NACD

ACCESS ▪ COMMUNICATIONS ▪ CCTV

# PERFORMANCE SPECIFICATION, 13/07/22.

# VIDEO SURVEILLANCE SYSTEMS (CCTV)

BATI CONNECT CLOUD
24/7/365
www.baticonnect.com

IPGUARD
4G/IP/GSM SMART
Visitor Door Entry

IPVIEW®
IP Video Entry

Secured by Design
SBD
Official Police Security Initiative

# 1. Introduction

Managing a building's security can be challenging; residents, visitors, employees, external contractors, and emergency services all need quick and convenient access to the building and surrounding premises at contrasting times, whilst unauthorised persons or those wishing to do harm need to be identified, prevented, or discouraged.

Understandably, building security needs differ by use and location. Designing a system that works for your building is crucial to safeguard legitimate individuals, whilst minimising the impact to the privacy and free movement.

# 2. What we mean by a Video Surveillance System

S29(6) of the Protection of Freedoms Act 2012 (PoFA) states that "surveillance camera systems" mean:

A. closed circuit television or automatic number plate recognition systems,
B. any other systems for recording or viewing visual images for surveillance purposes,
C. any systems for storing, receiving, transmitting, processing, or checking images or information obtained by systems falling within paragraph (a) or (b),
D. any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

Surveillance systems can be used to monitor and record the activities of individuals, often in high definition. As such, these systems can capture information about identifiable individuals and how they behave. This is likely to be personal data under data protection law.

Under the UK GDPR and DPA 2018, you have an obligation to implement appropriate technical and organisational measures that show you have considered and integrated the principles of data protection law into your processing activities.

It is important that you identify an appropriate lawful basis and justify any processing to be necessary and proportionate. If your surveillance system is processing the personal data of identifiable individuals, you are required to notify and pay a data protection fee to the Information Commissioner's Office (ICO) unless exempt.

You must have appropriate measures and records in place to be able to demonstrate your compliance. Specifically, under Article 30 of the UK GDPR, organisations are required to maintain a record of the processing activities taking place.

The records you keep should cover areas such as the purpose(s) for the lawful use of surveillance, any data sharing agreements you have in place and the retention periods of any personal data.

- **JUSTIFY** - Your reasons for having CCTV cameras and carry out a privacy impact assessment.
- **INFORM** - You must have signs posted indicating the use of CCTV.
- **RETAIN** - CCTV footage must only be retained for a specific period.
- **PERMIT** - Individuals can request CCTV footage that they appear in. This can take the form of Subject Access Requests and Discovery Requests
- **REDACT** - Personal Data belonging to other Parties, not relevant to a Person of Interest, must be Redacted.

- **ASSIST** – A request for CCTV footage should always be requested in writing from the Data Subject or a Legal Representative.
- **ENSURE** - Fully Compliant and Up to Date Data Processing Policies and Agreements must be in place.

## 3. Data Terms

**Data Processing**: Any action performed on data, whether automated or manual. Examples include collecting, recording, organizing, structuring, storing, using, and erasing data.

**Data Subject**: The person whose data is processed. If you are a property owner, these are your staff and contractors, the residents, and their visitors.

**Data Controller**: The person who decides why and how personal data will be processed. If you are a property owner or employee in the organisation who handles data, this is you.

**Data Processor**: A third party that processes personal data on behalf of a data controller. The GDPR (General Data Protection Regulation) has special rules for these organizations and cloud services.

**Personal data**: under Article 4(1) UK GDPR means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Biometric data**: means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, as defined at Article 4(14) UK GDPR.

**Personal Data Breach**: a security incident that negatively impacts the confidentiality, integrity, or availability of personal data; meaning that the Controller is unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 GDPR.

## 4. Capturing images of people outside the property boundary

If the system is designed so it captures only images within the boundary of the owners private domestic property, the data protection laws will not apply. If the system captures images of people outside the boundary, the Human Rights Act 1998 (HRA), General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) will apply, and you will need to ensure your use of CCTV complies with these laws.

The Surveillance Camera Code of Practice from the Biometrics and Surveillance Camera Commissioner provides guidance to enable operators of surveillance camera systems to make legitimate use of available technology in a way that the public would rightly expect and to a standard that maintains public trust and confidence.

## 5. Providing Access to CCTV to Data Subjects

Data protection law provides for the right of access to their personal data by individuals. This applies to any individual whose identifiable image has been recorded by a CCTV system.

When a data controller receives a request from an individual to access CCTV recordings, they must normally respond within one month. If the recording has already been deleted by the date the request was received, after the stated retention period has expired, the individual should be informed that the data no longer exists.

If an access request has been received, the data should not be deleted until the request has been fulfilled. Responding to an access request usually involves providing a copy of the recorded video, with detailed information of the legal basis and purpose for the data collection, and any disclosures that may have been made.

Where images of parties other than the requesting data subject appear on the CCTV recordings, the data controller must redact or blur the images of other identifiable parties and identifiable features, including objects, before supplying a copy to the subject.

Data controllers of CCTV systems should have a procedure in place to respond without undue delay to any data access requests. This could include use of a third-party processor to edit footage to retrieve images, edit and redact the images of any other persons, as necessary.

## 6. Disclosure of CCTV to Third Parties

A data controller may be asked to disclose CCTV recordings by a law enforcement body for a purpose other than that for which it was originally obtained, for example; assist in the investigation of a criminal offence. Normally a formal written request should be provided stating that a law enforcement body is investigating a criminal matter. For practical purposes a verbal request may be sufficient, however, it should be followed up with a written request.

A data controller may be requested to provide CCTV recordings to third parties to investigate an incident other than that for which it was originally obtained. In such cases, the same assessment procedure used for the stated purpose should be applied to determine if it can be justified for a genuinely legitimate interest. These requests will need to be assessed on a case-by-case basis to make sure that the principles of data protection are followed, and the rights of individuals are not prejudiced.

