SIL-Safety Instructions

SM/265/7/9/SIL-EN Rev. 03

Pressure-Transmitter 2600T
Models 265, 267, 269

Model 265GS/GC/GM/GG/GJ/GN/GR, 265DS/DC/DR
Model 265AS/AC/AM/AG/AJ/AN/AR, 265VS
Model 267JS, 269JS, 267CS/CR, 269CS/CR

Safety Integrity Level
SIL2
IEC 61508

ABB

Pressure-Transmitter 2600T

Models 265, 267, 269

SIL-Safety Instructions

SM/265/7/9/SIL-EN Rev. 03

02.2008

Manufacturer:

ABB Automation Products GmbH
Schillerstraße 72
32425 Minden
Germany
Tel.: +49 551 905-534
Fax: +49 551 905-555
CCC-support.deapr@de.abb.com

1 Field of Application

Measure differential, gauge and absolute pressure in accordance specifically with the safety engineering requirements of IEC 61508 / IEC 61511-1.

The measuring equipment meets the following requirements:

- Functional safety according to IEC 61508 / IEC 61511-1
- Explosion protection (depending on version)
- Electromagnetic compatibility according to EN 61326 and NAMUR recommendation NE 21

2 Your benefits

For use with:

- Limit pressure monitoring
- Continuous measurement
- Easy startup

3 Acronyms and abbreviations

Acronym	English	Explanation
HFT	Hardware Fault Tolerance	Hardware Fault Tolerance Ability of a functional unit (hardware) to continue to perform a required function in the presence of faults or errors.
MTBF	Mean Time Between Failures	Mean Time Between two Failures
MTTR	Mean Time To Repair	Mean time between occurrence of an error in a unit or system and its repair.
PFD	Probability of Failure on Demand	Probability of hazardous failures for a safety function on demand
PFD_{av}	Average Probability of Failure on Demand	Average probability of hazardous failures for a safety function on demand
SIL	Safety Integrity Level	Safety Integrity Level The international standard IED 61508 defines four discrete Safety Integrity Levels (SIL 1 to SIL 4). Each level corresponds to a range of probability for the failure of a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will perform the requested safety function.
SFF	Safe Failure Fraction	Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state.
TI	Test Interval between live testing of the safety function	Test interval between live testing of the safety function.
XooY	"X out of Y" voting (e.g., 2oo3)	Classification and description of the safety-related system with regard to redundancy and selection procedure used. "Y" specifies how often the safety function is performed (redundancy). "X" determines how many channels have to work properly. Example based on pressure measurement: 1oo2 architecture. A safety-related system decides that a predefined pressure limit is exceeded when one of the two pressure sensors reaches this limit. If a 1oo1 architecture is used, there is only one pressure sensor available.

4 Relevant standards

Standard	English	Explanation
IEC 61508, Part 1 to 7	Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)	Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)
IEC 61511, Part 1	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)	Functional safety – Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)

5 Terms

Terms	Explanation
Dangerous failure	A failure that has the potential to place the safety-related system in a dangerous state or render the system inoperative.
Safety-related system	A safety-related system performs the safety functions that are required to achieve or maintain a safe condition, e.g., in a plant. Example: pressure meter, logics unit (e.g., limit signal generator) and valve form a safety-related system.
Safety function	A specified function that is performed by a safety-related system with the goal, under consideration of a defined hazardous incident, of achieving or maintaining a safe condition for the plant. Example: limit pressure monitoring

6 Determining the Safety Integrity Level (SIL)

The achievable Safety Integrity Level is determined by the following safety-related parameters:

- Average probability of hazardous failures for a safety function on demand (PFD_{av})
- Hardware Fault Tolerance (HFT)
- Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF)

The specific safety-related parameters for the transmitter, as part of a safety function, are listed in the section "Safety-related parameters".

The following table shows the dependence of the Safety Integrity Level (SIL) on the Average Probability of Failure on Demand (PFD_{av}). The table applies the "low demand mode", i.e. the rate of requests for the safety-related system is maximum once a year.

