SLOVENSKI STANDARD
SIST EN 50132-1:2010

01-december-2010

Alarmni sistemi - Nadzorni sistemi CCTV za uporabo v aplikacijah varovanja - 1. del: Sistemske zahteve

Alarm systems - CCTV surveillance systems for use in security applications - Part 1: System requirements

Alarmanlagen - CCTV-Überwachungsanlagen für Sicherungsanwendungen - Teil 1: Systemanforderungen

Systèmes d’alarme - Systèmes de surveillance CCTV à usage dans les applications de sécurité - Partie 1: Exigences système

Ta slovenski standard je istoveten z: EN 50132-1:2010

ICS:

13.320	Alarmni in opozorilni sistemi	Alarm and warning systems
33.160.40	Video sistemi	Video systems

SIST EN 50132-1:2010 en,fr,de

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50132-1

March 2010

ICS 13.310;33.160.40

English version

Alarm systems - CCTV surveillance systems for use in security applications - Part 1: System requirements

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

Alarmanlagen -
CCTV-Überwachungsanlagen
für Sicherungsanwendungen -
Teil 1: Systemanforderungen

This European Standard was approved by CENELEC on 2010-03-01. 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, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

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

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 79, Alarm systems. It was submitted to the formal vote and approved by CENELEC on 2010-03-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

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)	2011-03-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-03-01

EN 50132 will consist of the following parts, under the general title *Alarm systems – CCTV surveillance systems for use in security applications:*

Part 1: System requirements;

Part 5: Video transmission;

Part 7: Application guidelines.

Contents

Figures

Tables

Introduction

This European Standard applies to CCTV Systems for surveillance of private and public areas. It includes four security grades and four environmental classes.

This European Standard is intended to assist CCTV System companies, manufacturers, system integrators, installer, consultants, owner, users, insurers and law enforcement in achieving a complete and accurate specification of the surveillance system. This European Standard does not specify the type of technology or the required image quality needed for a certain observation task.

Due to the wide range of CCTV system applications like security, safety, public safety etc. only the minimum requirements are covered in this European Standard.

For achieving an optimal surveillance system in terms of design, planning, operation, installation and maintenance, follow the Application Guidelines of EN 50132-7:1996. The specified operational requirements (Clause 5) should enable the above mentioned stakeholders to choose the functions that are important for their application with due consideration to the risk.

Special National standards apply as well.

This European Standard is not intended to be used for testing individual CCTV components.

1 Scope

This European Standard specifies the minimum requirements for CCTV Surveillance Systems installed for security applications. This European Standard specifies the minimum performance requirements and functional requirements to be agreed on between customer and supplier in the operational requirement, but does not include requirements for design, planning, installation, testing, operation or maintenance (see Application Guidelines in EN 50132-7:1996). This European Standard excludes installation of remotely monitored detector activated CCTV systems.

This European Standard also applies to CCTV Systems sharing means of detection, triggering, interconnection, control, communication and power supplies with other applications. The operation of a CCTV System shall not be adversely influenced by other applications.

Requirements are specified for CCTV components where the relevant environment is classified. This classification describes the environment in which the CCTV component may be expected to operate as designed. When the requirements of the four environmental classes are inadequate, due to the extreme conditions experienced in certain geographic locations, special national conditions may be applied.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CLC/TS 50398	Alarm systems – Combined and integrated alarm systems – General requirements
EN 50130-4	Alarm systems – Part 4: Electromagnetic compatibility – Product family standard: Immunity requirements for components of fire, intruder and social alarm systems
EN 50130-5	Alarm systems – Part 5: Environmental test methods
EN 50132-7:1996	Alarm systems – CCTV surveillance systems for use in security applications - Part 7: Application guidelines
EN 60065	Audio, video and similar electronic apparatus – Safety requirements (IEC 60065)
EN 60950-1	Information technology equipment – Safety – Part 1: General requirements (IEC 60950-1)
EN 61000-6-3	Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments (IEC 61000-6-3)

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
access levels
level of access to particular functions of the CCTV system, defining the user rights of the operator, to control and configure the system as well as the access to data's on the CCTV system

3.1.2
acknowledge
action of a user to accept a message or an indication

3.1.3
action
deliberate operation or act by the user which is part of alarm procedure

3.1.4
Advanced Streaming Format
proprietary digital audio/digital video container format, especially meant for streaming media

3.1.5
alarm
warning of the presence of any hazard to life, property or the environment

3.1.6
alarm condition
condition of an alarm system, or part thereof, which results from the response of the system to the presence of a hazard

3.1.7
alarm message
message from the system to the operator, to describe time, type and location of an alarm

3.1.8
alarm procedure
indications and manual or automatic controls as response to an alarm condition

3.1.9
alarm receiving centre
continuously manned centre to which information concerning the status of one or more alarm systems is reported

3.1.10
alert
warning addressed to persons in the danger environment or request for human intervention (police, fire brigade, etc.), caused by alarm, tamper or fault

NOTE Sometimes the term “alarm warning” is used instead.

EXAMPLE Visual-alert, acoustic/ audible-alert, external-alert.

3.1.11
alternative device
CCTV system component of the same type like the primary device

3.1.12
alternative power source
power source capable of powering the system for a predetermined time when a prime power source is unavailable

3.1.13
archive
data stored on a long term permanent, or partially permanent storage

EXAMPLE CD's or digital tape are considered to be 'archived'.

3.1.14
area of interest
region in the scene monitored by an image capturing device

3.1.15
attended operator desk
continuously manned workstation

3.1.16
archiving
see image data backup

3.1.17
audio video interleave format
proprietary multimedia format containing audio and video data in a standard container that allows synchronous audio-with-video playback

3.1.18
authentication
method to verify whether an image has been altered

3.1.19
authorization
permission to gain access to specified functions or components of a CCTV system

3.1.20
authorisation codes
physical or logical keys which permit access to CCTV functions

3.1.21
automatic number plate recognition
optical character recognition on images to read and extract the alphanumerics of the licence plate of vehicles

3.1.22
automatic teller machine
device that provides a method of financial transactions in public space without the need for a human clerk

3.1.23
backup image
an accurate and complete replica of the primary image, irrespective of media

3.1.24
bandwidth
(relating to interconnection) data transfer rate or amount of data that can be transferred from one point to another in a given time period

NOTE Bandwidth is quoted in bits per s.

3.1.25
capacity
(relating to recording) the total amount of stored information that a storage media or medium can hold. It is expressed as a quantity of bits or bytes

3.1.26
charge coupled device
sensor of imaging device, consisting of an integrated circuit with an array of linked, or coupled, light-sensitive capacitors

3.1.27
CCTV system
system consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes

3.1.28
channel
single path for conveying digital or analogue data, distinguished from other parallel paths

EXAMPLE Video input or output channel.

3.1.29
checksum
unique value or key computed by an algorithm for a data packet, based on the information it contains

NOTE It is passed along with the data to authenticate that the data has not been tampered with. Any change to the image data, metadata or image sequence would cause a change in the resultant checksum.

3.1.30
compression
the process of reducing the size of a data (image) file

3.1.31
compression rate
ratio of a file's or image's uncompressed size compared to its compressed size

NOTE A high compression rate means smaller image files and lower image quality and vice versa.

3.1.32
common interconnection
interconnection used by several video and data channels and/or other applications

3.1.33
communication
transmission of messages and/or signals between CCTV components

3.1.34
component
functional part of the CCTV system

3.1.35
continually
recurring frequently at regular intervals

3.1.36
contrast
(relating to image) difference in visual properties that makes an object (or its representation in an image) distinguishable from other objects and the background

NOTE In visual perception of the real world, contrast is determined by the difference in the colour and brightness of the object and other objects within the same field of view.

3.1.37
data
image, meta and other data of the CCTV system

3.1.38
data acquisition
sampling of information to generate data by processing of signals with appropriate sensors converting the measurement parameter to a signal

3.1.39
data backup
method to store original data in a media with the goal to recover the original data in case of data loss. destruction or system failure

3.1.40
database
structured collection of records or data. Records are retrieved in answer to queries

3.1.41
data identification
capability to find, retrieve or delete specific data without ambiguity e.g. by the use of unique IDs

3.1.42
data integrity
condition when data has not been modified or altered from its source either maliciously or by accident and in which data are maintained during any operation, such as transmission, storage, and retrieval, in order to preserve data for their intended use

3.1.43
data management
management of user-actions, audio-/video-data and general information's that are not part of the activity management

3.1.44
data manipulation protection
means to guarantee the integrity of data

EXAMPLE Certified data handling, encryption, watermarking and limited access to the data.

3.1.45
default (by)
parameter settings preset by the system unless changed

3.1.46
digital image
image consisting of pixels using ranges of discrete values

3.1.47
digital video recorder
system that is capable of recording, playback, backup and export of digital images captured by image sources. A video recorder may consist of one or multiple components, spread across a network

3.1.48
documentation
(relating to the system) paperwork (or other media) prepared during the design, installation and hand over of the system recording details of the CCTV system

NOTE Component documentation provided by the manufacturer of the device in paper or on another media.

3.1.49
electronic article surveillance
technological method for preventing shoplifting e.g. from retail stores

3.1.50
encryption
systematic encoding of a bit stream before transmission, so that the information contained in the bit stream cannot be deciphered by an unauthorised party;
scrambling of digital data that forms an image according to a key based algorithm in such a way that it is difficult to reconstruct the original recorded image without the key

NOTE A reverse algorithm is required to reconstruct the image. Data encryption shall not prevent authorised users to access the images.

3.1.51
essential functions
vital functions of a CCTV system, which are image capturing, transmission, recording and/or presentation

3.1.52
event
incident in the real world

EXAMPLE A fire (burning house), an intrusion (broken door) or moving person, a power-failure, a short circuit, presence of an intruder

3.1.53
event driven action
user or system activity driven by an alarm- or trigger-signal

3.1.54
event recording
event controlled recording or storing of image signals for a pre-determined time

3.1.55
exact copy
transfer of data from original recording location or master copy to secondary storage, if digital as bit for bit copy

3.1.56
export
transfer of data from the original location to a secondary storage location with a minimum of necessary changes

3.1.57
external input
external source connected to a dedicated input on the CCTV system

3.1.58
external interconnection
interconnections exchanging data over the boundary of the system