SIEMENS

SITRANS

Temperaturmessumformer Funktionale Sicherheit für SITRANS TW

Produktinformation

Einleitung 1

Allgemeine Sicherheitshinweise 2

Gerätespezifische Sicherheitshinweise 3

Anhang A

Liste der Abkürzungen B

Ergänzung zur Betriebsanleitung
7NG3242

11/2006
A5E00912141-01

Sicherheitshinweise

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

Gefahr

bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Warnung

bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Vorsicht

mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Vorsicht

ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Achtung

bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zugehörige Gerät/System darf nur in Verbindung mit dieser Dokumentation eingerichtet und betrieben werden. Inbetriebsetzung und Betrieb eines Gerätes/Systems dürfen nur von **qualifiziertem Personal** vorgenommen werden. Qualifiziertes Personal im Sinne der sicherheitstechnischen Hinweise dieser Dokumentation sind Personen, die die Berechtigung haben, Geräte, Systeme und Stromkreise gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Bestimmungsgemäßer Gebrauch

Beachten Sie Folgendes:

Warnung

Das Gerät darf nur für die im Katalog und in der technischen Beschreibung vorgesehenen Einsatzfälle und nur in Verbindung mit von Siemens empfohlenen bzw. zugelassenen Fremdgeräten und -komponenten verwendet werden. Der einwandfreie und sichere Betrieb des Produktes setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung und Montage sowie sorgfältige Bedienung und Instandhaltung voraus.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Automation and Drives
Postfach 48 48
90437 NÜRNBERG
DEUTSCHLAND

Dokumentbestell-Nr. A5E00912141-01
Ausgabe 11/2006

Copyright © Siemens AG 2006.
Änderungen vorbehalten

Inhaltsverzeichnis

1 Einleitung 5

1.1 Zweck dieser Dokumentation 5

1.2 Gültigkeitsbereich dieser Dokumentation 5

1.3 Historie 5

1.4 Weitere Informationen 6

2 Allgemeine Sicherheitshinweise 7

2.1 Sicherheitsbezogenes System 7

2.2 Safety Integrity Level (SIL) 8

3 Gerätespezifische Sicherheitshinweise 11

3.1 Anwendungsbereich 11

3.2 Sicherheitsfunktion 12

3.3 Einstellungen 13

3.4 Verhalten bei Störungen 14

3.5 Wartung/Überprüfung 14

3.6 Sicherheitstechnische Kenndaten 15

A Anhang 17

A.1 Literatur und Normen 17

A.2 SIL-Konformitätserklärung 18

A.3 Prüfbericht (Auszug) 19

B Liste der Abkürzungen 23

B.1 Abkürzungen 23

Glossar 25

Index 27

Tabellen

Tabelle 2-1 Safety Integrity Level 8

Einleitung 1

1.1 Zweck dieser Dokumentation

Diese Dokumentation enthält Informationen und Sicherheitshinweise, die Sie für den Einsatz des Geräts in sicherheitsbezogenen Systemen benötigen.

Sie richtet sich sowohl an Personen, die das Gerät mechanisch montieren, elektrisch anschließen, parametrieren und in Betrieb nehmen, als auch an Servicetechniker und Wartungstechniker.

1.2 Gültigkeitsbereich dieser Dokumentation

Dokumentation

Diese Dokumentation behandelt den Temperaturmessumformer lediglich als Teil einer Sicherheitsfunktion.

Die vorliegende Dokumentation gilt nur im Zusammenhang mit folgender Dokumentation:

Nr.	Name	Bestellnummer
/1/	Betriebsanleitung SITRANS TW 7NG3242	A5E00054075

1.3 Historie

Diese Historie stellt den Zusammenhang zwischen der aktuellen Dokumentation und der gültigen Firmware des Geräts her.

Die Dokumentation dieser Ausgabe gilt für folgende Firmware:

Ausgabe	Firmwarekennung Typenschild	Systemeinbindung	Installationspfad für PDM
01 11/2006	FW: ab 16.01.04	Ab PDM V 5.9	SITRANS TW

In der folgenden Tabelle stehen die wichtigsten Änderungen der Dokumentation verglichen mit der jeweils vorherigen Ausgabe.