Safety Integrity Level (SIL)		(low demand mode)
4	PFD_{av}	$\geq 10^{-5} \ldots < 10^{-4}$
3		$\geq 10^{-4} \ldots < 10^{-3}$
2		$\geq 10^{-3} \ldots < 10^{-2}$
1		$\geq 10^{-2} \ldots < 10^{-1}$

Sensor, logics unit and actuator form a safety-related system that performs a safety function. The Average Probability of Failure on Demand (PFD_{av}) is usually divided between the sensor, logics unit and actuator sub-systems.

Typical division of the Average Probability of Failure on Demand (PFD_{av}) into sub-systems

Sensor (e.g., pressure meter)	Logics unit (e.g., PLC)	Final control element (e.g., valve)
≤ 35%	≤ 15%	≤ 50%

Important

The 265xx transmitter is considered a component of a safety function in this document. The following table displays the achievable Safety Integrity Level (SIL) for the entire safety-related system for type B systems depending on the Safe Failure Fraction (SFF) and the Hardware Fault Tolerance (HFT). Type B systems are, for example, sensors with complex components such as microprocessors (see also IEC 61508, Part 2).

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1 (0) [1]	2 (1) [1]
< 60%	not permitted	SIL 1	SIL 2
60 … < 90%	SIL 1	SIL 2	SIL 3
90 … < 99%	SIL 2	SIL 3	-
≥ 99%	SIL 3	-	-

[1] In accordance with IEC 61511-1, section 11.4.3, the Hardware Fault Tolerance (HFT) can be reduced by one (value in brackets) for devices using sensors and final control elements with complex components, if the following conditions exist:

- The device is proven in use.
- The device allows users to adjust process-related parameters only, e.g., measuring range upscale or downscale failure direction, etc.
- The setup level of the device is protected, e.g., via jumper or password (in this case: numeric code or key combination).
- The function has a Safety Integrity Level (SIL) requirement of less than 4.

All conditions are fulfilled by the transmitter.

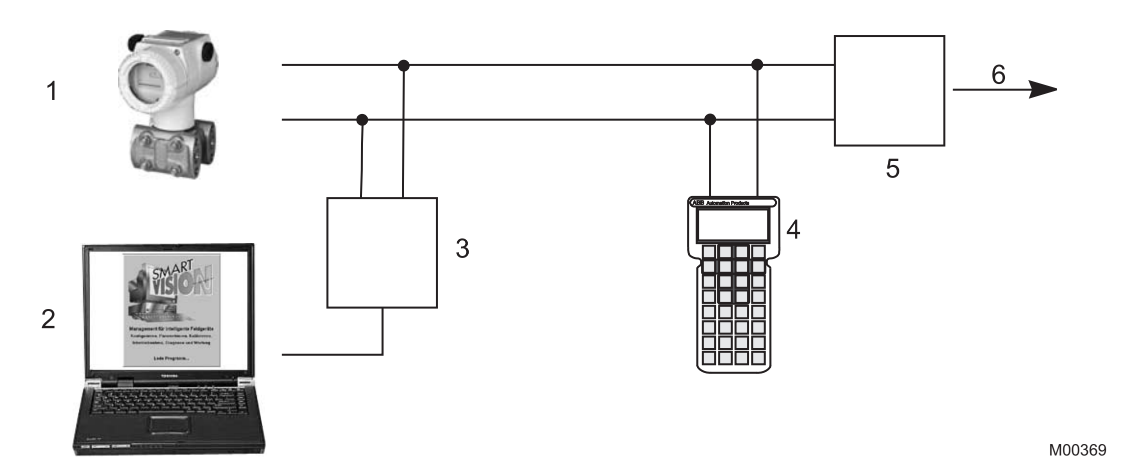

Fig. 1: Safety function (e.g., for limit pressure monitoring) with 265DS as sub-system

1 Transmitter 265DS [1]
2 PC with GUI (graphical user interface), e.g., DSV401 (SMART VISION) [2]
3 FSK modem
4 Handheld terminal [3]
5 Logics unit, e.g., PLC, limit signal generator, etc.
6 Actuator

[1] 265DS with local operation, option for setting upper and lower range limits as well as damping value.

[2] Computer with operating program, e.g., SMART VISION to configure all parameters such as alarm behavior, max. alarm, operating mode, etc.

[3] Handheld terminal for setting all parameters such as alarm behavior, max. alarm, operating mode, etc.

The 2600T transmitter generates an analog signal (4 … 20 mA) proportional to the differential pressure or the gauge/absolute pressure. The analog signal is fed to a downstream logics unit such as a PLC or a limit signal generator, and is monitored to determine with it exceeds a maximum value. In order to monitor errors, the logics unit must be able to detect both HI alarms (configurable between 21 … 22.5 mA) and LO alarms (3.6 mA).

7 Information for the safety function

Attention!

The mandatory settings and data for the safety functions are listed in the sections "Settings" and "Safety-related parameters".

For information about the response time of the transmitter, see the relevant data sheet.

Important

MTTR is set to 8 hours as default.

Safety-related systems without a self-locking function must be monitored or set to an otherwise safe condition after performing the safety function within MTTR.

8 Applicable device documentation

Depending on the version, the following documentation must be available for the transmitter:

Type	Operating instructions
265Dx/Vx	IM 265D/V
265Gx/Ax	IM 265G/A
267Cx/269Cx	IM 267C / 269C
267Jx/269Jx	IM 267C / 269C

For devices in explosion-proof design, the relevant EC-type examination test certificate must be present.

9 Behavior during operation and failure

Important

Behavior during operation and failure is described in the operating instructions.

10 Periodic checks

The operability of the measuring device must be tested at appropriate time intervals, e.g., calibration check (see the relevant operating instructions, sections on operation, calibration, maintenance and repairs). We recommend that you perform the test at least once a year. Users are responsible for selecting the type of check and the intervals within the specified period.

When you send a defective transmitter or module to the repair department, include information describing the error and, if possible, the cause. When ordering spare parts or replacement devices, please always provide the serial number (S/N) as well as the year of manufacture for the original device.

Address

ABB Automation GmbH

Parts & Repair

Schillerstrasse 72

32425 Minden

GERMANY

11 Setup

11.1 Alarm behavior and current output

In the event of a fault, the current value is set to the preselected value. You can change settings by using either the ABB operating program DSV401 (SMART VISION) or a handheld terminal.

Attention!

After entering all of the parameters, check the safety function. The transmitter allows users to simulate a signal current, independent of measured pressure, via the Simulation and Set Simulation Current options.

These options can be used via DSV401 (SMART VISION) and the HART handheld terminal.

11.2 Locking / Unlocking

Warning!

Changes to the measuring system and its settings after commissioning can have a negative effect on the safety function. For this reason, you should lock the control keys on the transmitter after entering all parameters and checking the safety function. This protects your entries against unintentional or unauthorized changes. When the keys on the device are locked, the control keys can only be unlocked again via the keys on the device.

M00055

Fig. 2

12 Safety engineering parameters

12.1 Prerequisites

- Communication via HART protocol is used only to configure and calibrate the device. It is also used for diagnostic functions but not for safety-related, critical operations.
- Self-diagnostic tests are processed cyclically within an hour and thereafter restart automatically.
- The repair period following a device fault is 8 hours.
- The mean temperature over a longer period of time is 40 °C.
- The transmitter is used only in applications with low request rates (low demand mode).
- Only the 4 ... 20 mA current signal is analyzed by the protective device.
- A dangerous failure is an error during which the output current no longer responds to the input signal or deviates by more than 2% from the upper range limit.
- The safety PLC must be designed to clearly detect errors that result in HI alarms as well as those that result in LO alarms.

