IEC 62676-1-1

Edition 1.0 2013-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 1-1: Exigences systèmes – Généralités

IEC 62676-1-1:2013

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62676-1-1

Edition 1.0 2013-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 1-1: Exigences systèmes – Généralités

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XA

ICS 13.320

ISBN 978-2-8322-1157-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 1-1: System requirements – General

FOREWORD

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

International Standard IEC 62676-1-1 has been prepared by IEC technical committee 79: Alarm and electronic security systems.

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

FDIS	Report on voting
79/432/FDIS	79/445/RVD

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

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

The reader's attention is drawn to the fact that Annex A lists all of the "in-some-country" clauses on differing practices of a less permanent nature relating to the subject of this standard.

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

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

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

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

INTRODUCTION

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

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

Part 1: System requirements

Part 2: Video transmission protocols

Part 3: Analog and digital video interfaces

Part 4: Application guidelines (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).

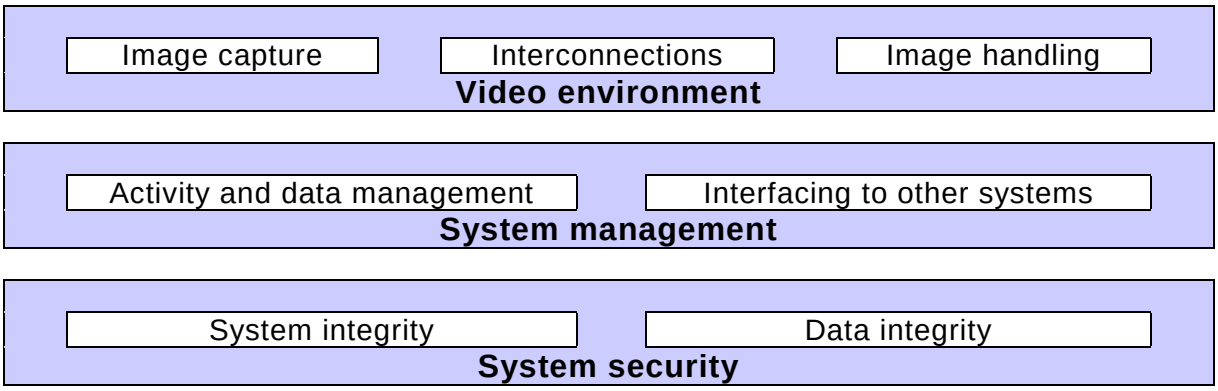


Figure 1 – VSS

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:

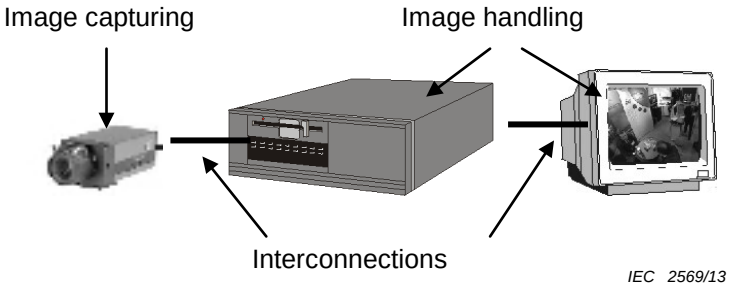


Figure 2 – Example for VSS

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:

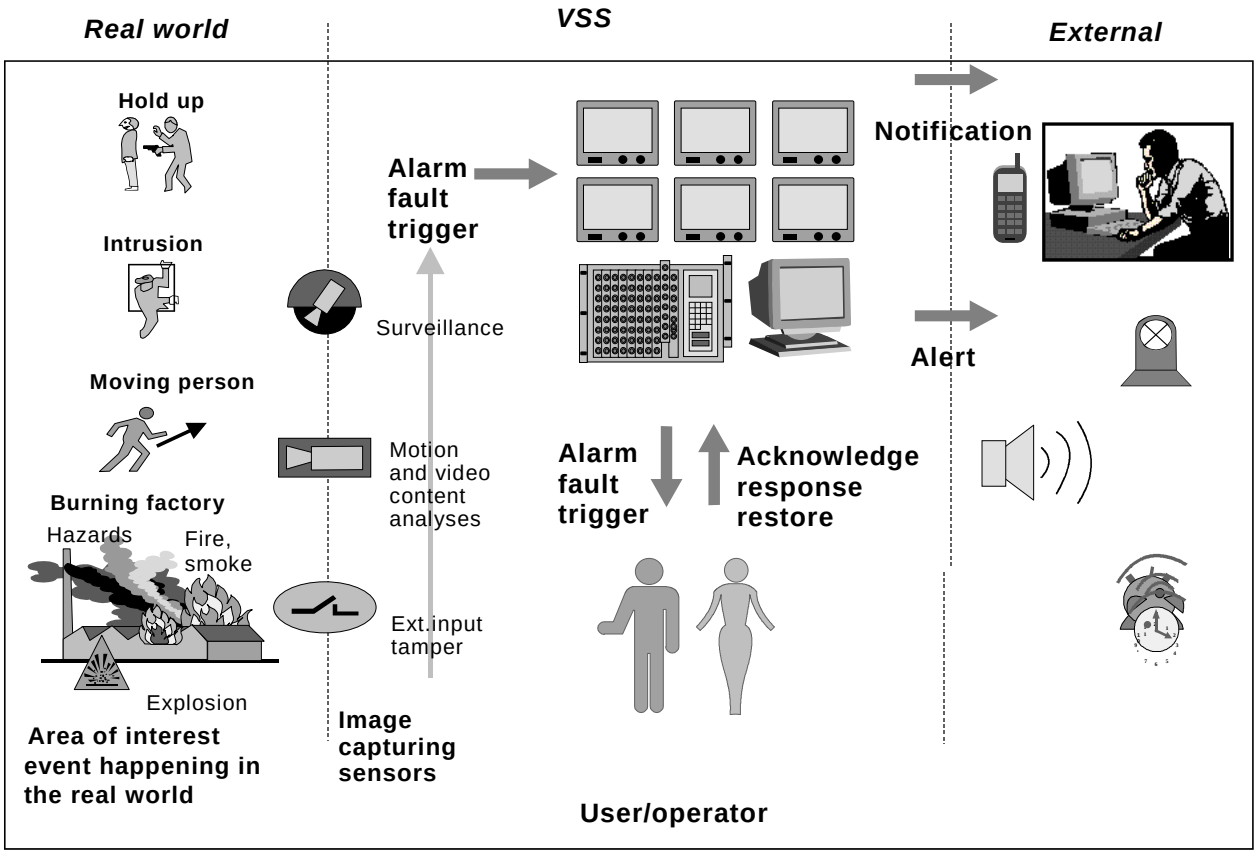


Figure 3 – Activity management

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)

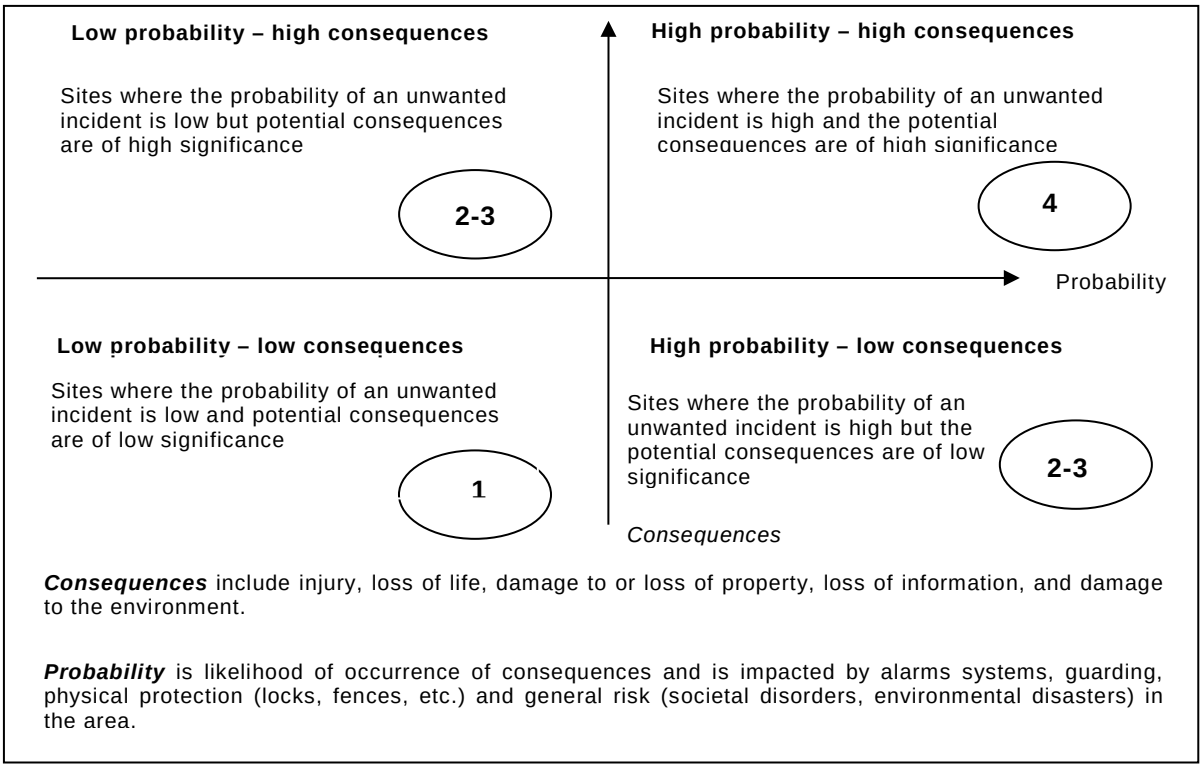
  A VSS intended for surveillance of low to medium risk situations. The VSS has low protection level and low restriction of access.

– 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.



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).

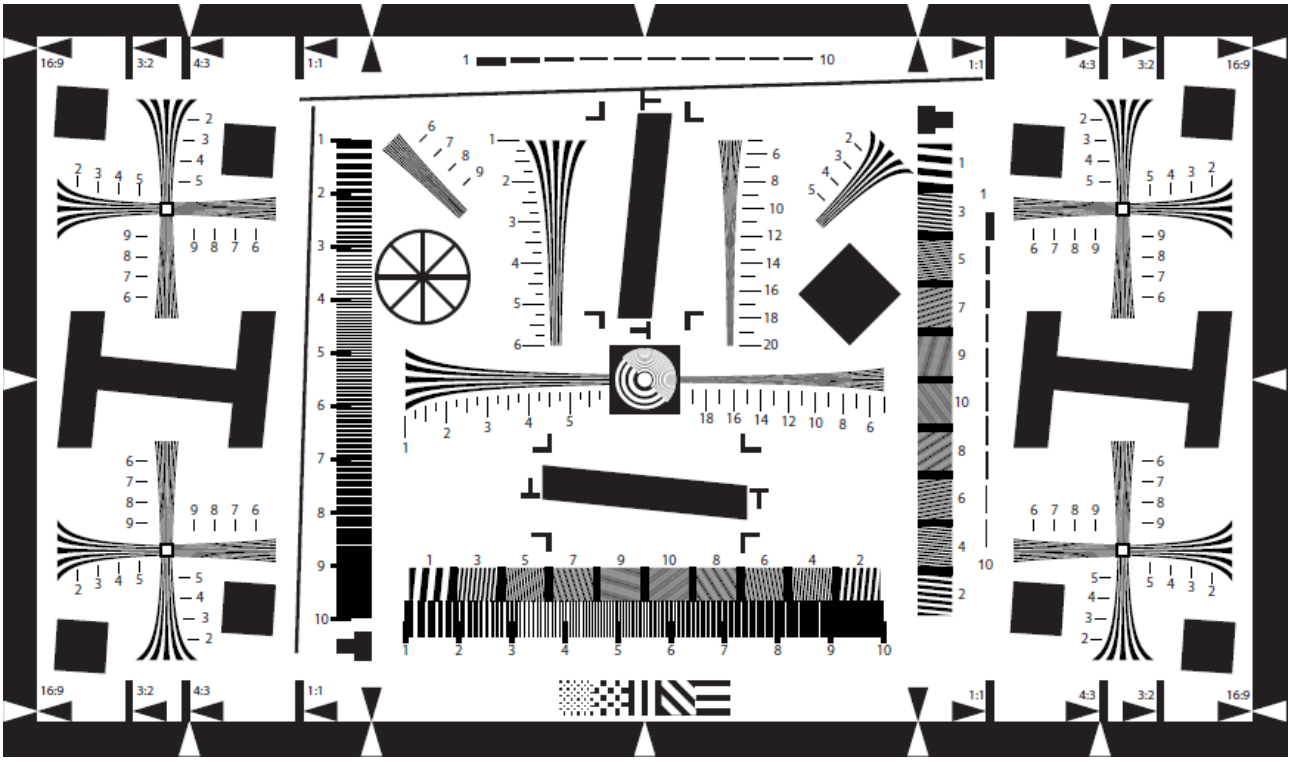
The 8.3.4 of IEC 62599-2:2010, requirement of Table 2 ´Voltage reduction of 100 % for a ´Duration of reduction´ of 250 ´no. of periods´ or ´cycles of the voltage wave´ is only applicable to VSS components, parts or systems in security applications, which are essential for the detection of an intruder, 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*

———————

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –

Partie 1-1: Exigences systèmes – Généralités

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toute divergence entre toute Publication de la CEI et la publication nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62676-1-1 a été établie par le comité d'études 79 de la CEI: Systèmes d'alarme et de sécurité électroniques.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
79/432/FDIS	79/445/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

L'attention du lecteur est attirée sur le fait que l'Annexe A donne une liste de tous les articles traitant des différences de pratiques à caractère moins permanent qui existent dans certains pays sur le sujet couvert par la présente norme.

Une liste de toutes les parties de la série CEI 62676, publiées sous le titre général *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

Le Comité d'études 79 de la CEI en charge des systèmes d'alarme et de sécurité électroniques ainsi que de nombreuses organisations gouvernementales, de laboratoires d'essai et de fabricants de matériel ont défini un cadre commun pour la transmission vidéosurveillance afin de permettre l'interopérabilité entre les produits.

La série de normes CEI 62676 dédiées aux systèmes de vidéosurveillance est divisée en 4 parties indépendantes:

Partie 1: Exigences systèmes

Partie 2: Protocoles de transmission vidéo

Partie 3: Interfaces vidéo analogiques et numériques

Partie 4: Directives d'application (à publier)

Chaque partie propose ses propres articles relatifs au domaine d'application, ainsi qu'aux références, définitions et exigences.

La série CEI 62676-1 comprend 2 sous-parties, respectivement numérotées 1-1 et 1-2:

CEI 62676-1-1, *Exigences systèmes – Généralités*

CEI 62676-1-2, *Exigences systèmes – Exigences de performances pour la transmission vidéo*

Cette première sous-partie de la série CEI 62676-1 s'applique aux systèmes pour la surveillance des zones privées et des zones publiques. Elle comprend quatre grades de sécurité et quatre classes d'environnement.

La présente Norme CEI est destinée aux parties suivantes qui sont concernées par les systèmes de vidéosurveillance (VSS): sociétés, fabricants, intégrateurs de systèmes, installateurs, consultants, propriétaires, utilisateurs, assureurs et organismes chargés de l'application de la loi, et leur fournit une spécification complète et précise du système de surveillance. La présente Norme internationale ne spécifie pas le type de technologie pour une tâche d'observation donnée.

Compte tenu de la diversité des applications des VSS, par exemple, la sécurité, la sûreté, la sécurité publique, les transports, etc., seules les exigences minimales sont couvertes par la présente Norme.

Pour les applications spécifiques, par exemple la sécurité intérieure, il est nécessaire d'appliquer des exigences supplémentaires, qui sont définies dans l'annexe à la présente norme.

La présente Norme CEI n'est pas destinée à être utilisée dans le cadre des essais des composants individuels des VSS.

Actuellement, les VSS équipent les réseaux de sécurité qui utilisent une infrastructure, des équipements et des connexions IT sur le site protégé proprement dit.

SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –

Partie 1-1: Exigences systèmes – Généralités

1 Domaine d'application

La présente partie de la CEI 62676 spécifie les exigences minimales et donne des recommandations pour les systèmes de vidéosurveillance (VSS), appelés jusqu'à présent CCTV, installés pour les applications de sécurité. La présente Norme spécifie les exigences minimales de performances et de fonctionnement à convenir entre le client, les organismes chargés de l'application de la loi, le cas échéant, et le fournisseur dans le cadre des exigences d'exploitation, mais elle n'inclut pas d'exigences pour la conception, la planification, l'installation, les essais, l'exploitation ou la maintenance. La présente Norme exclut l'installation de VSS activés par des détecteurs contrôlés à distance.

La présente Norme CEI s'applique aussi aux VSS qui partagent leurs moyens de détection, de déclenchement, d'interconnexion, de commande, de communication et d'alimentation avec d'autres applications. Le fonctionnement d'un VSS n'est pas perturbé par d'autres applications.

Des exigences sont spécifiées pour les composants VSS lorsque l'environnement correspondant est classifié. Cette classification décrit l'environnement dans lequel le composant VSS est supposé fonctionner conformément à sa conception. Lorsque les exigences des quatre classes d'environnement sont inappropriées en raison des conditions extrêmes qui règnent dans certaines zones géographiques, des conditions nationales particulières peuvent être appliqués (voir Annexe A).

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60065, *Appareils audio, vidéo et appareils électronique analogues – Exigences de sécurité*

CEI 60068-2-75, *Essais d'environnement – Partie 2-75: Essais – Essai Eh: Essais aux marteaux*

CEI 60529, *Degrés de protection procurés par les enveloppes (Code IP)*

CEI 60950-1, *Matériel de traitement de l'information – Sécurité – Partie 1: Exigences générales*

CEI 61000-6-1:2005, *Compatibilité électromagnétique (CEM) – Partie 6-1: Normes génériques – Immunité pour les environnements résidentiels, commerciaux et de l'industrie légère*

CEI 61000-6-2:2005, *Compatibilité électromagnétique (CEM) – Partie 6-2: Normes génériques – Immunité pour les environnements industriels*

CEI 61000-6-3, *Compatibilité électromagnétique (CEM) – Partie 6-3: Normes génériques – Norme sur l'émission pour les environnements résidentiels, commerciaux et de l'industrie légère*

CEI 61000-6-4, *Compatibilité électromagnétique (CEM) – Partie 6-4: Normes génériques – Norme sur l'émission pour les environnements industriels*

CEI 62262, *Degrés de protection procurés par les enveloppes de matériels électriques contre les impacts mécaniques externes (Code IK)*

CEI 62599-1:2010, *Systèmes d'alarme – Partie 1: Méthodes d'essais d'environnement*

CEI 62599-2:2010, *Systèmes d'alarme – Partie 2: Compatibilité électromagnétique – Exigences relatives à l'immunité des composants des systèmes d'alarme de détection d'incendie et de sécurité*

CEI 62676-4, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 4: Directives d'application*[1]

ISO 12233:2000, *Photographie – Appareils de prises de vue électroniques – Mesurages de la résolution*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1.1
niveau d'accès
niveau d'accès à des fonctions particulières du VSS, définissant les droits utilisateur d'un opérateur pour commander et configurer le système, ainsi que l'accès aux données sur le VSS

3.1.2
accuser réception
action d'un utilisateur qui consiste à accepter un message ou une indication

3.1.3
action
manœuvre ou acte délibéré de l'utilisateur qui fait partie de la procédure d'alarme

3.1.4
format de transmission en continu avancé
format de l'enveloppe audionumérique/vidéonumérique propriétaire, spécialement destiné aux modes de transmission en continu

3.1.5
alarme
avertissement de la présence d'un danger pour les êtres vivants, les biens ou l'environnement

---

1 À publier.

3.1.6
condition d'alarme
condition d'un système d'alarme, ou d'une partie de celui-ci, résultant de la réponse du système à la présence d'un danger

3.1.7
message d'alarme
message provenant du système et destiné à un opérateur pour décrire l'heure, le type et l'emplacement d'une alarme

3.1.8
procédure d'alarme
indications et commandes manuelles ou automatiques comme réponse à une condition d'alarme

3.1.9
centre de réception d'alarme
centre occupé en permanence, qui reçoit les informations concernant l'état d'un ou de plusieurs systèmes d'alarme

3.1.10
alerte
avertissement adressé aux personnes pour leur information ou pour demander une intervention (police, personnel de service, par exemple) en réponse à une alarme, une fraude ou un défaut

EXEMPLE: Alerte visuelle, alerte sonore/audible, alerte externe.

Note 1 à l'article: En anglais, le terme "alarm warning" est parfois utilisé à la place du terme "alert".

3.1.11
dispositif de secours
composant de VSS du même type que le dispositif principal

3.1.12
archive
données stockées sur un support non volatil ou volatil à long terme

EXEMPLE: Les CD ou les bandes numériques sont considérés comme des "archives".

3.1.13
zone d'intérêt
région d'une scène surveillée par un dispositif de capture d'image

3.1.14
format d'entrelacement audio vidéo
format multimédia propriétaire dans lequel des données audio et vidéo sont dans une enveloppe normalisée qui permet une lecture synchrone audio-avec-vidéo

3.1.15
authentification
méthode pour vérifier si une image a été altérée

3.1.16
autorisation
permission d'accès à des fonctions ou des composants spécifiques d'un VSS

3.1.17
codes d'autorisation
clés physiques ou logiques permettant l'accès aux fonctions VSS

3.1.18
reconnaissance automatique des plaques minéralogiques
reconnaissance optique de caractères sur des images pour lire et extraire les caractères alphanumériques des plaques d'immatriculation des véhicules

3.1.19
caisse automatique
appareil assurant un mode de transaction financière dans un espace public sans besoin de l'intervention d'un interlocuteur humain

3.1.20
matériel auxiliaire
système vidéo non utilisé comme mesure d'atténuation principale du risque

3.1.21
image de sauvegarde
réplique précise et complète d'une image primaire quel que soit le support

3.1.22
débit
(concernant l'interconnexion) débit de transfert de données ou quantité de données qui peut être transférée d'un point à un autre en un temps donné

Note 1 à l'article: Le débit est donné en bits par s.

3.1.23
capacité
(concernant l'enregistrement) quantité totale d'informations stockées qu'un support ou un moyen de stockage peut contenir.

Note 1 à l'article: Elle est exprimée comme une quantité de bits ou d'octets.

3.1.24
VSS
système comprenant une caméra, un dispositif de stockage, un équipement de surveillance et associé à des fins de transmission et de commande

Note 1 à l'article: Les systèmes CCTV sont inclus dans le terme plus général "VSS".

3.1.25
voie
chemin unique pour transporter des données numériques ou analogiques, distinct d'autres chemins parallèles

EXEMPLE: Voie d'entrée ou de sortie vidéo.

3.1.26
somme de contrôle
valeur unique ou clé calculée par un algorithme pour un paquet de données, fondée sur les informations qu'il contient

Note 1 à l'article: Elle est transférée avec les données pour authentifier que les données n'ont pas été falsifiées. Toute modification des données d'image, des métadonnées ou de la séquence d'images causerait une modification de la somme de contrôle qui en résulte.

3.1.27
compression
processus de réduction de la taille d'un fichier de données (image)

3.1.28
taux de compression
rapport de la taille non compressée d'un fichier ou d'une image avec sa taille compressée

Note 1 à l'article: Un taux de compression élevé signifie des fichiers images plus petits et une qualité d'image inférieure et inversement.

3.1.29
interconnexion commune
interconnexion utilisée par plusieurs voies vidéo et de données et/ou d'autres applications

3.1.30
communication
transmission de messages et/ou de signaux entre les composants VSS

3.1.31
composant
partie fonctionnelle du VSS

3.1.32
continuellement
d'une manière récurrente et fréquente à intervalles réguliers

3.1.33
contraste
(lié à l'image) différence dans les propriétés visuelles qui permet de distinguer un objet (ou sa représentation dans une image) d'autres objets et du fond

Note 1 à l'article: Dans la perception visuelle du monde réel, le contraste est déterminé par la différence de couleur et de luminosité de l'objet et des autres objets dans le même champ de vision.

3.1.34
donnée
image, métadonnée et autre donnée du VSS

3.1.35
acquisition de données
échantillonnage d'informations pour générer des données en traitant des signaux avec des capteurs appropriés convertissant le paramètre de mesure en un signal

3.1.36
sauvegarde des données
processus de copie des données permettant de récupérer l'enregistrement original en cas de perte ou d'endommagement de l'enregistrement original

3.1.37
base de données
collection structurée d'enregistrements ou de données. Les enregistrements sont extraits en réponse à des requêtes

3.1.38
identification de données
capacité à trouver, extraire ou supprimer des données spécifiques sans ambiguïté, par exemple, en utilisant des ID uniques

3.1.39
intégrité des données
condition d'une donnée qui n'a pas été modifiée ou altérée par rapport à sa source, que ce soit par malveillance ou de manière accidentelle et dans laquelle les données sont maintenues pendant toute opération, comme la transmission, le stockage et l'extraction, de manière à les préserver pour leur usage prévu

3.1.40
gestion des données
gestion des actions utilisateur, des données audio/vidéo et des informations générales qui ne font pas partie de la gestion d'activité

3.1.41
protection contre la manipulation des données
moyen pour garantir l'intégrité des données

EXEMPLE: Manipulation de données certifiées, encryptage, tatouage numérique et accès limité aux données.

3.1.42
défaut (par)
réglages de paramètres stockés dans un matériel par le fabricant, qui peuvent remplacer les réglages configurés durant la mise en service ou lors d'un usage ultérieur

3.1.43
décryptage
processus de modification de données cryptées en données simples à l'aide d'un algorithme et d'une clé cryptographiques

3.1.44
image numérique
image constituée de pixels utilisant des plages de valeurs discrètes

3.1.45
enregistreur vidéo numérique
système qui est capable d'enregistrer, de lire, de sauvegarder et d'exporter des images numériques capturées par des sources d'image.

Note 1 à l'article: Un enregistreur vidéo sur réseau est inclus dans cette définition.

3.1.46
documentation
(liée au système) fascicule papier (ou autre support) préparé au cours de la conception, de l'installation et du transfert des détails d'enregistrement système du VSS

Note 1 à l'article: La documentation d'un composant peut être fournie par le fabricant sur papier ou sur un autre support.

3.1.47
surveillance électronique d'articles
technologie destinée à empêcher le vol à l'étalage, par exemple, dans les magasins de détail

3.1.48
encryptage
transformation cryptographique des données qui occulte la signification d'origine de ces dernières afin qu'elles ne soient pas identifiées ou utilisées

3.1.49
intervalle équidistant
intervalle de temps constant, lors de l'échantillonnage des valeurs d'un signal continu

3.1.50
fonctions essentielles
fonctions vitales d'un VSS, que sont la capture, la transmission, l'enregistrement et/ou la présentation d'images

3.1.51
évènement
incident dans le monde réel

EXEMPLE: Un incendie (maison en feu), une intrusion (porte cassée) ou une personne en mouvement, une coupure d'électricité, un court-circuit, la présence d'un intrus.

3.1.52
action entraînée par l'évènement
activité d'un utilisateur ou d'un système entraînée par un signal d'alarme ou de déclenchement

3.1.53
enregistrement d'évènement
enregistrement contrôlé d'évènement ou stockage de signaux d'image pendant un temps prédéterminé

3.1.54
copie exacte
transfert de données de l'emplacement d'enregistrement original ou de copie originale vers un stockage secondaire; en technologie numérique, copie bit à bit

3.1.55
export
transfert de données de l'emplacement original vers un emplacement de stockage secondaire avec un minimum de modifications nécessaires

3.1.56
entrée externe
source externe connectée à une entrée dédiée sur le VSS

3.1.57
interconnexion externe
interconnexions échangeant des données au-delà de la limite du système

3.1.58
système externe
VSS recevant et envoyant des informations et des signaux de commande, mais ne fournissant pas de fonctions VSS

3.1.59
basculement
capacité de commuter automatiquement vers un composant ou un système redondant ou de secours, en cas de défaillance ou d'arrêt anormal d'un composant ou d'un système précédemment actif

3.1.60
sécurité intrinsèque
fonction ou méthode qui assure qu'une défaillance d'un équipement, d'un processus ou d'un système ne se propage pas au-delà des environs immédiats de l'entité qui a connu une défaillance

EXEMPLE: Appareil ne causant aucun dommage ou sinon un dommage minimal à d'autres appareils ou ne présentant pas de danger pour le personnel en cas de défaillance ou d'erreur de la part de l'opérateur.

Note 1 à l'article: Un système à sécurité intrinsèque a été conçu de telle manière que la probabilité d'une défaillance dans l'accomplissement de sa mission assignée soit très faible quels que soient les facteurs d'environnement.

3.1.61
défaut
condition du VSS sur un ou plusieurs composants ou interconnexions qui empêche le VSS ou une partie de celui-ci de fonctionner normalement

3.1.62
message de défaut
message provenant du système et destiné à un opérateur pour décrire l'heure, le type et l'emplacement d'un défaut

3.1.63
empreinte digitale
méthode de génération d'une 'empreinte digitale' unique de l'image originale enregistrée qui ne peut pas être reproduite si l'image est altérée

3.1.64

format d'échange graphique
format d'image bitmap 8 bits par pixel

3.1.65
danger
incident que le VSS est conçu pour détecter

EXEMPLE: Fumée ou mouvement.

3.1.66
éclairage
(lié à l'appareil d'imagerie) niveau d'éclairage (éclairement) au niveau du capteur de l'appareil d'imagerie;

(lié à la scène) niveau d'éclairage (éclairement) sur la zone à maintenir sous surveillance

3.1.67
image
représentation visuelle d'une scène visualisée par une caméra

Note 1 à l'article: Dans ce document, le terme image inclut les images multiples dans un flux d'images.

3.1.68
analyse d'image
extraction d'informations quantitatives d'une image permettant une exploitation facile par examen visuel

3.1.69
capture d'images
transformation d'images provenant d'un dispositif optique ou à balayage en signaux vidéo ou en format de donnée numérique

3.1.70
taux d'image
nombre d'images par seconde

3.1.71
chaîne de formation d'images
composants et fonctions qui affectent la qualité d'image et qui consistent à capter, coder, interconnecter, transmettre, manipuler, stocker, décoder et afficher des images

3.1.72
manipulation d'image
toute activité qui transforme une image d'entrée en image de sortie avec aussi peu de modifications que possible

3.1.73
traitement d'image
méthode consistant à modifier ou analyser des images (numériques) avec des algorithmes ou des procédures (logicielles)

EXEMPLE: Compression et encryptage d'images, méthodes pour l'analyse du contenu d'image.

3.1.74
scène d'image
collecte d'informations visuelles de la zone physique dans la largeur du capteur d'images où quelque chose se passe (incident ou évènement)

3.1.75
séquence d'images
groupe linéaire d'images manipulées comme une entité, généralement indexées dans le temps

3.1.76
source d'image
appareil qui délivre des données vidéo

3.1.77
flux d'image
série d'images consécutives issues de la même source d'image, qui sont transmises d'un composant du système à un autre

3.1.78
qualité d'image
mesure de l'approche de représentation précise d'un objet réel par une image observée, par l'association de la netteté, de la luminosité, de la reproduction des couleurs, de la résolution visuelle, de l'uniformité de l'éclairage, du contraste, de la géométrie, etc.

3.1.79
incident
événement ou activité présentant un intérêt, que le VSS est destiné à visualiser ou enregistrer et qui peut nécessiter une réaction de la part d'un opérateur

3.1.80
signalisation
information (sonore, visuelle ou sous toute autre forme) fournie pour assister l'utilisateur dans le fonctionnement d'un VSS

3.1.81
répétition de lecture instantanée
lecture d'images enregistrées peu de temps auparavant à partir des informations stockées

EXEMPLE: Lecture d'une séquence d'images immédiatement après un incident ou un évènement.

