


CPNI CCTV for CNI Perimeter Security guidance

Helping you get the most out of your perimeter security CCTV

 [Read disclaimer](#)

© Crown copyright 2017. This guidance is available under the Open Government Licence v3.0.

Disclaimer: This guidance is issued by the UK's Centre for the Protection of National Security (CPNI) with the aim of helping organisations that make up the national infrastructure improve their protective security. It is general guidance only and needs to be adapted for use in specific situations. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any expense, liability, loss or proceedings incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. You should make your own judgement as regards use of the guidance and seek independent advice as appropriate.

1. INSTALLING A CCTV SYSTEM

2. EQUIPMENT SELECTION

3. HUMAN FACTORS

4. COMMISSIONING AND MAINTENANCE

5. SUPPLEMENTARY EQUIPMENT

Principles: overview

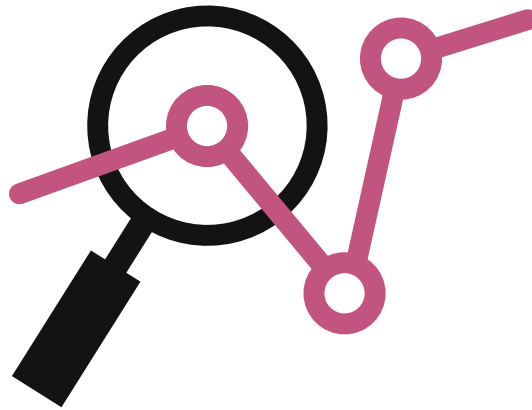


The following principles should be followed when installing a CCTV system:

- to detect an intruder, the target image must be at least 10% of screen height if being monitored by human operators
- Pan-Tilt-Zoom (PTZ) cameras could be used, mainly for tracking, to supplement fixed cameras
- CCTV can be monitored in three real-time modes:
 - by operators
 - by alarm triggers
 - by video analytics
- any video recording system must be able to provide usable and useful imagery for the whole life of the recording
- a well-trained and motivated security team is needed
- any CCTV installation should be underpinned by a clear and well thought out Operational Requirement.

-
- [i](#) Read more about [Principles](#)
 - [i](#) You may also want to read about [Operational Requirement](#)
 - [i](#) You may also want to read about [Cameras](#)
 - [↗](#) Go to [1. Installing a CCTV system](#)
 - [↗](#) Go to start of [CCTV perimeter security guidance](#)
 - [↗](#) Go to [Glossary](#)

Operational Requirement: overview




A **Level 1 Operational Requirement (OR)** is used for protecting critical assets against security threats. When you carry out a Level 1 OR, you:


- assess security risks
- identify risk mitigation options
- evolve and justify the actions that need to be taken and investments to be made.


A **Level 2 OR** addresses individual security measures. It should be carried out when there are any:

- alterations
- design changes
- new control rooms.


 Read more about [Operational Requirement](#)

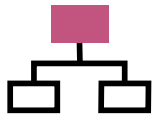
 You may also want to read about [Principles](#)

 You may also want to read about [Cameras](#)

 Go to [1. Installing a CCTV system](#)

 Go to start of [CCTV perimeter security guidance](#)

 Go to [Glossary](#)



Principles

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

CAMERA TYPES

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 MODES

CCTV can operate in three real-time modes:

MODE 1: MONITORING BY OPERATORS

If cameras are monitored by operators, the cameras on the perimeter should produce a quality image that allows an operator to detect any attempted intrusion or hostile activity. 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 to allow for consistent monitoring and assist with the detection of any issues.

If the perimeter is protected by other CPNI assured physical security measures (e.g. PIDS or Fencing), each camera image should be actively viewed at least once every **five** minutes. By doing this, all of the perimeter will be monitored, 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.

As humans we need minimum image sizes, however good the picture quality

- to **detect** an intruder, the target image must be at least **10%** of screen height
- to **recognise** someone, their image needs to be **50%** of screen height
- to **identify** someone, their image needs to be **100%** of screen height.

Where the security officer's CCTV display is a 'quad' screen (showing four images stacked two-high, two-deep) on one monitor, each image is reduced to half the height of a full screen. For detection, the target image will need to be at least 20% of the full screen height.

MODE 2: MONITORING TRIGGERED BY ALARM ACTIVATION

This mode can be used in a blank screen configuration. Blank screen configuration means that 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 is required, as an intruder may be able to carry out a very slow attack and breach the perimeter without detection. Mode 2 can be used in combination with mode 1 to verify an alarm activated by the alarm trigger.

MODE 3: MONITORING BY VIDEO ANALYTICS

Video analytics is the automatic analysis of video to determine whether there have been changes within a scene. If changes do occur an alarm is triggered to alert operators and allow them to investigate the cause of alarm.

Just like mode 2, this mode can be used in a blank screen configuration as explained above. Mode 3 can be used in combination with mode 1 to verify an alarm activated by the video analytics.

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 overlapping fields of view.

VIDEO RECORDING

Video recording is important for incident review and as evidence. 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 regularly after the recording date to confirm it is still of sufficient quality to meet the Operational Requirement.

SECURITY TEAM






CCTV systems should always be used in conjunction with other security measures and with lighting that suits the requirements 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.

-
-  You may also want to read about [Cameras](#)
 -  You may also want to read about [Operational Requirement](#)
 -  Go to [1. Installing a CCTV system](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



Operational Requirement

WHY CARRY OUT A SYSTEMATIC OPERATIONAL REQUIREMENT (OR)?

- To record user and operational needs
- to recommend appropriate security measures that manage risks to an acceptable level
- to structure the way you determine security.

THERE ARE TWO LEVELS OF OPERATIONAL REQUIREMENT – LEVEL 1 AND LEVEL 2

Level 1 OR	Level 2 OR
<p>A Level 1 OR is the main statement of the overall security need.</p> <p>It should involve all stakeholders – security managers, building owners, the people work in and use the building, those responsible for maintenance and support requirements, and operators of the current and proposed CCTV systems.</p> <p>In a Level 1 OR, you define:</p> <ul style="list-style-type: none"> • the site or building that the OR covers • assets to be protected • perceived threats (and probability of their occurrence) against the assets or adjacent facilities • consequences if assets are compromised or damaged • physical areas that contain the assets to be protected, and perceived • vulnerabilities of those areas to the threat(s) • what success looks like. 	<p>A Level 2 OR covers individual security measures considered in the CCTV system.</p> <p>The Level 2 OR will be the basis for your requirements document, or technical specification that can used for commissioning and during any testing and evaluation.</p> <p>In a Level 2 OR, you should:</p> <ul style="list-style-type: none"> • obtain a copy of the Level 1 OR • agree which Level 1 OR should be pursued • discuss a Level 2 checklist with stakeholders • write Level 2 Statement ensuring it relates to the Level 1 OR • produce a performance specification using a technical advisor • begin the procurement process. <p>• All Level 2 Solutions must be integrated as appropriate. CCTV will only be one Level 2 Statement of a series of complementary ORs.</p>

Only by completing a Level 1 and 2 OR can you decide if you require CCTV and what CCTV system you require.


