

2007-03-28

Automation, Software and Information Technology

**Test report about
the type approval of the
2600T Series Pressure Transmitter
Model: 268, release 2
of ABB SACE S.p.A.**

**Report-No.: 968/EZ 251.00/07
Date: 2007-03-28**

2007-03-28

**Test report about
the type approval of the
2600T Series Pressure Transmitter
Model: 268, release 2
of ABB SACE S.p.A.**

Report-No.: 968/EZ 251.00/07

Date: 2007-03-28

Pages: 12

Test object: 2600T Series Pressure Transmitter
Model: 268, release 2

Customer/Manufacturer: ABB SACE S.p.A
Via Statale 113
22016 Lenno (CO)
Italy

Order-No./Date: 3500096067/A01 dated 2004-08-18
3500102217/A01 dated 2004-10-27

Test Institute: TÜV Rheinland Industrie Service GmbH
Automation, Software and Information Technology (ASI)
Am Grauen Stein
51105 Köln
Germany

Department: Automation, Software and Information Technology (ASI)

TÜV-Offer-No./Date: 968/101/04 dated 2004-05-12
968/101a/04 dated 2004-09-23

TÜV-Order-No./Date: 9115604 dated 2004-09-02
9160443 dated 2004-11-04

Inspector: Dipl.-Ing. (FH) Oliver Busa

Test location: see Test Institute

Test duration: August 2004 - March 2007

The test results are exclusively related to the test samples.

This report must not be copied **in an abridged version** without the written permission of the Test Institute.

Contents	Page
1. Scope	4
2. Standards and previous test reports	4
3. Object of inspection	5
4. Tests and test results	6
4.1 General	6
4.2 General requirements	6
4.3 Safety requirements	7
4.4 Requirements resulting from application standards	7
4.5 Functional Safety Management	8
4.6 Review of the manufacturer documents	8
4.7 Measures to avoid systematic failures	8
4.8 Measures to control systematic and random faults in hardware and software	9
4.9 Review of the hardware architecture and design	9
4.10 Review of the software architecture and design	10
4.11 Review of the FMEA	10
4.12 Review of the reliability data and PFD/PFH calculations	10
4.13 Inspection of the electrical safety	11
4.14 Inspection of the environmental and EMC tests	11
5. Summary	12

1. **Scope**

Scope of this report is the type approval of the 2600T Series Pressure Transmitter model 268, release 2 of ABB SACE S.p.A.

The type approval should demonstrate that the safety related field device is suitable for risk reduction in applications that shall claim the safety integrity level 2 (SIL 2) in accordance to the IEC 61508.

Further it shall be shown that the test object can be used for risk reduction in applications that shall claim the safety integrity level 3 (SIL 3) in accordance to the IEC 61508 if the test object is used in a redundant configuration.

2. **Standards and previous test reports**

Functional Safety

- [1] IEC 61508:2000, parts 1 - 7
 Functional safety of electrical/electronic/programmable electronic safety related systems

Electrical safety and resistance against environmental conditions

- [2] EN 60068-2-6:1996
 Environmental Testing
 part 2: Test (Vibration)

Electromagnetic Compatibility

- [3] EN 55011/A2:2003
 Industrial, scientific and medical (ISM) radio-frequency equipment -
 Radio disturbance characteristics
- [4] EN 61000-6-2:2002
 Electromagnetic Compatibility (EMC)
 - Generic Standards
 - Immunity for Industrial Environments

Application Specific Standards

- [5] EN 61298-1:1996
 Process measurement and control devices -
 General Methods and procedures for evaluating performances
- [6] EN 60770-1:1997
 Transmitters for use in industrial-process control systems -
 Part 1: Methods for performance evaluation
- [7] ISA S84.01
 Application of safety instrumented systems for the process industry
- [8] NE 43
 Standardization of the signal level for the breakdown information of digital transmitters

Previous type approval reports

- [P1] Report-No.: AL63021C, Rev. 1.3 dated 2004-02-20, TÜV Süddeutschland Group - IQSE
- [P2] Statement FSM and Mechanical FMEA, dated 2004-09-24, TÜV Rheinland Group

3. Object of inspection

Test object of this approval is the 2600T Series Pressure Transmitter, model 268 release 2 of ABB SACE S.p.A. This safety related field device is an modified version of the already certified [P1] and field tested device.

The modifications consist of:

- modification of the primary electronics with two homogeneous redundant ASICs
- modification of the secondary electronics with enhanced supervision
- enhanced output stage with secondary shutdown
- second watchdog time with independent time-base
- improved power supply monitoring

Further the software has been modified to improve the internal diagnostic and to implement new functionalities caused by the architecture changes.

