Betriebsart mit niedriger Anforderungsrate ausführt (IEC 61508-2, 7.4.3.2.5).

Zugehörige Kenngröße ist der Wert PFD_{avg} (average Probability of dangerous Failure on Demand). Der Wert ist abhängig vom Prüfintervall T_{Proof} zwischen den Funktionstests der Schutzfunktion.

Zahlenwert siehe Kapitel "*Sicherheitstechnische Kennzahlen*".

Betriebsart mit hoher Anforderungsrate

Trifft "*Betriebsart mit niedriger Anforderungsrate*" nicht zu, so ist das Messsystem als sicherheitsrelevantes Teilsystem in der Betriebsart "*high demand mode*" einzusetzen (IEC 61508-4, 3.5.12).

Die Fehlertoleranzzeit des Gesamtsystems muss dabei größer sein als die Summe der Reaktionszeiten bzw. der Diagnosetestdauern aller Komponenten der Sicherheitsmesskette.

Zugehörige Kenngröße ist der Wert PFH (Ausfallrate).

Zahlenwert siehe Kapitel "*Sicherheitstechnische Kennzahlen*".

Annahmen

Bei der Durchführung der FMEDA wurden folgende Annahmen zugrunde gelegt:

- Ausfallraten sind konstant, Abnützung der mechanischen Teile sind nicht betrachtet

- Ausfallraten von externen Stromversorgungen sind nicht mit einberechnet
- Mehrfachfehler sind nicht betrachtet
- Die mittlere Umgebungstemperatur während der Betriebszeit beträgt 40 °C (104 °F)
- Die Umweltbedingungen entsprechen einer durchschnittlichen industriellen Umgebung
- Die Gebrauchsdauer der Bauteile liegt im Bereich von 8 bis 12 Jahren (IEC 61508-2, 7.4.7.4, Anmerkung 3)
- Die Reparaturzeit (Austausch des Messsystems) nach einem ungefährlichen Ausfall beträgt acht Stunden (MTTR = 8 h)
- Die Auswerteinheit kann "*fail low*"- und "*fail high*"-Ausfälle als Störung interpretieren und eine geeignete Störmeldung ausgeben
- Das Abtastintervall einer angeschlossenen Steuer- und Auswerteinheit beträgt max. 1 Stunde, um auf gefährliche erkennbare Ausfälle zu reagieren

Allgemeine Hinweise und Einschränkungen

Es ist auf einen anwendungsgemäßen Einsatz des Messsystems unter Berücksichtigung von Druck, Temperatur, Dichte und chemische Eigenschaften des Mediums zu achten.

Die anwendungsspezifischen Grenzen sind einzuhalten. Die Spezifikationen der Betriebsanleitung dürfen nicht überschritten werden.

Beim Einsatz als Trockenlaufschutz ist zu beachten:

- Anhaftung von Füllgut am Schwingsystem vermeiden (möglicherweise sind kleinere Prooftest-Intervalle notwendig)
- Im Füllgut eingelagerte Festkörper > 5 mm (0.2 in) vermeiden
- Schaumbildung mit einer Dichte > 0,5 g/cm^3 (0.018 lbs/in^3) vermeiden

1.3 Einstellhinweise

Bedienelemente

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

- DIL-Schalter zur Empfindlichkeitsumschaltung

Die Funktion der Bedienelemente ist in der Betriebsanleitung beschrieben.

1.4 Inbetriebnahme

Montage und Installation

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

Im Rahmen der Inbetriebnahme wird empfohlen, anhand einer Erstbefüllung die Sicherheitsfunktion zu überprüfen.

1.5 Verhalten im Betrieb und bei Störungen

Betrieb und Störung

Die Einstellelemente bzw. Geräteparameter dürfen im Betrieb nicht verändert werden.

Bei Veränderungen im Betrieb sind die Sicherheitsfunktionen zu beachten.

