MTS SENSORS

Temposonics®

Magnetostriktive lineare Positionssensoren

Sensor mit Ex-Zulassung

TH – SIL 2-fähig
Sicherheitshandbuch

Inhaltsverzeichnis

1. Einleitung

Dieses Handbuch enthält Richtlinien für die elektrische Installation und den Betrieb der Temposonics® Sensoren der T-Serie mit analogem Ausgangssignal in sicherheitsrelevanten Anwendungen. Das Modell TH der T-Serie ist nach IEC 61508 SIL (Safety Integrity Level) zertifiziert.

IEC 61508	Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme

2. Risikoanalyse

IEC 61508 SIL	$MTTF_d$	High Demand Mode PFH
3	hoch, 30 < 100 Jahre	$\geq 10^{-8}$ bis $< 10^{-7}$
2	mittel, 10 < 30 Jahre	$\geq 10^{-7}$ bis $< 10^{-6}$
1	niedrig, 3 < 10 Jahre	$\geq 10^{-6}$ bis $< 10^{-5}$
Keine speziellen Anforderungen	-x–x-	$\geq 10^{-5}$ bis $< 10^{-4}$

Abb. 1: Wahrscheinlichkeit eines gefahrbringenden Ausfalls

3. Systemdesign

3.1 Redundante Ausführung ohne interne Diagnostik

Redundante Ausführung bedeutet, dass 2 Sensoren jeweils mit eigenständigem Ausgang (mit invertierter Wirkungsrichtung) vorhanden sind. Die Validierung der Funktion wird anhand eines Kreuzvergleichs durchgeführt, wobei die korrekte Ausgabe von 2 Signalen eines Sensors wie folgt definiert ist:

Z = CH (A) + CH (–B) = 0
mit: Z = Ergebnis des Kreuzvergleichs
CH (A) = Ausgabe des Positionssignals
CH (–B) = Ausgabe des invertierten Positionssignals

Wird dieses erforderliche Ergebnis Z = 0 nicht erzielt, interpretiert die Steuerung dies als Systemfehler und versetzt das System in einen Not-Halt.

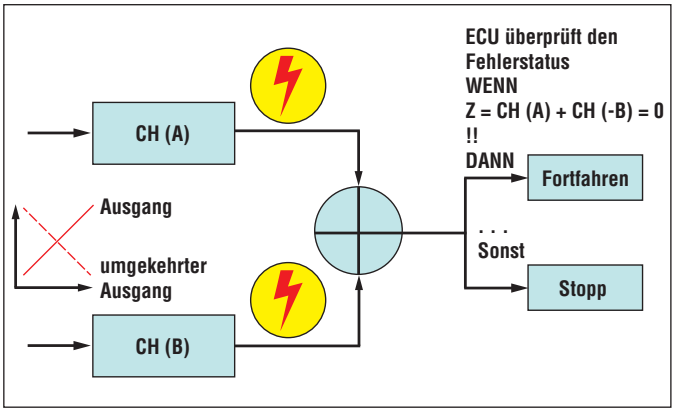

Abb. 2: Redundante Ausführung ohne Diagnostik

Ohne interne Kanaldiagnose kann das System nicht erkennen, welcher Kanal ausgefallen ist. Die Steuerung ist mit dem Vergleichsalgorithmus beschäftigt, die Verarbeitungskapazität wird reduziert.

3.2 Redundante Ausführung mit interner Diagnostik

Sensoren, die über eine eingebaute Eigendiagnosefunktion verfügen, können eine von der Verarbeitungsschleife unabhängige Fehlermeldung erzeugen. Der Sensor wird in den Fail-Safe-Zustand versetzt. In diesem Fall kann die Steuerung die Kanäle trennen, was es dem System ermöglicht in einen sicheren Betriebszustand zu schalten. In diesem Zustand arbeitet die Maschine im Einkanalbetrieb weiter, bis der ausgefallene Sensor ausgewechselt wird.

