

Temperatur-Messumformer Temperature Transmitters TH02, TH102, TH202

Hinweise zur funktionalen Sicherheit
Instructions for Functional Safety

D **Temperatur-Messumformer TH02, TH102, TH202**
Hinweise zur funktionalen Sicherheit
SIL – Sicherheitshinweise

GB **Temperature Transmitters TH02, TH102, TH202**
Instructions for Functional Safety
SIL – Safety Instructions



Inhalt/Content

Seite/Page

D Deutsch	3
GB English	10
Anhang/Appendix 1: Management Summary	17

Inhalt	Seite
1 Anwendungsbereich	4
2 Vorteile	4
3 Abkürzungen	4
4 Relevante Normen	4
5 Begriffe	5
6 Bestimmung des Safety Integrity Level (SIL)	5
7 Angaben für die Sicherheitsfunktion	7
8 Mitgeltende Gerätedokumentationen	7
9 Verhalten im Betrieb und bei Störung	7
10 Wiederkehrende Prüfungen	7
11 Einstellungen	7
11.1 Alarmverhalten und Stromausgang	7
12 Sicherheitstechnische Kenngrößen	8
12.1 Annahmen	8
12.2 Spezifische sicherheitstechnische Kenngrößen	8
13 SIL-Konformitätserklärung	9

1 Anwendungsbereich

Temperaturüberwachung von Feststoffen, Flüssigkeiten und Gasen aller Art in Behältern und Rohrleitungen, welche den besonderen Anforderungen der Sicherheitstechnik nach IEC 61508/IEC 61511-1 genügen sollen.

Die Messeinrichtung erfüllt die Anforderungen

- an funktionale Sicherheit gemäß IEC 61508/IEC 61511-1
- an Explosionsschutz (je nach Version)
- an elektromagnetische Verträglichkeit nach EN 61326 und NAMUR-Empfehlung NE 21.

2 Vorteile

Einsatz für

- Temperaturüberwachung
 - bis SIL 2, unabhängig bewertet (Functional Assessment) durch exida.com nach IEC 61508/IEC 61511-1
- Kontinuierliche Messung
- Einfache Inbetriebnahme

3 Abkürzungen

Abkürzung	Englisch	Deutsch
HFT	Hardware Fault Tolerance	Hardware Fehlertoleranz Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen.
MTBF	Mean Time Between Failures	mittlere Zeitdauer zwischen zwei Ausfällen
MTRR	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 _{av}	Average Probability of Failure on Demand	mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall
SIL	Safety Integrity Level	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 der sicherheitsbezogenen Systeme ist, um so geringer ist die Wahrscheinlichkeit, dass sie die geforderten Sicherheitsfunktionen nicht ausführen.
SFF	Safe Failure Fraction	Anteil ungefährlicher Ausfälle, Anteil von Ausfällen ohne Potential, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.
TI	Test Interval between life testing of the safety function	Prüfintervall zwischen Funktionstests der Schutzfunktion
XooY	"X out of Y" Voting (e.g. 2oo3)	Klassifizierung und Beschreibung des sicherheitsbezogenen Systems hinsichtlich Redundanz und angewandtem Auswahlverfahren. „Y“ gibt an, wie oft die Sicherheitsfunktion ausgeführt wird (Redundanz). „X“ bestimmt, wieviele Kanäle korrekt arbeiten müssen.

4 Relevante Normen

Norm	Englisch	Deutsch
IEC 61508, Teil 1 bis 7	Functional safety of electrical/electronic/programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (Zielgruppe: Hersteller und Lieferanten von Geräten)
IEC 61511, Teil 1	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)	Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie (Zielgruppe: Planer, Errichter und Nutzer)

5 Begriffe

Begriff	Erklärung
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. in einer Anlage zu erreichen oder aufrechtzuerhalten.
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.

6 Bestimmung des Safety Integrity Level (SIL)

Der erreichbare Safety Integrity Level wird durch folgende sicherheitstechnischen Kenngrößen bestimmt:

- mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall (PFD_{av})
- Hardware Fehlertoleranz (HFT) und
- Anteil ungefährlicher Ausfälle (SFF).

Die spezifischen sicherheitstechnischen Kenngrößen für TH02/102/202, als Teil der Sicherheitsfunktion, sind im Kapitel „Sicherheitstechnische Kenngrößen“ aufgeführt.

Die folgende Tabelle zeigt die Abhängigkeit des „Safety Integrity Level“ (SIL) von der mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion des gesamten sicherheitsbezogenen Systems“ (PFD_{av}). Dabei wird der „Low demand mode“ betrachtet, d. h. die Anforderungsrate an das sicherheitsbezogene System ist maximal einmal im Jahr.

