FMEDA and Prior-use Assessment

Project:
Pressure Transmitter 2600T / 2000T Series with 4..20 mA output

Customer:
ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 03/09-13
Report No.: ABB 03/09-13 R001
Version V1, Revision R1.2, March 2004
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with prior-use consideration according to IEC 61508 / IEC 61511 carried out on the pressure transmitter 2600T / 2000T Series with 4..20 mA output and software version V0.24. Table 1 gives an overview of the different types that belong to the considered pressure transmitter 2600T / 2000T Series.

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	Application	Sensor	Electronics
V1.1	265D*A 2010TD	Differential pressure	10mbar	2-6187 P1 (3) 2-6195 P1 (2) 764913_P1
	265J*A	Differential and absolute pressure	10mbar	2-6187 P1 (3) 2-6195 P1 (2) 764913_P1
V1.2	267C*A 269C*A 2010TC	Mass flow / Differential pressure	10mbar	2-6187 P1 (3) 2-6195 P1 (2) 764913_P1 9280 039 P1 (3)
V2.1	265D*(C,F,L,N) 2010TD	Differential pressure	60mbar to 20bar	2-6187 P1 (3) 2-6195 P1 (2) 2-6186 P1 (3)
	265J*(C,F,L,N)	Differential and absolute pressure	60mbar to 20bar	2-6187 P1 (3) 2-6195 P1 (2) 2-6186 P1 (3)
	265V*(F,L,N) 2010TA	Absolute pressure	400mbar to 20bar	2-6187 P1 (3) 2-6195 P1 (2) 2-6186 P1 (3)
V2.2	267C*(C,F,L,N) 269C*(C,F,L,N) 2010TC	Mass flow / Differential pressure	60mbar to 20bar	2-6187 P1 (3) 2-6195 P1 (2) 2-6186 P1 (3) 9280 039 P1 (3)
V3	265D*R 2010TD	Differential pressure	100bar	2-6187 P1 (3) 2-6195 P1 (2) 0764 908 P1 (3)
V4	265A* (C,F) 2020TA	Absolute pressure	60mbar and 400mbar	2-6187 P1 (3) 2-6195 P1 (2) 0764 892 P1 (3)
	265G* (C,F) 2020TG	Gauge	60mbar and 400mbar	2-6187 P1 (3) 2-6195 P1 (2) 0764 892 P1 (3)
V5	265A*(L,U) 2020TA	Absolute pressure	≥ 2,5bar	2-6187 P1 (3) 2-6195 P1 (2) 2-6149 P1 (3)
	265G*(L,U,R,V) 2020TG	Gauge	≥ 2,5bar	2-6187 P1 (3) 2-6195 P1 (2) 2-6149 P1 (3)

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 different devices can be equipped with or without display.

The failure rates 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 $\geq 10^{-3}$ to $< 10^{-2}$ 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 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 pressure transmitter 2600T / 2000T Series with 4..20 mA output is considered to be a Type B[1] component with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

As the pressure transmitter 2600T / 2000T Series with 4..20 mA output is supposed to be a proven-in-use device, an assessment of the hardware with additional prior-use demonstration for the device and its software was carried out. The prior-use investigation was based on field return data collected and analyzed by ABB Automation Products GmbH. This data cannot cover the process connection. The prior-use justification for the process connection still needs to be done by the end-user.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.1 the Type B pressure transmitter 2600T / 2000T Series with a hardware fault tolerance of 0 and a SFF of 60% to < 90% is considered to be suitable for use in SIL 2 safety functions The decision on the usage of prior-use devices, however, is always with the end-user.

Failure rates that are assigned to the various failure modes of the sensor part of the pressure transmitter 2600T / 2000T Series 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 [N6] and found to be within a reasonable range considering the much higher amount of operational hours.

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 depending on whether the pressure transmitter 2600T / 2000T Series with 4..20 mA output is used in an application for “low level monitoring”, “high level monitoring” or “range monitoring”. For these applications the following tables show how the above stated requirements are fulfilled.

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

Table 2: Summary for version V1.1 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		461	
Fail detected (int. diag.)	216		
Fail high (inherently)	245		245
Fail Low (detected by the logic solver)			231
Fail detected (int. diag.)	216		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		195	195
No Effect		137	137
Annunciation Undetected		1	1
Not part		54	54
MTBF = MTTF + MTTR		132 years	132 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{Sd}$ $\lambda_{high} = \lambda_{dd}$	15 FIT	138 FIT	462 FIT	195 FIT	75%	10%	70%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	461 FIT	138 FIT	15 FIT	195 FIT	75%	77%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	476 FIT	138 FIT	0 FIT	195 FIT	75%	78%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	231 FIT	138 FIT	245 FIT	195 FIT	75%	63%	56%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	245 FIT	138 FIT	231 FIT	195 FIT	75%	64%	54%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	476 FIT	138 FIT	0 FIT	195 FIT	75%	78%	0%

Table 3: Summary for version V1.1 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 8,54E-04	PFD_{AVG} = 4,26E-03	PFD_{AVG} = 8,50E-03

[2] DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for pressure transmitter 2600T / 2000T Series with 4..20 mA output.

Table 4: Summary for version V1.2 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		516	
Fail detected (int. diag.)	256		
Fail high (inherently)	260		260
Fail Low (detected by the logic solver)			272
Fail detected (int. diag.)	256		
Fail low (inherently)	16	16	
Fail Dangerous Undetected		216	216
No Effect		166	166
Annunciation Undetected		1	1
Not part		54	54
MTBF = MTTF + MTTR		118 years	118 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	16 FIT	167 FIT	516 FIT	216 FIT	76%	9%	70%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	516 FIT	167 FIT	16 FIT	216 FIT	76%	76%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	532 FIT	167 FIT	0 FIT	216 FIT	76%	76%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	272 FIT	167 FIT	260 FIT	216 FIT	76%	62%	55%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	260 FIT	167 FIT	572 FIT	216 FIT	76%	61%	73%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	532 FIT	167 FIT	0 FIT	216 FIT	76%	76%	0%

Table 5: Summary for version V1.2 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 9,43E-04	PFD_{AVG} = 4,70E-03	PFD_{AVG} = 9,38E-03

Table 6: Summary for version V2.1 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		391	
Fail detected (int. diag.)	189		
Fail high (inherently)	202		202
Fail Low (detected by the logic solver)			204
Fail detected (int. diag.)	189		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		198	198
No Effect		127	127
Annunciation Undetected		1	1
Not part		54	54
MTBF = MTTF + MTTR		145 years	145 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	15 FIT	128 FIT	391 FIT	198 FIT	73%	10%	66%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	391 FIT	128 FIT	15 FIT	198 FIT	73%	75%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	406 FIT	128 FIT	0 FIT	198 FIT	73%	76%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	204 FIT	128 FIT	202 FIT	198 FIT	73%	61%	51%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	202 FIT	128 FIT	204 FIT	198 FIT	73%	61%	51%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	406 FIT	128 FIT	0 FIT	198 FIT	73%	76%	0%

Table 7: Summary for version V2.1 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 8,65E-04	PFD_{AVG} = 4,31E-03	PFD_{AVG} = 8,60E-03

Table 8: Summary for version V2.2 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		446	
Fail detected (int. diag.)	229		
Fail high (inherently)	217		217
Fail Low (detected by the logic solver)			245
Fail detected (int. diag.)	229		
Fail low (inherently)	16	16	
Fail Dangerous Undetected		218	218
No Effect		156	156
Annunciation Undetected		1	1
Not part		54	54
MTBF = MTTF + MTTR		128 years	128 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	16 FIT	157 FIT	446 FIT	218 FIT	73%	9%	67%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	446 FIT	157 FIT	16 FIT	218 FIT	73%	74%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	462 FIT	157 FIT	0 FIT	218 FIT	73%	75%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	245 FIT	157 FIT	217 FIT	218 FIT	73%	61%	50%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	217 FIT	157 FIT	245 FIT	218 FIT	73%	58%	53%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	462 FIT	157 FIT	0 FIT	218 FIT	73%	75%	0%

Table 9: Summary for version V2.2 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 9,54E-04	PFD_{AVG} = 4,76E-03	PFD_{AVG} = 9,49E-03

