TTH200, TTH300, TTF200, TTF300
Temperature transmitter

Additional instructions for IEC 61508 compliant devices from HW-Rev. 02.00 and from SW-Rev. 03.01

Measurement made easy

—
TTH300
TTH200
TTF300
TTF200

Introduction

Safety Manual for head-mount and field-mount transmitters for temperature measurement. This document must be considered in conjunction with related operating instructions.

Additional information

Additional documentation on TTH200, TTH300, TTF200, TTF300 is available for download free of charge at www.abb.com/temperature.

Alternatively simply scan this code:

TTH200 **TTH300** **TTF200** **TTF300**

Table of contents

1 Application area

The TTH300, TTH200, TTF300, TTF200 temperature transmitter are head or field mounted 2-wire 4 to 20 mA devices with HART communication protocol for the temperature monitoring of solids, fluids and gases in containers and piping.
Combined with a single (TTH200/TTF200) or dual channel (TTH300/TTF300) temperature sensor, the temperature transmitters become a temperature sensor assembly.
The temperature sensors that can be connected to the temperature transmitter for SIL safety applications are:
- 2-, 3-, and 4-wire RTD sensors
- 2-wire thermocouple sensors

The order variant 'SIL2 - Declaration of Conformity' is capable to meet the SIL safety requirements for the integration in Safety Instrumented Systems in compliance to IEC 61508:2010 within the process industry sector according to IEC 61511:2016.

The area of safety application is limited to:
- up to SIL 2 as single (HFT=0) transmitter installation
- up to SIL 3 as redundant (HFT=1) transmitter installation
- as Low Demand Mode of operation

with further constraints as stated within this safety manual.

In case of questions and detected safety critical device failures please contact the ABB Customer Service Center by stating the 'Product Type Designator' and 'Functional Safety SIL' as request headlines.

Customer service center
Tel: +49 180 5 222 580
Email: automation.service@de.abb.com

2 Purpose

According to IEC 61508 and IEC 61511 the purpose of the safety manual is to document the important information required to enable the integration of this product into a safety-related system in compliance with the requirements of the IEC 61508 and IEC 61511 standard.

3   Safety function and Safety Data Overview

This chapter provides information's on the safety function and safety integrity data based on NE 130:2011 Form B.1.

General	
Device designation and permissible types	TTH300, TTH200, TTF300, TTF200 with
	• Communication Protocol HART: Order-Code H
	• SIL Declaration of Conformity: Order-Code CS
Safety-related output signal	4 to 20 mA
Fault current	Current Low Alarm Value <=3.6 mA
	Current High Alarm Value >= 21.0 mA
Safety function(s)	Single or redundant (TTx300 only) sensor channel application for resistance thermometer or thermocouple measurements generating a related 4 to 20 mA output signal

Device type acc. to IEC 61508-2	☐ Type A (HFT=0)	☒ Type B (HFT=0)
Operating Mode	☒ Low Demand Mode	☐ High Demand/Continuous Mode
Valid Hardware-Version	02.00.02	
Valid Software-Version	03.01.00	

Type of evaluation	☒ Complete HW/SW development process evaluation incl. FMEDA and change management acc. to IEC 61508-2,3
	☐ Evaluation of „Prior use´ performance for HW/SW incl. FMEDA and change management acc. to IEC 61508-2,3
	☐ Evaluation of HW/SW field data to verify ´prior use´ acc. to IEC 61511
	☐ Evaluation by FMEDA acc IEC 61508-2
Evaluation through - report no.	Exida.com GmbH:
	FMEDA Report ABB 21/03-184 R024 V1 R1 May 2021
	TÜV NORD Systems GmbH & Co. KG:
	Assessment Report 1435.IM.143431/21TB 2022-03.31 Version 1.0

Safety Integrity			
Systematic safety integrity		☐ SIL 2 capable	☒ SIL 3 capable
Hardware safety integrity	Single-channel use (HFT = 0)	☒ SIL 2 capable	☐ SIL3 capable
	Multi-channel use (HFT ≥ 1)	☐ SIL 2 capable	☒ SIL 3 capable

Failure Rates and Diagnostic Data		
Data for the Safety Configuration	Data for the transmitter without connected sensor at the environmental conditions listed within chapter See **FMEDA Failure Data** on page 15.	
Safety Deviation	±2% (±0.32 mA)	
	λDU 39 FIT	
	λDD 527 FIT	Failure Data incl. sensor combinations see chapter
	λSU 0 FIT	**FMEDA Failure Data** on page 15
	λSD 0 FIT	
SFF – Safe Failure Fraction	93%	
Fault Detection Time	15 Minutes	
Proof-Test Coverage PTC	95% (in using the procedure described with **Periodic Proof-Test and Maintenance** on page 11)	

