SLOVENSKI STANDARD
SIST EN 50133-1:1999

01-september-1999

Alarmni sistemi - Sistemi za nadzor dostopa za uporabo v aplikacijah varovanja - 1. del: Sistemske zahteve

Alarm systems - Access control systems for use in security applications - Part 1: System requirements

Alarmanlagen - Zutrittskontrollanlagen für Sicherungsanwendungen - Teil 1: Systemanforderungen

Systèmes d'alarme - Systèmes de contrôle d'accès à usage dans les applications de sécurité - Partie 1: Exigences système

Ta slovenski standard je istoveten z: **EN 50133-1:1996**

ICS:

13.320	Alarmni in opozorilni sistemi	Alarm and warning systems

SIST EN 50133-1:1999 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50133-1

October 1996

ICS 13.320

Descriptors: Alarm systems, control, access, buildings, safety, definitions, classifications, performance evaluation, tests, designation, marking

English version

Alarm systems - Access control systems for use in security applications Part 1: System requirements

Systèmes d'alarme - Systèmes de contrôle d'accès à usage dans les applications de sécurité
Partie 1: Règles relatives aux systèmes

Alarmanlagen - Zutrittskontrollanlagen für Sicherheitsanwendungen
Teil 1: Systemanforderungen

This European Standard was approved by CENELEC on 1995-11-28. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

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

CENELEC

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

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 79, Alarm systems.

The text of the draft was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 50133-1 on 1995-11-28.

The following dates were fixed:

- latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 1997-03-01

- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 1997-03-01

EN 50133 will consist of the following parts, under the general title "Alarm systems - Access control systems for use in security applications":

- Part 1 System requirements
- Part 2 Recognition equipment
- Part 3 Processing equipment - Display and programming equipment
- Part 4 Access point actuator
- Part 5 Communication
- Part 6 (free)
- Part 7 Application guidelines

Contents

Introduction

This standard describes the general requirements for functionalities of an access control system for use in security applications.

It also describes general components environmental requirements.

When a part of an access control system (eg. access point interface) forms a part of an intruder alarm system, that part shall also fulfil the relevant requirements of alarm intrusion standards.

This standard addresses the security application for each access point. An access control system may consist of any number of access points.

Different levels of confidence in identification of users requesting access at an access point have resulted in the definition of recognition classes.

The diversities of the market needs for access control systems have led to take into account systems with or without logging or time logging.

Access point actuators as electric door openers, electronic locks, turnstiles and barriers are covered by CEN/TC33 standards.

1 Scope

This standard specifies requirements for automated access control systems and components in and around buildings.

It includes :

- system architecture and general requirements of an access control system for security applications,

- requirements for functions,

- definition of the environmental and electromagnetic compatibility conditions,

- requirements for communication of an access control with others, such as access point actuators and sensors, alarm system, etc...

The standard does not apply to access point actuators and sensors.

2 Normative references

This European Standard incorporates by dated or undated reference, 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 Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies (including amendments).

EN 50081-1	1992	Electromagnetic compatibility - Generic emission standard - Part 1: Residential, commercial and light industry
EN 50081-2	1993	Electromagnetic compatibility - Generic emission standard - Part 2: Industrial environment
EN 50082	Series	Electromagnetic compatibility - Generic immunity standard
EN 55022	1994	Limits and methods of measurement of radio disturbance characteristics of information technology equipment (CISPR 22:1993)
EN 60950	1992	Safety of information technology equipment, including electrical business equipment (IEC 950:1991, modified)
IEC 68-1 + A1	1988 1992	Environmental testing - Part 1: General and guidance (harmonized as EN 60068-1:1994)
IEC 68-2-1	1990	Environmental testing - Part 2: Tests - Tests A: Cold (harmonized as EN 60068-2-1:1993)
IEC 68-2-2 + IEC 68-2-2A	1974 1976	Basic environmental testing procedures - Part 2: Tests - Tests B: Dry heat (harmonized as EN 60068-2-2:1993)

IEC 68-2-6 + A1 + A2	1982 1983 1985	Basic environmental testing procedures - Part 2: Tests - Test Fc and guidance: Vibration (sinusoidal) (harmonized as HD 323.2.6 S2:1988)
IEC 68-2-18	1989	Environmental testing - Part 2: Tests - Test R and guidance: Water
IEC 68-2-63	1991	Environmental testing - Part 2: Test methods - Test Eg: Impact, spring hammer (harmonized as EN 60068-2-63:1994)

3 Definitions

For the purpose of this standard, the following definitions apply :

3.1 **access:** Action of entry into or exit from a security controlled area.

