ICS 35.240.99
L67

中华人民共和国国家标准

GB/T XXXXX—XXXX

电子考场系统通用要求

General reguirements for electronic examination room system

（报批稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 2
4　缩略语 5
5　概述 7
6　视频巡考系统 7
6.1　系统结构 7
6.2　系统功能要求 11
6.3　音视频编解码要求 13
6.4　数据传输要求 15
6.5　数据交换要求 16
6.6　6.6 端口定义 16
6.7 设备控制协议 17
6.8 电子考场设备兼容性 21
7　无线电作弊防控系统 21
7.1　概述 22
7.2　系统功能要求 22
7.3　系统性能要求 23
7.4　传输与管理 24
8　身份识别系统 26
8.1　概述 27
8.1.1　系统组成架构 27
8.1.2　考生身份信息采集验证终端 27
8.1.3　考生身份识别管理系统软件 28
8.1.4　管理计算机 28
8.1.5　网络设备 28
8.2　考生身份信息采集验证终端技术要求 28
8.2.1　概述 28
8.2.2　手持式验证终端技术要求 29
8.2.3　立式验证终端技术要求 29
8.3　考生身份信息识别管理系统功能要求 29
8.3.1　考生身份信息识别与验证管理系统 29
8.3.2　考生信息采集 29
8.4　系统安全要求 30

9 指挥系统.....30
9.1 概述.....30
9.2 指挥中心功能要求.....30
9.3 指挥中心的布局与环境要求.....34
9.4 考务室技防设备系统.....35
9.5 试卷保密室技防设备系统建设要求.....35
附录A（规范性附录） 学校（机构）命名规则.....37
附录B（资料性附录） 电子考场设备兼容性检测.....38
附录C（资料性附录） 作弊防控系统功能与性能测试.....43
附录D（资料性附录） 身份识别系统测试.....47
参考文献.....49

前　言

本标准按照GB/T 1.1－2009给出的规则起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由全国信息技术标准化技术委员会（SAC/TC28）提出并归口。

本标准起草单位：清华大学、华南理工大学、上海交通大学、北京大学、南京大学、浙江大学、中国科技大学、中山大学、武汉大学、中国传媒大学、中国人民大学、东华大学、华东理工大学、广州大学、北京理工大学、中央民族大学、北京科技大学、北京信息科技大学、北京对外经济贸易大学、苏州科技大学、常州大学、内蒙古大学、北京竞业达数码科技股份有限公司、成都佳发安泰科技股份有限公司、杭州恒生数字设备科技有限公司、苏州科达科技股份有限公司、浙江宇视科技有限公司、北京艾威康电子技术有限公司、上海金桥信息股份有限公司、科大讯飞股份有限公司、天津天地伟业数码科技有限公司、浙江大华技术股份有限公司、杭州海康威视数字技术股份有限公司、杭州艾力特音频技术有限公司、广州云积软件技术有限公司、深圳市台电实业有限公司、中国华录松下电子信息有限公司、汉柏科技有限公司、苏州信颐系统集成有限公司、深圳市东微智能科技股份有限公司、长沙世邦通信技术有限公司、中国电子技术标准化研究院。

本标准主要起草人：钟晓流、丁泉龙、沈宏兴、陈学林、何山、钱震、王坚、崔建生、蔡志华、吴庚生、郑道林、左渠、肖波、季至宇、薛玉田、道焰、牛长山、马振平、杜建新、刘鹏图、刘志勇、王晓、江一山、夏卫、张宇燕、王鹏、李海霞、宋述强、余云涛、李莹、彭涛、张少华、王梁斌、赵峰、任军军、邹喜军、任俊峰、姚下丽、张赛晖、贾云龙、侯移门、冉旭、王博、朱利民、季青松、周迪、季海交、龚小峰、李家齐、葛萌、柳定一、杜中华、马震远、张爱军。

电子考场系统通用要求

1 范围

本标准从视频巡考系统、无线电作弊防控系统、身份识别系统和指挥系统四个部分规定了电子考场网上巡查系统的系统结构、功能要求、技术要求、系统安全性、无线电兼容性、环境适应性和可靠性等通用技术要求。

本标准适用于电子考场网上巡查系统的设计、建设和管理。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 2887-2011 计算机场地通用规范

GB 8702-2014 电磁环境控制限值

GB/T 9361-2011 计算机场地安全要求

GB/T 13000-2010 信息技术 通用多八位编码字符集（UCS）

GB/T 17975.1-2010 信息技术 运动图像及其伴音信息的通用编码 第1部分：系统

GB18030-2005 信息技术 中文编码字符集

GB/T 20090.1-2012 信息技术 先进音视频编码 第1部分：系统

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25068.5-2010 信息技术 安全技术 IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护

GB/T 25724-2017 公共安全视频监控数字视音频编解码技术要求

GB/T28181-2016 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 33782-2017 信息技术 学习、教育和培训 教育管理基础代码

GB 50799-2012 电子会议系统工程设计规范

GA450-2013 台式居民身份证阅读器通用技术要求

GA/T1011-2012 居民身份证指纹采集器通用技术要求

ISO/IEC 14496-3 信息技术 视听对象的编码 第3部分：音频（Information technology -- Coding of audio-visual objects -- Part 3: Audio）

ITU-T G.711-1988 话音频率的脉冲编码调制（Pulse code modulation (PCM) of voice frequencies）

ITU-TG.729-2012使用共轭结构代数代码激励线性预测（CS-CELP）的8kbit/s 语音编码（Coding of speech at 8k bit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)）

ITU-T G.721 3232k bit/s自适应差分脉冲编码调制(32kbit/s ADPCM adaptive difference pulse code modulation)

ITU—T VCEG AVC/H.264 视频编码标准(Advanced Video Coding)

ITU－T VCEG HEVC/H.265高效视频编码标准(High Efficiency Video Coding)

IETF RFC 2327 SDP: 会话描述协议（SDP: Session Description Protocol）

IETF RFC 3428 SIP:即时消息（SIP: Session Initiation Protocol (SIP) Extension for Instant Messaging）

3 术语和定义

下列术语和定义适用于本标准。

3.1

电子考场系统 online inspection system

以维护国家教育考试安全为目的，基于视音频、显示、存储及网络相关设备和相关软件，运用安全防范技术和技术手段组成的综合巡查系统。

3.2

中心管理单元 central management unit

教育考试电子考场系统中管理所有设备和资源的核心单元。

注：中心管理单元也是系统的中心信令控制服务器，具有注册服务器，代理服务器，重定向服务器，背靠背用户代理等SIP逻辑实体的功能。

3.3

媒体存储单元 media storage unit

教育考试电子考场系统中存储视音频数据的单元。

注：具有历史视音频文件检索和点播功能。

3.4

流媒体单元 streaming media unit

教育考试电子考场系统中对视音频媒体流进行转发的单元。

3.5

显示单元 display unit

教育考试电子考场系统中对解码后的视音频码流进行显示和收听的单元。

3.6

解码单元 decoding unit

教育考试电子考场系统中对视音频媒体流进行解码的单元。

3.7

网关单元 gateway unit

教育考试电子考场系统中进行控制协议转化和媒体流转码、转发的单元。

3.8

管理客户端 management client

教育考试电子考场系统中用户可直接操作的客户端软件。

注：用户可通过管理客户端执行系统功能。

3.9

用户终端 user terminal

经过指挥系统注册并授权的，有数据或设备操作需求的客户端设备。

3.10

指挥中心 dispatch and control center

电子考场系统中的某一级信息汇集、监视、控制、管理和共享的节点。

注：可与其它相关业务系统实施联动，支持相关部门实施业务管理。

3.11

无线电作弊 radio cheating

利用无线电通信工具和手段进行考试作弊的行为。

3.12

无线电作弊防控系统 radio cheating shielding system

对无线电作弊行为进行防控的系统。

3.13

无线电信号侦测子系统 radio signal detecting sub-system

安装于考点区域内适当位置，对该区域内异常无线电信号进行寻找的子系统。

注：具备频谱快速监测、异常信号识别、信号特征提取、信号还原取证及引导阻断子系统发送干扰信号的功能。

3.14

无线电信号阻断子系统 radio signal blocking sub-system

在无线电侦测子系统引导下发射阻断信号对异常信号进行干扰的子系统。

3.15

作弊防控管理子系统 cheating shielding management sub-system

安装在考点指挥中心，对考点区域内侦测子系统设备和阻断子系统设备集中控制管理，掌握设备工作状态，查看异常信号信息（时间、频率、类型、内容等）的子系统。

注：作弊防控管理子系统根据权限和具体管理内容不同，分为考点管理子系统和上级管理子系统，上级管理子系统部署于上级指挥中心，对下级作弊防控系统管理，包括系统设备信息、异常信号信息的汇总及呈现。

3.16

侦测引导阻断 detecting and blocking

当侦测系统检测到目标信号时，阻断系统发送阻断信号，实施阻断干预的技术。

3.17

背景频谱 background frequency spectrum

在考点区域内通过较长时间多次采集综合得到的日常信号，在系统工作时可以作为基准背景信号使用的频谱。

3.18

点频阻断 narrow band signal blocking

阻断信号为点频信号的阻断。

3.19

黑白名单 black and white list

一组具有特殊特征的名单列表，黑名单列表中的信号出现时应当将其阻断，白名单列表中的信号出现时系统不影响该频率的正常使用。

注：黑白名单可以是频点也可以是频段。

3.20

还原取证 evidence taken

对异常信号数据进行提取或者保存，为证据保留提供方便的技术手段。

3.21

侦测响应时间 detection response time

从异常信号出现到侦测发现该信号之间经历的时间。

3.22

侦测频率精度 frequencydetecting accuracy

侦测识别的异常信号频率和异常信号实际频率之间的频率间隔。

3.23

异常信号特征信息 abnormal signal characteristics

用以描述异常信号的关键参数信息。

注：包括频率、带宽、强度、调制方式等。

3.24

系统响应时间 system response time

从异常信号出现到系统发出阻断信号之间经历的时间。

3.25

图像识别 image recognition

利用计算机对图像进行处理、分析，以识别各种不同模式的目标和对像的技术。

3.26

生物识别 biometric recognition

通过计算机与光学、声学、生物传感器和生物统计学等手段结合，利用人体固有的生理特性（如指纹、脸像、虹膜等）和行为特征（如笔迹、声音、步态等）来鉴定个人身份的技术。

3.27

会话初始协议 session itiation protocol（SIP）

由互联网工程任务组（IETF:Internet Engineering Task Force）制定的，用于多方多媒体通信的框架协议。

注：会话初始协议是一个基于文本的应用层控制协议，独立于底层传输协议，用于建立、修改和终止 IP 网上的双方或多方多媒体会话。

3.28

信令安全路由网关 signaling security routing gateway

负责接收或转发域内外 SIP 信令，完成信令安全路由网关间路由信息的传递以及路由信令、信令身份标识的添加和鉴别等功能的应用服务器。

3.29

网关级联 gateway connection

两个信令安全路由网关之间按照上下级关系连接，上级中心信令控制服务器通过信令安全路由网关可调用下级中心信令控制服务器所管辖的监控资源，下级中心信令控制服务器通过信令安全路由网关向上级中心信令控制服务器上传本级中心信令控制服务器所管辖的监控资源。

3.30

前端设备 field device

提供图像及声音功能的摄录像等设备。

3.31

服务质量（QoS）quality of service（QoS）

可为不同的网络应用和网络流量提供可控和可预见的服务。通过 QoS，以太网系统能够对网络上传输的视频流等对实时性要求较高的数据提供优先服务，从而保证较低的时延。

3.32

紧急广播 emergency broadcast

应急指挥系统为应对突发事件而向其服务区发布的广播。

注：包括警报信号、指导公众疏散的信息和有关部门进行现场指挥的命令等。

3.33

寻呼 paging

寻人、寻物的广播；或根据现场需要临时向指定的服务区发布的广播。

3.34

强插 override

强行用某些广播内容覆盖正在广播的其它信号；或强行唤醒处于休眠状态的公共广播系统，发布紧急广播。

4 缩略语

AAC：高级音频编码技术（Advanced Audio Coding）

AVS：数字音视频编码标准（Audio and Video coding Standard）
AM：振幅调制（Amplitude Modulation）
DST：目的（Destination）
DVI：数字视频接口（DigitalVisual Interface）
FTP：文件传输协议（File Transfer Protocol）
FM：调频调制（Fequency Modulation）
FSK：频移键控（Frequency-shift Keying）
HDMI：High Definition Multimedia Interface
IPTD：IP包传输迟延变化（IP Packet Transfer Delay），
IPDV：IP包迟延变化（IP Packet Delay Variation）
IPLR：IP包丢失率（IP Packet Loss Ratio）
IPER：IP错误率（IP Packet Error Ratio）
INFO：信息（Information）
IP：互联网协议（Internet Protocol）
OSD：屏幕选单显示（On Screen Display）
PPS：图像参数集（Picture Parameter Set）
PS：节目流（Program Stream）
QoS：服务质量（Quality of Service）
RAID：磁盘阵列（Redundant Arrays of Independent Disks）
RTP 实时传输协议(Real-time Protocol)
RTCP：实时传输控制协议（Real-time Transport Control Protocol）
SATA：串行高级技术附件（Serial Advanced Technology Attachment）
SDP：会话描述协议（Session Description Protocol）
SIP：会话初始协议（Session Initiation Protocol）
SPS：序列参数集（Sequence Parameter Sets）
SRC：源（source）
SPR：伪IP包率（Spurious IP Packet Ratio）
SVAC：安全防范监控数字视音频编解码技术标准（Surveillance Video and Audio Coding）
TCP：传输控制协议（Transmission Control Protocol）
TS：传输流（Transport Stream）
TCP/IP：传输控制协议/互联网互联协议（Transmission Control Protocol/Internet Protocol）
UDP：用户数据报协议（User Datagram Protocol）
UPS：不间断电源（Uninterruptible Power Supply）
URI：全局资源标识符（Universal Resource Identifier）
VGA：一种视频传输标准（Video Graphics Array）
VLC：视频(Virtuna Light Communication)