Manufacturers documentation

The necessary documentation and software sources needed for the approval was handed over by the manufacturer and has been archived by the Test Institute (see CD-ROM, dated 2006-09-29).

The following tables include only the primary documents. Further detailed design and architecture documents, test plan and reports are referenced and listed in [H1].

No.	Description
H1	Project Description Annex1, Documentation structure (PDC.002), dated 08.01.2007
H2	General Requirement Specification (500.540.RS.99.01/00), dated 19.07.1999
H3	Safety Requirement Specification (RSD.007.01), dated 29.04.2003
H4	Change & Impact Analysis (SW) (TRP.025.01), dated 08.08.2005
H5	Change & Impact Analysis (HW) (TRP.030.00), dated 19.09.2005
H6	Hardware Architecture Design Specification (ADE.012.00), dated 23.02.2005
H7	Software Architecture Design Specification (ADE.004.003) dated 29.03.2003
H8	Software Functional Specification (FSP.010.03), dated 26.03.2007
H9	Transmitter FMEA (TRP.023.01), dated 21.07.2005
H10	System FMEA (TRP.026.01), dated 29.07.2005
H11	Component FMEA and DC calculation 2600T model 268 (TRT.070.01), dated 16.09.2005
H12	Excel-Sheet: 'Component FMEA model 268.xls'
H13	2600T Electronics models 264/268 Test Protocol (TSP.007.01), dated 07.11.2006
H14	2600T model 268 Type Test Report (TSP.009.00), dated 05.07.2006
H15	2600T Electronics models 264/268 Test Report (TRT.097.00), dated 07.11.2006
H16	2600T model 268 Type Test Report (TRT.099.00), dated 05.12.2006

No.	Description
H17	Hardware Fault Insertion Test Plan (TSP.006.00), dated 29.07.2006
H18	Hardware Fault Insertion Test Report (TRT.072.04), dated 26.03.2007
H19	C coding conventions (FSD.007.00), dated 09.08.2005
H20	Static analysis of 2600T safety source code (TRT.078.03), dated 23.03.2007
H21	Module Test (TRT.107.00), dated 23.03.2007
H22	Code Review (TRT.101.00), dated 04.01.2007
H23	Safety Manual (IM/266_8D_6), dated 03.2007

Table 1: Manufacturer Documents

No.	Description	CRC32
S1	Safety Firmware DF3011_04	0x5741C62E

Table 2: Software

4. Tests and test results

4.1 General

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspectors documentation.

All considerations concerning tolerance of the measurements, so far applicable, are stated in the inspectors documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

4.2 General requirements

The IEC 61508 adopts an overall safety lifecycle which shall be used to claim conformance with the standard. In general it distinguishes between measures to control and measures to avoid failures.

This overall safety lifecycle definition results in the following categories of requirements:

1. Requirements which have to be considered for the design of a safety related system. These requirements are mostly independent of the applications.
2. Requirements to ensure sufficient assistance during all phases of the safety lifecycle of safety related applications with all aspects of:
 - a. specification and planning of the safety application
 - b. operation and maintenance of the safety related product
 - c. verification, validation and modification of the safety related application

The requirements of the first category are addressed during the type approval product to claim conformance to the IEC 61508.

The requirements of the second category need to be fulfilled by the end-user, customer of the system, whereas the manufacturer documentation is considered in the context of the type approval to define conditions and requirements which assist the user in scope of the defined requirements.

4.3 Safety requirements

The safety related field instrument follows the Namur regulation NE 43 [6] of the standardization of signal level for the breakdown information of digital transmitters.

Whereas the safe state is user configurable to up or down scale alarm (< 4 mA or > 20 mA) in accordance to NE 43 [8].

The hardware safety integrity as listed in table 2 of IEC 61508, part 2, must be considered for the mechanical sensor part (Type A) of the 2600T Series Pressure Transmitter which must comply with these requirements.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - ≤ 90 %	SIL 2	SIL 3	SIL 4
90 % - ≤ 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 3: Hardware safety integrity, architectural constraints for Type A safety related subsystems

The hardware safety integrity as listed in table 3 of IEC 61508, part 2, must be considered for systems with microprocessor based components (Type B). The electronic part of the 2600T Series Pressure Transmitter must comply with these requirements.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 % - ≤ 90 %	SIL 1	SIL 2	SIL 3
90 % - ≤ 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 4: Hardware safety integrity, architectural constraints for Type B safety related subsystems

The Safe Failure Fraction shall be ≥ 60 % if a Hardware Fault Tolerance of 1 is considered as the system architecture.

4.4 Requirements resulting from application standards

The application specific requirements result from [5 - 8] and covers applications in the process industry.

Restrictions and conditions concerning the use of the safety related field device within the specified application standards are described in the safety manual [H23].

The requirements of the first category are addressed during the type approval product to claim conformance to the IEC 61508.

The requirements of the second category need to be fulfilled by the end-user, customer of the system, whereas the manufacturer documentation is considered in the context of the type approval to define conditions and requirements which assist the user in scope of the defined requirements.

4.3 Safety requirements

The safety related field instrument follows the Namur regulation NE 43 [6] of the standardization of signal level for the breakdown information of digital transmitters.

Whereas the safe state is user configurable to up or down scale alarm (< 4 mA or > 20 mA) in accordance to NE 43 [8].

The hardware safety integrity as listed in table 2 of IEC 61508, part 2, must be considered for the mechanical sensor part (Type A) of the 2600T Series Pressure Transmitter which must comply with these requirements.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - ≤ 90 %	SIL 2	SIL 3	SIL 4
90 % - ≤ 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 3: Hardware safety integrity, architectural constraints for Type A safety related subsystems

The hardware safety integrity as listed in table 3 of IEC 61508, part 2, must be considered for systems with microprocessor based components (Type B). The electronic part of the 2600T Series Pressure Transmitter must comply with these requirements.

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 % - ≤ 90 %	SIL 1	SIL 2	SIL 3
90 % - ≤ 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Table 4: Hardware safety integrity, architectural constraints for Type B safety related subsystems

The Safe Failure Fraction shall be ≥ 60 % if a Hardware Fault Tolerance of 1 is considered as the system architecture.

4.4 Requirements resulting from application standards

The application specific requirements result from [5 - 8] and covers applications in the process industry.

Restrictions and conditions concerning the use of the safety related field device within the specified application standards are described in the safety manual [H23].

4.5 Functional Safety Management

The Management of Functional Safety has been carried out on project level considering the certified quality assurance system of ABB SACE S.p.A based on ISO 9001. The development has been accompanied by the test institute as part of an independent Functional Safety Assessment [P2] on product level to prove compliance with the safety development lifecycle required by the IEC 61508.

The modifications and extensions to the product have been made under consideration of IEC 61508 [1], following the safety lifecycle in respect of appropriate documentation. The development lifecycle follows a well defined and hierarchical process and was inspected for compliance with IEC 61508.

The assessment has been finished with a positive result.

4.6 Review of the manufacturer documents

The documents listed in chapter 3 have been reviewed and were assessed concerning the completeness, consistency and conformity in accordance with the IEC 61508. Based on the document structure [H1] the documents were inspected regarding comprehensibility, completeness and consistency.

In detail the following points were considered during the inspection of the documentation:

- revision control system of the documents
- unambiguous attributes
- clear relationship between the documents
- comprehensibility
- completeness of the specification and documentation

Contradictions in the documentation have been discussed with the manufacturer and corrected in the documents.

The inspection of the documentation has been finished with a positive result.

4.7 Measures to avoid systematic failures

The measures to avoid failures have been inspected during a Functional Safety Assessment (FSA) within the manufacturer facilities in Lenno (CO), Italy. The application and effectiveness of the measures to avoid failures during the safety lifecycle have been assessed considering that the product shall also be used in redundant configurations in applications that shall claim SIL 3.

As a basis for modifications the manufacturer has carried out an impact analysis to evaluate the hardware and software changes [H4, H5].

The verification and validation tests include hardware fault insertion [H17] and hard- and software functional tests [H13]. In addition static analysis [H20] and manual code reviews [H22] have been performed on the software, in order to detect systematic failures.

The carried out reviews of the changes based on the impact analysis and the corresponding documentation and reviews of test and test results have been finished with a positive result.

It was demonstrated that the manufacturer complies with the safety lifecycle requirements of IEC 61508 considering the measures for failure avoidance as required by SIL 3.

