ABB MEASUREMENT & ANALYTICS | SIL-SAFETY MANUAL

TTH300, TTF300

Temperature transmitter

Additional instructions for IEC 61508 compliant devices

Measurement made easy

TTH300
TTF300

Introduction

TTH300, TTF300 sensor-head and field mounting for standard and high temperature measurement.

This document must be considered in conjunction with related operating instructions.

Additional information

Additional documentation on temperature transmitter is available for download free of charge at www.abb.com/temperature.
Alternatively simply scan this code:

TTH300

TTF300

Table of contents

1 Application area

The TTH300 and TTF300-*H Series temperature transmitter are 2-wire 4 to 20 mA devices for the temperature monitoring of solids, fluids and gases of all types in containers and piping.
Combined with a single or dual channel temperature sensor assembly, the temperature transmitters become a temperature sensor assembly.
The temperature sensors that can be connected to the temperature transmitters TT*300-*H for safety applications are:

- 2-, 3- and 4-wire RTD
- Thermocouple

The order variant 'SIL2 - Declaration of Conformity' meets the special SIL safety engineering requirements for the integration in Safety Instrumented Systems in compliance to **IEC 61508 Edition 2 part 1 to part 7**.

The area of safety application is limited to:

- Up to SIL 2 as single transmitter installation
- Up to SIL 3 as redundant transmitter installation
- Mode of safety operation: Low Demand Mode
- Hardware Fault Tolerance: HFT 0 (as single transmitter installation 1oo1)
- Architectural Constraints: SIL 2 (based on Type B, HFT 0 and SFF ≥ 90 %)
- Systematic Capability: SC 3 according IEC 61508

The safety data, constraints, assumptions, installation / maintenance instructions and operating limits defined in the related documents needs to be considered.
In case of questions and detected safety critical device failures please contact the **ABB Customer service center** (Keywords: Product Type Designator, SIL).

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

2 Purpose

According IEC 61508-2 Annex D 'Safety manual for compliant items' the purpose of this safety manual is to document the information which is required to enable the integration of this item into a safety-related system in compliance with the requirements of the IEC 61508 standard.

3 Terms and definitions

IEC 61508	International standard ‘Functional safety of electrical/electronic/programmable electronic safety-related systems’.
Safety integrity	Probability of a safety system satisfactorily performing the specified safety functions under all 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.
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 of an element when the element is applied in accordance with the instructions specified in the safety manual for the element.
Low demand mode	The safety function is only performed on demand with a demand interval a) no greater than one per year and b) greater than twice the proof test interval.
Dangerous failure	Failure in implementing the safety function that prevents a safety function from operating as expected.
Safe failure	Failure that results in the spurious operation of the safety function.
No effect failure	Failure without direct effect on the safety function.
FIT	Failure in Time (1x10-9 failures per hour) named λ Lambda
Failure rate	Conditional probability of failure per unit of time, usually declared as FIT λ_{DD} – detected dangerous failures λ_{DU} – detected dangerous failures λ_{SD} – detected safe failures λ_{SU} – intrinsic safe failures
PFD_{avg}	Average probability of dangerous failure on demand.
Safe failure fraction SFF	Ratio of safe plus dangerous detected failures to all failures. $SFF = (\lambda_{SD}+\lambda_{SU}+\lambda_{DD}) / (\lambda_{SD}+\lambda_{SU}+\lambda_{DD}+\lambda_{DU})$
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. $DC = \lambda_{DD} / (\lambda_{DU}+\lambda_{DD})$
Diagnostic test interval	Interval between on-line tests to detect faults.
Common cause failure	Failure causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure.
Systematic failure	Failure, related in a deterministic way to a certain cause, which can only be eliminated by design modification, manufacturing process, 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 significantly increases with time and the probabilistic failure rate estimation is meaningless.

Mission Time	Final plant operation time for the safety system. Used for the PFDAVG and Proof Test Interval calculation.
FMEDA	Failure Modes, Effects and Diagnostics Analysis.
MTBF	Mean Time Between Failure. MTBF = (1 / (λ total + λ AU + λ no effect + λ no part)) + MTTR.
MTTR	Mean Time to Repair.
MTTF	Mean Time to Failure.
DTM	Device Type Manager.
EDDL	Electronic Device Description Language.
FDI	Field Device Integration Technology based on EDDL.
DCS	Distributed Control System.
HMI	Human Machine Interface.
Multidrop	HART Bus Communication Mode.
Closed coupled	Short connecting lead to the temperature sensor with less than 1 m (39.37 in) in length and connecting lead laid with mechanical protection.
Extension wire	Long connecting lead to the temperature sensor with more than 1 m (39.37 in) in length or connecting lead 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.
NAMUR NE43	Standardization of the signal level for the breakdown information of digital 4 to 20 mA transmitter.
RTD	Resistance Temperature Detector.
TC	Thermocouple sensor.
SIS	Safety Instrumented System (e.g., sensors, logic solver, actuators).
LRV	Lower range value (measuring range lower limit).
URV	Upper range value (measuring range upper limit).
Sensor redundancy with drift detection	Assembly with two sensors and one electronics which allows to detect sensor drift failures.

4 Associated 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, TTF300	SM/TTX300SIL-EN	This Safety Manual
TTH300	DS/TTH300	Data Sheet
TTH300	OI/TTH300	Operating Instruction
TTH300	CI/TTH300	Commissioning Instruction
TTF300	DS/TTF300	Data Sheet
TTF300	OI/TTF300	Operating Instruction
TTF300	CI/TTF300	Commissioning Instruction

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.

5 Safety function

The TTH300-*H, and TTF300-*H transmitter are configurable single or dual sensor channel (RTD 2/3/4 wire, TC) digital devices generating a temperature related analog 4 to 20 mA output signal. The safety function refers strictly to the analog output signal.
The final device assembly consists of the device electronics TTH300-*H, or TTF300-*H, the attached temperature sensor, the housing with optional connected LCD indicator and the related process connections.

Alarm behavior and alarm current output

When a critical error is detected, an alarm current according 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.
(See Appendix FMEDA Report: Fail detected by internal diagnostics)

There are two selectable modes for the alarm current:

- HIGH ALARM (high alarm, maximum alarm current); this is the factory setting
- LOW ALARM (low alarm, minimum alarm current)

The high alarm current can be configured in a range from 20.0 to 23.6 mA.
The factory setting is 22 mA.
The low alarm current can be configured in a range from 3.5 to 4.0 mA.
The factory setting is 3.6 mA.

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 (e.g., by watchdog)
- Detected memory errors (e.g., non-volatile data, RAM, ROM)
  (See Appendix FMEDA Report: Fail low detected by safety logic solver)

Failures in some electrical parts are forcing independently of the configured alarm current the high alarm current range.
(See FMEDA Report: Fail high detected by safety logic solver)

The safety-related system (safety logic solver) must be able to detect both, the high and the low alarm state.
After switching on or restarting the transmitter electronics unit, the minimum alarm time is 10 to 15 seconds.

Overall safety accuracy

The value defined for the overall accuracy of the safety function for this device is ± 2 % of the measuring range.
The basic accuracy depends on the sensor model and is specified in the corresponding data sheets.

Diagnostic test interval

All safety-relevant errors are detected within a diagnostic test interval of 2 minutes.

Type classification

This device is declared as Type B complex element according IEC 61508.

Useful Lifetime

According IEC 61508-2, a useful lifetime, based on experience, should be assumed.
The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular.
Beyond the useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore, it is obvious that the PFDAVG calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.
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.

The useful lifetime by the worst components contributing to λ_{DU} (dangerous undetected failures) for the TTH300-*H, and TTF300-*H transmitter electronics at 40 °C average temperature conditions is assumed to approximately 500.000 hours.
When plant experience indicates a shorter useful lifetime, the number based on plant experience should be used.

Systematic Capability

This device has been qualified according the IEC 61508:2010 and fulfills the Part 1 - 3 requirements for a Systematic Safety Integrity of SC 3 (SIL 3 capable).
The overall functional safety management, development and change process has been assessed by TÜV Nord according IEC 61508:2000 with results reported within TÜV Report SLA-187/2009TTR-01.
The software modifications have been qualified according IEC 61508:2010.
The FMEDA has been performed by Exida Germany according IEC 61508:2010 with results reported within FMEDA Report 06/05-29 R012 Version V4. The summarized results are attached within Appendix ‘Exida FMEDA Report’.

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.

Safe Failure Fraction SFF

The IEC 61508 route 1H approach involves calculating the Safe Failure Fraction for the entire element. Related values are listed within ‘Appendix Exida FMEDA Report’.
The number listed assumes that the temperature sensing device and the transmitter together are 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 SFF.

Average probability of dangerous failure on demand PFD_{AVG}

For SIL2 applications, the PFD_{AVG} value of the overall SIS needs to be < 1.00E-02.
Assuming 35 % of these overall budget for the sensor assembly part leads to < 3.5E-03.
The SIS PFDAVG calculation must be done based on certain important variables including:
(1) Failure Rates, Failure Modes and Diagnostics
(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 by the device manufacturer it is the responsibility of the Safety Instrumented Function designer to perform the PFD_{AVG} calculations for the final assembled SIS in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for the demanded Safety Integrity Level (SIL).
The chapter ‘Example PFDAVG calculation’ contains related PFDAVG values for a single channel 1oo1 architecture on selected proof test inspection intervals as simplified calculation.

6 Constraints

The following constraints on the use of the compliant item needs to be considered:

- The entire valid range for the output signal must be configured between min. 3.8 mA and max. 20.5 mA (factory setting).
- The HART communication master must comply with the safety requirements of the customer application.
- No HART Multidrop Mode (forces current out to 4mA)
- The low alarm must be configured to a value ≤ 3.6 mA.
- The high alarm must be configured to a value ≥ 21 mA.
- To ensure reliable functioning of the current output, the terminal voltage at the device must be between
  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 must be capable to provide the required voltage level even when the current output is active with the configured high alarm.
- The head mounted electronics TTH300 with IP00 rating according IEC 60529 for the measurement loop must be protected against environmental influences by an suitable installation housing.

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

- During configuration and simulation
- With deactivated write protection
- During an inspection, proof test of the safety function

Before commissioning the device, check whether the device setup assures the system's safety function. Make also sure that the correct device has been installed at the correct measuring point.

Whenever the device is updated (if the device's mounting position is changed or the setup is modified, for example), the safety function of the device must be checked again.

Once the safety function has been checked, the device must be write-protected to prevent changes to the setup, since any change to the measurement system or parameters may impact the safety function.

7 Periodic proof test and maintenance

According IEC 61508-2 proof tests shall be undertaken 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

The below described proof test is a recommended variant which could be performed 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.

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 Device.
3	Deactivate the device write protection (refer to the relevant operating instructions).
4	Send a HART command, e. g., via EDD / DTM / FDI simulation functionality to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. (Test for voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible electrical part failures).
5	Send a HART command, e. g., via EDD/DTM/FDI simulation functionality to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. (Test for possible quiescent current related failures)
6	Activate the device write protection. (Refer to the relevant operating instructions) and wait at least 20 seconds for the non-volatile storage.
7	Restore the loop to full operation by Restart, Power Down and Power Up the Device.
8	Check the current output in performing a multi-point calibration (e. g., 5-point calibration) measurement of the temperature transmitter covering the applicable temperature range. (Test for possible sensor and electronics failures)
9	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. (Test for electronics failures that the analog current output corresponds to the provided input signal).
10	Remove the bypass from the safety DCS.

Table 1: 'Suggested steps for proof test'

The test is assumed to detect 95 % of possible dangerous faults on the related temperature transmitter and sensor assembly.

An appropriate simulator (Pt100 simulator, reference voltage sources) can also be used to check the transmitter electronics without sensor.

8 Installation, commissioning & configuration

The transmitter can be installed, configured, commissioned and maintained by personal with trained knowledge of temperature transmitters in general and the specific knowledge of the applicable documents content referenced within this safety manual.

The device has been configured and tested according to customer order. However, it can be configured via DTM / FDI / EDD through the HART interface. The parameters are described in the product instructions.
All configuration parameters that are changed may affect the safety function of the device. Therefore, the safety function shall be checked again after modifications in accordance to the recommended proof tests.

Activating / Deactivating write protection

- TTH300/TTF300 via DTM/FDI/EDD or local LCD display 'Write Protection'
- TTH300/TTF300 additionally via HW- write protection DIP switches
  (for details see the operating instruction).

Check write protection

Write protection could be checked as follows:

- Check whether the lock icon is displayed on the LCD 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.

Sensor redundancy with drift detection

The dual sensor redundancy with configured drift detection and alarm current output configuration (2 temperature sensors connected to one electronics) is able to detect and alarm signaling on around 95 % on the normally undetected sensor failures.
The related failure rates on sensor assembly configurations are listed within the related tables of 'Appendix Exida FMEDA Report'.

Configuration:
The sensor drift monitoring needs to be activated and configured via DTM or FDI as demanded for the sensor assembly.
The current output alarm behavior on the 'maintenance required' event from detected sensor drift failures needs to be configured as demanded for the safety logic solver.
Refer to the related operating instructions on more details.

Check sensor redundancy with drift detection

It is mandatory demanded to verify the sensor drift failure detection functionality for the final application including logic solver involvement.

9 Identification

Device

Type	Description	HW Version	SW version
TTH300-*H	Head-mount temperature transmitter	1.06 / 1.07	1.01.08 / 1.03.00
TTF300-*H	Field-mount temperature transmitter	1.06 / 1.07	1.01.08 / 1.03.00

For safety applications, only these versions were considered.

Optional Display

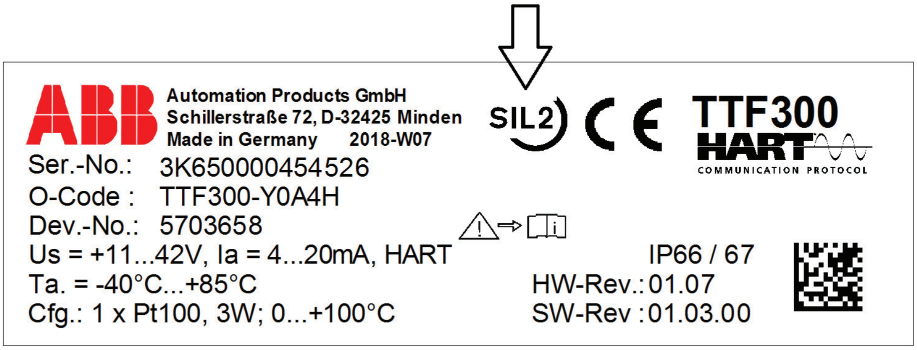
HMI Type A, AS	Optional LCD Indicator / display for TTH300
HMI Type B, BS	Optional LCD Indicator / display for TTF300

Attached Temperature Sensor Type (single or redundant)

2-, 3- and 4-wire RTD	Refer to attached Appendix Exida FMEDA Report
Thermocouple	Refer to attached Appendix Exida FMEDA Report

SIL marking

The order variant 'SIL2 - Declaration of Conformity' is marked as shown below.



Automation Products GmbH
Schillerstraße 72, D-32425 Minden
Made in Germany 2018-W07

Ser.-No.: 3K650000454526
O-Code : TTF300-Y0A4H
Dev.-No.: 5703658
Us = +11...42V, Ia = 4...20mA, HART IP66 / 67
Ta. = -40°C...+85°C HW-Rev.: 01.07
Cfg.: 1 x Pt100, 3W; 0...+100°C SW-Rev : 01.03.00

Figure 1: Name plate (example)

10 Example PFD_{AVG} Calculation

This example calculation demonstrates the PFD_{AVG} calculation performed for a temperature transmitter TT*300-*H according Table 2 of 'Appendix Exida FMEDA Report'.

Considering the following SIS application data:

- Architecture: 1oo1 (single channel, nonredundant, HFT 0)
- Proof Test Coverage: 95 %
- Mission Time: 10 years
- Mean Time to Restoration: 24 hours

The resulting PFD_{AVG} for a variety of proof test intervals is shown below:

PFD_{AVG}		
1 year Proof Test	2 years Proof Test	5 years Proof Test
PFD_{AVG} = 2.22E-04	PFD_{AVG} = 3.62E-04	PFD_{AVG} = 6.15E-04

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 2.2 % of the allowed range.

11 Failure modes, failure rates and diagnostics

Failure modes, the outputs and estimated failure rates of the compliant item (in terms of the behavior of its output) due to random hardware failures have been analyzed by ABB Automation Products GmbH and Exida GmbH in compliance to the IEC 61508 demands. See 'Appendix Exida FMEDA Report' on the related failure data.

Failure Rates

The failure rate data used by Exida in the attached FMEDA are the basic failure rates from the Siemens standard SN 29500. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

The listed SN 29500 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 (25 °C ambient temperature 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.

It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however, should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its 'useful life'.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from the proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data shall be adjusted to a higher value to account for the specific conditions of the plant.

Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during parameterization are not considered.
- The device is locked / protected against unintended operation/modification.
- The HART protocol is only used for setup and diagnostics purposes, not during normal operation.
- The device is installed per manufacturer's instructions.
- The correct parameterization is checked be the end user.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and / or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- External power supply failure rates are not included.
- As the optional display / control unit can interfere with the transmitter, the contribution to the dangerous undetected failure rate was considered.
- The worst case internal fault detection time is 2 minutes. Depending on the application, this interval needs to be considered directly in the SIL verification.
- Only the current output 4 to 20 mA is used for safety applications.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range low alarm and over-range high alarm and does not automatically trip on these states; therefore, these failures have been classified as dangerous detected failures.
- Materials are compatible with process conditions.
- The measurement / application limits are considered.
- Short circuit and lead breakage detection are activated.
- The minimum supply voltage used for the failure rate calculation is 15 VDC.

Diagnostics

The device's diagnostics setup meets the declared safety requirements in supporting the following runtime error detections:

- Sensor configuration RTD: wire break and short circuit
- Sensor configuration thermocouple: wire break
- Several electrical part failures
- AD-converter error
- Internal Power Supply error
- Internal communication error
- Program and Microcontroller supervision through watchdog
- Sensor limit range alarm (upper and lower limits)
- Flash ROM CRC16 error
- EEPROM CRC16 error
- RAM Physical – Pattern Test error
- RAM CRC16 data error
- Drift error detection if configured and verified for the final dual redundant sensor assembly

12 Notes on Cyber security

This product is designed to be connected to and to communicate information and data via a HART network interface. It is operator's sole responsibility to provide and continuously ensure a secure connection between the product and the plants 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 Automation Products GmbH 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.

13 Release history

Safety Manual History

Rev D: Added influence of optional display, safety manual separated for TTX200 and TTX300 series, safety manual renewed to IEC 61508:2010 demands – 2018.
Rev C: Safety manual for TTX200 and TTX300 series.

Device Version History

HW V1.07: 2016 – minor HW modification in two capacitor values for increased ex cable length.
HW V1.06: Initial released HW version.
SW 1.03.00: 2015 – HART 7 communication protocol added, DIP Switch Function for HART 5 as with pre-version 1.01.08.
SW 1.01.08: Improvement on wire break errors within environments with very high 50 Hz influence, bugfix operating hours counter.
SW 1.01.07: Initial version.

FMEDA History

V4R2: Added influence of optional display; May 29, 2018.
V4R1: Second HW and SW version added; January 20, 2016.
V4R0: Updated to IEC 61508:2010; January 20, 2016.
V3R0: TT*200 and TSP with TT+200 removed; November 6. 2012.
V2R0: Product named changed, software and hardware version updated; November 13, 2009.
V1R0: Internal review comments incorporated, software version updated; April 2, 2007.
V0R2: External Review comments incorporated; March 19, 2007.
V0R1: Initial version; January 11, 2007.

14 Appendix

Exida FMEDA Report

Failure Modes, Effects and Diagnostic Analysis

Project:
Temperature Transmitters TT*300-*H
with 4..20 mA output

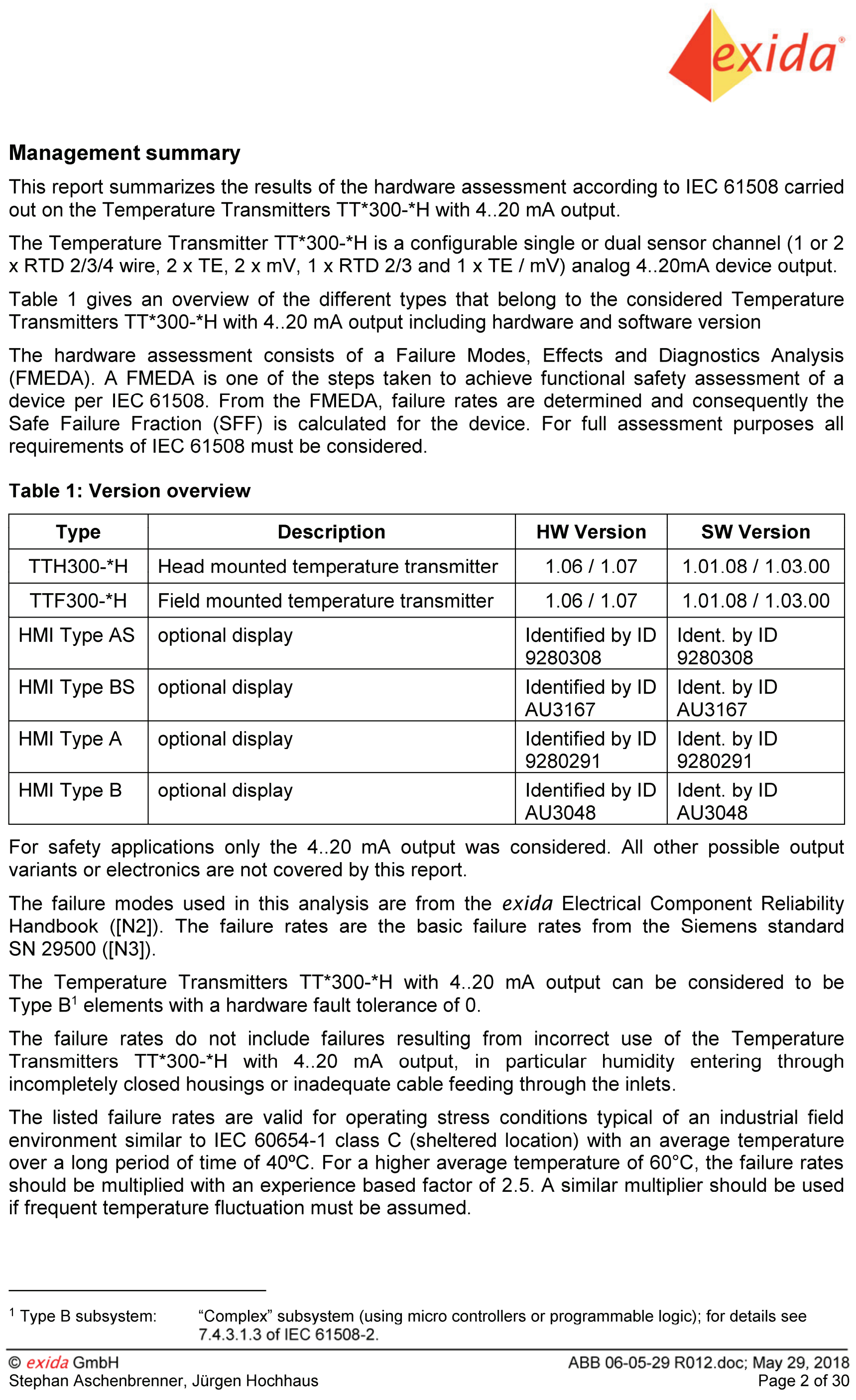
Customer:
ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 06/05-29
Report No.: ABB 06/05-29 R012
Version V4, Revision R2; May 2018
Stephan Aschenbrenner, Jürgen Hochhaus

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.

… 14 Appendix

… Exida FMEDA Report



Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the Temperature Transmitters TT*300-*H with 4..20 mA output.

The Temperature Transmitter TT*300-*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 TT*300-*H with 4..20 mA output 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
TTH300-*H	Head mounted temperature transmitter	1.06 / 1.07	1.01.08 / 1.03.00
TTF300-*H	Field mounted temperature transmitter	1.06 / 1.07	1.01.08 / 1.03.00
HMI Type AS	optional display	Identified by ID 9280308	Ident. by ID 9280308
HMI Type BS	optional display	Identified by ID AU3167	Ident. by ID AU3167
HMI Type A	optional display	Identified by ID 9280291	Ident. by ID 9280291
HMI Type B	optional display	Identified by ID AU3048	Ident. by ID AU3048