The legitimate interests of third parties do not oblige a data controller to disclose CCTV recordings but may permit disclosure subject to assessment. All requests should be retained by the data controllers and processors to ensure a future audit trail.

## 7. Recording audio on a CCTV system

Audio recording is very privacy intrusive. Conversations between members of the public should not be recorded. There are some limited exceptions to this, but in most cases any audio recording features will be disabled.

Audio recording must only be used for a fair and legal purpose, signs must be obviously positioned at all locations where it is in operation, clearly stating that CCTV surveillance with audio recording is taking place.

## 8. Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

You must provide individuals with privacy information including:

- your purposes for processing their personal data,
- your retention periods for that personal data,
- and who it will be shared with.

You must provide privacy information to individuals at the time you collect their personal data. For CCTV systems this is usually in the form of a CCTV in use warning sign with basic information:

- The categories of personal data obtained
- The purposes of the processing
- The lawful basis for the processing
- The name and contact details of the data controller

You must regularly review, and where necessary, update your privacy information and must bring any new uses of an individual's personal data to their attention before you start the processing.

## 9. Right to be forgotten

You should delete images of data subjects if they ask you and do this within one month. You can refuse to delete them if you specifically need to keep the data for a genuine legal dispute – in which case you need to tell them this and inform them they can make a challenge in court or complain to the ICO.

## 10. Restricting camera views and privacy masking

Cameras should be sited in such a way that they only monitor those spaces which are intended to be covered for the intended fair and lawful purpose.

Operators must be aware of the purpose(s) for which the scheme has been established, and that they are only able to use the equipment to achieve the purpose(s) for which it has been installed.

When designing a system, the spaces to be surveyed and those surrounding it should be considered from a DPA and HRA perspective and the level of privacy for each space determined.

The most effective way to restrict the field of view of a camera is by careful selection of camera position and lens field of view to prevent the camera from overlooking private areas.

With moveable Pan, Tilt and Zoom (PTZ) cameras this is achieved by setting pan and tilt movement limits within the control system's settings to restrict movement. When control system settings are used to limit the field of view, it is important that these are protected via a user access pass code so that they cannot be subsequently altered or overridden by unauthorised persons.

There are several ways that electronic masking may be applied. Masked areas of the image are commonly referred to as 'Zones'. Examples include:

1. Masked areas (usually rectangles) of solid, uniform colour so that no detail or movement in the scene covered by them can be seen through them.
2. Masks that blur or pixelate the image so that they cover to allow movement, but no fine detail can be seen, such that targets can still be tracked or incidents detected in areas covered by the masks.
3. Masks with controllable cameras to dynamically adjust the size and position of the zone in accordance with pan, tilt and zoom, that engage only when the camera zooms in on an area, using the diminutive size of an object when far away to conceal detail.

# 11. Designing a Building Video Surveillance System Strategy

## 11.1 User Requirement (UR)

This document is intended to address the safety and security requirements for all types of low and high-rise apartment blocks.

A Video Surveillance System (VSS, sometimes referred to as CCTV) is not a universal solution to security problems. As part of the overall security plan, it will help deter crime and criminal behaviour, assist with the identification of offenders, promote personal safety, and provide reassurance for residents and visitors.

### 11.1.1 Basic objectives and functions.

1. Safeguard residents, staff, contractors, and visitors.
2. Protect the building fabric, fixtures, and fittings.
3. Protect property, goods, and cash.
4. Discourage criminal and antisocial behaviour.
5. Provide an accurate record of security, criminal or health and safety related events.
6. Respect the privacy of individuals.
7. Comply with the National Security Inspectorate (NSI) code of practice for design, installation, and maintenance of CCTV surveillance systems NCP 104.3.

Establish the right level of image detail required to meet the objectives and avoid over-specifying to the point of excluding potentially suitable suppliers.

General considerations when planning a suitable level of surveillance to meet the objectives:

- Context: urban, suburban, or rural, environment, existing security, property construction.
- Occupancy: hours of occupancy of areas where risks have been identified, public access to risk areas.
- History of criminality: prevalence of any criminal activities and methods of attack.
- Threats to the CCTV system capability: vandalism of cables and cameras, loss of power or remote access, loss of illumination sources and unauthorised access to the system's operating systems, applications, or networks.

Where the system forms an extension to an existing building, development, phase or campus, the equipment selected must be compatible, unless this would reduce the performance of the new system.

### 11.1.2 Surveillance areas

In general, the following areas need to be considered when planning the areas under video surveillance.

1. Access controlled entry points and emergency egress points to the building.
2. Access and emergency egress points to building floors, basement, sub-basement, loft, or penthouse.
3. Communal lobbies, gardens, terraces, parking bays and other resident facilities.
4. Access points to internal building infrastructure locations such as tank rooms, lift motor rooms, intake rooms, etc.
5. External facilities such as bike stores, bin stores, smoking areas, external boiler rooms, security office, gate house, etc.
6. Pedestrian and vehicle access points to premises or grounds.
7. Lift cars
8. Post delivery areas

Development specific video surveillance layout drawings to be submitted for approval to client and the Design Out Crime Officer (DOCO) representing Secured by Design.

See pages 6 -28 of NACD Security Design Guide.

### 11.1.3 Activities to be captured

Intended target of surveillance at each location:

- Identify/recognise individuals or vehicles (utilising ANPR) for control of entry,
- Detect and observe vandalism or anti-social behaviour,
- Monitor common areas for staff and public safety, including vehicle and pedestrian traffic.
- Detect and observe personal attack, theft of property, goods, or cash
- Detect and observe environmental risks to individuals.

