

Internal and external fault behaviour of safety related electronic parts of gas appliances

ICS 23.060.40; 25.040.40; 27.060.20

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

Committees responsible for this Draft for Development

The preparation of this Draft for Development was entrusted to Technical Committee GSE/22, Safety and control devices for gas governors and gas burning appliances, upon which the following bodies were represented:

- Association of Control Manufacturers [TACMA (BEAMA Ltd.)]
- British Combustion Equipment Manufacturers' Association
- British Gas plc
- Department of Trade and Industry (Consumer Safety Unit, CA Division)
- Electricity Association
- LP Gas Association
- Society of British Gas Industries

This Draft for Development, having been prepared under the direction of the Engineering Sector Board, was published under the authority of the Standards Board and comes into effect on 15 April 1997

© BSI 10-1999

The following BSI reference relates to the work on this Draft for Development: Committee reference GSE/22

ISBN 0 580 26738 5

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	2
Text of ENV 1954	3
List of references	Inside back cover

National foreword

This Draft for Development has been prepared by Technical Committee GSE/22 and is the English language version of ENV 1954:1996 *Internal and external fault behaviour of safety related electronic parts of gas appliances*, published by the European Committee for Standardization (CEN). DD ENV 1954 was produced as a result of international discussion in which the United Kingdom participated.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature because the technology and methodology is under development. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the European organization responsible for its conversion to a European Standard. A review of this publication will be initiated two years after its publication by the European organization so that a decision can be taken on its status at the end of its three-year life. The commencement of the review period will be notified by an announcement in *BSI Update*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into a European Standard, to extend the life of the prestandard or to withdraw it. Comments should be sent in writing to the Secretary of BSI Technical Committee GSE/22 at BSI, 389 Chiswick High Road, London, W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

Reference should be made in the national foreword to any British Standards on the same subject that will remain in force during the life of the prestandard but will be withdrawn after it has been converted into a European Standard and implemented as a British Standard. Any informative national annexes (see 16.4) in the Draft for Development added to give guidance on provisions of the prestandard have to be referred to in the national foreword.

Cross-references

Publication referred to	Corresponding British Standard
ENV 50140:1993	DD ENV 50140:1994 <i>Electromagnetic compatibility. Basic immunity standard. Radiated radio-frequency electromagnetic field. Immunity test</i>
ENV 50141:1993	DD ENV 50141:1994 <i>Electromagnetic compatability. Basic immunity standard. Conducted disturbances induced by radio-frequency fields. Immunity test</i>
ENV 50142:1994	DD ENV 50142:1995 <i>Electromagnetic compatability. Basic immunity standard. Surge immunity tests</i>
EN 60730-1:1991	BS EN 60730 <i>Specification for automatic electrical controls for household and similar use</i> Part 1:1992 <i>General requirements</i>
EN 60742:1989	BS 3535 <i>Isolating transformers and safety isolating transformers</i> Part 1:1990 <i>General requirements</i>
IEC 384-14	BS 6201 <i>Fixed capacitors for use in electronic equipment</i> Part 3:1982 <i>Specification for fixed capacitors for radio interference suppression. Selection of methods of test and general requirements</i>

Publication referred to	Corresponding British Standard
IEC 801-2:1991	BS EN 60801 <i>Electromagnetic compatability for industrial-process measurement and control equipment</i> Part 2:1993 <i>Electrostatic discharge requirements</i>
IEC 947-1:1988	BS EN 60947 <i>Specification for low-voltage switchgear and control gear</i> Part 1:1992 <i>General rules</i>

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, the ENV title page, pages 2 to 28, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

ICS 23.060.40; 25.040.40; 27.060.20

Descriptors: Gas installation, gas appliances, safety devices, electronic equipment, specifications, classifications, safety, defects, failure

English version

Internal and external fault behaviour of safety related electronic parts of gas appliances

Comportement des parties électroniques
intéressant la sécurité dans les appareils
utilisant les gaz combustibles, en cas de défauts
internes et sous des contraintes externes

Fehlerverhalten von elektronischen Bauteilen
mit sicherheitstechnischen Anforderungen in
Gasgeräten bei inneren und/oder äußeren
Störungen

This European Prestandard (ENV) was approved by CEN on 1995-09-21 as a prospective standard for provisional application. The period of validity of this ENV is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the ENV can be converted into an European Standard (EN).

CEN members are required to announce the existence of this ENV in the same way as for an EN and to make the ENV available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the ENV) until the final decision about the possible conversion of the ENV into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Central Secretariat: rue de Stassart 36, B-1050 Brussels

© 1996 Copyright reserved to CEN members

Foreword

This European Prestandard has been prepared by Technical Committee CEN/TC 58, Safety and control devices for gas-burners and gas-burning appliances, the secretariat of which is held by BSI.

This European Prestandard has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this European Prestandard: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

Contents

	Page
Foreword	2
1 Scope	3
2 Normative references	3
3 Definitions	3
3.1 General	3
3.2 Definitions specific to complex electronics	4
4 Requirements	9
4.1 Fault control	9
4.2 Fault avoidance	10
5 Information	11
6 External fault behaviour	12
7 Fault behaviour under external influence	12
7.1 Performance tests	12
7.2 Climatic tests	12
7.3 Supply voltage variations	12
7.4 Supply voltage interruptions or decreases	12
7.5 Supply frequency variations	13
8 Electromagnetic phenomena	13
8.1 Voltage surges	13
8.2 Fast transient burst	14
8.3 Electromagnetic radiation — Immunity	14
8.4 Electrostatic discharges	14
9 Endurance	15
9.1 Design requirements	15
9.2 Test method	15

Annex A (normative) Failure modes for electronic components	16
Annex B (normative) Fault assessment flowcharts	25
Figure B.1 — Class B; Systems for non-permanent operation	25
Figure B.2 — Class C; Systems for non-permanent operation	26
Figure B.3 — Class B; Systems for permanent operation	27
Figure B.4 — Class C; Systems for permanent operation	28
Table 1 — Combinations of analytical measures during hardware development	10
Table 2 — Combinations of analytical measures to be taken during software development	10
Table 3 — List of information required	11
Table 4 — Short-term voltage decreases	13
Table 5 — Surge open circuit test voltage $\pm 10\%$ for ac mains systems	13
Table 6 — EFT/B open circuit output test voltage $\pm 10\%$	14
Table 7 — Severity levels	14
Table 8 — Severity levels	14
Table A.1 — Failure modes for normal electronic components	16
Table A.2 — Failure modes for complex electronic components	18

1 Scope

This prestandard applies to (programmable) electronic systems for gas installations including safety-relevant electronic actuators, sensors, converters, etc.

When an electronic safety system is designed to conform with the criteria stipulated in these requirements, it will have a safety class at least equal to that of a conventional (non-electronic) system.

For the purposes of evaluating the design of an electronic system, the present requirements recognize three distinct safety classes:

- Class A: Control functions which are not intended to be relied upon for the safety of the equipment.
- Class B: Control functions intended to prevent unsafe operation of the controlled equipment.
Examples of controls which may include Class B functions are:
 - thermal cut-outs;
 - pressure cut-outs.
- Class C: Control functions which are intended to prevent special hazards or whose failure could directly cause a hazard. Examples of controls which may include Class C functions are:
Automatic burner controls, thermal cut-outs for closed water heater systems (unvented), gas valve proving systems.

2 Normative references

This European Standard incorporates by dated or undated references, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this European prestandard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

ENV 50140:1993, *Electromagnetic compatibility. Basic Immunity Standard Radiated, radio-frequency electromagnetic field — Immunity test.*

ENV 50141:1993, *Electromagnetic compatibility. Basic Immunity Standard Conducted disturbances induced by radio-frequency fields — Immunity test.*

prENV 50142:1993, *Electromagnetic compatibility. Basic Immunity Standard — Surge Immunity test.*

EN 60730-1:1991, *Automatic electrical controls for household and similar use Part 1: General requirements.*

EN 60742:1989, *Isolating and safety isolating transformers — Requirements.*

IEC 335-1:1976, *Safety of household and similar electrical appliances Part 1: General requirements.*

IEC 384-14, *Fixed capacitors for use in electronic equipment Part 14: Sectional specification. Fixed capacitors for radio interference suppression. Selection of methods of test and general requirements.*

IEC 801-2:1991, *Electromagnetic compatibility for industrial-process measurement and control equipment. Electrostatic discharge requirements.*

IEC 801-4:1988, *Electromagnetic compatibility for industrial-process measurement and control equipment. Electrical fast transient/burst requirements.*

IEC 947-1:1990, *Low voltage switchgear and control gear Part 1: General rules.*

HD 323.2.6.S2:1988, *Environmental testing Part 2: Tests, test Fc and guidance vibration (sinusoidal).*

3 Definitions

For the purposes of this prestandard the following definitions apply.

3.1 General

3.1.1 systems for permanent operation

systems that are designed to remain in the running position for longer than 24 h without interruption

3.1.2 systems for non-permanent operation

systems that are designed to remain in the running position for less than 24 h

3.1.3 fault tolerance time

a maximum time for which the control of the process may be lost without a hazardous situation

3.1.4 fault/error detection time

the period of time between the occurrence of a fault/error in a control and the detection of that fault/error by the program, including the initiation, if any, of the control reaction

3.1.5

defined safe state

the state of the system, with the following characteristics:

- a) the system passively assumes a status in which the output terminals ensure a safe situation in all circumstances. When the effect is lifted, the system starts up in accordance with the appropriate requirements; or
- b) the system actively executes a protective action causing it to shut down and lock; or
- c) the system remains in operation, continuing to satisfy all safety related functional requirements.

3.2 Definitions specific to complex electronics

3.2.1 Definitions relating to the structure of controls using software

3.2.1.1

dual channel

a structure which contains two mutually independent functional means to execute specified operations

special provision may be made for control of common mode faults/errors. It is not required that the two channels each be algorithmic or logical in nature

3.2.1.2

dual channel (diverse) with comparison

a dual channel structure containing two different and mutually independent functional means, each capable of providing a declared response, in which comparison of output signals is performed for fault/error recognition

3.2.1.3

dual channel (homogeneous) with comparison

a dual channel structure containing two identical and mutually independent functional means, each capable of providing a declared response, in which comparison of internal signals or output signals is performed for fault/error recognition

3.2.1.4

single channel

a structure in which a single functional means is used to execute specified operations

3.2.1.5

single channel with functional test

a single channel structure in which test data is introduced to the functional unit prior to its operation

3.2.1.6

single channel with periodic self test

a single channel structure in which components of the control are periodically tested during operation

3.2.1.7

single channel with periodic self test and monitoring

a single channel structure with periodic self test in which independent means, each capable of providing a declared response, monitor such aspects as safety-related timing, sequences and software operations

3.2.2 Definitions relating to error avoidance in controls using software

3.2.2.1

dynamic analysis

a method of analysis in which inputs to a control are simulated and logic signals at the circuit nodes are examined for correct value and timing

3.2.2.2

failure rate calculation

a calculation of the theoretical number of failures of a given kind per unit (e.g. failures per hour or failures per cycle of operation)

3.2.2.3

hardware analysis

an evaluation process in which the circuitry and components of a control are examined for correct function within their specified tolerances and ratings

3.2.2.4

hardware simulation

a method of analysis in which circuit function and component tolerances are examined by use of a computer model

3.2.2.5

inspection

an evaluation process in which the hardware or the software specification, design or code is examined in detail by a person or group other than the designer or programmer in order to identify possible errors in contrast to the walk-through, the designer or programmer is passive during this evaluation

3.2.2.6

operational test

an evaluation process in which a control is operated under the extremes of its intended operating conditions (e.g. cycle rate, temperature, voltage) to detect errors in design or construction

3.2.2.7

static analysis-hardware

an evaluation process in which a hardware model is systematically assessed

the evaluation may typically be computer-aided and may include examination of parts lists and circuit layouts, an interface analysis and functional checks

3.2.2.8**static analysis — software**

an evaluation process in which a software program is systematically assessed without necessarily executing the program

the evaluation may typically be computer-aided and usually includes analysis of such features as program logic, data paths, interfaces and variables

3.2.2.9**systematic test**

a method of analysis in which a system or a software program is assessed for correct execution by the introduction of selected test data

for example see black box test and white box test

3.2.2.10**black box test**

a systematic test in which test data derived from the functional specification is introduced to a functional unit to assess its correct operation

3.2.2.11**white box test**

a systematic test in which test data based on the software specification is introduced to a program to assess the correct operation of sub-parts of the program

for example, data may be selected to execute as many instructions as possible, as many branches as possible and as many subroutines as possible

3.2.2.12**walk-through**

an evaluation process in which a designer or programmer leads members of an evaluation team through the hardware design, software design and/or software code the designer or programmer has developed, in order to identify possible errors in contrast to the inspection, the designer or programmer is active during this review

3.2.3 Definitions relating to fault/error control techniques for controls using software**3.2.3.1****full bus redundancy**

a fault/error control technique in which full redundant data and/or address are provided by means of redundant bus structure

3.2.3.2**multi-bit bus parity**

a fault/error control technique in which the bus is extended by two or more bits and these additional bits are used for error detection

3.2.3.3**single bit bus parity**

a fault/error control technique in which the bus is extended by one bit and this additional bit is used for error detection

3.2.3.4**code safety**

fault/error control techniques in which protection against coincidental and/or systematic errors in input and output information is provided by the use of data redundancy and/or transfer redundancy (see also 3.2.3.5 and 3.2.3.6)

3.2.3.5**data redundancy**

a form of code safety in which the storage of redundant data occurs

3.2.3.6**transfer redundancy**

a form of code safety in which data is transferred at least twice in succession and then compared this technique will recognize intermittent errors

3.2.3.7**comparator**

a device used for fault/error control in dual channel structures, which compares data from the two channels and initiates a declared response if a difference is detected

3.2.3.8**DC fault model**

a “stuck-at” fault model incorporating short circuits between signal lines

because of the number of possible short circuits in the device under test, usually only short circuits between related signal lines will be considered. A logical signal level is defined, which dominates in cases where the lines try to drive to the opposite level

3.2.3.9**equivalence class test**

a systematic test intended to determine whether the instruction decoding and execution are performed correctly. The test data is derived from the CPU instruction specification

similar instructions are grouped and the input data set is subdivided into specific data intervals (equivalence classes). Each instruction within a group processes at least one set of test data, so that the entire group processes the entire test data set. The test data can be formed from the following:

- data from valid range;
- data from invalid range;