EXTERNAL FACTORS TO TAKE INTO ACCOUNT


When designing and installing a CCTV system some things that you might want to consider are:


- **The proximity of the neighbours** – this could have an impact on the lighting or limit where you can place your cameras.
- **The time required for a response force to reach a point of attacked** – this might influence the type of camera installed in a particular location.
- The local environment – extensive vegetation along a fence line will affect video analytics could help hide an intruder if cameras are not in the correct position.

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

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


 You may also want to read about [Principles](#)

 You may also want to read about [Cameras](#)

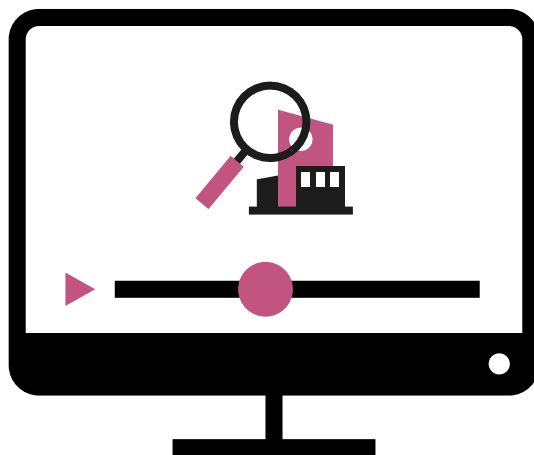
 Go to [1. Installing a CCTV system](#)

 Go to start of [CCTV perimeter security guidance](#)

 Go to the [CPNI website: Operational Requirement process](#)

 Go to [Glossary](#)

The selection process: overview

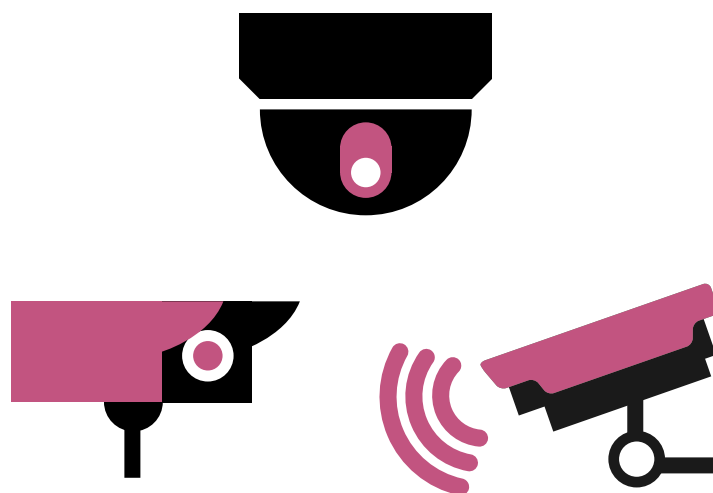


Things to consider:

- 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?

-
- [!\[\]\(5774573cf757c446bb08af21f46b2969_img.jpg\) Read more about The selection process](#)
 - [!\[\]\(a502cb21d600ba28a5cdf414d68eef89_img.jpg\) You may also want to read about Recording](#)
 - [!\[\]\(b90ad4352d6e82333440a21dde15d657_img.jpg\) You may also want to read about Video analytics](#)
 - [!\[\]\(c887fe1bc1f2363e586d4073ecf6e4e9_img.jpg\) You may also want to read about Perimeter lighting](#)
 - [!\[\]\(6b4f3dc203aec028edcb7a0552d685ad_img.jpg\) Go to 2. Equipment selection](#)
 - [!\[\]\(2c0c58cb268bb8420b6fc93187c8f293_img.jpg\) Go to start of CCTV perimeter security guidance](#)
 - [!\[\]\(fe8692d4568235edd536751307896fb2_img.jpg\) Go to Glossary](#)

Cameras: overview

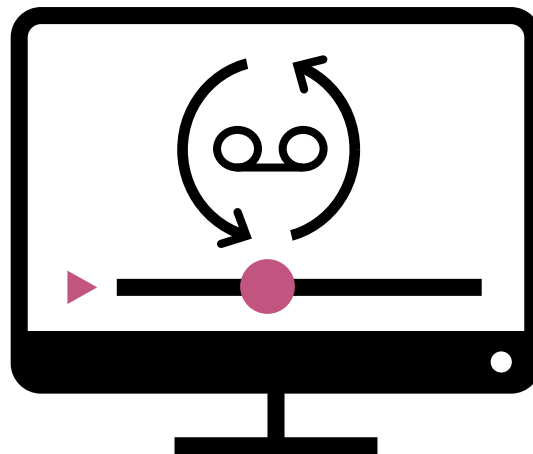


Analogue and digital cameras are different. In certain circumstances analogue cameras are entirely sufficient. Some applications will require the added functionality that digital cameras provide.

Once you have considered the camera type you need to think about how the camera should be positioned. Fixed cameras provide a known and consistent image whereas Pan-Tilt-Zoom (PTZ) cameras allow you to track a moving target.

-
- [!\[\]\(750841ae7100dc832cb0a4b3af4492f3_img.jpg\) Read more about Cameras](#)
 - [!\[\]\(78e449f8a1164b81ecbd00cd97498e27_img.jpg\) You may also want to read about Recording](#)
 - [!\[\]\(9931ff4a747d4e6edc8cfe9a6d936949_img.jpg\) You may also want to read about Video analytics](#)
 - [!\[\]\(d06bd4b5386b5ebdee91452b0403e593_img.jpg\) You may also want to read about Perimeter lighting](#)
 - [!\[\]\(9d34d65b16d32217c6053ef2fa9fa514_img.jpg\) Go to 2. Equipment selection](#)
 - [!\[\]\(dd255690041a8abf54ed85ffd3c0a03c_img.jpg\) Go to start of CCTV perimeter security guidance](#)
 - [!\[\]\(cf421f43e46a7f515fe04abc79c65063_img.jpg\) Go to Glossary](#)

Recording overview



When choosing a recording system, the reasons for recording should guide the type of recording system that you use.

