CPNI
Centre for the Protection of National Infrastructure

CCTV FOR CNI PERIMETER SECURITY

A GUIDANCE DOCUMENT

November 2014

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

The text of this publication may not be reproduced, nor may talks or lectures based on material contained within the document be given, without written consent from the Centre for the Protection of National Infrastructure (CPNI).

Aim

The aim of this document is to provide guidance to a CNI site on the selection, installation commissioning and effective use of perimeter CCTV to achieve one or more of the following:

- Detect an intruder within a reasonable time frame
- Verify an alarm from a Perimeter Intruder Detection System (PIDS)
- Provide support to a guard or security force
- Provide evidence suitable for use in court

Contents

Principles

Where it has been deemed necessary that a site be protected by CCTV, the following principles should be followed:

If the CCTV is being used as a detection system, viewed or verified by a human operator, the camera should be mounted in such a way that it will provide an image of an intruder which is a minimum of 10% of the screen height. This is the limit of the human vision system and no matter how good the quality of the image a human cannot detect an intruder that is less that 10% screen height. If using a quad screen (4 images on one monitor) this will be 20% screen height (10% height of each image on the screen).

Pan-Tilt-Zoom (PTZ) cameras may be used to supplement fixed cameras predominantly for tracking purposes. PTZ may be used to investigate alarms, but it must be remembered that if a camera is being used to examine a specific area, it is not covering the area it was covering pre event. Is that area being covered by another camera?

CCTV can operate in three real time modes:

- Monitoring by operators;
- Monitoring triggered by alarm activation;
- Monitoring by Video Analytics.

If the first mode is used, the cameras on the perimeter should present the image to the operator in a manner such that any attempted intrusion or hostile activity is detected. A balance must be struck between how long each camera image is on screen and how many times that image is displayed within a given time frame. If the perimeter is protected by other CPNI assured physical security measures (e.g. PIDS or Fencing), to maintain full security of the site, each camera image should be actively viewed at least once every FIVE minutes. By doing this, no area of the perimeter will be unmonitored, either by technology or human detection. Some scenes may need more frequent viewing due to operational business needs, cluttered or busy scenes or vulnerable points.

Modes 2 and 3 are often combined with mode 1 to verify an alarm activation. If modes 2 and 3 are used, recorded footage to show the lead up to and immediate time after the alarm (pre and post alarm footage) should be immediately displayed to the operator. This allows the operator to determine the cause of the alarm and any follow up action required. A second monitor should display the live view of the alarm area. At this point PTZ cameras may be used to track intruders until a response force can be deployed. In all modes, in order to maintain any intruder at 10% screen height, it will be necessary to use multiple cameras with interlocking fields of view.

Modes 2 and 3 can be used in a blank screen configuration thereby the monitor only becomes active when an alarm is triggered. Blank screen technology will not provide active monitoring and should only be used as a detector. If blank screen technology is to be used as a detector, separate consideration should be given to active monitoring. If blank screen monitoring is used and there is no alternative active monitoring, reviewing each section of the perimeter once every five minutes, an intruder may be able to carry out a very slow attack and breach the perimeter without detection.

Video recording is important for incident review and for evidential purposes. Any recording system must be able to provide usable and useful imagery for the whole life of the recording or there is little point storing the data. The use of compression techniques should be kept to a minimum as this will quickly reduce the quality of the imagery. Any recorded imagery should be checked at differing intervals after the recording date to confirm it is still of sufficient quality to meet the operational requirement.

> CCTV systems should always be used in conjunction with other security measures and with lighting commensurate with the requirement and aims of the system.

A well trained and motivated security team is vital for the efficient operation of any CCTV installation. Any situation detected by the CCTV security operators should be responded to in a timely and appropriate manner to maximise the deterrence effect of the CCTV system.

Any CCTV installation should be underpinned by a clear and well thought out Operational Requirement. This will be the measure as to whether the system does what it was designed for.

Five Minute Rule

CPNI recommends that all CCTV images covering the perimeter of a site including access points are **reviewed every five minutes**. This figure is derived from the CPNI physical attack methodology and testing standards. The time required to view each scene will depend on the quality of the image, how cluttered the scene is among other things. To demonstrate an achievable coverage, averaging five seconds per image, each operator can monitor 60 cameras, excluding breaks and other duties. All other cameras used to verify alarms should be monitored routinely.

Installing a CCTV System

When planning a CCTV installation, there are a number of considerations:

- Operational Requirement
- Equipment Selection/Siting
- Transmission Method
- Lighting
- Maintenance
- Video Analytics
- Thermal Imaging
- Human Factors
- IP Systems

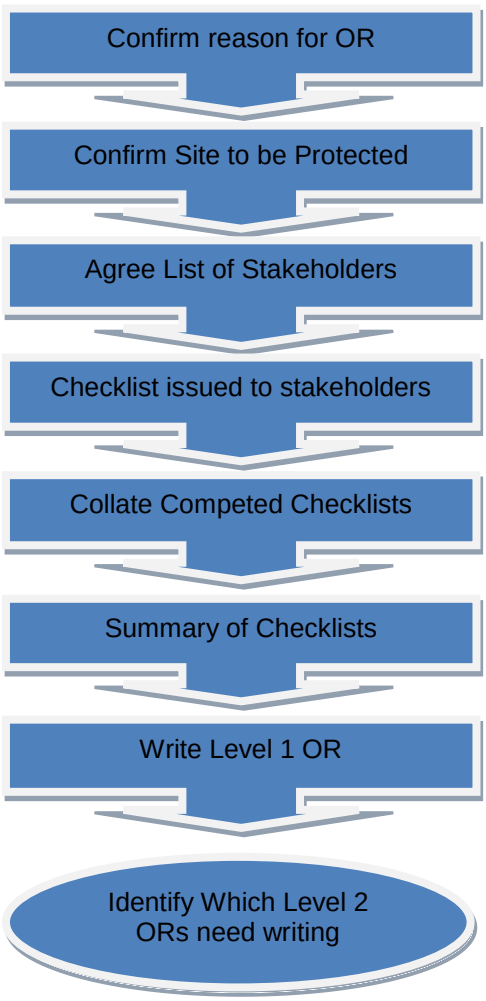
Operational Requirement

Put simply the Operational Requirement (OR) is a statement of security needs based on a thorough and systematic assessment of the problems to be solved and the hoped for solutions. What do I need my system to do?

The Level 1 OR provides a statement of the overall security need and includes the site to be considered, asset description, perceived threat, and consequence of compromise, perceived vulnerabilities, and success criteria.

Level 2 ORs follow on from the completed Level 1 OR and address individual security measures (fences, CCTV, control of access etc.) in a similar fashion to the Level 1 procedure, but which together provide the basis for a fully integrated security solution. Checklists are given, in this document, for a wide range of Level 2 ORs. Not all of these will be needed for every site.

Level 1 Operational Requirement



There are a number of factors to consider when drafting the OR.

It is important that all **stakeholders with an interest** in operational security are consulted and involved. Good communication at the correct level will result in a more efficient, fit for purpose system. Identify those stakeholders whose priorities may be considered the most important and how any conflicts can be resolved.

Identify any assets or key points that will require particular security surveillance. These may be human, (a gatehouse or reception for example), physical, (emergency gates or unmanned entrance/exit points) together with their value; human, financial, operational, political.

In order to protect a site, the **threat must be understood.** Identify what or who you are defending against. State the perceived threat and the likely abilities of the attackers. This may steer you towards a particular analytics system or suggest camera locations for example.

Set out the **consequences of compromise**. State what these are in financial terms, operational effectiveness, political impact, etc. Identify what would be the possible outcome if an intruder gained access to the site. This is effectively the justification for installing the perimeter CCTV system and may well dictate the budget!

Identify **areas of particular vulnerability**. Ensure that any points on the perimeter which may be considered as weak points are listed. This may include the key points suggested above as well as areas of remoteness or a fence line near residential areas or railway lines as examples. There are many others which will vary site to site. These areas may require special consideration when siting plans are drawn up.

Understand and then state, **the criteria for success**. What requirements are to be achieved in order that the CCTV is deemed to be fit for purpose.

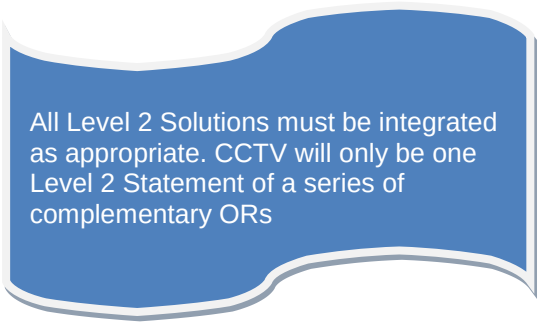
Recognise and document any other factors which may need to be taken into account when designing and installing a CCTV system. Examples might be the proximity of neighbours. This could have an impact on lighting or limit where you can site cameras. Another might be the time required for a response force to be able to reach a point of attack. This point might influence the type of camera installed in a particular location. The local environment could play a part; extensive vegetation along the fence line will affect video analytics and hide an approaching intruder if cameras are not placed correctly.