### 11.1.4 Application Guidelines

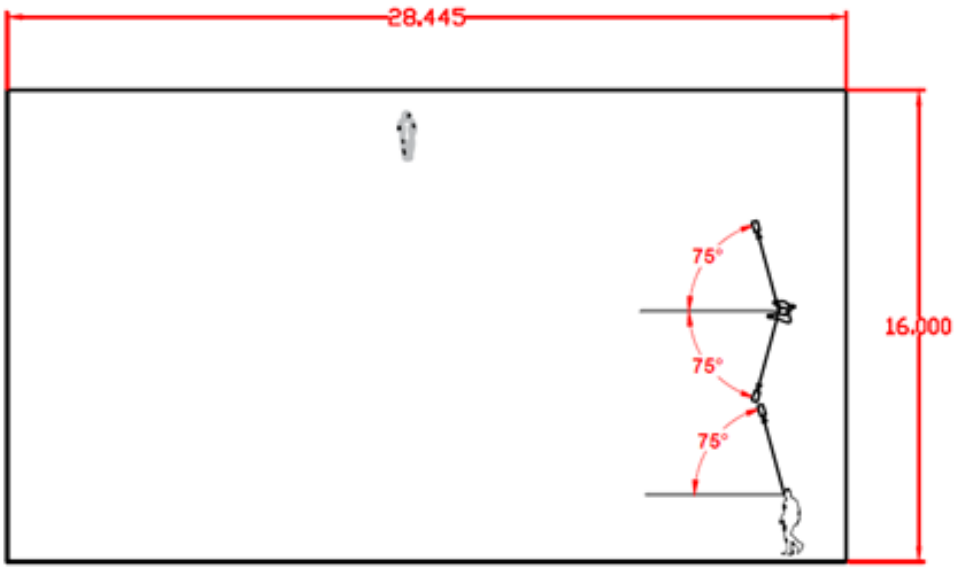
BS EN 62676-4 Video Surveillance Systems for use in security applications – Part 4: provides ideal target image categories expressed in minimum ideal pixels per metre (ppm) and % screen height (CCIR PAL format display) for a 1600 x 400 mm size human analogue.

#### Monitor: Minimum of 80 mm per pixel, not less than 5% screen height.

An observer should be able to monitor the number, direction, and speed of movement of people across a wide area.

#### Detect: Minimum of 40 mm per pixel, not less than 10% screen height.

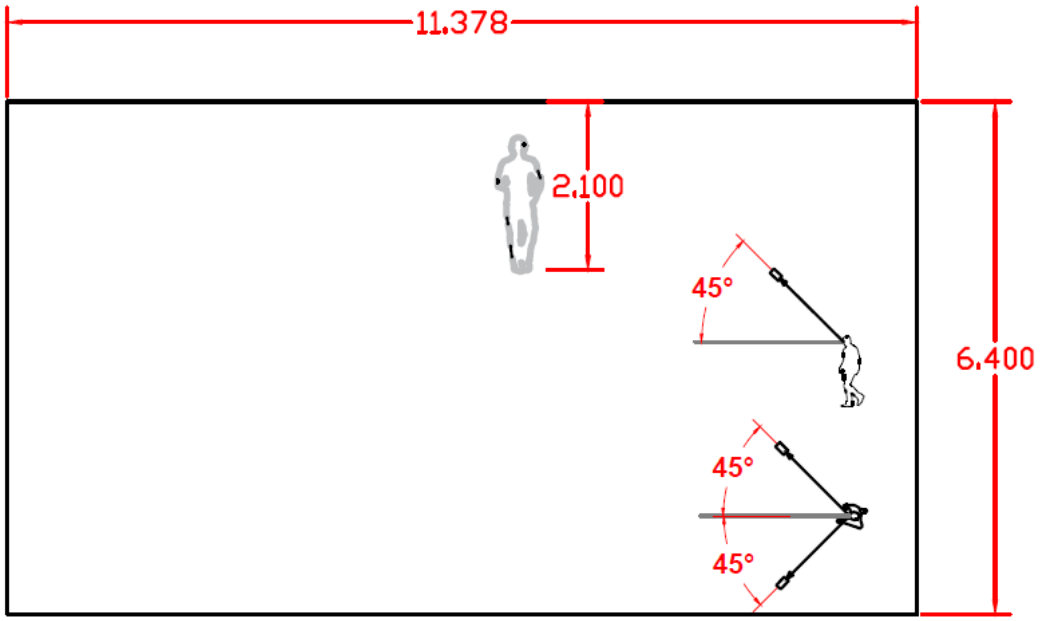
When alerted, an observer should be able to search the display screens and detect the presence of an individual person.




10% SCREEN HEIGHT = Detect = 25 ppm / 8ppf min
= 68 pixels/metre @ 1080p. Incident Angle 75°(V) & 75°(H)

## Observe: Minimum of 16 mm per pixel, not less than 25% screen height.

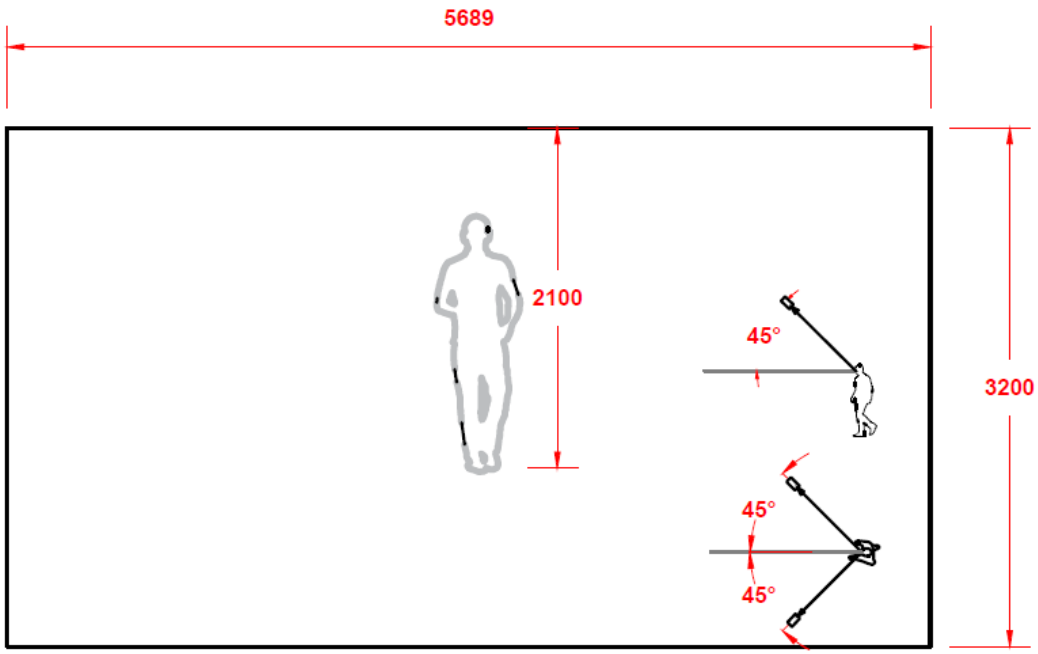
An observer should be able to see some characteristic details of the individual, and any activity surrounding the incident.



