BS EN 62676-4:2015

BSI Standards Publication

Video surveillance systems for use in security applications

Part 4: Application guidelines

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 62676-4:2015. It is identical to IEC 62676-4:2014. It supersedes BS 8495:2007 and BS IEC 62676-4:2014, which are withdrawn. It supersedes BS EN 50132-7:2012 which will be withdrawn on 13 April 2018.

National Annex NA gives recommendations on security grading application for Video Surveillance Systems (VSSs).

The UK participation in its preparation was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/10, Closed circuit television (CCTV).

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 89390 2

ICS 13.320

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2014.

Amendments/corrigenda issued since publication

Date	Text affected
31 July 2015	This corrigendum renumbers BS IEC 62676-4:2014 as BS EN 62676-4:2015. Also, Annex ZA and National Annex NA added

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62676-4

April 2015

ICS 13.320

Supersedes EN 50132-7:2012

English Version

Video surveillance systems for use in security applications - Part 4: Application guidelines (IEC 62676-4:2014)

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité - Partie 4: Directives d'application
(IEC 62676-4:2014)

Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 4: Anwendungsregeln
(IEC 62676-4:2014)

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 62676-4:2015 E

Foreword

This document (EN 62676-4:2015) consists of the text of IEC 62676-4:2014 prepared by IEC/TC 79 "Alarm and electronic security systems".

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2016-04-13
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2018-04-13

This document supersedes EN 50132-7:2012.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62676-4:2014 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62305 (series)	NOTE	Harmonized as EN 62305 (series).
IEC 62305-3	NOTE	Harmonized as EN 62305-3.
IEC 62305-4	NOTE	Harmonized as EN 62305-4.
ISO 22311:2012	NOTE	Harmonized as EN ISO 22311:2014.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 62676-1-1	-	Video surveillance systems for use in security applications - Part 1-1: System requirements - General	EN 62676-1-1	-
IEC 62676-1-2	-	Video surveillance systems for use in security applications -- Part 1-2: Video transmission - General video transmission - requirements	EN 62676-1-2	-
IEC 62676-2-1	-	Video surveillance systems for use in security applications -- Part 2-1: Video transmission protocols - General requirements	EN 62676-2-1	-
IEC 62676-2-2	-	Video surveillance systems for use in security applications - Part 2-2: Video transmission protocols - IP interoperability implementation based on HTTP and REST services	EN 62676-2-2	-
IEC 62676-2-3	-	Video surveillance systems for use in security applications - Part 2-3: Video transmission protocols - IP interoperability implementation based on WEB services	EN 62676-2-3	-
IEC 62676-3	-	Video surveillance systems for use in security applications -- Part 3: Analog and digital video interfaces	EN 62676-3	-

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 4: Application guidelines

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62676-4 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

This standard is based on EN 50132-7 (2012).

The text of this standard is based on the following documents:

FDIS	Report on voting
79/455/FDIS	79/466/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all the parts in the IEC 62676 series, under the general title *Video surveillance systems for use in security applications*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The IEC Technical Committee 79 in charge of alarm and electronic security systems together with many governmental organisations, test houses and equipment manufacturers has defined a common framework for video surveillance transmission in order to achieve interoperability between products.

The IEC 62676 series of standards on video surveillance system is divided into 4 independent parts:

Part 1: System requirements

Part 2: Video transmission protocols

Part 3: Analog and digital video interfaces

Part 4: Application guidelines

Each part offers its own clauses for the scope, normative references, definitions and requirements.

The purpose of this part of IEC 62676 is to provide guidance on how to ensure that video surveillance systems (VSS), thus far referred to as closed circuit television (CCTV), meet their functional and performance requirements.

This part of IEC 62676 will prove useful to those responsible for establishing operational requirements, writing specifications, selecting, installing, commissioning, using and maintaining a VSS.

VSS, in its simplest form, is a means of providing images from security cameras and recorders for viewing on a display via a transmission system. There is no theoretical limit to the number of cameras and displays which may be used in a VSS installation but in practice will be limited by the efficient combination of control and display equipment and the operator's ability to manage the system.

The successful operation of a VSS requires the active co-operation of the user in carrying out the recommended procedures.

Due to the wide range of VSS applications, for example security, safety, public safety, transportation, etc. only the minimum requirements are covered in this part of IEC 62676.

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 4: Application guidelines

1 Scope

This part of IEC 62676 gives recommendations and requirements for the selection, planning, installation, commissioning, maintaining and testing video surveillance systems (VSS) comprising of image capture device(s), interconnection(s) and image handling device(s), for use in security applications.

The objectives of this part of IEC 62676 are to:

a) provide a framework to assist customers, installers and users in establishing their requirements,

b) assist specifiers and users in determining the appropriate equipment required for a given application,

c) provide means of evaluating objectively the performance of the VSS.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62676-1-1, *Video surveillance systems for use in security applications – Part 1-1: System requirements – General*

IEC 62676-1-2, *Video surveillance systems for use in security applications – Part 1-2: System requirements – Peformance requirements for video transmission*

IEC 62676-2-1, *Video surveillance systems for use in security applications – Part 2-1: Video transmission protocols – General requirem*ents

IEC 62676-2-2, *Video surveillance systems for use in security applications – Part 2-2: Video transmission protocols – IP interoperability implementation based on HTTP and REST services*

IEC 62676-2-3, *Video surveillance systems for use in security applications – Part 2-3: Video transmission protocols – IP interoperability implementation based on Web services*

IEC 62676-3, *Video surveillance systems for use in security applications – Part 3: Analog and digital video interfaces*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1
camera housing
enclosure to provide physical and/or environmental protection of the camera, lens and ancillary equipment

3.1.2
camera sensitivity
image capturing device capability to produce an image in certain light conditions

3.1.3
VSS surveillance installation
installation consisting of the hardware and software components of a VSS, fully installed and operational for monitoring a defined security zone

3.1.4
VSS camera
unit containing an imaging device producing a video signal from an optical image

3.1.5
VSS camera equipment
unit containing a VSS camera plus appropriate lens and necessary ancillary equipment

3.1.6
VSS control unit
equipment for controlling and monitoring the required operational functions of the VSS

3.1.7
VSS technician
qualified person who is trained and competent in the installation, maintenance, servicing and fault-finding of VSSs

3.1.8
VSS
system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which may be necessary for the surveillance of a protected area

3.1.9
corrective maintenance
emergency servicing of a system, or part thereof, carried out in response to the development of a fault

3.1.10
corrective maintenance report
document that details the requirement for normal or emergency corrective maintenance and indicates the corrective action taken, as required by IEC 62676-4 or other applicable technical standards

Note 1 to entry: The report may be an electronic document.

3.1.11
company
organization providing design, installation or maintenance of the VSS system

3.1.12
detect
defined functional purpose of a camera to enable the operator to reliably and easily determine whether or not any target, such as a person, is present.

3.1.13
electronic iris
automatic electronic shutter which changes the camera sensitivity in relation to the varying light conditions in order to maintain the video output signal within defined limits

3.1.14
electronic shutter
arrangement in the camera changing its sensitivity by electronically controlling its exposure time

3.1.15
event recording
event controlled recording or storing of image signals for a pre-determined time

Note 1 to entry: refers to video recording not to system log of events.

3.1.16
external synchronisation
method of feeding reference timing signals to all connected devices to ensure that their video output signals are synchronous

3.1.17
focal length
f
measurement of the converging power of a lens, normally expressed in mm, which can be used to determine the angle of view for a given sensor size

3.1.18
geo data
digital information assigning a certain spatial location to the earth's surface

3.1.19
identify
defined functional purpose of a camera to enable identifyfication of an individual beyond reasonable doubt

3.1.20
inspect
defined functional purpose of a camera to enable the operator to obtain information from objects

Note 1 to entry: An example object may include text or a logo on clothing.

3.1.21
imaging device
device that converts an optical image into an electrical signal

3.1.22
imaging device illumination
level of illumination (luminance) at the photosensitive surface of the imaging device

3.1.23
iris
variable aperture mechanism which regulates the amount of light passing through the lens onto the imaging device of the VSS camera

3.1.24
Kell factor
subjective number of lines of resolution that can be visually perceived in a video display system, expressed as a percentage of the total number of lines of resolution

3.1.25
lens
optical device for projecting an image of a desired scene onto the photo sensitive surface of the imaging device

3.1.26
monitor
defined functional purpose of a camera to enable viewing of the number, direction and speed of movement of people across a wide area, providing their presence is known to the operator

3.1.27
NTSC
NTSC resolution
standard-definition video mode referring in digital applications to 486 lines or 720 × 486 pixels

3.1.28
image presentation device
device for converting video signals into pictures on a display screen

3.1.29
observe
defined functional purpose of a camera enabling characteristic details of an individual, such as distinctive clothing to be seen, whilst allowing a view of activity surrounding an incident

3.1.30
pan and tilt unit
motorised unit permitting the horizontal and vertical positioning of the camera equipment

3.1.31
PAL
PAL resolution
standard-definition video mode referring in digital applications to 576 lines or 720 × 576 pixels

3.1.32
pan, tilt, zoom
PTZ
function of a camera permitting the horizontal, vertical positioning of the camera together with the angle of view

3.1.33
picture storage
storing of fixed or video images

3.1.34
preventive maintenance
routine servicing of a system, carried out on a scheduled basis

3.1.35
preventative maintenance report
document which records the preventive maintenance carried out in accordance with IEC 62676-4 or other applicable technical standard

Note 1 to entry: The report may be an electronic document.

3.1.36
recognise
defined functional purpose of a camera to enable the operator to obtain recognition of an individual

3.1.37
risk assessment
systematic process to determine the impact of the consequences of hazards and threats relative to their probability

Note 1 to entry: The result of the analysis provides the basis for risk evaluation within a risk management process.

3.1.38
risk management
culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects

3.1.39
risk management process
systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk

3.1.40
scene illumination
level of illumination (luminance) on the area to be kept under surveillance

3.1.41
site plan
pictorial representation of the protected area showing the location and intended views of the VSS cameras

3.1.42
system design proposal
specification of the system design including location factors, site plan, field of view, detector range and coverage and control room design

3.1.43
time lapse recording
periodic recording of video images at pre-defined intervals

3.1.44
video signal
video channel being transmitted, streaming or not streaming, analog or digital

3.1.45
video signal amplitude
magnitude of the video signal

3.1.46
zoom lens
lens with adjustable focal length and therefore an adjustable angle of view

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ASB	anti-social behaviour
BNC	Bayonet Neill-Concelman (connector)
CCIR	Consultative Committee on International Radio
CCTV	closed circuit television
DVR	digital video recorder
EMC	electro-magnetic compatibility
CRT	cathode ray tube
FAT	factory acceptance testing
FPS	frames per second
Gbps	gigabits per second
HD	high definition
NVR	network video recorder
LCD	liquid crystal display
IP	internet protocol
IPD	image presentation device
Mbps	megabit per second
MPEG	motion picture experts group
OR	operational requirement
PTZ	pan tilt zoom
REST	REpresentational State Transfer (webservice)
RTSP	real time stream control protocol
SXGA	Super eXtended Graphics Adapter
TCP/IP	transmission control protocol/internet protocol
VRN	vehicle registration number
UAT	user acceptance testing
UDP	user datagram protocol
UPS	uninterruptible power supply
UTC	universal time coordinated
UV	ultra violet
VCA	video content analysis
VMS	video management system
VMD	video motion detection
WORM	write once read many
VSS	video surveillance system

4 General considerations

4.1 General considerations

A VSS is the combination of image capture devices, lighting, interconnections, image handling devices, etc. selected and installed to meet the customer's security surveillance requirements.

The recommended procedure for implementing a VSS is detailed in the following subclauses 4.2 to 4.8.

4.2 Risk assessment

4.2.1 General

Prior to VSS design, and to help understand its purpose, a threat assessment and risk analysis should be performed. The threats and hazards to the premises should be identified and assessed for their likelihood and impact. These represent the risk to the premises or organization.

A risk assessment should be carried out and the VSS should be designed to mitigate the assessed risks. VSS designs should be made in accordance with this standard.

NOTE ISO 31000:2009 describes the principles for the carrying out of a risk assessment.

There is no single model design for a VSS. The design should be based on the individual location and premises, the threats and content in these locations, and the anticipated threats or damage.

Examples of issues to be considered are included below:

a) cost of loss:
   1) what is the value for example financial, intellectual, etc. of the contents at the location?
   2) what is the effect of disruption to activities at the location?
b) location:
   1) what is the quality and extent of any existing physical security?
   2) is the location situated in a high crime risk area?
   3) are there adverse environmental conditions?
c) occupancy:
   1) is the location unoccupied for extended periods?
   2) are there security guards?
   3) do the public have access to the location?
d) theft, robbery and threat history:
   1) is there a history of thefts, robberies or threats at the location?
   2) and if so, what was the method of attack for any previous threat?

Results from this assessment are used to help to inform decisions about what type of VSS to specify and install.

4.2.2 Selection of security grades

The results of the risk assessment (see 4.2.1) should be used to determine the requirements of the VSS and its components. Where appropriate a security grade should be assigned to the components, sub-systems and functions of the VSS. The identified security grade requirements should be specified in the operational requirement (OR) and agreed by the customer and system designer.

The system shall be given an overall grade for which the grade dependent requirements of this standard shall apply. When identified by the OR, or system design proposal, the functions of the VSS may use a different grade but this shall be applied consistently throughout the system. This shall be recorded in the OR or system design proposal.

Depending on the level of risk, the security grade needs to be defined for the following VSS functions:

a) common interconnections
b) storage
c) archiving and backup
d) alarm related information
e) system logs
f) backup and restore of system data
g) repetitive failure notification
h) image handling device PSU monitoring
i) image buffer holding time
j) essential function device failure notification time
k) monitoring of interconnections
l) tamper detection
m) authorisation code requirements
n) time synchronisation
o) data authentication
p) export/copy authentication
q) data labelling
r) data (manipulation) protection

Individual functions of the VSS may be specified at different security grades: for example, a system generally specified at grade 1 with grade 4 storage including fail-safe image storage.

Any additional functions which are required above the security level may be defined individually in the OR.

4.3 Developing the operational requirements

The OR document shall be produced. This is a formal written statement of need, justifications and purpose of the proposed VSS. The installer should assess and determine whether production of the OR is to be completed before or after the site survey. See 5.2 for more details.

4.4 Site survey

Once a location has been chosen for a VSS installation a site survey should be undertaken. This is to familiarise the system designer with the specifics of the intended site, such as access constraints, siting of key components (cameras, controls, power supplies, etc.) and environmental factors including illumination in day and night mode (see Clause 6 for more details).

This should be completed by visiting the location to assess its suitability, and to note any issues for the system design phase.

If the location where the VSS is to be installed has not yet been constructed then the site survey may be carried out after a preliminary design has been created.

4.5 System design including site plan

Once the site survey and OR is completed the VSS can be designed and a system design proposal and specification needs to be prepared. The design shall take into account the various requirements and location factors identified in the previous stages. At this stage a site plan should be drawn up, including locations for the various key components such as cameras (including field of view), detectors (including range and coverage), control rooms, power supplies, interconnections, etc. See Clause 6 for more details.

4.6 Developing the test plan

Having designed the VSS, a test plan shall be produced to allow any installed system to be suitably proven. This test plan should include all the critical aspects of the VSS, such as image quality, system interconnectivity, coverage, camera view, etc. The purpose is to ensure that the system can be measured against its OR, and proved to be fit for its intended purpose. See Clause 13 for more information and 6.11.2 for tamper protection testing.

4.7 Installation, commission and hand over

The risk assessment, OR and system design (including a site plan) should all be used to help facilitate the VSS installation.

Having completed the installation, commissioning tests as specified in the test plan should be completed according to the OR.

Once this has been successfully completed the system can be formally handed from the installer to the owner. See Clause 15 for more details.

4.8 Documenting the system

Documentation should be completed supporting the design, installing and commissioning phases of the VSS. These should be collated and held by the owner as the system references. The risk assessment, OR, testing plan, site survey, system design and site plan (see Clauses 14 and 16) should be included, along with the following documents:

– testing results, as built plans/drawings, data interface descriptions;
– training, manuals, support documentation, etc.;
– maintenance plan including routine inspection cleaning, etc. (see Clause 17 for more details).

5 Operational requirements specifications

5.1 General

The purpose of the VSS installation shall be summarized in a document called "Operational Requirements". Further information can be found in the *CCTV operational requirements manual* (see Bibliography).

5.2 Purpose of the operational requirements

The operational requirements clearly state what the customer expects the functions of the system to do. If there is an agreement between the system designer and the customer, the OR could be defined within the system design proposal and specification. If so, this should be clearly stated within the document. The development/design process encourages clear thinking about who will use the VSS, where and when it will be used and, in particular, the purpose of the VSS. It is produced by VSS owners, operators and anyone who intends to use information from the VSS. The later stages of development of the OR shall involve those with the necessary skills to convert statements into a technical specification and test procedures.

At appropriate stages checks shall be made to ensure that the proposed implementation will meet the OR. Without an OR and a matching test procedure there is no practical methodology to assess whether the system can meet its required purpose.

5.3 Content of the operational requirements

5.3.1 General

The operational requirements shall consist of the following parts detailed in 5.3.2 to 5.3.16.

5.3.2 Basic objective/functionalities

The following basic functions shall be covered:

- Intended purpose(s) of the system (e.g. site monitoring, detection and/or monitoring and/or recording of attacks against individual and property, thefts, robberies or damage).
- Risk assessment, which informs the selection of the required security grade of the system according to IEC 62676-1-1.

5.3.3 Definition of surveillance limitations

The following limitations shall be covered:

- limitations imposed by legislation, city rules or similar orders;
- limitations such as privacy areas required by the customer or by the proximity of neighbours.

5.3.4 Definition of the site(s) under surveillance

Buildings, internal, external or separate areas, etc. which are covered by the VSS.

5.3.5 Definition of activity to be captured

The following activity definitions shall be covered:

- the intended targets of the system in each part of the site (e.g. unauthorized persons within an area bounded by a perimeter fence; vehicles entering the access driveway, etc.);
- the expected speed of the intended target;
- the intended observation category of the targets from the perspective of the operator (e.g. detection, recognition or identification of a person);
- whether external detection is required.

5.3.6 System/picture performance

The following performance parameters shall be covered:

- the key performance characteristics of the system and its displayed images (e.g. timescale for operator to view persons and track their movements throughout the scene);
- the degree of image detail required for the purpose which is to be observed in each of the live, recorded and exported views (i.e. it may be desirable or appropriate for a different resolution to be used in the live view than in the recorded view);
- definition of any image analysis functionality, together with expected accuracy and whether this is to be achieved by the operator or automatically by the system.

5.3.7 Period of operation

The following operation parameters shall be covered:

- definition of the operating hours for the system (e.g. daily between 21:00 and 08:00 and all day on Sundays and public holidays).

5.3.8 Conditions at the location

Definition of environmental conditions, which will apply and/or vary during the monitoring period and are significant in terms of system design (e.g. illumination of the site, potential obstacles in camera view, maximum and minimum temperatures, on-board).

5.3.9 Resilience

Definition of the ability of the system to continue operating despite the existence of adverse circumstances (e.g. ability to continue operating during sudden or unexpected loss of power for a significant or defined length of time, absence of single interconnection paths, whether all or parts of the system have the same requirement).

5.3.10 Monitoring and image storage

The following storage parameters shall be covered:

- definition of where, and by whom, the system shall be monitored and operated;
- definition of what is to be recorded (e.g. all images for 10 min before and after an event; all camera views at all times);
- definition of the retention period for recordings and circumstances in which this will change (e.g. all recorded images to be kept for, and erased after, 28 days except where they relate to a criminal event);
- definition of additional (remote) sites where the images shall be available;
- definition of procedures to be followed when extracting, storing and handling images and data from the system.

5.3.11 Exporting images

The following export parameters shall be covered:

- definition of how images will be exported for short sequences (e.g. a 10 min clip to be exported to WORM media; individual image snapshots exported to USB/IP storage device);
- definition of how images will be exported for long sequences (e.g. network download for full system archive);
- definition of required compatibility of exported media (e.g. sequences should be re-playable without the need for any software/codec/hardware that is not considered part of a standard desktop operating system).

5.3.12 Routine actions

Definition of actions that are required as a matter of normal routine (e.g. the monitoring service shall carry out routine video patrols at 2 h intervals throughout the monitoring period).

5.3.13 Operational response

The following response actions shall be covered:

- definition of the person responsible for the response (e.g. key holder, guarding service and/or police);
- definition of the type of response needed for each potential event (e.g. when a trespasser is observed the local law enforcement agency is contacted);
- definition of target times for each response (e.g. security personnel to attend scene within 3 min of event detection).

5.3.14 Operator workload

The following operator parameters shall be covered:

- definition of the number of display screens an operator is expected to monitor;
- definition of the number of alarm events the operator is expected to manage;
- definition of the number of live cameras the operator is expected to manage.

5.3.15 Training

Definition of required training for each role involved in the management and operation of the system.

5.3.16 Expansions

The following system expansions shall be covered:

- definition of any planned future extensions of the system, indicating any compatibility requirements;
- definition of method used to connect with other systems.

5.3.17 List of any other special factors not covered by the above

NOTE If the operational requirement (OR) cannot be met with current technology or resources it will be noted in the system design document.

5.4 System operational criteria

5.4.1 General

The system’s operational criteria involve the determination of:

- the operational procedures;
- the alarm response;
- the system response times.

5.4.2 Automation

The VSS shall be designed to enable the operator to analyse the content of the displayed images and take all necessary actions as defined by the OR.

Automatic processing can assist operators allowing them to concentrate on essential tasks.

Automation of the following functions shall be considered:

- video image switching;
- pre-position of image capture devices;
- equipment monitoring, health check and recording process;
- video content analysis;
- lighting control;
- image storage.

Some of the above functions can be controlled from:

- alarm conditions,
- externally triggered events,
- time related events,

- operator manual activations.

5.4.3 Alarm response

The signalling indication of an alarm condition to the VSS shall have priority over other events.

It should be defined in the OR whether or not the operator shall be able to take manual control of the system, following an alarm condition, regardless of the degree of automation.

Automation of image selection shall consider the following requirements:

- specification for the selection of the significant images/sequences in each area where an alarm condition occurs;
- allocation of displays to view the significant images/sequences from the selected image capture devices; on-screen displays with image source identification or animated diagrams of the system can be useful;
- presentation of alarm images on designated displays;
- handling of simultaneous alarm conditions;
- selection of image storage criteria.

5.4.4 System response times

The following response times shall be kept to an acceptable and specified minimum:

- time elapsing between the generation of an alarm condition and it being indicated on the VSS presentation device;
- switching time for the control centre to acknowledge receipt of an alarm;
- image capture device pre-positioning if functions like zoom and/or pan and tilt are specified;
- display equipment start up time or change from time lapse mode to normal mode if a time lapse recording is specified;
- change from continuous to alarm recording mode;
- operator’s response time if required.

In order to minimise response times, image capture devices, displays, recording devices, etc. shall be continuously powered and idle, and the system shall not generate more information than the operator can effectively manage.

The expected responses to the operator’s actions should be defined in the OR.

If the performance is low, due to a high alarm rate or high image flow, the graphic displays shall still appear “normal” and the system shall be able to allocate more resources to keep a proper response to the operator’s actions.

Acceptable system response times should be defined in the OR based on the viewing task and operational response, as shown in Table 1, for example:

– a system response shall always appear within 0 s to 0,2 s;
– a system response is considered delayed if the time is higher than 0,2 s;
– a system response is considered unacceptable if the response time to the operator’s action is longer than 2 s.

EXAMPLE PTZ Control for tracking targets.

Table 1 – Example System feedback – PTZ Control Responding time, performance and operator

System feedback		
Responding time	Performance	Operator
0 s to 0,2 s	Optimal	Doesn't notice response time.
0,2 s to 0,5 s	Delay	Feels the delay and tries to adapt.
0,5 s to 2 s	Strong delay	Is disturbed by the delayed response, System shall display "please wait…"
More than 2 s	Unacceptable	Loses response to manual actions, system shall display reasons and/or prompt messages like "screen will be available in xx seconds, …"

6 Equipment selection and performance

6.1 General

It is important to consider not only whether each component is capable of meeting the OR but also whether the components in conjunction with each other, and the system as a whole are able to meet the OR.

Consideration should be given to environmental factors for equipment selection (e.g. low power, disposal of consumable items, control of hazardous substances, etc.) (see 6.8, 7.1, 12.8 and 12.9).

6.2 Camera equipment

The lens and camera combination shall be selected such that the measured visual resolution, field of view and low-level light performance are capable of fulfilling the relevant requirements in the OR.

6.3 Camera and lens selection criteria

The selection criteria should take into account the following:

- for camera sensitivity and aperture number of the lens, the prevailing and intended worst case light levels and types of light including IR, etc.;
- the color, black and white or thermal sensitivity of the image sensor;
- the focal length of the lens in relation to the size of the image sensor in the camera to give the required fields of view;
- the measured visual resolution of the camera and lens to reproduce the detail to give the necessary information in the fields of view;
- the lens image area should be equal to or greater than the effective diagonal of the imaging device in the camera to avoid vignetting.

6.4 Camera selection

6.4.1 General

The camera equipment should satisfy the operational requirements under all anticipated environmental conditions.

The selection criteria shall take into account the following:

- white balance of colour cameras;

- dynamic range and noise of image sensor;
- relevant data protection regulations (e.g. support for masking of private zones);
- long exposure times in relation to movement blur;
- spectral sensitivity in relation to the type of illumination;
- provisions for external synchronisation, line-lock, internal sync, etc.;
- provisions for remote calibration of the imaging properties;
- back-up power supply.

6.4.2 PTZ

Pan tilt zoom (PTZ) cameras are imaging devices that are controlled either by an operator or by a VSS to change the field of view of the camera via mechanical or electronic means. The camera may have any individual function or combination of panning, tilting or zooming.

If a PTZ camera is being used it shall have a home location as defined in the OR. It is desirable to specify a number of preset locations, which provide views designated in the OR. These preset positions shall be annotated in the site plan. Preset positions may include other parameters such as shutter speed, iris setting, etc.

PTZ cameras are predominantly mechanical devices, target preset fields of view may alter over time and it is recommended that regular maintenance of the cameras is undertaken.

If the PTZ is required to track moving objects the characteristics of the camera, for example rotation speed, shall be assessed to ensure that they can meet this requirement.

Care should be taken to not view areas outside the remit of the installation. If areas fall within the field of view of cameras (either static or PTZ) which are not intended to be surveyed, privacy masking shall be adopted.

6.5 Lens and housing selection

Selection of the correct lens type is as important as the camera selection. A poor lens performance can significantly detract from the overall performance of the system.

When selecting the lens the following shall be taken into account:

- the aperture of the lens contributes to the image quality, by controlling the light available to the sensor so a lens with an appropriate aperture or aperture range should be selected and automatic or electronic iris is recommended;
- the lens field of view may be reduced by any overscan in the presentation device in which case a lens with a wider field of view than originally calculated may be required;
- internal lens reflections and flare can significantly impair the image so coated lens elements and/or appropriate housings or hoods should be considered;
- variable maximum aperture zoom lenses may increase the effective aperture number of the lens as the focal length is increased. A lens should be selected which allows sufficient light to fall on the sensor under all anticipated light conditions at all available focal lengths;
- filters to pass selective wavelengths should be specified (e.g. UV cut filter to reduce haze in bright sunlight conditions);
- consideration should be given to the environmental conditions in which the equipment is intended to operate with respect to the additional features which may be implemented into housings i.e. heaters, wipers, etc.;
- housing: all equipment installed shall be suitable to withstand the prevailing environmental conditions according to the environmental classes in IEC 62676-1-1.

Having selected the camera-lens combination, it is recommended that, for difficult scenes, a camera of the type selected should be evaluated in conditions similar to those to be encountered at the installation.

6.6 Site coverage/numbers of cameras

The location(s) of interest shall be established and documented on the site plan. The level of detail(s) desired for the stated activity (e.g. identify) shall then be established for each location in order that the number of cameras for the whole site can be determined based on the annotated site plan. The actual number of cameras will depend on the types of cameras selected (e.g. Static, PTZ, megapixel, etc.), lenses required to achieve desired view and any geographical constraints.

6.7 Field of view – object size

The size of an object (target) on the display screen shall have a relation to the operator task, for example identification, recognition, observation, detection or monitoring. In digital VSSs it is important to understand the relationship between the camera resolution and the screen display resolution. If the camera resolution is not equal to the display resolution, the displayed scene may not show the expected amount of detail. If the target is a person and the VSS has an installed equivalent PAL (576i) or NTSC (486i) resolution, the recommended minimum sizes of this target, as shown in Figure 1 (PAL resolution only for illustration), are

- to monitor or crowd control the target shall represent not less than 5 % for PAL and NTSC resolution of screen height (or shall represent more than 80 mm per pixel);
- to detect the target shall represent not less than 10 % for PAL and NTSC resolution of screen height (or shall represent more than 40 mm per pixel);
- to observe the target shall represent 25 % for PAL and 30 % for NTSC resolution of screen height (or shall represent more than 16 mm per pixel);
- to recognise the target shall represent not less than 50 % for PAL and 60 % for NTSC resolution of screen height (or shall represent more than 8 mm per pixel);
- to identify the target shall represent not less than 100 % for PAL and 120 % for NTSC resolution of screen height (or shall represent more than 4 mm per pixel);
- to inspect the target shall represent not less than 400 % for PAL and 450 % for NTSC resolution of screen height (or shall represent more than 1 mm per pixel).

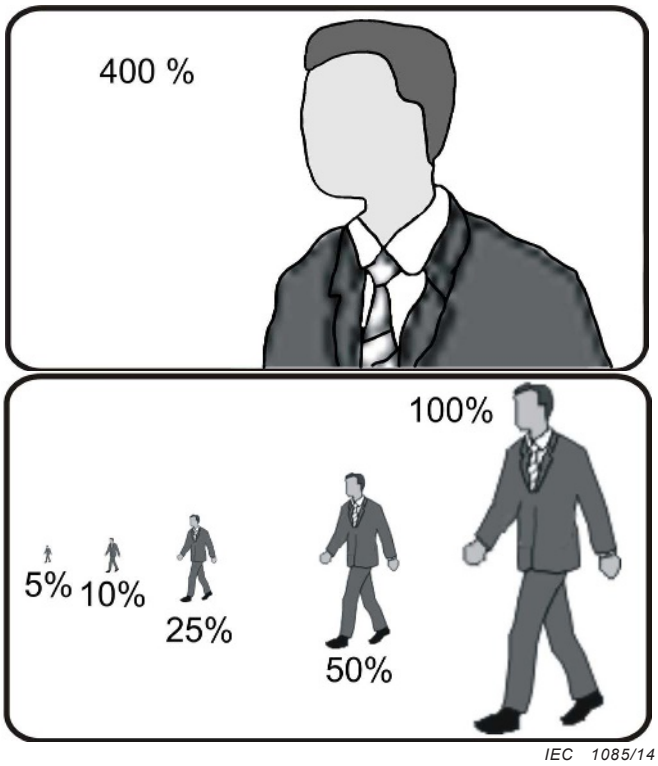


Figure 1 – Recommended minimum sizes for PAL (576i) resolution

Since the influx of digital systems in the VSS market there is variability in the capture, recording and display resolution. So a “recognise” requirement can no longer be simply equated to a 50 % screen height. For instance, through the use of megapixel cameras and high resolution displays it is now possible to provide the same image resolution as before using a smaller physical percentage of the screen.

Conversion tables have therefore been devised to show how the traditional percentage screen height criteria for the mentioned PAL (576i) or NTSC (486i) system will look under a range of non-PAL and non-NTSC resolutions. 576i and 486i have an equivalent progressive scan vertical resolution of approximately 400 pixels and 340 pixels respectively (see Kell factor), this figure has been used in the tables below. Table 2 shows the resolutions commonly encountered and Table 3 shows the equivalent screen heights needed to maintain the required resolution. These figures should be used only as a guideline to the proportion of the screen filled by the target as other factors also effect the available information in the image, see in particular 13.3.

Table 2 – Commonly encountered resolutions (in pixels)

	PAL (576i)	NTSC (486i)	1080p	720p	WSVGA	SVGA	4CIF (576p)	VGA	2CIF	CIF	QCIF
Height	400	340	1080	720	600	600	576	480	288	288	144
Width	720	720	1920	1280	1024	800	704	640	704	352	176

Table 3 – Person screen height equivalent for different digital resolutions (in percent)

Category	PAL	NTSC	1080p	720p	WSVGA	SVGA	4CIF	VGA	2CIF	CIF	QCIF
Inspect	400	450	150	250	300	300	300	350	600	600	1200
Identify	100	120	40	60	70	70	70	85	150	150	300
Recognise	50	60	20	30	35	35	35	45	70	70	150
Observe	25	30	10	15	20	20	20	25	35	35	70
Detect	10	10	10	10	10	10	10	10	15	15	30
Monitor	5	5	5	5	5	5	5	5	10	10	15

6.8 Field of view – Other considerations

Camera placement shall be based on achieving an optimum view which shall not be compromised by an easier installation procedure

When setting up a camera field of view it is important to consider other environmental or scene specific content, for example:

- Foliage: there is a seasonal variation in foliage, which could block the view. Trees and plants grow over time which could also block the view;
- Illumination: there might be spot lighting from external light sources and time controlled lighting which could impact the view;
- Sunlight: depending on time of day and seasonal variations the position of the sun could produce glare or provide poor illumination conditions;
- Reflections: windows, buildings, bodies of water or any other reflective objects can result in poor or excessive illumination conditions which can compromise the desired captured image;
- Street furniture/signage: temporary or new permanent structures such as signs or other buildings may block the field of view;
- Scene activity: if a specific task is required ensure that other scene activity does not compromise the desired image capture, for example a busy footpath in front of a doorway could occlude an identification shot.

Where person identification is the main purpose of the camera, the camera should be mounted around head height; cameras mounted significantly above head height may not be able to provide a full view of a person’s face.

6.9 Illumination

The existing lighting shall be evaluated for the level, direction and spectral content. Optimal light sources are those which have a spectrum that best matches the camera imaging device response.

If additional lighting is required, the number, type, siting and power of the light sources shall be determined taking the following parameters into consideration:

- light efficiency and photometric performance of the light source;
- shape of area to be surveyed by cameras: narrow or wide, spot or flood;
- sensitivity and spectral response of the cameras, particularly colour cameras;
- reflectance of the materials making up the majority of the surveyed area;
- time delay to reach the specified light output of the lamp after application of power;

- the loss of light output of the lamp due to ageing and lamp failure for example, LED-based illuminators can suffer degradation, in order to deliver a constant level of lighting performance throughout the life of the illuminator a compensation mechanism may be necessary;
- the new or additional light source selected shall give acceptable pictures under all likely working conditions;
- illumination over the scene being surveyed shall be as even as possible avoiding any area of very low light illumination. The ratio of maximum to minimum illumination within the covered area of any scene shall ideally be 10:1 or better;
- where possible lights shall be mounted so that they do not impair the camera picture quality, for example by producing heat haze in the field of view. The preferred position for the light is above the camera. The camera shall not view the scene through intense beams of light;
- where possible the light source should be a minimum of 2 m from the camera. Light sources attract insects which can cause overexposed hot spots , as can objects such as raindrops, snowflakes and falling leaves, this is of particular importance where VCA/VMD is used;
- the light sources should be located within a short distance to the object to be monitored;
- all illuminators including non-visible shall be positioned observing the minimum safety distance to prevent eye damage;
- there shall be safe access to the lamps for bulb changing;
- particular attention shall be paid to the direction of illumination. The aim is to produce a maximum of contrast for intruder detection. An object can only be detected if its brightness is different to that of its background;
- for inspection, identification and recognition purposes, illumination shall enable detailed features of the object as stated in the OR to be observed. If an accurate personal identification is required, it is recommended to direct the light sources into the expected direction of movement i.e. the faces of the targets should be illuminated;
- constant illumination or quickly changing lighting conditions, static or transient highlights in a uniform picture;
- environmental influences on visibility like rain, fog, etc.;
- if an additional light source is necessary, but illumination by white light is not desirable, IR spotlights and IR–sensitive b/w cameras or IR cameras can be used;
- illuminators with asymmetric optics can be used to increase the range of infrared illumination, helping to avoid uneven exposure of the scene;
- lights shall not be positioned such that they directly face cameras;
- high sensitivity cameras or fast lenses with large aperture can be used to avoid the need for additional lighting.

6.10 IP Video equipment

The different functionalities of a VSS may be covered either by physically separate components or devices, which cover multiple functions. They may be distributed over an IP network.

The functionality of image encoding and streaming may reside in video encoders, or combined together with image capturing in IP cameras or megapixel cameras; image storage may be accomplished by NVRs or network storage devices; if combined with image encoding, a DVR may be used. Video content analysis (VCA) and video motion detection (VMD) may be offered by all of these devices or separately in VMD devices or VCA servers. The image presentation on video displays may be done by video decoders or PC based workstations. All of this equipment may be monitored and controlled by a supervising video management system (VMS).

6.11 Tamper protection/detection

6.11.1 Camera tamper protection/detection

Once the VSS camera has been installed and commissioned it is essential to the successful operation of the VSS to maintain the agreed field of view. The camera shall be installed in such a way that it is difficult for an intruder to change the field of view for the camera. This should be achieved by installing in a suitable location/height, the use of appropriate physical mounting and possibly further by the use of security fixings. Furthermore the interconnections (e.g. cabling, antennae) should not be accessible and/or able to be torn off.

Depending on the security grade , if selected in the OR, of the VSS/camera, automatic methods shall be deployed to detect the change of field of view of the camera according to IEC 62676-1-1:2013, 6.3.2.3.

Consideration shall be given to the detection of loss of signal and camera obscuring or blinding on any connected camera. An audible and/or visual system alarm shall be generated for acknowledgement by system operators and a facility shall exist where this alarm can be mapped to an alarm output for connection to an alarm system, if defined in the OR.

6.11.2 System tamper protection/detection

The primary method for protecting the centrally located components of a VSS, such as image storage, control equipment, from tampering is to install the system in a suitably secure location (see 12.6), with appropriate access controls to both the location of the system, and the system/equipment according to IEC 62676-1-1:2013, 6.3.

6.12 System integration

For the combination and integration of other security systems into the VSS or vice versa the general requirements of CLC/TS 50398 should be applied.

For an individual integration of a VSS into any other system or vice versa, the integrator needs a full specification on the offered interfaces. In the next step an integrator needs to develop a programmatic implementation to operate the requested interfaces. This applies to systems with vendor specific interfaces.

Alternatively the integrator may choose different security applications from a single source, where all components are manufactured as a single brand by one vendor. The integration is limited to the products offered by this vendor and it is not possible to select the "best of breed" or expand the system at a later time by other brands or upgrade to new equipment.

Open VMS or frameworks may be chosen, where components from several vendors may be integrated via plug-ins, drivers or open interfaces. These IP video devices and their interface should be compatible to the general IP requirements of IEC 62676-2-1 in terms of: IP connectivity, video stream transport, video payload, stream control, eventing and device discovery and description. If the end-user selects a VSS or video components, which are based on interconnections compatible with IEC 62676-2, either based on REST or on Web Services, the integrator only needs to take care that the integrating system is compatible to IEC 62676-2 implementation.

The integration of a VSS may include video streaming, control, eventing, configuration, discovery and description and other interfaces.

7 Image presentation

7.1 Display types

The image presentation device(s) should be selected after taking into account the nature of the image viewing task, the conditions in the control room or other viewing space and whichever of the criteria in Table 3 are considered to be relevant. It should be considered whether displays are also used for viewing maps, floor plans, device lists, system status, alarm conditions, etc.

In simple terms, displays come in two main forms, the CRT (cathode ray tube) or the modern flat panel variety. Less commonly rear projection systems are used. The flat panel displays can either be LCD or plasma. Examples for display technologies are shown in Table 4.

Table 4 – Examples of display technologies

Type	Pros	Cons
CRT	Good picture quality Good contrast Much equipment was designed for reproduction on a CRT	High power consumption High heat generation High space requirements Manufacture largely discontinued Irreversible image burn-in
LCD (CCFL backlit)	Compact and light Low power consumption Wide range of screen sizes available High resolution	Possibly restricted viewing angle Lower image contrast Reversible image retention
LCD (LED backlit)	Compact and light Lower power consumption Wide range of screen sizes available High resolution Improved colour reproduction	Possibly restricted viewing angle
Rear projection	Seamless high resolution display surfaces Low power consumption	Space requirements similar to CRT monitors Initial investment cost
Plasma	Slim design, wall mountable High resolution, Larger maximum size than LCD Wider viewing angles than LCD Good black levels (no backlight)	Fragile High power consumption High heat generation Irreversible image burn-in

When selecting a display, the following should be considered:

- Size: Large size and high resolution flat panel displays can be effective as matrix displays for multiple cameras. High screen resolution will not improve the capture resolution. Rear projection video walls add seamless display of a mix of cameras and graphical canvas containing mapping, floor plans.
- Heat: The amount of heat a unit generates becomes significant as the size of the facility and number of displays increases and can impact not only on operator comfort but also on machine efficiency and air conditioning cost.
- Colour: Modern displays of all types have similar quality colour reproduction.
- Brightness: The light output of a display in Cd/m^2. The brightness of a display shall be adapted to the lighting conditions of the environment. As a rule of thumb, the brightness

level of bright content on a display should correspond to the brightness of a white sheet of paper held in front of the display. This is to avoid eye-strain due to brightness variations.

- Contrast: The ratio between white and black measured in a dark environment. This eliminates the influence of lighting in the room. As such, contrast has only an indirect influence on picture quality (see black level).
- Black level: The 'black level' of a screen refers to how well black image content is perceived in a normal lit environment.

  A good lighting layout in the room and the use of anti-glare technology on LCD screens or dedicated rear-projection screens is required to maintain good image quality.
- Burn in: Most screens can suffer from 'burn in' or image retention, where if the same background is displayed continuously for a long period, this can leave a permanent mark on the screen. Plasma and CRT screens have permanent burn-in. LCD shows reversible image retention on static content in a few months. Rear projection (using DLP technology) is image retention free.

7.2 Resolution

Display screens have different resolution depending on set-up and type. Display resolution shall be selected to match and complement the camera resolution and resultant video resolution. For larger display surfaces, the efficient display resolution can be defined according to the minimum visible size of a pixel.

The size and resolution of display screens should be considered together with the recommended display sizes in 12.4. An operator placed at a large distance may not be able to discern the details of a small high resolution monitor.

EXAMPLE A 50 in (127 cm) full HD display has a pixel size of 0,57 mm. A person with average eyesight can discern a single pixel up to a distance of 1,98 m. Table 5 contains a few additional values.

Table 5 – Example resolutions

Screen size	Resolution	Pixel size mm	Distance m
20 in (51 cm)	SXGA+ (1 400 × 1 050)	0,29	1,00
50 in (127 cm)	SXGA+ (1 400 × 1 050)	0,71	2,50
70 in (178 cm)	SXGA+ (1 400 × 1 050)	1,00	3,40
80 in (204 cm)	SXGA+ (1 400 × 1 050)	1,14	3,90
50 in (127 cm)	Full HD (1 920 × 1 080)	0,57	1,98
70 in (178 cm)	Full HD (1 920 × 1 080)	0,80	2,75
Rule of thumb: Distance (mm) = Pixel size (mm) / 0,000 290 7			

8 Transmission

8.1 Principles

8.1.1 General

Video can be transmitted and consumed either as an analogue or digital stream, it may be compressed or uncompressed. Each video type can be converted to the other. Conversions should be kept at an absolute minimum to preserve video quality throughout the whole VSS.

The purpose of the transmission subsystem in a VSS installation is to provide reliable transmission of video signals between the various VSS equipment in security, safety and monitoring applications.

The video transmission subsystem needs a security application to transport not only the video content itself, but also video related control (e.g. for replay), event and status signals.

The end user, installer and integrator need to decide on the adequate video transmission subsystem. Today, different kinds of video types and ways to transmit video exist: analogue, digital and IP, compressed and uncompressed, standard and high resolution, dedicated and shared interconnections, wired and wireless, short, long distance and remote.

For analogue non compressed video signals the transmission subsystems may consist of dedicated cable transmission media such as coaxial cable, twisted pair cable, fibre optic cable. Wireless transmission methods may include microwave, Infrared or radio transmission. Multiple analogue video signals may be combined in one physical transmission path using multiplexing techniques.

For analogue high resolution video transmission a dedicated cabling for VESA and VGA signals is recommended; for uncompressed digital high resolution video a transmission according to the HDMI and DVI standard is recommended. These types of video transmission are quite common for the connection of high quality video displays over a short range of about 15 m or more.

The analogue video transmission subsystem including video transmission devices such as transmitter, receiver or intermediate devices associated with the selected transmission media shall be selected by the installer and integrator in accordance with the signal and performance requirements of IEC 62676-3.

For remote accessibility, high image resolutions, digital recording and replay, integration, scalability and other purposes of the video transmission subsystem it is recommended to use IP video. When considering IP video the most important requirement is that the IP network is able to deliver the required amount of information, especially video streams, with minimum delay, loss and jitter. These performance requirements for IP networks define the design principles of the network. A video transmission subsystem in surveillance applications shall comply with the minimum requirements of IEC 62676-2-1. To guarantee this performance a detailed IP video design guide is given in IEC 62676-2-1. Integrators and Installers should follow the network planning of this standard. It is recommended that a network specialist is consulted early in any system design.

8.1.2 Selection of IP video performance classes

The end-user needs to decide on one out of 4 possible levels of performance of the network and the connected video transmission devices. The performance classes 1 to 4 are introduced by IEC 62676-2-1 and need to be selected according to the surveillance task:

a) time accuracy for video transport stream: Class T1 to T4;
b) interconnections – Timing requirements: Class I1 to I4;
c) throughput limitation capability: Class C1 to C4;
d) video stream priorizing: Class P1 to P4;
e) maximum network loss, latency and jitter: Class S1 to S4 and M1 to M4;
f) monitoring interval for interconnections: Security grade 1 to 4 (see 4.2.2).

For high security applications redundancy and security of the network needs to be considered.

8.1.3 Interoperability

If video transmission devices of different vendors shall be combined and operated together in a single IP network, it is necessary to take care of the compatibility. For this reason the integrator needs to select video transmission devices, which are compliant to IEC 62676-2 series. For a basic interoperability the IP video devices should be compatible to the protocol requirements of IEC 62676-2-1 in terms of IP connectivity based on TCP/IP and UDP, video

stream transport via RTP, one of the standardized video payload formats such as MPEG4 or H.264 and stream control based on RTSP. For eventing, device discovery and description there are different protocol options.

For a full interoperability of video stream transmission, stream control, eventing, discovery and description of network devices based on one framework, the integrator needs to select a high-level video IP protocol. He may choose a compatible implementation for IP video interoperability according to IEC 62676-2-2 based on REST services or IEC 62676-2-3 based on Web Services or any other open protocol which may be defined in the future, but is today not available.

If an IP video network is managed together with an IT network. It is recommended that the same administrators should have control over both networks.

8.2 Wired transmission links

The most common form of an analogue wired connection is a coaxial cable. This is generally terminated with BNC connectors for compatibility. Standard coaxial cable (RG59) is suitable for transmission links of up to around 200 m. Larger ranges can be achieved by using rectifying amplifiers or cables with less attenuation (such as RG6 or RG11).

Another option for wired video transmission is a twisted pair cable. Common examples are Cat-5 and Cat-6 cables, which comprise four twisted copper wire pairs, and are used for analogue or digital transmission.

Fibre optics is an alternative solution which provides high capacity, high speed and low latency, long transmission distance with low signal attenuation (km), resilience to electromagnetic interference, resilience to tapping.

8.3 Wireless transmission links

A VSS specifier should consider the needs of the viewer/system operator when designing the transmission network and appropriate network security. The main technology types have been summarised in Table 6.

Table 6 – Wireless transmission options

Link type	Transmission distance	Transmission frequencies	Link data rate (unidirectional)	Comments
Analogue RF	~30 m indoors ~100 m + Outdoors (Non line of sight)	2,4 GHz / 5 GHz (Unlicensed bands) Other frequencies can be used depending on spectral allocation and licensing details.	Dependant on installation specifics	Simple operation described here. More complex solutions can be offered.
"Wifi" (IEEE 802.11)	~30 m indoors ~100 m Outdoors (Non line of sight)	2,4 GHz / 5 GHz (Unlicensed bands)	Up to 74 MBits/s (IEEE 802.11n) Up to 19 MBits/s (IEEE 802.11g)	Generally not suitable for long range transmission. Range and throughput is heavily dependent on signal power at receiver.
Mobile WiMax (IEEE 802.16e)	Up to 50 km (Line of sight)	Depends on installation. Configurable to both open and licensed frequencies	Up to 70 MBit/s	System either delivers long transmission distance or high transfer rate, not both. Developing technology
2G GSM (Global System for Mobile Communications)	National/International assuming system is within cell coverage (Inner City ~300 m from cell site Rural ~ 8 km from cell site)	~800 MHz to 950 MHz or ~1,9 GHz to ~2,2 GHz (Limited to cellular phone licensed bands)	14,4 kBit/s	More suited to speech and very low bit rate video or stills transmission. Requires a cellular service provider. Performance is dependent on carrier load, atmospherics and infrastructure provision.
3G HSDPA (High speed downlink packet access)	National/International assuming system is within cell coverage (Inner City ~300 m from cell site Rural ~ 8 km from cell site)	~1,9 GHz to ~2,2 GHz (Limited to cellular phone licensed bands)	Currently up to 14,4 MBit/s	Requires a cellular service provider. Performance is dependent on carrier load and atmospherics and infrastructure provision.

8.4 Key considerations for IP based transmission systems

In a packet-based network, the performance of any video transmission device or application depends on the quality of service assigned to a particular application. To support video traffic adequate quality standards and performance figures shall be met for acceptable video streaming services. Especially four factors – throughput, latency, jitter, and packet loss – define the quality from the network point of view. How each is managed determines how effectively the network supports IP video traffic. A fifth factor ´redundancy´ or ´alternative routing´ is also an important consideration to help protect critical VSS- and operator-traffic.

- **Throughput:** "The size of the possible video stream pipe" (for example, 1 Mbps up through 10 Gbps). Several compression/decompression (codec) algorithms recommended by IEC 62676-1-2 can reduce the throughput needed for one IP video input to a fraction of the traditional coaxial cable exclusively reserved for a single camera in this dedicated interconnection.
- **Latency or delay**: "The travel time through the pipe" – how long it takes for a packet to travel through the network. Live video and other telemetric control such as PTZ sensitive to delay. Maximum latency shall be according to performance requirements of

IEC 62676-1-1:2013, Clause 5. Typically, the network is not the largest contributor to the latency chain.

- **Jitter or delay variation**: "The received flow variation or pumping of stream" – the continuity with which packets arrive at their destination. Jitter buffers can temporarily delay incoming packets to compensate the jitter, but only some of the delay variations. These buffers have limits and excessive buffering can result in additional latency. Maximum jitter shall be in accordance with the performance requirements of IEC 62676-1-2:2013, Clause 5.
- **Packet loss**: "The leak in the stream". Packets can get lost because of collisions on the LAN, overloaded network links, or for many other reasons. Loss of packets beyond a very small percentage will degrade video quality. Note that IP video stream uses the User Datagram Protocol (UDP), which, unlike TCP used in non-streaming applications, does not provide the retransmission of packets. Maximum packet loss shall be in accordance with the performance requirements of IEC 62676-1-2:2013, Clause 5.
- **Redundancy, alternative routing and protection switching**: "Identifying and replacing a broken link or stream" to enable a reliable video transmission via alternative routes.

These factors are defined and covered in more detail in IEC 62676-1-2 including their impact on the network design.

9 Video performance characteristics

9.1 Image compression

Image compression settings should always be dictated by the OR for each camera view, and not the storage capacity of a proposed system.

The compatibility of the image format transmitted, stored and exported from the VSS should be considered alongside image compression, many VSSs use proprietary codecs which are unable to be received and replayed by a widely available software application. See Clause 11.

The suitability of a profile level or type should be identified using an image quality test specific to the purpose of the camera view. A number of image quality tests are discussed in more detail in 13.3.

NOTE The live and the recorded views of the same scene can show different levels of quality, depending on which point in the image chain, the compression is applied.

Image quality tests for live, recorded and exported views should be defined to ensure the system is capable of meeting its OR.

9.2 Frame rate

The required frame rate should be determined for each individual camera view. There are multiple factors which should be taken into account when selecting the desired frame rate.

These factors include:

- the risk for the camera’s desired field of view as defined in the risk assessment,
- the purpose of the camera as defined in the OR,
- the anticipated activity in the area to be observed,
- the field of view of the camera,
- whether the frame rate is changed by an external trigger such as an alarm device or VCA or VMD alarm,
- whether the camera is observed by an operator, low frame rates can be difficult to view for sustained periods.

For example, a camera whose purpose is to capture a short pathway outside a building should be set with a sufficiently high frame rate that a person could not move from one side of the field of view to the other without appearing in a single frame.

Guidance on selecting an appropriate frame rate depending on the purpose and risk associated with each camera view is available in Annex D.

In systems which allow reduction of frame rate and/or of image resolution of stored video after a set period of time in order to lower the overall storage requirement the reduced quality storage shall still be fit for purpose.

9.3 Resolution

The resolution for a camera view shall be determined from the purpose of the camera as defined in the OR and required coverage. The camera should be able to achieve this resolution without using digital zoom. For example, if the "identify" category defined in 6.7 is required then any system with a resolution of 2CIF or below would require the subject to be very closely framed which is not practical in most cases.

If observation of a single wide area is required then a small number of high resolution cameras may be a better solution than a large number of lower resolution cameras. However, if the area contains a large amount of activity then consideration should be made to whether it is more suitable to be viewed by a single operator or multiple cameras.

10 Storage characteristics

The total storage requirement for a digital video recorder should be estimated before a system is installed, so that a hard drive of the appropriate capacity can be specified. It is vital to ensure that sufficient capacity is available so that compromises do not have to be made on either the image quality or retention time.

The storage capacity needed in a VSS depends on several factors, which are summarised in a) to f) below. Typical values for each variable are given in Table 7.

Table 7 – Factors affecting the storage capacity required for a video recorder

Variable	Frame size	Fps	Number of cameras	Operational hours	Retention period	Storage management
Typical range	5 kB to 50 kB	1 to 25	1 to 16+	1 to 24	24 h to 31 days	Add 1 day protected

a) Frame size: This value is the average size of each image as recorded. The actual figure will be a function of the image resolution (in pixels or TV lines) and the amount and type of compression applied to the image or video sequence (It is particularly dependent on whether inter-frame compression is used, in which case the average frame size will be an average of larger I-frames and smaller P-frames.) These factors are very much specific to the specific video recorder, which can make the image size difficult to estimate accurately, and assistance should be sought from the system supplier.

b) Frames per second (fps): The number of images recorded each second by a camera has a significant impact on the amount of data being generated. The preferred frame rate should have been identified during the level 2 OR capture process.

   This value could be dynamic if a camera is triggered by external alarms or motion detection. For some systems there may be no recording unless activity is detected. For others, there may be continuous recording at a low frame rate, say 1 fps, until activity is detected, when there will be a short period of recording at a high frame rate, say 12 fps. If this is the case an average value should be calculated by estimating the number of anticipated triggers in a 24 h operational period, for example:

- standard rate (R_S) = 1 fps;
- triggered rate (R_T) = 12 fps;
- triggered period (T) = 3 min;
- number of triggers anticipated per day (N) = 10;
- number of minutes per day at triggered rate = $N \times T$ = 30 min;
- number of triggered frames generated = 30 × 60 × R_T = 21 600;
- number of minutes per day at standard rate = 23 h 30 min = 1 410 min;
- number of standard frames generated per day = 1410 × 60 × RS = 84 600;
- total number of frames generated per day = 21 600 + 84 600 = 106 200;
- average frame rate per second = 106 200 / number of seconds in 24 h = 106 200 / 86 400 = 1,2 fps.

c) Number of cameras: This is the number of recorded cameras used for the whole system under consideration, as specified in the OR.

d) Operational hours: This is the number of hours the VSS will be operational, within a 24 h period, as specified in the OR.

   In a simple system this could be for the full 24 h per day, whereas in a more complex system it could be for a predefined number of hours whilst the premises are occupied/vacant.

e) Retention period: The time for which the video footage should be stored on the system before being overwritten, as specified in the OR.

f) Storage management: Where video data is to be prevented from being overwritten, there should be a facility to protect recordings from being deleted. The method and storage requirement should be defined in the OR. This should not reduce the retention period of the normal recording.

A general equation has been given to aid in estimating the total amount of storage required:

$$\left(\frac{S \times C \times H \times 3\,600}{1\,000\,000}\right) \times T_R$$

where

S is the image size in kB;

fps is the number of images per second;

C is the number of cameras in the system;

H is the total number of operational hours in a 24 h period;

T_R is the retention period;

3 600 is to convert seconds into hours (60 × 60);

1 000 000 is to convert kB to GB, approximately.

This equation can be used for very basic systems where all the cameras are recording at the same image size, frame rate and operational hours. For more complex systems a storage requirement can be calculated for each camera and the resultant totals added to give the overall requirement for that system.

EXAMPLE 1 A VSS is being specified for a custody suite that is required to capture high quality images of 20 kB per frame. 12 fps per camera are being generated, at an approximate stream rate of 240 kbits/s, and there are 8 cameras in the system. Each camera is recorded for 24 h per day, and the OR has stipulated a retention period of 31 days. The storage capacity is given by:

$$\left(\frac{20 \times 12 \times 8 \times 24 \times 3\,600}{1\,000\,000}\right) \times 31 = 5\,142 \quad \text{(GB)}$$

As can be seen this represents a large amount of data, and another strategy might need to be considered to ensure the amount of data being collected is manageable. In this case it might be considered that the amount of data being generated is necessary, in which case the storage provisions should be made. However it might be deemed more appropriate to reduce the image size/quality on half of the cameras, or to reduce the frame rate on some of the cameras. Another approach might be to use IR triggers or motion detection to trigger the image recording.

EXAMPLE 2 A retail outlet is installing a small VSS to view the access points (windows and doors) whilst the shop is closed. The image frame size has been to set to a 'medium' value (10 kB), and the resultant image checked for suitability against the level 2 OR requirements. The recorder will be triggered by motion detection and IR sensors and the average frame rate has been calculated as 2 fps for all the cameras. 6 camera locations have been identified to offer maximum coverage, and all the cameras will only be recording for the hours the venue is closed 7 pm until 7 am. As the reason for the system is to provide evidence after a break-in the retention time has again been set to 31 days. The storage requirement is given by:

$$\left(\frac{10 \times 2 \times 6 \times 12 \times 3\,600}{1\,000\,000}\right) \times 31 = 160 \quad \text{(GB)}$$

11 Image storage and export

11.1 Format of the compressed video data

Special or modified compression algorithms prevent the police and the courts having direct access to the video data without the use of proprietary software.

The compressed images (and audio if present) shall be encoded using standard compression formats (see IEC 62676-1-2 or Annex A "current video standard formats"). The compressed data shall comply strictly with the standards and contain the full information required to decode the images and audio.

The compression format and the means of locating the compressed data within the video files shall be made public.

11.2 Encryption

The images shall not be encrypted. The video format can contain checksums or other methods for ensuring that changes to the data may be detected but, where used, they may not alter the compressed image information.

NOTE There is no requirement for manufacturers to release information on methods used to ensure that their video files have not been tampered with. The police ensure that video data is valid for use within the criminal justice system by maintaining a clear chain of evidence – encryption can delay or prevent legitimate access to video evidence.

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

11.3 Basic metadata (time, date, camera identifier)

Being able to correctly identify the time at which an image is captured is often essential to the use of VSS in police investigation. Therefore:

- the data contained within the video files shall permit a time stamp and camera identifier to be associated with each image and audio sample. For video without audio, the time stamp shall have a resolution of no less than one second. Where both video and audio are present, the time stamps shall have sufficient resolution to permit synchronised playback of the audio-visual streams;
- the means for determining the time stamps and camera identifier on each image and audio sample shall be made public. There are many ways of encoding time stamps, but whichever is used shall be stated;

- the video format shall specify any time offsets that are applied to time stamps and give the method for converting each time stamp into a local time that is local to a time zone and which includes any applicable daylight-saving adjustment;
- time should auto update for changes between any daylight saving offsets and UTC;
- it should be considered, if precise timing is required, whether a network time server according to IEC 62676-1-2 is used;
- for additional metadata (e.g. geodata, floor level, VCA, PTZ positions, etc.) the format and compatibility shall be stated in the OR.

11.4 Multiplexing format

Where a video recording contains multiple steams of video (and audio) the video files shall incorporate metadata which allow the streams to be de-multiplexed. The method for de-multiplexing shall be made public.

It is permissible for the video format to contain other streams of data which are not essential for extracting the images and audio samples with their time stamps. The additional data streams may remain proprietary although it is recommended that their format is published so that they can be decoded independently of the manufacturer's software.

It is recommended that each video and audio stream has a name which may be meaningful to the user of the VSS. Where names are present, the method for associating streams and their names shall be made public.

11.5 Image enhancements

If the system provides enhancement tools such as image sharpening, brightening or zooming in on a particular part of the image then any applied enhancements should not change the original recording. If an enhanced image is exported, an audit trail documenting these changes should exist.

11.6 Image export

To facilitate replay and export the following should be adhered to:

- video data exported from a recorder shall have no loss of individual frame quality, change of frame rate or audio quality. There should be no duplication or loss of frames in the export process. The system should not apply any format conversion or further compression to the exported images, as this can reduce the usefulness of the content;
- any original metadata and/or authentication signatures shall be exported with the images;
- a simple user guide should be available locally for reference by a trained operator;
- the facility should be provided for the export of images from selected cameras within user-defined time periods;
- simultaneous export and recording should be possible without affecting the performance of the system except on systems that require removal of the primary storage media for export purposes;
- the export method of the system should be appropriate to the capacity of the system and its expected use.

If the export method is not appropriate there is a risk that if the police require video evidence they may need to remove the system, for example if 1 terabyte of data is required it is not practical to export this via a CD writer.

A number of methods exist for exporting images in native format from a system, for example:

- images are copied to removable digital media such as a floppy disk, DAT tape, flash card, CD-R or DVD, etc.;

- the removable hard disk, which holds the images, is physically removed from the system;
- images are exported via a port, such as USB, SCSI, SATA, FireWire or networking;
- documentation should be supplied to the user regarding both the retention period of the system and the approximate times to export each of the following;
- up to 15 min of recorded data per camera;
- up to 24 h of recorded data per camera;
- all of the data on the system;
- the system should display an estimated time to complete the export of the requested data. Export scenarios should be defined and documented which are proportional to the size of the export as above;
- the software application needed to replay the exported images should be included on the media used for export, otherwise viewing by authorized third parties can be hindered.

11.7 Replay of exported images

If the export format meets a common non-proprietary standard then a proprietary export player may not be necessary. If the manufacturer chooses to produce proprietary replay software then the exported images should be capable of being replayed on a computer via the exported software. This software should:

- have variable speed control including real time play, stop, pause, fast forward, rewind, and frame-by-frame forward and reverse viewing,
- display single and multiple cameras and maintain aspect ratio i.e. the same relative height and width,
- display a single camera at the maximum recorded resolution,
- permit the recordings from each camera to be searched by time and date,
- allow printing and/or saving (e.g. bitmap or JPEG) of still images with time and date of recording,
- allow for time synchronized multi-screen replay,
- allow for time synchronized switching between cameras upon replay,
- allow replay of associated audio and other metadata,
- be able to export the image sequences in a standard format at an equivalent quality to the original and still displaying time and date information (e.g. MPEG-2, MPEG-4, H.264 or MJPEG) with no significant increase in file size,
- clearly show the time and date, and any other information associated with each displayed image, without obscuring the image,
- if removable hard drives are used as a primary export option (dependent on download scale) then the drive should be replayable using a standard computer, for example, on a Windows based operating system; this functionality is also desirable for any hard drive used in a VSS where this is not the primary means of export.

12 VSS control room configuration

12.1 Control rooms

If the VSS has a requirement for live viewing, camera control, system management, or any other human intensive tasks, a control room should be specified to house these functions. The 'control room' could be a single workstation, or a large operations centre.

For the presentation of camera images to the operator either analogue or digital video displays may be used. Here the term display refers to both possible technical solutions.

12.2 Number, size and positioning of VSS video displays

In a control room environment

a) the operator shall be presented with a suitable number of video feeds (e.g. is the operator able to suitably view 8 cameras and perform the viewing tasks related to all of those camera views, and their anticipated levels of activity), and

b) the camera view shall be presented to the operator at a size sufficient to allow them to undertake the viewing tasks as above (e.g. is the operator being presented with views intended for identification tasks, but displayed as part of a quad view, at a lower resolution, reducing the amount of information available to the operator),

c) the operator shall be positioned so that they are able to view the information on the display correctly (e.g. is the operator using a display that is too far away to be able to observe relevant details).

12.3 Displays and screens mounted on or off the workstation

Displays that are used for close inspection of video images are commonly called incident or spot displays and positioned on the workstation. They allow for close inspection of images displayed and offer the greatest likelihood of an operator receiving accurate and timely information. Where appropriate spot displays should be positioned directly in front of the operator at between approximately 0,5 m to 1,5 m and of a sufficient size. They should also be placed so that the operator can easily turn their sitting position to face the displays.

It can be advantageous to site two, three or four incident displays on the work desk so that the operator can view video images on a primary display, and use the adjacent displays to show other images or other system details.

video displays can also be positioned off the workstation in a bank or array called video wall. This can be beneficial as a greater number of images can be presented. Displays in a bank shall be positioned at a greater distance from the operator and typically be larger in size, video images displayed in banks are useful for providing a general overview of the camera scenes rather than for picking out details.

Depending on the viewing distance every display or workstation screen may show multiple cameras, for example 4 camera images in a quad display on an analogue display, 9 or 16 in a split view or any other workstation screen layout depending on the capabilities of the system.

12.4 Recommended display sizes

For the selection of the screen size the distance between the display and user is the primary factor. A general rule should be that the viewing distance is between 3 to 5 times the size of the digital screen's diagonal. The exact number shall be determined based on the purpose of the camera view, and the viewing tasks the operator should be able to perform. See Table 5.

12.5 Number of camera images per operator

The number of camera views presented to a video operator shall be decided in the system design phase. There should be the capability to manage the number of camera views presented to the operator. Factors to consider when agreeing on the number of camera views to be presented to an operator may include:

- the risk associated with an event occurring and not being detected,
- the purpose of the observation,
- the type of activity and targets within the image,
- the expected frequency of incidents,
- how long an operator is likely to view an event for,
- other tasks carried out by the operator,

- and the competence of the operator.

To ensure the VSS cameras are being suitably viewed, and the operator is able to perform the viewing task for each view according to the OR, performance evaluations should be periodically undertaken or when there is any significant change to the viewing task or control room setup.

12.6 Number of work stations

The operational requirements should determine the number of workstations and associated equipment within the control room.

The analysis to determine the number of workstations required shall be undertaken based on the anticipated peak activity. The four main considerations shall be:

- expected number of alarms/events during the observed location(s) peak periods,
- required response time from an event occurring and the operator taking some action,
- expected time for an operator to return to normal viewing following an event response,
- number of cameras/locations to be monitored.

The time that an operator takes to manage an alarm depends on two factors:

a) the nature of the alarm/event, for example does the operator need an extended period to guide a guard to the incident or can the operator dismiss the alarm rapidly having viewed the location;
b) agreed standard operating procedure for an alarm notification, for example is a VSS tour of the entire site required following a perimeter alarm notification.

The VSS shall be designed such that at peak time the operators are able to manage alarms more quickly than new events arise. If this does not occur, then a backlog occurs and the response time increases.

There should be sufficient operator capacity within the control centre to ensure that all alarms/events can be met with an appropriate and agreed response. Failure to achieve this, especially at peak times, will result in alarms/events being missed, compromising the purpose of the VSS.

When designing the system display layout that an operator will use, consideration should be given to the logical grouping of camera views to allow rapid and intuitive view switching. This should be based on either the purpose of the camera or the location of the camera.

12.7 Equipment siting

The following criteria should be used for equipment siting:

- the control desk should be ergonomically designed with particular attention being paid to siting of video displays in order to avoid reflections from extraneous light sources on the display screens;
- video storage equipment and storage media should be installed in protected areas, preferably inaccessible to unauthorised persons;
- workstations shall be suitably protected from unauthorised use, either by access control or software permissions.

12.8 Backup power supply provision

Consideration should be given to the provision of an uninterruptible power supply (UPS) and/or backup power generator based upon the risk assessment.

Where defined in the OR there should be a backup power supply provision for cameras.

Where a UPS is to be installed the power consumption of the equipment shall be calculated for the purposes of determining the required specification of the UPS.

12.9 Operating temperature

The system design should consider maintenance of suitable operating temperature and environment.

Poor environmental conditions caused by external sources or the system components may impact operators and the life of equipment.

12.10 Lightning and surge protection

Where there is a risk of electrical interference/lightning strike, suitable protection should be provided as required. Suitable equipment earth points should also be provided as required. The system should comply with ISO/IEC 11801 series, IEC 62305 series, IEC 62305-3 and IEC 62305-4.

13 Defining the test plan

13.1 Purpose of the test plan

The test should be written to ensure that any expected functions and features of a VSS can be assessed. This assessment should cover any specific requirements identified during the design phase. The test plan should have two main purposes:

a) to support the acceptance of installed VSS capability;

b) to support periodic system/function validation.

This testing should cover two areas, user acceptance and technical acceptance.

13.2 User acceptance testing/inspection

User acceptance testing (UAT) is the process where an appropriate operator assesses the user interfaces and checks them to ensure that specifications have been correctly delivered by the installer. The UAT should include all specified features within the operators control, including image quality acceptance assessments, device control for example PTZ and camera response, camera view selection and event/alarm response. The UAT should be written in conjunction with the OR to ensure that every specification made in the OR has an appropriate reciprocal acceptance test.

13.3 Technical acceptance testing

13.3.1 Imaging chain consistency

Where a particular resolution, frame rate or other image quality level is defined in the OR it should be determined, using a suitable image quality test, that this is being maintained consistently throughout the imaging chain, from camera to display device to video recording device.

13.3.2 Image quality

The OR should define for each camera the required image performance and quality with any associated image quality tests. The OR should then be used as a checklist to verify all image performance and quality requirements.

13.3.2.1 Verification of image quality

The quality of the image should be verified using a test image or test scenario. Annex C contains test images for contrast, resolution, and colour reproduction. Annex C also contains test images for facial and number plate identification. The quality of the image should be measured on the presentation device(s) on which images will be viewed in normal operation of the VSS. Where there is a requirement pertaining to exporting the data the exported images should be tested to ensure they meet the OR. The system design proposal should stipulate the conditions under which the test image(s) should be used. For example, if the system will be used in both day and night conditions then separate tests should be performed for the different light conditions.

Other suitable test procedures may be used or be necessary. For example, the test image in Annex C is not suitable for evaluating images in the infrared range.

13.3.2.2 Contrast

The test image in Figure C.1 contains two quality levels for contrast:

– 11 grey steps; and

– 3 grey steps.

The OR should define which of these levels is to be achieved. The system will pass the test only if all grey steps are distinguishable on the specified scale.

Refer to Annex A for details of the test procedure.

13.3.2.3 Resolution

The resolution should be checked with reference to the target sizes (see 6.7) using the test target in Annex C.

13.3.2.4 Colour reproduction

The test image Figure C.1 contains 6 colour blocks at two different luminance levels. If the OR requires the system to reproduce colour then the appearance of the top line of blocks on the presentation device should be a representative reproduction of their colour on the test image under the prescribed lighting conditions.

Refer to Annex C for details of the test procedure.

13.3.2.5 Facial Identification

If the OR requires the system to be capable of producing images suitable for identifying faces then Annex B should be used.

The test consists of 9 human faces. It is designed to assess a VSS's ability to identify faces. A random selection is presented towards the camera at a prescribed person percentage screen height or distance from camera. An operator attempts to match the presented face to a reference list, the results of which are recorded and evaluated. The OR will specify the percentage screen height at which a pass should be achieved.

Refer to Annex B for details of the test procedure.

13.3.2.6 Inspect

If the OR requires the system to be capable of achieving the inspection category then the target should be reproduced at no lower resolution than 1 mm per pixel and the target should

represent a screen height of 400 % for PAL and 450 % for NTSC or equivalent identified in Table 3.

13.3.2.7 Recognise

If the OR requires the system to be capable of achieving the recognition category then the target should be reproduced at no lower resolution than 8 mm per pixel and the target should represent a screen height of 50 % for PAL and 60 % for NTSC or equivalent identified in Table 3.

13.3.2.8 Observe

If the OR requires the system to be capable of achieving the observation category then the target should be reproduced at no lower resolution than 16 mm per pixel and the target should represent a screen height of 25 % for PAL and 30 % for NTSC or equivalent identified in Table 3. The system should be tested to ensure that some characteristic details of individuals can be identified, such as distinctive clothing. Individuals should be able to be clearly distinguished from each other, i.e. it should be possible to determine with a high level of confidence how many people are in the field of view.

13.3.2.9 Detect

If the OR requires the system to be capable of producing images suitable for detecting the presence of an intruder then Annex E should be used. The target should be displayed at a minimum of 10 % screen height as specified in Table 3 and no lower resolution than 40 mm per pixel.

The test methodology sets out how the OR should define the criteria against which the system should be tested to determine whether an intruder could be detected within an acceptable time period following an alarm.

13.3.2.10 Monitor

If the OR requires the system to be capable of producing images for crowd control or monitoring then the target should be reproduced at no lower resolution than 80 mm per pixel and no less than 5 % screen height as specified in Table 3.

13.3.2.11 Number plate identification

If the OR requires the system to be capable of producing images suitable for identifying number plates then Annex B should be used.

The test consists of 9 groups of letters.

A random selection of letters is presented and the operator should record the letters they see. This test requires 100 % accuracy for a pass to be achieved. The OR will specify the location in the frame at which a pass should be achieved.

Refer to Annex B for details of the test procedure.

14 Summary of the documentation – Pre-installation

14.1 General

At this stage in the development of a VSS the following documentation should have been produced to assist and enable the needs of the end user to be met. These documents should be archived in a secure way so that they can be used as a reference guide to the system details.

14.2 Risk assessment

See 4.2, the threat to the premises should have been analysed to determine the risks. The VSS shall then be designed to mitigate the risks identified.

14.3 Operational requirements

See Clause 5 of this document encapsulating the purpose or purposes of the VSS, which incorporates the issues identified in the risk assessment, forms the benchmark against which the system performance can be measured.

14.4 Design specification

See 4.5.

14.5 Site plan

See 4.5 and 4.4.

14.6 Test plan

See Clause 13.

15 System installation and commissioning

15.1 Factory acceptance testing

A factory acceptance test (FAT) is an important method for ensuring quality, where the vendor demonstrates that the system design meets the contract and specifications. A FAT may be conducted if any major modification or customisation of standard products – software or hardware – is necessary. It is scheduled at the fabrication plant in which a representative sample of all purchased equipment will be demonstrated. After the conclusion of the design phase, the testing depth and conditions especially for the unique features of the installation should be agreed upon according to the OR. The FAT includes a representative sample of all equipment being supplied by the vendor. It is recommended that a FAT procedure is presented to the customer beforehand. With the FAT the particulars, completeness and functionality are assured, before the actual delivery to the site.

The degree of completion and the assured functionality should be documented. All discrepancies and non-conformities of the system are to be registered on a Non-Conformities List, including an agreement for the “time to complete”. Items incomplete, or not available for inspection or FAT are to be included on the Non Conformities List. In case of defects or open issues, these can be taken into consideration and implemented at manufacturer, integrator or installer site – before final delivery.

For all components, the existence and quality of the agreed-upon documents will be checked. These are manuals, assembly, installation and commissioning instructions, wiring plans, cabinet assembly plans. The components are designated according to the documentation and interfaces labelled. The shipping of the VSS installation to the actual site should be done in bigger building blocks like cabinets of equipment rather than as single components.

Besides the equipment tests, there are several secondary benefits that result and could include:

- initial informal hands-on training presented to the Buyer’s production team by the Manufacturer’s technicians,
- actual hands on training with customized software in site-specific setup, allows real-world operation,

- an installation scope meeting to review the critical parameters and tolerances regarding equipment set-up.

15.2 Installation process

The installation company shall check and evaluate all the existing documentation and verify that site conditions are still consistent with the final design.

Should any change be identified to the site conditions or the risk assessment, the operational requirements and the system design processes shall be revisited to ensure the intended system design will fulfil the operational requirements. If this not possible the design process shall be started again, using the new site conditions/risk assessment.

Prior to commencing work all relevant safety requirements shall be considered. These will vary with the nature of the premises and may involve special installation equipment when working in hazardous areas.

VSS installation methods shall be carried out by trained technicians who are familiar with the manufacturer installation requirements and good industry practise. If relevant conformity assessment exists the installer shall be appropriately certified.

Any change to site plans, installation plans, system designs and/or logical architecture should be included and attached to the final documentation and it should include change permissions and risk/issue/logs generated during the installation process.

15.3 User acceptance testing, commissioning and handover

The user acceptance test (UAT) shall ensure that the system installation meets the specifications and shall be agreed by both owner and installer. The testing depth and conditions especially for the unique features of the installation shall be conducted according to the operational requirements. The UAT shall include all equipment being installed by the installer. A UAT procedure may be presented to the customer beforehand. With the UAT the particulars, completeness and functionality are assured, before the actual commissioning of the site.

The degree of completion and the assured functionality shall be documented. All discrepancies and non-conformities of the system are to be registered on a non-conformities list, including an agreement for the “time to complete”. Items incomplete or not available for inspection or UAT are to be included on the non-conformities list. In case of defects or open issues, these can be taken into consideration and implemented at the manufacturer's, integrator's or installer's site – before the final commissioning of the site.

For all the components, the existence and quality of the agreed-upon documents will be checked. These are manuals, assembly, installation and commissioning instructions, wiring plans, cabinet assembly plans. The components are designated according to the documentation and interfaces labelled.

After a successful UAT the system can be considered commissioned and a formal acceptance document shall be signed by the owner.

This declaration of acceptance shall state that the VSS has been installed in accordance with the general and operational requirements and operates accordingly and that sufficient instruction and training has been provided to ensure the proper operation.

15.4 Declaration of conformance to standards

Once commissioning and handover is complete the installation company shall provide the customer with a declaration of conformance.

When the VSS or components of it are claimed to comply with any legislation, regulation(s), National or regional Standards, any such claims shall be included in the declaration of conformance.

16 Final documentation

16.1 General

This Clause 16 summarises the final document that should be created upon completion of the commission/handover of a VSS. The documentation of VSS shall be accurate, complete and unambiguous. Adequate information on installation, commissioning, operation and maintenance of the VSS shall be provided.

This list shall include the documents referenced in Clause 14 and shall also include the list below where relevant:

– any changes to the original plans/OR shall be indicated on the final documentation. A change log should be written if significant changes to the original plans are made, this log shall include change logic, change permissions/authority and final outcomes to ensure that an adequate record of the VSS is kept;
– the various document types below shall be completed and handed to the VSS owner as a part of the VSS commission/handover process in order to correctly manage maintenance and future expansion of the system;
– a list of recommended spares.

16.2 Complete system drawings

A site diagram showing the camera and other equipment locations as fitted shall be provided. When appropriate a system architecture drawing (describing the component locations, arrangements and interconnections) may be provided.

NOTE Drawings are provided in hard copy or digital format.

16.3 System commission (with camera specific audits)

The following documents should be handed over:

– factory acceptance testing/user acceptance testing results and sign off document (see 15.4);
– copy of commissioning declaration where the commission process has been formalised;
– copy of the maintenance contract/schedule where applicable;
– copy of user manual(s), including quick reference guide, system/component access procedures (system usernames/passwords/methods), and other training materials where relevant;
– reference images of all camera views as agreed with the customer should be made.

16.4 Interface descriptions

The installer shall provide a description of the interfaces for components like PTZ controllers, digital image capture devices, local or remote data export and video streaming.

Where applicable the installer shall provide the driver/system interface, API/documentation for a specific interface according to IEC 62676-2-1.

16.5 Compliance with legislation (informative)

Installers should be aware of national and local regulations and provide necessary documentation as appropriate.

The owner shall remain responsible for the VSS installation, and will have to prepare any compliancy documentation for the VSS, as required by local/national authority, including, public space, data protection, freedom of information, zone masking, human rights and planning permission (including any permissions to operate and any agreed permissions to install equipment).

17 Maintenance

17.1 Maintenance service agreements

Where preventive and/or corrective maintenance service is provided, it shall be in accordance with this standard.

17.2 Staff

Every company shall have sufficient VSS technicians to maintain and service all its installations in accordance with this code of practice (or other applicable technical standards including manufacturers' instructions).

17.3 Corrective maintenance

17.3.1 The emergency service (corrective maintenance) facility shall be so located and organised that, under normal circumstances, the company's VSS technician attends the premises within the time agreed in the contract with the customer.

17.3.2 A reliable system of communication between the control room, the customer and all VSS technicians shall be maintained at all times.

17.3.3 There shall be one or more stand-by VSS technicians. If there is only one VSS technician on call there shall be a support facility to meet the requirements of 17.3.1 above.

This requirement is also considered to be fulfilled if there is an existing cooperation with another expert installer.

17.3.4 VSS technicians and other duty engineering staff shall be available and shall keep in regular and frequent contact with their operational base.

17.3.5 The VSS technician shall determine the cause of any fault and then carry out one or more of the following**:**

a) repair and leave the VSS fully operational;

b) temporarily repair the VSS subject to the approval of the customer;

c) with the customer's approval, disconnect part of the system and obtain the customer's signature;

d) in the case of a fault in a video transmission system, to confirm the condition and change the system to alternative transmission (if installed) and obtain the customer's signature.

If the fault on the VSS cannot be located or positively confirmed, the VSS technician shall contact service control for instruction.

17.3.6 A report of all action taken shall be made on the corrective maintenance report and the customer's signature obtained. A copy is to be left with the customer.

17.3.7 Any parts of the VSS disconnected or temporarily repaired shall be recorded, obtaining the customer's authority, and should be reported for further action. The company shall ensure that action is taken as soon as possible and, in any case, in accordance with the contract for maintenance.

17.4 Preventive maintenance

17.4.1 It is essential that, where a maintenance service agreement has been entered into, companies have the capability to operate a planned programme of preventive maintenance visits.

It is recommended that a preventive maintenance visit should be made during or before the twelfth calendar month following the month of handover.

Thereafter, preventive maintenance visits (if agreed) shall be made at the frequency agreed in the contract with the customer.

17.4.2 When carrying out a preventive maintenance visit the VSS technician shall first establish with the customer whether there have been any problems with the VSS since the last preceding preventive maintenance visit.

The VSS technician shall examine the system documentation, or that kept by the customer, to see whether there have been any service calls or incidents since the last preceding routine visit. Where possible, the VSS technician shall also enquire whether there has been, or is likely to be, a change of use of the premises, a change of working procedures, or a change of tenure.

The VSS technician shall ensure that the customer (or the customer's representative) is still fully conversant with the operation of the VSS.

17.4.3 The VSS shall then be visually inspected, checking the following items:

a) The number and type of cameras, including lenses, are in accordance with that stated in the specification and any amendment. Draw the customer's attention to any deviations found.

b) Indicator lamps are working correctly. Replace faulty indicator lamps as required.

c) Warning labels are still in place. Replace missing labels as required.

d) All cables and conduits (including those that are flexible) are properly supported, undamaged and showing no signs of wear.

e) Ensure sound physical fixings of all equipment including examinations for loosening or corrosion of supports and fixings, including towers and brackets. Lubricate tower mechanisms, where applicable, in accordance with manufacturers' instructions and repair or replace brackets as necessary.

f) All glands and seals on external equipment. Repair or replace glands and seals as necessary to maintain the agreed specification.

17.4.4 The VSS shall then be functionally inspected, checking the following items:

a) The picture quality of each camera and correct display selection. Look for signs of condensation on windows of camera housings and limiting of picture highlights.

b) Where necessary, remove covers and housings and clean interiors.

c) All automatic and remote control camera functions comply with specification (e.g. pan, tilt, zoom, electronic iris, focus, wipers, washers, heaters) and that camera movement and fields of view are free from obstruction.

d) Operation of all displaying, switching, multiplexing and recording equipment (including time and date generators) is satisfactory.

All equipment, in particular video recording equipment, should be maintained and serviced in accordance with manufacturers' recommendations and instructions.

e) Function of all interfaces with alarms is satisfactory including correct triggering of alarms.

f) Operation of supplementary lighting is satisfactory.

Lamps should be replaced at frequencies recommended by manufacturers so as to minimise the possibility of failure between preventive maintenance visits. As the life of a particular lamp cannot be known with certainty, avoidance of such failure cannot be guaranteed.

Items requiring attention shall be rectified and/or reported as necessary, recording all such work on the preventive maintenance report.

17.4.5 Check that the performance of the system(s) continues to meet the agreed specification/operational requirement and any periodic test scheme agreed with the customer.

Annex A
(informative)

Current video standard formats

The following is a list of acceptable standard formats for export from VSSs according to IEC 62676-2. These are presented in no particular order. This is not an exhaustive list of acceptable formats, other formats are acceptable. The formats below are presented as examples of what level the compliance of a format should be defined i.e. stating "MPEG-4" alone is insufficient.

Video codecs:

- H.264, AVC (ISO/IEC 14496-10, *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding* ITU-T Rec. H.264);
- MPEG-4 part 2, ISO/IEC 14496-2, *Information technology – Coding of audio-visual objects – Part 2: Visual*;
- MPEG-2, ISO/IEC 13818-1, *Information technology – Generic coding of moving pictures and associated audio information: Systems*;
- ITU-T Rec. H.263, *Video coding for low bit rate communication*.

Still image formats:

- JPEG 2000, ISO/IEC 15444-1, *Information technology – JPEG 2000 image coding system: core coding system*;
- JPEG, ISO/IEC IS 10918-1 ITU-T Re. T.81.

Annex B
(normative)

Test protocol for VSS target

B.1 Scope of the test

This test is designed to assess a VSS's ability to create an image that conforms to the 100 % Identify criteria specified in this standard, and or the ability of the system to produce an accurate reproduction of a vehicle registration number (VRN), (and the subsequent ability of a VSS operator to interpret this image).

B.2 Test prerequisites

The following items are required to perform the test:

- Heads test targets – full sized (see Figure B.1)
- Heads control sheet
- Height measuring stick
- Number plates (see Figure B.2)
  Number plates are required if the VRN test is required.
- Test log sheet (see Table B)
- Answer sheet (see Table B)
- 2 people (auditor and VSS operator)
- 2-way communication between auditor and operator.

B.3 Preconditions

All observations are to be under normal viewing conditions (i.e. observer location, camera views presented, system display location and camera view layout all as in normal system operation).

The auditor and operator should not pre-agree the sequence of head/VRN targets to use, nor should the auditor present the targets in a sequential manner.

The OR for the VSS defines locations (covered by the cameras under test) where person identification or VRN recognition is either mandatory or desirable.

B.4 Face selection

The test pack comes with 9 face targets. These are designed to allow a range of different human characteristics to form the basis of any technical assessment of system fidelity.

The faces are grouped in 3 categories classed as; East Indian, European and African (labelled A to C), and 3 permutations within each broad classification (labelled 1 to 3).

The auditor should select any two faces from the pack to display to the camera. The selected faces should be changed every time a test is undertaken to prevent any undesirable testing patterns from developing.

B.5 Live view methodology (faces)

The operator should observe the feed of the camera being tested under normal viewing conditions in the control room.

a) The auditor should be positioned in the area defined in the OR as requiring Identification level coverage. The height measuring stick should be fully extended to 1,7 m and used to aid the location of the targets in the correct part of the field of view.

b) The auditor should present 2 randomly selected face images directly towards the camera under test. The faces should remain in the folder, which can be placed on top of the height measuring stick to aid positioning and for ease of display.

c) The auditor should record the reference numbers of the faces presented on the log sheet.

d) The operator should observe the live camera view and record the reference numbers of the perceived faces on the answer sheet, the faces should be displayed for a maximum of 30 s per pair.

e) The operator should print out a still of the camera view or save a screen grab (for record keeping).

   The saved or printed image should not be used to validate the on screen results. It should be retained as a record of test. If the saved or printed image requires quality testing the same approach as above should be used, but the printed or saved image used in place of the on screen display.

f) Repeat test in all locations where identification is stipulated by the VSS OR. (This could be multiple locations within one camera view through to multiple camera views of a single location.)

   Where it is impractical to test all cameras due to the size of the system, 5 individual views or 20 % of the views, whichever is the greatest, should be tested.

B.6 Live view methodology (VRN)

a) The operator should observe the feed of the camera being tested under normal viewing conditions in the control room.

b) The auditor should be positioned in the area defined in the OR as requiring VRN identification. NB for VRN plates this may be low in the frame.

c) The auditor should present 2 randomly selected VRN plates directly towards the camera under test. The plates can be attached to the folder by the Velcro strips on the inside to enable them to be presented easily.

d) The auditor should record the VRN plates presented on the log sheet.

e) The operator should observe the live camera view and record the characters of the perceived VRN plates on the answer sheet, the plates should be displayed for a maximum of 30 s per pair.

f) The operator should print out a still of the camera view or save a screen grab (for record keeping).

g) Repeat test in all locations where VRN identification is stipulated by the VSS OR. (This could be multiple locations within one camera view through to multiple camera views of a single location.)

B.7 Recorded view methodology (faces)

a) The operator should conduct the test under normal viewing conditions in the control room.

b) The operator should ensure the VSS is in its normal recording configuration to record the actions of the auditor.

c) The auditor should be positioned in the area defined in the OR as requiring Identification level coverage.

d) The auditor should present 2 randomly selected face images directly towards the camera under test.

e) The auditor should record the references of the faces presented on the log sheet.

f) The operator should locate the archive footage of the test on system.

g) The operator should observe the recorded view and record the reference numbers of the perceived faces on the answer sheet.

h) The operator should print out a still or save screen grab (for record keeping).

i) Repeat test where identification is stipulated by the VSS OR. (This could be multiple locations within one camera view through to multiple camera views of a single location.)

B.8 Recorded view methodology (VRN)

Repeat steps a) to i) above using the number plate targets. The targets should be presented at a suitable height to simulate a vehicle.

B.9 Motion

If motion testing is considered necessary then appropriate motion of the target can be applied as required. If vehicle motion is the requirement then it is suggested that the targets are affixed to a vehicle and if pedestrian motion is required then the target can be carried through the scene by the tester at the required speed.

B.10 Faces: scoring criteria

The targets have been designed to produce a two tiered result. The first level is the ability to correctly identify the broad demographic category; the second is the ability to correctly identify the correct face within that category. Higher quality systems should enable the operator to distinguish fine detail (i.e. the correct face). Poorer quality systems may only be sufficient to enable the operator to identify the broad category.

Each face should be marked accordingly:

– category correct (A, B, C): Y/N;

– face correct (1, 2, 3): Y/N.

If category and face is correct score is: 3.

If only category is correct score is: 1.

If neither are correct score is: 0.

This should be completed for both faces.

A final score of 6 is the most desirable outcome – Pass.

A final score of 4 is an acceptable outcome – Pass.

A final score of 3 should be considered borderline and re-tested.

A final score of 2 should be considered borderline and re-tested.

A final score of below 2 is the least desirable outcome – Fail.

B.11 VRN: scoring criteria

The VRN test has been designed to be a pass or fail test. If the observer is able to correctly identify all the characters displayed during the test then it is deemed that the system is suitable for human recognition of number plates. Otherwise the system cannot be considered to give an accurate result.

Table B.1 – Example auditor log sheet

Location: Store A, anytown		**Date:** 15/6/09	
Camera ID	**Live/ Archive**	**FACE 1**	**FACE 2**
Over till (4)	Live	A2	B1
Over till (4)	Archive	B1	C2
Main door (5)	Live	B2	C3
Main door (5)	Archive	A1	C1
Main door (6)	Live	C2	C3
Main door (6)	Archive	A3	B3
Etc.	Etc.	Etc.	Etc.

Table B.2 – Example control room observer log sheet

Location: Store A, anytown		**Date:** 15/6/09	
Camera ID	**Live/ Archive**	**FACE 1**	**FACE 2**
Over till (4)	Live	A2	B2
Over till (4)	Archive	B?	C?
Main door (5)	Live	B2	C3
Main door (5)	Archive	A1	C1
Main door (6)	Live	??	??
Main door (6)	Archive	A?	C?
Etc.	Etc.	Etc.	Etc.
NOTE One question mark indicates that the operator cannot identify the person A1 or A2 or A3, but only the group of people. Two question marks indicates that the operator cannot specify the group of people A, B or C nor can the operator identify the person of the test target B.12.			

Table B.3 – Example camera audit sheet

Location: Store A, Anytown						**Date:** 15/6/09			
		True		**Observed**		**Scores**			
		Face 1	**Face 2**	**Face 1**	**Face 2**	**Face 1**	**Face 2**	**Total**	**Pass / Fail**
Camera ID	**Live**	A2	B1	A2	B2	3	1	4	P
Over Till (4)	**Recorded**	B1	C2	B?	C?	1	1	2	R
Camera ID	**Live**	B2	C3	B2	C3	3	3	6	P
Main Door (5)	**Recorded**	A1	C1	A1	C1	3	3	6	P
Camera ID	**Live**	C2	C3	??	??	0	0	0	F
	Recorded								
NOTE One question mark indicates that the operator cannot identify the person A1 or A2 or A3, but only the group of people. Two question marks indicates that the operator cannot specify the group of people A, B or C nor can the operator identify the person of the test target B.12.									

Table B.4 – Blank auditor log sheet

Location:			Date:
Camera ID	Live/ Archive	FACE 1	FACE 2

Table B.5 – Blank control room observer log sheet

Location:			Date:
Camera ID	Live/ Archive	FACE 1	FACE 2

Table B.6 – Blank camera audit sheet

Location:		Date:						
		True		Observed		Scores		
		Face 1	Face 2	Face 1	Face 2	Face 1	Face 2	Total
Camera ID	Live							
	Recorded							
Camera ID	Live							
	Recorded							
Camera ID	Live							
	Recorded							
Camera ID	Live							
	Recorded							

Where VRN reproduction testing is required audit sheets similar to those provided in Tables B.1 to B.6 should be used.

B.12 Heads control sheet (for example only)

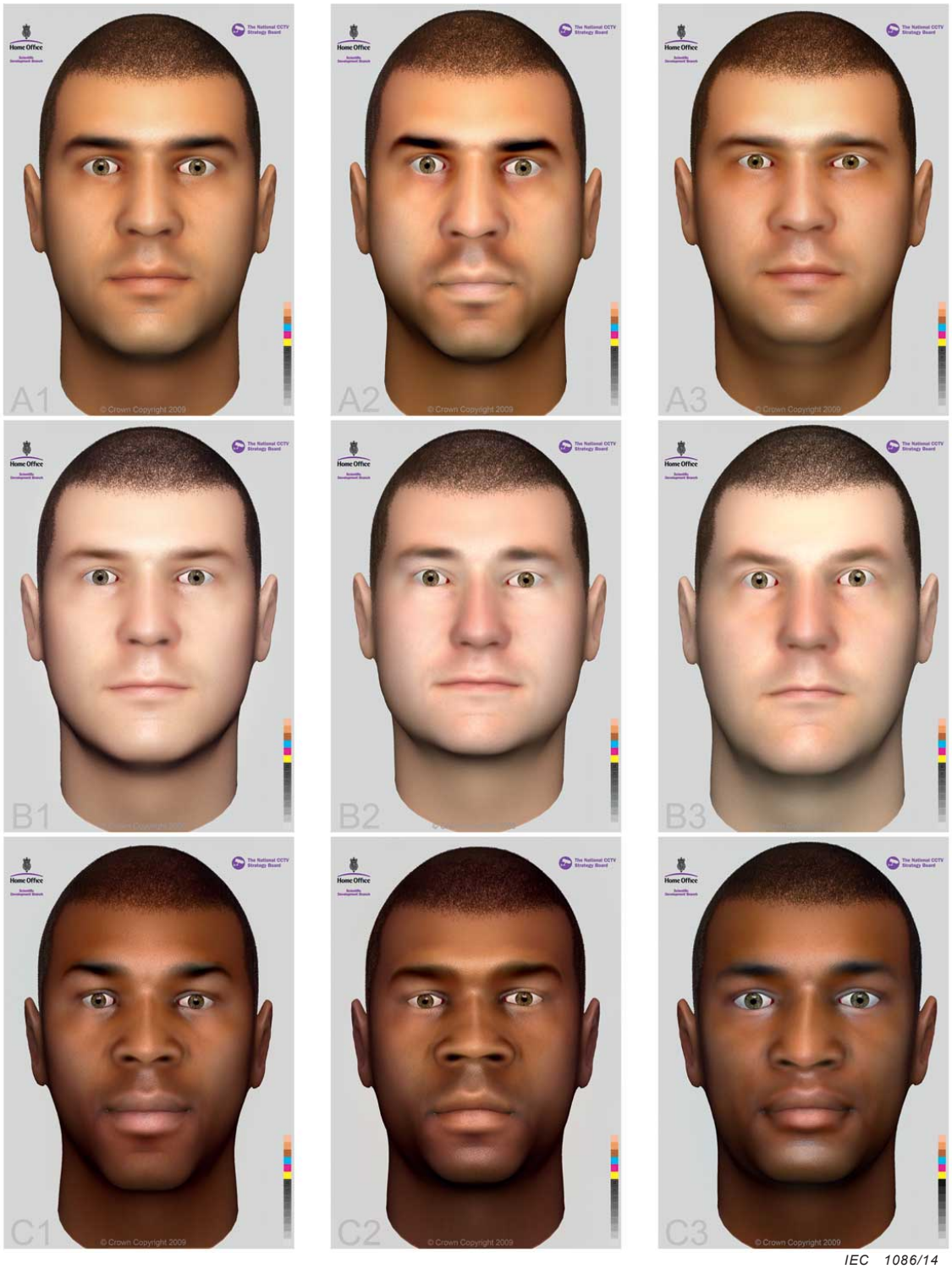


Figure B.1 – Heads control sheet

The test image in Figure B.1 can be downloaded from <https://www.gov.uk/cast-resources-for-the-crime-prevention-industry>.

B.13 VRN control sheet (for example only)

The purpose of the text legibility test is to evaluate whether a VSS is capable of providing images that are suitable for establishing textual details (specifically focused on vehicle registration marks). Test targets shall be used which provide letters with a similar shape like the following in Figure B.2:

Figure B.2 – VRN control sheet example

The test consists of 9 segments of vehicle registration number (VRN) characters. A random selection is presented towards the camera at an appropriate person, percentage, screen height, distance from camera.

An operator attempts to match the presented VRN to a reference list, thus determining the capability of the VSS.

Annex C
(normative)

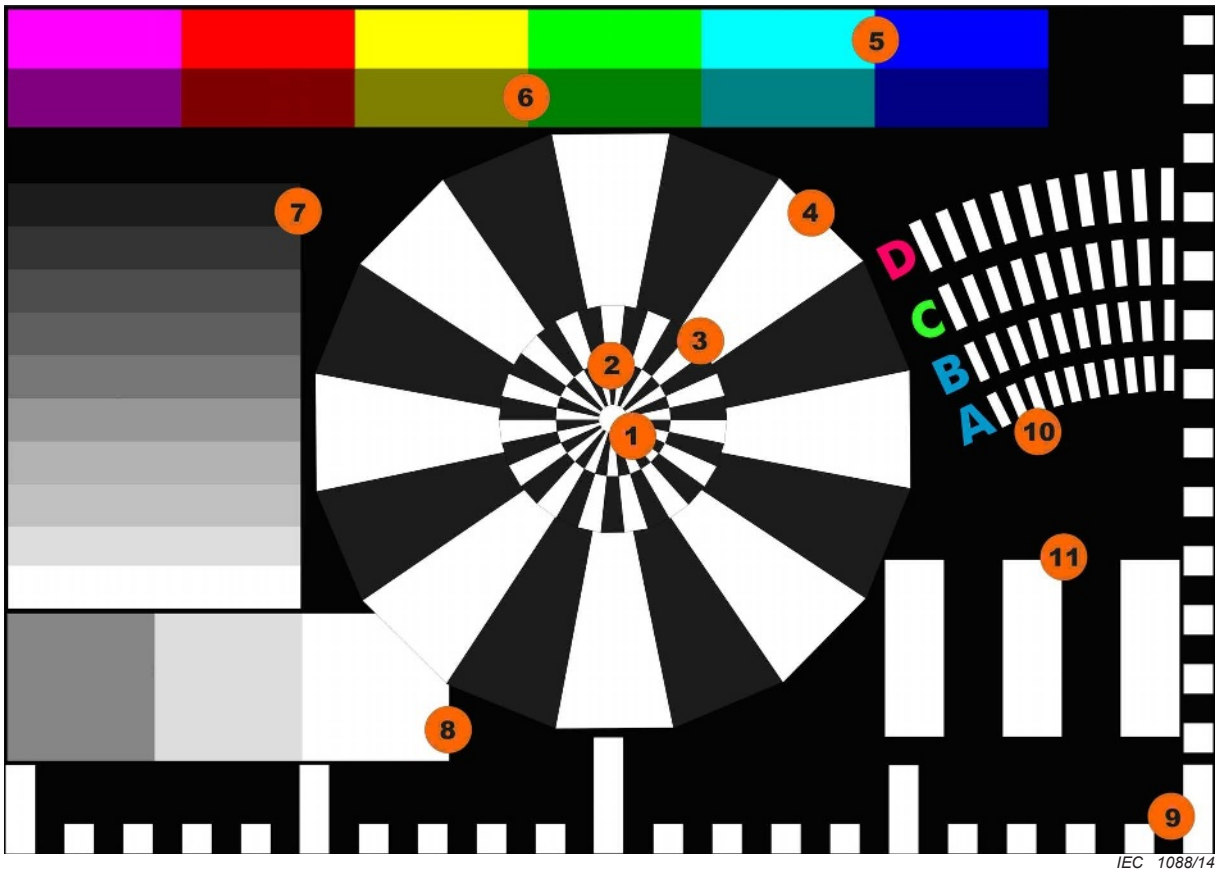
Test method of image quality – Guidance for the use of the video test target

The test method uses a standardised test target. It is used to evaluate the performance of a closed circuit television security system.

The test target (A3 format) is illustrated in Figure C.1.

The test target is easy to use for testing of coverage, determining acceptable image height, resolution, colour and contrast of the image. The test target is placed at strategic positions within the area of coverage as defined by the operational requirements or system specification, and detectability at each location is confirmed. This test should be carried out over the total light range over which the system is intended to operate.

As a basic principle horizontal and vertical angle between camera and test panel shall be smaller than 22,5° in order to avoid optical distortion, as exemplified in Figure C.2.



NOTE The key to the numbers in the figure is provided in the following pages.

The test image can be downloaded from <http://vds.de/fileadmin/vds_publikation/> or <https://www.gov.uk/cast-resources-for-the-crime-prevention-industry>.

Figure C.1 – A3 test target *(1 of 3)*

a)

If a differentiation of the 1 mm wide black and white segment peaks is possible, the quality level "**inspect**" is reached.

b)

If a differentiation of the 4 mm wide black and white segment peaks is possible, the quality level "**identify**" is reached.

c)

If a differentiation of the 8 mm wide black and white segments is possible at the middle circle, the quality level "**recognise**" is reached.

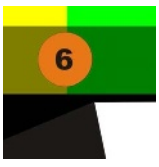
d)

If a differentiation of the 40 mm wide black and white segments at the outer circle is possible, the quality level "**detect**" is reached.

e)

6 colours can be differentiated: normal colour aptitude

NOTE Pink: Pantone 237 (Cyan 5 %, Magenta 50 %); Red: Pantone 485 (Magenta 95 %, Yellow 100 %); Yellow: (yellow 100 %); Green: pantone 360 (Cyan 60 %, Yellow 80 %); Blue turquoise: pantone 311 (Cyan 65 %, Yellow 15 %); Blue: pantone 285 (Cyan 90 %, Magenta 45 %)

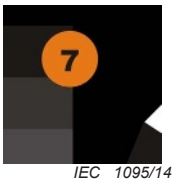


f)

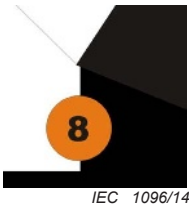
6 colours can be differentiated: raised colour aptitude

NOTE Apply a 50 % black filter on each colour from the first line

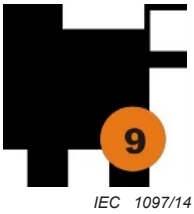
Figure C.1 – A3 test target *(2 of 3)*



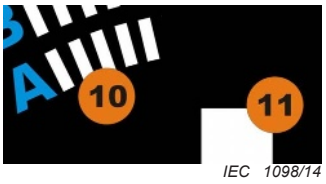
g) 11 grey scale values, deep black (background of test panel) and pure white



h) 3 grey scale values, deep black (background of test panel) and pure white



i) Centimetre ruler for determination of the field of view



j) NOTE For German accident prevention regulation

Notice for projection

1) Quality levels of images:
   - detection: 40 mm at real object relate to 1 pixel at least;
   - recognition: 8 mm at real object relate to 1 pixel at least;
   - identification: 4 mm at real object relate to 1 pixel at least;
   - inspect: 1 mm at real object relate to 1 pixel at least;

   Pixel-oriented definition of the image quality: guarantee of a minimal quality of the image with no influence of the camera resolution, image-data-processing procedures etc. ("one pixel remains one pixel")

   Attention when compressing data, live-image and recorded image are to be compared!
2) in general especially the performance feature "identification" can be guaranteed only for a part of the camera surveillance range – see Figure C.2;
3) dead ranges depending of the mounting height are to be considered – see Figure C.2;
4) for cameras that can zoom and can be moved at least two reference images should be determined and documented.

Figure C.1 – A3 test target *(3 of 3)*

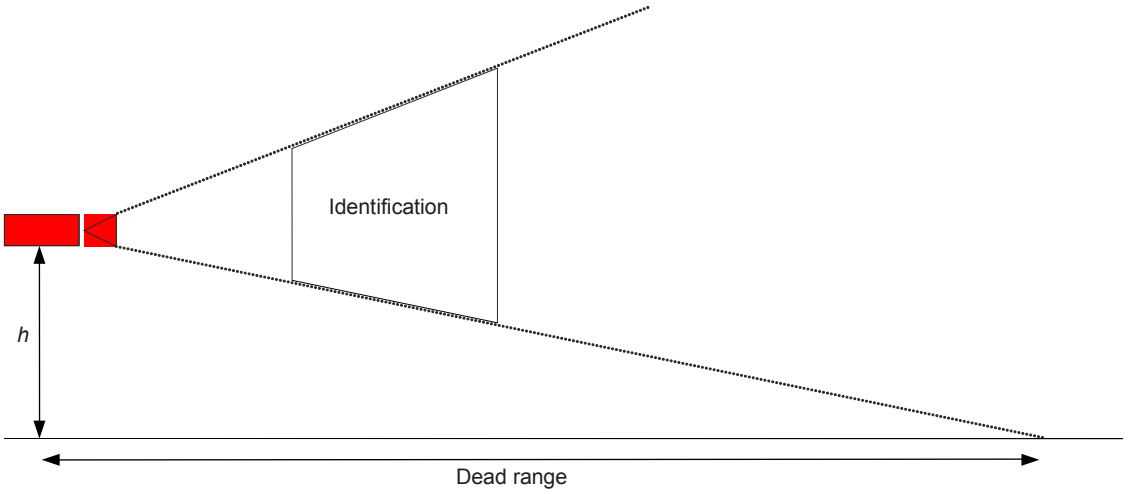


Figure C.2 – Avoiding optical distortion

Annex D
(informative)

Guide to specifying VSS parameters

One of the main failings of VSSs is that the owners and or installers do not have a clear idea of the purpose of each camera and the level of detail needed to achieve that purpose. Cameras that are attempting to perform too many functions or have no clear purpose are a waste of resource as they are unlikely to produce useable images. For these reasons it is highly desirable to have a clear OR not only for the site in general but also for each individual camera. This need not be as daunting a task as it may sound if the procedure outlined below is followed.

It is suggested that a modular approach is taken to specifying VSS, as common area types and risks exist across a broad range of environments. Table D.1 below contains examples of these building blocks with minimum image quality and frame rates dependant on the perceived risk level. The image quality (image size and compression level) consistent with each of the categories should be defined and tested using a suitable image quality test. The frame rates given are suggested minimum values. For those areas marked with an asterisk (*) it is acceptable that the default frame rate could be reduced if an alarm trigger mechanism is deployed that would cause the frame rate to increase on activation. Any system that relies on frame rate increasing after alarm trigger should buffer the video so that several seconds before the alarm trigger is captured at the higher frame rate.

Table D.1 – Suggested VSS building blocks *(1 of 2)*

Location	Activity	Image quality by risk level		
		High	Medium	Low
Aisles	Theft, health & Safety	Observe – 6 fps	Observe – 6 fps	Observe – 2 fps
ATM	Theft, assault, fraud	Identify – 12,5 fps	Identify – 6 fps	Identify – 6 fps
Bar area	ASB, theft, assault	Observe – 12,5 fps	Observe – 6 fps	Observe – 6 fps
Bin areas	Theft, candalism	Recognise – 6 fps	Observe – 6 fps	Observe – 6 fps
Car park – vehicle access	VRN	VRN – 12,5 fps	VRN – 12,5 fps	VRN – 12,5 fps
Car park – Parking	Theft, assault	Observe + PTZ – 6 fps	Detect + PTZ – 6 fps	Observe – 6 fps
Car Park – Pedestrian access	Any	Recognise – 6 fps	Observe – 6 fps	Observe – 2 fps
Cash counting	Theft, fraud	Identify – 12,5 fps	Identify – 6 fps	Identify – 6 fps

Table D.1 – Suggested VSS building blocks *(2 of 2)*

Location	Activity	Image quality by risk level		
		High	Medium	Low
Concourse/Street	Any	Observe + PTZ – 12,5 fps	Observe + PTZ – 6 fps	Observe 2 fps
Connections (escalators, lifts, stairs)	Any	Observe – 6 fps	Observe – 6 fps	* Observe – 6 fps
Cycle racks	Theft, vandalism	Recognise – 6 fps	Observe – 6 fps	Observe – 6 fps
Dance floor	ASB, theft, assault	Observe – 6 fps	Observe – 6 fps	Observe – 6 fps
Door – Customer	Any	Identify – 12,5 fps	Identify – 6 fps	Identify – 6 fps
Door – Secure	Any	Identify – 12,5 fps	Identify – 6 fps	* Identify – 6 fps
Frontage	Any	Observe + PTZ – 12,5 fps	Observe – 6 fps	Observe – 2 fps
Help point	Activity	Recognise – 12,5 fps	Observe – 6 fps	Observe – 6 fps
High value items	Theft	Recognise – 12,5 fps	Recognise – 6 fps	Observe – 6 fps
Lift interior	ASB	Recognise – 6 fps	Recognise – 6 fps	* Observe – 6 fps
Loading bay	Theft, vandalism, health and safety	Recognise – 6 fps	Observe – 6 fps	Observe – 2 fps
Perimeter	Activity	Detect – 2 fps	Detect – 2 fps	* Detect – 6 fps
Phone booth	Any	Observe – 6 fps	Observe – 6 fps	Observe – 2 fps
Sterile zone	Activity	Detect – 2 fps	Detect – 2 fps	* Detect – 6 fps
Stock room	Theft	Recognise – 12,5 fps	Observe – 6 fps	* Observe – 6 fps
Taxi rank / Drop-off area	Any	Observe + PTZ – 6 fps	Observe + PTZ – 6 fps	Observe – 6 fps
Tills	Robbery, assault, theft, fraud	Recognise – 12,5 fps	Recognise – 6 fps	Observe – 6 fps
Toilet access	Any	Recognise – 6 fps	Observe – 6 fps	Observe – 2 fps

Annex E
(normative)

Detection response testing and acceptability criteria

E.1 General

The detection test poses the question: can the observer easily pick out a suitably clothed target over the range of conditions defined in the OR? Tests are carried out by placing a suitably clothed average person height target, without the operator's knowledge, at locations in the areas under test, as defined in the OR. The operator is then alerted and the time he takes to find the target is measured. For fixed cameras, this could mean the time taken from the initiation of an alarm signal to the point where the operator has correctly acknowledged the presence and location of the target.

Testing PTZ cameras is more complex. The time could be taken from the initiation of an alarm signal to the point where the relevant camera has moved to an automatic pre-set position and/or the operator has driven the correct camera, including zoom and focus, and has correctly acknowledged the presence and location of the target.

The results of each detection test are assessed according to the following scale:

– level 3 – target easily seen; it would be immediately obvious and no mistake is possible;
– level 2 – fairly easily seen; the target needs to be searched for but would not be missed;
– level 1 – difficult to see; the target is only found after a careful and lengthy search that exceeds the allowed response time;
– level 0 – target not seen at all.

Timing the response of observers from the moment of an intruder alarm to their rejection or acceptance of the alarm is a significant measure of system performance. The acceptable response time depends on the delay expected to be provided by the barrier associated with the alarm system and should be included in the system specification. This timing is the recommended method of setting a threshold for distinguishing between response levels 1 and 2. The results will be, to some extent, operator dependent.

Although, ideally, all target detection scores will be level 3, level 2 is acceptable for effective VSS operation. Where test results are not to specification the contractor should rectify the problem. In some cases, system managers might be able to relax the OR based on suitable alternative security measures or a review of the risk.

E.2 False and nuisance alarms

Tests should be carried out without any targets and using false targets to see how long the operator takes to declare a false or nuisance alarm with confidence. Nuisance targets might include items such as a plastic dustbin, dustbin bag, football, etc. The following scoring scale is suggested:

– level 2 – when "no target" condition is declared correctly within the OR response time;
– level 1 – when "no target" condition is declared correctly outside the response time;
– level 0 – target declared when no target is present.

E.3 Setting the response time

The acceptable response time should be specified by the client. It should be practical and may be strongly influenced by a range of factors including:

- the delay provided by the barrier, i.e., the time taken to breach it;
- the area/volume viewed by the camera;
- the number of false targets (e.g. people who are entitled to be present in the area) which need to be recognised and accepted as present;
- the number of screens to be searched;
- the need to manually select cameras;
- the number of different pictures to be examined, following the alarm, to ensure that the whole alarmed area has been checked;
- the need to manipulate any of the cameras with a remote control unit in order to search an area.

Through careful design of the lighting system and camera siting, together with good control room design, large fixed camera systems with accurate and reliable operator cueing can reliably achieve response times as low as one or two seconds. With PTZ cameras the response time may be 30 s or more, depending on pan, zoom and focus speed and the area to be searched. For systems with barriers providing a very long delay for an intruder, a longer search time might be allowed. For one with a comparatively short delay in the barrier any time lost during the search might allow an intruder to pass unobserved through the detection and search zone. Where the required detection times cannot be reliably obtained with 10 % screen height targets then a larger target percentage may need to be specified.

E.4 PTZ response time test procedure

From the OR checklist and knowledge of the site, a location should be chosen where the system response time is to be measured. If, operationally, the camera covering that area may be parked anywhere, the test should be started with the camera set to one end of its pan range. If a camera has a pre-set or datum condition, the time to locate a target from this position should be the system response time. A suitably clothed target should be placed without the operator's knowledge at the agreed position. An alarm signal should then be initiated and the time should be noted for the operator to drive the camera and lens to a position where the presence and location of the target is correctly determined. This test should be initiated with the lens set at minimum focal length and the camera in its normal rest condition.

If tilting the cameras is necessary to search the whole area, this may dramatically increase the response time. It should not be assumed that targets will be visible to the operator if the pan speed is too fast, the lighting poor or the scene busy. A slower pan or modified search pattern may be required to improve the probability of detecting a target.

E.5 Observer cueing and prompting

It will be necessary to decide the method of observer prompting to be used during the tests. This may require technical solutions such as adding a trip mechanism to the alarm monitoring and control system. This will allow an alarm sector to be triggered or held off while the target is set up.

In some systems, when the alarm is triggered, the observer is prompted to look at each of a number of camera pictures providing coverage of the alarmed zone. The specification may call, for instance, for both sides of a barrier to be viewed and searched. The response time should include selection and search of all of these pictures.

E.6 Detection test locations

The security manager with his advisers should define the exact test points using his knowledge of likely attack points and likely weaknesses. It shall be remembered that these

tests and results may represent a key to unlock a security system. They shall, therefore, be treated as sensitive information. For a commissioning test programme, the contractor should be notified in advance of the conducting of the tests but the right should be reserved by the client to carry out further tests if necessary. The more notice given to the contractor the more likely it is that the client's expectations will be understood and taken into account in the design. The contractor should understand that tests will be carried out under worst case conditions for size and contrast, where the lighting is poor, the scene is cluttered or busy or where the background provides little contrast for targets. This gives the opportunity to either re-design in order to produce a larger target or to advise on changes to the lighting in order to raise the contrast of the target.

E.7 Target camouflage

The target should be dressed in suitable clothing to take account of local conditions and what intruders might be expected to wear. Target clothing for commissioning detection tests should be specified by the customer in the tender documents. It may be necessary to try a variety of camouflage materials in order to test fully the system performance. The standard material for the test should be disruptive pattern material (DPM), camouflage. Other colours which should be considered are black green and tan. Test results should be noted for each type of clothing used.

E.8 Tests with moving targets

An effective security system shall be capable of performing well with both moving and stationary targets. Some cameras will perform less well, others may allow a moving target to be more easily seen but perhaps only under certain conditions. Detection tests should, therefore, be carried out with the target moving as well as with it stationary. The results for both sets of tests, using the grading scheme given in 3.5.1, should be noted with the worst determining the limit of performance, unless otherwise stated in the specification. For instance, in an area where it would be unlikely for an intruder to remain stationary for any length of time a pass mark may be acceptable only with the target moving.

E.9 Test conditions

Before carrying out commissioning tests, the whole system should be set up correctly. To provide a performance benchmark, tests should be carried out under conditions that most closely reflect normal everyday use. As far as possible, the operator or observer should occupy his usual position carrying out normal duties. All components of the system should be in their "normal" mode. For instance, cameras which are adjustable should be in their rest position with zoom, focus and iris in whatever is the normal pre-set condition; monitors should be adjusted to their normal settings. Any "adjustment" to the system performance, even a simple task such as cleaning the monitor screens, which is not part of normal or prescribed procedure, may significantly affect the result of the test. Any factors which might, during normal operation, have an impact on the system performance should be noted. For example, the guard might have to leave the picture display monitors unattended in order to fulfil other duties; the monitor controls might be adjusted to suit particular conditions, for example, the effect of stray lights from buildings, traffic or sunlight entering the control room. The fact that the observers are alerted to the test will undoubtedly affect the results. Other important parameters will be the weather and the time of year of the test. If the weather is good, allowance will have to be made for loss of performance under poor conditions. The time of year will affect the angle and direction of sunlight. This might make observations difficult during critical periods of high activity such as the rush hour.

E.10 Testing a "live" system

For various reasons it may be impractical to meet all of the test conditions. For example, in a live system it is assumed that the perimeter intrusion detection system cannot be disabled

without the knowledge of the guards. Placing the target in a detection zone without tripping the alarm would then be impossible. In these circumstances, the observer's view of the monitor could be temporarily obstructed while the target is deployed.

E.11 Detection test results tables

Having decided the type and extent of the tests to be carried out, test procedure and results table can be drawn up based on the test specification table. The table and supporting test recording system shall allow for all of the results that will be needed for the performance analysis, such as the example in Table E.1. General statements such as test conditions might be made at the head of the test sheet or included in the columns. Any special test conditions to be taken into consideration during the test will have been specified in boxes 9 and 10 of the OR checklist.

Table E.1 – Detection test results

Task area reference code	Target height	Observer Response Time (ORT)	Observer response score	Is whole area covered?	Notes and comments
And test number noted on site plan	In % screen height or 'not displayed'	In seconds and how observer is cued	Level: 3 to 0 and Comments: Very clear, clear, indistinct, not discernible	Yes/No Show details on plan	Night/day and lighting, weather, clothing, moving or stationary

If there is a requirement for coverage of the same area for more than one purpose then there shall be a separate test row for each.

Where the VSS is used to verify an alarm state from a PIDS, each zone will need to be identified to ensure that all are tested.

Bibliography

IEC 62305 (all parts), *Protection against lightning*

IEC 62305-3, *Protection against lightning – Part 3: Physical damage to structures and life hazard*

IEC 62305-4, *Protection against lightning – Part 4: Electrical and electronic systems within structures*

ISO/IEC 11801, *Information technology – Generic cabling for customer premises*

ISO/IEC 23000 (all parts), *Information technology – Multimedia application format (MPEG-A)*

ISO 22311:2012, *Societal Security – Video-surveillance – Export interoperability*

ISO 31000:2009, *Risk management – Principles and guidelines*

EN 50174 (all parts), *Information technology – Cabling installation*

EN 50310, *Application of equipotential bonding and earthing in buildings with information technology equipment*

CLC/TS 50398, *Alarm systems – Combined and integrated alarm systems – General requirements*

Home Office Publication no 28/09, *CCTV operational requirements manual*

CNPP France, *R82 guideline for videosurveillance system installation rules*, available from <www.cnpp.com>

Image Test Target, VdS, available from <www.vds.de>

National Annex NA
(informative)
Security grading application for Video Surveillance Systems (VSSs)

NA.1 General

The following guidance is provided to assist system designers in the application of grading as specified in this standard. It provides some examples of how grading can be specified as well as documented.

Table NA.3 provides a simple overview of each functional grade requirement in BS EN 62676-1-1:2014.

NA.2 Selecting a security grade

NA.2.1 General guidance

The principle of grading in BS EN 62676-1-1 is to provide a shorthand way to simplify the specification of system requirements, i.e. make it easy to specify functions by identifying the grade dependent requirements as listed in the standard.

NA.2.2 Selecting an overall security grade with no grade variations

For practical purposes, system designers should select the simplest approach that will meet the needs of the customer. The recommended approach is to select a security grade and apply that single grade throughout the system.

NA.2.3 Selecting an overall security grade with some variations

If a single overall security grade is inappropriate, the grading may be varied between functions, with an overall grade selected that best reflects the performance of the system as a whole.

For example, using the functions listed in Subclause 4.2.2 of this standard, if the threat being considered is shoplifting, a varied grading may be assigned across the system. If a grade 4 was applied to system logs, it would be unlikely that the grade relating to data (manipulation) protection would also be grade 4. If, however, the threat is organized crime at a casino, then both functions may be assigned a grade 4.

NA.2.4 Variations of requirements within a specific function

There is an expectation that the grade of each function should be applied consistently within each function. However, most of the 18 functions in Subclause 4.2.2 of this standard contain more than one element (requirement) to the function, i.e. sub-functions, and it may be impractical to apply this methodology at all times.

There may be occasions where some of the requirements within a specific function are not necessary but have an impact on the system design. Where this is the case, it may be more appropriate to specify this independently of grading, either in the Operational Requirement document (OR) or system design proposal (SDP).

For example, a system could be defined as having storage meeting grade 4 requirements. One of the grade 4 requirements is the ability to replay an image from storage within 1 s after the incident or the actual recording of it. However, if the use of the system is not going to include continuous monitoring then this need is unlikely to occur and achieving it could prove onerous. In these circumstances, requirement for storage could be defined as grade 4 but a concession given against this criteria.

NA.3 Recording of the grade in VSS documentation

NA.3.1 General

This section provides, by way of examples, some possibilities of how the grading may be recorded in the system documentation.

As grading is fundamental to the integrity and resilience of the VSS, it is important that each functional requirement from the standard is identified in the OR and/or the SDP.

Depending on the site risk, this may be an overall grade with no variations or may include variations for specific functions, as permitted in the standard.

NA.3.2 Example documentation

Within the OR/SDP there needs to be clarity on how grading is applied and it is recommended that the information shown in the following examples be provided. Examples 1 and 3 demonstrate the use of a table format and Example 2 demonstrates the use of a list. Either of these methods or an alternative is acceptable but it is recommended that (especially if there are any variants) all of the functions are shown to avoid any confusion.

As the grading of tamper detection and protection can be applied independently due to site specific risks, these may need to be listed in the documentation (OR or SDP) on a location by location basis. Alternatively, if a common minimum grade of tamper can be applied then it would be useful to include this in the functional grade lists (this is not shown in the following examples).

NA.3.3 Example 1 – A VSS assigned an overall functional grade of 2 with no variations

For the purposes of the VSS protection level and restriction of access, the security grades of the functions described in Clause 5 of BS EN 62676-1-1 are as listed in Table NA.1.

Table NA.1

	Function	Grade		Function	Grade
a)	common interconnections	2	j)	essential function device failure notification time	2
b)	storage	2	k)	monitoring of interconnections	2
c)	archiving and backup	2	l)	authorization code requirements	2
d)	alarm related information	2	m)	time synchronization	2
e)	system logs	2	n)	data authentication	2
f)	backup and restore of system data	2	o)	export/copy authentication	2
g)	repetitive failure notification	2	p)	data labelling	2
h)	image handling device PSU monitoring	2	q)	data (manipulation) protection	2
i)	image buffer holding time	2			

According to the requirements of BS EN 62676-1-1, the system is considered to have an overall security grade of 2.

The grade for the tamper detection (and protection) function is not listed as the grading varies across the system according to the risk in the locality of the equipment. The tamper detection and protection provided is documented elsewhere.

NA.3.4 Example 2 – A VSS assigned an overall functional grade of 2 but where some functions have a different grade

For the purposes of the VSS protection level and restriction of access, the security grades of the functions described in Clause 5 of BS EN 62676-1-1 are as listed below:

a)	common interconnections	Grade 2
b)	storage	Grade 3
c)	archiving and backup	Grade 2
d)	alarm related information	Grade 2
e)	system logs	Grade 2
f)	backup and restore of system data	Grade 2
g)	repetitive failure notification	Grade 2
h)	image handling device PSU monitoring	Grade 2
i)	image buffer holding time	Grade 2
j)	essential function device failure notification time	Grade 2
k)	monitoring of interconnections	Grade 2
l)	authorization code requirements	Grade 2
m)	time synchronization	Grade 2
n)	data authentication	Grade 2
o)	export/copy authentication	Grade 2
p)	data labelling	Grade 2
q)	data (manipulation) protection	Grade 4

According to the requirements of BS EN 62676-1-1, the system is considered to have an overall security grade of 2.

The grade for the tamper detection (and protection) function is not listed as the grading varies across the system according to the risk in the locality of the equipment. The tamper detection and protection provided is documented elsewhere.

NOTE For the purposes of clarity, this could be recorded as overall security grade 2 (with variances as recorded).

NA.3.5 Example 3 – A VSS assigned an overall functional grade of 3 with a need to highlight functions that cannot be applied consistently

For the purposes of the VSS protection level and restriction of access, the security grades of the functions described in Clause 5 of BS EN 62676-1-1 are as listed in Table NA.2.

Table NA.2

	Description	Grade		Description	Grade
a)	common interconnections	3	j)	essential function device failure notification time	3
b)	storage	2*	k)	monitoring of interconnections	3
c)	archiving and backup	3	l)	authorization code requirements	3
d)	alarm related information	3	m)	time synchronization	3
e)	system logs	3	n)	data authentication	4
f)	backup and restore of system data	3	o)	export/copy authentication	4
g)	repetitive failure notification	3	p)	data labelling	4
h)	image handling device PSU monitoring	3	q)	data (manipulation) protection	3
i)	image buffer holding time	3			
* Attention is drawn to the separately documented information regarding the storage function.					

According to the requirements of BS EN 62676-1-1, the system is considered to have an overall security grade of 3.

The grade for the tamper detection (and protection) function is not listed as the grading varies across the system according to the risk in the locality of the equipment. The tamper detection and protection provided is documented elsewhere.

NOTE For the purposes of clarity, this could be recorded as overall security grade 3 (with variances as recorded).

NA.4 Tamper protection and detection requirements

Clause 5 of BS EN 62676-1-1 specifically states that different grades may be applied to tamper protection and detection requirements in various locations within the system. This is because the risk of parts of the system being tampered with may vary with location so it may be impractical to apply the same grade of tamper protection and detection throughout the system.

An assessment of the risk should be made for each location and then dealt with in one of two ways. Either the requirements can be covered by the use of grading, which is then recorded in the OR or SDP (e.g. by stating that cameras 1 to 5 need grade 3 tamper detection whereas cameras 6 to 12 are grade 2) or specific requirements can be given in the OR or SDP.

NA.5 Summary checklist of functions by grade

Table NA.3

Graded function	Relevant clauses and tables of BS EN 62676-1-1:2014	Clause has additional requirements that are not grade dependent	Grade 1	Grade 2	Grade 3	Grade 4
Common interconnections	Subclause 6.1.2.2	Y			S	S
Storage	Subclause 6.1.3.3 and Table 1	Y		D	D	D
Archiving and backup	Subclause 6.1.3.4 and Table 2	Y			D	D
Alarm related information	Subclause 6.2.2.3	Y			S	S
System logs	Subclause 6.2.2.4 and Table 3	Y		D	D	D
Backup and restore of system data	Subclause 6.3.2.1				S	S
Repetitive failure notification	Subclause 6.3.2.2.1	Y			S	S
Image handling device PSU monitoring	Subclause 6.3.2.2.2	Y				Y
Image buffer holding time	Subclause 6.3.2.2.2	Y			S	S
Essential function device failure notification time	Subclause 6.3.2.2.3				S	S
Monitoring of interconnections	Subclause 6.3.2.2.4 and Table 4				D	D
Tamper detection	Subclause 6.3.2.3.1 and Table 5 Also Subclause 6.3.2.3.2			D	D	D
Authorization code requirements	Subclause 6.3.2.4 and Table 7	Y	D	D	D	D
Time synchronization	Subclause 6.3.2.5				S	S
Data authentication	Subclause 6.3.3.2				S	S
Export/copy authentication	Subclause 6.3.3.2				S	S
Data labelling	Subclause 6.3.3.1 and Table 11	Y	D	S	S	D
Data (manipulation) protection	Subclause 6.3.3.3					Y

Key

Y = Applies

S = Requirements are the same for each grade

D = Requirements are different for each grade

= Not Applicable

This page deliberately left blank

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™