

Hinweise zur funktionalen Sicherheit



Temperatur-Messumformer

TTH200, TTR200, TTH300, TTF300, TTF350

SIL-Sicherheitshinweise

SM/TTX200/TTX300/SIL-DE

02.2011

Rev. A

Originalanleitung

Hersteller:

ABB Automation Products GmbH

Borsigstraße 2
63755 Alzenau
Deutschland
Tel.: 0800 1114411
Fax: 0800 1114422
vertrieb.messtechnik-produkte@de.abb.com

Kundencenter Service

Tel.: +49 180 5 222 580
Fax: +49 621 381 931-29031
automation.service@de.abb.com

© Copyright 2011 by ABB Automation Products GmbH
Änderungen vorbehalten

Dieses Dokument ist urheberrechtlich geschützt. Es unterstützt den Anwender bei der sicheren und effizienten Nutzung des Gerätes. Der Inhalt darf weder ganz noch teilweise ohne vorherige Genehmigung des Rechtsinhabers vervielfältigt oder reproduziert werden.

1	Anwendungsbereich	4
2	Akronyme und Abkürzungen	4
3	Geltende Normen	7
4	Mitgeltende Dokumente und Unterlagen	7
5	Begriffe und Definitionen	8
6	Sicherheitsfunktion.....	9
6.1	Messstelle für SIL Level 2 – Single Configuration	10
6.2	Messstelle für SIL Level 3 – Dual Configuration	11
7	Wiederkehrende Prüfungen	12
8	Konfiguration.....	13
9	SIL 2 TÜV-Zertifikat	16
10	Namur NE 93	16
11	Management Summary FMEDA – Failure Modes, Effects and Diagnostic Analysis.....	17

1 Anwendungsbereich

Temperaturüberwachung von Feststoffen, Flüssigkeiten und Gasen aller Art in Behältern und Rohrleitungen, welche den besonderen Anforderungen der Sicherheitstechnik nach IEC 61508 genügen sollen.

Die Betriebsgrenzwerte sind in den Datenblättern und Betriebsanleitungen der einzelnen Modelle beschrieben. Bei Fragen wenden Sie sich bitte an Ihren ABB-Partner.

2 Akronyme und Abkürzungen

Akronym / Abkürzung	Englisch	Beschreibung
HFT	Hardware Fault Tolerance	Hardware-Fehlertoleranz des Gerätes. 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.
λ_D	Dangerous	Rate gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems, entspricht $0,5 \lambda$ (mit angenommenen 50 % gefahrbringender Ausfälle und 50 % ungefährlicher Ausfälle).
λ_{DD}	Dangerous Detected	Rate erkannter gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems (Dies ist die Summe aller Raten gefahrbringender Ausfälle innerhalb eines Kanals eines Teilsystems).
λ_{DU}	Dangerous Undetected	Rate unerkannter gefahrbringender Ausfälle (je Stunde) eines Kanals eines Teilsystems (Dies ist die Summe aller Raten unerkannter gefahrbringender Ausfälle innerhalb eines Teilsystems).
λ_{SD}	Safe Detected	Rate erkannter ungefährlicher Ausfälle (je Stunde) eines Kanals eines Teilsystems (Dies ist die Summe aller Raten erkannter ungefährlicher Ausfälle innerhalb eines Kanals eines Teilsystems).
λ_{SU}	Safe Undetected	Rate unerkannter ungefährlicher Ausfälle (je Stunde) eines Kanals eines Teilsystems (Dies ist die Summe aller Raten unerkannter ungefährlicher Ausfälle innerhalb eines Kanals eines Teilsystems).

Akronym / Abkürzung	Englisch	Beschreibung
SIL	Safety Integrity Level	Die internationale Norm IEC 61508 definiert vier diskrete, so genannte Safety Integrity Levels (SIL 1 bis SIL 4). Jeder Level entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion. Je höher der Safety Integrity Level der sicherheitsbezogenen Systeme ist, umso geringer ist die Wahrscheinlichkeit, dass sie die geforderten Sicherheitsfunktionen nicht ausführen.
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle, d. h. der Anteil von Ausfällen ohne Potenzial, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.
Low Demand Mode	Low Demand Mode of operation	Messart mit niedriger Anforderungsrate. Messart, bei der die Anforderungsrate für das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist.
DCS	Distributed Control System	Steuerungssystem, das in industriellen Anwendungen zur Überwachung und Steuerung von dezentralen Geräten eingesetzt wird.
HMI	Human Machine Interface (Mensch-Maschine-Schnittstelle)	In diesem Fall ist das HMI ein kombiniertes Modul bestehend aus einer LCD-Anzeige mit oder ohne lokale Tastatur.
DTM	Device Type Manager	Ein DTM ist ein Softwaremodul, das bestimmte Funktionen für den Zugriff auf Geräteparameter, die Konfiguration und Bedienung der Geräte sowie für die Diagnose von Problemen bereitstellt. Der DTM selbst ist keine ausführbare Software. Erst in einem so genannten FDT-Container-Programm wird er aktiv.
LRV	Lower Range Value	Untere Messbereichsgrenze
URV	Upper Range Value	Obere Messbereichsgrenze
Multidrop	Multidrop-Modus	Im Multidrop-Modus werden bis zu 15 Feldgeräte parallel an ein einziges Leitungspaar angeschlossen. Das analoge Stromsignal dient lediglich dazu, die Geräte in Zweileitertechnik mit einem festen Strom von ≤ 4 mA zu versorgen.

