BS EN 62676-1-1:2014

Incorporating corrigendum July 2014

BSI Standards Publication

Video surveillance systems for use in security applications

Part 1-1: System requirements — General

National foreword

This British Standard is the UK implementation of EN 62676-1-1:2014, incorporating corrigendum July 2014. It is identical to IEC 62676-1-1:2013. It supersedes BS EN 50132-1:2010, which is withdrawn.

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 2014

ISBN 978 0 580 87833 6

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 31 May 2014.

Amendments/corrigenda issued since publication

Date	Text affected
30 September 2014	Implementation of CENELEC corrigendum July 2014: Supersession information inserted in EN title page and EN Foreword. Supersession information inserted in National Foreword

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62676-1-1

March 2014

ICS 13.320

Supersedes EN 50132-1:2010
Incorporating corrigendum July 2014

English version

Video surveillance systems for use in security applications - Part 1-1: System requirements - General

(IEC 62676-1-1:2013)

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité -
Part 1-1: Exigences systèmes -
Généralités
(CEI 62676-1-1:2013)

Videoüberwachungsanlagen für Sicherheitsanwendungen -
Teil 1-1: Systemanforderungen
(IEC 62676-1-1:2013)

This European Standard was approved by CENELEC on 2013-12-02. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC
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

Foreword

The text of document 79/432/FDIS, future edition 1 of IEC 62676-1-1, prepared by IEC TC 79 "Alarm and electronic security systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62676-1-1:2014.

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)	2014-09-02
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2016-12-02

This document supersedes EN 50132-1:2010

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 62676-1-1:2013 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 62676-2 Series	NOTE	Harmonised as EN 62676-2 Series.
ISO/IEC 13818-1	NOTE	Harmonised as EN ISO/IEC 13818-1.

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 When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
IEC 60065	-	Audio, video and similar electronic apparatus - Safety requirements	EN 60065	-
IEC 60068-2-75	-	Environmental testing - Part 2-75: Tests - Test Eh: Hammer tests	EN 60068-2-75	-
IEC 60529	-	Degrees of protection provided by enclosures (IP Code)	EN 60529	-
IEC 60950-1	-	Information technology equipment - Safety - Part 1: General requirements	EN 60950-1	-
IEC 61000-6-1	2005	Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments	EN 61000-6-1	2007
IEC 61000-6-2	2005	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments	EN 61000-6-2 + corr. September	2005 2005
IEC 61000-6-3	-	Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments	EN 61000-6-3	-
IEC 61000-6-4	-	Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments	EN 61000-6-4	-
IEC 62262	-	Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)	EN 62262	-
IEC 62599-1	2010	Alarm systems - Part 1: Environmental test methods	-	-
IEC 62599-2	2010	Alarm systems - Part 2: Electromagnetic compatibility - Immunity requirements for components of fire and security alarm systems	-	-
IEC 62676-4		Video surveillance systems for use in security applications - Part 4: Application guidelines	-	-
ISO 12233	2000	Photography - Electronic still-picture cameras - Resolution measurements	-	-

CONTENTS

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 (to be published)

Each part has its own clauses on scope, references, definitions and requirements.

This IEC 62676-1 series consists of 2 subparts, numbered parts 1-1 and 1-2 respectively:

IEC 62676-1-1, *System requirements – General*

IEC 62676-1-2, *System requirements – Performance requirements for video transmission*

The first subpart of this IEC 62676-1 series applies to systems for surveillance of private and public areas. It includes four security grades and four environmental classes.

This IEC Standard is intended to assist Video Surveillance System (VSS) companies, manufacturers, system integrators, installers, consultants, owners, users, insurers and law enforcement in achieving a complete and accurate specification of the surveillance system. This International Standard does not specify the type of technology for a certain observation task.

Due to the wide range of VSS applications e.g. security, safety, public safety, transportation, etc. only the minimum requirements are covered in this standard.

For specific applications e.g. in homeland security, additional requirements need to be applied, which are defined in the annex of this standard.

This IEC Standard is not intended to be used for testing individual VSS components.

Today VSSs reside in security networks using IT infrastructure, equipment and connections within the protected site itself.

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 1-1: System requirements – General

1 Scope

This part of IEC 62676 specifies the minimum requirements and gives recommendations for Video Surveillance Systems (VSS), so far called CCTV, installed for security applications. This Standard specifies the minimum performance requirements and functional requirements to be agreed on between customer, law-enforcement where applicable and supplier in the operational requirement, but does not include requirements for design, planning, installation, testing, operation or maintenance. This standard excludes installation of remotely monitored detector activated VSSs.

This IEC Standard also applies to VSS sharing means of detection, triggering, interconnection, control, communication and power supplies with other applications. The operation of a VSS is not be adversely influenced by other applications.

Requirements are specified for VSS components where the relevant environment is classified. This classification describes the environment in which the VSS component may be expected to operate as designed. When the requirements of the four environmental classes are inadequate, due to the extreme conditions experienced in certain geographic locations, special national conditions may be applied (see Annex A).

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 60065, *Audio, video and similar electronic apparatus – Safety requirements*

IEC 60068-2-75, *Environmental testing – Part 2-75: Tests – Test Eh: Hammer tests*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 60950-1, *Information technology equipment – Safety – Part 1: General requirements*

IEC 61000-6-1:2005, *Electromagnetic compatibility (EMC) – Part 6-1: Generic standards – Immunity for residential, commercial and light-industrial environments*

IEC 61000-6-2:2005, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*

IEC 61000-6-3, *Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments*

IEC 61000-6-4, *Electromagnetic compatibility (EMC) – Part 6-4: Generic standards – Emission standard for industrial environments*

IEC 62262, *Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)*

IEC 62599-1:2010, *Alarm systems – Part 1: Environmental test methods*

IEC 62599-2:2010, *Alarm systems – Part 2: Electromagnetic compatibility – Immunity requirements for components of fire and security alarm systems*

IEC 62676-4, *Video surveillance systems for use in security applications – Part 4: Application guidelines*[1]

ISO 12233:2000, *Photography – Electronic still-picture cameras – Resolution measurements*

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
access level
level of access to particular functions of the VSS, defining the user rights of an operator, to control and configure the system as well as the access to data on the VSS

3.1.2
acknowledge
action of a user to accept a message or an indication

3.1.3
action
deliberate operation or act by the user which is part of alarm procedure

3.1.4
Advanced Streaming Format
proprietary digital audio/digital video container format, especially meant for streaming media

3.1.5
alarm
warning of the presence of any hazard to life, property or the environment

3.1.6
alarm condition
condition of an alarm system, or part thereof, which results from the response of the system to the presence of a hazard

3.1.7
alarm message
message from the system to an operator, to describe time, type and location of an alarm

3.1.8
alarm procedure
indications and manual or automatic controls as response to an alarm condition

[1] To be published.

3.1.9
alarm receiving centre
continuously manned centre to which information concerning the status of one or more alarm systems is reported

3.1.10
alert
warning addressed to persons for their information or to request intervention (e.g. by police, service personnel) in response to an alarm, tamper or fault

EXAMPLE: Visual-alert, acoustic/ audible-alert, external-alert.

Note 1 to entry: Sometimes the term “alarm warning” is used instead.

3.1.11
alternative device
VSS component of the same type as the primary device

3.1.12
archive
data stored on a long term permanent or partially permanent storage

EXAMPLE: CD’s or digital tapes are considered to be ‘archived’.

3.1.13
area of interest
region in the scene monitored by an image capturing device

3.1.14
audio video interleave format
proprietary multimedia format containing audio and video data in a standard container that allows synchronous audio-with-video playback

3.1.15
authentication
method to verify whether an image has been altered

3.1.16
authorisation
permission to gain access to specified functions or components of a VSS

3.1.17
authorisation codes
physical or logical keys which permit access to VSS functions

3.1.18
automatic number plate recognition
optical character recognition on images to read and extract the alphanumerics of the licence plate of vehicles

3.1.19
automatic teller machine
device that provides a method of financial transactions in public space without the need for a human clerk

3.1.20
auxiliary equipment
video system used not as primary mitigation of the risk

3.1.21
backup image
an accurate and complete replica of the primary image, irrespective of media

3.1.22
throughput
(relating to interconnection) data transfer rate or amount of data that can be transferred from one point to another in a given time period

Note 1 to entry: Throughput is quoted in bits per s.

3.1.23
capacity
(relating to recording) the total amount of stored information that a storage media or medium can hold.

Note 1 to entry: It is expressed as a quantity of bits or bytes.

3.1.24
VSS
system consisting of camera equipment, storage, monitoring and associated equipment for transmission and controlling purposes

Note 1 to entry: CCTV systems are included in the more general term ´VSS´.

3.1.25
channel
single path for conveying digital or analogue data, distinguished from other parallel paths

EXAMPLE: Video input or output channel.

3.1.26
checksum
unique value or key computed by an algorithm for a data packet, based on the information it contains

Note 1 to entry: It is passed along with the data to authenticate that the data has not been tampered with. Any change to the image data, metadata or image sequence would cause a change in the resultant checksum.

3.1.27
compression
the process of reducing the size of a data (image) file

3.1.28
compression rate
ratio of a file's or image's uncompressed size compared to its compressed size

Note 1 to entry: A high compression rate means smaller image files and lower image quality and vice versa.

3.1.29
common interconnection
interconnection used by several video and data channels and/or other applications

3.1.30
communication
transmission of messages and/or signals between VSS components

3.1.31
component
functional part of the VSS

3.1.32
continually
recurring frequently at regular intervals

3.1.33
contrast
(relating to image) difference in visual properties that makes an object (or its representation in an image) distinguishable from other objects and the background

Note 1 to entry: In visual perception of the real world, contrast is determined by the difference in the colour and brightness of the object and other objects within the same field of view.

3.1.34
data
image, meta and other data of the VSS

3.1.35
data acquisition
sampling of information to generate data by processing of signals with appropriate sensors converting the measurement parameter to a signal

3.1.36
data backup
process of copying data to enable the recovery of the original recording in the event that the original recording is lost or damaged

3.1.37
database
structured collection of records or data. Records are retrieved in answer to queries

3.1.38
data identification
capability to find, retrieve or delete specific data without ambiguity e.g. by the use of unique IDs

3.1.39
data integrity
condition when data has not been modified or altered from its source either maliciously or by accident and in which data are maintained during any operation, such as transmission, storage, and retrieval, in order to preserve data for their intended use

3.1.40
data management
management of user-actions, audio-/video-data and general information's that are not part of the activity management

3.1.41
data manipulation protection
means to guarantee the integrity of data

EXAMPLE: Certified data handling, encryption, watermarking and limited access to the data.

3.1.42
default (by)
parameter settings stored in equipment by the manufacturer that can replace settings configured during commissioning or in later use

3.1.43
decryption
process of changing encrypted data into plain data using a cryptographic algorithm and key

3.1.44
digital image
image consisting of pixels using ranges of discrete values

3.1.45
digital video recorder
system that is capable of recording, playback, backup and export of digital images captured by image sources.

Note 1 to entry: A Network Video Recorder is included within this definition.

3.1.46
documentation
(relating to the system) paperwork (or other media) prepared during the design, installation and hand over of the system recording details of the VSS

Note 1 to entry: Component documentation may be provided by the manufacturer on paper or an alternative. medium

3.1.47
electronic article surveillance
technological method for preventing shoplifting e.g. from retail stores

3.1.48
encryption
cryptographic transformation of data that conceals the data original meaning to prevent it from being known or used

3.1.49
equidistant interval
constant distance in time, when sampling values of a continuous signal

3.1.50
essential functions
vital functions of a VSS, which are image capturing, transmission, recording and/or presentation

3.1.51
event
incident in the real world

EXAMPLE: A fire (burning house), an intrusion (broken door) or moving person, a power-failure, a short circuit, presence of an intruder.

3.1.52
event driven action
user or system activity driven by an alarm- or trigger-signal

3.1.53
event recording
event controlled recording or storing of image signals for a pre-determined time

3.1.54
exact copy
transfer of data from original recording location or master copy to secondary storage, if digital as bit for bit copy

3.1.55
export
transfer of data from the original location to a secondary storage location with a minimum of necessary changes

3.1.56
external input
external source connected to a dedicated input on the VSS

3.1.57
external interconnection
interconnections exchanging data over the boundary of the system

3.1.58
external system
VSS receiving and sending information and control signals but not providing VSS functions

3.1.59
failover
capability to switch over automatically to a redundant or standby component or system, upon the failure or abnormal termination of the previously active component or system

3.1.60
fail-safe
function or method which ensures that a failure of equipment, process, or system does not propagate beyond the immediate environs of the failing entity

EXAMPLE: A device causing no harm or at least a minimum of harm to other devices or hazards to personnel on failure or operator error.

Note 1 to entry: A fail-safe system has been designed in a way that the probability of a failure is extremely low to accomplish its assigned mission regardless of environmental factors.

3.1.61
fault
VSS condition of one or more components or interconnections that prevents the VSS or part thereof from operating normally

3.1.62
fault message
message from the system to an operator, to describe time, type and location of a fault

3.1.63
fingerprint
method of generating a unique ‘fingerprint’ of the original recorded image that cannot be reproduced if the image is altered

3.1.64

graphics interchange format
8-bit-per-pixel bitmap image format

3.1.65
hazard
incident that the VSS is designed to detect

EXAMPLE: Smoke or movement.

3.1.66
illumination
(related to imaging device) level of illumination (illuminance) at the sensor of the imaging device;

(related to scene) level of illumination (illuminance) on the area to be kept under surveillance

3.1.67
image
visual representation of a scene viewed by a camera

Note 1 to entry: In this document the term image includes multiple images in an image stream.

3.1.68
image analysis
the extraction of quantitative information from an image beyond which is readily apparent through visual examination

3.1.69
image capturing
transformation of images from an optical- or scanning-device in video-signals or digital data format

3.1.70
image rate
numbers of images per second

3.1.71
imaging chain
components and functions affecting the image quality consisting of image capturing, coding, interconnections, transmission, handling, storage, decoding and display

3.1.72
image handling
any activity that transforms an input image into an output image with as little changes as possible

3.1.73
image processing
method to change or analyse (digital) images with algorithms or (software) procedures

EXAMPLE: Compressing and encryption of images, methods for image content analysis.

3.1.74
image scene
collection of visual information of the physical area being across the width of the imaging sensor where something occurs (an incident or event)

3.1.75
image sequence
linear group of images handled as one entity, usually time indexed

3.1.76
image source
device that delivers video data

3.1.77
image stream
a series of consecutive images from the same image source which are transmitted from one system component to another

3.1.78
image quality
measurement of how accurately an observed image represents a real object as a collection of sharpness, brightness, color reproduction, visual resolution, evenness of illumination, contrast, geometry, etc.

3.1.79
incident
an occurrence or activity of interest that the VSS is intended to view or record and which may need a response by an operator

3.1.80
indication
information (in audible, visual or any other form) provided to assist the user in the operation of a VSS

3.1.81
instant replay
playback of recently recorded images from storage

EXAMPLE: Playback of an image sequence right after an incident or event.

3.1.82
interconnections
medium by which messages and/or signals are transmitted between VSS components

3.1.83
JPEG
a common standard for image compression, defined by the Joint Photographic Experts Group

EXAMPLE: A standard CRT has a Kell factor of 0,7 for NTSC pictures with a vertical visual resolution of 338 lines (483 × 0,7) and a PAL picture 403 lines (576 × 0,7).

Note 1 to entry: The JPEG file format is ISO 10918 series.

3.1.84
latency time
delay between initiation of a request and the required effect of the request

3.1.85
liquid crystal display
thin, flat display device made up of any number of colour or monochrome pixels arrayed in front of a light source or reflector

3.1.86
location identifying data
data which uniquely identifies the physical location of a device

3.1.87
logical authorisation key code
numeric or alphabetic codes entered by an authorized user to gain access to restricted functions or parts of the VSS

3.1.88
key
object with mechanical, logical or electronic code that unlocks a locking mechanism to transform encrypted data into original data

3.1.89
master copy
backup as identical copy of the original recording, in digital systems an exact bit for bit copy

3.1.90
maximum storage time
retention period or specified time for which images are to be held in a primary storage medium

3.1.91
meta data
any secondary information or data associated with images in a VSS

EXAMPLE: Time and date, text strings, location identifying data, audio and any other associated, linked or processed information.

3.1.92
monitoring
(relating to component condition) process of verifying that interconnections and components are functioning correctly;

(relating to operator activity) viewing live images in order to detect events or incidents

3.1.93
MPEG
common standard used for coding and compression of moving images, defined by Moving Picture Experts Group in different versions

EXAMPLE: Examples are MPEG-2 and MPEG-4.

3.1.94
multiplexer
switching device providing the simultaneous or sequential representation of several data streams such as video audio, etc. via one single transmission medium

3.1.95
normal operation
state of the VSS when not in power-up or power down procedures and no fault is present

3.1.96
non-relevant security application
security system not used as primary mitigation of the risk

3.1.97
notification
passing an alarm or a message of the VSS to an external system

3.1.98
object mask
means to mark an object of the area of interest in the camera image display

3.1.99
obscuring
preventing the imaging device from viewing any part of the area of interest other than by moving the device

3.1.100
operational requirement
key document for system designers, which clearly defines the operational parameters of the VSS according to the agreed expectations

3.1.101
operator
authorised individual (a user) using a VSS for its intended purpose

3.1.102
operator log
system log of events and operations which have been handled on a workstation or by a certain operator

3.1.103
original recording
first instance of unaltered images in persistent on-line storage, primary or original image stored on media suitable for long-term storage

3.1.104
physical authorisation key
implement used by an authorized user to gain access to restricted functions or parts of a VSS (mechanical key, magnetic card, electronic token or similar)

3.1.105
physical storage size
size of a storage medium expressed in its characteristic unit

EXAMPLE: For digital medium bytes, gigabyte (GB) or terabyte (TB) are used.

3.1.106
picture
image

3.1.107
pixel
smallest possible element of an image

Note 1 to entry: Acronym for picture element.

3.1.108
playback
viewing of previously recorded images from storage media

3.1.109
point of sale data
data generated by a point of sale terminal

3.1.110
power supply
part of the VSS to supply the VSS with electrical power

3.1.111
presentation
function of VSS displaying images and data to the user

3.1.112
prime power source
power source used to support a VSS under normal operating conditions

3.1.113
primary image
refers to the first instance in which an image is recorded onto any media

3.1.114
primary storage
storage used to store data that is not in active use and non-volatile for the preservation of stored information e.g. for later retrieval or in an event of power loss

3.1.115
privacy masking
blocking out or obscuring areas of an image for privacy reasons

3.1.116
protected
maintaining and preventing deletion of stored images, in original condition, for longer than the set retention time

3.1.117
redundant array of independent disks RAID 5
data storage architecture dividing and replicating data among multiple hard disks so that failure of one disk will not cause a loss of recorded data

3.1.118
relevant security application
security system used as primary mitigation of the risk

3.1.119
restore (alarm)
action of a user to change the state of a subsystem or detector from the alarm-, fault- or tamper condition to its previous condition

3.1.120
repetitive failure
rapidly repeating and duplicating signals for no identifiable reason causing additional or unwanted messages for the same fault condition

3.1.121
remote operation
operation at remote workstation connected by external interconnections that are not part of the VSS

3.1.122
resolution (format)
description of the size of a digital image in pixels e.g. 720P, 1080P, 640X480 etc. pixels/inch or number of pixels of a video-frame, monitoring device, print out

visual resolution – measure of the ability of a camera or video system to delineate and reproduce detail from the original scene or image

Note 1 to entry: Measurements are typically given in pixels/inch, height and width in pixels, total number of pixels etc

3.1.123
recording rate
image rate for one input channel or a complete recording device

3.1.124
recorded information
any data recorded on any recording medium (e.g. electronic, magnetic or optical) containing information of events and camera views that have happened in the past

3.1.125
redundancy
methods to secure a system against component failures by doubling elements which autonomously ensure operation in case of a failure

EXAMPLE: Redundant or fail-safe systems continue operation automatically with a second component in case of failure of the primary one. For redundant communication the system switches automatically to the second communication channel, if the first channel does not give a response.

3.1.126
remote video response centre
operation which is continually manned and capable of receiving multiple concurrent VSS images from remote locations for the purpose of interacting with site(s) to provide security and related services

3.1.127
remote workstation
a secondary or auxiliary control station located at some distance from the VSS or the protected premises

3.1.128
replay
playback of recorded images from storage

3.1.129
response
every control command, change of system conditions or information to external devices or persons driven by alarms, faults, messages or triggers

3.1.130
response time
time a system or functional unit takes to react to a given input

EXAMPLE: The response time of a presentation device is the amount of time a pixel takes to go from active (black) to inactive (white) or back to active (black) again. It is measured in ms.

3.1.131
risk
the likelihood, combined with the effect, of loss damage or harm

3.1.132
scene brightness
observed brightness of the scene, dependent on the scene illumination

3.1.133
secondary storage media
from original recording location separated storage media

3.1.134
stakeholder
any individual, group or organisation that might be affected by, or perceive itself to be affected by, the risk

3.1.135
storage
means for storing data or video for subsequent use or retrieval

EXAMPLE: Hard disk, flash drive, CD, DVD.

3.1.136
storage media
means where data is stored for later retrieval, viewing or processing

3.1.137
subsystem
part of a VSS located in a clearly defined part of the supervised premises capable of independent operation

3.1.138
surveillance
observation or inspection of persons or premises for security purposes through alarm - systems, VSS, or other monitoring methods

3.1.139
system configuration
methods to specify a VSS in structure of its elements, data handling, log files, data storage capabilities, user access levels and user control capabilities

3.1.140
system data
system configuration parameters

3.1.141
system integrity
ability of an application to function as designed and the measure of immunity from influence which could affect normal operation

3.1.142
system log
chronological list of events or operations which have occurred in the VSS, which allows the reconstruction of a previous activity and records the attributes of a change (such as date/time, operator)

EXAMPLE: A record book or its electronic equivalent into which all relevant details of the VSS, its operation, performance and its maintenance can be entered in a secure manner for later retrieval by authorised users.

3.1.143
system management
configuration and control of the VSS, as well as the administration of system data and components

3.1.144
system security
protection of the system against failures as tampering, illegal access, vandalism. Controlled physical or electronic access to the VSS or any component to prevent unauthorised access

3.1.145
system set-up
configuration of the system

3.1.146
tamper
unauthorised changes in the system e.g. unauthorised physical access in order to outwit the system or parts of it

3.1.147
time synchronisation
manual or automatic method to keep the time and date integrity between different components of the VSS, including daylight saving time changes

3.1.148
trajectory lines
means to mark the positions passed by a moving object of the area of interest in the image display

3.1.149
trigger
signal as reaction to an event in order to activate a function or a device

EXAMPLE: A moving person switches on a recording device.

3.1.150
user action
deliberate input from an operator to the system to monitor, control the system or to change conditions

EXAMPLE: Switch camera x to monitor y.

3.1.151
user interface
means by which a user operates a VSS

3.1.152
video content analysis
analysis of live or recorded video to detect activities, events or behaviour patterns as defined in the operational requirements

3.1.153
video loss
absence of video signal from a capturing device

3.1.154
video matrix
a unit for connecting several input video signals to several outputs

3.1.155
video recorder
device to record and replay video

3.1.156
video motion detection
algorithm, procedure or device to generate an alarm condition in response to a defined change of the contents of a given image sequence

3.1.157
watermark
information placed in a digital image to verify its authenticity and integrity without affecting the visible content of the image

3.1.158
workstation
control station for user operation

3.2 Abbreviations

ANPR	Automatic Number Plate Recognition
ARC	Alarm Receiving Centre
ASF	Advanced Streaming Format
ATM	Automatic Teller Machine
AVC	Advanced Video Coding
AVI	Audio Video Interleave Format
B/W	Black/White
CCD	Charge Coupled Device
CD	Compact Disc
CRT	Cathode ray tube
DVD	Digital Versatile Disk
EAS	Electronic article surveillance, anti-shoplifting system
EMC	Electromagnetic compatibility
FPS	Frames Per Second (frame rate)
GIF	Graphics Interchange Format
ID	Identifier
IP	Ingress Protection Ratings
IPS	Images Per Second (image rate)
ISO	International Standards Organization
JPEG	Joint Photographic Experts Group
LCD	Liquid Crystal Display
MPEG	Moving Picture Experts Group
OR	Operational Requirement
POS	Point Of Sales
RAID	Redundant Array of Independent Disks
RVRC	Remote Video Response Centre
SNR	Signal to Noise Ratio
UPS	Uninterruptable Power Supply
UTC	Universal Time Coordinated
VCA	Video Content Analysis
VMD	Video Motion Detection
VSS	Video Surveillance System

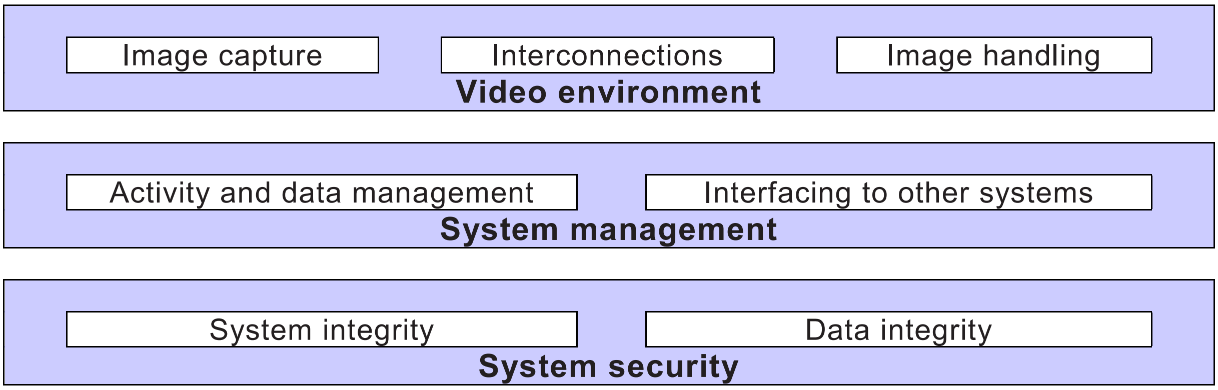
4 Functional description of the VSS

4.1 VSS

This Clause 4 is informative.

A VSS usually consists of equipment containing analogue and digital devices as well as software. Because the technology and, with it, the VSS equipment and their functionalities develop and change very rapidly, single devices and their requirements are not defined. Instead, this clause defines and describes the VSS as functional parts together with the relationships between them.

A VSS for security applications can be presented as functional blocks which portray the various parts and functions of the system (see Figure 1).



IEC 2568/13

Figure 1 – VSS

4.2 Video environment

4.2.1 General

The purpose of a VSS is to capture images of a scene, handle the images and display them to an operator with associated information for easy and effective usage. The entity consisting of VSS devices and interconnections between the devices can be described as **video environment**.

Instead of defining the actual devices that make up the VSS, the video environment is defined here in three functions:

- generation of video images (**image capture**);
- transmission and routing of video images and control signals (**interconnections**); and
- presentation, storage and analysis of the images (**image handling**).

The above-mentioned functions may reside in various hardware or software components of the system. Note that these functions do not necessarily always match up with separate devices, as several functions can be performed by a single device. As an example, a network camera device can capture the image (image capturing), store it temporarily (image handling), analyse it for VMD (image processing) and transmit it via the network (interconnections). Alternatively several devices in one system can perform the same function.

Figure 2 shows a simple practical example of the video environment:

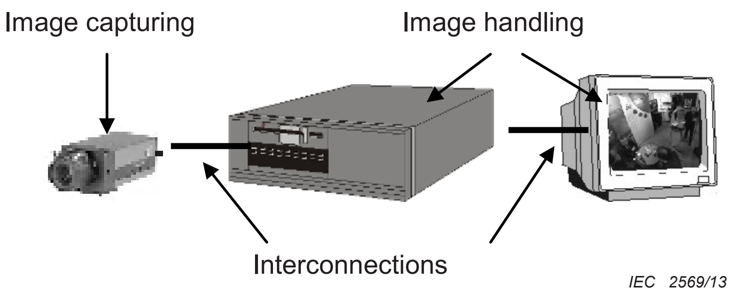


Figure 2 – Example for VSS

4.2.2 Image capture

The purpose of image capture is to generate and deliver an image of the real world in a format that can be used by the rest of the VSS.

The purpose of image capturing is to generate an image of the scene for later processing by the VSS. An image source captures an image of the scene, creates image data and delivers that data to the image handling functionality using the system interconnections. The image data can be in analogue (e.g. composite video) or digital (e.g. JPEG, MPEG-4) format.

4.2.3 Interconnections

Interconnections describe all transmission of data within the video environment. This includes two functions: **connections** and **communications**.

The communications describe all video and control data signals, which are exchanged between system components. These signals may be analogue or digital.

Connections cover the media used for the communication signals. Examples of connections are cables (e.g. twisted pair, coaxial or optical fibre), digital networks, wireless transmission as well as equipment e.g. a multiplexer or video matrix.

A VSS can be divided into components that are communicating through interconnections, which are not dedicated to the VSS. An example is a network which is shared with other applications.

4.2.4 Image handling

4.2.4.1 General

The functions of image handling include **analysis**, **storage** and **presentation** of an image or a sequence of images. The same functions can also be applied to other data (e.g. audio stream) and meta data. A VSS does not necessarily contain all of these functions.

Image handling can be performed by one or several devices that make up the VSS (e.g. monitors, recorders, image analysers, intelligent cameras and remote workstations). One device can also handle several image handling tasks (e.g. digital video recorder).

During image handling the images may be changed e.g. in resolution, image rate and compression.

4.2.4.2 Analysis

The video data that makes up the images can be analysed in order to extract information from live or recorded video data. In addition to the video data the analysis function can also use other data (e.g. audio stream) or meta data as inputs.

Analysis can be utilized for several purposes:

- proving the integrity of the system (e.g. camera position);
- interpreting the captured scene (e.g. automatic number plate recognition);
- detecting an event which may trigger an alarm (e.g. moving person or smoke detection).

4.2.4.3 Storage

The video image data (as well as other data or meta data) can be stored on a storage medium (e.g. magnetic, optical, electronic) for later retrieval. The first manifestation of an image in persistent and final form is called ´original image data´ or ´original recording´. The stored data can be in analogue or digital format. Precise copies may be made of digital data and called ´original´. The transfer of images from the original recording and location to another media is called ´image backup´ or ´master copy´ in case of an exact copy or otherwise if altered ´export´. Exported images may be used as working copy due to necessary compression or format conversions, image enhancements or similar processing.

4.2.4.4 Presentation of information

Presentation of information is the display of video images either as single (still) images or as video sequences consisting of consecutive video images in visible form that can be viewed by an operator. One or several video images may be displayed simultaneously. Additionally, other data (e.g. audio stream) and meta data can be presented.

Examples of devices for presenting information include monitor screens (e.g. CRT, plasma, LCD) or projectors.

4.3 System management

4.3.1 General

The user interface is a very important interface for activity and data management within VSSs. This interface significantly determines comfort, functionality and the actual security of a VSS.

Seen from the system management point of view, a VSS consists logically of two functions:

- **activity** and data management that captures, transmits, stores and presents video images, other data or meta data, This part also handles operator commands and system-generated activities e.g. alarm procedures and alerting of operators;
- **interfaces** that connect the VSS to other systems.

The above-mentioned logical functions of the system do not refer to separate devices, as one device can perform multiple tasks. For example, a recorder handles, stores and outputs the images and, at the same time, performs video content analysis and alerts an operator when an alarm procedure is activated.

4.3.2 Data management

A VSS manages information. In addition to the video data, it can also handle other acquired data e.g. audio, or meta data which can be acquired from another system or generated by the system. This information is managed partly by the system itself and partly by an operator.

The management of the above-mentioned information comprises data acquisition (e.g. image capturing), data transmission between system components (e.g. transmission of images from a camera to a recorder), storage of images (e.g. hard-disk recording) and data presentation (e.g. displaying of images on a monitor screen). These functionalities are mainly taken care by devices that make up the VSS, or by software residing in these devices (e.g. a database for storing video images).

The system can handle and generate meta data. There are different types of meta data that is managed by the system:

- data that is linked to the actual video data, e.g. POS data, license plate numbers, location identifying data. It can be acquired from another system or generated by the system itself (e.g. time stamps, image source identifiers);
- log files generated and stored by the system, describing system or operator activities;
- system data in form of system condition, storage media usage, etc.

An operator is responsible for responding to the presented information as defined in the operational requirements.

4.3.3 Activity management

Activity management comprises all the activities that are driven by events and any user actions.

An event is an occurrence in the real world, such as a fire (a house burning), an intrusion (a door broken) or another defined situation (a person moving). The event can involve a hazard endangering human lives or property.

An event can also be an occurrence that is targeted at the VSS, e.g. tampering of a system component.

The event can trigger an alarm procedure in the VSS. The trigger can be the output from image handling (e.g. VCA or VMD), a signal from a sensor (e.g. smoke or motion detector) or data received from another system (e.g. EAS gates or ANPR system).

When the alarm procedure is triggered, the VSS performs the tasks as defined in the operational requirements. Mostly, these tasks form a response to the hazard perceived.

This alarm response can involve internal activities (e.g. deliberate repositioning of a camera to change the view, recording or image presentation) as well as notification of an external system (e.g. access control or alarm receiving centre).

A typical task of the alarm procedure is also alerting an operator, who in turn can start other activities. The actions performed by an operator are defined in the operational requirements.

Figure 3 illustrates event driven activities:

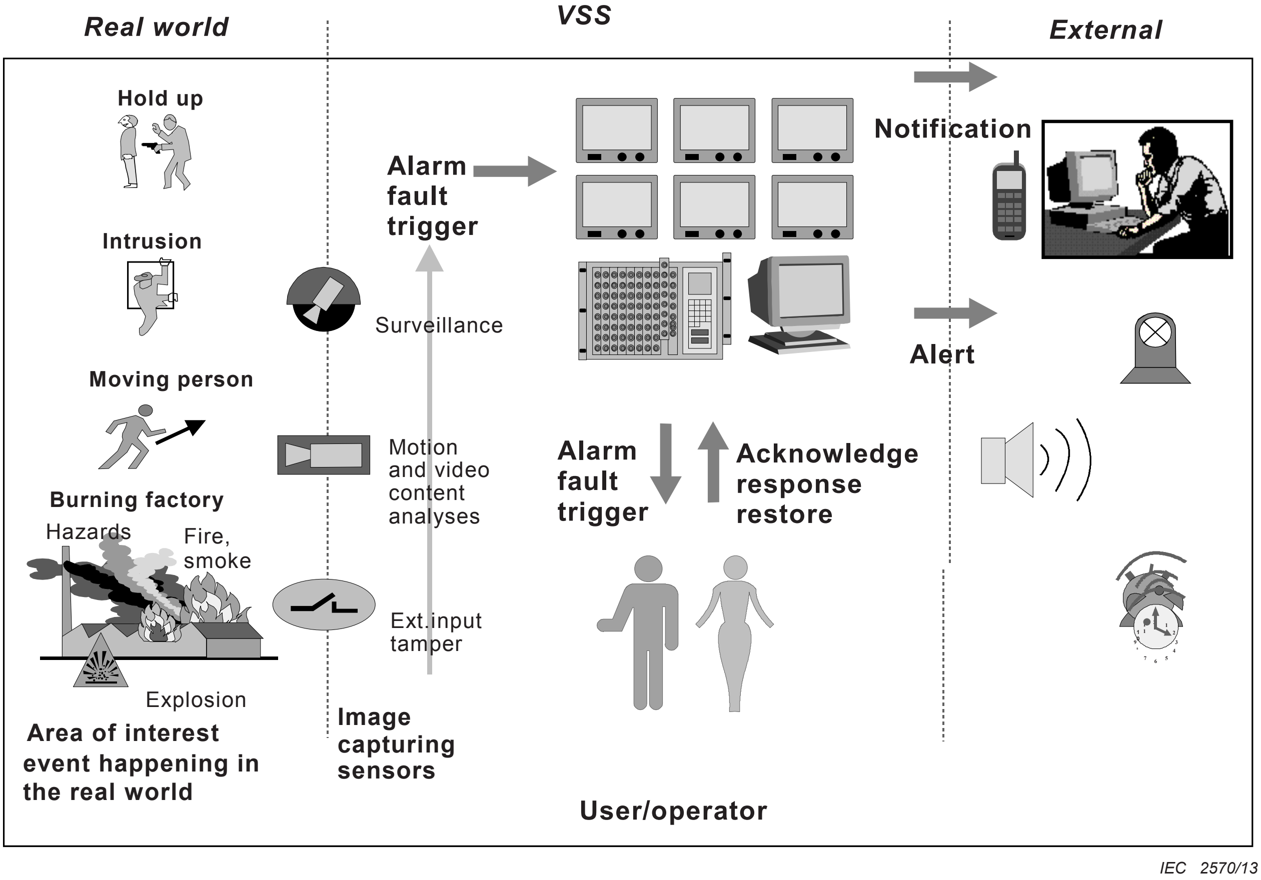


Figure 3 – Activity management

Activity management includes system configuration, system control, post event analysis and other activities started by an operator. Examples of these are positioning of a pan-tilt-zoom camera, redirection of images to a monitor, as well as data backup, export and printing. All of these activities are defined in operational requirements of the application.

4.3.4 Interfaces to other systems

For interfacing to other systems command and data formats need to be specified in detail for both systems. System interfaces allow mutual and comfortable access to functionalities and data.

A VSS may be interfaced to other systems, e.g.

- other security systems (e.g. other VSS, intrusion and hold-up alarm, access control or fire alarm systems),
- security management systems (e.g. alarm management systems or ARC (alarm receiving centres), RVRC),
- other, non-security systems (e.g. building management systems, automatic teller machines, Point-of-Sales equipment or automatic number plate recognition systems).

The interfaces between the systems can manage data communication, mutual system control, common databases, common user interfaces or other type of system integration.

In general, a distinction can be made between two kinds of transmission, where either the physical transmission path is part of the VSS or is provided by a third party as external interconnection.

4.4 System security

4.4.1 General

System security consists of **system integrity** and **data integrity**. System integrity comprises physical security of all system components and control of physical and logical access to the VSS. Data integrity covers logical access to the data and prevention of loss or manipulation of the data.

The purpose of system security is to protect from intentional and unintentional interference with the normal operation of the VSS.

NOTE This standard refers to system security where this can be provided by the system itself. Security may also be provided by physical measures, location of components, etc.

4.4.2 System integrity

System integrity comprises the protection of each system component or device as well as protection of the system as an entity. If external interconnections between system components are used, their protection is also part of the system integrity. Same applies also to interfaces with other systems.

System integrity consists of three parts:

- detection of failures of components, software and interconnections
- protection against tampering
- protection against unauthorized access to the system

4.4.3 Data integrity

Data integrity covers several important items:

- data identification (ensuring accurate identification of data source, time, date etc.);
- data authentication (prevention of modification, deletion or insertion of data);
- data protection (prevention of unauthorised access to the data).

5 Security grading

VSSs are graded to provide the level of security required. The security grades take into account the risk level which depends on the probability of an incident and the potential damage caused by it as shown in Figure 4.

NOTE It is the functions of the system rather than the VSS system components that are graded.

Due to the wide range of the surveillance tasks functions of a VSS may have different security grades within one system. 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. The tamper protection and detection requirements of 6.3.2.3 may be applied with different grades in various locations within the system as appropriate to the risk at that location. This shall be recorded in the OR or system design proposal. This shall be determined by a risk assessment and be explicitly defined in the OR. The security grades shall be applied, where VSS is identified as the primary mitigation of the risk. It shall be noted that the risks identified may be best mitigated by other means than VSS.

Sections of grading or the grading of individual functions may only apply, if determined to be relevant in the risk assessment, OR, or system design proposal. Where not specified the default security grade is 1.

There are four grades:

– low risk (grade 1)

  A VSS intended for surveillance of low risk situations. The VSS has no protection level and no restriction of access.

– low to medium risk (grade 2)

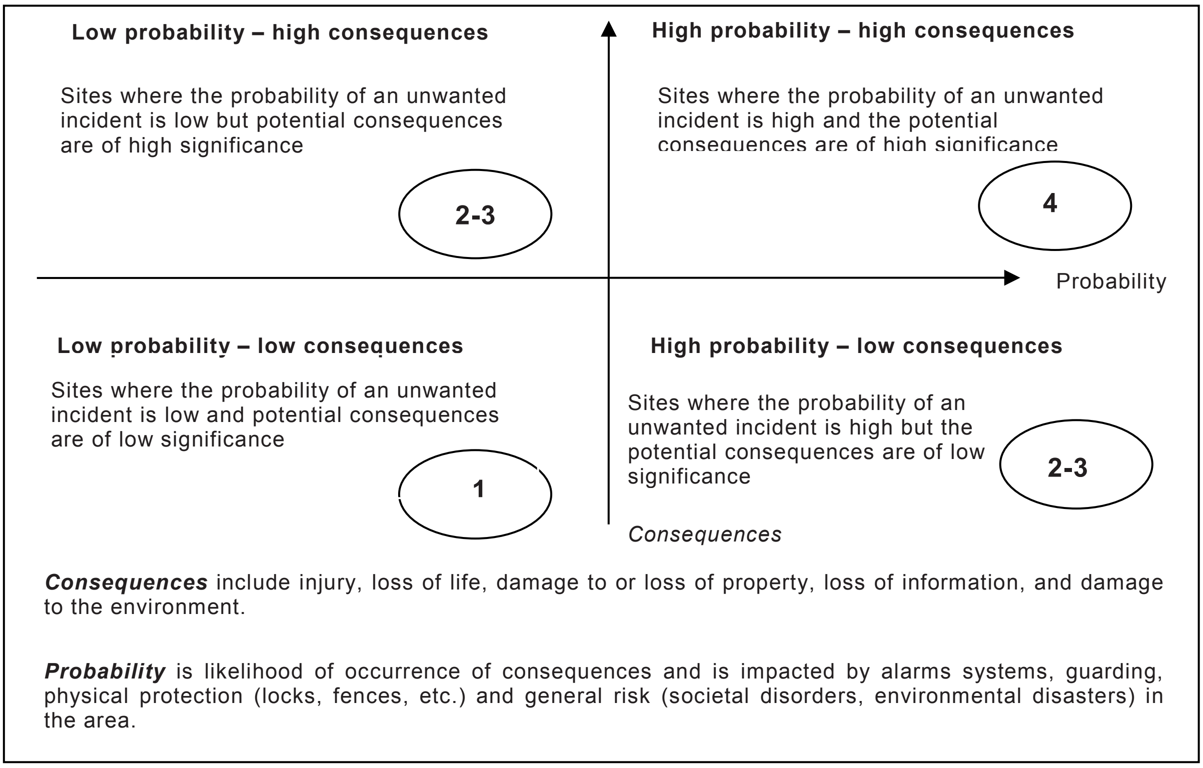
  A VSS intended for surveillance of low to medium risk situations. The VSS has low protection level and low restriction of access.

– medium to high risk (grade 3)

  A VSS intended for surveillance of medium to high risk situations. The VSS has high protection level and high restriction of access.

– high risk (grade 4)

  A VSS intended for surveillance of high risk situations. The VSS has very high protection level and very high restriction of access.


Low probability – high consequences
Sites where the probability of an unwanted incident is low but potential consequences are of high significance
2-3
High probability – high consequences
Sites where the probability of an unwanted incident is high and the potential consequences are of high significance
4
Probability
Low probability – low consequences
Sites where the probability of an unwanted incident is low and potential consequences are of low significance
1
High probability – low consequences
Sites where the probability of an unwanted incident is high but the potential consequences are of low significance
2-3
Consequences
Consequences include injury, loss of life, damage to or loss of property, loss of information, and damage to the environment.
Probability is likelihood of occurrence of consequences and is impacted by alarms systems, guarding, physical protection (locks, fences, etc.) and general risk (societal disorders, environmental disasters) in the area.

IEC 2571/13

Figure 4 – Risk and security grades

The functions of a VSS, which have specifications according to security grades, are:

1) Common interconnections
2) Storage
3) Archiving and backup
4) Alarm related information
5) System logs
6) Backup and restore of system data
7) Repetitive failure notification
8) Image handling device PSU monitoring

9) Image buffer holding time
10) Essential function device failure notification time
11) Monitoring of interconnections
12) Tamper detection
13) Authorisation code requirements
14) Time synchronisation
15) Data authentication
16) Export/copy authentication
17) Data labelling
18) Data (manipulation) protection

6 Functional requirements

6.1 Video environment

6.1.1 Image capture

The captured images of the area of interest shall have sufficient accuracy and detail to enable users to extract the appropriate information defined in the image quality requirements (see 6.5).

The capturing of images shall fulfil the customer objectives for image handling e.g. presentation and recording (concerning fps, resolution, colour depth and latency time) defined in the image quality requirements (see 6.5).

For image quality requirements at installation time, see IEC 62676-4.

6.1.2 Interconnections

6.1.2.1 General

Any interconnections shall be designed to minimise the possibility of signals or messages being delayed, modified, substituted or lost in accordance with the requirements defined in 6.3.2.3.1.

Monitoring of interconnections shall be provided in accordance with the requirements defined in 6.3.2.2.4 of the system security requirements.

6.1.2.2 Common interconnections

Image streams sharing common interconnection shall be designed and configured in a way that they do not adversely affect each other or any message transfer in any normal operation mode.

For security grades 3 and 4, if a VSS is designed and configured in a way that single or multiple operators request video images via common interconnections, the design of the system shall ensure that the available capacity is sufficient for the anticipated operation of the VSS. This may be achieved by configuring the maximum throughput of image streams on the VSS.

NOTE Consideration is given to prioritization of image streams, e.g. for recordings.

6.1.3 Image handling

6.1.3.1 Presentation

If the VSS is able to present information, the following properties shall be declared by the manufacturer in the documentation:

- maximum number of simultaneously displayed image sources;
- resolution of displayed image(s);
- size(s) of displayed image(s);
- display rate (number of images displayed per s);
- response time;
- colour / B/W.

When displaying images, whether they consist of the entire image source or a part of it, the proportions of the displayed image shall be the same as in the original image source. Any superimposed information e.g. timestamps, camera names produced by the system shall not affect the recorded image.

6.1.3.2 Analysis

Any superimposed information e.g. object masks, trajectory lines, and classification information, produced by the system shall be processed as meta data and shall not affect the image itself (see 6.3.3). Only a privacy mask is allowed to affect the field of view of an image for privacy reasons, in order to block out sensitive areas from view.

6.1.3.3 Storage

If storage or recording functions are available in the VSS following and Table 1 requirements apply.

Most systems modify the video images before they are stored (conversion between analogue and digital format, resolution changes, compression, watermarking, or encryption). In the documentation, all processes that might cause loss of information shall be clearly stated.

If redundant storage is not provided, images shall be stored on the storage medium in a manner that will enable the data to be displayed and copied using alternative devices.

EXAMPLE The storage medium is mounted into new device in case of a device failure.

Table 1 – Storage

The VSS shall be capable of	Security grade			
	1	2	3	4
Data backup and/or redundant recording			X	X
Operating a fail-safe storage (e.g. RAID 5, continuous mirror) or switching automatically over from one storage media to another in case of storage failure				X
Reacting to a trigger with a maximum latency time of		1 s	500 ms	250 ms
Replaying an image from storage with a maximum time after the incident or actual recording of			2 s	1 s

The following properties of the storage device(s) shall be declared by the manufacturer in the system documentation:

- type(s) and number of video input channels or image streams;
- type(s) and number of video output channels or image streams;
- type(s) and number of other input channels or data streams;
- maximum number of images stored per second for each channel or stream at the specified resolution;
- maximum total number of images stored per second at the specified resolution when all channels or streams are connected;
- maximum number of images displayed locally and/or at a remote workstation when storing at maximum rate;
- maximum number of images stored when displaying at maximum rate locally and/or remotely;
- resolution and size of stored images;
- maximum bit rate per storage device and per stream;
- storage capacity in hours at the chosen number of input channels or streams, images per second, resolution and quality;
- compression (methods available, settings, compression rates);
- time to recommence image storage after a system restart (e.g. on power loss).

The storing of video images shall not be influenced by any live image display and requests or image backup and export. The configured recording rate shall always be granted in every normal operation mode.

If a constant frame rate is specified the sequences of pictures shall provide images at equal time intervals.

The system shall be configurable such that a maximum storage time can be set. The VSS shall be capable of automatically deleting images once they have been stored for the set period of time. Recorded images marked as protected from being deleted, may be stored for a longer period of time. The maximum storage time allowable by the applicable national legislation should not be exceeded.

The VSS shall offer information about:

- the video input channels or streams being recorded;
- the image storage usage in capacity and recording time;
- remaining storage capacity.

The system shall be capable of indicating as specified in the system documentation, if the storage capacity is running low.

6.1.3.4 Image data backup / archiving

If storage or recording functions are available in the VSS following and Table 2 requirements apply.

It shall be possible to extract and preserve the image data for evidential or other purpose. It shall be possible to extract or move the stored data so that it can be viewed or replayed in an alternative location. A means of playing back the extracted image data (e.g. archive viewer system) shall be available without compromising the ability of the system to continue to function as designed.

If digital data is transferred to a secondary storage medium then it shall be an identical copy of the original data and shall be called ´exact copy´.

This data shall be viewable with an archive viewer system including all additional meta data (ATM, POS, VCA info, location identifying data etc.) or shall be recoverable into the primary system storage without any loss of information.

Table 2 – Archiving and backup

The archiving shall offer	Security grade			
	1	2	3	4
Authentication of every single image and image sequence				X
An automatically scheduled backup of alarm image data				X
A backup of alarm image data by manual request			X	X
Verify the successful image backup			X	X

6.1.3.5 Image export

If recording functions are available in the VSS the following requirements apply:

- the image export shall not alter the original recording in the primary storage. The system shall be able to offer the selection of time range and image source to be exported or copied;
- the exported data shall have an image source identifier and time stamp ´identifying´ images to guarantee order and completeness of image sequences;
- the system shall be able to export or copy a single image as well;
- The system documentation shall specify the export formats supported (see 6.1.3.6)

  NOTE The data format used in export usually does not represent all information stored e.g. metadata and audio. These formats have the advantage to be more common and easier to handle.
- Printing of images onto paper shall not be considered as image export and does not satisfy requirements for image export.

6.1.3.6 Data format

Compression algorithms that require the use of proprietary software to obtain direct access to VSS data shall not be used unless the information to achieve this is made available (e.g. by a Software Development Kit).

NOTE Special or modified compression algorithms prevent direct access to the VSS data without the use of proprietary software, which makes replay of images by third parties difficult.

The methods of storage and/or transmission for video, audio and metadata shall use standard formats, codec’s and containers. The data shall comply strictly with the standards and contain the full information required to decode the content.

The format and the means of locating the data within the VSS files shall be available as international published standards IEC, ISO or ITU.

The system shall 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 with no significant increase in file size.

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

The following list contains examples of acceptable international standards, but is not exclusive:

Video Codec’s:

– H.264: AVC: ISO/IEC 14496-10, ITU-T Rec. H.264: *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding*

– 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*

– H.263: ITU-T Rec. H.263 *Video coding for low bit rate communication*

– JPEG 2000: ISO/IEC 15444-1, *Information technology – JPEG 2000 image coding system: Core coding system*

– JPEG: ISO/IEC 10918-1 | ITU-T Rec. T.81 *Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines*

Audio codec´s:

– G.711: ITU-T Rec. G.711, *Pulse Code Modulation (PCM) of Voice Frequencies*

– G.726: ITU-T Rec. G.726, *40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation*

– AAC: ISO/IEC 14496-3, *Information technology – Coding of audio-visual objects – Part 3: Audio*

Video export and file formats:

– MP4: ISO/IEC 14496-14, *Information technology – Coding of audio-visual objects – Part 14: MP4 file format*

– MPEG-A: ISO/IEC 23000-10:2009, *Information technology – Multimedia application format (MPEG-A) – Part 10: Surveillance application format*

IP Video Protocol (Discovery, control, metadata, etc.):

– IEC 62676-2 (all parts), *Video Surveillance systems for use in security applications – Part 2: Video transmission protocols*

6.1.3.7 Encryption and watermark

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

If images are encrypted the encryption should not alter the image information. The methodology for encryption and decryption should be readily available to authorised users

6.1.3.8 Minimum metadata

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 VSS files shall, as a minimum, permit a UTC time stamp and camera identifier to be associated with each image and audio sample. For VSS without audio, the time stamp shall have a resolution of no less that 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 way of encoding time stamps, but whichever is used shall be stated.

The VSS 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

6.1.3.9 Multiplexing format

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

It is permissible for the VSS 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.

6.1.3.10 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.

6.1.3.11 Image export

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

– VSS data exported from a recorder shall have no loss of individual frame quality, change of image 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.
– Minimum metadata (see 6.1.3.8) and authentication signatures, where they exist, should be exported with the images.
– The system should be capable of exporting images, and audio where applicable, from selected cameras (and microphones) within user-defined time periods.
– The system should not lose functionality or performance during the export of data
– The export method of the system should be appropriate to the capacity of the system and its expected use.

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

NOTE 2 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.
- 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.

The system should display an estimated time to complete the export of the requested data 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.

6.1.3.12 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 shall be capable of being replayed on a computer via the exported software.

The replay application 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 (see 6.1.3.6) at an equivalent quality to the original and still displaying time and date information 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 capable of being replayed 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.

6.2 System management

6.2.1 Operation

Operation of the user interface shall be self-explanatory, simple and fast for an operator. The system status shall be detected, processed and displayed automatically. Alarm situations shall be identifiable and accessible immediately with a consistent documentation of the event.

6.2.2 Activity and information management

6.2.2.1 General

The system shall clearly distinguish between user requested and event-driven data. Alarm data may be given priority over continuously displayed data.

Images presented to an operator shall be clearly labelled as live or replayed video. In addition event driven video shall be clearly labelled as such to differentiate it from user requested video.

6.2.2.2 Status of system functions

The VSS shall always be able to offer information about the status of the essential functions.

6.2.2.3 Events and event driven activities

If the VSS is designed to handle event driven activities the following requirements apply.

Triggers or messages shall be retrieved from a queue in the order of their arrival except when a means to prioritise these inputs is provided.

Where the system provides the facility to prioritize alarms then the priority level shall also be indicated.

In this case messages or triggers shall be retrieved according to the priority levels. Where a number of messages or triggers of equal priority are in the queue they shall be retrieved in the order of their arrival.

General requirements for the indication of the priority are as follows:

- the system shall indicate when more alarms exist than are currently being displayed;
- in addition to the information actually displayed, additional information may be available on demand. The visibility of the prioritised information shall be preserved;
- any normal operation of the VSS shall not prevent the indication of an alarm.

It shall be possible to distinguish between different system conditions that may have triggered the activity and between an alarm, a fault or tamper.

The VSS shall offer means to indicate an alarm visually and audibly in order to get the attention of an operator.

The VSS shall offer means to acknowledge alarms.

For systems of security grades 3 and 4, on alarm the VSS shall be able to display alarm related information. The information presented for each alarm message shall include:

a) the origin or source of alarm;
b) the type of alarm;
c) the time and date of alarm.

6.2.2.4 System logs

Accurate and complete system logs shall be maintained for a period of time as defined in the OR. Data in the system log shall be organized and presented in chronological order. The system shall prevent unauthorised editing or deletion of system logs. A log shall be available for each operator’s workstation.

Following details given in Table 3 shall be logged:

Table 3 – System logs

The system shall log with time stamp (date and time), event, source	Security grade			
	1	**2**	**3**	**4**
Alarms		X	X	X
Tamper			X	X
Video loss and recovery from video loss			X	X
Power loss		X	X	X
Essential function failure and recovery from failure			X	X
Fault messages displayed to the user				X
System reset, start, stop		X	X	X
Diagnostic actions (health check)				X
Export, print/ hardcopy incl. the image source identifier, time range		X	X	X
User log in and log out at workstation with time stamp, successful and denied logins (local/ remote) including reason of denial (wrong password, unknown user, exceeded account)		X	X	X
Changes in authorisation codes			X	X
Control of functional cameras				X
Search for images and replay of images			X	X
Manual changes of recording parameters			X	X
Alarm acknowledge / restore			X	X
System configuration change			X	X
Date and time set and change with current time and new time			X	X

6.2.3 Interfacing to other systems

Common facilities shall comply with all standards for the applications (e.g. intrusion, access, VSS,..) in which they are used. Where requirements of more than one standard apply to a specific function or component, the standard with the strictest requirement shall take precedence for that function or component.

NOTE This applies directly, when several complying systems from different owners are interfaced together and are asked to provide consistent information.

All system security requirements as defined in 6.3 shall be fulfilled even in cases where the VSS is accessed or controlled by another system. The other system shall be seen as a system user with defined access rights.

Access levels to another system shall be consistent with the levels required by that system standard and shall not give unauthorised access to the VSS and vice versa.

6.3 System security

6.3.1 General

VSS security consists of system integrity and data integrity. System integrity includes physical security of all system components and control of access to the VSS. Data integrity will include prevention of loss or manipulation of data.

6.3.2 System integrity

6.3.2.1 General

VSS of security grades 3 and 4 shall be capable of backup and restore of all system data.

6.3.2.2 Detection of failures

6.3.2.2.1 Failures notification

For VSSs with a user interface which is normally manned by an operator (either remote or local), alarm conditions from the components and functions, where specified in this standard, shall cause an alert. The failure shall be notified at any time a new user logs in or the system restarts.

The information to be presented shall include:

- time and date;
- origin and type of failure.

In addition, where the system provides for the facility to prioritize messages then the priority level shall also be indicated.

Notification of failures shall never cover or hide any important information display such as the area of interest in live images.

For security grades 3 and 4, the system shall be able to detect repetitive failures from a component and shall be configurable to generate a single message which shall only be repeated each time a new user logs in or the system restarts.

6.3.2.2.2 Monitoring of power supply

For security grade 4, failure of the primary and, if available alternative, power supplies to the system shall be monitored, with notification according to 6.3.2.2.1. In any case power supply failure shall always be indicated locally. The VSS shall attempt to resume normal operation after recovering from power loss. If the system is unable to resume after power has been restored, with the settings which existed before the power failure, this shall be logged and also indicated to an operator.

The VSS shall be able to shutdown regular operation in a defined procedure without loss of stored data. For security grades 3 and 4 images shall not be held in a buffer for longer than 5 s without being written into the storage medium.

6.3.2.2.3 Monitoring of system functions and components

For security grades 3 and 4 the VSS shall manage device failure by indicating any failure of the essential functions within 100 s of the failure.

6.3.2.2.4 Monitoring of interconnections

If interconnections between system components are part of the VSS, they shall be monitored according to the following Table 4:

Table 4 – Monitoring of interconnections

The system shall	Security grade			
	1	2	3	4
Repeatedly verify the interconnection at regular intervals with a maximum of			30 s	10 s
Try to re-establish a interconnection with following number of retries before notification			5	2
Maximum time permitted before notification to an operator of an interconnection failure			180 s	30 s

6.3.2.3 Tamper protection and detection

6.3.2.3.1 General

The VSS shall be protected against tamper in accordance with Table 5.

If tamper is detected a tamper condition shall be set and a tamper alarm generated. The tamper alarm shall be logged and clearly separated from other conditions e.g. failure, alarm or normal operation.

Table 5 – Tamper detection

The system shall detect	**Security grade**			
	1	**2**	**3**	**4**
Video loss		X	X	X
If an image capturing device with a fixed field of view no longer includes the entire specified field of view			X	X
Deliberately obscuring or blinding of the imaging device range			X	X
The substitution of any video data at image source, interconnection or handling				X
Significant reduction of the contrast of the image				X

6.3.2.3.2 Tamper protection of camera housings

The image capturing devices shall be protected against tamper in systems of security grade 3 and 4. Cameras should be placed out of reach and the fixing screws shall be tamper proof, to prevent un-authorised repositioning.

NOTE Protection against tampering of image capturing devices is not a requirement to systems of grade 1 and 2.

An image capturing device offering protection against vandalism shall meet the following minimum requirements:

a) minimal IP rating degree of 44 in accordance with IEC 60529;

b) hammer tests according to IEC 60068-2-75.

The impacts shall be applied to the main parts such as housing, lens, etc. For physical attack resistance tests the device shall be mounted according to the manufacturer’s instructions on a rigid support as defined in IEC 62262 for all tests. Each test shall be performed by a single person.

c) IK degree of 07;

d) resistance for a minimum of 1 min against:
   - unfixing the device by unscrewing the fixing screws;
   - pulling out the device;
   - attack with simple tool such as a screwdriver of 4 mm to 7 mm in diameter and 60 mm to 200 mm in length;
   - attack with simple tool such as a plier;
   - attack with a lighter to apply heat;

e) resistance against attack with acid-sweet drink using 0,3 l of a commercial soft drink. Pour ½ of it over the device and splash the rest on the underside of the device.

After the tests the device shall continue normal operation.

6.3.2.4 Protection against unauthorized access

6.3.2.4.1 General

For each VSS access to operation and data shall be governed by an authorisation scheme. This also includes access through a remote workstation or through an external system integrated with the VSS.

6.3.2.4.2 Access levels

For all grades of the VSS, there shall be several user access levels to the functions of the VSS or part(s) thereof. The user accessing the system can be either an operator or another system:

- **Level 1 Access by any person**

  Functions required to be accessible at level 1 shall have no restriction on access.
- **Level 2 Access by any user**

  Functions affecting the operation of the system, without changing its configuration.

  Access to functions required to be accessible at level 2 shall be restricted by means of key, password, code or similar access-limiting means or device.
- **Level 3 Access by system administrators**

  Functions affecting configuration of system data.

  Access to functions required to be accessible at level 3 shall be restricted by means of key, password, code or similar access-limiting means or device.
- **Level 4 Access by service personnel or manufacturer**

  Access to component to change system design or to perform system maintenance.

  Access to functions required to be accessible at level 4 shall be restricted by means of key, password, code or similar access-limiting means or device. Access at this level is prevented until access has been permitted by a user at access level 2 or 3.

Table 6 specifies which functions shall be accessible at each access level independently of the security grade:

Table 6 – Level of access

Function	**Access levels**			
	1	**2**	**3**	**4**
System configuration	NP	NP	P	P
Change individual authorisation codes	NP	P	P	P
Assign and delete level 2 users and authorisation codes	NP	NP	P	P
Restoration to factory defaults	NP	NP	P	P
Upgrading of the system	NP	NP	P	P
Start / Stop VSS or component	NP	NP	P	P
Key P Permitted NP Not Permitted.				

6.3.2.4.3 Authorisation

The VSSs shall provide logical or physical means to restrict access to the system or system part(s) with a key, password, code or similar access-limiting means or device.

Permission to gain access to functions of the VSS shall be as specified in Table 7.

Table 7 – Authorisation code requirements

Authorisation code requirement	Security grade			
	1	2	3	4
Number of possible logical authorisation keys		> 10 000	> 100 000	> 1 000 000
Number of possible physical authorisation keys		> 3 000	> 15 000	> 50 000

The passwords of users shall never be displayed or stored in clear text.

A valid change of a password by the user itself shall always require a valid user login with the old one and the entry of the new password plus validation in an identical way.

6.3.2.4.4 Data access

The VSS shall provide methods for controlled access to data taking account of authorisation level according to following Table 8.

Table 8 – Data access

Function	Access Levels			
	1	2	3	4
View live images and data	P	P	P	P
View stored images and data, if recordings are available	NP	P	P	P
View information about storage, if storage is part of the VSS	NP	P	P	P
Print and save video data	NP	P	P	P
Exporting of images and data	NP	P	P	P
Deletion of images and data (only with confirmation)	NP	NP	P	P
Key P Permitted NP Not Permitted.				

6.3.2.4.5 Access to system logs

The VSS shall provide methods for controlled access to system logs taking account of authorisation level according to following Table 9.

Table 9 – Access to system logs

Function	Access Levels			
	1	2	3	4
View system logs	NP	P	P	P
Exporting from logs	NP	NP	P	P
Deletion of logs	NP	NP	NP	NP
Key P Permitted NP Not Permitted.				

6.3.2.4.6 Access to system set-up

The VSS shall provide methods for controlled access to system set-up taking account of authorisation level according to following Table 10.

Table 10 – Access to system set-up

Protection of access to system set-up	**Access Levels**			
	1	**2**	**3**	**4**
Configuration & set-up	NP	NP	P	P
Recovery from system failure	NP	P	P	P
Recovery from tampering	NP	P	P	P
Key P Permitted NP Not Permitted.				

6.3.2.5 Time synchronisation

For security grades 3 and 4 the time settings of various components of a VSS shall always be within ± 10 s of UTC.

NOTE This may be accomplished by verifying the time periodically.

6.3.3 Image and data integrity

6.3.3.1 Data identification

The VSS shall provide methods to identify data taking account of different security grades according to following Table 11.

Table 11 – Data labelling

The VSS shall uniquely label data by	**Security grade**			
	1	**2**	**3**	**4**
Location (e.g. name of site)		X	X	X
Source (e.g. capturing device labelled by camera number)		X	X	X
Date and time	X	X	X	X
Date and time in UTC including offset for local time				X

Date and time shall refer to the time when the image is captured.

NOTE The capture time usually is different from the time when the image is transmitted or stored.

The VSS shall always maintain the original data labels when data is exported.

6.3.3.2 Data authentication

To verify the integrity of images and other data, VSSs of security grades 3 and 4 shall provide a method (e.g. watermarking, checksums, fingerprinting) to authenticate image and meta data and their identity.

NOTE Data authentication is not a requirement to systems of grade 1 and 2.

The authentication method shall be applied at the time the data is recorded and shall notify the user if any of the following has occurred:

- any of the images has been changed or altered;
- one or more images have been removed from a sequence;
- one or more images have been added to a sequence;
- the data label has been changed or altered.

VSSs of security grades 3 and 4 shall also provide a method by which the authenticity of copied and exported data is verified.

The authentication method used shall be specified in the system documentation.

6.3.3.3 Data (manipulation) protection

VSSs of security grade 4 shall provide a method (e.g. encryption) to prevent unauthorized persons viewing the images and other data without permission.

VSSs of security grade 4 shall also provide a method to protect the confidentiality of copied and exported data.

The method used to protect the data confidentiality shall be specified in the system documentation.

6.4 Environmental requirements

6.4.1 VSSs as primary mitigation of the risk

IEC 62599-2 shall be applied to VSSs, where VSS is identified as the primary mitigation of the risk. These VSSs may be used for relevant security and safety applications e.g. as intruder or fire detection systems.

The environmental stability of the VSS shall be of the same level in all grades. The VSS shall operate correctly in the environmental class specified in Clause 7 it is designed for and exposed to EMC conditions described in IEC 61000-6-3, IEC 61000-6-4 and IEC 62599-1:2010. A VSS shall neither change state, suffer damage to components nor substantially change in performance. IEC 62599-1 describes environmental test methods which shall be applied to VSS components.

In 8.3.4 of IEC 62599-2:2010, the requirement of Table 2 ´Voltage reduction of 100 % for a ´Duration of reduction´ of 250 ´no. of periods´ or ´cycles of the voltage wave´ can be covered by VSSs in relevant security applications by the use of UPS.

Functional tests to be applied for component evaluation shall be at least a test or measurement of the essential functions of the component. Acceptance criteria shall be that there is no change in the functioning of the component and no significant change in any measurement, during the environmental testing. A VSS component shall provide protection against electrical shock and consequential hazards by achieving compliance with the requirements of IEC 60950-1 or IEC 60065.

6.4.2 VSSs as secondary mitigation of the risk

If VSSs or parts thereof are not used for relevant security or safety applications e.g. not as intruder or fire detection systems, they shall be compliant to IEC 61000-6-1 or IEC 61000-6-2 and do not need to be compliant to IEC 62599-2.

NOTE 1 The security family standard IEC 62599-2 needs only to be applied to relevant security applications, but not to video systems as auxiliary equipment. In these applications VSS is not identified as the primary mitigation of the risk.

NOTE 2 IEC 61000-6-1 and IEC 61000-6-2 include a lower degree of severity concerning voltage interruptions and a loss of functionality (e.g. image quality reduction) whilst conditioning (details see Clause 4 of IEC 61000-6-1:2005 and IEC 61000-6-2:2005).

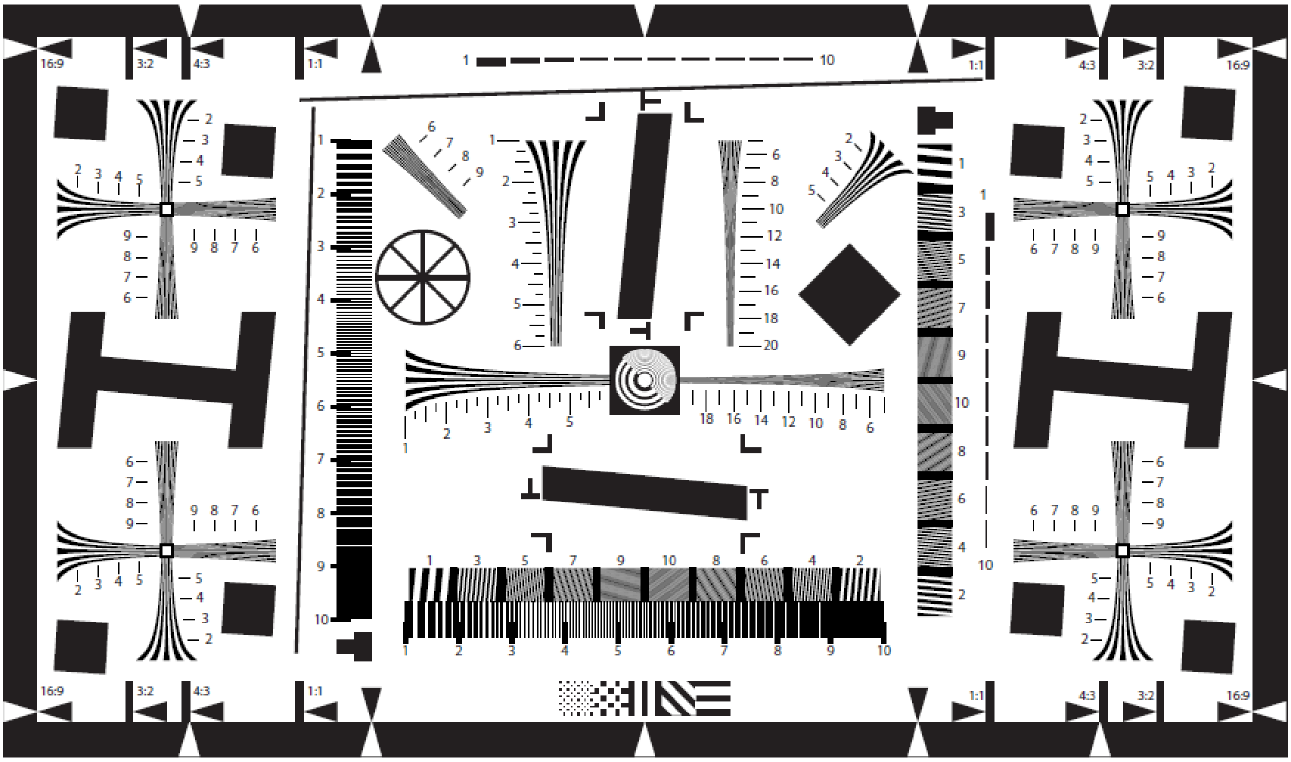
The 8.3.4 of IEC 62599-2:2010, requirement of Table 2 ´Voltage reduction of 100 % for a ´Duration of reduction´ of 250 ´no. of periods´ or ´cycles of the voltage wave´ is only applicable to VSS components, parts or systems in security applications, which are essential for the detection of an intruder, e.g. as part of an intruder detection system. This does not include image display, observation, monitoring, identification or recording of intruders.

6.5 Image quality

VSS shall use components that have been tested according to ISO 12233 to ascertain their maximum resolving power.

NOTE 1 These tests are performed under optimal conditions and may not be reproducible in field conditions. Tests of the installed system are not covered by this standard.

The imaging chain – consisting of image capturing, codec, transmission, handling, storage and display – shall be tested according to 6.1 of ISO 12233:2010 (see Figure 5). The results shall be documented and reported according to Clause 7 of ISO 12233:2010.



IEC 2572/13

Figure 5 – Reference to ISO 12233 resolution measurement chart (unit in ×100 lines)

These tests shall be performed, where the function exists, on each of the live, recorded and exported video and still images. Where multiple record or export settings or formats are available, a representative sample shall be tested and documented, clearly showing which level is associated with which set of parameters.

NOTE 2 In general the level of quality seen on the live view is not consistent through the rest of the imaging chain, for example further compression usually is applied to the video stream in the conversion to a still image exported from the system.

NOTE 3 Testing to ISO 12233 provides a measure of “static” visual resolution only and does not guarantee the visual resolution of a system where scene movement and complexity is random and variable.

7 Environmental classes

7.1 General

Components shall be suitable for use in one of the following environmental classes.

NOTE 1 Classes I, II, III and IV are progressively more severe and therefore, Class IV equipment is allowed for example, be used in Class III applications.

VSS components shall operate correctly when exposed to environmental influences specified in 7.2, 7.3, 7.4 and 7.5.

NOTE 2 The environmental conditions described in Clause 7 are those in which the VSS is expected to perform correctly; they are not necessarily the conditions to be used during the testing of VSS components.

7.2 Environmental Class I – Indoor, but restricted to residential/office environment

Environmental influences normally experienced indoors when the temperature is well maintained.

EXAMPLE In a residential or commercial property.

Temperatures vary in general between +5 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

7.3 Environmental Class II – Indoor – General

Environmental influences normally experienced indoors when the temperature is not well maintained.

EXAMPLE In corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouses where heating is intermittent.

Temperatures vary in general between –10 °C and +40 °C with average relative humidity of approximately 75 % non-condensing.

7.4 Environmental Class III – Outdoor, but sheltered from direct rain and sunshine, or indoor with extreme environmental conditions

Environmental influences normally experienced out of doors when the VSS components are not fully exposed to the weather.

EXAMPLE Temperatures in general vary between –25 °C and +50 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

7.5 Environmental Class IV – Outdoor – General

Environmental influences normally experienced out of doors when the VSS components are fully exposed to the weather.

EXAMPLE Temperatures vary in general between –25 °C and +60 °C/+55 °C including a sunshield with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

NOTE For environments other than above, e.g. on-board systems, additional conditions and requirements may apply.

8 Documentation

8.1 System documentation

Documentation relating to the components of a VSS shall be concise, complete and unambiguous. Information shall be provided sufficient to install, put into operation, operate and maintain a VSS.

System specification and block diagram including specification of configuration:

- installation details for operation and service;
- inspection and maintenance procedures/routines.

8.2 Instructions relating to operation

Instructions relating to the operation of the components of a VSS shall be designed to minimise the possibility of incorrect operation and be structured to reflect the access level of the user.

8.3 System component documentation

Documentation relating to VSS components shall be concise, complete and unambiguous. The documentation shall be sufficient to ensure the correct installation, putting into operation and maintenance of VSS components. Component documentation may be provided by the manufacturer on paper or an alternative medium. Sufficient information shall be provided to ensure the integration of each component with other VSS components. Component documentation shall include the following:

- installation guide / manual;
- technical system data specification:
  - performance specification;
  - min. requirements of equipment;
  - min. requirements of the environment;
  - standard to which component claims compliance;
- inspection & maintenance procedures/routines;
- name of manufacturer or supplier;
- name of system integrator or installer, if appropriate;
- description of equipment;
- name or mark of the certification body (for components which are required to be certified);
- environmental class.

Documentation shall be supplied to the user regarding the retention period of the system. The documentation should also provide the approximate times and methods to export each of the following, where available:

- 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 latency time of the system reaction to a trigger shall be specified in the system documentation

The method of defining the input priorities of alarm triggers shall be provided by the manufacturer in its documentation.

Annex A
(normative)

Special national conditions

Special national condition: National characteristic or practice that cannot be changed even over a long period, e.g. climatic conditions, electrical earthing conditions.

NOTE If it affects harmonization, it forms part of the International Standard.

For the countries in which the relevant special national conditions apply these provisions are normative, for other countries they are informative.

The special national conditions described below shall apply to the following countries: Denmark, Finland, Norway, Sweden, Canada and Russia.

Sub clause	Special national condition
7.5	Environmental Class IV – Outdoor – General: VSS components shall operate correctly when exposed to environmental influences normally experienced out of doors when a VSS components are fully exposed to the weather. Temperatures may be expected to vary between –40 °C and +60 °C with average relative humidity of approximately 75 % non-condensing. For 30 days per year relative humidity can be expected to vary between 85 % and 95 % non-condensing.

Annex B
(informative)

Video export in homeland security systems

In video systems for homeland security or societal security, which offer a video file export according to ISO 22311, Level 2 following requirements are considered:

The exported video file should offer:

1) Compatibility to ISO/IEC 23000-10
2) H.264/MPEG-4 AVC video codec according to ISO/IEC 14496-10
3) Timing information for the synchronization between different image sources (capture time) with an accuracy of 40 ms or better, to allow a frame by frame analysis of multiple views of the same scene in parallel

   In 6.3.2.5 Time synchronisation of various components of a general VSS shall only be within ± 10 s UTC and should be much more accurate for homeland security applications.
4) Information on Codec name and profile, Name of the video files container, resolution, image rate (in ips), and Camera ID should be offered as static data
5) Dynamic Metadata, provided as a real-time stream of XML documents according to 8.3.1 of IEC 62676-1-2 ´XML Documents as Payload´ along with the video, preserving the time information

Bibliography

IEC 62676-2 (all parts), *Video surveillance systems for use in security applications – Part 2: Video transmission protocols*

ISO/IEC 10918-1, *Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines*

ISO/IEC 13818-1, *Information technology – Generic coding of moving pictures and associated audio information: Systems*

ISO/IEC 14496-2, *Information Technology – Coding of audio-visual objects – Part 2: Visual*

ISO/IEC 14496-3, *Information technology – Coding of audio-visual objects – Part 3: Audio*

ISO/IEC 14496-10, *Information technology – Coding of audio-visual objects – Part 10: Advanced Video Coding*

ISO/IEC 14496-14, *Information technology – Coding of audio-visual objects – Part 14: MP4 file format*

ISO/IEC 15444-1, *Information technology – JPEG 2000 image coding system: Core coding system*

ISO/IEC 23000-10, *Information technology – Multimedia application format (MPEG-A) – Part 10: Surveillance application format*

ISO 10918 (all parts), *Information technology – Digital compression and coding of continuous-tone still images*

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

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

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

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.™