



Failure Modes, Effects and Diagnostic Analysis

Project:

Temperature transmitters TSP***, TT*200-*H and TT*3*0-*H
with 4..20 mA output

Customer:

ABB Automation Products GmbH
Alzenau
Germany

Contract No.: ABB 06/05-29

Report No.: ABB 06/05-29 R029

Version V2, Revision R0; November 2009

Stephan Aschenbrenner, Alexander Dimov

Management summary for TSP*** with TTH200-*H or TTH300-*H, 4..20 mA output

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the temperature transmitters TSP*** with TTH200-*H or TTH300-*H with 4..20 mA output.

The temperature transmitter TTH200-*H is a configurable single sensor channel (1 x RTD 2/3/4 wire, 1 x TE, 1 x mV) analog 4..20mA device

The temperature transmitter TTH300-*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.

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

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 29: Version overview

Type	Description	HW Version	SW Version
TSP***	Sensor TSP000 ... TSP999 with TTH200-*H	1.06	1.00.06
TSP***	Sensor TSP000 ... TSP999 with TTH300-*H	1.01	1.01.07

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

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 1,00E-03$ to $< 1,00E-02$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part.

For a SIL 2 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than $1,00E-02$, hence the maximum allowable PFD_{AVG} value for the sensor part would then be $3,50E-03$.

The temperature transmitters TSP*** with TTH200-*H and TSP*** with TTH300-*H with 4..20 mA output are considered to be Type B⁷ subsystems with a hardware fault tolerance of 0.

The failure rates do not include failures resulting from incorrect use of the temperature transmitters TSP*** with TTH200-*H and TSP*** with TTH300-*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 40°C. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

⁷ 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 TSP*** with TTH200-*H and TSP*** with TTH300-*H with 4..20 mA output communicate detected faults by an alarm output current $\leq 3,6\text{mA}$ or $\geq 21\text{mA}$. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled.

Table 30: Failure rates ⁸

Failure category	Failure rates (in FIT)
Fail Dangerous Detected	327
Fail dangerous detected (internal diagnostics or indirectly ⁹)	227
Fail high (detected by the logic solver)	23
Fail low (detected by the logic solver)	77
Annunciation detected	0
Fail Dangerous Undetected	41
Fail dangerous undetected	39
Annunciation undetected	2
No Effect	110
Not part	91

Table 31: IEC 61508 failure rates

λ_{SD}	λ_{SU} ¹⁰	λ_{DD}	λ_{DU}	SFF ¹¹	DC _S ¹²	DC _D ¹⁴
0 FIT	110 FIT	327 FIT	41 FIT	91%	0%	88%

Table 32: PFD_{AVG} values

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

A complete temperature sensor assembly consisting of the temperature transmitters TSP*** with TTH200-*H or TTH300-*H and a thermocouple or RTD can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added.

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

⁸ It is assumed that practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.

⁹ "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.

¹⁰ Note that the SU category includes failures that do not cause a spurious trip

¹¹ Note: SFF should be calculated for the sensor subsystem. This SFF is only for reference.

¹² DC means the diagnostic coverage (safe or dangerous) for the temperature transmitters by the safety logic solver.

Assuming that the temperature transmitter TSP*** with TTH200-*H and TSP*** with TTH300-*H will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution or the PFD_{AVG} value (T[Proof] = 1 year) for the thermocouple or RTD in a low stress environment is as follows:

Table 33: TSP* with thermocouple (close coupled)**

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

Table 34: TSP* with two thermocouples (close coupled)**

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

Table 35: TSP* with 2/3-wire RTD (close coupled)**

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

Table 36: TSP* with two 2/3-wire RTDs (close coupled)**

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

Table 37: TSP* with thermocouple and 2/3-wire RTD (close coupled)**

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

Table 38: TSP* with 4-wire RTD (close coupled)**

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

Table 39: TSP* with thermocouple (with extension wire)**

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

Table 40: TSP* with two thermocouples (with extension wire)**

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

Table 41: TSP* with 2/3-wire RTD (with extension wire)**

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

Table 42: TSP* with two 2/3-wire RTDs (with extension wire)**

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

Table 43: TSP* with thermocouple and 2/3-wire RTD (with extension wire)**

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

Table 44: TSP* with 4-wire RTD (with extension wire)**

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

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

A user of the temperature transmitters TSP*** with TTH200-*H and TSP*** with TTH300-*H with 4..20 mA output can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508, Edition 2000. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the temperature transmitters TSP*** with TTH200-*H and TSP*** with TTH300-*H with 4..20 mA output (see Appendix 2).