KENYA STANDARD **KS 2110-1:2009**

Installation and remote monitoring of detector activated CCTV systems.

Part 1: Code of practice

PUBLIC REVIEW DRAFT,MARCH 2009

 First Edition 2009

TECHNICAL COMMITTEE REPRESENTATION

The following organizations were represented on the Technical Committee:

Eveready Batteries Kenya Ltd.
Associated Battery Manufacturers
Kenya Railways Corporation
Securicor Alarms (K) Ltd.
Department of Defence
Ministry of Roads and Public Works
Kenya Power & Lighting Company Ltd.
Automotive Industrial Battery Manufacturers (A.I.B.M) (K) Ltd.
Ministry of Energy
Jomo Kenyatta University of Agriculture and Technology — Electrical Engineering Department.
Kenya Bureau of Standards — Secretariat

REVISION OF KENYA STANDARDS

In order to keep abreast of progress in industry, Kenya Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Managing Director, Kenya Bureau of Standards, are welcome.

ISBN

KENYA BUREAU OF STANDARDS (KEBS)

Head Office: P.O. Box 54974 Nairobi,Tel.: (+ 254 020) 502210-19,502543/45.,Fax: (+ 254 020) 503293
E-Mail: info@kebs.org, Web:http://www.kebs.org

Coast Regional Office
P.O. Box 99376, Mombasa
Tel.: (+254 041) 229563, 230939/40
Fax: (+254 041) 229448

Western Kenya Regional Office
P.O. Box 2949, Kisumu
Tel.: (+254 057) 23549, 22396
Fax: (+254 057) 21814

Rift Valley Regional Office
P.O. Box 8111, Eldoret
Tel.: (+254 053) 33151, 63377
Fax: (+254 053) 33150

Foreword

This Kenya Standard was developed by the Technical Committee on Extra-low Voltage equipment and is in accordance with the procedures of the Bureau.

This standard gives the code of practice for the installation and remote monitoring of detector activated CCTV systems.

In the preparation of this Kenya Standard, reference was made to the British Standard BS 8418:2003

Acknowledgement is hereby made for assistance derived from this source.

Introduction

This document is intended to provide recommendations to the following parties:

-Installers on best practice for the design, installation, commissioning and operation of detector activated CCTV systems;

-Remote video response centres (RVRCs) monitoring CCTV systems;

-Owners and users on the management of CCTV systems.

CCTV systems installed and monitored in accordance with this code of practice should be capable of obtaining a response to a confirmed incident from the police (or other responding authority).

When a detector senses an event, images are transmitted to, and displayed at, an RVRC and this is regarded as an alert. However, emergency response should not simply be called in relation to an alert. RVRC operators should view images for a period of time and might only call for emergency response if there is positive evidence in these images of unauthorized access to the site and of actual criminal or other untoward activity, i.e. an incident. The emergency response will be as agreed between the parties (see **7.2**).

The normal mode of operation for these CCTV systems is not to display images at an RVRC unless there has been an event at the site. However, depending on the terms and conditions of the contract with the owner, the RVRC operator may be permitted to view the site at other times. The owner may also be able to view the site remotely.

Installation and remote monitoring of detector activated CCTV systems Part 1: Code of practice

1 Scope

This Kenya Standard gives recommendations for the design, installation, commissioning, operation and remote monitoring of detector activated CCTV systems.

It is intended to be primarily of use to RVRC operators and owners of CCTV systems.

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.

BS 4737:1988 (all parts), *Intruder alarm systems.*

BS 5979:2007, *Code of practice for remote centres receiving signals from security systems.*

BS 7858:2006, *Code of practice for security screening of personnel employed in a security environment.*

BS 7958:2005, *Closed-circuit television (CCTV) - Management and operation - Code of practice.*

BS 7992:2002, *Code of practice for exterior deterrent systems.*

BS EN 50131-1:2006, *Alarm systems - Intrusion systems - Part 1: General requirements.*

BS EN 50132-7:1996, *Alarm systems - CCTV surveillance systems for use in security applications Part 7: Application guidelines.*

PD 0008:2004, *Code of practice for legal admissibility and evidential weight of information stored electronically.*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1
Activation
Transmission of images to a RVRC.

3.1.2
Alert
Activation where there is not positive evidence in images of unauthorized access to the site and of actual criminal activity.

3.1.3
CCTV control equipment
Equipment for receiving, processing and initiating the onward transmission of data.

3.1.4
Closed site
Site entirely surrounded by a soundly constructed and secure barrier, when the CCTV system is in a set condition, in order to deter unauthorized access.

3.1.5
CCTV system
System consisting of camera equipment, monitoring and associated equipment for transmission and control purposes, which might be necessary for the surveillance of a defined secure area.

3.1.6
Data
Information in the form of pictures, sound and any other associated, linked or processed information, including that about a person.

3.1.7
Detector
Device that detects an event.

3.1.8
Event
Activity within a secure area.

3.1.9
Incident
Activation where there is positive evidence in images of conditions requiring an emergency response and/or of actual criminal activity.

3.1.10
Initial activation
First activation that occurs after the CCTV system has been set, or after a previous incident or alert has been closed down during the set period

3.1.11
Open site
Site not entirely surrounded by a soundly constructed and secure barrier when the CCTV system is set.

3.1.12
RVRC operator
Person located at the RVRC specifically designated, trained and authorized to carry out monitoring of the CCTV system at the RVRC

3.1.13
Owner
Legal person or entity, agency or individual, designated as having overall responsibility for the formulation and implementation of the policies, purposes and control of a CCTV scheme

3.1.14
Ancillary control equipment (ACE)
Portable device used for setting a CCTV system.

3.1.15
Recorded material
Any data recorded on any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

3.1.16
Remote video response centre (RVRC)
Operation which is continually manned and capable of receiving multiple concurrent CCTV images from remote locations for the purpose of interacting with sites to provide security and related services.

3.1.17
Secure area
Area within the site to which access cannot be gained without the creation of an event

3.1.18
User
Person authorized by the owner to operate the CCTV system on site

3.1.19
Parked position
Position to which a pan, tilt and zoom (PTZ) camera automatically returns after a preset time or earlier on command

3.1.20
Set
Status of a CCTV system or part thereof in which an event results in activation

3.1.21
Reset
State of the CCTV system in which events are prevented from generating activation

3.1.22
Automatic timer
Device that sets and/or unsets the CCTV system at pre-programmed times

3.2 Abbreviations

For the purposes of this Kenya Standard, the following abbreviations apply.

ACE	Ancillary control equipment
CCTV	Closed circuit television
ISDN	Integrated Services Digital Network
PIR	Passive infrared
PSTN	Public Switched Telephone Network
PTZ	Pan, Tilt and Zoom
RVRC	Remote Video Response Centre
UPS	Uninterrupted Power Supply
VMD	Video Motion Detection

4 CCTV system design and installation

4.1 Detector positioning and configuration

Detector positioning and configuration should conform to the following recommendations.

a) Detectors should be installed in accordance with BS 7992:2002, BS 4737: or BS EN 50131-1:2006 as applicable. Cameras using video motion detection (VMD) should be installed to manufacturer installation instructions.

b) Detectors should only cause activation in areas within the specified field of view of associated cameras on the CCTV system. Detector field of view should not be greater than the associated camera field of view [see **4.2.1**)].

NOTE 1 : An exception to this would be where the associated camera view intentionally covers an area more likely to give the RVRC operator information about the event, than one within the range of the detector itself, e.g. where a detector inside a building causes an activation from a selected external camera.

c) Detector range should not overspill the site boundary.

NOTE 2: Problems might occur when the range of a passive infrared (PIR) detector extends to a public path or roadway. Where possible, detectors should be positioned facing inward.

NOTE 3 Care should be taken when a PIR detector is positioned to cover gates, as the detector range might extend through the gate. An active beam or curtain PIR detector traversing the gateway should be considered.

d) Detectors should be positioned in such a way that when looking horizontally across an area in an east-west plane they are not adversely affected by the, rising or setting of the sun. Secondary detectors oriented in a different direction and paired should be considered.

e) Multiple detectors should not be connected to a single input unless individually identified by the CCTV control equipment.

NOTE 4: This is particularly relevant when a PTZ camera is driven to multiple preset locations dependent on the detector or an area where an event is taking place. In these circumstances it is essential that the detector indicates independently at the RVRC, otherwise there is no method of determining that two incidents might have occurred in short succession.

f) Detectors should be suitable for the application and environment in which they are sited, e.g. internal or external, extremes of weather.

NOTE 5: PIR detectors vary considerably in sensitivity and those primarily designed for lighting control and door opening should not be used.

4.2 Camera positioning and configuration

4.2.1 *General*

Camera positioning and configuration should conform to the following recommendations.

a) The CCTV system should conform to BS EN 50132-7.

b) The positions of the cameras should be such that all areas of coverage of detectors can be viewed [see **4.1**b)].

NOTE 1 An exception to this would be where the associated camera view intentionally covers an area more likely to give the RVRC operator information about the event, than one within the range of the detector itself, e.g. where a detector inside a building causes an activation from a selected external camera.

c) For the purposes of verifying an event the field of view should be set to a 1.6 m high target filling a minimum of 10 % of picture height.

d) If recognition of an intruder is an objective, then larger image sizes should be considered (in excess of 50 % of picture height as a minimum).

e) The entry/exit route should either be viewed by a fixed camera or a PTZ camera with its parked position viewing the entry/exit route.

f) Care should be taken when using PTZ cameras. Where they are the sole means of viewing the field of detection they should be considered as multi-position fixed cameras by the utilization of presets, rather than as infinitely variable devices. The area to be viewed by each camera should be clearly identified, with any specific items to be checked highlighted. If a camera is required to survey a large area, the area should be divided into a series of discrete adjacent zones, each corresponding to a stored preset position. It should not be possible for an intruder travelling at 2 m/s to pass out of the field of detection before the camera can be moved to view the area.

*NOTE 2 Care should be taken to ensure that at each of its preset conditions the zoom setting enables conformance to [**4.2.1**b)].*

g) Wherever possible, care should be taken to ensure that cameras do not overlook public areas.

h) All equipment installed should be suitable to withstand the prevailing environmental conditions.

NOTE: 3 further information can be found in BS EN 50130-5.

i) All cameras should be uniquely identified using a name/label which will be displayed with or within the camera view at the RVRC and which corresponds to the name/label shown on the site plan for that camera view.

4.2.2 *Lighting*

Good lighting of the camera's field of view is essential and the following should be taken into account.

a) There should be sufficient lights on site to illuminate the camera's field of view.

b) It should be possible within 2 s of display of a complete picture at the RVRC for an RVRC operator to verify the presence or not of a human form 1.6 m high occupying not less than 10 % of picture height during day and night conditions [see **4.2.1**c)].

c) The lighting required for clear CCTV images should have their lamps changed in accordance with the manufacturer's recommendations. The RVRC operator should report any lamp failure to the owner within one working day of its discovery. The owner should rectify any known lamp failures within three working days of its discovery.

d) The owner should make weekly checks on the operation and effectiveness of the lighting.

NOTE 1: This could be achieved by viewing images recorded during the hours of darkness in the previous 24 h.

e) Lights should not be positioned such that they directly face cameras.

f) If clocks are used to control the lighting they should be adjusted accordingly.

NOTE 2: It might be desirable for the RVRC operator to control lighting on the site.

4.3 Audio challenge

An audio challenge facility is recommended except where its use is judged to reduce the effectiveness of the system or where there are noise pollution implications.

Where sites are equipped with audio challenge it should be clearly audible, without undue distortion within the range of all detectors.

NOTE: Care should be taken to avoid unwanted noise beyond the boundary of the site.

4.4 CCTV system performance and integrity

4.4.1 *Minimum performance requirements*

As a minimum, activation should initiate within 1 s of an event being detected, except where delayed procedures exist in accordance with **8.2**.

4.4.2 *Video transmission requirements*

The transmission system should send continuous video images while the RVRC operator is evaluating images.

4.4.3 *General*

Facilities might exist to omit any detector (when agreed in writing with the owner) either by RVRC operator action or automatically, e.g. the detector has a fault or regularly repeating operation, such as wind causing movement, that would prevent legitimate activation. If such omissions are implemented they should result in logs being generated, and should be recorded at the RVRC. As a minimum the log should uniquely identify the detector, time and date of omission and, either duration of omission or time and date of restore.

4.4.4 *Video integrity*

Camera signals should be monitored for video loss. Any video loss should be indicated without delay to the RVRC.

NOTE In some applications a video content detection system is necessary to determine whether an expected level of content of information exists within the image. This would protect against deliberate masking of the camera views, lens failure, or inappropriate lighting.

4.4.5 *Tamper*

All cabling to detectors should incorporate tamper detection. The detector enclosure should also be protected against tamper. To prevent tamper, the following measures should be taken.

a) Tamper circuits should be continuously monitored.

b) When the CCTV system is in the set condition, tamper Faults should be reported to the RVRC without delay.

c) When the CCTV system is in the unset condition, tamper faults should be reported to the RVRC and/or reported locally.

d) Any plugable connectors and control equipment should be contained within the secure area or within a suitable tamper monitored enclosure.

e) Where a camera, its housing or its alignment is likely to be tampered with tamper proofing should be installed.

4.4.6 *CCTV control equipment integrity*

The CCTV control equipment should be housed within a secure area. When the CCTV system is in a set condition, and the CCTV control equipment can be accessed without generating an immediate activation, the CCTV control equipment should be tamper protected (see **4.4.5**).

The control equipment should be protected using a secure validation process, e.g. a password, or electronic key, to avoid unauthorized access to the CCTV system.

The status of the CCTV system (set or unset) should be able to be determined by the RVRC and the CCTV system parameters should be remotely programmable from the RVRC.

NOTE It is desirable that the CCTV system is capable of remote diagnostics and remote correction.

If the CCTV system fails, the monitoring and control equipment on site should automatically attempt to restart. A failure to restart should be communicated as follows:

a) In the set condition to the RVRC;
b) In the unset condition locally and/or to the RVRC.

When the CCTV system failure is communicated to the RVRC, the CCTV system should send a restart signal to the RVRC if the CCTV system automatically restarts at any time.

4.4.7 *Event logs on site*

An ongoing event log should be maintained on site in a consolidated, dated and time retrievable format for a minimum period of six months, or until after the next maintenance visit (see **13.1**), whichever is the longer period. The event log should comprise as a minimum the following events:

a) Changes in CCTV system status, e.g. set, unset, part set;
b) Tampering and/or operation of detectors resulting in an incident or alert, or initiating an entry sequence;
c) Unsuccessful attempts to communicate with the RVRC;
d) Successful communication with the RVRC and confirmation that an alarm condition has been reported;
e) CCTV system exceptions, including restarts after mains supply failure, low battery and power failure.

4.4.8 *Communication integrity*

An alternative method of communication to the RVRC such as cellular telephone or an additional monitored telephone line, should be provided, if the primary transmission medium is not available, to enable line failure to be indicated at the RVRC.

4.4.9 *Retry procedure*

If the CCTV system fails to establish a connection with the RVRC, there should be an alternative connection option. As a minimum, the CCTV system should attempt to connect to the RVRC six times. This should be done either via two different numbered telephone lines (maximum three attempts per line) or using the single telephone number if the RVRC has the capability of allowing multiple ISDN/PSTN lines to be allocated to one number.

4.4.10 *Connection procedure*

Upon establishing a connection to the RVRC, and before transmission of data relating to the event, an authorization procedure should be performed between the equipment at the remote site and the RVRC to confirm the identity and authorization level of the systems at each end of the connection. In the event that the authorization procedure fails, for whatever reason, the system should abort the current connection attempt

and re-try. If authorization is not established the CCTV system should retry a further nine times within the same connection to attempt to gain authorization.

After 10 unsuccessful attempts, the connection should be terminated and re-tried using the alternative connection option (see **4.4.9).**

The procedure should take no more than 10 min to complete.

4.4.11 *Power supplies*

In the event of power failure, some facilities of a CCTV system can be lost. Power failure to the control equipment should be indicated to the RVRC. The use of an uninterrupted power supply (UPS) should be considered.

5 Commissioning

5.1 General

Commissioning a CCTV system before live operation can occur should be conducted in accordance with **5.2** to **5.7**.

5.2 Engineer walk test

The engineer walk test should be undertaken on site by the installing engineer in association with the owner and/or user and in conjunction with the company operating the RVRC. The basic tests should ensure compliance with this code of practice in the following aspects:

a) Field of view of detection devices and associated cameras (see Clause **4**);

b) Sensitivity of detectors, including those used to operate lighting (see **4.1** and **4.2.2**);

c) Clarity of images [see **4.2.1**d) and **9.4**];

d) The accuracy of recorded data, notably labels used to describe the CCTV system [see **4.2.1**i)].

5.3 Reference images

Reference images should be captured so that they can be used for comparison during live operation checks.

5.4 Night remote check

The RVRC should access the CCTV system remotely at night to ensure sufficient lighting exists to provide clear images of each intended view (see **4.2.2**).

5.5 Environmental soak test

The CCTV system should be left on test for 7 days following the engineer walk test (see **5.2**) to identify the trends in the protected environment, e.g. animal runs, shortcuts by pedestrians.

5.6 Faults

CCTV system configuration faults should be notified by the RVRC to the owner. The owner should arrange for any configuration faults to be corrected. All corrective actions should be carried out before the CCTV system is made live.

5.7 CCTV system acceptance certificate

The CCTV system acceptance certificate should be issued by the RVRC to the contracted party for whom the RVRC is providing monitoring. The certificate should confirm the date and time the CCTV system was accepted by the owner or his nominated representative and made live.

6 Site operational procedures

6.1 Setting/resetting procedures

6.1.1 *General*

The CCTV system should not cause activations during the setting or resetting procedures when carried out in accordance with the recommendations described in **6.1.2**, **6.1.3**, **6.1.4** and **6.1.5**.

6.1.2 *Local setting/resetting outside the secure area*

The entire setting and unsetting process should be completed from outside the secure areas in accordance with the following.

a) The setting device (keypad, card reader, etc.) should be fitted with tamper detection, which will operate if the cover/housing is removed so that its operation cannot be overridden.

b) The CCTV system states (set/unset) should be clearly indicated and visible from the setting location.

c) The setting/unsetting location should be permanently within the field of view of a camera. An exception to this may be when the setting/unsetting location is within another secure area of the CCTV system (see **6.1.3**).

d) When an ACE device is used to set the CCTV system, the setting/unsetting should only be affected from within the field of view of the camera in the CCTV system.

e) The range of the ACE device should be such that it is not possible to affect a setting/unsetting of the CCTV system from more than 10 m from the point of entry.

6.1.3 *Setting/resetting inside a secure area(s)*

The setting device should be inside the secure area and might be in the form of a discrete device, such as a keypad, key switch, or card reader.

a) Resetting

1) The device used to complete the resetting procedure should be inside a secure areas and might be in the form of a discrete device, e.g. a keypad, key switch or card reader.

2) Activation should not occur in the defined entry route during the resetting procedure.

3) Additional detectors not on the entry route may be rendered inactive for the duration of the unsetting procedure.

NOTE 1: This should be documented in the specification for the installed CCTV system.

4) There should be a time limit for the resetting procedure. If the time limit is exceeded an activation should take place.

5) Detection of an event not on the entry route, without prior initiation of the resetting procedure, should initiate activation.

b) Setting

1) The device used to initiate the setting procedure should be inside a secure areas and might be in the form of a discrete device, e.g. a keypad, key switch or card reader.

2) Detectors on the exit route should be disabled in the defined exit route during the setting procedure.

3) The setting procedure should be completed by one of the following:

i) Manual action of the user;

NOTE 2: This is the preferred solution wherever possible.

ii) Timer expiring.

4) If a detector is in an active state at the time of setting, an appropriate indication should be given at the setting/resetting location.

NOTE 3: See Annex A for further guidance on the setting procedure in the active state.

6.1.4 *Automatic timed setting and resetting*

There should be an on-site indication of the current set state.

NOTE: The use of an automatic timer for setting and/or resetting might not be acceptable for CCTV systems requiring emergency response.

6.1.5 *RVRC driven setting/resetting*

RVRC setting/resetting of the CCTV system or part of the CCTV system should be actioned as a result of a request to the RVRC. Such requests should only be made on an exceptional basis and should not be used as a routine setting/resetting method. An agreed validation process for this procedure should be agreed, and any RVRC action should be logged by the RVRC.

7 Owner responsibilities

7.1 Site information

The owner should provide the information requested in **10.1** to the RVRC before the CCTV system is commissioned.

7.2 Policy in response to activations

There should be a documented agreement between the RVRC and the owner as to what action will be taken upon receipt of an activation. In the event of there being no obvious cause of an activation, there should be an agreement between the RVRC and the owner as to the scope of RVRC operator action in determining whether an incident has taken place. This should cover the areas to be viewed, and whether images prior to the activation should be viewed from some or all of the areas.

NOTE The actions are likely to be dependant upon whether the site is an open site or closed site, and on whether the activation occurs in daylight or at night-time.

7.3 Staff access

The owner should ensure all authorized persons on site are informed that they should operate in a way that will minimize the occurrence of spurious activations as a result of their presence. In particular they should be made aware that if entry to the site is made, other than by the defined entry route, the RVRC should be notified in advance.

7.4 Exception reporting

There should be a documented agreement between the owner and the RVRC detailing the requirement for handling individual CCTV system exceptions, e.g. whether a user should be notified. This agreement might involve different criteria for lighting failure, video failure, detector failure, tamper, communication failure, etc. Some CCTV system exceptions can result in the RVRC operator reviewing images from site.

The owner might have other contractual obligations, e.g. insurers, third-party occupiers, who might be affected and they should be made fully aware of the agreement.

8 RVRC operator procedures

8.1 General

Information should be readily available to the RVRC operator to ensure that there is a clear understanding of the layout of the site and the areas to be viewed when a detector initiates an activation.

Stored images of the intended fields of view of all cameras on the CCTV system, and site plans should be made available to the RVRC operator in order to provide evidence if a potential intruder misaligns the camera(s).

8.2 Entry/exit and other delayed procedures

Where procedures involve a delay between an event being detected and activation occurring the RVRC operator should have direct access to at least a single image, or preferably an ongoing sequence (e.g. images of the initial entry and not just the point-at which the event was elevated to an activation), from the initiation of the first event. These procedures should be agreed and documented between the RVRC and owner.

The RVRC operator should have the means to view the image or images of the initial entry, and not just the point at which the event became established as activation.

NOTE: An example of this would be where a timed entry procedure exists. Some time might elapse between a person passing through the area and the point at which the event escalates from an entry procedure to activation.

8.3 Equipment failure

In the event of loss of monitoring facilities at the RVRC, data from affected CCTV systems should be routed to another RVRC. If this is not achieved in less than 15 h then CCTV systems should be monitored locally at the site.

8.4 Management and operation of the RVRC

The management and operation of the RVRC should reflect the recommendations set down in BS 7958 in so far as they reasonably apply to this code of practice.

9 RVRC specifications

9.1 Construction and facilities

As a minimum, the construction and facilities of the RVRC should be in accordance with the recommendations of BS 5979, Category II.

9.2 Logging and recording

The following should be logged or recorded at the RVRC:

a) Date and time of all activations;
b) Transmitted images (see 9.4);
c) Transmitted audio (see 9.5);
d) Telephone messages, particularly in relation to all owner and user requests;
e) Reports of incidents to the owner and emergency services.

9.3 Support equipment

Support equipment should include the following.

a) An RVRC logging system, recording all incidents and RVRC operator actions in response to the incident.

b) An inbound and outbound call logging and recording system, with indexing to the recordings of all telephone calls.

c) Sufficient RVRC operator terminals to meet the normal anticipated levels of activation in any given time period.

NOTE: This may vary depending on the time period, but there should be at least two RVRC operators on duty at all times.

d) Sufficient surplus equipment to ensure the capability to make and receive video and audio calls, and of controlling remote site CCTV systems even in the event of primary equipment failure.

e) Adequate facilities to queue the anticipated maximum number of activations above normal limits.

f) Sufficient incoming telephone lines and receiving equipment to ensure that there is adequate capacity to receive activations from all possible sites with at least one free line at all times, even when the anticipated maximum numbers of activations are being queued.

The site plan should show sufficient information (on-line if possible) to enable RVRC operators to describe accurately the nature of incidents as they occur.

9.4 Picture quality

Picture quality should be at least sufficient to enable an RVRC operator to determine the nature and detail of a viewed event as described in 4.2.1c).

9.5 Transmitted audio

Transmitted audio quality should be, as a minimum, clearly audible to the operator without undue distortion.

10 RVRC procedures

10.1 Site documentation: the connection form

The RVRC should obtain the following information at least 24 h before the CCTV system is commissioned:

a) Site address;
b) Installer details;
c) Site plan (see **8.1**);
d) Operational schedule (set/unset times, etc.);
e) Response plan (see **7.2**);
f) User contact details/emergency services details;
g) Associated intruder alarm system information;
h) Inventory of CCTV equipment installed;
i) Fault reporting procedure (see **5.6**).

10.2 Non-image records and event logs at the RVRC

Any non-image records and event logs at the RVRC should be maintained for a minimum of six months and should include the following:

a) Time of any communication from a site;
b) Time and date when an RVRC operator is allocated to a workstation and the identity of the RVRC operator;
c) Any RVRC operator actions as a result of an incident reported from site;
d) Time at which the RVRC operator closes down the session, in addition to any cause code recorded;
e) Any CCTV system exceptions received from remote sites;
f) Any CCTV system exceptions or failures within the receiving equipment and workstations;
g) Any special owner instructions, the time and date they are received, and the time and date at which they are implemented;
h) Times at which an RVRC operator initiates and closes a routine patrol of the site.

10.3 Storage of images received

All images received at the RVRC should be stored on a suitable medium, such as videotape or CD-ROM. Procedures should exist for indexing and accessing a particular incident.

The retention period should be assessed and agreed with the owner.

10.4 Images for evidential purposes

All images should have an audit trail to ensure the recorded material maintains total integrity and continuity at all times and to enable any images to be used for evidential purposes. If the recorded data is held on an electronic document management system, the system should conform to PD 0008:2004.

10.5 RVRC operator actions

RVRC operators should follow documented procedures (see **7.2**) when handling activations. They should be trained in the possible requirement for producing evidential images and the actions needed to produce these. Any information recorded from an activation should include anything of note that could be useful for investigative and evidential purposes.

10.6 Image quality check

If during the handling of an activation the quality of an image is identified as poor, a fixed format notice should be issued by the RVRC to the owner advising of the nature of the problem and requesting that remedial action be taken.

10.7 Critical data omissions

If, during the handling of an activation, critical data required to complete the response plan effectively is unavailable or inaccurate (e.g. a user who is no longer valid), a fixed format notification should be issued by the RVRC to the owner requesting the supply of the missing data.

11 Activation management

11.1 Classification of activations

A method of classifying activations should be adopted by the RVRC. As a minimum this classification system should distinguish between alerts and incidents. In addition, activity per detector/camera combination should be recorded and classified according to cause to enable the CCTV system to be managed effectively with regard to CCTV system faults or deficiencies.

11.2 Multiple false activations

In the event of an agreed number of false activations occurring from the same device, within a time period agreed with the owner, for no identifiable reason, or for a reason determined to be the environment, animal nuisance or detectors looking beyond the bounded property, the RVRC should disable the specified detector(s). In this situation the RVRC should notify the owner, on the basis agreed within the response plan (see **7.2**), of the action to be undertaken and require the owner to have false alarm causes investigated and eliminated before the detector is re-enabled.

12 Service levels

12.1 General

The RVRC should conform to BS 5979 and the recommendations given in **12.2**, **12.3** and **12.4** in respect of operations.

12.2 Activation response time

The evaluation of images received at the RVRC as a result of each initial activation should commence within 90 s of their arrival for 80 % of initial activations and 180 s of their arrival for 98.5 % of initial activations.

12.3 Local CCTV system fault reporting

The RVRC should notify the owner of any faults found on the CCTV the next working day.

12.4 Incident reporting

Incidents occurring during the period when the CCTV system is set should be reported to the owner's nominated contact within 4 h of the start of the next working day or sooner if so required by the owner .

13 General

13.1 Equipment maintenance

Before a site is accepted for monitoring, the owner should arrange for the CCTV system to be maintained in accordance with the manufacturer's recommendations for the duration of the monitoring service. This should include the provision of routine maintenance at agreed intervals.

Changes to the CCTV system and transmission equipment configuration should be controlled through the RVRC in order to avoid a breach of security.

Criteria for attendance/repair of CCTV systems should be agreed between the owner and maintenance provider and communicated to the RVRC.

Once a repair has been completed, the RVRC should undertake a full evaluation of the CCTV system to confirm that it is fully operational and meets the performance requirements in accordance with **4.4**. The owner and/or maintenance provider should be advised immediately if the CCTV system is not fully operational.

At the time of a routine maintenance visit any CCTV system specification documentation and operational logs should be reviewed with the RVRC, to determine if any deterioration in CCTV system operation has occurred. All maintenance visits should be approved by the RVRC.

13.2 Personnel screening

Any person with access to the RVRC or its records and personnel at installing and maintaining firms should be screened in accordance with the requirements of BS 7858 as a minimum.

Annex A
(Informative)
Setting procedure in the active state

Procedures should exist detailing what actions are to be taken in the event of the setting procedure being completed when a detector is in an active state. These can include the following.

a) The inability to complete the setting procedure until the faulty detector problem is solved.

b) Automatic omission of the faulty detector until the CCTV system is reset. This should be logged and reported to the RVRC as an exception.

c) An activation immediately associated with a faulty detector. This condition would then be processed in accordance with the owner's procedure, with subsequent notification to the owner.

Bibliography

Standards publications

BS EN 50130-5:1999, *Alarm systems — Part 5: Environmental test methods.*

Further reading

BS EN 50130-4:1996, *Alarm systems — Part 4: Electromagnetic compatibility — Product family standard: Immunity requirements for components of fire, intruder and social alarm systems.*

BS EN 50132-2-1:1998, *Alarm systems — CCTV surveillance systems for use in security applications — Part 2-1: Black and white cameras.*

BS EN 50132-4-1:2001, *Alarm systems — CCTV surveillance systems for use in security applications — Part 4-1: Black and white monitors.*

BS EN 50132-5:2001, *Alarm systems — CCTV surveillance systems for use in security applications — Part 5: Video transmission.*

