Home Office

Scientific Development Branch

CCTV Operational Requirements Manual 2009

Publication No. 28/09

N Cohen
J Gattuso
K MacLennan-Brown

CCTV Operational Requirements Manual

2009

N Cohen
J Gattuso
K MacLennan-Brown

28/09

5.0

CCTV Operational Requirements Manual

2009

N Cohen
J Gattuso
K MacLennan-Brown

Publication No. 28/09

5.0

ISBN: 978-1-84726-902-7

FIRST PUBLISHED APRIL 2009

Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
E-mail: hosdb@homeoffice.gsi.gov.uk
Website: http://science.homeoffice.gov.uk/hosdb/

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 previous CCTV Operational Requirements Manual, published by HOSDB in 2006.

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.

Contents

1 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 3 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 4. 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 (section 5) 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.

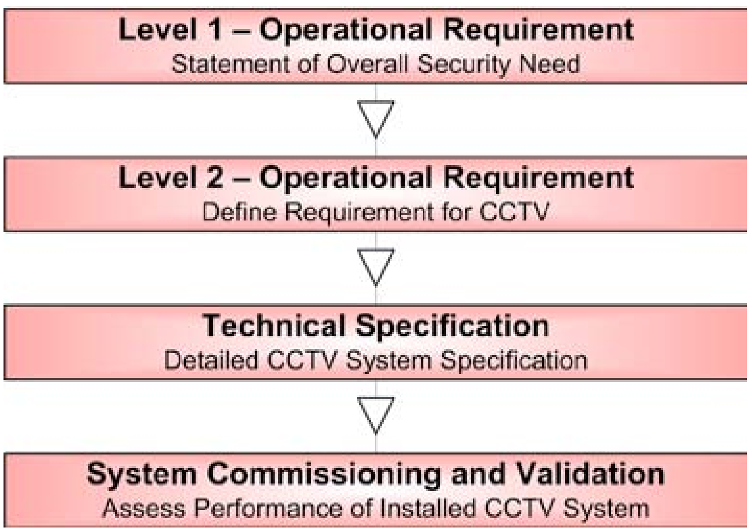


Figure 1: Key stages in specifying a CCTV system

2 Level 1 Operational Requirement

2.1 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.

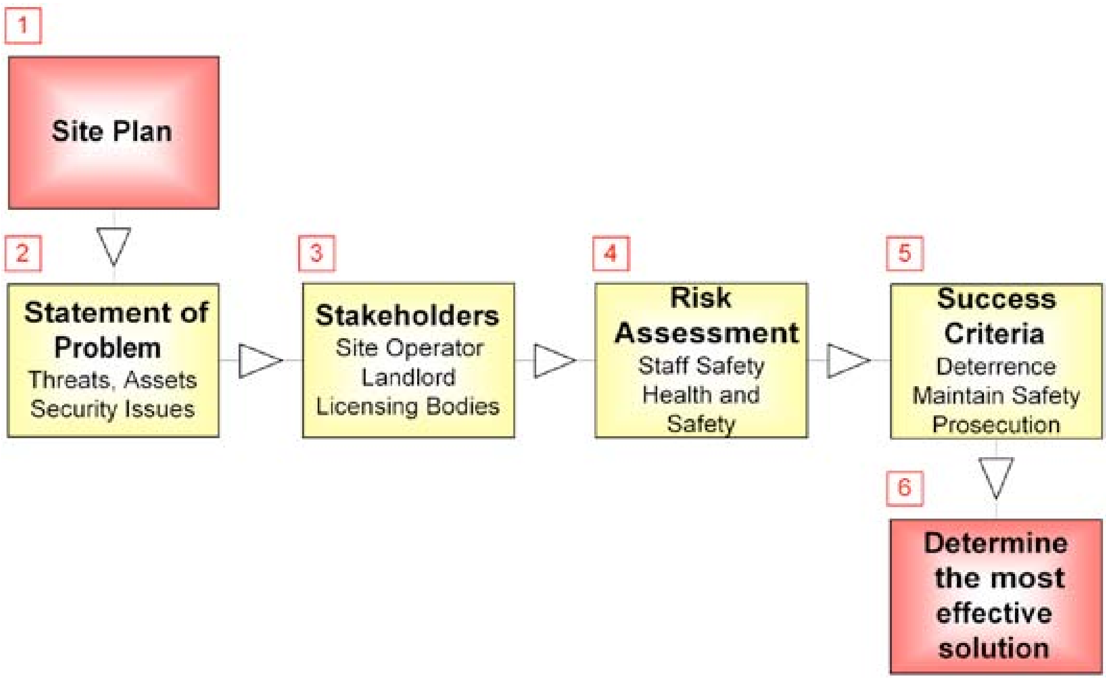


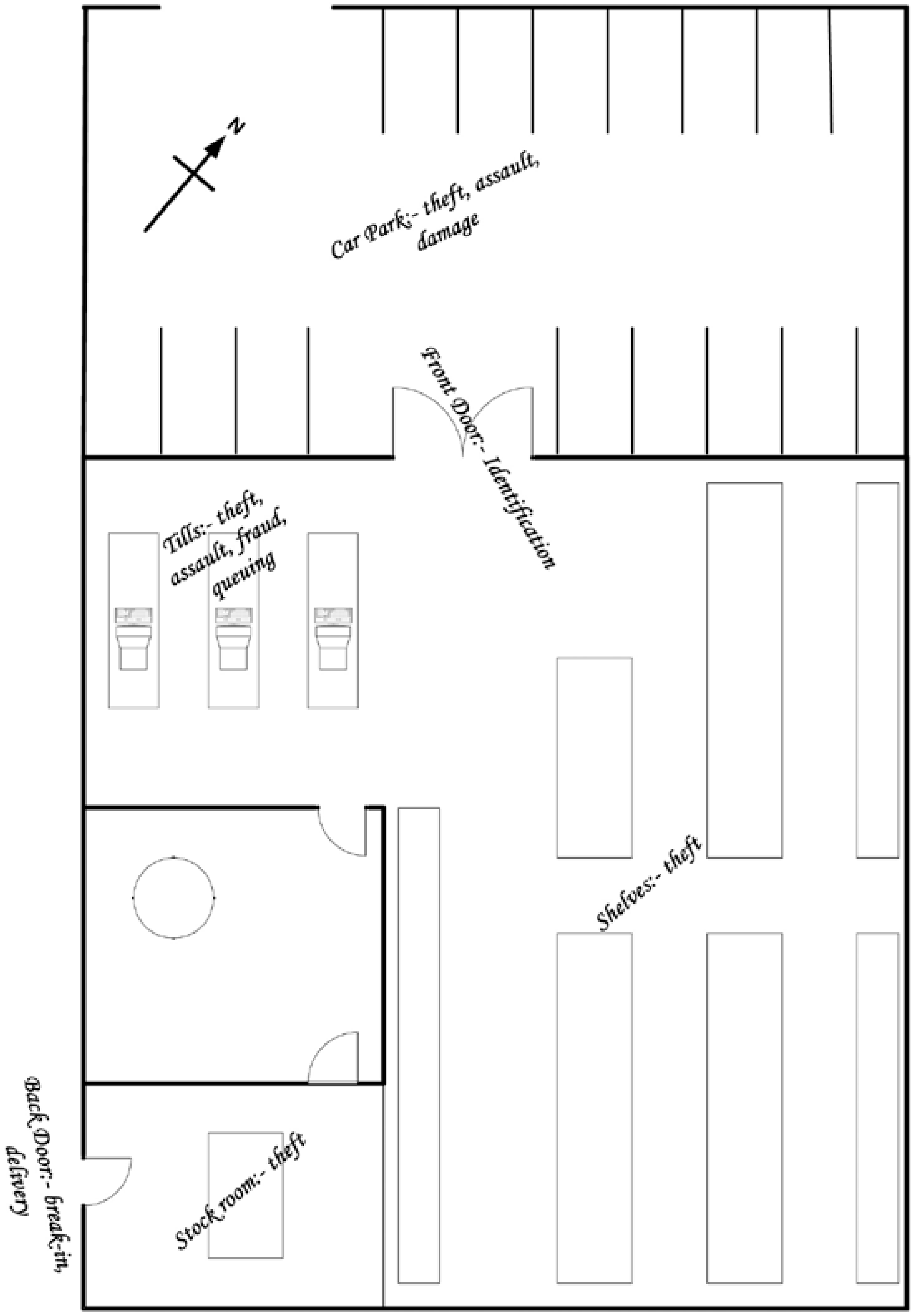
Figure 2: Level 1 OR checklist

2.2 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



2 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.

3 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.

4 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?

5 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

6 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.

3 Level 2 Operational Requirement

3.1 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, five 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.

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 across a wide area, 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.

Observe: A figure should occupy between 25% and 30% of the screen height. At this scale, some characteristic details of the individual, such as distinctive clothing, can be seen, whilst the view remains sufficiently wide to allow some activity surrounding an incident to be monitored.

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 100% of the screen height, picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.

Detect	Observe
	
10%	25%

Recognise	Identify
	
50%	100%

Figure 4: Height based 'levels of detail' for the more commonly used screen heights

The **Monitor** or **Detect** categories may be suitable for covering a wide area such as a car park. The **Observe** category is useful in areas where it is necessary to monitor a group of individuals such as outside nightclubs and pubs, or in town centres, as it provides reasonable detail of the subject whilst simultaneously providing some context to their activity by monitoring the area around them. The **Recognise** or **Identify** categories would be used for the cameras providing close-up images at the entry and exit points. In scenarios where the purpose of the camera is primarily access control and identity verification, a figure much greater than the 100% Identify setting may be required.

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 follow that it will be impossible to recognise or identify an individual if the image size is smaller than the 50% or 100% figures suggested. Equally, there is no guarantee that individuals will be identifiable just because they occupy >100% 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 when these guidelines were first developed, the systems all made use of the common PAL standard for video capture and display. Hence general observation categories could be developed, which were valid for all CCTV monitoring equipment. Since the influx of digital systems to the CCTV market there is now variability in the capture, recording and display resolution. So a 'Recognise' requirement can no longer be simply equated to a 50% screen height. For instance, through the use of megapixel cameras and high resolution displays it is now possible to provide the same image resolution as before using a much smaller physical percentage of the screen. Conversion tables have therefore been devised to show how the traditional percentage screen height criteria for a PAL system will look under a range of non-PAL resolutions. Table 1 shows the resolutions commonly encountered and Table 2 shows the equivalent screen heights needed to maintain the required resolution.

	PAL	1080p	720p	WSVGA	SVGA	VGA	2CIF	CIF	QCIF
Height	400[1]	1080	720	600	600	480	288	288	144
Width	720	1920	1280	1024	800	640	704	352	176

Table 1: Commonly encountered resolutions

Category	PAL	1080p	720p	WSVGA	SVGA	VGA	2CIF	CIF	QCIF
Identify	100	38	56	67	67	84	139	139	278
Recognise	50	19	28	34	34	42	70	70	139
Observe	25	10	14	17	17	21	35	35	70
Detect	10	4	6	7	7	9	14	14	28
Monitor	5	2	3	3	3	5	7	7	14

Table 2: Equivalent percentage screen heights for different **digital** resolutions. Green boxes indicate that it is reasonable to achieve the appropriate camera view. Red boxes indicate it may be unreasonable or difficult to achieve an appropriate camera view.

Caveats:

- The resolution being compared reflects the lowest resolution in the chain, not necessarily the display screen resolution.
- There is no significant image compression being applied to the image.
- The person imaged is of average height (5'4" to 5'8" or 1.64m to 1.76m)

The situation is further complicated for 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 4.6 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 installing a CCTV system.

[1] 400 vertical lines is the nominal PAL vertical resolution of 576 lines, adjusted by the Kell Factor of 0.7. This parameter allows a more accurate calculation of the effective resolution of interlaced video formats. For more information see: http://broadcastengineering.com/infrastructure/broadcasting_revisiting_kell/ Last accessed March 2009.

3.2 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.

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.

3.2.1 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.

1

Location

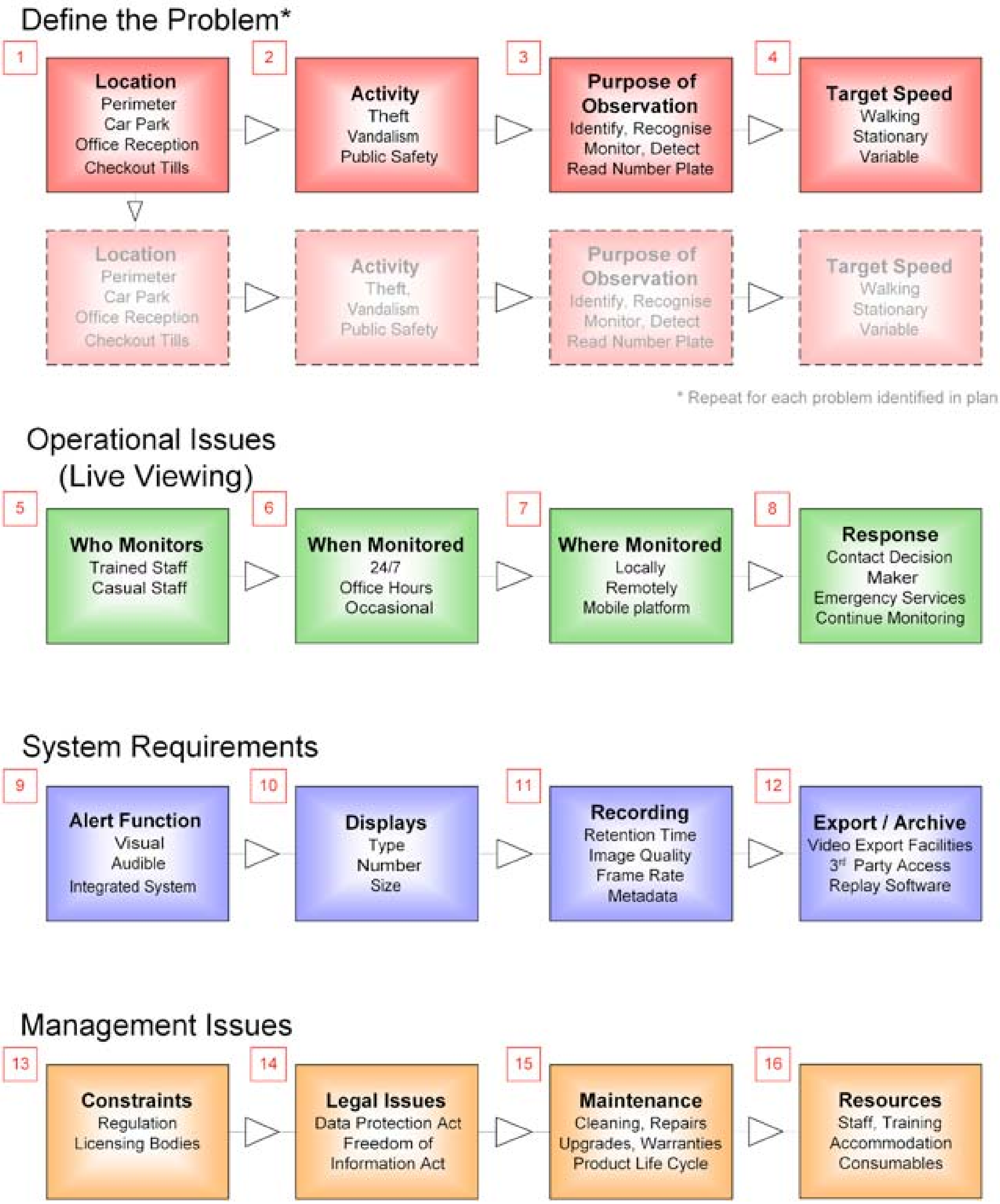
Where on your premises do you wish to monitor?

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.

Figure 5: Level 2 OR checklist for CCTV



2 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 five ‘levels of detail’ described in section 3.1 is most appropriate to your requirement.

You may wish to:

- **Monitor** a large area
- **Detect** individuals approaching a building
- **Observe** the actions of a group
- **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. So the cameras covering the car park would be set at the Detect (10%) level, but those at the entrance / exit would be set at the Identify (100%) level.

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 long exitless 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 (probably 6 or 12 fps). More information can be found in Section 4.6.4

3.2.2 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.

5 **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.

6 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.

7 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 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.

8 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.

It may well be helpful to stage scenarios in order to test the course of actions laid out in the operating procedures. This would ensure that staff are aware of the procedures and that the procedures themselves actually achieve what they set out to do. It is impossible in this document to set out specific test scenarios but these should mirror expected events as closely as possible.

A robust operating procedure not only aids the smooth running of the control room but is often invaluable in court when establishing integrity of evidence and dealing with legal challenges.

3.2.3 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.

9

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**
- There may be a requirement to prove that the system is functioning correctly and that nothing of interest occurred during the times it was not recording. This may be the case for instance in a custody suite where it may be necessary to prove no-one entered during specific times. One solution to this would be to set the system for a background record rate of 1 image per second during times when the alarm is not being triggered and an appropriately higher rate during alarm conditions.

> 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.

10 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 3.1), 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 4.5.1.

IP based CCTV systems often offer a **remote live monitoring** facility, over any internet enabled device such as a PDA, mobile phone or desktop computer. However, this usually operates within a constrained bandwidth, and so the transmitted live view often has heavy data compression, a reduced frame rate and reduced resolution, resulting in a significant drop in quality. Additionally there can be unacceptable latency added to control functions such as PTZ. It may also be the case that the images recorded locally are of higher quality than live view broadcast to the monitoring station. The transmitted image must be of sufficient quality to enable accurate interpretation of the events being displayed.