This is not an exhaustive list of the types of things that should be addressed when planning a CCTV installation. Each site will have its own peculiar and unique characteristics and problems which will require consideration

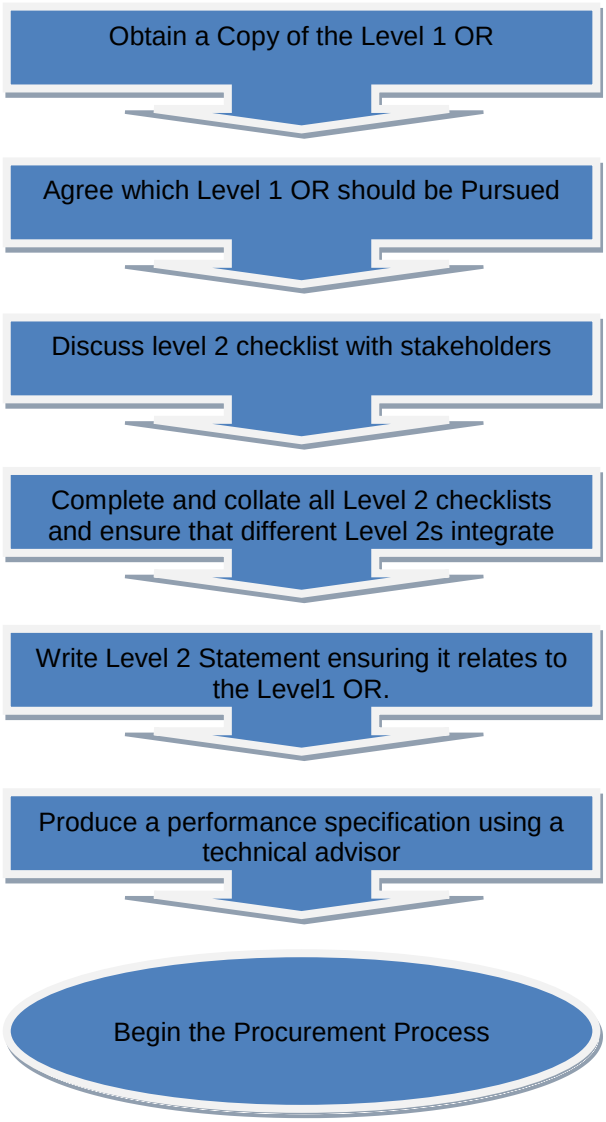
Level 2 Operational Requirement

The Level 2 OR statement is a written summary of the information collated from the checklists and not a specification document. It may be supported by completed checklists if felt useful. This statement should always be accompanied by a copy of the Level 1 OR statement so that the relationship with the identified security problem is clear.

The single statement should cover all the measures considered. This is to ensure that the performance specification will address fully the integration of measures to produce an effective solution.



The Level 2 OR statement and completed checklists provide the detail for the designer to produce a performance specification covering a range of possible solutions. Performance specifications will state parameters for proposed systems that stakeholders can compare with the ORs and make an informed decision on the security risk management for their site or building before moving forward to the procurement process.



A complete guide to the Operational Requirement process is available on the CPNI website in the Physical Security Section

Only by completing a level 1 and 2 Operational Requirement can you decide if you require CCTV and what CCTV system you require

Equipment Selection

There are a number of things to take into account when considering what type of equipment you may require in your perimeter CCTV installation. Not least, you should consider what other systems you will be using in your integrated security system. This could include lighting, PIDS and human patrols or guards. Lighting will be discussed later.

Things to consider:

What type of footage do you want?
Do you require evidential footage?
Will including colour information be important?

Will you be recording?
At what speed does the scene change?

What sort of lighting will you be employing?
Will the lighting support a guard response?

Cameras

Analogue or Digital?

Analogue and digital cameras are different. As to which is the best, it depends upon the requirement. In certain circumstances, analogue cameras are entirely sufficient. Other applications will require the added functionality of digital technology or networks.

Analogue	Digital
Set Format	Many Different Formats
Limited Functionality	Greater Functionality
Configuration Less Complex	Complex Configuration
Simple User Interface	User Interface can be Confusing
Potentially Less Expensive	Potentially More Expensive
Reduced cyber risk	Potentially vulnerable to cyber attack

Fixed Vs Pan Tilt Zoom

CPNI advise the use of fixed cameras when designing a perimeter security CCTV system. There are a number of reasons for this. Fixed cameras provide a known and consistent image. They can be configured to work to the optimum standard for that specific location e.g. the image screen height is known, lighting can tailored to that position, and the camera set up to perform best in the light levels available.

Pan Tilt Zoom (PTZ) cameras offer versatility of use but have inherent weaknesses, users may not be certain what they are looking at, they will certainly take longer to familiarise themselves with the scene and the camera may be left in the wrong position. PTZ cameras are also susceptible to distraction attacks i.e. an attacker may be able to draw the operator's attention and cause them to move the camera which could allow an attack in a now unmonitored area. They do however offer the ability to follow an intruder or look closely at an alarm area or location.