4 Terms and definitions

IEC 61508	International Standard 'Functional safety of electrical/electronic/programmable electronic safety-related systems'
IEC 61511	International Standard 'Functional safety – safety instrumented systems for the process industry sector'
Safety Integrity	Probability of a safety system satisfactorily performing the specified safety functions under the stated conditions.
SIL Safety Integrity Level	Discrete safety integrity level corresponding to a range of safety integrity values, where level 4 has the highest and level 1 has the lowest.
Functional safety	Part of the overall safety relating to the controlled system that depends on the correct functioning of the safety system and other risk reduction measures.
Safety function	Function to be implemented by a safety system or other risk reduction measures, that is intended to achieve or maintain a safe state for the controlled system, in respect of a specific hazardous event.
Safety deviation (formerly safety accuracy)	Change in the output due to (internal) component failures which was not rated as failure within the failure analysis
Hardware fault tolerance HFT n	Ability to continue to perform a required function in the presence of n hardware faults or errors.
Architectural constraints	The highest safety integrity level that can be claimed limited by the hardware constraints (SFF, HFT)
Systematic safety integrity SC	Measure on a scale of SC 1 to SC 4 on the systematic safety integrity when the element is applied in accordance with the instructions specified in the safety manual.
Low demand mode	The safety function is only performed on demand with a demand interval no greater than one per year and greater than twice the proof-test interval.
Dangerous failure	Failure that prevents the safety function from operating as expected
Dangerous detected failure	Dangerous failure but detected and forced to alarm state
Dangerous undetected failure	Dangerous failure not being diagnosed
Safe failure	Failure that results in a fail-safe state
No effect, no part failure	Failure without effect above the safety deviation or which are not part on the specified safety function
Annunciation failure	Failure within automatic diagnostics
Common cause failure	Failures from a single cause that affect more than one channel or component
FIT	Failure in Time (1×10^{-9} failures per hour) named λ Lambda
Failure rate	Number of failures per unit time assuming to be a constant value declared as FIT
	λ_{DD} – detected dangerous failures $\qquad$ λ_{DU} – undetected dangerous failures
	λ_{SD} – detected safe failures $\qquad$ λ_{SU} – safe failures
PFD$_{AVG}$	Average probability of dangerous failure on demand
Safe failure fraction SFF	Fraction of the overall failure rate that results to a safe failure SFF = $(\lambda_{SD}+\lambda_{SU}+\lambda_{DD})$ / $(\lambda_{SD}+\lambda_{SU}+\lambda_{DD}+\lambda_{DU})$
Proof-test	Periodic test performed to detect dangerous hidden failures and weaknesses in the mechanical integrity within the final application environment
Proof-test interval	Execution interval of the period proof-test
Proof-test coverage PTC	Fraction of detected dangerous failures by the periodic proof-test
Diagnostic coverage DC	Fraction of dangerous failures detected by on-line diagnostic tests. DC = λ_{DD} / $(\lambda_{DU}+\lambda_{DD})$

... 4 Terms and definitions

... Alarm behavior and alarm current output

Fault Detection Time	Worst case interval on the transmitter fault detection by on-line tests to output fault reaction
Common cause failure	Failure causing concurrent failures of two or more separate channels in a multiple channel system.
Systematic failure	Failure, related in a deterministic way to a certain cause, which can only be eliminated by design, manufacturing, operational procedures, documentation, or other relevant factors.
Random hardware failure	Failure, which results from degradation mechanisms in the hardware. For equipment comprising many electrical components those failures occur at predictable rates but at unpredictable random times.
Type A element Type B element	An element can be regarded as type A if, the failure modes of all constituent components are well defined; and the behavior of the element under fault conditions can be completely determined; and there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met. Otherwise, the element shall be regarded as type B.
MooN architecture	Voting redundancy architecture. e.g., 1oo2: 1 out of 2 redundant channel architecture 2oo3: 2 out of 3 redundant channel architecture
Useful lifetime	Beyond the useful lifetime the probability of failure increases with time and the probabilistic failure rate estimation is invalid.
Mission Time	Final plant operation time for the safety system. Used for the PFD_{AVG} and Proof-Test Interval calculation.
FMEDA	Failure Modes, Effects and Diagnostics Analysis
MTBF	Mean Time Between Failure MTBF = $(1 / (\lambda_{total} + \lambda_{AU} + \lambda_{no\ effect} + \lambda_{no\ part})) + MTTR$
MTTR	Mean Time to Repair
MTTF	Mean Time to Failure
DTM	Device Type Manager
EDD	Electronic Device Description
FIM	Field Information Manager
FDI	Field Device Integration
DCS	Distributed Control System
HMI	Human Machine Interface
Multidrop	HART Bus Communication Mode where output-signal is set to 4 mA
Closed coupled	Short connecting lead to the temperature sensor with less than 1 m (39.37 inches) in length and connecting leads laid with mechanical protection.
Extension wire	Long connecting lead to the temperature sensor with more than 1 m (39.37 inches) in length or connecting leads laid without mechanical protection.
Low stress	Low stress environment in terms of vibration and temperature cycling. The operation is below 67% maximum rating according to specification.
High stress	High vibration environment in terms of vibration and temperature cycling. The operation is above 67% maximum rating according to specification.
NAMUR NE43	Standardization of the signal level for the breakdown information of digital 4 to 20 mA transmitters
RTD	Resistance Temperature Sensor
TC	Thermocouple Temperature Sensor
SIS	Safety Instrumented System, e.g., consisting out of Sensors & Transmitter, Logic Solver and ESD Actuator
LRV	Lower range value (Measuring range lower limit)
URV	Upper range value (Measuring range upper limit)
Range A…B	ranges using two dots means running from the value A to the value B inclusively
Sensor redundancy with drift detection	Assembly with two sensors and one transmitter which allows to detect sensor drift failures.
Safety Assessment	Investigation based on evidence on the achieved safety integrity