11 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 used for most CCTV applications and is still recommended by police. In practice, however, it may be appropriate to select from a sliding scale of retention times, which varies according to the likely severity of the incident that requires monitoring. For example, a town centre or other large scheme that may capture details of a serious crime or major incident should retain all footage for 31 days. This is because in a major incident it may be valuable for the police to be able to review the video of the days prior to the event as well as of the event itself. However, it may not always be necessary for the owners of small premises to retain all data for 31 days, as the events captured are likely to be less serious in nature, or are 'one-off' incidents. In these cases a minimum retention time of 14 days could be recommended, as this provides sufficient time for the authorities to attend the scene and retrieve the video in the event of an 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). It is extremely important to be aware of this trade-off between retention time and recorded image quality when setting up the system.

Choose an appropriate frame rate for each camera to record, based on speed of motion see Q4 and Section 4.6.4. 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 section 4.6.

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. However, it should be noted that the increased complexity that results from the use of some RAID configurations can cause problems should large volumes of data need to be retrieved quickly from the system, as it may not be easy to rebuild a series of hard drives once they have been removed.

12 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 videocassette 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. (As noted earlier this process can be more complex if the hard drives are from a RAID recording system).

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 publications 09/05 *UK Police Requirements for Digital CCTV Systems*, 21/06 *Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems* and *58/07 Digital Imaging Procedure v2.1*.

3.2.4 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).

14 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 Regulation of Investigatory Powers Act (2000)

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 and system managers 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.

15 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)
- Fitness for purpose checks (including who performs them, and what activities are undertaken)
- 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. For further information on system maintenance see the British Security Industry Association (BSIA) Code of Practice for the *Planning, Installation and Maintenance of Closed Circuit Television Systems* (www.bsia.co.uk).

16 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 & 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 ongoing training commitments)

4 Technical Guidance

4.1 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.

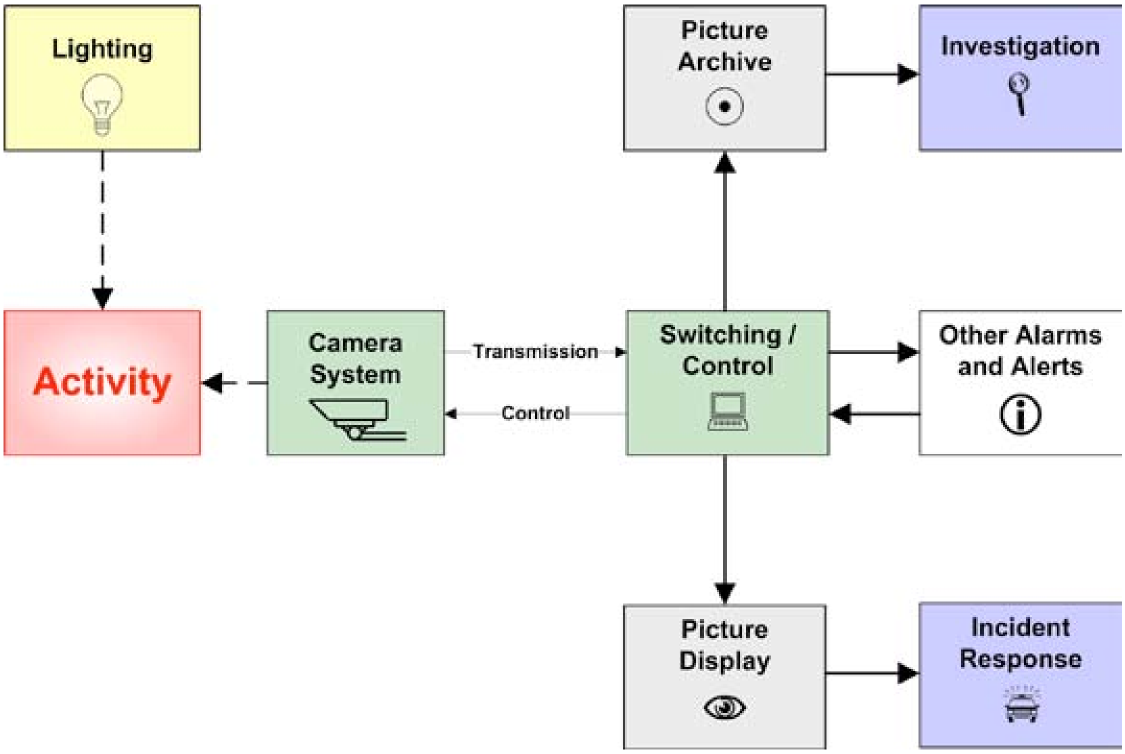


Figure 6: Constituent parts of a typical CCTV system

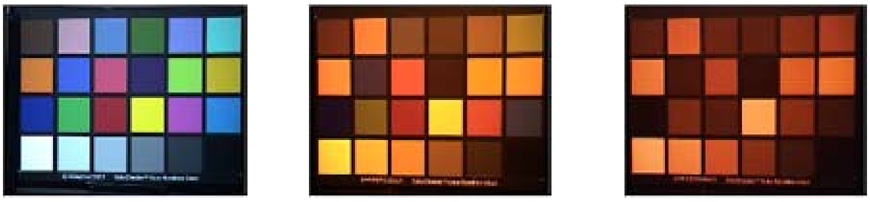
4.2 Lighting

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.

4.2.1 Light Levels

It is important to maintain a suitable light level over the scene being monitored. 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[2] figure 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 may have different levels of lighting / colour rendition. The same object may appear to be a different colour under different light sources, and in the case of low pressure sodium (yellow) lighting, nearly all the colour information may be lost, as shown in figure 7 below. An academic paper on this subject giving more detail is available[3].



Daylight | High pressure sodium | Low pressure sodium

Figure 7: Macbeth Colour Checker Chart® under different light sources, showing loss of colour information

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 (see section 4.3.6).

[2] Standard unit of luminance (lumens per square metre). 0.25lux equates to a full moon on a clear night, 400 lux being an average bright office.

[3] Colour Analysis and Verification of CCTV Images Under Different Lighting Conditions. R. A. Smith, K. MacLennan-Brown, J.F. Tighe, N. Cohen, S. Triantaphillidou, L.W. MacDonald. Proceedings of the SPIE Electronic Imaging, Image Quality and System Performance Conference 2008, vol. 6808 p.6808OY-1 – 6808OY-11

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. Bright light falling obliquely on the lens will cause **flare** which appears as a loss of contrast, causing colours to lack saturation and appear washed out, and can also lead to a loss of detail (figure 8a). 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, water surfaces or other shiny objects could also cause flare, as can car headlights.

This may not be noticed on cloudy days and only become apparent in bright sunshine, at night when supplementary lighting is turned on, or at certain times of the year. The addition of a lens hood to the camera will often help reduce the problem.

4.2.2 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[4] contrast ratio of minimum to maximum illumination within an artificially lit scene. In practice it is difficult for a non-specialist to measure contrast difference. A rule of thumb should be to observe the general guidance included below to avoid problematic lighting scenarios, and check in all lighting conditions that the required detail is present in both highlight and shadow areas.

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 an effect where a strongly backlit subject appears as a **silhouette**, too dark for any features to be properly distinguished, or the surrounding area is so overexposed that no detail is visible (figure 8b).

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. It is especially common on bright sunny days or at times when the sun is low in the sky. Overexposure can also spill into neighbouring regions causing loss of contrast and image detail over an area much bigger than that covered by the door or window.

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. Less obviously, most offices suffer from uneven illumination because the fluorescent light housings are designed to produce a pyramid shaped light output with the pyramid bases overlapping at desk height. This means that when a person walks under a light source their head area becomes significantly brighter and as they walk away this effect reverses. The impact of this problem is twofold; the person may appear significantly overexposed when under a light source, and secondly the camera

[4] i.e. no part of the scene should be more than 3 times brighter than the darkest area being observed. This is also true in reverse – no part of the scene should be less than 3 times dimmer than the brightest area being observed. This contrast ratio of illumination must also be matched by the dynamic range of both the camera and the display. Dynamic range is often expressed in values of several hundreds to one.

may not deal with this increase of contrast/dynamic range satisfactorily causing the automatic gain control (AGC) and other processing functions to activate, losing important scene detail. This problem can be combated by the use of a diffuser or increasing the number of light sources in high density pedestrian areas such as corridors where this may be an issue.

(a) (b)

Figure 8: (a) effect of flare and (b) silhouette effect

4.3 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 (internet protocol) and wireless technology, the method by which the camera transmits its images to the core system is also now an issue.