12.2 Specific safety-related parameters

Transmitter type	Flow range	SFF	PFDav	λdd + λs	λdu
265Dx (A)	10 mbar	75 %	8.54×10^{-4}	614 FIT	195 FIT
267Cx (A) 269Cx (A)	10 mbar	76 %	9.43×10^{-4}	698 FIT	216 FIT
265Dx (A,3,C,F,L,N)	10 mbar to 20 bar	73 %	8.70×10^{-4}	539 FIT	199 FIT
265Vx (F,L,N)	400 mbar to 20 bar				
267Cx (A,3,C,F,L,N) 269Cx (A,3,C,F,L,N) 267Jx (A,3,C,F,L,N) 269Jx (A,3,C,F,L,N)	10 mbar to 20 bar	74 %	9.59×10^{-4}	625 FIT	219 FIT
265Dx (R)	100 bar	74 %	24.4×10^{-4}	1651 FIT	558 FIT
265Ax (C,F)	60 mbar, 400 mbar	75 %	13.2×10^{-4}	918 FIT	303 FIT
265Gx (C,F)	60 mbar, 400 mbar				
265Ax (L,D,U,R)	≥ 2.5 bar	69 %	9.92×10^{-4}	511 FIT	227 FIT
265Gx (L,D,U,R,V)	≥ 2.5 bar				

λdd + λs: Failure rate for detected dangerous failures and safe failures

λdu: Failure rate for dangerous, undetected failures

The letters in parentheses indicate the order code for the measuring range.

Important

For additional information, see the Management Summary.

13 SIL declaration of conformity

DC/265/7/9/SIL
Rev. B

SIL CERTIFICATE OF CONFORMITY

Manufacturer: **ABB Automation Products GmbH**

Address: **Schillerstrasse 72 - D-32425 Minden**

Product name: **Pressure Transmitter 2600T - 265xx, 267xx, 269xx (4...20 mA)**

Functional safety according to IEC 61508 / IEC 61511

We as the manufacturer declare that the a.m. products are suitable for the use in a safety related application up to SIL 2 according to IEC 61511-1, provided that the attached safety instructions are observed. The assessment of the safety critical and dangerous random errors results, in case of an annual function test, in the following parameters:

SIL (Safety integrity level): **2** **Type: B**

HFT (Hardware failure tolerance): **0[1] (one-channel application)**

Transmitter Type	Measuring Range	SFF	PFDav	$\lambda_{dd} + \lambda_s$	λ_{du}
265D*A	10 mbar	75 %	$8{,}54 * 10^{-4}$	614 FIT	195 FIT
267C*A / 269C*A	10 mbar	76 %	$9{,}43 * 10^{-4}$	698 FIT	216 FIT
265D*(A,3,C,F,L,N) 265V*(F,L,N)	10 mbar to 20 bar 400 mbar to 20 bar	73 %	$8{,}7 * 10^{-4}$	539 FIT	199 FIT
267C* / 269C*(A,3,C,F,L,N) 267J* / 269J*(A,3,C,F,L,N)	10 mbar to 20 bar 10 mbar to 20 bar	74 %	$9{,}59 * 10^{-4}$	625 FIT	219 FIT
265D*R	100 bar	74 %	$24{,}4 * 10^{-4}$	1651 FIT	558 FIT
265A* / 265G*(C,F)	60 mbar, 400 mbar	75 %	$13{,}2 * 10^{-4}$	918 FIT	303 FIT
265A*(L,D,U,R) 265G*(L,D,U,R,V)	≥ 2,5 bar ≥ 2,5 bar	69 %	$9{,}92 * 10^{-4}$	511 FIT	227 FIT

1) according to chapter 11.4 of IEC 61511

For the prior-use investigation the instrument including the modifications was analysed.