Akronym / Abkürzung	Englisch	Beschreibung
	closed coupled	kurze Anschlussleitung zum Temperaturfühler, Länge kleiner 1 m (39,37 inch) und mechanisch geschützt verlegte Anschlussleitung.
	extension wire	lange Anschlussleitung zum Temperaturfühler, Länge größer 1 m (39,37 inch) oder mechanisch nicht geschützt verlegte Anschlussleitung.
	low stress	niedrige bis mittlere Belastung nach Datenblattangabe (Temperatur- und mechanische Belastung des Sensors)
	high stress	hohe Belastung nach Datenblattangabe (Temperatur- und mechanische Belastung des Sensors)
	Single Configuration	Einfache Konfiguration, d. h. Einsatz von einem Messumformer pro Messstelle. Das ergibt eine HFT = 0 (1oo1 Architektur) für entsprechenden SIL2.
	Dual Configuration	Zweifache Konfiguration, d. h. Einsatz von zwei Messumformern pro Messstelle. In dieser Konfiguration sind die beiden Stromsignale 4 ... 20 mA von der nachgeschalteten Logikeinheit, z. B. einer DCS, entsprechend auszuwerten. Das ergibt eine HFT = 1 (1oo2 Architektur) für entsprechenden SIL3.

3 Geltende Normen

Norm	Bezeichnung
IEC 61508, Teil 1 bis 7	Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme.

4 Mitgeltende Dokumente und Unterlagen

Neben den SIL-Sicherheitshinweisen sind folgende Unterlagen zu beachten:

Produktbezeichnung	Dokumentname	Dokumentart
TTH200	DS/TTH200	Datenblatt
TTH200	OI/TTH200	Betriebsanleitung
TTH200	CI/TTH200	Inbetriebnahmeanleitung
TTR200	DS/TTR200	Datenblatt
TTR200	OI/TTR200	Betriebsanleitung
TTR200	CI/TTR200	Inbetriebnahmeanleitung
TTH300	DS/TTH300	Datenblatt
TTH300	OI/TTH300	Betriebsanleitung
TTH300	CI/TTH300	Inbetriebnahmeanleitung
TTF300	DS/TTF300	Datenblatt
TTF300	OI/TTF300	Betriebsanleitung
TTF300	CI/TTF300	Inbetriebnahmeanleitung
TTF350	DS/TTF350	Datenblatt
TTF350	OI/TTF350	Betriebsanleitung
TTF350	CI/TTF350	Inbetriebnahmeanleitung

Die Dokumente können in den verfügbaren Sprachen über die ABB Internetseite „www.abb.de/temperatur“, heruntergeladen werden.

Darüber hinaus ist der Anwender dieses Produktes für die Einhaltung der jeweils geltenden Gesetze und Normen verantwortlich.

5 Begriffe und Definitionen

Begriffe	Definitionen
Gefahrbringender Ausfall	Ausfall mit dem Potenzial, das sicherheitsbezogene System in einen gefährlichen oder funktionsunfähigen Zustand zu versetzen.
Sicherheitsbezogenes System	Ein sicherheitsbezogenes System führt die Sicherheitsfunktionen aus, die erforderlich sind, um einen sicheren Zustand, z. B. einer Anlage, zu erreichen oder aufrechtzuerhalten. Beispiel: Ein Druckmessgerät, eine Logikeinheit (z. B. ein Grenzsinalgeber) und ein Ventil bilden ein sicherheitsbezogenes System.
Sicherheitsfunktion	Eine definierte Funktion, die von einem sicherheitsbezogenen System ausgeführt wird, mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalles, einen sicheren Zustand für die Anlage zu erreichen oder aufrechtzuerhalten. Beispiel: Grenztemperaturüberwachung.

6 Sicherheitsfunktion

Die Messumformer TTH200-.H, TTR200-.H, TTH300-.H, TTF300-.H und TTF350-.H erzeugen ein temperaturlineares Einheitssignal von 4 ... 20 mA. Sämtliche Sicherheitsfunktionen beziehen sich ausschließlich auf das analoge Ausgangssignal.

