IEC 62676-2-2

Edition 1.0 2013-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité –
Partie 2-2: Protocoles de transmission vidéo – Mise en œuvre de l'interopérabilité IP en fonction des services HTTP et REST

IEC 62676-2-2:2013

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It also gives information on projects, replaced and withdrawn publications.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 62676-2-2

Edition 1.0 2013-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité – Partie 2-2: Protocoles de transmission vidéo – Mise en œuvre de l'interopérabilité IP en fonction des services HTTP et REST

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX XF

ICS 13.320

ISBN 978-2-8322-1188-5

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 2-2: Video transmission protocols – IP interoperability implementation based on HTTP and REST services

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 62676-2-2 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
79/436/FDIS	79/449/RVD

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

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

A list of all 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 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.

INTRODUCTION

The IEC Technical Committee 79 in charge of alarm and electronic security systems together with many governmental organisations, test houses and equipment manufacturers have 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 62676-2 series consists of 3 subparts, numbered parts 2-1, 2-2 and 2-3 respectively:

IEC 62676-2-1, *Video transmission protocols – General requirements*

IEC 62676-2-2, *Video transmission protocols – IP interoperability implementation based on HTTP and REST services*

IEC 62676-2-3, *Video transmission protocols – IP interoperability implementation based on Web services*

This second subpart of this IEC 62676-2 series covers IP interoperability implementation based on HTTP and REST services. It is based on the requirements for IP video transmission protocols covered in IEC 62676-2-1, which defines protocol requirements to be fulfilled by any high-level IP video device interface.

VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

Part 2-2: Video transmission protocols – IP interoperability implementation based on HTTP and REST services

1 Scope

This part of IEC 62676 specifies a compliant IP video protocol based on HTTP and REST services.

Video transmission devices are often equipped with web servers that respond to HTTP requests. The HTTP response may contain XML content (for GET actions), XML response information (for SET actions), or various text/binary content (for retrieval of configuration data, etc.). REST is an approach to creating services that expose all information as resources in a uniform way. The ease of using REST is its uniform interface for operations. Since everything is represented as a resource, create, retrieve, update, and delete (CRUD) operations use the same URI. This specification leverages the features of HTTP and REST for IP video transmission.

A video transmission device supporting compliance to the requirements of this standard based on HTTP and REST Services as described in this document is declared as compatible to ´IEC 62676-2 HTTP and REST interoperability.´

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.

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

ISO/IEC 11172-3:1993, *Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s – Part 3: Audio*

ISO/IEC 13818-2, *Information technology – Generic coding of moving pictures and associated audio information: Video*

ISO/IEC 14496-2:2004, *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 14496-10:2012, *Information technology – Coding of audio-visual objects – Part 10: Advanced video coding*

IETF RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*

IETF RFC 1945, *Hypertext Transfer Protocol – HTTP/1.0*

IETF RFC 2046, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*

IETF RFC 2250, *Format de charge utile RTP pour la video MPEG1/MPEG2*

IETF RFC 2326, *Real Time Streaming Protocol (RTSP)*

IETF RFC 2435, *Format de charge utile RTP pour l video JPEG*

IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*

IETF RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication*

IETF RFC 2818, *HTTP Over TLS*

IETF RFC 3016, *Format de charge utile RTP pour flux audio/video MPEG-4*

IETF RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*

IETF RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*

IETF RFC 3629, *UTF-8 un format de transformation de l'ISO 10646*

IETF RFC 3640, *Format de charge utile RTP pour le transport de flux élémentaires MPEG-4*

IETF RFC 3984, *Format de charge utile RTP pour video H.264*

IETF RFC 4566, *SDP: Session Description Protocol*

ITU-T Recommendation G.726, *40, 32, 24, 16 kbit/s Adaptive Differential Pulse Code Modulation (ADPCM)*

ITU-T Recommendation H.264, *Advanced video coding for generic audiovisual services*

ITU-T Recommendation T.81, *Information technology – Digital compression and coding of continuous-tone still images – Requirements and guidelines*

3 Abbreviations

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

AAC	Advanced Audio Coding
API	Application Program Interface
AVP	Audio/Video Profile
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IETF	Internet Engineering Task Force
IO	I/O Input/Output
IP	Internet Protocol

IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISO	International Standards Organization
ITU	International telecommunications Union
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Expert Group
MPEG	Moving Pictures Experts Group
NTP	Network Time Protocol
NVS	Network Video Storage Device
POSIX	Portable Operating System Interface
PTZ	Pan / Tilt / Zoom
QoS	Quality of Service
REST	Representational State Transfer
RFC	(Request for comment) IETF Standards Draft
RTCP	Real Time Control Protocol.
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SOAP	Simple Object Access Protocol
SRTP	Secure Real-time Transport Protocol
SSID	Service Set ID
SSL	Secure Sockets Layer SAML Security Assertion Markup Language
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time-to-live
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
UTF	Unicode Transformation Format
UTF-8	8-bit Unicode Transformation Format URN Uniform Resource Name
UUID	Universally Unique Identifier
VMS	Video management system
VT	Video Transmission
VTD	Video Transmission device
W3C	World Wide Web Consortium
WPA	Wi-Fi Protected Access
XML	eXtensible Markup Language
Zeroconf	Zero Configuration Networking

4 Overview

Security and/or network management applications require the ability to change configurations and control the behaviours of IP video devices – cameras, encoders, decoders, recorders, etc. This functionality can be achieved by sending a standard HTTP(S) request to the unit. The basic principle of this IP Interoperability is to specify and define HTTP(S) application programming interfaces (APIs) for VT devices and their functionality; namely, for setting/retrieving various configurations, and controlling device behaviours.

The REST Service Model Version 1.1 is intended to assist the IEC working groups in creating new protocols or converting contributed protocols to a standard service model that will be common to all endorsed specifications. Adherence to this service model will ensure interoperability between compliant protocols.

This model is similar in nature to Web services but is geared towards lightweight computing requirements on devices. As such, these protocols will not use Simple Object Access Protocol (SOAP) as defined by the W3C-defined Web services but instead will use a simplified XML schema and/or xml schema documents (.xsd's).

Unless otherwise noted, all specifications of this clause should treat all configuration and management aspects as resources utilizing the REpresentational State Transfer (REST) architecture.

The Service Model is based on a REST architecture. While REST specifies that all interfaces are defined as resources, in the Model of this standard these resources are grouped by service. This architecture provides a convenient way to group related resources within a hierarchical namespace and lends itself to service discovery and future expansion.

Anybody is welcome to add services at any time provided said services adhere to the service model as defined herein. Every effort should be taken to maintain full backward compatibility when adding new services. The Service Model is designed to support expansion with backwards compatibility.

5 Design considerations

5.1 General

Network-attached devices are often equipped with a web server to maintain various web pages. These pages allow the devices to be configured through an internet browser. It is natural to reuse this web server and the HTTP protocol in order for external applications to configure and control the device. Thus, all resources will use a standard HTTP request which will be processed by the device's web server.

When possible, IP devices should implement HTTPS to support privacy of data. It is assumed that the network infrastructure is configured properly with firewall, 802.1x, etc. and other features to provide basic network level security. Additionally, because IP devices are typically endpoint devices, HTTPS is assumed to provide sufficient safeguard in combination with the other features mentioned above.

Some devices are not capable of implementing HTTPS and in certain deployments it may not be necessary (i.e. closed networks). Additionally, SSL/TLS implies certificate management on an endpoint which could pose other problems. Embedded devices may not have a "trusted" certificate without a client explicitly trusting the certificate or uploading a trusted certificate. Furthermore, certificates may need to be regenerated upon configuration changes (IP address, etc.).

As such, the protocols use the HTTP Get and Post methods as described in “Hypertext Transfer Protocol -- HTTP/1.0” (RFC 1945) and “Hypertext Transfer Protocol -- HTTP/1.1” (RFC 2616).

5.2 REST overview

REST is an approach to creating services that expose all information as resources in a uniform way. This approach is quite different from the traditional Remote Procedure Call (RPC) mechanism which identifies the functions that an application can call. Put simply, a REST Web application is noun-driven while an RPC Web application is verb-driven. For example, if a Web application were to define an RPC API for user management, it might be written as follows:

```
GET http://webserver/getUserList
GET http://webserver/getUser?userid=100
POST http://webserver/addUser
POST http://webserver/updateUser
GET http://webserver/deleteUser?userid=100
```

On the other hand, a REST API for the same operations would appear as follows:

```
GET http://webserver/users
GET http://webserver/users/user100
POST http://webserver/users
PUT http://webserver/users/user100
DELETE http://webserver/users/user100
```

Part of the simplicity of REST is its uniform interface for operations. Since everything is represented as a resource, create, retrieve, update, and delete (CRUD) operations use the same URI.

5.3 Conformance

5.3.1 General

Every protocol will define one or more compliant REST services. To ensure interoperability, the following conformance requirements are also implied in each protocol.

5.3.2 Minimum API set

In addition to the service specific mandatory requirements, a system/device shall support all of the mandatory services.

Each specification may define one or more compliant services. Each service and each contained resource shall be assigned a scope of either mandatory or optional. Within each implemented service type, all mandatory resources shall be implemented.

5.3.3 XML requirements

A system/device shall support the syntax as defined by the W3C XML 1.0 specification.

A system/device shall support the UTF-8 character set as described by http://www.w3.org/International/O-charset

Additionally, XML content shall correspond to the following Schemas as defined in Annex A:

- “ResourceList XML Schema”
- “ResourceDescription XML Schema”
- “QueryStringParameterList XML Schema”
- “ResponseStatus XML Schema”

Vendors may optionally extend this standard to include proprietary XML content as long as it does not conflict with the minimum set of APIs. In this case, it is recommended to use a vendor-specific XML namespace to avoid conflicting names that may arise with future revisions.

For example, if vendor XYZ123 Inc intends to extend the XML standard to include a <configOption> parameter, it is recommended to use <configOption xmlns="urn:XYZ123-com:configuration:options"> to avoid future namespace conflicts.

5.3.4 Protocol requirements

A system/device shall support transport of XML via either the HTTP/1.0 or HTTP/1.1 protocol as specified in RFC 1945 and RFC 2616, respectively. It is highly recommended that HTTP/1.1 is used in order to support key features (persistent connections, HTTPS, etc.). When HTTP 1.0 is implemented, the client applications shall not issue multiple messages to the target systems/devices.

5.4 HTTP methods and REST

The CRUD operations are defined by the HTTP method as shown in the table1 below.

Table 1 – HTTP methods

HTTP method	Operation
POST	Create the resource
GET	Retrieve the resource
PUT	Update the resource
DELETE	Delete the resource

Rules of thumb.

GET calls should never change the system state. They are meant to only return data to the requestor and not to have any side effects

POST calls should only be used to ADD something that did not already exist.

PUT calls are expected to update an existing resource but if the resource specified does not already exist, it can be created as well. This will be the assumed default behavior of PUT calls. If any resource wishes to deviate from this behavior, it should be considered an exception and this should be noted in the implementation notes of the resource.

5.5 HTTP status codes and REST

The following Table 2 shows how the HTTP status codes map to REST operations along with the general use case for response headers and bodies. For more information, please see the table under each REST API.

Table 2 – HTTP status codes and REST

HTTP status codes	REST meaning	POST	GET	PUT	DEL
200	"OK" - The request has succeeded. Header Notes: None Body notes: The requested resource will be returned in the body.		X	X	
201	"Created" - The request has created a new resource. Header notes: The *Location* header contains the URI of the newly created resource. Body notes: The response returns an entity describing the newly created resource.	X			
204	"No Content" - The request succeeded, but there is no data to return. Header notes: None Body notes: No body is allowed.			X	X
301	"Moved Permanently" - The requested resource has moved permanently. Header notes: The *Location* header contains the URI of the new location. Body notes: The body may contain the new resource location.		X		
302	"Found" - The requested resource should be accessed through this location, but the resource actually lives at another location. This is typically used to set up an alias. Header notes: The *Location* header contains the URI of the resource. Body notes: The body may contain the new resource location.		X		
400	"Bad Request" - The request was badly formed. This is commonly used for creating or updating a resource, but the data was incomplete or incorrect. Header notes: The Reason-Phrase sent with the HTTP status header may contain information on the error. Body notes: The response may contain more information of the underlying error that occurred in addition to the Reason-Phrase.	X		X	
401	"Unauthorized" - The request requires user authentication to access this resource. If the request contains invalid authentication data, this code is sent. Header notes: At least one authentication mechanism shall be specified in the *WWW-Authenticate* header. The Reason-Phrase sent with the HTTP status header may contain information on the error. Body notes: The response may contain more information of the underlying error that occurred in addition to the Reason-Phrase.	X	X	X	X
403	"Forbidden" - The request is not allowed because the server is refusing to fill the request. A common reason for this is that the device does not support the requested functionality. Header notes: The Reason-Phrase sent with the HTTP status header may contain information on	X	X	X	X