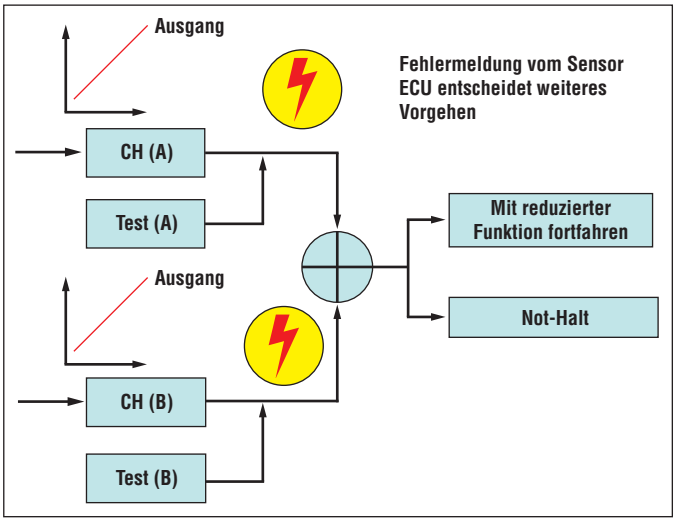

Abb. 3: Redundante Ausführung mit Diagnostik

3.3 Die Sicherheitsfunktion

Der Sicherheitssensor der T-Serie gibt kontinuierlich ein zur Magnetposition proportionales Positionssignal aus. Die eingebaute Diagnosefunktion prüft sicherheitsrelevante Hardware-Parameter. Im Fehlerfall liefert der Sensor ein Fehlerausgangssignal, welches das elektronische Steuerungsgerät (ECU) empfängt. Im Fehlerfall muss die ECU in geeigneter Weise reagieren, um die Notbetriebsfunktion zu gewährleisten. Das System fährt herunter oder arbeitet im Notbetrieb.

T-Serie Analog Safety	
Stromausgang	4…20 mA
Fehlerwert	< 3,6 mA (nahe 0 mA)

Abb. 4: T-Serie Ausgangsfunktion

Fehlertypen

1. Sichere Fehler (λ_{SD} und λ_{SU}) entdeckt und unentdeckt
2. Gefährliche Fehler (λ_{DD} und λ_{DU}) entdeckt und unentdeckt
   IEC 60079-14 und lokale Vorschriften.

Fehlertypen (λ) innerhalb sicherheitsbezogener Systeme		
Ausfallart	**entdeckt**	**unentdeckt**
Sicher (Fail Safe)	λ_{SD} sicher entdeckt	λ_{SU} sicher unentdeckt
	Der Sensor schaltet ohne entsprechenden Befehl der Steuerung in den sicheren Zustand.	
Gefährlich (Dangerous Fail)	λ_{DD} gefährlich entdeckt: Der Sensor befindet sich in einem gefährlichen Zustand (= inoperative function)	λ_{DU} gefährlich unentdeckt: Der Sensor kann nicht in den sicheren Zustand schalten

Abb. 5: Fehlertypen

4. Gerätespezifische Hinweise

4.1 Bestimmungsgemäße Verwendung / Zertifizierung

Bei der hier beschriebenen Ausführung der T-Serie handelt es sich um einen magnetostriktiven, linearen Positionssensor, der nach IEC 61508 zertifiziert ist. Dieser Sensor kann in der Betriebsart High Demand und Low Demand Mode eingesetzt werden. Der Sensor misst die relative Position eines verfahrbaren Magneten relativ zu dessen Null-Position. Das Ausgangssignal wird an eine externe Steuerung (ECU) übertragen und anforderungsgemäß verarbeitet.

4.2 Mechanischer und elektrischer Einbau

Neben den in der Betriebsanleitung der T-Serie dokumentierten Hinweisen existieren keine speziellen oder zusätzlichen Installationsanforderungen. Die Umgebungsbedingungen für den Betrieb sind im Abschnitt „Technische Daten“ der Betriebsanleitung (Dokumentennr. 551513) der T-Serie aufgeführt.

4.3 Betriebs- und Offline-Proof-Tests

Umfassende Informationen zu Leistung, Installation, Betrieb und technischen Daten für die Sicherheitsmodelle der T-Serie finden Sie in der Betriebsanleitung (Dokumentennr. 551513). Alle in der Betriebsanleitung für die analogen Sensoren der T-Serie dokumentierten Installationsempfehlungen sind anzuwenden. Für die Sicherheitsmodelle der T-Serie sind sämtliche Konfigurationen zulässig. Die Funktionstests der entsprechenden sicherheitsrelevanten Schaltkreise ermöglichen die zuverlässige Beurteilung aller verwendeten Komponenten (Sensor, Steuerung und weitere Bauteile). Die Verantwortung für die Durchführung des Proof-Tests trägt der Anwender (Prüfintervall 1 Jahr).

4.4 Wartung und Reparatur

Die Sicherheitsmodelle der T-Serie sind nicht für die Feldreparatur geeignet, sondern müssen zur Reparatur an MTS Sensors eingeschickt werden. Alle Bedienfehler, auf die keine 10 aufeinander folgenden Starts ohne Bedienfehler folgen, müssen im Fehlerbericht erfasst werden. Setzen Sie sich im Fehlerfall mit MTS Sensors in Verbindung.

4.5 Unzulässige und sicherheitskritische Arbeitsweisen

Alle Betriebsarten außerhalb der technischen Vorgaben sind unzulässig. Die jeweiligen Grenzwerte sind einzuhalten und dürfen nicht überschritten werden. Befolgt werden müssen insbesonders auch die Anweisungen der Betriebsanleitung. Änderungen an der Firmware sind grundsätzlich unzulässig. Sollte jemals eine Lagerungstemperatur von 93 °C überschritten werden, ist der Sensor auszuwechseln. Um die Einhaltung der Sicherheitswerte in Abb. 7 zu gewährleisten, muss der Sensor ausgewechselt werden, wenn die angegebene Betriebstemperatur überschritten wurde.

4.6 Häufige Fehlerursachen (CCF)

Bei der Ausführung der T-Serie wurden die folgenden häufigen Fehlerursachen (CCF = Common Cause Failures) berücksichtigt.
Diese Punkte können in die CCF-Fehleranalyse des Gesamtsystems einbezogen werden:

1. Der Sensor ist gegen Überspannung bis zur maximalen Betriebsspannung und Verdrahtungsfehler (VDC – GND) geschützt.
2. Die FMEDA-Gefährdungsanalyse mit Risikoeinschätzung liegt vor. Die FMEDA-Analyseergebnisse wurden bei der CCF-Fehleranalyse des Gesamtsystems berücksichtigt.
3. Die Entwickler dieses Sensors wurden entsprechend geschult, um die Ursachen und Folgen von CCF zu verstehen.
4. Der Sensor wurde geprüft auf: EMV (Störaussendung und Störfestigkeit), mechanische Belastungen (z.B. Erschütterungen, Druck), Umgebungseinflüsse wie Temperatur und Eindringen von Flüssigkeit. Der Sensor ist gegenüber den Einflüssen entsprechend der Angaben in den technischen Daten unempfindlich, vorausgesetzt, dass er versiegelt und dadurch geschützt ist.

4.7 Maßnahmen gegen vorhersehbaren Missbrauch

Zum Schutz gegen vorhersehbare Fehler beim Einsatz des Sicherheitssensors der T-Serie wurden folgende Maßnahmen getroffen:

1. Umfassender Schutz vor Verdrahtungsfehlern des Sensors.
2. Die Betriebsanleitung enthält ausführliche Anweisungen zur Vermeidung von Schäden während der Installation.
3. Um etwaige, beim Installieren entstandene Schäden zu erkennen, sollte die Sensorfunktion nach der Installation überprüft werden.

4.8 Aktionsplan für den Fehlerfall

Wenn der Sensor einen Bedienfehler ausgibt, muss der Sensor nach dem Fehler 10 Mal in Folge ohne Bedienfehler-Meldung (d.h. der Sensor gibt keinen Strom von weniger als 3,6 mA aus) arbeiten. Andernfalls muss der Sensor zur Überprüfung an MTS Sensors eingeschickt werden.

4.9 Produktidentifikation

Der Sensor der T-Serie steht in zahlreichen Ausführungen zur Verfügung, die sich im Hinblick auf Länge, Flanschtyp, Anschlusstyp, Explosionsschutz und Ausgangssignal unterscheiden. Der Buchstabe „S“ in Position 14 der Modellnummer gibt an, dass der Sensor für SIL 2 zugelassen ist. Alle Versionen mit der Option „S“ (Funktionssicherheit) sind SIL 2 kompatibel.

Beispiel T-Serie: TxxxxxxxxxxxSxxxx

5. T-Serie Analog Safety

5.1 Funktionale Beschreibung

Der analoge Sicherheitssensor der T-Serie ist gemäß IEC 61508 Typ B für die Hardware-Fehlertoleranz 0 eingestuft. Der Sensor führt eine Eigendiagnose durch und schaltet bei Auftreten eines Fehlers in den Fail-Safe-Zustand; dies bedeutet, dass die Sicherheitsfunktion nicht zur Verfügung steht. Damit der Sensor ein gültiges Ausgangssignal liefert, muss der Wert für die Dauer von 10 aufeinander folgenden Millisekunden im Bereich 3,8…20,5 mA liegen. Befindet sich das Ausgangssignal des Sensors zu einem beliebigen Zeitpunkt außerhalb von 3,6…21 mA, besteht somit ein Fehlerzustand. Der Fehler ist erst dann behoben, wenn das Ausgangssignal für die Dauer von 10 aufeinander folgenden Millisekunden innerhalb des gültigen Bereichs liegt. Der aktive Messbereich für die definierte Messlänge des Sensors beträgt 4…20 mA.

Online-Proof-Test

Unter folgenden Bedingungen wird ein Fehler ausgelöst:
- Fehlender oder beschädigter Positionsmagnet
- Ungültige Prüfsumme des Parameterspeichers
- Ungültige Prüfsumme des Programmspeichers
- Interner Hardwarefehler
- Magnetposition befindet sich außerhalb des gültigen Messbereichs

5.2 Offline-Proof-Testmethode zur Überprüfung der Sicherheitsfunktion

Mit dem Offline-proof-test kann die Sicherheitsfunktion des Sensors überprüft werden.
Empfohlene Funktionstests im Rahmen des Offline-tests:

Neben der eingebauten Funktionsprüfung des Sicherheitssensors der T-Serie kann die Betriebssicherheit durch eine externe Überprüfung weiter erhöht werden.
Wir empfehlen, die Funktion des analogen Sicherheitssensors der T-Serie folgendermaßen zu überprüfen:

1. Sicherheitsfunktion überbrücken und geeignete Vorkehrungen zur Vermeidung einer Fehlauslösung ergreifen.
2. T-Serie Sensor auf Nullpunkt einstellen.
3. Positionsmagneten des Sensors der T-Serie bis zum Ende der Messlänge verschieben, um die Beweglichkeit über die gesamte Messlänge zu überprüfen.
4. Sensor der T-Serie wieder auf den Nullpunkt einstellen.

5. 3-Punkt-Kalibrierung über den gesamten Arbeitsbereich des Sensors der T-Serie durchführen.
6. Überbrückung entfernen und Normalbetrieb aufnehmen.

Alle angewandten Methoden und Ergebnisse des Proof-Tests müssen in einem Prüfbericht festgehalten werden. Bei negativem Funktionstest ist es erforderlich, Sensor und System außer Betrieb zu setzen. Der Prozess muss auf geeignete Weise in einem sicheren Modus gehalten werden. Beachten Sie die aktuelle technische Dokumentation:

Betriebsanleitung (elektrischer Betrieb und Installation, MTS Dokumentennr.: 551513)

