

**Video surveillance systems for use in security applications -- Part 1-2: System requirements – Performance requirements for video transmission**

This document is a preview generated by EVS

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

See Eesti standard EVS-EN 62676-1-2:2014 sisaldab Euroopa standardi EN 62676-1-2:2014 inglisekeelset teksti.	This Estonian standard EVS-EN 62676-1-2:2014 consists of the English text of the European standard EN 62676-1-2:2014.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 14.03.2014.	Date of Availability of the European standard is 14.03.2014.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 13.320

### **Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele**

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:  
Aru 10, 10317 Tallinn, Eesti; [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

### **The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation**

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:  
Aru 10, 10317 Tallinn, Estonia; [www.evs.ee](http://www.evs.ee); phone 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

**Video surveillance systems for use in security applications -  
Part 1-2: System requirements – Performance requirements for video  
transmission  
(IEC 62676-1-2:2013)**

Systèmes de vidéosurveillance destinés à être utilisés dans les applications de sécurité -  
Part 1-2: Exigences systèmes -  
Exigences de performances pour la transmission vidéo  
(CEI 62676-1-2:2013)

Videoüberwachungsanlagen für Sicherheitsanwendungen -  
Teil 1-2: Allgemeine Anforderungen an die Videoübertragung  
(IEC 62676-1-2:2013)

This European Standard was approved by CENELEC on 2013-12-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

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

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

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

**CENELEC**

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

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

## Foreword

The text of document 79/433/FDIS, future edition 1 of IEC 62676-1-2, prepared by IEC TC 79 "Alarm and electronic security systems" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62676-1-2:2014.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2014-09-03
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2016-12-03

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

## Endorsement notice

The text of the International Standard IEC 62676-1-2:2013 was approved by CENELEC as a European Standard without any modification.

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

IEC 62676-2-3	NOTE	Harmonised as EN 62676-2-3.
ISO 19111	NOTE	Harmonised as EN ISO 19111.
ISO 19115	NOTE	Harmonised as EN ISO 19115.

## CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	8
2 Normative references.....	8
3 Terms, definitions and abbreviations.....	10
3.1 Terms and definitions.....	10
3.2 Abbreviations.....	24
4 Performance requirements.....	26
4.1 General.....	26
4.2 Network time services.....	27
4.2.1 General.....	27
4.2.2 Real-time clock.....	27
4.2.3 Accurate time services for the transport stream.....	27
4.3 Video transmission timing requirements.....	27
4.3.1 General.....	27
4.3.2 Connection time.....	27
4.3.3 Connection capabilities.....	28
4.4 Performance requirements on streaming video.....	28
4.4.1 Introduction latency, jitter, throughput.....	28
4.4.2 Requirements on network jitter.....	29
4.4.3 Packet loss.....	29
4.4.4 Level of performance.....	30
4.4.5 Packet jitter.....	30
4.4.6 Monitoring of interconnections.....	31
5 IP video transmission network design requirements.....	31
5.1 General.....	31
5.2 Overview.....	31
5.3 Digital network planning.....	32
5.3.1 General.....	32
5.3.2 Critical requirements for IP video streaming performance.....	32
5.3.3 Availability.....	33
5.4 Additional architecture principles.....	34
5.5 Network design.....	34
5.5.1 Small unicast network.....	34
5.5.2 Small multicast video network.....	35
5.5.3 Hierarchical VSS network.....	35
5.5.4 Effective video IP network capacity planning.....	36
5.5.5 Wireless interconnections.....	37
5.6 Replacement and redundancy.....	37
5.6.1 Redundant network design.....	37
5.6.2 Availability.....	38
5.7 Centralized and decentralized network recording and video content analytics.....	38
6 General IP requirements.....	39
6.1 General.....	39
6.2 IP – ISO Layer 3.....	39
6.3 Addressing.....	39

6.4	Internet control message protocol (ICMP).....	40
6.4.1	General .....	40
6.4.2	Diagnostic requirements .....	40
6.5	Diagnostics .....	41
6.6	IP multicast .....	41
6.6.1	General .....	41
6.6.2	Internet group multicast protocol (IGMP) requirements .....	41
7	Video streaming requirements .....	41
7.1	General .....	41
7.2	Transport protocol .....	42
7.2.1	General .....	42
7.2.2	JPEG over RTP .....	42
7.2.3	JPEG over HTTP .....	42
7.3	Documentation and specification .....	43
7.3.1	General .....	43
7.3.2	Non-compliant, proprietary and vendor specific payload formats.....	43
7.3.3	Receiving unsupported RTP payload formats.....	44
7.4	Streaming of metadata .....	44
7.4.1	General .....	44
7.4.2	XML documents as payload .....	44
7.4.3	General .....	44
8	Video stream control requirements .....	45
8.1	General .....	45
8.2	Usage of RTSP in video transmission devices .....	45
8.2.1	General .....	45
8.2.2	The use of RTSP with multicast .....	45
8.3	RTSP standards track requirements .....	46
8.3.1	General .....	46
8.3.2	High level IP video streaming and control interfaces.....	46
8.3.3	Minimal RTSP method and header implementation .....	46
8.3.4	RTSP authentication.....	46
9	Device discovery and description requirements .....	46
10	Eventing requirements.....	47
11	Network device management requirements.....	47
11.1	General .....	47
11.2	IP video MIB example.....	48
11.3	The SNMP agent and manager for video transmission devices .....	48
11.4	Performance requirements on the SNMP agent .....	49
11.5	VSS SNMP trap requirements for event management.....	50
12	Network security requirements .....	50
12.1	General .....	50
12.2	Transport level security requirements for SG4 transmission .....	51
	Bibliography.....	52
	Figure 1 – Network buffer .....	29
	Figure 2 – Network latency, jitter, loss .....	33
	Figure 3 – System design .....	34

Figure 4 – Small network .....	35
Figure 5 – Multicast network .....	35
Figure 6 – Hierarchical network.....	36
Figure 7 – Redundant network .....	38
Figure 8 – MIB structure .....	48
Table 1 – Time service accuracy for video transport stream .....	27
Table 2 – Interconnections – Timing requirements .....	28
Table 3 – Video transmission network requirements .....	28
Table 4 – Video transmission network requirements .....	28
Table 5 – Performance requirements video streaming and stream display .....	30
Table 6 – Video stream network packet jitter.....	31
Table 7 – Monitoring of interconnections.....	31

Document is a preview generated by EVS

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

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

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

The second subpart of this IEC 62676-1 series applies to video transmission. The purpose of the transmission system in a Video Surveillance System (VSS) installation is to provide reliable transmission of video signals between the different types of VSS equipment in security, safety and monitoring applications.

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



# VIDEO SURVEILLANCE SYSTEMS FOR USE IN SECURITY APPLICATIONS –

## Part 1-2: System requirements – Performance requirements for video transmission

### 1 Scope

This part of IEC 62676 introduces general requirements on video transmission. This standard covers the general requirements for video transmissions on performance, security and conformance to basic IP connectivity, based on available, well-known, international standards.

Clauses 4 and 5 of this standard define the minimum performance requirements on video transmission for security applications in IP networks. In surveillance applications the requirements on timing, quality and availability are strict and defined in the last section of this standard. Guidelines for network architecture are given, how these requirements can be fulfilled.

Clause 6 and the next clauses of this standard define requirements on basic IP connectivity of video transmission devices to be used in security applications. If a video transmission device is used in security, certain basic requirements apply. First of all a basic understanding of IP connectivity needs to be introduced which requests the device to be compliant to fundamental network protocols. These could be requirements which may be applied to all IP security devices even beyond IP video. For this reason requirements are introduced in a second step for compliance to basic streaming protocols, used in this standard for video streaming and stream control. Since security applications need high availability and reliability, general means for the transmission of the video status and health check events have to be covered. These are defined in general requirements on eventing and network device management. In security proper maintenance and setup is essential for the functioning of the video transmission device. Locating streaming devices and their capabilities is a basic requirement and covered in 'device discovery and description'.

### 2 Normative references

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

IEC 61709, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

IEC/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

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

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

ISO/IEC 10646, *Information technology – Universal multiple-octet coded character set (UCS)*

ISO/IEC 13818-9, *Information technology – Generic coding of moving pictures and associated audio information – Part 9: Extension for real time interface for systems decoders*

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

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

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

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

ITU-T Rec. G.726, *40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)*

IEEE Std 1413.1, *IEEE Guide for selecting and using reliability predictions based on IEEE 1413*

IETF RFC 1122, *Requirements for Internet Hosts – communication Layers*

IETF RFC 1157, *Simple Network Management Protocol*

IETF RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*

IETF RFC 2030, *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*

RFC 2069, *Digest Access Authentication*

IETF RFC 2131, *Dynamic Host Configuration Protocol*

IETF RFC 2246, *The TLS Protocol Version 1.0*

IETF RFC 2326:1998, *Real Time Streaming Protocol (RTSP)*

IETF RFC 2435, *RTP Payload Format for JPEG-compressed Video*

IETF RFC 2453, *RIP - Routing Information Protocol*

IETF RFC 2617, *HTTP Authentication Basic and Digest Access Authentication, June 1999.*

IETF RFC 3016, *RTP Payload Format for MPEG-4 Audio/Visual Streams.*

IETF RFC 3268, *Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)*

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

IETF RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

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 3984, *RTP Payload Format for H.264 Video*.

IETF RFC 4346, *The Transport Layer Security (TLS) Protocol Version 1.1*

IETF RFC 4541, *IGMP and MLD Snooping Switches*

IETF RFC 4566, *SDP Session Description Protocol*

IETF RFC 4607, *Source Specific Multicast for IP*

IETF RFC 4862, *IPv6 Stateless Address Auto configuration*

### **3 Terms, definitions and abbreviations**

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

#### **3.1 Terms and definitions**

##### **3.1.1**

##### **adaptive jitter buffering**

queuing of packets in switched networks exposed to unwanted variations in the communications signal to ensure the continuous video transmission over a network supported by the 'Adaptive' ability to adjust the size of the jitter buffer based on the measured jitter in the network

EXAMPLE: If the jitter increases, the buffer becomes larger and can store more packets; if the jitter decreases, the buffer becomes smaller and stores fewer packets.

##### **3.1.2**

##### **advanced encryption standard**

NIST encryption standard, also known as Rijndael, specified as unclassified, publicly-disclosed, symmetric encryption algorithm with a fixed block size of 128 bits and a key size of 128, 192 or 256 bits according to the Federal Information Processing Standards Publication 197

##### **3.1.3**

##### **American Standard Code for Information Interchange**

de-facto world-wide standard for the code numbers used by computers to represent all the upper and lower-case characters

##### **3.1.4**

##### **asymmetric algorithm**

algorithm used in the asymmetric cryptography, in which a pair of keys (a private key and a public key) is used to encrypt and decrypt a message to ensure the privacy of communications

##### **3.1.5**

##### **authentication**

process where an operators or systems identity is checked within a network

EXAMPLE: In networks, authentication is commonly done through the use of logon passwords.

##### **3.1.6**

##### **authentication server**

device used in network access control

Note 1 to entry: It stores the usernames and passwords that identify the clients logging on or it may hold the algorithms for access. For access to specific network resources, the server may itself store user permissions and