5 概述

电子考场系统包括视频巡考系统、无线电作弊防控系统、身份识别系统和指挥系统：

a) 视频巡考系统：对各考场及相关区域的视频图像进行本地监控，并上传至市考试院、省考试院和国家考试中心；

b) 无线电作弊防控系统：采用侦测引导阻断、点频阻断、扫频阻断等多种技术对手机、无线局域网、蓝牙、对讲机和其它作弊器材频段实施有效干扰，以达到考生无法接收外来无线电作弊内容目的。

c) 身份识别系统：由前端考生身份采集验证、硬件和考生身份识别管理系统软件两大部分组成，考生经过身份信息核对和确认，管理软件对刷卡考生进行统计与管理，并逐级上报上级部门；

d) 指挥系统：由指挥中心、考务室和试卷保密室组成。指挥中心分五个级别，每级均包括中心管理单元、流媒体单元、媒体存储单元、解码单元、显示单元、管理客户端和网关单元。

中学校（机构）的命名规则见附录A，电子考场设备兼容性检测参见附录B，作弊防控系统功能与性能测试参见附录C，身份识别系统测试参见附录D。

6 视频巡考系统

6.1 系统结构

6.1.1 概述

视频巡考系统分为学校、区县、地市、省、国家考试院五级部署。系统分级部署结构图见图1。

学校是视频巡考系统中前端。由摄像机、拾音器、信号处理.器等设备构成并通过IP网络接入校级指挥中心，它覆盖了考点内小型考场、大型考场、考务室及试卷保密室、走廊及出入口。

国家考试院、省、地市、区县和学校五级视频巡考系统通过IP网络进行联结。

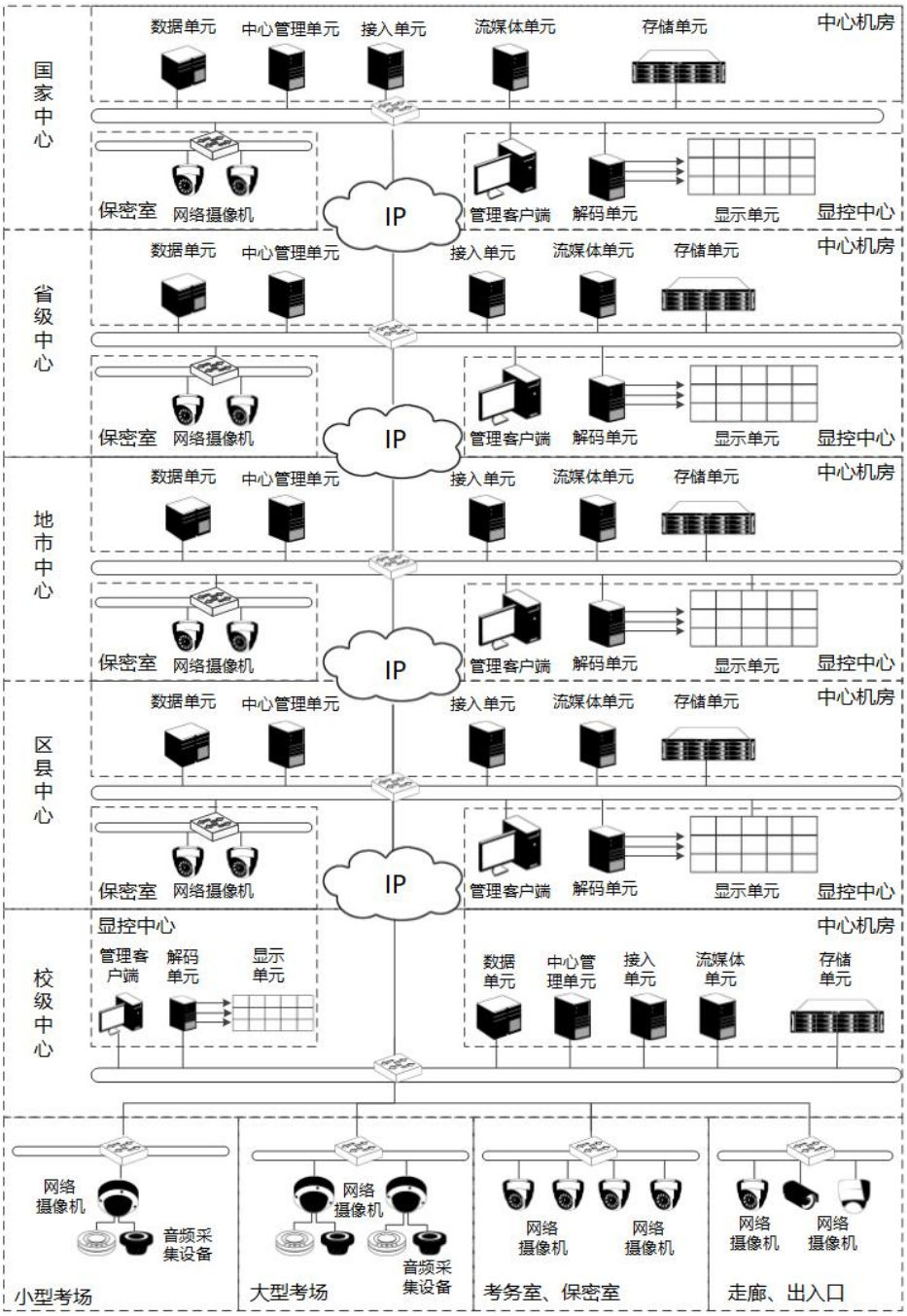


图1五级部署结构图

6.1.2 监控域内联网结构

视频巡查系统包括国家考试院、省、地市、区县、学校五级，其中国家考试院、省、地市、区县视频巡考系统组成基本相同，其主要包括指挥中心、中心管理单元，流媒体单元，媒体存储单元，解码单元，显示单元，管理客户端和网关单元。统称监控域，其内联网结构见图2。

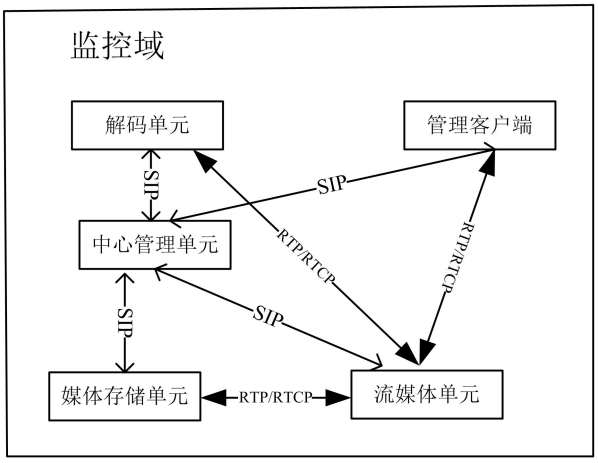


图2　监控域内联网结构

比于国家考试院、省、地市、区县四级视频巡考系统，校级巡考系统是最基层系统，需向上级联巡考系统，向下接入前端设备。校级巡考系统包括中心管理单元、流媒体单元、媒体存储单元、解码单元、显示单元、管理客户端和网关单元以及监控前端。校级监控域内联网结构见图3。

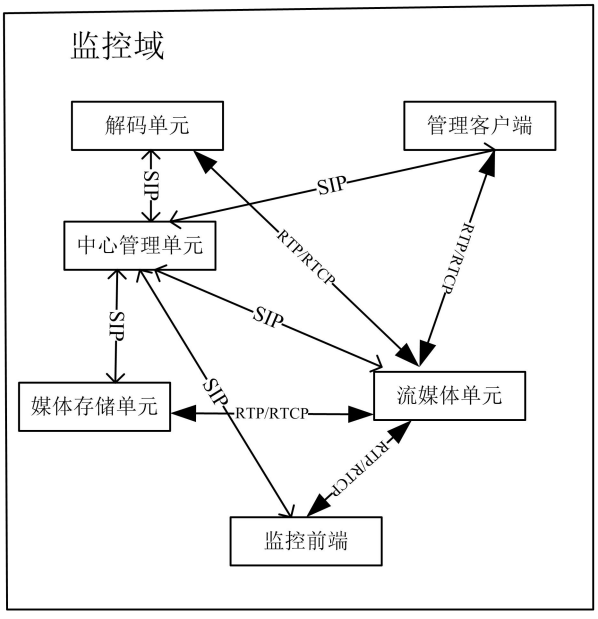


图 3　校级监控域内联网结构

监控域内各功能单元(设备)通过信令通道和流媒体通道进行互联。信令通道传输使用SIP协议的控制信令，流媒体通道使用RTP/RTCP协议传输视音频媒体流。

中心管理单元也是中心信令控制服务器，负责向各功能单元(设备)提供注册、路由选择等功能，是负责核心SIP信令应用处理的SIP服务器。

6.1.3 监控域间联网结构级联

国家、省、地市、区县、校级五级指挥中心的监控域构成了由上自下的级联关系。五级指挥中心的监控域级联关系见图4。

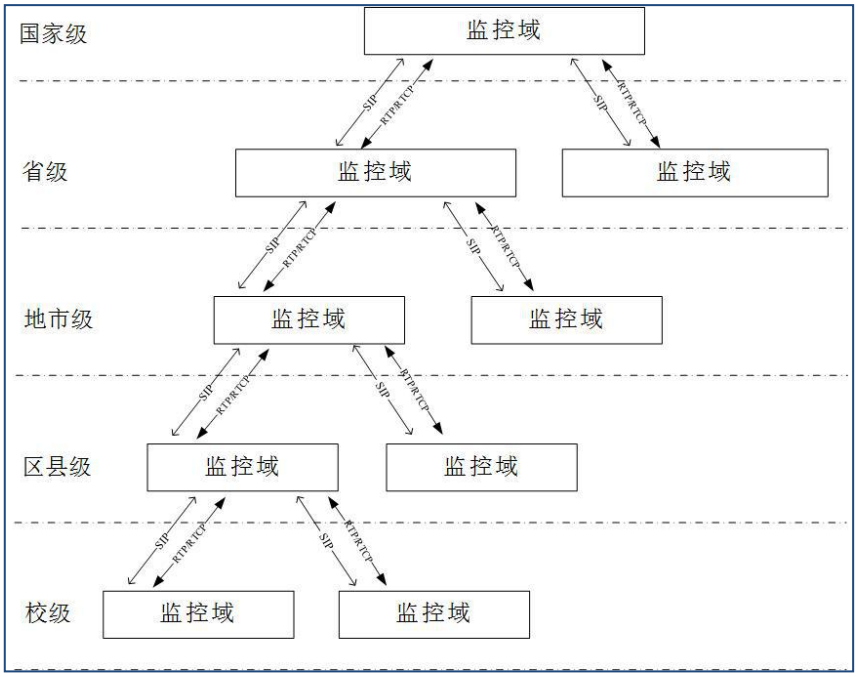
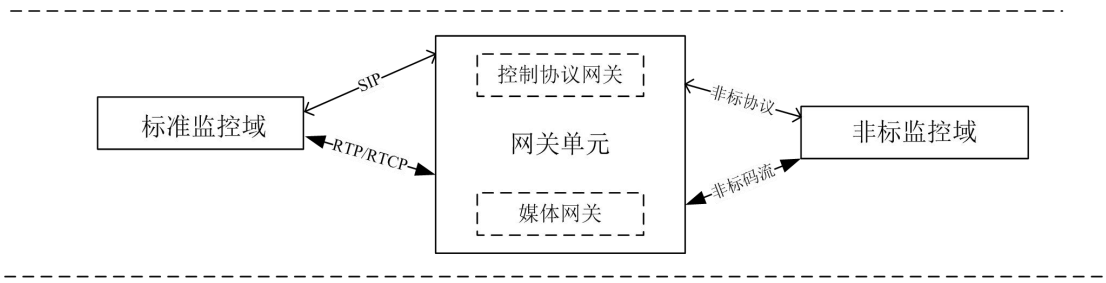


图 4 五级指挥中心的监控域级联关系

在上下级指挥中心的监控域互联结构中，监控域之间通过两个通道：信令通道和流媒体通道进行互联。其中信令通道用于传输遵循SIP协议的控制信令；流媒体通道使用RTP/RTCP协议传输视音频媒体流。

6.1.4 开放接口协议

实现标准电子考场系统与非标准电子考场系统之间的互联。使用网关单元进行互联，其互联结构见图5。



注：指挥中心的网关单元承担了控制协议网关和媒体网关的逻辑功能。

图 5 非标系统兼容性互联示意图

网关单元的控制协议和媒体网关功能如下：

a）代理非标准监控域设备在标准监控域的中心管理单元上进行注册；

b）将非标准监控域的网络传输协议与本标准中规定的网络传输协议进行双向协议转换；

c）将非标准监控域的设备控制协议与本标准中规定的控制协议进行双向协议转换；

d）将非标准监控域的设备地址与本标准中规定的设备地址进行双向地址转换；

e）将非标准监控域的媒体传输协议和数据封装格式与本标准规定的媒体传输协议和数据封装格式进行双向协议转换；

f）将非标准监控域的媒体数据压缩编码与本标准规定的媒体数据压缩编码进行双向转码。

6.1.5 通信协议结构

国家教育考试电子考场系统中进行视频，音频，数据等信息传输、交换、控制时，通信协议的结构见图6，其中信令通道用于传输遵循SIP协议的控制信令；流媒体通道使用RTP/RTCP协议传输视音频媒体流。

上述相关信令协议的应用均以传输层的TCP或UDP为传输基础。其关系如下图：

<table>
<tr><td>信令通道</td><td>流媒体通道</td></tr>
<tr><td>SIP</td><td>RTP/RTCP</td></tr>
<tr><td>TCP/UDP</td><td>TCP/UDP</td></tr>
<tr><td colspan="2">IP</td></tr>
</table>

图 6 通信协议结构

6.2 系统功能要求

6.2.1 音视频资源采集

视频巡考系统的音视频资源采集功能要求如下：

a）系统应支持前端音视频的采集，对目标进行实时、有效、清晰的监视，接入到本级指挥中心；

b）采集场所应包括考场、指挥中心、试卷保密室及指定相关区域；

c）前端摄像机应使用定焦摄像机；

d）考场监控区域应能保证监视无死角、无盲区；

e）音频采集设备应能保证教室及考场范围内的声音采集完整清晰。

6.2.2 实时巡查

视频巡考系统的实时巡查功能要求如下：

a）应能按照指定设备、指定通道进行音视频流的实时点播，支持点播音视频流的图像抓拍功能；

b）应根据逻辑考场号、物理考场号实时点播音视频流；

c）应能支持多组轮切并按预先设置同时进行实况图像轮流切换显示；

d）应支持对预览的视频通道进行多码流切换操作。

6.2.3 音视频存储

视频巡考系统的音视频存储功能要求如下：

e） 存储设备宜采用支持流式存储的存储设备；

f） 考场音视频存储设备最低应能保证3×24h录像存储空间。保密室存储设备最低应能保证10×24h录像存储空间。同时应具备录像锁定功能，锁定的录像不能被覆盖；

g) 宜支持省市一级的巡查系统的存储录制；
h) 音视频存储应保持信息原始完整性，不能丢失，不能篡改。

6.2.4 录像检索及回放

视频巡考系统的录像检索及回放功能要求如下：

a) 系统可按照指定设备、考场、时间、报警信息等要素检索历史图像文件并回放。支持按考场、时间、类型进行录像检索并回放及下载；应支持倍速播放、倒放、单帧步进、暂停、停止等录像回放控制模式；
b) 支持录像标签，并可以对标签的录像进行查询、回放等相关操作；
c) 支持回放录像的同时对指定的录像文件本地下载；
d) 下载录像文件的文件名应符合固定的格式标准。

6.2.5 用户管理

视频巡考系统的用户管理功能要求如下：

a) 应对用户基本信息、属性信息以及用户 ID 与用户证书的对应关系作管理；
b) 应对所有用户进行身份认证；
c) 应支持基于数字证书的用户认证；
d) 应实现统一的用户管理和授权，在身份鉴别的基础上，教育考试电子考场系统宜采用基于属性或基于角色的访问控制模型对用户进行访问控制；
e) 应按照五级结构设置不同的操作角色、应对用户的功能操作和数据操作分开管理，各级的功能和操作都能定制到具体功能；
f) 对用户和角色应具有域内实时冻结、实时解冻、有效期、IP 地址和 MAC 地址绑定的机制；
g) 对系统内用户进行添加、删除和权限分配操作，可详细登记用户信息：用户名、密码、用户级别、联系方式以及所属机构等。

6.2.6 设备管理

视频巡考系统的设备管理功能要求如下：

a) 支持批量修改域内 OSD 选单和全网设备时间同步。
b) 应提供设备的在线状态、工作状态、以及设备型号、使用期的实时显示，应提供设备整体的运行状态、网络状况等的统计分析视图。

6.2.7 日志管理

视频巡考系统的日志管理功能要求如下：

a) 各类设备及指挥中心应详细记录操作日志、参数设置日志、录像操作日志、网络访问日志、设备间通信日志、指挥中心与指挥中心间的级联操作日志、报警日志等日志信息。并能够在授权访问的情况下供上级系统查询访问；
b) 视频联网平台的日志应能记录系统内设备启动、异常、故障、恢复、关闭等状态信息及发生时间；
c) 各类日志保存天数应大于 30 天，不提供日志清除功能，超出天数及条数按覆盖方式处理；
d) 应具有日志信息查询和统计等功能。

6.2.8 报警联动

视频巡考系统的报警联动功能要求如下：

a) 提供多种报警业务：包括视频入侵检测报警、传感器入侵报警、视频丢失报警和硬盘空间提示报警。宜支持与其它业务系统进行报警联动接口。可在地图上联动显示或在客户端提示报警信息；
b) 播放联动视频，在地图上定位报警位置；
c) 应对保密室应依据报警信息实现自动录像、锁定、抓图等一系列的操作；
d) 应对考场、公共场合的视频应支持视频模糊、视频丢失等常见问题的报警联动。

6.2.9 应用接口

按GB/T 28181-2016相关规定，支持第三方使用本标准应用接口对系统平台进行访问。

6.3 音视频编解码要求

6.3.1 视频编码要求

6.3.1.1 H.264

H.264的视频编码作为必选格式，系统码流要求符合ITU－T VCEG AVC/H.264视频编码标准。系统码流具体要求为复合流方式采用PS/TS流的格式，系统输出码流率应满足表1分辨率与对应码流（除非特别说明，本标准中涉及的分辨率与对应码流率关系的帧率均为25帧/秒） 。

表 1 H.264 视频编码分辨率与对应码流率

分辨率	对应码流率 Mbps
3840×2160	10～12
1920×1080	4～6
1280×720	2～4
704×576	0.5～1

6.3.1.2 H.265

如果视频编码采用H.265，系统码流要求符合ITU－T VCEG HEVC/H.265高效视频编码标准。复合流方式采用PS/TS流的格式时，系统输出码流率应满足表2分辨率与对应码流。

表 2 H.265 视频编码分辨率与对应码流率

分辨率	对应码流率 Mbps
3840×2160	5～8
1920×1080	2～3
1280×720	1～2
704×576	0.5～1

6.3.1.3 AVS

AVS作为可选的的视频编码，系统码流一般要求应符合GB/T 20090.1-2012的规定，系统码流为复合流方式采用PS/TS流的格式时，系统输出码流率应满足表3分辨率与对应码流。

表 3 AVS 视频编码分辨率与对应码流率

分辨率	对应码流率 Mbps
1920×1080	4～6
1280×720	2～4
704×576	0.5～1

6.3.1.4 SVAC

SVAC作为可选的视频编码，系统码流要求应符合GB/T25724-2017的规定，具体要求为复合流方式采用PS/TS流的格式，视频流不包括B帧，系统输出码流率应满足表4分辨率与对应码流。

表 4 SVAC 视频编码分辨率与对应码流率

分辨率	对应码流率 Mbps
1920×1080	4～6
1280×720	2～4
704×576	0.5～1

6.3.2 视频解码要求

视频解码应满足表5格式、档次及级别要求。

表 5 视频解码要求

视频解码格式	编码档次	编码级别
H.264	Baseline、main-profile、high- profile	不低于Level 3
H.265	Main Profile	不低于Level 5
AVS	基准档次（Jizhunprofile）	不低于Level 2
SVAC	High -Profile	Level 6.2

6.3.3 音频编码要求

音频编码应满足表6格式、采样率及标准要求：

表 6 音频编码要求

音频编码要求	采样率(kHz)	符合要求
G.711	8	ITU-T Rec. G.711-1988 A 律
G.729	8	ITU-T Rec.G.729-1996 编码要求
MPEG Layer 2	8，32，48	ITU-TG.721 标准
AAC	32，48	ISO/IEC 14496-3 标准

6.3.4 音频解码要求

音频解码应满足表7格式、采样率及标准要求。

表 7 音频解码要求

音频解码要求	采样率(kHz)	符合要求
G.711	8	ITU-T Rec. G.711 测试序列
G.729	8	ITU-T Rec. G.729-1996 测试序列
MPEG Layer II	8，32，48	ITU-TG.721 标准
AAC	32，48	ISO/IEC 14496-3 标准

6.4 数据传输要求

6.4.1 网络传输协议要求

教育考试电子考场系统网络层应支持IP协议，传输层应支持TCP和UDP协议。

6.4.2 媒体传输协议要求

视音频流在基于IP的网络上传输时应支持RTP/RTCP协议；视音频流的数据封装格式应符合本标准6.6.2中的要求。

6.4.3 信息传输延迟时间

信息经由IP网络传输时，监控域中功能单元之间信息交互的延迟时间应不大于2s。

6.4.4 网络传输带宽

电子考场系统视频联网平台网络带宽设计应能满足前端设备接入视频联网平台、视频联网平台互联、用户终端接入视频联网平台的带宽要求并留有余量。

网络带宽的估算方法如下：

a) 前端设备接入视频联网平台所需的网络带宽应不小于允许并发接入的视频路数×单路视频码率；
b) 视频联网平台互联所需的网络带宽应不小于并发联接的视频路数×单路视频码率；
c) 用户终端接入视频联网平台所需的网络带宽应不小于并发显示的视频路数×单路视频码率；
d) 预留的网络带宽应根据视频联网平台的应用情况确定，一般应包括其它业务数据传输带宽、业务扩展所需带宽和网络正常运行需要的冗余带宽；
e) 视频码率按照表 1-表 4 对应的编码格式计算。

f） 监控前端接入指挥中心、指挥中心互联的带宽要求，按照 a）、b）估算并留有余量。

6.4.5 网络传输质量

网络传输质量要求如下：

a） 联网系统 IP 网络的传输质量（如传输时延、包丢失率、包误差率、虚假包率等）应符合如下要求：
   1） 网络时延上限值为 400ms；
   2） 时延抖动上限值为 50ms；
   3） 包丢率上限值为 1×10^{-3}；
   4） 包误差率上限值为 1×10^{-4}；

b） 表 8 中规定了以测量点(MP)为边界的端到端的 IP 网络性能指标，在根据实际运营经验修订(增大或减少)这些指标后，运营商应该能够满足这些指标；

c） 定义端到端的性能指标为 IP 包传送参考时间(IPRE)s 所对应的 IP 性能参数。端到端的 IP 网络路径包括一组把 IP 包从 SRC 传送到 DST 的电路域和网络域，但不包括：源主机和宿主机上的底层协议(IP 层、一层和二层)也是 IP 网的一部分。

表 8 IP 网络性能指标

项目			Qos 等级	
网络性能指标的性质		默认值	0 级	1 级(交互式)
IPTD	（IP 包传输迟延）上限值	需要规定	150ms	400ms
IPDV	IP 包迟延抖动上限值	需要规定	50ms	50ms
IPLR	包丢失率的上限值	需要规定	1×10^{-3}	1×10^{-3}
IPER	包误差率的上限值	1×10^{-4}	默认	默认
SPR	虚假包率的上限值	默认	默认	默认

6.4.6 网络通信安全

网络通信安全应符合GB/T25068.5-2010的规定。

6.5 数据交换要求

6.5.1 系统标识的统一命名规则

系统标识的统一命名规则见附录A。

6.5.2 媒体存储封装格式

音视频等媒体数据的存储封装格式应为PS格式或者TS格式，应符合GB/T 17975.1-2010的规定。

6.5.3 SDP 定义

SIP消息体中携带的SDP内容应符合IETF RFC 2327的相关规定，具体SDP要求见GB/T 28181-2016附录F。

6.5.4 媒体数据格式的转换

应支持将非 SIP 监控域的媒体数据转换为符合本标准6.3 中规定的媒体编码格式的数据。

6.5.5 信令字符集

应至少符合GB18030-2005信息技术中文字符编码集强制部分的要求，并应于GB/T 13000-2010相应部分建立映射关系。

6.6 端口定义

6.6.1 概述

SIP路由器及分发服务器的设备端口分为主用端口和备用端口。

6.6.2 主用端口

主用端口定义建议设置为音视频流的传输端口：9901，控制传输端口：9902，TELNET 端口：9923，FTP 端口：9921，备用：9903，音视频流的收发端口范围：55000～56999。

6.6.3 备用端口

备用端口定义建议设置为音视频流的传输端口：12001，控制传输端口：12002，TELNET 端口：12023，FTP 端口：12021，备用：12003。

6.7 设备控制协议

6.7.1 注册与注销

6.7.1.1 注册流程

设备控制协议的注册流程如下：

a) 监控域中各功能单元(设备)应向中心管理单元进行注册。注册时应进行认证，支持数字摘要认证方式和数字证书认证方式；
b) 功能单元(设备)向中心管理单元基本注册流程使用 GB/T 28181-2016 中 9.1.2.1 描述的信令流程：中心管理单元为此流程中的 SIP 服务器，请求注册的功能单元(设备)为此流程中的 SIP 代理；
c) 基本注册流程的信令描述见 GB/T 28181-2016 中 9.1.2.1；
d) 功能单元(设备)向中心管理单元基于数字证书的双向认证注册流程使用 GB/T 28181-2016 9.1.2.2.2 描述的信令流程：中心管理单元为此流程中的 SIP 服务器，请求注册的功能单元(设备)为此流程中的 SIP 代理；
e) 基于数字证书的双向认证注册流程的信令描述见 GB/T 28181-2016 9.1.2.2。

6.7.1.2 注销流程

监控域中各功能单元(设备)向中心管理单元进行注销的流程使用GB/T 28181-2016 9.1.2.3描述的信令流程：中心管理单元为此流程中的SIP服务器，请求注销的功能单元(设备)为此流程中的SIP代理。

6.7.2 设备控制流程

6.7.2.1 概述

监控域中的功能单元(设备)可向另一功能单元(设备) 发送设备控制命令。控制令的类型包括球机/云台控制、远程启动、录像控制、报警布防/撤防和报警复位等。设备控制使用RFC 3428的MESSAGE方法

实现。设备控制和应答命令采用GB/T 28181-2016的MANSCDP协议定义，使用RFC 3428的MESSAGE方法携带。MANSCDP协议定义见GB/T 28181-2016附录A。

6.7.2.2 无应答设备控制流程

无应答设备控制流程要求如下：

a) 无应答设备控制流程中：监控域中发起控制请求的功能单元(设备)发送设备控制命令，使用RFC 3428 的 MESSAGE 方法携带。接受控制请求的功能单元(设备)收到控制命令后，并不返回应答命令给发起控制请求的功能单元(设备)；
b) 无应答设备控制流程使用 GB/T 28181-2016 中 9.3.2.1 定义的信令流程：发起控制请求的功能单元(设备)为此流程中的源设备，接受控制请求的功能单元(设备)为此流程中的目标设备，中心管理单元为此流程中的 SIP 服务器；
c) 无应答设备控制流程的信令描述见 GB/T 28181-2016 中 9.3.3。

6.7.2.3 有应答设备控制流程

有应答设备控制流程要求如下：

a) 有应答设备控制流程中，监控域中发起控制请求的功能单元(设备)发送设备控制命令，使用RFC 3428 的 MESSAGE 方法携带。接受控制请求的功能单元(设备)收到控制命令后，返回 RFC 3428 的 MESSAGE 方法携带的应答命令给发起控制请求的功能单元(设备)；
b) 有应答设备控制流程使用 GB/T 28181-2016 中 9.3.2.2 定义的信令流程：发起控制请求的功能单元(设备)为此流程中的源设备，接受控制请求的功能单元(设备)为此流程中的目标设备，中心管理单元为此流程中的 SIP 服务器；
c) 有应答设备控制流程的信令描述见 GB/T 28181-2016 中 9.3.3。

6.7.3 设备信息管理

6.7.3.1 设备信息查询

设备信息查询功能要求如下：

a) 监控域中的功能单元(设备)可查询其它功能单元(设备)的设备信息、设备目录、设备状态、设备配置，监控前端的预置位等信息；
b) 设备信息查询流程使用 GB/T 28181-2016 中 9.5.2 描述的信令流程：发起查询请求的功能单元(设备)为此流程中的源设备，返回查询响应的功能单元(设备)为此流程中的目标设备，中心管理单元为此流程中的 SIP 服务器；
c) 设备信息查询流程的信令描述见 GB/T 28181-2016 中 9.5.1 和 9.5.3。

6.7.3.2 设备目录订阅与通知

设备目录订阅与通知功能要求如下：

a) 监控域中的功能单元(设备)可向其它功能单元(设备)订阅其设备目录信息，被订阅方当设备目录发生变化时要立即通知订阅方；
b) 设备目录订阅流程使用 GB/T 28181-2016 中 9.11.3.2 描述的信令流程：订阅方为此流程中的目录接收者，被订阅方为此流程中的目录拥有者；
c) 设备目录订阅流程的信令描述见 GB/T 28181-2016 中 9.11.3.1 和 9.11.3.3；
d) 设备目录通知流程使用 GB/T 28181-2016 中 9.11.4.2 描述的信令流程：订阅方为此流程中的目录接收者，被订阅方为此流程中的目录拥有者；
e) 设备目录通知流程的信令描述见 GB/T 28181-2016 中 9.11.4.1 和 9.11.4.3。

6.7.4 实时视音频点播

6.7.4.1 概述

实时视音频点播采用SIP协议中的INVITE方法实现会话连接，采用RTP/RTCP协议实现媒体传输。实时视音频点播的信令流程分为客户端主动发起和第三方呼叫控制两种方式。

6.7.4.2 客户端主动发起方式

客户端主动发起方式要求如下：

a) 客户端主动发起方式适用于监控域中的功能单元(设备)点播监控前端的实时视音频流。在客户端主动发起方式中：点播发起方首先向中心管理单元发起会话请求。中心管理单元收到点播发起方的媒体接收会话请求后，建立流媒体单元与监控前端之间的媒体流连接。当监控前端向流媒体单元发送实时媒体流之后，中心管理单元将点播发起方之前发送的媒体接收会话请求转发给流媒体单元，建立起点播发起方与流媒体单元之间的媒体流连接，完成点播发起方对监控前端产生媒体流的接收。

b) 当点播发起方不再接收媒体流时，向中心管理单元发起断开会话请求，依次断开点播发起方与中心管理单元、中心管理单元与流媒体单元以及流媒体单元与监控前端之间的会话连接。

c) 客户端主动发起方式的流程使用 GB/T 28181-2016 中 9.2.2.1 描述的信令流程：点播发起方为此流程中的媒体流接收者，监控前端为此流程中的媒体流发送者，中心管理单元为此流程中的 SIP 服务器，流媒体单元为此流程中的媒体服务器。

d) 客户端主动发起方式流程的信令描述见 GB/T 28181-2016 中 9.2.3。

6.7.4.3 实时点播的第三方呼叫控制方式

第三方呼叫控制方式适用于中心管理单元控制解码单元接收来自监控前端的实时视音频流。第三方呼叫控制方式要求如下：

a) 中心管理单元首先分别向流媒体单元和监控前端发起会话请求，建立流媒体单元和监控前端之间的媒体流传输，然后向解码单元发起会话请求，获取解码单元的 SDP 参数后又向流媒体单元发起会话请求，将解码单元的参数传递给流媒体单元，建立流媒体单元向解码单元的媒体传输，完成解码单元对监控前端的实时视音频流接收；

b) 当中心管理单元需要终止媒体流传输时，首先向解码单元发起断开会话连接，然后依次断开与流媒体单元、监控前端的会话连接；

c) 第三方呼叫控制方式的流程使用 GB/T 28181-2016 中 9.2.2.2 描述的信令流程：解码单元为此流程中的媒体流接收者，监控前端为此流程中的媒体流发送者，中心管理单元为此流程中的 SIP 服务器，流媒体单元为此流程中的媒体服务器；

d) 第三方呼叫控制方式的信令描述见 GB/T 28181-2016 中 9.2.3。

6.7.5 录像控制

6.7.5.1 录像启停

录像启停功能要求如下：

a) 监控域中的媒体存储单元完成录像功能；

b) 录像启停流程符合 GB/T 28181-2016 中 9.3.2.2 规定，媒体存储单元接收来自监控域中其它功能单元(设备)发起的录像启停操作命令；

c) 录像启停流程的控制命令使用 GB/T 28181-2016 的 MANSCDP 中定义，见 GB/T 28181-2016 附录 A.2.3 的命令定义。

6.7.5.2 录像检索

录像检索功能要求如下：

a) 监控域中的功能单元(设备)可检索媒体存储单元中录像文件的目录信息。录像文件的检索主要用区域、设备、录像时间段、录像地点、录像内容为条件进行查询，媒体存储单元返回视音频文件的检索结果；
b) 录像检索流程使用 GB/T 28181-2016 中 9.7.2 描述的信令流程：发起检索请求的功能单元(设备)为此流程中的目录检索方，媒体存储单元为此流程中的目录拥有方；
c) 录像检索流程的信令描述见 GB/T 28181-2016 中 9.7.1。

6.7.5.3 录像目录订阅和通知

录像目录订阅和通知功能要求如下：

a) 监控域中的功能单元(设备)可向媒体存储单元订阅其录像目录信息，媒体存储单元当录像目录发生变化时要立即通知订阅方；
b) 录像目录订阅流程使用 GB/T 28181-2016 中 9.11.3.2 描述的信令流程：订阅方为此流程中的目录接收者，媒体存储单元为此流程中的目录拥有者；
c) 录像目录订阅流程的信令描述见 GB/T 28181-2016 中 9.11.3.1 和 9.11.3.3；
d) 录像目录通知流程使用 GB/T 28181-2016 中 9.11.4.2 描述的信令流程：订阅方为此流程中的目录接收者，媒体存储单元为此流程中的目录拥有者；
e) 录像目录通知流程的信令描述见 GB/T 28181-2016 中 9.11.4.1 和 9.11.4.3。

6.7.6 录像回放

6.7.6.1 概述

录像回放分为客户端主动发起和第三方呼叫控制两种方式。

6.7.6.2 客户端主动发起方式

客户端主动发起方式要求如下：

a) 客户端主动发起方式适用于监控域中的功能单元(设备)回放媒体存储单元的视音频录像文件；
b) 在客户端主动发起方式中，回放发起方首先向中心管理单元发起会话请求。中心管理单元收到回放发起方的媒体接收会话请求后，建立流媒体单元与媒体存储单元之间的媒体流连接。当媒体存储单元向流媒体单元发送录像文件媒体流之后，中心管理单元将回放发起方之前发送的媒体接收会话请求转发给流媒体单元，建立起回放发起方与流媒体单元之间的媒体流连接，完成回放发起方对媒体存储单元的录像文件媒体流的接收。回放发起方在回放过程中可进行各项回放控制操作；
c) 当录像文件播放完毕时，媒体存储单元经中心管理单元向回放发起方发送文件发送完成消息。回放发起方收到文件发送完成消息后，向中心管理单元发起断开会话请求，依次断开回放发起方与中心管理单元，中心管理单元与流媒体单元，流媒体单元与媒体存储单元之间的会话连接；
d) 客户端主动发起方式的流程使用 GB/T 28181-2016 中 9.8.2.1 描述的信令流程：回放发起方为此流程中的媒体流接收者，媒体存储单元为此流程中的媒体流发送者，中心管理单元为此流程中的 SIP 服务器，流媒体单元为此流程中的媒体服务器；
e) 客户端主动发起方式的信令描述见 GB/T 28181-2016 中 9.8.3。

6.7.6.3 第三方呼叫控制方式

第三方呼叫控制方式要求如下：

a) 第三方呼叫控制方式适用于中心管理单元控制解码单元接收来自媒体存储单元中录像文件的视音频流；
b) 在第三方呼叫控制方式中，中心管理单元首先分别向流媒体单元和媒体存储单元发起会话请求，建立流媒体单元和媒体存储单元之间的媒体流传输，然后向解码单元发起会话请求，获取解码单元的 SDP 参数后又向流媒体单元发起会话请求，将解码单元的参数传递给流媒体单元，建立流媒体单元向解码单元的媒体传输，完成解码单元对媒体存储单元的录像文件媒体流的接收。解码单元在回放过程中可进行各项回放控制操作；
c) 当录像文件播放完毕时，媒体存储单元经中心管理单元向解码单元发送文件发送完成消息。中心管理单元需要终止媒体流传输时，首先向解码单元发起断开会话连接，然后依次断开与流媒体单元、媒体存储单元的会话连接；
d) 第三方呼叫控制方式的流程使用 GB/T 28181-2016 中 9.8.2.2 描述的信令流程：解码单元为此流程中的媒体流接收者，媒体存储单元为此流程中的媒体流发送者，中心管理单元为此流程中的 SIP 服务器，流媒体单元为此流程中的媒体服务器；
e) 第三方呼叫控制方式的信令描述见 GB/T 28181-2016 9.8.3。

6.7.6.4 录像回放控制信令

录像回放控制协议使用GB/T28181-2016中9.8.3.2描述的视音频回放控制协议。控制信令由SIP的INFO消息承载，信令定义参见GB/T28181-2016附录B。

6.7.7 报警管理

6.7.7.1 报警布撤防

报警布撤防要求如下：

a) 监控域中可设置各功能单元(设备)的报警布撤防功能；
b) 报警布防和撤防的信令流程使用 6.7.2.3 中描述的有应答设备控制流程：监控域中的功能单元(设备) 可接受来自其它功能单元(设备)的布撤防命令；
c) 报警布撤防命令见 GB/T 28181-2016 附录 A.2.3 定义，报警布撤防响应命令见 GB/T 28181-2016 附录 A.2.6 定义。

6.7.7.2 报警通知和分发

报警通知和分发要求如下：

a) 监控域中的功能单元(设备)产生报警事件时，可通过中心管理单元通知和分发到其它功能单元(设备)；
b) 报警通知和分发流程使用 GB/T 28181-2016 中 9.4.2 描述的信令流程：发送告警事件的功能单元(设备)为此流程中的源设备，接收告警事件的功能单元(设备)为此流程中的目标设备，中心管理单元为此流程中的 SIP 服务器；
c) 报警通知和分发流程的信令描述见 GB/T 28181-2016 中 9.4.3。

6.7.7.3 报警订阅与通知

报警订阅与通知要求如下：

a) 监控域中的功能单元(设备)可向其它功能单元(设备)订阅其产生的报警事件；

b) 报警事件订阅流程使用 GB/T 28181-2016 中 9.11.1.2 描述的信令流程：订阅报警事件的功能单元(设备)为此流程中的事件观察者，产生报警事件的功能单元(设备) 为此流程中的事件源；
c) 报警事件订阅流程的信令描述见 GB/T 28181-2016 中 9.11.1.1 和 9.11.1.3；
d) 报警事件通知流程使用 GB/T 28181-2016 中 9.11.2.2 描述的信令流程：接收报警事件的功能单元(设备) 为此流程中的事件观察者，通知报警事件的功能单元(设备) 为此流程中的事件源；
e) 报警事件通知流程的信令描述见 GB/T 28181-2016 中 9.11.2.1 和 9.11.2.3。

6.8 电子考场设备兼容性

各级教育考试机构建立的电子考场系统应能与“国家教育考试电子考场系统”互通直联。电子考场设备的兼容性检测参见附录B。

7 无线电作弊防控系统

7.1 概述

无线电作弊防控系统至少由无线电信号侦测子系统、无线电信号阻断子系统、无线电作弊防控管理子系统三部分组成：

a) 无线电信号侦测子系统部署在所辖考点区域内，时刻处于在线工作状态，所获得的异常信号特征信息能及时、准确的传递到无线电信号阻断子系统和作弊防控管理子系统；
b) 无线电信号阻断子系统由多台阻断设备组成，阻断设备部署在考点的各个考场内；
c) 作弊防控管理子系统通过管理平台对所辖无线电作弊防控系统内的侦测设备、阻断设备进行管理控制，实时查看无线电信号侦测子系统、无线电信号阻断子系统运行状态。

无线电信号阻断子系统、无线电信号侦测子系统、无线电信号作弊防控管理子系统采用有线网络连接。

无线电作弊防控系统与视频巡考系统、身份识别系统、指挥系统等之间互联互通，并接受上一级指挥控制中心的统一监管和指挥。

无线电作弊防控系统组成见图7，无线电作弊防控系统五级联网管理图见图8。

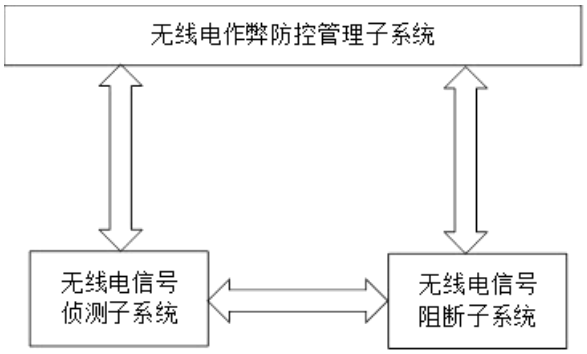


图 7 无线电作弊防控系统五级联网管理图

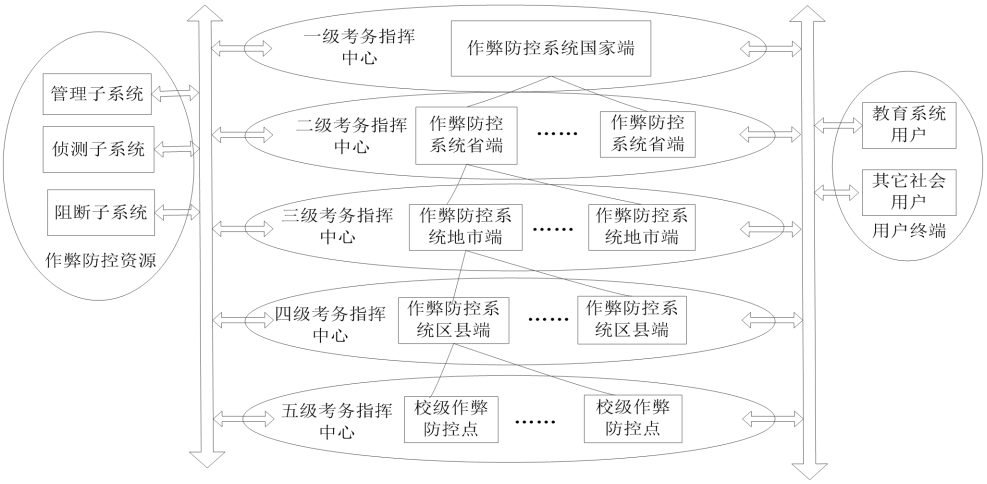


图 8 无线电作弊防控系统五级联网管理图

7.2 系统功能要求

7.2.1 侦测子系统

侦测子系统功能要求如下：

a) 应支持对考点区域内无线电信号进行快速扫频，及时发现和捕获可疑的异常信号；
b) 应支持对考点区域内常在背景信号进行扫描和存储，通过长时间多次采集和综合，确定考点常在无线电信号范围内，作为系统工作的背景频谱；
c) 应支持黑白名单信号处理；
d) 应支持对异常信号进行综合分析，提取异常信号特征信息；
e) 确定异常信号后应能自动实时向阻断子系统发送引导阻断命令，并对异常信号进行阻断；
f) 应支持在扫频发现异常信号并引导阻断设备发射干扰信号的同时，对异常信号进行采集、还原、取证并及时上传到考点管理子系统；
g) 侦测子系统的侦测频率范围应具有扩展性。

7.2.2 阻断子系统

阻断子系统功能要求如下：

a) 针对无线电通讯中使用的公众通讯频段，进行实时阻断；
b) 针对异常信号，系统采用“侦测引导阻断”方法，在异常信号出现期间发射干扰信号，异常信号消失后停止发射干扰信号，能同时对多个异常信号进行并发阻断；
c) 阻断设备具备扩展槽、扩展接口；
d) 阻断设备支持远程管理控制；
e) 阻断设备软件可通过网络进行集中批量升级。

7.2.3 作弊防控管理子系统

作弊防控管理子系统功能要求如下：

a) 应支持对所辖系统内侦测设备、阻断设备进行集中管理；
b) 应支持对所辖系统内全部或部分阻断设备工作状态进行实时控制；
c) 应支持查看所辖系统内侦测设备、阻断设备运行状态，查看关键信息；

d) 应能检查系统内各设备的基本状态，对侦测系统和阻断系统进行自检，并显示设备自检结果；
e) 应支持查询异常信号信息（时间、频率、信号类型等），调听还原的异常语音，调看还原的数传文本；
f) 应支持对考点异常信号情况进行汇总、统计和分析，输出相关结果；
g) 应支持对所辖系统内阻断设备软件进行集中批量升级；
h) 应支持用户权限管理。
i) 应支持记录系统的关键操作（模块开关控制、管理员重大操作等）日志；
j) 对异常数据存储和传输时应进行加密并建立相关密钥管理；
k) 应支持与上级管理系统进行连接,汇报所辖系统运行状态及作弊信号信息,接收上级指令包括：
   1) 同步上级考试计划，根据计划打开或关闭侦测设备、阻断设备；
   2) 同步上级黑白名单，进行相应处理；
   3) 向上级上传考点设备工作状态；
   4) 向上级上传考点作弊信号情况。

7.2.4 系统功能测试

系统功能测试参见附录C。

7.3 系统性能要求

7.3.1 侦测子系统

侦测子系统性能要求如下：
a) 侦测引导频率范围：50 MHz～3000 MHz；
b) 侦测响应时间：≤500 ms；
c) 侦测频率精度:≤25 KHz；
d) 侦测灵敏度:≤-80 dBm；
e) 侦测动态范围:≥70 dB；
f) 能够还原的信号类型：FM、AM、FSK。

7.3.2 阻断子系统

阻断子系统性能要求如下：
a) 侦测引导阻断频率范围：50 MHz～3000 MHz，公共通讯频道所定义的下行频率除外；
b) 侦测引导阻断响应时间：≤600ms；
c) 阻断信号带宽：0.7 倍作弊信号带宽≤阻断信号带宽≤5 倍作弊信号带宽；
d) 阻断效果：在 6 m×9 m 标准化考场空间内，信号强度≤-65 dBm 时，可有效屏蔽 95%以上区域；
e) 异常信号并发阻断≥20 个；
f) 电磁辐射控制限制应符合 GB 8702-2014 规定；

7.3.3 系统性能测试

系统性能测试参见附录 C。

7.4 传输与管理

7.4.1 数据编码要求

7.4.1.1 音频类数据

音频信号数据文件采用AAC方式进行编码，并封装为PS流用于网络传输。

7.4.1.2 字符类数据

采用图片叠加选单字符的方式来展示解调后的字符信息，选取异常信号频谱作为图片背景，并在其上叠加相应频谱信息及解调后的字符信息，图片应存储为BMP格式。如解调后的文字信息较多，则保存多张图片。

7.4.2 SIP URI 编码要求

一个典型的SIP URI如“学校.区县.市教育.省教育.国家教育@市.省.cn”，其中“市.省.cn”表示域（SIP路由）的物理位置，可以是域名，也可以是IP地址。而“学校.区县.市教育.省教育.国家教育”表示该URI的逻辑位置，用于SIP路由的解析。可以根据该URI构成一个树型结构，见图9。

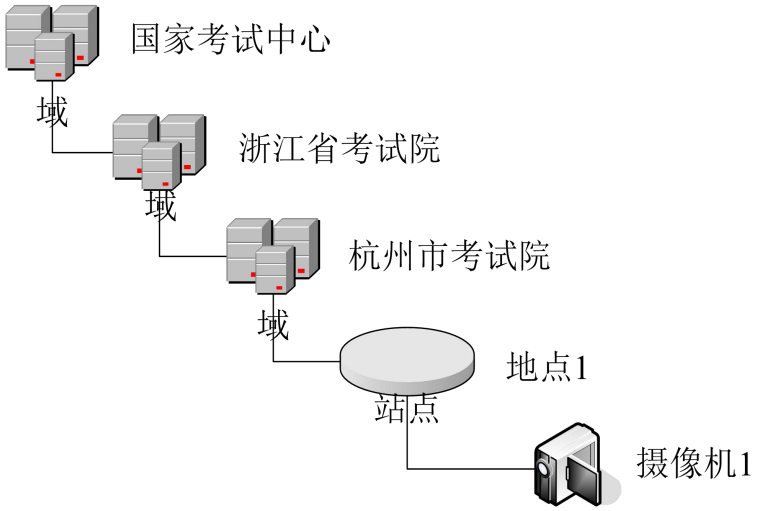


图 9 URI 构成树形结构

7.4.3 SIP URI 分类

7.4.3.1 点（Unit）

独立的功能单元,前端某一个侦测阻断或阻断设备是一个点，后端的用户也叫做一个点，每个点对应一个SIP URI。

7.4.3 .2 域（Domain）

有SIP路由支持的区域，包含所有该路由管理的设备和用户。

7.4.3 .3 组（Group）

无SIP路由支持的区域，是域的一个子集，可以包含一个小区域的所有设备，也可以包含一个部门的所有用户。

7.4.4 设备认证

设备只接收或转发经过认证的用户或设备发来的消息,使用SIP协议的认证机制,保证设备接收到的消息肯定是来自经过认证的用户或设备。

上下级作弊防控管理子系统之间、作弊防控侦测子系统与作弊防控管理子系统之间、作弊防控阻断子系统与作弊防控管理子系统之间，可使用SIP协议的认证机制。设备认证采用SIP REGISTER方法实现。

7.4.5 设备列表获取

设备列表的获取主要用于上级作弊防控中心获取下级作弊防控中心的作弊防控资源，资源包括组、作弊信号侦测点、作弊信号阻断点，采用逐级请求的方式获取。设备列表获取用SIP MESSAGE方法实现，消息体内容见表9。

表 9 作弊防控资源设备列表消息体内容

类型	类型说明
DCSS	作弊信号侦测设备 Device for Cheating Signal Surveillance
DBCS	作弊信号阻断设备 Device for Blocking Cheating Signal
PS	SIP 代理服务器(Sip Proxy Server、Sip Router)
MS	媒体代理服务器(Media Proxy Server)
DO	域(Domain)
DG	设备组(Group)
UG	用户组
UU	用户

设备列表的获取主要用于上级作弊防控中心获取下级作弊防控中心的作弊防控资源，资源包括组、作弊信号侦测点、作弊信号阻断点，采用逐级请求的方式获取。设备列表获取用SIP MESSAGE方法实现，见表10。

表 10 状态信息列表

状态	状态说明
ON	在线
OFF	离线
BUSY	阻断通道忙

7.4.6 阻断频点列表获取

阻断频点列表的获取主要用于上级作弊防控中心获取校级作弊防控点当前正在阻断的频点,频点包含默认阻断频点、可疑作弊频点、实际作弊频点,采用逐级请求的方式获取。设备列表获取用SIP MESSAGE方法实现，见表11。

表 11 阻断频点设备列表获取

类型	类型说明
DB	默认阻断的固定频段（Default Band）
CP	确认属实的作弊频点（Cheating Point）

7.4.7 控制指令下发

指令下发控制使用SIP MESSAGE信令实现，Content-Type： Application/FKECP。

注：FKECP：FK表示防控，ECP：Equipment Control Protocol设备控制协议。

7.4.8 作弊信号检索

作弊信号检索使用SIP MESSAGE信令来实现。

7.4.9 作弊信号回放

7.4.9.1 语音类信号回放

作弊信号回放使用SIP MESSAGE信令来实现。

7.4.9.2 字符类信号回放

作弊信号回放使用SIP MESSAGE信令来实现。

身份识别系统

8 身份识别系统

8.1 概述

8.1.1 系统组成架构

电子考场身份识别系统由前端考生身份采集验证终端硬件和考生身份识别管理系统软件两大部分组成。系统组成架构见图10。

考生身份识别管理系统软件分为校级管理平台和区域级管理平台：

a) 校级管理平台应具备以下功能：
   1) 管理前端考生身份采集验证终端硬件；
   2) 考生身份认证数据下发、收集、统计汇总、数据可视化；
   3) 支持向上级联。
b) 区域级管理平台应具备以下功能：
   1) 与考生报名系统数据接口功能；
   2) 考生身份认证数据下发、收集、统计汇总、数据可视化；
   3) 与区域级国家教育考试电子考场系统的考场巡查、调度指挥的接口功能；
   4) 支持系统级联。

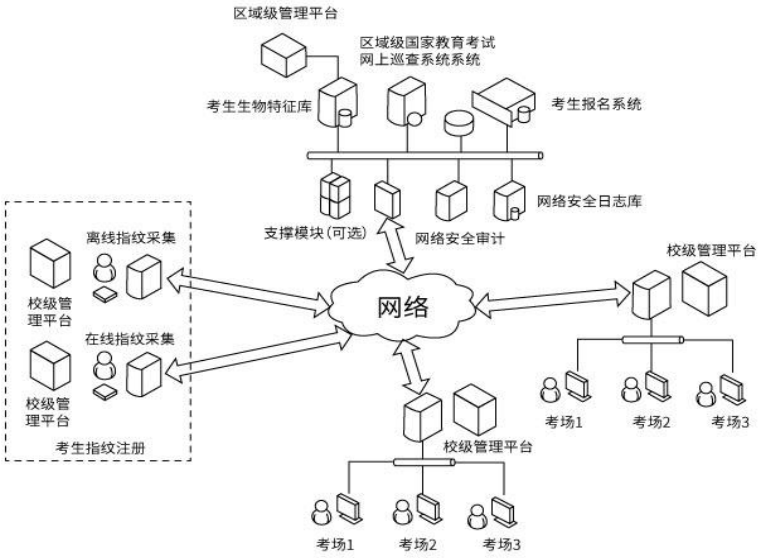


图 10 身份识别系统组成架构

8.1.2 考生身份信息采集验证终端

考生身份采集验证终端应包括身份证核对、生物特征识别、头像比对三个基本功能。实现考生生物特征、身份证和相片的“人证同一性”信息认定：

a) 身份核对子系统主要用于核实身份证上的有关信息；

b) 生物特征识别子系统通过获取考生的生物特征信息进行身份鉴定；

c) 头像比对子系统则通过自动方式查验考生的相片。

身份采集验证终端分为手持式和立式两种类型。见表12

表 12 身份采集验证终端分类

分类		基本功能要求
手持式	手持式识别终端A	能够读取显示考生身份证信息，并能够进行生物特征采集、验证、显示、查询等功能的身份认证终端设备。
	手持式识别终端B	能够读取显示考生身份证ID号，并能够进行生物特征采集、验证、显示、查询等功能的身份认证终端设备。
立式	立式识别终端	能够读取显示考生身份证信息，并能够进行生物特征采集、验证、显示、查询等功能的身份识别终端设备。

8.1.3 考生身份识别管理系统软件

考生身份识别管理系统软件主要由服务端和客户端两个部分组成：

a) 服务端：部署于后端，对身份识别系统提供基础的数据、管理、分析等服务，包括对生物特征进行比对、稽查、筛选等处理的技术或算法；

b) 客户端：部署于前端，面向用户，用于显示和呈现身份识别管理系统的界面、显示信息和识别结果。客户端呈现的内容包括但不限于：考试姓名、考生号、考场号、公民身份号码、照片、考试科目、识别比对结果等。

8.1.4 管理计算机

通过网络与验证终端连接，进行终端系统和后端系统的管理，监控验证过程。

8.1.5 网络设备

把各考场的验证终端连接起来，并且连到数据中心。

8.2 考生身份信息采集验证终端技术要求

8.2.1 概述

考生身份采集验证终端应能支持考生指纹识别和人脸识别技术;应支持考生生物特征在线和离线两种采集验证方式。

生物识别技术的有关技术要求如表13。

表 13 生物识别技术的有关技术要求

分类	要求	
指纹识别	传感器	半导体电容式传感器，支持活体识别， 360 度自动旋转符合 GA/T1011-2012
	指纹算法	符合 GA1012-2012
	图像分辨率	500dpi
	采集面积	18.00 mm × 12.8 mm
	使用寿命	≥100 万次
	指纹模版	＜512 字节 可调节
	指纹录入时间	＜1.1 s
	指纹对比时间	＜0.3 s
人脸识别	a） 支持人脸瞳距 60 像素以上人脸识别； b） 支持人脸在左右摆动 30°，上下俯仰 15° 内人脸识别； c） 支持戴眼镜，留胡子，刘海等轻微遮挡识别； d） 支持报名时照片、身份证照片与实时采集的人脸进行一一比对，人脸验证准确率≥97%。	

8.2.2 手持式验证终端技术要求

手持式验证终端技术要求如下：

a) 验证终端采用的指纹传感器，需同时具备采集和验证考生指纹的能力；

b) 验证终端采用指纹作为主要的认证方式，同时需提供人脸和身份证作为扩展的认证；

c） 验证终端指纹的验证时间≤2 秒/次；
d） 电池容量需满足正常工作≥4 h。

8.2.3 立式验证终端技术要求

立式验证终端技术要求如下：
a） 应支持指纹、人脸生物特征识别认证；
b） 验证终端的验证时间≤2 秒/次；
c） 身份证阅读设备应符合 GA/T450-2013 要求。

8.3 考生身份信息识别管理系统功能要求

8.3.1 考生身份信息识别与验证管理系统

考生身份信息识别管理系统功能应包括信息输入（考生生物特征现场采集，指纹、人脸、证件信息）；传输与存储（批量上传采集与验证结果到数据中心并自动存储备份）；信息比对（考试现场采集的考生生物特征及证件信息自动的与数据中心存储的原始数据比对）；输出（比对结果的输出与自动生成报表）等功能。

考生身份识别管理系统功能要求如下：
a） 应能与报名系统进行数据对接；
b） 应能控制采集终端进行考生生物特征及证件信息采集和存储；
c） 应能自动分考点按编排数据对考生考试信息进行打包下载。
d） 应具有对采集、验证数据进行查询、统计等基本功能；
e） 应支持存疑考生管理、缺考管理、人工审核、违纪管理、异常管理；
f） 应能实际反应出考生的验证轨迹，可对异常考生进行溯源追踪；
g） 应支持综合验证、相互校验。通过身份证件真伪识别、指纹比对、人脸图像识别等多种组合验证，以及各场次进场照片、指纹智能比对等。设备上应显示考生的姓名、性别、公民身份号码、报名时采集的相片、考生号、考点名称、考场和座位号。

8.3.2 考生信息采集

应具有采集考生指纹、人脸图像、身份证件等相关信息的能力，并自动生成身份识别信息数据库。

8.4 系统安全要求

考生身份识别系统安全应符合如下要求：
a） 应能对特定网段、服务进行物理和逻辑隔离，并建立访问控制机制；
b） 应有对网络和运行系统安全漏洞的周期检查机制；
c） 关键数据传送时，应有相应的措施加密通信；
d） 应具有良好的备份和恢复机制；
e） 内部网络业务处理计算机上需要安装企业级防病毒软件；
f） 应能够用模块（对应系统菜单）、功能（对应模块的子功能）两级定义系统功能权限，用角色定义一组系统模块、功能集合，通过向用户分配角色来管理用户权限。同时，通过对象权限定义用户能操作的数据，如全省、地市、区县、学校的数据；
g） 应能以日志的形式记录关键业务的操作过程。日志记录在数据库中，便于审计时查阅。

8.5 身份识别系统性能测试

身份识别系统性能测试参见附录D。

9 指挥系统

9.1 概述

指挥系统依据行政隶属关系及工作相关性，在国家级（部）教育考试院设置一级指挥系统，省、自治区、直辖市等考试中心设置二级指挥系统，市级考试中心或考务部门设置三级指挥系统，区（县）级招考办或考务部门设置四级指挥系统，各学校考点设置五级指挥系统。部、省、市、区（县）、校五级指挥系统形成上下级级联关系。

指挥系统包括了指挥中心以及受其监控的考务室和试卷保密室。指挥中心是指挥系统的核心。

9.2 指挥中心功能要求

9.2.1 视频显示及控制功能

指挥中心视频显示及控制系统功能要求如下：

a) 指挥中心应根据不同机构级别及需要建设拼接屏显示系统；
b) 巡查图像显示应以轮巡方式为主，大屏幕以 4 分屏或 9 分屏方式进行画面分割，轮巡时间设置为 5min，有 1 块～2 块屏单独显示选定考场或区域的图像；
c) 指挥中心应能通过信息显示屏同时显示本级及所属下级电子考场系统的图像和视频会议系统等的图像及信息；
d) 信息显示屏应能够将地图、告警、实况辅屏、配置等进行分屏显示；
e) 可支持天气、交通等信息显示。

9.2.2 指挥中心拾音、扩声与广播功能

指挥中心拾音、扩声与广播功能要求如下：

a) 指挥中心应具有独立的拾音系统、扩声系统和公共广播系统，供视频会议系统、广播系统和巡查系统音频采集、播放使用；
b) 扩声系统声学特性指标应参照 JYJS201102《多媒体教学环境工程建设规范》第二册中的 4.3.2.1 要求；
c) 广播覆盖区域应能分区控制，应具备手动选通或关闭任何广播分区功能；
d) 应具有强插功能。对任何选定的广播分区（包括已经关闭了的分区）强行插入寻呼广播或其他紧急广播；
e) 应能实现自动管理。包括定时接通/关闭广播系统的电源，定时播放通知、寻呼以及其他信息节目；
f) 可控制各考场、考务室内的广播设备播放对应音频；
g) 系统可扩展支持级联功能，可通过级联同步上下级配置和相关音频文件以及播放控制。

9.2.3 指挥中心视频会议系统功能

指挥中心视频会议系统功能要求如下：

a) 指挥中心的视频会议系统除应符合 GB50799-2012 中 4.3 性能设计要求，还应支持以双流的形式实现桌面共享，实时共享电子地图、方案等；
b) 视频会议系统在使用期间应能同时显示本地和对端图像，未使用期间可不显示；
c) 在电子考场系统上发现应急情况时，上级可通过视频会议系统向下级推送该巡查视频，并能够保证上下级所看的视频图像相同。

9.2.4 指挥中心调度指挥功能

指挥中心应具备电子考场资源的控制、管理和监视等功能。

9.2.5 指挥中心实时图像的点播功能

指挥中心实时图像的点播功能要求如下：

a) 指挥中心应支持按照指定设备、指定通道进行图像的实时点播；
b) 应支持点播图像的显示、缩放、抓拍和录像；
c) 应支持多用户对同一图像资源的同时点播；
d) 应支持基于地理信息系统的图像点播。

9.2.6 指挥中心管理平台功能

9.2.6.1 概述

指挥中心管理平台应具备管理功能及业务功能。实现中心管理、媒体转发、数据单元、前端接入、音视频解码等功能。

9.2.6.2 中心管理单元

中心管理单元功能要求如下：

a) 应具备平台配置、网管、用户管理、设备管理、日志管理、录像管理、电视墙管理、告警管理、系统远程维护等管理功能；
b) 应具备视频浏览、窗口轮巡、图像窗口可调、PTZ 控制、音频对讲、图片抓拍、录像回放、电子地图、报警设置、报警联动功能；
c) 直连前端接入路数要求应不低于 1000 路；
d) 应支持支持级联功能，能够实现向上接入上级指挥中心平台；
e) 应支持分域管理；
f) 应支持设备分组管理；
g) 应支持用户分组管理；
h) 应采用稳定性较高的操作系统和硬件设备作为中心管理单元设备，充分保证核心单元的安全性，并且核心单元具有备份机制；
i) 应保持高稳定性、高可靠性，能够满足 7×24h 不间断工作。

9.2.6.3 流媒体转发单元

流媒体转发单元功能要求如下：

a) 应支持堆叠或级联扩展其并发能力，单台并发能力不低于 300 路视频；
b) 应支持选择性开启转码服务，实现不同分辨率、不同格式的转换；
c) 多个流媒体单元一起使用时，流媒体单元间应可以实现负载均衡；

9.2.6.4 数据单元

数据单元功能要求如下：

a) 应支持主流数据库技术，支持双机热备机制；
b) 针对数据库应采用数据库代理、数据库中间件技术等多种有效技术进行处理，不直接对外开放数据库通讯端口，保证数据库系统安全可靠；

9.2.6.5 接入单元

接入单元主要解决非标系统与标准系统的正常对接，其应符合以下功能及性能要求：

a) 接入单元应支持将非标系统中的设备信息同步至标准系统中，可同步的前端数量不低于 1 万个；
b) 接入单元需将非标系统码流转换成标准系统码流再进行转发，并发转码能力应不低于 9 路；
c) 接入单元应支持双网段功能，匹配双网段的网络环境。

9.2.6.6 解码单元

解码单元功能要求如下：

a) 音视频解码设备应可以根据前端的视频编码格式、分辨率、帧率等参数自适应解码，解码音频默认与当前图像视频同步输出；
b) 音视频解码设备应按照平台信令提供的字幕内容，以及字符规格信息（包括字型、颜色、大小和位置），对各解码通道在相应的位置叠加相应内容的字幕；
c) 音视频解码设备应支持混合解码，多画面风格时，根据解码总能力进行限定，画面风格与最高解码分辨率不严格绑定。

9.2.7 指挥中心视频显示设备性能要求

指挥中心视频显示设备性能要求如下：

a) 显示设备的分辨率指标应高于系统对采集、传输过程规定的分辨率指标。建议支持分辨率为 1080P 及以上；
b) 应支持键盘、网络计算机双重控制方式；
c) 显示设备和信号切换设备的安全性应符合国家相关产品标准规定的安全要求；
d) 显示设备和信号切换设备的输入\输出接口应符合现行常见接口，如 DVI、HDMI、VGA、YPbPr、CVBS、BNC 等；
e) 信号切换数字视频网络虚拟交换/切换模式的系统应具有系统信息存储功能，在供电中断或关机后，对所有编程信息和时间信息均应保持；

9.2.8 指挥中心的数据存储

指挥中心的数据存储要求如下：

a) 宜采用前端存储、监控中心存储、客户端存储、存储备份相结合的分布式存储策略；
b) 配置的专用存储设备（如磁盘阵列、网络存储系统、光盘刻录机等）应能备份需要长期保留的信息，保存时间应该符合电子考场业务和安全管理的要求；
c) 考点指挥中心存储应至少存储考场、考务室、保密室等重要场所的现场音视频信息；
d) 监控中心存储设备宜集中存放在中心机房，应具有冗余、纠错及自动备份功能；宜采用网络存储技术，支持远程访问和高效存储；
e) 应支持图像存储和回放的双工模式，宜支持图像高码流记录和远程图像低码流传输的双码流、多码流模式。

9.2.9 指挥中心磁盘阵列

指挥中心资料存储应支持本地磁盘阵列方式或云存储方式，要求如下：

a) 应支持 RAID 冗余磁盘技术，支持 RAID0、1、5、6、10，支持热备盘；
b) 阵列系统宜有状态报警，提供控制台告警、指示灯告警、邮件告警等多种告警方式，且针对坏扇区磁盘的热顶替，支持虚拟磁盘；
c) 设备宜实现对考场录像的自动备份；

d) 系统性能与系统容量线性增长，单设备应具备不低于千兆网络传输能力，系统支持负载均衡；
e) 支持 SATA 硬盘，支持硬盘热插拔；
f) 单台设备支持冗余网口，支持网口绑定，冗余电源，实现负载均衡和冗余备份，实现负载均衡。
g) 应支持通过 WEB 方式对集群内所有的存储设备进行统一化集中管理，实现集群的配置、性能监控、运行状态监控、资源监控、日志记录以及故障报警等功能；
h) 系统的存储容量应能够保存六个月以上的音像资料。

9.2.10 历史图像的检索和回放功能

指挥中心应支持按照指定设备、时间、报警信息等要素检索历史图像资料并回放。

9.2.11 报警管理功能

指挥中心应支持实时接收报警源发送来的报警信息，包括身份识别异常、屏蔽系统异常信息，及时分发给相应的用户终端或系统、设备。

9.2.12 与其它系统的对接功能

指挥中心应能支持身份识别系统、屏蔽系统、巡查系统的接入。

9.2.13 管理人员 身份认证与权限管理功能

指挥中心管理人员的身份认证与权限管理功能要求如下：
a) 指挥中心应提供相关接口，接受身份验证系统的所有验证、统计数据、信息汇总；
b) 各种数据应可通过显示屏或电子地图系统统计图显示；
c) 指挥中心宜具有用户统一管理的门户对用户进行授权和认证。用户及权限管理可由各级管理平台独立控制。

9.2.14 设备管理功能

指挥中心应能对系统设备运行状态进行实时监测;对重要的设备进行冗余设置实现双机热备或者冷备。

9.2.15 网络信息安全管理功能

指挥中心应具备保证信息安全的功能，包括认证安全、传输安全、数据安全。应对某些重要的数据进行定期备份，对重要的数据应做异地备份。遵照信息安全标准 GB/T 22239-2008《信息系统安全等级保护基本要求》，本系统的安保等级定为二级。

9.2.16 系统安全审计

指挥系统安全审计功能要求如下：
a) 应对身份鉴别事件、系统管理员（安全员/审计员）/操作员所实施的操作、其它与系统安全相关的事件做审计，并做好相应的审计响应，例如实时报警、违例进程终止、服务取消等措施；
b) 应支持审计功能的开启和关闭。

9.2.17 有线电话

指挥中心应配备2门以上有线电话。

9.2.18 无线屏蔽系统工作状态显示

无线屏蔽系统工作状态显示功能要求如下：

a) 无线屏蔽系统可通过接口将系统工作状态、屏蔽工作状态等数据上传到指挥中心，通过电子地图或其他方式进行展示；

b) 已经安装侦测设备的考场，指挥中心应显示侦测频段等信息。

9.3 指挥中心的布局与环境要求

9.3.1 布局与要求

指挥中心宜具备指挥区、操作区、接待区、设备区、值班区等，具体布局与面积大小视所在建筑情况和需要而定：

a) 主显示屏幕的尺寸、安装位置可参照 JYJS201101《多媒体教学环境工程建设规范》第一册 7.4.2 和 7.4.3 的要求；

b) 扬声器系统的布置可参照 JYJS201102《多媒体教学环境工程建设规范》第二册 5.3.4 的要求。

9.3.2 环境要求

9.3.2.1 概述

环境要求除9.3.2.2、9.3.2.3规定之外的，均按照GB/T2887-2011执行。

9.3.2.2 声场及环境噪声要求

指挥区域、操作区域的声学指标应符合GB/T 9361-2011计算机场地安全要求。

9.3.2.3 抗电磁干扰性能要求

指挥中心抗电磁干扰性能应满足GB/T 2887-2011计算机场地通用要求的4.6.5条款要求。

9.3.3 电力保障

指挥中心电力保障系统要求如下：

a) 指挥中心配电系统应符合 GB/T 2887-2011 中 4.7.1a)的规定；

b) 电源质量应符合 GB/T 2887-2011 中 4.7.3 的规定。

9.3.4 照明等供电控制

指挥中心照明等供电控制要求如下：

a) 指挥中心终端及系统设备供电应独立控制；

b) 指挥中心终端及系统设备供电需配置 UPS 作为备用电源。在外来电源断电后，备用电源容量应至少能保证核心系统、重要监控点能正常工作 8 小时以上；

c) 指挥中心空调、新风换气等设备供电应独立控制。

9.3.5 防雷与接地要求

指挥中心的防雷与接地要求如下：

a) 指挥中心的防雷应满足 GB/T 9361-2011 计算机场地安全要求 10.3 的规定；

b) 指挥中心的接地应满足 GB/T 2887-2011 计算机场地通用要求的 4.8 的规定。

9.4 考务室技防设备系统

考务室技防设备系统建设要求如下：

a) 考务室在考试期间，应接受全面监控和录像，实施无线电信号屏蔽等安全措施；
b) 考务室应配备金属探测仪等安检设备；
c) 考务室应配备至少一门固定电话；
d) 在考试期间，所有防范设备应开启并处于正常工作状态，视频监控资料应当保存到考试结束后6个月。

9.5 试卷保密室技防设备系统建设要求

9.5.1 概述

保密室的技防设备系统主要由监控系统、报警系统、保密室网络及相关平台软件组成。条件允许应包含门禁系统。

9.5.2 技防系统架构及设备组成

试卷保密室技防系统架构及设备要求如下：

a) 监控系统前端采用高清网络摄像机，后端采用NVR（硬盘录像机），并能够与指挥中心巡查系统进行互联互通。视频监控资料应当保存到考试结束后6个月；
b) 报警系统发现有入侵行为，应能立即本地报警，并将警情上传到上级平台，通过上级平台能够对报警时间、类型、布防撤防等信息进行查询；
c) 试卷保密室网络应采用专网（或安全网络）将监控设备连接到本级（上级）指挥中心；
d) 在试卷保密室门口安装指纹门禁考勤一体机，实现对保密室进出人员的管理，需支持在平台软件查询刷卡记录。

9.5.3 试卷保密室报警系统

试卷保密室报警系统技术要求如下：

a) 根据保密室空间大小及布局选择吸顶或壁挂双鉴探测器；
b) 空间环境探测宜采用红外探测、多普勒效应探测技术；
c) 应能够自动触发报警，同时记录并上传报警信息；
d) 保密室门口应安装门磁探测器；
e) 通过管理中心报警管理软件，接收保密室上传的报警信号，并支持对报警信息进行查询统计。

9.5.4 试卷保密室网络

试卷保密室网络技术要求如下：

a) 试卷保密室应组建巡查专网，省级平台可以与各级保密室的网络设备进行相互访问，各市级平台能够直接与本市所有保密室网络设备进行相互访问，区县平台能够与本地保密室的网络设备进行相互访问。使用期间网络带宽独享，不低于10Mbps；
b) 各市及各区县之间通过路由限制进行逻辑隔离，禁止互相访问，从而形成全省互联，各区域彼此独立的保密室巡查专网。

9.5.5 试卷保密室门禁系统

试卷保密室门禁系统技术要求如下：

a) 系统应支持刷卡、指纹识别、人脸识别、密码等多种组合认证方式；
b) 应支持TCP/IP有线联网，支持跨网通讯传输各类事件信息，供各级平台软件进行查询；
c) 系统应具有防拆设计，支持防拆报警功能，并具有胁迫报警功能，遇紧急状况时，用户可输入胁迫码开门，同时系统会将胁迫事件发送至管理中心进行报警；

d) 系统应具有读卡错误超次警告功能，可设定最大读卡错误次数，超次后可设定系统自动停止操作，预防擅入并自我保全；
e) 系统应具有黑名单报警功能、门未关妥报警功能、门被外力开启报警功能，支持自定义警报解除码，报警发生时可以使用解除码消警；
f) 设备应内置电子时钟及看门狗程序设计，提供准确的日期、时间，以确保主机正常运作。

附 录 A
（规范性附录）
学校（机构）命名规则

A.1 代码结构

各级各类学校（机构）代码分5段，代码结构示意图见图A.1：

——第一段为“机构代码”，共 10 位，是按国家规定的设置标准和审批程序批准成立的各级各类学校（机构）拥有的全国唯一的代码标识；

——第二段为“学校驻地地域码”，共 12 位，采用国家统计局的《统计用区划代码》，用于标识学校所在地的区域；

——第三段为“属地管理部门驻地地域码（统计用）”，共 12 位，采用国家统计局的《统计用区划代码》，用于标识属地管理部门所在地的区域；

——第四段为“学校举办者码”，共 3 位，用于标识各级各类学校（机构）的举办者类别；

——第五段为学校（机构）的其他属性码，用于标识学校办学类型、类别和学校所在地的自然属性等。

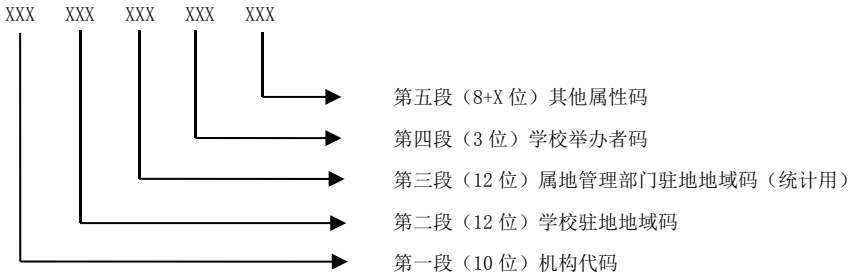


图 A.1 学校（机构）代码结构

A.2 编码方法

编码方法按照GB/T XXXXX-XXXX的规定执行。

A.3 代码更新与维护

教育部根据国家统计局每年公布的《区划和城乡代码》及各地学校（机构）变动情况，统一修订学校（机构）代码，并将调整后的新代码提供给相关单位使用。各地及时掌握本地区学校（机构）变动情况，定期对学校（机构）基本信息变动以及新生成代码进行审核，并及时报送教育部。

附 录 B
（资料性附录）
电子考场设备兼容性检测

B.1 电子考场设备

B.1.1 概述

电子考场系统互通直联的关键设备主要包括：

a) 流媒体服务器：又称视频服务器、数字视频服务器或视频编码器等，是用来实现将模拟音视频信号转换成数字音视频信号，放到网络传送，并实现本地存储的设备；

b) SIP 路由器：负责统一管理接入的各类 SIP 终端（包括用户、流媒体服务器、流媒体矩阵和媒体分发服务器等），按照统一命名规则（SIP URI）实现分级命名、联合定位等功能，并通过建立 SIP 路由器间的信任关系实现接入认证功能，进行终端访问呼叫过程控制及远程访问权限控制等功能；

c) 媒体分发服务器：又叫流媒体转发服务器，当多个用户并发访问同一路图像资源时，为减轻流媒体服务器的压力和节约网络传输开销，通过媒体分发模块与流媒体服务器间建立单路连接，然后采用组播、分发或广播的方式将音视频流分发给资源调用者；

d) d)解码器：又称流媒体矩阵，将数字化的音视频流还原成模拟信号，可以直接输出到监视器或电视机上进行显示的设备。

在设备选型时保证上述 4 类关键设备符合本标准要求，确保在各地自行建立的电子考场系统间实现互通直联。

B.1.2 测试流程

电子考场系统互联关键设备检测及互通联调测试流程分为3个阶段：

a) 厂商自测阶段，由待测厂商根据《规范》及本方案自行完成；

b) 网络流和稳定性测试阶段，需要现场进行；

c) 互通联调测试阶段，需要现场进行。

上述三个阶段的测试都通过后，该厂商生产的设备即符合本标准。

B.1.3 省级端测试环境

当设备厂商通过第一阶段的测试后，可以携带其设备到省级考试机构进行第二和第三阶段的测试，为此省级考试机构应该做如下准备工作：

a) 不低于 10M 的专线 Internet 接入（应有固定 IP 地址）；

b) 有局域网供厂商搭测试环境；

c) 监视器或电视机作为图像输出显示；

d) 安装 VLC（0.86 版）软件的电子计算机 2 台～3 台；

e) 厂商需提供的设备：SIP 路由器（可由电子计算机+专用软件模拟）1 台；

f) 视频服务器（带存储，且支持组播功能）1 台；解码器（支持组播功能）1 台；

g) 影碟机、摄像机和拾音器各 1 台作为音视频源（可共用）。

B.1.4 厂商自测阶段

B.1.4.1 概述

设备制造商设备接入电子考场系统时，厂商先进行自测。自测分为vlc检测和Elecard检测两种。

B.1.4.2 VLC检测方式

厂商从待检测视频服务器的输出上录制一段不少于 120 s的录像文件（根据情况，厂商也可以采用从网络上直接获取音视频流的方式来进行本步测试，方法见第二阶段网络流及稳定性测试部分说明），用 VLC软件（0.86版）进行播放，通过查看 VLC的报告，判定是否同时满足如下6条技术要求：

注：VLC播放器的下载地址是http://www.videolan.org。

a) 视频编码为 H.264

当以下两条信息成对出现时可判定该音视频流的视频编码格式为H.264，满足本标准中关于视频编码关于H.264的技术要求：

——当开始播放音视频流时，在报告开头部分出现如下信息：

ffmpeg debug: ffmpeg codec (H.264) started

——当终止播放时在报告的末端出现如下信息：

ffmpeg debug: ffmpeg codec (H.264) stopped

b) 视频编码为 MPEG4

当以下两条信息成对出现时可判定该音视频流的视频编码格式为 MPEG-4，满足本标准中关于视频编码的技术要求：

——当开始播放音视频流时，在报告开头部分出现如下信息：

ffmpeg debug: ffmpeg codec (MPEG-4 Video) started

——当终止播放时在报告的末端出现如下信息：

ffmpeg debug: ffmpeg codec (MPEG-4 Video) stopped

c) 封装为 TS

当以下两条信息成对出现时可判定该音视频流的封装格式为 TS，满足本标准中关于音视频流封装格式的技术要求：

——当开始播放音视频流时，在报告开头部分出现如下信息：

maindebug: using demux module "ts"

——当终止播放时在报告的末端出现如下信息：

main debug: removing module "ts"

d) 封装为 PS

当以下两条信息成对出现时可判定该音视频流的封装格式为 PS，满足本标准中关于音视频流封装格式的技术要求：

——当开始播放音视频流时，在报告开头部分出现如下信息：

main debug: using demux2 module "ps"

——当终止播放时在报告的末端出现如下信息：

main debug: removing module "ps"

e) 音频格式为 MPEG Layer II

当以下两条信息成对出现时可判定该音视频流的音频编码格式为 MPEG Layer II，满足本标准中关于音频编码的技术要求：

——当开始播放音视频流时，在报告开头部分出现如下信息：

main debug: using decoder module "mpeg_audio"

——当终止播放时在报告的末端如下信息：

main debug: removing module "mpeg_audio"

f) 音频格式为 AAC

当以下两条信息成对出现时可判定该音视频流的音频编码格式为 G711-ulaw，满足本标准中关于音频编码的技术要求：

——当开始播放音视频流时，在报告开头部分出现如下信息：

main debug: using decoder module "faad"

——当终止播放时在报告的末端出现如下信息：

main debug: removing module "faad"

B.1.4.3 Elecard检测方式

Elecard 检测方式如下：

a) 视频编码是否为 H.264

H.264视频包含SPS和PPS，通过Elecard Stream Analizer打开视频文件，在右侧显示框中会有H.264 Sequence Parameter Set和H.264 Picture Parameter Set两列，Elecard检测方式见图B.1。

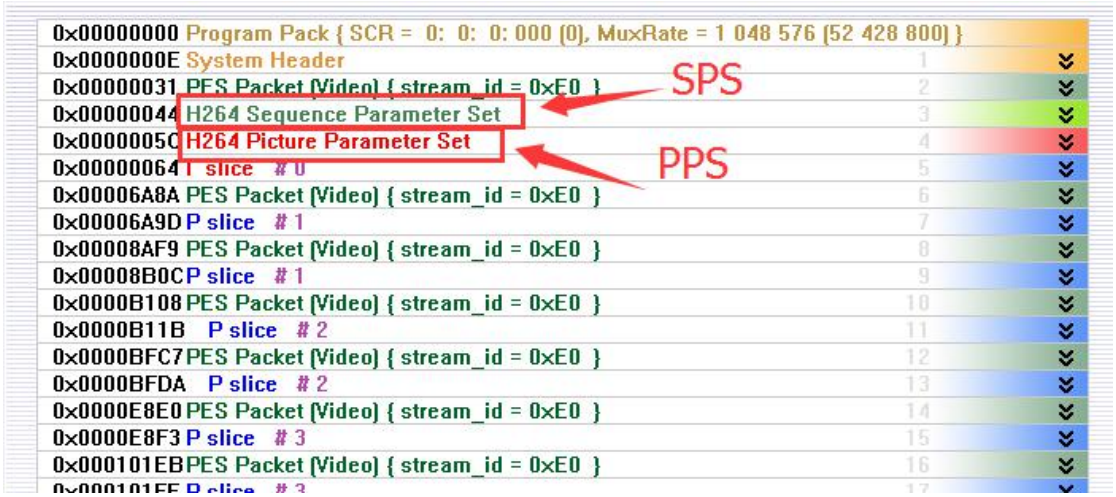


图 B.1Elecard 检测方式

b) 如何检测封装是否为 TS

通过抓包工具将视频数据去掉RTP头保存视频裸流成文件，使用Elecard Stream Analizer打开该视频文件，StreamInfo一栏显示StreamType：Transport，表示该视频流为TS流，见图B.2。

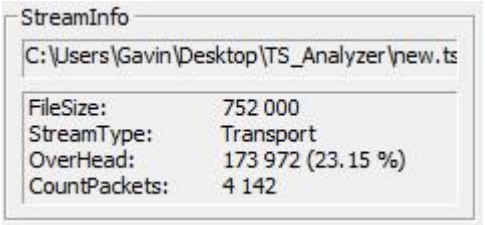


图 B.2视频流为 TS 流检测方式

c) 如何检测封装是否为 PS

StreamInfo一栏显示StreamType：Program，表示该视频流为PS流，见图B.3。

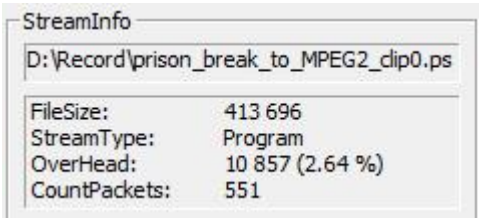


图 B.3视频流为 PS 流检测方式

d) 如何检测 SIP 协议是否符合标准

宜由厂家联合或者委托某单个厂家开发一套标准SIP协议检测软件，该检测软件能够覆盖所有SIP信令的检测点，以此来规范SIP协议检测标准。

B.2 检测架构要求

B.2.1 概述

音视频编解码测试方法由3部分组成：

a) 录像文件的 VLC 测试；

b) 设网络流的 VLC 测试；

c) 与符合规范的解码设备进行兼容测试。

B.2.2 录像文件的VLC测试

各设备厂商录制一段120 s的录像文件，用VLC来播放，如果不符合以下几点将认为不是标准的音视频流：

a）封装是 PS；

b）视频流是 H.264、H.265、SVAC 或者 MPEG-4；

c）音频流是 MPEG-Layer II，G.711，AAC_LC；

d）在 VLC 播放音视频同步。

B.2.3 设备网络流的VLC测试

厂商在通过以上测试后可进入下一步测试。VLC测试结构见图B.4。

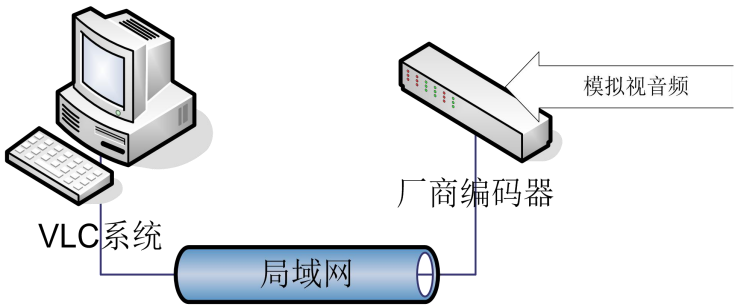


图 B.4VLC 测试结构

待测编码器通过网络发送音视频流，VLC系统接收如果不符合以下几点将认为不是标准的音视频流：

a）封装是 PS；

b）视频流是 H.264、H.265、SVAC 或者 MPEG-4；
c）音频流是 MPEG-Layer II，G.711，AAC_LC；
d）在 VLC 播放音视频同步；
e）连续运行 24 h 不宕机。

B.2.4 与符合规范的解码设备兼容测试

通过录像文件的VLC测试和设网络流的VLC测试的待测设备还应与符合规范的解码设备做直联互的兼容性测试，达到其互编互解。

附 录 C
（资料性附录）
作弊防控系统功能与性能测试

C.1 测试设备

测试设备包括：信号发生器、对讲机或可调频对讲机、侦测服务器、分贝仪、频谱仪。

C.2 系统功能测试

C.2.1 侦测捕捉能力测试

系统应能够实现对所在区域内出现的无线电作弊信号实施有效的侦测，能够快速检测到无线电信号的存在，并给出其频率值。测试方法如下：

a) 将信号源调至 50MHz～3000MHz 范围内任意频点发射信号；
b) 用频谱仪观察确认是否有对应信号产生；
c) 确认侦测服务器是否侦测到与频谱仪观察到的信号一致。

C.2.2 整体阻断性能测试

针对不同频段无线电信号的阻断需求，阻断子系统需能同时输出一定数量的阻断信号，信号数量≥20。测试方法如下：

a) 阻断信号包括点频阻断和全时阻断，全时阻断需依据具体通信频段进行划分；
b) 用频谱仪观察确认是否有对应信号产生。

C.2.3 绿色阻断方式测试

对于无需进行全时压制的频段，无作弊信号时，不发射阻断信号；当作弊信号出现时，自动发射阻断信号；作弊信号消失后，阻断信号停止发射。测试方法如下：

a) 无作弊信号时利用频谱仪观察有无屏蔽信号；
b) 通过可调节对讲机任意给出一个作弊信号；
c) 侦测服务器侦测到作弊信号,利用频谱仪观察阻断子系统有无屏蔽信号产生；
d) 关闭对讲机后观察作弊信号是否消失。

C.2.4 数据捕捉还原性能测试

侦测系统应能够对语音信号、数字信号进行精确捕捉，对捕捉到的数据信息进行有效存储及还原。测试方法如下：

a）语音、数据作弊设备距离侦测天线 9 米以外进行数据传输；
b）侦测服务器自动对数据信息进行捕捉储存；
c）确认捕捉到的数据能否被还原。

C.2.5 侦测引导阻断能力测试

待测系统发射的阻断信号频率无缝覆盖50MHz～3000 MHz。信号侦测子系统侦测接收到50MHz～3000 MHz内任一频点的可疑信号,通过网络发送控制命令给信号阻断子系统,信号阻断子系统接收到控制指令后开启相应的阻断频率对其覆盖。测试方法如下：

a）频谱仪放置在距离阻断设备正前方 3 米处；

b）信号发生器在每段待测频段随机指定一个“选测频点”进行发射；

c）侦测子系统频谱显示选测频点信号；

d）阻断子系统发射相对应的频点阻断信号；

e）频谱仪检测到阻断设备发出的信号。

C.2.6 阻断子系统邻频点阻断压力测试

系统应在50MHz～3000MHz范围拥有相邻作弊信号同时精确阻断的能力。测试方法如下：

a）信号发生器在50MHz～3000MHz范围内任意选择两个3MHz以内相邻频点输出；

b）阻断子系统输出选测频点的阻断信号；

c）频谱仪观察阻断子系统发出的信号频谱是否与信号发生器发出的一致。

C.2.7 固定频段的无线电信号的全实时阻断能力

针对固定频段的无线电信号,如手机、无线局域网(2.4G和5.8G)进行全实时阻断能力测试。测试方法如下：

a）待测系统的阻断设备统一置于场地中央。将频谱仪置于阻断设备 5 米以外；

b）阻断子系统输出相对应的阻断信号；

c）频谱仪观察阻断信号频谱信息；

d）测试手机、无线路由器等接收设备的接收信号能力是否被阻断。

C.2.8 对讲信号频段的阻断能力测试

针对无线对讲频段信号(136MHz～174MHz、400MHz～470MHz)两个频段，每个频段不小于多组信号的情况下，阻断无遗漏。测试方法如下：

a）待测系统的阻断设备统一置于场地中央。将频谱仪置于阻断设备 5 m 以外；

b）阻断子系统输出相对应的阻断信号；

c）频谱仪观察阻断信号频谱信息；

d）用户根据需求，确定测试多组以上对讲机，接收设备的整个屏蔽效果是否达标。

C.2.9 管理平台的测试

管理子系统应支持黑白名单功能，应能实时报告设备的运行情况、各设备的开关机状态、作弊信号发现和阻断的运行情况，并且具备侦测数据信息的分类、识别及频谱显示，支持作弊数据下载。测试方法如下：

a） 黑白名单，按照指定频率在系统上添加黑白名单，测试人员分别使用对讲机设置为黑名单频点和白名单频点，通过频谱仪观察阻断信号检查黑白名单功能是否同时生效；

b） 设备状态，对待测系统的阻断设备进行开机和关机操作，测试人员在用户管理接口上查看设备状态应符合设备开机和关机状态；

c） 在线控制,对待测系统的阻断设备进行在线控制,测试人员通过频谱仪观察控制信息是否生效；

d） 数据下载，测试人员确认侦测资料是否拥有下载功能；

e） 分类识别及频谱显示，直接在侦测平台观察侦测信息是否实现分类识别及频谱显示功能。

C.2.10 互联互通测试

互联互通指阻断子系统、侦测子系统通过SIP协议向不同生产侦测设备、阻断设备的厂家提供的管理子系统注册、列表获取、控制指令下发、信号文件还原等操作的互联互通.测试方法如下：

a) 设备生产厂家自行组建局域网，将阻断子系统、侦测子系统、管理子系统接入自行组建的局域网环境内；
b) 提供一个主交换机将各设备生产厂的连接组成一个各厂商设备在网络层的互通性；
c) 以抽签形式确定先后顺序，各设备生产厂商轮流模拟管理子系统，其他设备生产厂商的阻断子系统、侦测子系统向管理子系统注册，注册成功后在管理子系统上面查看各厂商设备的在线状态,控制阻断子系统模块通道的开关, 查询作弊信号信息，调听还原的作弊语音，调看还原的数传文本。

C.3 系统性能测试

C.3.1 侦测子系统

侦测子系统性能测试方法如下：

a) 侦测频率范围：50MHz～3000MHz，可扩展。
   1）信号源在 50MHz～3000MHz 频段内均匀间隔发射多个正弦波信号；
   2）信号强度设置为-60dBm，可以检测出该信号符合，否则不符合。
b) 侦测响应时间：≤500ms。
   1）信号源在 50MHz～3000MHz 频段内均匀间隔发射多个正弦波信号；
   2）设置驻留时间为 500ms，侦测可以实时监测到该信号，则符合。
c) 侦测频率精度：≤25KHz。
   1）信号源在 50MHz～3000MHz 频段内均匀间隔发射多个正弦波信号；
   2）信号强度设置为-60dBm，侦测给出该信号频率值；
   3）如果系统检测得到频率值与信号源设定频率偏差在 25KHz 内则符合，否则不符合。
d) 侦测灵敏度：≤-80dBm。
   1）信号源在 50MHz～3000MHz 频段内均匀间隔发射多个正弦波信号；
   2）信号强度设置为-80dBm，侦测可以检测出该信号则符合，否则不符合。
e) 侦测动态范围：≥70dB。
   1）信号源在 50MHz～3000MHz 频段内均匀间隔发射多个正弦波信号。
   2）部分信号强度设置为-80dBm，部分信号强度设置为-10dBm。
   3）如果-80dBm 和-10dBm 情况下，侦测都能检测出该信号，则符合。
f) 能够还原 FM、FSK、AM 等调试信号：
   1）信号源在 50MHz～3000MHz 频段内发射调制信号；
   2）设置信号调制方式为 AM，系统能还原调制内容则符合；
   3）设置信号调制方式为 FM，系统能还原调制内容则符合；
   4）设置信号调制方式为 FSK，系统能还原调制内容则符合；
   5）如果 AM、FM 和 FSK 体制方式都能还原，则本项测试通过，否则不通过。

C.3.2 阻断子系统

阻断子系统性能测试方法如下：

a) 阻断频率范围：无缝覆盖 50MHz～3000MHz，可扩展。

1） 侦测子系统设备在 50MHz～3000MHz 范围内任一频点引导阻断子系统设备发射阻断信号；
2） 采用频谱仪在阻断设备前方 6 米处测试对应频点频谱；
3） 如果频谱仪能观测到对应频点存在阻断信号则符合，否则不符合。

b） 阻断信号带宽：0.7～5 倍异常信号带宽。
1） 信号源在 50MHz～3000MHz 范围内发射信号，接入侦测设备使设备引导阻断设备发射阻断信号；
2） 采用频谱仪在阻断设备前方 6 米处测试对应频点频谱；
3） 读取信号源信号的 3dB 带宽值 X，阻断设备发射信号的 3dB 带宽 Y；
4） 如果 0.7≤Y/X≤5 则符合，否则不符合。

c） 异常信号并发阻断能力：≥20 个。
1） 侦测设备在 50MHz～3000MHz 范围内引导阻断设备发射 20 个频点的阻断信号；
2） 采用频谱仪在阻断设备前方 6 米处测试对应频点频谱；
3） 如果频谱仪上可看到 20 个对应频点上的阻断信号则符合，否则不符合。

d） 阻断效果：在 6 m×9 m 标准化考场空间内，异常信号强度≤-65dBm 时，屏蔽有效率≥95%。
1） 选取适当位置放置对讲机、语音类作弊器材和数传类作弊器材发射端设备，使得考场内作弊信号强度≤-65dBm；
2） 采用发射设备发射 X 个字符的作弊语音，考场内听取收到的语音并写出，如果考场内正确写出的字符个数为 Y 个，则对语音作弊信号阻断有效率为(X-Y)/X；
3） 采用发射设备发射 X 条作弊数传，考场内接收查看清晰的数传，如果考场内能正确读取的数传有 Y 条，则对数传作弊信号阻断有效率为(X-Y)/X。

C.4 侦测引导阻断响应时间的测试

侦测引导阻断响应时间的测试方法：系统响应时间≤600ms；

a） 信号采集设备置于信号采集分析状态；
b） 发射作弊信号或作弊模拟信号，侦测设备引导阻断设备后阻断设备发出阻断信号；
c） 记录作弊信号出现的时刻 t_1，记录阻断信号出现的时刻 t_2；
d） 如果（t_2-t_1）≤600ms 则符合，否则不符合。

附 录 D
（资料性附录）
身份识别系统测试

D.1 考生身份采集验证终端硬件测试

D.1.1 概述

提供两套指纹验证终端现场测试，其中一套须预存储120条模拟考生不同的指纹信息，另一套须预存储2000条模拟考生不同的指纹信息。

D.1.2 身份认证终端基本身份信息采集认证功能

身份认证终端基本身份信息采集认证功能测试包括如下内容：

a) 终端应具备指纹采集功能；
b) 终端应具备身份证扫描功能；
c) 终端应具备人脸信息的采集认证功能，人脸信息的采集应具有能够满足认证要求的清晰度。

D.1.3 终端信息存储量

身份认证设备应能存储5000条以上模拟考生详细资料，包括考生号、姓名、公民身份号码、考点、考场、照片、指纹等。

D.1.4 识别率测试

比对不正确指纹20次；比对正确指纹20次。

D.1.5 比对速度测试

测试100人身份信息的采集认证速率，测试5次。

D.1.6 验证终端脱机工作能力

身份识别终端应能够实现离线状态的身份信息采集和验证，并通过现场采集5人身份信息进行监测。

D.2 考生身份识别管理系统软件测试

D.2.1 生物特征及证件信息采集比对

生物特征信息采集功能测试，要求采集的考生生物特征信息与身份证信息一致。测试方法如下：

a) 采集指纹进行比对；
b) 视频拍摄进行人脸特征识别比对；
c) 扫描身份证件，进行对比验证。

D.2.2 身份识别信息管理平台

身份识别信息管理平台功能测试，主要包括如下内容：

a) 各种采集信息的统计、查询、管理；

b) 验证信息的统计、查询、管理；
c) 支持针对多场次考生的相互校验；
d) 支持打印相关报表、设置缺考、人工审核等考务业务；
e) 能够对采集、验证等各个阶段进行时间控制、角色权限控制；
f) 数据的安全性、正确性测试。

参考文献

[1] JYJS201101《多媒体教学环境工程建设规范》

[2] JYJS201102《多媒体教学环境工程建设规范》