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

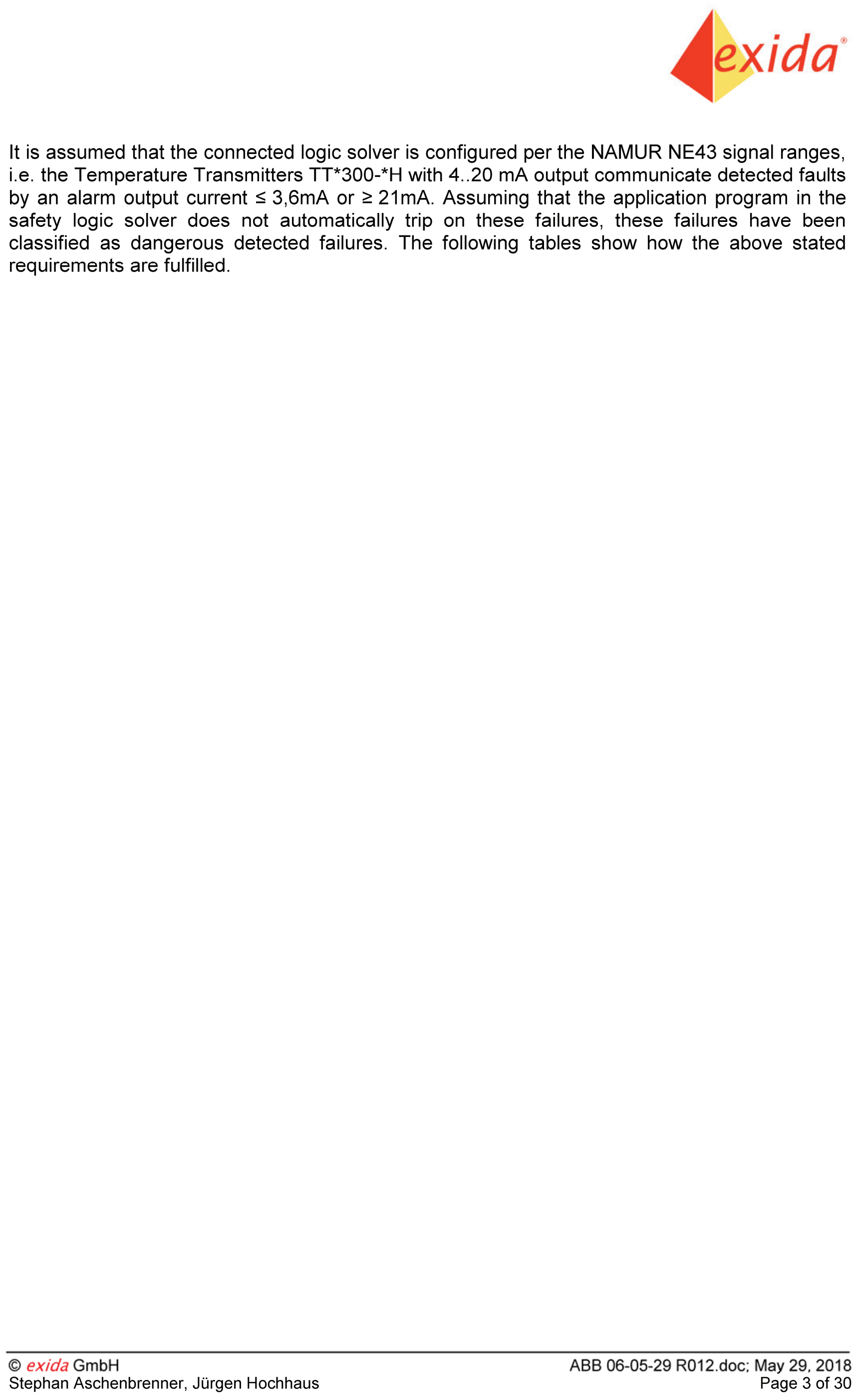
The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook ([N2]). The failure rates are the basic failure rates from the Siemens standard SN 29500 ([N3]).

The Temperature Transmitters TT*300-*H with 4..20 mA output can be considered to be Type B[1] elements with a hardware fault tolerance of 0.

The failure rates do not include failures resulting from incorrect use of the Temperature Transmitters TT*300-*H with 4..20 mA output, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

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



It is assumed that the connected logic solver is configured per the NAMUR NE43 signal ranges, i.e. the Temperature Transmitters TT*300-*H with 4..20 mA output communicate detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver 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.

© *exida* GmbH
Stephan Aschenbrenner, Jürgen Hochhaus

ABB 06-05-29 R012.doc; May 29, 2018
Page 3 of 30

… 14 Appendix

… Exida FMEDA Report

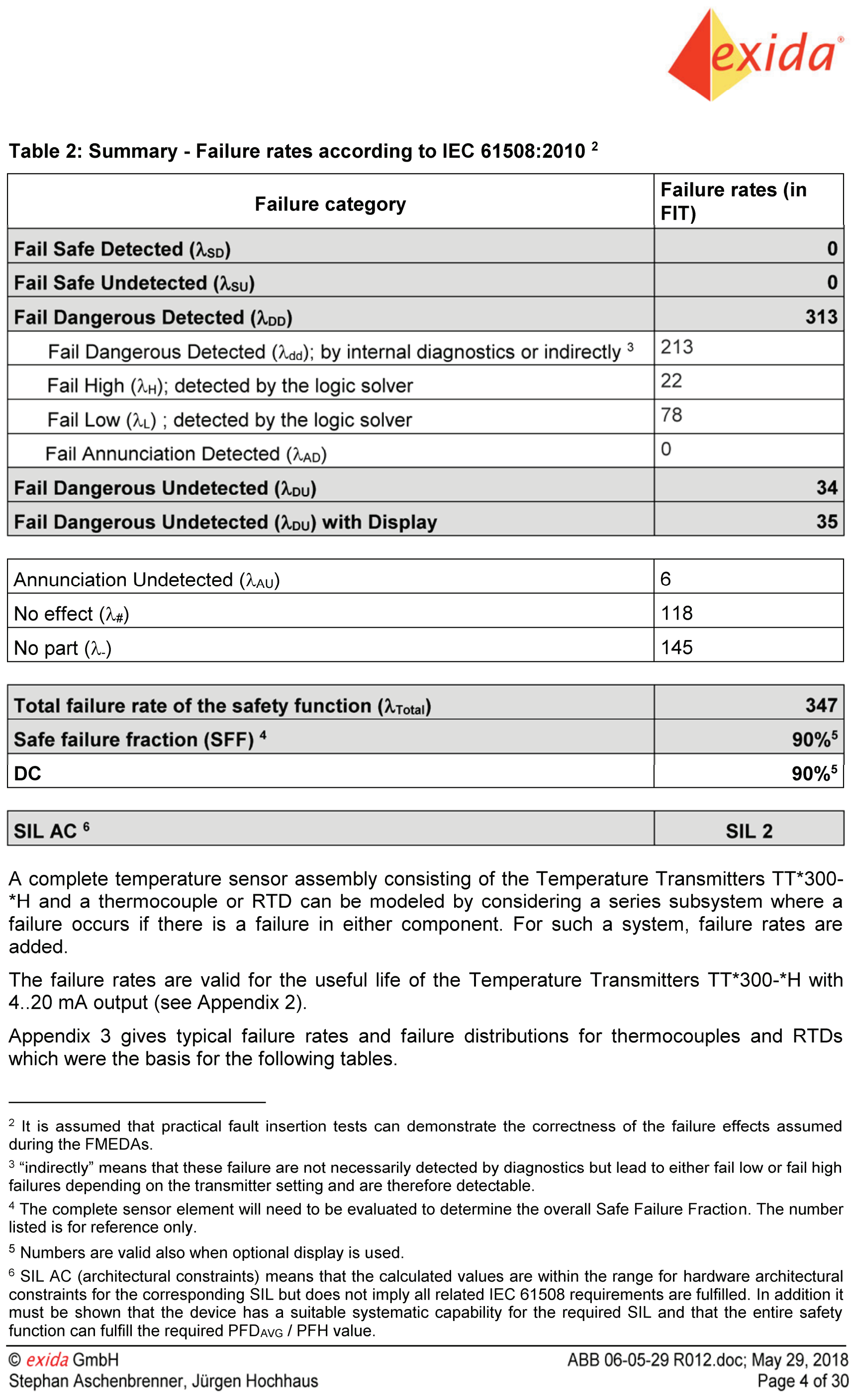


Table 2: Summary - Failure rates according to IEC 61508:2010 [2]

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**313**
Fail Dangerous Detected (λ_{dd}); by internal diagnostics or indirectly [3]	213
Fail High (λ_{H}); detected by the logic solver	22
Fail Low (λ_{L}) ; detected by the logic solver	78
Fail Annunciation Detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**34**
Fail Dangerous Undetected (λ_{DU}) with Display	**35**

Annunciation Undetected (λ_{AU})	6
No effect ($\lambda_{\#}$)	118
No part (λ_{-})	145

Total failure rate of the safety function (λ_{Total})	**347**
Safe failure fraction (SFF) [4]	**90%[5]**
DC	**90%[5]**

SIL AC [6]	**SIL 2**

A complete temperature sensor assembly consisting of the Temperature Transmitters TT*300-*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.

The failure rates are valid for the useful life of the Temperature Transmitters TT*300-*H with 4..20 mA output (see Appendix 2).

Appendix 3 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

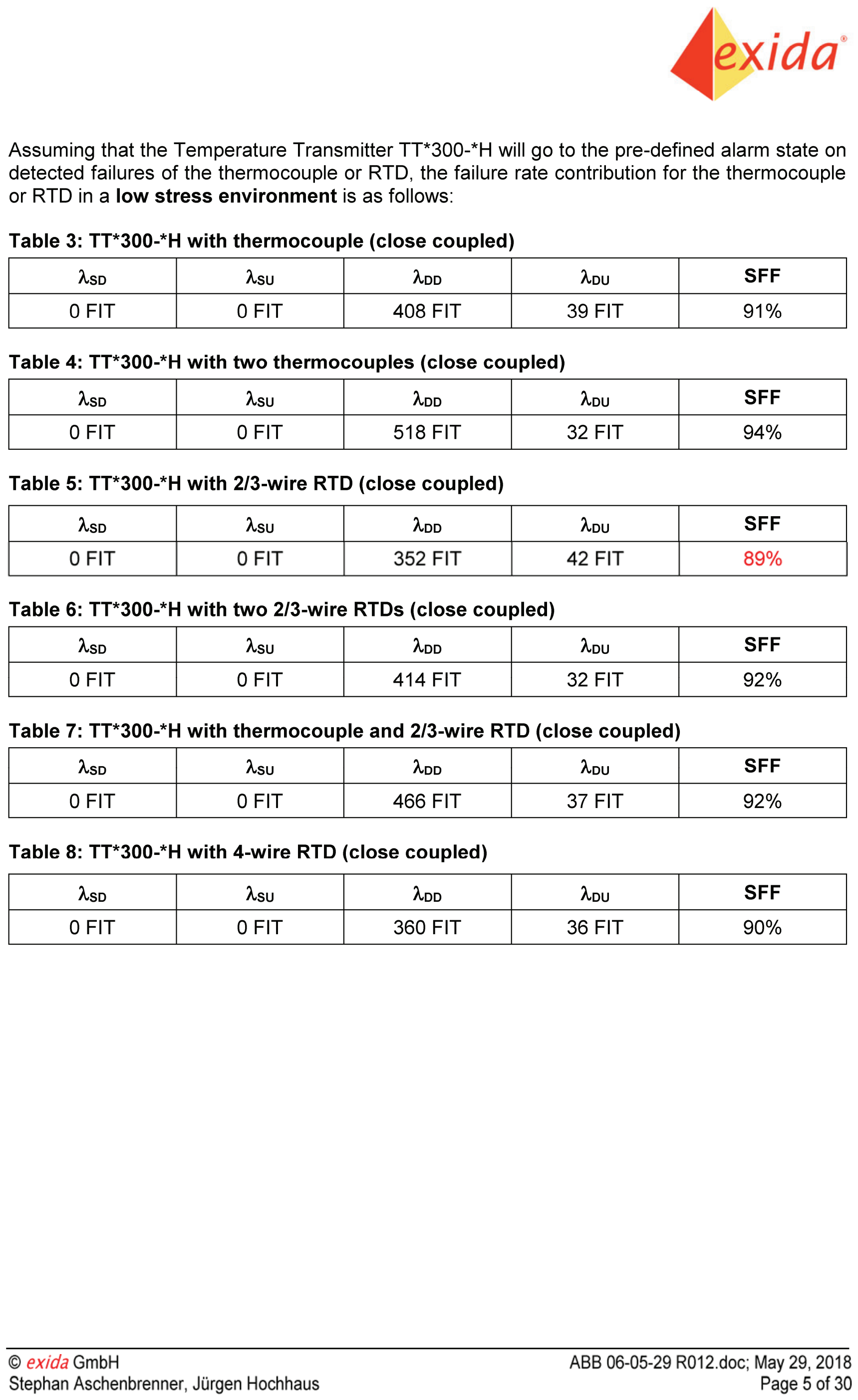
[2] It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

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

[4] The complete sensor element will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[5] Numbers are valid also when optional display is used.

[6] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD_{AVG} / PFH value.



Assuming that the Temperature Transmitter TT*300-*H will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution for the thermocouple or RTD in a **low stress environment** is as follows:

Table 3: TT*300-*H with thermocouple (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	408 FIT	39 FIT	91%

Table 4: TT*300-*H with two thermocouples (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	518 FIT	32 FIT	94%

Table 5: TT*300-*H with 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	352 FIT	42 FIT	89%

Table 6: TT*300-*H with two 2/3-wire RTDs (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	414 FIT	32 FIT	92%

Table 7: TT*300-*H with thermocouple and 2/3-wire RTD (close coupled)

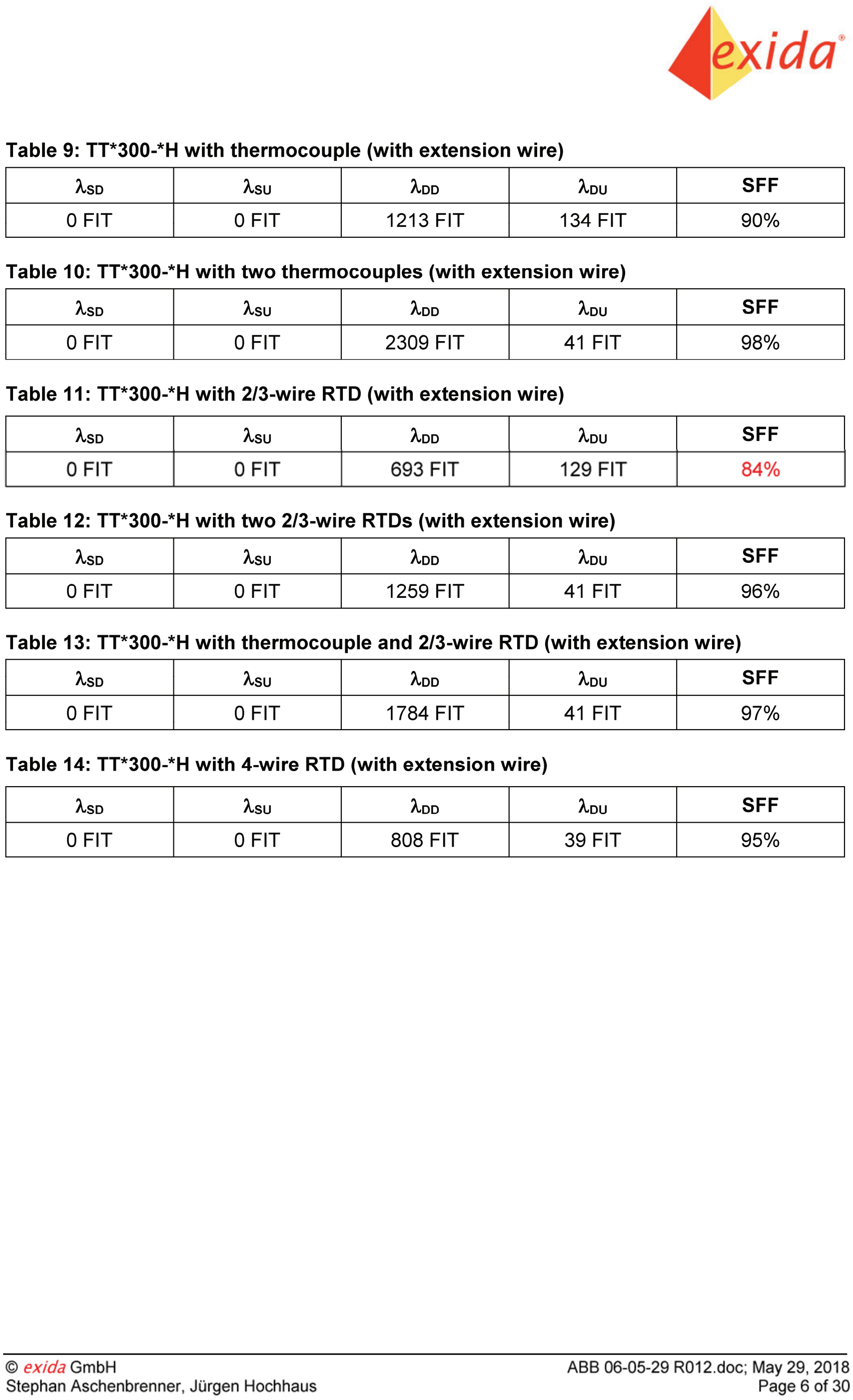
λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	466 FIT	37 FIT	92%

Table 8: TT*300-*H with 4-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	360 FIT	36 FIT	90%

… 14 Appendix

… Exida FMEDA Report



exida

Table 9: TT*300-*H with thermocouple (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	1213 FIT	134 FIT	90%

Table 10: TT*300-*H with two thermocouples (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	2309 FIT	41 FIT	98%

Table 11: TT*300-*H with 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	693 FIT	129 FIT	84%

Table 12: TT*300-*H with two 2/3-wire RTDs (with extension wire)

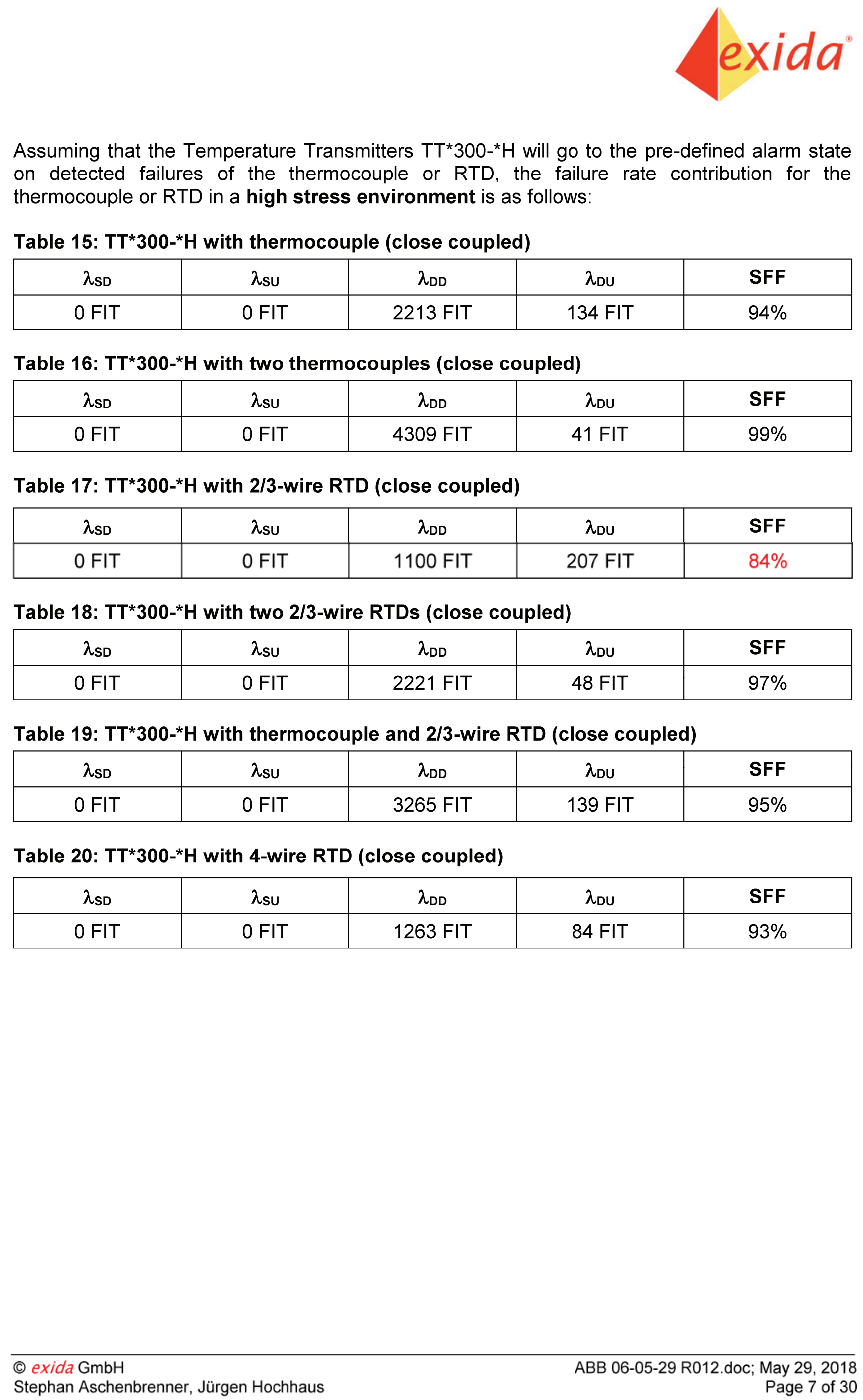
λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	1259 FIT	41 FIT	96%

Table 13: TT*300-*H with thermocouple and 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	1784 FIT	41 FIT	97%

Table 14: TT*300-*H with 4-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	808 FIT	39 FIT	95%



Assuming that the Temperature Transmitters TT*300-*H will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution for the thermocouple or RTD in a **high stress environment** is as follows:

Table 15: TT*300-*H with thermocouple (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	2213 FIT	134 FIT	94%

Table 16: TT*300-*H with two thermocouples (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	4309 FIT	41 FIT	99%

Table 17: TT*300-*H with 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	1100 FIT	207 FIT	84%

Table 18: TT*300-*H with two 2/3-wire RTDs (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	2221 FIT	48 FIT	97%

Table 19: TT*300-*H with thermocouple and 2/3-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	3265 FIT	139 FIT	95%

Table 20: TT*300-*H with 4-wire RTD (close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	1263 FIT	84 FIT	93%

… 14 Appendix

… Exida FMEDA Report

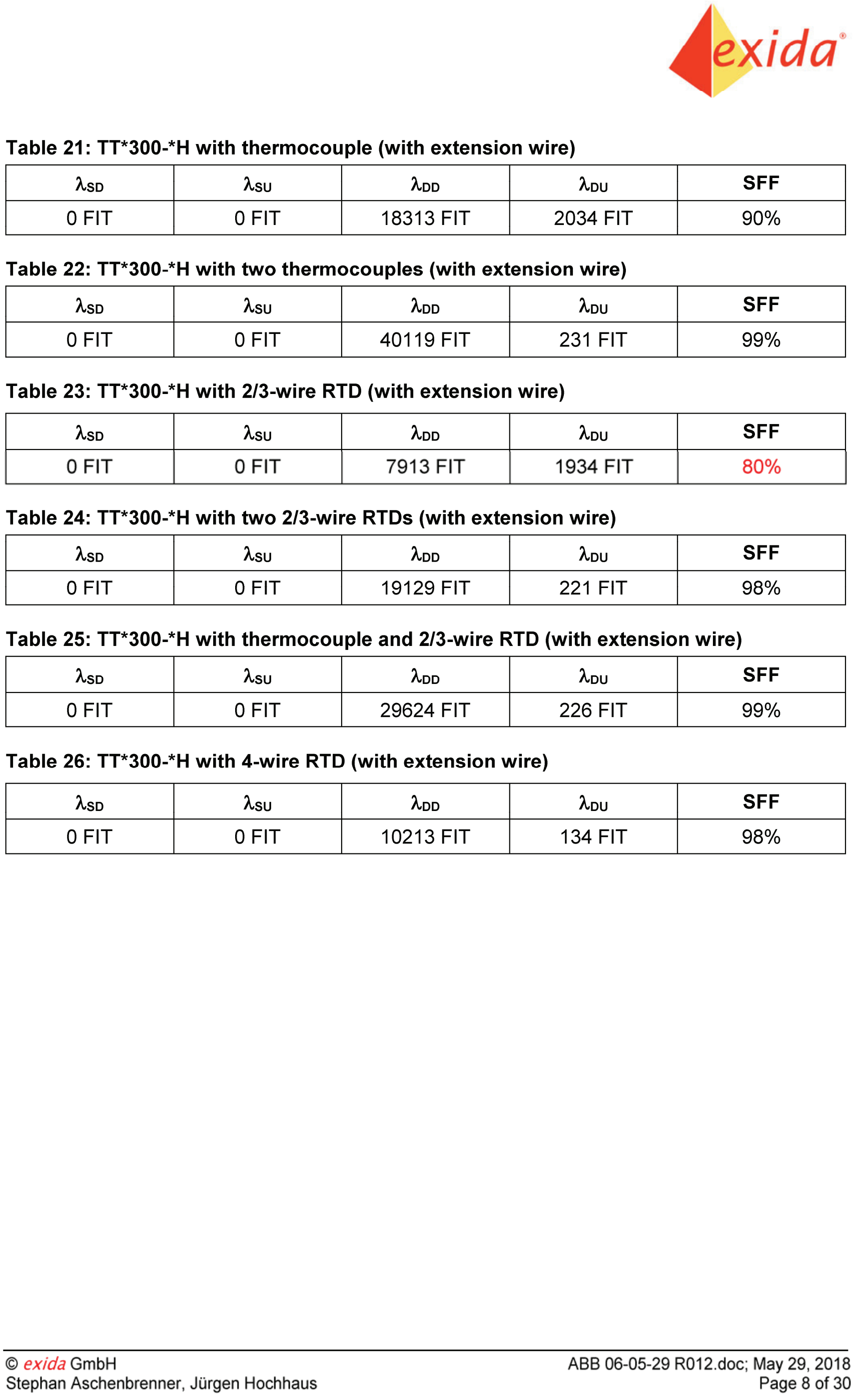


Table 21: TT*300-*H with thermocouple (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	18313 FIT	2034 FIT	90%

Table 22: TT*300-*H with two thermocouples (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	40119 FIT	231 FIT	99%

Table 23: TT*300-*H with 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	7913 FIT	1934 FIT	80%

Table 24: TT*300-*H with two 2/3-wire RTDs (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	19129 FIT	221 FIT	98%

Table 25: TT*300-*H with thermocouple and 2/3-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	29624 FIT	226 FIT	99%

Table 26: TT*300-*H with 4-wire RTD (with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF**
0 FIT	0 FIT	10213 FIT	134 FIT	98%

© *exida* GmbH
Stephan Aschenbrenner, Jürgen Hochhaus

ABB 06-05-29 R012.doc; May 29, 2018
Page 8 of 30

Notes

ABB Limited
Measurement & Analytics
Howard Road, St. Neots
Cambridgeshire, PE19 8EU
UK
Tel: +44 (0)870 600 6122
Fax: +44 (0)1480 213 339
Email: enquiries.mp.uk@gb.abb.com

ABB Automation Products GmbH
Measurement & Analytics
Schillerstr. 72
32425 Minden
Germany
Tel: +49 571 830-0
Fax: +49 571 830-1806

ABB Inc.
Measurement & Analytics
125 E. County Line Road
Warminster, PA 18974
USA
Tel: +1 215 674 6000
Fax: +1 215 674 7183

abb.com/temperature

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB.