COMITÉ EUROPÉEN DES ASSURANCES

Secrétariat Général
3bis, rue de la Chaussée d'Antin F 75009 Paris
Tél. : +33 1 44 83 11 83 Fax : +33 1 47 70 03 75
Web : cea.assur.org

CEA

Délégation à Bruxelles
Square de Meeûs, 29 B 1000 Bruxelles
Tél. : +32 2 547 58 11 Fax : +32 2 547 58 19
Web : cea.assur.org

PROPERTY INSURANCE COMMITTEE
Prevention Specifications

Insurers' Guide to Closed Circuit Television (CCTV) Installations used for Security Purposes

CEA 4042 : September 2003 (en)

Table of contents

1 Introduction

This document has been produced by CEA to offer guidance to insurers on the use of Closed Circuit Television (CCTV) Systems to protect insured property.

It explains how CCTV can be employed in order to reduce the risk of criminal attack, and to ensure an appropriate response in the event that an attack occurs. Comparisons are made with traditional forms of intruder alarm surveillance and comment is offered on the use of CCTV in conjunction with other forms of protection.

The document goes on to suggest a best practice approach to the specifying of CCTV installations in the form of insurers' requirements, and offers a questionnaire based tool for the evaluation and specification of such systems.

The insurers' requirements proposed in this document are not intended to override National Standards or statutory requirements, or any regulations imposed by local Police or Fire Services.

2 What is a CCTV system?

2.1 Development of CCTV

The first closed circuit television systems date back to the 1950s. With the availability of smaller vacuum tubes, the large “broadcast” cameras of the day could be replicated in much smaller and more affordable camera units. However, throughout the 1950s to 1970s, CCTV was slow to find a role for itself. The problem was the cost, both of the equipment and its ongoing technical support (reliability was a problem).

CCTV did, however, begin to take off in the late 1970s and by the early 1980s CCTV was established as a credible tool for a range of commercial security applications.

Towards the end of the 1980s, developments in semiconductors and integrated circuitry allowed smaller, more reliable solid state cameras with better performance. Colour cameras were also increasingly being used.

Developments in the video cassette recorder (VCR) during the 1980s also gave CCTV a boost. VCRs enabled CCTV images to be recorded at reasonable quality with very low cost.

Later, the arrival of multiplexing (the ability to sequentially or simultaneously display or record the images from several cameras) and practical video motion detection (VMD), took CCTV to the beginning of the digital age.

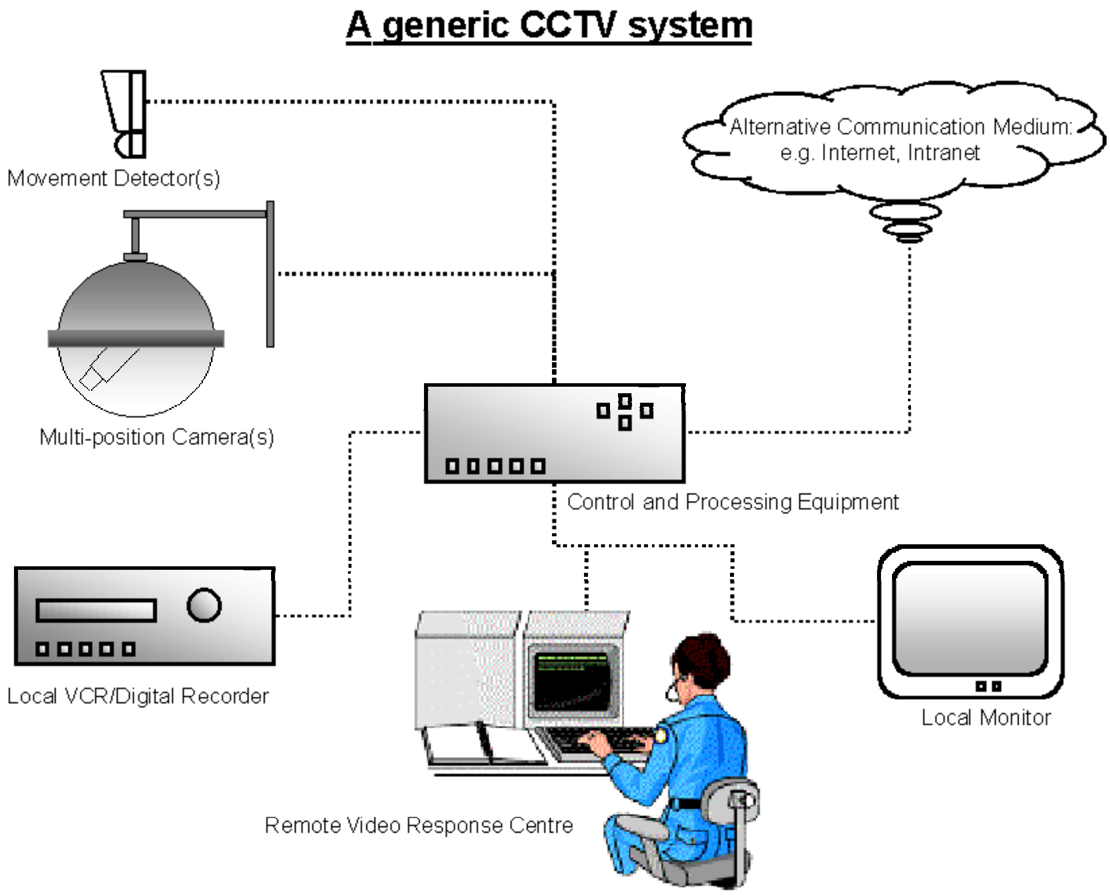
By the mid 1980s, CCTV had acquired a more “high tech” status gaining greater respect as a tool for crime prevention from both the private and public sectors.

In the early 1990s, dedicated commercial remote video monitoring services began to emerge. These facilities monitor numerous CCTV-protected customers, usually unmanned sites, and react to specific events. Remote monitoring is generally much less expensive than onsite guarding and is thus becoming increasingly popular.

2.2 Generic construction of a CCTV System

A central feature that defines a CCTV system is that it is “closed” – meaning that the system transmits signals and images to a pre-determined location, rather than being “open” and available to anyone with a receiver (as in broadcast TV).

The overall quality of images obtained will depend upon the quality of the poorest performing element, be it the camera, transmission system, storage or viewing system.


A generic CCTV system
Movement Detector(s)
Alternative Communication Medium:
e.g. Internet, Intranet
Multi-position Camera(s)
Control and Processing Equipment
Local VCR/Digital Recorder
Local Monitor
Remote Video Response Centre

All CCTV systems consist of:

- Camera(s)
- The processing and transmission of images between the camera and a designated location
- The means of monitoring and viewing images at the designated location.

CCTV systems typically comprise multiple components but with recent advances in technology, it is now possible to purchase a system comprising 2 hardware elements only – a camera (possibly incorporating detection and internal processing) and a remote PC (or even a mobile telephone). As with larger systems, the management system is of critical importance when decisions relating to the analysis of events and the transmission of images are delegated to the system itself. Software can be employed to determine what is seen by the camera (e.g. a person or a cat) and even body language.

It is expected that, in the future, technology improvements will permit the transmission of images over the internet with the same quality and speed that is currently available with point-to-point systems.

2.3 Types / Purposes of CCTV Systems

There are very many situations in which a CCTV system can prove to be a useful monitoring or surveillance tool. Not all of these applications are security related. For example, CCTV can be employed to help in the supervision of industrial processes, or crowd movements in Metro stations, or customer volumes in retail premises, thus potentially meeting the needs respectively of production control, personal safety and retail management / customer convenience.

In the crime-prevention field, applications are numerous, from a simple one-camera, one-monitor anti-shoplifting system at one end of the spectrum, to a multi-component installation protecting a large industrial or retail park at the other.

2.4 Considering CCTV as a possible security solution

CCTV is a rapidly developing and increasingly affordable technology and there is sometimes a temptation within the marketplace, to see it as a solution to all security problems. Like all security measures, however, it has its limitations and it is important to understand exactly what role it might play in, and what value it would add to, a particular situation.

In deciding whether there might be a possible role for CCTV in addressing a particular security issue, it is necessary to thoroughly understand the security hazards being addressed and whether the case for CCTV over competing technologies has merit. Therefore, before the decision is taken, use of all other available counter-measures should be fully considered, e.g.:

- perimeter barriers (walls, fences, gates etc)
- lighting
- manned guarding/patrolling
- visiting guards
- physical measures (locks and barriers for openings)
- cages, vaults, strongrooms and safes
- intruder alarms (site and buildings)
- risk modification/elimination

A CCTV system does not, in itself, prevent offending behaviour but in the right circumstances, it is a powerful tool allowing intervention in the unwanted act. However it is of little effect, except as a deterrent, if installed in isolation. It works best when integrated in a carefully structured package of measures that would normally include more than one of those listed above. Plainly, at the very least, CCTV must be supported by observers and responders unless its purpose is restricted to that of deterrence/gathering evidence.

Who/where is the observer?

What will be the response; what value will it have?

In a typical situation deemed suitable for CCTV it is a highly cost effective link in the security chain provided the other, well proven, principles have been observed:

security measures that “buy time” consistent with the predicted speed of response

layered protection in depth, according to the expected levels of threat

.

2.5 Comparison with Intruder Alarm Systems

There is a tendency for CCTV sometimes to be considered as an alternative to intruder alarm protection but there are, in fact significant differences.

In spite of the emergence of various national and international Codes, CCTV remains largely unregulated by comparison with intruder alarm installations.

The following chart illustrates some of the more important distinctions between the two technologies. It reflects the common industry practice across most of Europe (rather than what is technically possible).

Feature	CCTV	Intruder Alarm
Tamper protection/detection	No	Yes
Environmental immunity	No	Yes
Monitored telecomms path	No	Yes
Back-up power supply	No	Yes
Certification scheme	No	Yes
Installation standards and codes of practice	No	Yes
Standards for monitoring	No	Yes
Remote centre construction standards	No	Yes
Established conventions for response	No	Yes
Privacy laws	Yes	No

It can thus be seen that CCTV and intruder alarm protection are not wholly interchangeable. There are important differences which must be compensated for if CCTV is to be considered as an alternative to an intruder alarm.

On the other hand, the combination of CCTV with intruder alarm can provide a valuable additional level of security.

2.6 CCTV in conjunction with intruder alarm protection

CCTV and intruder alarms can be employed as entirely independent systems to protect the same premises. Alternatively, CCTV can be used to verify intruder alarm activation signals (in other words, to provide visual evidence of the cause of the intruder alarm activation). Used in this way, CCTV offers the chance of reducing the possibility of false alarms from intruder alarm systems by filtering-out non intruder related activations.

If CCTV is to be used in this way, it is important that:

- every detector in the intruder alarm system should be combined with a camera which has at least the same field of view, and
- the intruder alarm signal and CCTV image should be transmitted to the same remote centre otherwise there can be practical difficulties in tying the two together.

3 Is a CCTV system of particular relevance to insurers?

The most important criteria to determine whether a CCTV system is of particular relevance to insurers are formulated below as questions that can be answered with 'yes' or 'no'. The answer ('yes' or 'no') will either lead to the next question or to the conclusion that a certain system is not of relevance to insurers (i.e. will not provide protection of insured property).

Answering the questions can therefore be considered as a 'quick scan' method to evaluate a given CCTV system. A more detailed evaluation model is provided in Chapter 5 of this document.

Questions		**Remarks**
Is the insured responsible for the CCTV system?	No →	The CCTV system is not of primary relevance to insurers.*
Yes ↓		
Is the CCTV system installed to supervise public areas?	Yes →	The CCTV system is not of primary relevance to insurers.*
No ↓		
Is the CCTV system installed to protect insured property?	No →	CCTV systems that are installed not to protect the insured property are not of primary relevance to insurers.*
Yes ↓		
Is the location where the CCTV system is installed, well-lit and conducive for CCTV?	No →	The CCTV system is not of primary relevance to insurers.*
Yes ↓		
Are the monitors of the CCTV system permanently staffed by: a. the (staff of the) insured or b. a contracted RVRC(remote video response centre)? and / or: Is the CCTV system provided with video motion or movement detection software that alerts staff (or RVRC) to watch the monitor(s) when the image changes?	No →	If the monitors of the CCTV system: - are not staffed and - the system is not provided with video motion or movement detection software to alarm the staff the CCTV system is not of (or only of limited) primary relevance to insurers.*
Yes ↓		
Is the CCTV system linked to effective response a. by the insured directly or b. by a contracted remote video response centre (RVRC)?	No →	Without effective response a CCTV system is not of (or only of limited) primary relevance to insurers.*
Yes ↓		
Is the insured property at the location where the CCTV system is installed of exceptional value to thieves?	Yes →	Without any other means of protection a CCTV system is not suitable to protect insured property of higher than 'normal' value.
No ↓		
The evaluated CCTV system is of interest to insurers. For a more detailed evaluation: see chapter 5.	←Yes	Are other means of protection available to protect property of exceptional value?

* Note: The presence of a CCTV system may – in some cases – prevent people from stealing insured property. This of course is of relevance to insurers, which may also be the case when the CCTV system is provided with a facility to store images.

4 Requirements

The following paragraphs propose an approach towards the specifying of CCTV systems which should be required by insurers whenever such protection is deemed necessary as a condition of insurance cover.

4.1 Operational Requirements for a CCTV system

When CCTV is proposed as a security solution in any particular case, it is of critical importance that the key objectives and operational parameters for such a system are determined and defined in a structured manner at the outset to ensure that, once installed and operational, it properly fulfils its intended purpose.

This process will produce a high-level, aims-oriented specification, generally referred to as the Operational Requirement for the system.

The design, selection of equipment, monitoring and response arrangements for a CCTV installation will all flow logically from the defined Operational Requirement. It is thus, together with the selection of suitable, proficient contractors, the key to a successful, good quality installation. Responsibility for the development of the Operational Requirement lies primarily with the security solutions specifier (i.e. normally the customer and/or his security advisors/insurers). The document will normally comprise a number of stated objectives and site–specific facts that reflect the key issues which will influence the system design.

EN 50132-7 lists the contents of a well-defined Operational Requirement. The following headings are recommended as a standard model approach to achieving this but different risk-specific circumstances will demand additions or variations to the model in particular instances.

4.1.1 Basic objective

States the intended purpose(s) of the system (e.g. Detect intruders on the site after normal business hours and function as an aid to access control during business hours).

4.1.2 Description of targets

States who or what are the intended targets of the system. (e.g. Unauthorised persons within the confines of the perimeter fence, or vehicles entering the access driveway). The degree of image detail should also be stated (e.g. The images should permit identification, recognition or detection of persons or vehicles).

4.1.3 Activity to be captured

States what activity the system is to be designed to display (e.g. Persons moving into the monitored area).

4.1.4 Period of observation

States when the protection is to operate (e.g. Daily between 21.00 and 08.00, and all day on Sundays and public holidays).

4.1.5 System / Picture attributes

States the key performance characteristics and quality of the system and its displayed images (e.g. Should be able to detect immediately the presence of persons and track their movements throughout the site. Monochrome pictures will suffice).

4.1.6 Conditions at the location

States what factors will apply during the monitoring period that are significant in terms of system design. (e.g. Low pressure sodium lighting will illuminate the site throughout the monitored period. Up to four commercial vehicles will be stationed alongside the warehouse loading doors out of working hours).

4.1.7 Resilience

States how robust the system needs to be in relation to environmental conditions, vandalism, sabotage and power continuity (e.g. The location of the site is such that it is exposed to fog during autumn and winter months, which often reduces visibility to 100m. The system should be designed to operate effectively in such circumstances).

4.1.8 Monitoring and image storage

States where, and by whom, the system should be monitored and operated, and what is to be recorded (e.g. Monitoring will take place at an approved remote monitoring centre. Views triggered by alarms should be recorded at the remote centre in real time. Other views should be continuously recorded locally at site in time lapse mode).

4.1.9 Actions

States what actions are required when security is jeopardised and, if applicable, as a matter of normal routine (e.g. The subjects should be warned off by the remote monitoring centre operator using a public address facility. The monitoring service should carry out routine dial-up video patrols at 2-hour intervals throughout the monitoring period).

4.1.10 Response

Assuming that attendance at the site will be required in the event of certain contingencies, it should be stated exactly what type of response is needed (e.g. keyholder, guarding service and/or police) for different events (e.g. intruders, trespassers), and what the target time for response should be. For more details see paragraph 4.6.

4.2 Camera, Lens and Illumination

The camera is one of the most important components in a CCTV system. It takes the reflected light from the scene and changes the light into electrical signals which can be transferred, processed and evaluated. It is the eye of the system. The lens and illumination should be considered in direct conjunction with the camera. It is essential to harmonise the three parts on site. All parts have many characteristics which should be taken into account to achieve the best result. This can be a very complex task. The following remarks do not claim to be exhaustive. Needless to say, camera and lens technology is permanently developing. In any case, the instructions of the manufacturer should always be followed.

Three basic requirements should be met:

4.2.1 Proper illumination.

Cameras have different responses to the spectrum of light. Therefore it is necessary to choose the illumination with the appropriate spectrum.

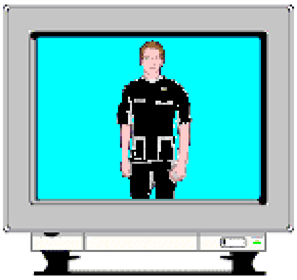
Depending on the camera light sensitivity and the light transmission through lenses, sufficient illumination should be ensured.

The best results will be obtained if the whole scene is illuminated by means of homogeneous light. Reflections, peak light and strong back light should avoided or appropriate measures should be taken, e.g. back light compensation.

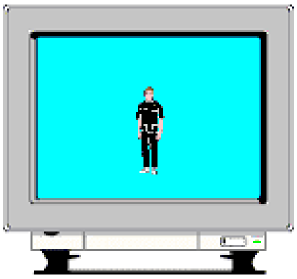
4.2.2 Suitable lens

Knowing that the picture area depends on the focal length, it is necessary to determine the scene size, the object distance and the grade of details to obtain in order to achieve the required features of the CCTV system. EN 50132-7 provides guidance for the recommended minimum sizes of targets in an image:

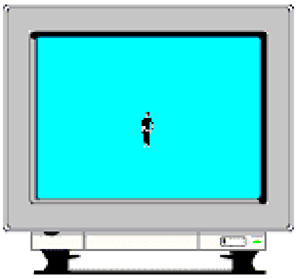
Identification – the target should represent not less than 120% of screen height.



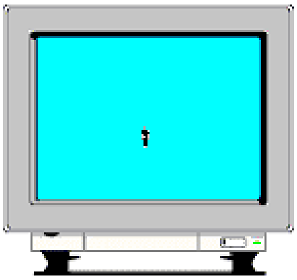
Recognition - the target should represent not less than 50% of screen height.



Detection - the target should represent not less than 10% of screen height



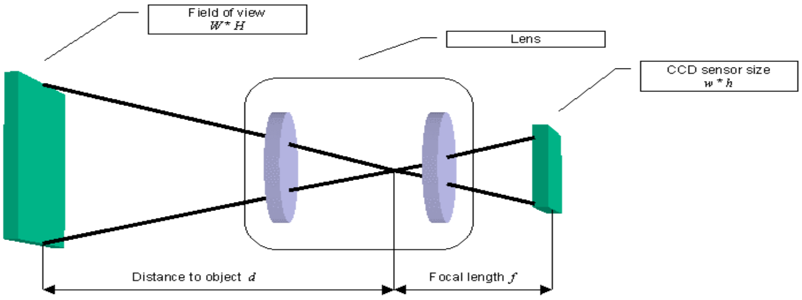
Monitoring - the target should represent not less than 5% of screen height.



The picture area does not only depend on the focal length but also on the CCD format. The following formula describes the connection:

$$w / W = h / H = f / d$$

f	focal length
d	distance to object
w	width of sensor
W	width of view
h	height of sensor
H	height of view



4.2.3 Correct camera

The available resolution of the camera determines whether suitable images can be achieved.

There are pros and cons to take into account in considering the use of a colour camera rather than black/white.

Pros	Cons
Colour may deliver additional information which could be important for the identification of an object.	The resolution of a colour camera is lower than a comparable b/w camera.
A colour image is more natural for the human eye.	The light sensitivity of a colour camera is lower than a comparable b/w camera.
	A colour camera is not suitable for infrared illumination

In most cases colour cameras should be preferred.

4.3 Video motion detection

In a Remote Video Response Centre (RVRC) or Local Monitoring Desk (LMD) [see paragraph 4.5] normally the screen is black unless the CCTV system generates an alarm. Therefore it is necessary to install some kind of motion detection. This could be done by a movement detector, by Video Motion Detection (VMD) or by a combination of both.

Video Motion Detection is a specialised technology incorporated into CCTV equipment or that can be ”bolted-on“ to any existing system originally supplied without the capability. VMD is designed to detect movement in a CCTV picture and allow this to trigger specified alerts and other responses.

In essence, it achieves this by dividing the picture into numerous cells and zones and comparing the brightness of pixels frame-by-frame, and cell by cell. By arranging the cells into zones in logical configurations according to the parts of the picture required to be sensitised and then applying modern data processing algorithms, it is possible to detect human targets whilst suppressing false alarms from passing clouds, waving flags, car headlights etc. These systems can be very impressive in stable internal environments but require very skilled setting up and lens selection in the outdoor situation where, even with powerful processing, users should be reconciled to frequent false alarms.

The technology is under continuous development yet its reputation for false triggering through inexpert commissioning and/or environmental factors has led to it being somewhat unpopular with remote surveillance services. Nevertheless, VMD can prove an invaluable tool for on-site monitoring operations with numerous scenes requiring simultaneous monitoring.