Table 10: Summary for version V3 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		1510	
Fail detected (int. diag.)	210		
Fail high (inherently)	1300		1300
Fail Low (detected by the logic solver)			225
Fail detected (int. diag.)	210		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		558	558
No Effect		124	124
Annunciation Undetected		1	1
Not part		54	54
MTBF = MTTF + MTTR		50 years	50 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	15 FIT	125 FIT	1510 FIT	558 FIT	74%	11%	73%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	1510 FIT	125 FIT	15 FIT	558 FIT	74%	92%	3%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	1525 FIT	125 FIT	0 FIT	558 FIT	74%	92%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	225 FIT	125 FIT	1300 FIT	558 FIT	74%	64%	70%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	1300 FIT	125 FIT	225 FIT	558 FIT	74%	91%	29%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	1525 FIT	125 FIT	0 FIT	558 FIT	74%	92%	0%

Table 11: Summary for version V3 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 3 years	T[Proof] = 5 years
PFD_{AVG} = 2,44E-03	PFD_{AVG} = 7,29E-03	PFD_{AVG} = 1,21E-02

Table 12: Summary for version V4 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		775	
Fail detected (int. diag.)	218		
Fail high (inherently)	557		557
Fail Low (detected by the logic solver)			233
Fail detected (int. diag.)	218		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		300	300
No Effect		125	125
Annunciation Undetected		1	1
Not part		56	56
MTBF = MTTF + MTTR		90 years	90 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	15 FIT	126 FIT	775 FIT	300 FIT	75%	11%	72%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	775 FIT	126 FIT	15 FIT	300 FIT	75%	86%	5%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	790 FIT	126 FIT	0 FIT	300 FIT	75%	86%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	233 FIT	126 FIT	557 FIT	300 FIT	75%	65%	65%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	557 FIT	126 FIT	233 FIT	300 FIT	75%	82%	44%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	790 FIT	126 FIT	0 FIT	300 FIT	75%	86%	0%

Table 13: Summary for version V4 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,31E-03	PFD_{AVG} = 6,53E-03	PFD_{AVG} = 1,30E-02

Table 14: Summary for version V5 – Failure rates

Failure category (Failure rates in FIT)		Fail-safe state = "fail high"	Fail-safe state = "fail low"
Fail High (detected by the logic solver)		386	
Fail detected (int. diag.)	189		
Fail high (inherently)	197		197
Fail Low (detected by the logic solver)			204
Fail detected (int. diag.)	189		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		222	222
No Effect		115	115
Annunciation Undetected		1	1
Not part		53	53
MTBF = MTTF + MTTR		144 years	144 years

Transmitter configured fail-safe state = "fail high" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	15 FIT	116 FIT	386 FIT	222 FIT	69%	11%	64%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	386 FIT	116 FIT	15 FIT	222 FIT	69%	77%	6%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	401 FIT	116 FIT	0 FIT	222 FIT	69%	78%	0%

Transmitter configured fail-safe state = "fail low" – Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	204 FIT	116 FIT	197 FIT	222 FIT	69%	64%	47%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	197 FIT	116 FIT	204 FIT	222 FIT	69%	63%	48%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	401 FIT	116 FIT	0 FIT	222 FIT	69%	78%	0%

Table 15: Summary for version V5 – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 9,71E-04	PFD_{AVG} = 4,84E-03	PFD_{AVG} = 9,66E-03

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. 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 table 3.1 of ANSI/ISA–84.01–1996 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. The boxes marked in red ( ) mean that the calculated PFD_{AVG} values do not fulfill the requirement for SIL 2 according to table 2 of IEC 61508-1.

The functional assessment has shown that transmitters of the pressure transmitter 2600T / 2000T Series with 4..20 mA output have a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of more than 69%. Based on the verification of "prior use" they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of the pressure transmitter 2600T / 2000T Series with 4..20 mA output can utilize these failure rates along with the failure rates for an impulse line, when required, 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 for different operating conditions is presented in section 5.2 to 5.6 along with all assumptions.

It is important to realize that the “don’t care” failures and the “annunciation” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.