Der gesamte gültige Bereich des Ausgangssignals ist auf ein Minimum von 3,8 mA und ein Maximum von 20,5 mA (Werkseinstellung) zu konfigurieren.



WARNUNG!

Im Safety-Betrieb darf HART-Kommunikation nur mit aktiviertem Schreibschutz stattfinden. Der HART-Master muss hierbei die Safety-Anforderungen der Kundenapplikation erfüllen.

Alarmverhalten und Stromausgang

Wenn kritische Fehler erkannt werden, wird der konfigurierte Alarmstrom erzeugt und einer nachgeschalteten Logikeinheit, z. B. einem DCS, zugeführt und dort auf das Überschreiten eines definierten maximalen Wertes überwacht. Es gibt zwei wählbare Modi für diesen Alarmstrom:

- HIGH ALARM (Hochalarm, maximaler Alarmstrom); dies ist die Werkseinstellung
- LOW ALARM (Tiefalarm, minimaler Alarmstrom)

Der Tiefalarmstrom kann in einem Bereich von 3,5 ... 4,0 mA konfiguriert werden. Die Werkseinstellung ist 3,6 mA.

Der Hochalarmstrom kann in einem Bereich von 20,0 ... 23,6 mA konfiguriert werden. Die Werkseinstellung ist 22 mA.

In den folgenden Fällen wird ein entdeckter Fehler unabhängig vom konfigurierten Alarmstrom innerhalb des Tiefalarmbereichs angezeigt:

- Fehler bei der Programmausführung
- Speicherfehler (nichtflüchtige Daten, RAM, ROM)

Nach Einschalten bzw. Neustart der Messumformer-Elektronik beträgt die minimale Tiefalarmzeit (LOW-Alarm, Start-Up Time) 10 ... 15 Sekunden.



WARNUNG!

Für eine sichere Fehlerüberwachung müssen die folgenden Bedingungen erfüllt sein:

- Der Tiefalarm muss auf einen Wert $\leq 3,6$ mA konfiguriert werden.
- Der Hochalarm muss auf einen Wert ≥ 21 mA konfiguriert werden.
- Das DCS muss die konfigurierten Hoch- bzw. Tiefalarme als Fehlfunktion erkennen und der Alarm muss entsprechend konfiguriert sein.



WARNUNG!

Um eine sichere Funktion des Stromausgangs zu gewährleisten, muss die Klemmenspannung am Gerät zwischen 11 V ... 42 V DC (Nicht-Ex-Ausführung) und 11 V ... 30 V DC (Ex-Ausführung) liegen.

Die DCS-Spannungsversorgung für den Messumformer muss in der Lage sein, den benötigten Spannungspegel auch dann bereitzustellen, wenn der Stromausgang mit dem konfigurierten Hochalarm läuft.

Unter den folgenden Bedingungen entspricht das Gerät nicht den Sicherheitsbestimmungen:

- Während der Konfiguration
- Bei deaktiviertem Schreibschutz
- Bei aktiviertem HART-Multidrop-Modus
- Während einer Simulation
- Während der Überprüfung der Sicherheitsfunktion



WARNUNG!

Zur Sicherheitsfunktion des Gerätes gehört das Grundgerät TTH200-.H, TTR200-.H, TTH300-.H, TTF300-.H und TTF350-.H mit angeschlossenem Sensor inklusive der Gehäuse und der verwendeten Prozessanschlüsse. Die Angaben der entsprechenden Dokumentation ist hierbei entsprechend zu berücksichtigen.

Gesamt-Sicherheitsgenauigkeit

Der definierte Wert für die Gesamt-Sicherheitsgenauigkeit der Sicherheitsfunktion dieses Gerätes beträgt $\pm 2 \%$ vom Messbereich.

Die Basisgenauigkeit ist sensortypabhängig und kann den entsprechenden Datenblättern entnommen werden.

Einschaltzeit und Safety-Betriebszustand

Nach dem Einschalten des Geräts werden alle Safety-relevanten Fehler nach 2 Minuten im Low Demand Mode erkannt.

