SLOVENSKI STANDARD
SIST ENV 1954:1997

01-avgust-1997

Obnašanje elektronskih varnostnih naprav za plinske aparate pri notranjih in/ali zunanjih motnjah

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

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

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

Ta slovenski standard je istoveten z: **ENV 1954:1996**

ICS:

91.140.40	Sistemi za oskrbo s plinom	Gas supply systems
97.100.20	Plinski grelniki	Gas heaters

SIST ENV 1954:1997 **en**

EUROPEAN PRESTANDARD

PRÉNORME EUROPÉENNE

EUROPÄISCHE VORNORM

ENV 1954

June 1996

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 existance 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

Contents **Page**

Annexes

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 organisations 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.

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 recognise 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 prestandard 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 characterics:

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

- data from the bounds

- extreme values and their combinations

The tests within a group are run with different addressing modes, so that the entire group executes all addressing modes.

3.2.3.10 *error recognizing means:* Independent means provided for the purpose of recognizing errors internal to the system.

Examples are monitoring devices, comparators, and code generators.

3.2.3.11 *Hamming distance:* A statistical measure, representing the capability of a code to detect and correct errors. The Hamming distance of two code words is equal to the number of bit differences in the two code words.

3.2.3.12 *input comparison:* A fault/error control technique by which inputs that are designed to be within specified tolerances are compared.

3.2.3.13 *internal error detecting or correcting:* A fault/error control technique in which special circuitry is incorporated to detect or correct errors.

3.2.3.14 *frequency monitoring:* A fault/error control technique in which the clock frequency is compared with an independent fixed frequency.

An example is comparison with the line supply frequency.

3.2.3.15 *logical monitoring of the program sequence:* A fault/error control technique in which the logical execution of the program sequence is monitored.

Examples are the use of counting routines or selected data in the program itself or by independent monitoring devices.

3.2.3.16 *time-slot monitoring of the program sequence:* A fault/error control technique in which timing devices with an independent time base are periodically triggered in order to monitor the program function and sequence.

An example is a watchdog timer.

3.2.3.17 *time-slot and logical monitoring:* A combination of 3.2.3.15 and 3.2.3.16.

3.2.3.18 *multiple parallel outputs:* A fault/error control technique in which independent outputs are provided for operational error detection or for independent comparators.

3.2.3.19 *output verification:* A fault/error control technique in which outputs are compared with independent inputs.

This technique may or may not relate an error to the output which is defective.

3.2.3.20 *plausibility check:* A fault/error control technique in which program execution, inputs or outputs are checked for correct program sequence, timing or data.

Examples are the introduction of an additional interrupt after completion of a certain number of cycles or checks for division by zero.

3.2.3.21 *protocol test:* A fault/error control technique in which data is transferred to and from computer components to detect errors in the internal communications protocol.

3.2.3.22 *reciprocal comparison:* A fault/error control technique used in dual channel (homogeneous) structures in which a comparison is performed on data reciprocally exchanged between the two processing units.

Reciprocal refers to an exchange of similar data.