BRITISH STANDARD

Code of practice for digital CCTV recording systems for the purpose of image export to be used as evidence

ICS 13.310

Publishing and copyright information

ISBN 978 0 580 57706 2

The following BSI references relate to the work on this standard:
Committee reference GW/1/10
Draft for comment 07/30156322 DC

Publication history

First published November 2007

Amendments issued since publication

Amd. no.	Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 10, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI and came into effect on 30 November 2007. It was prepared by Subcommittee GW/1/10, *Closed circuit television (CCTV)*, under the authority of Technical Committee GW/1, *Electronic security systems*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions in this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

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

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

Introduction

The demand for this British Standard is based on the change in technology away from the video cassette recorder (VCR) medium. In many cases this has been replaced by digital CCTV recording system (DCRS) technology with the result that specifiers and end users require guidance.

The rapid change towards DCRS technology is based on improved reliability, ease of use, ability to search for specific recorded data quickly, no need for daily attention, in particular, relating to the constant requirement to change video tapes and the retention thereof. This British Standard does not attempt to establish a preference for the digital recording medium to be adopted but does recommend the areas that should be considered when adopting DCRS technology.

The handling of evidential digital images within the Criminal Justice System is covered by the Digital Imaging Procedure [1], which states that digital recording technology provides no original that could be produced in evidence. All that is available for use as evidence is a copy of the first, probably temporary, recording in memory, and this will be admissible as evidence.

Its weight and admissibility as evidence can be influenced by:

a) Whether the image's audit trail from the digital recording device to the court is robust.

b) Whether the integrity of the image can be proven.

It is at the court's discretion whether the evidence is deemed admissible.

NOTE 1 Attention is drawn to the requirements of the Data Protection Act 1998 (DPA) [2].

NOTE 2 For further information refer to the CCTV Code of Practice published by the Information Commissioner's Office [3].

1 Scope

This British Standard gives recommendations for the specification, selection, installation and operation of digital CCTV recording systems (DCRS), for the purpose of generating CCTV images to be used as evidence in a court of law.

This document is aimed at assisting specifiers, installers, users, insurance companies, police authorities and purchasing organizations. Particular emphasis is placed on the following key areas.

a) Fitness for purpose of recorded images.

b) Audit trail.

c) Image integrity.

d) Time and date integrity.

e) Storage.

f) Export of images.

g) Replay of exported images.

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 8418, *Installation and remote monitoring of detector activated CCTV systems – Code of practice*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1 audit trail

data which allows the reconstruction of a previous activity, in its correct chronological place, or which enables the attributes of a change (such as date/time, operator) to be recorded

NOTE The audit trail can be generated by a computer system or manually.

3.1.2 authentication

evidence that the original recording has not been altered since first writing to storage medium and that the master copy is an exact copy of the original recorded digital images

3.1.3 CCTV camera

unit containing an imaging device producing a video or digital signal from an optical image

3.1.4 CCTV system

system consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes, which might be necessary for the surveillance of a defined area of interest

3.1.5 checksum

value, assigned by an algorithm to an image or metadata, which will change if the data is altered

3.1.6 compression

algorithmic means of reducing the amount of data required to represent video images

3.1.7 data encryption

method of scrambling the image data in such a way that a reverse algorithm is needed to reconstruct it

3.1.8 digital CCTV recording system (DCRS)

system that stores images, originating from either analogue or digital capture devices, in digital format

NOTE Examples include DVRs and Network Video Recorders.

3.1.9 digital image
representation of a scene as a finite set of digital values

3.1.10 digital watermarking
addition of verification information to images and associated data

NOTE Visible digital watermarking changes the original image to incorporate information. If the image file is altered, the watermark is also changed. Invisible watermarking can provide image authentication checks without visibly changing the original image.

