CCTV Operational Requirements Manual

Is your CCTV system fit for purpose?

N Cohen
J Gattuso
K MacLennan-Brown
# Contents

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
1 Foreword

The use of CCTV has become increasingly widespread throughout the UK over recent years. Originally deployed for protecting large establishments and monitoring city centres, CCTV systems are now installed routinely within shops, schools, and even individual vehicles on the public transport network. Additionally, the market has undergone a rapid transition from analogue to digital recording technology, which has had a significant impact on the design and functionality of CCTV systems.

These developments mean that an update is now required to the original CCTV Operational Requirements Manual, published by HOSDB (then PSDB) in 1994.

The focus of the document remains the same: to provide clear guidance to non-technical users wishing to buy a CCTV system that is fit for purpose. However, the new manual considers the additional issues of recorded image quality and data archiving that are essential parts of any digital CCTV system, but are often neglected when writing the specification.

Analogue CCTV recording systems were relatively simple to design as they relied mainly on the use of VHS tapes to capture the images. Digital recording systems, by contrast, are much more complex to specify. They record onto a hard drive, which can only store a limited amount of video; when it is full the oldest material will be overwritten with new. Therefore when specifying a system thought must be given to the capacity of the hard drive, the provision of a suitable method to create a permanent record of any key incidents (e.g. DVD writer) and the use of compression (which will affect the recorded image quality). Many of these issues are inter-related; thus improved recorded picture quality and higher frame rate may come at the expense of a reduced retention time on the system. One of the key aims of this publication is to provide some guidance on these complex factors.

Work is ongoing at HOSDB to investigate these issues in more detail and also to devise a means of assessing the image quality of digitally recorded CCTV. The results of this research will be published in future updates of this manual.
2 Introduction

There are four key stages when planning the installation of a CCTV system, summarised in figure 1. The first step is to define the problem, be it a security threat, public safety issue or other vulnerability. This is known as the Level 1 operational requirement (OR). Consider at this point whether the installation of a CCTV system is the most appropriate response to these concerns, or if there are alternative options.

Having developed a clear picture of the concerns that need to be addressed, attention can be turned to the specific issues relating to the CCTV system itself. This is known as the Level 2 operational requirement. Development of a level 2 OR helps the CCTV user/manager to:

- Further define the areas of concern
- Understand operational issues and responses
- Decide on the most suitable system requirements
- Identify any managerial implications

An OR checklist is provided in section 4 to guide the CCTV user through these issues and provide a structured series of questions to answer, that will ultimately form a clear operational requirement that can be passed to a manufacturer or supplier.

The third step is where a more detailed technical specification for the CCTV system is developed. Further information on the system design is provided in section 5. For example there is information on camera selection, the effects of compression on image quality, and guidance on how to estimate the storage capacity that should be included with the system.

The final stage in the process occurs when the system is installed and commissioned. At this point it is important to check that it meets the operational requirements and that the performance is fit for purpose.

![Figure 1: Key stages in specifying a CCTV system](image-url)
3 Level 1 Operational Requirement

3.1 Introduction

Before focusing on the requirement for the CCTV system itself, some thought should be given to the nature of the problem or threat that needs to be resolved. This high-level statement of the overall security need is known as the Level 1 Operational Requirement. A simple Level 1 OR checklist is shown in figure 2, and is accompanied by a set of explanatory notes. Completion of a Level 1 OR checklist should help to ensure that the strategic issues are analysed first and that the most appropriate solution is arrived at, even if this requires options other than CCTV to be considered.

3.2 Level 1 OR Checklist

1 Site plan
The first task when constructing an OR is to draw a site plan on which to mark the areas of concern. The more detail that can be included in this plan the better as this will aid in the placing of lights and cameras especially with regard to fields of view and potential environmental problems such as low sun or foliage. An example site plan is shown in figure 3, for large commercial premises with an attached car park.
Figure 3: Example site plan with threats marked
Statement of problem
What are the problems / threats/ security issues to be resolved?

The next step is to define the problems that affect the site. Some of these may be general threats but some may be specific to a given location. Typical threats or risks that might be identified include:

- Crowd control
- Theft
- Unauthorised entry
- Public safety

These potential problems and/or threats can be marked on the site plan. This can then be used to visualise the scale of the problem and the level of cover required. Some areas such as checkouts and entrances/exits may need cover for different activities i.e. to monitor flow of people and to identify people in the event of a theft or similar.

Stakeholders
Who are the stakeholders?

If the installation is likely to be complex and involve several different stakeholders, then they should all be consulted at this stage in the process and asked to identify their requirements on the site plan.

Risk Assessment
What is the realistic likelihood of the activity happening?

- Low / medium / high

What would be the consequences if the activity was not monitored and/or recorded?

- Minor / moderate / severe
- For example, will the activity result in financial loss or compromise the safety of your personnel or the public?

Can you prioritise the activities you wish to monitor?

Could you use alternative (or more cost-effective) methods to tackle the activity such as better lighting, fences or intruder alarms?

Is the activity likely to be a short or long term issue?

Success Criteria
After detecting an activity, what is a successful outcome?

- Prevention of theft of damage
- Identification of intruder
• Improvement in traffic flow at the checkout
• Deterring an activity

The success will be determined by a combination of how effectively the system performs and how well it meets the operational requirements.

How often will you expect a successful outcome?
(i.e. How effectively / reliably will the task have to be done?)

• All of the time
• On most occasions
• Always during the day, but only occasionally after hours

Determine the most effective solution

Once the problem areas and potential threats have been marked on the plan, then an assessment can be made of the most effective solutions. CCTV is likely to be only one of a range of possible options and should be considered in the context of a wider security/safety audit, alongside other measures such as:

• Lighting
• Physical protection / barriers
• Proximity alarms / intruder detection systems
• Improved site design / threat removal

There are, however, several scenarios where a correctly designed CCTV system may be of benefit. These usually fall into one of three broad categories:

• Safety / security
• Deterrence
• Crime investigation

Of these, it is often the requirement for post event crime investigation that is not given adequate consideration at the point when the CCTV system is designed and specified. This may only become apparent at a later time, when for instance the video is required for a police investigation. It may then be discovered that the recorded images are of a poor quality and not fit for purpose. Another common failing is that inadequate facilities are provided for the replay, archiving and sharing of the recordings. Awareness of these issues is of particular importance following the widespread transition from analogue to digital recording technology.

Once a decision has been made to install a CCTV system, a full Level 2 operational requirement should be developed, as described in the next section.
4 Level 2 Operational Requirement

4.1 Introduction

The purpose of this section is to provide a guide through the process from the decision “I need CCTV” to the commissioning of an effective system. The first and most important question to be addressed with any CCTV system is “What do I need to see?” closely followed by “Why do I need to see it?”

Most camera systems are designed to observe human activity. The application, however, can range from crowd control / public safety (where the movement of large numbers of people needs to be monitored over a wide area) to access control (where close-up, high quality imagery is required to enable individuals to be identified). The choice of CCTV camera in particular will depend on the nature of the activity to be observed.

To simplify the situation and provide guidance to a system specifier, four general observation categories have been defined, which are based on the relative size that a person appears on screen (figure 4). As part of the OR development, the user will be asked to decide which of these four categories best reflects the type of activity being observed. The CCTV installer will then be able to fit a suitable camera to meet the requirement.

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Detect</th>
<th>Recognise</th>
<th>Identify</th>
</tr>
</thead>
<tbody>
<tr>
<td>5%</td>
<td>10%</td>
<td>50%</td>
<td>120%</td>
</tr>
</tbody>
</table>

Figure 4: Height based ‘levels of detail’

**Monitor and Control:** A figure occupies at least 5% of the screen height and the scene portrayed is not unduly cluttered. From this level of detail an observer should be able to monitor the number, direction and speed of movement of people, providing their presence is known to him; i.e. they do not have to be searched for.

**Detect:** The figure now occupies at least 10% of the available screen height. After an alert an observer would be able to search the display screens and ascertain with a high degree of certainty whether or not a person is present.

**Recognise:** When the figure occupies at least 50% of screen height viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before.

**Identify:** With the figure now occupying at least 120% of the screen height, picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.
The purpose of these categories is to suggest appropriate image sizes to aim towards when specifying a system to meet a particular requirement, rather than to define a minimum standard. It does not necessarily follow that it will be impossible to recognise or identify an individual if the image size is smaller than the 50% or 120% figures suggested. Equally, there is no guarantee that individuals will be identifiable simply because they occupy >120% of the screen. Other factors, such as lighting and angle of view will also have an influence.

It should also be noted at this point that these guidelines were originally set up using a fully analogue PAL system and therefore may not transfer faultlessly into the digital domain. For most systems the above categorisation will be valid when considering the live picture view from a standard PAL camera displayed on a PAL monitor, for which the resolution is a fixed 576 lines. However, the situation will be more complex if the images are captured digitally and displayed on a computer monitor, as the resolution is no longer fixed. For this scenario it may be more appropriate to consider the number of ‘pixels on target’ when attempting to categorise the level of detail required in the image.

The situation is further complicated when considering the recorded imagery, as the recording process may have utilised image compression technology, which could result in a reduction in picture quality compared to the live view (see section 5.5 for further information). Put simply, this means that a figure that occupies 50% of the screen height and can be recognised from the live view may not be recognisable in the recorded view, as the compression process has led to a loss in picture detail. For this reason it is vital to inspect the recorded picture quality as well as the live view when purchasing a CCTV system. Work is currently being carried out by HOSDB to investigate the relevance of the chart in figure 4 to digital systems, and further information will be provided in future updates.

### 4.2 Level 2 OR Checklist for CCTV

The checklist (figure 5) summarises, in a step-by-step manner, the issues that should be considered when specifying a CCTV system. Each numbered box on the chart has a corresponding set of explanatory notes. Further details on the more technical aspects of a CCTV system such as cameras and lighting can be found in section 5.

The first set of issues (1-4) require you to refer back to the site plan and consider each marked threat / vulnerability in more detail. Parts 1-4 should be answered separately for every threat identified on the plan. However once this has been done the remaining sections of the chart should only need working through once.

Once completed, this checklist will form a comprehensive Operational Requirement that can be given to the contractor / supplier to help them to design a CCTV system that is fit for purpose.

The checklist can also be used as a basis for creating an operational code of practice for the CCTV facility, which may be required for a large installation and should also assist with defining the training needs of the operators.
Figure 5: Level 2 OR checklist for CCTV

Define the Problem*

1. Location
   - Perimeter
   - Car Park
   - Office Reception
   - Checkout Tills

2. Activity
   - Theft
   - Vandalism
   - Public Safety

3. Purpose of Observation
   - Identify, Recognise
   - Monitor, Detect
   - Read Number Plate

4. Target Speed
   - Walking
   - Stationary
   - Variable

Operational Issues (Live Viewing)

5. Who Monitors
   - Trained Staff
   - Casual Staff

6. When Monitored
   - 24/7
   - Office Hours
   - Occasional

7. Where Monitored
   - Locally
   - Remotely
   - Mobile platform

8. Response
   - Contact Decision Maker
   - Emergency Services
   - Continue Monitoring

System Requirements

9. Alert Function
   - Visual
   - Audible
   - Integrated System

10. Displays
    - Type
    - Number Size

11. Recording
    - Retention Time
    - Image Quality
    - Frame Rate
    - Metadata

12. Export / Archive
    - Video Export Facilities
    - 3rd Party Access
    - Replay Software

Management Issues

13. Constraints
    - Regulation
    - Licensing Bodies

14. Legal Issues
    - Data Protection Act
    - Freedom of Information Act

15. Maintenance
    - Cleaning, Repairs
    - Upgrades, Warranties
    - Product Life Cycle

16. Resources
    - Staff, Training
    - Accommodation
    - Consumables

* Repeat for each problem identified in plan
4.2.1 Define the Problem

The purpose of this section is to collect the information that the system provider will need in order to select suitable cameras, and to position them appropriately to capture the scene in the required level of detail. The general threats should already have been defined in the Level 1 Operational Requirement. These threats now need to be considered in more detail, on a location-by-location basis; therefore this section should be worked through separately for each location.

Location

*Where on your premises do you wish to monitor?*

Divide the site plan into specific zones or locations. A location may either be an area where a particular threat exists, or it may be a strategic location away from the threat, but where monitoring would be appropriate because high quality images of the offender could be obtained, such as a pinch point or doorway for access and egress. Consider whether there is a need to monitor throughout the site, in order to track individuals, and be aware of the location of any blind spots.

It is also possible that two or more separate activities require monitoring in a single area such as a car park, a warehouse or entrance. Treat each scenario separately when determining your operational requirements.

In a car park for instance you may have two locations; one where vehicles are monitored as they enter and leave, to control access and obtain vehicle registration information, and another where they are in the parking bays.

Activity

*What potential threat or activity do you wish to monitor?*

Types of activity that are commonly monitored are:

- Theft / shoplifting
- Public safety
- Flow of customers / crowds
- Unauthorised entry
- Anti-social behaviour / vandalism

Obvious examples include theft from vehicles in the car park or identification of people as they approach the reception desk at the entrance to a building. Other less obvious examples are to monitor the queues in the checkout area or identify people fly tipping on your premises.

A combination of activities may require monitoring. For example the walkway in a shopping centre may need observation to monitor crowd flow for public safety and to detect pick-pocketing or anti-social behaviour.
3 Purpose of the observation

How much detail do you need in the picture?

Consider which of the four ‘levels of detail’ described in section 4.1 is most appropriate to your requirement.

You may wish to:

- **Monitor** a large area
- **Detect** individuals approaching a building
- **Recognise** known individuals at an entrance
- Obtain images that would enable you (or the police) to **identify** an unfamiliar individual

A typical fixed camera can be specified to cover a narrow field of view with a high level of detail (for recognition / identification purposes), or a wide field of view at a lower level of detail (for monitoring / detection), but generally not both. Thus it is important to consider carefully which of these requirements is the more appropriate for each location.

There may be more than one purpose to the observation. For example, there may be a requirement to detect thefts from vehicles in a car park, but also to identify the offenders as they leave. However the image clarity required for identifying those people would need to be greater than that required to detect an action such as breaking into a vehicle.

4 Target speed

How fast will the target be moving?

This information is important to enable a suitable frame-rate to be set for recording the event.

The event may be monitored in real time, but most CCTV systems record in ‘time-lapse’ mode (to reduce the amount of storage required), with only a certain number of frames per second (fps) being stored. A low frame rate may be adequate if monitoring a corridor where little activity takes place (e.g. 1 fps), but a higher frame rate will be necessary if monitoring a busy area or a doorway through which people pass quickly (greater than 5 fps).

4.2.2 Operational Issues

This covers the day-to-day operation of the system; in other words who monitors the system, where they are monitoring and how they should respond in the event of an activity.

Most large CCTV installations will have a staffed control room from which events are monitored. Some smaller CCTV installations, however, are designed primarily to record video, which can be reviewed in the event of an
incident. A screen will usually be provided as part of the system, on which the live view can be displayed, but this may not be monitored regularly by the staff. The following section may therefore not be applicable for all systems, although as part of the OR development process, thought should nevertheless be given to whether occasional live monitoring may be required.

Who monitors

Who will be responsible for monitoring the CCTV screens?

The most common options are:

**Dedicated** personnel whose sole responsibility is to operate the system and respond to events.

**Casual** operation by personnel, as a secondary function to their main role, such as a receptionist.

Some systems are designed only for recording and post event investigation in which case **nobody** would be required to monitor the activities live.

Additionally consider whether personnel should receive training and if so to what level. Most public space CCTV operators must now be licensed by the SIA (Security Industry Authority), and to obtain a license must show they have been appropriately trained. See www.the-sia.org.uk for more details.

When monitored

What hours during the day, and what days in the week is live monitoring required?

It may be the case that the control room is staffed during the site’s opening hours but not at other times, or there may be a requirement for 24-hour monitoring.

Similarly, the same regime may be required every day, or a different regime may be appropriate at weekends, or at times of higher than normal risk such as after a football match or during a protest.

Where monitored

Where is the CCTV control room located?

The first decision is whether the monitoring is performed off site, perhaps by a specialist monitoring and response services company or at the premises.

If the monitoring is to be performed on the premises then a suitable location must be identified to accommodate the operators and the core system equipment.

Good design of the control room is fundamental to ensuring the effectiveness of your system. The layout should enable the observer to view each camera to the required level of detail.

The following points are worth considering:
• Size and shape of room

• Light and ventilation (Ensure that the light level is appropriate and that lights are positioned so as not to cause glare on the displays. Also, bear in mind that the equipment may generate significant heat, and additional ventilation or air-conditioning units may be required.)

• Security (e.g. access control to prevent unauthorised viewing or tampering, with access records kept)

• Proximity to the locations being monitored

• Ergonomics (Is the layout comfortable for the operators and does it allow them to maintain appropriate levels of alertness?) Is a Display Screen Equipment (DSE) assessment required?

See HOSDB Publication 14/98 CCTV: Making It Work, Control Room Ergonomics for additional guidance on the design of a control room.

**Response**

*What happens when an event occurs?*

Consider who decides when a response is necessary and what that response should be. For example, it might be appropriate for the operator to contact:

- a guard on patrol
- the site manager
- the emergency services
- the control room of a neighbouring CCTV facility

In some cases it may be appropriate to simply note the event and take no further action.

The CCTV control room should be equipped with suitable communication facilities to enable the operator to easily contact the relevant personnel.

Estimate an acceptable response time for the activities being monitored, and consider whether the operator should be instructed to continue monitoring the subject until the response arrives.

---

**While monitoring the reception area an operator identifies a person drunkenly stumbling towards the desk. His response would be to call the security guard to escort the unwanted visitor from the premises; then he would contact the receptionist and confirm he was aware of the situation and advise that a guard would attend.**

**Two suspects are spotted in a car park stopping at a vehicle and attempting to gain entry. The operator’s response would be to call internal security to intercept the suspects, and then contact the police to report the crime.**

**At a supermarket the operator notices that long queues are building up at a number of tills while others remain unmanned. In this instance the appropriate response is to contact the checkout manager.**
4.2.3 System Requirements

Having developed an operating procedure and decided on the observation requirements for each area of interest (Q1-4), attention should be focused on the features of the CCTV recording / display system itself.

Alert function

What action should the system take when an event is detected?

Many systems have some configurable automatic alert function, which will be activated when a particular event occurs. It may be desirable to integrate the CCTV with other protective security equipment such as an intruder detection system, which will detect an event such as the opening of a door and then activate the CCTV. Alternatively the event may be detected by the CCTV system itself, if it has an in-built video motion-detection (VMD) capability, or a more advanced Video Based Detection System (VBDS) capability, also known as “Intelligent Video”.

A decision should be made regarding what type of activity should trigger an alert, and then what form that alert should take, for example:

- a simple **audible** alarm such as a beep
- **visual** alarms such as a flashing light that pinpoints the location of the event on a plan of the facility on a screen in front of the operator
- a **text** message or an **image** sent to a key holder
- an **emergency relay** sent to the local police station
- **record event data**. Some systems do not record continuously, rather only when motion is detected. This is often done to reduce the storage requirement. However, this feature should be used with caution; false triggers such as flickering lights may cause continuous activation, which will in turn fill the hard drive more rapidly than expected. If alarm-activated recording is used, it could be desirable to be able to start the recording at a point several seconds before the actual event occurs, so that the lead-up to the event can be seen. In order to do this, a record buffer would be needed, i.e. short-term storage of all video, which is automatically overwritten unless an event is detected, in which case the appropriate section is retained. An alternative scenario is that all video is recorded at a high frame rate, and then some frames from the less significant sections are deleted after a set time.
- **display the view** from the camera on a monitor screen in front of the operator (It may be advisable for some monitor screens in the control room to remain blank under normal conditions, and to be activated only when an event is detected.)
- create a record of the event in an **audit log**

A person enters a corridor leading to a secure storage room. The corridor is not normally accessed so is not subject to continuous monitoring or recording. However, when the person is detected, the recorder is activated and an alarm sent to the control room operator, so they can decide what further action to take.
Display

How will the images be viewed?

If live monitoring is required, the following points need to be considered:

**The number of screens required** depends on the number of cameras but is also a balance between number of operators and how many displays they can effectively monitor at any one time. It has been suggested that a single operator should monitor no more than 16 screens simultaneously, although this depends on the circumstances; this figure may need to be reduced where the screens show high levels of activity or detail that need careful monitoring.

Some camera views may require constant monitoring and will thus need a dedicated screen; others may not in which case a single screen could be used to cycle between several cameras.

Separate displays (or a separate viewing area) may be required for reviewing recorded video.

**The number of cameras per display screen** will depend primarily on the activities you wish to detect and the display’s size. It may be the case that one display is split to show the view of several cameras, although this will reduce the resolution and effective screen height of the target (e.g. change “detect” to “monitor”, as discussed in section 4.1), and may not be suitable if the view is of particular importance or the scene is complex. A standard sized screen should display no more than four cameras. Another option would be for a given screen to display the views of several cameras in a regular sequence.

Displays are getting larger and cheaper so **size** will be partly a financial decision and partly dependent on the space available, although do be aware that having one big screen in the place of a few smaller ones can reduce the flexibility of the viewing system.

**The type of display** is a choice between traditional CRT screens and more modern LCD or plasma displays. Further information is given in section 5.4.

Recording

How long is the video retained on the system before being overwritten?

What image quality is required on the recorded image compared with the live image?

What frame rate is required for the recorded video?

What metadata (additional information) should be recorded with the video?

Most new CCTV systems rely on digital recording technology, where the video data is recorded onto a hard drive like that found in a standard computer. The drive has a finite storage capacity, so a digital CCTV recorder operating continuously can only retain video on the system for a set period before it is overwritten. A retention time of 31 days has traditionally been recommended for most CCTV applications, as this provides sufficient time for the authorities to attend the scene and retrieve the video in the event of a serious incident, but respects the advice of the Information Commissioner that data should not be retained for longer than necessary. The CCTV manager should make a decision on a suitable retention time for his/her application.
Some systems offer the additional facility of protecting sequences of particular interest to prevent them from being overwritten.

When a digital video recorder saves images it compresses them so that more data can be saved on the hard drives. This compression will almost invariably reduce the quality of the video. When purchasing and commissioning a CCTV recorder it is therefore vital to inspect the quality of the recorded images as well as the live view as there could be a substantial difference between the two.

Adjusting the recorder settings to increase the retention time will result in a reduction in the stored image quality (i.e. “Best Storage” settings give you the lowest quality recorded video).

Choose an appropriate frame rate for each camera to record, based on speed of motion from Q4. Different frame rates may be required at different locations.

The OR should specify the required retention time, recorded image quality and frame rate for each camera. The CCTV supplier will use this information to determine the appropriate storage capacity (hard drive size). More detailed technical information on image quality, recording and hard drive capacity is provided in sections 5.5 and 5.6.

Finally, decide whether additional metadata (text information) should be recorded alongside the video images. A key requirement is to include the time and date information, firstly to add evidential weight to the pictures, and secondly to allow the user to search through the recordings and retrieve the relevant video efficiently. There is often also a requirement to record the camera location and number.

There should be a mechanism for ensuring that the time and date information remains accurate (for example during the change from GMT to BST) and does not slowly drift from the true value. This mechanism can either be technical (such as the inclusion of a clock source automatically linked to the NPL time signal) or procedural (instruction to the operator to check and update the clock regularly).

Should the recorded data be of critical importance, it may be worthwhile to take additional measures to protect the recording system against the possibility of hard drive failure. This is usually achieved by specifying a RAID recording system (Redundant Array of Independent Discs). There are several RAID standards, but they commonly involve splitting / duplicating the data across more than one hard drive.

**Export / Archive**

*How will you export data from the system to create a permanent record?*

*Who will require access to the data (e.g. police etc.)?*

*How will they replay the video (e.g. is special software required)?*

A CCTV recorder should provide a means of creating a permanent record of an incident, which can then be provided as evidence for any subsequent investigation. With an analogue recorder the process was straightforward, as the relevant video cassette could be removed and retained. For a digital recorder, however, the incident must be copied from the internal hard drive to
a permanent storage medium such as a CD/DVD, before it is overwritten. The CCTV system therefore needs to be provided with a suitable export facility.

In most cases a CD or DVD writer will suffice for exporting single images and short video clips under about ten minutes in length.

For exporting longer video clips and for large scale archiving, the system should provide one of the following:

- the ability to export video to an external 'plug and play' hard drive via a USB or Firewire connection
- Network port
- Removable hard drive

Note that network and USB ports can operate at a range of speeds, the slower of which may not be suitable for transferring large volumes of data. The latest (and fastest) standard should be specified for a new system.

There may be a requirement for a system to be permanently connected to a network, to provide remote access either for data download or for live viewing, and possibly to provide a link to other CCTV systems as part of a larger CCTV network.

The exported video sequence may be in a non-standard format. If this is the case, it is important to ensure that the manufacturers provide additional software so that the video can be replayed and viewed on a standard computer. Many systems enable the replay software to be downloaded from the system at the same time as the data. If a removable hard drive is provided, then this should either be in a format that can be read on a standard computer (e.g. Windows based) or a separate replay machine should be provided to which the drive can be attached.

The video should be exported in its native file format (i.e. without converting between formats) to maintain image quality, and no additional compression should be applied during the export process.

Further guidance can be found in HOSDB publication 09/05 UK Police Requirements for Digital CCTV Systems and in HOSDB publication 21/06 Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems.

4.2.4 Management Issues

This section covers legal issues as well as resource requirements and the need for ongoing support and maintenance.

13

Constraints

What licensing regulations apply to the CCTV system?

This covers any rules or regulations applied by local or central government such as planning constraints, licensing or public safety provision. Additional conditions regarding CCTV provision could be applied by insurance
companies, or by any specialist regulatory authorities that oversee the facility. The views of these bodies should be sought as part of the stakeholder consultation process.

Increasingly CCTV operators have to be licensed especially when monitoring public places. For further information see the Security Industry Authority (www.the-sia.org.uk).

Legal issues
What laws apply to the storage of and access to information?

The Data Protection Act (1998) is designed to prevent the misuse of personal information. Legal obligations are placed on anybody who handles this type of information.

The Freedom of Information Act (2000) provides a right of access to any recorded information held by public authorities. Legal obligations are placed on public authorities to follow certain procedures when responding to requests for information.

For further information on these see The Information Commissioner’s Office (www.ico.gov.uk). The ICO also publish a CCTV Code of Practice. Other legislation of which to be aware:

The Human Rights Act (1998)
The Criminal Justice and Public Order Act (1994)
The Police and Criminal Evidence Act (1984)
The Protection from Harassment Act (1997)
The Criminal Procedure and Investigations Act (1996)
The Magistrates Court Rules (1981)
The Magistrates Court Act (1980)

CCTV operators should be aware of the requirements placed on them by these laws and should have procedures in place to enable them to comply. Note that laws can be amended, new ones introduced and old ones superseded so it is recommended to seek up-to-date advice.

Maintenance
What regular maintenance is required?

Who is responsible for ongoing maintenance tasks?

Without ongoing maintenance, systems will deteriorate. It should be decided who has responsibility for each of the following activities:

- Cleaning the equipment (in particular cleaning the camera housings)
- Repairing or replacing faulty equipment (an acceptable turnaround time from report to repair should be specified in any service contract)
• Maintaining camera positions and focus
• Upgrading the system (The expected working life of the equipment should be known, and upgrades planned for.)
• Equipment warranties

If cameras are placed in awkward or inaccessible locations, then maintenance could be more difficult. Health and safety regulations may also need to be consulted when carrying out maintenance operations.

Thought should also be given to how often the maintenance tasks should be performed. The schedule shown in table 1 is based on the British Security Industry Association (BSIA) Code of Practice for the Planning, Installation and Maintenance of Closed Circuit Television Systems and serves as a guide to help plan regular system maintenance. See www.bsia.co.uk for more detail.

<table>
<thead>
<tr>
<th>Task</th>
<th>Daily check</th>
<th>6 Monthly</th>
<th>Annually</th>
<th>After Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera function</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Camera alignment</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Lighting function</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Wash/wipe function</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PTZ function</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Picture quality</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Record duration</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Inside housings</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cabling</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1: Suggested maintenance schedule

Resources

What are the resources required to operate the system?

This covers all those associated costs and additional resources not directly attributed to the purchase of the system such as:

• Additional personnel costs to operate, manage and maintain the system
• Service contracts for maintenance and repair
• Allocation of space to house the central system and any personnel
• Other equipment such as furniture, blank recording media and a UPS (Uninterruptible Power Supply)
• Consumables
• Training costs (initial operator training plus any ongoing training commitments)
5 Technical Guidance

5.1 Introduction

This section is designed to provide further guidance and background information to assist those who wish to develop a more detailed set of technical specifications for their CCTV system. It may also help those who, whilst not involved in technical issues themselves, may need to discuss matters such as camera placement or recording requirements with the contractor who is responsible for the system design and installation.

The constituents of a typical CCTV system are shown in figure 6. It is important to consider each component in turn, starting with the scene illumination and concluding with the replay and review of recordings.

5.2 Lighting

Having total control over how the locations are lit is a rare luxury. However a simple understanding of light sources and levels, as well as scene contrast, will help to ensure that the system performs to the best of its ability.
5.2.1 Light Levels

Maintaining a suitable light level over the scene being monitoring is a big step to ensuring the system performs to its best ability. The **minimum light level** required will depend on the type of activity being monitored. Most cameras can operate at surprisingly low levels, well below the 3 Lux mark generally considered as the minimum for security purposes. As with our own vision, systems tend to be weaker at discerning colours and detail at low light levels and this gets worse as the light level drops. In modern offices the light level is adequate during working hours, but after hours this is rarely the case.

Artificial light may be required to maintain an effective visibility level. Externally, this could mean the use of floodlights, which may already be present as a public safety or security measure. However, it should be noted that different lighting systems (such as low pressure sodium) may have different levels of lighting / colour rendition.

In some circumstances, floodlights may be considered too intrusive, or meet with local opposition. In these cases, **near infrared** detection systems that are sensitive to ‘light’ beyond human vision can be used (usually integrated with a normal colour camera for daylight use). These systems tend to produce black and white images at night; during the day their ability to render colour may be poor unless a supplementary infrared filter is part of the camera.

On a bright sunny day the light level can reach 100,000 Lux, which can cause a problem for cameras if such bright light falls directly on the lens e.g. the low sun of winter mornings and evenings. This can lead to flare, which causes colours to lack saturation and appear washed out, and can also cause loss of detail (figure 7a). This effect may persist for several seconds after the cause is removed by either the sun going in or the camera being moved. Strong sunlight reflected into the camera by a window, surfaces of water or shiny objects could also cause flare, as can car headlights. The addition of a lens hood to the camera will often help reduce the problem.

![Figure 7: (a) effect of flare and (b) silhouette effect](image)

5.2.2 Scene Contrast

Keeping even levels of light across a scene ensures good contrast. Combining extreme levels leads to too much contrast resulting in a poor image. It is usually recommended that there should be no more than a 3:1 ratio of minimum to average illumination within an artificially lit scene.

When extremely high and low light levels are encountered in the same scene the contrast is often too great for a camera to handle effectively. This can lead to a silhouette effect where a subject is surrounded by bright light yet appears too dark for any features to be properly distinguished (figure 7b).

This is a key failing seen in many poorly designed CCTV systems. It frequently occurs with cameras facing out of entrances or close to shop windows or down dark corridors with a window at the end. This is especially true on bright sunny days or at times when the sun is low in the sky.

Poor lighting design resulting in uneven illumination is also a common cause of large contrast ranges. For example, industrial units tend to be lit from up high with strong lighting; this situation is then made worse by shadows created by high shelving units.

5.3 Camera

Bullet, pan-tilt-zoom, dome, indoor, outdoor, professional, vandal resistant, colour and covert are just a selection of camera types available for CCTV systems. Regardless of type they normally comprise two main components, a lens and a sensor element. Together these determine the camera’s capability including its image resolution, field of view and its low light level performance. Where the camera is positioned and how it is maintained are also important considerations. Additionally with the advent of IP and wireless technology, the method by which the camera transmits its images to the core system is also now an issue.

5.3.1 Field of View (FoV)

Also referred to as the angle of view or angle of coverage, the FoV is the amount of a given scene captured by the camera (figure 8). Three elements decide the FoV; the lens and sensor element within the camera and where this unit is positioned in relation to the scene. Note that a large FoV generally results in any target object being relatively small in comparison to that shown by a camera with a small FoV.

A camera with a large sensor element of 2/3” and a wide-angle lens of 5mm positioned 6 metres high on the side of a building will provide a large field of view. By contrast a camera with a small sensor element of 1/3” and a telephoto lens of 50mm positioned 2 metres high on an interior wall would provide a very small field of view.
Having determined the area of interest, the activity to be monitored, the observation criteria and target speed as part of the OR capture process, it should now be possible to estimate the most suitable FoV. When determining the FoV required of a camera avoid problem areas such as shadows and blind spots, and care should also be taken not to record areas outside the remit of the installation. See the BSIA privacy masking guidelines for further information (www.bsia.co.uk).

For greater accuracy in determining the FoV you require, perform an internet search on CCTV Lens Calculator and select one of the options provided. These require you to enter some basic details of the scene and perform the relevant calculation.

![Figure 8: Effect on FoV of varying lenses with a constant distance](image)

As an alternative (or as a supplement) to using fixed-view cameras it may be beneficial to use a camera with a pan-tilt-zoom (PTZ) capability. This gives the operator the ability to cover a wide area but also zoom in to focus on an incident wherever it occurs within the original field of view, providing greater detail and assisting with identification of the subject. It can also be used to pan across a scene to track a target. PTZ cameras are often used as a back up or in addition to cameras with fixed FoVs. However, PTZs can be deployed unmanned with fixed ‘security patrols’ or with preset triggered sequences, for example being programmed to zoom into a car number plate and person operating a petrol pump, triggered when the nozzle is removed from its stand. Disadvantages of PTZ cameras are their cost compared with a fixed camera, plus the additional work usually placed on the control room operator. It should also be remembered that they usually only cover a small area at a time.

To detect an incident that may occur anywhere within a large area, such as vandalism or theft from a car park, a series of wide-angle cameras may be appropriate (i.e. a camera with a large FoV). These are also often presented as a cost-effective solution, as fewer cameras will be needed to cover the whole area. They should ideally be spaced closely enough to ensure that any person approaching within the selected area was observed by at least one camera and was visible on the monitor at a minimum of 10% screen height, enabling them to be detected by the operator.

However, utilising only wide-angle cameras may not provide sufficient detail to enable an individual to be identified. Thus it may be necessary to include at least one camera that can capture more detailed information (i.e. obtain a clear shot of a face or car registration plate). The best place to site a camera for identification purposes may be a ‘pinch point’ such as an entrance/exit gate or doorway, i.e. somewhere that a person has to pass on their way in or out of the premises.
5.3.2 Low Light Level Performance

Cameras that operate in very low light levels should not be used to compensate for poor lighting, if possible. However as previously discussed in section 5.2.1 some situations may arise where supplemental lighting cannot be used and an infrared sensitive camera may be required. Infrared cameras can operate in daylight, but often provide poor colour rendition as shown in figure 9, though the addition of an infrared filter for daytime use will improve this.

Figure 9: Two images taken from an IR sensitive camera without filter; note colour shift between the IR image taken in the dark on the left, and the well lit image on the right.

5.3.3 Image Resolution

Cameras come in a vast array of resolutions normally measured in TVLs (Television Lines). Even now, when digital cameras are more often rated by their maximum number of pixels, the historic industry trend has been to convert this into an equivalent TVL number. Presently, cameras tend to have a TVL rating between 300 and 700, although higher resolution cameras are increasingly available.

In general a greater number of lines equates to a higher image resolution. However due to often inaccurate measurements a camera with 520 TVLs will not necessarily have a higher resolution than one with 480. As a good rule of thumb always ensure that the observer can comfortably resolve the amount of detail required for both for live monitoring and in the recorded review.

5.3.4 Placement

However carefully the type of camera and lighting levels has been considered, if the camera is positioned poorly then all the effort can be wasted. When specifying the camera placement consider the points below.

- Create the required field of view. Camera placement should be based on achieving an optimum view; the choice of location should not be dictated by ease of installation.
• Consider the effects of daily and seasonal variations in light especially low sun

• Consider the changes in foliage growth between winter and summer

• Consider protection from damage and the environment such as vandalism or driving rain

• Be aware of temporary or new permanent structures such as signs or other buildings blocking the FoV

• Remember the need to perform maintenance such as cleaning or repairs

• Consider how power will be supplied to the camera and data transmitted from it.

• Ensure that the camera is fixed firmly and does not wobble in the breeze. Stability may be a problem if the camera is fixed to a tall pole in an exposed location.

• Where suspect identification is the main priority, place the camera at head height. Ceiling mounted cameras may not be able to provide a full view of the suspect’s face.

The need for physical protection, both from the weather and from human interference is important. It may be advisable to locate the camera above head height, to minimise the possibility of vandalism. However, this may compromise the field of view and make facial identification more difficult, and may also make regular cleaning and maintenance awkward.

5.3.5 Transmission

Wired transmission was for many years the only mainstream method of transmitting video between the camera and the recording unit. However the availability of wireless transmission has boon in recent years and the CCTV industry has not been left out.

Wired

Whether it is through traditional coaxial cable, modern Cat 5 (or Cat 6) as used in computer networks or optical fibre, wired networks are generally the popular choice. They are relatively cheap, rarely affected by the environment and transmit large amounts of data. Some cameras can be powered through the data transmission cable, removing the need for extra electrical cabling. Standard coaxial cable is also a secure transmission method.

Downsides are few in most cases; installation within a building is usually straightforward, but laying cables outdoors can be awkward and expensive where they have to be buried in the ground. Retrofitting cable in old, especially listed, buildings can also be an issue. Furthermore, trying to transmit over large distances (over 100m with Cat5/6 and over 300m with coaxial) can cause data loss.
**Wireless**

Most wireless cameras operate on the 2.4GHz frequency band. This open band is shared with many other systems such as wireless computer networks, but also cordless telephones, baby monitors, garage door openers and wireless doorbells.

The potential for interference is high and can be caused by almost any other high-powered wireless transmitter regardless of its operating frequency. This is particularly true of mobile phone networks and microwave ovens. Data may also be less secure if transmitted wirelessly, with there being the possibility of accidental viewing by third parties, unless the signal is encrypted.

On the plus side, though, they are quick to install and may be a more acceptable solution where the desire to avoid cable is an issue. Although most of the wireless cameras on the market only have a limited range of about 100 metres there is the potential to create links using specialist technology of up to 10 km.

**IP**

This is the method of transmitting information across a data (digital) network. IP is more commonly seen in computer based Local Area Networks (LANs) and other digital networks.

As CCTV applications migrate towards full digital systems, IP is increasingly used to connect cameras and other related devices. Its usage can be both wired and wireless with appropriate consideration given to the type of connection to be used.

Using IP based systems can provide other operational benefits. Device telemetry, control and adjustment could be achieved remotely and remote viewing and re-viewing could be implemented when deployed with enabled equipment, over a suitable data network. However, the temptation to add cameras to an existing LAN can often cause data loss or slow down response times as the volume of information travelling the network is hugely increased. Latency and slow responses can become a problem when trying to control the movement of PTZ cameras, for example. Data security may also require consideration if the CCTV system is part of a larger shared network.
5.4 Displays

In the majority of cases the decision on which type of monitor is chosen will be partly financial and partly practical. For instance, if only a small area is allocated to act as a control room then bulky displays can be ruled out. Even if a large area is allocated, apportioning large amounts of a budget to supersize the displays may not necessarily be money well spent.

In simple terms displays come in two forms, the traditional CRT (Cathode Ray Tube) design or the modern flat screen variety. (A third, less common option is a rear projection system.) The flat screen displays can either be LCD (liquid crystal display) or plasma, sometimes known as PDP (plasma display panel). A summary of display technology is shown in table 2.

Generally CRTs will provide a superior image especially where movement is concerned, but the trade off is their bulk, weight and heat generation when compared with flat screens. Flat screens tend to suffer from an effect known as motion blur, which makes detail on a moving object difficult to resolve (for example the registration plate of a moving vehicle). They have nevertheless become the first choice for most CCTV systems, in the same way that they have taken over the consumer television market.

It should be noted that most screens can suffer from image burn (image persistence), where if the same background scene is displayed continuously for a long period, this can be burnt in, leaving a permanent mark on the screen.

<table>
<thead>
<tr>
<th>Type</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRT</td>
<td>Best attainable picture quality</td>
<td>High power consumption</td>
</tr>
<tr>
<td></td>
<td>Robust technology</td>
<td>High heat generation</td>
</tr>
<tr>
<td></td>
<td>Much equipment was designed for reproduction on a CRT</td>
<td>High space requirements</td>
</tr>
<tr>
<td></td>
<td>Low cost</td>
<td>Manufacture largely discontinued</td>
</tr>
<tr>
<td>LCD</td>
<td>Compact and light</td>
<td>Poor movement reproduction</td>
</tr>
<tr>
<td></td>
<td>Low power consumption</td>
<td>Restricted viewing angle</td>
</tr>
<tr>
<td></td>
<td>Wide range of screen sizes available</td>
<td>Low image contrast</td>
</tr>
<tr>
<td></td>
<td>Low cost</td>
<td></td>
</tr>
<tr>
<td>Plasma</td>
<td>Slim design, wall mountable</td>
<td>Fragile</td>
</tr>
<tr>
<td></td>
<td>Larger maximum size than LCD</td>
<td>High power consumption</td>
</tr>
<tr>
<td></td>
<td>Wider viewing angles than LCD</td>
<td>High heat generation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expensive</td>
</tr>
</tbody>
</table>

Table 2: Summary of display technologies

It is worth noting that there are many new flat screen display technologies in development that aim to retain the benefits of the current screens yet provide the image quality associated with CRT.
5.5 Image Quality

Human visual perception of an image is hard to quantify, but there are some simple measures that can be taken to ensure that the image quality is optimised for whatever activity is being monitored.

Consider four areas when determining the required image quality:

**Clarity** – Is the picture sharp enough, and is there any lens distortion?

**Detail** – Is there enough to identify objects?

**Colour** – Is it natural?

**Artefacts** – Are there elements in the image that should not be there? And are they obtrusive?

5.5.1 Compression

Compression can be the biggest cause of image quality loss with digital video recordings, especially when used to excess.

‘Lossless’ compression is a technique that reduces the size of files without impacting on the image quality. There is a limit, however, to the amount of size reduction that can be achieved with lossless techniques, and thus ‘lossy’ compression is more common. This can result in much smaller files, thus maximising the amount of video that can be stored on the system, but picture information is discarded during the compression process. The more compression is applied, the smaller the file size, but the greater the loss of image quality in terms of clarity, detail and colour. Compression may also create unwanted artefacts within the image (i.e. unnatural effects and noise).

An additional method of compression used in video is known as interframe compression. This works by comparing one frame in the video with the previous one, and only storing the differences. Certain frames are known as I-frames (where “I” stands for independent), and these are coded separately. Between the I-frames are a series of predicted P-frames. Interframe compression results in much smaller file sizes than if all frames were encoded separately, but there may be an adverse effect on the video sequence, and it may not be as effective if there are large changes between frames, as can be the case with time-lapse video. Some CCTV systems use interframe compression, some do not.

Common compression codecs include JPEG, MPEG and MJPEG and also H263 and H264. Each uses their own complex method of compressing images but each is based on either Wavelet or DCT (Discrete Cosine Transform). Wavelet compression is becoming more popular because the compression artefacts are less obvious and the final file sizes are smaller than those for images compressed via DCT to an equivalent quality level.

Figure 10 describes the different effects of Wavelet and DCT compression methods on an image.
Figure 10: Effects of compression on image quality

<table>
<thead>
<tr>
<th>DCT Compression</th>
<th>Wavelet Compression</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Live View Image (High Resolution)" /></td>
<td><img src="image2" alt="Recorded Image (Low Resolution)" /></td>
</tr>
<tr>
<td>Blocking is visible in the sky and colour changes exist on the boundaries.</td>
<td>Blocking and blurred detail is visible in both the sky and trees.</td>
</tr>
<tr>
<td>Very clear blocking and slight ambiguity with some of the characters.</td>
<td>Low resolution images and heavy DCT compression provides images of very little use. Significant blocking and very little detail remain in the image.</td>
</tr>
<tr>
<td>Above, the car’s number plate is clearly visible and the model’s features can be easily described. Below however some of the characters on the number plate have become ambiguous and the model’s features are much harder to discern.</td>
<td>Low resolution images and heavy Wavelet compression provides images of little use. Extensive blurring ensures little detail remains.</td>
</tr>
<tr>
<td>The difference between these two images is the resolution. Above the image resolution is typical for a live viewed image whereas below, the resolution has been reduced as often occurs when the image is recorded. Image compression technology, as shown in the side panels, may further reduce the recorded picture quality.</td>
<td>Good retention of character definition and image shape.</td>
</tr>
<tr>
<td>Image is generally smeared with a loss of detail throughout.</td>
<td>Image is smeared with very little detail in both sky and trees.</td>
</tr>
</tbody>
</table>
5.6 Recording

In many cases CCTV systems are used mainly as a deterrent or for live monitoring, with the recorded image quality being a secondary consideration. However, not configuring the recording system correctly could be a costly mistake; particularly should the video be required as evidence in court.

Analogue systems based on standard VHS recorders were straightforward to operate. Video was recorded onto tapes and when each tape was full, the old one was ejected and a replacement inserted. A single tape could generally hold 24 hours of (time-lapse) video, so tapes could be changed on a daily basis. A stock of 31 tapes would provide a month’s storage, after which the oldest tape could be re-used.

Digital video recorders tend to record on standard hard drives as found on most computers (although ideally they should be of better quality and reliability as they will be running continuously, possibly for years). When the drive is full, the oldest data on the system will be overwritten with new material. Digital recorders can store many days if not weeks of video from multiple cameras, but be warned that invariably most systems on any setting will not store images of the same quality as seen on the live view.

Consider the following when deciding on how best to record and save your video:

- How many days worth of video do you need to retain?
- What image quality do you require from your recorded video?
- How many frames per second do you require?

Remember that for an off-the-shelf CCTV recorder, increasing the retention time may result in a decrease in image quality, because the compression level needs to be raised to fit more video on the hard drive, i.e. Best Storage usually means Worst Image Quality. Thankfully hard drives are getting lower in price and higher in capacity, so should become less of a constraint when specifying a system.

5.6.1 Frame Rates

With most cameras 25 frames (images) per second are captured, which gives the appearance of smoothly flowing motion and is more than adequate for most scenarios. However in order to reduce the amount of video that needs to be stored CCTV systems allow this figure to be reduced.

Broadcast quality video is recorded at 25 frames per second (fps), but for CCTV recorded in time-lapse mode, frame rates of 5-8 fps are more common, although rates as low as 1 fps are used.

If target speed is high or the scene complex then a high frame rate is advised (more than 5 fps), but if the target is slow the frame rate could be reduced to optimize storage. It is also possible to have variable frame rates so a low rate is used until an alarm is triggered then the rate is increased. This works best if the system can buffer a few seconds of recording from before the alarm trigger, so that events leading up to the trigger can also be seen clearly.
5.6.2 Storage Capacity

The total storage requirement for a digital CCTV recorder should be estimated before a system is installed, so that a hard drive of the appropriate capacity can be specified. It is vital to ensure that sufficient capacity is available so that compromises do not have to be made on either the image quality or retention time.

The storage capacity needed in a CCTV system depends on several factors, which are summarised below. Typical values for each variable are given in table 3.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Image Size</th>
<th>Frames Per Second</th>
<th>Number of Cameras</th>
<th>Operational Hours</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Range</td>
<td>5kB – 50kB</td>
<td>1 – 25</td>
<td>1 – 16+</td>
<td>1 – 24</td>
<td>24 Hours – 31 Days</td>
</tr>
</tbody>
</table>

Table 3: Factors affecting the storage capacity required for a CCTV recorder

**Image Size** – This value is the average size of each image as recorded. The actual figure will be a function of the image resolution (in pixels or TV lines) and the amount and type of compression applied to the image or video sequence (It is particularly dependent on whether interframe compression, as discussed in section 5.5.1 is used, in which case the average frame size will be an average of larger I-frames and smaller P-frames.) These factors are very much dependent on the specific CCTV recorder, which can make the image size difficult to estimate accurately, and assistance should be sought from the system supplier.

**Frames per second** – The number of images recorded each second by a camera has a significant impact on the amount of data being generated. The preferred frame rate should have been identified during the level 2 OR capture process.

This value could be dynamic if a camera is triggered by external alarms or motion detection. For some systems there may be no recording unless activity is detected. For others, there may be continuous recording at a low frame rate, say 1 fps, until activity is detected, when there will be a short period of recording at a high frame rate, say 12 fps. If this is case an average value should be calculated by estimating the number of anticipated triggers in a 24-hour operational period, e.g.

- Standard rate ($R_S$) = 1 fps
- Triggered rate ($R_T$) = 12 fps
- Triggered period ($T$) = 3 mins

Number of triggers anticipated per day ($N$) = 10
Number of minutes per day at triggered rate = $N \times T = 30$ mins
Number of triggered frames generated = $30 \times 60 \times R_T = 21600$

Number of minutes per day at standard rate = 23 hrs 30 mins = 1410 mins
Number of standard frames generated per day = $1410 \times 60 \times R_S = 84600$

Total number of frames generated per day = $21600 + 84600 = 106200$
Average frame rate per second = $106200 / \text{number of secs in 24 hrs}$

= $106200 / 86400 = 1.2$ fps
**Number of cameras** – This is the number of active cameras used for the whole system under consideration, as specified in the OR.

**Operational hours** – This is the number of hours the CCTV system will be operational, within a 24-hour period, as specified in the OR.

In a simple system this could be for the full 24 hours per day, whereas in a more complex system it could be for a predefined number of hours whilst the premises are occupied / vacant.

**Retention Period** – The time for which the CCTV footage should be stored on the system before being overwritten, as specified in the OR.

A general equation has been given to aid in estimating the total amount of storage required:

\[
\left( \frac{\text{Size} \times \text{fps} \times C \times \text{Hours} \times 3,600}{1,000,000} \right) \times TR = \text{Approximate Storage Requirement (GB)}
\]

Where:

- \(\text{Size}\) = Image size in kB
- \(\text{fps}\) = Images per second
- \(C\) = Number of cameras in the system
- \(\text{Hours}\) = Total number of operational hours in a 24 hour period
- \(TR\) = Retention period

3,600 is to convert seconds into hours (60 x 60)
1,000,000 is to convert kB to GB

This equation can be used for very basic systems where all the cameras are recording at the same image size, frame rate and operational hours. For more complex systems a storage requirement can be calculated for each camera and the resultant totals added to give the overall requirement for that system.

**Example 1**

A CCTV system is being specified for a custody suite that is required to capture high quality images. 12 frames per second are being generated and there are 8 cameras in the system. Each camera is recorded for 24 hours per day, and the OR has stipulated a retention period of 31 days.

\[
\left( \frac{10 \times 12 \times 8 \times 24 \times 3,600}{1,000,000} \right) \times 31 = 2600 \text{ (GB)}
\]

As can be seen this represents a huge amount of data, and another strategy might need to be considered to ensure the amount of data being collected is manageable. In this case it might be considered that the amount of data being generated is necessary, in which case the storage provisions should be made. However it might be deemed more appropriate to reduce the image size/quality on half of the cameras, or to reduce the frame rate on some of the cameras. Another approach might be to use IR triggers or motion detection to trigger the image recording as discussed on page 16.
Example 2
A retail outlet is installing a small CCTV system to protect the access points (windows and doors) whilst the shop is closed. The image size has been set to a medium value, and the resultant image checked for suitability against the level 2 OR requirements. The recorder will be triggered by motion detection and IR sensors and the average frame rate has been calculated as 2 fps for all the cameras. 6 camera locations have been identified to offer maximum coverage, and all the cameras will only be recording for the hours the venue is closed 7pm until 7am. As the reason for the system is to provide evidence after a break-in the retention time has again been set to 31 days.

$$\left(\frac{5 \times 2 \times 6 \times 12 \times 3,600}{1,000,000}\right) \times 31 = 80 \text{ GB}$$
6 System Validation

The final step in the process is to check that all of the functions specified in the operational requirements have been met by the installed system, a user manual has been supplied and that the system has been set up correctly. In particular, test:

- Camera’s field of view
- Live and recorded image quality
- Storage time provided by the system
- Operation of the alarms and motion detection features

It is important to check that the field of view and image quality from each camera allow you to see the target with the required level of detail (i.e. enables you to either identify, recognise, detect or monitor the target as set out in section 4.2.1). One method for doing this is to use a Rotakin® test target, which is a panel shaped as the silhouette of a person, marked with resolution bars and with the ability to rotate. Further details can be found in HOSDB publication 14/95 *Performance Testing of CCTV Perimeter Surveillance Systems*.

The Rotakin should be placed within the field of view of each camera and its size measured on screen. The percentage screen height that it occupies can be calculated to see if it meets the minimum requirements for the relevant observation category (i.e. 5% for monitor, 10% for detect, 50% for recognise and 120% for identify). The ease with which the test pattern printed on the Rotakin can be resolved should give an additional indication of the image quality and level of detail that the system can provide. A human volunteer could act as a substitute should no Rotakin be available.

Once the live camera view has been checked, it is vital that the quality of the recorded images is also assessed to confirm that there has not been an unacceptable loss in detail during the recording process.

It should be noted at this point that the Rotakin was originally designed to assess the image quality of analogue CCTV systems and may not be entirely appropriate for digital systems, for the reasons discussed in section 4.1. Work is currently being undertaken at HOSDB to design test targets suitable for digital systems.

Once the system has been installed and commissioned, record and export some sample video that can be used as a reference of image quality and camera field of view for use during future system maintenance operations. This will highlight any change or degradation that occurs in the system over time.
<table>
<thead>
<tr>
<th>Location 1: Tills</th>
<th>Activity: Theft, Assault, Fraud, Customer flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of observation:</td>
<td>Identify</td>
</tr>
<tr>
<td>Target speed:</td>
<td>Fast (i.e. Not scanning items, ‘Dipping’ in till)</td>
</tr>
<tr>
<td>Camera:</td>
<td>Narrow field of view, lighting OK may need one per till?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location 2: Front door</th>
<th>Activity: N/A (Door is key pinch point. Camera placed here to capture high quality image of target who may have committed crime elsewhere on premises.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of observation:</td>
<td>Identify</td>
</tr>
<tr>
<td>Target speed:</td>
<td>Walking pace</td>
</tr>
<tr>
<td>Camera:</td>
<td>Narrow field of view, lighting OK (inward facing)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location 3: Shelves</th>
<th>Activity: Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of observation:</td>
<td>Recognise</td>
</tr>
<tr>
<td>Target speed:</td>
<td>Walking – but shoplifting activity occurs quickly, so high frame rate required</td>
</tr>
<tr>
<td>Camera:</td>
<td>Medium field of view, lighting OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location 4: Stock room</th>
<th>Activity: Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of observation:</td>
<td>Recognise</td>
</tr>
<tr>
<td>Target speed:</td>
<td>Medium</td>
</tr>
<tr>
<td>Camera:</td>
<td>Wide field of view, lighting OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location 5: Back door</th>
<th>Activity: Theft, Break in, Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of observation:</td>
<td>Detect / Recognise</td>
</tr>
<tr>
<td>Target speed:</td>
<td>Walking / stationary</td>
</tr>
<tr>
<td>Camera:</td>
<td>Wide field of view, needs extra lighting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location 6: Car park</th>
<th>Activity: Theft, Assault, Damage, Accident (public safety)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of observation:</td>
<td>Detect / Recognise</td>
</tr>
<tr>
<td>Target speed:</td>
<td>Walking / stationary</td>
</tr>
<tr>
<td>Camera:</td>
<td>Wide field of view, needs extra lighting</td>
</tr>
</tbody>
</table>
Appendix B: Blank OR Checklist

### Level 1 OR

<table>
<thead>
<tr>
<th>Statement of problem</th>
<th>Stakeholders</th>
<th>Risk Assessment</th>
<th>Success Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Level 2 OR for CCTV

<table>
<thead>
<tr>
<th>Define the Problem</th>
<th>Location</th>
<th>Activity</th>
<th>Purpose of Observation</th>
<th>Target Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define the Problem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Who Monitors</td>
<td>When Monitored</td>
<td>Where Monitored</td>
<td>Response</td>
<td></td>
</tr>
<tr>
<td>Alert Functions</td>
<td>Displays</td>
<td>Recording</td>
<td>Export / Archive</td>
<td></td>
</tr>
<tr>
<td>Constraints</td>
<td>Legal Issues</td>
<td>Maintenance</td>
<td>Resources</td>
<td></td>
</tr>
</tbody>
</table>