5.3 Sicherheitstoleranz

Angaben zur Betriebsgenauigkeit des Sensors finden Sie in der Betriebsanleitung (Dokumentennr. 551513). Die Genauigkeit zur Gewährleistung der Sicherheit des Analogsensors der T-Serie beträgt 1,0 % der Messlänge. Nachstehend ist ein Berechnungsbeispiel zur Bestimmung der maximalen sicheren Position des Sensormagneten aufgeführt:

Messlänge: 80 mm
Magnetgeschwindigkeit: 100 mm/s
Worst-Case-Ansprechzeit: 10 ms

Sicherheitstoleranz
= 1 % × 80 mm
= 0,8 mm

Ansprechzeittoleranz (in Bewegung)
= 100 mm/s × 10 ms
= 1,0 mm

5.4 Daten zur Bescheinigung und Fehlerrate

Fehlerraten der FMEDA-Gefährdungsanalyse sind nach IEC 61508 generiert. Es gelten folgende Annahmen:

– Der Sensor kann im Low oder High Demand Mode arbeiten.
– Die Fehlerraten externer Stromversorgungen werden nicht berücksichtigt.
– Erwähnte SFF- und PFD_{avg}-Werte sind dem FMEDA-Bericht zu entnehmen.
– Im Fehlerfall schaltet der analoge Sensor der T-Serie in den Fail-Safe-Zustand.
– Die Steuerung muss das Fehlersignal richtig interpretieren.
– Die Werte der Umgebungsbedingungen sind der gültigen Betriebsanleitung (Dokumentennr. 551513) zu entnehmen.
– Der PFD-Wert wird ausgehend von einem 1-jährigen Proof-Testintervall berechnet.

Die Einhaltung der Fehlerraten setzt voraus, dass die Nutzungsdauer der Komponenten nicht überschritten wird. Die Nutzungsdauer ist definiert als diejenige Zeitspanne, in der die Fehlerrate relativ konstant ist.

T-Serie (SIL 2: Analog Safety)	IEC 61508
Sicherheitsniveau	SIL 2
Gerätetyp	B
$MTTF_d$	100 Jahre @ 60 °C; 44 Jahre @ 80 °C
PFD_{avg}	3,49E-04 @ 60 °C; 9,85E-04 @ 80 °C
Diagnostic response time (Fail Detection Time)	25 ms (max) 1 sek. für CRC Fault Detection
% von SIL 2 Bereich für PFD	3,5 % @ 60 °C; 9,9 % @ 80 °C
Hardware fault tolerance (HFT)	0
Lebensdauer	50 Jahre @ 60 °C; 18 Jahre @ 80 °C

Abb. 6: T-Serie Parameter

Gerät @ 1 % Genauigkeit	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
T-Serie @ 60 °C	0	100	802	62	93,6 %
T-Serie @ 80 °C	0	283	2266	175	93,6 %
T-Serie @ 85 °C	0	400	3205	248	93,6 %