25.10.2007
Date

Dr. Wolfgang Scholz
Head of Research & Development

Manfred Klüppel
Head of Quality Assurance

14 Management summary

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 V3, Revision R0, October 2007
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 V0.26. 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	Differential pressure	10mbar	2-6187 P1 (3) 2-6251 P1 (2) 764913_P1
V1.2	267C*A 269C*A	Mass flow / Differential pressure	10mbar	2-6187 P1 (3) 2-6251 P1 (2) 764913_P1 9280 039 P1 (3)
V2.1	265D*(A,3,C,F,L,N)	Differential pressure	10mbar to 20bar	2-6187 P1 (3) 2-6251 P1 (2) 9280281_P1 (3)
	265V*(F,L,N)	Absolute pressure	400mbar to 20bar	2-6187 P1 (3) 2-6251 P1 (2) 9280281_P1 (3)
V2.2	267C*(A,3,C,F,L,N) 269C*(A,3,C,F,L,N)	Mass flow / Differential pressure	10mbar to 20bar	2-6187 P1 (3) 2-6251 P1 (2) 9280281_P1 (3) 9280 039 P1 (3)
	267J*(A,3,C,F,L,N) 269J*(A,3,C,F,L,N)	Differential pressure	10mbar to 20bar	2-6187 P1 (3) 2-6251 P1 (2) 9280281_P1 (3) 9280 039 P1 (3)
V3	265D*R	Differential pressure	100bar	2-6187 P1 (3) 2-6251 P1 (2) 0764 908 P1 (3)
V4	265A* (C,F)	Absolute pressure	60mbar and 400mbar	2-6187 P1 (3) 2-6251 P1 (2) 9280293_P1 (3)
	265G* (C,F)	Gauge	60mbar and 400mbar	2-6187 P1 (3) 2-6251 P1 (2) 9280293_P1 (3)
V5	265A*(L,D,U,R)	Absolute pressure	≥ 2,5bar	2-6187 P1 (3) 2-6251 P1 (2) 2-6149 P1 (3)
	265G*(L,D,U,R,V)	Gauge	≥ 2,5bar	2-6187 P1 (3) 2-6251 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.

---

[1] 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)		460	
Fail detected (int. diag.)	216		
Fail high (inherently)	244		244
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		138	138
Annunciation Undetected		1	1
Not part		116	116
MTBF = MTTF + MTTR		123 years	123 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	139 FIT	460 FIT	195 FIT	75%	10%	70%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	460 FIT	139 FIT	15 FIT	195 FIT	75%	77%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	475 FIT	139 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	139 FIT	244 FIT	195 FIT	75%	63%	56%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	244 FIT	139 FIT	231 FIT	195 FIT	75%	64%	54%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	475 FIT	139 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)		515	
Fail detected (int. diag.)	256		
Fail high (inherently)	259		259
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		116	116
MTBF = MTTF + MTTR		111 years	111 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	515 FIT	216 FIT	76%	9%	70%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	515 FIT	167 FIT	16 FIT	216 FIT	76%	76%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	531 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	259 FIT	216 FIT	76%	62%	55%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	259 FIT	167 FIT	572 FIT	216 FIT	76%	61%	73%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	531 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)		398	
Fail detected (int. diag.)	197		
Fail high (inherently)	201		201
Fail Low (detected by the logic solver)			212
Fail detected (int. diag.)	197		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		199	199
No Effect		122	122
Annunciation Undetected		4	4
Not part		116	116
MTBF = MTTF + MTTR		134 years	134 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	398 FIT	199 FIT	73%	10%	66%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	398 FIT	126 FIT	15 FIT	199 FIT	73%	75%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	413 FIT	126 FIT	0 FIT	199 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]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	212 FIT	126 FIT	201 FIT	199 FIT	73%	61%	51%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	201 FIT	126 FIT	212 FIT	199 FIT	73%	61%	51%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	413 FIT	126 FIT	0 FIT	199 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} = 8,70E-04	PFD_{AVG} = 4,34E-03	PFD_{AVG} = 8,65E-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)		454	
Fail detected (int. diag.)	237		
Fail high (inherently)	217		217
Fail Low (detected by the logic solver)			253
Fail detected (int. diag.)	237		
Fail low (inherently)	16	16	
Fail Dangerous Undetected		219	219
No Effect		151	151
Annunciation Undetected		4	4
Not part		116	116
MTBF = MTTF + MTTR		119 years	119 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	155 FIT	454 FIT	219 FIT	74%	9%	67%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	454 FIT	155 FIT	16 FIT	219 FIT	74%	74%	7%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	470 FIT	155 FIT	0 FIT	219 FIT	74%	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]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	253 FIT	155 FIT	217 FIT	219 FIT	74%	61%	50%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	217 FIT	155 FIT	253 FIT	219 FIT	74%	58%	53%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	470 FIT	155 FIT	0 FIT	219 FIT	74%	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} = 9,59E-04	PFD_{AVG} = 4,78E-03	PFD_{AVG} = 9,54E-03

abb 03-09-13 r001 v3r0.doc, October 9, 2007
Page 7 of 11

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		125	125
Annunciation Undetected		1	1
Not part		116	116
MTBF = MTTF + MTTR		49 years	49 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	1510 FIT	558 FIT	74%	11%	73%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	1510 FIT	126 FIT	15 FIT	558 FIT	74%	92%	3%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	1525 FIT	126 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	126 FIT	1300 FIT	558 FIT	74%	64%	70%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	1300 FIT	126 FIT	225 FIT	558 FIT	74%	91%	29%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	1525 FIT	126 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

© exida.com GmbH
Stephan Aschenbrenner

abb 03-09-13 r001 v3r0.doc, October 9, 2007
Page 8 of 11

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)		783	
Fail detected (int. diag.)	227		
Fail high (inherently)	556		556
Fail Low (detected by the logic solver)			242
Fail detected (int. diag.)	227		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		303	303
No Effect		116	116
Annunciation Undetected		4	4
Not part		118	118
MTBF = MTTF + MTTR		85 years	85 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	120 FIT	783 FIT	303 FIT	75%	11%	72%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	783 FIT	120 FIT	15 FIT	303 FIT	75%	86%	5%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	798 FIT	120 FIT	0 FIT	303 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
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	242 FIT	120 FIT	556 FIT	303 FIT	75%	65%	65%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	556 FIT	120 FIT	242 FIT	303 FIT	75%	82%	44%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	798 FIT	120 FIT	0 FIT	303 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} = 1,32E-03	PFD_{AVG} = 6,60E-03	PFD_{AVG} = 1,31E-02

abb 03-09-13 r001 v3r0.doc, October 9, 2007
Page 9 of 11

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)		380	
Fail detected (int. diag.)	184		
Fail high (inherently)	196		196
Fail Low (detected by the logic solver)			199
Fail detected (int. diag.)	184		
Fail low (inherently)	15	15	
Fail Dangerous Undetected		227	227
No Effect		115	115
Annunciation Undetected		1	1
Not part		114	114
MTBF = MTTF + MTTR		134 years	134 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	380 FIT	227 FIT	69%	11%	62%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	380 FIT	116 FIT	15 FIT	227 FIT	69%	77%	6%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	395 FIT	116 FIT	0 FIT	227 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
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	199 FIT	116 FIT	196 FIT	227 FIT	69%	64%	46%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	196 FIT	116 FIT	199 FIT	227 FIT	69%	63%	46%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	395 FIT	116 FIT	0 FIT	227 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} = 9,92E-04	PFD_{AVG} = 4,94E-03	PFD_{AVG} = 9,86E-03

abb 03-09-13 r001 v3r0.doc, October 9, 2007
Page 10 of 11

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 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 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.

ABB has Sales & Customer Support
expertise in over 100 countries worldwide.

www.abb.com/pressure

Printed in the Fed. Rep. of Germany (02.2008)

3KXP200007R4801

SM/265/7/9/SIL-EN Rev. 03

ABB Limited
Howard Road, St. Neots
Cambridgeshire, PE19 8EU
UK
Tel: +44 (0)1480 475 321
Fax: +44 (0)1480 217 948

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

ABB Automation Products GmbH
Schillerstr. 72
32425 Minden
Germany
Tel: +49 551 905-534
Fax: +49 551 905-555
CCC-support.deapr@de.abb.com