BS EN 50132-1:2010

Incorporating corrigendum June 2010

BSI Standards Publication

Alarm systems — CCTV surveillance systems for use in security applications

Part 1: System requirements

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 50132-1:2010, incorporating corrigendum June 2010.

The UK participation in its preparation was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/10, Closed circuit television (CCTV).

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 72198 4

ICS 13.310; 13.320; 33.160.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2010.

Amendments/corrigenda issued since publication

Amd. No.	Date	Text affected
	30 September 2010	Implementation of CENELEC corrigendum June 2010: modification to 6.3.2.2.2

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50132-1

March 2010

ICS 13.310;33.160.40

Incorporating corrigendum June 2010

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

3.1.59
external system
system not directly connected to the CCTV system exchanging data over the boundary of the systems from outside to inside

3.1.60
failover
capability to switch over automatically to a redundant or standby component or system, upon the failure or abnormal termination of the previously active component or system

3.1.61
fail-safe
function or method which ensures that a failure of equipment, process, or system does not propagate beyond the immediate environs of the failing entity

EXAMPLE A device causing no harm or at least a minimum of harm to other devices or hazards to personnel on failure or operator error.

NOTE A fail-safe system has been designed in a way that the probability of a failure is extremely low to accomplish its assigned mission regardless of environmental factors.

3.1.62
fault
condition of the system which prevents the CCTV system or parts thereof functioning normally

3.1.63
fault message
message from the system to the operator, to describe time, type and location of a fault

3.1.64
fingerprint
method of generating a unique ‘fingerprint’ of the original recorded image that cannot be reproduced if the image is altered

3.1.65
frame rate
numbers of frames per second

3.1.66
graphics interchange format
8-bit-per-pixel bitmap image format

3.1.67
hazard
danger criteria of any event or incident, used to be detected by a sensor

EXAMPLE Smoke or movement.

3.1.68
illumination
(related to imaging device) level of illumination (illuminance) at the sensor of the imaging device;
(related to scene) level of illumination (illuminance) on the area to be kept under surveillance

3.1.69
image
visible representation of a frame as rectangular grid of pixels; see also picture

3.1.70
image analysis
extraction of quantitative information from an image beyond which is readily apparent through visual examination

3.1.71
image capturing
transformation of images from an optical- or scanning-device in video-signals or digital data format

3.1.72
image handling
any activity that transforms an input image into an output image with as little changes as possible

3.1.73
image processing
method to change or analyse (digital) images with algorithms or (software) procedures

EXAMPLE Compressing and encryption of images, methods for image content analysis.

3.1.74
image scene
collection of visual information of the physical area being across the width of the imaging sensor where something occurs (an incident or event)

3.1.75
image sequence
linear group of images handled as one entity, usually time indexed

3.1.76
image source
device that delivers video data

3.1.77
image stream
a series of consecutive images from the same image source which are transmitted from one system component to another

3.1.78
incident
activity that raises cause for concern that an offence has been, is being or is about to be, committed, or that an occurrence has taken place warranting specific action by an operator

3.1.79
indication
information (in audible, visual or any other form) provided to assist the user in the operation of a CCTV system

3.1.80
instant replay
playback of recently recorded images from storage

EXAMPLE Playback of a image sequence right after an incident or event.

3.1.81
interconnections
medium by which messages and/or signals are transmitted between CCTV system components

3.1.82
interface
(relating to system) means to exchange data between the CCTV system and an external system

EXAMPLE Digital inputs.

3.1.83
JPEG
common standard for image compression, defined by the Joint Photographic Experts Group

NOTE The JPEG file format is ISO 10918.

3.1.84
latency time
time delay between the moment something is initiated, and the moment one of its effects begins

NOTE The time from the source sending a signal to the destination receiving it.

3.1.85
liquid crystal display
thin, flat display device made up of any number of colour or monochrome pixels arrayed in front of a light source or reflector

3.1.86
location identifying data
data which uniquely identifies the physical location of a device

3.1.87
logical authorisation key code
numeric or alphabetic codes entered by an authorized user to gain access to restricted functions or parts of the CCTV system

3.1.88
key
object with mechanical, logical or electronic code that unlocks a locking mechanism to transform encrypted data into original data

3.1.89
master copy
backup as identical copy of the original recording, in digital systems an exact bit for bit copy

3.1.90
master image
backup image

3.1.91
maximum storage time
retention period or specified time for which images are to be held in primary storage media

3.1.92
meta data
any secondary information or data associated with images in a CCTV system

EXAMPLE Time and date, text strings, location identifying data, audio and any other associated, linked or processed information.

3.1.93
message
series of signals routed by a network which include identification, function data and the various means for providing its own integrity, immunity and proper reception

3.1.94
monitoring
(relating to component condition) process of verifying that interconnections and components are functioning correctly;
(relating to operator activity) viewing live images in order to detect events or incidents

3.1.95
MPEG
common standard used for coding and compression of moving images, defined by Moving Picture Experts Group in different versions

NOTE Examples are MPEG-2 and MPEG-4

3.1.96
multiplexer
switching device providing the simultaneous representation of several data streams such as video audio, etc. via one single transmission media

3.1.97
normal operation
state of the CCTV system when not in power-up or power down procedures

3.1.98
notification
passing an alarm or a message of the CCTV system to an external system

3.1.99
object mask
means to mark an object of the area of interest in the camera image display

3.1.100
obscuring
preventing the imaging device from viewing any part of the area of interest other than by moving the device

3.1.101
operational requirement
key document for system designers, which clearly defines the functions of the CCTV system according to the customer expectations

NOTE Refer to EN 50132-7:1996, Clause 5 ‘Operational requirements’.

3.1.102
operator
authorised individual (a user) using a CCTV system for its intended purpose

3.1.103
operator log
system log of events and operations which have been handled on a workstation or by a certain operator

3.1.104
original recording
first instance of unaltered images in persistent on-line storage, primary or original image stored on media suitable for long-term storage

3.1.105
personal digital assistant
handheld computers that were originally designed as personal organizers

3.1.106
physical authorisation key
implement used by an authorized user to gain access to restricted functions or parts of a CCTV system (mechanical key, magnetic card, electronic token or similar)

3.1.107
physical storage size
size of a storage media expressed in its characteristic unit

EXAMPLE For digital media bytes, gigabyte (GB) or terabyte (TB) are used.

3.1.108
picture
image

3.1.109
pixel
smallest element of an image

NOTE Acronym for picture element.

3.1.110
playback
viewing of previously recorded images from storage media

3.1.111
point of sale data
data generated by a point of sale terminal

3.1.112
power supply
part of the CCTV system to supply the CCTV system with electrical power

3.1.113
presentation
function of CCTV system displaying images and data to the user

3.1.114
prime power source
power source used to support a CCTV system under normal operating conditions

3.1.115
primary image
refers to the first instance in which an image is recorded onto any media

3.1.116
primary storage
storage used to store data that is not in active use and non-volatile for the preservation of stored information e.g. for later retrieval or in an event of power loss

3.1.117
privacy masking
blocking out or obscuring areas of an image for privacy reasons

3.1.118
protected
maintaining and preventing deletion of stored images,in original condition, for longer than the set retention time

3.1.119
redundant array of independent disks
data storage architecture that divides and/or replicates data among multiple hard drives

3.1.120
restore (alarm)
action of a user to change the state of a subsystem or detector from the alarm-, fault- or tamper condition to its previous condition

3.1.121
repetitive failure
rapidly repeating and duplicating signals for no identifiable reason causing additional or unwanted messages for the same fault condition

3.1.122
remote operation
operation at remote workstation connected by external interconnections that are not part of the CCTV system

3.1.123
resolution
pixels/inch or number of pixels of a video-frame, monitoring device, print out

3.1.124
recording rate
frame rate for one input channel or a complete recording device

3.1.125
recorded information
any data recorded on any recording medium (e.g. electronic, magnetic or optical) containing information of events and camera views that have happened in the past

3.1.126
redundancy
methods to secure a system against component failures by doubling elements

EXAMPLE Redundant or fail-safe systems continue operation automatically with a second component in case of failure of the primary one. For redundant communication the system switches automatically to the second communication channel, if the first channel does not give a response.

3.1.127
remote video response centre
operation which is continually manned and capable of receiving multiple concurrent CCTV images from remote locations for the purpose of interacting with site(s) to provide security and related services

3.1.128
remote workstation
secondary or auxiliary control station located at some distance from the CCTV system or the protected premises

3.1.129
replay
playback of recorded images from storage

3.1.130
response
every control command, change of system conditions or information to external devices or persons driven by alarms, faults, messages or triggers

3.1.131
response time
time a system or functional unit takes to react to a given input

EXAMPLE The response time of a presentation device is the amount of time a pixel takes to go from active (black) to inactive (white) or back to active (black) again. It is measured in ms.

3.1.132
risk
likelihood, combined with the effect, of loss damage or harm

3.1.133
scene brightness
observed brightness of the scene, dependent on the scene illumination

3.1.134
secondary storage media
from original recording location separated storage media

3.1.135
sensitivity
(relating to imaging device) necessary level of image device illumination in order to produce an acceptable image

3.1.136
signal to noise ratio
ratio between the signal strength and the noise levels in an audio or video signal

3.1.137
storage
means for storing data or video for subsequent use or retrieval

EXAMPLE Hard disk, flash drive, CD.

3.1.138
storage media
means where data is stored for later retrieval, viewing or processing

3.1.139
subsystem
part of a CCTV system located in a clearly defined part of the supervised premises capable of independent operation

3.1.140
surveillance
observation or inspection of persons or premises for security purposes through alarm-systems, CCTV systems, or other monitoring methods

3.1.141
system configuration
methods to specify a CCTV system in structure of its elements, data handling, log files, data storage capabilities, user access levels and user control capabilities

3.1.142
system data
system configuration parameters

3.1.143
system integrity
ability of an application to function as designed and the measure of immunity from influence which could affect normal operation

3.1.144
system log
chronological list of events or operations which have occurred in the CCTV system, which allows the reconstruction of a previous activity and records the attributes of a change (such as date/time, operator)

EXAMPLE A record book or its electronic equivalent into which all relevant details of the CCTV system, its operation, performance and its maintenance can be entered in a secure manner for later retrieval by authorised users.

3.1.145
system management
configuration and control, of the CCTV system as well as the administration of system data and components

3.1.146
system security
protection of the system against failures as tampering, illegal access, vandalism. Controlled physical or electronic access to the CCTV system or any component to prevent unauthorised access

3.1.147
system set-up
configuration of the system

3.1.148
tamper
unauthorised changes in the system like unauthorised physical access in order to outwit the system or parts of it

3.1.149
time synchronisation
manual or automatic method to keep the time and date integrity between different components of the CCTV system, including daylight saving time changes

3.1.150
trajectory lines
means to mark the positions passed by a moving object of the area of interest in the image display

3.1.151
trigger
signal as reaction on an event in order to activate a function or a device

EXAMPLE A moving person switch on a recording device.

3.1.152
user action
deliberate input from an operator to the system to monitor, control the system or to change conditions

EXAMPLE Switch camera x to monitor y.

3.1.153
user interface
means by which a user operates a CCTV system

3.1.154
video content analysis
analysis of live or recorded video to detect activities, events or behaviour patterns as defined in the operational requirements

3.1.155
video loss
system failure, when the video signal from a capturing device is missing

3.1.156
video matrix
unit for connecting several input video signals to several outputs

3.1.157
video recorder
device to record and replay video

3.1.158
video motion detection
algorithm, procedure or device to generate an alarm condition in response to a change of the contents of a given image sequence

3.1.159
watermark
form of checksum, describes changes in pixel values to incorporate information, which changes if the image file is altered without compromising the integrity of the original recorded digital image

3.1.160
workstation
control station for user operation

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

AOI	Area Of Interest
ANPR	Automatic Number Plate Recognition
ARC	Alarm Receiving Centre
ASF	Advanced Streaming Format
ATM	Automatic Teller Machine
AVI	Audio Video Interleave Format
B/W	Black/White
CCD	Charge Coupled Device
CD	Compact Disc
CRT	Cathode Ray Tube
EAS	Electronic Article Surveillance, anti-shoplifting system
FPS	Frames Per Second (frame rate)
GIF	Graphics Interchange Format

ISO	International Standards Organization
JPEG	Joint Photographic Experts Group
LCD	Liquid Crystal Display
MPEG	Moving Picture Experts Group
PDA	Personal Digital Assistant
POS	Point Of Sales data
RAID	Redundant Array of Independent Disks
RVRC	Remote Video Response Centre
SNR	Signal to Noise Ratio
VCA	Video Content Analysis
VMD	Video Motion Detection

4 Functional description of the CCTV system (informative)

4.1 CCTV system

A CCTV system usually consists of equipment containing analogue and digital devices as well as software. Because the technology and, with it, the CCTV equipment and their functionalities develop and change very rapidly, single devices and their requirements are not defined. Instead, this clause defines and describes the CCTV system as functional parts together with the relationships between them.

A CCTV system for security applications can be presented as functional blocks which portray the various parts and functions of the system (see Figure 1).

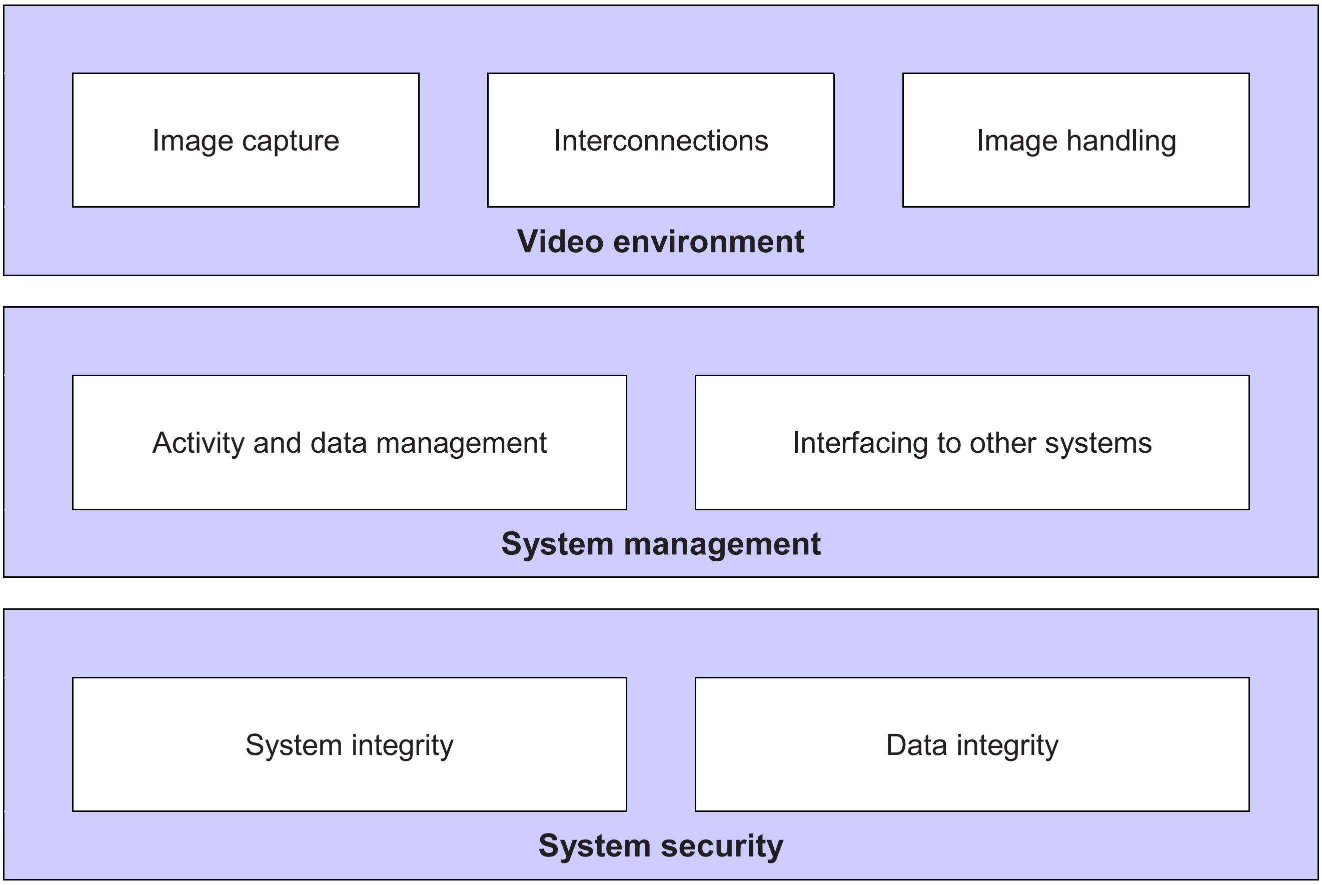


Figure 1 – CCTV system

4.2 Video environment

4.2.1 General

The purpose of a CCTV system is to capture images of a scene, handle the images and display them to the operator. The entity consisting of CCTV devices and interconnections between the devices can be described as **video environment**.

Instead of defining the actual devices that make up the CCTV system, the video environment is defined here in three functions:

- generation of video images (**image capture**);
- transmission and routing of video images and control signals (**interconnections**); and
- presentation, storage and analysis of the images (**image handling**).

The above-mentioned functions may reside in various hardware or software components of the system. Note that these functions do not necessarily always match up with separate devices, as several functions can be performed by a single device. As an example, a network camera device can capture the image (image capturing), store it temporarily (image handling), analyse it for VMD (image processing) and transmit it via the network (interconnections). Alternatively several devices in one system can perform the same function.

Figure 2 shows a simple practical example of the video environment:

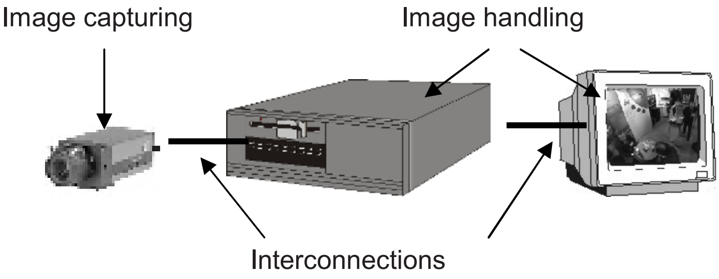


Figure 2 – Example for CCTV system

4.2.2 Image capture

The purpose of image capture is to generate and deliver an image of the real world in a format that can be used by the rest of the CCTV system.

The purpose of Image Capturing is to generate an image of the scene for later processing by the CCTV system. An image source captures an image of the scene, creates image data and delivers that data to the image handling functionality using the system interconnections. The image data can be in analogue (e.g. composite video) or digital (e.g. JPEG, MPEG-4) format.

4.2.3 Interconnections

Interconnections describe all transmission of data within the video environment. This includes two functions: **connections** and **communications**.

The communications describe all video and control data signals, which are exchanged between system components. These signals may be analogue or digital.

Connections cover the media used for the communication signals. Examples of connections are cables (e.g. twisted pair, coaxial or optical fibre), digital networks, wireless transmission as well as equipment like a multiplexer or video matrix.

A CCTV system can be divided into components that are communicating through interconnections, which are not dedicated to the CCTV system. An example is a network which is shared with other applications.

4.2.4 Image handling

4.2.4.1 Generalities

The functions of image handling include **analysis**, **storage** and **presentation** of an image or a sequence of images. The same functions can also be applied to other data (e.g. audio stream) and meta data. A CCTV system does not necessarily contain all of these functions.

Image handling can be performed by one or several devices that make up the CCTV system (e.g. monitors, recorders, image analysers, intelligent cameras and remote workstations). One device can also handle several image handling tasks (e.g. digital video recorder).

During image handling the images may be changed e.g. in resolution, frame rate and compression.

4.2.4.2 Analysis

The video data that makes up the images can be analysed in order to extract information from live or recorded video data. In addition to the video data the analysis function can also use other data (e.g. audio stream) or meta data as inputs.

Analysis can be utilized for several purposes:

- proving the integrity of the system (e.g. camera position);
- interpreting the captured scene (e.g. automatic number plate recognition);
- detecting an event which may trigger an alarm (e.g. moving person or smoke detection).

4.2.4.3 Storage

The video image data (as well as other data or meta data) can be stored on a storage medium (e.g. magnetic, optical, electronic) for later retrieval. The first manifestation of an image in persistent and final form is called ´original image data´ or ´original recording´. The stored data can be in analogue or digital format. Precise copies may be made of digital data and called ´original´. The transfer of images from the original recording and location to another media is called ´image backup´ or ´master copy´ in case of an exact copy or otherwise if altered ´export´. Exported images may be used as working copy due to necessary compression or format conversions, image enhancements or similar processing.

4.2.4.4 Presentation of information

Presentation of information is the display of video images either as single (still) images or as video sequences consisting of consecutive video images in visible form that can be viewed by an operator. One or several video images may be displayed simultaneously. Additionally, other data (e.g. audio stream) and meta data can be presented.

Examples of devices for presenting information include monitor screens (e.g. CRT, plasma, LCD) or projectors.

4.3 System management

4.3.1 General

The user interface is a very important interface for activity and data management within CCTV systems. This interface significantly determines comfort, functionality and the actual security of a CCTV system.

Seen from the system management point of view, a CCTV system consists logically of two functions:

- **activity** and data management that captures, transmits, stores and presents video images, other data or meta data, This part also handles operator commands and system-generated activities like alarm procedures and alerting of operators;
- **interfaces** that connect the CCTV system to other systems.

The above-mentioned logical functions of the system do not refer to separate devices, as one device can perform multiple tasks. For example, a recorder handles, stores and outputs the images and, at the same time, performs video content analysis and alerts the operator when an alarm procedure is activated.

4.3.2 Data management

A CCTV system manages information. In addition to the video data, it can also handle other acquired data like audio, or meta data which can be acquired from another system or generated by the system. This information is managed partly by the system itself and partly by the operator.

The management of the above-mentioned information comprises data acquisition (e.g. image capturing), data transmission between system components (e.g. transmission of images from a camera to a recorder), storage of images (e.g. hard-disk recording) and data presentation (e.g. displaying of images on a monitor screen). These functionalities are mainly taken care by devices that make up the CCTV system, or by software residing in these devices (e.g. a database for storing video images).

The system can handle and generate meta data. There are different types of meta data that is managed by the system:

- data that is linked to the actual video data. It can be acquired from another system (e.g. POS data, license plate numbers, location identifying data) or generated by the system itself (e.g. time stamps, image source identifiers);
- log files generated and stored by the system, describing system or operator activities;
- system data in form of system condition, storage media usage, etc.

The operator is responsible for responding to the presented information as defined in the operational requirements.

4.3.3 Activity management

Activity management comprises all the activities that are driven by events and any user actions.

An event is an occurrence in the real world, such as a fire (a house burning), an intrusion (a door broken) or another defined situation (a person moving). The event can involve a hazard endangering human lives or property.

An event can also be an occurrence that is targeted at the CCTV system, like tampering of a system component.

The event can trigger an alarm procedure in the CCTV system. The trigger can be the output from image handling (e.g. VCA or VMD), a signal from a sensor (e.g. smoke or motion detector) or data received from another system (e.g. EAS gates or ANPR system).

When the alarm procedure is triggered, the CCTV system performs the tasks as defined in the operational requirements. Mostly, these tasks form a response to the hazard perceived.

This alarm response can involve internal activities (e.g. deliberate repositioning of a camera to change the view, recording or image presentation) as well as notification of an external system (e.g. access control or alarm receiving centre).

A typical task of the alarm procedure is also alerting the operator, who in turn can start other activities. The actions performed by the operator are defined in the operational requirements.

Figure 3 illustrates event driven activities:

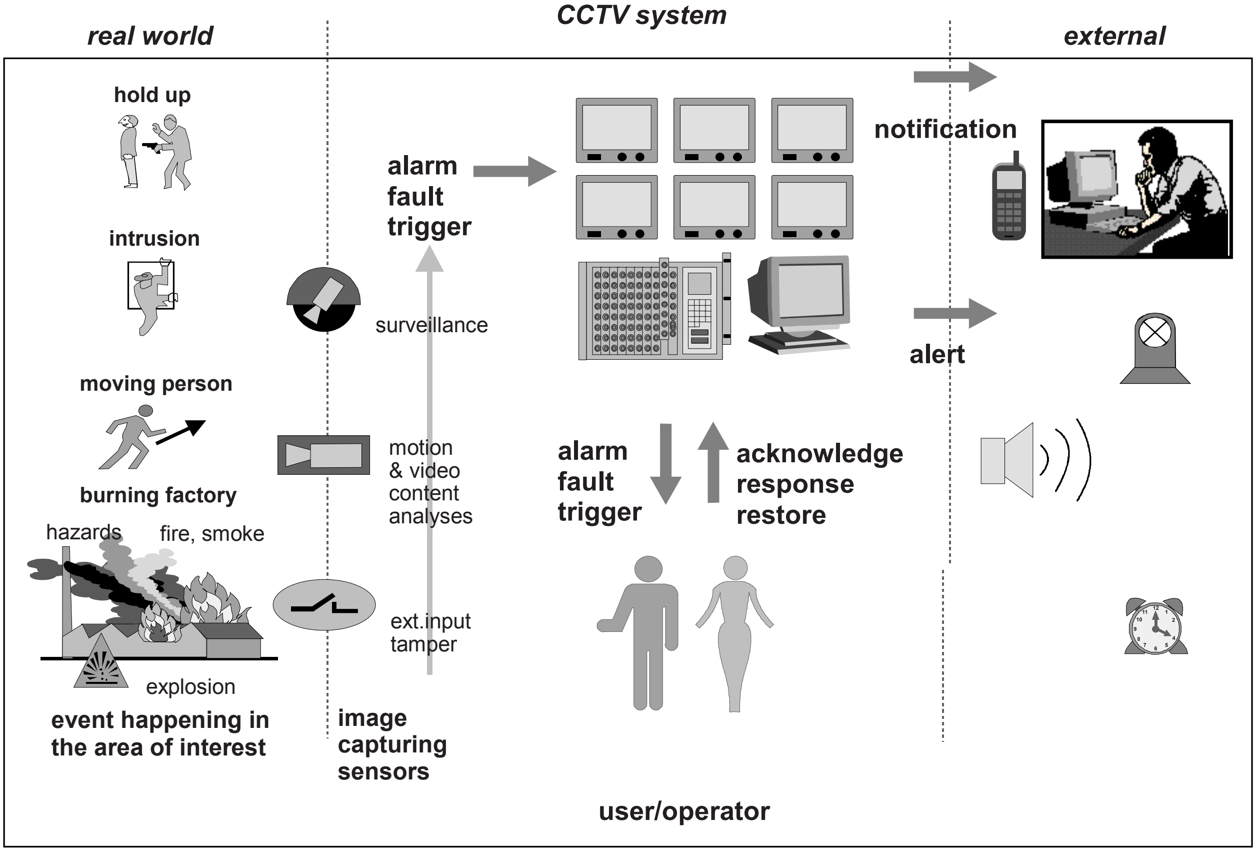


Figure 3 – Activity management

Activity management includes system configuration, system control and other activities started by the operator. Examples of these are positioning of a pan-tilt-zoom camera, redirection of images to a monitor, as well as data backup, export and printing. All of these activities are defined in operational requirements of the application.

4.3.4 Interfaces to other systems

For interfacing to other systems command and data formats need to be specified in detail for both systems. System interfaces allow mutual and comfortable access to functionalities and data.

A CCTV system may be interfaced to other systems, like

- other security systems (e.g. other CCTV, intrusion and hold-up alarm, access control or fire alarm systems),
- security management systems (e.g. alarm management systems or ARC (alarm receiving centres), RVRC),
- other, non-security systems (e.g. building management systems, automatic teller machines, Point-of-Sales equipment or automatic number plate recognition systems).

The interfaces between the systems can manage data communication, mutual system control, common databases, common user interfaces or other type of system integration.

The requirements for interfacing or integrating an alarm system with other systems are described in the European Technical Specification CLC/TS 50398.

In general, a distinction can be made between two kinds of transmission, where either the physical transmission path is part of the CCTV system or is provided by a third party as external interconnection.

4.4 System security

4.4.1 General

System security consists of **system integrity** and **data integrity**. System integrity comprises physical security of all system components and control of physical and logical access to the CCTV system. Data integrity covers logical access to the data and prevention of loss or manipulation of the data.

The purpose of system security is to alert any failures and to protect from intentional and unintentional interference.

4.4.2 System integrity

System integrity comprises the protection of each system component or device as well as protection of the system as an entity. If external interconnections between system components are used, their protection is also part of the system integrity. Same applies also to interfaces with other systems.

System integrity consists of three parts:

- detection of failures of components, software and interconnections;
- protection against tampering;
- protection against unauthorized access to the system.

4.4.3 Data integrity

Data integrity covers several important items:

- data identification (ensuring accurate identification of data source, time, date etc.);
- data authentication (prevention of modification, deletion or insertion of data);
- data protection (prevention of unauthorised access to the data).

5 Security grading

CCTV systems and components are graded to provide the level of security required. The security grades take into account the risk level which depends on the probability of an incident and the potential damage caused by it.

Due to the wide range of the surveillance tasks, the components, sub-systems and functions of a CCTV system may have different security grades within one system. This shall be explicitly defined in the OR.

There are four grades:

- low risk (grade 1)

  A CCTV system intended for surveillance of low risk situations. The CCTV system has no protection level and no restriction of access.

  EXAMPLE Small storage area (less than 400 m²) of products of low desirability (e.g. vegetable or newspapers), located in low risk areas. Services company with an activity implying no values or confidential information (e.g. sugar refinery)

- low to medium risk (grade 2)

  A CCTV system intended for surveillance of low to medium risk situations. The CCTV system has low protection level and low restriction of access.

  EXAMPLE Large storage area (more than 400 m²) of products of low desirability (e.g.vegetable or newspapers), located in low risk areas. Services company with an activity implying no values but confidential information (e.g. medical laboratory). Safety applications in areas such as paper mills or recycling plants.

- medium to high risk (grade 3)

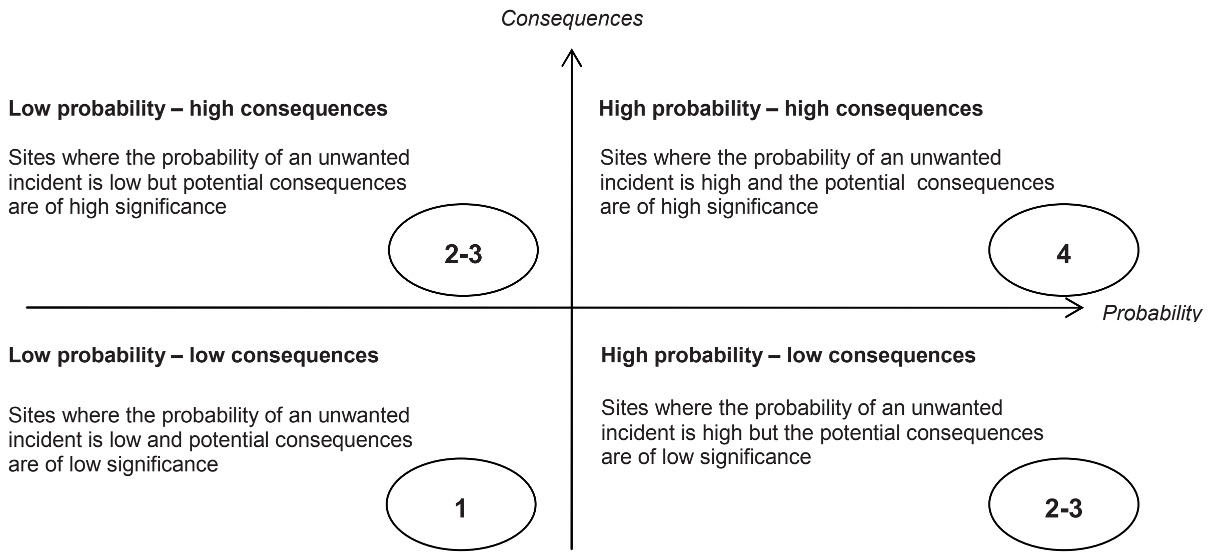
  A CCTV system intended for surveillance of medium to high risk situations. The CCTV system has high protection level and high restriction of access.

  EXAMPLE Large storage area (more than 400 m²) of products of low desirability, located in high risk areas (e.g. shopping centre) or small storage area (less than 400 m²) of desirable products (e.g.white goods or drugs), located in low risk areas. Services company with an activity implying values but no confidential information (e.g.warehouse with high value items like white goods or cigarettes). Protection of public buildings, harbours, airports, banks, refineries against sabotage or terrorist attack.

- high risk (grade 4)

  A CCTV system intended for surveillance of high risk situations. The CCTV system has very high protection level and very high restriction of access.

  EXAMPLE Storage areas of desirable or extremely desirable products (e.g. jewellery, high demand controlled drugs); storage located in high risk areas (cellphone or cigarettes selling areas in shopping complex). Services company with an activity implying values and confidential information (e.g. army laboratory, Government offices).



Low probability – high consequences

Sites where the probability of an unwanted incident is low but potential consequences are of high significance

High probability – high consequences

Sites where the probability of an unwanted incident is high and the potential consequences are of high significance

Low probability – low consequences

Sites where the probability of an unwanted incident is low and potential consequences are of low significance

High probability – low consequences

Sites where the probability of an unwanted incident is high but the potential consequences are of low significance

Consequences include injury, loss of life, damage to or loss of property, loss of information, and damage to the environment.

Probability is likelihood of occurrence of consequences and is impacted by alarms systems, guarding, physical protection (locks, fences, etc.) and general risk (societal disorders, environmental disasters) in the area.

Figure 4 – Risk and security grades

6 Functional requirements

6.1 Video environment

6.1.1 Image capture

The captured images of the area of interest shall have sufficient accuracy and detail to enable users to extract the appropriate information defined in the operational requirements (see EN 50132-7:1996).

The capturing of images shall fulfil the customer objectives for image handling e.g. presentation and recording (concerning fps, resolution, colour depth and latency time) defined in the operational requirements (see EN 50132-7:1996).

6.1.2 Interconnections

6.1.2.1 Generalities

Any interconnections shall be designed to minimise the possibility of signals or messages being delayed, modified, substituted or lost.

Monitoring of interconnections shall be provided in accordance with the requirements defined in 6.3.2.2.4 of the system security requirements.

6.1.2.2 Common interconnections

Image streams sharing common interconnection shall be designed and configured in a way that they do not adversely affect each other or any message transfer in any normal operation mode.

For security grades 3 and 4, if a CCTV system is designed and configured in a way that single or multiple operators request video images via common interconnections and the simultaneous request of image streams by all possible workstations may exceed the available capacity of the common interconnection at any time, then the CCTV system shall offer means to configure the maximum bandwidth of image streams for every image source and to configure the maximum bandwidth or number of image streams to the operator workstations.

6.1.3 Image handling

6.1.3.1 Presentation

If the CCTV system is able to present information, the following properties shall be declared by the manufacturer in the documentation:

- type of presentation device (e.g. analogue monitor, digital monitor, PDA, projector);
- maximum number of simultaneously displayed image sources;
- resolution of displayed image(s);
- size(s) of displayed image(s);
- display rate (number of images displayed per s);
- response time;
- colour / B/W.

When displaying images, whether they consist of the entire image source or a part of it, the proportions of the displayed image shall be the same as in the original image source. Any superimposed information like timestamps, camera names produced by the system shall not affect the image itself.

6.1.3.2 Analysis

Any superimposed information like object masks, trajectory lines, and classification information, produced by the system shall be processed as meta data and shall not affect the image itself (see 6.3.3). Only a privacy mask is allowed to affect the area of interest of an image for privacy reasons, in order to block out sensitive areas from view.

6.1.3.3 Storage

If storage or recording functions are available in the CCTV system following requirements apply.

Most systems modify the video images before they are stored (conversion between analogue and digital format, resolution changes, compression, watermarking, or encryption). In the documentation, all processes that might cause loss of information shall be clearly stated.

It shall be possible to move the storage media, in order to display the data with an alternative device. In this case the alternative device shall be capable of displaying all recorded data.

NOTE This may especially be necessary in case of a device failure.

Table 1 – Storage

The CCTV system shall be capable of	**Security grade**			
	1	**2**	**3**	**4**
data backup			X	X
operating a fail-safe storage (e.g. RAID 5, continuous mirror) or switching automatically over from one storage media to another in case of storage failure				X
reacting to a trigger with a maximum latency time of		1 s	500 ms	250 ms
replaying an image from storage with a maximum time after the incident or actual recording of			2 s	1 s

The following properties of the storage media(s) shall be declared by the manufacturer in the system documentation:

- type(s) and number of video input channels;
- type(s) and number of video output channels;
- type(s) and number of other input channels;
- maximum number of images stored per second for each channel at the specified resolution;

  NOTE Sequences of pictures shall provide images at equidistant intervals.
- maximum total number of images stored per second at the specified resolution when all channels are connected;
- maximum number of images displayed locally and/or at a remote workstation when storing at maximum rate;
- maximum number of images stored when displaying at maximum rate locally and/or remotely;
- resolution and size of stored images;
- storage capacity in hours at the chosen number of input channels, images per second, resolution and quality;
- compression (methods available, settings, compression rates);
- time to recommence image storage after a system restart (e.g. on power loss).

The storing of video images shall not be influenced by any live image display and requests or image backup and export. The configured recording rate shall always be granted in every normal operation mode.

The system shall be configurable such that a maximum storage time can be set. The CCTV system shall be capable of automatically delete images once they have been stored for the set period of time. Recorded images marked as protected from being deleted, are stored for a longer period of time. The maximum storage time allowable by the applicable national legislation should not be exceeded.

The CCTV system shall offer information about:

- the video input channels being recorded;
- the image storage usage in capacity and recording time;
- remaining storage capacity.

The system shall be capable of indicating as specified in the system documentation, if the storage capacity is running low.

6.1.3.4 Image data backup / archiving

If storage or recording functions are available in the CCTV system following requirements apply.

It shall be possible to extract and preserve the image data for evidential or other purpose. A means of playing back the extracted image data (e.g. archive viewer system) shall be available without compromising the ability of the system to continue to function as designed.

If digital data is transferred to a secondary storage medium then it shall be an identical copy of the original data and shall be called ´exact copy´.

This data shall be viewable with an archive viewer system including all additional meta data (ATM, POS, VCA info, location identifying data, etc.) or shall be recoverable into the primary system storage without any loss of information.

Table 2 – Archiving and backup

The archiving shall offer	Security grade			
	1	2	3	4
authentication of every single image and image sequence				X
an automatically scheduled backup of alarm image data				X
a backup of alarm image data by manual request			X	X
verify the successful image backup			X	X

6.1.3.5 Image export

If recording functions are available in the CCTV system the following requirements apply:

- the image export shall not alter the original recording in the primary storage. The system shall be able to offer the selection of time range and image source to be exported or copied;
- the exported data shall have an image source identifier and time stamp ´identifying´ images to guaranty order and completeness of image sequences;
- the system shall be able to export or copy a single image as well;

- the data format used in export may not be able to represent all information stored e.g. metadata and audio. These formats may be more common and easier to handle. The system documentation shall specify the formats supported e.g. JPEG, ASF, AVI, Video CD, etc.;
- printing images onto paper uses a different physical media and does not comply with these requirements.

6.2 System management

6.2.1 Operation

Operation of the user interface shall be self-explanatory, simple and fast for the operators. The system status shall be detected, processed and displayed automatically. Alarm situations shall be identifiable and accessible immediately with a consistent documentation of the event.

6.2.2 Activity and information management

6.2.2.1 Generalities

The system shall clearly distinguish between user requested and event-driven data. Alarm data shall always be given priority over continuously displayed data.

Images presented to the operator shall be clearly labelled as live or replayed video. In addition event driven video shall be clearly labelled as such to differentiate it from user requested video.

6.2.2.2 Status of system functions

The CCTV system shall always be able to offer information about the status of the essential functions.

6.2.2.3 Events and event driven activities

If the CCTV system is designed to handle event driven activities the following requirements apply.

The latency time of the system reaction to a trigger shall be specified in the system documentation.

Triggers or messages shall be retrieved from a queue in the order of their arrival except when a means to prioritise these inputs is provided.

In this case messages or triggers shall be retrieved according to the priority levels. The method of defining the input priorities shall be provided by the manufacturer in its documentation. Where a number of messages or triggers of equal priority are in the queue they shall be retrieved in the order of their arrival.

General requirements for the indication of the priority are as follows:

- the system shall indicate when more alarms exist than are currently being displayed;
- beside the information actually displayed, additional information may be available on demand. The visibility of the prioritised information shall be preserved;
- any normal operation of the CCTV system shall not prevent the indication of an alarm.

It shall be possible to distinguish between different system conditions that may have triggered the activity and between an alarm, a fault or tamper.

The CCTV system shall offer means to indicate an alarm visually and audibly in order to get the attention of the operator.

The CCTV system shall offer means to acknowledge alarms.

For systems of security grades 3 and 4, on alarm the CCTV system shall be able to display alarm related information. The information presented for each alarm message shall include:

a) the origin or source of alarm;

b) the type of alarm;

c) the time and date of alarm.

In addition, where the system provides the facility to prioritize alarms then the priority level shall also be indicated.

6.2.2.4 System logs

Accurate and complete system logs shall be maintained for a period of time as defined in the OR. Data in the system log shall be organized and presented in chronological order. The system shall prevent unauthorised editing or deletion of system logs. An log shall be available for each operator’s workstation.

Following details shall be logged:

Table 3 – System logs

The system shall log with time stamp (date and time), event, source	**Security grade**			
	1	**2**	**3**	**4**
alarms		X	X	X
tamper			X	X
video loss and recovery from video loss			X	X
power loss		X	X	X
essential function failure and recovery from failure			X	X
fault messages displayed to the user				X
system reset, start, stop		X	X	X
diagnostic actions (health check)				X
export, print/ hardcopy incl. the image source identifier, time range			X	X
user log in and log out at workstation, successful and denied logins (local/ remote) including reason of denial (wrong password, unknown user, exceeded account)			X	X
changes in authorisation codes			X	X
control of functional cameras				X
search for images and replay of images			X	X
manual changes of recording parameters			X	X
alarm acknowledge /restore			X	X
system configuration change			X	X
date and time set and change with current time and new time			X	X

6.2.3 Interfacing to other systems

If a CCTV system is interfaced to another system the European Technical Specification CLC/TS 50398 shall be applied.

Common facilities shall comply with all application standards for which they are standard-required. The most severe integrity requirement of each of the standards shall apply.

All system security requirements as defined in 6.3 shall be fulfilled even in cases where the CCTV system is accessed or controlled by another system. The other system shall be seen as a system user with defined access rights.

Access levels to another system shall be consistent with the levels required by that system standard and shall not give unauthorised access to the CCTV system and vice versa.

6.3 System security

6.3.1 Generalities

CCTV system security consists of system integrity and data integrity. System integrity includes physical security of all system components and control of access to the CCTV system. Data integrity will include prevention of loss or manipulation of data.

6.3.2 System integrity

6.3.2.1 Generalities

CCTV systems of security grades 2, 3 and 4 shall be capable of backup and restore of all system data.

6.3.2.2 Detection of failures

6.3.2.2.1 Failures notification

For CCTV systems with a user interface which is normally manned by an operator (either remote or local), alarm conditions from the specified components shall cause an alert. The failure shall be notified at any time a new user logs in or the system restarts.

The information to be presented shall include:

- time and date;
- origin and type of failure.

In addition, where the system provides for the facility to prioritize messages then the priority level shall also be indicated.

Notification of failures shall never cover or hide any important information display such as the area of interest in live images.

For security grades 3 and 4, the system shall be able to detect repetitive failures from a component and shall generate a single message which shall only be repeated each time a new user logs in or the system restarts.

6.3.2.2.2 Monitoring of power supply

For security grades 3 and 4, failure of the primary and, if available alternative, power supplies to the image handling device shall be monitored. If the CCTV system is viewed remotely then an indication of this failure shall be made to the remote location. In any case power supply failure shall always be indicated locally. If the system is unable to resume after power has been restored, with the settings which existed before the power failure, this shall be logged and also indicated to the operator.

The CCTV system shall be able to shutdown regular operation in a defined procedure without loss of stored data.

For security grades 3 and 4 images shall not be held in a buffer for longer than 5 s without being written into the storage medium.

The CCTV system shall resume normal operation after recovering from power loss.

6.3.2.2.3 Monitoring of system functions and components

For security grades 3 and 4 the CCTV system shall manage device failure by indicating any failure of the essential functions within 100 s of the failure.

6.3.2.2.4 Monitoring of interconnections

If interconnections between system components are part of the CCTV system, they shall be monitored according to the following table:

Table 4 – Monitoring of interconnections

The system shall	Security grade			
	1	2	3	4
repeatedly verify the interconnection at regular intervals with a maximum of			30 s	10 s
try to re-establish a interconnection with following number of retries before notification			5	2
notify the operator after failure of an interconnection latest after			180 s	30 s

6.3.2.3 Tamper protection and detection

The CCTV system shall be protected against tamper by reference to Table 5.

If tamper is detected a tamper condition shall be set and a tamper alarm generated. The tamper alarm shall be logged and clearly separated from other conditions like failure, alarm or normal operation.

Table 5 – Tamper detection

The system shall detect	Security grade			
	1	2	3	4
equipment tamper to such equipment as defined in the OR			X	X
video loss		X	X	X
if an image capturing device no longer includes the entire specified field of view			X	X
deliberately obscuring or blinding of the imaging device range			X	X
the substitution of any video data at image source, interconnection or handling				X
significant reduction of the contrast of the image				X

6.3.2.4 Protection against unauthorized access

6.3.2.4.1 Generalities

For each CCTV system access to operation and data shall be governed by an authorisation scheme. This also includes access through a remote workstation or through an external system integrated with the CCTV system.

6.3.2.4.2 Access levels

For each security grade of the CCTV system, there shall be several user access levels to the functions of the CCTV system or part(s) thereof. The user accessing the system can be either an operator or another system:

- **Level 1 Access by any person**

  Functions required to be accessible at level 1 shall have no restriction on access.

- **Level 2 Access by any user**

  Functions affecting the operation of the system, without changing its configuration.

  Access to functions required to be accessible at level 2 shall be restricted by means of key, password, code or similar access-limiting means or device.

- **Level 3 Access by system administrators**

  Functions affecting system configuration.

  Access to functions required to be accessible at level 3 shall be restricted by means of key, password, code or similar access-limiting means or device.

- **Level 4 Access by service personnel or manufacturer**

  Access to component to change system design or to perform system maintenance.

  Access to functions required to be accessible at level 4 shall be restricted by means of key, password, code or similar access-limiting means or device. Access at this level is prevented until access has been permitted by a user at level 3 access.

Table 6 specifies which functions shall be accessible at each access level independently of the security grade:

Table 6 – Level of access

Function	Access levels			
	1	**2**	**3**	**4**
System configuration	NP	NP	P	P
Change individual authorisation codes	NP	P	P	P
Assign and delete level 2 users and authorisation codes	NP	NP	P	P
Restoration to factory defaults	NP	NP	P	P
Upgrading of the system	NP	NP	P	P
Start / Stop CCTV system or component	NP	NP	P	P

Key
P Permitted
NP Not Permitted.

6.3.2.4.3 Authorisation

The CCTV systems shall provide logical or physical means to restrict access to the system or system part(s) with a key, password, code or similar access-limiting means or device.

Permission to gain access to functions of the CCTV system shall be as specified in Table 7.

Table 7 – Authorisation code requirements

Authorisation code requirement	Security grade			
	1	2	3	4
Logical authorisation key differs		> 10 000	> 100 000	> 1 000 000
Physical authorisation key differs		> 3 000	> 15 000	> 50 000

The passwords of users shall never be displayed or stored in clear text.

A valid change of a password by the user itself shall always require a valid user login with the old one and the entry of the new password plus validation in an identical way.

6.3.2.4.4 Data access

The CCTV system shall provide methods for controlled access to data taking account of authorisation level.

Table 8 – Data access

Function	Access levels			
	1	2	3	4
View live images and data	P	P	P	P
View stored images and data, if recordings are available	NP	P	P	P
View information about storage, if storage is part of the CCTV system	NP	P	P	P
Print and save video data	NP	P	P	P
Exporting of images and data	NP	NP	P	P
Deletion of images and data (only with confirmation)	NP	NP	P	P
Key P Permitted NP Not Permitted.				

6.3.2.4.5 Access to system logs

The CCTV system shall provide methods for controlled access to system logs taking account of authorisation level.

Table 9 – Access to system logs

Function	Access levels			
	1	2	3	4
View system logs	NP	P	P	P
Exporting from logs	NP	NP	P	P
Deletion of logs	NP	NP	P	P
Key P Permitted NP Not Permitted.				

6.3.2.4.6 Access to system set-up

The CCTV system shall provide methods for controlled access to system set-up taking account of authorisation level.

Table 10 – Access to system set-up

Protection of access to system set-up	Access levels			
	1	2	3	4
Configuration & set-up	NP	NP	P	P
Recovery from system failure	NP	P	P	P
Recovery from tampering	NP	P	P	P
Key P Permitted NP Not Permitted.				

6.3.2.5 Time synchronisation

For security grades 3 and 4 the time settings of various components of a CCTV system shall be always be within ± 10 s of UTC.

6.3.3 Image and data integrity

6.3.3.1 Data identification

The CCTV system shall provide methods to identify data taking account of different security grades.

Table 11 – Data labelling

The CCTV system shall uniquely label data by	Security grade			
	1	2	3	4
location (e.g. name of site)		X	X	X
source like capturing device (e.g. camera number)		X	X	X
date and time	X	X	X	X
date and time in UTC including offset for local time				X

The CCTV system shall always maintain the original data labels when data is exported.

6.3.3.2 Data authentication

To verify the integrity of images and other data, CCTV systems of security grades 3 and 4 shall provide a method (e.g. watermarking, checksums, fingerprinting) to authenticate image and meta data and their identity.

The authentication method shall be applied at the time the data is recorded and shall notify the user if any of the following has occurred:

- any of the images has been changed or altered;
- one or more images have been removed from a sequence;
- one or more images have been added to a sequence;
- the data label has been changed or altered.

CCTV systems of security grades 3 and 4 shall also provide a method by which the authenticity of copied and exported data is verified.

The authentication method used shall be specified in the system documentation.

6.3.3.3 Data (manipulation) protection

CCTV systems of security grade 4 shall provide a method (e.g. encryption) to prevent unauthorized persons viewing the images and other data without permission.

CCTV systems of security grade 4 shall also provide a method to protect the confidentiality of copied and exported data.

The method used to protect the data confidentiality shall be specified in the system documentation.

6.4 Environmental requirements

The environmental stability of the CCTV system shall be of the same level in all grades. The CCTV system shall operate correctly in the environmental class specified in Clause 7 it is designed for and exposed to EMC conditions described in EN 61000-6-3 and EN 50130-4. A CCTV system shall neither change state, suffer damage to components nor substantially change in performance. EN 50130-5 describes environmental test methods which shall be applied to CCTV system components.

Functional tests to be applied for component evaluation shall be at least a test or measurement of the essential functions of the component. Acceptance criteria shall be that there is no change in the functioning of the component and no significant change in any measurement during the environmental testing. A CCTV system component shall provide protection against electrical shock and consequential hazards by achieving compliance with the requirements of EN 60950-1 or EN 60065.

7 Environmental classes

7.1 Generalities

Components shall be suitable for use in one of the following environmental classes.

NOTE 1 Classes I, II, III and IV are progressively more severe and therefore Class IV equipment may, for example, be used in Class III applications.

CCTV components shall operate correctly when exposed to environmental influences specified in 7.2, 7.3, 7.4 and 7.5.

NOTE 2 The environmental conditions described in Clause 7 are those in which the CCTV system is expected to perform correctly, they are not necessarily the conditions to be used during the testing of CCTV components.

7.2 Environmental Class I – Indoor

Environmental influences normally experienced indoors when the temperature is well maintained.

EXAMPLE In a residential or commercial property.

NOTE Temperatures may be expected to vary between +5 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

7.3 Environmental Class II – Indoor – General

Environmental influences normally experienced indoors when the temperature is not well maintained.

EXAMPLE In corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouses where heating is intermittent.

NOTE Temperatures may be expected to vary between -10 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

7.4 Environmental Class III – Outdoor – Sheltered

Environmental influences normally experienced out of doors when the CCTV components are not fully exposed to the weather.

NOTE Temperatures may be expected to vary between -25 °C and +50 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

7.5 Environmental Class IV – Outdoor – General

Environmental influences normally experienced out of doors when the CCTV components are fully exposed to the weather.

NOTE Temperatures may be expected to vary between -25 °C and +60 °C/+55 °C incl. a sunshield with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

8 Documentation

8.1 System documentation

Documentation relating to a CCTV system shall be concise, complete and unambiguous. Information shall be provided sufficient to install, put into operation, operate and maintain a CCTV system.

System specification and block diagram incl. specification of configuration:

- installation details for operation and service;
- inspection and maintenance procedures/routines.

8.2 Instructions relating to operation

Instructions relating to the operation of a CCTV system shall be designed to minimise the possibility of incorrect operation and be structured to reflect the access level of the user.

8.3 System component documentation

Documentation relating to CCTV system components shall be concise, complete and unambiguous. The documentation shall be sufficient to ensure the correct installation, putting into operation and maintenance of CCTV system components. Sufficient information shall be provided to ensure the integration of each component with other CCTV system components.

Component documentation shall include the following:

- installation guide / manual;
- technical system data specification:
  - – performance specification;
  - – min. requirements of equipment;
  - – min. requirements of the environment;
  - – standard to which component claims compliance;
- inspection & maintenance procedures/routines;
- name of manufacturer or supplier;
- name of system integrator or installer;
- description of equipment;
- name or mark of the certification body (for components which are required to be certified);
- security grade of the component;
- environmental class.

Annex A
(normative)

Special national conditions

Special national condition: National characteristic or practice that cannot be changed even over a long period, e.g. climatic conditions, electrical earthing conditions.

NOTE If it affects harmonization, it forms part of the European Standard.

For the countries in which the relevant special national conditions apply these provisions are normative, for other countries they are informative.

The special national conditions described below shall apply to the following countries: Denmark, Finland, Norway, Sweden.

Clause	Special national condition
7.5	Environmental Class IV – Outdoor – General:
	CCTV components shall operate correctly when exposed to environmental influences normally experienced out of doors when a CCTV components are fully exposed to the weather.
	Temperatures may be expected to vary between -40 °C and +60 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

Bibliography

ISO 10918 (series) Information technology – Digital compression and coding of continuous-tone still images

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™