Abb. 7: Sicherheitswerte für maximale Betriebstemperatur

6. Fachbegriffe und Abkürzungen

Fachbegriff	Beschreibung
Cat.	Sicherheitskategorie gemäß EN 954-1
E/E/PE	Elektrisch / Elektronisch / programmierbare Elektronik
FIT	Failure In Time (1×10-9 Fehler pro Stunde)
FMEDA	Failure Mode, Effects und Diagnostic Analysis (Analysemethode zur quantitativen Ermittlung von Ausfallarten und Ausfallraten)
FSM	Functional Safety Management (Funktionale Sicherheit)
HFT	HFT=x, wobei x die Anzahl der Fehler angibt, die die Ausführung ohne Beeinträchtigung der Sicherheitsfunktion zulässt.
High Demand Mode	Betriebsart mit hoher oder kontinuierlicher Anforderung der Sicherheitsfunktion. Anforderungsrate an sicherheitsbezogenes System mehr als einmal pro Jahr.
Low Demand Mode	Modus, in dem die Häufigkeit der erfolgten Betriebsanforderungen an ein sicherheitsrelevantes System nicht mehr als einmal pro Jahr und nicht mehr als das Zweifache der Proof-Test-Häufigkeit beträgt.
$MTTF_d$	Mean Time to Dangerous Failure (mittlere Zeit bis zum gefahrbringenden Ausfall)
PFD_{avg}	Probability of Failure on Demand (mittlere Ausfallwahrscheinlichkeit einer Sicherheitsfunktion bei niedriger Anforderung)
PFH	Probability of dangerous Failure per Hour (Mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls innerhalb einer Stunde)
SFF	Der SFF Wert gibt den Anteil der ungefährlichen Ausfälle im System an. Dazu wird das Verhältnis der Rate der sicheren Fehler zusammen mit der Rate der erkannten Fehler in Bezug zur Gesamt-Ausfallrate des Systems gesetzt.
SIF	Safety Instrumented Function (Sicherheitstechnische Funktion)
SIL	Safety Integrity Level (Sicherheits-Integritätslevel)
SIS	SIS (Safety Instrumented System) – Implementierung einer oder mehrerer sicherheitsgerichteter Funktionen. SIS ist aus einer beliebigen Kombination von Bauteilen und Elementen zusammengesetzt.
SLC	Safety Lifecycle (Sicherheits-Lebenszyklus)
Type A component	„Nicht komplexe“ Komponente (mit getrennten Elementen); siehe IEC 61508-2 Punkt 7.4.4.1.2
Type B component	„Komplexe“ Komponente (mit Mikrocontroller oder programmierbarer Logik); siehe IEC 61508-2 Punkt 7.4.4.1.3
V&V	Verifikation und Validierung
Verifikation	Der Nachweis besagt, dass für jede Lebensphase die Ergebnisse einer Phase mit den vorgegebenen Anforderungen dieser Phase übereinstimmen. Die Bestätigung / Verifikation wird in der Regel durch Analyse und / oder Test durchgeführt.
Validierung	Der Nachweis besagt, dass das sicherheitsrelevante System bzw. die Kombination der sicherheitsrelevanten Systeme und externe Maßnahmen zur Risikominimierung in allen Aspekten den Anforderungen der Sicherheitsintegration entsprechen. Die Validierung (oder alternativ Bestätigung) wird in der Regel durch Tests durchgeführt.

Notizen

MTS SENSORS

Sensor mit Ex-Zulassung

Dokumentennummer:
551504 Revision B (DE) 05/2016

STANDORTE

USA
MTS Systems Corporation
Sensors Division
3001 Sheldon Drive
Cary, N.C. 27513, USA
Tel. +1 919 677-0100
Fax +1 919 677-0200
info.us@mtssensors.com
www.mtssensors.com

DEUTSCHLAND
MTS Sensor Technologie
GmbH & Co. KG
Auf dem Schüffel 9
58513 Lüdenscheid, Deutschland
Tel. +49 2351 9587-0
Fax +49 2351 56491
info.de@mtssensors.com
www.mtssensors.com

JAPAN
MTS Sensors Technology Corp.
737 Aihara-machi,
Machida-shi,
Tokyo 194-0211, Japan
Tel. +81 42 775-3838
Fax +81 42 775-5512
info.jp@mtssensors.com
www.mtssensors.com

CHINA
MTS Sensors
Room 504, Huajing Commercial Center,
No. 188, North Qinzhou Road
200233 Shanghai, China
Tel. +86 21 6485 5800
Fax +86 21 6495 6329
info.cn@mtssensors.com
www.mtssensors.com

FRANKREICH
MTS Systems SAS
Zone EUROPARC Bâtiment EXA 16
16/18, rue Eugène Dupuis
94046 Creteil, Frankreich
Tel. +33 1 58 4390-28
Fax +33 1 58 4390-03
info.fr@mtssensors.com
www.mtssensors.com

ITALIEN
MTS Systems Srl.
Sensor Division
Via Camillo Golgi, 5/7
25064 Gussago (BS), Italien
Tel. +39 030 988 3819
Fax +39 030 982 3359
info.it@mtssensors.com
www.mtssensors.com

RECHTLICHE HINWEISE

ISO 9001 CERTIFIED

Reg.-No. 003095-QM08

SIL 2 IEC 61508