For the best security, both types of camera should be used within a system to achieve an optimal solution: fixed cameras to cover the perimeter and supplementary PTZ for investigating a situation or tracking an attacker

Recording

When choosing a recording system, the reasons for recording should be borne in mind. What is it you wish to record? If it is for evidential purposes, the quality, resolution and frames per second should be sufficient as to enable identification and capture all pertinent details within the scene. That may mean that compression schemes may not be suitable. If you are using CCTV with any form or automated alarm, i.e. PIDS you may wish to set the system such that you are able to get instant playback for X seconds before and Y seconds after an alarm activation without interruption of the main recording. For maximum situational awareness for an operator this function should be enabled. It is recommended that 5 seconds of pre alarm footage and 10 seconds of post alarm footage are displayed automatically on the generation of an alarm.

It must be understood that any form of compression will reduce the quality of image. However, depending on the OR this may be acceptable. If you are trying to track an intruder and identifying only the colour of their clothing a heavier resolution compression may well be tolerated. If you are trying to view / record facial features, small details or vehicle number plates lower compression will be required.

With compression it is best to preform both a subjective test and a quantative test. Use of the CCTV standard test targets such as Rotakin and the Home Office's "Faces" will allow you to do this.

Certain recording systems will apply increasing compression over time to maximise the time you can store CCTV footage. This can affect both the quality of the image (resolution) and the number of frames per second (fps). This is carried automatically and you may not realise the footage has been degraded until it is needed for post event investigation.

Even if your CCTV system does not apply further compression over time it may still record at a lower quality or fps than the live view. It is always best to review both the live view and recorded imagery to confirm it meets your Operational Requirements and will need to be carried out at varying times, CPNI recommend you check video footage, 1 min, 1 hour, 1 day, 1 week 1 month after the footage is recorded.

Camera positioning

When positioning cameras for perimeter CCTV coverage, a number of factors must be taken into account or understood.

- Cameras should be located such that the images overlap and the cameras are “Self protecting” i.e. each camera’s mounting position can be seen by another camera view to prevent tampering
- All areas required by your Operational Requirement must be covered;
- Cameras should be located such that maintenance can be easily carried out;
- Mounting poles must not be usable as climbing aids and on the secure side;
- The environment must be taken into account (sun, wind, foliage growth in summer etc.) including the change of season;
- Neighbouring sites or residential areas should be carefully considered to ensure privacy is not compromised;
- Cameras should be positioned, numbered and laid out to allow operators to easily follow an intruder from one view to another;
- Camera poles/cameras should be labelled to assist a response force’s identification but to not assist an intruder. The use of landmarks is also an option;
- If you intend to use ANPR (Automatic Number Plate Recognition), video analytics or biometric recognition, you may need to alter your camera positions from the ideal position for human operation. It may be worth considering another camera for these applications when human operators need to use the imagery.

Video Analytics

Video Analytics can be described as the capability of automatically analysing video in order to detect and determine changes within a scene. It can be a good tool to use in an integrated security solution.

Put simply, Video Analytics systems detect changes in CCTV images.
Those changes may relate to:

- Changes in grey scale or colour;
- Size of a change (i.e. area affected);
- Speed of a change;
- Direction of a change;
- Any combination of the above.

For perimeter security applications, the i-LIDS **Sterile Zone Intruder Detection** system is most applicable. Systems can be configured to register and then alarm if anything ventures into the sterile zone.

When using video analytics, as with any other automated detection system, the detection rate and false alarm rate need to be balanced against each other. A high detection rate is required to ensure that all potential intrusions onto the site are detected and acted upon. However a high detection rate increases the sensitivity of the system. As the sensitivity of the system increases, the false alarm rate often increases and too many false alarms become unmanageable for security officers. Large numbers of false alarms can lead to CCTV operator complacency and true alarms subsequently being ignored.

False alarms due to environmental conditions and wildlife can be minimised as the system can tuned to an individual site. This process of installation and tuning can take a long time to accomplish as a full range of environmental conditions is necessary, some of which only occur in specific seasons Therefore is it not unusual for a system to take over 1 year to tune

Some systems will attempt to do this automatically and “learn” what false alarms look like. The system effectively builds a library of false alarms so that it can recognise and then ignore them. However this type of technology can also learn regular but unwanted behaviours which should be detected and the learning algorithm should be regularly tested to ensure they still provide the required level of detection.

Most perimeter security detection system should have a false alarm rate of below 10 alarms per kilometre per day. Security officers should expect to regularly deal with alarms and the control room should be adequately resourced to allow the alarm to be promptly dealt with. All systems should be regularly checked to ensure they are operating correctly; this is especially important where false alarm rates are very low.