4.3.1 Lens / aperture

The lens which focuses the image onto the camera sensor is often purchased separately from the camera. If this is the case it is imperative to ensure that the two are compatible both in terms of lens mount and sensor coverage. The lens in combination with the camera sensor dictates the field of view produced by the system which ranges from wide angle to telephoto. A fuller discussion of this is in section 4.3.4. The aperture is a set of blades that physically control the amount of light that can enter the sensor. They function like the iris of an eye and are sometimes referred to as an iris. Some cameras have controls marked 'iris' or 'auto iris' that adjust the sensitivity of this function. It should also be noted that as the aperture gets wider the depth of field will reduce.

4.3.2 Shutter

Some CCTV cameras have electronic shutters that perform the same function as camera shutters. In a video camera without a user controlled shutter the sensor collects data for 1/25th of second in the PAL system or 1/30th of a second in the NTSC system.

An electronic shutter limits the time in which the sensor can build a charge, which is comparable in function to a mechanical shutter allowing light through to the sensor. Reducing the time the shutter is open will reduce the instances of motion blur (smearing) and/or camera shake but will require a corresponding increase in available light or a wider aperture. To an extent this increased light requirement can be managed by the gain controls without affecting the aperture, although the best solution is to increase the available light.

Conversely, increasing the time the shutter is open will allow for greater amounts of light to fall on the sensor and thus allow narrower apertures and increased depth of field, but will increase the chance of motion blur.

The limiting factors on available shutter speeds are the desired frame rate and the available light. The shutter must have time to operate within the duration of the frame capture, i.e. a camera operating at 25 fps must have a shutter duration of less than 1/25th of a second, but also allow enough light through for the sensor.

If the required shutter speed, gain and aperture combination cannot be achieved then thought must be given to adjusting the ambient light levels.

4.3.3 Sensor

The sensor is the device that actually ‘records’ the scene view, with current cameras having either CCD (charge coupled device) or CMOS (complimentary metal-oxide-semiconductor) sensors. Sensors have both different sizes, which can change the field of view, and different pixel densities which affect the resolution.

4.3.4 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 9). 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.

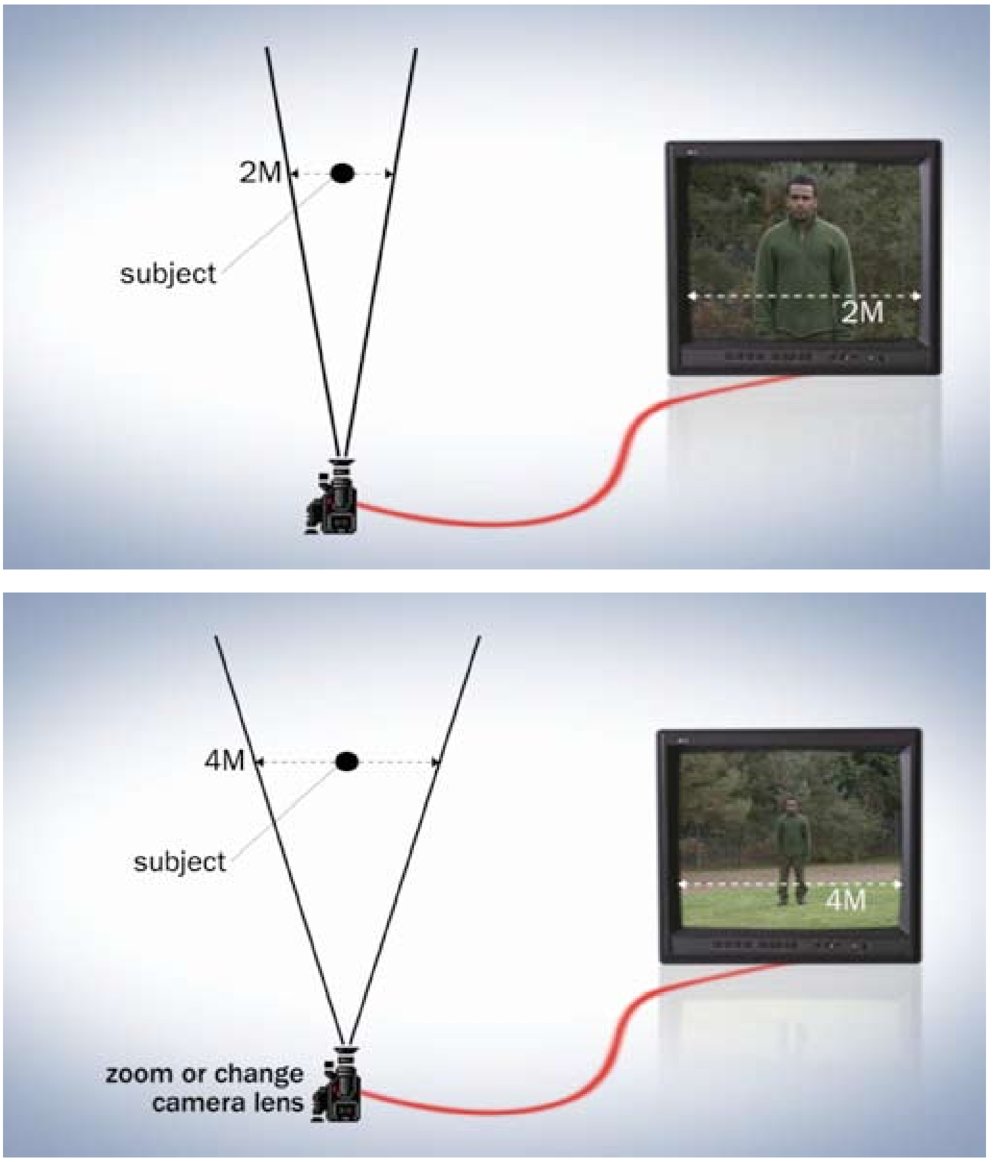


Figure 9: Effect on FoV of varying lenses with a constant distance

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.

As a quick reference, the information given in Table 3 shows how the subject size and distance from the camera determines the most appropriate combination of sensor element and lens. The subject height given refers to the vertical percentage of the screen occupied by a person of average height (1.7m). Image width shows the horizontal distance covered by the lens when a person occupies this specified vertical percentage assuming a picture aspect ratio of 4:3.

Subject Height		**100%**	**50%**	**25%**	**10%**
Image Width		**2.2m**	**4.5m**	**9m**	**22m**
Sensor element	**Lens (mm)**	**Subject Distance (m)**			
1/3"	50	26	50	105	250
	25	13	26	52	120
	12.5	6.5	13	26	60
	8.5	4.4	8.6	17.5	41
	3.5	1.8	3.6	7.2	17
1/2"	50	18	36	72	175
	25	9	18	36	85
	12.5	4.6	9	18	43
	8.5	3.2	6.2	14	29
	3.5	1.3	2.6	5	12
2/3"	50	13	26	51	120
	25	6.5	13	26	60
	12.5	3.2	6.5	13	30
	8.5	2.2	4.4	8.6	20
	3.5	0.85	1.8	3.6	8.5

Table 3: The subject distance required to achieve specified subject heights for different combinations of sensor size and lens focal length

Table 3 can be used in the following way. The required subject height will be specified in the operational requirement whilst the possible camera placements (and thus subject distance) will be dictated by environmental factors noted on the plan. Given both these constraints a suitable camera can be specified. For example, we need an image with a subject height of 50% from a camera aimed at an internal doorway and the most suitable mounting position for the camera is 6m away. If we look down the 50% subject height column of Table 3, we find two possible solutions, either a $^1/_2$” sensor and an 8.5mm lens or a 2/3” sensor and 12.5mm lens.

The lens focal length and sensor size combinations that are required to ensure a 1.6m high subject occupies 50% of the display is illustrated graphically in figure 10, over a range of subject-camera distances. It can be seen that more than one combination of lens and sensor could be used at certain distances.

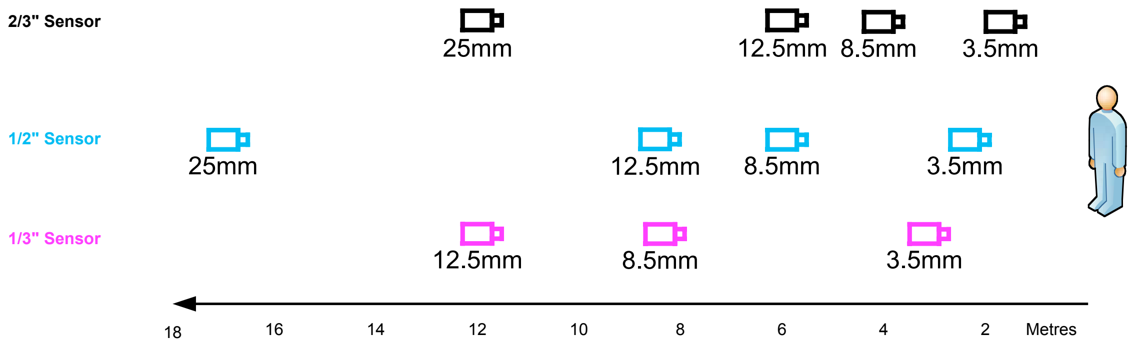


Figure 10: Sensor and lens combinations required to produce a subject height of 50% across a range of camera distances

> 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.