Claims are made that, compared with unaided monitoring of numerous sequencing or split screen views, the use of VMD can reduce the chance of intrusion going undetected by a factor of 20. VMD is potentially much more discriminatory than use of conventional detectors (e. g. PIR`s) and can be employed where separate detectors are not practicable.

A VMD system can be programmed to display alarmed scenes in sequence highlighting the location of movement on the display and even tracing on screen the path taken by the intruder in the field of view. Such features can be very powerful aids to increasing the effectiveness on the observers.

The output from the VMD system can be applied in various ways:

- Operate visual/audible indicator
- Display alarmed scene on normally blank screen
- Start up storage device or switch from time lapse to real time
- Send images to another location
- Email images

The sophistication, power and facilities of the various VMD products are variable. Genuine VMD should not be confused with crude on-board motion detection in some cameras/multiplexers with “activity detection” often used in storage devices to “ration” storage capacity.

4.3.1 General rules

Internal use

It is very effective when targeted with thought e. g. on a sensitive fire exit or a valuable painting.
Continuous, even lighting is preferred – sunlight via large rooflights might be problematic.

External use

The use of VMD should be avoided where there are moving objects in view (e.g. waving trees, flags, normal traffic).
The system should be able to accommodate the effects of perspective/target size variation and agile enough to detect fast moving objects and multiple triggering in quick succession.
Fixed view cameras on solid mountings should be required.
Systems should be used that detect objects moving in a selected direction (e. g. toward a building).

4.3.2 Special rules

When using VMD in security applications it should be taken into account that there are three kinds of alarm.

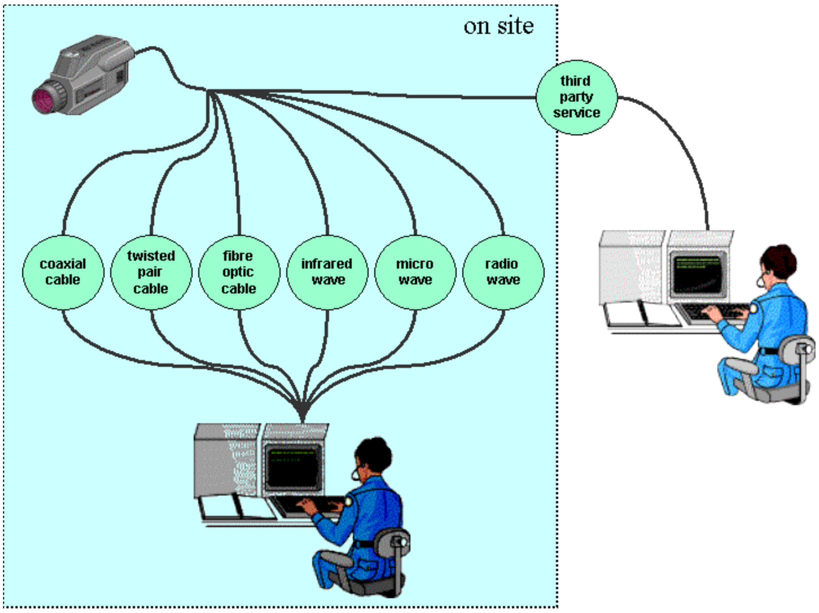
- The “correct” alarm which is caused by an intruder, for instance. This kind of alarm should be detected with high probability.
- The “false” alarm which is caused by improper installation or equipment. For example, that will happen if the camera is insufficiently fixed.
- The “nuisance” alarm which is hardly to avoid with the present state of technology, but should be reduced to a minimum.

The installer and the user should define the following topics:

- How many nuisance alarms are acceptable per day?
- How fast does the system have to detect; what speed of the target does the system have to observe?
- Is day and night detection required? In case of night observation, VMD should be capable of adjusting the light sensitivity in order to achieve sufficient alteration in contrast.

The minimum height of the target at the monitor should be considered. The minimum should be 5 % of the monitor’s dimensions. Otherwise the operator may be unable to distinguish an animal from an intruder.

4.4 Transmission System



The diagram shows the various methods of transmitting an image from the camera to the monitor. Often more than one transmission method will be used within one installation.

Each method has his own special requirements. Nevertheless it is always the same task.

The transmission system should be capable of reproducing the video signal accurately at the receiving end without loss of required information. The receiving centre should conform with the requirements described in paragraph 4.5 below.

In general, a distinction can be made between two kinds of transmission:

- The physical transmission path is part of the CCTV system.
- The physical transmission path is provided by a third party.

<u>The physical transmission path is part of the CCTV system</u>

The LMD is on site. All decisions concerning the transmission path can be made by the installer in consultation with the customer.
Cable should be installed in as inconspicuous and fail-safe a manner as possible within the premises.
The availability of the transmission path should be at least 98,5% per year.
The equipment should give an alert when the signal is lost or a failure occurs.
The picture should be conveyed without significant loss of quality caused by the transmission system.

<u>The physical transmission path is provided by a third party</u>

There is an RVRC. A third party is responsible for the transmission path.
Transmission of CCTV is usually achieved using one of the services offered by a public telephone utility or an in-house network. With modern compression methods, it is possible to send usable pictures over a standard telephone link but the most popular method is ISDN which is faster and more reliable. Increasingly, CCTV is being conveyed by networks such as LANs, WANs, Intranets and the Internet itself. Assessment of the resilience and integrity of such a set-up is really a matter for a telecoms specialist and there are too many variables for relevant requirements to be set out in this document.
The relationship between picture quality and picture transmission rate should be defined during the system design process.
The availability of the transmission path should be at least 95% per year.

4.5 CCTV Monitoring

The monitoring of a CCTV system may be provided:

1. 'in-house' by a Local Monitoring Desk (LMD) or

by a third party Remote Video Response Centre (RVRC).

4.5.1 Requirements for CCTV Monitoring

As the RVRC provides its services to several (or many) clients and the services are comparable to those of a third party Alarm Receiving Centre for intruder alarm systems (ARC), it is clear that the RVRC should meet requirements that, for the greater part, are the same as those for ARCs. Due to the special tasks and functions however, the RVRC also should meet a number of more specific requirements. The requirements for LMDs are similar to, albeit less comprehensive than, those for RVRCs.

The 'general' requirements for LMDs and RVRCs should be based on document CEA 4036 (Recommendations for Remote Monitoring Centres). (Clearly some of these requirements are too severe for LMDs and a forthcoming Code of Practice will identify which particular requirements are not appropriate).

Specific requirements for a RVRC are specified below in paragraph 4.5.2.

The less comprehensive requirements for a LMD are given in paragraph 4.5.3.

In addition to the given requirements, it should be noticed that the quality of the services delivered by LMDs and RVRCs also strongly depend on:

- the quality of the CCTV systems being monitored
- the transmission medium
- the proprietary video compression and transmission system
- the proprietary hardware/software at both ends of the link (incl. the interface)
- the workload of the operator (e.g. number/size of sites, performance of the installations, breadth of services being provided)
- the arrangements for responding to events
- the effectiveness of the liaison between the client, installer and RVRC

4.5.2 Specific requirements for a RVRC

4.5.2.1 Operators

The RVRC should be manned with not less than two operators.

An operator with little working experience in a RVRC should be coached by an operator who has a working experience of at least 6 months.

The number of clients under contract, the size of CCTV systems of these clients, the services to be provided and the way the tasks of the operators are organised, should enable operators, when handling an alarm signal from a CCTV system, to respond within 1 minute to other alarm signals from other contracted CCTV systems.

In order that the operator can, at exceptional times, address multiple system alarms arriving in quick succession, there should not be any limitations applied by the equipment to prevent switching from one alarm to another.

4.5.2.2 Technical means

Each operator should be provided with 2 screens only. The first screen should display the images of the CCTV systems under surveillance, whilst the second screen should display the information concerning the area under surveillance (including a graphical representation of the site), the CCTV system (including the position of the cameras) and the instructions that were agreed with the client in case of an alarm.

In this document the screen to display the images is called the ‘image screen’, and the screen to display further information is called the ‘management screen’.

The two screens should normally be ‘black’, unless the operator is carrying out a video surveillance with one of the CCTV systems under contract, or unless one of these systems generates an ‘alarm’. Such an alarm should, of course, have priority over ‘normal’ surveillance tasks with CCTV systems that are not in the alarm mode.

When the management screen is in operation it should indicate:

which system (client) is connected to the screen

and whether the screen is on because of the reception an alarm signal or for routine surveillance duties or other circumstances e.g. fault reported.

In case of an alarm triggered by one of the CCTV systems, it should be possible to have access to:

- live video pictures
- information about the detector or camera that generated the alarm in the form of:
  - at least 3 frozen images, at an interval of 5 seconds maximum, of the scene just before the alarm was generated
  - a map showing which detector or camera generated the alarm
- written instructions about ‘what to do’ in accordance with the contract with the client
- the report about the previous received alarm
- a report about the malfunctioning or closing down of one or more cameras or detectors in the CCTV system. (Such a report should automatically result in an instruction to send the client a recommendation to have the system serviced by the installer).

Icons at the graphical representation (map) should give information about the CCTV system, including:

- the position of all cameras and detectors, including the direction of the cameras (if appropriate)
- the position of microphones and speakers, if the CCTV the system has audio facilities
- an indication of previous alarms in the current monitoring session.

The operator should be able to switch from one camera to another and to display the images of a maximum of 4 cameras on the split screen. The minimum size of the diagonal of each image within a split screen should not be less than 18 cm.

For CCTV systems with audio facilities the operator should be able to discriminate by zone:

1. between speakers and

2. between microphones

in order to be able to

1. communicate by speech

2. identify the source of sound on the site.

All received images should be recorded and kept in storage for a period of 1 month or in accordance with national regulations.

All operator activities should be recorded and kept in store for a period of at least 3 months.

4.5.2.3 Contracted CCTV systems

Where there is an approved certification scheme for CCTV installations, the quality of each CCTV system under contract to an RVRC should be proven by a certificate. (In territories where there is no such certification scheme, consideration should be given to introducing one with the aim of producing certified installers using certified components and plans).
Each CCTV system should be maintained under contract in accordance with 4.10.
The RVRC should receive a copy of this contract or written confirmation that there is a maintenance contract.
In most cases, fixed camera positions are preferred to movable cameras. If movable cameras are used, they should preferably be programmed to return to pre-set positions. (In most cases cameras that can be moved freely by operators are not advisable).
Zoom lenses should, after use by the operator, automatically return to pre-set positions.
In case of a failure in the power supply of one of the CCTV systems, a fault signal should be sent to the RVRC.

4.5.3 Specific requirements for a LMD

The requirements for an in-house Local Monitoring Desk (LMD) are similar, though a little less comprehensive, to those for a third party monitoring centre (RVRC) as outlined in 4.5.2. This is of course because an LMD is situated in-house and usually has only one CCTV system to monitor. The requirements for LMDs therefore follow the requirements for an RVRC, albeit that the unnecessary requirements are left out.

4.5.3.1 Operators

The LMD should, at all times during surveillance hours, be manned with an experienced operator.
An operator without working experience in the LMD should be coached by an operator who has a working experience of at least 1 month.

4.5.3.2 Technical means

Each operator should be provided with 2 screens only. The first screen should display the images of the CCTV system, whilst the second screen (the management screen) should display the information concerning the area under surveillance (including a graphical representation of the site), the CCTV system (including the position of the cameras) and the instructions that in the event of an alarm.

At an LMD it is possible (depending on the risk) to replace the management screen by a manual containing all the necessary information.

The screen(s) should normally be ‘black’, unless the operator is carrying out a video surveillance, or unless the system generates an ‘alarm’ or some other actionable event occurs e.g. fault. Such an alarm should, of course, have priority over ‘normal’ surveillance tasks.

When the management screen is in operation it should indicate whether the screen is on because of the reception an alarm signal or for routine surveillance duties.

In the event of an alarm triggered by the CCTV system, it should be possible to have access to:

- live video pictures
- information about the detector or camera that generated the alarm in the form of:
  - at least 3 frozen images, at an interval of 5 seconds maximum, of the scene at the moment the alarm was generated
  - a map showing which detector or camera generated the alarm
- written instructions about ‘what to do’
- the report about the previous received alarm
- a report about the malfunctioning or closing down of one or more cameras or detectors in the CCTV system. (Such a report should automatically result in an instruction to have the system serviced by the installer).

Icons at the graphical representation (map) should give information about:

- the position of all cameras and detectors
- the position of microphones and speakers if the CCTV system has audio facilities
- an indication of previous alarms in the current monitoring session

The operator should be able to switch from one camera to another and to display the images of a maximum of 4 cameras on the split screen. The minimum size of the diagonal of each image within the split screen should not be less than 18 cm.

For a CCTV system with audio facilities, the operator should be able to discriminate by zone

1. between speakers and
2. between microphones

in order to be able

1. to communicate by speech
2. identify the source of sound on the site.

All received images should be recorded. Any recorded images relating to actual criminal activity should be kept until agreed by the relevant authorities that they may deleted, and "suspicious" incident recordings should be kept for a minimum of one month.

All operator activities should be recorded and kept in store for a period of at least 1 month.

4.5.3.3 The CCTV system

The CCTV system should, of course, fulfil the requirements given in paragraph 4.5.2.3 (other than those that relate specifically to RVRCs).

4.6 Appropriate Response

As indicated earlier in this Guide, a CCTV system which has been installed for the protection of insured property will normally only receive the approval of insurers if the proposed response to witnessed events is deemed appropriate and adequate.

A CCTV system that has been installed simply to record events for future reference (e.g. evidential purposes) will generally not be suitable for insurers' needs.

There are various types of response available, and there is no single solution which can be applied to all circumstances. It is a case-by-case decision as to the type (or types) of response that is (are) considered appropriate.

The types of response available will generally fall under one of the following headings:

Audio challenge. - The RVRC or LMD challenges the "subject" verbally using microphones installed about the protected site. The challenge may be either pre-recorded or (preferably) "live and personal".

Keyholder. - The RVRC or LMD summon the Keyholder (either the CCTV owner, his staff, or his appointed professional response company).

Police. - The RVRC or LMD contacts the police and requests their attendance. (Note: the preparedness of the police to attend CCTV-witnessed events, and the terms under which they will agree to do so, will differ from country to country).

Other authorities. - The RVRC or LMD contacts other authorities according to the purpose of the installation and/or the nature of the event. (e.g. Fire service, rescue service, ambulance service).

The circumstances in which a response should occur, and the nature of that response, should be stated in a written agreement or contract between the owner/manager of the CCTV system and the RVRC (or, if the monitoring is in-house, it should be stated in written assignment instructions for the LMD operator). In many cases, it will be appropriate to prescribe a 2-stage response for site protection, i.e.:

Stage 1 - audio challenge

Stage 2 - summon keyholder and/or police in the event that the audio challenge does not result in the desired outcome.

Clearly, where the required response involves attendance at the site, insurers will need to be satisfied that the anticipated attendance time is acceptable.

4.7 Documentation

As a minimum, the documentation presented to the user by the installer should include:

- operating instruction
- circuitry diagram
- register of the cameras
    - location
    - illumination
    - limits in operation time
    - pan, tilt, zoom
    - special features (audio transmission, motion detection)
- image storage procedure
- site plan
    - camera positions
    - field of view
    - scale
- Transmission medium (including security)
- System log-book
- Contract for maintenance and (where appropriate) remote monitoring

4.8 Qualifications of Installers and Monitoring Centres

CEA Requirements for installers of fire protection and intruder alarm systems are in course of preparation. It is proposed that when this document is completed, it forms the basis of the qualification requirements for CCTV installers and RVRC operators.

As with all forms of security contract, it is advisable to use only firms which are certified by an insurer-approved certification scheme for the installation of CCTV systems and for RVRCs (as appropriate). Where no such scheme exists, it is advisable that insurers introduce one based upon the CEA document 'CEA base requirements for installers of fire detection and alarm systems and/or intruder alarms' Where an existing certification scheme falls short of the requirements detailed in this document, insurers should aim to superimpose the CEA requirements.

It is also recommended that an insurer-approved scheme be introduced for the certification of installations where such a scheme does not already exist.

4.9 Test Procedures and Handover

The system should work correctly for 8 days under the observation of the installer before it is put into definite operation. The installer should provide the documentation for the system and a system log book.

The customer and the operating staff should be instructed by the installer in the correct use of the system. The installer should point out that the customer is responsible for the system after handover and should ensure proper operation and maintenance. Furthermore the customer should immediately inform the maintenance service about detected failures and other irregularities. All such matters should be registered in the system log book.

4.10 Maintenance and Inspection

Periodical inspections and preventative maintenance are necessary to guarantee the function of the system.

All work on the system should be carried out by qualified personnel with suitable replacement parts and the technical documentation.

Inspection

There should be routine 6 monthly inspections by the maintenance service company.

The system should be thoroughly inspected and tested during the visit.

The following topics should be especially inspected:

- the transmission paths
- all components to ensure they are fixed as defined
- all components to check for mechanical damage
- the supervised area of each camera
- the storage, operation and display equipment
- the complete site to check for any disturbance influence or changed environment (e.g. a rearrangement of rooms)

Preventative maintenance

On an annual basis there should be:

- replacement of each component which has a limited life time
- adjustment of components

as necessary.

The 6-monthly inspection could be a part of the preventative maintenance.

Each inspection or preventative maintenance visit, and any extension to or modification of the system should be registered in the system log book.

5 Insurers’ CCTV Evaluation and Specification Model Questionnaire

The following questionnaire is offered as a useful tool for insurers in:

- evaluating an existing CCTV system
- specifying a new CCTV system

It is proposed that a more detailed Code of Practice should be developed jointly by insurers and the CCTV industry. In the course of this work it is expected that this Questionnaire will be further refined.

See chapter		Yes	No	Comments
	Introduction			
3.	Is the insured responsible for the system?			
3.	Is the system installed to protect insured property?			
2.4	Which are the supporting measures? (e.g. physical measures, perimeter barriers, safes, visiting guards etc.)			
2.6	Is the CCTV system in conjunction with an intruder alarm system?			
3.	Is the insured property at the location where the CCTV system is installed of exceptional value to thieves?			
	When the answer to the previous question is 'yes', which are the supporting measures?			
4.7	Documentation			
	Is the following documentation available?			
	Operating instructions			
	Circuitry diagram			
	Register of cameras			
	Image storage procedure			
	Site plan			
	Transmission medium			
	System logbook			
	Maintenance contract			
	Remote monitoring contract			
4.1	Operational Requirements			
	Is there an Operational Requirement document in accordance with EN 50132-7 ?			
	Does the Operational Requirement document support insurer's requirements?			
4.1.1	What is the basic objective of the system?			
4.1.2	What or who are the intended targets of the system?			
4.1.3	What activity is to be captured?			
4.1.5	What is the purpose of the target image of each camera? (identification/recognition/detection)			

See chapter		Yes	No	Comments
4.2	Camera, lens and illumination			
4.2.1	Illumination			
	Is illumination available when needed?			
	Is the spectrum of the illumination appropriate for the cameras?			
	Is the illumination homogeneous?			
4.2.2	Lenses			
	Are the lenses of the cameras suitable for the purposes described in the Operational Requirements document?			
4.2.3	Cameras			
	Is each camera successfully tested:			
	For resolution?			
	Light sensitivity?			
	If movable cameras are used, are they programmed to return to pre-set position?			
4.3	Video Motion Detection (VMD)			
	What type of detection is used?			
	Video Motion Detection?			
	Movement detectors?			
	None			
	Is the VMD suitable for the purposes described in the Operational Requirements document?			
	Is the number of nuisance alarms per day not exceeding the defined number?			
	Is the speed of detection according to the required speed in the Operational Requirements document?			
	Is the VMD capable to adjust the light sensitivity if necessary?			
4.4	Transmission system			
	Which type of transmission is used?			
	Transmission is part of the CCTV system leading to the LMD.			
	Third party transmission to RVRC			
	Is the transmission path monitored?			
	Is the availability of the transmission path at least 95% per year?			

See chapter		Yes	No	Comments
4.5	Monitoring			
	What is the period of observation? (24 hours / overnight / weekends)	▨	▨	
	What type of monitoring is employed? (in-house / RVRC / both / switched)	▨	▨	
	Do the video monitoring arrangements meet the insurer's requirements? (Alarm-activated only / routine video patrols?)			▨
4.5.1	Does the RVRC, if used, meet the requirements under 4.5.1 ?			▨
4.5.2	Does the LMD, if used, meet the requirements under 4.5.2 ?			▨
	Is the contract for monitoring satisfactory?			▨
4.6	Response			
	Are actions / responses prescribed in writing?			▨
	What are the actions / responses? (proactive or reactive only)	▨	▨	
	Do the prescribed actions / responses meet insurer's requirements?			▨
	What images are to be recorded?	▨	▨	
	Where are these recorded images to be stored?	▨	▨	
4.8	Installer			
	Does the installer meet the requirements of CEA 4036 'Certification of installers'?			▨
	Is the contract for maintenance satisfactory?			▨
4.9	Test Procedures and Handover			
	Is the CCTV system handed over to the insured by the installer?			▨
	Was the insured instructed by the installer when the system was handed over?			▨
4.10	Maintenance and Inspection			
	Is the system inspected and tested every 6 months ?			▨
	Is the system maintained by the installer at least once a year?			▨

▨ Not applied

6 References

CEA 4036	Recommendations for Remote Monitoring Centres
EN 50132	Alarm systems – CCTV surveillance systems for use in security applications

(END)