Auftretende Störmeldungen sind in der Betriebsanleitung beschrieben.

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

Ein Austausch der Elektronik ist einfach möglich und in der Betriebsanleitung beschrieben. Dabei sind die Hinweise zur Parametrierung und Inbetriebnahme zu beachten.

Werden aufgrund eines festgestellten Fehlers die Elektronik oder der gesamte Sensor ausgetauscht, so ist dies dem Hersteller zu melden (inklusive einer Fehlerbeschreibung).

1.6 Wiederkehrender Funktionstest

Begründung und Durchführung

Der wiederkehrende Funktionstest dient dazu, die Sicherheitsfunktion zu überprüfen, um mögliche, nicht erkennbare gefährliche Fehler aufzudecken. Die Funktionsfähigkeit des Messsystems ist deshalb in angemessenen Zeitabständen zu prüfen.

Es liegt in der Verantwortung des Betreibers, die Art der Überprüfung zu wählen. Die Zeitabstände richten sich nach dem in Anspruch genommenen PFD_{avg}-Wert laut Tabelle und Diagramm im Abschnitt "*Sicherheitstechnische Kennzahlen*".

Bei hoher Anforderungsrate ist in der IEC 61508 kein wiederkehrender Funktionstest vorgesehen. Ein Nachweis der Funktionstüchtigkeit wird hier in der häufigeren Inanspruchnahme des Messsystems gesehen. In zweikanaligen Architekturen ist es jedoch sinnvoll, die Wirkung der Redundanz durch wiederkehrende Funktionstests in angemessenen Zeitabständen nachzuweisen.

Die Prüfung ist so durchzuführen, dass die Sicherheitsfunktion im Zusammenwirken aller Komponenten einwandfrei nachgewiesen wird.

Dies ist bei einem Anfahren der Ansprechhöhe im Rahmen einer Befüllung gewährleistet. Wenn eine Befüllung bis zur Ansprechhöhe nicht praktikabel ist, so ist das Messsystem durch geeignete Simulation des Füllstandes oder des physikalischen Messeffekts zum Ansprechen zu bringen.

Die bei den Tests verwendeten Methoden und Verfahren müssen benannt und deren Eignungsgrad spezifiziert werden. Die Prüfungen sind zu dokumentieren.

Verläuft der Funktionstest negativ, muss das gesamte Messsystem außer Betrieb genommen werden und der Prozess durch andere Maßnahmen im sicheren Zustand gehalten werden.

In einer mehrkanaligen Architektur gilt dies getrennt für jeden Kanal.

Einfacher Funktionstest

Wenn die Bedingungen der nachfolgenden Hinweise zutreffen, kann durch Unterbrechung der Spannungsversorgung von mindestens zwei Sekunden ein einfacher Funktionstest ausgelöst werden.

Dies kann geschehen durch:

- Manuelle Unterbrechung der Versorgungsleitung
- Unterbrechung der Versorgungsleitung durch eine nachgeschalte Steuerung (SSPS)

- Betätigung der **Testtaste** an einem nachgeschalten Auswertgerät (geeignete Auswertgeräte finden Sie im Kapitel "*Technische Daten*" der Betriebsanleitung

Hinweis:
Bedingungen für den einfachen Funktionstest:

- Eine mechanische Beschädigung des Schwingelements sowie Korrosion ist ausgeschlossen
- Die Bildung von Anhaftungen am Schwingelement, die zu einer erheblichen Dämpfung der Schwingfrequenz führt, ist ausgeschlossen
- Es dürfen sich keine Feststoffanteile im Medium befinden, die sich in der Schwinggabel verklemmen können

1.7 Sicherheitstechnische Kennzahlen

Grundlagen

Die Ausfallraten der Elektronik, der mechanischen Teile des Messwertaufnehmers, sowie des Prozessanschlusses wurden durch eine FMEDA nach IEC 61508 ermittelt. Den Berechnungen sind Bauelementeausfallraten nach SN 29500 zugrunde gelegt. Alle Zahlenwerte beziehen sich auf eine mittlere Umgebungstempertur während der Betriebszeit von 40 °C (104 °F).