4.3.5 Pan-Tilt-Zoom Cameras

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.

4.3.6 Infra-Red Sensitive Cameras

As previously discussed (section 4.2.1) some situations may arise where pictures are required at night or in poorly lit areas. If light levels are low and supplemental lighting cannot be used then an infrared sensitive camera (day/night camera) may be required. This will usually function as a normal colour camera during the day, but in addition produce black and white images at night or under poor light conditions where a standard camera would not function. It should be noted, however, that infrared cameras will often provide poor colour rendition during the day, as shown in figure 11, though the addition of an infrared filter for daytime use will improve this. It is recommended that wherever possible ambient light levels are increased in preference to the use of infrared cameras due to the supplementary benefits of a well lit area.

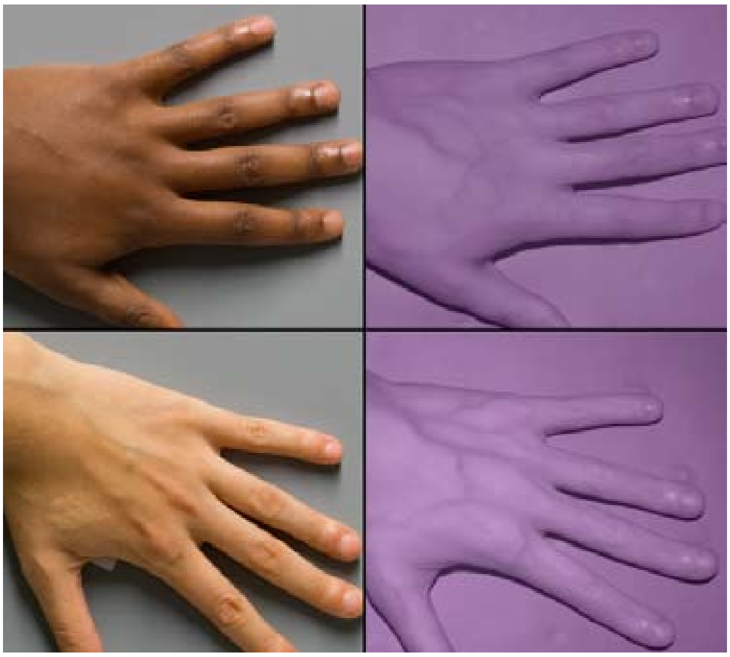


Figure 11: The effect of infra-red illumination on the reproduction of skin tone and scarring

4.3.7 On-board Image Processing

Within a camera there are usually a number of automatic functions designed to improve the output picture quality of the camera. These normally have a positive effect but occasionally the camera placement or camera setup can be such that the automated camera processing is detrimental, reducing the effectiveness of the camera.

Automatic gain control (AGC)

The automatic gain control has a function similar to that of the iris in the lens. It is an electronic modifier that alters the sensitivity of the imaging chip to ensure a good exposure level across a broad range of ambient light levels. The advantages of this system are that it is independent of the iris and complementary to it, thus allowing adjustment for scene brightness without changing the iris aperture and therefore the depth of field. On the negative side it can be slow to respond, taking up to two seconds to react to large changes in scene brightness, such as the sun coming out from behind a cloud, or lights switching on or off.

At low light levels it can also introduce significant amounts of noise into the picture. This can make it difficult to ascertain fine detail from a low light scene where a camera has significantly boosted its signal level using AGC.

White balance and colour

As humans we automatically colour correct what we are looking at in order to make objects we know to be white look white. For example, if you see an ambulance at night lit by low pressure sodium light it still looks white even though a camera would see it as orange. Cameras can be set to try to mimic this by assuming the brightest part of the scene is white and correcting the whole scene based on this information (auto white balance). Some cameras also have preset white balances for common lighting types such as fluorescent, tungsten, daylight etc.

4.3.8 Image resolution at the camera

Cameras come in a vast array of resolutions normally measured in TVLs (Television Lines – a measure of vertical picture resolution). Even now, when digital cameras are more often rated by their maximum number of pixels, the 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. There are several points to be borne in mind when considering the necessary camera resolution:

- If the camera hasn’t captured the data or the compression scheme has discarded it, it cannot be replaced.
- There is no point in capturing data at a significantly higher resolution than your recording and display system can cope with.
- Factors such as sensor array type and size, presence and type of anti-aliasing filter, etc. may have a serious impact on perceived sharpness regardless of actual pixel count.
- High resolution cameras can require proportionally brighter light sources.

Regardless of TVL rating analogue cameras output a PAL picture format (therefore a fixed 576 visible number of TVLs). Equally IP or digital cameras output a fixed pixel based format regardless of the camera sensor size or quoted TVL resolution.

TVL resolution is not directly comparable to a vertical pixel resolution. That is to say, a camera with a quoted resolution of 400 TVLs does not have 400 horizontal pixel lines. This problem is becoming less significant as digital cameras are quoted in a pixel resolution rather than in TVLs.

Any conversion from analogue video to digital video will invariably involve some loss of detail if the conversion process does not match the analogue native picture with the output digital format.

Furthermore, as display technology moves away from CRT based viewing towards LCD and other technologies the use of TVL figures becomes less sensible. All replacement display technologies report resolution in pixel figures, so if camera resolution is quoted in pixels, and video feeds are also in pixels then all the various specifications of the system components can be more easily compared.

4.3.9 The IP camera

IP (internet protocol) cameras collect image information in the same way as analogue cameras, but then encode and transmit the pictures digitally across a network, either a LAN (local area network) or the internet.

They have advantages over analogue cameras, firstly in the ease with which the pictures can be viewed remotely, and secondly in that they are not limited by the requirement to transmit the data at standard PAL resolution, and are thus capable of capturing higher quality images. An increasing variety of high resolution IP cameras are available, often referred to as megapixel cameras (for example a resolution of 1280 x 1024 is equivalent to 1.3 megapixels).

IP cameras can generate large volumes of data, and for this reason it is often possible to adjust the amount of compression that is applied before the video content leaves, thus reducing the volume of data that needs to be transmitted. However, this function should be used with care, and the camera optimised to give the best quality imagery for the available transmission bandwidth. A large sensor or a megapixel camera may be capable of generating very high quality imagery, but if poorly set up may in fact produce heavily compressed low resolution video (see section 4.6).

There is a limit to the maximum data output rate, due to the amount of processing required within the camera to correctly organise the information and prepare it for transmission. This can affect the performance of many megapixel cameras, seen in the fact that as the resolution of the camera increases the maximum frame rate decreases.

A further bottleneck is the IP transmission network. There is a finite bandwidth available within IP networks, constrained by a number of factors outlined in section 4.4, and this bandwidth may be shared by several cameras. It may therefore be necessary to adjust the data compression on camera (frame resolution, frame rate and level of compression) in order to stay within the available transmission bandwidth whilst ensuring that the overall video quality meets that stipulated in the operational requirement.

4.3.10 Camera placement

However carefully the camera/lens combinations and lighting levels have been considered, if the camera is positioned poorly then all the effort can be wasted. When specifying the camera placement the points below should be considered:

- 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 or though mechanical vibration. 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.
- When using the identify criteria it is recommended that clear space is left above the head in order to allow for variations in person height and discrepancies in recording systems.

> 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.

4.4 Transmission

The technology used for transmitting the video signal from one location to another is a key component of any CCTV system. There is an increasing array of options available, moving away from the traditional standard analogue coaxial cable solution, and so more thought now needs to be given to the choice of transmission method.

The most significant advance in recent years has been the development of IP based transmission. This is an approach for transmitting any digitised data in a robust and manageable way over a variety of link types. Its use in the CCTV field is growing, and often results in new approaches to solving problems.

As with any system design it is important that the specifier understands the implications of choosing one method over another. Both the physical and financial constraints of the intended CCTV system need to be considered. For example, is the CCTV transmission network a greenfield build, or will it be a retro fit? What level of link security is demanded by the application or the object of the surveillance?

This section provides an introduction to analogue and digital video signals, and an overview of wired and wireless transmission options.

4.4.1 Video signal type

Video can be transmitted and consumed either as an analogue or digital feed. Each video type can be converted to the other; however any conversions should be kept down to an absolute minimum to preserve video quality throughout the whole system.

The benefits of using analogue transmission are primarily that the technology is currently widely understood and widely deployed. As each video link has its own physical connection, fault finding is relatively simple. This video signal is mono-directional (simplex). This is a broadcasted approach, meaning that the video source is unaware of the status of any connected equipment. The transmission device, e.g. camera, will transmit the video information, usually as a PAL signal regardless of there being an attached receiver.

In its purest form a digital video stream is directly analogous to an analogue video stream, in that a single video stream is simply digitised (i.e. turned into 0s and 1s that can interpreted as the original video feed) and transmitted over a digital link. Thus the signal leaves one device and is received in another, in real time.

When considering streamed digital video it is important that the network is able to deliver the information within a tightly controlled timing window. If errors occur as the data crosses the network (e.g. suffers corruptions or is significantly delayed) the video stream can become corrupt. If data is lost or delayed there is no inbuilt mechanism that will request repeat delivery of corrupted sections. This means the focus needs to be on the timely and accurate delivery of information. Various networking processes are invoked to assist with this, such as the use of ‘Quality of Service’ (QoS) parameters to control the total network traffic or compression techniques that reduce the impact of small corruptions within the data stream like error detection and error concealment.

Digital video, however, can also be treated as a data file as opposed to a data stream. Transmitting a video file is where a video signal is captured and encapsulated as a single file. This file can then be transmitted across a network for consumption elsewhere.

When a data file is transmitted across a network the timely delivery is of much less importance than the accurate delivery of every packet. The file transfer approach has in-built mechanisms to detect errors and request damaged or missing packets to be re-sent. Through using this approach the completeness of the file can be guaranteed. However the delivery time cannot as it will be dependent on other traffic on the network, available bandwidth and errors observed across the link.

There are many transmission options available to a system installer to provide appropriate connectivity across a digital network. The simplest is the use of an Internet Protocol (IP) camera over a basic network. Whilst the creation of an IP network is relatively straightforward, a full understanding of how the video is transmitted requires an in-depth knowledge of networking infrastructure and protocols, which is beyond the scope of this document. It is recommended that a network specialist be consulted early in any system development if a data network is to be used.

As most offices and a lot of homes have at least a rudimentary digital data network for sharing information and internet connections, CCTV systems both large and small are increasingly making use of this existing network. Care should be taken to ensure suitable network bandwidth and if appropriate, network security.

4.4.2 Wired transmission

The most common form of an analogue wired connection is a coaxial cable. This is generally terminated with BNC connectors for compatibility. Standard coaxial cable (RG59) is suitable for transmission links of up to around 200 metres, although larger diameter cable (such as RG6 or RG11) will give an increased range.

Another option for wired video transmission is a twisted pair cable. Common examples are Cat-5 and Cat-6 cables, which comprise four twisted copper wire pairs, and are used for analogue or digital transmission.

Wired digital transmission systems come in a variety of different standard speeds. 10BASE-T is an increasingly outdated infrastructure that supports transmission speeds of up to 10 Mbits/s. (The use of the ‘T’ suffix here denotes twisted pair cable.) This was superseded by 100BASE-T which supports transmission speeds of up to 100 Mbit/s. The latest amendment is Gigabit Ethernet or 1000BASE-T supporting 1Gbit/s transmission. 10 Gigabit Ethernet (supporting 10 Gbit/s transmission) standards have been ratified, and 100 Gigabit Ethernet transmissions are being developed.

The actual transmission speed achieved is very much dependent on several factors: the output rate of the transmitting device, the network infrastructure

(Cat-5/6, mains cabling, fibre links, etc), the network setting (e.g. QoS, transmission protocols) and other network traffic levels.

4.4.3 Wireless transmission

This has been a significant growth area, and most CCTV system suppliers offer some form of wireless transmission link, either analogue or digital. On a small scale, wireless links that are designed to link a single video channel to the CCTV system are becoming more common in the marketplace. These range in complexity from an insecure short hop analogue radio frequency link to remote access over the mobile phone transmission network. A CCTV specifier should consider the needs of the viewer / system operator when designing the transmission network and appropriate network security. The main technology types have been summarised in Table 4.

Link Type	Transmission Distance	Transmission Frequencies	Link Bandwidth	Comments
Analogue RF	~30 m indoors ~100 m + Outdoors (Non Line of Sight. Line of Sight can be significantly greater)	2.4 GHz / 5 GHz (Unlicensed bands) Other frequencies can be used depending on spectral allocation and licensing details.	Dependent on installation specifics	Simple operation described here. More complex solutions can be offered.
'Wifi' (IEEE 802.11)	~30 m indoors ~100 m Outdoors (Non Line of Sight)	2.4 GHz / 5 GHz (Unlicensed bands)	Up to 74 MBits/s (802.11n) Up to 19 MBits/s (802.11g)	Generally not suitable for long range transmission. Range and throughput is heavily dependant on signal power at receiver.
Mobile WiMax (IEEE 802.16e)	Up to 50 km (Line of sight)	Depends on installation. Configurable to both open and licensed frequencies	Up to 70 MBit/s	System either delivers long transmission distance or high transfer rate, not both. Developing technology
2G GSM (Global System for Mobile Communications)	National/International assuming system is within cell coverage (Inner City ~1/2 mile from cell site Rural ~ 5 miles from cell site)	~800-950 MHz or ~1.9 to ~2.2 GHz (Limited to cellular phone licensed bands)	14.4 kBit/s	More suited to speech and very low bit rate video or stills transmission. Requires a cellular service provider. Performance is dependant on carrier load, atmospherics and infrastructure provision.
3G HSDPA (High speed downlink packet access)	National/International assuming system is within cell coverage (Inner City ~1/2 mile from cell site Rural ~ 5 miles from cell site)	~1.9 to ~2.2 GHz (Limited to cellular phone licensed bands)	Currently up to 14.4 MBit/s Developments in technology will increase throughput	Requires a cellular service provider. Performance is dependant on carrier load and atmospherics and infrastructure provision.

Table 4: Wireless transmission options

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 super-size the displays may not necessarily be money well spent.

4.5.1 Display type

In simple terms displays come in two main forms, the CRT (Cathode Ray Tube) or the modern flat panel variety (less commonly rear projection systems.) The flat panel displays can either be LCD (liquid crystal display) or plasma. A summary of display technology is shown in Table 5.

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 panels. Flat panels tend to suffer from an effect known as motion blur, which can make 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.

There are, however, many new flat panel display technologies in development that aim to retain the benefits of the current screens yet provide the image quality associated with CRT. LCD screens are improving, particularly in terms of viewing angle and overall size.

Type	Pros	Cons
CRT	Best attainable picture quality Robust technology Much equipment was designed for reproduction on a CRT Low cost	High power consumption High heat generation High space requirements Manufacture largely discontinued
LCD	Compact and light Low power consumption Wide range of screen sizes available High resolution Low black level Low cost	Poor movement reproduction Possibly restricted viewing angle Lower image contrast
Plasma	Slim design, wall mountable High resolution Larger maximum size than LCD Wider viewing angles than LCD	Fragile High power consumption High heat generation High black level Expensive

Table 5: Summary of display technologies

- **Size**: Large size and high resolution flat panel displays can be effective as matrix displays for multiple cameras. High screen resolution will not improve the capture resolution.
- **Heat**: The amount of heat a unit generates becomes significant as the size of the facility increases and can affect not only operator comfort but also machine efficiency.
- **Colour:** Modern displays of all types have similar quality colour reproduction.
- **Black level**: The 'black level' of a screen refers to how well the screen performs in a well lit environment. The lower the black level the better the screen works in higher brightness environments.
- **Burn in**: Most screens can suffer from 'burn in' or image burn, where, if the same background is displayed continuously for a long period, this can leave a permanent mark on the screen. Plasma and CRT screens are particularly susceptible to this.

4.5.2 Control room ergonomics

However much time, effort and expense is put into the correct installation of the CCTV cameras and lighting, most of it will be wasted if the viewing area is poorly designed. The number of monitors that an operator has to view and their relative size and distance from the monitoring station are key factors in effective monitoring of CCTV. Whilst an in-depth treatise on control room ergonomics is beyond the scope of this document a few useful guidelines on the issues involved are given below.

Viewing conditions

All the effort spent selecting screens and setting viewing angles will be wasted if attention is not paid to the lighting in the viewing area. Harsh directional light from natural or artificial sources that causes glare on the screens or unnecessarily raises the overall lighting level in the viewing area, will drastically reduced the perceived image quality of the monitors. If an externally facing window is required in the viewing area then ideally it should not face either the operators or the monitors.

Display design and layout

The relationship between the size of the display and the viewing distance is critical. Several different values are given for optimal screen height at a particular viewing distance but most of these fall in the range of 3-5 times the screen height[5] or 2-5 times the screen diagonal. It should be noted that these figures are for 4:3 aspect ratio images and in the case of multiplex displays refers to the displayed image height not the screen height.

Various monitoring methods for a control room exist including:

- Multi-screen multi-view video wall approach where as much information as possible is displayed at any one time. If continuous

[5] Recommendation ITU-R BT.500 "Methodology for the Subjective Assessment of the Quality of Television Pictures" published by the International Telecommunication Union Radiocommunication sector is the de-facto standard for viewing environments used by the broadcast television industry.

monitoring of an area is required and/or automated alarms are inappropriate then this is often the best method. The allocation of video feeds to specific monitors should be carefully thought out to ensure those requiring close attention are positioned in the most convenient locations. This video wall approach is usually complemented by spot monitors on each operator's workstation, from which a selected camera view can be monitored more closely. It is often also desirable to add the facility for an operator to send a feed of particular importance to a central monitor on the video wall.

- Blank screen method, whereby the monitor or monitors are blank until an alarm (VMD, door alarm, fire alarm etc.) is triggered whereupon the relevant camera feed is shown on the monitor. This type of scenario works well when the area to be monitored is adequately covered by supplementary alarms, and can allow the operator to engage in other duties apart from CCTV monitoring. Care must be taken with this approach to ensure that sufficient monitors are available to monitor a serious situation with multiple alarm events.
- Combinations of the above are most usually found, with areas requiring highest supervision constantly being displayed and with alarms causing their attendant video feeds to take priority on the display(s). This may well be the case with, for instance, small retail outlets where the single screen is usually split to display feeds from the shop floor cameras, changing to a single view of the back door or loading bay if the bell is rung or the alarm triggered.

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

4.5.3 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? Ensure that the lens or lens / camera combination is of sufficient quality for the task in hand.

Detail – Is there enough to identify objects? Check that image quality is not compromised by trying to achieve a large FoV at the cost of image detail, and that lighting levels permit a useable depth of focus. If necessary break the scene into smaller sections.

Colour – Is it natural? Is it necessary? If accurate colour reproduction is important then ensure the lighting is of sufficient quality and quantity to allow the cameras to achieve this.

Artefacts – Are there elements in the image that should not be there? And if so are they obtrusive? If this is the case then depending on the artefact, either the amount of compression needs to reduced or the camera/lighting placement needs to be addressed.

4.6 Recording

In many cases CCTV systems are used 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 images 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 high 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 this should become less of a constraint when specifying a system.

4.6.1 Compression

It is both impractical and unnecessary to store all the information generated by a CCTV camera and various schemes exist to reduce (or compress) the amount of data stored. Three main things can be altered in order to control volume of data stored:

- The interval between the images that are stored, or temporal compression.
- The number of pixels used to make up the image, or spatial compression
- And finally the amount and efficiency of the data storage, or data compression

Some or all of the above are adjustable using the settings available on CCTV systems. The first and most obvious is the interval between stored images, often referred to as the *frame rate,* which is considered in section 4.6.4.

Adjustments to spatial compression (i.e. resolution) are normally only available on high-end digital cameras, though some recording systems and analogue cameras offer various CIF image formats (where CIF stands for Common Intermediate Format, and includes QCIF 176 x 144 pixels, CIF 342 x 288 and 4CIF 704 x 576).

Data compression can be the biggest cause of image quality loss with digital video recordings, especially when used to excess. 'Lossless' data compression is a technique that reduces the size of files without affecting 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).

Another method of data compression used specifically 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 (Intra-coded frames), and these are coded separately. Between the I-frames are a series of predicted P-frames and bi-directional predicted B-frames.

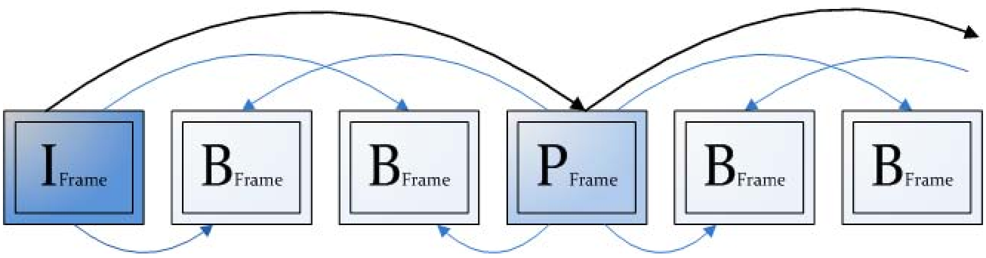


Figure 12: Different frame types in compressed video

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 or panned / zoom shots. Some CCTV systems use interframe compression, some do not.

One of the largest problems to date with digital CCTV imagery has been that there is no single standard encoder/decoder (codec) used to both generate the compressed footage and decompress it for viewing. As video compression technology is constantly developing, there are many approaches to compression. Some methods are widely employed, but more often a proprietary version of a codec is required to view the recorded content.

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 artefacts are less obvious and the final file sizes are smaller than those for images compressed via DCT to an equivalent quality level. Figure 13 describes some of the different effects of Wavelet and DCT compression methods on an image.

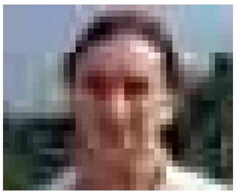
Figure 13: Effects of compression on image quality

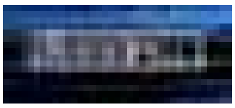
DCT Compression

Blocking is visible in the sky and colour changes exist on the boundaries

Very clear blocking and slight ambiguity with some of the characters

Blocking and blurred detail is visible in both the sky and trees





Low resolution images and heavy DCT compression provides images of very little use
Significant blocking and very little detail remains in the image

Live View Image (High Resolution)

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.

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.

Recorded Image (Low Resolution)

Wavelet Compression

Image is generally smeared with a loss of detail throughout

Good retention of character definition and image shape

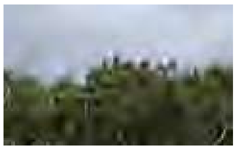


Image is smeared with very little detail in both sky and trees

Low resolution images and heavy Wavelet compression provides images of little use
Extensive blurring ensures little detail remains

4.6.2 Effect of compression on quality

Though the images in figure 13 show extreme examples of compression, the levels shown are often found in digital CCTV systems. It is worth noting that high resolution images that are highly compressed would show similar image quality to lower resolution images with less compression. Therefore there is no point in paying for expensive high resolution cameras if you are not prepared to invest in sufficient storage space and instead make use of heavy compression.

Equally, frame rate or temporal compression should be set as required by the operational requirement for that camera, not reduced to a level dictated by storage requirements.

4.6.3 Cascaded compression

In some CCTV systems a video stream that has been compressed by one codec is then re-compressed using a second (different) codec, for instance when a 'Convert to AVI' output option is selected. This can mean that compression artefacts generated by the first codec are preserved and indeed sometimes exacerbated by the second codec, drastically reducing image quality. For these reasons cascaded compression should be avoided at all costs and output generated by an 'export to AVI' or similar function should be checked very carefully.

4.6.4 Frame Rates

With PAL 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 6-12 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 6, probably 12 fps), but if the target is slow the frame rate could be reduced to optimise storage.

One method of reducing the storage overhead is to use an archiving strategy that allows the frame rate to be adjusted either 'on the fly' or automatically within the archive.

In the 'on the fly' method the recorded frame rate has two settings. The first is the base frame rate. This is generally low, often in the region of 1 to 6 fps. If the camera is triggered the recording rate is increased to a faster rate, in the region of 12 to 25 fps. The triggers can be external system elements, e.g. PIR sensors, motion detection within the camera / CCTV system or interaction by an observer.

Alternatively, where a system is installed to monitor frequent activity, but the activity is archived for a number of days it may be possible to use an automated decimation process. In this method the CCTV is recorded at a high frame rate as the base level. After a fixed period of time (which must allow for adequate detection and subsequent extraction of video to permanent storage) the frame rate is automatically reduced by deleting frames at regular intervals. It might then be beneficial to reduce the image resolution, and / or to increase the amount of compression applied, to gain further reductions as long as the reduced quality stored is still fit for purpose.

4.6.5 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 6.

Variable	Frame Size	Frames Per Second	Number of Cameras	Operational Hours	Retention Period
Typical Range	5kB – 50kB	1 – 25	1 – 16+	1 – 24	24 Hours – 31 Days

Table 6: Factors affecting the storage capacity required for a CCTV recorder

Frame 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 4.6.1 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 specific to 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 operational requirement 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 the 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 x T = 30 mins
Number of triggered frames generated = 30 x 60 x 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 x 60 x R_S = 84600

Total number of frames generated per day = 21600 + 84600 = 106200

Average frame rate per second = 106200 / number of secs in 24 hrs
= 106200 / 86400 = 1.2 fps

Number of cameras – This is the number of recorded cameras used for the whole system under consideration, as specified in the operational requirement.

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

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:

$$\left(\frac{\text{Size x fps x C x Hours x 3,600}}{\text{1,000,000}}\right) \text{x } T_R = \text{Approximate Storage Requirement (GB)}$$

Where:

Size = Image size in kB
fps = Images per second
C = Number of cameras in the system
Hours = Total number of operational hours in a 24 hour period
T_R = 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 of 20kB per frame. 12 fps per camera 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. The storage capacity is given by:

$$\left(\frac{20 \text{ x } 12 \text{ x } 8 \text{ x } 24 \text{ x } 3{,}600}{1{,}000{,}000}\right) \text{x } 31 = 5142 \text{ (GB)}$$

As can be seen this represents a large 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.

Example 2

A retail outlet is installing a small CCTV system to monitor the access points (windows and doors) whilst the shop is closed. The image frame size has been to set to a 'medium' value (10kb), 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. The storage requirement is given by:

$$\left(\frac{10 \times 2 \times 6 \times 12 \times 3{,}600}{1{,}000{,}000}\right) \times 31 = 160 \text{ GB}$$

5 System Validation

5.1 System Design Specification

The primary objective of CCTV system design is to ensure the operational requirements are met. A design specification should be developed to include equipment specifications for each item that comprises the CCTV system, identifying the particular functions to be performed by the equipment and the performance criteria to be met.

Where the specification has been supplied by the contractor, it should be checked to ensure that it addresses all of the points raised in the operational requirement. A more detailed validation should be performed to ensure that the specified equipment is capable of meeting the performance criteria required by the operational requirement and the contractor should assure compatibility of the components. Relevant calculations can be carried out to demonstrate the capability of the equipment to meet the performance criteria.

5.2 System Commissioning

During the commissioning of the CCTV system, it is important to verify that all of the functions specified in the operational requirements have been provided by the installed system, a user manual has been supplied and that the system has been set up correctly.

A documented system test procedure should be developed, based on the design specification, and this should be used to verify all the functions and the performance of the CCTV system. Any deviations from the expected performance should be noted. In particular, tests should be carried out to verify:

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

Some sample video should be recorded and exported from each camera. This can be used as a reference of image quality and camera field of view during future system maintenance operations and will highlight any change or degradation that occurs in the system over time.

5.2.1 Live Product

It is important to ensure 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 read a number plate or otherwise monitor the target as set out in section 3.1). The live or on-screen view should be checked for the following:

- Does the picture provide a suitable frame rate for the activity being monitored?
- Is the picture of sufficient quality for the operator to effectively perform their monitoring tasks?

5.2.2 Recorded Product

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. The recorded picture should be checked for the following factors:

- Does the picture provide a suitable frame rate for the activities to be reviewed effectively?
- Is the picture of sufficient quality for the reviewer to effectively perform their tasks?
- Is the imagery viewable by anyone who needs to have access to it in order to perform their role?
- Can the content be extracted from the system simply, in sufficient volume and in a suitable format?

5.2.3 Test Target

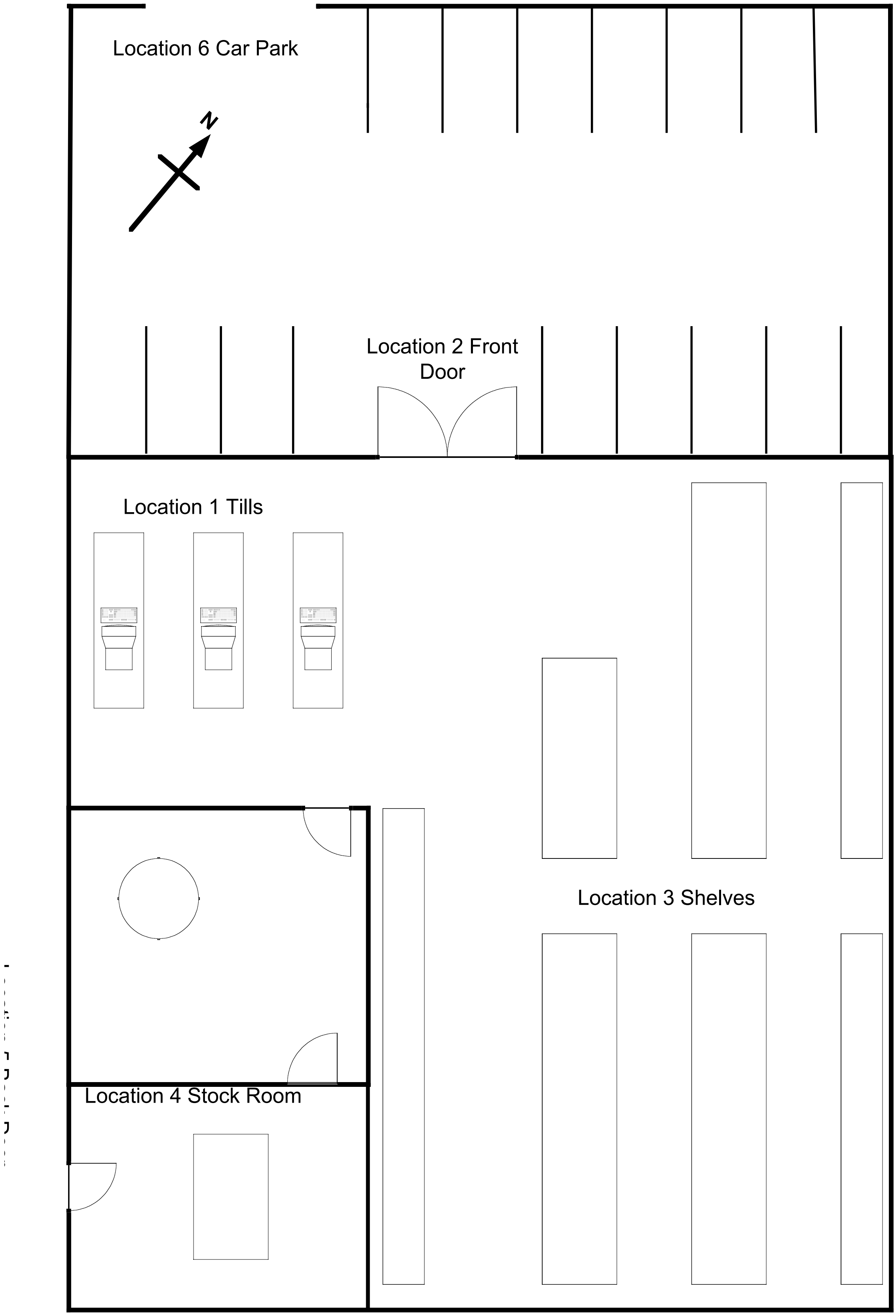
A suitable test target should be employed that contains the required level of detail to test the operational parameters of the system. Please refer to the HOSDB website for up-to-date information on suitable test targets and testing regimes.

5.3 System Auditing

To get best value from a CCTV system its performance should be monitored and benchmarked regularly as part of a documented system audit. This process could be carried out alongside the routine maintenance cycle. If regular performance reviews are appropriately recorded it should be possible to observe any degradation of performance, or any requirement non-compliance.

The camera view should be checked periodically as required by the maintenance contract to ensure that the view is as specified in the original operational requirement. Camera housings might have moved, fixings may corrode or other elements may be added to the scene to obscure the view. Further guidance is available from the BSIA (Form 120, Guidelines for the Maintenance and Servicing of CCTV surveillance systems). A useful auditing tool is to undertake a periodic system walk round. This activity should include every camera in the system, and at each camera identify the useful field of view, point of focus, depth of field and efficiency of alarms.

Appendix A: Example Completed Site Plan



Location 1: Tills	
Activity:	Theft, Assault, Fraud, Customer flow
Purpose of observation:	Identify
Target speed:	Fast (i.e. Not scanning items, 'Dipping' in till)
Camera:	Narrow field of view, lighting OK may need one per till?

Location 2: Front door	
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.)
Purpose of observation:	Identify
Target speed:	Walking pace
Camera:	Narrow field of view, lighting OK (inward facing)

Location 3: Shelves	
Activity:	Theft
Purpose of observation:	Recognise
Target speed:	Walking – but shoplifting activity occurs quickly, so high frame rate required
Camera:	Medium field of view, lighting OK

Location 4: Stock room	
Activity:	Theft
Purpose of observation:	Recognise
Target speed:	Medium
Camera:	Wide field of view, lighting OK

Location 5: Back door	
Activity:	Theft, Break in, Delivery
Purpose of observation:	Detect / Recognise
Target speed:	Walking / stationary
Camera:	Wide field of view, needs extra lighting

Location 6: Car park	
Activity:	Theft, Assault, Damage, Accident (public safety)
Purpose of observation:	Detect / Recognise
Target speed:	Walking / stationary
Camera:	Wide field of view, needs extra lighting

Appendix B: Blank OR Checklist

Level 1 OR

Statement of problem	Stakeholders	Risk Assessment	Success Criteria

Level 2 OR for CCTV

	Location	Activity	Purpose of Observation	Target Speed
Define the Problem				

Define the Problem	Operational Issues	System Requirements	Management Issues
	Who Monitors	Alert Functions	Constraints
	When Monitored	Displays	Legal Issues
	Where Monitored	Recording	Maintenance
	Response	Export / Archive	Resources

Home Office

Scientific Development Branch

ISBN: 978-1-84726-902-7

Home Office Scientific Development Branch
Sandridge
St Albans
AL4 9HQ
United Kingdom

Telephone: +44 (0)1727 865051
Fax: +44 (0)1727 816233
E-mail: hosdb@homeoffice.gsi.gov.uk
Website: http://science.homeoffice.gov.uk/hosdb