You need to think about whether you need recordings for:

- evidential purposes
- use with a form of automated alarm i.e. PIDS.

You may also want to consider how you use compression with a recording system and the effect that this will have on image quality.

-
- [!\[\]\(49aa2e1da5fe39294864e9598c593810_img.jpg\) Read more about Recording](#)
 - [!\[\]\(7d0a8d8b1031f74abe67b09fcf4a2322_img.jpg\) You may also want to read about Cameras](#)
 - [!\[\]\(6557fa7496e6a507d2326ea0bef061ee_img.jpg\) You may also want to read about Video analytics](#)
 - [!\[\]\(1fe0339452ba17bd8ae951d8509f80d6_img.jpg\) Go to 2. Equipment selection](#)
 - [!\[\]\(3f7dbef097b87c46047901c2927193e7_img.jpg\) Go to start of CCTV perimeter security guidance](#)
 - [!\[\]\(f421354329041d30b231dbd0377dc4a4_img.jpg\) Go to Glossary](#)

Video analytics: overview



Video analytics is the automatic analysis of video to determine whether there have been changes within a scene.

If changes do occur an alarm is triggered to alert operators and allow them to investigate the cause of alarm. Changes may relate to:

- changes in greyscale or colour
- size of a change (i.e. area affected)
- speed of a change
- direction of a change
- any combination of the above.

i Read more about [Video analytics](#)

i You may also want to read about [Cameras](#)

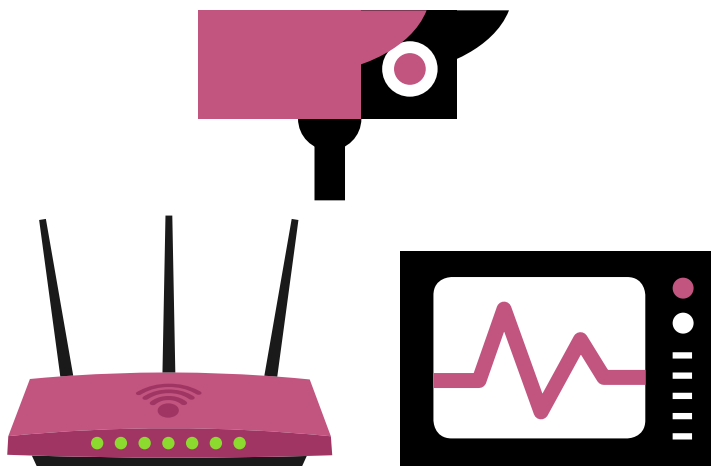
i You may also want to read about [Situational awareness](#)

↗ Go to [2. Equipment selection](#)

↗ Go to start of [CCTV perimeter security guidance](#)

↗ Go to [Glossary](#)

Transmission methods: overview



To determine which method you are going to use for **transmitting CCTV images** back to the control room you should consider:

- the distance required
- the bandwidth required
- initial installation costs
- running costs
- security requirements
- operating environment.

i Read more about [Transmission methods](#)

i You may also want to read about [Cameras](#)

i You may also want to read about [Recording](#)

[↗](#) Go to [2. Equipment selection](#)

[↗](#) Go to start of [CCTV perimeter security guidance](#)

[↗](#) Go to [Glossary](#)



The selection process

There are a number of things to think about when considering what type of equipment you may need in your perimeter CCTV installation. Not least, you should consider what other systems you will be using in your integrated security system.

Other systems could include:




- lighting
- PIDS
- human patrols or guards.

You might want to ask yourself these questions to help work out the best equipment:

- 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?



Remember to always refer back to your OR documents.

-
- i** You may also want to read about [Cameras](#)
 - i** You may also want to read about [Recording](#)
 - i** You may also want to read about [Perimeter lighting](#)
 -  Go to [2. Equipment selection](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



Cameras

ANALOGUE OR DIGITAL?

Analogue and digital cameras are different. It depends on your requirement as to which option is the best. In certain circumstances, analogue cameras are entirely sufficient. Other applications will require the added functionality of digital technology or networks.

ANALOGUE	DIGITAL
Set format	Multiple formats
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 be 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.

CAMERA POSITIONING

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

- Cameras should be positioned so that the images overlap and each camera's mounting position can be seen by another camera view to prevent tampering and to ensure that the system is "self-protecting".
- All areas required by your Operational Requirement must be covered.
- Cameras should be located in a place where maintenance can be easily carried out.
- Mounting poles must be placed on the secure side and they should be in a position so that they can't be used to help somebody climb.


- 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. Landmarks can also be used to help with identification.
- If you intend to use Automatic Number Plate Recognition (ANPR), 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.

 You may also want to read about [Perimeter lighting](#)

 You may also want to read about [Video analytics](#)

 Go to [2. Equipment selection](#)

 Go to start of [CCTV perimeter security guidance](#)

 Go to [Glossary](#)



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 of 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 perform both a subjective test and a quantitative 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 out 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.

-
-  You may also want to read about [Cameras](#)
 -  You may also want to read about [Video analytics](#)
 -  Go to [2. Equipment selection](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)

Video analytics is the automatic analysis of video to determine whether there have been changes within a scene. If changes do occur an alarm is triggered to alert operators and allow them to investigate the cause of alarm. It can be a good tool to use in an integrated security solution.

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

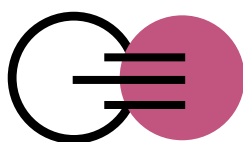
For perimeter security applications, the CPNI Sterile Zone Intruder Detection system is most applicable. Systems can be configured to register zones and then alarm if anything ventures into the sterile zone.



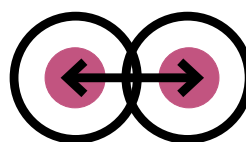
Changes in greyscale or colour



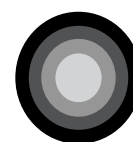
Size of a change (i.e. area affected)



Speed of a change



Direction of a change



Any combination of these.

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 be tuned to suit an individual site. The process of installing and tuning a video analytics system can take a long time to accomplish as a full range of environmental conditions is necessary, some of which only occur in specific seasons. It is not unusual for a system to take over 1 year to fine-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 where necessary.

Video analytics should be tested regularly to ensure that they still provide the required level of detection. Some technologies that “learn” what false alarms are can also learn regular but unwanted behaviours which should be detected

Most perimeter security detection systems 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

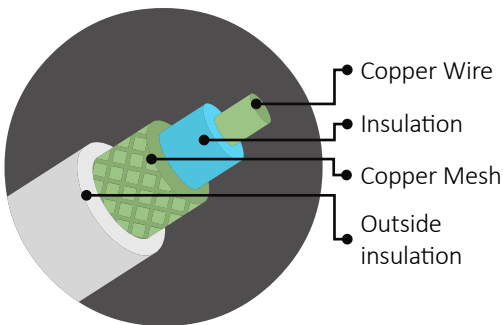
-
-  You may also want to read about [Cameras](#)
 -  You may also want to read about [Perimeter lighting](#)
 -  You may also want to read about [The control room](#)
 -  Go to [2. Equipment selection](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



Transmission methods

When considering which method (or combination of methods) are going 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.



COAXIAL CABLE

Capacity – 1 camera, can be multiplexed

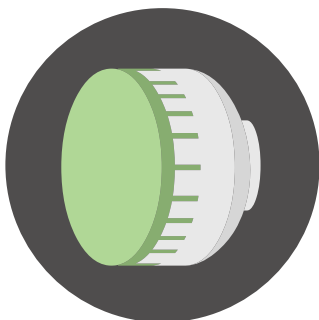
Distance – up to 300m, can be retransmitted

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 – up to 300MBps or higher

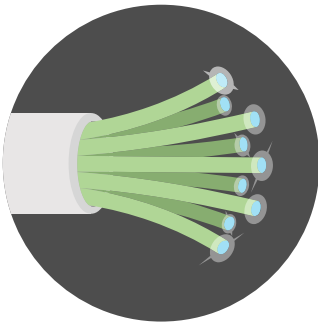
Distance – 20km line of sight

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

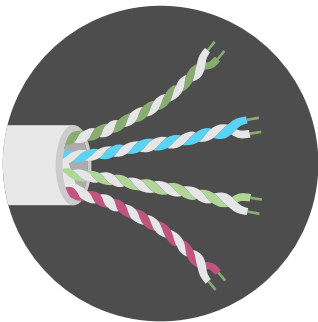
Distance – up to 50km on an individual run

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 per pair

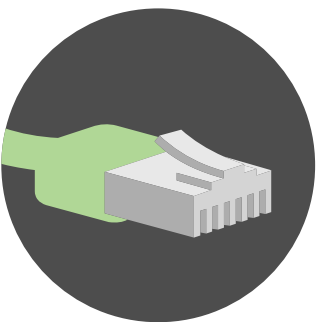
Distance – up to 1500m, can be repeated

Security – tapping possible

Installation – low cost materials

Maintenance – little maintenance

Environment – less susceptible to interference.



ETHERNET

Capacity – many cameras if used with IP, depending on image quality required

Distance – <300m between switches

Security – tapping possible, tampering possible

Installation – low cost material, expensive to install

Maintenance – cabling lasts a long time, switches have limited lifespan

Environment – less susceptible to interference, often already installed in the building.



WiFi

Capacity – 1GB dependent


Distance – around 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 it can become very crowded and bandwidth can be unstable.

 You may also want to read about [Cameras](#)

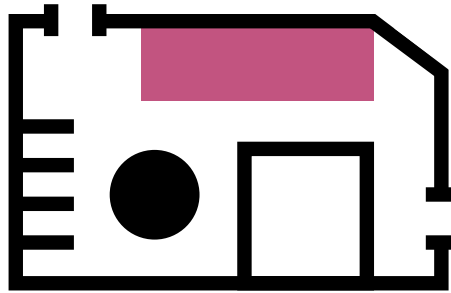
 You may also want to read about [Recording](#)

 Go to [2. Equipment selection](#)

 Go to start of [CCTV perimeter security guidance](#)

 Go to [Glossary](#)

The control room: overview



“Human factors” is about how humans interact with technology, when thinking about your CCTV systems this covers the operators and guard force. Maximise the effectiveness of the operators and security officers by:

- limiting tasks to 20 minutes
- using the correct size of monitors at the right angle and distance from the user
- using good quality desks and seating
- regulating the temperature so that the control room is comfortable
- ensuring that lighting is controlled and glare reduced.

[!\[\]\(0aff635c4179ba9e710b00f4b01d3b20_img.jpg\) Read more about The control room](#)

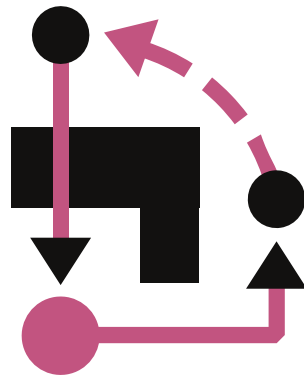
[!\[\]\(830769b31eeeaca920791081939ff8ba_img.jpg\) You may also want to read about Situational awareness](#)

[!\[\]\(0b5e7e25e8775f7e7e80906ada4f0021_img.jpg\) Go to 3. Human factors](#)

[!\[\]\(8bba887393ca45b761e5cb49e755e762_img.jpg\) Go to start of CCTV perimeter security guidance](#)

[!\[\]\(6bb0e4f14c4133b37d2887cb37e67ddd_img.jpg\) Go to Glossary](#)






Situational awareness: overview



Situational awareness is being aware of, and understanding, what's going on – and what's the right action to take in this situation (given what you know about it and what your resources are).

The situational awareness cycle:

1. Taking information about the environment the operator is controlling and/or monitoring.
2. Understanding how this information relates to the situation as a whole.
3. Carrying out the most appropriate action in response to the situation (and then back to one).

-
-  Read more about [Situational awareness](#)
 -  You may also want to read about [The control room](#)
 -  Go to [3. Human factors](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



The control room

“Human factors” is about how humans interact with technology, when thinking about your CCTV systems this covers the operators and guard force. Ultimately all decisions and escalation are carried out by a human and 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. When thinking about control rooms it is always best to consider the human aspect and work from there.

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 therefore the CCTV system.

The CCTV checklist:








- ✓ Comfortable working temperature
- ✓ Good quality seating
- ✓ Good quality desks
- ✓ Correct size of monitor
- ✓ Correct distance and angle of monitor to reduce eye strain
- ✓ Correct lighting
- ✓ 20 minute shifts.

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.

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.

-
-  You may also want to read about [Situational awareness](#)
 -  You may also want to read about [Cameras](#)
 -  Go to [Human factors in CCTV control rooms: A best practice guide](#)
 -  Go to [Human factors in CCTV control rooms checklists](#)
 -  Go to [3. Human factors](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



Situational awareness

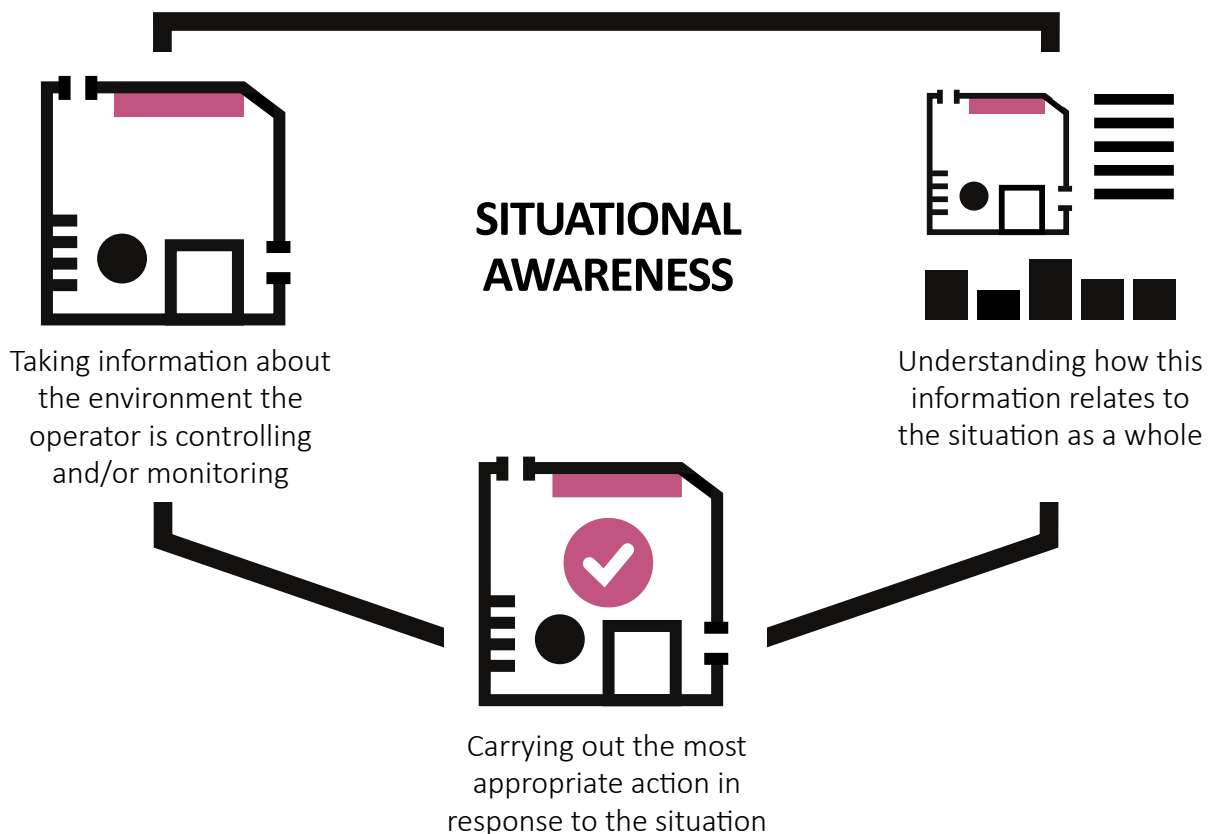
The process of understanding what is happening in a dynamic situation is called situational awareness. This is essentially: 'knowing what is going on so you can figure out what to do'. While this may sound obvious, loss of situational awareness can rapidly lead to inaccurate assumptions, poor decisions 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.

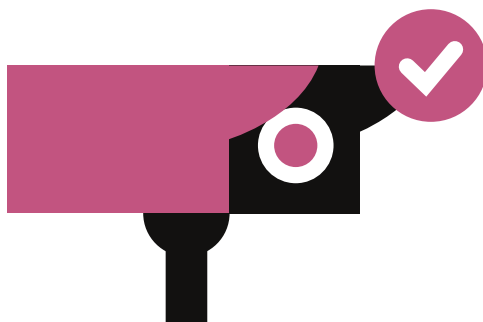
Standard Operating Procedures (SOPs) should be known to every Security Control Room Officer – having these clearly written in an accessible folder for use during an incident can help officers to remember these procedures.

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 operator’s view to understand the benefits and limitations of the CCTV system.



-
-  You may also want to read about [The control room](#)
 -  You may also want to read about [Operational requirement](#)
 -  Go to [3. Human factors](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)

Commissioning: overview









Once a CCTV system has been installed it must be commissioned properly to ensure that the OR was met and the system does what it needs to.

When commissioning a system the technician should use the Rotakin test. The Rotakin test evaluates the performance of your CCTV system and it was developed to make sure that a system is capable of producing suitable images for the operator.

A CCTV system should be set so that an operator can see images at the following screen heights:

- 10%- able to detect
- 50%- able to recognise
- 100%- able to identify

-
-  Read more about [Commissioning](#)
 -  You may also want to read about [Cameras](#)
 -  You may also want to read about [The control room](#)
 -  Go to [4. Commissioning and Maintenance](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)







Maintenance: overview



To ensure that a CCTV system continues to operate as designed and commissioned, preventative maintenance is required.

When you're considering maintenance don't forget:

- Cameras
- Lighting
- Cabling
- Connections
- Out of hours contracts.

-
-  Read more about [Maintenance](#)
 -  You may also want to read about [Cameras](#)
 -  You may also want to read about [Transmission methods](#)
 -  Go to [4. Commissioning and Maintenance](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



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.

Use our checklists below when thinking about commissioning, you will need to refer back to your OR for an extensive checklist but you can use these to get started:

Cameras and Lighting

- ✓ Check that field of view and requirements are within specification.
- ✓ Is Rotakin viewable at all points around the perimeter?
- ✓ Is Rotakin viewable at the correct percentage screen height at all points around site?
- ✓ Is the lighting uniform and supportive of the CCTV?
- ✓ Can the CCTV imagery been seen 24 hours a day?

Picture presentation

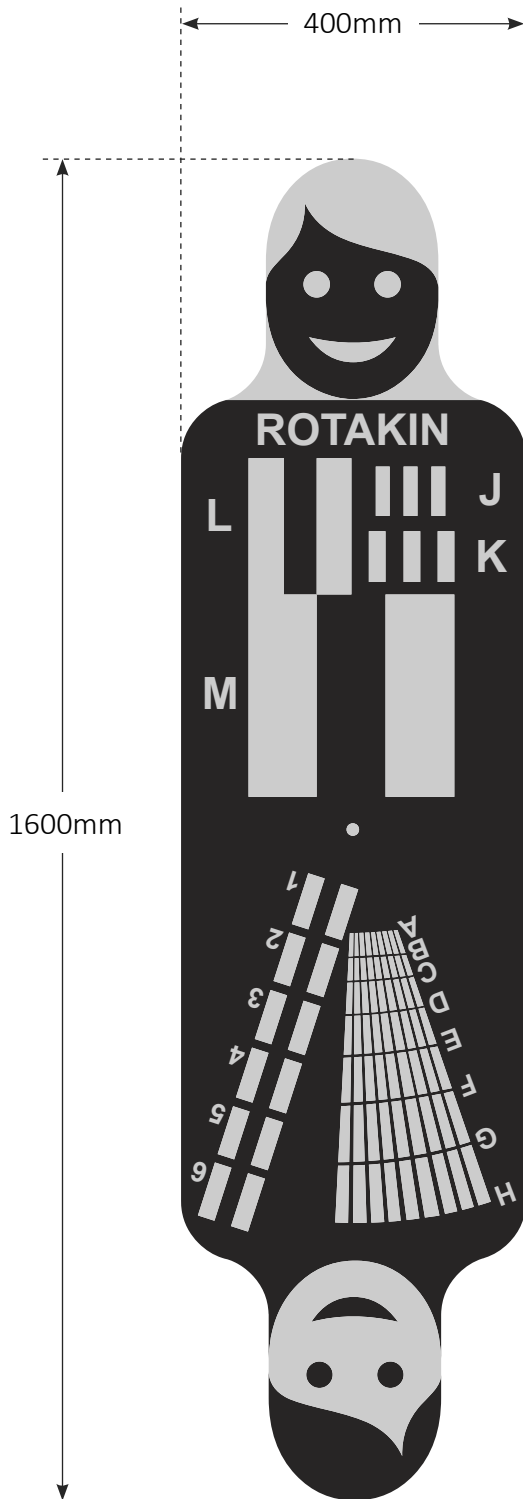
- ✓ Are the pictures viewable and of good quality within the control room and other viewing locations?
- ✓ Can ALL guards use the imagery (different people will have different requirements from the imagery and user interface)?
- ✓ Is it possible to read the specified resolution bar on Rotakin?

Recording

- ✓ Is there sufficient 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 measures as intended- including during normal running and alarm activation?



When commissioning a system the technician should use the Rotakin test. The Rotakin test evaluates the performance of your CCTV system based on the picture quality and image screen height.








ROTAKIN TEST

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.

-
-  You may also want to read about [Maintenance](#)
 -  You may also want to read about [Cameras](#)
 -  You may also want to read about [Transmission methods](#)
 -  Go to [4. Commissioning and Maintenance](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [CPNI Physical Security/CCTV](#)
 -  Go to [Glossary](#)



Maintenance







To ensure 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.

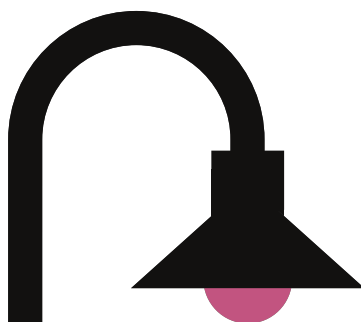
Cabling and connections should be checked regularly. Both physically with inspections and electronically to ensure that they are still performing to the correct specification.

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.

-
-  You may also want to read about [Commissioning](#)
 -  You may also want to read about [Cameras](#)
 -  You may also want to read about [Transmission methods](#)
 -  Go to [4. Commissioning and Maintenance](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)

Perimeter lighting: overview



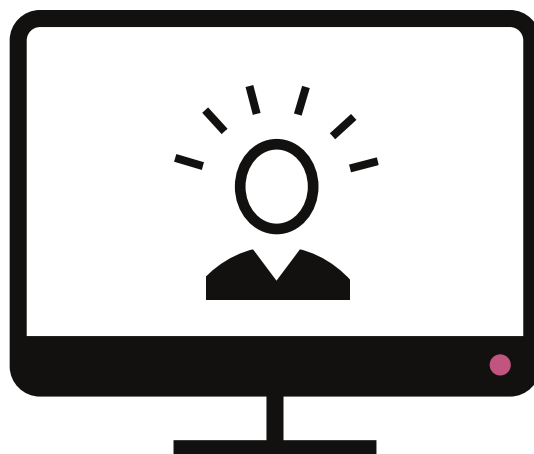
Perimeter lighting should be used to create a uniform and well-lit strip around a site, both inside and outside the perimeter.

Things to consider:

- 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.

-
- [!\[\]\(f2fdbbba686c1099e6b2b8779766e2d3_img.jpg\) Read more about Perimeter lighting](#)
 - [!\[\]\(b3cfbfd04368a71f4c64e073908d25d7_img.jpg\) You may also want to read about Cameras](#)
 - [!\[\]\(4f8bc95274d4d489592709b569351eb7_img.jpg\) You may also want to read about Thermal imaging](#)
 - [!\[\]\(68986557a06757f8727dab2acf01c000_img.jpg\) Go to 5. Supplementary equipment](#)
 - [!\[\]\(3bbb1d3234ca5d7e3145ce1334035a2b_img.jpg\) Go to start of CCTV perimeter security guidance](#)
 - [!\[\]\(d654786d397f9e11efa637705495f10d_img.jpg\) Go to Glossary](#)

Thermal imaging: overview



Thermal imagers use the heat radiated from objects to determine the class of a target – whether vehicle, person or animal. Thermal imagers can be used as part of a CCTV system, giving longer operational ranges than traditional and infrared cameras.

Thermal imagers can be monitored in three real-time modes:

- by human operators
- by alarm triggers
- by video analytics.

i Read more about [Thermal imaging](#)

i You may also want to read about [Cameras](#)

i You may also want to read about [Video analytics](#)

↗ Go to [5. Supplementary equipment](#)

↗ Go to start of [CCTV perimeter security guidance](#)

↗ Go to [Glossary](#)

IP systems: overview









Internet protocol (IP) enabled camera systems provide a unique challenge. They may be subject to attack and should be protected.

There should be an adequate level of separation between any IT infrastructure within the protected zones and the IP camera networks.

There are three levels for protection that you can use:

- base
- enhanced
- high.

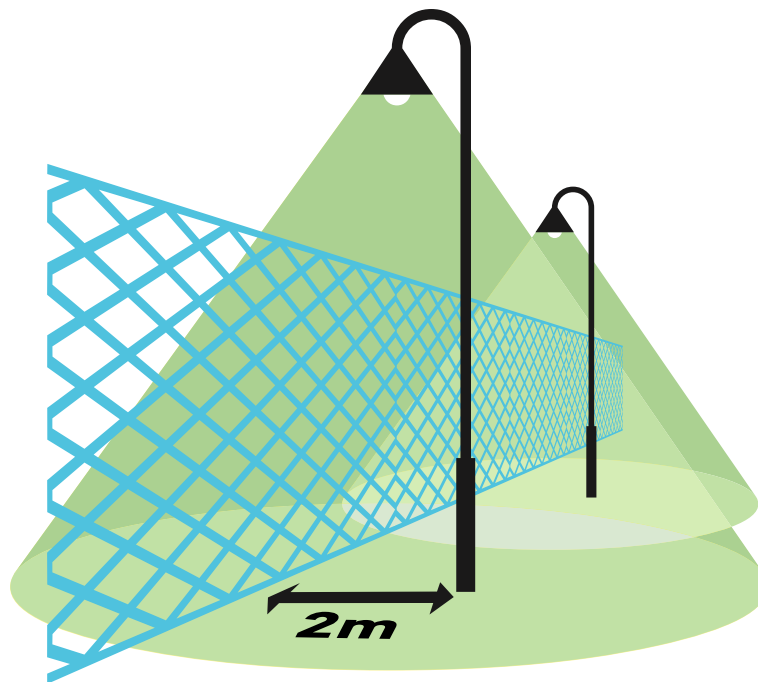
When using any level of protection encryption must be enforced to mitigate against false images being sent via replay attacks.

-
-  Read more about [IP systems](#)
 -  You may also want to read about [Cameras](#)
 -  You may also want to read about [Video analytics](#)
 -  Go to [5. Supplementary equipment](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



Perimeter 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 places the luminaire directly above the fence line. This reduces shadows and dark spots along the fence.



The mounting poles should be a minimum of 2m inside the perimeter fence to ensure that they can't be climbed up by an intruder to defeat any Perimeter Intruder Detection System (PIDS) that may be on the fence.






When selecting perimeter lighting you should think about the sensitivity of your cameras to lighting and how they detect colour to ensure that operators get the best images possible.

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

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

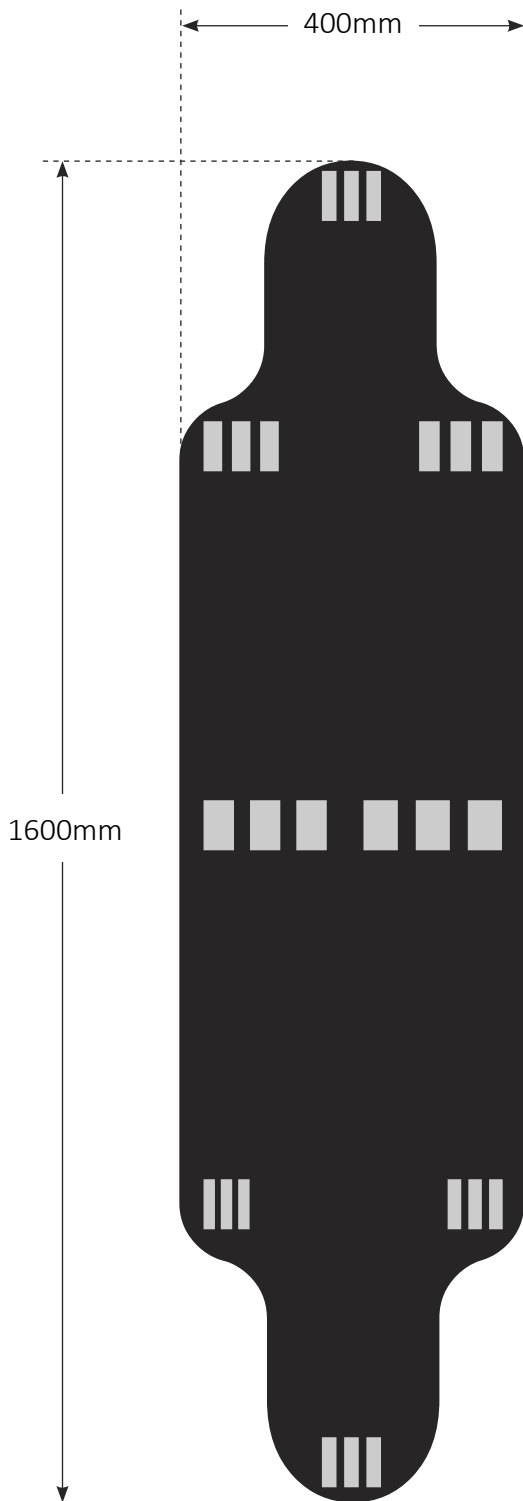
Below is a summary of points to consider when thinking about perimeter lighting:

- 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.

-
-  You may also want to read about [Cameras](#)
 -  You may also want to read about [Thermal imaging](#)
 -  Go to [5. Supplementary equipment](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)



Thermal imaging



Thermal imagers use the heat radiated from objects to determine the class of a target – whether vehicle, person or animal. Thermal imagers can be used as part of a CCTV system, giving longer operational ranges than traditional and infrared cameras. As a result, thermal imagers can only be used to determine the class of a target. It will not allow an operator to identify or recognise the person or the colour of a vehicle. Thermal imagers 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. 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.

Thermal imaging may be used 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.

-
-  You may also want to read about [Cameras](#)
 -  You may also want to read about [Perimeter lighting](#)
 -  You may also want to read about [Commissioning](#)
 -  Go to [5. Supplementary equipment](#)
 -  Go to start of [CCTV perimeter security guidance](#)
 -  Go to [Glossary](#)

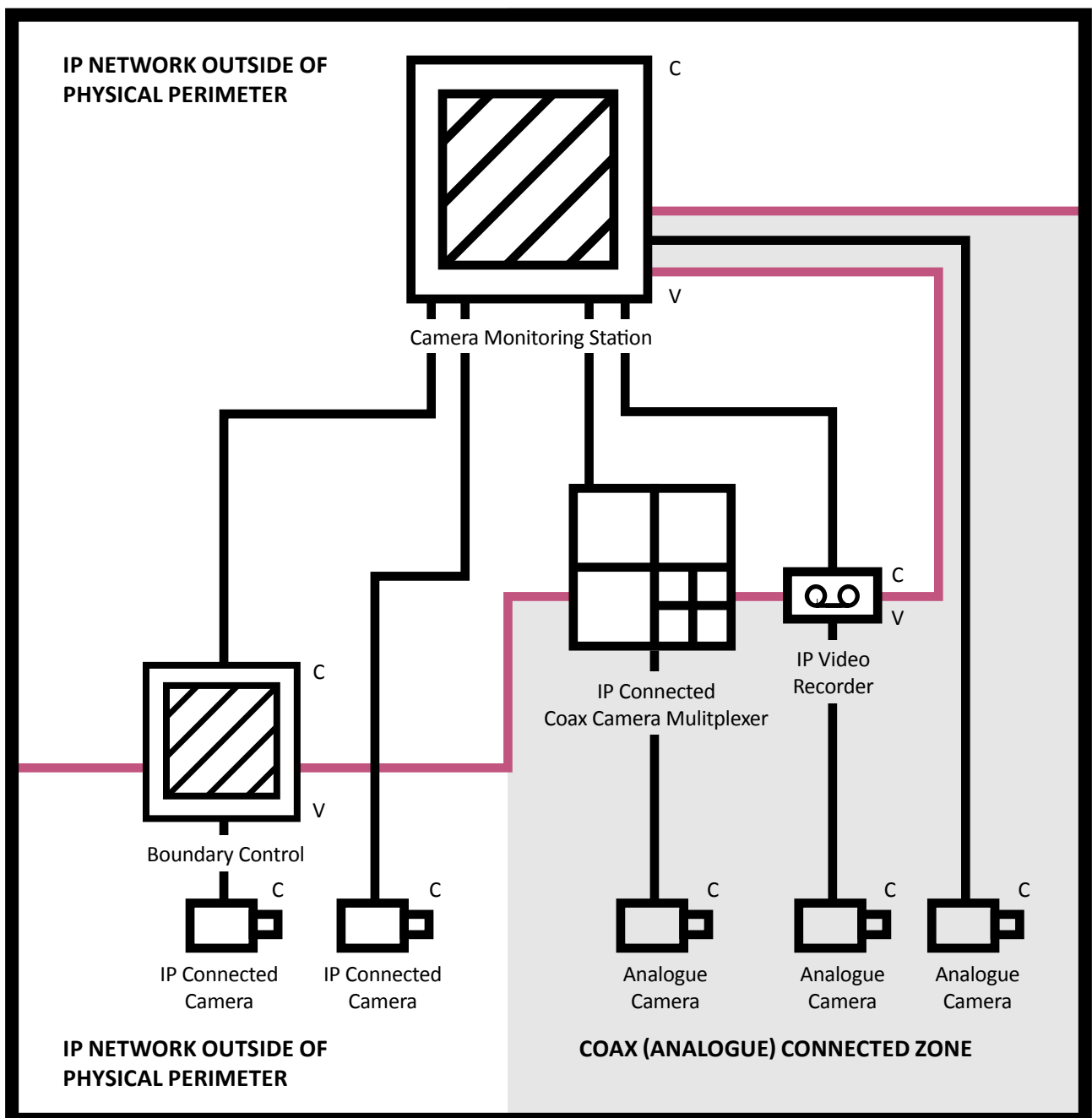


IP systems

IP systems and IP cameras provide a unique challenge for perimeter security as they may be subject to attack and need to 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.

The diagram below shows a typical CCTV layout.



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

Base

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

Enhanced and High


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 Commercial Product Assurance (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.

High

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.


Network level monitoring might include Address Resolution Protocol (ARP) monitoring, port scanning and persistent heart-beat verification.

 You may also want to read about [Cameras](#)

 You may also want to read about [Recording](#)

 Go to [5. Supplementary equipment](#)

 Go to start of [CCTV perimeter security guidance](#)

 Go to [Glossary](#)



Recommendations

50

Further reading

- BS EN 50132
- CPNI Guide to Producing Operational Requirements for Security Measures
- CPNI Security Control Rooms Guidance Document
- CPNI/SSG Guide to Security Lighting
- Home office CCTV commissioning
- Human Factors in CCTV control rooms CPNI website
- Thermal Imager guidance CPNI website
- Thermakin Standard CPNI website.



Glossary, acronyms and abbreviations

ANPR Automatic Number Plate Recognition	Automatic number plate recognition analyses vehicle registration numbers to alert when a new plate is found.
ARP Address Resolution Protocol	Used for mapping a network link to a physical address so that you can determine the machine providing specific network links.
Biometric technology	The measurement and analysis of people's physical and behavioural characteristics. Measurements can include iris, fingerprint and face scans.
Blank screen technology	Monitors will display a blank screen until an alarm is activated. On activation the screen would then display images to the operator.
CPA Commercial Product Assurance	Ensures that products and their developers are tested against security standards.
Ghosting	Double images showing on the CCTV screens due to a malfunctioning camera.
Human factors	The interaction between humans and technology.
IP camera	Internet protocol cameras send and receive data over the internet. They can also be referred to as 'webcams' or 'internet cameras'.
IR Infrared	
Luminaire	Electric light.
Multiplexed	A system where multiple signals or pieces of data can be sent via one communication link that is separated out again at the receiving end.
OR Operational requirement	A statement of what a site needs in order to fulfil its aims, with a systematic assessment of possible problems and solutions required to achieve those aims.
PIDS Perimeter intruder detection system	An electronic detection system designed to detect and alert when a site's perimeter is attacked or crossed. Can be either barrier/fence mounted or free standing.
PTZ Pan-Tilt-Zoom	A type of camera that can be moved and focussed by remote control, allowing the image to follow a moving target or scan a wider area.
Replay attack	A replay attack is a form of attack on the network in which a valid data transmission is maliciously or fraudulently delayed or repeated.
RFI Radio Frequency Interference	Interference that degrades the quality of images produced by CCTV.

Rotakin test	Evaluates the performance of your CCTV system based on the picture quality and image screen height.
Scene	The recording area for a camera as seen by the operator.
SOP Standard Operating Procedure	
Thermakin test	Used to evaluate the performance of your thermal imaging system.
Video analytics	The automatic analysis of video to determine whether there have been changes within a scene.