

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Video Surveillance Systems (VSS) for use in security applications –
Part 2-11: Video transmission protocols – Interop profiles for VMS and cloud
VSaaS systems for safe cities and law enforcement**

**Systèmes de vidéosurveillance destinés à être utilisés dans les applications de
sécurité –
Partie 2-11: Protocoles de transmission vidéo – Profils d'interopérabilité pour les
systèmes VMS et VSaaS en nuage pour la sécurité urbaine et le maintien de
l'ordre**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
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 corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online and once a month by email.

IEC 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: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) 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 IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC 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.

IEC Just Published - webstore.iec.ch/justpublished

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

Service Clients - webstore.iec.ch/csc

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

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Video Surveillance Systems (VSS) for use in security applications –
Part 2-11: Video transmission protocols – Interop profiles for VMS and cloud
VSaaS systems for safe cities and law enforcement**

**Systèmes de vidéosurveillance destinés à être utilisés dans les applications de
sécurité –
Partie 2-11: Protocoles de transmission vidéo – Profils d'interopérabilité pour les
systèmes VMS et VSaaS en nuage pour la sécurité urbaine et le maintien de
l'ordre**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 13.320

ISBN 978-2-8322-8828-3

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions and abbreviated terms	8
3.1 Terms and definitions.....	8
3.2 Abbreviated terms.....	8
4 Overview	9
4.1 General.....	9
4.2 Location information	9
4.2.1 Preliminary	9
4.2.2 Detailed location information in 3D and complex spaces.....	10
4.2.3 Special case of infrastructures routinely connected to third parties/authorities	10
4.3 Digital signature.....	10
5 Video System InterOp Profile Requirements	11
5.1 General requirements	11
5.2 Offline-export of collected videos (level 0V)	13
5.2.1 General	13
5.2.2 File format	13
5.2.3 Video codec.....	13
5.2.4 Audio codec.....	13
5.2.5 Static metadata	13
5.2.6 Digital signature	14
5.3 Offline-export with video-metadata &-events (level 0M and 0E).....	14
5.3.1 General	14
5.3.2 Timed metadata.....	14
5.3.3 Events and alarms	14
5.4 Access given to selected cameras (live camera streams with near-real-time replay) (Level 1 V)	14
5.4.1 General	14
5.4.2 Authentication and security.....	14
5.4.3 Camera access.....	15
5.4.4 Live access and replay control.....	15
5.4.5 Real-time streaming.....	15
5.5 Access given to videos and associated metadata (level 1M)	15
5.6 Video operator hand-over to third party (hand-over taken by the authorities) (level 2)	15
5.6.1 General	15
5.6.2 PTZ control.....	15
5.6.3 Analytics.....	15
5.7 Metadata sharing (sharing of the metadata only) (level 3)	15
Annex A (informative) Example of specifications of cartographic data format linked to video-surveillance	16
A.1 General.....	16
A.2 Format and content of the CSV file	16
Bibliography.....	19

Figure 1 – Typical signature scheme.....	11
Figure A.1 –Example of an indoor map (metro system – Paris)	18
Table 1 – Levels	12
Table A.1 – Specification of the document fields	16

IECNORM.COM : Click to view the full PDF of IEC 62676-2-11:2024

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**VIDEO SURVEILLANCE SYSTEMS FOR
USE IN SECURITY APPLICATIONS –****Part 2-11: Video transmission protocols – Interop profiles for VMS and
cloud VSaaS systems for safe cities and law enforcement****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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62676-2-11 has been prepared by IEC technical committee 79: Alarm and electronic security systems. It is an International Standard.

The text of this International Standard is based on the following documents:

Draft	Report on voting
79/697/CDV	79/702/RVC

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 62676 series, 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 document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document 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

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

The IEC 62676 series of standards on video surveillance systems (VSS) is divided into six independent parts:

Part 1: System requirements;

Part 2: Video transmission protocols;

Part 3: Analog and digital video interfaces;

Part 4: Application guidelines;

Part 5: Data specifications and image quality performance for camera devices;

Part 6: Performance testing and grading of real-time intelligent video.

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

Today there is a lack in directive standards giving precise requirements for VSS in certain situations involving third parties (and especially the authorities), compared to intrusion or fire detection alarm systems, while video applications are becoming more important for public security.

In most cases, such situations apply to one or more independent regular operational systems (or systems of systems) and correspond to exceptional events or security incidents where authorities, first responders, etc. need immediate access to the data (video and associated information) through a single third-party Video Management System (VMS) for a timely response.

Since the surveillance systems are a crucial asset in crime prevention, crisis management, or forensic applications to assist the law-enforcement agencies and smart cities, the goal of this document is to provide a fully interoperable interface for VMS and Cloud Video Surveillance-as-a-Service (VSaaS) Systems with third-party:

- security operations centres,
- professional remote video monitoring,
- remote access by law-enforcement and authorities,

for sharing their digital video-surveillance contents and associated metadata.

This document builds upon the IEC 62676 family of standards and complements it. It does not specify any detailed requirements on application guidance and video observation objectives, on system availability, cyber security, privacy, national and legal constraints, operational procedures, environmental conditions, or technical protocols.

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 2-11: Video transmission protocols – Interop profiles for VMS and cloud VSaaS systems for safe cities and law enforcement

1 Scope

Based on the IP video features offered by the IEC 62676-2 protocol series, this document defines minimum requirement profiles for Video Management Systems (VMS) and cloud Video-Surveillance-as-a-Service (VSaaS) Systems to optimize interfacing with third parties.

It defines minimum required VMS interoperability levels from video export to exclusive video control, for the sake of remote support, for example in crisis situations, regulating governmental organizations, national law enforcement, private security service companies, public transport operators and other authorities.

This document is intended to set the common technical basis for national regulations requiring inter-organizational remote, local or on-site access, for example so that authorities can be granted temporary access to the VSS in the case of emergency situations.

This standard is accordingly expected to supersede ISO 22311 (Societal Security – Video-surveillance – Export interoperability).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60839-11-31:2016, *Alarm and electronic security systems – Part 11-31: Electronic access control systems – Core interoperability protocol based on Web services*

IEC 60839-11-32, *Alarm and electronic security systems – Part 11-32: Electronic access control systems – Access control monitoring based on Web services*

IEC 62676 (all parts), *Video surveillance system for use in security applications*

IEC 62676-2-31:2019, *Video surveillance system for use in security applications – Part 2-31: Live streaming and control based on web services*

IEC 62676-2-32:2019, *Video surveillance system for use in security applications – Part 2-32: Recording control and replay based on web services*

IEC 62676-2-33:2022, *Video surveillance system for use in security applications – Part 2-33: Cloud uplink and remote management system access*

ISO 23601, *Safety identification – Escape and evacuation plan signs*

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 14496-12:2022, *Information technology – Coding of audio-visual objects – Part 12: ISO base media file format*

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

ISO/IEC 23008-2, *Information technology – High efficiency coding and media delivery in heterogeneous environments – Part 2: High efficiency video coding*

ITU-T/Rec G.711, *Pulse code modulation (PCM) of voice frequencies*

ITU-T/Rec G.722, *7 kHz audio-coding within 64 kbit/s*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the IEC 62676 series apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.2 Abbreviated terms

FOV	field of view for a camera
GPS	Global Positioning System, the widespread GNSS (global navigation satellite system) for universal geolocation
LEA	law-enforcement agency
PTZ	pan, tilt and zoom of a camera
RTSP	Real Time Streaming Protocol
SVG	Scalable Vector Graphics
TLS	Transport Layer Security
VMS, lower	video management system, installed in single locations
VMS, upper	video management system, connecting as client to the lower VMS
VSaaS	cloud Video Surveillance-as-a-service Systems

4 Overview

4.1 General

The IEC 62676 series of video-surveillance standards has been established to ensure interoperability and performance within systems, whatever their size is, up to systems of systems. The objective of this document, within this family, is to define minimum additional requirements to ensure that all the compliant video-surveillance systems not only perform as expected by their owners, but also can play their societal role by supporting at the same time the relevant authorities. Such authorities can be as diverse as the various first responders, such as police investigators, or as diverse as the services of smart cities, all with varied use cases.

In this context, with the authorities mastering their own assets, this document concentrates on the requirements put on the "low-level" systems producing the videos and associated data, allowing flexibility in the implementation by the "authorities" of their receiving or processing (client) system.

Such requirements rely, for each parameter and feature, on the provisions of the IEC 62676-2 series. For the implementer's convenience, these requirements are associated to functional levels and sub-levels as described in Table 1.

Contrary to the other parts of the IEC 62676-2 series, the above provisions shall accommodate the fact that most of the context relative to the site monitored by the producing system is generally stored locally at the system level and that it is accordingly the responsibility of the producing system to ensure that, whatever video and associated data are transferred to the third party, they are provided with the minimum information to allow understanding by the third-party end-users of the videos in their environment (this is especially true when GPS localization is not enough to show FOV obstacles or masking, such as indoors and in 3D infrastructures).

The other specificity is that, as entities involved are different and information is often sensitive, local or national provisions can apply in relation to information security and privacy; typically, an authentication by a state-of-the-art signature of the information shared is generally expected, as well as the encryption of the transmitted data.

Nevertheless, as subject information is often critical in emergency situations, dispositions shall be taken by the low-level VMS owners to ensure that first responders (and more generally authorities) can have a timely, without pre-notice, access to it in all circumstances.

These specificities are further detailed in 4.2.

4.2 Location information

4.2.1 Preliminary

The location information box ('loci' box) as defined in (3GPP TS 26.244 version 16.1.0, Release 16, Table 8.10) and referred to by IEC 62676-2-32:2019, Clause 9 provides basic information about the location of the capture.

The GPS position as indicated in 3GPP TS 26.244 version 16.1.0 is however often not enough to allow interpretation of the videos by the third party when the monitored environment is 3D, underground structures or on-board vehicles unless special arrangements (as described in 4.2.2) are in place to maintain up-to-date detailed site descriptions in the third-party system.

This is especially true when the third party is connected simultaneously to several adjacent, but different, low-level systems.

4.2.2 Detailed location information in 3D and complex spaces

This gap has already been identified by first-responders for emergency escape situations and is covered by posting mandatory 2D maps derived from ISO 23601. To complement the GPS coordinates, the positions and FOV of the relevant cameras, as well as GPS reference points (to allow correlations and bridges between maps), could easily be added to the map. For universal readability, such maps shall be encoded as PDF files, SVG images or JPEG images.

The difficulty is that, at this stage, the above referenced 'loci' box is not designed to carry such images or drawings. This might change as technology evolves. In the meantime, one of the three following options shall be used:

- Use one of the cameras of the low-level system to carry (full-time or not) a picture of the above-described drawing.
- If providing such image or drawing can be achieved without accessibility risk and without delay, it shall be proposed to give access to the same information through an URL or any other electronics means
- The systematic sharing in advance of the mapping information between the low-level systems and the third parties shall be encouraged, as described in 4.2.3.

Optionally, an extension will allow application of the above to cameras onboard vehicles. For instance, localization onboard the vehicle combined with the position of the vehicle allows to define in front of which point of a platform the door of a train is, where an incident has been detected.

4.2.3 Special case of infrastructures routinely connected to third parties/authorities

When a VMS is scheduled to be routinely used by a third party, the above complexity (see 4.2.2) shall be avoided by transferring the geolocation with each video shared and by sharing once and for all the relevant mapping information.

Annex A describes a possible way to achieve such a transfer of information .

4.3 Digital signature

Several methods, including digital signing, hashing, and encrypting, can be used to secure the contents of an exported file.

The signature identifies the individual responsible for performing the file export as well as any subsequent operations on the exported file and provides some assurance. As called for in IEC 62676-2-32, a signature is generally required when video-surveillance data are exchanged between entities.

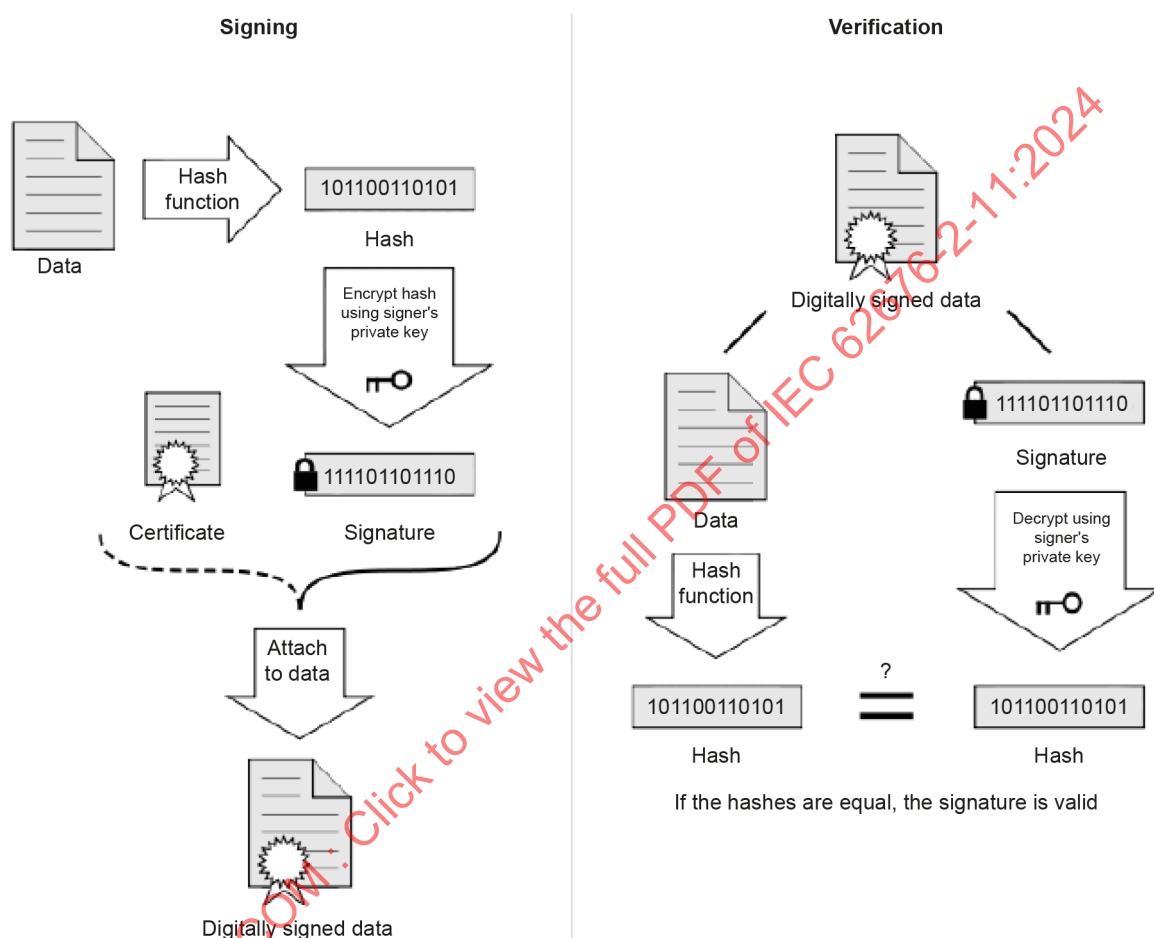
All data a user wishes to carry away separately are put into a metaphorical bag. The bag is then sealed to enable tamper detection. Anyone wanting to use the data from the bag first examines the seal. The data in the bag are identical with the original data as long as the seal is intact; see Figure 1.

Here, the metaphorical bag is represented by a file and the seal is represented by a signature over all data in the file.

The "bag of evidence" approach builds on procedures for media data and related metadata to be securely extracted from a trusted storage in a separate file. This approach defines which metadata have to be preserved in order to provide accurate replay. Data are provided "as is" without any further assertions, whatsoever, to perpetuate evidence.

Processing power reliefs include usage of hash functions before signature algorithms are applied. Multiple stages of signatures might be applied to collect additional information into a single sealed file.

State-of-the-art International Standards are applied for the file structure, and for the hash and signature algorithms. The surveillance application format defined in ISO/IEC 23000-10 and the RSA2048 signature as well as the SHA-256 hash algorithm approved by NIST come into operation for the most widespread interoperability.



IEC

Figure 1 – Typical signature scheme

5 Video System InterOp Profile Requirements

5.1 General requirements

As seen from the source (low-level) system, the key functionalities to meet for satisfying the targeted authorities need are summarized in Table 1, split into 4 generic classes of situations:

- Manual export of files to authorities for forensics investigations (level 0)
- Remote access to live stream given to authorities by the low-level system to some relevant videos during an incident (level 1)
- Hand-over (partial or in-full) taken by the authorities on the low-level systems in case of major incidents or special events (level 2)
- Transfer of the events and/or of analytics (but not of the videos) for non-security usage to an authority, like a smart-city management system (level 3).

In addition to the pure video (and audio, if any) contents, an optional capability allows to cover whatever external events that can be associated with these videos and/or the metadata produced by the analytics running on these video streams.

As stated above, dispositions shall be taken by the low-level VMS owners to ensure that first responders (and more generally authorities) can have a timely, without pre-notice, access to it in all circumstances.

Table 1 – Levels

Content	V (Video only)	M (Video + video Metadata)	E (video + all relevant Events & metadata)
Level 0 Files export for forensics usage	0V – Offline export of collected videos	0M – Offline export with video-metadata.	0E – Offline export with all metadata.
	Basic manual export with minimum features to support investigations with videos from different sources, including a representation of cameras localization and FOV understandable by a 3 rd party and clock double check when exporting. As applicable, this export can rely on a copy on physical removable media or on remote file transfers.	Manual export (0V) with events also embedded to help finding interesting zones in the records.	Manual export with video metadata, external events (0M) and whatever metadata analytics results that could have been produced over the period of interest.
Level 1 Access given to selected cameras	1V – Access given to selected cameras	1M – Access given to videos and associated metadata	
	Access to camera streams provided by the low-level system to a defined client system (typically to first responders and the authorities during an incident).	Access to camera streams (1V) with key events embedded to help operator at client to be alerted by alarms.	
Level 2 Video operator hand-over	2V – Video operator hand-over to third party	2M – Video operator hand-over with Video-metadata	2E – Video operator hand-over with all metadata
	Access to and control live of cameras, including corresponding recently recorded streams, provided by the low-level system to a defined client system (typically to first responders and the authorities during a major incident). The operator of the client system is provided with an understandable representation of cameras localization and FOV.	Same as 2V with relevant events embedded to help operator at client to be alerted by alarms relevant for the cameras monitored.	Same as 2M with also whatever available and localized relevant metadata analytics results.
Level 3 Data sharing without video		3M – Video-metadata sharing	3E – Varied metadata sharing
		Contribution of a low-level video surveillance system to a privacy protective smart city control room (or equivalent), where only time stamped and geo-localized events, but no videos, are provided.	Same as 3M with privacy compliant metadata

These levels correspond to different minimum interoperability requirements which may apply simultaneously to a given system: export of recorded files for forensics investigations and real-time (as well as near-real-time) access to several cameras, allowing to identify the clips to export.

Subclause 5.2 provides for each of the above defined levels (i.e., use cases), the relevant minimum requirements for interoperability.

5.2 Offline-export of collected videos (level 0V)

5.2.1 General

Subclause 5.2 defines the minimum requirements applicable to the file formats used to export the collected contents (video, audio and associated metadata) to achieve interoperability on conducting post-event investigations.

By standardizing the export file format with date and time, data collection will be improved and investigators can effectively triage data acquired from VMS systems. This implies that the time used in 5.2 is the absolute time (UTC) associated with the capture of the relevant video frame or information, which can be different from the VMS ingest time.

5.2.2 File format

Compliant VSS systems shall be able to export video and associated information using ISO Base File Format in accordance with ISO/IEC 14496-12. Exports should make use of fragmented representation for better resilience to errors.

5.2.3 Video codec

A compliant system shall export one video track containing one of the following formats:

- H.264 video in accordance with ISO/IEC 14496-10;
- H.265 video in accordance with ISO/IEC 23008-2.

Devices may support exporting multiple parallel video streams.

5.2.4 Audio codec

In case audio data is included, it shall have its own track as defined in ISO/IEC 14496-12.

The data shall be compressed with one of the following formats:

- G.711 Law A as defined in ITU-T/Rec-G.711;
- G.722 as defined in ITU-T/Rec-G.722; or
- MPEG4-AAC in Low Complexity Profile (AAC-LC), as defined in ISO/IEC 14496-3.

5.2.5 Static metadata

5.2.5.1 General

Subclause 5.2.5 describes the requirement on supplemental static file information.

The file static metadata shall include the following information in the surveillance export box (suep box), as defined in IEC 62676-2-32:2019, Clause 9:

- descriptions of source of the tracks;
- absolute start time; and
- date and time of the export.

5.2.5.2 Location information metadata in export

The location information box ('loci' box) as defined in 3GPP TS 26.244 shall be present and include the GPS position (Long-Lat) of the capture.

Furthermore, if there is a risk of location ambiguity, like in multi-level buildings or underground infrastructures, the location information box shall also contain the GPS location (altitude) of the capture.

A device may provide supplemental information, such as a drawing of the scene via a URL reference. This reference may not be openly accessible for security reasons.

5.2.6 Digital signature

The export file shall include at least one digital signature as defined in IEC 62676-2-32:2019, 9.4 and as described in 4.2 of this document.

5.3 Offline-export with video-metadata &-events (level 0M and 0E)

5.3.1 General

A device supporting level 0M shall fulfil all requirements of level 0V plus those defined in 5.3.2 and 5.3.3.

5.3.2 Timed metadata

The system shall export one metadata track containing scene description and event information as defined in IEC 62676-2-31. The track shall be encoded as 'metx' box as defined in ISO/IEC 14496-12:2022, 12.3.

5.3.3 Events and alarms

The metadata track shall hold all events generated by the data source during the export time interval. For event descriptions, see IEC 60839-11-31:2016, Clause 10 and IEC 62676-2-31:2019, 6.3.8.

For event types not defined in above references, refer to the topic and format definitions provided by the appropriate standards bodies.

5.4 Access given to selected cameras (live camera streams with near-real-time replay) (Level 1 V)

5.4.1 General

A device supporting level 1 shall also support all requirements of level 0V.

5.4.2 Authentication and security

All communication shall be secured by TLS. Both client and server shall use a certificate based on authentication in accordance with RFC 5246 or later.

The VMS shall expose a web service in accordance with IEC 60839-11-31 for commands and events that can be reached via HTTPS.

The VMS shall expose an RTSP server that provides both live and replay media streams over HTTPS, in accordance with IEC 62676-2-31, Clause 10.

5.4.3 Camera access

The VSS shall support discovery of its associated cameras, as defined in IEC 62676-2-33:2022, Clause 7.

5.4.4 Live access and replay control

The VSS shall support access to live video, as defined by IEC 62676-2-31.

The VSS shall support playback of recorded video, audio and metadata as defined in IEC 62676-2-32:2019, Clause 7. Access to recorded material can be restricted to the near past, depending on regulatory requirements.

5.4.5 Real-time streaming

A device supporting level 1 shall support secure media streaming using RTSP over HTTP, as defined in IEC 60839-11-31 and IEC 60839-11-32.

5.5 Access given to videos and associated metadata (level 1M)

A device supporting level 1M shall support all requirements of level 1V.

A conformant device shall support streaming of metadata, including scene description and events over HTTP.

5.6 Video operator hand-over to third party (hand-over taken by the authorities) (level 2)

5.6.1 General

A device supporting level 2 (incl. 2V, 2M and 2E) shall support all requirements specified for levels 0 and 1.

5.6.2 PTZ control

A device supporting level 2 shall support the PTZ service interfaces for the configuration and operation of movable cameras, as defined in IEC 62676-2-31:2019, Clause 8.

5.6.3 Analytics

The analytics service allows configuration of individual rules and individual analytics modules, as defined in IEC 62676-2-31:2019, Clause 9.

5.7 Metadata sharing (sharing of the metadata only) (level 3)

The contents of 5.5 and 5.6 apply, but with video fields not populated.

Annex A (informative)

Example of specifications of cartographic data format linked to video-surveillance

A.1 General

This document aims to define the files format to integrate third-party mapping information into VSS for safe city and law enforcement. It is based on files containing camera information and partner plans.

In order to ensure a security continuum, law enforcement VSS systems aim to federate third-party systems (transport operators, shopping centres, exhibition sites, etc.) via technical devices allowing dialogue between systems. To be effective, the partners' accessible cameras must be represented on maps. In fact, the cartographic data provide operators with the relevant information for the choice of adapted video sources. The sharing of this information from third party systems can be done in the form of CSV files containing data on partner plans and camera locations.

As a prerequisite, the law enforcement VSS must include a cartographic management system.

A.2 Format and content of the CSV file

The mapping information is provided in the form of a reference table listing the cameras, the plans, as well as the navigation links between the plans. The reference table shall be provided in CSV format, with the semicolon as a separator. The fields of the table are the following columns of the CSV file; the order of the columns shall be respected:

Partner; Map; File; Type; ID_Camera; Name; Link; GPS_Pos; HV_Pos; Angle; Icon

These elements are used to:

- position a partner camera on a map (georeferenced or background image);
- integrate a partner plan (image) into the cartographic management system;
- position navigation links between maps.

Table A.1 describes the specifications of the document fields.

Table A.1 – Specification of the document fields

Field	Authorized values	Description
Partner	text	Name of partner. This unique identifier is used as a key for the association of all the resources of the third-party system.
Map	text	Name of the georeferenced map or site map. This unique identifier is used as a key for the association of objects on the card.
File	text	URL to access the site map image file (JPEG or PNG). Only used when the field Type = 'Map' (i.e. when a plan is integrated into the cartographic management system).
Type	'Map','Camera','Place'	Map: a site map to import or update. Camera: a camera to place on a georeferenced map or a sitemap in image format. Place: a navigation link to place on a map or site map. The navigation link will take you to another map or plan.

Field	Authorized values	Description
ID_Camera	text	Camera identifier in the third-party system. Only used when the field type = 'Camera'. For these objects, this field is used as a correspondence key with the configuration database of the video system. For a given partner, this field shall therefore be unique.
Name	text	Name displayed near the object on the georeferenced map or site map. Only used when the field type = 'Camera' or 'Place'.
Link	text	Name of the map or site map to be reached by a 'Place' type object. Only used when the field type = 'Place'
GPS_Pos	'POINT'(GPS coordinates)	Latitude and longitude in WGS84 format in decimal degrees. This field shall be completed only if the resource concerned needs to be placed on a georeferenced map (empty field if object placed on a site map image file).
HV_Pos	'POINT'(number, number) or 'POLYGON' (number, number, number)	'POINT'(number, number): Point position of an object of type 'Camera' or 'Place' on the site map image file, value expressed in pixels from the top left corner of the image. 'POLYGON' (number, number, number): polygon space of a 'Place' object on the site map image file, value expressed in pixels from the top left corner of the image This field shall be completed only if the object is to be placed on a site map image file (empty field if object placed on a georeferenced map).
Angle	number [0-359]	Angle (0-359) characterizing the orientation of the camera object (clockwise, 0 ° = 12 h).
Icon	text	Icon set representing the 'Place' or 'Camera' objects

EXAMPLE 1

Integration of the level -1 plan of the Gare du Nord:

SNCF; Gare_du_Nord_-1; 192.168.0.10/Map/SNCF/Gare_du_Nord_-1.png; Map;;;;; ,

In that case the fields, ID_Camera, Name, Link, GPS_Pos, HV_Pos, Angle and Icon are empty.

EXAMPLE 2

Positioning on the georeferenced cartography of an exterior camera of the municipality of Versailles:

Versailles; Map_Outdoor_Paris_Area;; Camera; 12345; Camera 23 Versailles;; POINT(48.80,2.133);; 255 , /icon_type_camera1.jpg

In that case, the fields File, Link and HV_Pos are empty.

EXAMPLE 3

Positioning of an indoor camera in the Champs Elysées metro station:

RATP; Map_RATP_Metro_Champs_Elysees;; Camera; 34567; Camera Quai Ligne 2;; POINT(356;222)..; 10 , /icon_type_camera1.jpg

In that case, the fields File, Link and GPS_Pos are empty.

EXAMPLE 4

Positioning of a navigation link from the georeferenced outdoor map to the Louvre museum map:

Louvre; Map__Outdoor_Paris_Area;; Place;; Musée du Louvre; Map_Louvre_museum; POINT(48.86,2.33);; ..; , /icon_type_museum.jpg

In that case, the fields File, ID_Camera HV_Pos Angle are empty.

EXAMPLE 5

Positioning of a navigation link from the interior plane of level -1 Gare du Nord to the plane of level -2 Gare du Nord:

SNCF; Gare_du_Nord_-1 ;; Place;; Niveau -2; Gare_du_Nord_-2;; POLYGON(22; 45, 66, 18, 22); , /icon_type_navigation.jpg

In that case, the fields File, GPS_Pos and Angle are empty.

Figure A.1 shows an example of an indoor map with camera and navigation links:

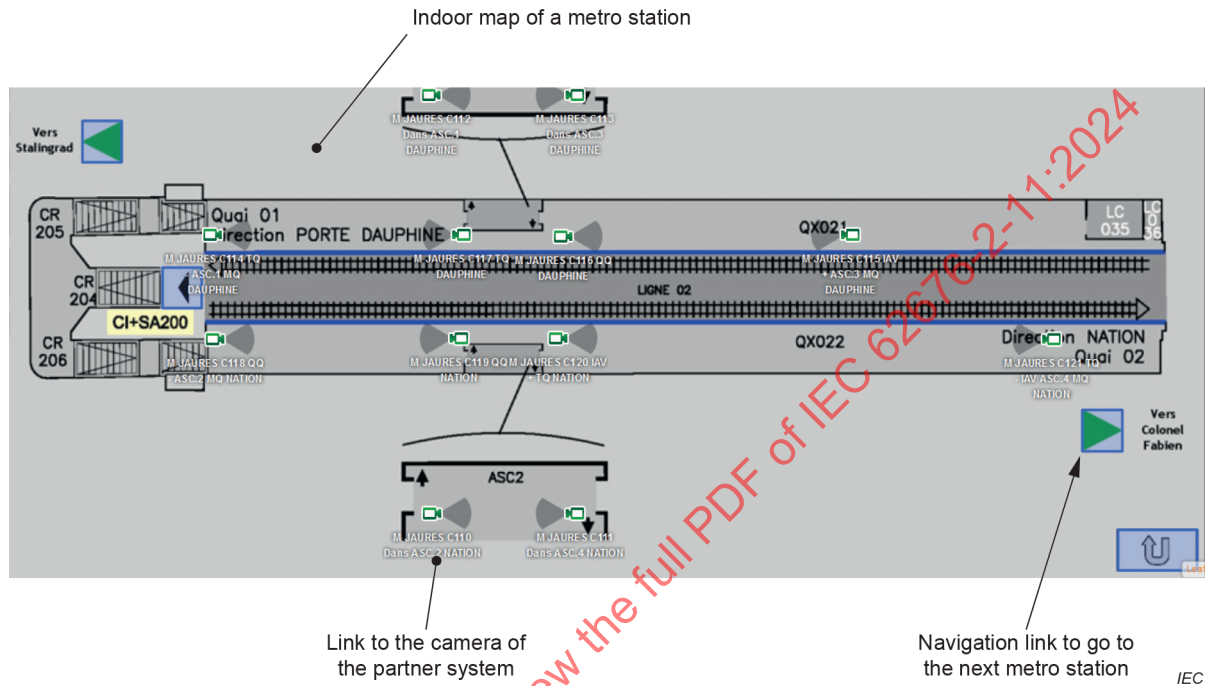


Figure A.1 –Example of an indoor map (metro system – Paris)

Bibliography

ISO 30137-4, *VSS Biometrics – Biometrical Data in Image Streams*

TS 50136-9, *Alarm systems – Alarm transmission systems and equipment – Part 9: Requirements for common protocol for alarm transmission using the Internet Protocol (IP)*

IEC TS 60839-7-8, *Alarm systems – Part 7-8: Message formats and protocols for serial data interfaces in alarm transmission systems – Requirements for common protocol for alarm transmission using the Internet protocol*

3GPP TS 26.244 v16.1.0 Release 16, *Transparent end-to-end packet switched streaming service (PSS); 3GPP file format (3GP)*

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

IECNORM.COM : Click to view the full PDF of IEC 62676-2-11:2024

SOMMAIRE

AVANT-PROPOS	22
INTRODUCTION.....	24
1 Domaine d'application	25
2 Références normatives	25
3 Termes, définitions et abréviations	26
3.1 Termes et définitions	26
3.2 Abréviations.....	26
4 Vue d'ensemble	27
4.1 Généralités	27
4.2 Informations de localisation	28
4.2.1 Informations préliminaires.....	28
4.2.2 Informations de localisations détaillées en 3D et dans des espaces complexes	28
4.2.3 Cas particulier des infrastructures couramment connectées à des tiers/autorités	28
4.3 Signature numérique.....	29
5 Exigences relatives aux profils d'interopérabilité des systèmes vidéo	30
5.1 Exigences générales.....	30
5.2 Export hors ligne des vidéos collectées (niveau 0V).....	32
5.2.1 Généralités	32
5.2.2 Format de fichier	32
5.2.3 Codec vidéo	32
5.2.4 Codec audio	32
5.2.5 Métadonnées statiques	33
5.2.6 Signature numérique	33
5.3 Export hors ligne avec les métadonnées et événements vidéo (niveaux 0M et 0E).....	33
5.3.1 Généralités	33
5.3.2 Métadonnées variables au cours du temps	33
5.3.3 Événements et alarmes	33
5.4 Accès aux caméras sélectionnées (flux de caméras en direct avec possibilité de lecture en léger différé) (niveau 1 V)	34
5.4.1 Généralités	34
5.4.2 Authentification et sécurité	34
5.4.3 Accès aux caméras	34
5.4.4 Accès en direct et contrôle de la relecture	34
5.4.5 Flux en temps réel	34
5.5 Accès aux vidéos et aux métadonnées associées (niveau 1M).....	34
5.6 Transfert de contrôle de l'opérateur vidéo à un tiers (prise de contrôle par les autorités) (niveau 2)	34
5.6.1 Généralités	34
5.6.2 Contrôle PTZ	34
5.6.3 Analyses.....	35
5.7 Partage de métadonnées (partage des métadonnées uniquement) (niveau 3)	35
Annexe A (informative) Exemple de spécifications de format de données cartographiques liées à la vidéosurveillance	36
A.1 Généralités	36

A.2 Format et contenu du fichier CSV	36
Bibliographie.....	39
Figure 1 – Schéma de signature type.....	30
Figure A.1 – Exemple de carte intérieure (Métro – Paris).....	38
Tableau 1 – Niveaux	31
Tableau A.1 – Spécification des champs du document.....	36

IECNORM.COM : Click to view the full PDF of IEC 62676-2-11:2024

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**SYSTÈMES DE VIDÉOSURVEILLANCE DESTINÉS À ÊTRE
UTILISÉS DANS LES APPLICATIONS DE SÉCURITÉ –****Partie 2-11: Protocoles de transmission vidéo –
Profils d'interopérabilité pour les systèmes VMS et VSaaS
en nuage pour la sécurité urbaine et le maintien de l'ordre**

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – 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 l'IEC"). 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 l'IEC, participent également aux travaux. L'IEC 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 l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC 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 l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC 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 l'IEC. L'IEC 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 l'IEC, 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 l'IEC, 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 l'IEC ou de toute autre Publication de l'IEC, 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'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'a pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse <https://patents.iec.ch>. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de propriété.

L'IEC 62676-2-11 a été établie par le comité d'études 79 de l'IEC: Systèmes d'alarme et de sécurité électroniques Il s'agit d'une Norme internationale.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
79/697/CDV	79/702/RVC

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

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications/.

Une liste de toutes les parties de la série IEC 62676, publiées sous le titre général *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité*, se trouve sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

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

INTRODUCTION

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

La série de normes IEC 62676 qui traite des systèmes de vidéosurveillance (VSS, Video Surveillance Systems) est divisée en six parties indépendantes:

Partie 1: Exigences systèmes – Généralités;

Partie 2: Protocoles de transmission vidéo;

Partie 3: Interfaces vidéo analogiques et vidéo numériques;

Partie 4: Directives d'application;

Partie 5: Spécifications des données et performances de la qualité d'image pour les dispositifs de caméra;

Partie 6: Essai de performance et classification des dispositifs et systèmes d'analyse intelligente en temps réel de contenus vidéo destinés aux applications de vidéosurveillance.

Chaque partie possède ses propres articles pour le domaine d'application, les références normatives, les définitions et les exigences.

Contrairement à ce qu'il se passe pour les systèmes d'alarme de détection d'intrusion ou d'incendie, on observe actuellement un manque de normes directives contenant des exigences précises pour les VSS confrontés à certaines situations impliquant des tiers (et en particulier les autorités), alors que l'importance des applications vidéo pour la sécurité publique ne cesse de croître.

Dans la plupart des cas, ces situations mettent en jeu un ou plusieurs systèmes opérationnels classiques indépendants (ou systèmes de systèmes) en réponse à des événements exceptionnels ou à des incidents de sécurité pour lesquels il est nécessaire que les autorités, les primo-intervenants, etc. disposent sans délai d'un accès immédiat aux données (vidéo et informations associées) via un système de gestion vidéo (VMS, Video Management System) tiers unique permettant de garantir une réponse rapide.

Les systèmes de surveillance constituant un outil capital dans la prévention du crime, la gestion des crises ou les enquêtes judiciaires en support aux forces de l'ordre et aux villes intelligentes, l'objectif du présent document est de fournir une interface garantissant l'interopérabilité complète pour les systèmes VMS et de vidéosurveillance en tant que service (VSaaS, Video Surveillance-as-a-Service) en nuage avec les tiers tels que:

- les centres des opérations de sécurité,
- la télésurveillance vidéo professionnelle,
- l'accès à distance par les forces de l'ordre et les autorités,

afin de partager leur contenu de vidéosurveillance numérique et les métadonnées associées.

Le présent document s'appuie sur la famille de normes IEC 62676 et la complète. Il ne spécifie aucune exigence détaillée concernant les recommandations d'application et la nature de l'observation vidéo, ni sur la disponibilité des systèmes, la cybersécurité, la confidentialité, les contraintes nationales et juridiques, les procédures opérationnelles, les conditions d'environnement ou les protocoles techniques.

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

Partie 2-11: Protocoles de transmission vidéo – Profils d'interopérabilité pour les systèmes VMS et VSaaS en nuage pour la sécurité urbaine et le maintien de l'ordre

1 Domaine d'application

À partir des fonctionnalités de vidéo sous IP offertes par la série de protocoles de l'IEC 62676-2, le présent document définit des profils d'exigences minimales pour les systèmes de gestion vidéo (VMS) et de vidéosurveillance en tant que service (VSaaS) en nuage afin d'optimiser l'interfaçage avec les systèmes tiers.

Il définit les niveaux d'interopérabilité minimaux exigés entre VMS, de l'export de vidéos à une prise en main complète à distance, à des fins d'assistance, par exemple, dans les situations de crise, pour les organismes gouvernementaux de réglementation, les forces de l'ordre nationales, les sociétés de services de sécurité privée, les opérateurs de transport public et autres autorités.

Le présent document vise à fournir une base technique commune aux réglementations nationales qui exigent un accès inter-organisationnel aux VSS (à distance, en local ou sur site), par exemple pour que des autorités puissent s'y connecter de façon temporaire en cas d'urgence.

La présente norme est destinée à remplacer l'ISO 22311 (Sécurité sociétale – Vidéosurveillance – Interopérabilité de l'export).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. 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).

IEC 60839-11-31:2016, *Systèmes d'alarme et de sécurité électroniques – Partie 11-31: Systèmes de contrôle d'accès électronique – Protocole de base d'interopérabilité en fonction des services Web*

IEC 60839-11-32, *Systèmes d'alarme et de sécurité électroniques – Partie 11-32: Systèmes de contrôle d'accès électronique – Commande de contrôle d'accès en fonction des services Web*

IEC 62676 (toutes les parties), *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité*

IEC 62676-2-31:2019, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2-31: Transmission en continu en direct et contrôle basé sur les services web*

IEC 62676-2-32:2019, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2-32: Contrôle d'enregistrement et lecture en fonction des services Web*

IEC 62676-2-33:2022, *Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2-33: Liaison montante au nuage et accès au système de gestion à distance*

ISO 23601, *Identification de sécurité – Plans d'évacuation et de secours*

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

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

ISO/IEC 14496-12:2022, *Technologies de l'information – Codage des objets audiovisuels – Partie 12: Format ISO de base pour les fichiers médias*

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

ISO/IEC 23008-2, *Technologies de l'information – Codage à haute efficacité et livraison des médias dans des environnements hétérogènes – Partie 2: Codage vidéo à haute efficacité*

UIT-T/Rec G.711, *Modulation par impulsions et codage (MIC) des fréquences vocales*

UIT-T/Rec G.722, *Codage audiofréquence à 7 kHz à un débit inférieur ou égal à 64 kbit/s*

RFC 5246, *Protocole Sécurité de la couche Transport (TLS) version 1.2*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de la série IEC 62676 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <https://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>

3.2 Abréviations

FOV (Field Of View)	champ de vision d'une caméra
GPS (Global Positioning System)	système mondial de localisation, GNSS (Global Navigation Satellite System, système mondial de navigation par satellite) largement répandu pour la géolocalisation universelle
LEA (Law-Enforcement Agency)	forces de l'ordre
PTZ (Pan Tilt and Zoom)	panoramique, inclinaison et zoom (se dit d'une caméra capable d'être pilotée angulairement et de zoomer)
RTSP (Real Time Streaming Protocol)	protocole de flux en temps réel
SVG (Scalable Vector Graphics)	graphiques vectoriels adaptables
TLS (Transport Layer Security)	sécurité de la couche transport

VMS, lower (Video Management System), inférieur	système de gestion vidéo local
VMS, upper (Video Management System), supérieur	système de gestion vidéo, qui se connecte en tant que client aux VMS inférieurs
VSaaS (Video Surveillance-as-a-Service)	systèmes de vidéosurveillance en tant que service en nuage

4 Vue d'ensemble

4.1 Généralités

La série de normes de vidéosurveillance IEC 62676 a été établie afin d'assurer l'interopérabilité et les performances à l'intérieur des systèmes, quelle que soit leur taille, jusqu'aux systèmes de systèmes. L'objectif du présent document, au sein de cette famille, est de définir des exigences minimales supplémentaires pour assurer que tous les systèmes de vidéosurveillance conformes fonctionnent non seulement comme l'attendent leurs propriétaires, mais puissent aussi jouer leur rôle sociétal en assistant également les autorités compétentes. Ces autorités peuvent être aussi diverses que les différents primo-intervenants, les enquêteurs de la police ou les services des villes intelligentes, le tout avec des cas d'utilisation variés.

Dans ce contexte, où les autorités gèrent leurs propres infrastructures, le présent document porte sur les exigences imposées aux systèmes de "niveau inférieur" qui produisent les vidéos et données associées, pour permettre une certaine souplesse d'utilisation par les "autorités" via leur système de réception ou d'exploitation (client).

Ces exigences s'appuient, pour chaque paramètre et fonctionnalité, sur les dispositions de la série IEC 62676-2. Pour en faciliter la mise en œuvre, ces exigences sont associées à des niveaux et sous-niveaux fonctionnels qui sont décrits dans le Tableau 1.

Contrairement à ce qui est le cas pour les autres parties de la série IEC 62676-2, les dispositions ci-dessus doivent tenir compte du fait que la majeure partie du contexte relatif au site surveillé par le système source y reste généralement stockée localement et qu'il incombe par conséquent au système source de s'assurer que, quelles que soient les vidéos et données associées transférées au tiers, celles-ci soient fournies avec les informations minimales pour permettre à ce tiers de comprendre les vidéos dans l'environnement correspondant (cela est particulièrement vrai lorsque la localisation GPS ne suffit pas pour localiser les obstacles ou le masquage du champ de vision des caméras, notamment à l'intérieur et dans les infrastructures en 3D).

L'autre spécificité est que, comme les entités concernées sont différentes et que les informations sont souvent sensibles, des dispositions locales ou nationales peuvent s'appliquer en matière de sécurité et de confidentialité; en général, une authentification par une signature (conforme à l'état de la technique) des informations partagées est attendue, ainsi que le chiffrement des données transmises.

Néanmoins, comme les informations en question sont souvent essentielles dans les situations d'urgence, des dispositions doivent être prises par les propriétaires du VMS de niveau inférieur pour assurer que les primo-intervenants (et plus généralement les autorités) puissent y avoir accès sans délai, ni préavis et en toutes circonstances.

Ces spécificités sont décrites plus en détail au 4.2.

4.2 Informations de localisation

4.2.1 Informations préliminaires

La case d'information relative à la localisation (case "loci") définie dans le document (3GPP TS 26.244 v16.1.0 Release 16, Tableau 8.10) et traitée à l'Article 9 de l'IEC 62676-2-32:2019 fournit des informations de base sur la localisation de la capture.

La position GPS indiquée dans le document 3GPP TS 26.244 version 16.1.0 n'est toutefois souvent pas suffisante pour permettre l'interprétation des vidéos par le tiers lorsque l'environnement surveillé est en 3D, dans des structures souterraines ou à bord de véhicules, si ne sont pas mises en place des dispositions spéciales (décrites au 4.2.2) pour maintenir à jour, dans le système tiers, les descriptions détaillées du site.

Cela est particulièrement vrai lorsque le tiers est connecté simultanément à plusieurs systèmes de niveau inférieur physiquement adjacents, mais différents.

4.2.2 Informations de localisations détaillées en 3D et dans des espaces complexes

Cette difficulté à se localiser a déjà été identifiée par les primo-intervenants confrontés aux évacuations d'urgence et est couverte par l'affichage obligatoire de cartes en 2D selon l'ISO 23601. Pour compléter les coordonnées GPS, les positions et champs de vision des caméras concernées, ainsi que les points de référence GPS (pour permettre des corrélations et des correspondances entre les cartes), peuvent facilement être ajoutés à la carte. En vue d'une lisibilité universelle, ces cartes doivent être codées, sous forme de fichiers PDF ou d'images SVG ou JPEG.

La difficulté réside dans le fait qu'à ce stade, la case "loci" susmentionnée n'est pas conçue pour comporter une telle image ou un tel schéma, mais cela peut être amené à changer avec l'évolution de la technologie. En attendant, l'une des trois options suivantes doit être retenue:

- utiliser l'une des caméras du système de niveau inférieur pour faire remonter (à temps plein ou non) une image du schéma décrit ci-dessus;
- si une telle image ou un tel schéma peuvent être obtenus sans risque pour l'accessibilité et sans délai, il doit être proposé de donner accès à ces mêmes informations par le biais d'une URL ou de tout autre moyen électronique;
- le partage systématique à l'avance des informations de cartographie entre les systèmes de niveau inférieur et les tiers doit être encouragé, comme cela est décrit au 4.2.3.

En option, une extension permettra d'appliquer ce qui précède aux caméras embarquées dans des véhicules. Par exemple, la localisation à bord du véhicule combinée à la position du véhicule permet de définir devant quel point d'un quai se trouve la porte d'un train dans lequel un incident a été détecté.

4.2.3 Cas particulier des infrastructures couramment connectées à des tiers/autorités

Lorsqu'il est prévu qu'un VMS soit régulièrement utilisé par un tiers, la complexité décrite ci-dessus (4.2.2) doit être évitée en transférant la géolocalisation avec chaque vidéo partagée et en partageant une fois pour toutes les informations cartographiques pertinentes.

L'Annexe A décrit une manière possible de réaliser ce transfert d'informations.

4.3 Signature numérique

Plusieurs méthodes, dont la signature numérique, le hachage et le chiffrement, peuvent être utilisées pour sécuriser le contenu d'un fichier exporté.

La signature identifie la personne responsable de l'export du fichier ainsi que de toute opération ultérieure sur le fichier exporté et fournit une certaine assurance. Comme le prévoit l'IEC 62676-2-32, une signature est généralement exigée lorsque des données de vidéosurveillance sont échangées entre des entités.

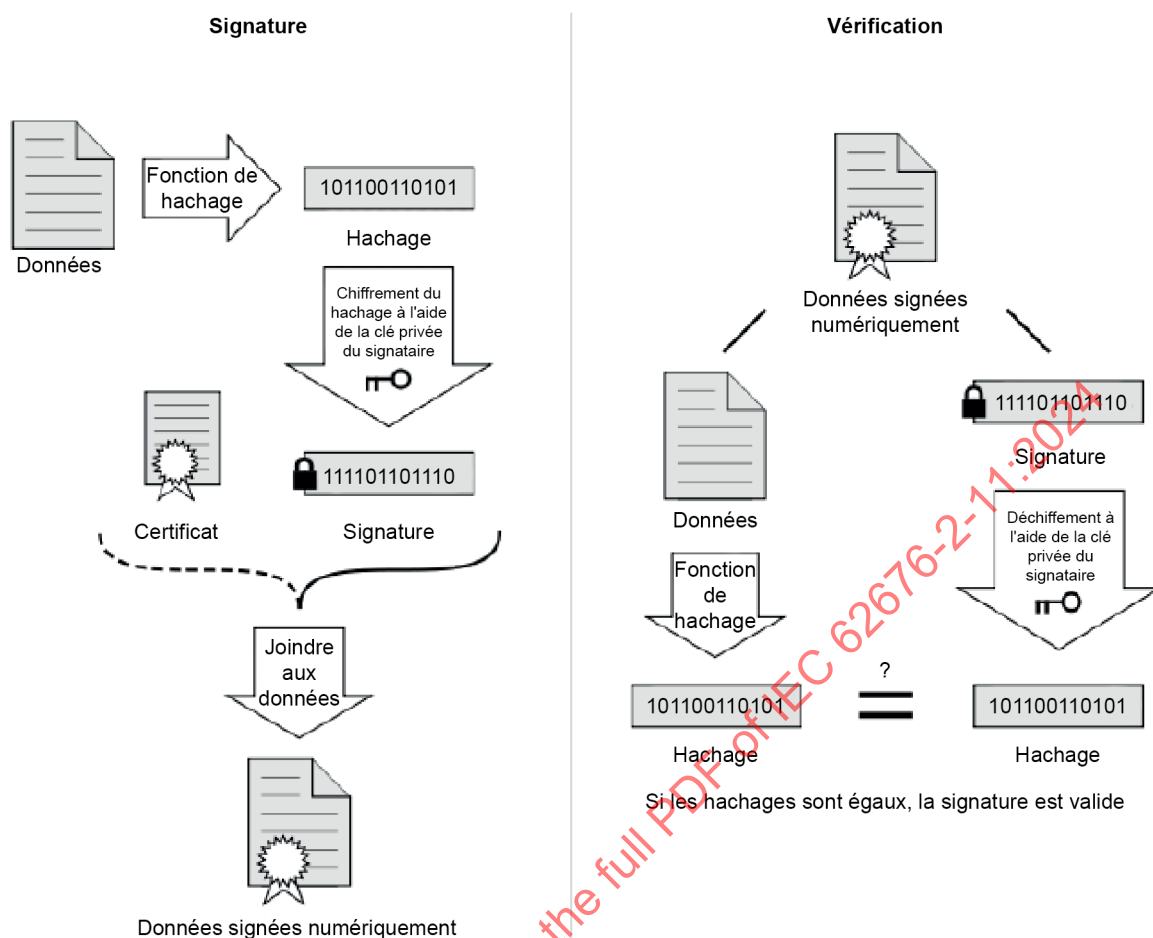
Toutes les données qu'un utilisateur souhaite acheminer séparément sont placées dans un contenant métaphorique. Le contenant est ensuite scellé afin de détecter toute violation. Toute personne qui souhaite utiliser les données du contenant examine en premier lieu le sceau. Les données du contenant sont identiques aux données d'origine tant que le sceau est intact; voir la Figure 1.

Ici, le contenant métaphorique est représenté par un fichier et le sceau est représenté par une signature pour toutes les données du fichier.

L'approche "à preuves multiples" repose sur des procédures applicables aux données multimédias et aux métadonnées associées, à extraire en toute sécurité d'un emplacement de stockage fiable dans un fichier distinct. Cette approche définit les métadonnées qui doivent être protégées afin d'assurer une lecture exacte. Les données sont fournies "telles qu'elles" sans assertion complémentaire, de quelque nature que ce soit, afin de conserver les preuves.

Les décharges de puissance de traitement comprennent l'utilisation de fonctions de hachage avant l'application des algorithmes de signature. Plusieurs niveaux de signatures peuvent être appliqués afin de recueillir les informations complémentaires dans un seul fichier scellé.

Des Normes internationales conformes à l'état de la technique sont appliquées pour la structure du fichier, ainsi que pour les algorithmes de hachage et de signature. Le format d'application de surveillance défini par l'ISO/IEC 23000-10 et la signature RSA2048 ainsi que l'algorithme de hachage SHA-256 agréé par le NIST sont mis en œuvre pour l'interopérabilité la plus étendue.



IEC

Figure 1 – Schéma de signature type

5 Exigences relatives aux profils d'interopérabilité des systèmes vidéo

5.1 Exigences générales

Vues du système source (niveau inférieur), les principales fonctionnalités à satisfaire pour répondre aux besoins des autorités ciblées sont récapitulées dans le Tableau 1 et réparties selon quatre classes génériques de situations:

- export manuel de fichiers à destination des autorités à des fins d'enquête judiciaire (niveau 0);
- accès à distance au flux en direct accordé aux autorités par le système de niveau inférieur pour certaines vidéos pertinentes lors d'un incident (niveau 1);
- transfert de contrôle (partiel ou total) des systèmes de niveau inférieur aux autorités en cas d'incidents majeurs ou d'événements spéciaux (niveau 2);
- transfert des événements et/ou des analyses (mais pas des vidéos) à une autorité pour une utilisation non liée à la sécurité, comme un système de gestion de ville intelligente, (niveau 3).

Outre le contenu purement vidéo (et audio, le cas échéant), une fonctionnalité facultative permet de couvrir tous les événements externes qui peuvent être associés à ces vidéos et/ou aux métadonnées produites par l'analyse de ces flux vidéo.

Comme cela est indiqué ci-dessus, des dispositions doivent être prises par les propriétaires du VMS de niveau inférieur pour s'assurer que les primo-intervenants (et plus généralement les autorités) peuvent y avoir accès en temps utile, sans préavis et en toutes circonstances.

Tableau 1 – Niveaux

Contenu	V (vidéo uniquement)	M (vidéo + métadonnées vidéo)	E (vidéo + tous les événements et toutes les métadonnées pertinents)
Niveau 0 Export de fichiers à des fins d'enquête judiciaire	0V – Export hors ligne des vidéos collectées	0M – Export hors ligne avec les métadonnées vidéo	0E – Export hors ligne avec toutes les métadonnées
	Export manuel de base avec des fonctionnalités minimales pour aider les enquêtes, comportant des vidéos en provenance de différentes sources et une représentation de la localisation et du champ des caméras compréhensible par un tiers, avec une double vérification de l'horloge lors de l'export. Le cas échéant, cet export peut se faire avec une copie sur support physique amovible ou des transferts de fichiers à distance.	Export manuel (0V) comportant également les événements pour aider à trouver les zones d'intérêt dans les enregistrements.	Export manuel avec les métadonnées vidéo, les événements externes (0M) et toutes les métadonnées de résultats d'analyse qui ont pu être produits sur la période d'intérêt.
Niveau 1 Accès donné aux caméras sélectionnées	1V – Accès donné aux caméras sélectionnées	1M – Accès aux vidéos et aux métadonnées associées	
	Accès aux flux des caméras accordé par le système de niveau inférieur vers un système client défini (en général aux primo-intervenants ou aux autorités lors d'un incident).	Accès donné aux flux des caméras (1V) avec des événements clés intégrés pour permettre à l'opérateur du système client d'être alerté par des alarmes.	
Niveau 2 Transfert de contrôle de l'opérateur vidéo	2V – Transfert de contrôle de l'opérateur vidéo à un tiers	2M – Transfert de contrôle de l'opérateur sur vidéos et métadonnées vidéo associées	2E – Transfert de contrôle de l'opérateur vidéo sur les vidéos et toutes les métadonnées associées
	Accès et contrôle en direct des caméras, y compris des flux récemment acquis par ces caméras, généré par le système de niveau inférieur à un système client défini (en général aux primo-intervenants ou aux autorités lors d'un incident majeur). L'opérateur du système client est assisté par une représentation compréhensible de la localisation et du champ de vision des caméras.	Comme pour 2V, avec des événements pertinents intégrés pour permettre à l'opérateur du système client d'être alerté par les alarmes relatives aux caméras concernées.	Comme pour 2M, avec en outre toutes les métadonnées résultats d'analyse pertinentes, disponibles et localisées.
Niveau 3 Partage de données sans vidéo		3M – Partage des métadonnées vidéo	3E – Partage de différentes métadonnées
		Contribution d'un système de vidéosurveillance de niveau inférieur à une salle de commande de ville intelligente (ou équivalent) qui garantit la confidentialité et où seuls sont fournis des événements horodatés et géolocalisés, mais pas de vidéos.	Comme pour 3M, avec des métadonnées respectant les règles de confidentialité.

Ces niveaux correspondent à différentes exigences minimales relatives à l'interopérabilité qui peuvent s'appliquer simultanément à un système donné, comme l'export de fichiers enregistrés à des fins d'enquête judiciaire, et l'accès en temps réel (et en temps quasi réel) à plusieurs caméras, permettant d'identifier les clips à exporter.

Le Paragraphe 5.2 fournit, pour chacun des niveaux définis ci-dessus (c'est-à-dire les cas d'utilisation), les exigences minimales d'interopérabilité pertinentes.

5.2 Export hors ligne des vidéos collectées (niveau 0V)

5.2.1 Généralités

Le Paragraphe 5.2 définit les exigences minimales applicables aux formats de fichier utilisés pour exporter les contenus collectés (vidéo, audio et métadonnées associées) afin d'assurer l'interopérabilité nécessaire aux enquêtes après un événement.

En normalisant le format de fichier d'export avec la date et l'heure, la collecte des données est améliorée et les enquêteurs peuvent trier efficacement les données acquises à partir des systèmes VMS. Cela implique que l'heure utilisée en 5.2 soit l'heure absolue (UTC) associée à la capture de la trame vidéo ou de l'information pertinente, qui peut être différente de l'heure d'ingestion du VMS.

5.2.2 Format de fichier

Les systèmes VSS conformes doivent être capables d'exporter la vidéo et les informations associées en utilisant le format de fichier de base ISO selon l'ISO/IEC 14496-12. Il convient que les exports utilisent une représentation fragmentée pour une meilleure résilience aux erreurs.

5.2.3 Codec vidéo

Un système conforme doit exporter une piste vidéo selon l'un des formats suivants:

- vidéo H.264 selon l'ISO/IEC 14496-10;
- vidéo H.265 selon l'ISO/IEC 23008-2.

Les dispositifs peuvent prendre en charge l'export de plusieurs flux vidéo en parallèle.

5.2.4 Codec audio

Si des données audio sont incluses, elles doivent disposer de leur propre piste, comme cela est défini dans l'ISO/IEC 14496-12.

Les données doivent être compressées selon l'un des formats suivants:

- G.711 loi A, comme défini dans la Recommandation G.711 de l'UIT-T;
- G.722, comme défini dans la Recommandation G.722 de l'UIT-T; ou
- MPEG4-AAC en profil de faible complexité (AAC-LC), comme défini dans l'ISO/IEC 14496-3.

5.2.5 Métadonnées statiques

5.2.5.1 Généralités

Le 5.2.5 décrit les exigences relatives aux informations statiques supplémentaires des fichiers.

Les métadonnées statiques du fichier doivent inclure les informations suivantes dans la case d'export de surveillance (suep box), définie dans l'Article 9 de l'IEC 62676-2-32:2019:

- description de la source des pistes;
- heure absolue de début; et
- date et heure de l'export.

5.2.5.2 Métadonnées d'informations de localisation dans l'export

La case d'information relative à la localisation (case "loci") définie dans le document 3GPP TS 26.244 doit être présente et inclure la position GPS (longitude-latitude) de la capture.

En outre, s'il existe un risque d'ambiguïté quant à la localisation, par exemple dans les bâtiments à plusieurs niveaux ou les infrastructures souterraines, la case d'information relative à la localisation doit également contenir l'information d'altitude GPS de la capture.

Un dispositif peut fournir des informations supplémentaires comme un schéma de la scène par le biais d'une référence URL. Cette référence peut ne pas être librement accessible pour des raisons de sécurité.

5.2.6 Signature numérique

Le fichier d'export doit comporter au moins une signature numérique, comme défini au 9.4 de l'IEC 62676-2-32:2019 et comme décrit au 4.2 du présent document.

5.3 Export hors ligne avec les métadonnées et événements vidéo (niveaux 0M et 0E)

5.3.1 Généralités

Un dispositif qui prend en charge le niveau 0M doit satisfaire à toutes les exigences du niveau 0V ainsi qu'à celles définies au 5.3.2 et au 5.3.3.

5.3.2 Métadonnées variables au cours du temps

Le système doit exporter une piste de métadonnées qui contient une description de la scène et des informations relatives à l'événement, comme défini dans l'IEC 62676-2-31. La piste doit être codée comme la case "metx" définie au 12.3 de l'ISO/IEC 14496-12.

5.3.3 Événements et alarmes

La piste de métadonnées doit comporter tous les événements générés par la source de données pendant l'intervalle de temps objet de l'export. Pour la description des événements, voir l'Article 10 de l'IEC 60839-11-31:2016 et le 6.3.8 de l'IEC 62676-2-31:2019.

Pour les types d'événements non définis dans les références ci-dessus, se référer aux définitions et formats fournis par les organismes de normalisation compétents.