6.1 Messstelle für SIL Level 2 – Single Configuration

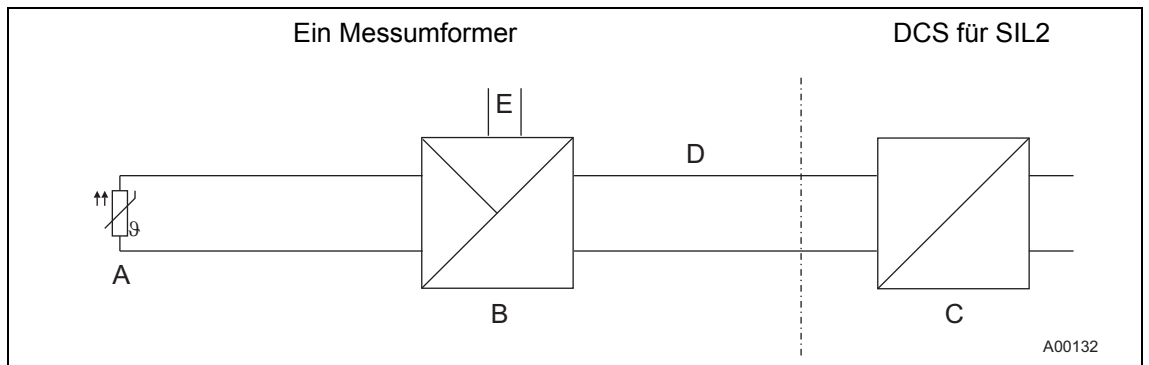


Abb. 1

- A Sensor
- B Messumformer
- C DCS

- D 4 ... 20 mA Messkreis
- E Schnittstelle für LCD-Anzeiger

6.2 Messstelle für SIL Level 3 – Dual Configuration

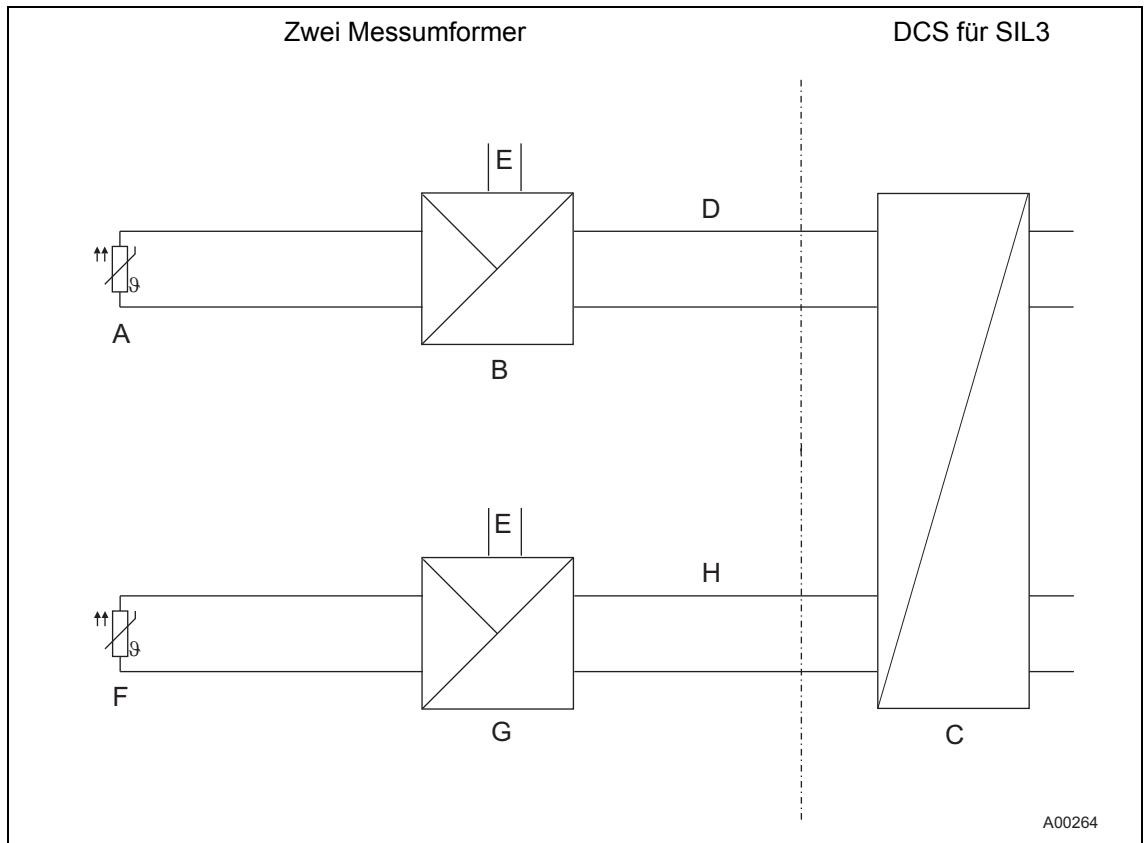


Abb. 2

- | | |
|----------------------------------|------------------|
| A Sensor 1 | F Sensor 2 |
| B Messumformer 1 | G Messumformer 2 |
| C DCS | H Messkreis 2 |
| D Messkreis 1 | |
| E Schnittstelle für LCD-Anzeiger | |



WICHTIG (HINWEIS)

Die sicherheitstechnischen Kenngrößen sind Kapitel 11 „Management Summary FMEDA – Failure Modes, Effects and Diagnostic Analysis“, Seite 17, zu entnehmen.

7 Wiederkehrende Prüfungen

Sicherheitsüberprüfungen

Die Sicherheitsfunktion der gesamten Sicherheitsschleife ist regelmäßig gemäß IEC 61508 zu überprüfen. Die Intervalle für die Überprüfung werden bei der Berechnung der individuellen Sicherheitsschleifen einer Anlage bestimmt.

Es liegt in der Verantwortung des Betreibers, die Art der Überprüfung und die Zeitabstände im genannten Zeitraum zu wählen. Der PFD_{AV} -Wert hängt vom gewählten Prüfzeitintervall ab. Für die PFD_{AV} -Werte in der SIL-Konformitätserklärung beträgt das Prüfzeitintervall $T[Proof]$ zur Überprüfung der Sicherheitsfunktion 1 Jahr. Andere Prüfzeitintervalle mit den entsprechenden PFD_{AV} -Werten sind dem Kapitel „Management Summary FMEDA“ zu entnehmen.

Die Überprüfung muss so durchgeführt werden, dass die korrekte Funktion der Sicherheitseinrichtung im Zusammenspiel mit allen Komponenten nachgewiesen werden kann.

Ein mögliches Verfahren für die wiederkehrenden Prüfungen zur Entdeckung gefährlicher und unentdeckter Gerätestörungen wird im Folgenden beschrieben. Wobei 99 % der du-Fehler des Messumformers durch diese Überprüfung erkannt werden.

Überprüfung der Sicherheitsfunktion

Zur Überprüfung der Sicherheitsfunktion des Geräts ist folgendermaßen vorzugehen:

1. Das Sicherheits-DCS überbrücken oder andere geeignete Maßnahmen ergreifen, um ein unbeabsichtigtes Auslösen des Alarms zu verhindern.
2. Den Schreibschutz deaktivieren (siehe jeweilige Betriebsanleitung).
3. Den Stromausgang des Messumformers mit Hilfe des EDD / DTM-Simulationsbefehls (Diagnose / Simulation / Stromausgang) auf einen Hochalarmwert einstellen.
4. Prüfen, ob das Stromausgangssignal diesen Wert erreicht.
5. Den Stromausgang des Messumformers mit Hilfe des EDD / DTM-Simulationsbefehls auf einen Tiefalarmwert einstellen.
6. Prüfen, ob das Stromausgangssignal diesen Wert erreicht.
7. Den Schreibschutz aktivieren (siehe jeweilige Betriebsanleitung) und mindestens 20 Sekunden warten.
8. Das Gerät durch Abschalten neu starten.
9. Den Stromausgang mit Referenztemperatur überprüfen, für den LRV-Wert (untere Messbereichsgrenze: 4 mA) und den URV-Wert (obere Messbereichsgrenze: 20 mA) per 2-Punkt Kalibrierung.
10. Die Überbrückung des Sicherheits-DCS entfernen oder den normalen Betriebszustand auf andere Weise wiederherstellen.
11. Nach der Durchführung des Tests müssen die Ergebnisse dokumentiert und entsprechend archiviert werden.

Die Überprüfung des Messumformers ohne Sensor kann auch mit einem entsprechenden Simulator (Pt100-Simulator, Referenz-Spannungsquellen) erfolgen. Hierbei ist der Sensor gemäß den SIL-Anforderungen der Kundenapplikation zu prüfen. Temperaturfühler SensyTemp TSP können gemäß der OI/TSP per Schnellprüfung überprüft werden.

8 Konfiguration

Das Gerät wurde gemäß Kundenauftrag konfiguriert und getestet.

Trotzdem kann das Gerät über die LCD-Anzeige mit lokaler Tastatur oder via DTM / EDD über die HART-Schnittstelle konfiguriert werden. Andere Konfigurationshilfsmittel wie mobile Handheld-Terminals werden in dieser Anleitung nicht beschrieben.

Während der Konfiguration ist der sichere Betrieb des Gerätes nicht garantiert.



WARNUNG!

Überprüfungen:

Vor der Inbetriebnahme des Gerätes muss überprüft werden, ob die Gerätekonfiguration die Sicherheitsfunktion des Systems gewährleistet.

Sicherstellen, dass das richtige Gerät an der richtigen Messstelle installiert wurde.

Nach jeder Veränderung des Gerätes, wie z. B. eine Änderung der Einbauposition des Gerätes oder eine Änderung der Konfiguration, ist die Sicherheitsfunktion des Gerätes erneut zu überprüfen.

Nach der Überprüfung der Sicherheitsfunktion ist das Gerät gegen Bedienung per Schreibschutz zu sichern, da jede Änderung des Messsystems oder der Parameter die Sicherheitsfunktion beeinträchtigt.

Zur Gewährleistung der Sicherheit muss das Gerät schreibgeschützt sein.

Dies kann durch die folgenden Schritte erreicht werden:

Aktivierung / Deaktivierung des Schreibschutzes

1. TTH300-.H, TTF300-.H und TTF350-.H über die LCD-Anzeige mit lokaler Tastatur.

Die Menüfolge „Konfig. Gerät“, „Schreibschutz“ und dann für Schreibschutz-Aktivierung Passwort ungleich „0110“ eingeben und für Schreibschutz-Aufhebung Passwort „0110“ eingeben. (siehe Betriebsanleitung)

2. TTH200-.H, TTR200-.H, TTH300-.H, TTF300-.H und TTF350-.H über DTM / EDD.

Die Menüfolge „Gerät“, „Schreibschutz“ aktivieren.

Wenn das Gerät verriegelt (schreibgeschützt) ist, kann es nicht konfiguriert werden. Dieser Schutz bezieht sich auf das gesamte Gerät. Schreibschutz-Aufhebung Passwort „0110“.

3. TTR200-.H, TTH300-.H, TTF300-.H und TTF350-.H, HW-Schreibschutz via DIP-Schalter Konfiguration on / off (siehe Betriebsanleitung)

**WARNUNG!****Überprüfungen:**

Der Schreibschutz muss wie folgt überprüft werden:

1. TTH300-.H, TTF300-.H und TTF350-.H Verriegelung über die LCD-Anzeige mit lokaler Tastatur:
 - Überprüfen, ob das Verriegelungssymbol auf der LCD-Anzeige angezeigt wird.
 - Das Menü „Fehlersignalisierung“ auswählen und sicherstellen, dass das Bearbeitungssymbol (Bearb.) nicht auf der LCD-Anzeige angezeigt wird.
 - Sicherstellen, dass das Drücken der Bearbeitungstaste (Bearbeiten / Edit) auf der LCD-Anzeige zu keiner Reaktion führt.
2. TTH200-.H, TTR200-.H, TTH300-.H, TTF300-.H und TTF350-.H Sicherung über DTM / EDD:
 - LCD-Anzeige mit lokaler Tastatur verfügbar: Prüfen wie unter Punkt 1 beschrieben.
 - Keine LCD-Anzeige mit lokaler Tastatur verfügbar (Überprüfung des Schreibschutzes): Die Menüfolge <Gerät>, <Parametrieren> Stromausgang / Dämpfung auswählen und z. B. den Dämpfungswert verändern. Anschließend „Gerät_Daten im Gerät speichern“ auswählen und sicherstellen, dass eine Meldung mit dem Inhalt „Gerät ist schreibgeschützt“ angezeigt wird.

**WARNUNG!**

Der Software-Schreibschutz verriegelt sich nicht wieder automatisch. Er bleibt so lange entriegelt, bis er explizit zurückgesetzt wird.

Diagnosekonfiguration

Die Diagnosekonfiguration des Gerätes erfüllt die Sicherheitsanforderungen und beinhaltet die folgenden Fehlererkennungen:

- Sensorboard Kommunikation Fehler
- Sensorboard Fehler
- Sensorboard A/D-Wandler Fehler
- Messfehler Gerätetemperatur
- Sensor Grenzwertalarm oben und unten
- TTH300-.H, TTF300-.H und TTF350-.H, Sensor Fehler Ch. 1. und Ch. 2.
 - Sensorkonfiguration Widerstandsthermometer, R in Zwei-, Drei- und Vierleiterschaltung mit Leitungsbruch und Kurzschluss
 - Sensorkonfiguration Thermoelement, mV mit Leitungsbruch
 - Redundanz-Mode Ch 1. und Ch 2. bei aktivierter Driftüberwachung

Konfigurationsparameter mit Einfluss auf die Sicherheitsfunktion

Alle Konfigurationsparameter, die über die LCD-Anzeige mit lokaler Tastatur, DTM / EDD bzw. per HART-Kommunikation bei deaktiviertem Schreibschutz geändert werden, haben Einfluss auf die Sicherheitsfunktion des Gerätes. Die Beschreibung der Parameter erfolgt in der Betriebsanleitung. Die Überprüfung der Sicherheitsfunktion erfolgt gemäß den SIL-Sicherheitshinweisen.

Für den Redundanz-Mode mit Driftüberwachung müssen die folgenden Parameter im DTM, EDD beim TTH300-.H TTF300-.H und TTF350-.H eingestellt werden:

Redundanz-Mode beim TTH300-.H, TTF300-.H und TTF350-.H

- Impulsausgang aktiv
- Impulszeit 60 s, Dauerimpuls
- Driftwert konfiguriert gemäß Kundenapplikation
- Driftdauer maximal 120 s.

