ABB MEASUREMENT & ANALYTICS | SAFETY MANUAL

261GS/GC/GG/GJ/GM/GN/GR 261AS/AC/AG/AJ/AM/AN/AR

Pressure transmitters

Engineered solutions for all applications

Measurement made easy

—

261Gx, 261Ax

Introduction

The 2600T family provides comprehensive range of top quality pressure measurement products, specifically designed to meet the widest range of applications ranging from arduous conditions in offshore oil and gas to the laboratory environment of the pharmaceutical industry.

This document has to be read in conjuction with 261 operating manuals.

For more information

Further publications for 2600T series pressure products are available for free download from www.abb.com/pressure

Models 261GS/GC/GG/GJ/GM/GN/GR
Models 261AS/AC/AG/AJ/AM/AN/AR

SIL-Safety Instructions
SM/261/SIL-EN

Rev. E (= Rev. 05)
Issue date: 12.2018

Translation of the original instruction

Contents

1 Application area

Absolute or gauge pressure measurement that shall meet the safety requirements according to IEC 61508.
The operative limits are described in the Data Sheet SS/261GS/AS.

2 Acronyms and abbreviations

Acronym / Abbreviation	Designation	Description
HFT	Hardware Fault Tolerance	The hardware fault tolerance of the device. This is the capability of a functional unit to continue the execution of the demanded function in case of faults or deviations.
MTBF	Mean Time Between Failures	This is the mean time period between two failures.
MTTR	Mean Time To Repair	This is the mean time period between the occurrence of a failure in a device or system and its repair.
PFD	Probability of Failure on Demand	This is the likelihood of dangerous safety function failures occurring on demand.
PFD_{AVG}	Average Probability of Failure on Demand	This is the average likelihood of dangerous safety function failures occurring on demand.
SIL	Safety Integrity Level	The international standard IEC 61508 specifies four discrete safety integrity levels (SIL 1 to SIL 4). Each level corresponds to a specific probability range regarding the failure of a safety function. The higher the safety integrity level of the safety-related systems, the lower likelihood of non-execution of the demanded safety functions.
SFF	Safe Failure Fraction	The fraction of non-hazardous failures, i.e. the fraction of failures without the potential to set the safety-related system to a dangerous or impermissible state.
Low demand mode	Low demand mode of operation	Measuring mode with low demand rate. Measuring mode, in which the demand rate for the safety-related system is not more than once a year and is not greater than double the frequency of the periodic test.
DCS	Distributed Control System	Control systems that are used in industrial engineering applications to monitor and control distributed equipment.
HMI	Human Machine Interface	Here, the HMI is the combined module consisting of LCD and local keypad.
DTM	Device Type Manager	The DTM is a software module that provides functions for accessing device parameters, configuring and operating the devices and diagnosing problems. By itself, a DTM is not executable software. It only 'comes to life' in an so called FDT 'container' program.
LRV	Device Configuration	Lower Range Value of the measurement range
URV	Device Configuration	Upper Range Value of the measurement range
Multidrop	Multidrop mode	In multidrop mode, up to 15 field devices are connected in parallel to a single wire pair. The analog current signal serves just to energize the two-wire devices providing a fixed current of 4mA.

3 Standards and definitions of terms

3.1 Standard IEC 61508 2000 (Edition 1), Part 1 to 7

— English
  Functional safety of electrical / electronic / programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices).

— German
  Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme (Zielgruppe: Hersteller und Lieferanten von Geräten).

3.2 Dangerous failure

A failure that has the potential to place the safety-related system in a dangerous state or render the system inoperative.

3.3 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.

3.4 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

4 Safety function

The transmitters 261G / 261A produces an analog signal (4 ... 20 mA) proportional to the absolute or gauge pressure. All safety functions exclusively refer to this output.
The total valid range of the output signal shall be configured to a minimum of 3.8 mA and a maximum of 20.5 mA (Factory Default).

4.1 Alarm response and current output

In case of detected critical faults the configured alarm current will be produced - this is fed to a subsequent logic unit, e.g. a DCS and monitored for violation of a defined maximum value.
There are two selectable modes for this alarm current:

- HIGH ALARM (Max Alarm current) which is the factory default setting
- LOW ALARM (Min Alarm current)

The low alarm current is configurable from 3.5 to 4.0 mA with a factory default setting to 3.5 mA.
The high alarm current is configurable from 20.0 mA to 23.6 mA with a factory default setting 21 mA.
The reaction time after the occurrence of a critical error until the output of the alarm current
amounts to ≤ 2 min.
In the following cases a detected failure will be immediately signalled within the LOW ALARM range independent from the configured alarm current:

- Program execution error
- Memory Error (Non Volatile Data, RAM, ROM)

WARNING!
For a safe fault monitoring the following conditions must be fulfilled:

- The LOW ALARM must be configured with a value ≤ 3.6 mA.
- The HIGH ALARM must be configured with a value ≥ 21 mA.
- The DCS must be capable of recognizing the configured High Alarms or Low Alarms as a malfunction detection.

WARNING!
For a safe current output operation the terminal voltage at the device must be given from 11 V DC to 42 V DC.

The DCS loop must be capable to provide the required voltage level even if the current output operates on the configured HIGH ALARM.
The device is not safety compliant during the following conditions:

- During Configuration
- If the HART Multidrop mode is activated
- During Simulation
- During Test of the safety function

WARNING!
The safety function of the devices includes the basic device with main electronics, sensor electronics and sensor through to the sensor diaphragm and directly fitted process connection.

The fraction of failures without the potential to put the device into a dangerous function status is given by the SFF value shown in chapter “Safety engineering parameters”.

4.2 Total Safety Accuracy

The defined value for the “Total Safety Accuracy“ of the safety function of this device is:
±2 % of URL (Upper Range Limit)
See appropriate Data Sheet SS/261GS/AS, SS/261GC/AC or SS/261GR/AR for the base accuracy specifications of this device.

4.3 Turn on time

After a power-up of the device, the signal can be considered to be safe after 2 minutes.

5 Applicable device documentation

For the transmitters of the models 261Gx / 261Ax the following documents must be observed:

- Operating Instructions IM/261Gx/Ax
- Data Sheet SS/261GS/AS or SS/261GC/AC or SS/261GR/AR + SS/S261
- Online Help for Device Type Manager for Transmitter Series 2600T (261)

6 Recurring tests

6.1 Safety inspections

The safety function for the entire safety loop must be checked regularly in accordance with IEC 61508. The inspection intervals are defined when calculating the individual safety loops for a system.