Ausgabe	Bemerkung
01 11/2006	Erstausgabe

1.4 Weitere Informationen

Informationen

Wir weisen darauf hin, dass der Inhalt der Anleitung nicht Teil einer früheren oder bestehenden Vereinbarung, Zusage oder eines Rechtverhältnisses ist oder diese abändern soll. Sämtliche Verpflichtungen der Siemens AG ergeben sich aus dem jeweiligen Kaufvertrag, der auch die vollständige und allein gültige Gewährleistungsregelung enthält. Diese vertraglichen Gewährleistungsbestimmungen werden durch die Ausführungen der Anleitung weder erweitert noch beschränkt.

Der Inhalt spiegelt den technischen Stand zur Drucklegung wieder. Technische Änderungen sind im Zuge der Weiterentwicklung vorbehalten.

Siemens-Niederlassungen

Wünschen Sie weitere Informationen oder treten besondere Probleme auf, die in der Anleitung nicht ausführlich genug behandelt werden, können Sie die erforderliche Auskunft über die örtliche Siemens-Niederlassung anfordern. Ihre örtliche Siemens-Niederlassung finden Sie im Internet.

Produktinformation im Internet

Die Anleitung ist Bestandteil der bestellbaren oder mitgelieferten CD. Weiterhin ist die Anleitung im Internet auf der Siemens-Homepage verfügbar.

Auf der CD finden Sie außerdem das technische Datenblatt mit den Bestelldaten, das Software Device Install für SIMATIC PDM zum Nachinstallieren und die benötigte Software.

Siehe auch

Siemens-Niederlassungen (http://www.siemens.de/prozessinstrumentierung/kontakte)

Anleitungen und Handbücher
(http://www.siemens.de/prozessinstrumentierung/dokumentation)

Produktinformation SITRANS T im Internet (http://www.siemens.de/sitranst)

Allgemeine Sicherheitshinweise

2

2.1 Sicherheitsbezogenes System

Dieses Kapitel beschreibt die funktionale Sicherheit allgemein und nicht gerätespezifisch. Die Geräte in den Beispielen sind stellvertretend gewählt. Die gerätespezifischen Informationen folgen im nächsten Kapitel.

Beschreibung

Sensor, Logikeinheit/Leitsystem und Aktor bilden zusammen ein sicherheitsbezogenes System, das eine Sicherheitsfunktion ausführt.