Sensortyp-Freistilkennlinie und Callendar-Van Dusen beim TTH300-.H, TTF300-.H und TTF350-.H

Die Verwendung von diesen beiden Konfigurationen erfordert eine Überprüfung an mindestens 3 Stützpunkten zur Überprüfung der konfigurierten Kennlinie. Für komplexe Kurven sind entsprechend der Komplexität mehr Stützpunkte zu überprüfen.

9 SIL 2 TÜV-Zertifikat

Certificate

SLA 0187/09-01, Ver. 1.0

TÜV NORD SysTec GmbH & Co. KG hereby certifies

ABB Automation Products GmbH

Borsigstr. 2
63755 Alzenau / Germany

that the
Temperature Transmitters

**TTH200-.H / TTR200-.H / TTH300-.H
TTR300-.H / TTF300-.H / TTF350-.H**

are capable for safety related applications up to SIL 2, SIL 3 pending on the architecture and meets the requirements listed in the following standard.

IEC 61508: 2000;
Functional safety of electrical/electronic/programmable electronic safety-related systems
SIL 2 capability for single transmitter use
SIL 3 capability for dual transmitter use

The certification is based on the report SLA-0187/2009TTR-01 in the valid version. This certificate entitles the holder to use the pictured Safety Approved mark.

Expiry date: 2015-12-22
Reference No.: G.SCC.DL.06.045.01.SLA

Gerhard M. Rieger
Branch Manager
Augsburg, 2010-12-21

TÜV NORD SysTec GmbH & Co. KG, Branch South, Halderstraße 27, 86150 Augsburg, Germany

10 Namur NE 93

Die Temperatur-Messumformer TTH200-.H, TTR200-.H, TTH300-.H, TTF300-.H und TTF350-.H erfüllen die Anforderungen gemäß Namur NE 93.

11 Management Summary FMEDA – Failure Modes, Effects and Diagnostic Analysis



Management summary for TT*200-*H and TT*3*0-*H, 4..20 mA output

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the temperature transmitters TT*200-*H and TT*3*0-*H with 4..20 mA output.

The temperature transmitter TT*200-*H is a configurable single sensor channel (1 x RTD 2/3/4 wire, 1 x TE, 1 x mV) analog 4..20mA device.

The temperature transmitter TT*3*0-*H is a configurable single or dual sensor channel (1 or 2 x RTD 2/3/4 wire, 2 x TE, 2 x mV, 1 x RTD 2/3 and 1 x TE / mV) analog 4..20mA device output.

Table 1 gives an overview of the different types that belong to the considered temperature transmitters including hardware and software version

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.

Table 1: Version overview

Type	Description	HW Version	SW Version
TTH200-*H	Head mounted temperature transmitter	1.06	1.00.06
TTR200-*H	Rail mounted temperature transmitter	1.01	1.00.06
TTH300-*H	Head mounted temperature transmitter	1.06	1.01.07
TTR300-*H	Rail mounted temperature transmitter	1.01	1.01.07
TTF300-*H	Field mounted temperature transmitter	1.06	1.01.07
TTF350-*H	Field mounted temperature transmitter	1.06	1.01.07

For safety applications only the 4..20 mA output was considered. All 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 $\geq 1,00E-03$ to $< 1,00E-02$ for SIL 2 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 2 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-03.

The temperature transmitters TT*200-*H and TT*3*0-*H with 4..20 mA output are considered to be Type B¹ subsystems with a hardware fault tolerance of 0.

The failure rates do not include failures resulting from incorrect use of the temperature transmitters TT*200-*H and TT*3*0-*H with 4..20 mA output, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

¹ Type B subsystem: "Complex" subsystem (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 40°C. 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.

It is assumed that the connected logic solver is configured per the NAMUR NE43 signal ranges, i.e. the temperature transmitters TT*200-*H and TT*3*0-*H with 4..20 mA output communicate detected faults by an alarm output current $\leq 3,6\text{mA}$ or $\geq 21\text{mA}$. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled.

Table 2: Failure rates ²

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	327
Fail dangerous detected (internal diagnostics or indirectly ³)	227
Fail high (detected by the logic solver)	23
Fail low (detected by the logic solver)	77
Annunciation detected	0
Fail Dangerous Undetected	41
Fail dangerous undetected	39
Annunciation undetected	2
No Effect	110
Not part	91

Table 3: IEC 61508 failure rates

λ_{SD}	λ_{SU} ⁴	λ_{DD}	λ_{DU}	SFF ⁵	DC _S ⁶	DC _D ⁸
0 FIT	110 FIT	327 FIT	41 FIT	91%	0%	88%

Table 4: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 1,79E-04	PFD _{AVG} = 8,95E-04	PFD _{AVG} = 1,79E-03

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 Note: SFF should be calculated for the sensor subsystem. This SFF is only for reference.

⁶ DC means the diagnostic coverage (safe or dangerous) for the temperature transmitters by the safety logic solver.