3.1.82
interconnexions
support par lequel les messages et/ou les signaux sont transmis entre les composants du VSS

3.1.83
JPEG
norme communément utilisée pour la compression des images, définie par le Joint Photographic Experts Group

EXEMPLE: Un CRT standard a un facteur de Kell de 0,7 pour les images NSTC avec une résolution visuelle verticale de 338 lignes (483 × 0,7) et une image PAL de 403 lignes (576 × 0.7).

Note 1 à l'article: Le format de fichier JPEG est donné par la série ISO 10918.

3.1.84
temps de latence
délai qui s'écoule entre l'initiation d'une requête et l'effet exigé de la requête

3.1.85
écran à cristaux liquides
dispositif d'affichage mince et plat constitué d'un nombre quelconque de pixels en couleur ou monochromes regroupés devant une source de lumière ou un réflecteur

3.1.86
donnée d'identification de l'emplacement
donnée qui identifie de façon unique l'emplacement physique d'un dispositif

3.1.87
code de clé d'autorisation logique
codes numériques ou alphabétiques entrés par un utilisateur autorisé pour avoir accès à des fonctions ou à des parties protégées du VSS

3.1.88
clé
objet avec un code mécanique, logique ou électronique qui libère un mécanisme de verrouillage pour transformer des données cryptées en données originales

3.1.89
copie originale
sauvegarde d'une copie identique de l'enregistrement original, dans les systèmes numériques, copie exacte bit à bit

3.1.90
temps de stockage maximal
délai de conservation ou durée spécifiée pendant laquelle il est nécessaire de maintenir les images dans un support de stockage principal

3.1.91
métadonnée
toute information secondaire ou donnée associée à des images dans un VSS

EXEMPLE: Heure et date, chaînes de texte, donnée d'identification de l'emplacement, information sonore et toute autre information associée, liée ou traitée.

3.1.92
contrôle
(lié à la condition du composant) processus de vérification que les interconnexions et les composants fonctionnent correctement;

(lié à l'activité de l'opérateur) visualisation d'images en direct pour détecter les évènements ou les incidents

3.1.93
MPEG
norme communément utilisée pour le codage et la compression des images animées, définie par le Moving Picture Experts Group en différentes versions

EXEMPLE: A titre d'exemples, on peut citer MPEG-2 et MPEG-4.

3.1.94
multiplexeur
dispositif de commutation assurant la représentation simultanée ou séquentielle de plusieurs flux de données, vidéo audio, etc. via un seul support de transmission

3.1.95
fonctionnement normal
état du VSS hors procédures de mise sous tension ou hors tension et en l'absence de défaut

3.1.96
application de sécurité non pertinente
système de sécurité non utilisé comme mesure d'atténuation principale du risque

3.1.97
notification
transmission d'une alarme ou d'un message du VSS à un système externe

3.1.98
masque d'objet
moyen de marquer un objet de la zone considérée dans l'affichage de l'image de la caméra

3.1.99
obscurcissement
processus dont le but est d'empêcher l'appareil d'imagerie de visualiser toute partie de la zone considérée d'une autre manière qu'en déplaçant l'appareil

3.1.100
exigence d'exploitation
document clé pour les concepteurs de systèmes, qui définit clairement les paramètres d'exploitation du VSS conformément aux attentes convenues

3.1.101
opérateur
individu (un utilisateur) autorisé à utiliser un VSS pour son usage prévu

3.1.102
journal de l'opérateur
journal système des évènements et des opérations qui ont été pris en compte dans une station de travail ou par un opérateur donné

3.1.103
enregistrement original
première occurrence d'images non modifiées dans un stockage en ligne permanent, image primaire ou originale stockée sur le support adapté pour le stockage à long terme

3.1.104
clé d'autorisation physique
élément utilisé par un utilisateur autorisé pour accéder à des fonctions ou des parties protégées d'un VSS (clé mécanique, carte magnétique, jeton électronique ou analogue)

3.1.105
taille de stockage physique
taille de support de stockage exprimée dans son unité caractéristique

EXEMPLE: Pour les octets des supports numériques, on utilise les gigaoctets (GB) ou les téraoctets (TB).

3.1.106
image
image

3.1.107
pixel
plus petit élément possible d'une image

Note 1 à l'article: Acronyme pour élément d'image.

3.1.108
lecture
visualisation d'images préalablement enregistrées à partir des supports de stockage

3.1.109
donnée relative au point de vente
donnée générée par le terminal d'un point de vente

3.1.110
alimentation
partie du VSS qui l'alimente en énergie électrique

3.1.111
présentation
fonction d'un VSS qui affiche les images et les données pour l'utilisateur

3.1.112
source d'alimentation principale
source d'alimentation utilisée pour maintenir un VSS dans des conditions normales de fonctionnement

3.1.113
image primaire
fait référence à la première fois où une image est enregistrée sur un support

3.1.114
stockage principal
stockage utilisé pour les données qui ne sont pas utilisées de manière active et qui ne sont pas volatiles pour la préservation des informations stockées, par exemple, pour une extraction ultérieure ou en cas de coupure d'alimentation

3.1.115
masquage de confidentialité
caviardage ou zones obscurcies d'une image pour des raisons de confidentialité

3.1.116
protégé
maintenir et éviter la suppression d'images stockées, dans leur état original, pendant plus longtemps que le temps de conservation prévu

3.1.117
ensemble redondant de disques indépendants RAID 5
architecture de stockage de données qui divise et duplique des données sur plusieurs disques durs de sorte que la défaillance d'un disque ne provoque pas la perte des données enregistrées

3.1.118
application de sécurité pertinente
système de sécurité utilisé comme mesure d'atténuation principale du risque

3.1.119
restaurer (une alarme)
action d'un utilisateur qui consiste à modifier l'état d'un sous-système ou d'un détecteur en le basculant de la condition d'alarme, de défaut ou de fraude dans la condition antérieure

3.1.120
défaillance répétitive
signaux qui se répètent et se dupliquent rapidement pour une raison qui ne peut pas être identifiée et qui provoquent des messages supplémentaires ou involontaires pour la même condition de défaut

3.1.121
télécommande
exploitation d'une station à distance reliée par des interconnexions externes qui ne font pas partie du VSS

3.1.122
résolution (format)
description de la taille d'une image numérique en pixels, par exemple 720P, 1080P, 640X480 etc. pixels/pouce ou nombre de pixels d'une trame vidéo, d'un appareil de contrôle ou d'une impression

résolution visuelle – mesure de la capacité d'une caméra ou d'un système vidéo à définir et reproduire un détail de la scène ou de l'image originale

Note 1 à l'article: Les mesures sont généralement données en pixels/pouce, la hauteur et la largeur en pixels, le nombre total de pixels, etc.

3.1.123
vitesse d'enregistrement
taux d'image pour une voie d'entrée ou un appareil d'enregistrement complet

3.1.124
informations enregistrées
toute donnée enregistrée sur un support d'enregistrement quel qu'il soit (par exemple, électronique, magnétique ou optique) contenant des informations des évènements et des scènes prises par les caméras dans le passé

3.1.125
redondance
méthodes pour protéger un système contre les défaillances de composants en doublant les éléments qui assurent le fonctionnement de façon autonome en cas de défaillance

EXEMPLE: Les systèmes redondants ou à sécurité intrinsèque continuent à fonctionner automatiquement avec un deuxième composant lorsque le composant principal connaît une défaillance. Pour la communication redondante, le système bascule automatiquement sur la deuxième voie de communication si la première ne donne pas de réponse.

3.1.126
centre de réponse vidéo à distance
mode de fonctionnement qui prévoit une présence permanente de personnel et qui peut recevoir plusieurs images VSS simultanément en provenance de sites distants pour interagir avec un ou plusieurs sites et offrir des services de sécurité et associés

3.1.127
station distante
poste de commande secondaire ou auxiliaire éloigné du VSS ou des locaux protégés

3.1.128
répétition de lecture
lecture d'images enregistrées provenant du stockage

3.1.129
réponse
toute commande de contrôle, toute modification des conditions du système ou toute information vers les dispositifs externes ou les personnes émanant d'alarmes, de défauts, de messages ou de déclenchements

3.1.130
temps de réponse
temps mis par un système ou une unité fonctionnelle pour réagir à une entrée donnée

EXEMPLE: Le temps de réponse d'un appareil de signalisation est le temps mis par un pixel pour passer d'actif (noir) à inactif (blanc) ou à de nouveau actif (noir). Il est mesuré en ms.

3.1.131
risque
probabilité, combinée aux conséquences, de dommages liés à la perte ou de détérioration

3.1.132
luminosité de la scène
luminosité observée de la scène, dépendant de son éclairage

3.1.133
support de stockage secondaire
support de stockage séparé de l'emplacement d'enregistrement d'origine

3.1.134
partie prenante
tout individu, tout groupe ou toute organisation susceptible d'être affecté, ou de se considérer comme affecté, par le risque

3.1.135
stockage
moyens utilisés pour stocker des données ou des vidéos en vue d'une utilisation ou d'une extraction future

EXEMPLE: Disque dur, disque dur à mémoire flash, CD, DVD.

3.1.136
support de stockage
moyen pour stocker des données pour une extraction, une visualisation ou un traitement ultérieur

3.1.137
sous système
partie d'un VSS située dans une partie clairement définie des locaux contrôlés et pouvant fonctionner indépendamment

3.1.138
surveillance
observation ou contrôle de personnes ou de locaux à des fins de sécurité au moyen de systèmes d'alarme, de VSS ou d'autres méthodes de surveillance

3.1.139
configuration du système
méthodes pour spécifier un VSS selon la structure de ses éléments, la manipulation des données, les fichiers journaux, les capacités de stockage des données, les niveaux d'accès utilisateur et les capacités de commande utilisateur

3.1.140
données système
paramètres de configuration du système

3.1.141
intégrité du système
capacité d'une application à fonctionner comme prévu et mesure de l'immunité aux influences qui pourraient affecter le fonctionnement normal

3.1.142
journal système
liste chronologique des évènements ou des opérations qui se sont produits dans le VSS et qui permet la reconstruction d'une activité antérieure et qui enregistre les attributs d'une modification (comme la date/l'heure, l'opérateur)

EXEMPLE: Un livre d'enregistrement ou son équivalent électronique dans lequel tous les détails applicables du VSS, son fonctionnement, ses performances et sa maintenance peuvent être entrés de manière sûre pour une extraction ultérieure par des utilisateurs autorisés.

3.1.143
gestion du système
configuration et commande du VSS, ainsi que l'administration des données et des composants du système

3.1.144
sécurité du système
protection du système contre les défaillances comme les fraudes, les accès illégaux, le vandalisme. Accès physique ou électronique contrôlé au VSS ou à tout composant pour empêcher un accès non autorisé.

3.1.145
réglage du système
configuration du système

3.1.146
fraude
modifications non autorisées dans le système, par exemple, un accès physique non autorisé pour contourner le système ou des parties de celui-ci

3.1.147
synchronisation temporelle
méthode manuelle ou automatique pour maintenir l'intégrité de l'heure et de la date entre différents composants du VSS, y compris les changements d'heure liés aux économies d'énergie

3.1.148
lignes de trajectoire
moyens utilisés pour marquer les emplacements de passage d'un objet mobile dans la zone considérée de l'affichage d'image

3.1.149
déclenchement
signal en réaction à un évènement pour activer une fonction ou un dispositif

EXEMPLE: Personne se déplaçant détectée sur un appareil d'enregistrement.

3.1.150
action de l'utilisateur
entrée réalisée délibérément par un opérateur dans le système pour surveiller, contrôler le système ou modifier les conditions

EXEMPLE: Bascule la caméra × sur le moniteur y.

3.1.151
interface utilisateur
moyen par lequel un utilisateur fait fonctionner un VSS

3.1.152
analyse du contenu vidéo
analyse de vidéo en direct ou de vidéo enregistrée pour détecter les activités, les évènements ou les types de comportement tels qu'ils sont définis dans les exigences d'exploitation

3.1.153
perte vidéo
absence de signal vidéo provenant d'un dispositif de capture

3.1.154
matrice vidéo
unité pour connecter plusieurs signaux vidéo d'entrée sur plusieurs sorties

3.1.155
enregistreur vidéo
appareil pour enregistrer et lire des vidéos

3.1.156
détection de mouvement vidéo
algorithme, procédure ou dispositif pour générer une condition d'alarme en réponse à une modification définie du contenu d'une séquence d'images donnée

3.1.157
opération de tatouage numérique
informations placées dans une image numérique pour vérifier son authenticité et son intégrité sans affecter le contenu visible de l'image

3.1.158
station de travail
station de commande exploitée par l'utilisateur

3.2 Abréviations

ANPR Automatic Number Plate Recognition (Reconnaissance automatique des plaques minéralogiques)

ARC Alarm Receiving Centre (Centre de réception d'alarme)

ASF Advanced Streaming Format (Format de transmission en continu avancé)

ATM Automatic Teller Machine (Caisse automatique)

AVC Advanced Video Coding (Codage vidéo avancé)

AVI Audio Video Interleave Format (Format d'entrelacement audio vidéo)

B/W Black/White (Blanc/Noir)

CCD Charge Coupled Device (Dispositif à transfert de charge)

CD Compact Disc (Disque compact)

CEM Compatibilité électromagnétique

CRT Cathode ray tube (Tube cathodique)

DVD Digital Versatile Disk (disque numérique polyvalent)

EAS Electronic article surveillance, anti-shoplifting system (Surveillance électronique d'articles, système contre le vol à l'étalage)

FPS Frames Per Second (Trames à la seconde/taux de trames)

GIF Graphics Interchange Format (Format d'échange graphique)

ID Identificateur

IP Ingress Protection Ratings (Caractéristiques assignées de protection contre la pénétration)

IPS Images Par Seconde (Taux d'image)

ISO Organisation Internationale de Normalisation

JPEG Joint Photographic Experts Group

LCD Liquid Crystal Display (Ecran à cristaux liquides)

MPEG Moving Picture Experts Group

OR Operational Requirement (Exigence d'exploitation)

POS Point Of Sales (Point de vente)

RAID Redundant Array of Independent Disks (Ensemble redondant de disques indépendants)

RVRC Remote Video Response Centre (Centre de réponse vidéo à distance)

SNR Signal to Noise Ratio (Rapport signal sur bruit)

UPS Uninterruptable Power Supply (Alimentation sans coupure)

UTC Universal Time Coordinated (Temps universel coordonné)

VCA Video Content Analysis (Analyse du contenu vidéo)

VMD Video Motion Detection (Détection de mouvement vidéo)

VSS Video Surveillance System (Système de vidéosurveillance)

4 Description fonctionnelle du VSS

4.1 VSS

Cet Article 4 est informatif.

Un VSS se compose généralement d'équipements qui contiennent des dispositifs analogiques et numériques ainsi que des logiciels. Puisque la technologie et, avec elle, les équipements

VSS et leurs fonctionnalités se développent et se modifient très rapidement, les appareils individuels et leurs exigences ne sont pas définis. Au lieu de cela, le présent article définit et décrit le VSS comme des unités fonctionnelles ainsi que les relations qui existent entre elles.

Un VSS pour des applications de sécurité peut être présenté comme un ensemble de blocs fonctionnels qui représentent les différentes parties et fonctions du système (voir Figure 1).

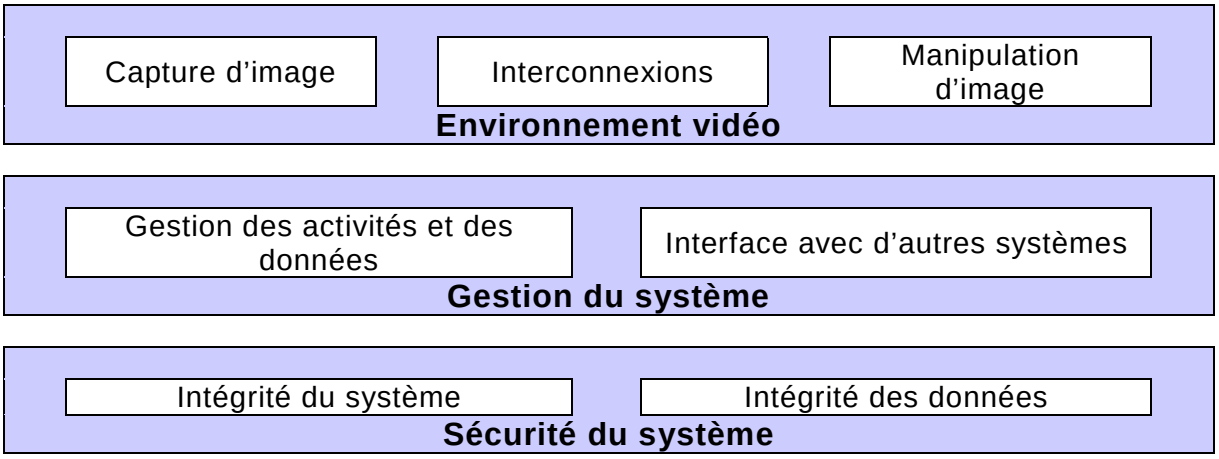


Figure 1 – VSS

4.2 Environnement vidéo

4.2.1 Généralités

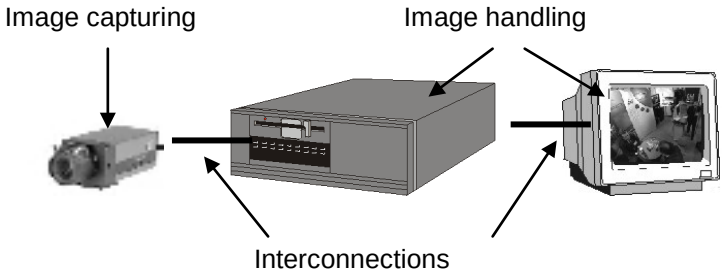
Un VSS est destiné à capturer des images d'une scène, à les manipuler et à les afficher pour un opérateur, avec des informations associées pour une utilisation facile et efficace. L'ensemble qui se compose d'appareils VSS et d'interconnexions entre les appareils peut être décrit comme l'**environnement vidéo**.

Au lieu de définir les appareils réels qui forment le VSS, l'environnement vidéo est défini ici avec trois fonctions:

- génération d'images vidéo (**capture d'image**);
- transmission et routage d'images vidéo et de signaux de commande (**interconnexions**); et
- présentation, stockage et analyse d'images (**manipulation d'images**).

Les fonctions mentionnées ci-dessus peuvent se trouver dans différents composants matériels et logiciels du système. Noter que ces fonctions ne sont pas nécessairement toujours réparties sur plusieurs appareils individuels car plusieurs fonctions peuvent être assurées par un même appareil. A titre d'exemple, un appareil constitué d'une caméra réseau peut capturer l'image (capture d'image), la stocker temporairement (manipulation d'image), l'analyser avec un VMD (traitement d'image) et la transmettre via le réseau (interconnexions). A l'inverse, plusieurs appareils d'un même système peuvent assurer la même fonction.

La Figure 2 montre un exemple pratique simple d'environnement vidéo:



Légende

Anglais	Français
Image capturing	Capture d'image
Image handling	Manipulation d'image
Interconnections	Interconnexions

Figure 2 – Exemple de VSS

4.2.2 Capture d'image

La capture d'image consiste à générer et à fournir une image du monde réel sous un format qui peut être utilisé par le reste du VSS.

La capture d'image est destinée à générer une image de la scène pour un traitement ultérieur par le VSS. Une source d'image capture une image de la scène, crée des données d'image et fournit ces données à la fonctionnalité de manipulation d'image en utilisant les interconnexions du système. Les données d'image peuvent être en format analogique (par exemple, vidéo composite) ou numérique (par exemple, JPEG, MPEG-4).

4.2.3 Interconnexions

Les interconnexions décrivent l'ensemble des transmissions de données à l'intérieur de l'environnement vidéo. Ceci inclut deux fonctions: **connexions** et **communications**.

Les communications décrivent tous les signaux de données vidéo et de commande qui sont échangés entre les composants du système. Ces signaux peuvent être analogiques ou numériques.

Les connexions couvrent les supports utilisés pour les signaux de communication. Les connexions sont par exemple les câbles (par exemple, à paire torsadée, coaxial ou à fibre optique), les réseaux numériques, les transmissions sans fil, ainsi que les matériels, par exemple, multiplexeur ou matrice vidéo.

Un VSS peut être divisé en plusieurs composants qui communiquent par des interconnexions qui ne lui sont pas dédiées. Un exemple de ce cas est celui d'un réseau qui est partagé avec d'autres applications.

4.2.4 Manipulation d'image

4.2.4.1 Généralités

Les fonctions de manipulation d'image incluent l'**analyse**, le **stockage** et la **présentation** d'une image ou d'une séquence d'images. Les mêmes fonctions peuvent aussi être

appliquées à d'autres données (par exemple, flux audio) et à des métadonnées. Un VSS ne contient pas nécessairement toutes ces fonctions.

La manipulation d'image peut être réalisée par un ou plusieurs appareils qui constituent le VSS (par exemple, moniteurs, enregistreurs, analyseurs d'images, caméras intelligentes et stations de travail distantes). Un appareil peut également traiter plusieurs tâches de manipulation d'images (par exemple, enregistreur vidéonumérique).

Au cours de la manipulation, les images peuvent être modifiées, par exemple, leur résolution, leur taux d'image et leur compression.

4.2.4.2 Analyse

Les données vidéo qui constituent les images peuvent être analysées pour extraire des informations des données directes ou des données vidéo enregistrées. En plus des données vidéo, la fonction d'analyse peut aussi utiliser d'autres données (par exemple, flux audio) ou métadonnées comme entrées.

L'analyse peut être utilisée pour plusieurs usages:

- prouver l'intégrité du système (par exemple, la position de la caméra);
- interpréter la scène capturée (par exemple, reconnaissance automatique des plaques minéralogiques);
- détecter un évènement susceptible de déclencher une alarme (par exemple, personne en mouvement ou détection de fumée).

4.2.4.3 Stockage

Les données des images vidéo (ainsi que les autres données ou les métadonnées) peuvent être stockées sur un support de stockage (par exemple, magnétique, optique, électronique) pour une extraction ultérieure. La première manifestation d'une image sous une forme persistante et finale est appelée ´donnée d'image originale´ ou ´enregistrement original´. Les données stockées peuvent être en format analogique ou numérique. Des copies précises peuvent être faites des données numériques, elles sont appelées ´originaux´. Le transfert d'images de l'enregistrement et de l'emplacement original vers un autre support est appelé ´sauvegarde d'image´ ou ´copie originale´ dans le cas d'une copie exacte ou sinon ´export´ s'il y a eu des modifications. Les images exportées peuvent être utilisées comme des copies de travail dues à la compression ou à la conversion de formats, aux améliorations d'image ou à des traitements similaires qui sont nécessaires.

4.2.4.4 Présentation des informations

La présentation des informations est l'affichage des images vidéo soit comme images individuelles (figées) soit comme séquences vidéo avec des images vidéo consécutives sous forme visible par un opérateur. Une ou plusieurs images vidéo peuvent être affichées de manière simultanée. De plus, d'autres données (par exemple, flux audio) et métadonnées peuvent être présentées.

Les écrans des moniteurs (par exemple, CRT, plasma, LCD) ou les projecteurs constituent des exemples d'appareils pour présenter les informations.

4.3 Gestion du système

4.3.1 Généralités

L'interface utilisateur est une interface très importante pour la gestion de l'activité et des données dans les VSS. Cette interface détermine de manière significative le confort, la fonctionnalité et la sécurité réelle d'un VSS.

Du point de vue de la gestion du système, un VSS comporte logiquement deux fonctions:

- **activité** et gestion des données qui capture, transmet, stocke et présente des images vidéo, d'autres données ou des métadonnées. Cette partie traite aussi les commandes de l'opérateur et les activités générées par le système, par exemple, les procédures d'alarme et d'alerte des opérateurs;
- les **interfaces** qui relient le VSS aux autres systèmes.

Les fonctions logiques du système mentionnées ci-dessus ne font pas référence à des appareils séparés dans la mesure où un appareil peut assurer des tâches multiples. Par exemple, un enregistreur manipule, stocke et restitue les images et, en même temps, il assure l'analyse du contenu vidéo et alerte un opérateur lorsqu'une procédure d'alarme est activée.

4.3.2 Gestion des données

Un VSS gère les informations. En plus des données vidéo, il peut aussi manipuler d'autres données acquises, par exemple, les données audio ou les métadonnées qui peuvent être acquises à partir d'un autre système ou générées par le système. Ces informations sont gérées partiellement par le système lui-même et partiellement par un opérateur.

La gestion des informations mentionnées ci-dessus comprend l'acquisition de données (par exemple, capture d'images), la transmission de données entre composants du système (par exemple, transmission d'images d'une caméra vers un enregistreur), le stockage des images (par exemple, enregistrement sur disque dur) et la présentation des données (par exemple, affichage des images sur un écran de moniteur). Ces fonctionnalités sont principalement prises en charge par les appareils qui composent le VSS ou par les logiciels de ces appareils (par exemple, base de données pour le stockage des images vidéo).

Le système peut manipuler et générer des métadonnées. Il existe différents types de métadonnées qui sont gérés par le système:

- données qui sont liées aux données vidéo réelles, par exemple, donnée POS, numéros des plaques d'immatriculation, données d'identification de l'emplacement. Elles peuvent être acquises par un autre système ou générées par le système lui-même (par exemple, datages, identificateurs de source d'image);
- fichiers journaux générés et stockés par le système décrivant les activités du système ou de l'opérateur;
- données système sous la forme de condition système, d'usage de supports de stockage, etc.

Un opérateur a la responsabilité de répondre aux informations présentées comme défini dans les exigences d'exploitation.

4.3.3 Gestion des activités

La gestion des activités comprend toutes les activités qui sont engendrées par des évènements et des actions des utilisateurs.

Un évènement est une occurrence dans le monde réel, comme un incendie (maison en feu), une intrusion (une porte fracturée) ou une autre situation définie (une personne en mouvement). L'évènement peut impliquer un danger pour des personnes ou des biens.

Un évènement peut aussi être quelque chose qui est ciblé au niveau du VSS, par exemple, une fraude sur un composant du système.

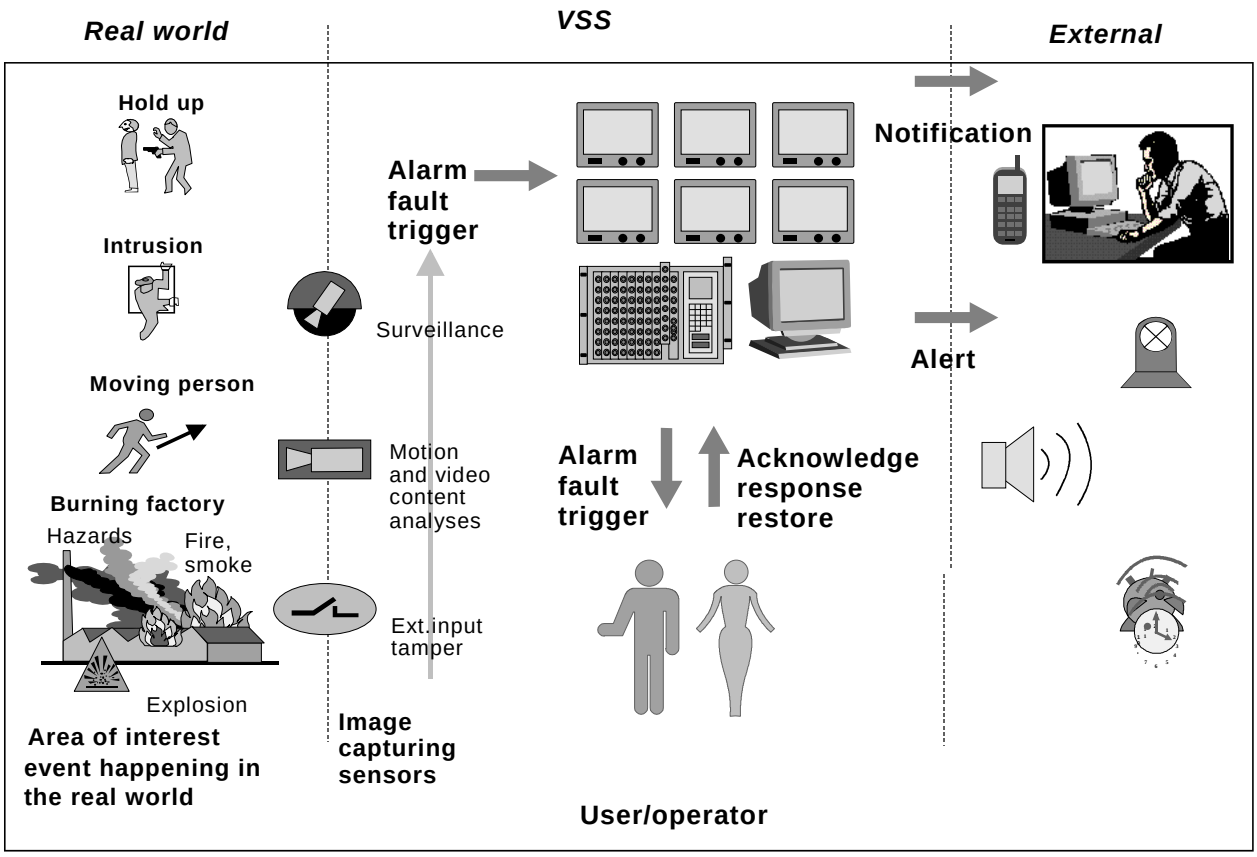
L'évènement peut déclencher une procédure d'alarme dans le VSS. Le déclenchement peut être le résultat d'une manipulation d'image (par exemple, VCA ou VMD), un signal provenant d'un capteur (par exemple, détecteur de fumée ou de mouvement) ou des données reçues d'un autre système (par exemple, portes EAS ou système ANPR).

Lorsque la procédure d'alarme est déclenchée, le VSS effectue les tâches telles qu'elles sont définies dans les exigences d'exploitation. La plupart du temps, ces tâches sont une réponse au danger perçu.

Cette réponse d'alarme peut impliquer des activités internes (par exemple, repositionnement délibéré d'une caméra pour modifier l'angle de prise de vue, enregistrement ou présentation d'image), ainsi qu'une notification d'un système externe (par exemple, contrôle d'accès ou centre de réception d'alarme).

Une tâche type de la procédure d'alarme alerte aussi un opérateur qui, à son tour, peut lancer d'autres activités. Les actions réalisées par un opérateur sont définies dans les exigences d'exploitation.

La Figure 3 illustre les activités entraînées par un évènement:



IEC 2570/13

Légende

Anglais	Français
Real world	Monde réel
VSS	VSS
external	externe
Hold up	Hold up
Alarm fault trigger	Alarme, défaut, déclenchement
alert	alerte
Moving person	Personne en mouvement
Motion & video content analyses	Analyses de contenu de déplacement et vidéo
Acknowledge, response, restore	Accuser réception, réponse, restauration

Anglais	Français
Burning factory	Usine en feu
hazards	dangers
Fire, smoke	Feu, fumée
Ext. input tamper	Fraude d'entrée ext.
Area of interest	Zone considérée
Event happening in the real world	Événement se produisant dans le monde réel
Image capturing sensors	Capteurs, capture d'image
User/operator	Utilisateur/opérateur

Figure 3 – Gestion d'activités

La gestion d'activités inclut la configuration du système, la commande du système, l'analyse à posteriori et d'autres activités lancées par un opérateur. On peut donner comme exemples, la position d'une caméra à zoom panoramique vertical, la redirection des images vers un moniteur, ainsi que la sauvegarde, l'export et l'impression de données. Toutes ces activités sont définies dans les exigences d'exploitation de l'application.

4.3.4 Interfaces avec les autres systèmes

Pour l'interface avec les autres systèmes, les formats de commande et de données sont à spécifier en détail pour les deux systèmes. Les interfaces systèmes permettent un accès mutuel et confortable aux fonctionnalités et aux données.

Un VSS peut être interfacé avec d'autres systèmes, par exemple.

- d'autres systèmes de sécurité (par exemple, autre VSS, alarme contre les intrusions et les holdups, systèmes de contrôle d'accès ou d'alarme incendie),
- des systèmes de gestion de la sécurité (par exemple, systèmes de gestion d'alarme ou ARC (centres de réception d'alarmes), RVRC),
- d'autres systèmes non liés à la sécurité (par exemple, systèmes de gestion de bâtiment, caisses automatiques, matériel pour points de vente ou systèmes de reconnaissance automatique des plaques d'immatriculation).

Les interfaces entre les systèmes peuvent gérer la communication des données, la commande du système commun, les bases de données communes, les interfaces utilisateurs communes ou d'autres types d'intégration de système.

En général, une distinction peut être faite entre deux types de transmission, soit le chemin de transmission physique fait partie du VSS, soit il est fourni par une tierce partie comme interconnexion externe.

4.4 Sécurité du système

4.4.1 Généralités

La sécurité du système comprend l'**intégrité du système** et l'**intégrité des données**. L'intégrité du système comprend la sécurité physique de tous les composants du système et la commande des accès physiques et logiques au VSS. L'intégrité des données couvre l'accès logique aux données et la prévention de la perte ou de la manipulation des données.

La sécurité du système est destinée à protéger des interférences intentionnelles et involontaires avec le fonctionnement normal du VSS.

NOTE La présente norme se réfère à la sécurité du système lorsqu'elle peut être assurée par le système lui-même. La sécurité peut également être assurée par des mesures physiques, l'emplacement des composants, etc.

4.4.2 Intégrité du système

L'intégrité du système comprend la protection de chaque composant ou appareil du système ainsi que la protection du système en tant qu'entité. Si des interconnexions externes entre composants du système sont utilisées, leur protection fait également partie de l'intégrité du système. La même chose s'applique aussi aux interfaces avec les autres systèmes.

L'intégrité du système se compose de trois parties:

- détection des défaillances des composants, des logiciels et interconnexions
- protection contre l'accès frauduleux
- protection contre l'accès non-autorisé au système

4.4.3 Intégrité des données

L'intégrité des données couvre plusieurs points importants:

- identification des données (assurant une identification précise de la source de données, de l'heure, de la date, etc.);
- authentification des données (prévention de modification, suppression ou insertion de données);
- protection des données (prévention de l'accès non-autorisé aux données).

5 Grade de sécurité

Les VSS sont classés par grades pour fournir le niveau de sécurité exigé. Les grades de sécurité tiennent compte du niveau de risque qui dépend de la probabilité d'un incident et du dommage potentiel qu'il peut causer, comme indiqué à la Figure 4.

NOTE Ce sont les fonctions du système plutôt que les composants du système VSS qui sont classées par grade.

Compte tenu de la large gamme de tâches de surveillance, les fonctions d'un VSS peuvent avoir des grades de sécurité différents dans un système. On doit attribuer au système un grade global pour lequel les exigences tributaires du grade dans la présente norme doivent s'appliquer. Lorsqu'elles sont identifiées par l'OR, ou la proposition de conception du système, les fonctions du VSS peuvent utiliser un grade différent mais ceci doit être appliqué de façon cohérente dans l'ensemble du système. Les exigences de protection et de détection de la fraude du 6.3.2.3 peuvent être appliquées avec différents grades dans différents emplacements au sein du système en fonction du risque au niveau de cet emplacement. Cela doit être enregistré dans l'OR ou la proposition de conception du système. Cela doit être déterminé par une appréciation du risque et être explicitement défini dans l'OR. Les grades de sécurité doivent être appliqués, lorsque le VSS est identifié comme mesure d'atténuation principale du risque. Il doit être noté que les risques identifiés peuvent être atténués dans les meilleures conditions par des moyens autres que le VSS.

Les sections de grade de sécurité ou le grade des fonctions individuelles peuvent s'appliquer uniquement si cela a été considéré comme pertinent dans l'appréciation du risque, l'OR ou la proposition de conception du système. En l'absence de spécification, le grade de sécurité par défaut est 1.

Il existe quatre grades:

– risque faible (grade 1)

  VSS destiné à la surveillance des situations présentant un risque faible. Le VSS ne possède pas de niveau de protection, ni de restriction d'accès.

– risque faible à moyen (grade 2)

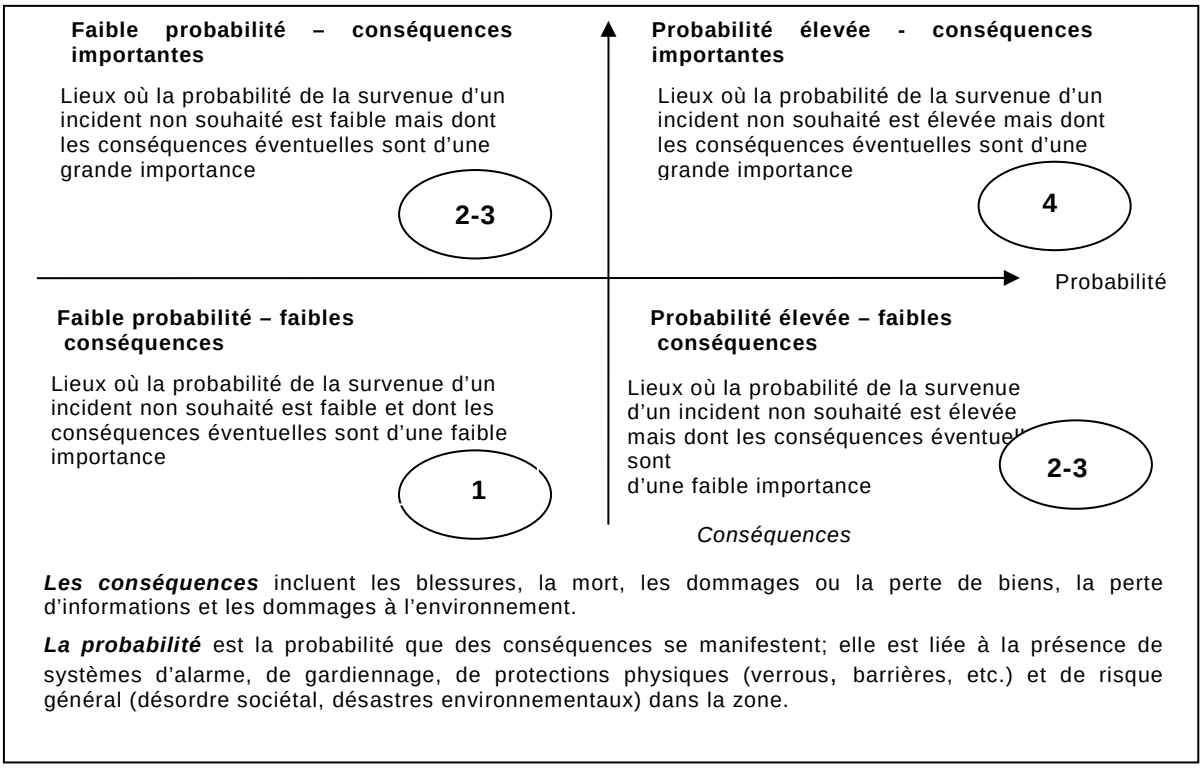
VSS destiné à la surveillance des situations présentant un risque faible à moyen. Le VSS possède un faible niveau de protection et une faible restriction d'accès.

– risque moyen à élevé (grade 3)

VSS destiné à la surveillance des situations présentant un risque moyen à élevé. Le VSS possède un niveau de protection élevé et une restriction d'accès importante.

– risque élevé (grade 4)

VSS destiné à la surveillance des situations présentant un risque élevé. Le VSS possède un niveau de protection très élevé et une restriction d'accès très importante.



IEC 2571/13

Figure 4 – Risques et grades de sécurité

Les fonctions d'un VSS, dont les spécifications sont conformes aux grades de sécurité, sont les suivantes:

1) Interconnexions communes
2) Stockage
3) Archivage et sauvegarde
4) Informations liées à l'alarme
5) Journaux système
6) Sauvegarde et restauration des données système
7) Notification des défaillances répétitives
8) Surveillance PSU du dispositif de manipulation d'image
9) Temps de conservation de la mémoire tampon des images
10) Temps de notification des défaillances des dispositifs à fonctions essentielles
11) Surveillance des interconnexions
12) Détection de la fraude

13) Exigences relatives au code d'autorisation
14) Synchronisation temporelle
15) Authentification des données
16) Authentification des exports/copies
17) Etiquetage des données
18) Protection (contre la manipulation) des données

6 Exigences fonctionnelles

6.1 Environnement vidéo

6.1.1 Capture d'image

Les images capturées de la zone considérée doivent avoir une précision suffisante et fournir suffisamment de détails pour permettre aux utilisateurs d'extraire les informations appropriées définies dans les exigences concernant la qualité d'image (voir 6.5).

La capture d'images doit remplir les objectifs du client en termes de manipulation d'image, par exemple, la présentation et l'enregistrement (en ce qui concerne fps, résolution, profondeur de couleur et temps de latence) comme cela est défini dans les exigences concernant la qualité d'image (voir 6.5).

Pour les exigences relatives à la qualité d'image au moment de l'installation, voir la CEI 62676-4.

6.1.2 Interconnexions

6.1.2.1 Généralités

Toute interconnexion doit être conçue pour minimiser la possibilité de signaux ou de messages retardés, modifiés, remplacés ou perdus conformément aux exigences définies en 6.3.2.3.1.

La surveillance des interconnexions doit être prévue conformément aux exigences définies en 6.3.2.2.4 des exigences de sécurité du système.

6.1.2.2 Interconnexions communes

Les flux d'images partageant l'interconnexion commune doivent être conçus et configurés de manière à ne pas s'affecter défavorablement entre eux ni à affecter les transferts de messages dans tout mode de fonctionnement normal.

Pour les grades de sécurité 3 et 4, si un VSS est conçu et configuré d'une manière telle que les opérateurs simples ou multiples demandent des images vidéo via des interconnexions communes, la conception du système doit garantir que la capacité disponible est suffisante pour le fonctionnement anticipé du VSS. Cela peut être réalisable en configurant le débit maximal des flux d'images sur le VSS.

NOTE La priorisation des flux d'images est prise en compte, par exemple pour les enregistrements.

6.1.3 Manipulation d'image

6.1.3.1 Présentation

Si le VSS est capable de présenter des informations, les propriétés suivantes doivent être déclarées par le fabricant dans la documentation:

- nombre maximal de sources d'images affichées simultanément;

- résolution de la (des) image(s) affichée(s);
- taille(s) de la (des) image(s) affichée(s);
- vitesse d'affichage (nombre d'images affichées à la seconde);
- temps de réponse;
- couleur / noir et blanc.

Lors de l'affichage des images, qu'il s'agisse d'une source d'image entière ou d'une partie de celle-ci, les proportions de l'image affichée doivent être les mêmes que celles de la source d'image originale. Toute information superposée, par exemple, le datage, les noms de caméra, produite par le système ne doit pas affecter l'image enregistrée.

6.1.3.2 Analyse

Toute information superposée, par exemple, les masques d'objets, les lignes trajectoires et les informations de classification produites par le système, doit être traitée comme des métadonnées et ne doit pas affecter l'image elle-même (voir 6.3.3). Seul un masque de confidentialité est autorisé à affecter le champ de vision d'une image pour des raisons de confidentialité afin de cacher des zones sensibles.

6.1.3.3 Stockage

Si le stockage ou les fonctions d'enregistrement sont disponibles dans le VSS, les exigences suivantes et celles du Tableau 1 s'appliquent.

La plupart des systèmes modifient les images vidéo avant qu'elles ne soient stockées (conversion entre format analogique et format numérique, modifications de résolution, compression, tatouage numérique ou encryptage). Dans la documentation, tous les processus qui pourraient causer une perte d'information doivent être clairement indiqués.

En l'absence de stockage redondant, les images doivent être stockées sur le support de stockage de manière à pouvoir afficher et copier les données avec des appareils de remplacement.

EXEMPLE Le support de stockage est monté sur un nouvel appareil en cas de défaillance d'appareil.

Tableau 1 – Stockage

Le VSS doit être capable	Grade de sécurité			
	1	2	3	4
De sauvegarder les données et/ou l'enregistrement redondant			X	X
De réaliser un stockage à sécurité intrinsèque (par exemple, RAID 5, miroir continu) ou de basculer automatiquement d'un support de stockage à un autre dans le cas de défaillance de stockage				X
De réagir à un déclenchement avec un temps de latence maximum de		1 s	500 ms	250 ms
De répéter la lecture d'une image à partir du stockage avec un temps maximal après l'incident ou l'enregistrement réel de			2 s	1 s

Les propriétés suivantes du ou des dispositifs de stockage doivent être déclarées par le fabricant dans la documentation du système:

- type(s) et nombre de voies d'entrée vidéo ou de flux d'images;
- type(s) et nombre de voies de sortie vidéo ou de flux d'images;
- type(s) et nombre d'autres voies d'entrée ou de flux de données;
- nombre maximal d'images stockées par seconde pour chaque voie ou chaque flux à la résolution spécifiée;

- nombre total maximal d'images stockées par seconde à la résolution spécifiée lorsque toutes les voies ou tous les flux sont connectés;
- nombre maximal d'images affichées localement et/ou au niveau d'une station de travail distante lors d'un stockage à vitesse maximale;
- nombre maximal d'images stockées lors d'un affichage à vitesse maximale localement et/ou à distance;
- résolution et taille des images stockées;
- débit binaire maximum par dispositif de stockage et par flux;
- capacité de stockage en heures au nombre choisi de voies ou de flux d'entrée, images à la seconde, résolution et qualité;
- compression (méthodes disponibles, réglages, débits de compression);
- temps nécessaire pour recommencer le stockage d'image après le redémarrage du système (par exemple, à la suite d'une perte d'alimentation).

Le stockage des images vidéo ne doit pas être influencé par un affichage et des demandes d'image en direct quels qu'ils soient, ni par une sauvegarde ou un export d'image. La vitesse d'enregistrement configurée doit toujours être fournie quel que soit le mode de fonctionnement normal.

Si un taux de trame constant est spécifié, les séquences d'images doivent produire des images à des intervalles de temps égaux.

Le système doit pouvoir être configuré de manière qu'un temps de stockage maximal puisse être réglé. Le VSS doit être capable de supprimer automatiquement des images à l'expiration de leur durée de stockage prévue. Les images enregistrées qui sont marquées comme étant protégées contre la suppression, peuvent être stockées pendant une durée plus longue. Il convient de ne pas dépasser la durée de stockage maximale autorisée par la législation nationale applicable.

Le VSS doit offrir des informations concernant:

- les voies ou les flux d'entrée vidéo qui sont enregistrés;
- l'usage pour le stockage d'images en termes de capacité et de temps d'enregistrement;
- la capacité de stockage restante.

Le système doit être capable d'indiquer, comme cela est spécifié dans la documentation du système, si la capacité de stockage s'amenuise.

6.1.3.4 Sauvegarde / archivage des données d'image

Si le stockage ou les fonctions d'enregistrement sont disponibles dans le VSS, les exigences suivantes et celles du Tableau 2 s'appliquent.

Il doit être possible d'extraire et de préserver les données d'images en vue d'apporter des preuves ou à d'autres usages. Il doit être possible d'extraire ou de déplacer les données stockées de manière à pouvoir les visualiser ou répéter leur lecture en un autre lieu. Un moyen de lecture des données d'images extraites (par exemple, système de visualisation d'archives) doit être disponible sans compromettre l'aptitude du système à continuer à fonctionner tel qu'il est conçu.

Si les données numériques sont transférées vers un support de stockage secondaire, il doit alors s'agir d'une copie identique des données originales et cette copie doit être appelée ´copie exacte´.

Ces données doivent pouvoir être visualisées avec un système de visualisation d'archives intégrant toutes les métadonnées supplémentaires (ATM, POS, info VCA, données d'identification de l'emplacement, etc.) ou elles doivent pouvoir être reprises dans le système de stockage primaire sans perte d'information.

Tableau 2 – Archivage et sauvegarde

L'archivage doit offrir	Grade de sécurité			
	1	2	3	4
L'authentification de chaque image individuelle et de chaque séquence d'images				X
Une sauvegarde programmée automatiquement des données d'image d'alarme				X
Une sauvegarde de données d'image d'alarme sur demande manuelle			X	X
La vérification que la sauvegarde d'image a été réalisée correctement			X	X

6.1.3.5 Export d'image

Si les fonctions d'enregistrement sont disponibles dans le VSS, les exigences suivantes s'appliquent:

- l'export d'image ne doit pas altérer l'enregistrement original dans le stockage primaire. Le système doit être capable d'offrir le choix de la plage temporelle et de la source d'image à exporter ou à copier;
- les données exportées doivent posséder un identificateur de source d'images et des images ´identifiant´ le datage pour garantir l'ordre et le caractère complet des séquences d'images;
- le système doit être capable également d'exporter ou de copier une image individuelle;
- La documentation du système doit spécifier les formats d'export pris en charge (voir 6.1.3.6)

  NOTE Le format de données utilisé en export ne représente généralement pas toutes les informations stockées, par exemple, métadonnées et informations sonores. Ces formats ont l'avantage d'être plus communs et faciles à manipuler.

- L'impression d'images sur papier ne doit pas être considérée comme un export d'image et ne satisfait pas aux exigences relatives à l'export d'image.

6.1.3.6 Format de données

Les algorithmes de compression qui nécessitent l'utilisation d'un logiciel exclusif pour obtenir un accès direct aux données VSS ne doivent pas être utilisés sauf si les informations permettant l'accès direct sont mises à disposition (par exemple par un Software Development Kit).

NOTE Des algorithmes de compression spéciaux ou modifiés empêchent un accès direct aux données VSS sans logiciel exclusif, ce qui rend la répétition de lecture des images difficile pour les tierces parties.

Les méthodes de stockage et/ou transmission des données vidéo ou audio et des métadonnées doivent utiliser des formats, des codecs (codeurs-décodeurs) et des enveloppes standard. Les données doivent satisfaire strictement aux normes et contenir les informations complètes nécessaires pour le décodage du contenu.

Le format et les moyens de localisation des données dans les fichiers VSS doivent être disponibles sous forme de normes internationales publiées CEI, ISO ou UIT.

Le système doit être capable d'exporter les séquences d'images sous un format standard à une qualité équivalente au format original, tout en affichant les informations relatives à l'heure et à la date sans augmentation significative de la taille du fichier.

Le format des fichiers VSS doit permettre de déterminer la taille et le facteur de forme de chaque image.

La liste suivante contient des exemples de normes internationales acceptables, sans toutefois être exclusive:

Codecs vidéo:

- H.264: AVC: ISO/CEI 14496-10, UIT-T Rec. H.264*: Technologies de l'information – Codage des objets audiovisuels – Partie 10: Codage vidéo évolué*
- MPEG-4 partie 2: ISO/CEI 14496-2, *Technologies de l'information – Codage des objets audiovisuels – Partie 2: Codage visuel*
- MPEG-2: ISO/CEI 13818-1, *Technologies de l'information – Codage générique des images animées et du son associé: Systèmes*
- H.263: UIT-T Rec. H.263 *Codage vidéo pour communications à faible débit*
- JPEG 2000: ISO/CEI 15444-1, *Technologies de l'information – Système de codage d'images JPEG 2000: Système de codage de noyau*
- JPEG: ISO/CEI 10918-1 | UIT-T Rec. T.81 *Technologies de l'information – Compression numérique et codage des images fixes de nature photographique: Prescriptions et lignes directrices*

Codecs audio:

- G.711: UIT-T Rec. G.711, *Modulation par impulsions et codage (MIC) des fréquences vocales*
- G.726: UIT-T Rec. G.726, *Modulation par impulsions et codage différentiel adaptatif (MICDA) à 40, 32, 24, 16 kbit/s*
- AAC: ISO/CEI 14496-3, *Technologies de l'information – Codage des objets audiovisuels – Partie 3: Codage audio*

Export de vidéos et formats de fichiers:

- MP4: ISO/CEI 14496-14, *Technologies de l'information – Codage des objets audiovisuels – Partie 14: Format de fichier MP4*
- MPEG-A: ISO/CEI 23000-10:2009, *Technologies de l'information – Format pour application multimédia (MPEG-A) – Partie 10: Format pour application à la surveillance*

Protocole de vidéo IP (Découverte, contrôle, métadonnées, etc.):

- CEI 62676-2 (toutes les parties), *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2: Protocoles de transmission vidéo*

6.1.3.7 Encryptage et tatouage numérique

Le format VSS peut contenir des sommes de contrôle ou d'autres méthodes qui permettent d'assurer que les modifications des données peuvent être détectées mais, lorsqu'elles sont effectives, ne doivent pas affecter les informations relatives aux images comprimées.

En cas de cryptage des images, il convient que le cryptage ne modifie pas les informations relatives aux images. Il convient que la méthodologie de cryptage et de décryptage soit immédiatement accessible aux utilisateurs autorisés.

6.1.3.8 Métadonnées minimales

La capacité d'identification correcte de l'heure de capture d'une image est souvent essentielle pour l'utilisation du VSS dans les enquêtes de police. Par conséquent:

Les données contenues dans les fichiers VSS doivent, au minimum, permettre d'associer un datage UTC et un identificateur de caméra à chaque image et chaque échantillon sonore. Pour un VSS dépourvu d'un équipement audio, le datage doit avoir une résolution d'au moins une seconde. Lorsque le système comporte à la fois un équipement vidéo et audio, les datages doivent avoir une résolution suffisante pour permettre une lecture synchronisée des flux audio-visuels.

Les moyens de détermination des datages et de l'identificateur de caméra sur chaque image et chaque échantillon sonore doivent être rendus publics. Il existe de nombreuses méthodes différentes de codage des datages, mais toute méthode utilisée, quelle qu'elle soit, doit être indiquée.

Le format VSS doit spécifier les décalages temporels éventuels appliqués aux datages et préciser la méthode de conversion de chaque datage en une heure locale qui est propre à un fuseau horaire, et qui inclut tout ajustement applicable lié aux économies d'énergie.

Il convient que la mise à l'heure soit automatique pour les changements constatés entre les décalages éventuels liés aux économies d'énergie et le temps UTC.

6.1.3.9 Format de multiplexage

Lorsqu'un enregistrement VSS contient plusieurs flux de données vidéo (et audio), les fichiers VSS doivent intégrer des métadonnées qui permettent le démultiplexage des flux. La méthode de démultiplexage doit être rendue publique.

Il est admis que le format VSS contienne d'autres flux de données non essentiels pour l'extraction des images et des échantillons sonores avec leurs datages. Les flux de données supplémentaires peuvent rester exclusifs bien qu'il soit recommandé de publier leur format, de sorte qu'ils puissent être décodés indépendamment du logiciel du fabricant.

Il est recommandé que chaque flux vidéo et audio ait un nom qui peut être significatif pour l'utilisateur du VSS. Lorsque les flux comportent des noms, la méthode d'association des flux et de leurs noms doit être rendue publique.

6.1.3.10 Améliorations d'image

Si le système fournit des outils d'amélioration tels que l'affinage d'image, la surbrillance d'une image ou le zoomage sur une partie spécifique de l'image, il convient alors que les améliorations appliquées ne modifient pas l'enregistrement d'origine. En cas d'export d'une image améliorée, il convient que ces changements soient documentés par un enregistrement d'audit.

6.1.3.11 Export d'image

Pour faciliter le processus de répétition de lecture et d'export, il convient de respecter la procédure suivante.

– Les données VSS exportées à partir d'un enregistreur ne doivent pas présenter de perte de qualité des trames individuelles, ni de changement du taux d'image ou de la qualité sonore. Il convient que le processus d'export ne comporte pas de reproduction ou de perte de trames. Il convient que le système n'applique aucune conversion de format ou compression supplémentaire des images exportées, dans la mesure où cela peut réduire le caractère utile du contenu.
– Il convient d'exporter les métadonnées minimales (voir 6.1.3.8) et les signatures d'authentification, lorsqu'elles existent, avec les images.
– Il convient que le système soit capable d'exporter des images et des informations sonores le cas échéant, à partir des caméras (et des microphones) sélectionnés dans les délais définis par l'utilisateur.

– Il convient que le système conserve sa fonctionnalité ou ses performances au cours de l'export des données.

– Il convient que la méthode d'export du système soit adaptée à la capacité de ce dernier et à son utilisation prévue.

NOTE 1 Lorsque la méthode d'export n'est pas appropriée, le risque existe que les pouvoirs publics, s'ils exigent des preuves vidéo, retirent le système, par exemple, si 1 téraoctet de données est requis, l'exportation de celui-ci via un graveur de CD n'est guère réalisable.

NOTE 2 Il existe de nombreuses méthodes d'exportation des images sous format d'origine à partir d'un système, par exemple:

- Les images sont reproduites sur un support numérique amovible tel qu'une disquette, une cassette audionumérique, une carte mémoire, un CD-ROM ou un DVD.
- le disque dur amovible, qui contient les images, est retiré physiquement du système.
- les images sont exportées via un port, tel qu'un port USB, SCSI, SATA, FireWire ou une mise en réseau.

Il convient que le système affiche une heure estimée de réalisation de l'export des données demandées. Il convient que l'application logicielle nécessaire pour la répétition de lecture des images exportées soit intégrée au support utilisé pour l'export. Dans le cas contraire, la visualisation des images par les parties tierces agréées peut être empêchée.

6.1.3.12 Répétition de lecture des images exportées

Si le format d'exportation satisfait à une norme non exclusive commune, l'utilisation d'un lecteur d'export exclusif peut ne pas être nécessaire. Si le fabricant décide de produire un logiciel de répétition de lecture exclusif, les images exportées doivent alors pouvoir faire l'objet d'une répétition de lecture sur un ordinateur via le logiciel exporté.

Il convient que l'application de répétition de lecture:

- comporte un système de réglage de vitesse variable, y compris les fonctions de lecture en temps réel, arrêt, pause, avance rapide, rebobinage, et visualisation image par image vers l'avant et inverse;
- affiche les caméras simples et multiples, et maintienne un facteur de forme, c'est-à-dire les mêmes hauteur et largeur relatives;
- affiche une caméra simple à la résolution enregistrée maximale;
- permette de rechercher les enregistrements de chaque caméra par l'heure et la date;
- permette l'impression et/ou la sauvegarde (par exemple, bitmap ou format JPEG) d'images fixes avec l'heure et la date d'enregistrement;
- permette une répétition de lecture multi-écran à synchronisation temporelle;
- permette un basculement à synchronisation temporelle entre caméras lors de la répétition de lecture;
- permette une répétition de lecture de métadonnées audio et autres métadonnées associées;
- soit capable d'exporter les séquences d'images sous un format standard (voir 6.1.3.6) à une qualité équivalente au format original, tout en affichant les informations relatives à l'heure et à la date sans augmentation significative de la taille du fichier;
- indique clairement l'heure et la date, ainsi que toute autre information associée à chaque image affichée, sans assombrir l'image.

Si des lecteurs de disque dur amovibles sont utilisés comme option principale d'export (selon l'échelle de téléchargement), il convient alors que le lecteur puisse faire l'objet d'une répétition de lecture au moyen d'un ordinateur standard, par exemple, sous un système d'exploitation Windows. Cette fonctionnalité est également souhaitable pour tout lecteur de disque dur utilisé dans un VSS où il ne s'agit pas du moyen d'export principal.

6.2 Gestion du système

6.2.1 Fonctionnement

Le fonctionnement de l'interface utilisateur doit être compréhensible par lui-même sans indication complémentaire, simple, et rapide pour un opérateur. Le statut du système doit être détecté, traité et affiché de manière automatique. Les situations d'alarme doivent être identifiables et accessibles immédiatement avec une documentation cohérente de l'évènement.

6.2.2 Gestion d'activité et d'information

6.2.2.1 Généralités

Le système doit clairement faire la distinction entre les données demandées par l'utilisateur et les données générées par un évènement. Les données d'alarme peuvent être prioritaires par rapport aux données affichées en permanence.

Les images présentées à un opérateur doivent être clairement étiquetées comme images en direct ou vidéo lue. En outre, les vidéos générées par un évènement doivent être clairement étiquetées pour les différentier des vidéos demandées par l'utilisateur.

6.2.2.2 Statut des fonctions du système

Le VSS doit toujours être capable d'offrir des informations sur le statut des fonctions essentielles.

6.2.2.3 Événements et activités générées par des évènements

Si le VSS est conçu pour traiter des activités générées par des évènements, les exigences suivantes s'appliquent.

Les déclenchements ou les messages doivent être extraits dans leur ordre d'arrivée sauf lorsqu'un moyen est prévu pour placer des priorités pour ces entrées.

Lorsque le système possède un dispositif qui permet d'identifier la priorité des alarmes, alors le niveau de priorité doit aussi être indiqué.

Dans un tel cas, les messages ou les déclenchements doivent être extraits conformément aux niveaux de priorité. Lorsque de nombreux messages ou de nombreux déclenchements de priorité égale sont en attente, ils doivent être extraits dans leur ordre d'arrivée.

Les exigences générales pour l'indication de la priorité sont les suivantes:

- le système doit indiquer s'il existe plus d'alarmes que celles actuellement affichées;
- outre les informations effectivement affichées, des informations supplémentaires peuvent être disponibles sur demande. La visibilité des informations prioritaires doit être préservée;
- le fonctionnement normal du VSS ne doit pas empêcher l'indication d'une alarme.

Il doit être possible de faire la distinction entre différentes conditions du système qui peuvent avoir déclenché l'activité et entre une alarme, un défaut ou une fraude.

Le VSS doit offrir des moyens pour indiquer une alarme visuellement et de manière sonore pour obtenir l'attention d'un opérateur.

Le VSS doit offrir des moyens pour accuser réception des alarmes.

Pour les systèmes de grades de sécurité 3 et 4, en cas d'alarme, le VSS doit être capable d'afficher les informations liées à l'alarme. Les informations présentées pour chaque message d'alarme doivent inclure:

a) l'origine ou la source de l'alarme;

b) le type d'alarme;

c) l'heure et la date de l'alarme.

6.2.2.4 Journaux système

Des journaux système précis et complets doivent être tenus à jour pendant une durée définie dans l'OR. Les données dans le journal système doivent être organisées et présentées dans l'ordre chronologique. Le système doit empêcher une édition ou une suppression non-autorisée des journaux système. Un journal doit être disponible pour chaque station de travail de l'opérateur.

Les détails suivants, donnés dans le Tableau 3, doivent être consignés:

Tableau 3 – Journaux système

Le système doit consigner en incluant le datage (date et heure), l'événement, la source	Grade de sécurité			
	1	2	3	4
Alarmes		X	X	X
Fraude			X	X
Perte vidéo et reprise à partir d'une perte vidéo			X	X
Perte d'alimentation		X	X	X
Défaillance de fonction essentielle et reprise après défaillance			X	X
Messages de défaut affichés pour l'utilisateur				X
Réinitialisation, démarrage et arrêt du système		X	X	X
Actions de diagnostic (vérification de santé)				X
Export, impression / copie papier, y compris identificateur de source d'image, plage temporelle		X	X	X
Connexion et déconnexion utilisateur au niveau de la station de travail avec datage, connexions réussies et refusées (locales/à distance), y compris la raison du refus (mot de passe incorrect, utilisateur inconnu, nombre autorisé d'essais dépassé)		X	X	X
Modifications des codes d'autorisation			X	X
Contrôle des caméras fonctionnelles				X
Recherche d'images et lecture d'images			X	X
Modifications manuelles des paramètres d'enregistrement			X	X
Accusé réception / restauration d'alarme			X	X
Modification de la configuration du système			X	X
Réglage de date et d'heure et modification avec l'heure courante et la nouvelle heure			X	X

6.2.3 Interfaces avec les autres systèmes

Les installations communes doivent être conformes à toutes les normes pour les applications (par exemple, intrusion, accès, VSS, ...) dans lesquelles elles sont utilisées. Lorsque les exigences de deux normes ou plus s'appliquent à une fonction ou un composant spécifiques, la norme comportant l'exigence la plus stricte doit prévaloir pour cette fonction ou ce composant.

NOTE Ceci s'applique directement, lorsque plusieurs systèmes conformes de propriétaires différents font l'objet d'une mise en interface commune et qu'on leur demande de fournir des informations cohérentes.

Toutes les exigences de sécurité du système telles qu'elles sont définies en 6.3 doivent être remplies même au cas où le VSS subit un accès ou est contrôlé par un autre système. L'autre système doit être perçu comme un utilisateur système avec des droits d'accès définis.

Les niveaux d'accès à un autre système doivent être cohérents avec les niveaux exigés par cette norme système et ne doivent pas donner un accès non-autorisé au VSS et inversement.

6.3 Sécurité du système

6.3.1 Généralités

La sécurité du VSS comprend l'intégrité du système et l'intégrité des données. L'intégrité du système comprend la sécurité physique de tous les composants du système et la commande d'accès au VSS. L'intégrité des données inclura la prévention des pertes ou la manipulation des données.

6.3.2 Intégrité du système

6.3.2.1 Généralités

Les VSS de grades de sécurité 3 et 4 doivent être capables de sauvegarder et restaurer toutes les données du système.

6.3.2.2 Détection des défaillances

6.3.2.2.1 Notification des défaillances

Pour les VSS dont l'interface utilisateur est normalement gérée par un opérateur (soit à distance, soit localement), des conditions d'alarme émanant des composants et des fonctions, lorsqu'ils sont spécifiés dans la présente norme, doivent déclencher une alerte. La défaillance doit être notifiée à chaque fois qu'un nouvel utilisateur se connecte ou que le système redémarre.

Les informations à présenter doivent inclure:

- l'heure et la date;
- l'origine et le type de défaillance.

En complément, lorsque le système possède un dispositif qui permet d'identifier la priorité des messages, le niveau de priorité doit aussi être indiqué.

La notification des défaillances ne doit jamais couvrir ou cacher tout affichage d'information important comme la zone considérée des images en direct.

Pour les grades de sécurité 3 et 4, le système doit être capable de détecter des défaillances répétitives provenant d'un composant et doit être configurable pour générer un seul message, lequel doit uniquement être répété à chaque fois qu'un nouvel utilisateur se connecte ou que le système redémarre.

6.3.2.2.2 Surveillance de l'alimentation

Pour le grade de sécurité 4, la défaillance de l'alimentation principale et, le cas échéant, de l'alimentation de secours du système doit être surveillée, avec notification conformément au 6.3.2.2.1. Dans tous les cas, une défaillance de l'alimentation doit toujours être indiquée localement. Le VSS doit tenter de reprendre son fonctionnement normal à la fin de la perte d'alimentation. Si le système n'est pas capable de redémarrer après le rétablissement de

l'alimentation, avec les réglages qui existaient avant la défaillance de l'alimentation, cela doit être consigné dans le journal et également indiqué à un opérateur.

Le VSS doit être capable de cesser son fonctionnement normal au cours d'une procédure définie sans perte de données stockées. Pour les grades de sécurité 3 et 4, des images ne doivent pas être conservées dans une mémoire tampon pendant plus de 5 s sans être inscrites sur le support de stockage.

6.3.2.2.3 Surveillance des fonctions du système et des composants

Pour les grades de sécurité 3 et 4, le VSS doit gérer les défaillances du dispositif en indiquant toute défaillance des fonctions essentielles dans les 100 s qui suivent la défaillance.

6.3.2.2.4 Surveillance des interconnexions

Si des interconnexions entre composants de système font partie du VSS, elles doivent être surveillées selon le Tableau 4 suivant:

Tableau 4 – Surveillance des interconnexions

Le système doit	Grade de sécurité			
	1	2	3	4
Vérifier de manière répétée l'interconnexion à intervalles réguliers avec un maximum de			30 s	10 s
Essayer de ré-établir une interconnexion avec le nombre suivant d'essais avant la notification			5	2
Temps maximal autorisé avant notification à un opérateur de la défaillance d'une interconnexion			180 s	30 s

6.3.2.3 Protection et détection de la fraude

6.3.2.3.1 Généralités

Le VSS doit être protégé contre les fraudes conformément au Tableau 5.

Si une fraude est détectée, une condition de fraude doit être établie et une alarme de fraude doit être générée. L'alarme de fraude doit être consignée dans le journal et clairement séparée des autres conditions, par exemple, la défaillance, l'alarme ou le fonctionnement normal.

Tableau 5 – Détection de la fraude

Le système doit détecter	Grade de sécurité			
	1	2	3	4
La perte vidéo		X	X	X
Si un dispositif de capture d'image avec un champ de vision fixe n'inclut plus la totalité du champ de vision spécifié			X	X
L'obscurcissement ou l'aveuglement délibéré de la gamme d'appareils d'imagerie			X	X
La substitution de toute donnée vidéo au niveau de la source d'image, de l'interconnexion ou de la manipulation				X
La réduction significative du contraste de l'image				X

6.3.2.3.2 Protection contre la fraude des carters

Les dispositifs de capture d'images doivent être protégés contre la fraude dans les systèmes avec grades de sécurité 3 et 4. Il convient de placer les caméras hors de portée, et les vis de fixation doivent être inviolables, afin d'empêcher tout repositionnement non autorisé.

NOTE La protection contre la fraude des dispositifs de capture d'images n'est pas une exigence pour les systèmes de grade 1 et 2.

Un dispositif de capture d'images qui offre une protection contre le vandalisme doit satisfaire aux exigences minimales suivantes:

a) degré de protection IP minimal 44 conformément à la CEI 60529;

b) essais au marteau conformément à la CEI 60068-2-75.

Les impacts doivent être appliqués sur les parties principales telles que le carter, la lentille, etc. Pour les essais de résistance aux attaques physiques, le dispositif doit être monté, selon les instructions du fabricant, sur un support rigide tel que défini dans la CEI 62262 pour tous les essais. Chaque essai doit être effectué par une seule personne.

c) degré IK de 07;

d) résistance pendant 1 min au minimum contre:
   - le démontage du dispositif par le dévissage des vis de fixation;
   - l'extraction du dispositif;
   - une attaque avec un outil simple tel qu'un tournevis d'un diamètre de 4 mm à 7 mm et d'une longueur de 60 mm à 200 mm;
   - une attaque avec un outil simple tel qu'une pince;
   - une attaque avec un briquet pour application de chaleur;

e) résistance contre une attaque par épandage d'une boisson sucrée et acide, avec déversement de 0,3 l d'une boisson gazeuse disponible dans le commerce. Verser la moitié sur le dispositif et projeter du reste de la boisson sur la face inférieure du dispositif.

Après les essais, le dispositif doit continuer à fonctionner normalement.

6.3.2.4 Protection contre l'accès non autorisé

6.3.2.4.1 Généralités

Pour chaque VSS, l'accès au fonctionnement et aux données doit être régi par une procédure d'autorisation. Ceci inclut aussi l'accès par une station de travail distante ou par un système externe intégré au VSS.

6.3.2.4.2 Niveaux d'accès

Pour tous les grades du VSS, il doit y avoir plusieurs niveaux d'accès utilisateur aux fonctions du VSS ou à une ou des parties de celui-ci. L'utilisateur qui accède au système peut être soit un opérateur, soit un autre système:

- **Niveau 1 Accès à toute personne**

  Les fonctions dont il est nécessaire qu'elles soient accessibles au niveau 1 ne doivent comporter aucune restriction d'accès.

- **Niveau 2 Accès par tout utilisateur**

  Fonctions affectant le fonctionnement du système sans changer sa configuration.

  L'accès à ces fonctions dont il est nécessaire qu'elles soient accessibles au niveau 2 doit être protégé au moyen d'une clé, d'un mot de passe, d'un code ou de tout autre moyen ou dispositif de limitation d'accès analogue.

- **Niveau 3 Accès par les administrateurs du système**

  Fonctions affectant la configuration des données du système.

  L'accès à ces fonctions dont il est nécessaire qu'elles soient accessibles au niveau 3 doit être protégé au moyen d'une clé, d'un mot de passe, d'un code ou de tout autre moyen ou dispositif de limitation d'accès analogue.

- **Niveau 4 Accès par le personnel de maintenance ou le fabricant**

  Accès au composant pour modifier la conception du système ou pour réaliser la maintenance du système.

  L'accès à ces fonctions dont il est nécessaire qu'elles soient accessibles au niveau 4 doit être protégé au moyen d'une clé, d'un mot de passe, d'un code ou de tout autre moyen ou dispositif de limitation d'accès analogue. L'accès à ce niveau est bloqué jusqu'à ce qu'il soit autorisé par un utilisateur au niveau d'accès 2 ou 3.

Le Tableau 6 spécifie quelles fonctions doivent être accessibles à chaque niveau d'accès indépendamment du grade de sécurité:

Tableau 6 – Niveau d'accès

Fonction	Niveaux d'accès			
	1	2	3	4
Configuration du système	NP	NP	P	P
Modification des codes d'autorisation individuelle	NP	P	P	P
Assignation et suppression des utilisateurs et codes d'autorisation de niveau 2	NP	NP	P	P
Restauration des valeurs par défaut réglées en usine	NP	NP	P	P
Amélioration du système	NP	NP	P	P
Démarrage / Arrêt du VSS ou d'un composant	NP	NP	P	P
Légende P Permis NP Non permis.				

6.3.2.4.3 Autorisation

Les VSS doivent fournir des moyens logiques ou physiques pour restreindre l'accès au système ou aux parties de système avec une clé, un mot de passe, un code ou un moyen ou un dispositif de limitation d'accès analogue.

La permission d'accéder aux fonctions du VSS doit être spécifiée dans le Tableau 7.

Tableau 7 – Exigences relatives aux codes d'autorisation

Exigence relative au code d'autorisation	Grade de sécurité			
	1	2	3	4
Nombre de clés possibles d'autorisation logique		> 10 000	> 100 000	> 1 000 000
Nombre de clés possibles d'autorisation physique		> 3 000	> 15 000	> 50 000

Les mots de passe des utilisateurs ne doivent jamais être affichés ou stockés en clair.

Une modification valable d'un mot de passe par l'utilisateur lui-même doit toujours nécessiter une connexion d'utilisateur valable avec l'ancien mot de passe et la saisie du nouveau mot de passe plus une validation de manière identique.

6.3.2.4.4 Accès aux données

Le VSS doit fournir des méthodes pour l'accès contrôlé aux données tenant compte du niveau d'autorisation conformément au Tableau 8 ci-dessous.

Tableau 8 – Accès aux données

Fonction	Niveaux d'accès			
	1	2	3	4
Visualisation d'images et de données en direct	P	P	P	P
Visualisation d'images et de données stockées si les enregistrements sont disponibles	NP	P	P	P
Visualisation des informations sur le stockage, si celui-ci fait partie du VSS	NP	P	P	P
Impression et sauvegarde de données vidéo	NP	P	P	P
Exportation d'images et de données	NP	P	P	P
Suppression d'images et de données (uniquement avec confirmation)	NP	NP	P	P
Légende P Permis NP Non Permis.				

6.3.2.4.5 Accès aux journaux systèmes

Le VSS doit fournir des méthodes pour l'accès contrôlé aux journaux systèmes tenant compte du niveau d'autorisation conformément au Tableau 9 ci-dessous.

Tableau 9 – Accès aux journaux systèmes

Fonction	Niveaux d'accès			
	1	2	3	4
Visualisation des journaux systèmes	NP	P	P	P
Exportation à partir des journaux	NP	NP	P	P
Suppression des journaux	NP	NP	NP	NP
Légende P Permis NP Non Permis.				

6.3.2.4.6 Accès au réglage du système

Le VSS doit fournir des méthodes pour l'accès contrôlé au réglage du système tenant compte du niveau d'autorisation conformément au Tableau 10 ci-dessous.

Tableau 10 – Accès au réglage du système

Protection de l'accès au réglage du système	Niveaux d'accès			
	1	2	3	4
Configuration & réglage	NP	NP	P	P
Reprise après défaillance du système	NP	P	P	P
Reprise après accès frauduleux	NP	P	P	P
Légende P Permis NP Non Permis.				

6.3.2.5 Synchronisation temporelle

Pour les grades de sécurité 3 et 4, les réglages temporels des différents composants d'un VSS doivent toujours être à ± 10 s du temps universel coordonné (UTC).

NOTE Cela peut se faire en vérifiant régulièrement l'heure.

6.3.3 Intégrité des images et des données

6.3.3.1 Identification des données

Le VSS doit fournir des méthodes pour identifier les données en tenant compte des différents grades de sécurité conformément au Tableau 11 ci-dessous.

Tableau 11 – Étiquetage des données

Le VSS doit étiqueter les données de manière unique par	Grade de sécurité			
	1	2	3	4
Emplacement (par exemple, nom du site)		X	X	X
Source (par exemple, appareil de capture étiqueté par numéro de caméra)		X	X	X
Date et heure	X	X	X	X
Date et heure en heure UTC, y compris le décalage par rapport à l'heure locale				X

La date et l'heure doivent faire référence à l'heure de capture de l'image.

NOTE L'heure de capture est généralement différente de l'heure de transmission ou de stockage de l'image.

Le VSS doit toujours maintenir les étiquettes de données originales lorsque les données sont exportées.

6.3.3.2 Authentification des données

Pour vérifier l'intégrité des images et autres données, les VSS de grades de sécurité 3 et 4 doivent fournir une méthode (par exemple, tatouage numérique, sommes de contrôle, relevé d'empreintes digitales) pour authentifier l'image et les métadonnées et leur identité.

NOTE L'authentification des données n'est pas une exigence pour les systèmes de grade 1 et 2.

La méthode d'authentification doit être appliquée au moment où les données sont enregistrées et doit avertir l'utilisateur si l'un des cas de figure suivants se présente:

- une des images a été modifiée ou altérée;

- une ou plusieurs images a/ont été retirée(s) d'une séquence;
- une ou plusieurs images a/ont été ajoutée(s) à une séquence;
- l'étiquette de donnée a été modifiée ou altérée.

Les VSS de grades de sécurité 3 et 4 doivent également fournir une méthode pour vérifier l'authenticité des données copiées et exportées.

La méthode d'authentification utilisée doit être spécifiée dans la documentation du système.

6.3.3.3 Protection (contre la manipulation) des données

Les VSS de grade de sécurité 4 doivent fournir une méthode (par exemple, cryptage) pour empêcher la visualisation, sans autorisation, d'images et d'autres données par des personnes non autorisées.

Les VSS de grade de sécurité 4 doivent aussi fournir une méthode pour protéger la confidentialité des données copiées et exportées.

La méthode utilisée pour protéger la confidentialité des données doit être spécifiée dans la documentation du système.

6.4 Exigences relatives à l'environnement

6.4.1 VSS utilisés comme mesure d'atténuation principale du risque

La CEI 62599-2 doit être appliquée aux VSS, lorsque le VSS est identifié comme mesure d'atténuation principale du risque. Ces VSS peuvent être utilisés pour les applications de sureté et de sécurité pertinentes, par exemple, comme système d'alarme anti-intrusion ou système de détection d'incendie.

La stabilité vis à vis de l'environnement du VSS doit être du même niveau dans tous les grades. Le VSS doit fonctionner correctement dans la classe d'environnement spécifiée à l'Article 7 pour laquelle il est conçu et exposé aux conditions CEM décrites dans les CEI 61000-6-3, CEI 61000-6-4 et CEI 62599-1:2010. Un VSS ne doit jamais changer d'état, ses composants ne doivent jamais subir d'endommagement ou ses performances ne doivent jamais varier de manière significative. La CEI 62599-1 décrit les méthodes d'essai d'environnement qui doivent être appliquées aux composants du VSS.

