BS EN 62676-1-2:2014
Incorporating corrigendum April 2015

BSI Standards Publication

Video surveillance systems for use in security applications

Part 1-2: System requirements — Performance requirements for video transmission

National foreword

This British Standard is the UK implementation of EN 62676-1-2:2014, incorporating corrigendum April 2015. It is identical to IEC 62676-1-2:2013. It supersedes BS EN 50132-5-1:2011 and BS EN 50132-5-2:2011, which are withdrawn.

The UK participation in its preparation was entrusted by Technical Committee GW/1, Electronic security systems, to Subcommittee GW/1/10, Closed circuit television (CCTV).

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 90613 8
ICS 13.320

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2014.

Amendments/corrigenda issued since publication

Date	Text affected
31 March 2016	Implementation of CENELEC corrigendum April 2015: EN title and Foreword pages updated with supersession details

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62676-1-2

March 2014

ICS 13.320

Supersedes EN 50132-5-1:2011 and EN 50132-5-2:2011.

English version

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 Sicherungsanwendungen -
Teil 1-2: Allgemeine Anforderungen an die Videoübertragung
(IEC 62676-1-2:2013)

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

Ref. No. EN 62676-1-2:2014 E

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

This document supersedes EN 50132-5-1:2011 and EN 50132-5-2:2011.

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.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

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

Publication	Year	Title	EN/HD	Year
IEC 61709	-	Electric components - Reliability - Reference conditions for failure rates and stress models for conversion	EN 61709	2011
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: Video system requirements	EN 62676-1-1	-
IEC 62676-2-1	-	Video surveillance systems for use in security applications - Part 2-1: Video transmission protocols - General requirements	EN 62676-2-1	-
ISO/IEC 10646	-	Information technology - Universal 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 system 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 Recommendation G.711	-	Pulse code modulation (PCM) of voice frequencies	-	-
ITU-T Rec .726	-	General Aspects of Digital Transmission Systems, Terminal Equipment - 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 (SNMP)	-	-
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	-	-

Publication	Year	Title	EN/HD	Year
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	-	Routing Information Protocol	-	-
IETF RFC 2617	-	HTTP Authentication: Basic and Digest Access Authentication	-	-
IETF RFC 3016	-	RTP Payload Format for MPEG-4 Audio/Visual Streams	-	-
IETF RFC 3268	-	Advanced Encryption Standard (AES) Ciphersuites 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	-	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 Autoconfiguration	-	-

CONTENTS

INTRODUCTION

The IEC Technical Committee 79 in charge of alarm and electronic security systems together with many governmental organisations, test houses and equipment manufacturers 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

company policies or provide access to directories that contain the information. Protocols such as RADIUS, Kerberos and TACACS+, and 802.1x are implemented in an authentication server to perform user authentications.

3.1.7
authenticity
integrity and trustworthiness of data or an entity; validity and conformance of the information, or identity of a user

Note 1 to entry: The authenticity can be secured and verified using cryptographic methods.

3.1.8
authorization
approval, permission, or empowerment for a user or a component to do something

3.1.9
backbone
high-speed line or series of connections that forms a major pathway within a network

3.1.10
backbone layer
larger transmission line that carries data gathered from smaller communication lines that interconnect with it, e.g. a line or set of lines that local area networks connect to, in order to span distances efficiently e.g. between buildings

3.1.11
Bit/s
bit per second
unit of measurement of how fast data is transferred from one node to another

3.1.12
bridge
device that is used to connect two networks including passing data packets between them using the same protocols

3.1.13
client
component that contacts and obtains data from a server

3.1.14
client/server
communication system providing services e.g. video streams, storage, logon access, data communication management and clients (workstations) subscribing these services

3.1.15
codec
compression-decompression or enCOder/DECoder process

3.1.16
common gateway interface
CGI
standardized method of communication between a client, e.g. web browser, and a server, e.g. web server

Note 1 to entry: This note applies to the French language only.

3.1.17
compression delay
delay caused by the compression of data

3.1.18
congestion
situation in which the traffic presents on the network exceeds available network throughput/ capacity

3.1.19
core layer
part of the network providing optimal transport between sites or system functionality e.g. recording

3.1.20
data encryption standard
DES
cryptographic algorithm method developed by the US National Bureau Standards

Note 1 to entry: This note applies to the French language only.

3.1.21
dynamic host configuration protocol
DHCP
protocol by which a network component obtains an IP address (and other network configuration information) from a server on the local network

Note 1 to entry: This note applies to the French language only.

3.1.22
distribution layer
part of the network providing policy-based connectivity

3.1.23
domain name system
DNS
system that translates Internet domain names into IP addresses

Note 1 to entry: This note applies to the French language only.

3.1.24
dual homing
single device offering two or more network interfaces

3.1.25
dynamic jitter buffer
collecting and storing video data packets for processing them in evenly spaced intervals to reduce distortions in the display

3.1.26
encryption
type of network security used to encode data so that only the intended destination can access or decode the information

3.1.27
fail-over
the capability of an application to recover from a failure on an entity by automatically switching over to a surviving instance, providing no loss of data or continuity, also known as ‘run-time failover’ and often used in connection with

3.1.28
forensics
field of science of applying digital technologies to legal questions arising from criminal investigations

3.1.29
frame
data structure that collectively represents a transmission stream including headers, data, and the payload and provides information necessary for the correct delivery of the data

3.1.30
gateway
hardware or software set-up that translates between two dissimilar protocols

3.1.31
H.261
ITU video coding standard originally designed for ISDN lines and data rate with multiples of 64 Kbit/s using real time protocol (RTP)

3.1.32
H.263
ITU standard supporting video compression (coding) for streaming video via RTP based on and replacing the H.261 codec

3.1.33
H.264
ISO ITU-T MPEG-4 Part 10 standard, also named Advanced Video Coding (AVC) supporting video compression (coding) from low bit-rate network streaming applications to HD video applications with near-lossless coding for network-friendly video representation

3.1.34
host
computer on a network that is a repository for services available to other components on the network

3.1.35
hot-swap
property of controller which allows circuit boards or other devices to be removed and replaced while the system remains powered up and in operation

3.1.36
Hyper Text Mark-up Language
HTML
coding language used to create Hypertext documents for use on the World Wide Web

Note 1 to entry: This note applies to the French language only.

3.1.37
Hypertext Transfer Protocol
HTTP
connection oriented protocol for transmitting data over a network or protocol for moving hyper text files across the Internet

Note 1 to entry: This note applies to the French language only.

3.1.38
Hypertext Transfer Protocol Secure
HTTPS
encrypts and authenticates communication between server and clients

Note 1 to entry: This note applies to the French language only.

3.1.39
Internet Control Message Protocol
ICMP
error protocol indicating, for instance, that a requested service is not available or that a host or router could not be reached

Note 1 to entry: This note applies to the French language only.

3.1.40
identification
ID
a machine-readable character string

3.1.41
IEEE 802.1x
method for authentication and authorization in IEEE-802 networks using an authentication server e.g. RADIUS server

3.1.42
Institute of electrical and electronics engineers
IEEE
professional association of engineers for the advancement of technology

3.1.43
Internet group management protocol
IGMP
communications protocol used to manage the membership of IP multicast groups

Note 1 to entry: This note applies to the French language only.

3.1.44
Internet protocol
IP
network layer 3 protocol in the OSI model containing addressing and control information to enable data packets to be routed in a network and primary network layer protocol in the TCP/IP protocol suite according to IETF RFC 791

Note 1 to entry: This note applies to the French language only.

3.1.45
Internet protocol address
IP address
address of a host computer used in the Internet Protocol

Note 1 to entry: The IP address corresponds to a fully qualified domain name. At present, it consists of 32 bits and is generally represented by a sequence of four decimal numbers (each in the range from 0 to 255), separated by dots. The IP address of a computer usually comprises two parts: a part corresponding to the network number of the network on which this computer is located, and a part identifying the computer within its network. In the new version IPv6 of the Internet Protocol, the IP address consists of 128 bits.

Note 2 to entry: The Internet protocol is not limited to the Internet, and may be used on other networks.

3.1.46
IP
Internet protocol
main protocol used in conjunction with TCP (Transfer Control Protocol)

SEE: TCP/IP.

3.1.47
Images per second
IPS
measurement or unit for the rate of pictures transmitted or displayed to create a video stream

Note 1 to entry: A rate of 25 IPS (PAL) or 30 IPS (NTSC) is considered to be real-time or full motion video.

3.1.48
Internet Protocol, version 4
IPv4
most widely used version of the Internet Protocol (the "IP" part of TCP/IP)

3.1.49
Internet Protocol Version 6
IPv6
successor to IPv4

Note 1 to entry: Already deployed in some cases and gradually spreading, IPv6 provides a huge number of available IP Numbers – over a sextillion addresses. IPv6 allows every device on the planet to have its own IP Number.

3.1.50
jitter
delay variation or continuity the packets arrive at their destination

Note 1 to entry: ´The received flow variation or pumping of stream´.

3.1.51
kilobits per second
kbit/s
unit of data transmission rate

3.1.52
latency
time that elapses between the initiation of a network request for data and the start of the actual data transfer

3.1.53
layer 2 switch
OSI (Open Systems Architecture) data link layer device responsible for transmitting data across the physical links in a network

3.1.54
layer 3 device
OSI device that determines network addresses, routes for information transport

EXAMPLE: A router is a layer 3 device; switches can also have layer 3 capability.

3.1.55
local area network
LAN
communications network serving users and devices within a limited geographical area, such as a building or a protected area

Note 1 to entry: This note applies to the French language only.

3.1.56
local-access layer
part of the network bringing edge devices into the network and providing operator access

3.1.57
login
account name used to gain access to a component to be used in combination with a password or the act of connecting to a component or system by giving valid credentials (usually “username" and "password")

3.1.58
managed switch
switch that can be monitored and administered in the network via its own IP address

3.1.59
media access control address
MAC address
unique identifier attached to network adapters i.e a name for a particular adapter

Note 1 to entry: This note applies to the French language only.

3.1.60
management information base
MIB
a structured collection of information for remote servicing using the SNMP protocol

Note 1 to entry: This note applies to the French language only.

3.1.61
multipurpose Internet mail extensions
MIME
standard for defining the type of payload streamed from a server to a client

Note 1 to entry: This note applies to the French language only.

EXAMPLE: ´video/h264´ is used for streaming H.264 encoded video.

3.1.62
MJPEG
motion JPEG
ISO/IEC digital video encoding standard, where each video frame is separately compressed into a JPEG image

3.1.63
MPEG-4
digital video encoding and compression standard that uses interframe encoding to significantly reduce the size of the video stream being transmitted compared to intraframe only encoding

Note 1 to entry: In interframe coding, a video sequence is made up of so called I- or key-frames that contain the entire image. In between the key-frames are delta frames, which are encoded with only the incremental differences. This often provides substantial compression because in many surveillance video sequences, only a small part of the pixel is different from one frame to another.

3.1.64
multicast
throughput-conserving technology that reduces throughput usage by simultaneously delivering a single stream of information, here video content, to multiple network recipients

3.1.65
N+1 fail-over
fail-over capability of N identical applications in operation by automatically switching over to 1 unused application instance

3.1.66
N+n redundancy
capacity of a parallel redundant system with N representing the number of applications needed to meet the critical load and n is the number of extra applications for redundancy purposes

3.1.67
network connectivity
the physical (wired or wireless) and logical (protocol) connection of a computer network or an individual device to a network

3.1.68
network design
way of arrangement of the various clients and servers in a network for the purposes of connectivity, performance, and security

3.1.69
network layer
Layer 3 of the OSI reference model, controlling communication links and data routing across one or more links

3.1.70
network management
administrative services performed in managing a network, such as network topology and software configuration, monitoring network performance, maintaining network operations, and diagnosis and troubleshooting problems

3.1.71
network performance
to stream data in accordance with requests from the security application

Note 1 to entry: Since video streaming is mostly real-time, it is critical to be delivered within a specific time.

3.1.72
network topology
pattern of connection between nodes in a network, e.g. hierarchical topology

3.1.73
node
communication device attached to a network or end point of a network connection such as a device attached to a network such as a workstation, IP video device, printer, etc.

3.1.74
network time protocol
NTP
standard for synchronizing computer system clocks in packet-based communication networks

Note 1 to entry: This note applies to the French language only.