5   Other relevant documents

The following corresponding product documents must be taken into consideration in addition to this SIL safety manual:

Product designation	Document name	Document type
TTH300	DS/TTH300	Data Sheet
TTH200	DS/TTH200	Data Sheet
TTF300	DS/TTF300	Data Sheet
TTF200	DS/TTF200	Data Sheet
TTH300	OI/TTH300	Operating instructions
TTH200	OI/TTH300	Operating instructions
TTF300	OI/TTF300	Operating instructions
TTF200	OI/TTF200	Operating instructions
TTH300, TTF300	COM/TTX300/HART	Interface Description

The documents can be downloaded in the available languages from the ABB website at 'www.abb.com/temperature'.
In addition, the user of this device is responsible for ensuring compliance with applicable legal regulations and standards.

6   Safety function

The safety function of the named transmitters is limited to the configurable single or dual sensor channel applications for RTD or thermocouple measurements generating a temperature related analog 4 to 20 mA output signal.

No other functions are declared and qualified as safety function.

The safety function refers strictly to the analog output signal.

The final device assembly consists of the device electronics, the attached temperature sensor, the housing with optional connected display and the related process connections.

Alarm behavior and alarm current output

When a critical error is detected, an alarm current according to NAMUR NE 43 is generated which must be evaluated and processed by the safety logic solver.

Detected failures by internal diagnostics generates the configured alarm current.

The transmitter supports two selectable modes for the alarm current:

• LOW ALARM; this is the factory default setting
• HIGH ALARM

The low alarm current can be configured in a range from 3.5 to 4.0 mA.
The factory default setting is 3.5 mA.
The **low alarm current value** for safety applications shall be configured **within 3.5 to 3.6 mA**.

The high alarm current can be configured in a range from 20.0 to 3.6 mA.
The factory default setting is 22 mA.
The **high alarm current value** for safety applications shall be configured **within 21.0 to 23.6 mA**.

The safety-related system (safety logic solver) must be able to detect both, the high and the low alarm state.

In the following cases and by some electrical part failures, an error is forced independently of the configured alarm current to the low alarm current range:

• detected runtime errors by the watchdog monitoring
• detected runtime errors by current readback monitoring
• detected memory errors

Also, failures in some electrical parts force the current into a high alarm current range independent of the configured alarm current.

... 6 Safety function

Safety Deviation

The basic accuracy depends on the sensor type and the specified data within in the corresponding data sheets and the final measurement application.

Deviation on the output current by more than **±2% (±0.32 mA)** is defined as the safety deviation for this transmitter.

Self-Diagnostics and Test Interval

The transmitter performs the following runtime error detections:
- Sensor configuration RTD: wire break and short circuit failure detection
- Sensor configuration thermocouple: wire break failure detection
- Dual Sensor configuration with activated drift detection: Sensor drift failure detection
- AD-converter failure detection by runtime diagnostics
- Program and microcontroller failure detection supervised by an independent watchdog and independent shutdown path
- Output stage failure detection by current readback monitoring and independent shutdown path
- Memory failure detection by CRC32 checksum and double inverse storage

Safety-critical errors are detected and signaled by alarm behavior within a fault detection time **of 15 minutes**.

Safety Response Time

The transmitter temperature measurement update cycle time is up to 200 ms.

With a PV Damping (PT1) configured to 0 seconds and the 'EMC Filter Strength' configured to a 'low' the 10 to 90% rise time from input to output signal is up to 1 second.

The Damping can be configured in the range of 0 to 100 seconds by the end user, and it will result in an increase of the rise time up to 2.3 x the configured damping time.

The Filter to increase EMC robustness can be configured by the end user in the range of 'Low', 'Medium', 'High'. Values other than 'Low' will result in an increase of the rise time with a factor up to 4.5.

The TTx300 series dual sensor application with sensor drift detection will result in an increase of the rise time with a factor up to 2.5.

Furthermore, the overall temperature measurement safety response time is highly dependent on the final measurement application including thermowell heat transfer.

It is the responsibility of the end user to consider and validate the impact of the above-mentioned response time behaviors.

Type Classification

This transmitter is declared as Type B complex element with HFT = 0 according to IEC 61508:2010.

Useful Lifetime

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid. A constant failure rate is assumed by the probabilistic estimation method and the provided failure rates. The useful lifetime is highly dependent on the components itself and its operating conditions – temperature and humidity in particular. The temperature transmitters TT*300-**H do not contain components by design with reduced useful lifetime which are contributing to dangerous undetected failure rate and therefore to the PFD_{AVG} calculation.

Therefore, there is no limiting factor to the useful lifetime.

When final plant experience and related field monitoring data indicates a limiting useful lifetime by related operating conditions, then the plant experience-based lifetime based must be used and considered on proof-test intervals and replacements.

SIL Capability

This transmitter has been developed and qualified according to IEC 61508:2010 and fulfills the requirements for a Systematic Safety Capability of **SC 3 (SIL 3 capable)**.

The functional safety management, development and change process has been assessed by the independent Organization TÜV NORD Systems GmbH & Co. KG, Augsburg, Germany with results reported within:

Assessment Report 1435.IM.143431/21TB 2022-03.31 Version 1.0

Note
The systematic safety integrity indicated by the systematic capability can be achieved only when the instructions and constraints are observed. Where violations occur, the claim for systematic capability is partially or wholly invalid.

The transmitter can meet the requirements regarding the target failure measures within a safety instrument system up to:

SIL 3 @ HFT=1 (dual transmitter use)
and
SIL 2 @ HFT=0 (single transmitter use)

where SIL 3 @ HFT=1 demands two transmitters operated as HFT 1 safety redundancy (e.g., 1oo2, 2oo3).

When using redundant transmitter configurations, a common cause failure factor should be included in the safety calculation (e.g., by using IEC 61508-6:2010 Table D.1)

Safe Failure Fraction SFF

The used IEC 61508 **Route 1H** approach involves calculating the Safe Failure Fraction (SFF).

Related SFF values on the transmitter and related sensor applications as temperature sensor assembly are listed within the chapter **FMEDA Failure Data** on page 15.

Average Probability of Dangerous Failure on Demand PFD$_{AVG}$

The PFD$_{AVG}$ calculation must be done based on certain important variables including:
(1) Failure Rates and Failure Modes
(2) Redundancy Architecture incl. Common Cause Failures
(3) Proof-Test Coverage, Proof-Test Interval, Proof-Test Duration
(4) Mission Time
(5) Operational/Maintenance Capability
(6) Mean Time to Repair

As only (1) is under control of the device manufacturer, it is the responsibility of the SIS designer to perform the PFD$_{AVG}$ calculations for the final assembled SIS in order to determine suitability for the demanded Safety Integrity Level (SIL).

Accordingly, the PFD$_{AVG}$ and the Architectural constraints (in terms of HFT & SFF) must be verified for each application by the end user and the transmitter must be properly designed into the target safety instrumented function.

The chapter **Example PFDAVG Calculation** on page 19 contains related PFD$_{AVG}$ values for a single channel 1oo1 architecture on selected proof-test inspection intervals as a simplified example calculation.

7 Safety Operation Constraints

The following constraints need to be considered when using the transmitter for SIL safety applications:

- Only the current output 4 to 20 mA shall be used for safety applications
- The entire valid range of the output signal has been verified by the end user
- The HART communication channel shall comply with the security requirements of the final customer application
- The HART communication shall only be used for configuration, simulation and diagnostic purposes
- The transmitter write protection shall be activated during safety operation
- The safety parameters are configured as specified within this safety manual
- The correct parameterization in terms of the SIS safety function shall be checked be the end user
- The proof-test specified within this safety manual (or an equivalent test as specified for the final SIS safety function) shall be performed before activating the safety operation and in periodical cycles as demanded by the final PFD_{AVG} demands.
- The device is installed per manufacturer's instructions
- To ensure reliable functioning of the current output, the terminal voltage at the transmitter shall be within
- 11 to 42 V DC (non-explosion-proof design) and 11 to 30 V DC (explosion-proof design)
- The DCS power supply for the transmitter shall be capable to provide the required voltage level even when the current output is active with the configured high alarm
- The head-mount transmitter shall be protected against environmental influences by a suitable installation housing
- The safety-related system (safety logic solver) must be able to safe detect both, the high and the low alarm current state
- Materials are compatible with the final process conditions

- The robustness against EMC-disturbances has been tested to the requirements of NAMUR NE21:2017 which fulfills also the demands of IEC 61326-3-2:2017 Annex B, C, D
- Strong Surge EMC interference can lead to short-term deviations of up to 1 second in the output signal. If the final application environment offers such interference pulses, an DCS input filtering with a time constant of at least 1 second should be carried out.
- The ambient temperature range is restricted to −40 to 85 °C
- The environmental, measurement and application limits must be considered accordingly for the SIL safety application

The transmitter does not meet safety requirements under the following conditions:

- during installation, configuration, repair and simulation
- with deactivated write protection
- during an inspection or proof-test

Before commissioning the transmitter in a safety loop application, the end user must check whether the transmitter setup confirms to the system's safety function.

The end user must verify also that the correct transmitter has been installed at the correct measuring point.

Whenever the transmitter operating conditions are changed (for instance, if the mounting position is changed or the setup is modified), the safety function of the transmitter must be checked again.

Once the safety function has been checked, the transmitter must be write-protected to prevent inadvertent changes to the device setup.

8   Periodic Proof-Test and Maintenance

According to IEC 61508 and IEC 61611 proof-testing shall be performed to reveal dangerous faults which are undetected by automatic diagnostic tests.

The end user is responsible for selecting the type and the intervals according the overall safety system demands.

The inspections must be conducted in a manner that enables users to verify the proper function of the safety equipment in combination with all related components.

Proof-Test (transmitter)

The below described proof-test is a recommended variant which could be performed after installation, configuration changes and within the required periodical proof-test interval derived from the safety instrument system engineering demands (e.g. 1oo1, 1oo2 or 2oo3 architecture) and related PFD_{AVG} calculations.

- This proof-test is assumed to detect 95% of possible dangerous faults on the related temperature transmitter electronics.
- This proof-test does not include failures from the sensor assembly, e.g. failures from process connections, electrical sensor connections or thermowells which shall be subject of appropriate sensor proof-testing measures by the end user.

Step	Test Action (consecutive steps)
1	Bypass the safety DCS or take other appropriate action to avoid a false trip.
2	Restart, Power Down and Power Up the transmitter.
3	Deactivate the transmitter write protection (refer to the relevant operating instructions).
4	Force the transmitter to the high alarm current output in using the device driver (FDI/DTM/EDD) simulation functionality and verify that the analog current reaches that simulation value. (This verifies supply problems such as a low loop power supply voltage or increased wiring resistance, and also tests for other possible electrical part failures)
5	Force the transmitter to the low alarm current output in using the device driver (FDI/DTM/EDD) simulation functionality and verify that the analog current reaches that simulation value. (This verifies possible quiescent current related failures)
6	Activate the transmitter write protection.
7	Restore the loop to full operation by Restart, Power Down and Power Up the Device.
8	Check the activated write protection.
9	Check the measurement function in performing a multi-point measurement (e.g., 5-point calibration) covering the applicable temperature range. (this verifies possible sensor-configuration and electronics failures)
10	Apply an adequate input signal (e.g., short circuit, wire break) to reach the pre-defined alarm level and verify that the safe state is reached. (This verifies electronics failures from input to output stage). *
11	Remove the bypass from the safety DCS.

*   Suggested proof-test on the RTD wire compensation:

3-wire RTD channel 1: wire-break on terminal 2

3-wire RTD channel 2: wire-break on terminal 5

4-wire RTD: wire-break on terminal 4

Repair & Replacement

In case of detected failures, corrective actions may be demanded.
Possible safety critical failures shall be reported to the ABB Customer service center.
Defective transmitters send to ABB for repair or failure analysis should include information's about the failure effect, hardware & software versions, the safety application and environmental conditions.

9   Installation, Commissioning and Configuration

The transmitter shall be installed, configured, commissioned and maintained by personnel with trained knowledge of temperature transmitters in general, the specific knowledge on the related functional safety application and the specific knowledge of this safety manual and applicable documentation content referenced within chapter **Other relevant documents** on page 7 of this safety manual.

The transmitter has been configured and tested according to the customer order. However, the transmitter can be configured via local HMI and related Device drivers (FDI/DTM/EDD) through the HART interface.

Any configuration, installation or repair change may affect the safety function of the transmitter.

Therefore, the safety function shall be checked again after configuration, installation or repair change in using the described 'Proof-Test' and 'Safety Parameter Configuration'.

The constraints and limitations as provided within the operating instruction and data sheet as referenced within chapter **Other relevant documents** on page 7 must be considered by the end user, especially in terms of:
*   Intended use and improper use
*   Use in potentially explosive atmospheres
*   Design and function
*   Product identification
*   Transportation and storage
*   Installation and ambient conditions
*   Electrical connections
*   Commissioning and operation
*   Diagnosis, maintenance and repair

10 Safety Parameter Configuration

The transmitter can be configured in using the optional mounted local HMI (with limited functionality) or in using Device drivers (FDI/DTM/EDD) through the HART Interface.

For SIL safety applications these device drivers can be used:

Device driver package	Technology
FDI Package ABB TTX300 HART	FDI
FDI Package ABB TTX200 HART	FDI
DTM 700 Package ABB TTX300 HART	FDT
DTM 700 Package ABB TTX200 HART	FDT
EDD Package ABB TTX300 HART	EDD
EDD Package ABB TTX200 HART	EDD

The latest released version is available on:
https://new.abb.com/products/measurement-products
Temperature Measurement Products - Head-mount Temperature Transmitters
Temperature Measurement Products - Field-mount Temperature Transmitters

In addition to the Safety Operation Constraints as specified within chapter Safety Operation Constraints the following parameters must be configured as specified within the table to operate the transmitter within SIL safety applications.
All listed parameters are also checked by the SIL Check Function on their correct values (see description on the SIL Check Function within this chapter).

Parameter for transmitter

Single sensor application

FIM Parameter	Value	Function of the Value
Set/Reset Write Protection	Yes	Enables the write protection for local HMI and HART access. Note: For TTH300 & TTF300 the write protection can also be performed by an assigned "Key Value".
Current Output Low Alarm Value	3.5 to 3.6 mA	Alarm Value configured within the safety application range
Current Output High Alarm Value	21.0 to 23.6 mA	Alarm Value configured within the safety application range
Loop current mode	Enabled	Current Output follows the measurement variable
Output Simulation	Deactivated	Current Output is not forced to a fixed value by simulation
Current Output at Maintenance	Pulse Time = 0 s	Current Output is acting without special pulse signaling
Sensor 1 Configuration	Type: RTD or TC *	Sensor type is configured to either RTD or TC measurements
Alert Simulation	OFF	Diagnostic events are not forced by simulations
Measurement Mode	PV is sensor 1	Current output follows the measurement at the sensor 1 channel

Dual sensor application with sensor drift detection

FIM Parameter	Value	Function of the Value
Sensor 2 Configuration	Type: RTD or TC *	2nd sensor type is configured to either RTD or TC measurements
Drift Detection	Activated	Sensor Drift Detection is activated
Redundancy Configuration	Safety	On a detected sensor failure, the output is forced to alarm current, and the transmitter is not switched to the 2nd sensor without alarm current
Measurement Mode	PV is Redundancy sensor 1/sensor 2	In combination with the activated drift detection the current output follows the measurement at sensor 1 with redundancy drift detection in using the measurement at sensor 2
NAMUR Configuration Sensor-drift detected	Failure	A detected sensor drift above the configured drift value and inhibit time will force the output to alarm current
NAMUR Configuration Redundancy: Sensor 1 not available	Failure	On a detected sensor 1 failure the digital NAMUR diagnostic state results to Failure
NAMUR Configuration Redundancy: Sensor 2 not available	Failure	On a detected sensor 2 failure the digital NAMUR diagnostic state results to Failure

* If thermocouple is used as sensor application the correct configuration and function in terms of the cold junction compensation (Internal; External; Fixed) must be considered and checked by the end user.

Further, the impact of Damping and EMC Filtering as described within chapter **Safety function** on page 7 shall be considered.

... 10 Safety Parameter Configuration

Check activated write protection

The activated write protection shall be checked as follows:
- Check whether the lock icon is displayed on the display if mounted.
- Modify a parameter (e.g., Damping), save device data in device and check whether the message 'Device is write-protected' is displayed.

Note

The software write protection does not lock again automatically. It remains unlocked until it is specifically activated.

Note

For TTH300 & TTF300 the write protection can also be performed by an assigned "Key Value".

Sensor redundancy with drift detection

The dual sensor redundancy (two temperature sensors connected to one temperature transmitter) with configured drift detection detects around ~95% on the normally undetected sensor drift failures.
The related failure rates on sensor assembly configurations are listed within chapter **FMEDA Failure Data** on page 15.

Note

The sensor drift monitoring needs to be activated via Device drivers (FDI/DTM/EDD) and the configuration in terms of 'Drift value' and 'Drift Detection Time' must be configured and checked as demanded for the final sensor assembly. If the 'Drift Detection Time' is configured to values > 15 minutes the device self-diagnostic test interval needs to be increased accordingly within the safety loop design.

SIL Check Function

If the transmitter has been ordered as order variant 'SIL - Declaration of Conformity' the SIL Check Function is activated by ABB factory settings.

The SIL Check Function can be invoked via Device drivers (FDI/DTM/EDD) or the local HMI (if mounted) and verifies important transmitter settings as listed in chapter **Safety Parameter Configuration** on page 12 to support the end user in verifying the correct setup of parameters.

After performing the related parameter verifications, the transmitter results are provided by feedback messages as ´SIL Configuration Check not passed´ with related deviation details or as 'SIL Configuration Check passed'.

Note

In terms of detected deviations and a 'SIL Configuration Check not passed' state the transmitter will **not** lead to an 'Alarm Current State' and it is under the end user responsibility to check the deviation, accept the deviation or to undertake appropriate precautions.

11 Identification

Device

Type	Description	HW Version	SW Version
TTH300-**H	Head-mount temperature transmitter	02.00.02	03.01.00
TTH200-**H	Head-mount temperature transmitter	02.00.02	03.01.00
TTF300-**H	Field-mount temperature transmitter	02.00.02	03.01.00
TTF200-**H	Field-mount temperature transmitter	02.00.02	03.01.00

For safety applications, only these versions were considered.

Optional Display

HMI Type A, AS	Optional display for TTH300 identified by ID 9280291/218548
HMI Type B, BS	Optional display for TTF300 identified by AU3048B/AU3167

Attached Temperature Sensor Type (single or redundant)

2-, 3- and 4-wire RTD	refer to FMEDA Failure Data
Thermocouple	refer to FMEDA Failure Data

SIL marking

The order variant 'SIL - Declaration of Conformity' is marked with a SIL logo on the Name plate as specified within the Chapter ´Product Identification´ of the referenced operating instruction.

12 FMEDA Failure Data

This chapter provides the summary of the probabilistic estimation on failure data according to **FMEDA Report ABB 21/03-184 R024 V1 R1 May 2021 from Exida.com GmbH, Germany.**

The failure rates of electronic components used in the FMEDA analysis are the basic failure rates from the Siemens Standard SN 29500:2016 valid for operating stress conditions typical for industrial field environments similar to IEC 60653-1 class C (sheltered location) with an average temperature over a long period of time of 40°C (25°C ambient plus internal self-heating).

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 (daily fluctuation of > 15°C) must be assumed.

The failure rates of attached RTD or TC temperature sensors used in the FMEDA analysis are basic failure rates from the Exida Electrical Component Reliability Handbook 4th Edition, 2017 separated for the environmental conditions:

Closed coupled	Short connecting lead to the temperature sensor with less than 1 m (39.37 inches) in length and connecting leads laid with mechanical protection.
Extension wire	Long connecting lead to the temperature sensor with more than 1 m (39.37 inches) in length or connecting leads laid without mechanical protection.
Low stress	Low vibration environment or the use of a cushioned sensor. The operation is below 67% maximum rating according to specification.
High stress	High vibration environment. The operation is above 67% maximum rating according to specification

The failure rates do not include failures resulting from incorrect use, in particular humidity or chemicals entering through incompletely closed housings or inadequate process connections and cable feeding through inlets.

Further details are documented within the provided FMEDA report and shall be considered respectively.

... 12 FMEDA Failure Data

Transmitter - TTH300, TTH200, TTF300, TTF200

The FMEDA carried out on the worst-case configuration leads under the assumptions and constrains described in this manual to the following failure rate data for the transmitter without temperature sensors.

Failure category	Failure Rates (in FIT)
Fail Safe Detected (λSD)	**0**
Fail Safe Undetected (λSU)	**0**
Fail Dangerous Detected (λDD)	**527**
• Fail detected (detected by internal diagnostics)	382
• Fail high (detected by safety logic solver)	23
• Fail low (detected by safety logic solver)	87
• Annunciation detected (λAD)	35
Fail Dangerous Undetected (λDU)	**38**
Fail Dangerous Undetected (λDU) with Display	**39**
Annunciation Undetected (λAU)	17
No effect / No part	1495
Total failure rate (safety function)	**566**
SFF	93% *
DC	93% **
MTBF	202 years
SIL AC	**SIL 2**

*   Numbers are valid also when optional display is used.

** SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL.

The temperature transmitter electronics with temperature sensors become a temperature sensor assembly.

The following tables on failure rates of electronics and temperature sensors are based on data derived from the Exida Electrical Component Reliability Handbook 4th Edition, 2017. The numbers listed assumes that the temperature sensor assembly are considered to be an element according to IEC 61508:2010. However, it would also be possible to consider both parts as separate elements where each element must fulfill the related safety demands in terms of SFF by itself. (see also section 7.4.4.2.3 in IEC 61508-2)

Further details which should be considered are documented within the referenced FMEDA Report.

Transmitter with one sensor TT*200-**H or TT*300-**H

Low stress - Closed coupled condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Thermocouple	20	0 FIT	0 FIT	622 FIT	44 FIT	93%
4-wire RTD	28	0 FIT	0 FIT	574.5 FIT	41.5 FIT	93%
2/3-wire RTD	32	0 FIT	0 FIT	566.4 FIT	47.5 FIT	92%

Low stress - Extension wire condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Thermocouple	19	0 FIT	0 FIT	1427 FIT	139 FIT	91%
4-wire RTD	27	0 FIT	0 FIT	1022 FIT	44 FIT	95%
2/3-wire RTD	31	0 FIT	0 FIT	907 FIT	134 FIT	87%