3.1.11 event
video and/or other data recorded on the DCRS that could be of interest

3.1.12 event log
ordered list of events that have been recorded on the DCRS, and/or operations that have been applied to the DCRS

3.1.13 exact copy
bit-for-bit replication of digital images

3.1.14 export
transfer and/or copying of data from the original stored location to an alternative storage location

3.1.15 fit for purpose
meets defined operational requirements for the recording and replaying of images originating from each individual camera

3.1.16 image clarity
degree of visibility of relevant information in an image

NOTE Relevant information is that which is defined in BS EN 50132-7 and the HOSDB CCTV operational requirements manual [4].

3.1.17 master copy
exported exact copy made from the original recording and labelled as the master copy

3.1.18 metadata
data used as a supplement to other data

NOTE For example, the time and date of when an image is recorded.

3.1.19 original recording
first instance of digital images recorded to the DCRS

3.1.20 removable hard disk drive
hard disk drive designed to be removed without disassembly of the DCRS

3.1.21 replay
viewing of previously recorded images from the DCRS

3.1.22 retention period
length of time for which digital images are to be held on the DCRS to meet the purpose of the application

3.1.23 storage
media on which digital images are stored

NOTE Examples include hard disk drive, tape, CD, DVD, flash memory.

3.2 Abbreviations

CCTV	closed circuit television
CD	compact disc
CD-R	compact disc – recordable
DCRS	digital CCTV recording system
DVD	digital versatile disk
DVR	digital video recorder
RAID	redundant array of independent disks
SAN	storage area network
VCR	video cassette recorder

4 General recommendations

NOTE 1 Before evaluating the clarity of the recorded images, ensure that the purpose of the system is defined in the Operational Requirement; this should state what the customer expects the digital CCTV recording system (DCRS) to do. Factors affecting the clarity of images the DCRS records include:

a) subject size within the field of view of the camera;

b) lighting of subjects within field of view;

c) camera and lens specification;

d) transmission medium;

e) system maintenance.

The installation of the CCTV system should be in accordance with BS EN 50132-7.

NOTE 2 The requirements of prEN 50132-1 should also be considered.

If appropriate, the installation of the CCTV system should be in accordance with BS 8418.

NOTE 3 Attention is drawn to the HOSDB CCTV operational requirements manual [4].

NOTE 4 Some CCTV systems are capable of recording audio as well as images. Where this is the case the audio should be correctly synchronized to the images. The audio data should be treated in the same manner as image data with regard to its integrity.

5 Fitness for purpose of recorded images

The DCRS should be capable of meeting the Operational Requirement arising from each camera. It should be verified that the DCRS meets the required performance criteria in the following areas:

a) Level of recorded digital image compression per camera.

NOTE Too much compression will result in loss of detail due to blurring and/or blocking depending on the degree of compression applied. Compression is typically applied to reduce the amount of space required to store the digital images. Less compression is better for image clarity.

b) Image per second record rate per camera.

NOTE Low image per second record rates might miss certain activity. However, higher image per second record rates will require more data to be stored.

c) Recorded digital image resolution.

NOTE An insufficient resolution setting will result in loss of detail/ clarity of received images. Resolution is typically reduced to minimize the amount of space required to store the digital images. High resolution recording equivalent to the minimum resolution of the capture device is better for image clarity.

NOTE Each of these parameters might be adjustable to reflect changes in operating conditions such as differentiation between event/non-event.

6 Audit trail

As the methods of operation and management of the DCRS can affect the integrity of evidence, actions and events for the DCRS should be logged.

The information in an audit trail should be retained for at least 6 months.

As a minimum the following events should be logged in the audit trail.

a) User logon and logoff.
   1) ID of the user.
   2) The time and date of the event.

b) Time and date changes (automated and manual).
   1) System time and date at the point of change.
   2) New time and date immediately after the point of change.
   3) ID of user making the change.

c) When recording is started or stopped manually.
   1) Time and date the recording is started or stopped.
   2) ID of user starting or stopping recording.

d) Any enhancement applied to images.
   1) Unique identifier of enhanced image.
   2) Time and date of image enhancement.
   3) ID of user enhancing the image.
   4) Details of enhancement(s).