The operator is responsible for selecting the type of check and the intervals within the specified period (see the PFDAV value which depends on the selected maintenance interval).

Inspections must be conducted in a manner that enables users to verify the proper function of the safety equipment in combination with all components.

One possible procedure for recurring tests to detect hazardous and unidentified device errors is described in the following section.

6.2 Safety Function check

For check the safety function of the device proceed as follows:

1. Bridge the safety DCS or take other appropriate measures to prevent inadvertent triggering of alarms.
2. Deactivate the write lock (see Chapter “Configuration”).
3. Set the current output of the transmitter to a HIGH-ALARM value by means of the DTM Simulation command (Sequence Diagnostics/Simulation/Current Output).
4. Check whether the current output signal reaches this value.
5. Set the current output of the transmitter to a LOW-ALARM value by means of the DTM Simulation command
6. Check whether the current output signal reaches this value.
7. Activate the write lock (see Chapter “Configuration”) and wait 10 seconds.
8. Restart the device by power down.
9. Compare the applied pressure for LRV (lower range value, 4 mA) and URV (upper range value, 20 mA) with the measured pressure (current output).
10. Remove the bridging of the safety DCS or restore normal operation in another way.
11. After the test has been performed, the results must be documented and stored in a suitable manner.

6.3 Expected service life of the components used

The applied failure rates of the components are valid within the usable service life according to IEC 61508-2 section 7.4.7.4 note 3.

6.4 Repair

Defective devices should be returned to the ABB service and repair department, possibly with the type of malfunction and possible reason stated.

Use the original packaging or a suitably secure packaging for returning the device for repair or for recalibration. Include the properly filled out return form with the device (see appendix).

According to EC guidelines for hazardous materials, the owner of hazardous waste is responsible for its disposal or must observe the following regulations for its shipping:

All delivered devices to ABB Automation Products GmbH must be free from any hazardous materials (acids, alkali, solvents, etc.).

When ordering spare units please notify the serial number (on the type plate of the original device).

Please contact Customer Center Service acc. to page 2 for nearest service location.

7 Configuration

This device is configured and tested as specified by the customer order.
Nevertheless this device can be configured by the local HMI or DTM via HART® Interface. Other configuration tools like Handheld Terminals are not described in this manual.
During this configuration a safe operation of the device shall not be granted.

IMPORTANT (NOTE)
Checks:
- Before the first start-up of the device as a part of a safety function check that the device configuration fulfills the safety function of the system.
- Check that the right device is installed on the right measuring point.
- After every change to the device as a part of a safety function, such as a change to the installation position of the device or configuration, the safety function of the device shall be checked.
- After the safety function has been checked, the operation of the device must be locked because a change to the measuring system or parameters can compromise the safety function.

The device must be write-protected for the safety operation.
This could be realized in the following steps:

7.1 Enabling / Disabling the Write Locking

1. Write Locking via local HMI:
   Select the menu sequence “Device Setup”, “Write Protect” and than “Yes”.
2. Write Locking via DTM:
   Select the menu sequence “Configure”, “Basic Parameters”, “Write Protection” and select “Device write locked”.
   If the device is locked (write-protected) it cannot be configured. This protection refers to the entire device.

WARNING!
The software write lock does not lock again automatically. It is released until it is explicitly set back.

IMPORTANT (NOTE)
Checks:
The write protection shall be verified in the following way:
1. If the locking was done via local HMI:
   - Check, that the Lock-symbol is displayed on the local LCD.
   - Select the menu “Device Setup_Offset” and check that the Edit-symbol is not shown on the LCD
   - Check, that pressing the Edit-key has no reaction on the LCD
2. If the locking was done via DTM:
   - HMI is available: check like described under 1.
   - No local HMI is available (checking of write protection):
     Select the menu sequence “Configure_Pressure Measurement_Pressure_Output Parameters” and change e.g. the Damping value. Then select “Device_Save to device” and check that a message occurs with the content “Write protected”.

7.2 Zero and Span adjustment with local key

The device can be also be configured via a local key button on the electronic system for adjust zero and span. To access the adjusting key on the electronic system the housing cover must be unscrewed. The key is located in a bore hole and can be pressed with a small pin or screwdriver (see Operating Instructions IM/261Gx/Ax).

WARNING!
This local key is not write protected by the locking mechanism described above!

7.3 Diagnostic Configuration

The diagnosis configuration of this device is safety compliant and includes the following failure detections:

Diagnosis Detection
Pressure Sensor Measurement Failure
Sensor Temperature Measurement Failure
Sensor Board Failure
ADC Failure
Electronic Temperature Measurement Failure
EEPROM Defect
EEPROM Data defect
Sensor Board Communication Error
Invalid Floating Point Calculation
RAM, ROM Failure (not configurable)
Program Execution Failure (not configurable)

This failure configuration is password protected and cannot be changed by the operator.

7.4 Configuration parameters that have an influence on the safety function

The following table shows parameters which could be changed via local HMI or DTM and may have an influence in the safety function of this device:

Device Parameter	Description	DTM Parameter	HMI Parameter	Valid Range	Safety Instruction
Write Protection	Write access to the entire device is locked	<Basic Parameters> <General> <Write Protection>	<Device Setup> <Write Protect>	HMI: Yes = Locked No = unlocked	Locked required for safety function
HART Polling Address	Address used for Multidrop mode	<SMART VISION> <Set slave address>	-/-	0 … 15	Only address 0 is allowed
PV Damping Value	PT1 Filter for the Primary Variable Pressure	<Pressure Measurement> <Output Parameters> <Damping>	<Device Setup> <Damping>	0 ... 60 s	Check Safety Function
Lower Range Value	The lowest value of the measured value to which the transmitter is adjusted	<Pressure Measurement> <Scaling > <Lower Range Value>	<Device Setup> <Apply PV> <Lower Range Value>	Sensor Limits -5 %	Check Safety Function
		<Device Setup> <Set PV> <Lower Range Value>	<Device Setup> <Set PV> <Lower Range Value>		
Upper Range Value	The highest value of the measured value to which the transmitter is adjusted	<Pressure Measurement> <Scaling > <Upper Range Value>	<Device Setup> <Apply PV> <Upper Range Value>	Sensor Limits +5 %	Check Safety Function
		<Device Setup> <Set PV> <Upper Range Value>	<Device Setup> <Set PV> <Upper Range Value>		
Offset Shift	Parallel shift of Lower Range and Upper Range Value	<Pressure Measurement> <Parallel Shift>	<Device Setup> <Offset>	New Range within Sensor Limits +/-5 %	Check Safety Function
Current Alarm Selection	High Alarm or Low Alarm Selection	<Basic Parameters> <Current> <Alarm Current>	<Device Setup> <Fault Current>	Upscale =High Alarm Downscale =Low Alarm	Check Safety Function
Low Alarm Current	Value which is active for low Alarm	<Basic Parameters> <Current> <Alarm Current>	-/-	3.5 … 4 mA	only 3.5 and 3.6 mA are allowed
High Alarm Current	Value which is active for High Alarm	<Basic Parameters> <Current> <Alarm Current>	-/-	20 … 23.6 mA	only values greater 21 mA are allowed

Device Parameter	Description	DTM Parameter	HMI Parameter	Valid Range	Safety Instruction
Minimum Current	Current value which is used for the lower range value	<Basic Parameters> <Current> <Minimum Current>	-/-	3.5 … 4 mA	Only values between 3.8 and 4 mA are allowed
Maximum Current	Current value which is used for the upper range value	<Basic Parameters> <Current> <Maximum Current>	-/-	20 … 23.6 mA	Only values between 20 mA and 20.5 mA and are allowed
Zero Shift	Zero adjustment of the measuring cell	<Pressure Measurement> <Zero Shift>	<Calibrate> <Zero Trim>	Execute function	Check Safety Function
Factory Reset	Restores the configuration data to the values set at factory	<Device> <Reset> <Reset to factory default>	<Device Setup> <Factory Reset>	Execute function	Check Safety Function
Current Simulation	Forces the Current Output Signal	<Diagnostics> <Simulate> <Current Output>	-/-	3.5 ... 23.6 mA	Check, that simulation is deactivated or perform a Reset
Device Reset	Performs a Reset of the device	<Device> <Reset> <Warm start>	-/-	Execute function	Same as after power lost
Calibrate Current Output	Calibrates the 4 mA and 20 mA Point of the Current Output	<Calibrate> <Current> <Adjust 4 mA> <Adjust 20 mA>	-/-	+/- 0.5 mA from current value	Check Safety Function
Diagnosis Simulation	Forcing of the Diagnostic States	<Diagnostics> <Simulate> <Device Status>	-/-	Execute function	Check, that simulation is deactivated or perform a Reset
Pressure Calibration Lower Point	Calibrates the pressure sensor measurement	<Calibrate> <Pressure> <Lower Balance Point>	-/-	Sensor Limits -10 %	Check Safety Function
Pressure Calibration Upper Point	Calibrates the pressure sensor measurement	<Calibrate> <Pressure> <Upper Balance Point>	-/-	Sensor Limits +10 %	Check Safety Function
Installation angle	Configuration of mounting angle	<Device Setup> <Installation angle>	<Device Setup> <Installation angle>	0 degrees 45 degrees 90 degrees 135 degrees 180 degrees	Check Safety Function

8 Safety engineering parameters

8.1 Models 261GS and 261AS.

For all other models the relevant values for diaphragm seals has to be added, see next paragraph.

Term	Value	
Safety Device	2600T Model 261	
Valid software version	1.5.1	
Valid hardware version	1.05 , 1.06	
Type of Assessment	Full IEC 61508 assessment	
SIL capability	2	
HFT	0	
Component Type	B	
Measuring mode	Low demand mode	
Transmitter Sensor Code	2600T Model 261 xx ranges C, F, L, D, U, R, V with metallic diaphragm	2600T Model 261 xx ranges C, F with ceramic diaphragm
SFF	95 %	94 %
PFDAVG for T [Proof] = 1 year	1.03E-04	1.57E-04
PFDAVG for T [Proof] = 5 years	5.13E-04	7.85E-04
PFDAVG for T [Proof] = 10 years	1.03E-03	1.57E-03
λSD	0 FIT	0 FIT
λSU [1]	108 FIT	143 FIT
λDD	402 FIT	464 FIT
λDU	23 FIT	36 FIT

[1] Note that the SU category includes faiulures that do not cause a spurious trip

8.2 Diaphragm seals

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the diaphragm seals S261.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or sause operation different from the design analyzed.
- Materials are compatible with process conditions and process fluids.
- The mean time to restoration (MTTR) alter a safe failure is 24 hours.
- The Remote Seals S261 are installed per manufacturer's instructions.
- The stress levels are average for an industrial outdoor environment and for the process wetted parts with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.

The calculated numbers consider the worst-case configuration of the remote seals. The influence of the ambient temperature on remote seals especially with capillaries should carefully be considered and are not included as part of this analysis. Further information about the possible impact of diaphragm seals on the features of the pressure transmitter is described in ABB datasheets.

The FMEDA carried out on the diaphragm seals S261 for high trip applications (“high trip" corresponds to applications where the alarm level is reached by an increasing pressure level) leads under the above assumptions to the following failure rates.

	Normal service	Severe service (abrasive particles exist in the process fluid / material)
Fail Safe (λ_{safe})	0 FIT	0 FIT
Fail Dangerous ($\lambda_{dangerous}$)	58 FIT	94 FIT
No effect	1 FIT	1 FIT
External leakage	5 FIT	6 FIT
Total failure rate (safety function)	58 FIT	94 FIT
SFF[1]	---	---
SIL AC[2]	---	---

The FMEDA carried out on the diaphragm seals S261 for low trip applications (“low trip" corresponds to applications where the alarm level is reached by a decreasing pressure level) leads under the above assumptions to the following failure rates.

	Normal service	Severe service (abrasive particles exist in the process fluid / material)
Fail Safe (λ_{safe})	58 FIT	94 FIT
Fail Dangerous ($\lambda_{dangerous}$)	0 FIT	0 FIT
No effect	1 FIT	1 FIT
External leakage	5 FIT	6 FIT
Total failure rate (safety function)	58 FIT	94 FIT
SFF[1]	---	---
SIL AC[2]	---	---

[1] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction
[2] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

9 Appendix

Statement on the contamination of devices and components

Repair and / or maintenance work will only be performed on devices and components if a statement form has been completed and submitted.
Otherwise, the device / component returned may be rejected. This statement form may only be completed and signed by authorized specialist personnel employed by the operator.

Customer details:

Company:

Address:

Contact person: Telephone:

Fax: E-Mail:

Device details:

Typ: Serial no.:

Reason for the return/description of the defect:

Was this device used in conjunction with substances which pose a threat or risk to health?

□ Yes □ No

If yes, which type of contamination (please place an X next to the applicable items)?

Biological	□	Corrosive / irritating	□	Combustible (highly / extremely combustible)	□
Toxic	□	Explosiv	□	Other toxic substances	□
Radioactive	□				

Which substances have come into contact with the device?

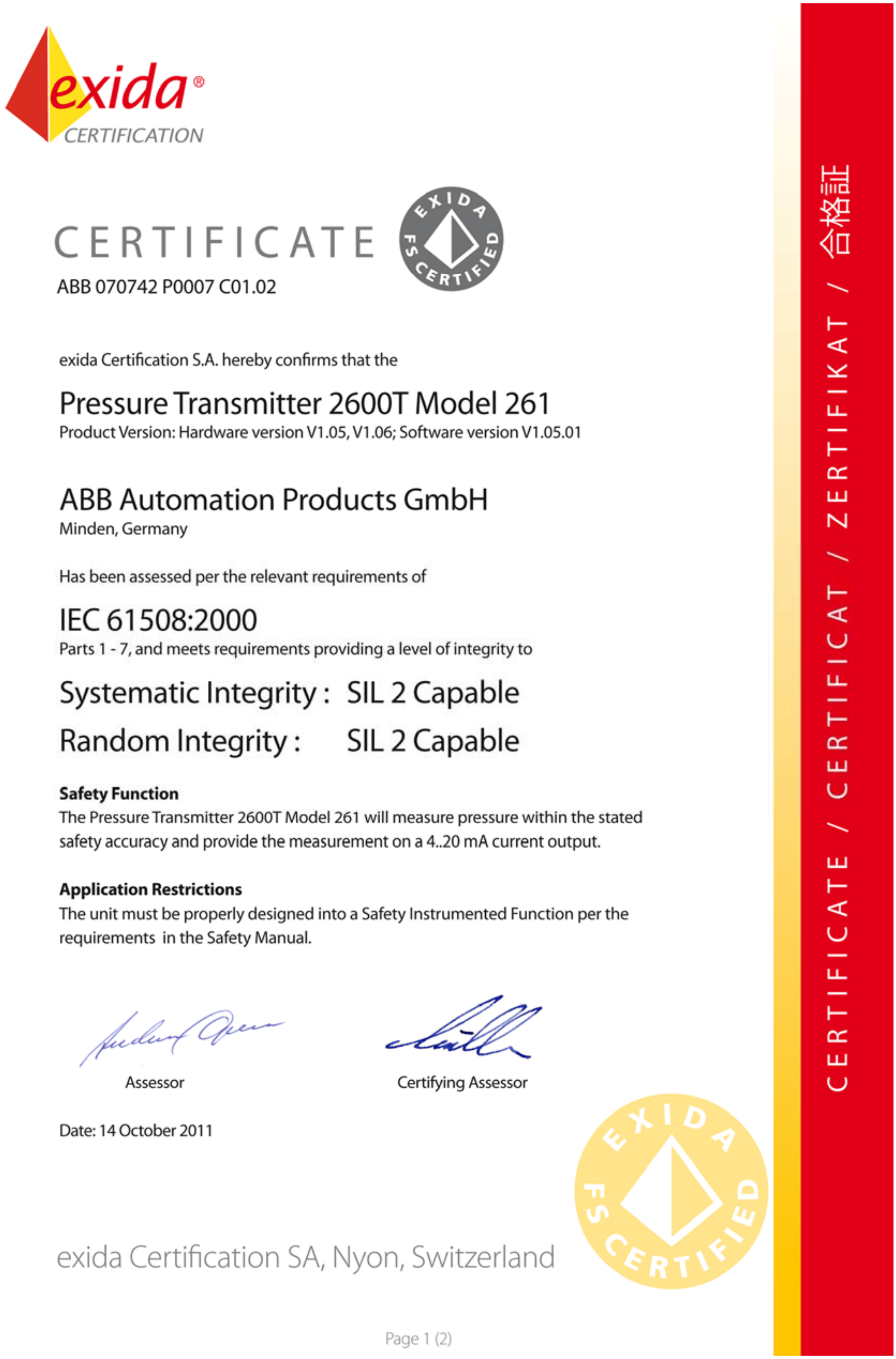
1.

2.

3.

We hereby state that the devices / components shipped have been cleaned and are free from any dangerous or poisonous substances.

Town/city, date Signature and company stamp



exida CERTIFICATION

CERTIFICATE

EXIDA FS CERTIFIED

ABB 070742 P0007 C01.02

exida Certification S.A. hereby confirms that the

Pressure Transmitter 2600T Model 261

Product Version: Hardware version V1.05, V1.06; Software version V1.05.01

ABB Automation Products GmbH

Minden, Germany

Has been assessed per the relevant requirements of

IEC 61508:2000

Parts 1 - 7, and meets requirements providing a level of integrity to

Systematic Integrity :	SIL 2 Capable
Random Integrity :	SIL 2 Capable

Safety Function

The Pressure Transmitter 2600T Model 261 will measure pressure within the stated safety accuracy and provide the measurement on a 4..20 mA current output.