Für eine höhere durchschnittliche Temperatur von 60 °C (140 °F) sollten die Ausfallraten erfahrungsgemäß mit einem Faktor von 2,5 multipliziert werden. Ein ähnlicher Faktor gilt, wenn häufige Temperaturschwankungen zu erwarten sind.

Die Berechnungen stützen sich weiterhin auf die im Kapitel "*Projektierung*" genannten Hinweise.

Nutzungsdauer

Nach 8 bis 12 Jahren werden sich die Ausfallraten der elektronischen Bauelemente vergrößern, wodurch sich die daraus abgeleiteten PFD- und PFH-Werte verschlechtern (IEC 61508-2, 7.4.7.4, Anmerkung 3).

Ausfallraten

	Überlaufschutz (Max.-/A-Betrieb)	**Trockenlaufschutz (Min.-/B-Betrieb)**
λ_{sd}	35 FIT	141 FIT
λ_{su}	101 FIT	91 FIT
λ_{dd}	141 FIT	35 FIT
λ_{du}	25 FIT	35 FIT
MTBF = MTTF + MTTR	3,31 x 10^6 h	3,31 x 10^6 h

Fehlerreaktionszeit

Fehlerreaktionszeit	< 1,5 sek.

Spezifische Kennzahlen

Einkanalige Architektur (1oo1D)

SIL	SIL2
HFT	0
Gerätetyp	Typ A

	Überlaufschutz (Max.-/A-Betrieb)	Trockenlaufschutz (Min.-/B-Betrieb)
SFF	91 %	88 %
PFD_{avg}		
T_{Proof} = 1 Jahr	< 0,011 x 10^{-2}	< 0,016 x 10^{-2}
T_{Proof} = 5 Jahre	< 0,055 x 10^{-2}	< 0,078 x 10^{-2}
T_{Proof} = 10 Jahre	< 0,11 x 10^{-2}	< 0,155 x 10^{-2}
PFH	< 0,025 x 10^{-6}/h	< 0,035 x 10^{-6}/h

Zeitabhängiger Verlauf von PFD_{avg}

Der zeitliche Verlauf von PFD_{avg} verhält sich im Zeitraum bis 10 Jahren annähernd linear zur Betriebszeit. Die oben genannten Werte gelten nur für das T_{Proof}-Intervall, nach dem ein wiederkehrender Funktionstest durchgeführt werden muss.

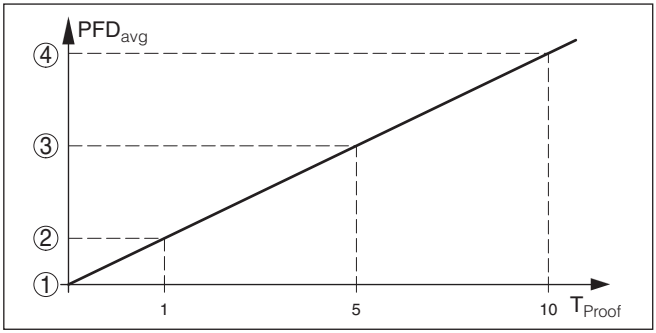

Abb. 1: Zeitabhängiger Verlauf von PFD_{avg} (Zahlenwerte siehe oben dargestellte Tabellen)

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

Mehrkanalige Architektur

Spezifische Kennzahlen

Wird das Messsystem in einer mehrkanaligen Architektur eingesetzt, so sind die sicherheitstechnischen Kennzahlen der gewählten Struktur der Messkette anhand der oben angegebenen Ausfallraten speziell für die gewählte Applikation zu berechnen.

Es ist ein geeigneter Common Cause Faktor zu berücksichtigen.

Änderungen vorbehalten