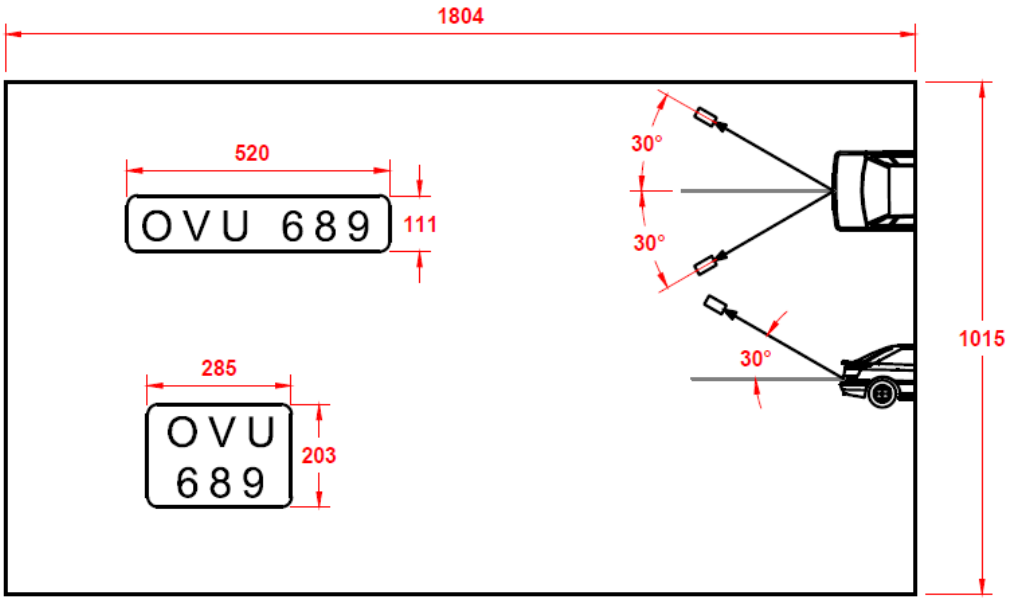

25% SCREEN HEIGHT = Observe = 62.5ppm / 20ppf min
= 169 pixels/metre @ 1080p. Incident Angle 45°(V) & 45°(H)

## Recognise: Minimum of 8 mm per pixel, not less than 50% screen height.

The observer should be able to Recognise a known individual with a high degree of confidence.



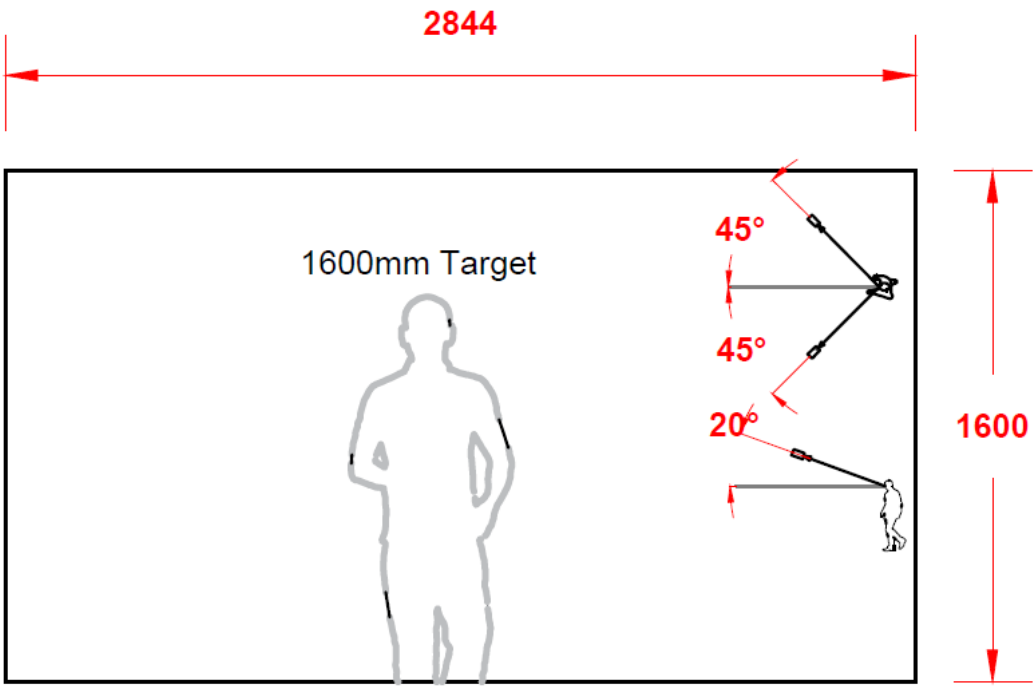

50% SCREEN HEIGHT = Recognition = 125ppm / 40ppf min
= 338 pixels/metre @ 1080p. Incident Angle 45°(V) & 45°(H)




License plate view for ANPR purposes.
Plate = 20% +/- screen height = 400ppm /128ppf min = 940ppm @1080p.
Incident angle 30°(V) & 30°(H)

## Identify: Minimum of 4 mm per pixel, not less than 100% screen height.

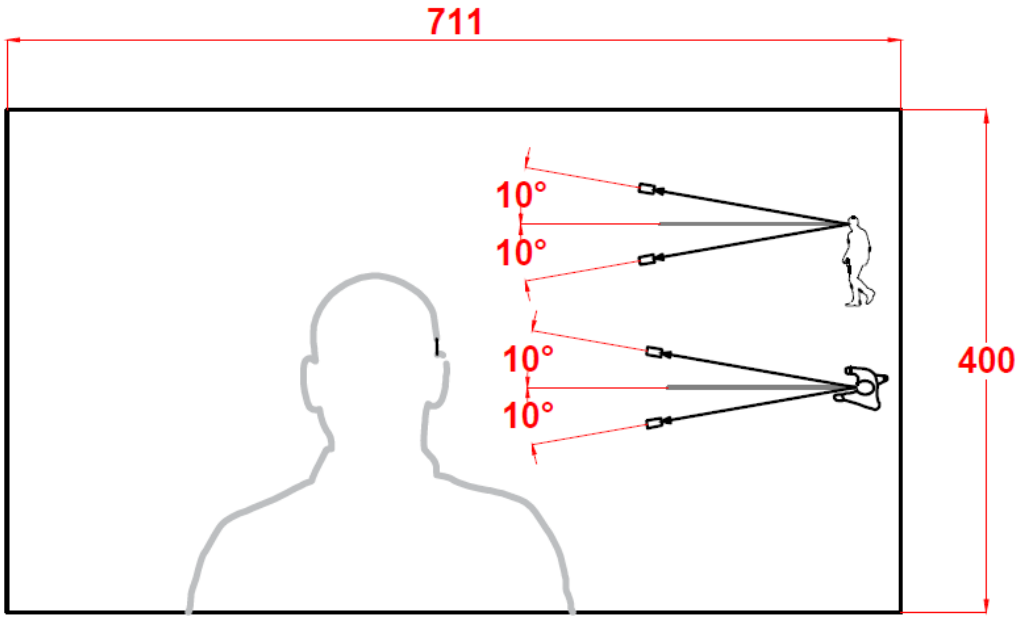
The observer should be able to identify an individual beyond reasonable doubt.




100% SCREEN HEIGHT = Identify = 250ppm / 80ppf min
= 675 pixels/metre @ 1080p. Incident Angle 20°(V) & 45°(H)

### Inspect: Minimum of 1 mm per pixel, not less than 400% screen height.

The observer should be able to resolve information from objects in the image, for example text or a logo on clothing.




400% SCREEN HEIGHT = Inspect = 1000ppm / 320ppf min
= 2700 pixels/metre @ 1080p. Incident Angle 10°(V) & 10°(H)

### 11.1.5 System/image performance

| Context (UR) | | | | | | Equipment (To be completed) | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ref# | Location | Target | Activity | Purpose | View | Scene(Lux) | Rate (ips) | Format | Make | Model | Lens | Mounting |
| | Entry and egress | Mixed | Unauthorised entry | Identify | Access control point | | | | | | | |
| | Communal | Human | vandalism, anti-social behaviour, staff and public safety, personal attack, theft of property, goods, or cash | observe | Lobbies, gardens, terraces, circulation | | | | | | | |
| | Facilities | Human | Unauthorised entry, staff and public safety, vandalism, theft of property | Recognise | tank rooms, lift motor rooms, intake rooms, bike stores, smoking areas, external boiler rooms | | | | | | | |
| | Carparks | Mixed | Unauthorised entry, anti-social behaviour, staff and public safety, vandalism, theft of property | Observe | Parking bays | | | | | | | |

The use of video content analysis AI analytics or smart motion detection to identify security or safety events providing active deterrents in the form of audio challenge, siren, or strobe.

Typical events of interest will include the following…

- Perimeter breach,
- Loitering detection,
- Object removal or abandoned object,
- Real time face detection with known/stranger mode,
- Automatic Number Plate Recognition,
- AI search via meta data of humans or vehicles,
- Contact between vehicle and pedestrian traffic
- Traffic data statistics,

## Operational periods

The system will be set to record 24/7.

## Environmental conditions

Generally, town locations within built up areas, with at least 15% of the surface built on, and/or on which the average height of buildings exceed 15 metres.

Generally, UK wind exposure zone 1 or zone 2.

| Typical illumination levels (in lux) | |
|---|---|
| Moonless; overcast night sky | 0.0001 |
| Moonless; clear night sky | 0.001 |
| Quarter moon on cloudless night | 0.01 |
| Deep twilight | 1 |
| Twilight | 10 |
| Well lit main road | 30 |
| Stairs/passages | 60 |
| Offices/Retail Store | 500-750 |
| Daylight | 10 000-25 000 |
| Full sunlight | 32 000-130 000 |

## Monitoring, record, and store

Live monitoring may take place from a front of house reception desk, or back of house facilities management office. There should be physical and organisational measures in place to prevent unauthorised persons from viewing live or recorded images.

Remote monitoring may take place from an offsite concierge office or via mobile devices.

Where the system is not monitored in real time, consideration should be given to cloud server back-up of critical cameras and health monitoring of the equipment connected to the security LAN.

All recording equipment must be located in a secure back of house area within lockable cabinets to prevent unauthorised access.

### Export
Systems should be able to export data in an open file format. Where native file formats are used the media player should be embedded with the exported media. Images must be watermarked and encrypted when the intended use is for evidential purposes.

### Operational response
If any operational responses are needed following incidents detected or reported by the surveillance system details may be included in a separate cause and effect document.

### Operator requirements
The number and configuration of operator workstations must be capable of monitoring live events and alarms within acceptable operator workloads.

### System expansion
The system should be designed with at least 50% increase in capacity of all power, transmission and recording functions, and be easily and cost effectively expandable thereafter.

### Audio
Consideration should be given to live one way or two-way audio, where this would provide an active deterrent or enhanced response to the security events identified by the system objectives.

### Limitations of surveillance
Where images and other information captured relates to identifiable individuals, their processing must comply with all legal obligations. A Privacy Impact Assessment should be made to identify any technical or organisational measures required to safeguard physical and information privacy.

## 11.2 Legislation and standards

Data Protection Act (DPA) 1998 https://ico.org.uk/

Protection of Freedoms Act (PoFA) 2012 Surveillance Camera Commissioner

Private Security Industry Act (PSIA) 2001 http://www.the-sia.org.uk/

Town & Country Planning Act (TCPA) 1990

Clear Neighbourhoods and Environment Act (CNEA) 2005

### 11.3 System Design Schedule (SDS)

The system design must address all the requirements captured in the UR considering any constraints imposed by limitations identified, from privacy impact assessment.

The agreed system design must be fully documented in a SDS with a unique reference number and a means to identify revisions caused by any design changes.

Any limitations identified which prevent the UR from being met or any deviations from the UR and any subsequent changes to the system design must be documented and be signed off by the client or the client's representative.

### 11.4 Site Plan (BS EN 62676-4 Clause 6.6)

A site plan must be included in the SDS which details the locations of interest (risk areas and targets) and key system components, including:

- cameras (including field of view and distance to risk areas and targets),
- detection (including range and coverage),
- illumination (ambient and supplemental),
- control equipment (monitor and record).

## Camera equipment (BS EN 62676-4 Clause 6.2, 6.3 & 6.4)

Lens and camera combinations must be selected to ensure resolution, object size, field of view and illumination performance meets the UR.

## Functional cameras (PTZ) (BS EN 62676-4 Clause 6.4.2)

Functional cameras must be capable of tracking the fastest expected target, must return automatically to a home location after a predefined period, and any pre-set positions must be annotated on the site plan.

### 11.5 Equipment housings (BS EN 62676-4 Clause 6.5)

All equipment and associated housings must be suitable for the expected environmental conditions.

### 11.6 Field of view/object size (BS EN 62676-4 Clauses 6.7 & 6.8)

The quality of the image on the display must have sufficient detail to meet the UR.

For target images where the requirement is to identify or recognise individuals, cameras should be placed as close to head height as possible. Where the requirement is to observe, detect or monitor, cameras should be mounted at a height that achieves the required coverage.

Installation height is generally between 2.5 metres and 5 metres; however, this depends completely on; the form of target, the level of detail required, the building structure and the camera/lens combination.

When selecting the camera field of view, it is important to consider the environment and scene content, for example:

- Foliage: Growth of or seasonal variations in foliage may obscure views.
- Illumination: luminaires located adjacent to the camera may cause poor image quality due to glare and reflections.
- Sunlight: depending on time of day or seasonal variations, the position of the sun could produce glare or backlight the target.
- Reflections: windows, buildings, water, or any other reflective objects can result in poor or excessive illumination.
- Street furniture and signage: temporary or new permanent structures such as signs or other buildings may obscure views.
- Scene activity: other scene activity may obscure the target.

### 11.7 Detectors, video analysis, triggers, alerts, and thermal imaging

- Detection areas must be within the associated cameras field of view.
- Detectors must be able to cover the area where targets are required to be detected.
- Detectors must be positioned so that activity outside of the target area does not cause activations.

### 11.8 Thermal imaging devices

Thermal imagers can be used as part of a CCTV system, where operational ranges greater than traditional visible and infrared illuminated cameras are required.

Thermal imagers can be used to determine the class (vehicle, person, animal) of a target but will not allow an operator to identify an individual person.

Object classifications relevant to thermal imagers should not be confused with the image categories used for conventional CCTV images.

- Detection: ability to distinguish an object from the background
- Recognition: ability to classify the object class (animal, human, vehicle, boat)
- Identification: ability to describe the object in detail (a man with a hat, a deer, an SUV)

Where thermal imaging is used as part of the system design the DORI (Detection, Observation, Recognition, Identification) category and range should be stated in the UR and specified in the SDS.

### 11.9 Illumination (BS EN 62676-4 Clause 6.9)

Designers should be aware that whilst camera manufacturers may claim their products will work down to extremely low lux levels, the cameras may not be able to achieve the necessary level of detail required by the UR at these levels of illumination. This is especially valid when there is a need to capture images of moving objects.

During the design process, consideration must be given to the existence of other sources of external illumination such as sunlight, reflections from buildings or large bodies of water, car lights etc., that may affect the quality of images.

### 11.10 Video/audio performance (BS EN 62676-4 Clause 9.1)

Camera settings should be appropriate to the scene content. Scenes containing rapidly changing light and colour detail may be degraded by high compressions or low bit rates. Additional capacity should be allowed in the design as this may not be apparent until the system is tested.

Image quality tests for live, recorded and exported views must be defined within the test and commission plan to ensure the system can meet the UR.

### 11.11 Video frame rate (BS EN 62676-4 Clause 9.2)

The required frame rate must be determined for each individual camera view and target speed.

### 11.12 Video resolution (BS EN 62676-4 Clause 9.3)

Camera video resolution must be selected to achieve the level of detail and coverage identified in the UR.

The resolution format should be able to achieve the level of detail needed to fulfil the UR without using digital zoom.

### 11.13 Storage (BS EN 62676-4 Clause 10)

Appropriate memory must be selected to meet the total system storage requirements with additional 50% capacity.

### 11.14 Data compression (BS EN 62676-4 Clause 11.1)

Standard publicly available compression algorithms must be used.

Compression formats that prevent data being restored to its original state, for example MPEG and MJPEG, should not be used.

### 11.15 Encryption (BS EN 62676-4 Clause 11.2)

Consideration must be given to the need to encrypt data at rest and data in transit.

### 11.16 Metadata (BS EN 62676-4 Clause 11.3)

The format of the video files must allow the size and aspect ratio of each image to be determined.

For video without audio, the time stamp must have a resolution of no less than one second.

Where both video and audio are present, the time stamps must have sufficient resolution to permit synchronised playback of the audio-visual streams.

Requirements for additional metadata; for example geo-data, floor level, Video Content Analysis (VCA), PTZ positions, etc. will be stated in the UR.

### 11.17 Image enhancements (BS EN 62676-4 Clause 11.5)

Image enhancement tools must not change the original recording.

Where an enhanced image is exported, an audit trail documenting changes to the original image must exist.

### 11.18 Image export (BS EN 62676-4 Clause 11.6)

Data exported from a recorder must have no loss of individual frame quality, change of frame rate or audio quality, there should be no duplication or loss of frames in the export process.

The system must not apply any format conversion or further compression to the exported images. Original metadata and authentication signatures must be exported with the images.

Simultaneous export and recording must be possible without affecting the performance of the system. If proprietary software is required to play back images, then this must be exported with the images.

Displays (BS EN 62676-4 Clause 7.1 & 7.2)

Monitors and other viewing devices must be selected and positioned to meet the requirements of the operator's tasks.

### 11.19 Network cabling and transmission equipment (BS EN 62676-4 Clause 8)

The system designer must select the most suitable internal (LAN) and external (WAN) communications infrastructure.

The network must be designed to ensure data is not lost or corrupted during transmission and that image integrity is maintained.

If sharing a network with other applications and devices consideration should be given to implementing VLANs, quality of service management and end point security.

- National and CENELEC standards
- Design – EN 50173 -6:2018 Part 6: Distributed Building Services
- Installation – EN 50174
- Grounding and Bonding – EN 50310 and EN 50174
- Testing – EN 50173
- Management – BS 6701

### 11.20 Network security

Physical and technical security measures must be put in place to prevent unauthorised access to the system.

Access to all system components, applications, and operating systems must be restricted to authorised individuals or processes.

Vulnerabilities in the following areas should be assessed and mitigated or managed:

- Firewalls and internet gateways
- Configuration security
- Network access control
- Malware
- Security updates and patch management

The capability of all system products should be assessed to ensure these can be made secure against malicious attacks.

- TLS communications
- detailed audit logs
- IEEE 802.1x authentication
- enhanced security mode
- complex password enforcement
- protocol control
- archive and failover
- camera tamper detection

- protected camera LAN
- SHA-2 certificates
- Active Directory Integration

https://www.cyberaware.gov.uk/cyberessentials/files/requirements.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014636/Secure_by_Default_Requirements_and_Guidance_FINAL.pdf

https://www.securedbydesign.com/internet-of-things

### 11.21 Tamper (BS EN 62676-4 Clause 6.11)

Cameras should be of a vandal resistance design or placed in locations where physical access is restricted to reduce the possibility of the field of view being altered or cabling damaged.

The system must be capable of detecting signal loss, scene change or camera blanking.

Record, store, control, and network equipment must be installed in suitably secure locations and cabinets.

All system tamper alerts must be logged, and where specified in the UR, a notification sent to local or remote operator.

### 11.22 Backup power supplies (BS EN 62676-4 Clause 12.8)

Uninterruptible power supplies (UPS) must be provided to protect sensitive system components and to maintain any specific functions identified in the UR.

Where the mains power outage time exceeds the UPS backup time the system must execute a safe shutdown procedure of sensitive equipment. All system components must then revert to full operation following mains restore.

### 11.23 Audio

Where specified, must be clearly audible without undue distortion and within the area of coverage of the relevant detectors/cameras. Audio levels should be set to avoid noise pollution to neighbouring properties.

Audio recording should only be carried out where it can be justified as being necessary and must be in accordance with all applicable legislation.

### 11.24 Operator workstations (BS EN 62676-4 Clause 12.2)

Where there is a requirement for live viewing, camera control or system management, the operator must be positioned relative to the display equipment so that they are able to comfortably carry out the tasks identified in the UR.

The number and size of the displays must be sufficient to enable the operator to view the number of images and alerts identified in the UR.

Workstations and display equipment must be suitably protected from unauthorised use, by physical and application access control.

### 11.25 Cabling

Where risks of mechanical or malicious damage are identified in the UR, cables must be protected by the use of suitable conduit, trunking, or armour.

Cable types selected must meet manufacturer's recommendations and be suitable for the environment in which they are installed.

### 11.26 Supporting structures

Masts, towers, and brackets, used to mount system components must be capable of supporting the equipment weight plus cabling and remain stable and secure during the expected climactic conditions.

Where identified in the UR anti-climb measures should be taken to prevent unauthorised access.

### 11.27 Training (BS EN 62676-4 Clause 5.3.15)

The SDS must include details of the training to be provided, who is to receive the training and when.

### 11.28 Maintenance (BS EN 62676-4 Clause 16.3)

An assessment of the type and frequency of preventive maintenance must be included in the SDS.

An assessment of the ongoing requirements to maintain the integrity of the system's network, software and firmware security must be included in the SDS. All 'critical' patches and updates should be implementable outside of normal maintenance periods.

## 12. Installation

### 12.1 General (BS EN 62676-4 Clause 15.2)

Where site conditions or the risk assessment have changed, the UR and/or the SDS must be revised to ensure the intended system design will meet the UR. All aspects of the design which are no longer appropriate must be reviewed and modified to meet the new site conditions or risk assessment.

### 12.2 Documenting changes (BS EN 62676-4 Clause 15.2)

Change to site plans, installation plans, system designs or system architecture must be agreed and recorded on the latest SDS version.

### 12.3 Access to shared networks

Permission must be gained from the network administrator or owner prior to the connection of any external devices, such as laptops and memory sticks, to shared networks. Devices must have up to date anti-virus software and security updates.

### 12.4 Power requirements

Power supplies, including PoE switches and injectors, must be capable of meeting the largest load likely to be placed upon them under normal operating conditions.

Power supplies must be located within a secure area, or in a secure enclosure protected from tampering.

All equipment housings containing mains voltages must be clearly marked.

### 12.5 Cable installation (BS 7671)

Extra-low voltage and signalling cable must not be installed in ducting/trunking which is carrying mains cable or parallel to mains cables unless suitably screened, insulated and/or segregated.

Wherever possible, extra-low voltage cables must not be brought into any item of equipment through the same entry point as mains cables.

Fixed interconnection cables must be supported by appropriate fixings, trunking, or ducts.

Plastic or PVC components used as part of the installation of cables must be suitable for the environment in which it is installed.

Cables carrying data and other level signals, or voltages must be of a type and size compatible with the rate of data transfer, anticipated levels of electrical interference and any voltage drop.

Network data cabling must be tested for the correct wire mapping, short and open circuits, cross talk, attenuation, and speed. The results of this testing must be documented.

Cables, connectors, patch panels, termination blocks and outlet sockets must be compatible.

Network devices should be connected via patch panels or outlet sockets using stranded pre-terminated patch cables.

Cabling must be clearly labelled at each termination point with source and destination. A cross-reference chart showing the relationship between cables and devices must be included with the handover documents.

# 13. Test, Commission & Handover (BS EN 62676-4 Clause 15.3)

As part of the commissioning and handover process, a Site Acceptance Test of the system must take place.

## 13.1 Test (BS EN 62676-4 Annex B & C)

A system test, against the test plan documented in the UR/SDS, must be conducted to ensure that all expected functions and features of the system are met.

- Images testing - scenario or target based.
- Image chain consistency of each camera; live, replayed and exported.
- Detection coverage – cause, effect, and response.
- Broadcast and recorded - information is clear and detectable from the areas defined by the UR and SDS.
- Network loading tests of systems capability to operate in the worst-case operational scenario.
- Network vulnerability and penetration testing where risks have been identified.

Testing must cover the operational period of the system so that image chain consistency is recorded during best- and worst-case lighting scenarios.

Legislative requirements that affect the design of the system must be assessed for compliance:

- Privacy Impact Assessments.
- Data protection requirements and policies.
- Local and national planning legislation.
- Display Screen Equipment legislation.

All results must be documented and include the details of all tests carried out and evidence captured:

- User acceptance checks,
- reference stills and videos,
- configuration files
- network load statistics,
- penetration test reports,
- etc.

## 13.2 Commissioning

The commissioning process must include a demonstration of the capability of all system components to meet the UR/SDS. This may be carried out as well as or as part of the Site Acceptance Test (SAT).

A physical inspection must be carried out to check the security and correct installation of all system components (including system interconnections). The results of this inspection must be documented.

## 13.3 Handover

A formal handover of the system must be carried out and recorded with installer and user (or users representative) sign-off.

Operator training must be carried out as documented as specified in the UR and SDS.

### 13.4 System security

Unless otherwise agreed in writing, all system accounts used by the installer must be deleted or locked and the user passwords changed when the system is handed over, including remote access rights to the system.

## 14. Documentation (BS EN 62676-4 Clause 14 & 16)

The following documentation must be provided to the customer:

- UR, unless included in the SDS (BS EN 62676-4 Clause 14.3).
- SDS, (BS EN 62676-4 Clause 14.4).
- As fitted documentation (this can be a marked up and amended copy of the SDS).
- Test plan and commissioning results (BS EN 62676-4 Clause 14.6).
- Certificate of acceptance.
- NSI certificate of compliance

The results of testing provided to the customer must as a minimum include:

- Reference images from each of the cameras as representative throughout the operational period defined in the UR.
- Operating instructions and manuals (BS EN 62676-4 Clause 16.3).
- System account details and passwords (BS EN 62676-4 Clause 16.3).
- Handover checklist, signed by the installer and user.

## 15. Preferred specialist

NACD Ltd: Contact email: estimating@nacd.co.uk Tel: 01442-211848 Web: www.nacd.co.uk

## 16. Ownership

Full ownership, with full access rights to the system, belongs solely to the end client reference the entirety of the systems, installations and programming.

# Appendix A. Legislation and standards

## UK GDPR and Data Protection Act (DPA) 2018

All CCTV systems are potentially subject to the requirements of the Data Protection Act. To assist designers, operators and owners of CCTV systems, the Information Commissioner's Office (ICO) has published several documents to provide guidance on the design, installation and operation of CCTV systems including information on data retention periods, the requirements for signage and the use of audio recording. To obtain more information, please go to https://ico.org.uk/

## Protection of Freedoms Act (PoFA) 2012

Relevant authorities, as defined in the PoFA, using CCTV for surveillance of public space are required to comply with this legislation. To assist relevant authorities to comply with this legislation, the Home Office has produced guidance in the form of a Surveillance Camera Code of Practice giving 12 Guiding Principles to be followed when designing, installing, and operating public space surveillance camera systems. To obtain more information, please go to https://www.gov.uk/government/organisations/surveillance-camera-commissioner

## Private Security Industry Act (PSIA) 2001

The Security Industry Authority (SIA) license individuals engaged in public space CCTV surveillance and in other security related activities. If you enter a contract with third-party providers of monitoring services, you should only use companies where the individuals providing CCTV monitoring service hold the appropriate SIA licenses. Visit www.the-sia.org.uk and see the British Standard BS 7958 Closed circuit television (CCTV) -Management and operation -Code of Practice for further information.

## Town & Country Planning Act (TCPA) 1990

The Town and Country Planning (General Permitted Development) (England) Order 2015 Schedule 2 Part 2 Class places restrictions on the siting and quantity of CCTV cameras deployed on the outside of buildings.

## Clear Neighbourhoods and Environment Act (CNEA) 2005

The Clean Neighbourhoods and Environment Act provides for local authorities to enforce restrictions on sources of lighting or noise pollution. Consideration should therefore be given to ensuring any additional illumination or audio broadcast deployed as part of the system does not become subject to a light or noise pollution order.

**NACD Limited**
Unit 8, Heron Business Park, Eastman Way, Hemel Hempstead, Hertfordshire, HP2 7FW.
01442 211848 estimating@nacd.co.uk www.nacd.co.uk
Registered in England No. 3212230 c/o The HHC Partnership Ltd, 52 High Street, Pinner HA5 5PW. VAT Reg No. GB 695 1188 04.