**April 2022**

# Civil Traffic Enforcement Certification of Approved Devices for Scotland Low Emission Zones

**This Document is based upon the UK Department for Transport Document: "The Certification of Approved Devices" version 1, Issued 28th February 2008.**

# Civil Traffic Enforcement Certification of Approved Devices for Scotland Low Emission Zones

## Table of Contents



## Table of Figures

# Chapter 1 General Introduction

## 1.1 Introduction

Low Emission Zones (LEZs) are to be introduced into Scotland's 4 biggest cities by the end of May 2022.

The introduction of LEZs and the associated penalty charge regime will give local authorities the powers to enforce LEZ contraventions under the Transport (Scotland) Act 2019 and to use similar camera-based systems for enforcement. The approved device specifications are outlined within the Low Emission Zone (Scotland) Regulations 2021. These systems are required to be reviewed and accepted by the Scottish Ministers in order to be recognised as an "approved device". The Vehicle Certification Agency will be appointed to review systems and submit recommendations to Scottish Ministers.

This document describes the acceptance procedures and requirements for any local authority considering introducing a LEZ. It underpins, and must be read in conjunction with, applicable legislation concerning "approved devices" made under the Transport (Scotland) Act 2019 and The Low Emission Zone (Scotland) Regulations 2021, which prescribe the fundamental requirements that must be met. This document details the considerations which, when applied collectively, will demonstrate whether equipment is fit for purpose and meets the statutory requirements, as well as best practice. The Scottish Government and local authorities will produce guidance on other operational aspects of the enforcement activity.

A device may be designed and produced by one manufacturer or may be a system specified by a Contractor or system designer incorporating sub-systems and/or equipment produced by one or more manufacturer.

Civil enforcement reduces the burden of proof for contraventions from 'beyond reasonable doubt' to 'the balance of probability'. Systems can use equipment that is automatic, and any appropriate technology may be used.

This document is concerned with ensuring that the acceptance of such devices or systems meets the 'balance of probability' criterion, although some of the requirements might go beyond this and meet the 'beyond reasonable doubt' principle.

The overall objective is to ensure that evidence produced by devices certified in accordance with the procedure described is defensible if challenged.

Consideration is also given to the need for all those involved to be able to demonstrate that the operation of the acceptance process is transparent, fair and ultimately defensible in law, and that the individual applications also satisfy those criteria.

Following this introduction there are four chapters that describe the acceptance procedure:

Chapter 2 explains how applications for acceptance should be made and defines how subsequent changes to the system will be dealt-with.

Chapter 3 covers the particular considerations that apply to attended systems - i.e. those that record evidence as seen by an operator at the time a potential contravention is observed. It is expected that systems for the enforcement of Low Emissions Zones (LEZs) will largely be unattended systems.

Chapter 4 covers the considerations that apply to unattended systems – those that record potential contraventions automatically for subsequent review.

Chapter 5 contains annexes of abbreviations and terminology used in the document and other supplementary material.

To allow for the expected range of technologies that are likely to be used and to allow for future-proofing, some of the certification criteria are presented as guidance. Any relaxation from the criteria specified herein will require a full justification during certification. Of necessity, all sections of this document are not specific about the technology to be used for contravention recording, target imaging and evidence recording. As a result, manufacturers, test houses and purchasers should agree how the tests in this document will be applied to the specific technology used in individual products.

The original Department for Transport document was the result of consideration by a number of authorities, manufacturers, and organisations involved with the technology or in enforcement activities generally as listed in Annex 2.

## 1.2 The Policy Context

Although improvements have been made, Scotland is facing legal (environmental), health and social justice challenges around air pollution, where non-compliance with domestic and European air quality legislation is predominantly due to road-based emissions.

Pollution hotspots associated with nitrogen dioxide ($NO_2$) and particulate matter (PM) remain in a number of Scottish towns and cities. The Scottish Air Quality website provides a summary of the Scottish Air Quality objectives and standards - as set out in the Air Quality (Scotland) Regulations 2000 - along with the locations of Air Quality Management Areas and the action plans proposed by local authorities to review, assess and mitigate air pollution in their areas.

The Programme for Government (PfG) 2018 committed to the introduction of LEZs into Scotland's four biggest cities between 2018 and 2020 and into Air Quality Management Areas by 2023 where the National Low Emissions Framework (NLEF) appraisals support this approach. The PfG 2017 commitment to put Scotland's first LEZ in place by 2018 was met with Glasgow City Council introducing a LEZ (for buses at least) on the 31 December 2018.

The PfG 2021 commits to decarbonising the public transport network, launching the first phase of the Scottish Zero Emission Bus Challenge Fund, worth £50 million. It also reiterates Scottish Government's drive to phase out the sale of new petrol and diesel cars by 2030 and build our Electric Vehicle capacity and infrastructure.

Transport Scotland is working in partnership with Scotland's 4 largest city authorities to deliver the PfG commitments noted above.

The National Transport Strategy (NTS2) sets out the Scottish Government's transport vision for the next 20 years. The aspiration of NTS2 toward air pollution is that 'the people of Scotland will be able to travel in towns and cities without concerns about air quality affecting their health.' An NTS2 outcome is to 'promote greener, cleaner choices' where the intent on air quality is to 'reduce the transport sector's emissions to support our national objectives on air quality and climate change'. This goal will be achieved via a suite of enablers that include 'Reducing emissions generated by the transport system to improve air quality' and 'Support management of demand to encourage more sustainable transport choices.

Transport will play a key role in addressing both the global climate emergency and helping to deliver Scotland's net-zero emission target by 2045. The update to the Scottish Government's Climate Change Plan was published in December 2020 to reflect the increased ambition of the new targets set in the Climate Change (Emissions Reductions Targets) (Scotland) Act published in October 2019. The Policy Memorandum on Emission Reductions Targets notes that 'raising the ambition of Scotland's targets for reducing greenhouse gas emissions will enhance Scotland's efforts at tackling climate change, with likely benefits to climatic factors. In addition, positive secondary effects are expected for air quality, population and human health, and material assets, due in large part to the further decarbonisation of energy generation and transport.'

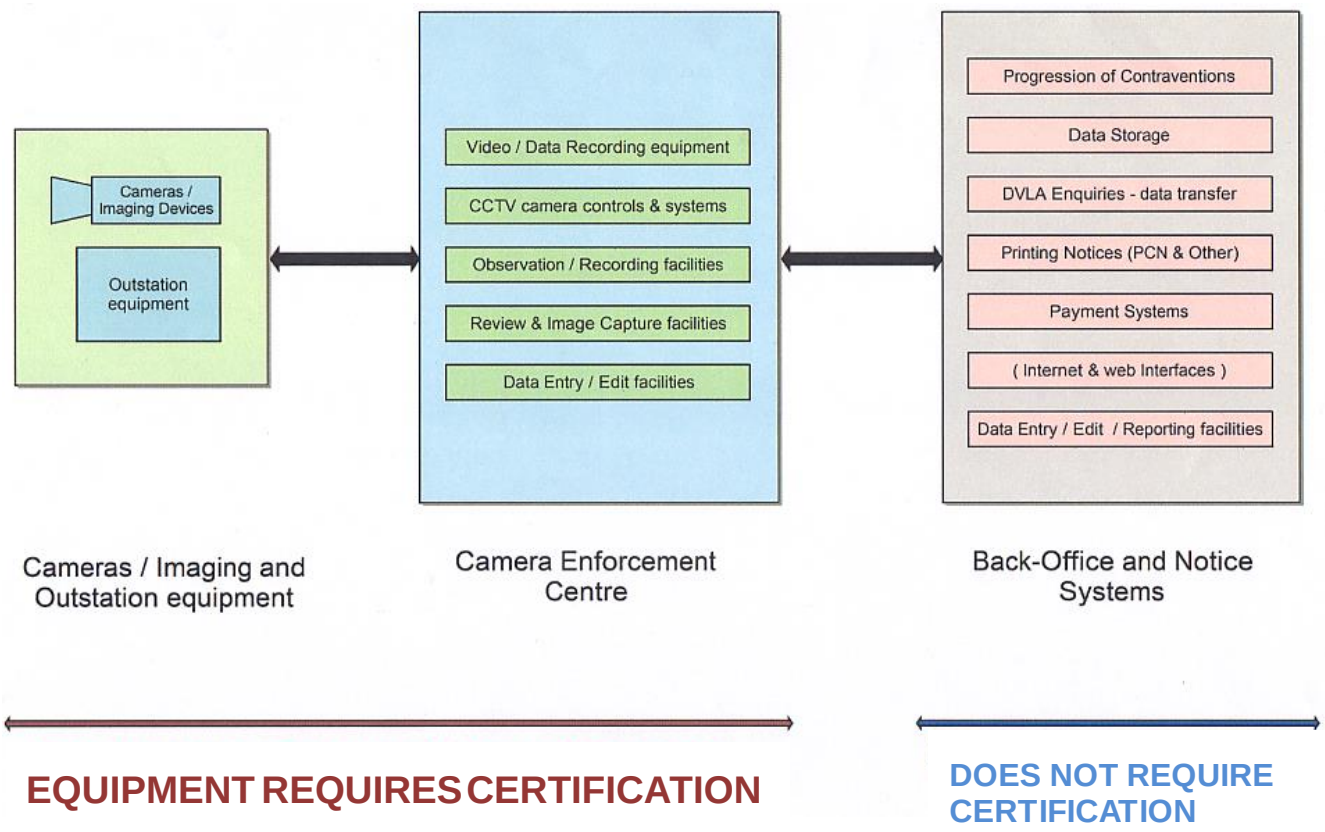
Part 2 of the Transport (Scotland) Act 2019 contains provisions that enable the creation and civil enforcement of LEZs by local authorities and allows Scottish Ministers to set nationally consistent standards on matters such as, but not limited to, emissions standards, penalties, and exemptions.

LEZs are to use new powers under the Transport (Scotland) Act 2019 for a road access restriction scheme (where vehicles that do not meet LEZ Euro emission standards (and do not meet any LEZ exemptions) are not allowed to enter a LEZ and are subject to a penalty if they enter the LEZ). The secondary legislation for enforcement of LEZs, The Low Emission Zones (Scotland) Regulations 2021 and The Low Emission Zones (Emission Standards, Exemptions and Enforcement) (Scotland) Regulations 2021, came into force in May 2021.

## 1.3 Scope

The elements of a civil traffic enforcement system that are subject to certification by Scottish Ministers are shown in Figure 1.

**Figure 1 Typical civil traffic enforcement system showing elements subject to certification**



# Chapter 2 General Requirements for Certification of Systems

## 2.1 Certification Process

### 2.1.1 Technical Construction File

Applicants should document their systems in a Technical Construction File (TCF), which is submitted to Scottish Ministers to gain certification. The suggested contents for the file are listed in section 5.5. There is nothing to stop the file containing more information than is listed.

The file should be sufficiently detailed so that important aspects of the system outlined in this document are clear and can be assessed. Essentially the file should provide at least the necessary evidence that the design is in accordance with relevant requirements.

The file must be maintained, with any future changes as outlined in section 2.2 recorded promptly. It is recommended that the TCF be a controlled document that is modular and easily maintained as the system changes. As a minimum there should be a proper index or list of all the documents enclosed in the current version of the TCF.

### 2.1.2 Test House Tests

Where a test house is employed to test a new system, they must record in the Technical Construction File compiled by the applicant details of the tests carried out. This file must then be augmented with the site-specific testing records made as a result of on-site commissioning of the system. These site-specific records must be approved and signed-off by a competent person that may be either a representative of a test house appropriately qualified to certify site-based testing or an experienced and competent member of staff from the enforcing authority or its consultants or the maintenance organisation working on that authority's behalf.

### 2.1.3 Legacy Systems

Where a legacy system is to be certified, the Technical Construction File must include documents containing the details described in paragraph 2.1.1 above. Evidence of previous certification or approval (where available) should be included. Upon first certification, the system must be tested and certified and the test records included in the Technical Construction File.

It is expected that systems for the enforcement of LEZs will not be legacy systems.

### 2.1.4 Application by a Manufacturer

A Manufacturer may apply to gain prior certification for their system. This system can then be used by any individual Traffic Authority.

When a system is used under a manufacturer's certification, both the Traffic Authority and the manufacturer must ensure that the system in use is exactly as described in the manufacturer's Technical Construction File and in accordance with any

recommendations it contains or as modified by agreement with Scottish Ministers. They declare this by signing a declaration form and submitting it to Scottish Ministers. The system can be used by the traffic authority once they have received an acknowledgement.

### 2.1.5 Applications to the Scottish Government

Scottish Ministers will decide whether to issue a letter of certification on the basis of the results of a review of the Technical Construction File and any other exchanges that take place subsequently, (See section 2.3). Scottish Ministers will retain the TCF and any associated information, and, where necessary, will advise of any further steps necessary to achieve certification.

## 2.2 Modifications to Certified Equipment

This section describes the requirements for the management of changes and modifications to certified traffic enforcement systems. All modifications to certified systems, (regardless of category assessed) should be maintained in the Technical Construction File.

The applicant must maintain records of the serial numbers or dates of delivery of equipment that is manufactured to a revised Technical Construction File.

### 2.2.1 Requirements

It is a requirement that all modifications that are made to an accepted system are notified to Scottish Ministers. This should be by ensuring that the Technical Construction File is kept up to date. The method of notification is subject to agreement by Scottish Ministers.

Applicants are required to assess whether the change is a Significant Change, a Minor Change or a Supplier Equivalent change. The three categories are defined below.

Scottish Ministers will consider the applicant's assessment but reserves the right to reclassify any modification at his/her sole discretion. Further evidence may be requested to justify any classification.

Apart from "Supplier Equivalent" changes, Scottish Ministers' agreement to the classification of the proposed change and any necessary (re) certification must be obtained prior to any enforcement activity with changed equipment.

### 2.2.2 Significant Change

A significant change is any modification made to an enforcement system that increases or changes its **functionality**. The replacement of subsystems or components that change the way the system performs its task are considered significant changes. In general, these will require fairly major changes to the system explanations and specifications in the Technical Construction File. Where such change occurs, a full re-certification is likely.

Changes of software version or variant of the enforcement application (but not necessarily any operating system) are considered significant changes.

### 2.2.3 Minor Change

Changes which improve the **performance** of subsystems or components, but where the function carried out within the overall system by them has not changed are considered minor changes. This is unless an increase in overall system capacity is achieved.

Software maintenance or upgrades where the functions carried out by the software have not changed (or been added to) are considered minor changes. These include low-level driver updates and bug fixes except those responsible for any of the following areas: Cryptography, evidence authentication, Enforcement Schedules and secure interfaces.

In general, where a minor change is made, limited or no re-certification testing will be required. The extent of this re-certification will be subject to agreement between the body seeking equipment re-certification and Scottish Ministers.

### 2.2.4 Supplier Equivalent

A supplier equivalent change is one where a generic component or subsystem of the enforcement equipment is replaced with a functionally equivalent item from the same or another supplier. In order to be considered functionally equivalent, the component must have sufficiently similar performance in terms of value and tolerance. This is intended to facilitate maintenance of the system rather than modification. A supplier equivalent change will not usually be subject to re-certification. However, the Technical Construction File must be maintained accordingly.

No software changes are permitted in this category. If a supplier-equivalent change to hardware triggers a driver or operating system update then the software change is likely to be considered a "minor change".

### 2.2.5 Variation

These provisions are intended to provide a rigorous control over the configuration management of certified enforcement equipment in order to maintain confidence of all stakeholders. It is not the intention of these requirements to restrict Scottish Ministers unduly and it remains within the discretion of Scottish Ministers to nominate a reduced level of testing wherever that is deemed appropriate. Some examples of where this discretion could be used include (but are not limited to):

- Where elements of the design being submitted have already been part of a certified system and are used unchanged
- Where elements of the design are outside the scope of a significant change and are demonstrably unaffected by that change
- Where compliance with certain requirements is intrinsic to components within the enforcement system being certified.

In these cases, it might be acceptable for restrict Scottish Ministers to accept a reduced level of recertification. Applications for this test scope reduction should be agreed on a case-by-case basis before the start of certification.

## 2.3 Freedom of Information

The Scottish Ministers will respect the confidentiality of any commercially sensitive information provided as part of the certification process. The Scottish Ministers may disclose any information as required by law or judicial order. In the event of a request for information made under the Freedom of Information (Scotland) Act 2002 or the Environmental Information (Scotland) Regulations 2004, the Scottish Ministers will consider the appropriateness of such a request, the extent to which any exemptions may apply, and their obligations under the UK General Data Protection Regulation and the Data Protection Act 2018.

## 2.4 Certification Procedures

The Local Authority or Contractor shall demonstrate compliance to this standard through the process described in Chapter 2.

Scottish Ministers may, at their sole discretion, seek review of the submitted documents by:

The Vehicle Certification Agency

1 the Eastgate Office Centre

Eastgate Road

Bristol, BS5 6XX

**Email:** civil-enforcment@VCA.gov.uk

# Chapter 3 Requirements for Attended Systems

It is expected that systems for the enforcement of Low Emissions Zones, (LEZs) will largely be unattended systems, the requirements for which are set out in Chapter 4.

## 3.1 Imaging Devices / Cameras

At least one each of the views described below must be captured. Multiple views may be permitted.

### 3.1.1 Image requirements

#### *3.1.1.1 Context View (CV)*

The context image must provide a clear, sharp and free of motion blur image of the vehicle in its context within the road environment. The context image must have the same resolution as the CCTV camera as defined in 3.1.2.1 below. This should be a colour image. Monochrome images at night are considered acceptable.

#### *3.1.1.2 Close-up View (CUV)*

The close-up image must provide a clear, sharp and free of motion blur image of the VRM in its context within the vehicle committing the *potential* contravention. The close-up image must have a resolution that allows the VRM to be read unambiguously. This should be a colour image, (unless the image is from the ANPR camera).

#### *3.1.1.3 Frame rate*

Where an image sequence is to be captured rather than single images; the system must record close-up and context views. The frame rate of the evidence pack image sequence must be a minimum of 5 frames per second or equivalent with no two images being, on average, more than 200ms apart.

### 3.1.2 Minimum Technical requirements for CCTV Cameras

Cameras equipped with ANPR functionality should also meet the requirements given in Annex 3, (Section 5.3).

#### *3.1.2.1 Resolution of the CCTV Camera*

The camera (and associated transmission and recording equipment) must have a resolution of 720 x 576 pixels. Cameras may use a higher resolution.

#### *3.1.2.2 Zoom Capability of the CCTV Camera*

Most CCTV cameras will use an optical zoom lens to zoom in and out – at the full standard resolution for that camera. Where a digital zoom facility is used, the full video frame obtained must not be less than the equivalent of 20% of the minimum resolution (i.e. ≈ 144 x 115 pixels) at the point of video capture on the camera. This is

the equivalent of a 5x digital zoom on a PAL resolution camera – but may be the equivalent of a larger digital zoom on a higher definition camera.

#### *3.1.2.3 Low Light Performance*

The CCTV camera must be capable of producing usable video at 2.0 lux. This should allow enforcement to be carried out even with average quality street lighting. If cameras have an illuminator fitted, they should still meet this requirement as enforcement should be able to continue if the Illuminator fails.

#### *3.1.2.4 Environmental Operating Conditions*

Attention should be given to the environmental operating range of the camera equipment (e.g. temperature, power supply fluctuations, humidity, etc.) indicated by the manufacturer prior to it being procured or used for traffic enforcement purposes. Cameras must not be used for enforcement outside the manufacturer's indicated acceptable operating conditions.

#### *3.1.2.5 Electromagnetic Compatibility*

The CCTV camera must comply with the current legislation that applies to all apparatus liable to cause electromagnetic disturbance or the performance of which is liable to be affected by such disturbance. This is the UK Electromagnetic Compatibility Regulations 2016 (UKCA mark). Also, European Directives 2004/104/EC (E mark), or 2004/108/EC (CE mark) may be accepted under certain circumstances. This legislation prescribes the relevant protection requirements, compliance procedures, and the technical documents and/or marking that must be associated with the equipment.

### 3.1.3 Factors for consideration in relation to the procurement, siting and operation of CCTV cameras and associated systems

The following information (Section 3.1.3) has been produced to assist the providers of Traffic Enforcement systems. This is based on current best practice and user experience, but is ***not*** a requirement for the certification of systems. Sample test procedures are given in Section 5.4.

#### *3.1.3.1 Imaging Device, CCTV Camera*

Most current CCTV cameras are likely to employ a CCD or CMOS device to obtain the image. Previously only ½ inch CCDs were capable of recording adequate quality and resolution images. However, with emerging technologies and miniaturisation, smaller imaging devices (e.g. ¼ inch CCDs) are likely to be capable of providing high quality images at an appropriate resolution that would meet the requirements for enforcement.

#### *3.1.3.2 Camera / lens arrangements*

Traditionally professional quality CCTV cameras have come as two-part combinations with a camera body (including a defined lens mount – such as a 'C' or 'CS' mount) and a separate lens (for which many options would be available). This arrangement allows for a wide range of camera combinations and facilities that would

be suitable for enforcement. However there are now also various miniaturised integrated camera/lens units that can provide high specification imaging facilities and that might meet the requirements for enforcement in a smaller sized unit that is more consistent with the environmental aspirations of many Local Authorities. Either camera arrangement is acceptable in principle, subject to meeting the other requirements for providing high quality images for use in enforcement.

#### *3.1.3.3 Zoom Speed*

The time required for a camera to zoom between the CUV and the CV should be sufficiently low to allow satisfactory operation across the required range of the enforcement zone. Particularly at sites where there are a large number of contraventions, or where long enforcement zones are being monitored, fast zoom lenses can ease the camera operator's enforcement duties and might be particularly effective in operation.

#### *3.1.3.4 Shutter Speed*

The camera might need to be capable of working at fast shutter speeds, to reduce blurring of the video images of vehicles passing the camera. Depending on site specific conditions, a shutter speed of between 1/250 and 1/1000 second might be necessary to obtain clear images of VRMs - to prevent images becoming blurred through movement of the vehicle during the exposure (of each video frame). However this might cause problems in low lighting conditions. Therefore, for maximum flexibility of operation, the CCTV camera should be capable of being (remotely) switched between different shutter speed settings. Typically this may be done using software and/or hardware activated by an operator / observer at the CCTV control room. Large horizontal or vertical angles of view (from oblique and/or high locations) might require video to be recorded using the faster shutter speeds indicated. (Note – whilst all cameras have a shutter speed, this generally relates to an electronic 'virtual' shutter – not a physical camera shutter).

#### *3.1.3.5 Stability of the CCTV camera during PTZ operations*

On some cameras the quality of the images recorded whilst panning, tilting or zooming might be reduced or become blurred. This will depend on the camera/lens combination, the motor equipment performing PTZ operations, the stability of the column that the camera is mounted on – and other factors (such as the height of the camera – and current weather conditions). This might restrict useful images being recorded for enforcement purposes except when the camera is virtually stationary in the CUV and CV views. However, faster shutter speeds might resolve this problem.

#### *3.1.3.6 Quality of the camera and lens (or the camera/lens combined unit)*

Very high quality camera/lens combinations might make it possible to clearly identify a VRM with a less zoomed-in view. Conversely, (relatively) lower quality equipment might require longer (and possibly faster) zoom lenses to show the VRM as a higher percentage of the frame width in order to compensate for the reduction in quality.

### *3.1.3.7 Quality of other system components*

In specifying a camera enforcement system, consideration needs to be given to all the components of the system, as these could have an effect on the required specification for CCTV cameras. Overall, the quality of the recorded images (and any extracted still images from the image stream) will depend on the quality of the camera/lens combinations; the communication systems and cabling between systems; the recording equipment; and the facilities for grabbing still images from the image stream. If there is any noticeable degradation of the video recordings when re-played, (by comparison with the image stream as observed by an operator) or the images grabbed, the quality of some components of the full system might need to be re-assessed.

### *3.1.3.8 Electronic Enhancement of Video and Still Images*

Most cameras will provide some automatic and manually operated facilities to improve the quality of the image being viewed (and recorded) – such as auto-iris (brightness), white balance, contrast and saturation levels. Some cameras might provide other more advanced facilities (e.g. to reduce headlight glare). Whilst recordings should ***not*** be adjusted or enhanced after they have been recorded, it is normally necessary to use some additional processing (e.g. using image filtering technology) to produce acceptable still photo images from the image stream. This is particularly necessary for recordings from analogue video streams where some form of de-interlacing is necessary to produce acceptable still images of moving vehicles.

### *3.1.3.9 Environmental Conditions*

CCTV cameras might be required to operate in a wide range of operating conditions. However temperature, humidity and other factors can affect camera operation and the clarity and accuracy of the images produced. When procuring (or using existing) cameras, consideration should therefore be given to the environment in which the camera will need to work, in order to ensure that it is operated for enforcement purposes within the manufacturer's indicated operating conditions.

### *3.1.3.10 Maintainability*

It is essential that CCTV cameras on-street are inspected and cleaned regularly, and maintained as necessary, to ensure that clear video recordings are obtained. It might therefore be desirable for the same or similar cameras to be used at more than one site – to increase the ease and consistency for operation and maintenance.

### *3.1.3.11 Other Site Related issues:*

#### 3.1.3.11.1 Height of the camera

This affects the vertical angle of view of the VRM, and it's readability by an observer.

#### 3.1.3.11.2 Horizontal angle of view (in relation to the direction of traffic)

This affects the horizontal angle of view of the VRM, and it's readability by an observer. However it also increases the potential for the speed of a vehicle to cause

blurring of the images recorded on video. More oblique angles of view are therefore more likely to require faster shutter speeds to obtain clear video images.

#### 3.1.3.11.3 Proximity of the Enforcement Zone

If the enforcement zone is very close (just underneath the camera) – or too far away, there might be problems obtaining satisfactory video images. A video zone very close to the camera might require fast combined PTZ operations – particularly if the enforced area is not directly in line with the camera - and this might be difficult for operators to carry out. Distant observations might occasionally suffer from mist/fog/haze reductions in visibility that could make VRMs more difficult to read.

#### 3.1.3.11.4 Street Lighting

Where street lighting is poor, it might be more difficult to read a VRM and also to identify a vehicle type (make and model) in hours of darkness or poor light – which is necessary for enforcement purposes. Improvements to street lighting – and cameras with better low light sensitivity - could overcome these problems.

#### 3.1.3.11.5 Landmarks

A location specific landmark or marker may usefully be included in the captured images, as an additional identifier of the location.

## 3.2 Time, date and location data

The enforcement equipment must maintain a system clock that is regularly synchronised to a nationally recognised standard clock. The system clock must, at all times, be within 10 seconds of coordinated universal time (UTC) as disseminated in the United Kingdom by the National Physical Laboratory using the MSF transmitter. The system clock must be synchronised with a suitable standard clock a minimum of once in any 14-day period. The specified synchronisation period is based on the longest time that the MSF transmission is likely to be unavailable for maintenance etc. Authorities are advised to be mindful of this (and the impact of similar factors on other independent national clocks, where used) when setting their synchronisation schedule; more frequent checks might be appropriate.

Each image within a context sequence should contain embedded data consisting of time, date, a unique frame identifier and the enforcement location, and must be fit for purpose. Fixed or redeployable camera enforcement locations may be shown by references taken from a schedule.

3.2.1 Where computer network time protocols or a satellite service is used for time synchronisation, (e.g. the Global Positioning System, Galileo, etc.) the time synchronised should be shown to be traceable to a nationally recognised standard clock.

3.2.2 It should always be clear whether Universal Time or British Summer Time is being displayed.

## 3.3 Transmission systems

3.3.1 Transmission systems must be demonstrably transparent to video, camera command and telemetry signals and be reasonably immune to third party interference such that transmitted images remain fit for purpose.

3.3.2 Where back-office systems are distributed across several sites or where home working may be permitted. An appropriate security policy should be in place along with suitable encryption to protect evidential recordings.

3.3.3 Where back-office systems are hosted by a third party, details of the ownership and technical details of remote facility or data centre should be supplied in the TCF along with details of communications links and security policy. (ISO 27001 compliance for example)

## 3.4 Recording Systems

Recording systems must;

- Comply with at least one of the options described in 3.4.1, 3.4.2 or 3.4.3 below.
- Comply with the EMC requirements in 3.1.2.5
- Have appropriate Security, Reliability and Integrity safeguards, as outlined in sections 3.4.2.1.3/4/5
- Ensure that the copying (or transmission) process for images must not further compress or otherwise modify the format or quality of the original recordings.

### 3.4.1 Digital Recording with no data redundancy or recovery facilities

Where recording takes place on a system with no real time data recovery or data redundancy facilities, two simultaneous recordings onto separate storage devices must be made at the time of capture. It is preferred, but is not a requirement, that the two copies be made after conversion to the digital domain. In this scenario, it would be acceptable for the second recording to be made at lower resolution and frame rate or at higher compression settings than the first. In the case that the second recording is made at lower resolution, frame-rate or at higher compression, then once a decision to proceed with issuing a PCN is made, (after review of the contravention), a further exact digital copy of the master copy of the evidence must be made on a separate storage device or a removable storage medium.

### 3.4.2 Digital Recording with Data redundancy & recovery facilities

Where an enforcement system provides digital facilities for recording video data such that the system provides Security, Integrity and Reliability, (see definitions below), it may be considered to comply in full with the requirement for dual simultaneous recording - as the recorded data is securely stored on a minimum of two independent storage devices, and recovery of data should be possible even if one or more storage devices fail.

#### *3.4.2.1 Method for Single Recording systems*

##### 3.4.2.1.1 Initial Process

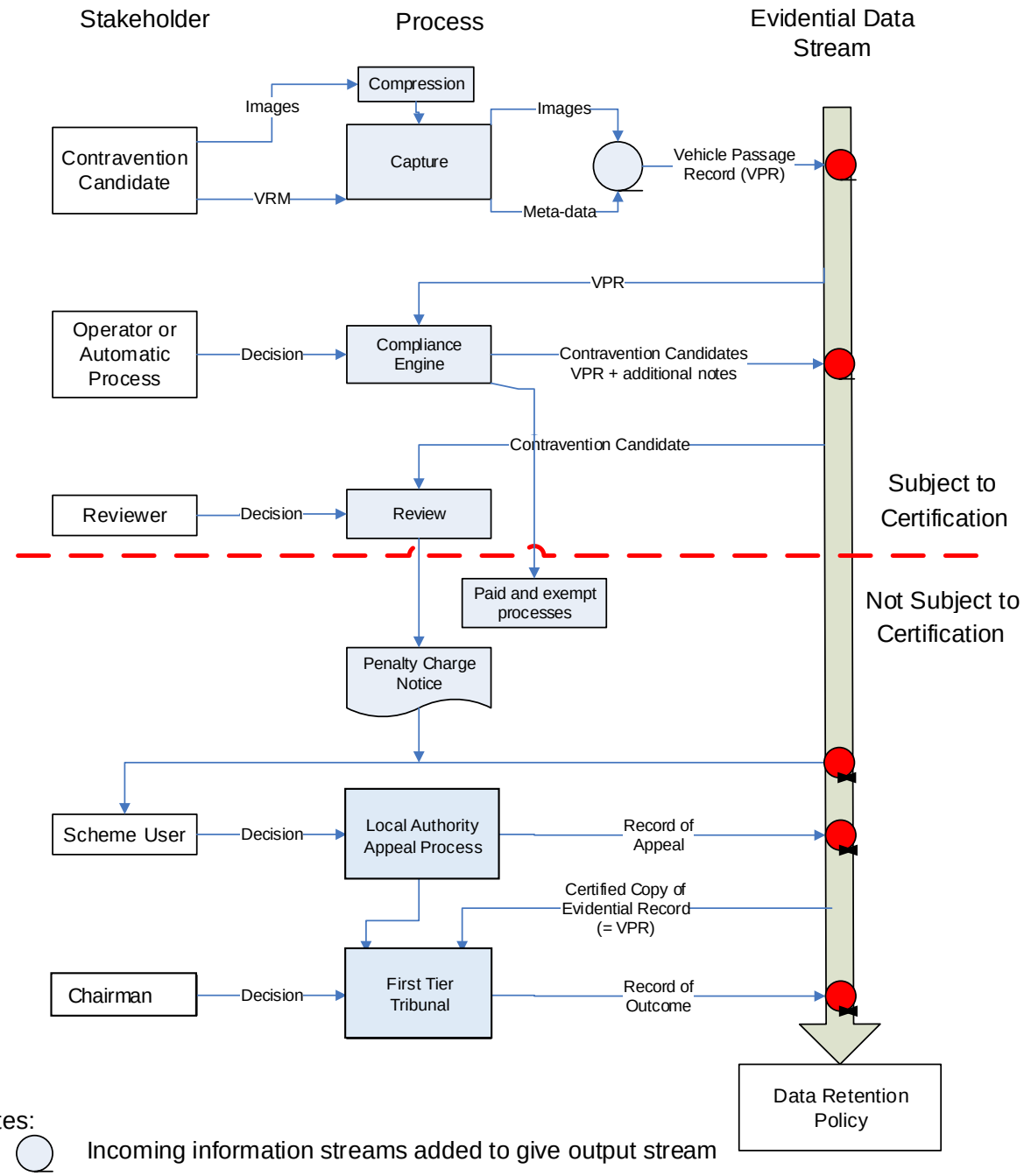
a) Record images from CCTV Matrix – of a whole Enforcement session - onto a secure server (or other high volume digital storage device) – at the time of observation.

b) Identify start and end of *potential* contraventions during enforcement session – using start/end controls - that are tagged (or otherwise identified) on the recording.

c) Images of the *potential* Contraventions (from the start to the end point of each contravention – possibly including an additional period of the image stream before and after each image) are copied to a Traffic Enforcement Video Store – TEVS - (possibly with related text contravention data) – on a secure server (or other secure high volume digital storage device). The copying process for producing these video images must not further compress or otherwise modify the format or quality of the original video recordings. See figure 2.

**Figure 2 Traffic Enforcement Data Flow**

The data flow diagram on the next page illustrates the typical process for a PCN which is challenged by the recipient. These principles apply to both attended and unattended systems - i.e. irrespective of whether capture is by operator or automatic process.




Notes:

1. Incoming information streams added to give output stream

2. Incoming information streams added to evidential stream

3. Information that is aded to the evidential stream shall not be changed or deleted until the data retention policies dictate that deletion / destruction is permitted. Normally this is a defined period after the PCN is resolved (either paid or withdrawn).

4. Compression of the images for evidential purposes should ensure that the close-up and context views remain fit for purpose. Lossy compression techniques may be acceptable provided that the fitness for purpose requirements are met.

d) Each image is reviewed to assess if the *potential* contravention is an actual violation of the LEZ at the site. If necessary, additional earlier or later video (not contained in the images) might be available for viewing at this time to clarify whether the apparent contravention is an actual violation.

e) Still images of each ***confirmed*** Contravention are selected, extracted (grabbed) and stored with (or linked to) the Contravention data records (that are likely to be in text format) during the Contravention Review process.

f) Contravention data (including still images from the recording) is sent for processing – so that a PCN can be issued to the owner / driver of the vehicle (note – the PCN issuing process is ***not*** described further here as it is outside the scope of this certification process).

g) Video recordings of the full enforcement sessions may be deleted or overwritten after the Contravention Review process is complete – as the Contravention video evidence is now securely stored in the TEVS.

h) **If there is an appeal against the PCN**, a further video copying and transfer process is required. This is described in Section 3.4.2.1.2 below.

i) If there is no appeal, and the PCN is cleared or paid, all video, video images, and contravention data should be deleted after the PCN is cleared or paid (although this should be after an appropriate archive period).

#### 3.4.2.1.2 Where Working copies are required

The following is a recommended process for creating and storing further copies of Contraventions (on removable media – or in an electronic format that may be encrypted and sent by e-mail or by some other form of electronic transfer) is only likely to arise if there is a request to view the recording of the Contravention, or if the PCN is referred for review by the local authority or appeal to the First Tier Tribunal: -

a) The Master copy is effectively considered to be the video image which is stored on the TEVS. A separate Master or Working copy of the contravention would ***not*** normally be produced on removable media.

b) Working copies of a Contravention are produced directly from the Master copy which is held on the TEVS – **if and when these are required** for viewing; for sending to the local authority for review or First Tier Tribunal on appeal, the appellant (and/or their representatives); for use in the local authority review of First Tier Tribunal; or for supplying to other approved parties as determined in local procedures. Unless specifically required (for example - for display only to authorised viewers on a web site), the copying process for producing these working copies should ***not*** compress or otherwise modify the format or quality of the original video recordings. The copies may be on a removable WORM medium (CD-R, DVD-R, or similar) – or a computer file, for example – for sending by e-mail (which may be encrypted) or for use to display on a web site (to authorised persons).

c) Once the PCN review or appeal process has concluded a legally binding decision, all video recordings, video images, WORM media and contravention data should be deleted or destroyed (although this should be after an appropriate archive period in accordance with applicable legislation).

#### 3.4.2.1.3 Data Safeguards

As all the *potential* contravention data in this process may be held within a single digital recording system, additional safeguards are required to protect the evidential quality of the data. These safeguards should be the digital equivalent of the physical safeguards used to protect contravention data on Analogue systems using removable media. The following provisions are general requirements. Other requirements may be determined by the Scottish Tribunals or in local system procedures.

#### 3.4.2.1.4 Integrity

The system must provide facilities to ensure that if (image) data is amended or altered in any way, the changes are detectable. Typical examples might include hash functions or watermarking of the data. Where a hash function is used, a change to the data would show up as an error, whereas a watermark would normally become visible in some way if the data is altered. Other methods might also be viable.

#### 3.4.2.1.5 Security

The system must provide a means to protect the data and system information so that only people who are authorised to access, use, edit, copy or delete the data have access to it for these purposes. Typically, this may involve a hierarchy of password protection so that individuals are only able to carry out the activities for which they are authorised. Physically, this might also require the systems to be located in secure areas so that only authorised operational and maintenance personnel can get access to these computer systems.

If the recording system is connected to a PCN processing (or other) system via a network or the Internet, the contravention and recorded data must be secured so that it is inaccessible via this connection except to authorised users and systems. This might require the use of firewalls, data encryption and/or other measures to prevent unauthorised access to the contravention evidence.

Where data is released from a secure environment, (e.g. to send the data to an adjudicator), this is likely to require other forms of protection. Where data is sent electronically (e.g. by e-mail or using FTP transfer), data encryption is likely to be required – to ensure that unauthorised persons cannot see or amend the data. Data released on removable media should be secured in a WORM format (i.e. the DVD, CD, etc. should be 'closed' – so that it is not possible to amend the data on the media).

#### 3.4.2.1.6 Reliability

It is important that should an equipment failure occur on the computer system, or on one or more of the storage devices, the computer systems should (so far as is possible) continue to operate, and that enforcement data is retained – or is available on the system in some other way such that it is recoverable. Typically this might be achieved through the use of RAID server technology. However, regular data backup facilities might be an alternative or complementary means of achieving this objective.

It should be noted that, where suitable digital storage arrangements are made using

RAID servers or an equivalent technology, and there is a sufficient degree of data redundancy such that data is preserved even if one or more storage devices fail, this form of storage will be considered to provide the digital equivalent of a dual recording capability. This is because the data is clearly stored more than once in the system such that data recovery is still possible even if some data is lost as a result of an equipment failure.

Power protection might also be required (e.g. Uninterruptible Power Supplies for the system) to ensure that the computer system does not corrupt data in the event of a sudden power failure.

### 3.4.3 Recordings to Removable media (e.g. video tapes and DVDs)

Where the recording system employs removable media, two recordings of the image stream must be made on separate media (e.g. tape, flash memory or DVD disk) at the same time. One of the resulting media will be preserved as the Master and stored securely until no longer needed, whilst the other will be deemed to be the Working copy and used to process the *potential* contravention and for later processes. The recordings may be analogue or digital.

### 3.4.4 Electromagnetic Compatibility

The provisions of paragraph 3.1.2.5 must also be applied to recording systems.

# Chapter 4 Requirements for Unattended Systems

## 4.1 Introduction

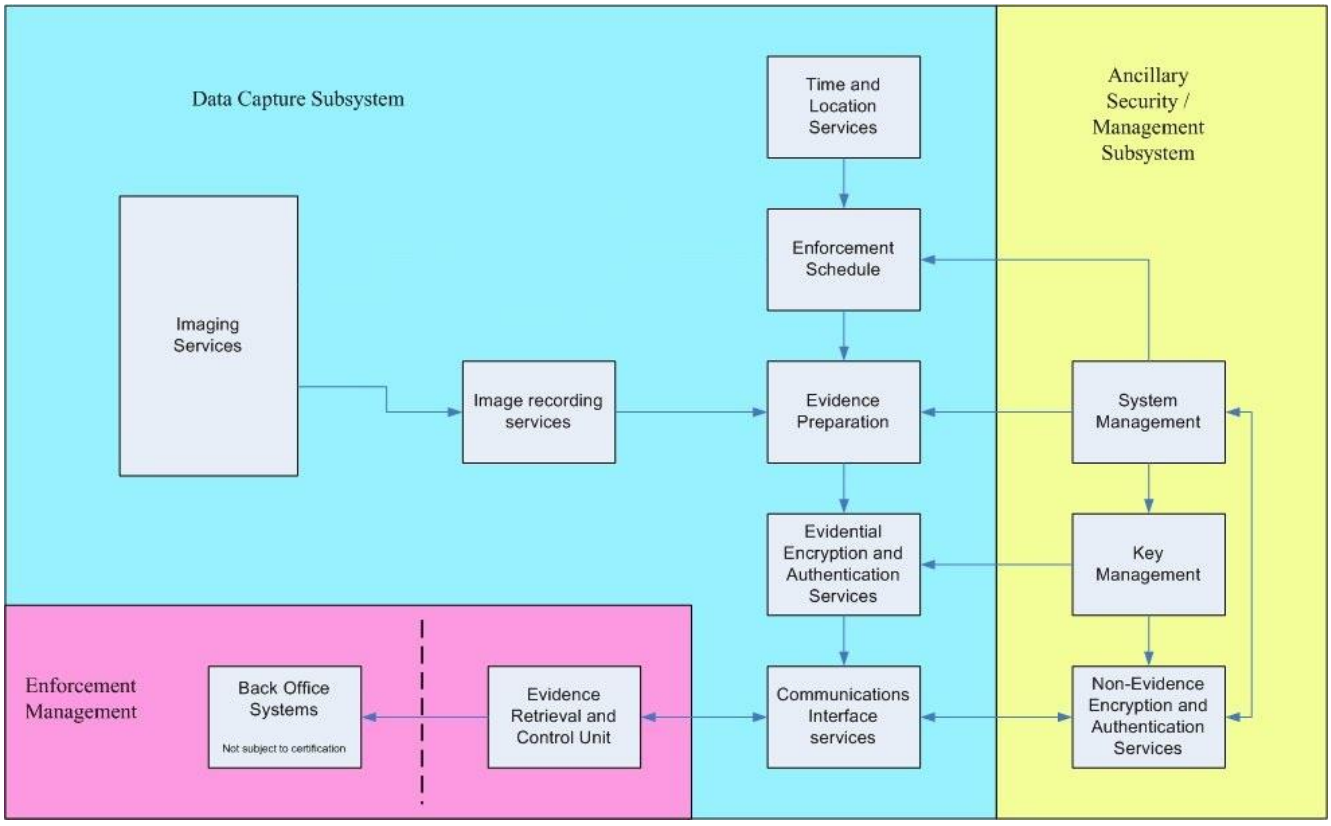
Systems will be required to include positive mechanisms to prevent recording at times outside enforceable hours. In the case of mobile systems, they should include a mechanism to allow the location of the enforcement camera to be determined with sufficient accuracy to restrict enforcement to locations at which a contravention might be committed.

## 4.2 Functional Requirements

These requirements are presented as a series of statements of fitness for purpose. In a number of cases, it has been necessary to define the requirements using definitive limits. It should be noted that where definitive limits are given, then these are the minimum acceptable criteria.

These requirements are presented based upon the illustrative design shown in Figure 3. Each of the main sections of this part reflects the top level functional groupings shown with the shaded areas of the diagram. Within each major section, the functional elements that make up functional grouping will be described in detail.

**Figure 3 Illustrative Enforcement System Functional Block Diagram**



### 4.2.1 Data Capture

This section covers requirements for the components of an unattended enforcement system that are to do with the acquisition of evidence of a *potential* contravention and the functions necessary to compile the evidence into coherent evidence packages (hereinafter called Evidence Packs).

#### *4.2.1.1 Imaging Services*

This section describes the fundamental requirements for the image quality and the camera operational performance.

Cameras equipped with ANPR functionality should also meet the requirements given in Annex 3, (Section 5.3).

#### *4.2.1.2 Image requirements*

Imaging services must generate images that at least meet the resolution requirements described in paragraph 3.1.2.1 and that allow a system operator to simultaneously determine the target vehicle registration mark (VRM) and to examine the context under which the contravention took place. In this context, the term simultaneously shall be taken as meaning that the context and close-up images have demonstrably been taken at a point that is demonstrably within 0.5 seconds of the contextual image. All images must, as a minimum, be marked with location, time, date and a unique frame identifier and must be fit for purpose.

General advice given in Section 3.1.3 also applies for unattended systems.

##### 4.2.1.2.1 Context View

The provisions for attended systems in paragraph 3.1.1.1 apply to unattended systems also.

##### 4.2.1.2.2 Close-up View

The provisions for attended systems in paragraph 3.1.1.2 apply to unattended systems also except that the close-up view is permitted to be monochrome and may, if required, be taken with an infra red (IR) sensitive camera and illuminated with an IR source.

##### 4.2.1.2.3 Frame rate

The provisions of paragraph 3.1.1.3 apply to unattended systems also, (only where an image sequence is to be captured rather than single images). It is permissible for a single close-up view to be captured provided that this image is demonstrably contemporaneous with the context image sequence.

##### 4.2.1.2.4 Low Light Performance

The provisions for attended systems in paragraph 3.1.2.3 apply to unattended systems also.

### 4.2.2 Time and Location Services

Time and Location services provide the enforcement system with the time, date and, where appropriate, location information that is used both to determine (when used in conjunction the enforcement schedule) whether a contravention has taken place and to record the same information for evidential purposes. For both these reasons, it is imperative that both time and location information are accurate. Clock synchronisation events must be recorded in the systems operations logs and, if unsuccessful for more than the required synchronisation period specified in paragraph 3.2, an Evidential Alarm shall be raised, and associated with all vehicle passage records created until the cause of the alarm is resolved.

#### *4.2.2.1 Time and date*

The unattended enforcement system must maintain a reference clock as described in paragraph 3.2.

#### *4.2.2.2 Location*

For mobile systems, the enforcement equipment must be capable of determining the location and direction of travel of the camera with sufficient precision that an enforcement officer viewing the resulting evidence can unambiguously identify the place that the contravention took place. This requirement must be met for all conditions of the built environment (including, but not limited to, urban canyons, bridges and tunnels). The location system must update sufficiently regularly that this requirement is met for all permitted enforcement vehicle speeds. Failure of the location system to generate an appropriate location reference must cause enforcement to be suspended and must be recorded in the system log.

***4.2.2.3*** If a mobile system is in motion and attempting to capture a potential contravention of a moving vehicle then it must ensure that the required close up & context views specified in sections 3.1.1/4.2.1.2 are properly captured. Alternatively, a mobile system may be operated only whilst it is stationary.

***4.2.2.4*** Consideration should be given to the accuracy with which location may be determined whilst mobile systems are operating close to the edge of the defined LEZ.

***4.2.2.5*** For static and redeployable systems, the site commissioning procedure must be used to enter the known location of the enforcement equipment (if the system does not capture its own location).

### 4.2.3 Contravention Capture

Contravention Capture provides the mechanisms for detecting that a potential contravention is taking place, for determining that it is taking place at an enforceable time (and in the case of mobile systems at an enforceable location) and recording the evidential information necessary to allow appropriate enforcement actions to be taken.

#### *4.2.3.1 Contravention Detection*

Unattended systems must have a mechanism that sorts and detects possible contravention candidates. This may be by manual or automatic means. In operation, the contravention detection systems shall seek to minimise the number of false positive contravention detections. This part of the system shall not be a part requiring certification; however, information on the processes and procedures used shall be made available to Scottish Ministers or their representative during the assessment process.

#### *4.2.3.2 Enforcement Schedule*

Unattended enforcement systems must incorporate a mechanism that prevents enforcement evidence from being gathered at times that there is no valid enforceable regulation. In the case of mobile systems, the enforcement schedule functionality has to ensure that both the location and the time are enforceable before permitting the gathering of evidential data. It shall be noted that it is permitted for mobile systems to allow a positive guard-band around an enforcement zone to allow for possible navigation system or camera orientation errors.

#### *4.2.3.3 Evidence Recording*

This clause applies only where an image sequence is to be captured rather than single images**.**

This component is responsible for ensuring that when a *potential* contravention is detected, an appropriate amount of pre-trigger and post trigger image sequence is recorded to allow an enforcement operator to determine whether a contravention took place and that no mitigating circumstances were present. This image sequence must be recorded with sufficient image refresh rate that it is clear that a specific action took place.

This component of the enforcement system must comply with the image sequence compression requirements described in note 4 to Figure 2.

### 4.2.4 Evidence Packaging and Transmission

In order to be useful an unattended enforcement system has to be able to get the captured evidence back to a back-office facility where the evidence is reviewed and an enforcement officer decides about whether a penalty charge notice is justified. To do this, the evidence has to be packaged and transmitted securely to the back office.

Transmission may take place over a secure private network in which case encryption is not required and the data merely needs protecting by means of appropriate evidence package authentication. Where data is to be transmitted over a network that is accessible to any third party, then both encryption and evidence package authentication must be used. In addition, where a third-party accessible network is used, a secure interface must be used at both ends of the link. The secure interface must reject any communications coming from any source other than an Evidence Retrieval and Control Unit (ERCU) using a predefined schedule or protocol.

The provisions for attended systems in section 3.3 apply to unattended systems also.

#### *4.2.4.1 Evidence packaging*

Prior to transmission, the collected evidence for each *potential* contravention must be packaged into a single coherent whole that can be verified as a complete package. This evidence pack must contain, as a minimum, an image showing the context of the contravention taking place, a close up view and metadata relating to the circumstances of the contravention.

##### 4.2.4.1.1 Authentication

Once complete, the evidence pack must be authenticated using a suitable authentication algorithm. Annex 6 provides further details of suitable authentication techniques.

##### 4.2.4.1.2 Cryptographic services

Cryptographic services (Encryption and decryption) are required where any part of the data channel between the unattended outstation and the back office is carried over a publicly accessible network and when the back office is operated using communications links across more than one site, (including any form of wireless communication). Data must be encrypted using a suitable data encryption technique. Annex 6 provides further details of suitable encryption techniques.

Where data encryption is required, all data exchanged between the back office and the unattended outstation must be appropriately encrypted. Data relating directly to the evidence collected (evidential data) and all other (non-evidential) data must be encrypted with different keys.

Where Vehicle Passage Records are stored locally at the outstation and have not yet been encrypted ready for transmission; appropriate security is still required. This may take the form of an encrypted filing system. In which case the filing system keys are still subject to deletion on unauthorised access (in accordance with Annex 6 clause 5.6.2.9).

#### *4.2.4.2 Management Functions*

It must not be possible to take any kind of control over the unattended outstation other than by the delivery of correctly authenticated system control packets (including but not limited to: enforcement schedules, status polls and key management).

Whenever an enforcement outstation is installed on a network that is accessible to a third party, the unattended outstation must provide a secure interface through which only authorised traffic can pass. This interface must be demonstrably resistant to a real time attack.

### 4.2.5 System Management

The unattended outstation must provide a number of management functions. These must be responsible for the recovery and implementation (at the appropriate time) of the enforcement schedule, the recovery and implementation of the initial keys (or key encryption keys) and the management of system operation, including the secure shutdown of the system in the event of any unauthorised access.

The system management functions must also monitor the operation of the system and suspend enforcement should any of the following conditions apply.

- Local environmental parameters exceed certified limits.
- Clock sync failure.
- Location missing / error >30m as indicated by failure of GPS or similar locating system to lock or as indicated by an inconsistent step in reported position.
- Encryption keys out of date.
- Enforcement Schedule out of date.

In the event that enforcement is suspended, the system must transmit a clear-text alarm message indicating that it has suspended enforcement. In addition, a cipher-text (encrypted) detailed status message describing the fault detected must be transmitted to the back-office.

The gathering of vehicle passage records may continue during the period of suspended enforcement, and may be used for charging purposes. It is recognised that it is only possible to distinguish between those vehicle passage records required for charging, and those required for enforcement at some time after they have been captured.

#### *4.2.5.1 System management and Audit trail*

System management functions are also responsible for the preparation of a range of evidential support information such as audit trail information and other data, such as the system log, that might be useful to the enforcement operator in judging whether an enforceable contravention has taken place. Any such management data must be packaged as defined by the manufacturer and regularly transmitted to the back office as an integrity protected and authenticated package. System management information must be protected with a second set of encryption / authentication keys. These 'non-evidence' keys must be of similar security level to those used to protect evidential data.

With the exception of urgent system alarms, which may be in clear-text (unencrypted), all system management information must be protected as described above.

#### *4.2.5.2 User Access*

System management functions are responsible for the management of user access to the unattended enforcement system. Any attempt to access the unattended enforcement system must be logged in the system audit trail and access to the system shall only be permitted where the user validates their access using a Password, Personal Identification Number or a service token. The TCF must clearly show when security is under sufficient threat to constitute an unauthorised access, in which case the system must inhibit any enforcement recording that is in progress and securely delete all encryption keys or unsecured evidence packs.

Remote user access is permissible where the level of security is shown to be sufficient for the extra risk posed by remote access.

### 4.2.6 Enforcement management

The enforcement management component of the unattended enforcement system, also known as the back-office is that part of the system housed in a secure environment (a trusted environment). The back office is made up of a number of interlocking functions. These are: the secure interface, the evidence retrieval and control unit, the internal secure interface and enforcement management system.

The back-office provisions for attended systems in sections 3.3.2 & 3.3.3 also apply to unattended systems.

#### *4.2.6.1 Secure interface*

Where there is an external interface to the back-office it must be provided with a secure interface that mirrors the functionality of the secure interface housed in the outstation. This secure interface must only permit the receipt of correctly formed data packets (including but not limited to evidence packs, evidential support packages, outstation status messages and outstation alarms).

#### *4.2.6.2 Evidence retrieval and control unit*

The Evidence Retrieval and Control Unit (ERCU) manages all communications with the unattended enforcement systems. It is responsible to acting as a gateway for evidential and non-evidential information being received from the unattended enforcement systems and for enforcement control information being sent from the back office to the outstations.

Where the ERCU is receiving evidential data from unattended enforcement systems, it is recommended that the ERCU should ensure that the data is received within 48 hours of the possible contravention taking place, before writing the evidence pack to the internal secure interface. In any case this must be within a maximum of 14 days.

Where the internal secure interface is an air gap, the ERCU must write the evidence pack to Write Once Read Many (WORM) media within a maximum of 14 days of the possible contravention being detected.

#### *4.2.6.3 Internal secure interface*

The internal secure interface (represented by a dashed line on Figure 3) isolates the publicly accessible or external components from the secure environment that manages the enforcement operation. Where an applicant wishes to retain compatibility with the criminal process as documented by the Home Office DSTL, this must be an air-gapped interface with no direct data connection. In this case data must be written to WORM media within 48 hours of capture to ensure that the evidence cannot be compromised.

Where compatibility with the criminal process is not required, an appropriate arrangement of firewalls and transfer servers may be used.

Where the enforcement management system does not provide secure and reliable storage for evidence data, then the internal secure interface must generate WORM media as described above.

#### *4.2.6.4 Enforcement management system*

The operation of the enforcement management system (EMS) is not part of the certification requirements for the system and this description is only given here to aid reader understanding. The enforcement management system provides the system operators the facilities to view retrieved evidence packs, to issue penalty charge notices if appropriate, to prepare enforcement schedules and to monitor the health of any outstations connected to it. It is an assumed requirement on the EMS that it provides reliable and secure storage for evidence data. If this is not the case, the internal secure interface must generate all evidence on WORM media.

#### *4.2.6.5 Additional Functionality*

Systems may provide additional functionality to assist in traffic management activities. However, any such functionality must not affect compliance with this document for civil Traffic Enforcement and should comply with other legal obligations.

## 4.3 Non-Functional Requirements

This section is concerned with those environmental factors that could cause the evidence generated by an enforcement system to be tainted by some question of incorrect operation. It is not intended that this section in any way replaces the normal environmental requirements that would be included as part of the procurement statement of requirements. Indeed, these requirements will normally be insufficient for procurement purposes.

### 4.3.1 Thermal

Unattended enforcement systems must be capable of being stored, unpowered, for long periods under adverse conditions.

In operation, the unattended enforcement system must function correctly in all respects over at least the ambient temperature range of -10°C to +40°C. At all temperatures above 20°C, the unattended enforcement system must operate correctly in the presence of 80% relative humidity. It should be noted that these are the minimum requirements and manufacturers are free to seek certification of unattended enforcement equipment to wider temperature ranges if required.

Unattended enforcement equipment must be fitted with a sensor to raise an evidential alarm if the system is detected as operating outside the temperature range certified.

### 4.3.2 Electromagnetic Compatibility

Unattended systems must be immune to interference from a wide variety of electromagnetic threats in accordance with the legislation described in paragraph 3.1.2.5.

## 4.4 Recommended Design Limits and Tests

This section will describe the design limits that are necessary to meet the fitness for purpose requirements in sections 4.2 and 4.3 above. It also describes recommended tests that should be carried out on any system submitted for certification. It is made

up of a number of parts. In each part, suggested test methods are provided together with illustrative test limits. It is the responsibility of the designer seeking certification to provide a fully worked up test procedure for the approval of Scottish Ministers. It should be noted that whilst this section is guidance, any deviations from the limits given in this section will require a full and detailed justification before certification will be granted.

### 4.4.1 Recommended Tests for Functional Requirements

#### *4.4.1.1 Data Capture*

This section covers testing of those functions that are to do with the capture of a potential contravention and preparation of the evidence pack.

#### *4.4.1.2 Context Image Capture*

##### 4.4.1.2.1 Image quality

The context images should be checked and confirmed to be of adequate resolution, focus, clarity and substantially free from motion blur and compression artefacts. The minimum resolution for the context images should be 720 Pixels wide by 288 Pixels high. (Note: this reduced image height applies only for a de-interlaced PAL video signal)

##### 4.4.1.2.2 Frame rate

This clause applies only where an image sequence is to be captured rather than single images.

The context image stream should comprise a minimum of 5 frames per second and no two images should, on average, be more than 200ms apart. This should be confirmed by counting the number of frames in each second of the context image sequence.

##### 4.4.1.2.3 Embedded data

In addition to the image of the context of the potential contravention, each image within the context sequence should contain embedded data consisting of the time, date, a unique frame identifier, and, where not in a fixed location, the enforcement location, and be fit for purpose. It should be noted that, if compliance with the Home Office DSTL requirements is sought, this information should be (in the order given): the date in days, month, and year, the time in hours, minutes, and seconds, the day of the week, location and frame count from the beginning of the recording.

#### *4.4.1.3 Close-up view capture*

The unattended enforcement outstation should generate an image that it is possible to unambiguously read the contravening vehicle's VRM. The close up view should have the following minimum characteristics:

- The image presented as the close-up view should have a minimum resolution of 720 Pixels wide by 288 pixels high. (Note: this reduced image height only applies for a de-interlaced PAL video signal).

- The vehicle registration mark should be represented by a parallelogram of at least 140 pixels wide by 30 Pixels high for a vehicle displaying a 'one line' style plate in accordance with The Road Vehicles (Display of Registration Marks) Regulations 2001.

#### *4.4.1.4 Time and Location*

##### 4.4.1.4.1 Time

System time accuracy should be tested by recording a number of simulated traffic contraventions with a clock accurately synchronised to a reference time source present in the field of view of the context camera. A number of simulated contravention captures should be carried out. For all tests, the time recorded on the evidence pack should be within 10 seconds of the time displayed on the reference clock. The test should be repeated 14 days later and again the time difference should be less than 10 seconds.

It should be noted that there are a number of possible sources for reference time and that they may differ in the absolute time recorded by an offset that is from time-to-time altered. The preferred reference source that should be used for traffic enforcement is the time broadcast by the National Physical Laboratory via the MSF transmitter.

##### 4.4.1.4.2 Location

A mobile system should be driven around a predetermined route (of at least 5km) over at least 10 accurately and evenly distributed surveyed datum points returning to the original location. The route should include a variety of built-up environments. Simulated contraventions, including the locations should be recorded at each of the datum points by the enforcement system and compared with the known values for the datum point. The average error of the location fix should be less than 10m. (The end point should be one of the datum points.)

#### *4.4.1.5 Metadata*

The data supplied as part of the evidence pack should be checked and should contain, as a minimum, the following items:

- Time and Date that the suspected contravention was detected.
- The evidence pack unique identifier.
- The unique identifier for the equipment that captured the suspected contravention.
- The location at which the contravention was detected (for mobile unattended enforcement systems only). (In this context, "location" means the point at which a contravention will be first detected or the point at which the close-up view best shows the VRM).

In addition, it should be noted that the encryption and authentication information appended to the evidence pack prior to transmission is not treated as meta-data.

#### *4.4.1.6 System Management*

##### 4.4.1.6.1 Key Management

The operation of the key management suite should be demonstrated for all anticipated key operations. This includes, but is not limited to, the following items:

- Receive, validate and implement new keys for both evidential and non-evidential data.
- Manage key validity periods and inhibit the generation of evidence if any keys have expired.
- Secure deletion of key data in the event of any unauthorised access to the system.

Any operation that modifies, or has the potential to modify, a key should be logged in the system audit log and this should be confirmed.

##### 4.4.1.6.2 Environmental Monitoring

Unattended systems performance in the event of environmental conditions exceeding the certified range should be demonstrated. In the minimum case, this should be the production of an evidential alarm in the event that the systems temperature exceeds the certified range. This should be demonstrated for both extremes of temperature.

##### 4.4.1.6.3 System Audit Logging

The system audit log should be transmitted back to the back office regularly and should contain a record of any significant event at the outstation. Testing should confirm that all events identified in this document and any additional elements as identified by the system designer are in fact recorded in the system audit log file. Testing should also confirm that system audit logs are integrity protected and authenticated.

### 4.4.2 Recommended Tests for Non Functional Requirements

#### *4.4.2.1 Thermal*

##### 4.4.2.1.1 Storage

The unattended outstation should be held, without power, for at least three hours at -25°C and then +70°C, with low humidity. The units should then be allowed to return to room temperature and tested to ensure correct operation.

##### 4.4.2.1.2 Operational

The equipment should function within specification over an ambient temperature range of at least -10°C to + 40°C. At all temperatures above 20°C, it must operate correctly in the presence of 80% relative humidity. The temperature should be varied in 5°C steps, and the equipment left for 30 minutes or longer to obtain thermal equilibrium; the equipment should function correctly at each temperature step.

# Chapter 5 Annexes

## 5.1 Annex 1. Abbreviations and Terminology

### 5.1.1 ABBREVIATIONS

**AD –** Approved Device (see definition below)

**ANPR** – Automatic Number Plate Recognition

**BLE** – Bus Lane Enforcement

**LEZ** – Low Emissions Zone

**CCD** – Charge-Coupled Device (see definition below)

**CCTV** – Closed Circuit Television - is the use of video cameras to transmit video images to a specific, limited set of monitors.

**CLEF** – Commercial Evaluation Facility (see definition below)

**CMOS** – Complementary Metal Oxide Semiconductor (see definition below)

**CUV** – Close-up View (see definition below)

**CV** – Context View (see definition below)

**DEFRA** – Department for Environment, Food and Rural Affairs

**DfT** – Department for Transport

**DSTL** – The Defence Science and Technology Laboratory is the primary delivery organisation for the provision of the science and technology required by the Home Office. (Previously CAST and formerly HOSDB)

**DVD** – Digital Video Disk (various formats are available)

**DVLA** – Driver and Vehicle Licensing Agency

**DVR** – Digital Video Recorder (generally uses hard disk or DVD)

**EAL** – Evaluation Assurance Level

**EBU** – European Broadcasting Union – sets standards for video and broadcasting

**EMC** – Electromagnetic Compatibility

**EMS** – Enforcement Management System

**ERCU** – Evidence Retrieval & Control Unit

**FTP** – File Transfer Protocol (a protocol that allows users to copy files between their local system and any system that can be reached on the network)

**GPS** – Global Positioning System

**IACS** – International Association of Classification Societies

**JAQU** – Joint Air Quality Unit, (see definition below)

**ISO** – International Organisation for Standardisation

**MSF** – The radio signal which broadcasts the national time standard for the UK. (The letters do not stand for anything. MSF is simply a call sign which uniquely identifies the broadcast).

**PAL** – Phase Alternating Line - an analogue colour video encoding system used in broadcast television systems in large parts of the world, including UK and Europe

**PCN** – Penalty Charge Notice (issued for Traffic contraventions under a Civil Enforcement regime)

**PTZ** – Pan, Tilt and Zoom – standard camera controls for CCTV mechanically operated cameras

**RAID** – Redundant Array of Independent Disks. A method of storing data more reliably on (computer) file servers (see definition below)

**TCF** – Technical Construction File (see definition below)

**TEVS** – Traffic Enforcement Video Store – area of file storage (typically on a computer file server) where video of *potential* contraventions is securely stored.

**TRO** – Traffic Regulation Order (in London, this is referred to as a Traffic Management Order – or **TMO**)

**VCR** – Video Cassette Recorder (generally uses VHS tapes)

**VPR -** Vehicle Passage Record (see definition below)

**VRM** – Vehicle Registration Mark – as displayed on the front and rear 'number plates' of most road vehicles (but only on the rear of motorcycles) in accordance with applicable legislation.

**WORM** – (Write Once, Read Many) - A recording medium that once written to, cannot be amended - e.g. a (non-rewritable) CD or DVD.

### 5.1.2 TERMINOLOGY

Note: some of these terms might have a more generic meaning – but are explained here in relation to Video, Camera and Recording Systems for civil traffic enforcement.

**ANPR** – Automatic Number Plate Recognition: a technology which uses optical character recognition on camera images to read a vehicle's number plate.

**Approved Device** – The combination of camera(s) and recording system which meets the specified requirements for civil traffic enforcement in applicable legislation and guidance. For Low Emissions Zone Applications the requirements should be those set out in this document.

**Attended CCTV system** – A system that relies on an operator to observe and log potential contraventions as they happen.

**Authentication** (of a video signal or file) – Authentication establishes the authenticity or credibility of a video signal or file. Typically this might be through use of Hash functions or (digital) Watermarks.

**CCTV (Video) Matrix** – The core of most traditional *analogue* CCTV systems is the video (hardware) matrix. This is typically an electronics rack that is situated close to the control room. The matrix is a switch that routes video inputs from cameras to video outputs that are fed to monitors and DVRs / VCRs or other equipment for recording as required, normally using desk-mounted keyboard controls.

- A ***virtual matrix*** runs on a data network that carries information encoded as TCP/IP (Transfer Control Protocol / Internet Protocol). Whereas an analogue hardware matrix switches video and PTZ (pan/tilt/zoom) controls, a virtual matrix can also handle the processing of alarm and access control data. It can also accommodate the communications required for VOIP (Voice over IP) and bi-directional, full-duplex audio.

**Charge-Coupled Device (CCD)** – This is an image sensor technology, consisting of an integrated circuit containing an array of linked, or coupled, light-sensitive capacitors. CCDs are used to obtain images in most CCTV cameras.

**Close-Up View (CUV)** – The camera should be capable of zooming in to obtain a clear close-up view (CUV) of the VRM. In general the close-up view should be able to show a (horizontal style) Vehicle Registration Mark (VRM) as between around 15% to 30% of the video frame width to enable the VRM to be clearly recognised. However, depending on other factors, this range may be extended to between around 10% and 35% of the frame width.

**Context View (CV)** – The camera should be capable of zooming out to show a clear context view (CV) of the vehicle within the enforcement zone. Typically, a (horizontal style) VRM should be displayed as between around 3% and 10% of the video frame width – although it is not necessary for the VRM to be clearly readable in this view. This view should allow an observer to clearly identify that the vehicle is the same as that shown in the CUV image.

**Controlled Document** – A reference document that, through the course of its lifecycle may be reviewed, modified and distributed several times. When a controlled document is revised, it supersedes the previous version. So version control is required to ensure the correct version of the document can be referenced.

**Contractor** – The Contractor is the organisation employed by the Owner to be responsible for the overall design, coordination and building of the Enforcement Project. It may act as a lead organisation of a group employed by the Owner, such as a Systems Integrator.

**Contravention Candidate** – A Vehicle Passage Record identified by the Compliance Engine process as a possible contravention through non-payment of the toll for a certain amount of time after passage. (See Figure 2: **Traffic Enforcement Data Flow** on page 16)

**Commercial Evaluation Facility (CLEF)** - A CLEF is a commercial evaluation facility that is certified under the ITSEC (Information Technology Security Evaluation Criteria) scheme to undertake testing of system security.

**Complementary Metal Oxide Semiconductor (CMOS) Device** – This is an image sensor technology, consisting of an array of CMOS transistors. Recent developments in CMOS technology have produced image sensors that rival the quality of the more mature CCD technology.

**Encryption Key** – An encryption key is a data string that is used by an encryption process to convert the clear-text data into the cipher-text string for transmission. Dependent upon the encryption method chosen, these keys may be single shared values or a matched pair of public / private keys. In all cases, the private key or the shared key must be kept secret.

**Enforcement Schedule** – The enforcement schedule contains data that is used, normally by an unattended enforcement system, to determine whether enforcement action is justified at a particular location at a given time and if action is justified, and then what types of contravention are permitted at that time / location.

**Enforcement Zone** – The Enforcement zone is a component of an enforcement schedule. It relates to a particular geographical area and dictates what contraventions can be enforced and during what hours.

**Evidence Pack** – An evidence pack is a package of evidential data that is used to 'prove' a contravention has taken place. It will normally contain a close-up view a context image sequence and a small amount of meta-data (such as time, date, location, contravention number, and unit number). It will often be encrypted and authenticated. It is advisable that the evidence pack contains the *minimum* information necessary to demonstrate a contravention has taken place.

**Evidence Retrieval and Control Unit (ERCU)** – This device acts as a secure extension to the remote contravention detection equipment. It allows the collection of contravention information at a convenient 'office' location. One of its main functions is to preserve the evidential integrity of the contravention records by processing encrypted data through a pair of secure interfaces to a public communications network. The ERCU operates on the "benefit of doubt" principle.

In systems that are being designed to be compatible with the criminal process or are to be type Approved by the Home Office, the ERCU writes data to a WORM media within 24 hours to protect data from tampering.

**Evidential Data** – Evidential data is only that data that is required to demonstrate to an enforcement officer or an adjudicator that a contravention has taken place. It is considered good practice for the evidential data to contain the minimum necessary information
**Frame rate** – The frame rate of an evidence package is the number of complete images rendered by the enforcement system in any second. It should be noted that some image encoding algorithms do not encode complete frames. For these encoders, the frame rate requirements will be met if the encoded video provides a clear impression of scene movement.

**Hash function** – An algorithm that calculates a value from the contents of a data file which can then be used to detect alterations to the file. Similar to a checksum but with greater security, hash functions play an important role in secure cryptographic systems, where authentication is as important as hiding the data from third parties.

**Illuminator** – A device for illuminating a scene so that a camera may be able to capture an image. In practice, usually a light source, with a lens or mirror for concentrating light

**Integrity** – The provision of facilities (on computer storage systems) to ensure that if data is amended, the changes are detectable. Typical examples include hash functions and watermarking of the data – so that if the data is amended, the hash function shows an error – or the watermark becomes visible.

**Joint Air Quality Unit (JAQU)** – A time limited joint unit formed by the Department for Environment, Food and Rural Affairs, (DEFRA) & the Department for Transport, to oversee the implementation of the 2017 NO2 plan.

**Legacy System** – A system that employs pre-existing equipment (either wholly or in part) and certification is required (either wholly or in part) in order to comply with applicable legislation.

**Low Emissions Zone (LEZ)** – An area in which a local authority has brought measures into place to improve the air quality. The creation of Low Emission Zones in Scotland is part of the Scottish Government's Cleaner Air for Scotland 2 (CAFS 2), which aims to improve air quality and address sources of pollution.

**Master Copy** – The original video image of the contravention, which is held securely (usually in the Traffic Enforcement Video Store) pending determination of any PCN procedure.

**Matrix** – see CCTV Matrix

**Mobile system** – A capture system installed in a vehicle and able to move from place to place. It can operate when stationary or while moving

**Negative Guard Band** – A negative guard band is one where although the reported position of the enforcement device is within the defined enforcement zone, enforcement does not take place because it is within the allowed error margin.

**Non-Evidential Data** – Non-Evidential Data is all data other than evidential collected or generated by an enforcement system component. In practice this may include information that demonstrates that the system is operating normally, logged data relating to the normal operation of the system (such as the generation, transmission of data packets, the updating of keys etc) and information to assist an enforcement operator in processing a contravention record (for example the suspect vehicle's VRM could be returned as non-evidential data).

**Portable** – A capture system capable of being carried between locations. It may be set up on a temporary basis, rather than being fixed (redeployable) or mobile (vehicle mounted).

**Optical Character Recognition**, (OCR) – is the recognition of printed or written text characters by a computer. In OCR processing, the scanned-in image is analysed for light and dark areas in order to identify each alphabetic letter or numeric digit.

**Positive Guard Band** – A positive guard-band is one where although the reported position is outside the enforceable area, it is within the allowed error margin so enforcement is permitted.

**RAID Server** – A file server using RAID technology. The acronym RAID (redundant array of independent disks) refers to a data storage scheme using multiple hard drives to share or replicate data among the drives. Depending on the configuration of the RAID (typically referred to as the RAID level), the benefit of RAID is to increase data integrity, fault-tolerance, throughput or capacity, compared with single drives. Note: RAID 0 does not provide any form of data redundancy and should not be used in enforcement applications

**Redeployable** – A capture system, which is fixed whilst operating, rather than mobile. But capable of being moved between designated locations on a relatively short-term basis.

**Reliability** – The ability of (computer & similar) systems to continue to operate and retain valuable data even if some parts of the system fail. RAID servers are a good example of this in practice.

**Salt** – In cryptography, a salt comprises random bits that are used as one of the inputs to a key derivation function. (The other input is usually a password or passphrase). A salt can also be used as a key in a cipher or other cryptographic algorithm.

**Security** – The protection of data and system information (on computer storage systems) so that only people who are authorised to access, use, copy or delete the data have access to it for these purposes. Typically, this may involve a hierarchy of password protection so that individuals are only able to carry out the activities that they are authorised to do. Where data is released from a secure environment, this is likely to require other forms of protection – such as data encryption – to ensure that unauthorised persons cannot see or amend the data.

**Server** (File server) – A form of disk storage that hosts files within a network.

**Synchronisation Period** – The maximum time between successful clock synchronisation events.

**Systems Integrator** – A Person or Organisation that specializes in bringing together component subsystems into a whole and ensuring that those subsystems function together, a practice known as system integration.

**System Operator** – The Organisation or service provider that runs the Enforcement system on behalf of the Local Authority or Enforcement System Owner when the project has been completed. (This may also be the contractor).

**Technical Construction File (TCF)** – The information that describes in full the enforcement system's design and operation. The file forms the basis of an application for certification as an "approved device" to DfT and records changes made to the enforcement system during its life.

**Unattended CCTV system** – A system that records potential contraventions automatically for subsequent review.

**Unique Frame Identifier** – sequential unique numbering of each image or frame of a recording such that it is synchronous, (i.e. it increments coincidentally with each change of frame or image), and from which the correct order or position of an image in a sequence can be identified. This can be a simple frame count or by adding frames to hours, minutes and seconds in the time display. It may take the form of a timer, (milliseconds, for instance), if the resolution is sufficient to uniquely identify each frame.

**Vehicle Passage Record** – Information captured as a record of the passage of a vehicle through a toll zone for billing or enforcement purposes.

**Version** – Software unique identifying number. An instance or a configuration of a piece of software. Once a version is completed, it cannot be changed without creating a new version. Once the development team considers a software version as being sufficiently mature, the software version can be turned into a software *release.*

**Variant** – A software version that is an *alternative* to another version. A variant or variation is the same version of a piece of software that meets a conflicting requirement. For instance, the same version of software doing the same job in the same way but designed to control different hardware.

**Watermark (digital)** – A Watermark is a (generally invisible) identification and authentication mark that is embedded into a (video) signal or file that can be detected if required. It can be used to confirm the integrity and/or source (or authorship) of the video file.

**Working Copy** – A video image of a contravention either produced directly from the Master Copy or made contemporaneously with it for the purpose of evidence review and related procedures.

## 5.2 Annex 2. Organisations contributing to the production of the original Department for Transport document

British Security Industry Association
Department for Transport
EMC Test Labs Association
Institution of Engineering and Technology
ITS-UK
Manchester City Council
Newham Borough Council
Nottingham City Council
Pips technology
Qinetiq
Redflex Traffic Systems Pty Ltd
Sheffield City Council
Siemens Traffic Controls
Transport for London and technical advisers Atkins
Transport Research Laboratory
TUV Product Service Ltd
Vehicle Certification Agency
Westminster City Council

## 5.3 Annex 3. LEZ - Technical Systems Guidance in Scotland

There is a document "*LEZ – Technical Systems Guidance in Scotland*" available on the Transport Scotland website: https://www.transport.gov.scot. This document is intended as a guide for local authorities when purchasing and operating Automatic Number Plate Recognition (ANPR) camera systems for Low Emission Zone (LEZ) enforcement in Scotland. It describes the key technical issues and requirements for the design and specification, procurement, installation, operation and maintenance of roadside camera and back-office systems in preparation for the introduction of LEZs in Scotland.

ANPR camera-based solutions have been used for many years across the UK to enforce traffic regulations for parking and bus lanes. Following the development of Clean Air Zones (CAZ) in England and the Low and Ultra Low Emission Zones (LEZ, ULEZ) in London, these technical solutions – along with matters of good practice – have been advanced to provide the additional functionality required to implement and operate these zones in a robust, secure and effective manner.

Particular focus is given in this document to the following areas:

- ANPR camera technology;
- Back-office systems technology and functionality;
- General capabilities and limitations of ANPR cameras and the ANPR Back Office System;
- Key issues and requirements for data communications networks;
- Systems and processes for vehicle identification;
- Integration and interfacing, including:
  - with existing systems and services, e.g. Penalty Charge Notice (PCN) processing and PCN payment;
  - with local data services, e.g. local exemptions databases; and
  - with national data services, e.g. Driver and Vehicle Licencing Agency (DVLA) database, national exemptions database.
- Processes for handling vehicle exemptions at both local and national levels;
- Processes for identifying the compliance status of UK-registered vehicles;
- Processes for identifying the compliance status of non-UK vehicles; and
- Processing penalties for LEZ contraventions (UK and non-UK vehicles).

The document also identifies key issues for consideration in relation to:

- The design and specification of LEZ systems;
- Tendering and procurement for LEZ systems;
- Installation, testing and acceptance of LEZ systems; and
- LEZ systems operation and maintenance.

## 5.4 Annex 4. Attended Systems Check List

**Sample Test Procedures**

| No | Action | Comments |
|---|---|---|
| **A** | **Observational Tests of CCTV Cameras** | |
| 1 | Start video recording of 'test' (or ensure that recording is running) | On some (mainly server based digital) systems, recording may be continuous |
| 2 | Pan & Tilt camera to align with 1st approach | |
| 3 | Zoom camera out to Context View (CV) of approach - at the ***minimum*** viable range | |
| 4 | Measure time to 'zoom in' from the CV to a Close-Up View (CUV) of a VRM on this approach - at the ***maximum*** viable range | Zoom times may be measured to the nearest second - using a manual or electronic stopwatch facility |
| 5 | Ensure that the VRM is clearly readable on screen | |
| 6 | If appropriate - recording of this test may be stopped | |
| 7 | Repeat tests (1-6) for other enforced approaches visible from this camera | |
| 8 | Repeat tests (1-7) for all enforcement cameras, for all enforced approaches visible from each camera | |
| **B** | **Playback & Review tests (for recording and image grab facilities)** | |
| 1 | Playback the video recordings taken during tests (section A) on the Review facility | Recording may be on tape, disk (typically CD or DVD), server or other digital recording equipment |
| 2 | Grab images of CV and CUV on each enforceable approach on each camera | |
| 3 | Ensure that CV and CUV images are relatively sharp and clear, and that the VRM of a vehicle is clearly readable in the CUV | |
| 4 | Repeat 2 & 3 for all enforceable cameras and approaches | |

**NOTES**

1 *Video recordings and grabbed images for all enforceable cameras and approaches should be retained (on disk) for the Technical Construction File for the system - for approval purposes.*

2 *The above procedures might be more appropriate for vehicles observed from the rear, moving away from the camera. For forward facing cameras, where vehicles approach the camera, the CUV might need to be observed at the maximum viable range, and the CV at the minimum viable range. In these circumstances, which will be site specific - a lower zoom range might be required.*

3 *Whilst it is **not** a requirement to repeat the above procedures in varying light and weather conditions, the documentation for these tests should indicate the lighting and weather conditions under which the tests were conducted.*

4 *Where a number of very similar or identical specification New or Legacy CCTV cameras require approval as a part of a System certification, by agreement with Scottish Ministers, tests from a sample of these cameras is likely to be acceptable.*

5 *For cameras on mobile vehicles, a practicable target range for observing vehicles/contraventions should be set (say 50 - 100m) – and representative samples taken of (perhaps) two sites.*

## 5.5 Annex 5. Suggested Technical Construction File Contents

These are the suggested contents of the Technical Construction File required for civil traffic enforcement applications.

1. Name and address of various participants in the Enforcement Project, name of principal contact, (plus email & phone number). Specifically:
    a. The Local Authority or System Operator
    b. The relevant Contractors
2. Name, title and qualifications and/or experience of the competent person who commissions the system and signs test declarations. (Also name and address of any external test house and engineer if necessary).
3. It is recommended that the technical construction file be a controlled document that is modular and easily maintained as the system changes. As a minimum there should be a proper index or list of all the documents enclosed in the current version of the file.
4. A list of all the equipment; the serial numbers of significant items of that equipment (recording equipment, servers etc.); and a list of the software that is used in the system.
5. A description of the system architecture in full, as well as details of any significant design elements. This should be with reference to issues discussed in the guidance. We suggest it should include:
    - Software versions (and issue dates). For Manufacturers, it is recommended that software change logs be included. As all software versions likely to be in service with customers should be covered.
    - The number of workstations, minimum hardware specifications for computers and servers.
    - Camera handling capacity and planned number of cameras deployed with camera designations and locations.
    - Specifications for the system and ancillary equipment to demonstrate compliance with any performance minima specified in the guidance.
6. Test reports and declarations demonstrating the required performance as applicable. Which tests were performed and why the tests were selected or omitted.
7. A security policy. This may be used to explain how evidence is safeguarded. This should cover home working if appropriate. (See sections 3.4.2 and 4.2.5)
8. Where the application relates to bus lane enforcement under the Transport Act 2000, documentary evidence of prior home office approval or evidence of use for civil bus lane enforcement in London prior to November 2005 as applicable.
9. A maintenance plan. This should include any transitional arrangements that may be required for upgrades or replacements of equipment. This should also cover any policy for temporary replacements; involving mobile enforcement vehicles for example.
   Where necessary, the plan must identify what routine calibration is required and how that will be carried out.

# 5.6 Annex 6. Data Security

## 5.6.1 INTRODUCTION

This annex describes the requirements for data security for a civil certified enforcement system. This data security annex is based upon the same requirements as are published for the Home Office by DSTL for equipment intended to be Type Approved under the criminal process.

It is reproduced here in its current form at the time of publication of this document. However, with the discretion of the Secretary of State, any subsequent updates to these requirements by DSTL should be included, in order to remain compatible with the criminal process.

***5.6.1.1*** Subject to the generation of an appropriate Protection Profile, it is intended that the requirements for data security will move to implement the common criteria at Evaluation Assessment Level 4 in accordance with ISO / IEC 15408. At that time, this annex will be withdrawn and replaced with the required protection profile.

***5.6.1.2*** The integrity and full certification of the evidence by the public and the adjudication service is of paramount importance. It is therefore essential this continues to be ensured by the use of data protection methods that will themselves be recognised as adequate by the stakeholders. The following data protection is required for devices used for automatic unattended operation but key lengths that offer enhanced security (e.g. 256 bit) will be permitted.

## 5.6.2 GENERAL REQUIREMENTS

***5.6.2.1*** The purpose of the data protection is to ensure that a defence based on an allegation that the data could be tampered with by anyone accessing the network will be implausible and have no credibility at review or appeal. The standard data security measures used by major financial institutions for the protection of financial data meet that requirement and are specified in published international standards. It is a requirement that data protection as used in the financial sector is applied to the evidence data produced by all devices approved for automatic unattended use.

***5.6.2.2*** If the following data protection measures are adhered to, then any public or private data network, including digital radio networks, may be used.

***5.6.2.3*** A financial sector data protection system provides three levels of protection:

i. Authentication
ii. Encryption
iii. Error protection.

***5.6.2.4*** Authentication is the principal element in establishing the integrity of the evidence. A Message Authentication Code (MAC) comprising 4, 8, 10, 12 or 16 8-bit bytes of data is computed and appended to the image and associated evidence data (evidence package). The MAC is a complex function of a 112 bit, a 128 bit or a 168 bit

authentication key. The integrity of a received evidence package is verified when re-computing its MAC using the same key produces the same answer.

***5.6.2.5*** Encryption transforms the evidence package into unrecognisable random data. For the encryption, another 112 bit, 128 bit or 168 bit encryption key, chosen to be different from the authentication key, must be used.

***5.6.2.6*** For any data network, standard error correction methods such as a 32 bit Cyclic Redundancy Check (CRC) must be used to ensure no accidental errors can be introduced during the transmission process.

***5.6.2.7*** The data protection process implemented in the device at the roadside site, which must be undertaken in the following order, must be to:

i. Calculate the MAC of the whole evidence package
ii. Encrypt the evidence package
iii. Append the MAC to the encrypted evidence package
iv. Compute the CRC for each transmission segment
v. Transmit each segment

***5.6.2.8*** At the receiving end, the process which must be undertaken in the following order, must be to:

i. Check each CRC and request re-transmission when necessary
ii. Decrypt the evidence package
iii. Recalculate the MAC from the decrypted evidence package
iv. Compare this MAC with the transmitted MAC
v. Accept as valid data only if they are the same.

***5.6.2.9*** Physical security must be provided at each site. Any unauthorised access must be detected and must cause all security keys to be securely deleted.

***5.6.2.10*** Each site must have a mechanism such as back-up battery so that, on detection of a failure of the mains supply, it can close down operations in a controlled manner maintaining the integrity and security of the stored data and enable operations to be automatically resumed when power is returned. Encryption keys may be retained across power outages providing there has been no unauthorised access.

### 5.6.3 DATA PROTECTION STANDARDS

***5.6.3.1*** The data protection must be based on the following published standards.

***5.6.3.2*** Both the authentication and encryption process are based around any sub- process known as a block cipher. For the traffic enforcement system the same block cipher must be used. Systems being submitted for certification must use either AES 128 or use the Triple Data Encryption Algorithm (TDEA) specified in NIST Special Publication SP800-67 using either option 2 or option 3 (known as 2TDEA and 3TDEA respectively). Option two requires two different 56 bit keys while 3TDEA requires three different 56 bit keys. After the 1 January 2010, systems using 2TDEA must move to AES 128 or 3TDEA. Beyond 1 January 2030, all systems must use

AES 128. However, other block ciphers recommended by NIST as providing comparable security strengths may be used with the agreement of Scottish Ministers.

***5.6.3.3*** The authentication process must follow that described in the draft recommendation given in NIST Special Publication 800-38B for the CMAC Authentication Mode. Systems must use CMAC with AES 128 and a MAC length of 64 bits. The length of the MAC generated will be 64 bits long. In the case of the 2TDEA or the 3TDEA a salt 64 bits long will be used. On 1 January 2010 systems using 2TDEA must move to using AES 128 or 3TDEA and generate a 64 bit MAC, the 3TDEA systems using a 64 bit salt. Beyond 1 January 2030 all systems will use CMAC with an AES 128 block cipher and generate an 80 bit MAC with a 16 bit salt.

***5.6.3.4*** The encryption process for systems to be certified by Scottish Ministers must use AES 128 in Cipher Block Chaining (CBC) mode as described in NIST Special Publication SP 800-38A. On 1 January 2010, systems using 2TDEA must move to using AES 128 or 3TDEA in CBC mode. Beyond 1 January 2030 all systems must use AES 128 in CBC mode.

***5.6.3.5*** The above data protection system requires the encryption and authentication keys to be known at both ends of the communication link. The security depends on these remaining unknown by any third party. Good security requires frequent changes of the keys and different keys used at each site. All systems must generate new encryption and authentication keys for each evidence pack generated in the road-side equipment. A key management system must be provided as part of the back office. It must automatically generate, store, distribute over the data network, synchronise and destroy keys securely. It must be as transparent to users as far as possible.

***5.6.3.6*** The keys generated and used in the roadside sites for data encryption and authentication must be sent over the network encrypted using KEKs (Key Encryption Keys). The KEKs must be manually loaded and changed no less frequently than annually. Systems must use AES with a 192 bit or longer KEK. Systems migrating using 2TDEA or 3TDEA must use 3TDEA and so use 3 KEKs. These higher level Key Encrypting Keys (KEKs) do not need frequent changing and must be securely distributed manually to each site. This distribution is part of the evidential chain. Other methods of key encryption recommended by NIST may be acceptable if agreed with Scottish Ministers.

## 5.7 Statutory Clauses added as requirements

Taken from The Low Emission Zones (Scotland) Regulations 2021, Schedule 6, Approved Devices.

5.7.1 The device must include a camera which is —

(a) securely mounted on a vehicle, a building, a post or other structure,

(b) mounted in such a position that vehicles driving within in a selected area of a low emission zone can be surveyed by it,

(c) connected by secure data links to a recording system, and

(d) capable of producing, in one or more pictures, an image or images of the vehicle in relation to which the low emission zone contravention was committed of sufficient detail to show the vehicle's —

(i) registration mark in legible form, and

(ii) enough of its location to show the circumstances of the contravention,

at the time of the contravention.

**5.7.2** Where the device includes a facility to print a still image, that image when printed must be endorsed with the time and date when the frame was captured and its unique number.