3.2 **access control system:** System which comprises all the constructional and organisational measures as well as those pertaining to the apparatus which are required for controlling access.

3.3 **access control unit:** Device which makes the decision to release one or several access points and manages the associated control sequence.

3.4 **access group:** A number of users sharing the same access level.

3.5 **access grid:** One or more security controlled areas allocated to an access level.

3.6 **access level:** User authority in terms of access to a specified access grid and, if applicable, associated time grid.

3.7 **access point:** The location at which access can be controlled by a door, turnstile or other secure barrier.

3.8 **access point interface:** Device which controls releasing and securing of an access point.

3.9 **access point reader:** Device used to extract recognition data from a token or biometric. The device can have an associated keypad when used with memorised information.

3.10 **alert:** Request for human intervention after the activation of an indicator.

3.11 **annunciation:** Presentation of the information to management or other systems.

3.12 **apas:** Access point actuators and sensors. Examples of actuators are electric door openers, electric locks, turnstiles and barriers. Examples of sensors are contacts, switches, pressure signalling devices and door switches.

3.13 **apas closed:** An apas is closed when the access point does not afford free passage.

3.14 **apas open(ed):** An apas is open(ed) when the access point affords free passage.

3.15 **apas violation:** Unauthorised operation of an access point.

3.16 **biometric:** Information which is referring to unique physiological attributes of the user.

3.17 **event:** A change occurring within an access control system.

3.18 **false acceptance:** The granting of access to an unauthorised user.

3.19 **false rejection:** The denial of access to an authorised user.

3.20 **fault condition:** Any condition which leads to interruption or degradation of the access control system's functionality.

3.21 **memorised information:** Information known to the user.

3.22 **normal condition:** The access control system is fully functional and able to process all events according to the pre-set rules.

3.23 **power supply:** That part of an access control system which provides power for the operation of the system or any part thereof.

3.24 **processing:** The comparing of information with pre-set rules to make decisions concerning the granting or denying of access to users and/or the comparing of events with pre-set rules to produce appropriate actions.

3.25 **programmability:** Ability to receive and store pre-set rules.

3.26 **release:** The signal to the apas that access has been granted.

3.27 **security controlled area:** Area surrounded by physical barrier, including one or more access points.

3.28 **tamper protection:** Methods used to protect an access control system or part thereof against deliberate interference.

3.29 **time grid:** One or more time zones allocated to an access level.

3.30 **time zone:** One or more time slots combined with calendar information.

3.31 **time slot:** Interval of time between two given moments indicating the beginning and end of a valid period within a time zone.

3.32 **token:** Recognition data provided by access cards, keys, tags, etc.

3.33 **transaction:** An event which corresponds to the release of an access point following recognition of a user identity.

3.34 **user:** A person requesting passage through an access point.

3.35 **user identity:** Information which is transferred directly or via a token by the user to the recognition equipment.

4 Diagrams

4.1 Basic functions of an access control system

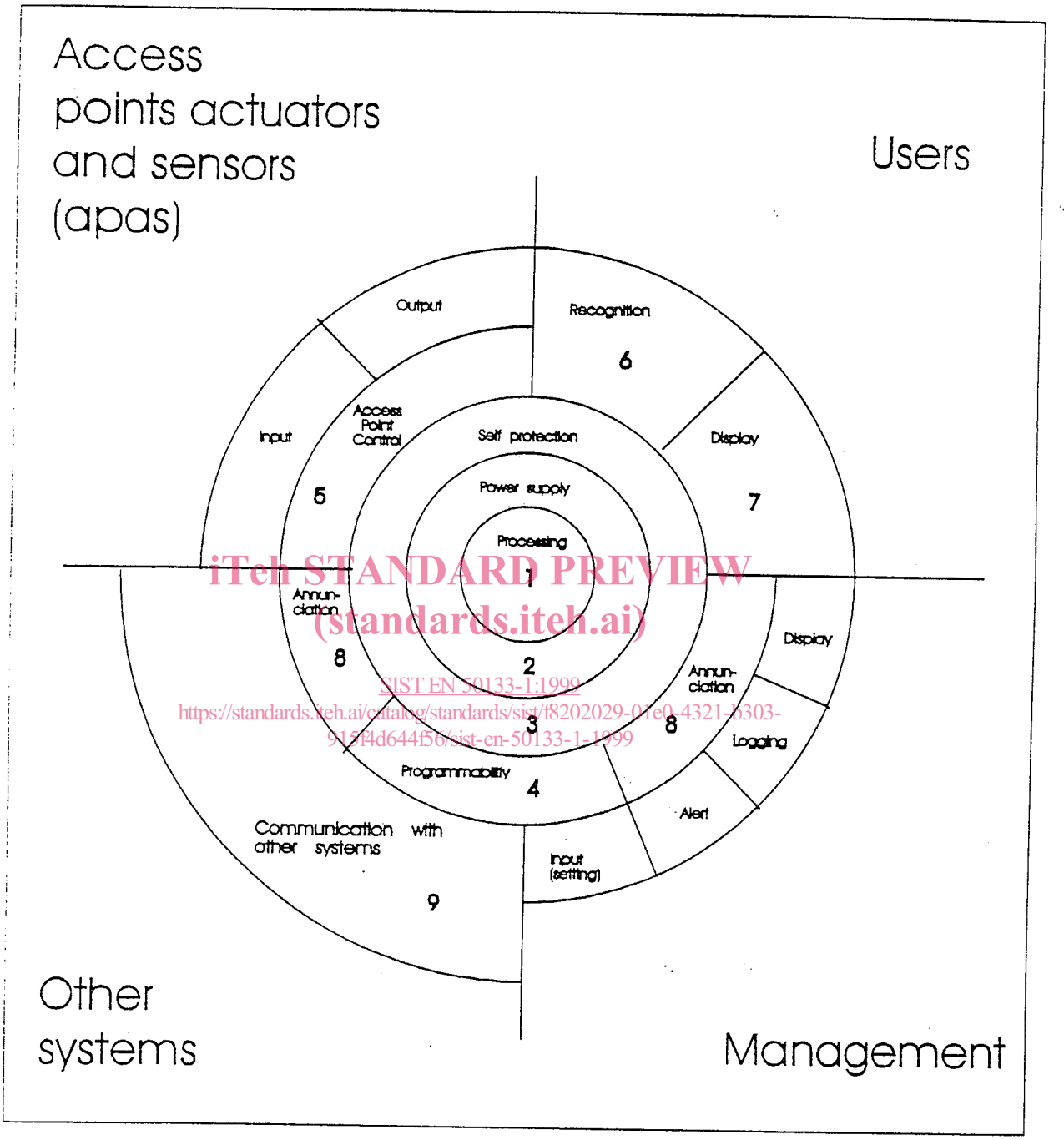

Figure 1: Basic functions of an access control system

The basic functions of an access control system are :

processing (1), power supply (2), self protection (3), programmability (4), access point control (5), recognition (6), display for the user (7), annunciation (8), communication with other systems (9).

4.2 Components of an access control system

The following diagram is an example of the distribution of functions in an access control system.

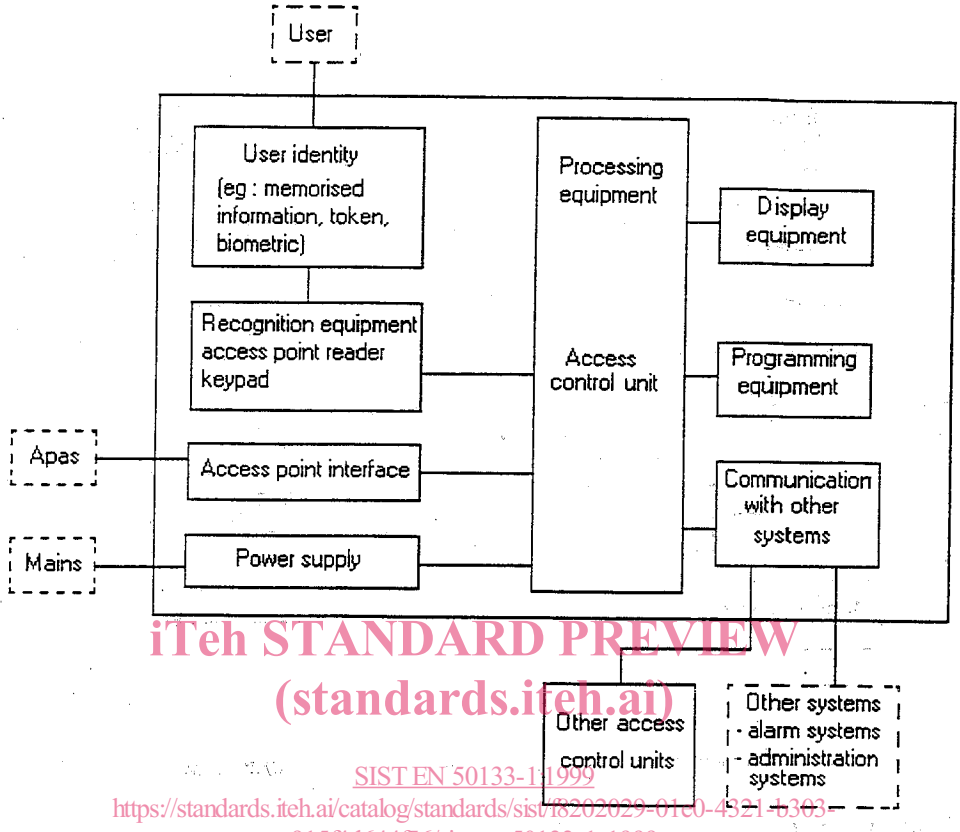

Figure 2: Distribution of functions in an access control system

NOTE: In figure 2, all components surrounded by dotted lines are not covered by this standard.

The functions may be distributed in more than one component, or may be integrated in one box.

4.3 Process of granting access

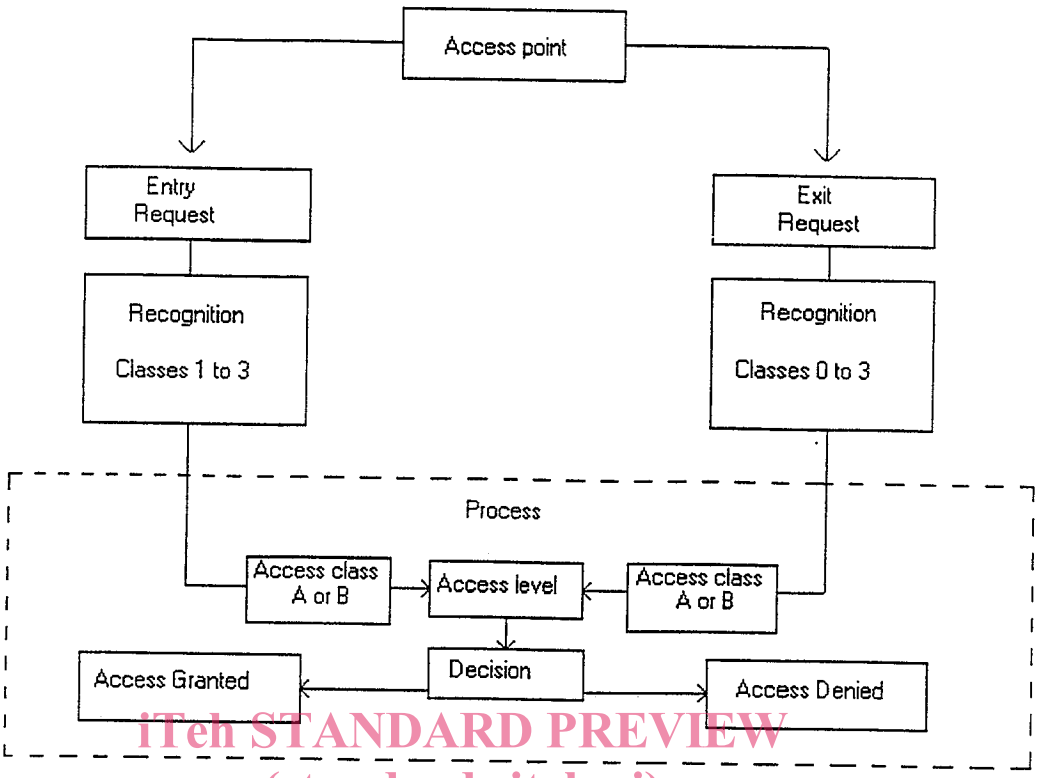

Figure 3: Traditional application of granting access

Figure 3 shows a traditional application. For other applications, the entry and exit can be reversed. The access control system, for each access point, shall have at least a positive recognition in one direction.

5 General requirements

5.1 Security classification

The security of an access control system is based on the recognition classification and the access classification.

The security classification can be defined for each access point for entry and exit individually.

The security classification is an independent combination of the recognition classes and the access classes.

5.1.1 Recognition classification

The following classification for access control systems is based on the level of confidence in the identification of authorised users.

The classification indicates the quality of relationship between the recognition used by a specific system and the actual user.