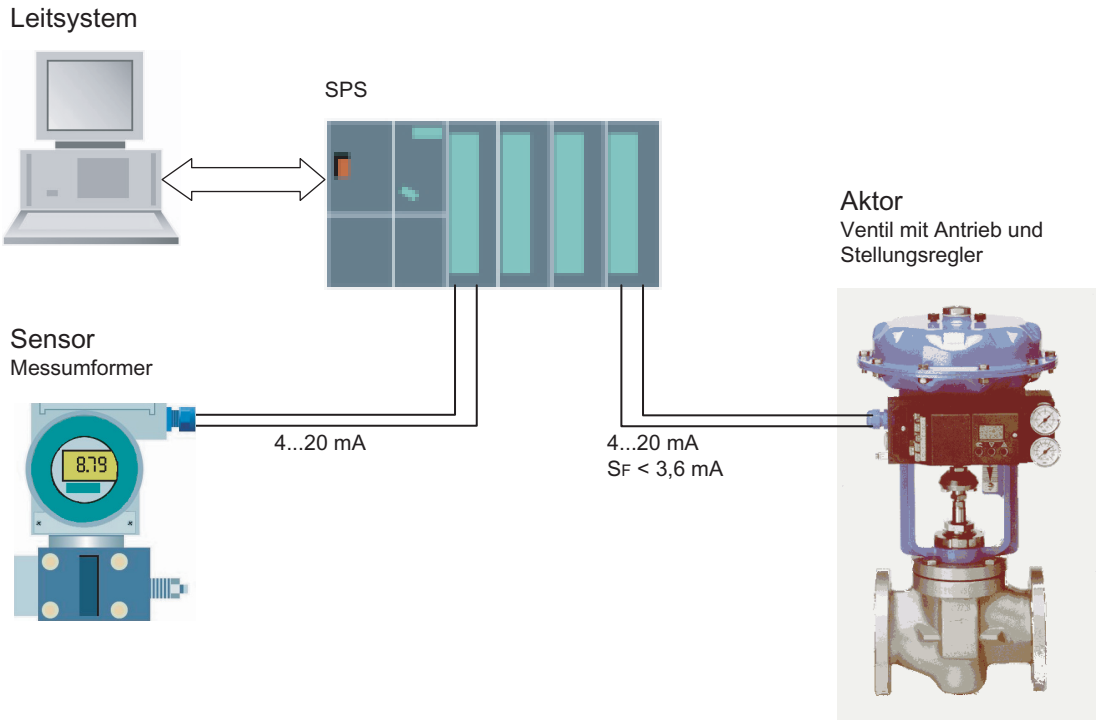


Bild 2-1 Beispiel für ein sicherheitsbezogenes System

S_F Ausfallsignal

Funktionsweise des Beispiels

Der Messumformer erzeugt ein prozessbezogenes analoges Signal. Das nachgeschaltete Leitsystem überwacht dieses Signal auf Unterschreiten oder Überschreiten eines voreingestellten Grenzwerts. Im Störfall erzeugt das Leitsystem ein Ausfallsignal von < 3,6 mA oder > 22 mA für den angeschlossenen Stellungsregler, der das zugehörige Ventil in die vorgegebene Sicherheitsstellung bringt.

2.2 Safety Integrity Level (SIL)

Die internationale Norm IEC 61508 definiert vier diskrete Safety Integrity Level (SIL) von SIL 1 bis SIL 4. Jeder Level entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion.

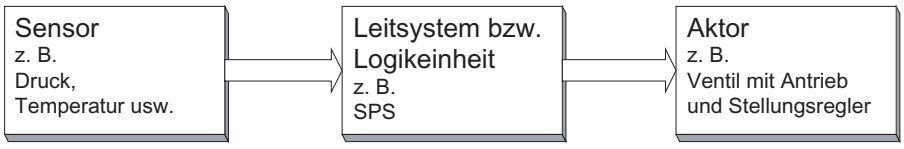
Beschreibung

Die folgende Tabelle zeigt die Abhängigkeit des SIL von der "mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion des gesamten sicherheitsbezogenen Systems" (PFD_{AVG}). Dabei wird der "Low demand mode" betrachtet, d. h. die Sicherheitsfunktion wird durchschnittlich maximal einmal im Jahr angefordert.

Tabelle 2-1 Safety Integrity Level

SIL	PFD_{AVG}
4	$\geq 10^{-5} ... < 10^{-4}$
3	$\geq 10^{-4} ... < 10^{-3}$
2	$\geq 10^{-3} ... < 10^{-2}$
1	$\geq 10^{-2} ... < 10^{-1}$

Die "mittlere Wahrscheinlichkeit gefahrbringender Ausfälle des gesamten sicherheitsbezogenen Systems" (PFD_{AVG}) teilt sich üblicherweise auf die drei Teilsysteme des folgenden Bildes auf.



PFD_{AVG}-Anteil < 35 % < 15 % < 50%

Bild 2-2 Beispiel PFD-Aufteilung

Die folgende Tabelle zeigt den erreichbaren Safety Integrity Level (SIL) des gesamten sicherheitsbezogenen Systems für Teilsysteme vom Typ B abhängig vom Anteil ungefährlicher Ausfälle (SFF) und der Hardwarefehler-Toleranz (HFT). Teilsysteme vom Typ B sind z. B. analoge Messumformer und Abschaltventile ohne komplexe Komponenten, z. B. Mikroprozessoren (siehe auch IEC 61508, Teil 2).

SFF	HFT		
	0	1 (0) [1)]	2 (1) [1)]
< 60 %	Nicht zulässig	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

[1)] Nach IEC 61511-1, Abschnitt 11.4.4

Nach IEC 61511-1, Abschnitt 11.4.4 kann bei Sensoren und Aktoren mit komplexen Komponenten die Hardwarefehler-Toleranz (HFT) um eins reduziert werden (Werte in Klammern), wenn für das Gerät folgende Bedingungen zutreffen:

- Das Gerät ist betriebsbewährt.
- Der Anwender kann nur prozessbezogene Parameter konfigurieren, z. B. Stellbereich, Signalrichtung im Fehlerfall, Grenzwerte usw.
- Die Konfigurationsebene der Firmware wird gegen unbefugte Bedienung gesperrt.
- Die Funktion hat einen geforderten SIL von weniger als 4.

Der Messumformer erfüllt diese Bedingungen.

Gerätespezifische Sicherheitshinweise

3

3.1 Anwendungsbereich

Übersicht

Der SITRANS TW, 4-Leiter-Tragschienengerät ist ein Messumformer mit universeller Eingangsschaltung. Folgende Fühler und Signalquellen können Sie anschalten:

- Widerstandsthermometer
- Thermoelemente
- Widerstandsgeber/Potentiometer
- mV-Geber
- Als Sondervariante:
  - V-Geber
  - Stromquellen

Warnung

Der Messumformer SITRANS TW, 4-Leiter-Tragschienengerät ist ein Wartengerät. Er darf als zugehöriges Betriebsmittel immer nur außerhalb des explosionsgefährdeten Bereichs montiert werden.

Die Messumformer in der Geräteausführung "Zündschutzart eigensicher" besitzen eine EG-Baumusterprüfbescheinigung und erfüllen die entsprechenden harmonisierten Europäischen Normen der CENELEC. Sie können zur Messung von Prozessgrößen in gasexplosionsgefährdeten Bereichen (Zone 1, 0) verwendet werden. Eine Messung von Prozessgrößen in Zone 0 ist nur zulässig, wenn auch die Sensoren für Zone 0 zugelassen sind.

Der Messumformer darf auch für staubexplosionsgefährdete Bereiche der Zonen 20 bzw. 21 eingesetzt werden. In diesen Fällen ist sicherzustellen, dass die Geräte, die an diesen Stromkreis angeschlossen werden, die Anforderungen für die Kategorie 1D bzw. 2D erfüllen und entsprechend zertifiziert sind.

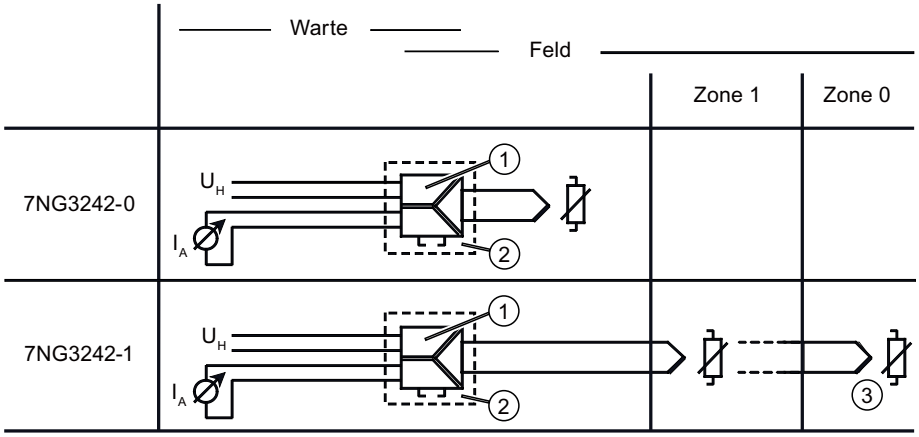


Bild 3-1 Einsatzgebiete der Messumformer in Ex- und in Nicht-Ex-Ausführung

① Messumformer ② Feldgehäuse (bei Bedarf, handelsüblich)
③ Nur in Verbindung mit den vorgeschriebenen Schutzanforderungen für den Sensor

Anforderungen

Der Temperaturmessumformer erfüllt folgende Anforderungen:

- Funktionale Sicherheit bis SIL 1 nach IEC 61508 bzw. IEC 61511-1, ab der Firmware-Version FW: ab 16.01.04
- Explosionsschutz bei entsprechenden Varianten
- Elektromagnetische Verträglichkeit nach EN 61326

3.2 Sicherheitsfunktion

Sicherheitsfunktion für Temperaturmessumformer

Die Sicherheitsfunktion bei den Temperaturmessumformern ist das Messen von Temperatur. Sie bezieht sich auf den Ausgangsstrom von 4 bis 20 mA und gewährleistet in diesem Bereich eine Genauigkeit von ±2 % des Messwerts.

Warnung

Die verbindlichen Einstellungen und Bedingungen sind in den folgenden Kapiteln aufgeführt:

Einstellungen (Seite 13)

Sicherheitstechnische Kenndaten (Seite 15)

Zur Erfüllung der Sicherheitsfunktion sind diese Bedingungen unbedingt zu beachten.

Siehe auch

Sicherheitstechnische Kenndaten (Seite 15)

3.3 Einstellungen

Die folgenden Einstellungen gelten für folgende SITRANS TW:

- mit Stromausgang "4..20mA"
- Temperaturmessung über Widerstandsthermometer oder Thermoelement

Falls ihr Gerät nicht den oben genannten Anforderungen entspricht, finden Sie in der Beschreibung auch, wie Sie das Gerät umstellen müssen.

Nach der Montage und Inbetriebnahme gemäß Betriebsanleitung sind folgende Einstellungen zu beachten:

Bedienen/Projektieren

Achten Sie bei der Bedienung/Projektierung darauf, dass die technischen Daten des Temperaturmessumformers in der jeweiligen Geräteausführung eingehalten sind.

Gerät auf Stromausgang umstellen

1. Falls Ihr Gerät auf Spannungsausgang eingestellt ist, dann öffnen Sie das Gerät.
2. Öffnen Sie die Steckbrücken X6 und X7 und schließen Sie die Steckbrücke X8.

Parameter kontrollieren

Falls Ihr Gerät auf Spannungsausgang eingestellt ist, dann stellen Sie das Gerät auf Stromausgang um. Sie stellen in SIMATIC PDM unter "Ausgangsparameter - Analogausgang" den Parameter "AAusg-Typ" auf "mA".

Falls Ihr Gerät auf Stromausgang "0..20mA" eingestellt ist, dann stellen Sie in SIMATIC PDM unter "Ausgangsparameter - Analogausgang" den Parameter "AAusg-Modus" auf "4..20mA".

Sicherheitsfunktion überprüfen

Wir empfehlen:

- Kontrollieren Sie den Status auf Warnungen und Fehlermeldungen.
- Kontrollieren Sie den oberen und unteren Alarmstromwert.
- Führen Sie eine 2-Punkt-Kalibrierung durch.
- Kontrollieren Sie die Messgenauigkeit, die für die Sicherheitsfunktion im Bereich von ±2 % liegen muss. Sie kontrollieren die Messgenauigkeit z. B. durch einen Sensorabgleich.

Schutz gegen Konfigurationsänderung

Nach der Parametrierung/Inbetriebnahme:

Schließen Sie den Kurzschluss-Stecker X9.

Damit ist die Bedienung über die HART-Kommunikation gesperrt.

Verweis

Handlungsanweisungen finden Sie in folgender Dokumentation:

Betriebsanleitung SITRANS TW 7NG3242
Bestellnummer A5E00054075

3.4 Verhalten bei Störungen

Reparatur

Defekte Geräte sind mit Angabe der Störung und Ursache an die Reparaturabteilung einzusenden. Bei Bestellung von Ersatzgeräten bitte die Seriennummer des Originalgeräts angeben. Die Seriennummer finden Sie auf dem Typenschild.

Anschrift der zuständigen SIEMENS Reparaturstelle, Ansprechpartner, Ersatzteillisten usw. finden Sie im Internet.

Siehe auch

Services&Support (http://www.siemens.de/automation/service&support)

Partner (http://www.automation.siemens.com/partner)

3.5 Wartung/Überprüfung

Intervall

Wir empfehlen, die Funktionsfähigkeit des Temperaturmessumformers in regelmäßigen Zeitabständen von einem Jahr zu überprüfen.

Sicherheitsfunktion überprüfen

Wir empfehlen:

- Kontrollieren Sie den Status auf Warnungen und Fehlermeldungen.
- Kontrollieren Sie den oberen und unteren Alarmstromwert.
- Führen Sie eine 2-Punkt-Kalibrierung durch.

- Kontrollieren Sie die Messgenauigkeit, die für die Sicherheitsfunktion im Bereich von ±2 % liegen muss. Sie kontrollieren die Messgenauigkeit z. B. durch einen Sensorabgleich.

Sicherheit überprüfen

Prüfen Sie regelmäßig die Sicherheitsfunktion des gesamten Sicherheitskreises gemäß IEC 61508/61511. Die Testintervalle werden unter anderem bei der Berechnung jedes einzelnen Sicherheitskreises einer Anlage (PFD_{AVG}) bestimmt.

3.6 Sicherheitstechnische Kenndaten

Die für den Systemeinsatz erforderlichen sicherheitstechnischen Kenndaten sind in der "SIL Konformitätserklärung" aufgelistet. Diese Werte gelten unter den folgenden Bedingungen:

- Der Temperaturmessumformer SITRANS TW wird nur in Anwendungen mit niedriger Anforderungsrate für die Sicherheitsfunktion eingesetzt (low demand mode).
- Die Kommunikation mit dem HART-Protokoll wird ausschließlich verwendet für Folgendes:
  - Die Gerätekonfiguration
  - Das Auslesen von Diagnosewerten
- Die sicherheitsrelevanten Parameter/Einstellungen wurden vor dem sicherheitsbezogenen Betrieb über HART-Kommunikation eingegeben. Einstellungen (Seite 13)
- Die Sicherheitsfunktions-Prüfung ist erfolgreich abgeschlossen.
- Der Messumformer wird gegen ungewollte und unbefugte Veränderungen/Bedienung gesperrt.
- Für den Messumformer gelten folgende Voraussetzungen:
  - Der Ausgang gibt ein Stromsignal aus.
  - Das Stromsignal liegt in Bereich von 4 bis 20 mA.
  - Das Stromsignal wird von einem sicheren System ausgewertet.
- Die aufgeführten Fehlerraten gelten für typische Beanspruchung einer industriellen Umgebung wie in IEC 60654-1 Klasse C. Die IEC 60654-1 Klasse C bedeutet, geschützter Einsatzort, mit einer mittleren Temperatur über einen längeren Zeitraum von 40 °C.
- Die Berechnung der Fehlerrate basiert auf einer MTTR von 8 Stunden.

Die berechnete Mean Time Between Failures (MTBF) für den Temperaturmessumformer SITRANS T beträgt ca. 165 Jahre.

Die maximale Einsatzzeit des SITRANS TW in einer Sicherheitsanwendung beträgt 57 Jahre. Ersetzen Sie das Gerät nach dieser Zeit.

Siehe auch

SIL-Konformitätserklärung (Seite 18)

Anhang

A

A.1 Literatur und Normen

Nr	Norm	Beschreibung
/1/	IEC 61508 Teil 1-7	Funktionale Sicherheit folgender Systeme: • Sicherheitsbezogen • Elektrisch • Elektronisch • Programmierbar Zielgruppe: Hersteller und Lieferanten von Geräten
/2/	IEC 61511 Teil 1-3	Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie Zielgruppe: Planer, Errichter und Nutzer

A.2 SIL-Konformitätserklärung

SIEMENS

Declaration of Conformity

Functional Safety according to IEC 61508 and IEC 61511

Siemens AG
Automation & Drives
Sensors & Communication
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Product:	**SITRANS TW universal transmitter:**	
Ordering Nr. :	7NG3242-*A***	115/230 V AC/DC
	7NG3242-*B***	24 V AC/DC

We as manufacturer declare that the following failure rates for the above identified devices may be used in the relevant calculations required for IEC 61508 / 61511 safety instrumented system (SIS) compliance. The device is capable of temperature measurement with an accuracy of 2% of full span for a safety instrumented function of Safety Integrity Level (SIL) 1. The provided Functional Safety Application Manual shall be observed. Product revisions will be carried out by the manufacturer in accordance with IEC 61508.

The proven in use was carried out by exida GmbH in accordance with IEC 61508 / IC 61511.

Safety Related Characteristics

Device Type	**B**
SIL Safety Integrity Level	**1**
HFT	**0**
PFD_{AVG}	**$8{,}57*10^{-4}$**
λ_{SD} Safe detected Failure Rate	**0 FIT**
λ_{SU} Safe undetected Failure Rate	**117 FIT**
λ_{DD} Dangerous detected Failure Rate	**204 FIT**
λ_{DU} Dangerous undetected Failure Rate	**196 FIT**
SFF Safe Failure Fraction	**62 %**

These characteristics are valid for low demand mode of operation within an 1oo1 architecture. (Guidance to calculation see IEC 61508-6, annex B). The PFD_{AVG} value is valid under the assumption of Mean Time To Repair MTTR = 8h and Proof Test Interval T1 = 8760h.

Karlsruhe, 2006, October 20th

Siemens AG

Bernhard Brendel, Manager R&D Temperature

Martin Michler, A&D SC Functional Safety Manager

No. A5E00982418A-01

A.3 Prüfbericht (Auszug)

Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output and software version V4.0.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

For safety applications only the 4..20 mA output was considered. Any other possible output variants or electronics are not covered by this report.

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-2}$ to $< 10^{-1}$ for SIL 1 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part.

For a SIL 1 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-01, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-02.

The temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output are considered to be Type B[1] components with a hardware fault tolerance of 0. For Type B components with a SFF of 60% to < 90% a hardware fault tolerance of 0 is sufficient according to table 3 of IEC 61508-2 for SIL 1 (sub-) systems.

As the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. The proven-in-use investigation was based on field return data collected and analyzed by SIEMENS AG, A&D PI T2. This data cannot cover the process connection. The proven-in-use justification for the process connection still needs to be done by the end-user.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6, the Type B temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output with a hardware fault tolerance of 0 and a SFF of 60% to < 90% are considered to be suitable for use in SIL 1 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

It is assumed that the connected logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output communicate detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver detects but does not automatically trip on these failures, these failures have been classified as dangerous detected failures.

The failure rates listed above do not include failures resulting from incorrect use of the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

---

[1] Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

The following tables show how the above stated requirements are fulfilled.

Table 1: Failure rates [2]

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	**204**
Fail dangerous detected (internal diagnostics or indirectly[3])	87
Fail high (detected by the logic solver)	1
Fail low (detected by the logic solver)	115
Annunciation detected	1
Fail Dangerous Undetected	**196**
Fail dangerous undetected	193
Annunciation undetected	3
No Effect	**117**
Not part	**160**

Table 2: IEC 61508 failure rates

λ_{SD}	λ_{SU} [4]	λ_{DD}	λ_{DU}	SFF	DC_S [5]	DC_D [5]
0 FIT	117 FIT	204 FIT	196 FIT	62%	0%	51%

Table 3: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 8,57E-04	**PFD_{AVG} = 4,28E-03**	**PFD_{AVG} = 8,53E-03**

A complete temperature sensor assembly consisting of the temperature transmitters SITRANS TW Series 7NG3242 and a thermocouple or RTD can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

Appendix 4 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

[2] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

[3] "indirectly" means that these failure are not necessarily detected by diagnostics but lead to either fail low or fail high failures depending on the transmitter setting and are therefore detectable.

[4] Note that the SU category includes failures that do not cause a spurious trip

[5] DC means the diagnostic coverage (safe or dangerous) for the pressure transmitters by the safety logic solver.

Assuming that the temperature transmitter SITRANS TW Series 7NG3242 will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution or the PFD_{AVG} value for the thermocouple or RTD in a low stress environment is as follows:

Table 4: SITRANS TW Series 7NG3242 / thermocouple (close coupled) in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD_{AVG} = 8,80E-04	PFD_{AVG} = 4,40E-03	PFD_{AVG} = 8,80E-03	67%

λ_{SD} = 0 FIT
λ_{SU} = 117 FIT
λ_{DD} = 299 FIT
λ_{DU} = 201 FIT

Table 5: SITRANS TW Series 7NG3242 / 4-wire RTD (close coupled) in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD_{AVG} = 8,69E-04	PFD_{AVG} = 4,35E-03	PFD_{AVG} = 8,69E-03	64%

λ_{SD} = 0 FIT
λ_{SU} = 117 FIT
λ_{DD} = 251,5 FIT
λ_{DU} = 198,5 FIT

The boxes marked in green (▭) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 1 according to table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-02.

A user of the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508, Edition 2000. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the temperature transmitters SITRANS TW Series 7NG3242 with 4..20 mA output (see Appendix 2).

Liste der Abkürzungen

B

B.1 Abkürzungen

Abkürzung	Ausgeschrieben in Englisch	Bedeutung
HFT	Hardware Fault Tolerance	Hardwarefehler-Toleranz: Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen.
MTBF	Mean Time Between Failures	Mittlere Zeitdauer zwischen zwei Ausfällen
MTTR	Mean Time To Repair	Mittlere Zeitdauer zwischen dem Auftreten eines Fehlers in einem Gerät oder System und der Reparatur
PFD	Probability of Failure on Demand	Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall
PFD_{AVG}	Average Probability of Failure on Demand	Mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle: Anteil von Ausfällen ohne Potenzial, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.
SIL	Safety Integrity Level	Die internationale Norm IEC 61508 definiert vier diskrete Safety Integrity Level (SIL 1 bis SIL 4). Jeder Level entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion. Je höher der Safety Integrity Level des sicherheitsbezogenen Systems ist, um so geringer ist die Wahrscheinlichkeit, dass es die geforderten Sicherheitsfunktionen nicht ausführt.
SIS	Safety Instrumented System	Ein sicherheitsbezogenes System (SIS) führt die Sicherheitsfunktionen aus, die erforderlich sind, um einen sicheren Zustand in einer Anlage zu erreichen oder aufrechtzuerhalten. Es besteht aus Sensor, Logikeinheit/Leitsystem und Aktor.
FIT	Failure In Time	Ausfallhäufigkeit Anzahl der Fehler innerhalb 10^9 Stunden
TI	Test Interval	Prüfintervall der Schutzfunktion

Abkürzung	Ausgeschrieben in Englisch	Bedeutung
MooN	"M out of N" Voting	Klassifizierung und Beschreibung des sicherheitsbezogenen Systems hinsichtlich Redundanz und angewandtem Auswahlverfahren. Ein sicherheitstechnisches System oder Teil, das aus "N" unabhängigen Kanälen besteht. Die Kanäle sind derart miteinander verbunden, dass jeweils "M" Kanäle genügen, damit das Gerät die sicherheitstechnische Funktion ausführt. Beispiel: Druckmessung: 1oo2-Architektur. Ein sicherheitsbezogenes System entscheidet, dass eine vorgegebene Druckgrenze überschritten ist, wenn einer von zwei Drucksensoren diese Grenze erreicht. Bei einer 1oo1-Architektur ist nur ein Drucksensor vorhanden.

Glossar

Aktor

Wandler, der elektrische Signale in mechanische oder andere, nicht elektrische Größen umsetzt.

Ausfall/Fehler

Ausfall:
Beendigung der Fähigkeit eines Betriebsmittels zur Ausführung einer geforderten Funktion.

Fehler:
Ungewollter Zustand eines Betriebsmittels, gekennzeichnet durch die Unfähigkeit, eine geforderte Funktion auszuführen.

Fehler

→ *Ausfall/Fehler*

Fehlersicher

Fähigkeit einer Steuerung, auch beim Auftreten von Fehlern/Ausfällen einen sicheren Zustand der gesteuerten Einrichtung, z. B. Maschine, Prozess, zu erhalten oder die Einrichtung in einen sicheren Zustand zu bringen.

Fehlertoleranz

Fehlertoleranz N bedeutet, dass eine Einrichtung bei Vorhandensein von N Fehlern die vorgesehene Aufgabe noch ausführen kann. Bei N+1 Fehlern versagt die Einrichtung bei der Ausführung der vorgesehenen Funktion.

Gefahrbringender Ausfall

Ausfall mit dem Potenzial, das sicherheitsbezogene System in einen gefährlichen oder sicherheitstechnisch funktionsunfähigen Zustand zu versetzen.

Risiko

Kombination der Wahrscheinlichkeit eines Schadeneintritts und des Schadensausmaßes.

Safety Instrumented Function

→ *SIF*

Safety Integrity Level

→ *SIL*

Sensor

Wandler, der mechanische oder andere, nicht elektrische Größen in elektrische Signale umsetzt.

Sicherheitsbezogenes System

Ein sicherheitsbezogenes System (SIS, Safety Instrumented System) führt die Sicherheitsfunktionen aus, die erforderlich sind, um einen sicheren Zustand in einer Anlage zu erreichen oder aufrechtzuerhalten. Es besteht aus Sensor, Logikeinheit/Leitsystem und Aktor.

Beispiel:
Ein Druckmessumformer, ein Grenzsignalgeber und ein Stellventil bilden ein sicherheitsbezogenes System.

Sicherheitsfunktion

Definierte Funktion, die von einem sicherheitsbezogenen System ausgeführt wird, mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls, einen sicheren Zustand für die Anlage zu erreichen oder aufrechtzuerhalten.

Beispiel:
Grenzdrucküberwachung

SIF

Ein Teil/Funktion eines sicherheitsbezogenen Systems, welches das Risiko für das Auftreten eines gefahrbringenden Ausfalls reduziert.

SIL

Die internationale Norm IEC 61508 definiert vier diskrete Safety Integrity Level (SIL) von SIL 1 bis SIL 4. Jeder Level entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion. Je höher der SIL des sicherheitsbezogenen Systems ist, desto höher ist die Wahrscheinlichkeit, dass die geforderte Sicherheitsfunktion funktioniert.

Der erreichbare SIL wird durch folgende sicherheitstechnischen Kenndaten bestimmt:

- Mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall (PFD_{AVG})
- Hardwarefehler-Toleranz (HFT)
- Anteil ungefährlicher Ausfälle (SFF)

Index

A

Aktor, 7
Ausfallsignal, 7

D

Dokumentation
    vorauszusetzende, 5

E

Einsatzzeit
    maximal, 15
Einstellungen, 13

F

Firmware, 5

H

Historie, 5

K

Kenndaten
    sicherheitstechnisch, 15

L

Leitsystem, 7

M

Mean Time Between Failures, 15
Messgenauigkeit, 13
MTBF, 15
MTTR, 15

P

Produktinformation im Internet, 6

S

Schreibschutz, 14
Sensor, 7
Sensorabgleich, 13
Sicherheit
    überprüfen, 15
Sicherheitsfunktion, 12
    überprüfen, 13, 14
Siemens-Niederlassung, 6

T

Technischen Daten, 13

U

Überprüfung, 14

W

Wartung, 14
Weitere Information, 6