CPNI
Centre for the Protection of National Infrastructure

PUBLISH DATE:
June 2020

CLASSIFICATION:
Official

Testing Installed Video Analytic Systems

Version 2.0

Introduction

Video analytic systems have been tested under either the CPNI / CAST i-LIDS test programme (up to April 2015) or the CPNI Video Analytics programme (April 2015 onwards) and have been approved for listing in the Catalogue of Security Equipment (CSE) as perimeter detection systems.

Video analytic systems are tested as 'black boxes' in a test lab environment against a range of camera inputs. The performance of any video analytics system is heavily dependent on the camera used, camera set-up and camera view. As such, once installed and tuned, each analytics channel (camera view) should be attack-tested to confirm that the required detection performance is being met.

Installation and Commissioning

The Operational Requirement (OR) should be written, and a need for perimeter detection shown, before any detection system is installed or modifications made. The OR will highlight the technology options available and, more importantly, detail success criteria for the implemented solution. Testing cannot be carried out until the outcome is decided and documented.

A suitable video analytics system should be chosen from the CSE and used for the purpose that it was tested i.e. systems approved as 'Sterile Zone' should be used in a sterile zone application. If the video analytics system is a discrete hardware system it is detailed in the CSE. If the video analytics system is a software-based system details of the computer requirements will be listed in the CSE. These should be considered minimum technical requirements and should always be met.

When commissioning the system each video channel (camera view) will need to be individually tuned by the security installer. This may take several attempts to tune correctly. Tuning of the system should be undertaken over different seasons of the year and during different phases of site operation, for example but not limited to: during silent hours, day to day running and with occasional gross scene changes (rail deliveries, site movements, large plant operating). It should be expected for the commissioning phase to take up to 12 months to complete.

Pass Criteria

The following two performance measures need to be balanced when installing a detection system onto site:

> The detection rate needs to be maximised – this can be achieved by increasing the sensitivity of a detection system
>
> The false alarm rate needs to be minimised – this can be achieved by decreasing the sensitivity of a detection system

These two metrics are interdependent and there is no designed balance point. Careful balancing of the detection rate and the false alarm rate must be undertaken to gain the most benefit from a video analytics detections system. **CPNI recommends that a minimum detection rate of 95% is used.**

Before any testing can take place, a site must determine the balance of these two criteria and where they want to set the level for each one.

Detection Rate

A site must determine what percentage of attacks they wish to detect. With all technology and humans, it is nearly impossible to detect 100% of attacks. Both humans and technology can be defeated or deceived, and this should be realised when setting the detection rate. A risk-based approach needs to be taken and consideration given to the fact that a site will contain layers of security, detection systems, CCTV and security officers. Sites may well be happy only detecting 75% of attacks based on their risk model or may want a higher security assurance and may ask for greater detection rate. **CPNI recommends that a detection level greater than 95% is used.**

False Alarm Rate

Based on human factors research **CPNI recommends** that an achievable and realistic figure is between **5 – 10 false alarms per day, per km of perimeter** monitored by the detection system. Although it may seem that a higher figure is tolerable, in reality operators will be unable to cope with the higher workload and will find ways to overcome the alerting system. This will be either by ignoring the alerts, immediately silencing the alerts with no investigation, or inhibiting the alerts (either via software or via some physical and possibly destructive means). Sites with a smaller perimeter may be able to have a less stringent requirement in this area as the number of security officers per km may potentially be higher.

CCTV Purpose - Detection of Verification

Video based detection systems are by their very nature coupled with CCTV giving a number of options:

CCTV is used with a video analytics detection system purely as a detection system. A human **will never** view the CCTV footage

CCTV is used with a video analytics detection system and a security officer will view the CCTV footage post event (no live footage during an incident will be viewed)

CCTV is used with a video analytics detection system and a security officer will view the CCTV footage live, to verify an attack and manage an intrusion attempt.

If option 1 is used, the CCTV cameras can be setup to maximise the effectiveness of the video analytics system. No consideration needs to be given to the human vision system as humans will not be viewing the footage. As no verification of the alarm takes place, this option may well lead to the unnecessary deployment of the response force.

If option 2 is used, the CCTV cameras must be set-up to enable a human to be able to effectively view the footage. Illumination, contrast and brightness must all be set for viewing by a security officer. Screen height does not need to be set to a minimum of 10% Rotakin[1] but should be set such that when the footage is zoomed to PAL resolution the Rotakin is a minimum of 10% screen height.

If option 3 is used the CCTV cameras must be set up to enable a human to effectively view the footage and the screen height must be a minimum of 10% Rotakin. This enables the security officer to view the CCTV footage following an alert and be able to detect a potential intruder. Any clutter in the scene will reduce the effectiveness of the operator to detect within the scene and this should be taken into consideration.

The installer of the video analytics system should set-up and commission the system as per the requirements decided above and commission the system ready for testing.

[1] Rotakin – CCTV Test Target, designed by Home Office, used to test CCTV camera performance.

Testing

Testing can commence once a site has determined the screen height requirement, false alarm rate and detection rate.

Screen height

The first thing to confirm should be the screen height of each camera. Screen height should be confirmed at a minimum of 10% Rotakin. This should be done by holding a Rotakin test target in every camera view (front and back, left and right of the view) and confirming that the minimum size of Rotakin is 10% screen height.

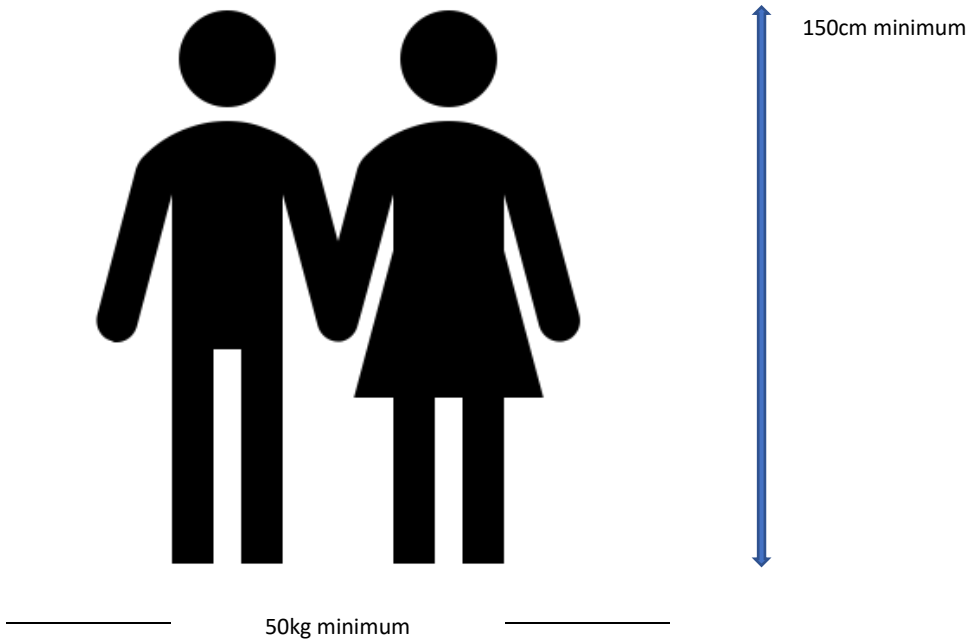
False alarm rate

The false alarm rate should then be tested. This should be a long-term test, through a number of seasons and a range of weather and conditions. **CPNI recommends this is carried out over a minimum period of nine months.**

Detection rate

Once the screen height and false alarm rate have been confirmed to be suitable, and at least at the level determined by the site, the configuration settings should be set and not changed during the detection rate trials.

Personnel used to undertake the attacks should conform to the following:



Attack Types

Detection trials should be undertaken with the following attack types:

1. Crawl
2. Leopard Crawl
3. Roll
4. Creep Walk
5. Interrupted Walk
6. Walk
7. Run/Jog
8. Bicycle
9. Vehicle
10. Shielded/obscured attack using cover

And conducted thus…

- All attacks begin 5m outside of the detection range of the video analytics system.
- Each attack will be carried out 10 times to give an average, totalling 100 attacks per area
- Attacks should be undertaken in a variety of weather conditions
- Attacks should be undertaken at a variety of times throughout the day and night
- Attacks will be repeated at least three times in a 12 month period, to cover 3 seasons.

Area 1: Angled attacks towards a point

Each of the 10 attack types should be conducted at a number of angles as shown below:

Ten attacks of each attack style should be conducted (100 attacks). These will be distributed over at least five different angles with at least two different attacks to be performed at each angle.

Figure 1 shows the layout in more detail, along with the angles to be used.

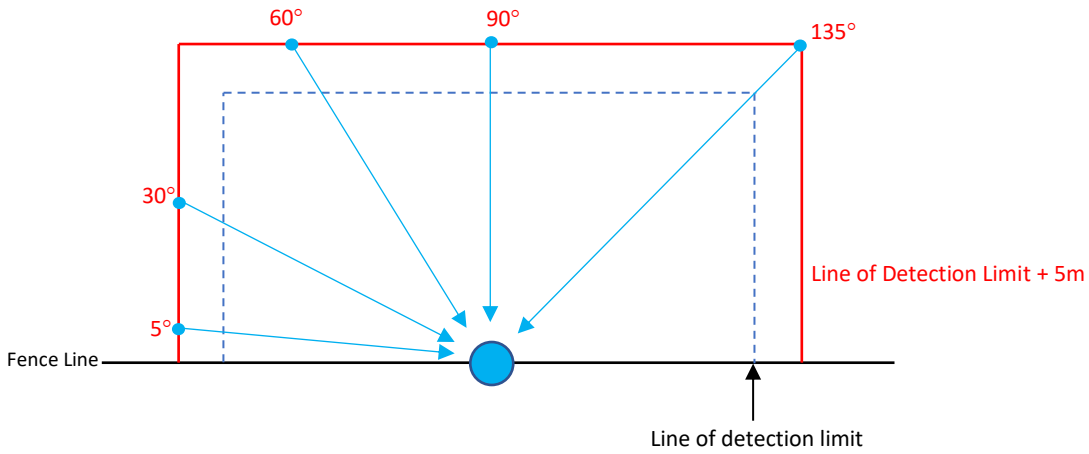


Figure 1 Attack locations for rectangular detection zone

In some instances, a semi-circular monitored area may be required. Figure 2 shows the layout which would be used in this situation.

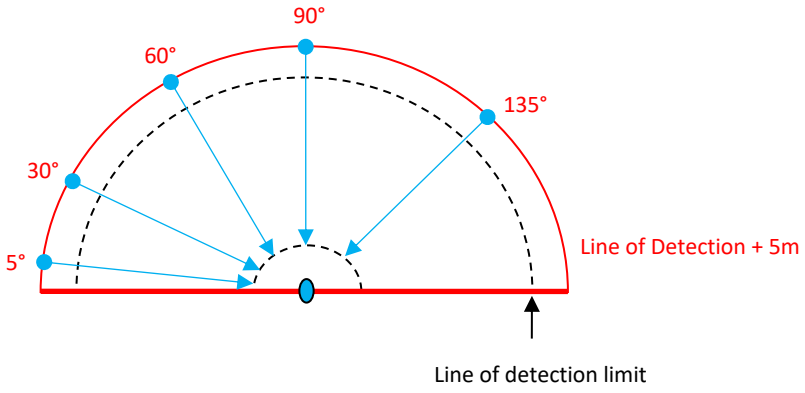


Figure 2: attack locations for semi-circular detection zone

Area 2: Lateral angled attacks

Angled attacks should be carried out at a continuous angle of 45° varying the start and end points. Ten attacks of each attack style should be conducted (100 attacks) and should be distributed along three places, equally spaced along the detection perimeter with at least two attacks types at each position.

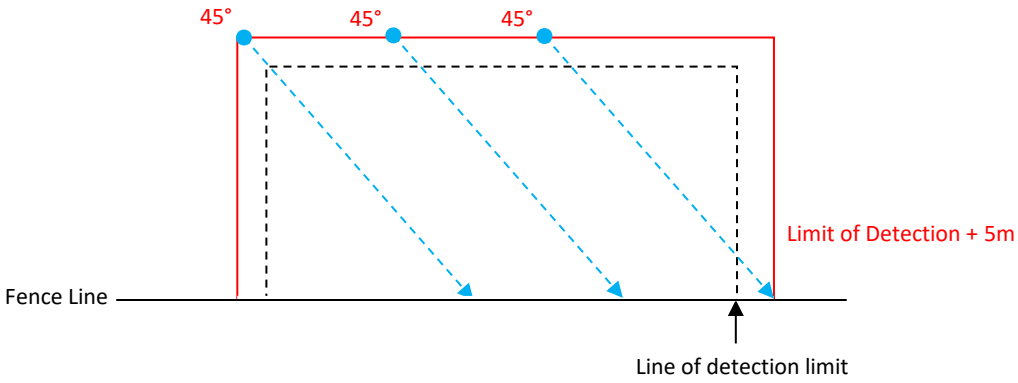


Figure 3: attack locations for rectangular detection zone

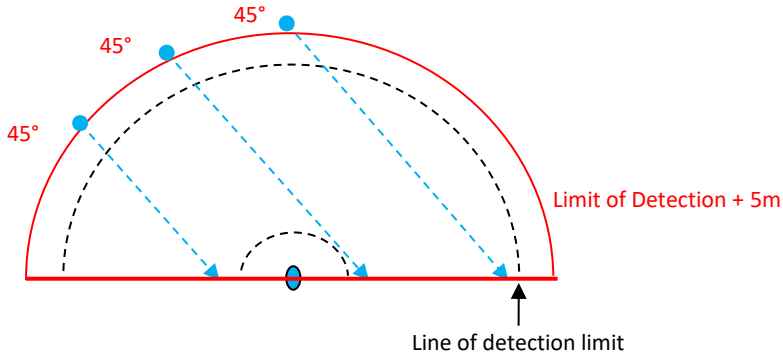


Figure 4: attack locations for semi-circular detection zone

Area 3: Horizontal attacks

Once the angled attacks have been completed a number of horizontal and vertical attacks should be undertaken: The first set of attacks should be conducted parallel to the site's perimeter (normally a fence line). Ten attacks of each attack style should be conducted (100 attacks) and should be distributed along three places, with at least two attacks types at each position. Attacks should be undertaken at 25%, 50% and 75% of the limit of the detection zone from the site perimeter.

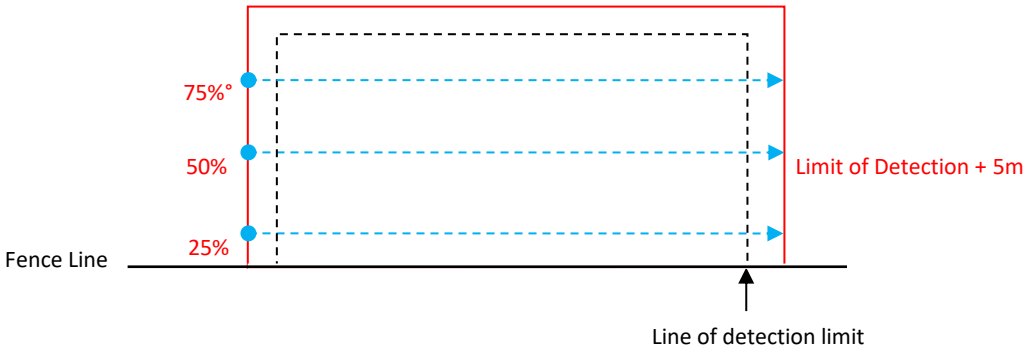


Figure 5: attack locations for rectangular detection zone

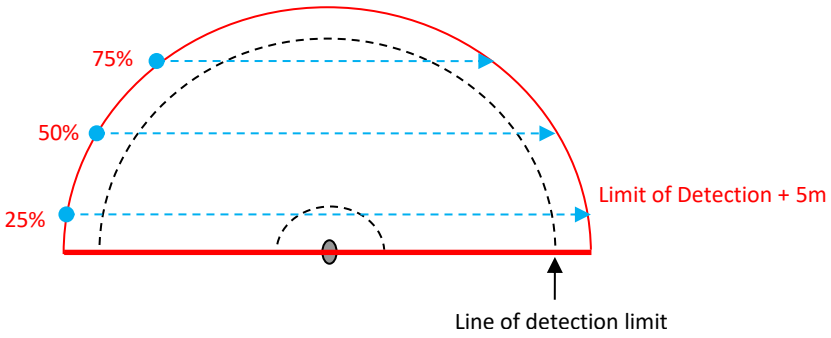


Figure 6: attack locations for semi-circular detection zone

Area 4: Vertical attacks

Next, vertical attacks should be undertaken, which run at right angles to the site perimeter (normally a fence line). Ten attacks of each attack style shall be conducted (100 attacks) and should be distributed along three places, with at least two attacks types at each position. Attacks should be undertaken at 25%, 50% and 75% of the limit of the width of the detection zone.

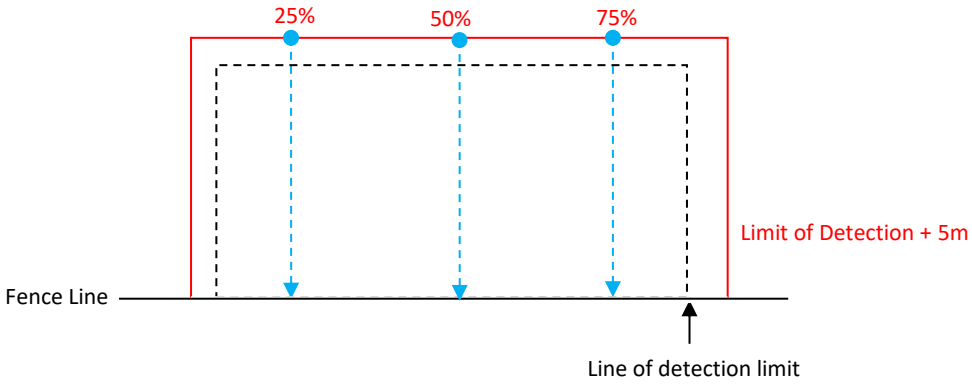


Figure 7: attack locations for rectangular detection zone

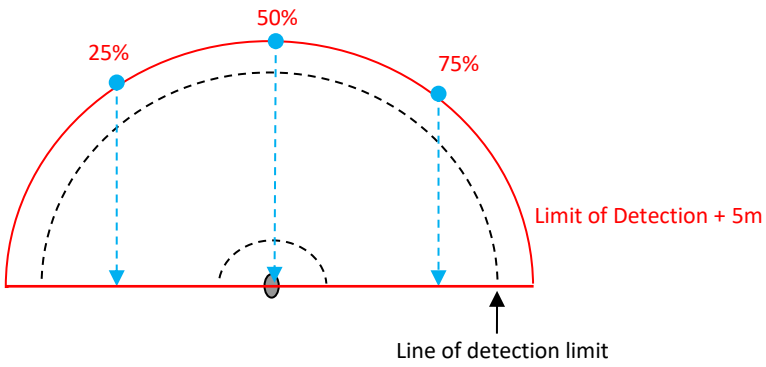


Figure 8: attack locations for semi-circular detection zone