A complete temperature sensor assembly consisting of the temperature transmitters TT*200-*H and TT*3*0-*H 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 3 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

Assuming that the temperature transmitter TT*200-*H and TT*3*0-*H 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 (T[Proof] = 1 year) for the thermocouple or RTD in a **low stress environment** is as follows:

Table 5: TT*200-*H and TT*3*0-*H with thermocouple (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	422 FIT	46 FIT	92%	2,01E-04

Table 6: TT*3*0-*H with two thermocouples (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	533 FIT	38 FIT	94%	1,68E-04

Table 7: TT*200-*H and TT*3*0-*H with 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	366 FIT	50 FIT	90%	2,17E-04

Table 8: TT*3*0-*H with two 2/3-wire RTDs (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	428 FIT	39 FIT	93%	1,70E-04

Table 9: TT*3*0-*H with thermocouple and 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	481 FIT	43 FIT	93%	1,90E-04

Table 10: TT*200-*H and TT*3*0-*H with 4-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	375 FIT	44 FIT	91%	1,90E-04

Table 11: TT*200-*H and TT*3*0-*H with thermocouple (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	1227 FIT	141 FIT	90%	6,17E-04



Table 12: TT*3*0-*H with two thermocouples (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	2323FIT	48 FIT	98%	2,10E-04

Table 13: TT*200-*H and TT*3*0-*H with 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	707 FIT	136 FIT	85%	5,95E-04

Table 14: TT*3*0-*H with two 2/3-wire RTDs (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	1274 FIT	47 FIT	96%	2,08E-04

Table 15: TT*3*0-*H with thermocouple and 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	1799 FIT	48 FIT	97%	2,09E-04

Table 16: TT*200-*H and TT*3*0-*H with 4-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	822 FIT	46 FIT	95%	2,01E-04

Assuming that the temperature transmitters TT*200-*H and TT*3*0-*H 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 (T[Proof] = 1 year) for the thermocouple or RTD in a **high stress environment** is as follows:

Table 17: TT*200-*H and TT*3*0-*H with thermocouple (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	2227 FIT	141 FIT	94%	6,17E-04

Table 18: TT*3*0-*H with two thermocouples (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	4323 FIT	48 FIT	98%	2,10E-04

Table 19: TT*200-*H and TT*3*0-*H with 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	1114 FIT	214 FIT	85%	9,36E-04

Table 20: TT*3*0-*H with two 2/3-wire RTDs (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	2236 FIT	55 FIT	97%	2,42E-04



Table 21: TT*3*0-*H with thermocouple and 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	3280 FIT	146 FIT	95%	6,38E-04

Table 22: TT*200-*H and TT*3*0-*H with 4-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	1277 FIT	91 FIT	93%	3,98E-04

Table 23: TT*200-*H and TT*3*0-*H with thermocouple (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	18327 FIT	2041 FIT	90%	8,94E-03

Table 24: TT*3*0-*H with two thermocouples (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	40133 FIT	238 FIT	99%	1,04E-03

Table 25: TT*200-*H and TT*3*0-*H with 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	7927FIT	1941 FIT	80%	8,50E-03

Table 26: TT*3*0-*H with two 2/3-wire RTDs (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	19143 FIT	228 FIT	98%	9,98E-04

Table 27: TT*3*0-*H with thermocouple and 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	113 FIT	29638 FIT	233 FIT	99%	1,02E-03

Table 28: TT*200-*H and TT*3*0-*H with 4-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	PFD _{AVG}
0 FIT	110 FIT	10227 FIT	141 FIT	98%	6,17E-04

The boxes marked in yellow (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in green (■) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 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-03.



A user of the temperature transmitters TT*200-*H and TT*3*0-*H 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 its 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 TT*200-*H and TT*3*0-*H with 4..20 mA output (see Appendix 2).

ABB bietet umfassende und kompetente Beratung in über
100 Ländern, weltweit.

www.abb.de/temperatur

ABB optimiert kontinuierlich ihre Produkte, deshalb
sind Änderungen der technischen Daten in diesem
Dokument vorbehalten.

Printed in the Fed. Rep. of Germany (02.2011)

© ABB 2011

3KXT200005R4803



ABB Automation Products GmbH

Borsigstr. 2
63755 Alzenau
Deutschland
Tel: 0800 1114411
Fax: 0800 1114422
vertrieb.messtechnik-produkte@de.abb.com

ABB Automation Products GmbH

Im Segelhof
5405 Baden-Dättwil
Schweiz
Tel: +41 58 586 8459
Fax: +41 58 586 7511
instr.ch@ch.abb.com

ABB AG

Clemens-Holzmeister-Str. 4
1109 Wien
Österreich
Tel: +43 1 60109 3960
Fax: +43 1 60109 8309
instr.at@at.abb.com