GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 13.310

CCS A 91

GB/T 28181-2022

Replacing GB/T 28181-2016

Technical requirements for information transmission, switch and control in video surveillance networking system for public security

公共安全视频监控联网系统信息传输,交换,控制技术要求

Issued on: December 30, 2022 **Implemented on: July 01, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

Table of Contents

Technical requirements for information transmission, switch and control in video surveillance networking system for public security

1 Scope

This document specifies the peer-to-peer networking structure of the video surveillance networking system for public security (hereinafter referred to as "surveillance networking system"), the basic requirements and security requirements for transmission, exchange, and control, as well as the technical requirements for control, transmission process, and protocol interface.

This document is applicable to the scheme design, system testing, acceptance and related device development and production of the video surveillance networking system for public security. Other video surveillance networking systems can be implemented by using this document as reference.

2 Normative references

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

GB/T 4754, *Industrial classification for national economic activities*

GB/T 10114-2003, *Rules for the code representation of administrative divisions under counties*

GB 18030, *Information technology - Chinese coded character set*

GB/T 25724, *Technical specifications for surveillance video and audio coding*

GB 35114, *Technical requirements for information security of video surveillance network system for public security*

GA/T 380, *Coding rules for public security organs*

ISO/IEC 13818-1:2019, *Information technology - Generic coding of moving pictures and associated audio information - Part 1: Systems*

ISO/IEC 14496-2:2004, *Information technology – Coding of audio-visual objects -*

3.1.3 user terminal

A client device that is registered and authorized by a networking system and has operational requirements for data and/or devices within the system.

3.1.4 session initiation protocol; SIP

Developed by the Internet Engineering Task Force (IETF), it is a framework protocol for multi-party multimedia communication.

NOTE: Session initiation protocol is a text-based application layer control protocol, independent of the underlying transport protocol. It is used to establish, modify and terminate two-party or multi-party multimedia sessions on IP networks.

3.1.5 session control

The process of establishing, modifying or ending a communication between one or more participants.

3.1.6 SIP surveillance realm

A monitoring system consisting of front-end device, user terminals, servers, and networks conforming to the provisions of this document.

3.1.7 non-SIP surveillance realm

Surveillance systems that do not comply with the provisions of this document.

3.1.8 the third party controller

A SIP user agent (UA), capable of creating a session between two other user agents.

NOTE: Third party controllers are generally implemented using back-to-back user agents (B2BUA).

3.1.9 the third party call control

The third party controller initiates, establishes, and releases sessions between two or more parties, and is responsible for the media negotiation between the parties.

3.1.10 user agent

SIP logical end entity specified by IETFRFC 3261. It is composed of user agent client (UAC) and user agent server (UAS). UAC is responsible for initiating calls, and UAS is responsible for receiving calls and responding.

3.1.11 proxy server

SIP logical entity specified by IETF RFC 3261. Through it, the request from the user agent client (UAC) is forwarded to the user agent server (UAS), and the response

message of the UAS is forwarded back to the UAC.

3.1.12 register server

SIP logical entity specified by IETF RFC 3261, which has the function of receiving registration requests, saving the information carried in the requests, and providing location services within the domain.

3.1.13 redirect server

SIP logical entity specified by IETF RFC 3261. The server is responsible for planning SIP routing and telling the requester the obtained signaling next-hop address information, so that the requester can directly send a request to the next hop according to this address.

3.1.14 back to back user agent

SIP logical entity specified by IETF RFC 3261. It acts as a user agent server (UAS) to receive request messages and process the messages. At the same time, in order to decide how to respond to the request message, it also acts as a user agent client (UAC) to send the request message.

NOTE: A back to back user agent (B2BUA) differs from a proxy server in that a B2BUA needs to maintain a state of the conversations it creates.

3.1.15 functional entity

A collection of logic units that implement some specific functions.

NOTE: A physical device can consist of multiple functional entities. A functional entity may also consist of multiple physical devices.

3.1.16 source device

A device that actively initiates a service request.

3.1.17 target device

A device that finally responds to service requests.

3.1.18 SIP client

An entity that complies with the provisions of IETF RFC 3261 and has the functions of registration, establishment/termination of session connection, reception and playback of video and audio streams, etc. It mainly includes user interface, user agent (UA), media decoding module and media communication module.

3.1.19 SIP device

Peer-to-peer networked networking system platforms and devices shall not send application-independent messages to each other's SIP ports. Avoid application-independent messages from occupying SIP message processing resources of networking system platforms and devices.

This document is based on basic protocols such as IETF RFC 3261 and specifies the various business functions of monitoring and networking. If this document has special provisions for various functions, it shall follow this document, otherwise it shall follow the reference agreement such as IETF RFC 3261.

4.3.3 Session description protocol

The session negotiation and media negotiation of the session establishment process between devices in the networking system shall be described by the IETF RFC 4566 protocol. The main content includes session description, media information description, and time information description. Session negotiation and media negotiation information shall be carried and transmitted in the message body of the SIP message.

4.3.4 Control description protocol

Control commands related to front-end device control, alarm information, and device directory information of the networking system shall be described in MANSCDP and shall comply with the provisions of Annex A. Networking system control commands shall be carried and transmitted in the message body of the SIP message MESSAGE.

4.3.5 Media playback control protocol

The playback control command of historical video and audio shall use MANSRTSP. The protocol description shall comply with the provisions of Annex B. It shall realize the remote control of video and audio streams such as normal, fast, pause, stop, and random drag and play between devices between end-to-end. The historical media playback control command is carried and transmitted by the message body of the SIP message INFO.

4.3.6 Media transmission and media codec protocol

RTP transmission shall be supported when the media stream is transmitted on the IP network of the networking system. The media stream sending source shall support the function of controlling the peak value of media stream sending. The RTP load shall be in one of two formats: Video and audio data or video and audio elementary stream data based on PS encapsulation shall comply with the provisions of Annex C. The transmission of the media stream shall adopt the RTP protocol stipulated in IETF RFC 3550. Provide time stamp information in real-time data transmission and synchronization of each data stream. The RTP timestamps of all RTP packets encapsulated in the same frame of video and audio packets are the same, and different from the RTP timestamps of RTP packets of different frames of video and audio packets. The RTCP protocol stipulated in IETF RFC 3550 shall be adopted to provide reliable

guarantee for the sequential transmission of data packets. Provide flow control and congestion control.

5 Transmission requirements

5.1 Requirements for network transmission protocol

The network layer of the networking system shall support the IP protocol. The transport layer shall support TCP and UDP protocols.

5.2 Requirements for media transfer protocol

Video and audio streams shall support RTP/RTCP protocol when transmitted on IP-based network. The data encapsulation format of video and audio streams shall meet the requirements of 4.3.6.

When video and audio streams are transmitted on an IP-based network, it is advisable to extend support for the TCP protocol. The protocol shall comply with the provisions of Annex D.

5.3 Information transmission delay time

When networking system information is transmitted via an IP network, the end-to-end information delay time (including the time elapsed during information collection, encoding, network transmission at the sending end, and information decoding and displaying at the receiving end) shall meet the following requirements:

a) The end-to-end information delay time between the front-end device and the corresponding device directly connected to the monitoring center shall not be greater than 2 s.

b) The end-to-end information delay time between the front-end device and the user terminal device shall not be greater than 4 s.

5.4 Network transmission bandwidth

The network bandwidth design of the networking system shall be able to meet the bandwidth requirements of front-end device access to the monitoring center, peer-to-peer networking of monitoring center, and user terminal access to the monitoring center. There shall be allowance.

5.5 Network transmission quality

The transmission quality (such as transmission delay, packet loss rate, packet error rate, false packet rate, etc.) of the networking system IP network shall meet the following requirements:

6.2 Media encoding-decoding

Video codec in networking system shall adopt SVAC, H.264, H.265 or MPEG-4. SVAC is preferred. The audio encoding-decoding shall be G.711, G.722.1, G.723.1, G.729, SVAC or AAC. Relevant technical requirements shall comply with the provisions of Annex F.

6.3 Media storage encapsulation format

The storage and packaging format of media data such as video and audio in the networking system shall be PS format. See ISO/IEC 13818-1:2019 for the format.

6.4 Definition of SDP

The SDP content carried by the SIP message body in the networking system shall comply with the relevant requirements of IETF RFC 4566. The required fields shall comply with the provisions of Annex G.

6.5 Conversion of network transmission protocol

It shall support the two-way protocol conversion between the network transmission protocol of the non-SIP surveillance realm and the network transmission protocol specified in 5.1.

6.6 Conversion of control protocol

It shall support the two-way protocol conversion between the device control protocol in the non-SIP surveillance realm and the session initiation protocol, session description protocol, control description protocol and media playback control protocol specified in 4.3.

6.7 Conversion of media transfer protocol

It shall support the two-way protocol conversion between the media transmission protocol and data encapsulation format of the non-SIP surveillance realm and the media transmission protocol specified in 5.2 and the data encapsulation format specified in 4.3.6.

6.8 Conversion of media data format

It shall support the conversion of the media data in the non-SIP surveillance realm to the data in the media encoding format specified in 6.2.

6.9 Peer-to-peer networking with other systems

The peer-to-peer networking between the networking system and other systems shall comply with the requirements of Annex A and Annex E.

6.10 Signaling character set

The SIP signaling character set of networking systems and device shall adopt the encoding format in GB 18030.

6.11 Multipath cascaded networking structure

If some networking system management platforms have multiple upper-level platforms, the entire cascaded networking is not the tree structure shown in Figure 2 and Figure 3. There is a possibility that the upper-level platform accesses the target device of the lower-level platform through multiple paths. The management platform shall support this function according to the technical requirements in Annex H.

7 Control requirements

7.1 Registration

Registration meets the following requirements:

a) It shall support the working mode of registering with the SIP server when the device or system enters the networking system.

b) Device or system registration shall be extended to support carrying protocol version identification. The protocol version identification shall comply with the provisions of Annex I.

c) If the device or system registration is unsuccessful, it is advisable to re-register after a certain random time delay.

d) It is advisable to implement the registration redirection function. Dynamically assign access servers to devices, so as to cope with server-side load balancing and fault migration when large-scale devices are connected.

e) See 9.1 for the session control process of device or system registration.

7.2 Real-time video and audio on demand

Real-time video and audio on demand meets the following requirements:

a) It shall support real-time video and audio on demand according to specified device and specified channels. Support multi-user simultaneous demand for the same video and audio resources.

b) See 9.2 for the session control process of real-time video and audio on demand. The session description information adopts the format specified in 6.4.

7.3 Control

The control meets the following requirements:

a) It shall support sending control information to designated devices, such as camera pan/tilt control, video control, arming/disarming of alarm devices, etc., so as to realize the remote control of various actions of the device.

b) It shall support remote start, alarm reset, forced key frame, frame zoom in, frame zoom out, guard position control, PTZ precise control and other controls.

c) It shall support the formatting of the camera memory card.

d) It shall support automatic and manual tracking of targets in live video images.

e) It shall support parameter configuration of the device, including basic parameters, video parameter range, SVAC encoding, SVAC decoding, video parameter properties, recording plan, alarm recording, video screen occlusion, screen flip, alarm reporting switch, front-end OSD settings, image capture configuration.

f) See 9.3 for the session control process of device control. The device control command SIP message body adopts XML encapsulation, and complies with the provisions of Annex A.

7.4 Alarm event notification and distribution

Alarm event notification and distribution shall meet the following requirements:

a) It can receive the alarm information sent by the alarm source in real time. Distribute the alarm information to the corresponding user terminals or systems and device in a timely manner according to the alarm handling plan.

b) See 9.4 for the session control process of receiving and distributing alarm information. The SIP message body of the alarm event notification command is encapsulated in XML and conforms to the format specified in Annex A.

7.5 Device information query

Device information query shall meet the following requirements:

a) Support hierarchical query and obtain information such as device directory, device information, device status, device configuration, device preset position, watchdog position, cruise track list, cruise track, PTZ accurate status, memory card status and other information of registered devices or systems in the networking system.

b) See 9.5.2 for the query session control process. The SIP message body of the query command for device directory, device information, device status, device configuration, device preset position, guard position, cruise track list, cruise track,

PTZ precise status, and memory card status is encapsulated in XML and complies with the provisions of Annex A.

c) Support querying the basic information of the device, such as device manufacturer, device model, version, supported protocol type, etc.

d) The organization method of the device directory shall be in accordance with the relevant provisions of Annex J.

7.6 Status information submission

Status information submission shall meet the following requirements:

a) Support the collection and detection of monitoring device, alarm device, related servers and connected network systems in the network by actively reporting.

b) See 9.6 for the session process of reporting status information. The SIP message body of the status information reporting command is encapsulated in XML and complies with the provisions of Annex A.

7.7 Retrieval of historical video and audio files

Retrieval of historical video and audio files shall meet the following requirements:

a) Support retrieval of historical video and audio files of a specified time period on a specified device.

b) See 9.7 for historical video and audio retrieval process.

7.8 Playback of historical video and audio

Playback of historical video and audio meets the following requirements:

a) It shall support remote playback of historical video and audio data at a specified time on a specified device or system. The playback process shall support media playback controls such as normal playback, fast playback, slow playback, screen pause, and random drag and drop.

b) It shall support the function of video rewinding and rewinding and dragging.

c) For the session control and video and audio playback control process of historical video and audio playback, see 9.8. The session description information adopts the format stipulated by the SDP protocol. Video and audio playback control commands shall adopt the MANSRTSP protocol format specified in Annex B.

7.9 Download of historical video and audio files

Download of historical video and audio files shall meets the following requirements:

a) Support the download of historical video and audio files for a specified period on a specified device.

b) See 9.9 for the historical video and audio download process.

7.10 Network time calibration

Network time calibration meets the following requirements.

a) The IP network access device in the networking system shall support the unified timing of SIP signaling. The access device shall accept the time service carried by the SIP server through the Date field of the message header during registration.

b) The IP network server device in the networking system shall support the network unified time calibration service of the NTP (see IETF RFC 2030) protocol. The network time calibration device is divided into clock source and client. It supports the working mode of client/server. The clock source shall support TCP/IP, UDP and NTP protocols, and can output the input or self-generated time signal in standard NTP packet format.

7.11 Subscriptions and notifications

It shall support subscription and notification mechanism, event and directory subscription and notification. For specific protocol signaling process, see 9.11.

7.12 Voice broadcast and voice intercom

It shall support voice broadcast and voice intercom mechanism. For protocol signaling process, see 9.12.

7.13 Device software upgrade

It shall support software upgrades for designated devices. For protocol signaling process, see 9.13.

7.14 Image capture

It is advisable to support designated devices for image capture and transfer the captured images to designated positions. For protocol signaling process, see 9.14.

8 Transmission, exchange, control security requirements

8.1 Device identity authentication

Device identity authentication meets the following requirements:

a) It shall support unified coding for all devices connected to the system. For device

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------