High stress - Closed coupled condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Thermocouple	22	0 FIT	0 FIT	2427 FIT	139 FIT	94%
4-wire RTD	30	0 FIT	0 FIT	1477 FIT	89 FIT	94%
2/3-wire RTD	34	0 FIT	0 FIT	1314.2 FIT	211.8 FIT	86%

High stress - Extension wire condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Thermocouple	21	0 FIT	0 FIT	18527 FIT	2039 FIT	90%
4-wire RTD	29	0 FIT	0 FIT	10427 FIT	139 FIT	98%
2/3-wire RTD	33	0 FIT	0 FIT	8127 FIT	1939 FIT	80%

... 12 FMEDA Failure Data

Transmitter with two sensors TT*300-**H

Drift monitoring, Low stress - Closed coupled condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Two Thermocouples	36	0 FIT	0 FIT	727 FIT	40 FIT	94%
Two 2/3-wire RTDs	40	0 FIT	0 FIT	622 FIT	40 FIT	94%
Thermocouple & 2/3-wire RTD	44	0 FIT	0 FIT	674 FIT	44 FIT	93%

Drift monitoring, Low stress - Extension wire condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Two Thermocouples	35	0 FIT	0 FIT	2517 FIT	49 FIT	98%
Two 2/3-wire RTDs	39	0 FIT	0 FIT	1468 FIT	49 FIT	98%
Thermocouple & 2/3-wire RTD	43	0 FIT	0 FIT	1992 FIT	49 FIT	97%

Drift monitoring, High stress - Closed coupled condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Two Thermocouples	38	0 FIT	0 FIT	4517 FIT	49 FIT	98%
Two 2/3-wire RTDs	42	0 FIT	0 FIT	2430 FIT	56 FIT	97%
Thermocouple & 2/3-wire RTD	46	0 FIT	0 FIT	3473 FIT	147 FIT	96%

Drift monitoring, High stress - Extension wire condition

Sensor	FMEDA Table	λSD	λSU	λDD	λDU	SFF
Two Thermocouples	37	0 FIT	0 FIT	40327 FIT	239 FIT	99%
Two 2/3-wire RTDs	41	0 FIT	0 FIT	19337 FIT	229 FIT	98%
Thermocouple & 2/3-wire RTD	45	0 FIT	0 FIT	29832 FIT	234 FIT	99%

13 Example PFD_{AVG} Calculation

An Average Probability of Dangerous Failure on Demand (PFD$_{AVG}$) calculation is performed for a single (1oo1) Temperature Transmitter by Exida using Exida's exSILentia tool.

The worst-case failure rate data used in the calculation are given in chapter **FMEDA Failure Data** on page 15 Table "Electronics - TTH300, TTH200, TTF300, TTF200".

A Mission Time of 10 years has been assumed, a Mean Time to Restoration of 24 hours, a proof-test coverage of 95% (see **Periodic Proof-Test and Maintenance** on page 11) and a maintenance capability of 100%.

The resulting PFD$_{AVG}$ values for variety of proof-test intervals are displayed below.

T [Proof] = 1 year	T [Proof] = 2 years	T [Proof] = 5 years
PFD$_{AVG}$ = **2.60E-04**	PFD$_{AVG}$ = **4.22E-04**	PFD$_{AVG}$ = **9.09E-04**

For SIL 2 applications, the PFD$_{AVG}$ of the safety function needs to be < 1.00E-02.

This means that for a SIL 2 application, the PFD$_{AVG}$ for a 1-year Proof-Test Interval is approximately equal to 2.6% of the allowed range.

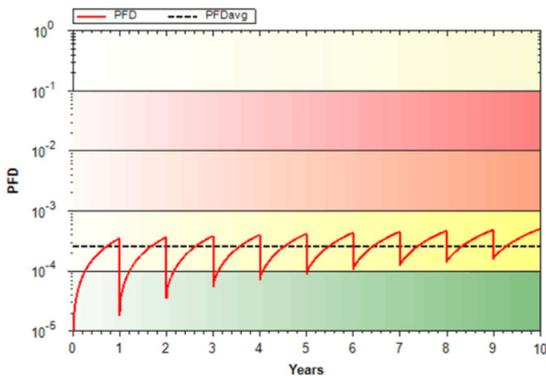The resulting PFD graph for a proof-test of 1 year is shown below:

Figure 1:   PFD graph

14 Cyber security disclaimer

This product is designed to be connected to and to communicate information and data via a network interface. It is operator's sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be).
Operator shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.
ABB and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

15 Release history

Safety Manual History

Rev A: Safety Manual for TTH200/300 and TTF200/300 Series Hardware Version 02.00.02 and Software Version 03.01.00

Device Version History

HW 02.00.02:   Initial version
SW 03.01.00:   Initial version

FMEDA History

2021:   Initial version, ABB 21/03-184 R024 V1 R1 May 2021

Assessment Report History

2022 - Assessment Report 1435.IM.143431/21TB 2022-03.31 Version 1.0