Safety Integrity Level (SIL)		(Low demand mode)
4	PFD _{av}	$\geq 10^{-5} \dots < 10^{-4}$
3		$\geq 10^{-4} \dots < 10^{-3}$
2		$\geq 10^{-3} \dots < 10^{-2}$
1		$\geq 10^{-2} \dots < 10^{-1}$

Sensor, Logikeinheit und Aktor bilden zusammen ein sicherheitsbezogenes System, das eine Sicherheitsfunktion ausführt. Die „mittlere Wahrscheinlichkeit gefahrbringender Ausfälle des gesamten sicherheitsbezogenen Systems“ (PFD_{av}) teilt sich auf die Teilsysteme Sensor, Logikeinheit und Aktor üblicherweise gemäß auf.

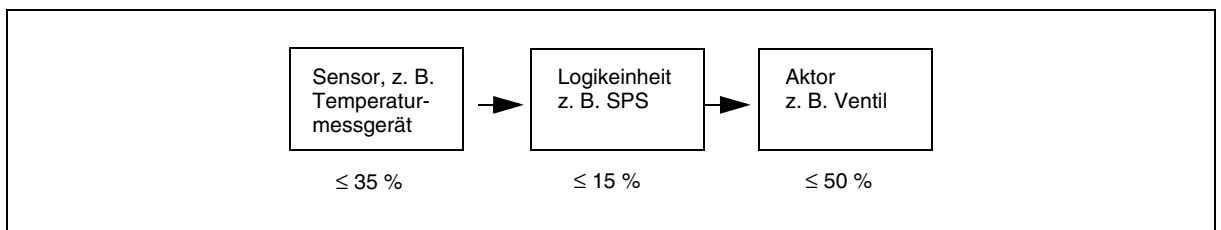


Bild 6-1: Übliche Aufteilung der „mittleren Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall“ (PFD_{av}) auf die Teilsysteme



Hinweis!

Diese Dokumentation behandelt die Messumformer TH02/102/202 als Teil einer Sicherheitsfunktion.

Die folgende Tabelle zeigt den erreichbaren „Safety Integrity Level“ (SIL) des gesamten sicherheitsbezogenen Systems für Systeme vom Typ B abhängig vom „Anteil ungefährlicher Ausfälle“ (SFF) und der „Hardware Fehlertoleranz“ (HFT). Systeme vom Typ B sind z. B. Sensoren mit komplexen Komponenten wie z. B. Mikroprozessoren (siehe auch IEC 61508, Teil 2).

Anteil ungefährlicher Ausfälle	Hardware Fehlertoleranz (HFT)		
	0	1 (0) ¹⁾	2 (1) ¹⁾
< 60 %	nicht erlaubt	SIL 1	SIL 2
60...< 90 %	SIL 1	SIL 2	SIL 3
90...< 99 %	SIL 2	SIL 3	–
≥ 99 %	SIL 3	–	–

1) Nach IEC 61511-1, Abschnitt 11.4.3, kann bei Sensoren und Aktoren mit komplexen Komponenten die „Hardware Fehlertoleranz“ (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. Messbereich, Signalrichtung im Fehlerfall usw.
- Die Konfigurationsebene des Gerätes ist geschützt, z. B. über eine Brücke oder ein Passwort (hier: Zahlencode oder Tastenkombination).
- Die Funktion hat einen geforderten „Safety Integrity Level“ (SIL) von weniger als 4.

Alle Bedingungen treffen für die Messumformer TH02/102/202 zu.

