SLOVENSKI STANDARD

SIST EN 50132-5-1:2012

01-februar-2012

Nadomešča:

SIST EN 50132-5:2001

Alarmni sistemi - Nadzorni sistemi CCTV za uporabo v aplikacijah varovanja - 5.1. del: Video prenos - Splošne zahteve za zmogljivosti video prenosa

Alarm systems - CCTV surveillance systems for use in security applications - Part 5-1: Video transmission - General video transmission performance requirements

Alarmanlagen - CCTV-Überwachungsanlagen für Sicherungsanwendungen - Teil 5-1: Allgemeine Leistungsanforderungen an die Videoübertragung

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Systèmes d’alarme – Systèmes de surveillance CCTV à usage dans les applications de sécurité - Partie 5-1: Exigences générales de performance pour la vidéotransmission

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/89652519-1edb-4f95-a6f6-78d070aca2f6/sist-en-50132-5-1-2012

Ta slovenski standard je istoveten z: EN 50132-5-1:2011

ICS:

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

SIST EN 50132-5-1:2012 en

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 50132-5-1:2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

SIST EN 50132-5-1:2012

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50132-5-1

December 2011

ICS 13.310; 33.160.40

Supersedes EN 50132-5:2001 (partially)

English version

Alarm systems - CCTV surveillance systems for use in security applications - Part 5-1: Video transmission - General video transmission performance requirements

Systèmes d'alarme – Systèmes de surveillance CCTV à usage dans les applications de sécurité - Partie 5-1:Exigences générales de performance pour la vidéotransmission

Alarmanlagen - CCTV-Überwachungsanlagen für Sicherungsanwendungen - Teil 5-1: Allgemeine Leistungsanforderungen an die Videoübertragung

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

This European Standard was approved by CENELEC on 2011-10-31. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre 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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

© 2011 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 50132-5-1:2011 E

SIST EN 50132-5-1:2012

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50132-5-1:2012
78d070aca2f6/sist-en-50132-5-1-2012

SIST EN 50132-5-1:2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figures

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

Tables

SIST EN 50132-5-1:2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

SIST EN 50132-5-1:2012

Foreword

This document (EN 50132-5-1:2011) has been prepared by CLC/TC 79, "Alarm systems".

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2012-10-31
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2014-10-31

This document, together with EN 50132-5-2 and future EN 50132-5-3, supersedes EN 50132-5:2001.

This document introduces new general requirements on video transmission.

EN 50132 consists of the following parts, under the generic title *Alarm systems – CCTV surveillance systems for use in security applications*

Part 1	System requirements
Part 5-1	General video transmission performance requirements
Part 5-2	IP video transmission protocols
Part 5-3	Video transmission – Analog and digital video transmission
Part 7	Application guidelines

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-

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

SIST EN 50132-5-1:2012

Introduction

The European Electrotechnical Standardisation Organisation for alarm systems together with many governmental organisations, test houses and equipment manufacturers has defined a common framework for surveillance video transmission in order to achieve interoperability between products.

This video transmission standard is divided into 3 independent parts and sections:

Part 1: General video transmission performance requirements

Part 2: IP video transmission protocols

Part 3: Analog and digital video transmission

Each part offers its own clauses on scope, references, definitions, requirements.

The purpose of the transmission system in a closed circuit television (CCTV) installation is to provide reliable transmission of video signals between the different types of CCTV equipment in security, safety and monitoring applications.

Today CCTV surveillance systems reside in security networks using IT infrastructure, equipment and connections within the protected site itself.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

SIST EN 50132-5-1:2012

1 Scope

This European Standard introduces general requirements on video transmission. A detailed specification on analog video transmission over different media including signal and performance requirements is already defined in prEN 50132-5-3. For the growing number of surveillance applications based on IP video transmission the requirements are defined in 2 standards. This standard covers in the following clauses the general requirements for video transmissions on performance, security and conformance to basic IP connectivity, based on available, well-known, international standards. In areas where more detailed IP requirements are necessary additional specifications are given, in order to reach compatibility. In this European Standard no detailed and special CCTV protocols are defined. In Part 2 of this European Standard, a detailed video IP protocol, messages and commands on top of the general connectivity and performance requirements of Part 1 are defined. Part 2 defines an IP protocol for full interoperability (e.g. PTZ control, eventing, etc.) of video transmission devices used in surveillance applications.

The first section of this standard defines the minimum performance requirements on video transmission for security applications in IP networks. In surveillance applications, the requirements on timing, quality and availability are strict and defined in the last section of this standard. Guidelines for network architecture on how these requirements can be fulfilled are given.

The second section of this European Standard defines requirements on basic IP connectivity of video transmission devices to be used in security applications. If a video transmission device is used in security, certain basic requirements apply. First of all a basic understanding of IP connectivity needs to be introduced which requests the device to be compliant to fundamental network protocols. These could be requirements which may be applied to all IP security devices even beyond IP video. For this reason, requirements are introduced in a second step for compliance to basic streaming protocols, used in this standard for video streaming and stream control. Since security applications need high availability and reliability, general means for the transmission of the video status and health check events need to be covered. Theses are defined in general requirements on eventing and network device management. In security proper maintenance and setup is essential for the functioning of the video transmission device: Locating streaming devices and their capabilities is a basic requirement and covered in "device discovery and description".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

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.

EN 50132-1, *Alarm systems — CCTV surveillance systems for use in security applications — Part 1: System requirements*

EN 50132-7, *Alarm systems — CCTV surveillance systems for use in security applications — Part 7: Application guidelines*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1
adaptive jitter buffering
queuing of packet s in switched networks exposed to unwanted variations in the communications signal to ensure the continuous video transmission over a network supported by the "Adaptive" ability to adjust the size of the jitter buffer based on the measured jitter in the network

SIST EN 50132-5-1:2012

EXAMPLE If the jitter increases, the buffer becomes larger and can store more packets; if the jitter decreases, the buffer becomes smaller and stores fewer packets.

3.1.2
advanced Encryption Standard (AES)
NIST encryption standard, also known as Rijndael, specified as unclassified, publicly-disclosed, symmetric encryption algorithm with a fixed block size of 128 bits and a key size of 128 bits, 192 bits or 256 bits according to the Federal Information Processing Standards Publication 197

3.1.3
ASCII (American Standard Code for Information Interchange)
de-facto world-wide standard for the code numbers used by computers to represent all the upper and lower-case characters

3.1.4
asymmetric algorithm
algorithm used in the asymmetric cryptography, in which a pair of keys (a private key and a public key) is used to encrypt and decrypt a message to ensure the privacy of communications

3.1.5
authentication
process where an operators or systems identity is checked within a network

EXAMPLE In networks, authentication is commonly done using logon passwords.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.6
authentication server
device used in network access control which stores the usernames and passwords that identify the clients logging on or which may hold the algorithms for access

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

NOTE For access to specific network resources, the server may itself store user permissions and company policies or provide access to directories that contain the information. Protocols such as RADIUS, Kerberos and TACACS+, and 802.1x are implemented in an authentication server to perform user authentications.

3.1.7
authenticity
integrity and trustworthiness of data or an entity; validity and conformance of the information, or identity of a user

NOTE The authenticity can be secured and verified using cryptographic methods.

3.1.8
authorization
approval, permission, or empowerment for a user or a component to do something

3.1.9
backbone
high-speed line or series of connections that forms a major pathway within a network

3.1.10
backbone layer
larger transmission line that carries data gathered from smaller communication lines that interconnect with it, e.g. a line or set of lines that local area networks connect to, in order to span distances efficiently e.g. between buildings

3.1.11
Bits-per-Second (BpS)
unit or measurement of how fast data is transferred from one node to another

SIST EN 50132-5-1:2012

3.1.12
bridge
device used to connect two networks including passing data packets between them using the same protocols

3.1.13
certificate authority
issuer of security certificates used in SSL connections

3.1.14
client
component that contacts and obtains data from a server

3.1.15
client/server
communication system providing services like video streams, storage, logon access, data communication management and clients (workstations) bscribing these services

NOTE A Hub is a communication device that contains multiple ports

3.1.16
codec
compression-Decompression or enCOder/DECoder process

3.1.17
Common Gateway Interface (CGI)
standardized method of communication between a client, e.g. web browser, and a server, e.g. web server

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.18
compression delay
delay caused by the compression of data

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

3.1.19
congestion
situation in which the traffic presents on the network exceeds available network bandwidth/ capacity

3.1.20
core layer
part of the network providing optimal transport between sites or system functionality e.g. recording

3.1.21
Data Encryption Standard (DES)
cryptographic algorithm method developed by the US National Bureau Standards

3.1.22
Dynamic Host Configuration Protocol (DHCP)
protocol by which a network component obtains an IP address (and other network configuration information) from a server on the local network

3.1.23
distribution layer
part of the network providing policy-based connectivity

3.1.24
Domain Name System (DNS)
system that translates Internet domain names into IP addresses

SIST EN 50132-5-1:2012

3.1.25
dual homing
single device offering two or more network interfaces

3.1.26
dynamic Jitter buffer
collecting and storing video data packets for processing them in evenly spaced intervals to reduce distortions in the display

3.1.27
encryption
type of network security used to encode data so that only the intended destination can access or decode the information

3.1.28
fail-over
capability of an application to recover from a failure on an entity by automatically switching over to a surviving instance, providing no loss of data or continuity, also known as "run-time failover" and often used in connection with

3.1.29
forensics
field of science of applying digital technologies to legal questions arising from criminal investigations

3.1.30
frame
data structure that collectively represents a transmission stream including headers, data, and the payload and provides information necessary for the correct delivery of the data

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/09653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

3.1.31
gateway
hardware or software set-up that translates between two dissimilar protocols

3.1.32
H.261
ITU video coding standard originally designed for ISDN lines and data rate with multiples of 64Kbit/s using RTP

3.1.33
H.263
ITU standard supporting video compression (coding) for streaming video via RTP based on and replacing the H.261 codec

3.1.34
H.264
ISO ITU-T MPEG-4 Part 10 standard, also named Advanced Video Coding (AVC) supporting video compression (coding) from low bit-rate network streaming applications to HD video applications with near-lossless coding for network-friendly video representation

3.1.35
Host
computer on a network that is a repository for services available to other components on the network

3.1.36
hot-swap
property of controller which allows circuit boards or other devices to be removed and replaced while the system remains powered up and in operation

SIST EN 50132-5-1:2012

3.1.37
Hyper Text Mark-up Language (HTML)
coding language used to create Hypertext documents for use on the World Wide Web

3.1.38
Hypertext Transfer Protocol (HTTP)
connection oriented protocol for transmitting data over a network or protocol for moving hyper text files across the Internet

3.1.39
Hypertext Transfer Protocol Secure (HTTPS)
encrypts and authenticates communication between server and clients

3.1.40
Internet Control Message Protocol (ICMP)
error protocol indicating, for instance, that a requested service is not available or that a host or router could not be reached

3.1.41
ID identification
machine-readable character string

3.1.42
IEEE 802.1x
method for authentication and authorization in IEEE-802 networks using an authentication server e.g. RADIUS server

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.43
Institute of Electrical and Electronics Engineers (IEEE)
professional association of engineers for the advancement of technology

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070ee23f6/sist-en-50132-5-1-2012

3.1.44
Internet Group Management Protocol (IGMP)
communications protocol used to manage the membership of IP multicast groups

3.1.45
Internet Protocol (IP)
network layer 3 protocol in the OSI model containing addressing and control information to enable data packets to be routed in a network and primary network layer protocol in the TCP/IP protocol suite according to IETF RFC 791

3.1.46
IP Address (Internet Protocol Address)
unique number consisting of 4 parts separated by dots, e.g. 196.162.245.2, of a device attached to an IP network

NOTE Each device on an IP network uses a unique address. Every IP data packet contains a source address (sender) and a destination address (recipient). Each IP address consists of 32-bits that are arranged into four 8-bit “octets” (x.x.x.x). IP addresses range from 0.0.0.0 to 255.255.255.255.

3.1.47
IP Internet Protocol
main protocol used in conjunction with TCP (Transfer Control Protocol) (see TCP/IP)

3.1.48
IPS Images per Second
measurement or unit for the rate of pictures transmitted or displayed to create a video stream

NOTE A rate of 25 IPS (PAL) or 30 IPS (NTSC) is considered to be real-time or full motion video.

SIST EN 50132-5-1:2012

3.1.49
Internet Protocol, version 4 (IPv4)
most widely used version of the Internet Protocol (the "IP" part of TCP/IP.)

3.1.50
Internet Protocol Version 6 (IPv6)
successor to IPv4

NOTE Already deployed in some cases and gradually spreading, IPv6 provides a huge number of available IP Numbers - over a sextillion addresses. IPv6 allows every device on the planet to have its own IP Number.

3.1.51
Institute of Radio Engineers (IRE)
unit or measurement of the analog video amplitude that divides the area from the sync level to peak white level into 140 equal units

NOTE 140 IRE equals 1Volt peak-to-peak. The range of active video is 100 IRE.

3.1.52
KBit/s Kilobits per second
unit of data transmission rate

3.1.53
latency
time that elapses between the initiation of a network request for data and the start of the actual data transfer

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.54
layer 2 switch
OSI (Open Systems Architecture) data link layer device responsible for transmitting data across the physical links in a network

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

3.1.55
layer 3 device
OSI device that determines network addresses, routes and quality of service for information transport

EXAMPLE A router is a Layer 3 device; switches can also have Layer 3 capability.

3.1.56
Local Area Network (LAN)
communications network serving users and devices within a limited geographical area, such as a building or a protected area

3.1.57
local-access layer
part of the network bringing edge devices into the network and providing operator access

3.1.58
login
account name used to gain access to a component to be used in combination with a password or the act of connecting to a component or system by giving valid credentials (usually „username" and "password")

3.1.59
managed switch
switch that can be monitored and administered in the network via its own IP address

3.1.60
Media Access Control (MAC) Address
unique identifier attached to network adapters acting like a name for a particular adapter

SIST EN 50132-5-1:2012

3.1.61
Management Information Base (MIB)
structured collection of information for remote servicing using the SNMP protocol

3.1.62
Multipurpose Internet Mail Extensions (MIME)
standard for defining the type of payload streamed from a server to a client

EXAMPLE "video/h264" is used for streaming H.264 encoded video.

3.1.63
MJPEG (Motion JPEG)
digital video encoding standard, where each video frame is separately compressed into a JPEG image

3.1.64
Motion Pictures Experts Group (MPEG) standard
ISO/IEC video and audio encoding standard

3.1.65
MPEG-4
digital video encoding and compression standard that uses interframe encoding to significantly reduce the size of the video stream being transmitted compared to intraframe only encoding

NOTE In interframe coding, a video sequence is made up of so called I- or key-frames that contain the entire image. In between the key-frames are delta frames, which are encoded with only the incremental differences. This often provides substantial compression because in many surveillance video sequences, only a small part of the pixel is different from one frame to another.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.66
multicast
bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information, here video content, to multiple network recipients

SIST EN 50132-5-1:2012
https://standards.iteh.ai/catalog/standards/sist/99653519-1adb-4d05-ab2f-78d070aca2f6/sist-en-50132-5-1-2012

3.1.67
N+1 fail-over
fail-over capability of N identical applications in operation by automatically switching over to 1 unused application instance

3.1.68
N+n redundancy
capacity of a parallel redundant system with N representing the number of applications needed to meet the critical load and n is the number of extra applications for redundancy purposes

3.1.69
network connectivity
physical (wired or wireless) and logical (protocol) connection of a computer network or an individual device to a network

3.1.70
network design
way of arrangement of the various clients and servers in a network for the purposes of connectivity, performance, and security

3.1.71
network layer
layer 3 of the OSI Reference Model, controlling communication links and data routing across one or more links