Application Restrictions

The unit must be properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

Assessor

Certifying Assessor

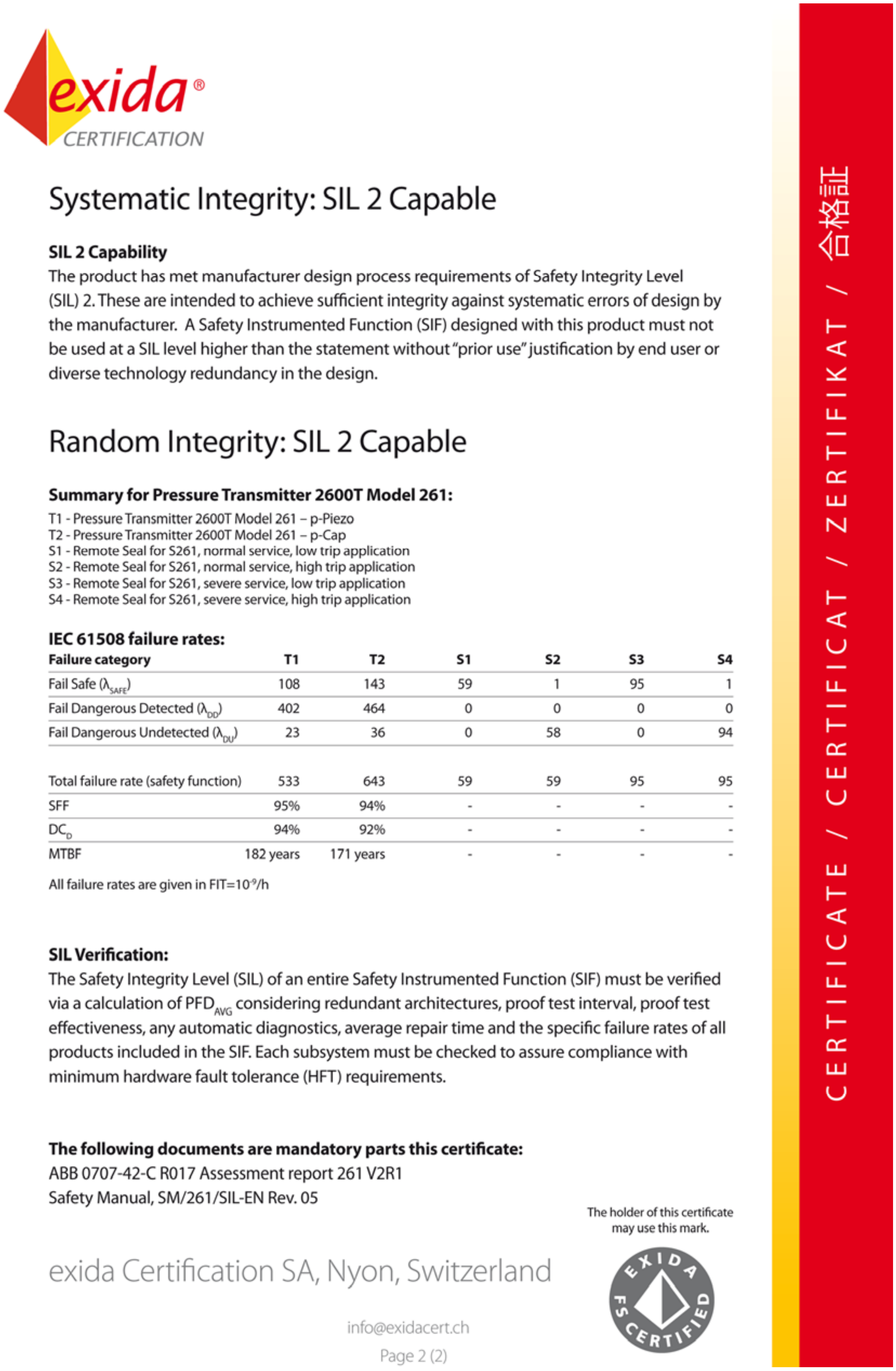
Date: 14 October 2011

exida Certification SA, Nyon, Switzerland

EXIDA FS CERTIFIED

Page 1 (2)

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証



exida® CERTIFICATION

Systematic Integrity: SIL 2 Capable

SIL 2 Capability

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 2. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than the statement without "prior use" justification by end user or diverse technology redundancy in the design.

Random Integrity: SIL 2 Capable

Summary for Pressure Transmitter 2600T Model 261:

T1 - Pressure Transmitter 2600T Model 261 – p-Piezo
T2 - Pressure Transmitter 2600T Model 261 – p-Cap
S1 - Remote Seal for S261, normal service, low trip application
S2 - Remote Seal for S261, normal service, high trip application
S3 - Remote Seal for S261, severe service, low trip application
S4 - Remote Seal for S261, severe service, high trip application

IEC 61508 failure rates:

Failure category	**T1**	**T2**	**S1**	**S2**	**S3**	**S4**
Fail Safe (λ_{SAFE})	108	143	59	1	95	1
Fail Dangerous Detected (λ_{DD})	402	464	0	0	0	0
Fail Dangerous Undetected (λ_{DU})	23	36	0	58	0	94
Total failure rate (safety function)	533	643	59	59	95	95
SFF	95%	94%	-	-	-	-
DC_D	94%	92%	-	-	-	-
MTBF	182 years	171 years	-	-	-	-

All failure rates are given in FIT=10^{-9}/h

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are mandatory parts this certificate:

ABB 0707-42-C R017 Assessment report 261 V2R1
Safety Manual, SM/261/SIL-EN Rev. 05

The holder of this certificate may use this mark.

EXIDA FS CERTIFIED

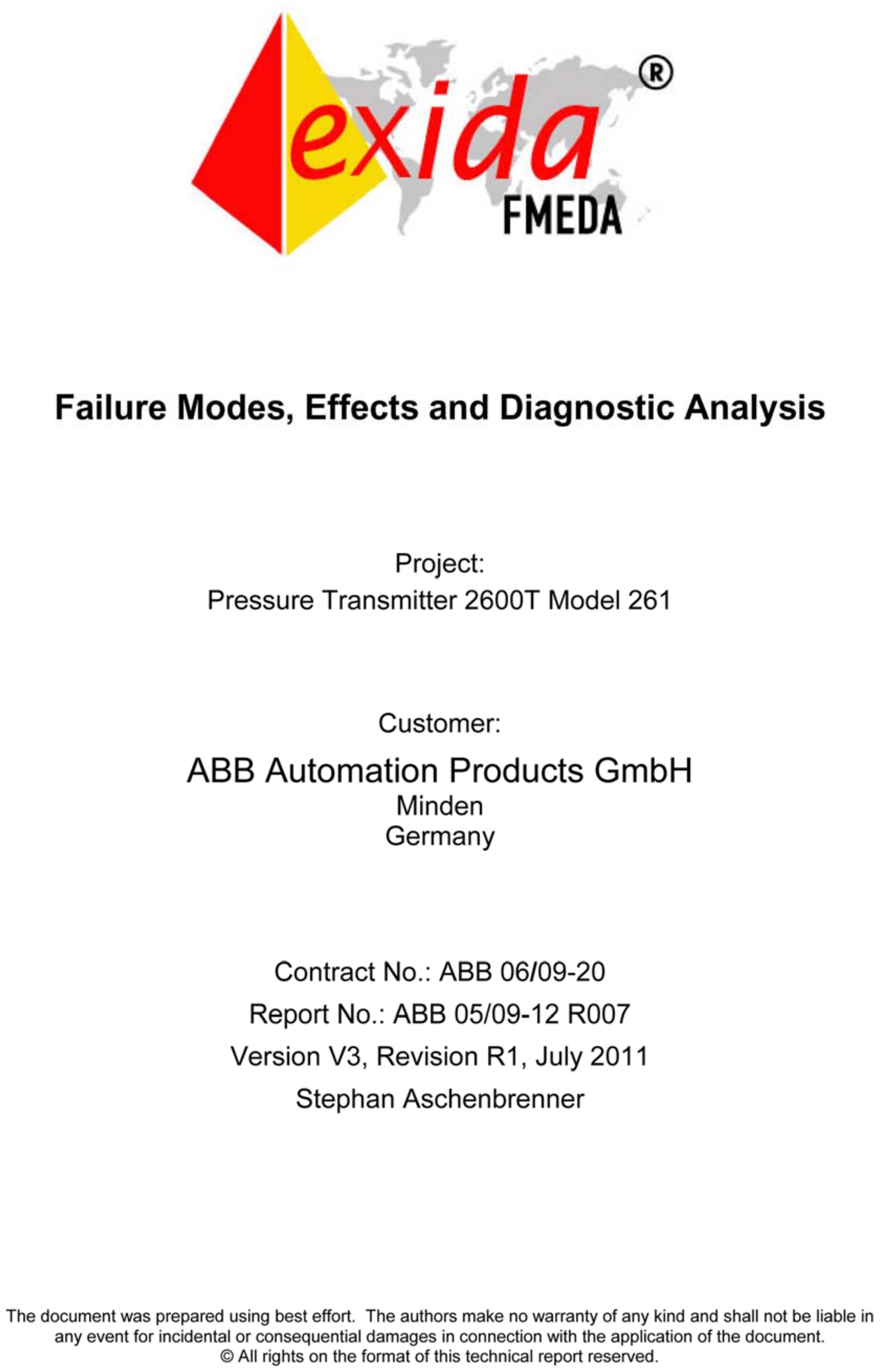
exida Certification SA, Nyon, Switzerland

info@exidacert.ch

Page 2 (2)

CERTIFICATE / CERTIFICAT / ZERTIFIKAT / 合格証

11 Management Summary



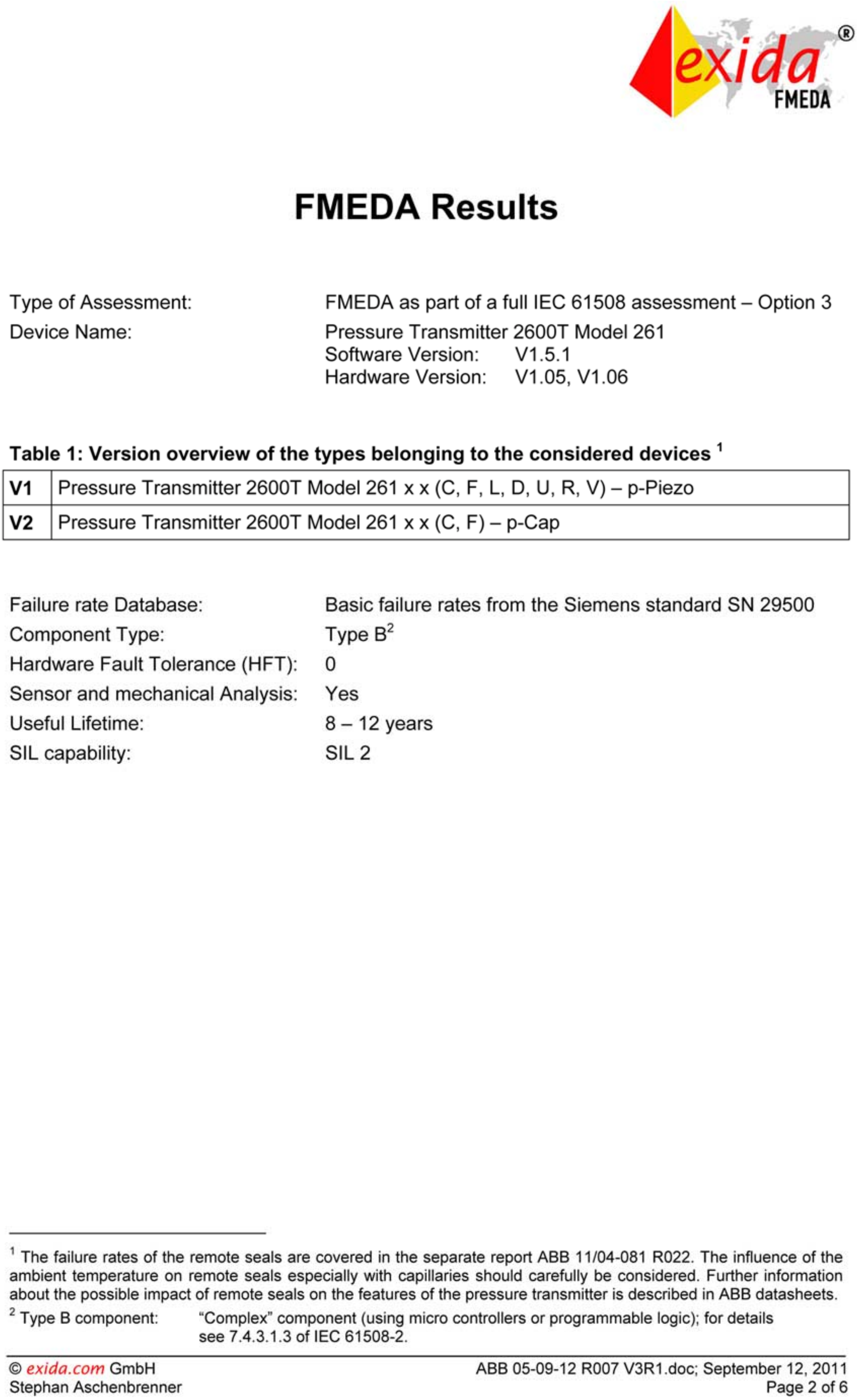
Failure Modes, Effects and Diagnostic Analysis

Project:
Pressure Transmitter 2600T Model 261

Customer:
ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 06/09-20
Report No.: ABB 05/09-12 R007
Version V3, Revision R1, July 2011
Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.



FMEDA Results

Type of Assessment:	FMEDA as part of a full IEC 61508 assessment – Option 3
Device Name:	Pressure Transmitter 2600T Model 261 Software Version: V1.5.1 Hardware Version: V1.05, V1.06

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

V1	Pressure Transmitter 2600T Model 261 x x (C, F, 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 B[2]
Hardware Fault Tolerance (HFT):	0
Sensor and mechanical Analysis:	Yes
Useful Lifetime:	8 – 12 years
SIL capability:	SIL 2

[1] The failure rates of the remote seals are covered in the separate report ABB 11/04-081 R022. The influence of the ambient temperature on remote seals especially with capillaries should carefully be considered. Further information about the possible impact of remote seals on the features of the pressure transmitter is described in ABB datasheets.

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

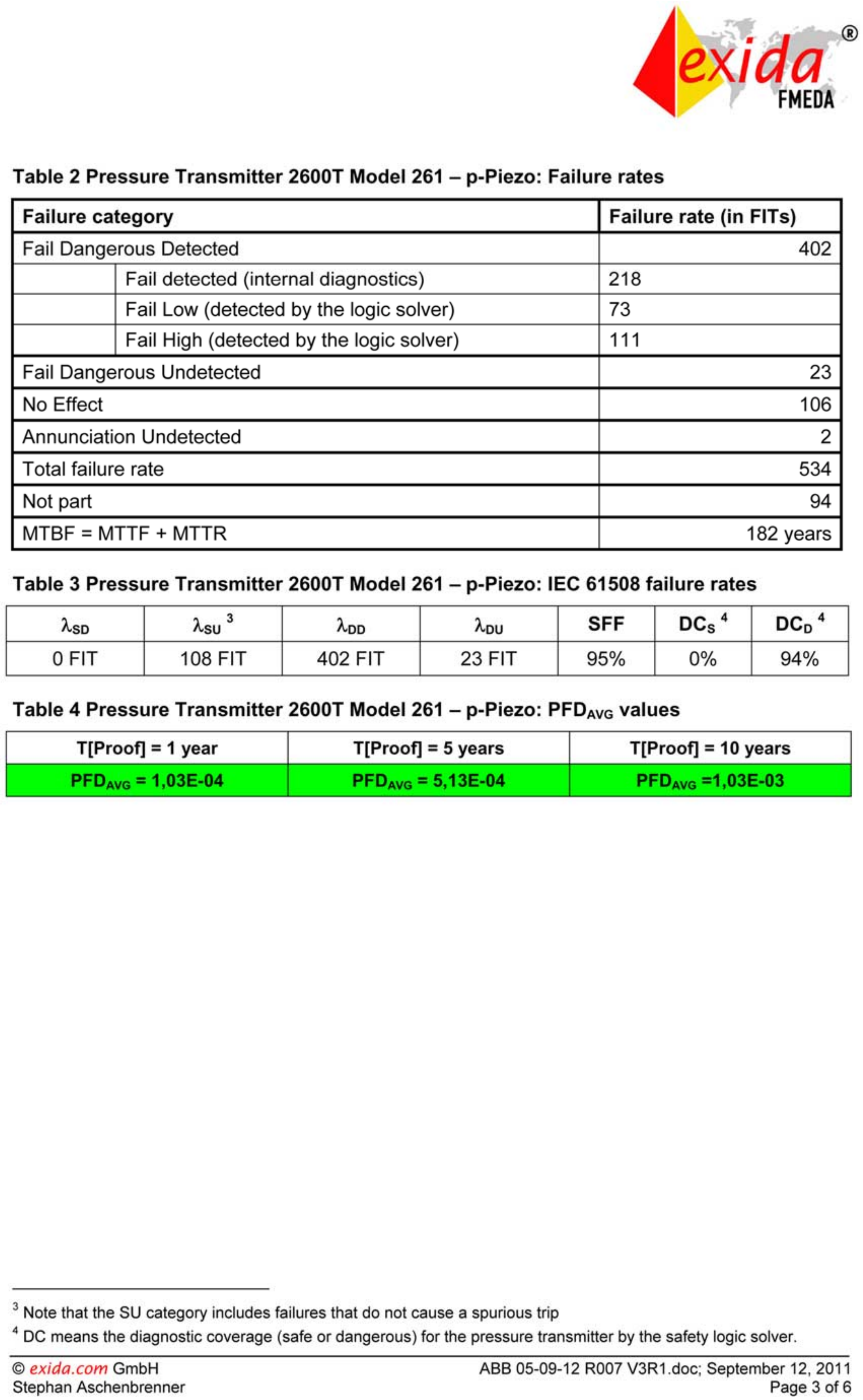


Table 2 Pressure Transmitter 2600T Model 261 – p-Piezo: Failure rates

Failure category		Failure rate (in FITs)
Fail Dangerous Detected		402
	Fail detected (internal diagnostics)	218
	Fail Low (detected by the logic solver)	73
	Fail High (detected by the logic solver)	111
Fail Dangerous Undetected		23
No Effect		106
Annunciation Undetected		2
Total failure rate		534
Not part		94
MTBF = MTTF + MTTR		182 years

Table 3 Pressure Transmitter 2600T Model 261 – p-Piezo: IEC 61508 failure rates

λ_{SD}	λ_{SU} [3]	λ_{DD}	λ_{DU}	SFF	DC_S [4]	DC_D [4]
0 FIT	108 FIT	402 FIT	23 FIT	95%	0%	94%

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} = 1,03E-04	PFD_{AVG} = 5,13E-04	PFD_{AVG} =1,03E-03

[3] Note that the SU category includes failures that do not cause a spurious trip

[4] 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		464
	Fail detected (internal diagnostics)	280
	Fail Low (detected by the logic solver)	73
	Fail High (detected by the logic solver)	111
Fail Dangerous Undetected		36
No Effect		141
Annunciation Undetected		2
Total failure rate		644
Not part		96
MTBF = MTTF + MTTR		154 years

Table 6 Pressure Transmitter 2600T Model 261 – p-Cap: IEC 61508 failure rates

λ_{SD}	λ_{SU} [5]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [6]	**DC_D** [6]
0 FIT	143 FIT	464 FIT	36 FIT	94%	0%	92%

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} = 1,57E-04	**PFD_{AVG} = 7,85E-04**	**PFD_{AVG} = 1,57E-03**

[5] Note that the SU category includes failures that do not cause a spurious trip

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

Appendix to the 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* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. 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}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

