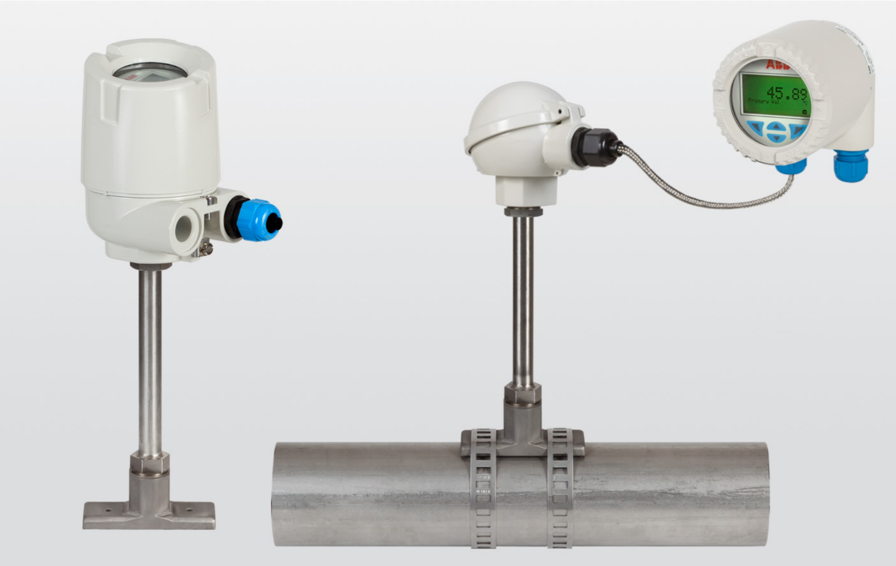
ABB MEASUREMENT & ANALYTICS SIL-SAFETY MANUAL | SM/TSP341-N/HW02/SIL_IEC_61508-EN REV. A

NINVA™ TSP341-N, TTF300-N

Sensor for non-invasive temperature measurement



Additional instructions for IEC 61508 compliant devices from HW-Rev. 02.00 and from SW-Rev. 13.02

Measurement made easy

—
TSP341-N with integrated head-mount transmitter TTH300-N (left).

TSP341-N Remote sensor apparatus (right)

Introduction

SIL Safety Manual for non-invasive temperature measurement devices.
This document must be considered in conjunction with the related operating instructions.

Additional information

Additional documentation on NINVA™ TSP341-N, TTF300-N is available for download free of charge at www.abb.com/temperature.

Alternatively simply scan this code:

TSP341-N

TTF300-N

Table of contents

1 Application area

The product scope of this SIL safety manual is assigned to the product variants:

- **NINVA™ TSP341-N with integrated head-mount transmitter TTH300-N:**
  further named 'TSP341-N Integrated' and 'the device …' within this manual
- **NINVA™ TSP341-N Remote sensor apparatus with connected field-mount transmitter TTF300-N:**
  further named 'TSP341-N Remote' and 'the device …' within this manual

The 'TSP341-N Integrated' and 'TSP341-N Remote' are isolated two-wire 4 to 20 mA temperature measurement devices.

The 'N' is used to indicate the non-invasive temperature measurement principle.

Classic temperature measurement in the process industry is made by directly introducing the temperature sensor into the measuring medium. The measuring medium (gaseous, liquid or paste-like) is usually in a vessel or piping and highly influences the selection of traditional invasive measurements. Depending on the process properties, the temperature sensor needs special protection to protect it from chemical and mechanical loads. For example, abrasive dust or sands which move through the piping at high speeds, present a special challenge.

To protect the temperature sensor, the thermowells used must be inspected regularly and replaced as needed. Chemically aggressive or abrasive media can lead to the erosion of thermowell material. A thermowell placed in flowing media can also begin to vibrate due to vortex formation and in extreme cases it can break. Therefore, guidelines and standards for the stability of thermowells have become more restrictive over time, and so the costs of maintenance and exchange have increased as well. In addition, to prevent potential catastrophic failure, thermowells used must be inspected regularly and replaced as needed in known critical conditions.

These life cycle costs are in addition to capital expenditure costs incurred during planning and designing temperature measurement points. Engineering costs for stability calculations, structural flanges to support and seal the thermowells, and welding and fabrications costs all add up to the total capital expenditure.

The weaknesses mentioned above can be eliminated if the process temperature could be measured non-invasively.

In using ABB's non-invasive approach, it is possible to get an accurate measurement of the process temperature without the need for a thermowell.

The TSP341-N (NINVA™) combines non-invasive temperature measurement with the established HART® communications protocol in two-wire technology. Therefore, the device can be integrated seamlessly into the vast majority of existing and future process facilities.

The non-invasive temperature measurement can turn a metal pipe carrying a process media into a temperature sensor.

Using model-based algorithms in the transmitter electronics to compensate for ambient and surface contact conditions, a NINVA™-Temperature sensor delivers an accurate measurement of the surface temperature of the pipe.

When coupled with process conditions, the device provides a non-invasive approach to measure the process temperature without the need for a thermowell for the vast majority of process conditions.

Note
The difference between the surface temperature and the process temperature under any given process condition can be calculated by the end user using standard heat transfer models for fluids flowing in pipes. To estimate the related measurement performance ABB supports the end users by a related ´NINVA™ Performance predictor´ - tool which is available online at:

NINVA performance predictor

In case of questions and detected safety critical device failures please contact the ABB Customer Service Center or the Product Responsible Unit 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 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
TSP341-N	DS/TSP-341-N	Data Sheet
TTF300-N	DS/TTF300	Data Sheet
TSP341-N	OI/TSP341-N	Operating Instruction
TTF300-N	OI/TTF300	Operating Instruction
TTH300-N/TTF300-N	COM/TTx300-N/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.

4 Standards and literature

Standards

Ref	Standard	Revision
RS1	**IEC 61508**'Requirements for electrical/electronic/programmable electronic safety-related systems'	Edition 2.0
RS2	**IEC 61511** 'Functional safety – Safety instrumented systems for the process industry sector'	Edition 2.0
RS3	**Siemens SN 29500** 'Failure Rates of components'	2016-11
RS4	**NAMUR NE 43** 'Standardization of the Signal Level for the Failure Information of Digital Transmitters'	2021-07-26
RS5	**NAMUR NE 130** 'Selection of field devices for safety instrumented systems with due regard to prior use' used Supplement 1 (NE 130: Form B.1)	2023-07-14
RS6	**NAMUR NE 24** 'Requirements on measuring inserts for temperature sensors'	2016-10-07

Literature

Ref	Literature	Revision
RL1	Exida White Paper 'Mechanical Failure Rate Data for Low Demand Applications'	Rev 4
RL2	Exida Webinar 'Using a Spreadsheet to do FMEDA'	04/2023
RL3	Exida 'EMCRH 02 Mechanical (Mechanical Failure Data)'	Third Edition
RL4	Exida 'EMCRH 01 Electrical (Electrical Failure Data)'	Third Edition
RL5	Exida White Paper 'The Key Variables Needed for PFDavg Calculation'	1.2 / 2016
RL6	NAMUR NA 106 'Flexible proof testing of field devices in safety instrumented systems'	2018-09-06

5 Reference documents

The following documents are referenced for the functional safety approval justification.

Ref	Reference document	Revision
RF1	Exida FMEDA Report Temperature Transmitters TT*200-**H and TT*300-**H with 4 to 20 mA output ABB 21/03-184 R024	V1 R1 2021
RF2	IIM-FM-02-2024-TT TTx NINVA Ed2 FMEDA Report Rev 1.1	1.1 2024
RF3	Assessment Report TÜV Nord 1435.IM.154935_23_TB_V1_0_EN_ABB_TempTrans_TSP341_TTx300	07/2024

6 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 (IEC 61508)	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 function (IEC 61511)	Function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to 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 (1x10-9 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 λ_{DU} – undetected dangerous failures
	λ_{SD} – detected safe failures 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. $DC = \lambda_{DD} / (\lambda_{DU}+\lambda_{DD})$
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.

… 6 Terms and definitions

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 $\mathrm{PFD}_{\mathrm{AVG}}$ and Proof-Test Interval calculation.
FMEDA	Failure Modes, Effects and Diagnostics Analysis
MTBF	Mean Time Between Failure $\mathrm{MTBF} = (1 / (\lambda_{\mathrm{total}} + \lambda_{\mathrm{AU}} + \lambda_{\mathrm{no\ effect}} + \lambda_{\mathrm{no\ part}})) + \mathrm{MTTR}$
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
NAMUR NE43	Standardization of the signal level for the breakdown information of digital 4..20 mA transmitters
RTD	Resistance 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
Safety Assessment	Investigation based on evidence on the achieved safety integrity
Dual channel	A dual channel configuration is one with two channels that independently perform the same function. Channels may be identical or diverse.
NINVA™	ABB trademark used for non-invasive measurement products.
Temperature sensor apparatus	Measurement unit including contact and reference sensor except transmitter electronics.
Transmitter	Electronics to convert the sensor signal into the output signal
Sensor	Term used for: • basic temperature sensor element in terms of RTD • complete NINVA™ temperature measurement device
Measuring Inset	Exchangeable sensor assembly containing the contact and reference sensor.
Contact sensor	Sensor element with 3 wire sensor used for the contact temperature measurement on the process surface.
Reference sensor	Sensor element with 3 wire sensor used for the non-invasive reference measurement
'SIL Check'	Device function which can be executed via local HMI or device drivers capable to detect certain invalid configuration settings for SIL safety operations.
ADC	Analog to Digital Converter
MCU	Microcontroller Unit
Rise time	The interval of time between the instants at which the instantaneous value of a pulse first reaches a specified lower value and then a specified upper value. Unless otherwise specified, the lower and upper values are fixed at 10 % and 90 % of the pulse magnitude. (IEC 60770)

7 Product identification

Type	Description	HW Version	SW Version
TSP341-N with TTH300-N	NINVA™ TSP341-N temperature sensor with integrated head-mount electronics TTH300-N	02.00.02	13.02.00
TSP341-N with TTF300-N	NINVA™ TSP341-N remote sensor apparatus with wire connected field-mount electronics TTF300-N	02.00.02	13.02.00

Optional Display

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

For safety applications, only these versions were considered.

Both variants only with the related products order codes:

‘H’ coding for the order option HART/4 to 20 mA
‘CS’ coding for the order option SIL

SIL marking

The order variant **‘CS – SIL - Declaration of Conformity’** is marked with a SIL logo on the name plate.

8 SIL Safety Data Summary

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

General	
Product Responsible Unit	ABB AG, Division Process Automation Schillerstraße 72 32425 Minden, Germany

General		
Device designation and permissible designs	• TSP341-N with integrated transmitter TTH300-N • TSP341-N remote sensor apparatus with connected transmitter TTF300-N Related device order codes: **'H'** for Communication Protocol HART / 4 to 20 mA **'CS'** for SIL compliance	
Safety-related output signal	4 to 20 mA	
Fault current	Current Low Alarm Value: ≤ 3.6 mA Current High Alarm Value: ≥ 21.0 mA	
Measurement / function assessed / safety function(s)	Non-invasive surface temperature to 4 to 20 mA output signal	
Device type acc. to IEC 61508-2	☐ Type A (sensor)	☒ Type B (Electronics)
Operating Mode	☒ Low Demand Mode	☐ High Demand/Continuous Mode
Valid Hardware-Version	02.00.xx	
Valid Software-Version	13.02.xx	
Type of assessment (single choice only)	☒ Complete HW/SW assessment incl. FMEDA and modification process as part of development according to IEC 61508-2,3	
	☐ Assessment based on prior-use proof incl. FMEDA and modification process as part of development according to IEC 61508-2,3	
	☐ Analysis of HW/SW field data to prove prior use according to IEC 61511	
	☐ Assessment by means of FMEDA according to IEC 61508-2	
Assessment by (incl. report no + FMEDA data source)	TÜV NORD Systems GmbH & Co KG, Germany, Augsburg	
Assessment documentation	Assessment Report TÜV Nord 1435.IM.154935_23_TB_V1_0_EN_ABB_TempTrans_TSP341_TTx300	

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

FMEDA (Failure modes effects and diagnostics analysis)	
Safety function	Non-invasive surface temperature to 4 to 20 mA output signal
λDU	88
λDD	608
λSU	0
λSD	0
SFF – Safe Failure Fraction	62% on Type A Sensor 93% on Type B Electronics
Safety Deviation [1]	± 2 % (+- 0.32 mA) on the 4 to 20 mA output signal
Fault Detection Time	15 Minutes (worst case detection & reaction time)
PTC	94 % (see chapter **Periodic proof-test and maintenance** on page 17)

9 SIL safety function

NINVA™ measurement function

As stated within the chapter 'application area', two variants of the non-invasive temperature measurement devices are within this SIL functional safety scope:

- 'TSP341-N with integrated head-mount transmitter TTH300-N'
- 'TSP341-N remote sensor apparatus with connected field mount transmitter TTF300-N'

The safety function of these devices is to provide a reliable and accurate measurement of the surface temperature of the pipe or vessel it is attached to. This temperature is termed the non-invasive temperature which is provided as 4 to 20 mA output signal according NAMUR NE 43.

On detected failures an alarm current according NAMUR NE 43 is provided.

The non-invasive temperature can be correlated with the process temperature by the end user when the process conditions (flow, density, viscosity and pipe conditions) under which the sensor is being used are known.

This correlation with the process temperature is therefore under the responsibility of the end user and cannot be specified by ABB as device manufacturer.

Note
The difference between the surface temperature and the process temperature under any given process condition can be calculated by the end user using standard heat transfer models for fluids flowing in pipes. To estimate the related measurement performance ABB supports the end users by a related 'NINVA™ Performance predictor´ - tool which is available online at:

NINVA performance predictor

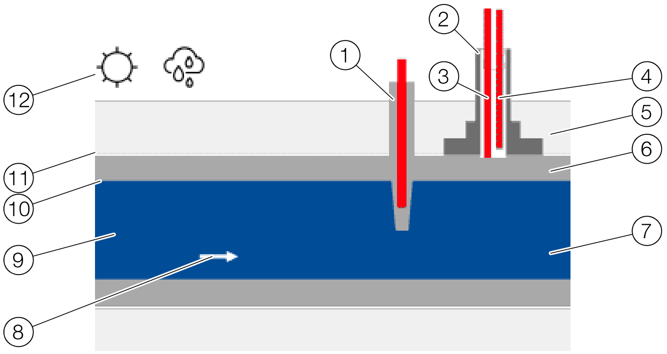
NINVA™ measurement principle

The TSP341-N sensor apparatus employed in both variants is equipped with the exchangeable 'measuring inset' which contains two 3-Wire Pt100 RTD sensors:

- One sensor is utilized to measure the contact temperature.
- The second sensor is used to measure the temperature near the contact measurement point and is termed the reference value.

The two temperature measurements are used to compensate for typical surface sensor errors (contact and ambient errors) and calculate the true surface temperature of the pipe or vessel.

This non-invasive measurement principle is illustrated below beside the traditional thermowell measurement principle.

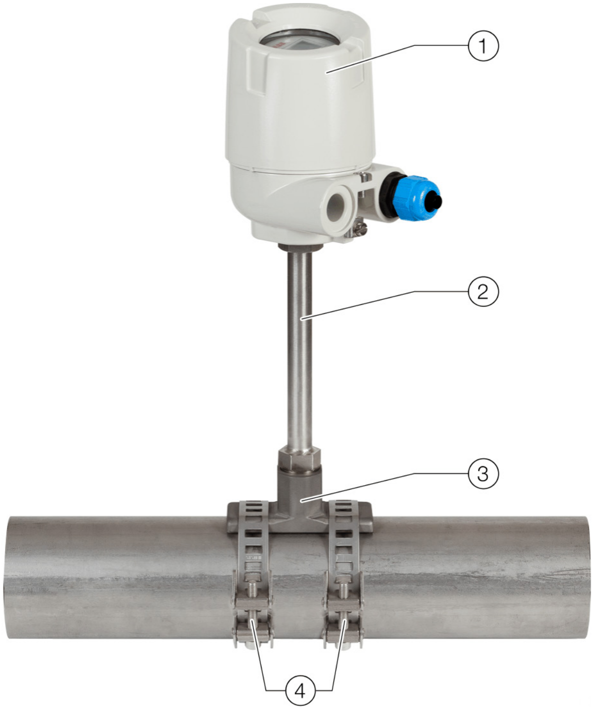


① Traditional invasive thermowell
② NINVA™ TSP341-N
③ Contact sensor
④ Reference sensor
⑤ Insulation
⑥ Pipe or vessel wall
⑦ Measuring medium
⑧ Flow direction
⑨ Medium temperature – T_{medium}
⑩ Wall Inner temperature – T_{swi}
⑪ Surface temperature – T_{surf}
⑫ Ambient temperature – T_{amb}

Figure 1: NINVA™ temperature measurement principle

… 9 SIL safety function

NINVA™ installation principle



① Connection head with transmitter
② Extension tube
③ Retaining plate
④ Clamp collars

Figure 2: NINVA™ sensor with integrated head-mount transmitter TTH300-N

For non-invasive temperature measurement, the NINVA™ temperature sensor can be fastened to a pipe or vessel surface using two clamp collars ④ which fixes the retaining plate ③ of the sensor.

Clamp collars with different thermal expansion coefficients are available to adapt to the pipe or vessel material.

Other process connection and mounting methods, like welding, are not considered within the safety analysis and needs to be qualified by the end user (e.g. using related field experience).

The transmitter can be configured using the optional local display unit or software tools such as the ABB Field Information Manager (FIM).

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 final device is assembled using
- the NINVA™ temperature sensor apparatus including measuring inset, extension tube and mounting parts
- the connection head (AGL/AGS, AGLD/AGSD, BUZ) with the optional display
- the transmitter electronics (TTH300-N or TTF300-N) and related cable connection (remote variant)

The area of SIL safety applications is limited to:
- up to SIL 2 as single (HFT=0) transmitter installation
- for the 'Low Demand Mode' safety operation

Further constraints as stated within this safety manual.

The safety function refers strictly to the analog output signal and the stated measurement function.
No other functions are declared and qualified as safety function.

Alarm behavior and alarm 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.

The device 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 23.6 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 safe detect both, the high and the low alarm current state.

Failure source	Alarm reaction	Failure rates
electrical part failures (e.g. capacitor short circuit)	**LOW ALARM** by design	see λ_{DD} Fail low
electrical part failures (e.g. resistor wire break)	**HIGH ALARM** by design	see λ_{DD} Fail high
sensor failures detected by internal diagnostics. **ADC failures** detected by internal diagnostics	Configured Current Alarm Mode: **LOW ALARM** (Factory Default) **or** **HIGH ALARM** (if configured)	see λ_{DD} Fail detected
electrical part failures (e.g. MCU) or **software failures** detected by internal independent watchdog	**LOW ALARM** by independent shutdown path	see λ_{DD} Fail detected
parts failures or too low supply voltage detected by internal current readback monitoring	**LOW ALARM** by independent shutdown path	see λ_{DD} Fail detected
memory failures (FLASH, RAM, EEPROM) detected by the internal diagnostics (double inverse & CRC32)	**LOW ALARM** by independent shutdown path	see λ_{DD} Fail detected

Self-diagnostics test interval

Safety-critical errors are detected and signaled by alarm output within a fault detection time of 15 min (worst case).

Safety deviation

The term ´safety deviation´ is defined as the change in the output signal due to internal component failures which was not rated as failure within the failure analysis. Used value on the safety deviation: ±2 % (±0.32 mA).

Response time

The response time of the non-invasive temperature is highly dependent on the final measurement application and must be verified carefully by the end user. (refer to chapter **SIL safety function** on page 9)

The following transmitter design items are known to influence on the measurement response time:

The average update cycle time on the NINVA™ temperature measurement value is ≈ 400 ms.

The configurable ‘process variable damping’ is implemented as digital 1st order PT1 Filter with related rise time influence of $t_{90}\% \approx 2.3 *$ damping value (0 to 100s)

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.

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

Type classification according to IEC 61508

This NINVA™ TSP341-N temperature sensor apparatus is declared as Type A element with HFT=0.
The TTH300-N & TTF300-N transmitter electronics is declared as Type B complex element with HFT=0.

… 9 SIL safety function

Useful lifetime

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. Although a constant failure rate is assumed by the probabilistic estimation method this only applies within the useful lifetime of related components as beyond their useful lifetime the probability of failure might significantly increase with time. As the useful lifetime is highly dependent on operating conditions the final plant experience shall be used to justify and adopt the below stated lifetimes.

Transmitter-Electronics TTH300-N/TTF300-N

The Temperature Transmitters TTH300-N and TTF300-N do not contain components with reduced useful lifetime which are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation.
Therefore, there is no limiting factor to the useful lifetime.

Mechanical TSP341-N sensor apparatus

According to the used Exida Material Failure Data the 'Useful Life' of the mechanical sensor assembly is estimated to 15 years. This means higher failure rates may be expected after this time period. The final field experience data shall be used to justify and adapt the lifetime to shorter or even longer 'Useful Life' periods.

SIL systematic capability

This device has been developed and qualified according to IEC 61508:2010 and fulfills the requirements for a Systematic SIL Safety Capability of SC 2 (SIL 2 capable).

The functional safety management, development and change process has been assessed by the independent organization TÜV NORD Systems GmbH & Co. KG, Augsburg, Germany.

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 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 Mode Effect & Diagnostics Analysis´.

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 term (1) is under control of the device manufacturer, it is the responsibility of the safety system designer to perform the PFD_{AVG} calculations for the final assembled safety system 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 PFD_{AVG} Calculation' contains related PFD_{AVG} values for a single channel 1oo1 architecture on selected proof-test inspection intervals as an example calculation.

10 SIL 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 signal is used for functional safety applications.
- The HART® protocol is only used for configuration and diagnostics purposes.
- The HART communication channel shall comply with the cyber security requirements of the final customer application
- Related parameters are configured as specified within the safety manual.
- The correct parameterization in terms of the safety function is verified by the end user.
- To ensure a reliable operation of the current output, the terminal voltage at the transmitter shall be within 11 to 42 V DC (Non-Ex application) and 11 to 30 V DC (Ex application).
- The robustness against EMC-disturbances has been tested to the requirements of NAMUR NE21:2017 which also fulfills the demands of IEC 61326-3-2:2017 Annex B, C, D which shall be considered within the related final plant operation environment
- 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 implemented.
- 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 ambient temperature range is restricted as stated within the related data sheets.
- The device is installed according to the manufacturer’s instructions.
- The application program within the safety logic solver is configured according to NAMUR NE43 to detect both fail low and fail high failure states. (otherwise, the related failure rates shall be used as dangerous undetected failures)
- It is verified, that materials are compatible with the final process conditions.
- Known aspects within NAMUR NE24 are considered, especially in terms of limitations regarding long-term stability, response behavior & limits of applications on thin film RTD sensing elements.
- The measurement / application limits (including temperature and vibration ranges) according to the data sheet are considered.
- The stated ‘intended use’ aspects within the operating instruction are considered.
- The stated ‘improper use’ aspects within the operating instruction are considered.
- The minimum terminal voltage at the transmitter is ensured.
- The measuring accuracy and response time has to be evaluated by the end user according to the final process application demands. Consider also ‘How to effectively use a non-invasive measurement’ and ‘Insulation of the measuring point’ within the related operating instruction OI/TSP341-N.
- The TSP341-N process mounting is considered as clamp mounted with the correct sizing to the final process demands.
- The proof-test specified within this safety manual (or an equivalent test as specified for the final safety function) shall be performed in periodical cycles as demanded by the final PFD_{AVG} demands.

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

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

Whenever the device 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 device must be write-protected to prevent inadvertent changes to the device setup.

11 SIL Safety Configuration

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

The latest released versions of the device drivers are available on:

ABB-Library – NINVA TSP341-N – Software Downloads

SIL Check Function

If the device 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 checks important device settings as listed above to support the end user in verifying the correct setup of parameters.

After performing the related parameter verifications, the 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 resulting state 'SIL Configuration Check not passed' the device 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.

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.

SIL safety parameter

In addition to the constraints as specified within the chapter 'SIL Safety operation constraints' the below named parameters must be configured as specified to operate the device within SIL safety applications.

The marked 'SIL Check' parameters are also checked by the 'SIL Check Function' for their correct values.

Function / Parameter	Local HMI Parameter	Check Value	Functionality	SIL Check
Measurement Mode Input Sensor 1 Input Sensor 2	<Easy Setup> <Measurement Mode>	**Non-invasive**	The measurement mode is configured to the non-invasive measurement and the sensors are configured to Pt100 (IEC751) 3-wires.	X
Primary Variable assignment	<Easy Setup> <In-Output Assignment>	**Surface Temp.** or Non-invasive Temp.	The current output is assigned to the non-invasive measurement. Surface temperature & Non-invasive temperature are identical values for SIL orders controlled by ABB factory settings.	X
Sensor Pair Value	<Easy Setup> <Sensor Pair Value>	**for TTF300-N value as provided by ABB**	The TTF300-N is connected by the end user to an TSP341-N remote sensor apparatus. Therefore, the end user must configure the Sensor Pair Value as provided by ABB on the TSP341-N remote sensor.	
Loop current mode	<Communication> <Current Loop Mode>	**Enabled**	Current Output follows the measurement variable (no HART Multidrop-Mode)	X
HART Burst Mode	<Communication> <HART Burstmode>	**OFF**	The HART Burst mode is not activated.	X
Output Simulation	<Diagnostics> <Looptest>	**0 mA** = Off	Current Output is not forced to a fixed value by simulation.	X
Current Alarm Mode	<Process Alarm> <Reaction on error>	**Low Alarm** or **High Alarm**	The end user shall check if the configuration is correct according to his final safety logic solver requirements. (see also 'Failure sources and related alarm reaction')	
Measurement range	<Easy Setup> <PV Lower Range Value> <PV Upper Range Value> <PV Unit>	**Range** **-40 to +400 °C**	The measurement range shall be within the range of -40 to +400 °C.	X
Damping	<Easy Setup> <PV Damping>	**Range 0 to 100s**	Check the influence on a configured damping > 0s to the final application requirements.	
Set/Reset device write protection by 'protection flag'	<Device Setup> <Write Protection> <SW Write Protection>	**Enabled**	Enables the write protection for local HMI and HART access.	X
Set/Reset device write protection by assigned ´key value´	<Device Setup> <Write Protection> <Enter Key Value>	****	Enables the write protection by an assigned 'Key Value'.	X
Alert Simulation	device driver only	**OFF**	Diagnostic events are not forced by simulations	X
Current Output Low Alarm Value	device driver only	**3.5 to 3.6 mA**	Alarm Value is configured within the safety application range	X
Current Output High Alarm Value	device driver only	**21.0 to 23.6 mA**	Alarm Value is configured within the safety application range	X
Current Output at Maintenance	device driver only	**Pulse Time = 0 s**	Current Output is acting without special pulse signaling	X
EMC Filter	device driver only		Check the influence on a configured > 0s to the final application requirements	
Electronic temperature failure NAMUR configuration	device driver only	**FAILURE** (Default)	Check if failures on the electronic temperature measurement are assigned as FAILURE.	X

12 FMEDA – Failure Mode Effect and Diagnostics Analysis

According to IEC 61508 the failure modes, failure rates and the architectural constraints of an element must be determined. This analysis uses the **Route 1_H** approach according 7.4.4.2 of IEC 61508-2 which involves calculating the Safe Failure Fraction for the entire element.

The following assumptions were made during the FMEDA:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Failures during installation & parameterization are not considered.
- External power supply failure rates are not included.
- As the optional display unit can interfere with the device, the contribution to the dangerous undetected failure rate is considered.
- The sensor environment is rated as low stress environment under consideration of the short extension wire length by the non-invasive sensor design, the embedded and filled RTD sensor housing by the non-invasive sensor design and a considered low vibration stress within the final operating environment (maximum 63 % of the datasheet limits).
- Sufficient tests are performed prior to shipment by ABB to verify the absence of vendor and/or manufacturing defects.
- The 'SIL Check function' provided by the device software has been executed via HMI or device drivers and related results have been considered carefully.

The FMEDA carried out under the assumptions described above and the references described within chapter 'References' lead to the following failure rates on the 'TSP341-N with integrated transmitter TTH300-N' and 'TSP341-N remote sensor apparatus with connected TTF300-N'.

Failure category	**Failure Rates FIT**
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	0
Fail Dangerous Detected (λ_{DD})	608
Fail detected (detected by internal diagnostics)	463
Fail high (detected by safety logic solver)	23
Fail low (detected by safety logic solver)	87
Annunciation detected (λ_{AD})	35
Fail Dangerous Undetected (λ_{DU})	88
Annunciation Undetected (λ_{AU})	17
No effect / No part	1547
Total failure rate (safety function)	696
SFF Type A Sensor	62 %
DC Type A Sensor	62 %
SFF Type B Electronics	93 %
DC Type B Electronics	93 %
MTBF safety function	164 years
SIL AC	SIL 2

13 Using the FMEDA results

Safe Failure Fraction

In terms of the safety function the device can be modelled as a serial combination of the element's sensor and electronics. According to IEC 61508-2 7.4.4.2.3 the maximum SIL that can be claimed is determined by the series element with the lowest safety integrity level for the achieved safe failure fraction as shown within the table below:

Element	**61508 Type**	**SFF**	**SIL**
TSP341-N Mechanical Sensor apparatus	A	62%	**SIL 2**
Electronics TTH300-N/TTF300-N	B	93%	**SIL 2**

Covered Elements and mounting method

The stated failure rates contain the elements:

a ‘Mechanical parts‘ incl. clamp mounted process connection.
b ‘Electrical parts’ (in terms of TTH300-N / TTF300-N and related connectors)
c ‘Optional Display’

Other process connection and mounting methods like welding are not considered and need to be qualified by the end user and related field monitoring data.

SIL AC

SIL AC (architectural constraints) means that the calculated SFF values are within the range for the corresponding SIL according to Table 2 and Table 3 of IEC 61508-2.

Ambient Conditions

The failure data of electronic components used within the FMEDA analysis are 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 higher average ambient temperatures > 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) is expected at the measurement location.

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.

14 Periodic proof-test and maintenance

General

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 to 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.

The proof-tests described below are recommended variants which could be performed after installation, configuration changes and within the required periodical proof-test interval derived from the safety instrument system engineering demands and related PFD_{AVG} calculations.

The stated proof-test methods can also be executed by flexible proof-test periods according NAMUR NE 106:2018.

… 14 Periodic proof-test and maintenance

Proof-Test A – 'Electronics'

This proof-test is able to detect possible undetected dangerous faults on the related temperature transmitter electronics.

λDU detected by proof-test: 37 FIT
PTC on total λDU: 42 %

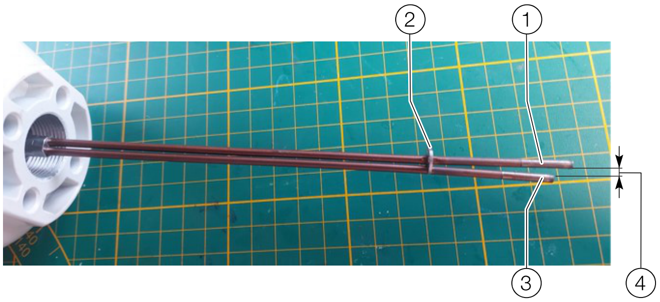
Step	Test Action (consecutive steps)
1.	Bypass the safety DCS or take other appropriate action to avoid a false trip.
2.	Restart, Power Down and Power Up the transmitter.
3.	Deactivate the transmitter write protection (refer to the relevant operating instructions).
4.	**Force the transmitter to the high alarm current output in using the device driver (FDI/DTM/EDD) simulation functionality and check 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 check 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 dangerous electronics failures)
10.	**Apply an adequate failure input signal (e.g., RTD short circuit or wire break) to reach the pre-defined alarm level and check that the expected safe state is reached.** (this verifies electronics failures from input to output stage).
11.	Remove the bypass from the safety DCS.

Table 1: Suggested steps for proof-test electronics

Proof-test B – 'NINVA™ measuring inset'

This proof-test is able to detect possible undetected dangerous faults on the related exchangeable NINVA™ measuring inset:

λ_{DU} detected by proof-test: 32 FIT
PTC on total λ_{DU}: 37 %



① Contact sensor
② Separating disc, should not be broken or lost
③ Reference sensor, slightly bent away
④ Distance: 7.0 mm, +0.5 mm

Figure 3: Proof-test B 'NINVA™ measuring inset'

Step	Test Action (consecutive steps)
1	Bypass the safety DCS or take other appropriate action to avoid a false trip.
2	Remove the measuring inset by loosening the housing from the neck tube and extracting the head and inset assembly.
3	**Check both 3-wire PT100 RTD measurement sensors in performing a multi-point measurement (at least 2-point calibration) on the targets for the applicable temperature measurement performance.**
4	**Check, the measurement inset on visible corrosions by optical inspection.**
5	**Check, by optical inspection, that the separating disc between the RTD sensors is in place and mechanically stable (not broken or loose).**
6	**Check, by optical inspection, that the reference sensor is bent away from the contact sensor with a distance of at least 7 mm between them.**
7	Remount the measuring inset.
8	Remove the bypass from the safety DCS.

Table 2: Suggested steps for proof-test 'NINVA™ measuring inset'

Proof-Test C – 'NINVA™ sensor assembly'

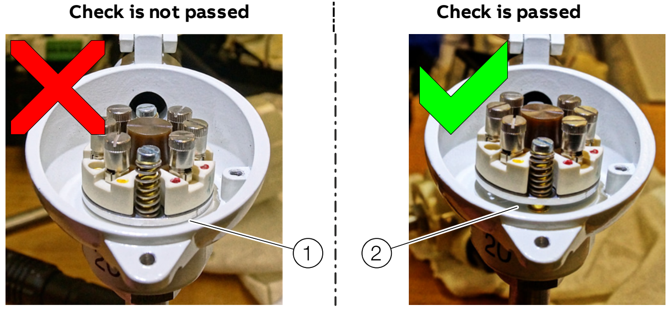
This proof-test is able to detect possible dangerous undetected faults on the related non-invasive temperature sensor in terms of the mechanical sensor parts except the RTD sensors measuring inset.

λDU detected by proof-test:	14 FIT
PTC on total λDU:	15 %

Step	Test Action (consecutive steps)
1.	Bypass the safety DCS or take other appropriate action to avoid a false trip.
2.	Check the mounting stability by holding the neck tube and attempt to move the neck tube in all directions to check for movement greater than 2 to 3 mm in any direction. Watch the following video for detailed information:
3.	**Check if the contact sensor is contacting the surface:** There must be a visible gap between and steel disk that transmitter or terminal board is installed upon, compare photos attached. If there is no visible gap, the check is not passed. See **Figure 4** for BUZ housing and **Figure 5** for AGL/AGS housing.
4.	On detected deviations, remove any insulation if present, reinstall the sensor assembly as per the operating instructions and repeat Step 2 and Step 3.
5.	Remove the bypass from the safety DCS.

Table 3: Suggested steps for proof-test 'NINVA™ sensor assembly'

BUZ housing

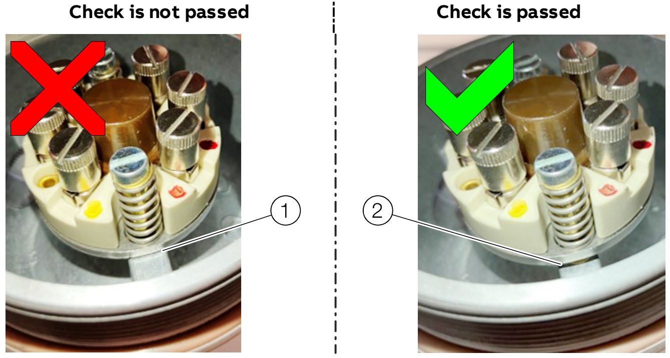


① No visible gap, contact sensor is not in touch with the surface.

② Visible gap, contact sensor is in touch with the surface. (the gap may be smaller than depicted here)

Figure 4: BUZ housing

AGL/AGS housing



① No visible gap, contact sensor is not in touch with the surface.

② Visible gap, contact sensor is in touch with the surface. (the gap may be smaller than depicted here)

Figure 5: AGL/AGS housing

… 14Periodic proof-test and maintenance

Proof-Test D – 'NINVA$^{\text{TM}}$ measuring tip contact'

This proof-test is able to detect possible dangerous undetected faults on the related non-invasive measuring tip contact to the process surface.

λDU detected by proof-test:	Not quantified
PTC on total λDU:	Not quantified

Step	Test Action (consecutive steps)
1.	Bypass the safety DCS or take other appropriate action to avoid a false trip.
2.	Remove any insulation if present
3.	Unmount the sensor assembly
4.	**Check by visual inspection for optimal contact; the measuring inset tip must have no visible corrosion or contamination and the measurement surface under the inset tip must clear of contamination or particles.**
5.	Remount the sensor assembly according to mounting instructions. Watch the following video for detailed information:
6.	Re-install any insulation if former present
7.	Remove the bypass from the safety DCS.

Table 4: 'Suggested steps for proof-test NINVA™ measuring tip contact'

Proof-Test Summary

All proof-test procedures together are able to detect around 94 % of the possible undetected dangerous faults as shown below:

Proof Test Procedure	**PTC**
Proof-Test A – 'Electronics'	**42%**
Proof-Test B – 'NINVA$^{\text{TM}}$ Measuring Inset'	**37%**
Proof-Test C – 'NINVA$^{\text{TM}}$ sensor assembly'	**15%**
Proof-Test D – 'NINVA$^{\text{TM}}$ measuring tip contact'	not quantified
Proof Test TOTAL	**94%**

15 Installation, Commissioning and Configuration

The named temperature measurement devices shall be installed, configured, commissioned and maintained by personnel with trained knowledge of temperature measurement 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 ‘Associated documents’ of this safety manual.

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

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

Therefore, the safety function shall be checked again after configuration, installation or repair change in using the described aspects on ‘Proof-Test’ and ‘SIL Safety Configuration’.

The constraints and limitations as provided within the operating instruction and data sheet as referenced within chapter ‘Associated documents’ must be considered by the end user, especially in terms of:

- Intended use and improper use
- Use in potentially explosive atmospheres
- Product identification
- Transportation and storage
- Installation and ambient conditions
- Electrical connections
- Commissioning and operation
- Diagnosis, maintenance and repair

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.

On www.abb.com/cybersecurity under ‘Additional resources’, ‘Alerts and notifications’ you will find notifications about newly discovered software vulnerabilities. It is recommended that you visit this website regularly and activate ‘Subscribe to email alerts’ to receive email notifications about ‘ABB cyber security alerts and notifications’.

16 Example PFD_{AVG} Calculation

An Average Probability of Dangerous Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) NINVA™ TSP341-N temperature sensor.

To support simplicity and transparency the PFD_{AVG} calculation was performed in using the below listed formula as references within RL5 Exida White Paper 'The Key Variables needed for PFD_{AVG} Calculation'.

This formula postulates two conditions:

$$PFDavg = \lambda_{DD} * MTTR + \left[C_{PT} * \lambda_{DU} * \frac{TI}{2}\right] + \left[(1 - C_{PT}) * \lambda_{DU} * \frac{MT}{2}\right]$$

a) no trip shutdown on dangerous detected failures of the safety instrumented system during repair time (MTTR)
b) safe shutdown during periodical proof testing

Value	Description
PFD_{AVG}	Average Probability of dangerous failure on demand
λ_{DU}	rate of dangerous undetected failures = 88 FIT (see **FMEDA – Failure Mode Effect and Diagnostics Analysis** on page 16)
λ_{DD}	rate of dangerous detected failures = 608 FIT (see **FMEDA – Failure Mode Effect and Diagnostics Analysis** on page 16)
MTTR	mean time to repair = 24 hours (assumed end user practice
CPT	Proof Test Coverage = 94 % (all proof tests as stated within Appendix 1: Possible Proof)
TI	Proof Test Interval = 1 year, 2 years, 5 year
MT	Mission Time = 15 years (assumed end user practice as operating time before replacement)

The resulting PFD_{AVG} values for the used variety of proof-test intervals are displayed below.

T [Proof] = 1 year	T [Proof] = 2 years	T [Proof] = 5 years
PFD_{AVG} = **7.24E-04**	PFD_{AVG} = **1.09E-03**	PFD_{AVG} = **2.17E-03**
% SIL 2 = 7.2%	% SIL 2 = 10.9%	% SIL 2 = 21.7%

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

This means:
On a 15-year operation with a 1-year Proof-Test Interval the PFDAVG is approximately equal to 8 % of the allowed SIL 2 range.

On a 15-year operation with a 2-year Proof-Test Interval the PFD_{AVG} is approximately equal to 11 % of the allowed SIL 2 range.

On a 15-year operation with a 5-year Proof-Test Interval the PFD_{AVG} is approximately equal to 22 % of the allowed SIL 2 range.

17 Release history

Safety Manual History

Revision	Description
Rev. A	First Version

Device Version History

Revision	Description
Hardware 02.00.02	first version with SIL approval
Software 13.02.00	first version with SIL approval

Assessment Report History

Revision	Description
07/2024	First Version – TÜV Nord 1435.IM.154935_23_TB_V1_0_EN_ABB_TempTrans_TSP341_TTx300

ABB Measurement & Analytics

For your local ABB contact, visit:
www.abb.com/contacts

For more product information, visit:
www.abb.com/temperature

3KXT161316R4901

SM/TSP341-N/HW02/SIL_IEC_61508-EN Rev. A 08.2024