   NOTE If multiple enhancements were applied, the order in which they were applied should be logged.

e) Exporting of images.
   1) Unique identifier of exported image.

   NOTE For example, the time and date the exported image was recorded and the camera label from which it originated.

   2) Time and date of image export.
   3) ID of user exporting the image.

f) Images that have been manually tagged or untagged to prevent or permit overwriting.

   1) Unique identifier of tagged/untagged image.

   2) ID of user tagging/untagging the image.

g) Manual deletion of images.

   1) Unique identifier of deleted image.

      NOTE For example, the time and date the deleted image was recorded and the camera label from which it originated.

   2) Time and date of image deletion.

   3) ID of user deleting the image.

h) What (if any) removable medium is used for primary storage.

   NOTE An additional audit trail might need to be kept to record the movement and/or storage of removable media to ensure the evidential integrity of stored data.

NOTE For further information refer to BIP 0008-1.

7 Image integrity

The integrity of images on the DCRS should be maintained by preventing unauthorized access. Protection methods should not prevent images being provided to authorized third parties such as the police.

NOTE 1 Control of access to images can be achieved by physical and/or electronic means (e.g. passwords and data encryption).

It should be possible for an authorized user to export the audit trail, event log and user-definable system settings relevant to the images.

It should be ensured that the DCRS manufacturer is capable of providing a statement that can be used in support of any image authentication method employed. If such a method is used, it should not interfere with processing carried out by authorized third parties such as the police.

NOTE 2 Image authentication methods aim to detect whether tampering has taken place. Such techniques can be included in the functionality of DCRS. The most commonly employed methods at time of writing are the use of checksums and digital watermarking.

8 Time and date integrity

As part of each image's metadata, the time and date of recording should be logged.

NOTE In terms of evidence the time and date information of the image is often key.

The precision of the time recorded in the metadata should be appropriate to the image per second record rate.

The user should be made aware of the need to regularly check that the time and date (including time zones).

Daylight saving time changes should be accommodated by the DCRS.

When a DCRS has multiple recording components it should be possible to synchronize time and date information between them either manually or automatically.

9 Storage

9.1 Storage capacity

Adequate storage capacity should be available in order to meet the predetermined Operational Requirement for the following.

a) Recording retention period.

b) Image per second rate.

c) Resolution/compression of image.

Allowance should also be made for the predicted activity levels within each camera's field of view. Capacity for the storage of supporting audit trail and metadata should also be taken into account.

NOTE 1 When determining the retention period the Operational Requirement should allow for event discovery through to replay/export by all interested parties.

NOTE 2 The required clarity of images should not be compromised to increase storage period.

It should be possible for the user to electronically protect specific images to prevent them being overwritten before viewing or exporting. Expected overall record durations should take account of the amount of storage space likely to be used by protected images.

NOTE 3 Many DCRSs overwrite the oldest images when the storage capacity becomes full regardless of the intended retention period.

9.2 Storage functionality

In order to assist the user in management of the system the DCRS should indicate:

a) how many days and hours of recording the system has stored or the time of the earliest recording on the system; and

b) an estimated retention period based on the changing of settings.

9.3 Removable storage media

If the system uses removable media (e.g. removable hard disk drives) for primary storage of all video and associated metadata then the following should be adhered to.

- If the medium is replaced with a blank, then the DCRS software/configuration should be capable of being restored by the user.
- The system should operate fully after the replacement medium is installed, such that the system will have the full storage capacity available without needing the intervention of a technician.

NOTE An additional audit trail might need to be kept to record the movement and/or storage of removable media to ensure the evidential integrity of stored data.

10 Export of images

10.1 Image enhancements

If the DCRS provides enhancement tools such as image sharpening, brightening or zooming in on a particular part of the image then any applied enhancements should not change the original recording. If an enhanced image is exported, an audit trail documenting these changes should exist as defined within Clause **6**.

10.2 Image export

To facilitate replay and export the following should be adhered to.

a) A simple user guide should be available locally for reference by a trained operator.

b) The facility should be provided for the export of images from selected cameras within user-defined time periods.

c) Simultaneous export and recording should be possible without affecting the performance of the system except on systems that require removal of the primary storage media for export purposes.

d) The export method of the DCRS should be appropriate to the capacity of the system and its expected use.

NOTE 1 If the export method is not appropriate there is a risk that if the police require video evidence they may need to remove the DCRS, for example if 1 terabyte of data is required it is not practical to export this via a CD writer.

NOTE 2 A number of methods exist for exporting images in native format from a DCRS, for example:

a) images are copied to removable digital media such as a floppy disk, DAT tape, flash card, CD-R or DVD.

b) the removable hard disk, which holds the images, is physically removed from the DCRS.

c) images are exported via a port, such as USB, SCSI, SATA, FireWire or networking.

e) Documentation should be supplied to the user regarding both the retention period of the system and the approximate times to export each of the following.

1) Up to 15 minutes of recorded data per camera.

2) Up to 24 hours of recorded data per camera.

3) All of the data on the system.

f) The system should display an estimated time to complete the export of the requested data.

g) The software needed to replay the images should be included on the media used for export, otherwise viewing by authorized third parties can be hindered.

h) The system should not apply any format conversion or further compression to the exported images, as this can reduce the usefulness of the content.

i) Any original metadata and/or authentication signatures should be exported with the images.

11 Replay of exported images

Exported images should be capable of being replayed on a computer via the exported software. This software should:

a) have variable speed control including frame-by-frame forward and reverse viewing;

b) display single and multiple cameras and maintain aspect ratio i.e. the same relative height and width;

c) display a single camera at the maximum recorded resolution;

d) permit the recordings from each camera to be searched by time and date;

e) allow printing and/or saving (e.g. bitmap or JPEG) of still images with time and date of recording;

f) allow for time synchronized multi-screen replay;

g) allow for time synchronized switching between cameras upon replay;

h) allow replay of associated audio and other metadata;

i) be able to export the image sequences in a standard format at an equivalent quality to the original and still displaying time and date information (e.g. MPEG-2, MPEG-4 or MJPEG);

j) clearly show the time and date, and any other information associated with each displayed image, without obscuring the image.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

prEN 50132-1, *Alarm systems – CCTV surveillance systems for use in security applications – Part 1: System requirements*[1)]

BIP 0008-1, *Code of practice of legal admissibility and evidential weight of information stored electronically*

Other publications

[1] HOME OFFICE SCIENTIFIC DEVELOPMENT BRANCH. *Digital imaging procedure*. Publication 58/07, Version 2.0, November 2007.[2)]

[2] GREAT BRITAIN. Data Protection Act 1998. London: The Stationery Office.

[3] THE INFORMATION COMMISSIONER'S OFFICE. *CCTV code of practice*. July 2000.[3)]

[4] HOME OFFICE SCIENTIFIC DEVELOPMENT BRANCH. *CCTV operational requirements manual – Is your CCTV system fit for purpose?* Publication 55/06, Version 4, 2007. ISBN 978 1 84726 138 0.[2)]

Further reading

HOME OFFICE/ASSOCIATION OF CHIEF POLICE OFFICERS (ACPO). *UK Police requirements for digital CCTV systems*. Publication 09/05, February 2005. [2)]

1) In preparation.

2) Available from Home Office Scientific Development Branch, Sandridge, St Albans, Hertfordshire, AL4 9HQ and http://scienceandresearch.homeoffice.gov.uk/hosdb/publications/.

3) Available from The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF and http://www.ico.gov.uk/tools_and_resources/document_library.aspx.

This page deliberately left blank

BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards 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 this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111.
Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI 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@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

389 Chiswick High Road
London
W4 4AL