SLOVENSKI STANDARD
SIST EN 50133-7:2000

01-april-2000

Alarmni sistemi - Sistemi za nadzor dostopa za uporabo v aplikacijah varovanja - 7. del: Smernice za uporabo

Alarm systems - Access control systems for use in security applications - Part 7: Application guidelines

Alarmanlagen - Zutrittskontrollanlagen für Sicherungsanwendungen - Teil 7: Anwendungsregeln

Systèmes d'alarme - Systèmes de contrôle d'accès à usage dans les applications de sécurité - Partie 7: Guide d'application

Ta slovenski standard je istoveten z: **EN 50133-7:1999**

ICS:

13.320	Alarmni in opozorilni sistemi	Alarm and warning systems

SIST EN 50133-7:2000 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50133-7

August 1999

ICS 13.320

English version

Alarm systems - Access control systems for use in security applications Part 7: Application guidelines

Systèmes d'alarme - Systèmes de contrôle d'accès à usage dans les applications de sécurité
Partie 7: Guide d'application

Alarmanlagen - Zutrittskontrollanlagen für Sicherungsanwendungen
Teil 7: Anwendungsregeln

This European Standard was approved by CENELEC on 1999-01-01. 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, Czech Republic, 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

Ref. No. EN 50133-7:1999 E

Contents

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 50133-7 on 1999-01-01.

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) 2000-03-01
- latest date by which the national standards conflicting with the EN have to be withdrawn (dow) 2000-03-01

Introduction

This European standard has been established as a source of information for the managers and purchasers of access control systems and as a guideline for the establishment of tenders and for the installers and the maintainers

This European standard mainly covers the people flow to or in Security Controlled Areas and may also be used to control the flow of other things such as cars.

1 Scope

This standard provides guidelines for the application of an automated access control system and components in and around buildings based upon the EN 50133 series of standards.

It covers system design, installation, handover, operation and maintenance of access control systems.

The guidelines are intended for access control systems for use in security applications. They cover systems ranging from a simple single access point up to complex multiple access point systems.

An access control system is able to actuate and monitor access point actuators and sensors (apas). However, these guidelines do not cover the apas.

The access control system may be able to communicate with other systems (for example: an intrusion alarm system).

This standard does not recommend whether or not an automated access control system should be installed in any given premises.

2 Normative references

This standard incorporates by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate place 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.

EN 50133-1	1996	Alarm systems - Access control systems for use in security applications Part 1 : System requirements

3 Definitions

For the purpose of this standard, the definitions listed in EN 50133-1 and the following definitions apply :

3.1 anti-passback :

3.1.1 logical anti-passback : Operating mode which requires user validation when leaving a security controlled area in order to be able to re-enter and vice versa.

3.1.2 timed anti-passback : Operating mode which inhibits the access granting process at an access point or to a security controlled area for a preset period for a particular user once that user has been granted access.

3.1.3 area controlled anti-passback : Operating mode which requires the user to be present in a designated security controlled area in order to be able to enter another security controlled area.

3.2 apas : (EN 50133-1) Access point actuators and sensors.

EXAMPLE 1 : Actuators: electric door openers, electric locks, turnstiles and barriers.

EXAMPLE 2 : Sensors : contacts, switches, pressure signalling devices and door switches.

3.3 degraded mode : Mode where access is granted without performing all the full processing according to definition 3.24 of EN 50133-1.

3.4 duress alarm : Information providing the same results as a memorised information and which initiates an alert.

3.5 fail safe : Mode where apas affords free passage (apas open(ed)) when the power is removed.

3.6 fail secure : Mode where apas does not afford free passage (apas closed) when the power is removed.

3.7 logging : Recording of events.

3.8 override : Access granted by bypassing the decision process .

3.9 presence check : Control of the number (max., min.) of persons within a security controlled area.

3.10 singularisation : Limitation to one user passing an access point at the same time.

3.11 two users access condition : Procedure which ensures that access is granted provided two users have demonstrated their right of access within a preset period.

NOTE : A glossary of other common terms is provided in annex A.

4 General

An access control system comprises all the constructional and organisational facilities together with equipment required for controlling access.

The objective of the access control system is :

- to decide :
  - who is granted access.
  - where the access can be obtained.
  - if applicable, when the access is granted.
- to minimize the risk of unauthorised access.

Particular care should be taken to minimise inconvenience to authorised users.

The implementation of an access control system should be in accordance with the following sequence:

a) design of the system;

b) installation of the system;

c) hand-over of the system;

d) operation of the system;

e) maintenance of the system;

The process of implementation should follow national regulations.

An implementation plan should be agreed with the purchaser.

NOTE : It is advisable that a risk assessment should be performed before implementation

5 System design

5.1 Consultation

The requirements for the system design should be determined by consultation between the purchaser of the system (or his representative) and other interested parties.

The system design should be based on EN 50133-1.

If the system is to communicate with other applications particular care should be taken to meet the requirements of all applications. Measures should be taken to avoid contention.

5.2 Considerations

5.2.1 Access point

From information provided by the purchaser and the result of risk assessment, evaluate for each access point:

- security classification for entry and exit (recognition, time grid, logging.)
- user flow (number of persons in a period of time.)
- relation to other systems (for example : intrusion alarm system, CCTV, administration system,...)
- safety requirements (for example : emergency exits, fire protection...)
- requirements for annunciation (for example : display, logging, alert...)
- operation of access control system in fault conditions (for example : the need for a second source of power, equipment or cable failures ,...)
- environmental conditions of the site.
- other relevant conditions (risk of vandalism,...)
- the number of users and access levels taking into account both present and predicted future needs.
- location of the equipment.
- ease of operation (user, management, serviceability,...)
- co-operation of users (motivation, training,...)
- physical strength of apas and building structure corresponding to the security classification.
- necessity for user singularisation at the apas.
- method of return to apas closed (for example : automatic door closing equipment.)
- the cable routes, the type of cable, the maximum cable length.
- suitability of the recognition equipment (life time of equipment, user flow, environment,...)
- operating configuration for apas (fail safe, fail secure,...)
- measures for disabled persons.
- measures for deliveries and baggage.
- the management of the system (programming, annunciation).

5.2.2 Multiple access points

For a system with multiple access point evaluate, in addition to the above :

- the security classification for access points leading to the same security controlled area.
- the total number of users and access levels taking into account both present and predicted future needs,
- the capacity of the logging device,
- the communication links (availability , reliability , security) between different sites and / or other systems,
- co-ordination of annunciation functions (location, procedures, presentation,...).