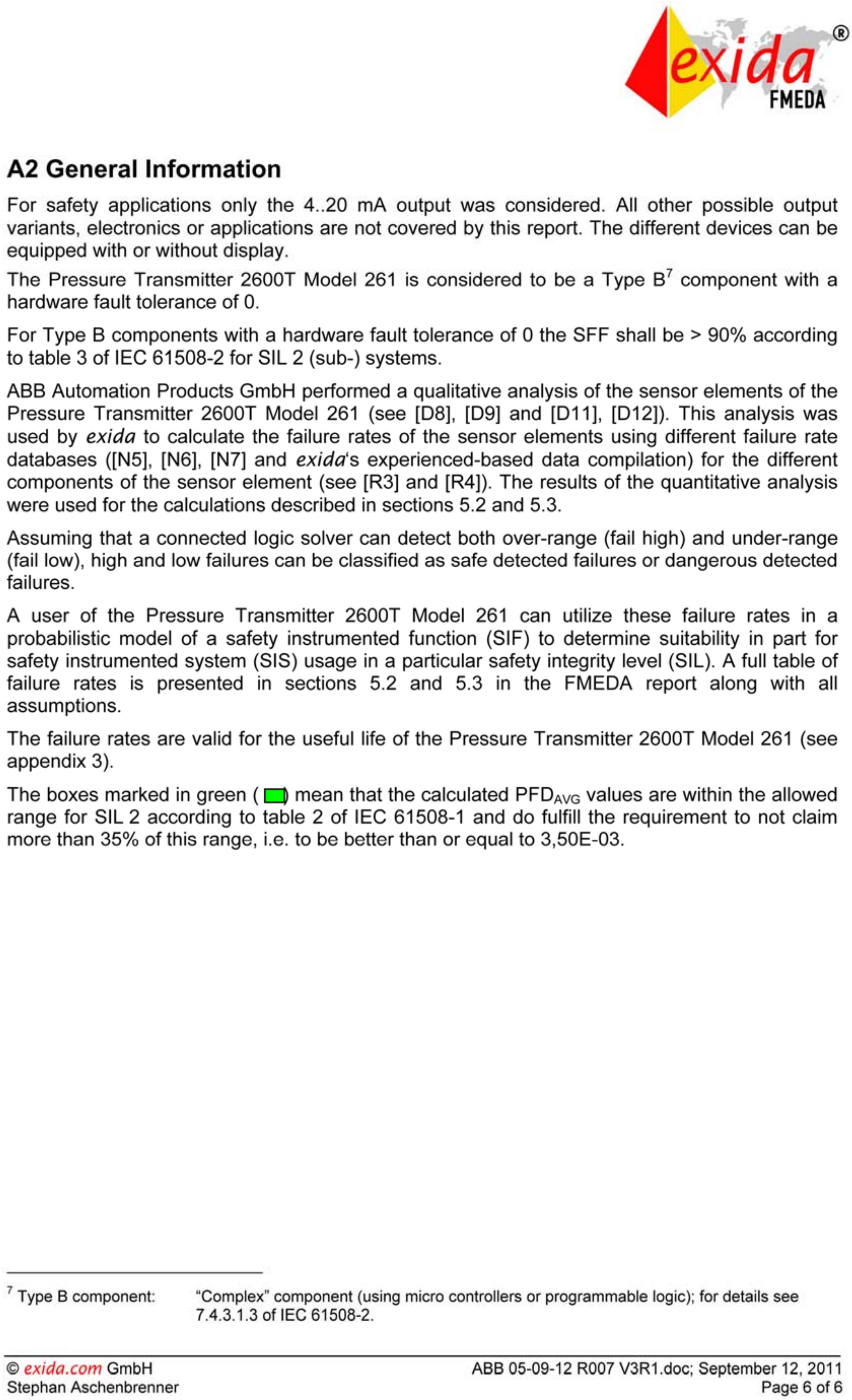
Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per 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* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.



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 B[7] 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 elements of the Pressure Transmitter 2600T Model 261 (see [D8], [D9] and [D11], [D12]). This analysis was used by *exida* to calculate the failure rates of the sensor elements using different failure rate databases ([N5], [N6], [N7] and *exida*'s experienced-based data compilation) for the different components of the sensor element (see [R3] and [R4]). The results of the quantitative analysis were used for the calculations described in sections 5.2 and 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 sections 5.2 and 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.

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

Failure Modes, Effects and Diagnostic Analysis

Project:
Remote Seals S261

Customer:
ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 11/04-081
Report No.: ABB 11/04-081 R022
Version V1, Revision R0; September 2011

Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management summary

This report summarizes the results of the mechanical assessment carried out on the Remote Seals S261 in the versions listed in the mechanical drawings referenced in section 2.4.1.

The mechanical 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) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

ABB Automation Products GmbH and *exida* together did a quantitative analysis of the Remote Seals S261 to calculate the failure rates using *exida*'s component database (see [N2]) for the different mechanical components.

The Remote Seals S261 are classified as Type A[1] elements with a hardware fault tolerance of 0.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

The following tables show the failure rates per IEC 61508:2010 for the worst case configurations of the considered Remote Seals S261.

Table 1: Remote Seals S261 for high trip applications [2] [3]

	Profile 3 / 4 [4]	
	Normal service	**Severe service**
Fail Safe (λ_{safe})	**0 FIT**	**0 FIT**
Fail Dangerous ($\lambda_{dangerous}$)	**58 FIT**	**94 FIT**
No effect	1 FIT	1 FIT
External leakage	5 FIT	6 FIT

Total failure rate (safety function)	**58 FIT**	**94 FIT**
SFF [5]	**---**	**---**

SIL AC [6]	**---**	**---**

[1] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

[2] "high trip" corresponds to applications where the alarm level is reached by an increasing pressure level.

[3] The calculated numbers consider the worst-case configuration of the remote seals. The influence of the ambient temperature on remote seals especially with capillaries should carefully be considered and are not included as part of this analysis. Further information about the possible impact of remote seals on the features of the pressure transmitter is described in ABB datasheets.

[4] See appendix 3 for detailed definitions. Profile 4 was used for the process wetted parts.

[5] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction.

[6] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table 2: Remote Seals S261 for low trip applications [7] [8]

	Profile 3 / 4 [9]	
	Normal service	**Severe service**
Fail Safe (λ_{safe})	**58 FIT**	**94 FIT**
Fail Dangerous ($\lambda_{dangerous}$)	**0 FIT**	**0 FIT**
No effect	1 FIT	1 FIT
External leakage	5 FIT	6 FIT

Total failure rate (safety function)	**58 FIT**	**94 FIT**
SFF [10]	**---**	**---**

SIL AC [11]	**---**	**---**

A user of the considered Remote Seals S261 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).

The failure rates are valid for the useful life of the considered Remote Seals S261 (see Appendix 2) when operating as defined in the considered scenarios.

[7] "low trip" corresponds to applications where the alarm level is reached by a decreasing pressure level.

[8] The calculated numbers consider the worst-case configuration of the remote seals. The influence of the ambient temperature on remote seals especially with capillaries should carefully be considered and are not included as part of this analysis. Further information about the possible impact of remote seals on the features of the pressure transmitter is described in ABB datasheets.

[9] See appendix 3 for detailed definitions. Profile 4 was used for the process wetted parts.

[10] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction.

[11] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

ABB Ltd.
Measurement & Analytics
Howard Road St. Neots
Cambridgeshire PE19 8EU
UK
Tel: +44 (0)1480 475321
Fax: +44 (0)1480 217948

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

ABB S.p.A.
Measurement & Analytics
Via Luigi Vaccani 4
22016 Tremezzina (CO)
Italy
Tel: +39 0344 58111

abb.com/pressure

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB.