



Failure Modes, Effects and Diagnostic Analysis

Project:

Pressure Transmitter 2600T Model 261

Customer:

ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 05/09-12

Report No.: ABB 05/09-12 R007

Version V1, Revision R1.2, March 2006

Stephan Aschenbrenner

Assessment Results

Type of Assessment: FMEDA as part of a full IEC 61508 assessment – Option 3
 Device Name: Pressure Transmitter 2600T Model 261
 Software Version: V1.3.0
 Hardware Version: V1.05

Table 1: Version overview of the types belonging to the considered devices

V1	Pressure Transmitter 2600T Model 261 x x (L, D, U, R, V) – p-Piezo
V2	Pressure Transmitter 2600T Model 261 x x (C, F) – p-Cap

Failure rate Database: Basic failure rates from the Siemens standard SN 29500
 Component Type: Type B¹
 Hardware Fault Tolerance (HFT): 0
 Sensor and mechanical Analysis: Yes
 Useful Lifetime: 8 – 12 years
 SIL capability: SIL 2

Table 2 Summary for Pressure Transmitter 2600T Model 261 – p-Piezo – Failure rates

Failure category	Failure rate (in FITs)
Fail Dangerous Detected	405
221	224
73	73
111	111
Fail Dangerous Undetected	34
No Effect	108
Annunciation Undetected	2
Not part	94
MTBF = MTTF + MTTR	178 years

Table 3 Pressure Transmitter 2600T Model 261 – p-Piezo

λ_{sd}	λ_{su}^2	λ_{dd}	λ_{du}	SFF	DC _S ³	DC _D ³
0 FIT	110 FIT	405 FIT	34 FIT	93%	0%	92%

Table 4 Pressure Transmitter 2600T Model 261 – p-Piezo: – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 1,47E-04	PFD _{AVG} = 7,34E-04	PFD _{AVG} = 1,47E-03

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

² Note that the SU category includes failures that do not cause a spurious trip

³ DC means the diagnostic coverage (safe or dangerous) for the pressure transmitter by the safety logic solver.

Table 5 Pressure Transmitter 2600T Model 261 – p-Cap – Failure rates

Failure category	Failure rate (in FITs)
Fail Dangerous Detected	613
284	284
73	73
256	255
Fail Dangerous Undetected	72
No Effect	142
Annunciation Undetected	2
Not part	96
MTBF = MTTF + MTTR	123 years

Table 6 Pressure Transmitter 2600T Model 261 – p-Cap

λ_{sd}	λ_{su}^4	λ_{dd}	λ_{du}	SFF	DC _S ⁵	DC _D ⁵
0 FIT	144 FIT	613 FIT	72 FIT	91%	0%	89%

Table 7 Pressure Transmitter 2600T Model 261 – p-Cap: – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 3,14E-04	PFD _{AVG} = 1,57E-03	PFD _{AVG} = 3,14E-03

⁴ Note that the SU category includes failures that do not cause a spurious trip

⁵ DC means the diagnostic coverage (safe or dangerous) for the pressure transmitter by the safety logic solver.

Appendix to the Assessment Results

A1 Assessment Options

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the software development process.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). In addition this option consists of an assessment of the proven-in-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

A2 General Information

For safety applications only the 4..20 mA output was considered. All other possible output variants, electronics or applications are not covered by this report. The different devices can be equipped with or without display.

The Pressure Transmitter 2600T Model 261 is considered to be a Type B⁶ component with a hardware fault tolerance of 0.

For Type B components with a hardware fault tolerance of 0 the SFF shall be > 90% according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

ABB Automation Products GmbH performed a qualitative analysis of the sensor element p-piezo of the Pressure Transmitter 2600T Model 261 (see [D8] and [D9]). This analysis was used by *exida* to calculate the failure rates of the sensor element using different failure rate databases ([N5], [N6], [N7] and *exida*'s experienced-based data compilation) for the different components of the sensor element (see [R4]). The results of the quantitative analysis were used for the calculations described in sections 5.2.

Failure rates that are assigned to the various failure modes of the sensor element p-cap of the Pressure Transmitter 2600T Model 261 were obtained from field failure data using only operational hours from the warranty period of operation. Confidence Interval calculations were done using a chi-square distribution and an upper limit failure rate based on a 70% confidence factor per IEC 61508. The failure rate results were compared with industry databases [N5] and found to be within a reasonable range considering the much higher amount of operational hours. The results of this analysis were used for the calculations described in sections 5.3.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures.

A user of the Pressure Transmitter 2600T Model 261 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 5.2 to 5.3 in the FMEDA report along with all assumptions.

The failure rates are valid for the useful life of the Pressure Transmitter 2600T Model 261 (see appendix 3).

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.

⁶ Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.