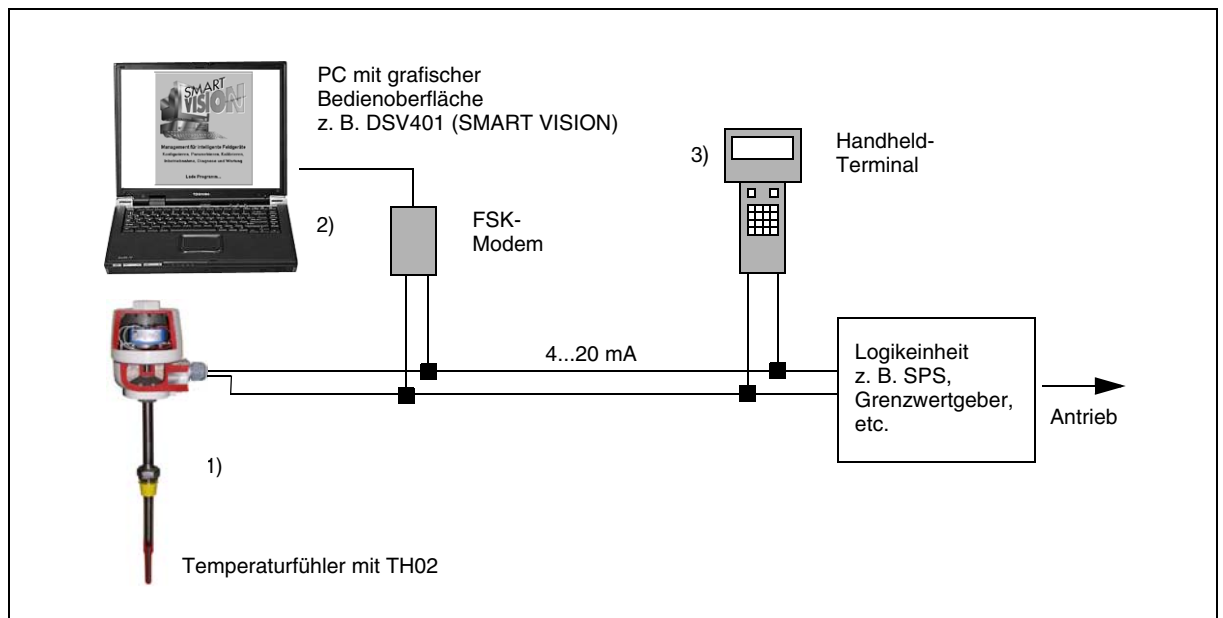


Bild 6-2: Sicherheitsfunktion (z. B. zur Grenztemperaturüberwachung) mit TH02 als Teilsystem

- 1) Temperatursensoren mit TH02
- 2) Computer mit Bedienprogramm z. B. DSV401 (SMART VISION) zur Einstellung aller Parameter wie z. B. Alarmverhalten, max. Alarm, Betriebsart usw.
- 3) Handheld-Terminal zur Einstellung aller Parameter wie z. B. Alarmverhalten, Max. Alarm, Betriebsart usw.

Der Messumformer TH02/102/202 erzeugt ein der Temperatur proportionales analoges Signal (4...20 mA). Das analoge Signal wird einer nachgeschalteten Logikeinheit wie z. B. einer SPS oder Grenzwertgeber zugeführt und dort auf das Überschreiten eines maximalen Wertes überwacht. Zur Störungsüberwachung muss die Logikeinheit sowohl HI-Alarme (einstellbar von 21...22,5 mA) als auch LO-Alarme (3,6 mA) erkennen können.

7 Angaben für die Sicherheitsfunktion



Achtung!

Die verbindlichen Einstellungen und Angaben für die Sicherheitsfunktionen sind in den Kapiteln „Einstellungen“ und „Sicherheitstechnische Kenngrößen“ aufgeführt.

Für die Reaktionszeit des Messumformers siehe Datenblatt.



Hinweis!

MTTR wird mit 8 Stunden angesetzt.

Sicherheitsbezogene Systeme ohne selbstverriegelnde Funktion müssen nach Ausführung der Sicherheitsfunktion innerhalb MTTR in einen überwachten oder anderweitig sicheren Zustand gebracht werden.

8 Mitgeltende Gerätedokumentationen

Für den Messumformer muss je nach Ausführung folgende Dokumentation vorhanden sein:

Betriebsanleitung 42/11-49XA

9 Verhalten im Betrieb und bei Störung



Hinweis!

Das Verhalten im Betrieb und bei Störung wird in der Betriebsanleitung beschrieben.

10 Wiederkehrende Prüfungen

Die Funktionsfähigkeit des Messumformers ist in angemessenen Zeitabständen zu prüfen. Wir empfehlen die Prüfung mindestens einmal im Jahr durchzuführen. Es liegt in der Verantwortung des Betreibers, die Art der Überprüfung und die Zeitabstände im genannten Zeitraum zu wählen.

11 Einstellungen

11.1 Alarmverhalten und Stromausgang

Bei einer Störung, wird der Stromwert auf den von Ihnen gewählten Wert gesetzt. Die Einstellungen können Sie entweder mittels des ABB Bedienprogramms DSV401 (SMART VISION) oder mittels Handheld-Terminal vornehmen.

12 Sicherheitstechnische Kenngrößen

12.1 Annahmen

- Kommunikation mit HART-Protokoll wird nur verwendet, um das Gerät zu konfigurieren, zu kalibrieren oder für Diagnosefunktionen; aber nicht für sicherheitstechnisch kritische Operationen.
- Die Reparaturzeit nach einem Gerätefehler beträgt 8 Stunden.
- Die mittlere Temperatur über einen langen Zeitraum betrachtet beträgt 40 °C.
- Der Messumformer wird nur in Anwendungen mit niedriger Anforderungsrate eingesetzt (low demand mode).
- Ausschließlich das Stromsignal 4...20 mA wird von der Schutzeinrichtung ausgewertet.
- Die Schutzeinrichtung ist so ausgelegt, dass sowohl Fehler, die zum Hochalarm, als auch Fehler, die zum Tiefalarm führen erkannt werden, unabhängig von der Auswirkung, sicher oder gefährlich, auf die Schutzfunktion.

12.2 Spezifische sicherheitstechnische Kenngrößen

Messumformer-Typ	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TH02/102/202, TH02/102/202-Ex	75 %	$6,60 * 10^{-4}$	471 FIT	151 FIT
TH02/102/202, TH02/102/202-Ex mit Thermoelement, low stress	92 %	$1,76 * 10^{-3}$	5221 FIT	401 FIT
TH02/102/202, TH02/102/202-Ex mit Widerstandsthermometer (4-Leiter), low stress	93 %	$7,49 * 10^{-4}$	2451 FIT	171 FIT
TH02/102/202, TH02/102/202-Ex mit Widerstandsthermometer (2-, 3-Leiter), low stress	78 %	$2,41 * 10^{-3}$	2071 FIT	551 FIT
$\lambda_{dd} + \lambda_s$: Fehlerrate gefährliche entdeckte und sichere Fehler λ_{du} : Fehlerrate gefährliche unentdeckte Fehler				

Weitere Detailinformationen siehe Management Summary in Anhang 1

13 SIL-Konformitätserklärung

49/11-80DE
Rev. 1.01



SIL-KONFORMITÄTSERKLÄRUNG

Hersteller: ABB Automation Products GmbH
Adresse: Borsigstraße 2 – D-63755 Alzenau
Produkt: Temperatur Transmitter TH02, TH02-EX, TH102, TH102-EX, TH202, TH202-EX

Funktionale Sicherheit nach IEC 61508 / IEC 61511

Wir erklären als Hersteller, dass die o.g. Geräte für den Einsatz in einer sicherheitsrelevanten Anwendung bis einschließlich SIL 2 entsprechend der IEC 61511-1 geeignet sind, wenn beiliegende Sicherheitshinweise beachtet werden.
Die Analyse der sicherheitskritischen und gefährlichen Zufallsfehler liefert unter der Annahme einer jährlichen Funktionsprüfung folgende Parameter:

SIL (Sicherheitsintegritätslevel): 2 **Typ: B**
HFT (Hardwarefehlertoleranz): 0¹⁾ (einkanalige Verwendung)

Messumformer-Typ	Messbereich	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TH02/102/202, TH02/102/202-EX	gem. IEC751, gem. IEC584	75 %	$6,60 \cdot 10^{-4}$	471 FIT	151 FIT
TH02/102/202, TH02/102/202-EX mit Thermoelement, low stress	gem. IEC584	92 %	$1,76 \cdot 10^{-3}$	5221 FIT	401 FIT
TH02/102/202, TH02/102/202-EX mit Widerstands- thermometer 4-Leiter, low stress	gem. IEC751	93 %	$7,49 \cdot 10^{-4}$	2451 FIT	171 FIT
TH02/102/202, TH02/102/202-EX mit Widerstands- thermometer 2/3-Leiter, low stress	gem. IEC751	78 %	$2,41 \cdot 10^{-3}$	2071 FIT	551 FIT

1) gemäß Kapitel 11.4 der IEC 61511

Im Rahmen des Nachweises der Betriebsbewährtheit wurde das Gerät einschließlich des Änderungswesens beurteilt.

02.03.2004

Datum

Harald Müller
Leiter Hardwareentwicklung

Wilhelm Mergler
Leiter Qualitätsmanagement

Ref.: FMEDA and Prior-use Assessment for Temperature Transmitter TH*02 exida.com

Content	Page
1 Field of application	11
2 User benefits	11
3 Acronyms and abbreviations	11
4 Relevant standards	11
5 Terms and definitions	12
6 Determination of the Safety Integrity Level (SIL)	12
7 Specifications for the safety function	14
8 Applicable device documentation	14
9 Behavior during operation and in case of malfunction	14
10 Periodic checks	14
11 Settings	14
11.1 Alarm behavior and current output	14
12 Safety-related characteristics	15
12.1 Assumptions	15
12.2 Specific safety-related characteristics	15
13 SIL conformity declaration	16

1 Field of application

Temperature monitoring of all types of solids, liquids and gases in vessels and tubings/pipelines that shall meet the special safety requirements according to IEC 61508/IEC 61511-1.

The measuring unit meets the requirements regarding

- functional safety in accordance with IEC 61508/IEC 61511-1
- explosion protection (depending on the version)
- electromagnetic compatibility in accordance with EN 61326 and NAMUR recommendation NE 21.

2 User benefits

Use for

- Temperature monitoring
 - up to SIL 2, independently assessed (functional assessment) by exida.com in acc. with IEC 61508/IEC 61511-1
- Continuous measurement
- Easy commissioning

3 Acronyms and abbreviations

Acronym / Abbreviation	Designation	Description
HFT	Hardware Fault Tolerance	The hardware fault tolerance of the device. This is the capability of a functional unit to continue the execution of the demanded function in case of faults or deviations.
MTBF	Mean Time Between Failures	This is the mean time period between two failures.
MTTR	Mean Time To Repair	This is the mean time period between the occurrence of a failure in a device or system and its repair.
PFD	Probability of Failure on Demand	This is the likelihood of dangerous safety function failures occurring on demand.
PFD _{av}	Average Probability of Failure on Demand	This is the average likelihood of dangerous safety function failures occurring on demand.
SIL	Safety Integrity Level	The international standard IEC 61508 specifies four discrete safety integrity levels (SIL 1 to SIL 4). Each level corresponds to a specific probability range regarding the failure of a safety function. The higher the safety integrity level of the safety-related systems, the lower the likelihood of non-execution of the demanded safety functions.
SFF	Safe Failure Fraction	The fraction of non-hazardous failures, i.e. the fraction of failures without the potential to set the safety-related system to a dangerous or impermissible state.
TI	Test interval between life testing of the safety function	Time interval between the functional tests of the safety function.
XooY	"X out of Y" Voting (e.g. 2oo3)	Classification and description of the safety-related system regarding redundancy and the selection procedure used. "Y" indicates how often the safety function is carried out (redundancy). "X" determines how many channels must work properly.

4 Relevant standards

Standard	Designation
IEC 61508, Part 1 to 7	Functional safety of electrical/electronic/programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)
IEC 61511, Part 1	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)

5 Terms and definitions

Terms	Definitions
Dangerous failure	Failure with the potential to set the safety-related system to a dangerous or inoperative state.
Safety-related system	A safety-related system carries out the safety functions needed to establish or maintain a safe state e.g. in a plant.
Safety function	A defined function carried out by a safety-related system in order to establish or maintain a safe state of the plant, under consideration of a specified dangerous incident.

6 Determination of the Safety Integrity Level (SIL)

The reachable safety integrity level depends on the following safety-related characteristics:

- Average probability of failure on demand (PFD_{av})
- Hardware fault tolerance (HFT)
- Safe failure fraction (SFF).

The specific safety-related characteristics for the TH02/102/202 as a part of the safety function are detailed in chapter "Safety-related characteristics".

The following table shows the dependence of the safety integrity level (SIL) on the average probability of failure on demand (PFD_{av}). The "Low demand mode" is considered here, i.e. the maximum demand rate of the safety-related system is once per year.

Safety Integrity Level (SIL)		(Low demand mode)
4	PFD _{av}	$\geq 10^{-5} \dots < 10^{-4}$
3		$\geq 10^{-4} \dots < 10^{-3}$
2		$\geq 10^{-3} \dots < 10^{-2}$
1		$\geq 10^{-2} \dots < 10^{-1}$

The sensor, the logic unit and the final control element form together a safety-related system which carries out a safety function. The average probability of failure on demand (PFD_{av}) is usually distributed over the subsystems (sensor, logic unit and final control element) as seen in the illustration below.

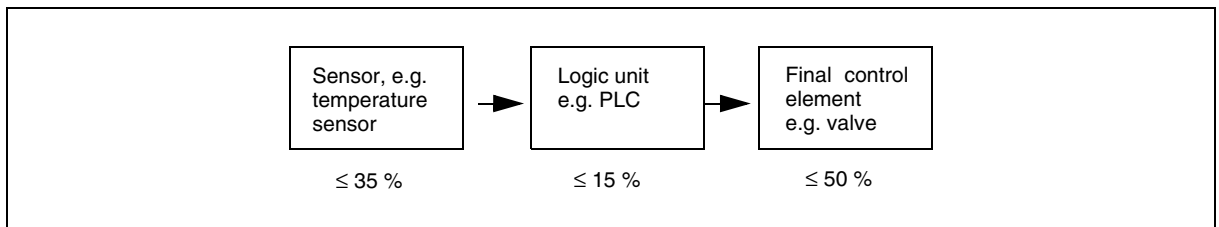


Fig. 6-1: Normal distribution of the average probability of failure on demand (PFD_{av}) over the subsystems



Note!

This documentation is valid for the transmitters TH02/102/202 as part of a safety function.

The following table shows the reachable safety integrity level (SIL) of the entire safety-related system for systems of type B, depending on the safe failure fraction (SFF) and the hardware fault tolerance (HFT). Systems of type B are e.g. sensors with complex components like microprocessors (see also IEC 61508, Part 2).

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1 (0) ¹⁾	2 (1) ¹⁾
< 60 %	impermissible	SIL 1	SIL 2
60...< 90 %	SIL 1	SIL 2	SIL 3
90...< 99 %	SIL 2	SIL 3	–
≥ 99 %	SIL 3	–	–

¹⁾ Acc. to IEC 61511-1, Part 11.4.3, the hardware fault tolerance (HFT) of sensors and final control elements with complex components can be decreased by one (value in brackets), if the following requirements are met:

- The device is proven-in-field.
- The user can only configure process-related parameters like the measuring range, signal direction in case of fault, etc.
- The device configuration level is access-protected, e.g. by jumper or password (here: code number or key combination).
- The function has a required safety integration level (SIL) less than 4.

The transmitters TH02/102/202 meet all requirements.

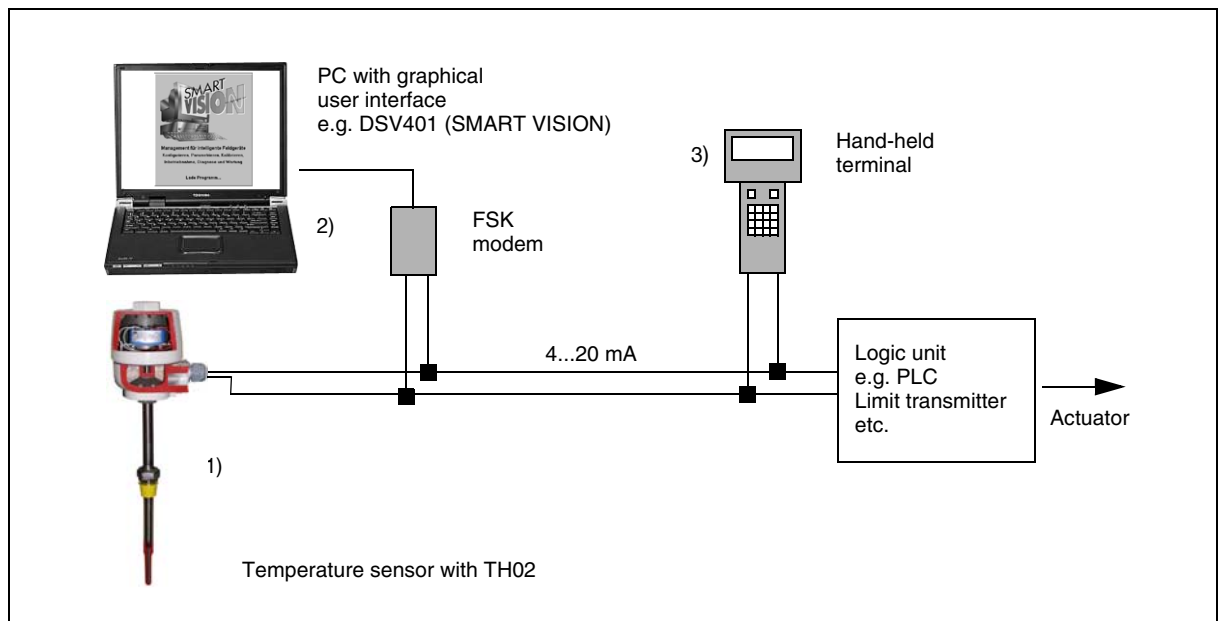


Fig. 6-2: Safety function (e.g. for temperature limit monitoring) with TH02 as a subsystem

- 1) Temperature sensor with TH02
- 2) Computer with user interface like DSV401 (SMART VISION) for setting all parameters like alarm behavior, max. alarm, operating mode, etc.
- 3) Hand-held terminal for setting all parameters, e.g. alarm behavior, max. alarm, operating mode, etc.

The transmitter TH02/102/202 produces an analog signal (4...20 mA) proportional to the temperature. This analog signal is fed to a subsequent logic unit, e.g. a PLC or limit transmitter, and monitored for violation of a defined maximum value. The logic unit must be capable of recognizing HI alarms (adjustable between 21 and 22.5 mA) and LO alarms (3.6 mA) to allow for malfunction detection.

7 Specifications for the safety function



Caution!

Refer to chapters "Settings" and "Safety-related characteristics" of this document for the mandatory settings and specifications for the safety function.

See the relevant data sheet for the transmitter response time.



Note!

An MTTR of 8 hours is specified.

Safety-related systems without an auto-locking function must be set to a monitored or otherwise safe state within the MTTR after execution of the safe function.

8 Applicable device documentation

The following documentation must be available for the transmitter, depending on the model:

Operating instructions 42/11-49XA

9 Behavior during operation and in case of malfunction



Note!

The behavior during operation and in case of malfunction is detailed in the operating instructions.

10 Periodic checks

The operativeness of the transmitter must be checked at appropriate intervals. We recommend to perform the checks at least once a year. It is the operator's responsibility to define the type of checks and the checking intervals in the stated time period.

11 Settings

11.1 Alarm behavior and current output

In case of a malfunction the current is set to the selected value. The settings can be made via the ABB user interface DSV401 (SMART VISION) or via a hand-held terminal.

12 Safety-related characteristics

12.1 Assumptions

- HART communication is only used for configuring, adjusting or diagnosing the device, but not for safety-relevant critical operations.
- The repair time after a device fault is 8 hours.
- The long-time average temperature is 40°C.
- The transmitter is only used for low demand mode applications.
- Only the 4...20 mA current signal is evaluated by the safety device.
- The safety device is designed such that both faults leading to a high alarm and faults leading to a low alarm are detected, irrespective of the effect (safe or dangerous) on the safety function.

12.2 Specific safety-related characteristics

Transmitter type	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TH02/102/202, TH02/102/202-Ex	75 %	$6.60 * 10^{-4}$	471 FIT	151 FIT
TH02/102/202, TH02/102/202-Ex with thermocouple, low stress	92 %	$1.76 * 10^{-3}$	5221 FIT	401 FIT
TH02/102/202, TH02/102/202-Ex with RTD (4-wire), low stress	93 %	$7.49 * 10^{-4}$	2451 FIT	171 FIT
TH02/102/202, TH02/102/202-Ex with RTD (2-wire/3-wire), low stress	78 %	$2.41 * 10^{-3}$	2071 FIT	551 FIT
$\lambda_{dd} + \lambda_s$: Fault rate of detected dangerous and of safe faults λ_{du} : Fault rate of undetected dangerous faults				

For details refer to the management summary in Appendix 1

13 SIL conformity declaration

49/11-80EN
 Rev. 1.01



SIL DECLARATION OF CONFORMITY

Manufacturer: ABB Automation Products GmbH
Address: Borsigstraße 2 – D-63755 Alzenau
Product name: Temperature Transmitter
 TH02, TH02-EX, TH102, TH102-EX, TH202, TH202-EX

Functional safety according to IEC 61508 / IEC 61511

We as the manufacturer declare that the a.m. products are suitable for the use in a safety related application up to SIL 2 according to IEC 61511-1, provided that the attached safety instructions are observed. The assessment of the safety critical and dangerous random errors results, in case of an annual function test, in the following parameters:

SIL (Safety integrity level): 2 **Type: B**
HFT (Hardware failure tolerance): 0¹⁾ (one-channel application)

Transmitter Type	Measuring Range	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
TH02/102/202, TH02/102/202-EX	according to IEC751, according to IEC584	75 %	$6,60 \cdot 10^{-4}$	471 FIT	151 FIT
TH02/102/202, TH02/102/202-EX with Thermocouple low stress	according to IEC584	92 %	$1,76 \cdot 10^{-3}$	5221 FIT	401 FIT
TH02/102/202, TH02/102/202-EX with 4-wire RTD low stress	according to IEC751	93 %	$7,49 \cdot 10^{-4}$	2451 FIT	171 FIT
TH02/102/202, TH02/102/202-EX with 2/3-wire RTD, low stress	according to IEC751	78 %	$2,41 \cdot 10^{-3}$	2071 FIT	551 FIT

1) according to chapter 11.4 of IEC 61511

For the prior-use investigation the instrument including the modifications was analysed.

02.03.2004

Date

Harald Müller
 Head of Hardware Development

Wilhelm Mergler
 Head of Quality Management

Ref.: FMEDA and Prior-use Assessment for Temperature Transmitter TH*02 exida.com

Anhang/Appendix 1: Management Summary



FMEDA and Prior-use Assessment

Project:
Temperature Transmitter TH*02 with 4..20 mA output

Customer:
ABB Automation Products GmbH
Alzenau
Germany

Contract No.: ABB 03/09-13
Report No.: ABB 03/09-13 R002
Version V1, Revision R1.1, March 2004
Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.



Management summary

This report summarizes the results of the hardware assessment with prior-use consideration according to IEC 61508 / IEC 61511 carried out on the temperature transmitter TH*02 with 4..20 mA output and software version V1.10. The statements made in this report are also valid for further software versions as long as the assessed modification process is considered. Any changes are under the responsibility of the manufacturer. Table 1 gives an overview of the different types that belong to the considered temperature transmitter.

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

TH02	Temperature transmitter, head mounted TH02/TH02-Ex
TH102	Temperature transmitter, rail mounted TH102/TH102-Ex
TH202	Temperature transmitter, field mounted TH202/TH202-Ex

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 temperature transmitters TH02 and TH202 can be equipped with or without display.

The failure rates 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 $\geq 10^{-3}$ to $< 10^{-2}$ 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 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 assembly consisting of TH*02 and a thermocouple or RTD supplied with TH*02 would then be $3,50E-03$.

The temperature transmitter TH*02 with 4..20 mA output is considered to be a Type B¹ component with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

As the temperature transmitter TH*02 with 4..20 mA output is supposed to be a proven-in-use device, an assessment of the hardware with additional prior-use demonstration for the device and its software was carried out. The prior-use investigation was based on field return data collected and analyzed by ABB Automation Products GmbH. This data cannot cover the process connection. The prior-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 transmitter TH*02 with a hardware fault tolerance of 0 and a SFF of 60% to < 90% is considered to be suitable for use in SIL 2 safety functions. The decision on the usage of prior-use devices, however, is always with the end-user.

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



Table 2: Summary for TH*02 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = “fail high”	Fail-safe state = “fail low”
Fail High (detected by the logic solver)		251	
Fail detected (int. diag.)	233		
Fail high (inherently)	18		18
Fail Low (detected by the logic solver)			310
Fail detected (int. diag.)	233		
Fail low (inherently)	77	77	
Fail Dangerous Undetected		151	151
No Effect		141	141
Annunciation Undetected		2	2
Not part		25	25
MTBF = MTTF + MTTR		176 years	176 years

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on whether the temperature transmitter TH*02 with 4..20 mA output is used in an application for “low level monitoring”, “high level monitoring” or “range monitoring”. For these applications the following table shows how the above stated requirements are fulfilled.

Transmitter configured fail-safe state = “fail high” – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S ²	DC _D ²
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	77 FIT	143 FIT	251 FIT	151 FIT	75%	35%	63%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	251 FIT	143 FIT	77 FIT	151 FIT	75%	64%	34%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	328 FIT	143 FIT	0 FIT	151 FIT	75%	70%	0%

Transmitter configured fail-safe state = “fail low” – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S ²	DC _D ²
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	310 FIT	143 FIT	18 FIT	151 FIT	75%	69%	11%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	18 FIT	143 FIT	310 FIT	151 FIT	75%	11%	67%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	328 FIT	143 FIT	0 FIT	151 FIT	75%	70%	0%

² DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for the temperature transmitter TH*02 with 4..20 mA output.



It is important to realize that the “don’t care” failures and the “annunciation” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

Table 3: Summary for TH*02 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 6,60E-04	PFD _{AVG} = 3,30E-03	PFD _{AVG} = 6,58E-03

A complete temperature sensor assembly consisting of TH*02 and a closely coupled thermocouple or cushioned RTD supplied with TH*02 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.

Section 5.2 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

Assuming that TH*02 is programmed to drive its output high on detected failures of the thermocouple or RTD ($\lambda_{low} = \lambda_{dd}, \lambda_{high} = \lambda_{sd}$), the failure rate contribution or the PFD_{AVG} value for the thermocouple or RTD in a low stress environment is as follows:

Table 4: Summary for the sensor assembly TH*02 / thermocouple in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD _{AVG} = 1,76E-03	PFD _{AVG} = 8,78E-03	PFD _{AVG} = 1,76E-02	92%

$\lambda_{sd} = 5001 \text{ FIT}$

$\lambda_{su} = 143 \text{ FIT}$

$\lambda_{dd} = 77 \text{ FIT}$

$\lambda_{du} = 401 \text{ FIT}$

Table 5: Summary for the sensor assembly TH*02 / 4-wire RTD in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD _{AVG} = 7,49E-04	PFD _{AVG} = 3,74E-03	PFD _{AVG} = 7,49E-03	93%

$\lambda_{sd} = 2231 \text{ FIT}$

$\lambda_{su} = 143 \text{ FIT}$

$\lambda_{dd} = 77 \text{ FIT}$

$\lambda_{du} = 171 \text{ FIT}$

Table 6: Summary for the sensor assembly TH*02 / 2/3-wire RTD in low stress environment

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	SFF
PFD _{AVG} = 2,41E-03	PFD _{AVG} = 1,21E-02	PFD _{AVG} = 2,41E-02	78%

$\lambda_{sd} = 1851 \text{ FIT}$

$\lambda_{su} = 143 \text{ FIT}$

$\lambda_{dd} = 77 \text{ FIT}$

$\lambda_{du} = 551 \text{ FIT}$



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 table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to $3,50E-03$. The boxes marked in red (■) mean that the calculated PFD_{AVG} values do not fulfill the requirement for SIL 2 according to table 2 of IEC 61508-1.

The functional assessment has shown that the temperature transmitter TH*02 with 4..20 mA output has a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and a Safe Failure Fraction (SFF) of more than 75%. Based on the verification of "prior use" it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the temperature transmitter TH*02 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 for different operating conditions is presented in section 5.1 along with all assumptions.

Die Wortmarke Industrial^{IT} und alle weiteren aufgeführten
Produktnamen in der Schreibweise XXXXX^{IT} sind
registrierte oder angemeldete Warenzeichen von ABB.

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 (04.04)

© ABB 2004



ABB Automation Products GmbH

Borsigstr. 2
63755 Alzenau
Germany
Tel: +49 551 905-534
Fax: +49 551 905-555
CCC-support.deapr@de.abb.com