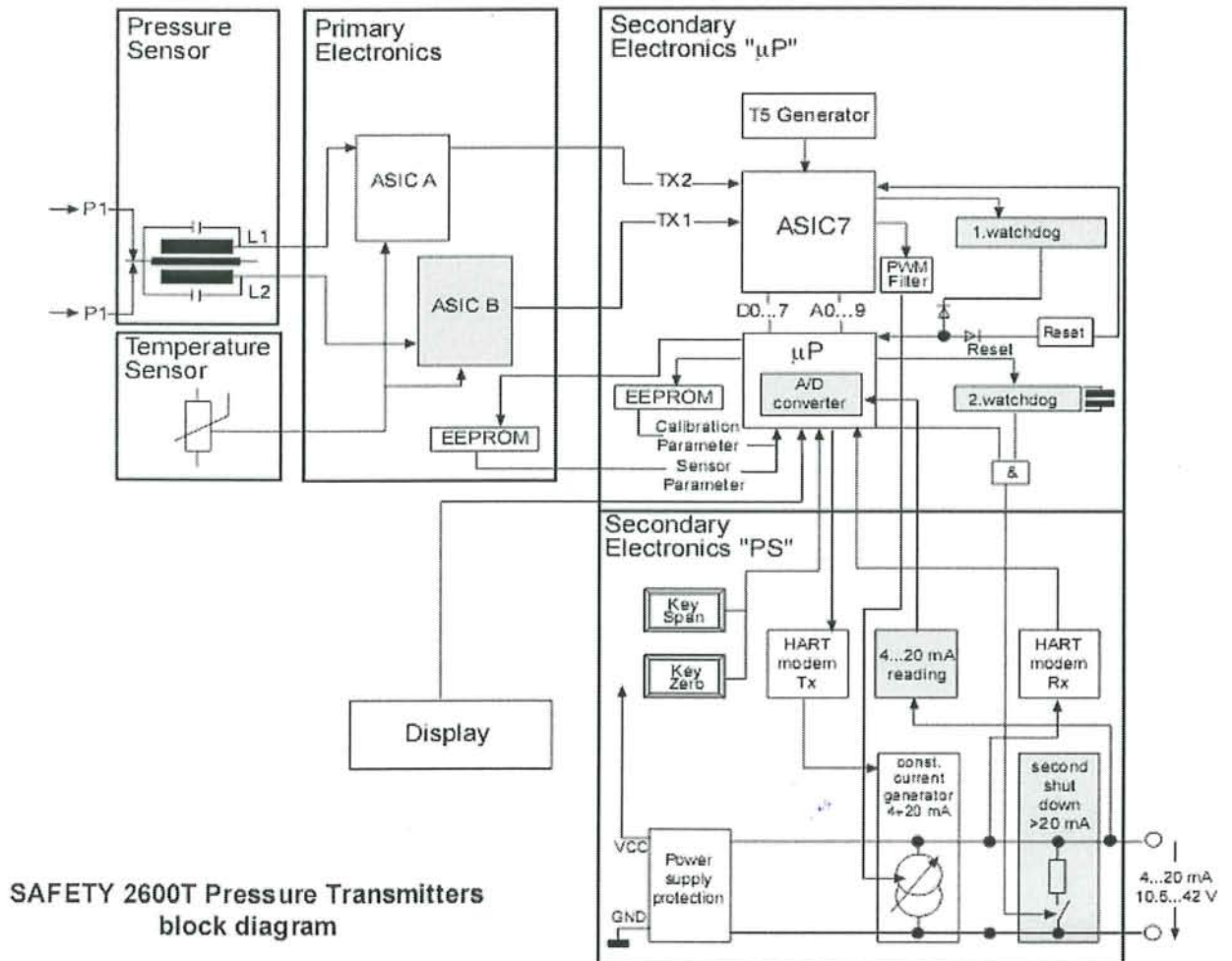
4.8 Measures to control systematic and random faults in hardware and software

The measures to control systematic and random hardware faults are based on the existing approval [P1]. The improvements have been done on several parts of the architecture as described in section 3.

The implemented measures have been inspected and claim to demonstrate the effectiveness as required by SIL 2 in accordance to IEC 61508.

4.9 Review of the hardware architecture and design

The general architecture and design of the safety pressure transmitter is based on the already certified model [P1]. The changes have been done on the parts marked in grey.



Picture 1: Safety 2600T Pressure Transmitter block diagram

The primary electronics convert the pressure signal measured by the pressure sensor to an electronic pulse-width signal and introduce a second ASIC which converts the input frequency into two redundant pulse-width signals. These signals are further provided to the secondary electronics using two independent lines.

The ASIC7 located on the secondary electronics converts the two independent pressure signals and stores them in two different RAM locations where they are used by the μP to perform the necessary calculations and consistency checks.

Two independent watchdogs supervise the correct working of either the μ C and the ASIC.

For diagnostic purposes the μ P converts the analog feedback signal of the 4.. 20 mA output current loop and compares it with the actual output current.

A second shut-down path allows the independent shut-down in case of μ P clock failure or a failure within the analog output stage and forces the output signal to the up-scale alarm value.

The review of the hardware architecture and design was finished with a positive result.

4.10 Review of the software architecture and design

During the approval the measures for failure avoidance according to the requirements for SIL 3 corresponding to the IEC 61508-3 [1] have been considered.

The firmware as listed in section 3 is based on the already approved firmware release as listed in [P1]. The manufacturer performed a change and impact analysis [H4] and modified the software in accordance to this analysis corresponding to the architecture and functional design specifications [H7, H8].

Due to the fact that the previous software was difficult to maintain the software was reordered to follow a stronger modularisation keeping the focus on maintainability and failure avoidance as required by IEC 61508-3.

All changes have been performed under consideration that the main calculation and consistency functions would be unmodified.

The theoretical review of the software modifications were reviewed together with the developer and were finished with a positive result.

4.11 Review of the FMEA

The mechanical and electronic FMEAs [H9, H10, H11] and corresponding fault injection tests [H17] were adapted to the modifications. Sample fault injection tests have been carried out together with the Test Institute [H18].

The FMEAs and the review of fault injection test were finished with a positive result.

4.12 Review of the reliability data and PFD/PFH calculations

The calculations regarding the probability of failures on demand (PFD) as defined within IEC 61508-1 was performed by the manufacturer [H10-H12] and has been reviewed by the Test Institute.

The internal hardware fault tolerance (HFT) of the system can be considered as 1 [P1]. On the basis of the FMEA the probability of a dangerous failure was calculated. The following assumptions were made:

- The failure rate is constant over lifetime.
- Without considering the diagnostic functions, it is assumed that 50 % of all failures are safe and the other 50 % are dangerous.
- For the calculation a Proof Test Interval (T1) of 10 Year [H12] was used.

PFD (electronic sensor part)

The calculated PFD_{avg} for the sensor considering the electronic part [H12] is:

$$\text{PFD}_{\text{avg}} (T1=10\text{y}) \approx 5 * 10^{-4}$$

The result shows that after 10 years $\approx 5 \%$ of SIL 2 are consumed.

PFH (electronic sensor part)

The calculated PFH for the sensor considering the electronic part [H12] is:

$$\text{PFH} = \lambda_{\text{DU}} \approx 1,1 * 10^{-8} \text{ h}^{-1}$$

PFD (mechanical and electronic sensor parts)

The calculated PFD_{avg} for the sensor considering the mechanical and electronic part [H12] is:

$$\text{PFD}_{\text{avg}} (T1=10\text{y}) \approx 2,7 * 10^{-3}$$

The result shows that after 10 years $\approx 27 \%$ of SIL 2 are consumed.

PFH (mechanical and electronic sensor parts)

The calculated PFH for the sensor considering the mechanical and electronic part [H12] is:

$$\text{PFH} = \lambda_{\text{DU}} = 6,1 * 10^{-8} \text{ h}^{-1}$$

The review shows that the product claims the SIL 2 requirements of IEC 61508 in low as well as high demand mode of operation. This means that the PFD/PFH is lower than the limit defined in IEC 61508-1 of $\geq 10^{-3}$ to $< 10^{-2}$ for PFD and of $\geq 10^{-7}$ to $< 10^{-6}$ for PFH. After 10 years of usage $\approx 27 \%$ of SIL 2 are consumed.

Further the reviews have shown that the mechanical (Type A) and electronic part (Type B) fulfil the requirements concerning the Safe Failure Fraction as defined in 4.3.

4.13 Inspection of the electrical safety

The product is supplied with SELV (Safe Extra Low Voltage) and the Ingress Protection (IP) rating is carried out as IP67.

The review regarding electrical safety was finished with a positive result.

4.14 Inspection of the environmental and EMC tests

The standards [2 - 6] were used to test the device under environmental conditions and EMC requirements.

The tests were carried out by partly by the manufacturer himself and an accredited test laboratories. The results [H16] have been accepted by the Test Institute after review.

5. Summary

The carried out tests and analyses have shown, that the 2600T Series Pressure Transmitter, model 268 release 2 can be used in applications claiming SIL 2 according to IEC 61508.

Further it can be used in applications claiming SIL 3 according to IEC 61508 if two sensors are used in a homogenous redundant configuration (HFT=1).

The conditions, mentioned in chapter 4.12 of this report must be considered.

All conditions, which the user must comply with for safely using the product, are described in detail in the corresponding manuals [H23].

Cologne, 2007-03-28
TIS/ASI/Kst. 968 bu-nie

The inspector



Dipl.-Ing. (FH) Oliver Busa