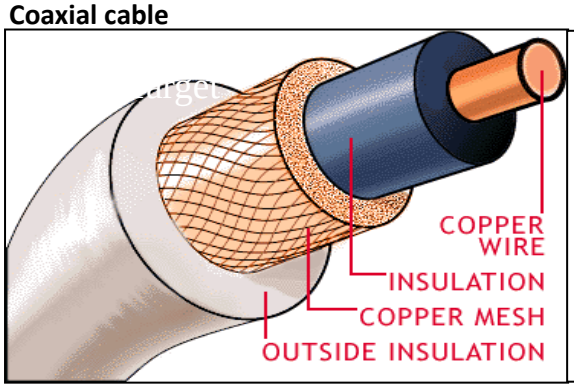
Transmission Methods

When considering which method (or combination of methods) to be used for transmitting the CCTV images back to the control room a number of factors should be considered.

- The distance required
- The bandwidth required
- Initial installation costs
- Running costs
- Security requirements
- Operating environment

The Options:

Coaxial cable

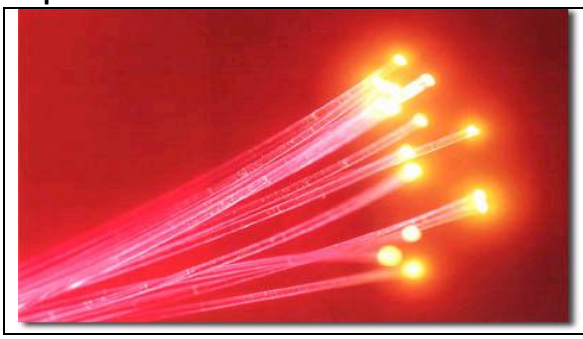


Capacity – 1 camera (can be multiplexed)
Distance – upto 300m (can be retransmitted)
Security – Tapping possible, tampering easy
Installation – low cost materials, expensive installation
Maintenance – minimal if appropriate cable is selected
Environmental – Crushing can cause 'ghosting'
Can pick up interference from motors, etc.

Microwave

Capacity – upto 300Mbps or higher
Distance – 20km line of sight
Security – Tapping possible, encryption to be used
Denial of service through intrusional or accidental jamming are possible
Installation – Specialist, may need a tower
Maintenance – Regular cleaning
Environment – Affected by heavy rain
Needs stable mount
Requires high point for antenna

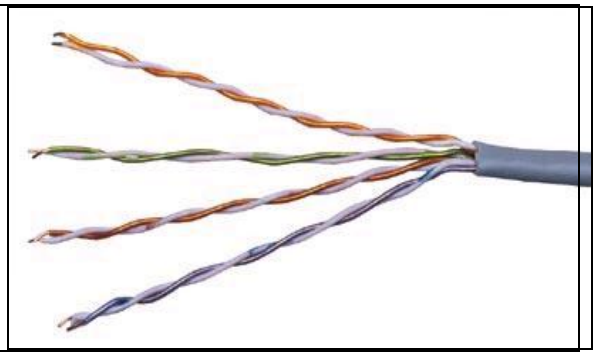
Optical Fibre



Capacity – 10Gbps or higher, variable
Distance – up to 50km on an individual run
Security – Tapping difficult,
Installation – Materials and installation expensive
Maintenance – Minimal, expensive to repair
Environment – Resistant to RF interference
Easily crushed or cut

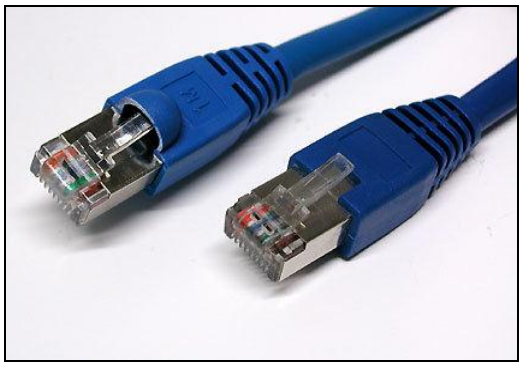
Twisted Pair

Capacity – 1 camera/pair,
Distance – upto 1500m, can be repeated
Security – Tapping possible,
Installation – Low cost materials
Maintenance – Little maintenance
Environment – Less susceptable to interferance



Ethernet

Capacity –Many cameras if used with IP depending on image quality.
Distance - <300m between switches
Security – Tapping possible Tampering possible
Installation – Low cost material, expensive to install
Maintenance – cabling last a long time, switches etc have limited lifespan
Environment – Less susceptible to interference: Often already installed in a building.



WiFI

Capacity –1GB - dependant
Distance – circa 200m
Security – Tapping possible, requires encryption
Installation – Materials can be expensive
Maintenance – Minimal
Environment – Reliant on local area WiFi usage
Same as microwave,
On an unlicensed band and can become very crowded and bandwidth can be unstable

Commissioning/Maintenance

Commissioning

Once a CCTV system has been installed it must be commissioned correctly to ensure that the OR was met and that the system does what is required of it. Below are a few points to remember, though this is not exhaustive.

Cameras and Lighting	Check that field of view and requirements are within specification. Is Rotakin viewable at all point around the perimeter? Is Rotakin viewable at the correct percentage screen height at all points around site? Is the lighting uniform, supportive of the CCTV and can the CCTV imagery been seen 24 hours a day?
Picture presentation	Are the pictures viewable and of good quality within the control room and other viewing locations? Can ALL guards use the imagery (diffent people will have different requirements from the imagery and user interface)? Is it possible to read the specified resolution bar on Rotakin?
Recording	Is there sufficent storage to hold imagery for the required period of time? Ensure that if compression is used, the images held are of a usable quality, both on the live and recorded view. Is the recorded footage still suitable after different time periods 1hr, 1day, 1 week, 1 month?
System Verification	The CCTV system should be tested and commissioned as part of the integrated security system. Does the CCTV system integrate with other physical security meassures as intended – including during normal running and alarm activation?

When commissioning a system, the technician should use the **ROTAKIN** test target to establish picture quality and image screen height. The following screen heights will be used depending on the OR of the CCTV system based on Home Office recommendations.

Detect	10%
Recognise	50%
Identify	100%

For systems which incorporate **Thermal Imaging** cameras, the **THERMAKIN** test target is available for commissioning purposes.

For information on the design, manufacture and use of Thermakin, information is available on the CPNI website under Physical Security/CCTV

Maintenance

In order that a CCTV system continues to operate as designed and commissioned, preventative maintenance is required, This may be as simple as a **regular cleaning routine**. A dirty camera lens will not give usable CCTV imagery.

Preventative maintenance should be undertaken to ensure that the whole system is performing to the operational requirement.

Cabling and connections should be checked regularly. Both physically with inspections and electronically to ensure that they are still performing to the correct specification.

A **maintenance contract** should be in place with clearly defined responsibilities. i.e. what the installer/maintenance company is responsible for and what the site is responsible for. For example, who pays for spare parts or replacement cameras if one should fail?

Maintenance contracts should be specified and documented in order to avoid confusion at a later date. A particular area of concern would be **out of hours** repair.

Perimeter Security Lighting

Perimeter lighting should be used to create a uniform, well lit strip around a site, both inside and outside the perimeter. This becomes an effective deterrent as an intruder must pass through this well lit area before they reach the perimeter fence. The luminaire should be mounted on an outreach arm on the lighting column which locates the luminare directly above the fence line. This reduces shadows and dark spots along the fence.

Example of perimeter lighting.

The mounting poles should be a minimum of 2m inside the perimeter fence to ensure that they do not act as climbing aids to an intruder to defeat any Perimeter Intruder Detection System (PIDS) that may be on the fence.

When observing with CCTV the sensitivity and spectral response of the camera sensor must be taken into account when selecting perimeter lighting;

Black and white sensors are inherently more sensitive than colour sensors and can be used with Infra-Red (IR) lighting. However they will not display colour information.

Colour cameras are not sensitive to Infra-Red light and will not work with IR illuminators, however , day/night switchable cameras will operate under IR illumination.

Below is a summary of points to consider when thinking about perimeter lighting.

- Create a well-lit, uniform strip around the Perimeter fence
- Lighting should be even, lighting levels should be 3:1 min to average
- Minimum illumination of 3 lux (5 Lux on commissioning).
- Illuminate both sides of the fence (secure and insecure side)
- Lighting columns must not be an aid to climbing

Thermal Imaging

Thermal imagers can be used as part of a CCTV system, giving longer operational ranges than traditional visible band and infrared illuminated cameras. Thermal imagers use the heat radiated from the object, as opposed to the light reflected from its surface, to form an image. As a result, thermal imagers can **only be used to determine the class** (vehicle, person, animal) of a target. It will **not allow** an operator to identify or recognise the person or the colour of a vehicle. Also they **cannot** see through glass

Thermal imagers are sold on the fact that they allow for greater detection ranges than traditional CCTV, this is true but may only be useful in certain circumstances. These are detailed below.

CPNI have produced guidance on the specification, installation, operation and maintenance of thermal imagers, which can be **found on the CPNI website**.

Thermal Imagers can be operated in 3 real time modes:

- Monitoring by human operators
- Monitoring triggered by an alarm activation
- Monitoring by Video Analytics

If the thermal imager system is to be used purely with a dedicated video analytics system and a human is not expected to verify the alarm or view the footage, thermal imagers can be used at longer distances and can detect with only a few pixels moving within the image. However, many sites will want to verify an alarm before deploying a response force to investigate.

If the image from a thermal imager is to be viewed by an operator then the system will be limited by the human vision system. For detection tasks, a target image will be required to fill 10% of the screen height for reliable detection.

Before deciding on thermal imaging as a solution, a **thermal survey** should be carried out to ensure targets will be visible. Occasional heat sources (e.g. machinery, air conditioning units, etc.) and environmental conditions can vary at different times of the day and throughout the year.

For commissioning and testing a thermal imaging system, Rotakin is not suitable as it does not provide contrast in the thermal band. As such the Thermakin Standard is available for the end to end testing of thermal imaging systems. Thermakin is a passive (no power required) human sized test target which provides contrast in the thermal band and should be used in a similar fashion to Rotakin, to confirm camera coverage. Full details are available on the CPNI website.

Human Factors/Control Room

"Human factors" is about how the humans interact with the technology. Ultimately all decisions and escalation are carried out by a human and as such the system should be tailored to take account of this. Organisations which operate CCTV systems often focus on the technical or equipment requirements and neglect the role of the operator. Below is a very brief overview of some of the issues which must be taken into account when considering the security officer as a pivotal part of the integrated security solution.

Control Room

Human attention span is limited and tasks that require intensive sustained vigilance such as monitoring CCTV feeds should be covered in brief shifts of 20 minutes.

The design and layout of a CCTV control room can go a long way to maximising the effectiveness of the operator or security officer and therefor the CCTV system. Simple things like a comfortable working temperature can be vital as is good quality seating and desks. Monitors of the correct size and viewing distance/angle are important minimise eye strain.

Control of room lighting is important, variations in lighting levels, as well as glare, can cause problems and should be controlled.

Glare can be avoided by:

- Not positioning light sources immediately in front of or behind the operator;
- Using moveable lights or diffusers;
- Avoid reflective surfaces such as worktops;
- Placing monitors at right angles to light sources.

For further information see the CPNI website Physical Security Section:

- Human factors in CCTV control rooms: A best practice guide;
- Human factors in CCTV control rooms checklists.

Situational Awareness

The process of understanding what is happening in a dynamic situation is called situational awareness. This is essentially: 'knowing what is going on so you can figure out what to do'. While this may sound obvious, loss of situational awareness can rapidly lead to inaccurate assumptions, poor decisions and errors of action – with potentially negative consequences. Situational awareness in control rooms can be influenced by many factors:

- CCTV operators must receive accurate information about the current state of any situation – information from cameras, detection systems, alarms and communications equipment – then convey this information to the correct people.

- Operators should be able to understand the results of any action taken in order to make further decisions.

This all stems from appropriate training and familiarity with the **standard operating procedures** in force within a particular site and control room. **Understanding is vital**.

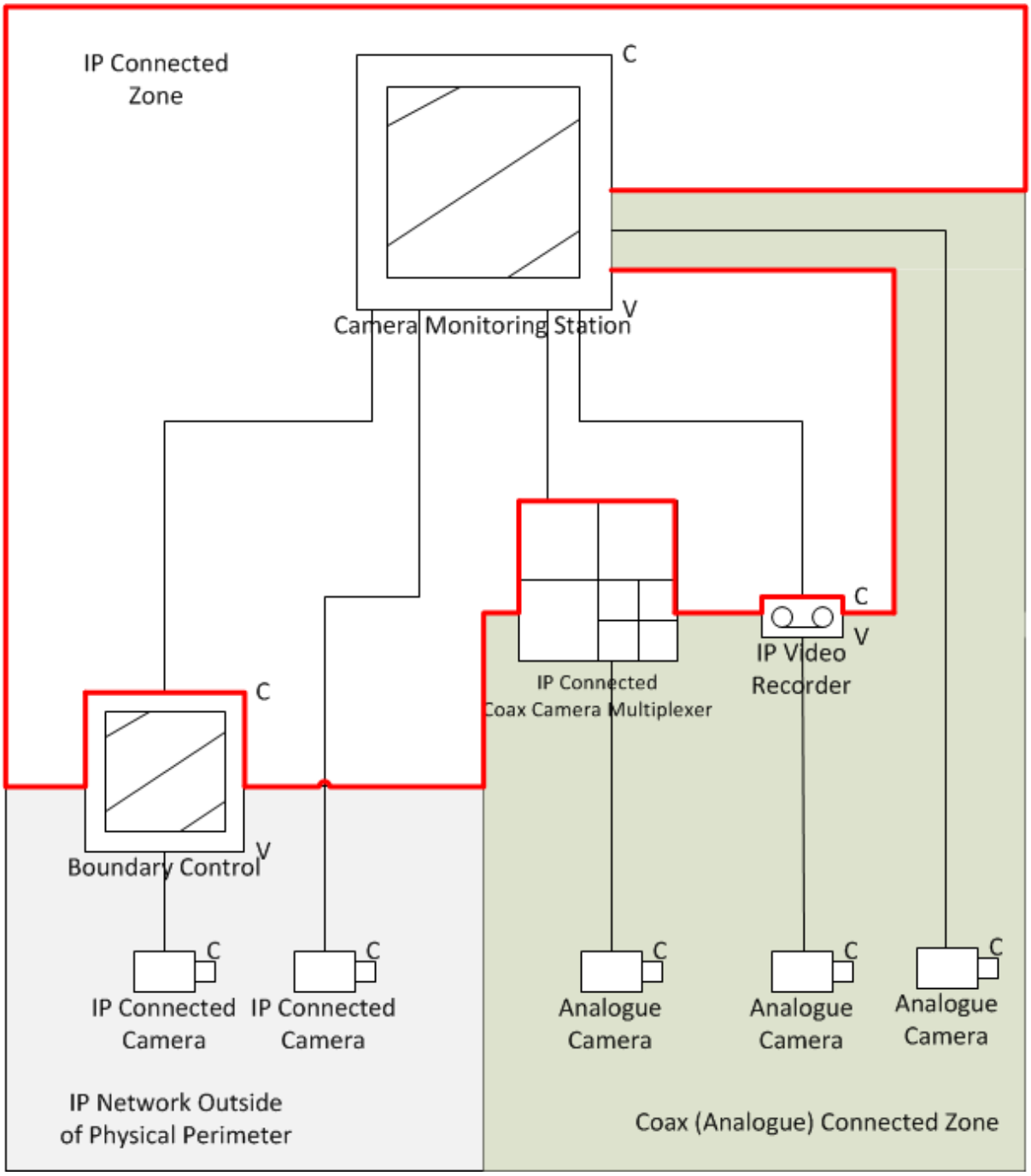
Standard Operating Procedures (SOP's) should be known to every Security Control Room Officer – Having these clearly written in an accessible folder for use during an incident can assist as an aid memoire.

CCTV operators should regularly "walk the ground" to understand the wider context of what they are seeing and further their situational awareness. If control room operators do not understand what lies out of camera view they cannot be expected to make decisions based on that information. Conversely Patrolling Security Officers should experience the CCTV operators view to understand the benefits and limitations of the CCTV system.


Taking information about the environment the operator is controlling and/or monitoring
Understanding how this information relates to the situation as a whole
Situation Awareness
Carrying out the most appropriate action in response to the situation

IP Systems

The diagram below shows a typical CCTV layout.



IP enabled Camera systems provide a unique challenge.

IP systems may be subject to attack and should be protected.

Regardless of whether the protection level is BASE, ENHANCED or HIGH, an adequate level of separation between any IT infrastructure within the protected zone and the IP Camera networks must be demonstrated.

To provide adequate mitigation against false images being sent via replay attacks at ALL protection levels, encryption must be enforced.

At BASE level of protection, simple IP address filters (deployed on the Camera's or integrated PTZ controls) may be considered sufficient.

At ENHANCED and HIGH protection levels, then full isolation of the IP network that extends outside of the boundaries of the protected zone (e.g. the network that connects to the camera), from that of the management station is required. In the case of ENHANCED this should consist of a CPA approved firewall. In the case of HIGH protection levels, this should be a full CPA approved proxying device that allows no direct connections to the internal network.

It is recommended this isolation is enforced by a CPA evaluated firewall.

At HIGH protection levels, then the IP network that extends outside of the boundaries of the protected zone (e.g. the network that connects to the camera), should be subjected to network level monitoring that is capable of detecting both the addition, removal and change of any system on the network.

This might include ARP monitoring, port scanning and persistent heart-beat verification.

Summary

The perimeter CCTV system must be regarded as part of an overall security solution which may include some or all of the following;

CCTV
PIDS
Video Analytics
Security Lighting
Guard Force/Patrols
Security Control Room
Standard Operating Procedures

By integrating each system correctly and appropriately the CCTV installation will provide an effective deterrent and detection solution and will record any incident. Getting any of the main components wrong will compromise the quality and effectiveness of the installation.

Achieving the best security solution begins with the Operational Requirement. It is vital that before the CCTV system is designed the required outcome is recognised. You have to know what you need the system to give you. Only then can you instruct a design and installation team.

Further Relevant Documentation

This document is intended as high level guidance only. For further information a number of publications available:

- BS EN 50132;
- Thermal Imager guidance CPNI Website;
- Thermakin Standard CPNI Website;
- CPNI/SSG Guide to Security Lighting;
- The CPNI Guide to Producing Operational Requirements for Security Measures (physical Security page);
- Human Factors in CCTV control rooms CPNI website;
- CPNI Security Control Rooms Guidance Document.