Note 2 to entry: NTP uses the connectionless network protocol UDP (see UDP) for enabling time to be reliably transmitted over networks with variable packet runtime.

3.1.75
packet loss
the loss of data packets during transmission over a network

Note 1 to entry: ´The leak in the stream´.

3.1.76
packet switching
method used to transmit data in a network from many different sources on the same connection, directed along different routes to many different sinks at the same time

3.1.77
packets
data structures that collectively represent the transmission stream including headers and data associated with the network layer when the communication protocol is connection-oriented

3.1.78
physical topology
the physical layout of the network; how the cables are arranged; and how the components are connected

3.1.79
port
number or identifier for a particular service on a server, mostly standardized for certain services e.g. RTSP, UPnP, HTTP, etc.

3.1.80
protocol
set of rules governing how two components or entities communicate

Note 1 to entry: Protocols are used in all levels of communication. There are hardware and software protocols.

3.1.81
protocol data unit
PDU
unit of data equivalent to the frame which is passed between protocol layers

Note 1 to entry: This note applies to the French language only.

3.1.82
remote authentication dial-in user service
RADIUS
protocol using an authentication server to control network access

Note 1 to entry: This note applies to the French language only.

3.1.83
rapid spanning tree protocol
RSTP
link layer network protocol that ensures a loop-free topology for any bridged LAN including the basic function to prevent network loops and ensuing multicast functionality

Note 1 to entry: This note applies to the French language only.

3.1.84
redundancy (network)
alternative routing or protection switching to enable a reliable video transmission e.g. by Resilient Packet Ring (RPR),Spanning Tree Protocol (STP), Rapid Spanning Tree (RSTP)

Note 1 to entry: ´Identifying and replacing a broken link or stream´

3.1.85
request for comments
RFC
proposed and published internet standards, reviewed by the Internet Engineering Task Force, as consensus-building body that facilitates discussion, and eventually a new standard (STD) is established

Note 1 to entry: This note applies to the French language only.

3.1.86
router
device that routes information between interconnected networks, able to select the best path to route a message by determining the next network point to where a packet should be forwarded on its way to its final destination

Note 1 to entry: A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router handles the connection between 2 or more Packet-Switched networks by passing packets designated by source and destination addresses through and deciding on the actual route to send them on.

3.1.87
resilient packet ring
RPR
Layer 2 MAC-based protocol technology defined by IEEE's 802.17 for fast recovery from connection link failures and cuts at Layer 2

Note 1 to entry: This note applies to the French language only.

3.1.88
real-time control protocol
RTCP
supporting protocol for real-time transmission of groups within a network

quality-of-service feedback from receivers to the multicast group and support for synchronization of different media streams e.g. video, audio, metadata

Note 1 to entry: This note applies to the French language only.

3.1.89
real-time transport protocol
RTP
Internet protocol for transmitting real-time data such as video

Note 1 to entry: RTP itself does not guarantee real-time delivery of data. It only provides mechanisms for the sending and receiving streaming data. Typically is based on the UDP protocol.

Note 2 to entry: This note applies to the French language only.

3.1.90
real time streaming protocol
RTSP
control protocol standard (RFC 2326) for delivering, receiving and controlling real-time data streams such as video, audio and metadata and starting entry point for negotiating transports such as RTP, multicast and unicast, including the negotiating of Codec’s

Note 1 to entry: Can be considered as "remote control" for controlling video streams delivered by a server.

Note 2 to entry: This note applies to the French language only.

3.1.91
security certificate
SC
piece of exchanged information that is used by the SSL protocol to establish a secure connection

Note 2 to entry: This note applies to the French language only.

3.1.92
segment
section of a network

3.1.93
server
software program that provides services to other applications in the same or other computers

3.1.94
simple network management protocol
SNMP
set of standards for communication with devices connected to a TCP/IP network for the management of network nodes (servers, workstations, routers, switches and hubs, video transmission devices, etc), enabling network administrators to manage network performance, find, solve network problems and plan network extensions

EXAMPLE: Management systems get notified of network node problems by receiving traps or change messages from network devices implementing SNMP according to IETF RFC 1157, 1441, 3410.

Note 1 to entry: This note applies to the French language only.

3.1.95
simple network management protocol version 1
SNMPv1
simple request/response protocol for management system issuing requests to a managed network device that in return send a response according to IETF RFC 1157

3.1.96
simple network management protocol version 2
SNMPv2
identical protocol to SNMPv1 adding and enhancing some protocol operations and the SNMPv2 trap operation based on a different message format for replacement of the SNMPv1 trap according to IETF RFC 1441

3.1.97
simple network management protocol version 3
SNMPv3
SNMP protocol version adding security and remote configuration capabilities to the previous SNMP versions including the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control according to IETF RFC 3410

3.1.98
simple network time protocol
SNTP
adaptation of the Network Time Protocol (NTP) synchronizing computer clocks on a network, when the accuracy of the full NTP implementation is not needed according to IETF RFC 2030

Note 1 to entry: This note applies to the French language only.

3.1.99
single point of failure
SPOF
a component in a device, or a node in a network, which, if it were to fail would cause the entire device or network to fail, normally eliminated by adding redundancy

Note 1 to entry: This note applies to the French language only.

3.1.100
six nines availability
availability A of a system defined as A = MTBF/(MTBF + MTTR), describing the total time of availability for operation as a proportion of the total time no less than 0,999 999 or 99,999 9 %

3.1.101
simple network time protocol
SNTP
a simplified version of NTP

Note 1 to entry: This note applies to the French language only.

SEE: NTP.

3.1.102
simple object access protocol
SOAP
protocol for client-server communication used to exchange service requests and responses "on top of" HTTP exchanging data in a particular XML format specifically designed for use with SOAP

Note 1 to entry: This note applies to the French language only.

3.1.103
speed of data transfer
the rate at which information is transmitted through a network, usually measured in megabits per second

3.1.104
secure socket layer
SSL
application layer security protocol to enable encrypted, authenticated communications across networks

Note 1 to entry: This note applies to the French language only.

3.1.105
storage area network
SAN
high-speed network or sub network whose primary purpose is to transfer data between network devices and storage systems consisting of a communication infrastructure, providing physical connections, a management layer and storage elements

Note 1 to entry: This note applies to the French language only.

3.1.106
streaming performance
quality of the network stream determining how an operator perceives the information including the factors availability, errors, caused by noise, congestion or component failures, delay, jitter, throughput, loss

3.1.107
subnet mask
method that allows one large network to be broken down into several smaller ones

Note 1 to entry: Depending on the network class (A, B, or C), some number of IP address bits are reserved for the network address (subnet) and some for the host address. For example, Class A addresses use 8 bits for the subnet address and 24 bits for the host portion of the address.

3.1.108
switch
device that connects network devices to hosts, allowing a large number of devices to share a limited number of ports

3.1.109
transmission control protocol/Internet protocol
TCP/IP
suite of protocols that define networks and the Internet in general

Note 1 to entry: This note applies to the French language only.

3.1.110
throughput (network)
digital transmission capacity to support the required quality of the video stream

EXAMPLES: 1 Mbit/s up through 10 Mbit/s.

Note 1 to entry: The size of the possible video stream pipe.

3.1.111
time protocol
network protocol allowing time clients to obtain the current time-of-day from time servers

3.1.112
topology
(physical) network configuration including cables other equipment

(logical) flow of data between logical entities including the specification of protocols involved independent of the physical location

3.1.113
transceiver
transmitter/receiver
device that receives and sends signals over a medium

3.1.114
transport stream
TS
content binary stream usually in reference to an MPEG-2 AV stream format

Note 1 to entry: This note applies to the French language only.

3.1.115
user datagram protocol
UDP
stateless protocol for the transfer of data without provision for acknowledgement of packets received

Note 1 to entry: This note applies to the French language only.

3.1.116
universal plug and play
UPnP
architecture for pervasive peer-to-peer network connectivity of devices of all form factors

Note 1 to entry: It is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks. It is a distributed, open networking architecture that leverages TCP/IP and Web technologies to enable seamless networking in addition to control and data transfer among networked devices.

Note 2 to entry: This note applies to the French language only.

3.1.117
unmanaged switch
basic switch that does not offer remote network administration capability

3.1.118
uniform resource identifier
URI
address for resources available on a network starting with a “scheme" such as HTTP or RTSP

Note 1 to entry: This note applies to the French language only.

3.1.119
uniform resource locator
URL
unique address for a file that is accessible on the Internet

Note 1 to entry: This note applies to the French language only.

Note 2 to entry: URL was previously Universal Resource Locator.

3.1.120
unicode transformation format
UTF
character code preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values

Note 1 to entry: This note applies to the French language only.

3.1.121
UTF-8
encoding schema with UCS-2 or UCS-4 characters as a varying number of octets, where the number of octets, and the value of each, depend on the integer value assigned to the character in ISO/IEC 10646

3.1.122
video transmission device
VTD
video device with at least one IP network interface handling video

Note 1 to entry: This note applies to the French language only.

3.1.123
wide area network
WAN
network connecting computers within large areas, e.g. beyond the limits of a single protected site

Note 1 to entry: This note applies to the French language only.

3.1.124
workstation
computer connected to a network at which operators interact with the video display

3.1.125
XML
eXtensible Markup Language
widely used protocol for defining data formats, providing a very rich system to define complex data structures

Note 1 to entry: This note applies to the French language only.

3.1.126
XML schema
definition including constrains of data in an XML document

3.2 Abbreviations

AAC	Advanced Audio Codec
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Automatic Teller Machine
AVC	Advanced Video Codec
CIF	Common Intermediate Format
CPU	Central Processing Unit
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVR	Digital Video Recorder
DVB	Digital Video Broadcast
GPS	Geo Positioning System
H.264-CBP	ISO/IEC 14496-10 and ITU H.261 Reduced complexity Baseline Profile
HD	High Definition
HTTP	Hypertext Transfer Protocol
I/O	Input / Output
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IESG	Internet Engineering Steering Group
IGMP	Internet Group Multicast Protocol
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
JPEG	Joint Picture Experts Group
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MD 5	Message Digest Algorithm Version 5
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MJPEG	Motion JPEG
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NTP	Network Time Protocol
NTSC	National Television System Committee
NVR	Network Video Recorder

OASIS	Organization for the Advancement of Structured Information Standards
OID	Object Identifier
OR	Operational Requirements
OSI	Open Systems Interconnection
PAL	Phase Alternation Line
PC	Personal Computer
PDU	Protocol Data Unit
PING	Packet Internet Groper
POS	Point of Sales
PPM	Packets Per Million
PTZ	Pan / Tilt / Zoom
RFC	(Request for comment) IETF Standards Draft
RPR	Resilient Package Ring
RSA	(Public Key Cryptosystem invented by) Rivest, Shamir and Adleman
RTCP	Real Time Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
SSM	Source-Specific Multicast
STD	Standard
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TS	Transport Stream
TTL	Time-to-live
UCS	Universal Character Set
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
VACM	View-based Access Control Model
VCA	Video Content Analysis

VSS	Video Surveillance System
VT	Video Transmission
VTD	Video Transmission device
W3C	World Wide Web Consortium
WAN	Wide Area Network
WSDL	Web Services Description Language
XML	eXtensible Markup Language

4 Performance requirements

4.1 General

This video transmission standard addresses the requirements of devices in security applications with differing application characteristics, such as embedded, PC based, operator workstations, and others. Digital encoding and decoding video devices, VSS client workstations, video storage, NVRs and DVRs have a differing set of functions in video streaming and network connectivity. The following summarizes these functionalities:

– stream encoding
– stream receiving and decoding
– stream recording
– live streaming and displaying
– playback streaming and replaying
– camera controlling
– health and status monitoring
– video content analysis
– metadata creation and streaming
– auxiliaries

Due to the nature of non-analog video transmission, especially video IP networks, using shared connections, compression and streaming techniques, following requirements shall be applied:

For different applications, such as PTZ camera tracking, recording, video motion detection, remote monitoring, etc., there are different requirements on the performance of VTDs. Therefore this standard introduces different performance classes. For each application the requirements shall be specified and include classes for: time service accuracy (Table 1), interconnection timing (Table 2), throughput sharing (Table 3 and 4), streaming (Table 5), network jitter (Table 6) and monitoring (Table 7).

Different functions of the system can have different performance classes.

NOTE Performance classes are independent of security grades.

These requirements do not apply to mobile cell based interconnections, but shall be applied to fixed wireless network connections and transport applications, such as on-board systems.

If minimum requirements on the network performance for the proper operation of a VTD or VSS exist, these shall be defined and documented.

The requirements start at a lower class 1 and grow with the classes, the higher the number.

4.2 Network time services

4.2.1 General

The Video Transmission Device (VTD) will require network time services for a real-time clock, eventing, logging and for the video transport stream (TS).

The VTD shall never start streaming video for recording purposes, if the requirements below on the accuracy of the time stamping of the video frames cannot be granted. This shall especially be verified after start-up or re-initiation after power loss of the VTD. Otherwise the integrity of the stream recordings may be corrupted and may not allow the correct replay not only of the concerned frame sequences, but also of other recordings. This has even higher impact on images used for the evidential purposes.

4.2.2 Real-time clock

The real time clock in the Video Transmission device should be synchronized with a time normal using RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI. The addresses of the SNTP servers should come from the Time Server DHCP option (4). The more accurate system time shall be used as default: the SNTP best accuracy is 0,25 µs, whereas the usage of the ´Time Server´ according to RFC 868 offers only a best accuracy of 1 s.

4.2.3 Accurate time services for the transport stream

As an option, Network Time Protocol (NTP) (Version 3) as detailed in RFC 1305 should be implemented when time services with an accuracy of 1 ms to 50 ms according to the requirements of Table 1 are needed. The IP addresses of the time servers should come from the Network Time Server DHCP option (42). The Network Time Protocol should be tried first and only on failure shall Simple Network Time Protocol be used. A null Network Time Server DHCP option (42) means no server is available and Simple Network Time Protocol should be used.

Table 1 – Time service accuracy for video transport stream

Class	T1	T2	T3	T4
Time service accuracy for transport stream	80 ms	40 ms	5 ms	1 ms

The NTP timestamps in the Real Time Protocol header shall increase steadily over consecutive packets in the RTP stream. They should correspond to local time and shall be adjusted, if necessary, to stay consecutive. After VTD restart, the system time re-synchronisation may be delayed up to 10 s for SNTP or up to 15 s for time server protocol (NTP).

4.3 Video transmission timing requirements

4.3.1 General

Video Transmission devices and their interconnections shall be designed in accordance with the system requirements IEC 62676-1-1 as part of the VSS.

4.3.2 Connection time

The connection time needed to initiate the transmission of a stream from a source to a receiver is of interest. This time has to be considered especially in systems where camera roundtrips, sequencing or guard tours of different cameras is needed. The initial connection time shall be much lower than the dwell time of the camera sequence, see Table 2.

Table 2 – Interconnections – Timing requirements

Video transmission devices shall have a maximum	Class			
	I1	I2	I3	I4
Initial connection time for every new video stream request of	2 000 ms	1 000 ms	500 ms	250 ms

NOTE In RTSP Multicast streams an I-Frame request optimizes this connection time.

4.3.3 Connection capabilities

If a VSS video transmission network is designed and configured in a way that single or multiple video transmission receiver devices request video images and the simultaneous request of image streams by all possible receivers may exceed the available capacity of the network at a time, the video transmission device shall offer means according to following Table 3.

Table 3 – Video transmission network requirements

Video transmission devices in a shared network shall offer means to configure:	Class			
	C1	C2	C3	C4
the maximum data rate of video streams for every video channel			X	X
the maximum data rate for all available video streams of a single device			X	X
the maximum data rate or number of video streams to all client devices in the network			X	X

Table 4 – Video transmission network requirements

Video transmission devices in a shared network shall offer means to:	Class			
	P1	P2	P3	P4
Prioritize certain streams over others, e.g. streams for recording or alarms over live image streams			X	X
Prioritize certain users over others, e.g. for PTZ control			X	X

At no time the video transmission receiver shall allow the opening and initializing of connections to new video stream sources on cost of the video streams already displayed or recorded in order to avoid frame loss

At no time the video transmission receiver shall allow the display of live streams on cost of the video streams recorded, in order to avoid frame loss.

If the qualities of video for live viewing by an operator and for recording needs to be different, the video transmission device shall offer a minimum of 2 streams of different quality settings.

If the quality of video for continuous recording and for event based alarm recording needs to be different, the video transmission device shall offer an additional stream, if the quality setting is different from the other 2.

4.4 Performance requirements on streaming video

4.4.1 Introduction latency, jitter, throughput

Recommendations given in this subclause are informative.

Video streams are sensitive to accumulated delay, which is known as latency. The network contributes to latency in several ways:

- Transmission delay – The length of time a video packet takes to cross the given media. Transmission delay is determined by the speed of the transmission media and the size of the video packet.
- Forwarding delay – The length of time an internetworking device (such as a switch, bridge, or router) takes to send a packet that it has received.
- Processing delay – The time required by a networking device for looking up the route, changing the header, and other switching tasks. In some cases, the packet header has also to be manipulated. For example, the encapsulation type has to be changed. Each of these steps can contribute to the processing delay.
- Coding/Decoding Delay – The time required to encode and/or decode an image to or from a video stream, which is influenced by the performance of the VTD and the type, profile and level of CoDec. For instance the H.264 profiles ´Main´ with 350 ms and ´Baseline´ Profile with 120 ms coding delay or MPEG4 may offer a delay of 110 ms and MPEG2 Low Delay with less than 180 ms.
- Display Delay – The time required by the presentation unit to change the appearance of a picture element, usually not to be considered

4.4.2 Requirements on network jitter

If a VSS network sends video data with variable latency, it introduces jitter. The most common technique to reduce jitter is to store incoming video data in a buffer from where it is displayed. The buffer reduces the effect of jitter like a shock absorber.

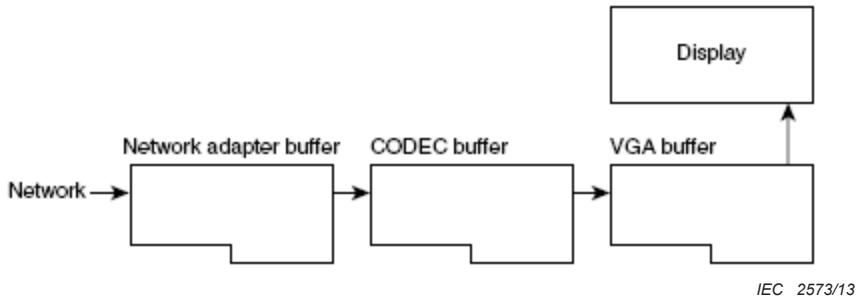

Figure 1 – Network buffer

The overall need is that even when video traffic has a jitter, the operator watching the video images shall not be destructed. For that reason, video security networks shall use techniques to minimize jitter for live and replay streams.

One way to provide minimized jitter and packet loss is to increase network speeds to assure that sufficient throughput is available during event- and peak-traffic times.

4.4.3 Packet loss

There are different reasons for network packet loss. Packet loss may be introduced by network congestion, where a network is over-utilized or –subscribed, other traffic may be blocking, and network infrastructure equipment may face problems and fail. The network may be configured in a wrong way e.g. with duplicate IP addresses.

In IP video streaming packet loss may have impact on the video quality, may cause frame blocking, local image distortions with unclear images areas, smear, artefacts, pixelization, blur, flicker, decreasing frame rates, frozen images. In addition packet loss can also cause excessive latency and delay possibly leading to VTD stream disconnections.

NOTE In broadcast industry a packet loss of 100 ppm or one lost packet per minute for 2CIF MPEG-4 real-time streams is generally considered as un-viewable and 2 ppm or one lost packet per hour as unacceptable for the user according to the DVB standard.

The impact of packet loss on video streaming depends upon a number of factors including the percentage of packet loss, the distribution of loss over time and the capabilities of the VTDs to handle loss. In differential encoded video streams the current frame is predicted from the previously transmitted video. Video packets are dependent on previous packets. If these packets have not been successfully received, then the current packet is not useful. This is known as loss propagation. This propagation stops with the arrival of intra coded frames (I-Frames).

The VTD shall be capable to detect packet loss and compensate the effects. The VTD shall be able to provide an acceptable operator and user experience and video perception during packet loss. The reduction of the visual effects associated with the stream delivery is critical to the end-user retention. At least the visual impression of the packet loss shall be masked or hidden according to the needs to fulfil the surveillance task and objective. A VTD shall offer state-of-the art error and loss concealment techniques. The VTD shall offer any packet loss or error concealment capability e.g. by using packet information of the encoded video from neighbouring macroblocks, prior or future frames, in order to estimate the video content of the current frame.

4.4.4 Level of performance

When addressing performance needs of Streaming-Video traffic, the following requirements apply, see Table 5.

Table 5 – Performance requirements video streaming and stream display

Class	S1	S2	S3	S4
Maximum Loss	240 ppm	120 ppm	60 ppm	30 ppm
Maximum one-way latency live stream (incl. encoding, networking, decoding, display)	600 ms	400 ms	200 ms	100 ms
Max Trick Play (Pause, Single Step,,..) Reaction Time	400 ms	200 ms	200 ms	100 ms
Round-trip latency incl. visualisation and control e.g. PTZ	700 ms	500 ms	300 ms	200 ms
Round-trip latency incl. visualisation and control e.g. PTZ, when moving objects need to be monitored and tracked	650 ms	450 ms	250 ms	150 ms

Streaming video archives and recordings have easier performance requirements because they are not sensitive to delay (the video can take some time to cue up) and are largely not jitter sensitive (because of application buffering). Streaming-Video might contain valuable content, such as security applications, in which case it requires performance guarantees.

Since the performance of video streaming is evaluated best by the visual impression, it is best to test and verify the display performance parameters. The general requirement for the display of streaming video shall offer a smooth visual impression to the end-user. The display jitter shall be no more than 1/10 of the frame rate interval.

4.4.5 Packet jitter

The maximum peak-to-peak packet jitter is defined as the variation in delay between the live or replay source of the stream and the end device. The peak-to-peak jitter, J, implies that the deviation in network delay, d, is bounded by $-J/2 \leq d \leq +J/2$. To give a technical comparison and an example, the Video Transmission device according to Class M4 shall comply with the Real Time Interface Specification of ISO/IEC 13818-9 with jitter of 20 ms.

Table 6 – Video stream network packet jitter

Class	M0 ms	M1 ms	M2 ms	M3 ms	M4 ms
Maximum peak-to-peak packet jitter	-	160	80	40	20

The VTD receiver has to offer a buffer for compensating the specified jitter. This actually means that a VTD has to offer bigger buffers to achieve a proper receiving and decoding of video frames with larger jitter. This delay adds up in the VTD receiver buffer, which shall be large enough to compensate for variation in the inter-arrival times (jitter).

4.4.6 Monitoring of interconnections

Table 7 specifies the maximum permitted period for an interconnection or signal to be unavailable. If an IP video connection for streaming, health check, or eventing is failing and the maximum permitted period is exceeded a tamper or fault signal or message shall be generated as specified in IEC 62676-1-1.

Table 7 – Monitoring of interconnections

The system shall offer	Security grade			
	1	2	3	4
Maximum permitted duration of device unavailability			180 s	30 s
Maximum detection time for live signal loss		8 s	4 s	2 s
The requirement above is intended to establish if communication is possible by monitoring the communication video to ascertain if it is available to convey a signal or message. Monitoring may take the form of listening for jamming when a video transmission device communicates via shares interconnections with other devices or other applications.				

NOTE These requirements correspond to IEC 62676-1-1:2013, Table 4 requirement 3 and Table 5 requirement ´video loss´

5 IP video transmission network design requirements

5.1 General

To give an understanding how the IP video network performance requirements of the previous clauses are covered in an installation, it’s not only important to select and configure standardized IP video surveillance components, but also to provide an appropriate network structure. To ensure the performance of a video transmission network according to the requirements listed above following procedure to design a network is recommended:

Overall a VSS and its interconnections shall be designed in accordance with IEC 62676-1-1. There are three important elements to consider when designing an effective VSS:

– technical infrastructure
– operational requirements (OR)
– operational-processes and -procedures

This section details the design requirements for the VSS installation, focusing on IP connections and communications.

5.2 Overview

The two most important design elements are determining the number of video streaming servers and sources (i.e. IP video encoding devices) and the number of receivers or clients (user Interfaces, workstations, recording devices, decoders), because they define the load,

which can vary very much. These two factors are closely related, and influence each other. It is a combination of these two elements that have impact on a successful system design.

5.3 Digital network planning

5.3.1 General

For a proper network design follow these steps:

1) Map the necessary logical connections of the planned physical network infrastructure
2) Define a topology that matches the required connectivity
3) Plan network redundancy
4) Define baseline network traffic data based on continuous video stream at required visual resolution for recording and display of static and moving scenes
5) Simulate video stream traffic to verify this baseline data
6) Define capacity needs on average and peak video stream data based on user requested video to workstations, continuous video stream recordings and motion or alarm video recordings
7) Define a figure for the average and maximum simultaneity of streaming sources, the so-called selective factor
8) Identify each network link's throughput requirement in access-, distribution- and core layer
9) Identify potential bottlenecks. WAN links can be IP video traffic bottlenecks
10) Examine thoroughly the network hardware infrastructure to ensure support for immediate and future expansion in surveillance or Video Streaming capacity needs
11) Accurately document the network's topology, actually used capacity and maximum capacity.

5.3.2 Critical requirements for IP video streaming performance

5.3.2.1 General

To support video traffic equivalent quality standards and performance figures shall be met for acceptable video streaming services (see Figure 1). Four factors – throughput, latency, jitter, and packet loss – are critical from the network point of view. The management of each determines how effectively the network supports IP video traffic. In this standard an approach is specified, where a proper network design and overall system management guarantees the quality and performance of the video stream.

A fifth factor ´alternative routing´, the so-called ´protection switching´, is also an important consideration to help protect critical VSS- and operator-traffic.

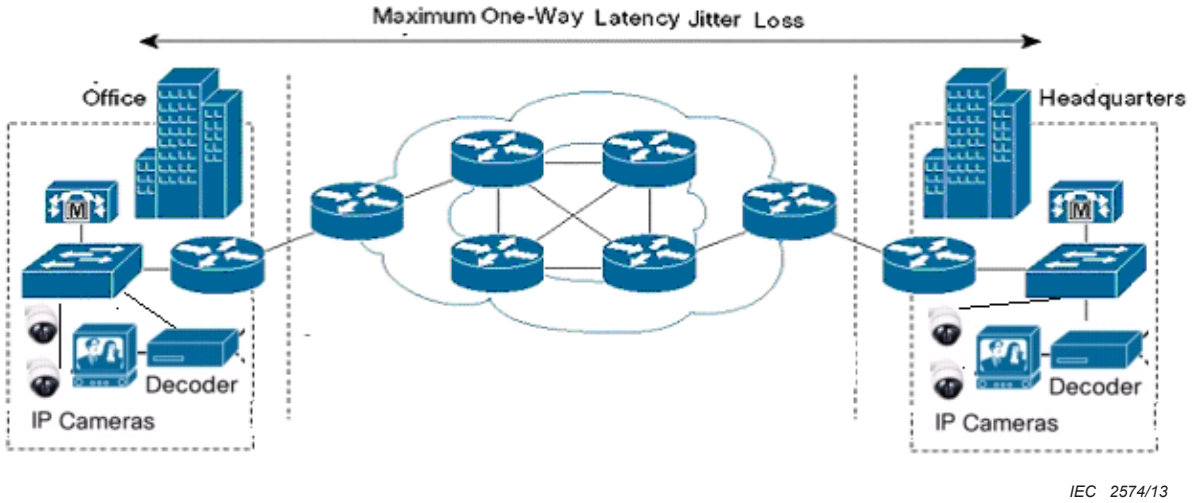

Figure 2 – Network latency, jitter, loss

5.3.2.2 Throughput: stream capacity planning

Before video related data is placed on a network, it has to be ensured that the network can support all existing applications (if any) together with the required data rate associated with the quality of video to be transported over the network. First, calculate the minimum data rate requirements for each major video node. The sum represents the minimum data rate requirement for any specific link. This amount shall consume no more than 75 % of the total data rate available on that link. This 75 % rule assumes that some data rate is necessary for overhead traffic. Examples of overhead traffic include routing protocol updates and keep-alives, as well as additional applications, such as VSS management and configuration traffic.

5.3.2.3 Streaming performance and stream management

One of the key requirements for the deployment of IP video is the ability to offer a streaming quality equivalent to the existing analogue VSS over Coax as a means for a much higher video throughput and quality. Perceived Video quality is very sensitive to three key performance criteria in a digital packet network, in particular: delay, packet loss, achievable bit rate (influencing compression level and artefact, resolution and framerate) IP, by its nature, provides a best-effort service and does not provide guarantees about the key criteria listed above.

5.3.3 Availability

The required availability can be achieved in an IP video network by using redundant and load-balancing and -sharing equipment and networks. The connection of a video encoder, the access gateway, trunk gateway and network video recorder need to be fault tolerant. The types of functionality often used to achieve fault tolerance include:

– redundant hardware
– redundant network connections
– N+n redundancy
– hot-swap capability
– fail-over capability for all components
– N+1 fail-over capability for one out of N identical components
– no single point of failure, except cameras and encoding
– dual network port video source devices e.g. IP cameras or encoders
– configuration, software and firmware that can be changed and upgraded without loss of service.

Alternative network traffic-protection schemes such as RSTP according to IEEE 802.1w shall provide a spanning tree convergence after a topology change or network failure within 1 second. STP shall respond within 30 s to 50 s.

5.4 Additional architecture principles

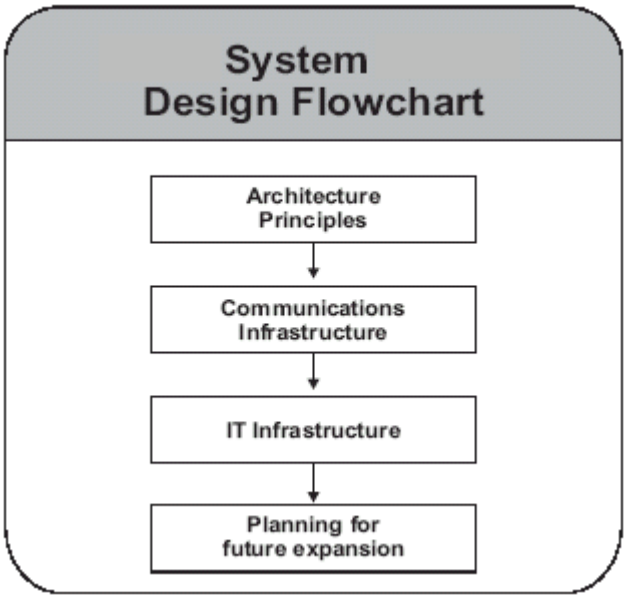

Figure 3 – System design

The architecture shall be based on the following principles:

1) separate functional components of the system to provide reliability and redundancy
2) ensure a controlled environment for reliability of devices and the comfort of operators
3) understand the design parameters in normal operation and in a second step in alarm-, or peak- situations, when event response times are higher than planned. When the VSS installation grows in size, the peak loads tend to average over time and sites
4) other principles (see Figure 3)

5.5 Network design

5.5.1 Small unicast network

The Figure 4 below depicts a LAN with three video surveillance workstations A, B and C, a video server D, a network video printer E, and a router F. This network is used to support a small surveillance system with up to 30 IP video channels.

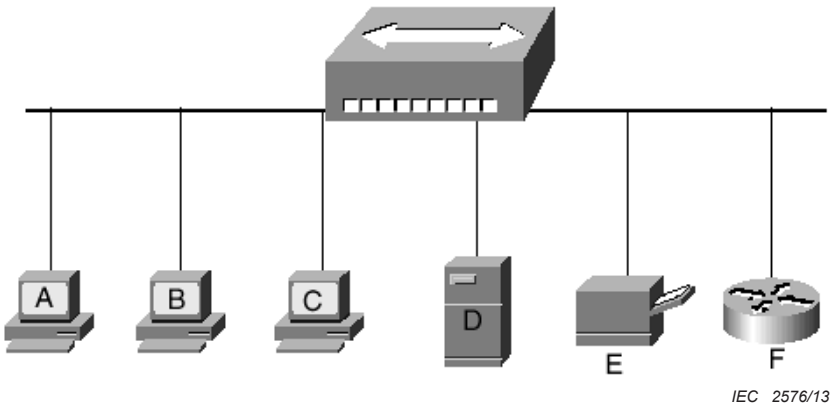

Figure 4 – Small network

5.5.2 Small multicast video network

The Figure 5 below depicts a LAN with three fixed workstations, a video server, a network multicast switch and more than 30 cameras. This network is used to support a small multicast surveillance system with over 30 IP video channels and multiple operators and clients monitoring most of the time the same video sources.

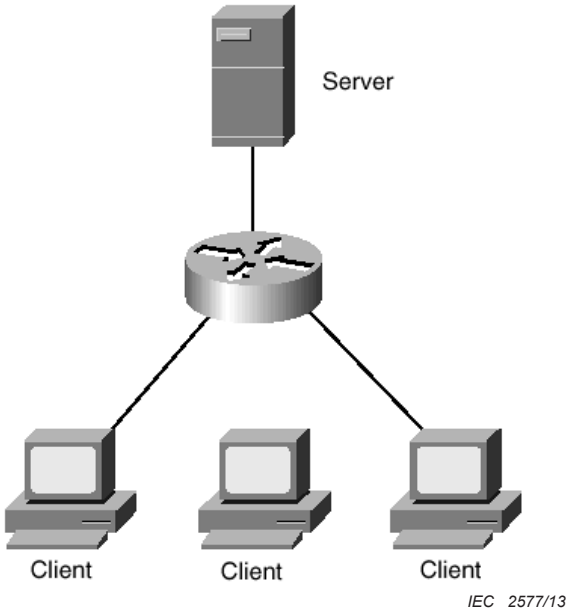

Figure 5 – Multicast network

5.5.3 Hierarchical VSS network

A hierarchical network design includes the following three layers of Figure 6:

- the backbone layer or core layer that provides optimal transport between sites or system functionality e.g. recording
- the distribution layer that provides connectivity
- the local-access layer that brings video transmission devices into the network and provides operator access

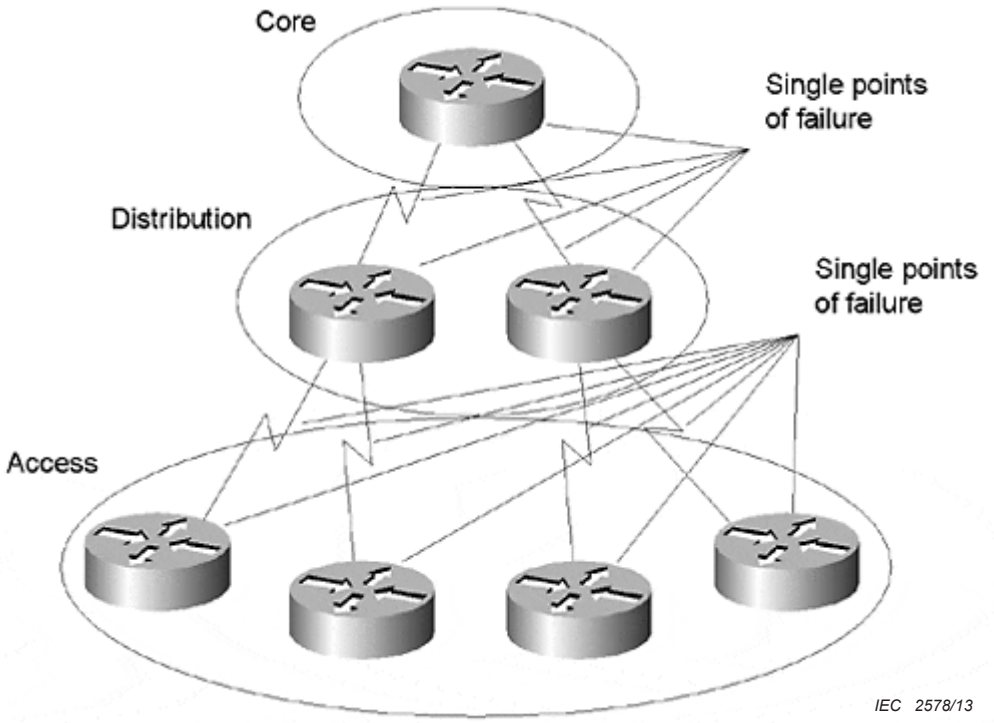

Figure 6 – Hierarchical network

Larger IP Video networks shall be based on the hierarchical network model. This model divides a network into three layers: core, distribution, and access layer.

The access layer is responsible for connecting devices to the network. Its defining characteristics generally are a high port density and/or the ability to overcome physical edge device or "last mile" challenges.

The distribution layer is where policies are applied. It is where access-lists and CPU intensive routing decisions shall occur (as opposed to just a default route or default gateway). Distribution layer designs focuses on aggregating access devices into components with high processing resources so that policies can be applied.

The core layer is the "backbone" of the network. Its job is simply to move high amounts of video stream packets from multiple video sources A to video receiver B as fast as possible and with the least possible manipulation.

Core and distribution are only separated into different switches in large networks. Very often in smaller IP video environments, one switch takes over both the tasks of the core and the distribution layer.

5.5.4 Effective video IP network capacity planning

IP video and network engineers, consultants and administrators characterize network capacity as the amount of traffic the network is designed to handle. Discussing network capacity in IP video systems becomes more a measure of how many simultaneous video streams the network can process. This concept of **"peak load"**, the maximum assumed video stream volume that the network shall be able to handle, will be the basis of the capacity planning process. During **capacity planning** the following shall be considered:

- number of encoders/cameras on the network
- video codec’s and their performance in the VSS solution

- existing data traffic on the network
- decentralized or centralized recording and video content analysis
- connectivity to network storage, video recorders, video motion detectors
- number of streams of the encoders provided and the number of clients each one supports
- number of users and video operator clients in the network
- existing local area network (LAN) and/or wide area network (WAN) designs
- existing and selected network's hardware infrastructure
- network redundancy
- spare throughput available in the network

5.5.5 Wireless interconnections

When wireless interconnections are employed the factors below shall be considered:

1) siting of antennas to ensure reliable communication with other system components;
2) possibility of other RF equipment interfering with VSS interconnection equipment;
3) proximity of large metal objects to the equipment antenna;
4) possibility of intruders to interfere or block the interconnection.

5.6 Replacement and redundancy

5.6.1 Redundant network design

Redundancy provides alternate routes around single points of failure (SPOF).

Redundant network designs try to meet requirements for network availability by duplicating network links and interconnectivity devices. Redundancy eliminates the possibility of having a single point of failure on the network. The goal is to duplicate any required component whose failure could disable critical applications. The component could be an analog video matrix switch, a core router, a camera, a video encoder or decoder, a power supply, a network trunk line, a digital video recorder and so on.

Since redundancy is expensive to deploy and maintain, redundant topologies should be implement only where needed. A level of redundancy shall only be selected according to the requirements of the operational requirements for availability and affordability. Redundancy adds complexity to the network topology. Redundancy for cameras may be covered by a PTZ camera able to navigate to the scene of several static cameras or by a positioning of cameras, where the field of view of one camera is part of the following camera at a lower quality level.

A single point of failure is any device, interface on a device, or link that can inhibit the VSS from a certain surveillance task if it fails. Networks that follow a strong, hierarchical model tend to have many single points of failure because of the emphasis on summarization points and points of entry between the network layers. For example, in a strict hierarchical network, such as the one depicted in Figure 6, every device and every link is a single point of failure.

There are different designs to provide redundancy in the **core layer**. If the entire core network is in one building or one small protected site, each router is connected to two high speed LANs, Router A and B of Figure 7.

If the core routers are not all in one building or within one protected site the options become more limited.

The two most common methods for providing redundancy at the **distribution layer** are dual homing and backup links to other distribution layer routers

Dual homing **access layer** devices are the most common way of providing redundancy to remote locations within one protected site, but it is also possible to interconnect access layer devices to provide redundancy.

In Figure 7 Router G and Router H are access layer routers that are dual-homed with the backup circuit connected to different branches of the distribution layer.

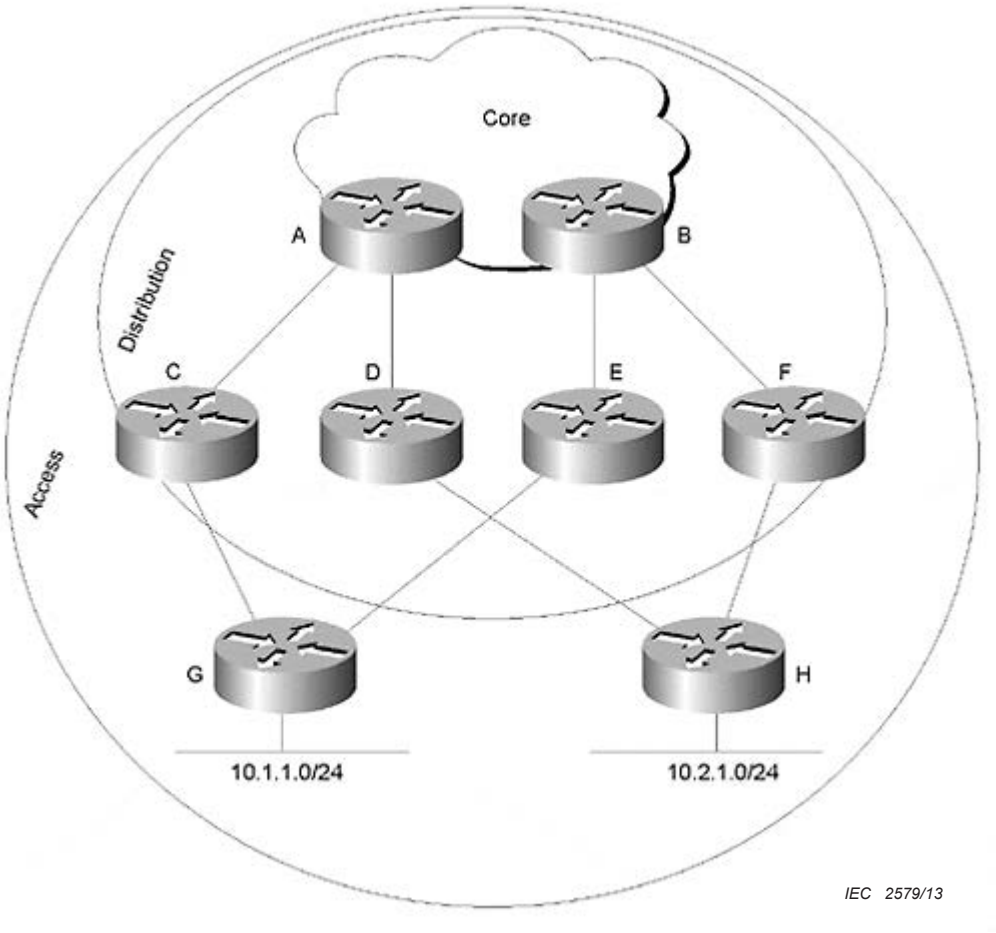

Figure 7 – Redundant network

5.6.2 Availability

Operational requirements (OR) assuredly demand a level of availability of the video network.

The mean time between failures (MTBF) of the components shall be considered when designing the network, the same for the mean time to repair (MTTR). Designing logical redundancy in the network is as important as physical redundancy. The VSS assembly shall have a minimum MTBF of 16 000 h based on IEC/TR 62380, IEC 61709, and IEEE 1413.1-2002.

5.7 Centralized and decentralized network recording and video content analytics

A VSS network can include all possible variants of centralized recording and video content analytics (VCA) or decentralized recording and VCA at the camera location.

There are many factors that influence the decision for centralized or decentralized recording and VCA. For example if the network covers several buildings, recording shall be located in each building. But central viewing and evaluating the recorded video data is easier in a centrally recording environment. Centralized recording is realized when the storage devices

are connected to the core switch, the same for centralized VCA. The entire network shall be able to transport the recorded video data or the streams to be analysed.

Decentralized recording or VCA is realized when the storage or VCA devices are connected to the Access layer switch. The network is segmented into “traffic zones”. The recorded or analyzed video data stays within the subnets and does not flood the network. If decentralized recording or VCA is realized, the access switches shall be designed for the expected traffic.

From the IT point of view the centralized solution will always be preferred. A centralized solution is easier to manage, backed up and easier to scale. Additionally all management software and hardware is concentrated e.g. in the control centre or in a part of the building. “At the edge” there is only cameras and encoders. The disadvantage of centralized recording or VCA is that one needs very powerful (and expensive) core switches. Another disadvantage is that fall-back solutions are complex. If the core switch fails, the entire system stops working when there is no failover. The decentralized solution offers more stability. When a switch or network segment fails, recording and VCA in the other segments are not affected. The scalability of decentralized recording is restricted. When new cameras are added to all network segments, the storages in the segment are possibly too small and shall be exchanged. In a centralized solution it is sufficient to exchange or expand the central storage device. Direct recording to NVR or network attached storage (NAS) is completely independent from switches. As long as the encoder and the storage device are up and running, recording continues. But therefore a number of small storage devices are needed which might be much more expensive than one large storage device.

A disadvantage of centralized VCA is that analysis is performed on the transmitted video stream, which is compressed in the given resolution and frame rate including artefacts.

6 General IP requirements

6.1 General

The intent of this clause is to specify basic network requirements and protocols, with a preference for existing, well-known and well accepted standards. This interface specification is written to provide the minimal set of requirements for video streaming and supporting protocols between VTD servers and clients. Overall the IP network shall support DNS, IPv4, DHCP, TTL, optionally IPv6.

6.2 IP – ISO Layer 3

All entities of a video transmission device shall be capable of implementing IP (Internet Protocol) as Layer 3 protocol. In order to ensure interoperability with existing TCP/IP networks, the entities shall implement IPv4 as defined in RFC 791. Support for IPv6 as defined in RFC 2460 is optional.

NOTE In the remainder of this text all references to IP (only ´IP´) is interpreted as IPv4.

6.3 Addressing

The foundation for networking is IP addressing. Each VTD shall have a Dynamic Host Configuration Protocol (DHCP) client and search for a DHCP server when the device is first connected to the network. If no DHCP server is available, in a so-called unmanaged network, the device shall assign itself an address. If during the DHCP transaction, the device receives a domain name, for example, through a DNS server or via DNS forwarding, the device should use that name in subsequent network operations; otherwise, the device should use its IP address.

This clause defines the IEC 62676-1-2 IP configuration compliance requirements on VTDs. The main requirements are listed below.

IP Configuration

The video transmission device shall have at least one network interface that gives it IP network connectivity and allows video and data exchange between video transmission devices e.g. between video transmission server and client.

It shall be possible to make static IP configuration on the video transmission device using a network or local configuration interface.

IPv4 addressing

The video transmission device should support dynamic IP configuration of local-link address according to RFC 3927.

The video transmission device may support any additional IP configuration mechanism.

IPv6 addressing

A video transmission device that supports IPv6 shall support stateless IP configuration according to RFC 4862 or shall support stateful IP configuration according to RFC 3315 or both.

DHCP

The video transmission device shall support dynamic IP configuration according to RFC 2131.

The preferred method of assigning an IP address to an entity is via DHCP according to RFC 2131. Each node supporting this layer shall have a function to obtain address setting information using a DHCP server. For operation, it is highly recommended that a DHCP server is deployed into an IP video network.

This standard does not specify any dynamic IP address setting method other than DHCP.

6.4 Internet control message protocol (ICMP)

6.4.1 General

ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.

6.4.2 Diagnostic requirements

To facilitate troubleshooting, the system entities shall implement the ´PING command according ICMP (RFC 792). According to RFC 1122 any host shall accept an echo-request and issue an echo-reply in return.

Any network host shall be able to send ICMP “echo request” packets to the video transmission target and listen for ICMP “echo response” replies. This provides a valuable diagnostic capability.

All video transmission clients shall be compliant to RFC 1122, that any host shall accept an echo-request and issue an echo-reply in return.

According to the Echo Request/Reply of RFC 792, every host shall implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies. An ICMP Echo Request destined to an IP broadcast or IP multicast address shall be silently discarded.

The IP source address in an ICMP Echo Reply shall be the same as the specific-destination address of the corresponding ICMP Echo Request message. Data received in an ICMP Echo Request shall be entirely included in the resulting Echo Reply.

6.5 Diagnostics

For an easier diagnosis and maintenance of the video transmission network and its devices, the VTD should signal the basic network connection status via indicators e.g. LEDs next to the network connector, which should show the operating status and indications of possible failures and malfunctions:

If no other specification is given for a VTD, following indicator colours should represent the listed network connection status: A steady lighted green indicator should signal the status for a 10 Mb network connection, a green and orange for 100 Mb, orange for 1 Gb. A blinking of the indicator(s) every second should represent an ongoing data transmission. If no connection can be established, the indicator(s) should not be lighted. A lighted red indicator should signal the start-up process of a VTD. During a firmware upgrade the indicator should fast blink red. A blinking red every second should signal a VTD failure or defect such as broken power supply, fans, a corrupt configuration or firmware.

6.6 IP multicast

6.6.1 General

If a VTD is supporting multicast, then it shall operate according to RFC 1112. If a VTD is not supporting multicast according to this standard, it shall be clearly specified that the ´VTD is not supporting multicast´. All multicasting devices shall support Source Specific Multicast (SSM) extensions according to RFC 4607. The use of Any-source multicast (where the source IP address is not specified) is not recommended. For Source Specific Multicasting, the addressing scheme shall comply with RFC 4607 (range 232/8).

6.6.2 Internet group multicast protocol (IGMP) requirements

6.6.2.1 General

VDTs should be capable of generating IGMP messages to join/leave a multicast group. The minimum version of IGMP implemented should be version 3 according to RFC 3376.

6.6.2.2 IGMP snooping

Layer 2 devices (i.e. network switches) shall be capable of supporting “IGMP snooping” according to RFC 4541 and shall not flood multicast traffic indiscriminately out of all their interfaces in case of the availability of an IGMP querier.

7 Video streaming requirements

7.1 General

Today a lot of incompatible video streaming and stream control implementations exist, although standards are used. In this clause general requirements for the application of existing standards on video streaming are introduced.

The following clause contains requirements for the use of video stream transport in VTDs. The requirements are organized into a subclause that covers requirements common among all video transports and subclauses that cover requirements for specific video transport protocols such as RTP and others.

Video Transmission clients and servers shall support an IP-based network interface for the transport of session control and video data.

Control and video data shall be sent using TCP/IP according to STD 7 RFC 793 and/or UDP/IP according to STD 6 RFC 768. An overview of the protocol stack can be found in Figure 2 of this standard.

7.2 Transport protocol

7.2.1 General

The video transmission devices shall support UDP and/or TCP.

NOTE IEC 62676-2 series defines a protocol, how a VTD requests streams in the selected mode UDP or TCP.

Video transport requires real-time behaviour, provided in IP networks by the Real Time Protocols (RTP). RTP provides support for re-ordering, dejittering and media synchronization. All media streams transferred by the RTP protocol shall conform to RFC 3550, RFC 3551, RFC 3984, RFC 3016 and JPEG over RTP according to IEC 62676-2 series.

The RTP/UDP profile is the simplest and most widely supported option in current network streaming video systems. A VT device shall support the RTP/UDP protocol and should support RTP/UDP multicasting. RTP via TCP is an alternative means of media transport and a VTD may support this option according to RFC 4571. The RTSP/RTP over TCP provides the option of reliable transport. Furthermore, RTSP/RTP over TCP permits traversal of Network Address Translators and Firewalls.

The RTP Control Protocol (RTCP) provides feedback on streaming performance being provided by RTP and synchronization of different media streams. The RTCP protocol shall conform to RFC 3550.

All devices and clients shall support RTSP according to RFC 2326 for session initiation and playback control. RTSP shall use TCP as its transport protocol, the default TCP port for RTSP traffic is 554. The Session Description Protocol (SDP) shall be used to provide media stream information and SDP shall conform to RFC 4566.

7.2.2 JPEG over RTP

JPEG over RTP shall be basically in accordance with RFC 2435. This implementation only supports default Huffman tables, the aspect ratio is limited to 1:1 and 1:2 and the image size is limited to 2 040 x 2 040 pixels due to limited bit field of the RTP/JPEG header

For JPEG images of other aspect ratios, such as PAL or NTSC and for 4 mega pixel image sensors and more, an RTP extension header shall be included after the original standard header according to RFC 3550. The header extension shall be ignored by VTDs, not supporting these features. This may have the effect on incompatible VTD receivers that the stream is decoded, but offers e.g. the wrong aspect ratio.

7.2.3 JPEG over HTTP

If a VTP supports JPEG over HTTP it shall be in accordance with RFC 2453.

HTTP streaming separates each image into individual HTTP replies. RTP streaming creates packets of a sequence of JPEG images that can be received by VTD clients. A special mime-type ´multipart/x-mixed-replace;boundary=´ shall signal the VTD to receive several parts as reply separated by a special boundary, which is defined within the MIME-type. The TCP connection is active as long as the VTD receiver requests new frames and the VTD server provides frames.

7.3 Documentation and specification

7.3.1 General

The specification of the VTD and its video streaming interface shall document the number of VTD clients and/or servers being able to be connected for live and/or replay video streaming. If necessary the frame rate and quality of the video stream shall be specified as well.

RTP Payload Formats For interoperability purposes, the allowed set of media streaming options and formats for video, audio and meta data based on RTP is defined by this standard.

At least one of the following video streaming specifications shall be supported for compatibility reasons:

- JPEG over RTP
- MPEG-4 according to ISO/IEC 14496-2
- H.264 according to ISO/IEC 14496-10

and the following audio codecs:

- G.711 according to ITU-T G.711
- G.726 according to ITU-T G.726
- AAC according to ISO/IEC 14496-3

7.3.2 Non-compliant, proprietary and vendor specific payload formats

VTDs may support next to the listed compliant payloads additionally non-compliant or proprietary RTP payload formats. These are used when the real-time video format is proprietary and not intended to be part of any standardized system. However these proprietary formats shall be correctly documented and registered, because

– usage in standardized environments such as SDP. RTP needs to be configured regarding used RTP profiles, payload formats and their payload types. To accomplish this there is a need for registered names to ensure that the names do not collide with other formats.
– integration of 3rd party video devices: RTP payload formats are used for supporting proprietary formats. A written specification of the format will save time and money for both parties interoperating with each other: interoperability will much easier to accomplish.
– to ensure interoperability between different implementations on different platforms.

To avoid name collisions there is a central register keeping tracks of the registered Media Type names used by different RTP payload formats. When it comes to proprietary formats, they shall be registered in the vendors own tree. All vendor specific registrations uses sub-type names that start with “vnd.<vendor- name>”. All names that use names in the vendors own trees are not required to be registered with IANA. However registration is recommended if used at all in public environments.

New RTP payload Media Types may be registered in the standards tree by other standard bodies. The requirements on the organization are outlined in the media types registration document (RFC 4855 and RFC 4288). This registration requires a request to the IESG, which ensures that the registration template is acceptable.

Registration of the RTP payload name is something that is required to avoid name collision in the future. The list of already registered media types can be found at IANA (http://www.iana.org/assignments/media-types/video).

Vendor specific extensions shall use the payload type range 77-95, which is marked "unassigned"

7.3.3 Receiving unsupported RTP payload formats

A RTP payload format for a codec is a set of rules that define how the codec's video frames are packed within RTP packets. This is usually defined by an IETF RFC (or, for newer payload formats, an IETF Internet-Draft).

By default, the VTD video client will ignore any sub session whose RTP payload format it does not understand (because, if it doesn't know the RTP payload format, it doesn't know how to extract data from the incoming RTP stream).

The VTD client shall not be negatively influenced by incompatible video streams with unknown or corrupt codecs or video formats.

Vendor specific extensions shall use the payload type range 77-95, which is marked "unassigned"

7.4 Streaming of metadata

7.4.1 General

In video surveillance networks it is necessary to transport additional data next to the video stream, the so called Metadata. ATM/POS-, VCA-, GPS-, Geolocation, Number Plates, Access Control Cardholder IDs are some of the most common types of metadata. In general there are three alternatives to transport metadata assets with the actual video content:

– multiplexing: combined streaming containing video and metadata (not recommended);

– separate metadata and video data streams;

– multiple metadata streams (one for each type of metadata) and one video data stream.

Combined/multiplexed streaming has several disadvantages since the combined stream approach depends on a specific payload format, which provides the auxiliary header section where the metadata can be transported. Some RTP payload formats, such as for MPEG-4 Elementary Streams (RFC 3640), but other payload formats used in video surveillance do not provide the section ´auxiliary´. This conflicts with the requirements for interoperability. Furtheron saving on processing overhead by handling only one stream, brings some overhead due to the (de)multiplexing of the video and metadata.

End users expect that the metadata will be delivered with no, or a low level, of information loss. Therefore, a mechanism based on RTP shall be used and is specified here, which enables metadata arrival in correct order, and with detection and indication of loss. Metadata shall be transmitted on a separate RTP session in its own payload format.

7.4.2 XML documents as payload

7.4.3 General

If complex data formats need to be streamed as metadata, requiring a very rich system of complex data structures, XML documents shall be transmitted as RTP payload.

In a RTSP session the SDP description for metadata of Content Type and Subtype "application" shall be used as a dynamic payload type

```
SDP Example:

Client->Server: DESCRIBE rtsp://140.10.2.3/VideoChannel/1/h264 RTSP/1.0
CSeq: 1

Server->Client: RTSP/1.0 200 OK
CSeq: 1
Content-Type: application
```

```
Content-Length: XXX
```

The Metadata stream itself is then transported by RTP.

XML shall be streamed directly with one XML document after each other, via RTP. For synchronisation to the video stream a RTP timestamp shall be used with the time of occurrence. Only UTC timestamps shall be used within the metadata stream. This pure XML Metadata payload shall signal through the XML root node ´<?xml version="1.0" encoding="UTF-8"?> and the XML namespace xmlns used such as "http://www.xxx.org/ver10/schema" or "urn:yyy-org" that an XML document stream is following.

NOTE A XML Metadata schema and namespace for video surveillance applications is defined in IEC 62676-2-3.

8 Video stream control requirements

8.1 General

Today a lot of incompatible video streaming and stream control implementations exist, although standards are used. In this clause general requirements for the application of existing standards on video stream control are introduced,

In this clause the use of the Real Time Streaming Protocol (RTSP) according to RFC 2326 for live streaming and/or playback capable Video Transmission devices is specified.

RTSP is an application-level protocol for control over the delivery of data with real-time properties. Here the use of RTSP for VSSs is specified.

Session establishment refers to the method by which a Video Transmission client obtains the initial session description. The initial session description can e.g. be an URL to the content.

An example for a valid request from a Video Transmission client is:

```
rtsp://140.10.10.22:554/VideoChannel/1/h264/1/trackID=1
```

8.2 Usage of RTSP in video transmission devices

8.2.1 General

Live video streaming

The Live Stream is characterized as the equivalent of the traditional analog VSS. The actual video streams are typically delivered in multicast mode. This means that the presentation is linear and that there is no support for trick mode operation e.g. pause, fast forward and similar. The display is a continuous flow of data and events and not on demand.

Replay including trick modes

The Replay Streaming with Trick Modes is characterized as the equivalent of the Live Streaming with the addition to support for trick mode operation e.g. pause, reverse, fast forward and similar. Therefore the actual video streams are delivered in unicast mode only. The presentation is a continuous flow of events as well.

8.2.2 The use of RTSP with multicast

Optionally, it is possible to use RTSP for joining multicasts of Live Streaming.

NOTE In principle a multicast does not support trick mode operation, therefore it cannot be used.

Specifically, firewalls will be able to ascertain the incoming port being used i.e. this will allow them to open the ports and do any necessary port forwarding. Furthermore, it can be useful if the RTSP video server wishes to count the number of video clients subscribed.

When no indication is given by RTSP whether the mode of delivery is unicast or multicast, according to RFC 2326 the default video stream shall be delivered in multicast mode.

For any VTD shall the maximum number of unicast streams supported be specified.

8.3 RTSP standards track requirements

8.3.1 General

Following RTSP Requirements apply for Video Transmission Devices:

The video transmission device shall support the Real Time Streaming Protocol (RTSP) according to IETF RFC 2326: RTSP video transmission clients and servers shall implement all required features of the minimal RTSP implementation described in Appendix D of RFC 2326:1998.

8.3.2 High level IP video streaming and control interfaces

If any other interfaces, e.g. based on web services or HTTP requests, offer the initiation of streaming and retrieval of a video stream URI, this shall be in addition to the methods defined in this clause. It shall always be possible to refer to an URI according to the requirements of this clause.

VTDs offering a high-level interface for streaming and stream control shall support as well the minimal video stream control Interface introduced in the following including their minimum requirements:

8.3.3 Minimal RTSP method and header implementation

RTSP video transmission receiver shall implement the mandatory methods PLAY, OPTIONS, DESCRIBE, SETUP, TEARDOWN in the direction of the video transmitter (R->T). The default port number for a VTD RTSP server is 554. All clients and server shall implement all required features of the minimal RTSP implementation described in Appendix D of RFC 2326:1998.

8.3.4 RTSP authentication

The documentation of VTDs shall specify the methods supported for authentication. A VTD shall support one of the two methods ´Basic-´ or ´Digest-Authentication´ for the RTSP interface and the HTTP interface. In any case the Authentication has to be implemented according to RFC 2617 – HTTP Authentication: Basic and Digest Access Authentication. RTSP servers supporting HTTP digest authentication shall implement it according to RFC 2069. Digest Access Authentication is recommended in security grade 3 and 4 systems, because of the higher security provided. The range of valid user names, accounts and passwords to access a RTSP session is configured in the VTD.

9 Device discovery and description requirements

Any VT device shall offer means to be detected in the network and offer a description about its video features and capabilities.

A VTD has to offer protocols for device discovery and description in an IP video network. The VTD shall support at least one of the 2 methods: WS-Discovery and/or Zeroconf.

In this standard, only the basic support of this functionality is required. In IEC 62676-2 series additionally a detailed protocol implementation is defined and required for these 2 device discovery and description methods.

10 Eventing requirements

A VTD has to offer protocols to signal the health status and events associated to the video source. According to IEC 62676-1-1 a VTD shall signal video loss, signal noise, signal too bright, too dark and camera deposition. The notification of motion and other video content analysis events in the video image shall be done by the same means. These states need generally to be signalled via the video IP interface in a defined manner by standardizes values, attributes or events, in order to let a VTD client exactly know the detailed status of any VTD server independent of device type, manufacturer or integrator software.

In this standard only the basic support of this eventing functionality is required. In IEC 62676-2 series eventing methods and detailed protocol implementations are defined and required.

Additionally following requirements for device management apply, if a VTD is operated in an IT network or office network environment:

11 Network device management requirements

11.1 General

This subclause concerns recommendations.

The two disciplines of IT networks and security networks are converging more and more. The end-users such as administrators are more and more responsible for both: IT equipment, security devices and their interconnecting networks.

If an IP based video surveillance system is operated in an IT environment, it is best to offer management services for video transmission devices using typical protocols for these kind of networks. Networks in industry, offices or within any IT environment already use the Simple Network Management Protocol (SNMP) to monitor and manage their information infrastructure. This enables the end-user, e.g. an administrator of a network including office and security network devices, to monitor e.g. the proper setup and operation of all the equipment by a single means at one end-point based on a single protocol:

Therefore VTDs should include the ability to communicate with enterprise-wide management systems based on the Simple Network Management Protocol (SNMP). VTDs should offer the capability to integrate into an SNMP-compliant management system that gives e.g. an administrator a single view of the various software and hardware transmission resources of this complex, distributed video network system.

If a VTD is operated in an IT environment, where it is needed to monitor and check the health status not only of office equipment, but also of security equipment such as IP video devices, the VTD should offer support for SNMP.

The VTD device should support SNMP in line with the requirements of this clause.

A Management Information Base (MIB) is a Simple Network Management Protocol (SNMP) specification containing definitions of management information so that video transmission devices and essential network components can be remotely monitored, configured and controlled. They are today used extensively in network elements such as routers, printers, hubs, switches and storage devices and more and more in IP Cameras, DVRs, encoders and decoders. In general there are four high level services for the management of video transmission network devices:

- faults and failures,
- alarm and events,
- status information and configuration,
- performance.

Fault and Failure management in security networks is based on root cause analysis involving remote identification and correction of network problems. Remote fault management monitors the health of the video transmission and network infrastructure, components, subsystems, and interfaces. Configuration and Status management enables the remote setup of network devices, interfaces and services. Performance management involves analysis of processing trends and network problems so that proactive actions can be taken to assure network availablility and finally the security of the protected site.

11.2 IP video MIB example

This subclause concerns recommendations

The following Figure 8 shows a high-level diagram of the MIB that is used to monitor VT devices. The organization of the MIB is defined in RFC 1155. For VSSs the private MIB 31373 is reserved and should be used.

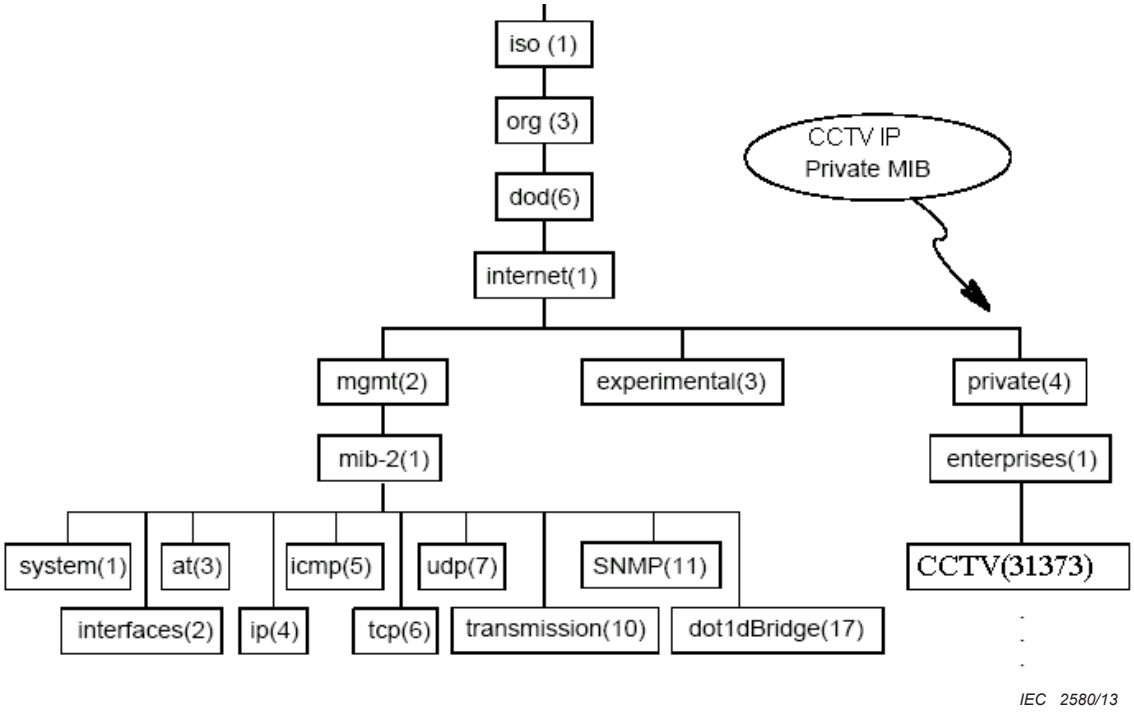

Figure 8 – MIB structure

11.3 The SNMP agent and manager for video transmission devices

This subclause is informative.

SNMP management is based on the agent/manager model described in the network management standards of the International Organization for Standardization (ISO). In this model, a network or systems manager exchanges monitoring and control information about system and network resources with distributed software components, the so-called ´agents´.

Any system or network resource that is manageable through the exchange of information is a managed resource. This can be a software resource e.g. a PC based network video recorder or digital video recorder or a hardware resource e.g. an IP camera, video encoder or decoder.

Agents typically are part of a managed resource and function as a kind of ´collection devices´ that assemble and send data about this managed resource as answer on a request from a SNMP manager. In addition, VTD agents should have the ability to issue unsolicited reports to managers when they detect certain predefined thresholds or conditions on the managed resource e.g. video loss events, detection of motion, hardware problems. In SNMP terminology, these unsolicited event messages are called trap notifications. This trap notification is a message about the occurrence of an event or the crossing of a predefined threshold, sent to a SNMP manager by a SNMP agent.

A manager is based on an information structure on properties of the managed resources provided by the agents. This is built by the Management Information Base (MIB). When new agents, e.g. with attaching a video transmission system to a network, are added and shall be included into the management of a SNMP manager, the manager shall understand the structure of this new MIB component defining the features and capabilities of the resources. These features have to be defined in an SNMP-compliant MIB and are called ´objects´. The definition of a common MIB shared by all different types of video transmission devices in a security network provides even for very heterogeneous recourses of a distributed system within the protected site a unified view and single way to manage system and network resources.

Network devices such as routers can send notifications to SNMP managers when particular events occur. For example, a SNMP agent might send a message to a SNMP manager when an error occurs.

SNMP notifications can be sent as traps or inform requests. An SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU. Traps are sent only once, while an inform may be retried several times.

11.4 Performance requirements on the SNMP agent

This subclause is normative.

If a VSS is using SNMP for the health check and monitoring of VTDs, the following performance requirements are important for a reliant communication and shall be applied: For this reason any VTDs or IP video device in security applications shall comply to these requirements, even beyond of the SNMP interface defined in this standard including vendor specific MIBs.

1) The agent shall be capable of giving a SNMP-RESPONSE to a SNMP-GET with multiple variables. The agent shall be able to respond to a SNMP-GET with multiple OIDs in one SNMP packet.
2) In polling mode, the values of the OIDs shall reflect the real state of the queried video transmission device hardware within 5 s of a state transition and also be signalled by TRAP within 5 s of a state transition, if that TRAP is enabled.
3) The “Request ID” used during the query by the manager is to be used again in the response (SNMP response).
4) The response times for GETs are to be met in accordance with requirement 2) of this subclause.
5) The agent shall work in a stable manner. The stable state of the video transmission agent is characterised as follows:
   – the video transmission devices to be controlled can be operated at all times;
   – the agent always supplies a RESPONSE to all valid REQUESTs;
   – neither the agent nor the connected video transmission device executes a restart during operation without this being requested.
   – The agent’s parameter settings are retained during operation and only change because of control actions.

6) All the counters shall be zeroed when warm or cold starting the agent. The current state of the device (contained in the saved TRAP mask) is to be transferred after booting up by means of TRAP/notification.

7) If VTD system components cannot be accessed internally or the agent is not capable of providing information about these components, the integer value of 0 (undefined) shall be returned in response to a Get, GetNext and GetBulk request for the OID of these system components. At the same time, the error status shall be set to NoError. If the system is not capable of implementing a received SET request, the command shall be correctly acknowledged, although it shall not be saved. SNMP set requests are generally acknowledged (if no SNMP error occurs) with NoError and the correct Varbinds-OID (e.g. Local Mode). Trap, notification and SNMP get requests provide information relating to the successful execution of the command.

8) If an OID is obsolete, this is to be skipped during a ´walk´. In the case of a REQUEST, the SNMP error 'NOSUCHNAME' is to be used as a response, i.e. the agent behaves as though the OID does not exist.

9) To detect lost TRAPs, a global TRAP counter ("eventCounter") is implemented in the CommonVarbinds-MIB. Prior to sending a TRAP/notification, the OID even-Counter value is to be incremented by 1. The current value can be queried using the OID eventCounter.

10) The TRAP priority is sent with a TRAP and shall correspond to the defined priority of the respective event. It carries the OID of the event priority.

11) A minimum of 10 entries for each individual SNMP table defined in this standard shall be supported, exceptions shall be specified.

11.5 VSS SNMP trap requirements for event management

This subclause is normative.

Polling applications are the most common type of SNMP monitoring applications written to check the status of devices. All listed items have to be provided as managed objects through SNMP GET messages

Event management provides the ability to receive asynchronous events/traps from a video transmission device, and allows the user to manage the incidents and problems indicated by this event. Example events are fan, video loss or disk alerts

VTDs shall be able to send TRAPS or INFORMS for state changes for the following items and objects to the configured receiving address:

- auxiliaries e.g. Digital I/O;
- video input status e.g. motion, video loss, depositioning, signal tampering;
- recording;
- alarm;
- temperature, fan speed and CPU load limit passed.

12 Network security requirements

12.1 General

This clause defines a security architecture for VTD. The video transmission device shall have in the higher security grade 4 the ability to provide authentication, integrity checking and encryption on all network interfaces. The intent of this architecture is to provide peer entity, data origin, and network device authentication, as well as video data confidentiality and integrity. Other types of communication security, such as operator authentication, access control and non-repudiation, are not provided in this clause. Systems that require these services may add them to VTD in a proprietary manner.

All data communication outside secured technical room areas shall be encrypted in the security grade 4. AES with 128 bit key for symmetric and RSA with 1 024 bit key shall be provided. Native encryption shall not be accepted. The VTDs shall not store any form of passwords in clear text. All such passwords either in configuration files or a database shall be encrypted.

A VTD according to this standard shall support transport level security for the security grade 4.

12.2 Transport level security requirements for SG4 transmission

Transport level security provides a protection of all video data between a VTD client and a server. Transport Layer Security (TLS) shall be provided by a VTD for encrypted transport. The TLS protocol offers authenticated transport sessions between 2 VTDs and takes care of confidentiality and integrity of the transported data.

A VTD compliant to this standard shall support in security grade 4 TLS 1.0 according to the IETF standard RFC 2246 and TLS 1.1 according to RFC 4346. Optionally the VTD may support TLS 1.2 according to RFC 5246.

The VTD shall offer protection for the transport of all data and information concerning streaming, stream control and eventing.

The VTD client and server shall support the cipher suites TLS_RSA_WITH_AES_128_CBC_ SHA and TLS_RSA_WITH_NULL_SHA from RFC 2246 and RFC 3268.

Bibliography

IEC 62676-2-3, *Video surveillance systems for use in security applications – Part 2-3: Video transmission protocols – IP interoperability implementation based on Web services*

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

ISO/IEC 10918-5, *Information technology – Digital compression and coding of continuous-tone still images: JPEG File Interchange Format (JFIF)*

ISO/IEC 14496-1, *Information technology – Coding of audio-visual objects – Part 1: Systems*

ISO/IEC 15444 (all parts), *Information technology – JPEG 2000 image coding system*

ISO 8601, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ISO 19111, *Geographic information – Spatial referencing by coordinates*

ISO 19115:2003 (all parts), *Geographic information – Metadata*

ITU Recommendation H.241, *Extended video procedures and control signals for ITU-T H.300 series terminals*

SCTE 52, *Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification*

SMPTE 298M-1997, *Television, Universal Labels for Unique Identification of Digital Data*

FIPS PUB 180-2, *Secure Hash Standard (SHS)*

FIPS PUB 197, *Advanced Encryption Standard (AES)*

FIPS PUB 46-3, *Specification for the Data Encryption Standard, National Institute of Standards and Tech*

FIPS PUB 81, *DES Modes of Operation, National Institute of Standards and Technology*

IETF Draft avt-rtp-h264-rcdo, *RTP Payload Format for H.264 RCDO Video*

IETF Draft avt-rtp-klv, *RTP Payload Format for SMPTE 336M Encoded Data*

IETF Draft avt-rtp-rfc3984bis, *RTP Payload Format for H.264 Video*

IETF Draft avt-rtp-svc, *RTP Payload Format for SVC Video*

IETF Draft avt-srtp-big-aes, *The use of AES-192 and AES-256 in Secure RTP*

IETF Draft HTTPMU, *HTTPU HTTP Multicast over UDP, HTTP Unicast over UDP*

IETF Draft RTP/AVPF, *Extended RTP Profile for RTCP-based Feedback (RTP/AVPF)*

IETF Draft RTP/RTX, *RTP Retransmission Payload Format*

IETF Draft, *SSDP Simple Service Discovery Protocol*

IETF RFC 052, *IAB Recommendations*

IETF RFC 792, *Internet Control Message Protocol*

IETF RFC 826, *An Ethernet Address Resolution Protocol*

IETF RFC 868, *Time Protocol*

IETF RFC 1034, *XML- Extensible Markup Language. W3C recommendation*

IETF RFC 1035, *Domain Names – Concepts and Facilities*

IETF RFC 1089, *SNMP over Ethernet*

IETF RFC 1109, *Ad-hoc Review*

IETF RFC 1155, *Structure of Management Information*

IETF RFC 1156, *Management Information Base (MIB-I)*

IETF RFC 1161, *SNMP over OSI*

IETF RFC 1187, *Bulk table retrieval*

IETF RFC 1212, *Concise MIB definitions*

IETF RFC 1214, *OSI MIB*

IETF RFC 1215, *Traps*

IETF RFC 1229, *Generic-interface MIB extensions*

IETF RFC 1305, *Network Time Protocol (Version 3) specification, implementation and analysis*

IETF RFC 1321, *The MD5 Message-Digest Algorithm, April 1992*

IETF RFC 1341, *MIME- Multipurpose Internet Mail Extensions*

IETF RFC 1738, *Uniform Resource Locators (URL)*

IETF RFC 1889, *Real Time Transport Protocol (RTP)*

IETF RFC 1901, *Community-based SNMPv2*

IETF RFC 1902, *Structure of Management Information for SNMPv2*

IETF RFC 1903, *Textual Conventions for SNMPv2*

IETF RFC 1904, *Conformance Statements for SNMPv2*

IETF RFC 1910, *User-based Security Model*

IETF RFC 2045, *Multipurpose Internet Mail Extensions (MIME) Part One Format of Internet Message Bodies*

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

IETF RFC 2104, *Keyed Hashing for Message Authentication*

IETF RFC 2190, *RTP Payload Format for H.263 Video Streams*

IETF RFC 2250, *RTP Payload Format for MPEG1/MPEG2 Video*

IETF RFC 2271, *An Architecture for Describing SNMP Management Frameworks*

IETF RFC 2272, *Message Processing and Dispatching for SNMP*

IETF RFC 2273, *SNMPv3 Applications*

IETF RFC 2274, *User-Based Security Model (USM) for SNMPv3*

IETF RFC 2275, *View-Based Access Control Model (VACM) for the SNMP*

IETF RFC 2279 UTF-8, *A transformation format of ISO 10646 (character encoding)*

IETF RFC 2387, *Format for representing content type*

IETF RFC 2396, *Uniform Resource Identifiers (URI) Generic Syntax*

IETF RFC 2429, *RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)*

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

IETF RFC 2576, *Coexistence between SNMP Versions*

IETF RFC 2616, *HTTP Hypertext Transfer Protocol 1.1*.

IETF RFC 2782, *A DNS RR for specifying the location of services (DNS SRV)*

IETF RFC 2790, *Host Resources MIB*

IETF RFC 2818, *HTTP over TLS*

IETF RFC 2863, *Interfaces Group MIB*

IETF RFC 2929, *Domain Name System (DNS)*

IETF RFC 3339, *Date and Time on the Internet Timestamps*

IETF RFC 3379, *Internet Group Management Protocol*

IETF RFC 3411, *An Architecture for Describing SNMP Management Frameworks*.

IETF RFC 3412, *Message Processing and Dispatching for SNMP*

IETF RFC 3413, *SNMP Applications*

IETF RFC 3414, *User-Based Security Model (USM) for SNMPv3*

IETF RFC 3415, *View-Based Access Control Model (VACM) for the SNMPIETF RFC 3412 Message*

Processing and Dispatching for the Simple Network Management Protocol

IETF RFC 3512, *Configuring Networks and Devices with Simple Network Management Protocol (SNMP)*

IETF RFC 3555, *MIME Type Registration of RTP Payload Formats*

IETF RFC 3556, *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol*

IETF RFC 3584 (Best Current Practice), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

IETF RFC 3640, *RTP Payload Format for Transport of MPEG-4 Elementary Streams*.

IETF RFC 3711, *The Secure Real-time Transport Protocol (SRTP)*.

IETF RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP USM*

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local addresses*

IETF RFC 3986, *Uniform Resource Identifier (URI) Generic Syntax*

IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*

IETF RFC 4571, *Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport*

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option*

IETF RFC 4855, *Media Type Registration of RTP Payload Formats*

IETF RFC 4288, *Media Type Specifications and Registration Procedures*

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

IETF RFC 5104, *Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)*

IETF RFC 5371, *RTP Payload Format for JPEG 2000 Video Streams*.

IETF RFC 5372, *Payload Format for JPEG 2000 Video Extensions for Scalability & Main Header Recovery.*

IETF RFC 5590 (Proposed), *Transport Subsystem for the SNMP*

IETF RFC 5591 (Proposed), *Transport Security Model for the SNMP*

IETF RFC 5592 (Proposed), *Secure Shell Transport Model for the SNMP*

IETF RFC 5608 (Proposed), *Remote Authentication Dial-In User Service (RADIUS) Usage for SNMP Transport Models.*

IETF RFC 2222, *Simple Authentication and Security Layer (SASL)*

IETF RFC 3264, *An Offer/Answer Model with Session Description Protocol (SDP)*

IETF RFC 3376, *Internet Group Management Protocol, Version 3*

IETF STD 16 RFC 1213, *Management Information Base (MIB-II)*

IETF STD 5 RFC 1112, *Host extensions for IP multi-casting*

IETF STD 5 RFC 791, *Internet Protocol*

IETF STD 6 RFC 768, *User Datagram Protocol*

IETF STD 62 RFC 3411, *An Architecture for Describing SNMP Management Frameworks*

IETF STD 62 RFC 3412, *Message Processing and Dispatching for the SNMP*

IETF STD 62 RFC 3413, *Simple Network Management Protocol (SNMP) Application*

IETF STD 62 RFC 3414, *User-based Security Model (USM) for version 3 of the SNMPv3*

IETF STD 62 RFC 3415, *View-based Access Control Model (VACM) for the SNMP*

IETF STD 62 RFC 3416, *Version 2 of the Protocol Operations for the SNMP*

IETF STD 62 RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*

IETF STD 62 RFC 3418, *Management Information Base (MIB) for the SNMP*

IETF STD 7 RFC 793, *Transmission Control Protocol*

MISB Standard 0107, *Bit and Byte Order for Metadata in Motion Imagery Files and Streams*

MISB RP 0701, *Common Metadata System Structure (CMS)*

MISB RP 0702, *Content part of CMS*

OASIS Standard Web Services Base Notification 1.3

OASIS Standard Web Services Dynamic Discovery (WS-Discovery)

SMPTE 359M-2001, *Television and Motion Pictures, Dynamic Documents*

W3C Extensible Markup Language (XML) 1.0 (Third Edition), W3C Recommendation

W3C SOAP 1.2, Part 1 Messaging Framework

W3C SOAP, Message Transmission Optimization Mechanism

W3C SOAP, Version 1.2 Part 2 Adjuncts (Second Edition)

W3C Web Services Addressing (WS-Addressing) W3C Recommendation,

W3C Web Services Addressing 1.0 – Core

W3C Web Services Description Language (WSDL) 1.1

W3C Web Services Eventing (WS-Eventing), W3C Recommendation

W3C XML Path Language (XPath), W3C Recommendation

W3C XML Schema Part 1 Structures Second Edition, W3C Recommendation

W3C XML Schema Part 2 Datatypes Second Edition, W3C Recommendation

W3C XML-binary Optimized Packaging

W3C XML-NMSP – Namespaces in XML, W3C Recommendation

W3C XML 1.0, Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation

W3C XML Namespaces, Namespaces in XML, W3C Recommendation

W3C XML Information Set, XML Information Set, W3C Recommendation

W3C XML Schema: XML Schema Part 1: Structures, W3C Recommendation

W3C XML Schema: XML Schema Part 2: Datatypes, W3C RecommendationW3C WS-Addressing, Web Services Addressing 1.0 – Core, W3C Recommendation

W3C Web Services Eventing (WS-Eventing), W3C Recommendation

W3C WSDL 1.1, Web Services Description Language (WSDL) 1.1, W3C Recommendation

W3C WSDL Binding for SOAP 1.2, WSDL 1.1 Binding Extension for SOAP 1, W3C ecommendation

———————

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.