Dans le 8.3.4 de la CEI 62599-2:2010, l'exigence du Tableau 2 ´Réduction de tension de 100 % pour une "Durée de réduction´ de 250 ´nombre de périodes´ ou ´cycles de l'onde de tension" peut être satisfaite par les VSS dans les applications de sécurité pertinentes, par l'utilisation d'un système UPS.

Les essais fonctionnels à appliquer pour l'évaluation des composants doivent être au moins un essai ou une mesure des fonctions essentielles du composant. Les critères d'acceptation doivent reposer sur l'absence de changement dans le fonctionnement du composant et l'absence de changement significatif dans toute mesure pendant l'essai d'environnement. Un composant d'un VSS doit assurer la protection contre les chocs électriques et les dangers consécutifs, en étant conforme aux exigences de la CEI 60950-1 ou de la CEI 60065.

6.4.2 VSS utilisés comme mesure d'atténuation secondaire du risque

Si les VSS ou des parties de ces derniers ne sont pas utilisés pour les applications de sûreté ou de sécurité pertinentes, par exemple, non comme un système de détection anti-intrusion ou un système de détection d'incendie, ils doivent être conformes à la CEI 61000-6-1 ou la CEI 61000-6-2, mais il n'est pas nécessaire qu'ils soient conformes à la CEI 62599-2.

NOTE 1 Il est nécessaire d'appliquer la norme de sécurité CEI 62599-2 uniquement aux applications de sécurité pertinentes, mais non aux systèmes vidéo, comme matériel auxiliaire. Dans ces applications, le VSS n'est pas identifié comme la mesure d'atténuation principale du risque.

NOTE 2 La CEI 61000-6-1 et la CEI 61000-6-2 incluent un degré de sévérité moindre concernant les interruptions de tension et une perte de fonctionnalité (par exemple, réduction de la qualité d'image), avec conditionnement (pour les détails, voir Article 4 de la CEI 61000-6-1:2005 et de la CEI 61000-6-2:2005).

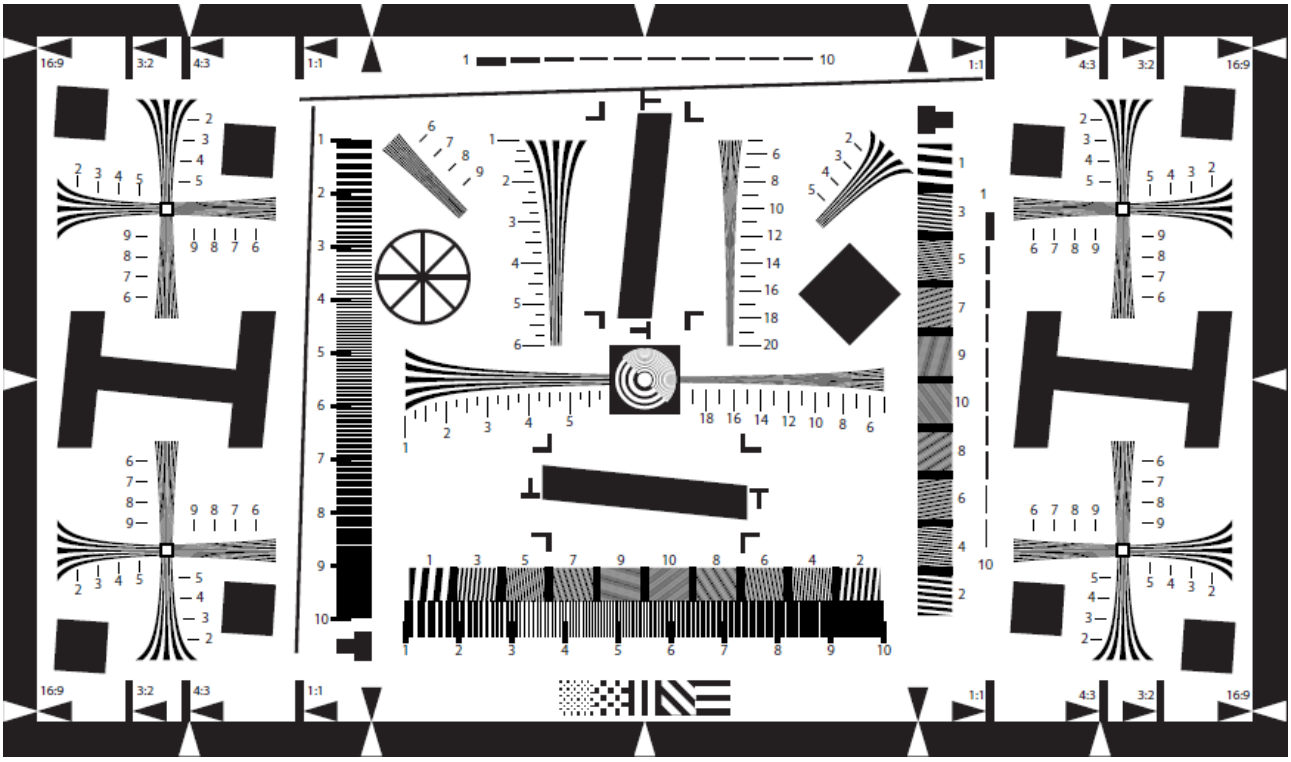
Dans le 8.3.4 de la CEI 62599-2:2010, l'exigence du Tableau 2 ´Réduction de tension de 100 % pour une "Durée de réduction´ de 250 ´nombre de périodes´ ou ´cycles de l'onde de tension" est applicable uniquement aux composants, parties ou systèmes VSS dans les applications de sécurité, qui sont essentielles pour la détection d'un intrus, par exemple, comme partie intégrante d'un système de détection anti-intrusion. Ceci n'inclut pas l'affichage des images, l'observation, la surveillance, l'identification ou l'enregistrement des intrus.

6.5 Qualité d'image

Le VSS doit utiliser des composants qui ont été soumis à l'essai conformément à l'ISO 12233 afin de déterminer leur pouvoir de résolution maximum.

NOTE 1 Ces essais sont réalisés dans des conditions optimales et peuvent ne pas être reproductibles dans des conditions de terrain. Les essais du système installé ne sont pas couverts par la présente norme.

La chaîne de formation d'images – consistant en la capture, le codage/décodage, la transmission, la manipulation, le stockage et l'affichage des images – doit être soumise à l'essai selon le 6.1 de l'ISO 12233:2010 (voir Figure 5). Les résultats doivent être documentés et consignés dans un rapport selon l'Article 7 de l'ISO 12233:2010.



IEC 2572/13

Figure 5 – Référence à l'ISO 12233 diagramme de mesure de la résolution (unité en × 100 lignes)

Ces essais doivent être effectués, lorsque la fonction existe, sur chacune des images vidéo et fixes en direct, enregistrées et exportées. Lorsque plusieurs réglages ou formats d'enregistrement ou d'export sont disponibles, un échantillon représentatif doit être soumis à l'essai et documenté, en indiquant clairement quel niveau est associé avec quel ensemble de paramètres.

NOTE 2 En général, le niveau de qualité observé sur l'image en direct est cohérent sur tout le reste de la chaîne de formation d'images, par exemple, une compression supplémentaire est généralement appliquée au flux vidéo dans la conversion en une image fixe exportée à partir du système.

NOTE 3 Les essais selon l'ISO 12233 fournissent uniquement une mesure de la résolution visuelle "statique" et ne garantissent pas la résolution visuelle d'un système lorsque le mouvement et la complexité de la scène sont aléatoires et variables.

7 Classes d'environnement

7.1 Généralités

Les composants doivent être prévus pour une des classes d'environnement suivantes.

NOTE 1 Les classes I, II, III et IV suivent un ordre de sévérité croissant, il est donc permis d'utiliser les composants de classe IV, par exemple, dans les applications de classe III.

Les composants VSS doivent fonctionner correctement lorsqu'ils sont exposés à des influences environnementales spécifiées en 7.2, 7.3, 7.4 et 7.5.

NOTE 2 Les conditions d'environnement décrites à l'Article 7 sont celles pour lesquelles le VSS est supposé fonctionner correctement, et elles ne sont pas nécessairement celles à utiliser pendant les essais des composants VSS.

7.2 Classe d'environnement I – Intérieur, mais limitée à un environnement d'habitation / de bureau

Influences environnementales normalement subies à l'intérieur lorsque la température est bien maintenue.

EXEMPLE Dans un local d'habitation ou à usage commercial.

Les températures varient en général entre +5 °C et +40 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %.

7.3 Classe d'environnement II – Intérieur – Généralités

Influences environnementales normalement subies à l'intérieur lorsque la température n'est pas bien maintenue.

EXEMPLE Dans les couloirs, les halls ou les cages d'escalier et lorsque la condensation peut apparaître sur les vitres et dans les zones de stockage non chauffées et les entrepôts où le chauffage est intermittent.

Les températures varient en général entre –10 °C et +40 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %.

7.4 Classe d'environnement III – Extérieur, mais protégée contre les effets directs de la pluie et des rayons du soleil, ou intérieur avec des conditions environnementales extrêmes

Influences environnementales rencontrées normalement à l'extérieur et lorsque les composants VSS ne sont pas directement exposés aux intempéries.

EXEMPLE Les températures varient en général entre –25 °C et +50 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %. Pendant 30 jours par an, l'humidité relative est supposée pouvoir varier entre 85 % et 95 % sans condensation.

7.5 Classe d'environnement IV – Extérieur – Généralités

Influences environnementales rencontrées normalement à l'extérieur et lorsque les composants VSS sont directement exposés aux intempéries.

EXAMPLE Les températures varient en général entre –25 °C et +60 °C/+55 °C, y compris un écran contre les rayons du soleil avec un taux moyen d'humidité relative sans condensation d'environ 75 %. Pendant 30 jours par an, l'humidité relative est supposée pouvoir varier entre 85 % et 95 % sans condensation.

NOTE Pour les environnements autres que ceux mentionnés ci-dessus, par exemple les systèmes embarqués, des conditions et exigences supplémentaires peuvent s'appliquer.

8 Documentation

8.1 Documentation du système

La documentation relative aux composants d'un VSS doit être concise, complète et sans ambiguïté. Des informations suffisantes doivent être fournies pour installer, mettre en fonctionnement, utiliser et maintenir un VSS.

Spécification système et schéma de blocs, y compris spécification de configuration:

- détails d'installation pour l'exploitation et l'entretien;
- procédures/routines de contrôle et de maintenance.

8.2 Instructions relatives au fonctionnement

Les instructions relatives au fonctionnement des composants d'un VSS doivent être conçues pour minimiser les mauvais fonctionnements possibles et être structurées pour refléter le niveau d'accès de l'utilisateur.

8.3 Documentation des composants du système

La documentation relative aux composants du VSS doit être concise, complète et sans ambiguïté. La documentation doit être suffisante pour garantir une installation correcte, la mise en fonctionnement et la maintenance des composants du VSS. La documentation des composants peut être fournie par le fabricant sur papier ou sur un autre support. Des informations suffisantes doivent être fournies pour garantir l'intégration de chaque composant avec n'importe quel autre composant du VSS. La documentation d'un composant doit comprendre:

- un guide/manuel d'installation;
- la spécification des données techniques du système:
  - la spécification de performances;
  - les exigences minimales du matériel;
  - les exigences minimales de l'environnement;
  - la norme à laquelle le composant prétend répondre;
- les procédures/routines de contrôle et de maintenance;
- le nom du fabricant ou du fournisseur;
- le nom de l'intégrateur système ou de l'installateur, le cas échéant;
- la description du matériel;
- le nom ou la marque de l'organisme de certification (pour les composants qui sont à certifier);
- la classe d'environnement.

La documentation doit être fournie à l'utilisateur concernant la période de conservation du système. Il convient que la documentation fournisse également les durées approximatives et les méthodes d'export de chacun des éléments suivants, le cas échéant:

- durée maximale de 15 min des données enregistrées par caméra;
- durée maximale de 24 h des données enregistrées par caméra;
- toutes les données du système.

Le temps de latence de réaction du système avant déclenchement doit être spécifié dans la documentation du système.

La méthode de définition des priorités d'entrée des déclencheurs d'alarme doit être donnée par le fabricant dans sa documentation.

Annexe A
(normative)

Conditions nationales particulières

Condition nationale particulière: Caractéristique ou pratique nationale qu'il n'est pas possible de modifier même sur une longue période, telle que, par exemple, des conditions climatiques ou des conditions électriques de mise à la terre.

NOTE Si elle affecte l'harmonisation, elle fait partie intégrante de la Norme internationale.

Pour les pays pour lesquels les conditions nationales particulières pertinentes sont applicables, ces dispositions sont normatives, pour les autres pays, elles sont informatives.

Les conditions nationales particulières décrites ci-dessous doivent s'appliquer aux pays suivants: Danemark, Finlande, Norvège, Suède, Canada et Russie.

Paragraphe	Condition nationale particulière
7.5	Classe d'environnement IV – Extérieur – Généralités:
	Les composants VSS doivent fonctionner correctement lorsqu'ils sont soumis aux influences environnementales normalement constatées à l'extérieur dans le cas où des composants VSS sont pleinement exposés aux intempéries.
	Les températures sont supposées varier entre –40 °C et +60 °C avec un taux moyen d'humidité relative sans condensation d'environ 75 %. Pendant 30 jours par an, l'humidité relative peut varier entre 85 % et 95 % sans condensation.

Annexe B
(informative)

Export de vidéos dans les systèmes de sécurité intérieure

Dans les systèmes vidéo destinés à la sécurité intérieure ou à la sécurité sociétale, qui proposent un export de fichiers vidéo conformément à l'ISO 22311, les exigences suivantes de niveau 2 sont prises en compte:

Il convient que le fichier vidéo exporté offre:

1) Une compatibilité avec l'ISO/CEI 23000-10
2) H.264/MPEG-4 Codec vidéo AVC conformément à l'ISO/CEI 14496-10
3) Une information de rythme pour la synchronisation entre les différentes sources d'images (heure de capture) avec une précision de 40 ms ou plus, afin de permettre une analyse image par image des vues multiples de la même scène en parallèle

   Dans le 6.3.2.5, la synchronisation temporelle de divers composants d'un VSS général doit correspondre uniquement à ± 10 s du temps UTC, et il convient qu'elle soit bien plus précise pour les applications de sécurité intérieure.
4) Il convient que les informations concernant le nom et le profil des codecs, le nom du répertoire de fichiers vidéo, la résolution, le taux d'image (en ips) et l'identificateur de caméra soient proposées comme données statiques
5) Des métadonnées dynamiques, fournies comme flux en temps réel de documents XML selon 8.3.1 de la CEI 62676-1-2 "Documents XML comme charge utile", accompagnées de la vidéo, et qui protègent les informations temporelles

Bibliographie

CEI 62676-2 (toutes les parties), *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2: Protocoles de transmission vidéo*

ISO/CEI 10918-1, *Technologies de l'information – Compression numérique et codage des images fixes de nature photographique: Prescriptions et lignes directrices*

ISO/CEI 13818-1, *Technologies de l'information – Codage générique des images animées et du son associé: Systèmes*

ISO/CEI 14496-2, *Technologies de l'information – Codage des objets audiovisuels – Partie 2: Codage visuel*

ISO/CEI 14496-3, *Technologies de l'information – Codage des objets audiovisuels – Partie 3: Codage audio*

ISO/CEI 14496-10, *Technologies de l'information – Codage des objets audiovisuels – Partie 10: Codage visuel avancé*

ISO/CEI 14496-14, *Technologies de l'information – Codage des objets audiovisuels – Partie 14: Format de fichier MP4*

ISO/CEI 15444-1, *Technologies de l'information – Système de codage d'image JPEG 2000: Système de codage noyau*

ISO/CEI 23000-10, *Technologies de l'information – Format pour application multimédia (MPEG-A) – Partie 10: Format pour application à la surveillance*

ISO 10918 (toutes les parties), *Technologies de l'information – Compression numérique et codage des images fixes de nature photographique*

ISO 22311, *Sécurité sociétale – Vidéosurveillance – Interopérabilité de l'export*

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch