

Report
on the
Certificate

Z10 04 02 42206 007

Safety Related Field Device
SAFETY 2600T PRESSURE TRANSMITTER

Manufacturer:

ABB SACE S.p.A.
Via Statale 113
I - 22016 Lenno (Co)

Report No.: AL63021C
Revision 1.3 dated 2004-02-20
Order No.: 70029198

Testing Body:

TÜV Automotive GmbH
TÜV Süddeutschland Group
Automation, Software and Electronics - IQSE

Certification Body:

TÜV Product Service GmbH
TÜV Süddeutschland Group
Ridlerstraße 65
D-80339 München

Revision Log

Revision	Name	Date	Changes/History
1.0	A. Beer	2002-08-23	Initial
1.1	A. Beer	2003-03-11	Application conditions
1.2	A. Beer	2003-08-18	Change of name from ABB Instrumentation S.p.A. to ABB SACE S.p.A.
1.3	W. Henke	2004-02-20	New software rel. 2.0 Appendix to the calculation of PFH (4.1.2)

Content	Page
1 Purpose and scope	4
2 System overview	4
2.1 System architecture	4
2.2 The term 'Functional Safety' used.....	4
2.3 Some abbreviations in common use	5
3 Certification requirements	6
3.1 Basis of Certification	6
3.2 Certification documentation	6
3.3 Functional safety.....	7
3.4 Basic safety	7
3.5 Environmental testing	7
3.6 Electromagnetic compatibility	7
4 Results.....	8
4.1 Functional Safety	8
4.2 Basic safety	13
4.3 Environmental stress testing.....	13
4.4 Electromagnetic Compatibility.....	13
4.5 Product-related quality management and product care.....	13
5 General conditions and restrictions	14
5.1 Application conditions	14
5.2 Commissioning conditions	14
5.3 Run-time conditions	15
6 Overall result and certificate number	15

Tables

Table 1: Functional safety standards	7
Table 2: Environmental testing.....	7
Table 3: Electromagnetic compatibility standards	7
Table 4: Result of the FMEA.....	8
Table 5: PFH distribution	10

1 Purpose and scope

The SAFETY 2600T PRESSURE TRANSMITTER is a Safety Related Field Device suitable for safety-related applications with a high level of potential danger, e.g. gauge and absolute pressure, flow and liquid level measurement in industrial environments.

TÜV Automotive GmbH has been contracted by ABB SACE S.p.A. to certify the Safety Related Field Device SAFETY 2600T PRESSURE TRANSMITTER.

This report summarizes the user related results of the tests and inspections performed on the SAFETY 2600T PRESSURE TRANSMITTER system based on the certification requirements outlined under clause 3.1 and reported by the documentation listed under clause 3.2.

2 System overview

2.1 System architecture

The SAFETY 2600T PRESSURE TRANSMITTER implements a 1oo1 architecture with diverse software on single channel hardware for continuous mode of operation.

The SAFETY 2600T PRESSURE TRANSMITTER shall perform frequently self-tests or diagnostic failure indication and safe state at the output in case of a failure. The parameter 'safe state' < 4 mA or > 20 mA is user configurable. Carrying out its intended safety function see clause 5.1 'Application conditions'.

The HART protocol allows remote re-ranging, calibration and diagnostics without any interference to the safety related functions.

Detailed architectural, configuration and implementation requirements are described in the manual 'operating instructions' of the SAFETY 2600T PRESSURE TRANSMITTER.

2.2 The term 'Functional Safety' used

The term 'Functional Safety' is the ability of a safety-related system to carry out the actions necessary to achieve a (defined) safe state for the equipment under control (EUC) or to maintain the safe state for the EUC.

2.3 Some abbreviations in common use

Abbreviation	Explanation
T1	Proof Test Interval in h
MTTR	Mean Time To Restoration in h
DC	Diagnostic Coverage in %
t	Time in years
$PFD_{TOT}(t)$	Sum of the failure rates of the three elements Secondary electronics PS board, Secondary electronics microprocessor board and Primary electronics, h^{-1} . $PFD_{Sensor}(t) + PFD_{uP}(t) + PFD_{PS}(t)$
$PFD(t)$	Probability of Failure on Demand. $PFD(t) = P_{dd}(t) + P_{du}(t)$
$PFD_{TOT\ AVG}$	Average in time of the function $PFD_{TOT}(t)$
PFH	Probability of a dangerous failure per hour
PFH_{TOT}	Probability of a dangerous failure per hour of the whole system.
P_i	Probability that the system can be found in the state with the short cut i. "i" stands for dd, du, sd, su or dca.
Rate	Probability that the system can be found in a dangerous state per hour in h^{-1}
dd-state	dangerous detected state
du-state	dangerous undetected state
sd-state	safe detected state
su-state	safe undetected state
dca	the "do not care-state" is a special safe state
h	hour
FIT	Failures In Time in $10^{-9} h^{-1}$

Table 1: Abbreviations

3 Certification requirements

3.1 Basis of Certification

The certification of the SAFETY 2600T PRESSURE TRANSMITTER will be according to the regulations and standards listed in clause 3.3 to 3.6 of this document. This will certify the successful completion of the following test segments:

- I. Functional Safety
 - A. Quantitative analysis of the hardware / 'Safe Failure Fraction'
 - B. Software analysis for the safety-related software components
 - C. Descriptive safety as given by the operating instructions
- II. Basic Safety with ATEX-Certification
- III. Environmental Stress Testing
 - A. Climatic and temperature stress
 - B. Mechanical stress
- IV. Electromagnetic Compatibility
 - A. Electromagnetic susceptibility
 - B. Electromagnetic emission
- V. Product-related quality management and product care

Certification is dependent on successful completion of all of the test segments above.

3.2 Certification documentation

Documentation of this certification is based on the TECHNICAL REPORT ON TESTING FUNCTIONAL SAFETY, AL63041T, Rev.: 1.5 of 2004-02-20.

Based on the specified purpose of use of the SAFETY 2600T PRESSURE TRANSMITTER in safety critical process protection applications the certification is based on the following set of standards. The issuance of the certificate states compliance with these references unless specifically noted otherwise.

3.3 Functional safety

The testing for functional safety is to be performed using the following standards and guidelines:

IEC 61508-1:1998 (to the extent applicable)	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
IEC 61508-2: 2000	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3: 1998	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements
IEC 61508-6: 2000	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the application of parts 2 and 3

Table 1: Functional safety standards

3.4 Basic safety

The technical requirements are covered by ATEX certification according Directive 94/9/EC.

3.5 Environmental testing

To complete and to specify the technical requirements resulting from the essential requirements of the Directives listed above the environmental testing is to cover the following standards:

IEC 60068-2-*	Basic environmental testing procedures
---------------	--

Table 2: Environmental testing

3.6 Electromagnetic compatibility

To complete and to specify the technical requirements resulting from the essential requirements of the Directives listed above, the testing of electromagnetic compatibility is to cover the following standards:

EN 61000-6-2: 1999	Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments
EN 55011: 1998	Industrial, scientific and medical (ISM) radio-frequency equipment – Radio disturbance characteristics
EN 55022: 1998	Industrial, scientific and medical – Radio disturbance characteristics

Table 3: Electromagnetic compatibility standards

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the 'Safety Related Field Device' SAFETY 2600T PRESSURE TRANSMITTER comply with the testing criteria specified in clause 3 for intermittent or continuous mode of operation in applications up to SIL 2.

The safe state < 4 mA or > 20 mA of the analog output is user configurable.

General conditions and restrictions for application, commissioning, run-time are defined in clause 5.

4.1.1 'Safe Failure Fraction' and quantitative analysis of the hardware

The Diagnostic Coverage and Safe Failure Fraction evaluation has been elaborated following the requirements of IEC 61508 part 2 and 6. For the calculation of the failure rate λ , the software „Reliability Workbench by ITEM Software Ltd“, based on MIL 217 Handbook, has been used. The total results are listed in table 4.

Safe failure	295 FIT
Dangerous failure	706 FIT
Safe detected failure	134 FIT
Safe undetected failure	160 FIT
Dangerous detected failure	669 FIT
Dangerous undetected failure	37 FIT
Do not care	181 FIT
Diagnostic Coverage	94,88 %
Safe Failure Fraction	96,73 %

Table 4: Result of the FMEA

The 'Proof Test Interval' (see below) may be specified by using the method of calculation of the IQSE (in accordance with the QSAA statistical calculation), within the assemblies have to be completely tested in order to detect an initial fault before combination with a possible second fault becomes harmful. Most of the following abbreviations can be found in the international norm IEC 61508-6.

4.1.2 Results of the 'Markov Calculation'

For the calculation of the probability of the system to be in a dangerous state, there has been added the probability of the system to be in the dangerous detected state to the probability to be in the dangerous undetected state. This function in time is called PFD(t) and has been calculated for every subsystem.

$$PFD_i(t) = P_{dd}(t) + P_{du}(t) \text{ with } i = \text{Sensor, uP or PS}$$

In order to calculate the total failure rate PFD_{TOT} , the failure rates of the three elements PRIMARY ELECTRONICS: „I“, SECONDARY ELECTRONICS: „H“/board „uP“ and SECONDARY ELECTRONICS: „H“/board „PS“ have been added.

$$PFD_{TOT}(t) = PFD_{\text{Sensor}}(t) + PFD_{\text{uP}}(t) + PFD_{\text{PS}}(t)$$

The Probability of a dangerous failure per hour (PFH) can be calculated by:

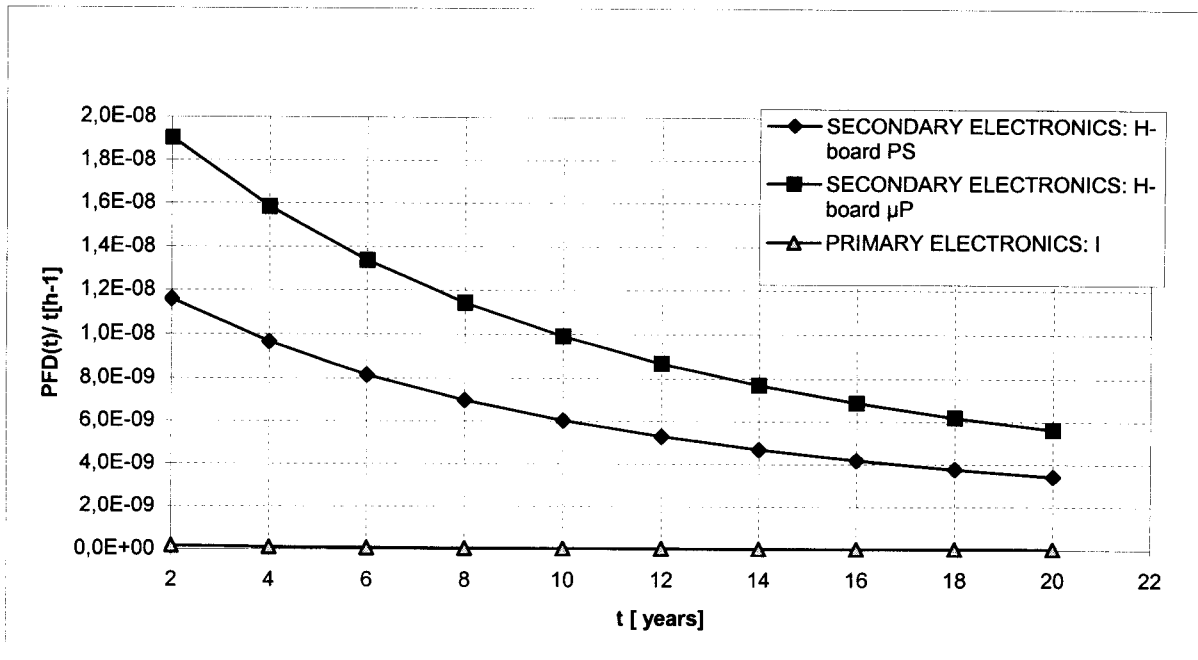
$$PFH_{TOT} = PFD_{TOT}(t) / t \text{ with } t = \text{the life time of the system}$$

After a passing life time the system is shut down. PFD_{TOTAVG} is well suited to describe PFH_{TOTAVG} .

$$PFH_{TOTAVG} = \frac{1}{n} \sum_{i=1}^n \frac{PFD_{TOTAVG}(t_i)}{t_i}$$

Graph 1 shows $PFD_{\text{Sensor}}(t)/t$, $PFD_{\text{uP}}(t)/t$ and $PFD_{\text{PS}}(t)/t$ as results of the Markov calculation. The inputs for one calculation were:

- Failure rates, λ_i
- Proof Test Interval, $T1 = 10$ years
- Mean Time To Restoration, $MTTR = 8$ hours



Graph 1: PFD/ t results of primary- and secondary electronics

The SIL 2 failure measures for a safety function, allocated to the SAFETY 2600T PRESSURE TRANSMITTERS operating in high demand or continuous mode of operation must be $\geq 10^{-7}$ to $< 10^{-6} \text{ h}^{-1}$ for the probability of a dangerous failure (table 3 of IEC 61508 part 1).

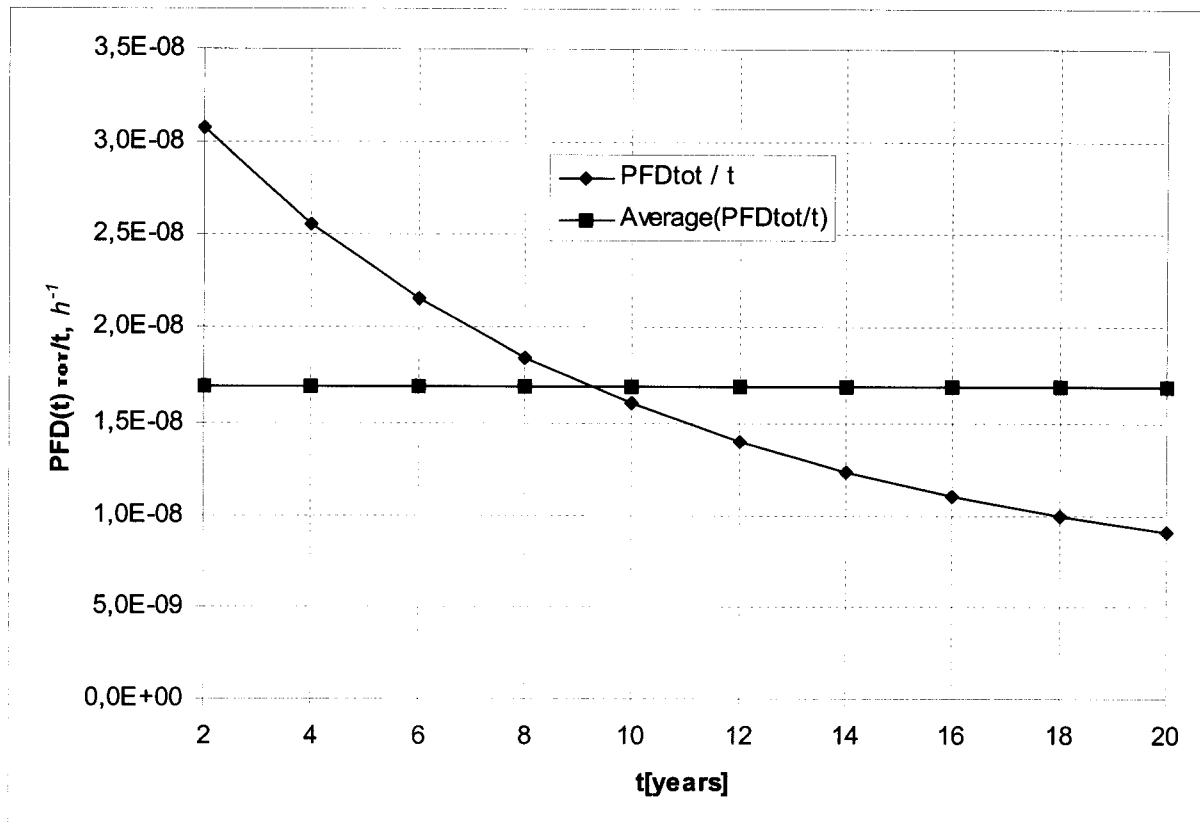
PFH_{TOT} in table 9 is the PFH value of sensor / input interface components as defined in the standard IEC 61508-6 for functional safety in chapter 3.1. In the block diagram model of the standard, there are given three components which deliver contributes to the total probability of failure on demand (PFH_{TOTAVG}). The recommended distribution is shown in the table below.

Component	Distribution of total PFH	PFH
Sensor / Input interface	35%	$3,5 \cdot 10^{-7}$
Logic system	15%	$1,5 \cdot 10^{-7}$
Output interface and final element	50%	$5,0 \cdot 10^{-7}$

Table 5: PFH distribution

The SIL 2 failure measures for operating in high demand or continuous mode of operation must be less than $3,5 \cdot 10^{-7} \text{ h}^{-1}$ for the probability of a dangerous failure a dangerous failure.

Graph 2 shows $PFH_{TOT} = PFD_{TOT}(t) / t$. The parameters are the same as in graph 1. PFD_{TOT}(t) was gained by adding the three functions PFD(t) in graph 1.



Graph 2: PFD_{TOT}(t)/ t, PFH_{TOT AVG} for continuous mode of operation T1=10 years, MTTR = 8h

Result:

The total average probability of failure per hour is calculated to

$$PFH_{TOTAVG} = 1,69 \cdot 10^{-8} \text{ h}^{-1}.$$

This is less than the admissible value $3,5 \cdot 10^{-7} \text{ h}^{-1}$ of table 7. The quantitative requirements of SIL 2 are satisfied in the case of:

- Proof Test Interval, T1=10 years
- Mean Time To Restoration, MTTR=8 h.

The PFH_{TOTAVG} shows, that even the quantitative requirements of SIL 3 are satisfied according to IEC 61508-1, table 3.

4.1.3 Analysis of the software

The analysis of the operating system software (including self-test) included the following operations:

- Analysis of the specification
- Analysis of system calls
- Code inspection of implemented self-tests
- Definition of representative tests
- Modifications from V1.0 (31/05/2000) to V2.0 (03/04/2003)

4.1.3.1 Safety-related software under certification

The operating software including self-tests has been certified 'safety-related'. The actual revision 2.0 of the firmware is dated 2003-04-03.

4.1.3.2 Interference free software component

The interference free¹ software component 'HART-command' is not the subject of this certification. Absence of impact of not certified components on 'safety-related' components is enforced.

4.1.4 Fault reaction time

The SAFETY 2600T PRESSURE TRANSMITTER shall perform frequently self-tests or diagnostic failure indication and safe state at the output in case of a failure. The parameter 'safe state' < 4 mA or > 20 mA is user configurable.

The fault-tolerance time² of the process controlled by the SAFETY 2600T PRESSURE TRANSMITTER shall be greater than the worst-case response time. The procedure for modifications and existing restrictions are described in the manual 'operating instructions'.

In general, responsibility for monitoring the process during and after the modification lies entirely with the organization and person responsible for the modification. Since on-line modifications are generally associated with an increased level of risk the approval of on-line

¹ Interference free software component: Property of a unit not to cause faulty state in connected units even if it fails

² The fault-tolerance time denotes a characteristic of the process and describes the period of time, in which the process can be controlled by a faulty control-output signal, without entering a dangerous condition.

modifications is at the discretion of the testing and inspection center responsible for approval of the system's application.

4.2 Basic safety

The tests of the electrical safety (ATEX-certification) executed by a notified body show that the standards specified in clause 3 are covered.

4.3 Environmental stress testing

The tests of the environmental stress tests executed by a notified test laboratory show that the standards specified in clause 3 are covered.

4.4 Electromagnetic Compatibility

The documentation of the electromagnetic compatibility tests executed by a notified test laboratory show that the standards specified in clause 3.5 are covered.

4.5 Product-related quality management and product care

An ISO 9001 certified quality assurance and control system governs all software and hardware components developed and manufactured in course of the safety evaluation.

The European procedures for demonstrating conformity (93/465/EWGB-93/465/EECB-93/465/CEEB-ix, Council Decision of 22 July 1993 concerning the modules for the various phases of the conformity assessment procedures and the rules for the affixing and use of the CE conformity marking, which are intended to be used in the technical harmonization direct) provide similar significance to the type testing and the manufacturer's quality assurance in production and product maintenance. As part of the certification process TÜV Automotive also performs a procedure that is tailored to the assessed product in order to assess the consistency of product quality while accounting for product modifications and their identifiably (follow-up service).

5 General conditions and restrictions

The use of the SAFETY 2600T PRESSURE TRANSMITTER shall comply with the current version of the safety parts of the manuals 'operating instructions', and the following implementation and installation requirements have to be followed if the SAFETY 2600T PRESSURE TRANSMITTER system is used in safety-related installations.

The SAFETY 2600T PRESSURE TRANSMITTER is a safety-related product and the recommendations based on the experience and judgement of the ABB SACE S.p.A. documented in the manuals shall therefore be carefully followed. The information, recommendations, specifications and safety instructions given in the belonging manuals shall be read and understood.

5.1 Application conditions

- 5.1.1. The specific guidelines in the manual 'operating instructions' shall be followed.
- 5.1.2. The fault tolerance period of the process controlled by the SAFETY 2600T PRESSURE TRANSMITTER shall be greater than the worst-case response time.
- 5.1.3. A well-defined shutdown procedure shall be specified.
- 5.1.4. Operator alarms as exclusive means of shutdown are only permitted under supervised operation and if the fault tolerance time of the controlled process is sufficiently long to ensure a safe manual reaction and shutdown and the operator has sufficient independent means to supervise the process. Installations that must react to shutdown conditions quicker than achievable with manual intervention or installations running unsupervised shall incorporate an automatic fault reaction procedure.
- 5.1.5. The operating conditions as specified in the manual 'operating instructions' shall be met. Attention should be paid to the parameter 'safe state' < 4 mA or > 20 mA.

5.2 Commissioning conditions

- 5.2.1. Prior to commissioning, a complete functional test of the safety-relevant function shall be performed.
- 5.2.2. All timing requirements shall be validated.
- 5.2.3. Any application modification after commissioning shall result in a re-validation of the entire system.
- 5.2.4. The proper fail-safe configuration of the safety-critical fail-safe analog output shall be verified. Only configurations covered by the manual 'operating instructions' are covered by the certification.

5.3 Run-time conditions

- 5.3.1. Proof test interval, T1 = 10 years. It is necessary to perform this periodic test to detect dangerous failures. The correct working of the second shut down and the second watchdog shall be verified.
- 5.3.2. Failed SAFETY 2600T PRESSURE TRANSMITTER should be replaced as quickly as practical to minimize the probability of multiple fault accumulation. The calculations of the Probability-of-Failure-on-Demand of the safety-related SAFETY 2600T PRESSURE TRANSMITTER are based on a mean time to restoration of 8h.
- 5.3.3. The procedure described in the manual 'operating instructions' has to be followed.
- 5.3.4. The approval authority for the plant assessment shall grant modifications.

6 Overall result and certificate number

The tests performed and the quality assurance measures implemented by the manufacturer have shown that the SAFETY 2600T PRESSURE TRANSMITTER system comply with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections.

This report specifies technical details and implementation conditions required for the application of the Safety Related Field Device SAFETY 2600T PRESSURE TRANSMITTER by ABB SACE S.p.A. on the certificate:

Z10 04 02 42206 007

Munich, 2004-02-20

TÜV Automotive GmbH
TÜV Süddeutschland Group
Automation, Software and Electronics - IQSE
Technical Certifier



A. Beer