ICS 13.310
CCS A 91

团 体 标 准

T/CDAFXH 1—2024

企业事业单位视频安全技术规范

2024－06－01 发布　　2024－06－01 实施

成都市安全防范协会　　发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　系统结构 2
6　证书和密钥要求 3
7　设备身份认证 3
8　设备要求 3
9　功能要求 4
10　性能要求 5
参考文献 7

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由成都安全防范协会提出。

本文件由成都安全防范协会归口。

本文件起草单位：成都市公安信息技术研究所、成都安全防范协会、神贝慧联(成都)科技有限公司、成都市标准化研究院、360数字安全科技集团有限公司、北京启明星辰信息安全技术有限公司、四川通信科研规划设计有限责任公司。

本文件主要起草人：赵敬千、宋擘、王永宁、汪宏宇、石琼、庄永、陈旭、宋文杰、王博文、黄宝、才虹丽。

企业事业单位视频安全技术规范

1 范围

本文件规定了企业事业单位视频安全技术规范的术语和定义、缩略语、系统结构、证书与密钥要求、设备身份认证、设备要求与功能要求、性能要求。

本文件适用于企业事业单位视频安全系统的设计与应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 28181 安全防范视频监控联网系统 信息传输、交换、控制技术要求

GB 35114-2017 公共安全视频监控联网信息安全技术要求

GA/T 1400.1-2017 公安视频图像信息应用系统 第1部分：通用技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

视频安全管控系统 video security control system

通过安全准入、安全调阅、视频水印等技术手段保障视频数据在存储、使用、分发环节存在的安全风险问题，包括非授权访问监控视频数据、视频存储文件泄漏和篡改、视频文件非法传播、泄漏无法溯源等。

3.2

前端设备 front-end device

公共安全视频监控联网系统中安装于监控现场的信息采集、编码/处理、存储、传输、安全控制等设备。

3.3

视频水印 video watermarking

用户能在视频内容中添加用户信息、时间信息、警示信息等，用于标记视频内容的来源便于事后追溯，水印类型包含显性水印、隐性水印或二维码水印。

3.4

设备准入 equipment access

在网络环境中对终端设备（如计算机、服务器等）进行的一种安全控制措施，包括对终端设备的安全合规状态进行检查和评估，只有通过认证的合法设备才能接入网络。

3.5

设备指纹 device fingerprint

用于唯一标识设备身份的特征信息，主要包括 IP、MAC、设备类型、设备型号、设备厂商、操作系统等。

3.6

安全审计 security audit

对水印设置、视频监控文件的操作、导出申请、审批授权、下载导出等行为进行记录。

4 缩略语

下列缩略语适用于本文件。

IPC：网络摄像机（IP CAMERA）
DVR：数字视频录像机（Digital Video Recorder）
NVR：网络硬盘录像机（Network Video Recorder）
SSH：安全外壳协议（Secure Shell）
FTP：文件传输协议（File Transfer Protocol）
Telnet：远程登录协议（Telecommunications Network）

5 系统结构

5.1 系统组成

以国产信创和可信技术为基础底座，围绕安全准入、安全调阅、汇聚联网、智能化应用、运维等核心应用组成，并符合 GB 35114-2017 中 4 章的要求，系统功能模块组成图如图 1 所示。

图1 系统功能模块组成图

5.2 系统架构

5.2.1 系统架构应合理，具备良好的扩展性和可维护性。
5.2.2 应采用成熟可靠的技术手段，确保系统的稳定运行。
5.2.3 宜支持多级联网架构。

5.3 外部连接

5.3.1 企事业小型、中小型单位和重点单位等场所的局域网端应分别以轻量网关、中量网关、视频安全管控系统连接接入视频资源,对象包括 IPC、DVR、NVR、视频平台、人脸抓拍摄像机、人脸门禁、车辆道闸等设备。
5.3.2 互联网、专网端应将视频资源通过可信认证后传输至二级视频安全管控平台，再通过可信认证后传输至一级视频安全管控平台。
5.3.3 系统外部连接关系如图 2 所示。

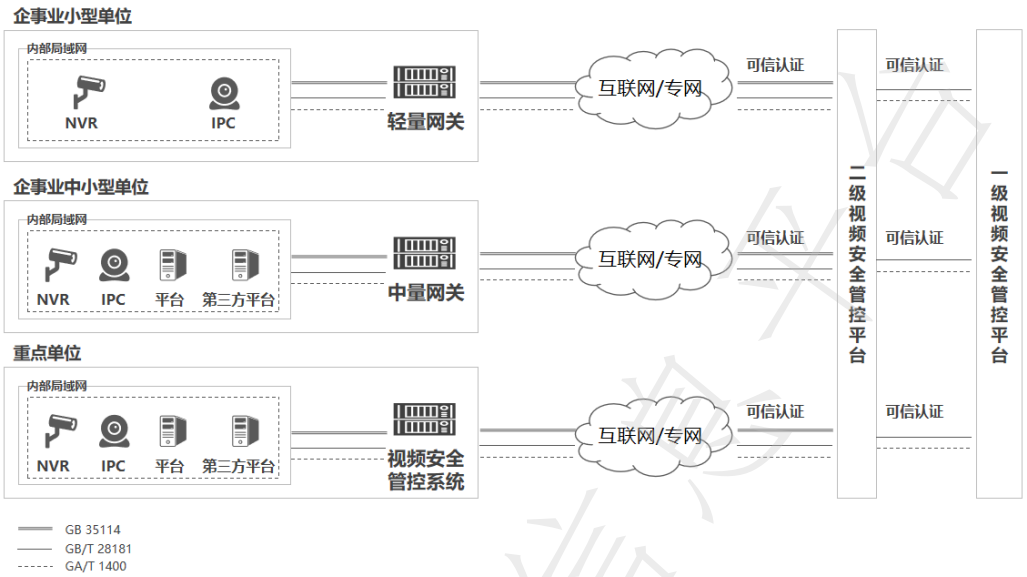

图2　系统外部连接关系图

6　证书和密钥要求

应符合GB 35114-2017中第5章的要求。

7　设备身份认证

应符合GB 35114-2017中第6章6.4的要求。

8　设备要求

8.1　外观要求

8.1.1　设备表面不应有明显的凹痕、划伤、裂缝、变形和污迹等。
8.1.2　表面涂层均匀，不应出现起泡龟裂、脱落和磨损现象。
8.1.3　金属零部件应无锈蚀，文字标识应清晰、完整。

8.2　结构要求

8.2.1　设备的机械结构应具备足够的强度和稳定性,以承受正常和预期的工作负荷。
8.2.2　应采用先进的技术和架构，保证系统的稳定性和性能，能够高效地处理大量的数据和请求。

8.3　物理接口要求

8.3.1　应具有两个或以上网络接口,网络接口间应保持逻辑隔离。
8.3.2　网络接口类型应为以太网接口、4G/5G 接口、WIFI 接口等。

8.4　设备软硬件要求

8.4.1　软件应采用国产操作系统和数据库。
8.4.2　硬件应采用一体机的模式，软件统一装在同一台硬件环境中。
8.4.3　一体机宜支持可信认证。

8.5　信息安全要求

8.5.1　应符合 GB 35114—2017 中第 6 章和 GA/T 1400.1-2017 中第 11 章的相关要求。
8.5.2　信息传输应符合 GB/T 28181 的要求，传输过程宜进行数据加密。

8.5.3　系统的密码使用和管理应符合国家密码管理的规定。

9　功能要求

9.1　基础服务

9.1.1　应具备国产数据库数据读写服务。
9.1.2　应具备资产扫描、设备准入、网络监测、漏洞检测、视频等基础服务，其中视频服务应具备以下功能：

——视频流查看、回放、录像文件导出等功能；
——通过叠加视频水印，对视频泄密进行朔源；
——提供视频转码服务，对叠加水印后的视频提供的给第三方平台查阅、预览和回放；
——提供视频共享服务，支持视频共享给上级平台或第三方平台。

9.1.3　相关协议应符合 GB/T 28181 和 GA/T 1400.1-2017 的要求。

9.2　安全准入

9.2.1　应支持前端设备的准入控制，主动发现接入网络的前端设备标识，提取设备指纹，识别协议信息，形成设备资产目录。
9.2.2　应支持根据终端设备的 IP 地址(网段)、MAC 地址、终端类型等组合作为设备的准入识别指纹特征，对终端进行自动准入。
9.2.3　应支持视频协议准入，支持基于协议特征的应用协议控制机制。
9.2.4　应支持设备指纹准入，支持基于设备厂商、设备类型、设备特征等设备属性的准入控制。
9.2.5　应支持黑/白名单方式的调阅身份准入控制，对违规接入进行告警和通知，控制非法设备的接入行为。

9.3　网络防护

9.3.1　应自动识别摄像机私接、仿冒、异常网络行为、异常协议等安全风险，检测仿冒摄像机 MAC 地址/IP 地址/应用协议等攻击行为，支持设置相应告警参数、处理动作并记入告警日志。
9.3.2　应支持通过网络主动扫描方式，能够对网络内部的资产进行自动识别和分类，设备类别至少可自动区分为视频监控设备、终端设备、应用服务设备，网络设备、网络打印机、安全运维类设备等；支持设备品牌、操作系统类别、设备型号等信息的识别和分类。
9.3.3　应支持对 SSH、Telnet、FTP、windows 远程桌面（RDP）进行弱口令检查，支持对常用的数据库系统进行弱口令或身份认证检查。
9.3.4　应支持识别主流厂商摄像头设备，对接入的网络摄像头的登录通用口令和弱口令进行识别和检测，弱口令字典可手动加载进行更新。
9.3.5　应支持对常见视频监控设备漏洞、Windows 系统漏洞、数据库漏洞、网络应用的漏洞等进行扫描检测。
9.3.6　应支持生成安全检测报告、资产统计报告、报警信息统计报告，提供资产、弱口令、安全漏洞、违规外联等多维度的数据汇总及统计分析。

9.4　可信认证

9.4.1　宜支持通过可信认证证书接入上级可信节点，支持执行上级下发的可信策略。
9.4.2　应支持基于硬件可信根对系统进行可信安全度量，阻止非可信系统的接入。
9.4.3　应支持使用国密算法进行可信度量，包括对可执行程序、安装包、动态库、静态库等静态度量和对系统运行环境可信状态信息的进行实时采集、可信验证的动态度量。
9.4.4　宜支持向上级可信节点发送可信状态报告和对下级可信节点的可视化管理，可信状态监控等。

9.5　安全调阅

9.5.1　预览和回放

9.5.1.1　应支持实时流预览功能，支持云台控制，可查看视频已叠加水印，支持不低于 9 分屏预览。

9.5.1.2　应支持录像回放功能，可查看视频已叠加水印，支持不低于 4 分屏回放。
9.5.1.3　应支持 H.264 和 H.265 格式视频流。

9.5.2　视频和大屏水印

9.5.2.1　应支持在调阅的视频数据中叠加字符信息、图片信息或将字符生成二维码，可配置显性水印、隐性水印。
9.5.2.2　水印中应包含自定义内容、用户、调阅时间，并可设置水印内容、位置、大小等信息。
9.5.2.3　应支持拼接大屏显示水印、隐性水印或二维码水印，包含用户信息、时间信息、警示信息等。
9.5.2.4　应支持拼接屏幕、全屏幕水印，用于事后追溯，不应影响视频观看效果。
9.5.2.5　应提供专有控制软件实现屏幕控制，实时显示输入输出状态，并可给不同用户提供不同操作权限

9.5.3　文件导出

9.5.3.1　应通过管理员（审批员）授权，在用户终端将视频监控文件制作成外发数据，宜支持文件数据加密。
9.5.3.2　应具有对外发送文件设置密码、文件时效、文件打开次数等功能。
9.5.3.3　应支持屏蔽主流截屏、录屏软件，防止调阅电脑通过截屏、录屏的方式外泄视频敏感信息。

9.6　视频安全审计

9.6.1　应支持安全审计，能对水印设置、视频监控文件的操作、导出申请、审批授权、下载导出等行为进行记录。
9.6.2　记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等，支持对审计数据进行统计、查询、分析和生成审计报表。

9.7　视频共享

9.7.1　与其他视频平台之间的对接应符合 GB/T 28181 的要求。
9.7.2　应支持多个下级平台注册到本级平台，支持本平台注册到多个上级平台，实现多级串联。
9.7.3　应支持上级平台对视频进行实时调阅、回放和云台控制等动作，并记录操作日志。
9.7.4　应支持在提供的上级平台的视频流中加入显性水印、隐性水印或二维码水印，对共享视频泄密进行溯源。

9.8　智能化应用

9.8.1　应支持视频快速检索分析功能，能够快捷提取视频中的人、机动车和非机动车等移动目标和目标特征。
9.8.2　应支持规则排查功能，可通过绊线、周界、冷区、目标类型、目标颜色、时间范围进行排查。
9.8.3　应支持对目标类型的二级筛选，包括：戴帽、带包、带伞、性别、年龄、上衣类型、上衣图案、下衣类型、下衣图案、上身颜色、下身颜色。
9.8.4　应支持对图像进行处理，应包含图像增强、人像修复等功能。

9.9　智能化运维

9.9.1　应具备对设备状态进行检测功能，包括网络连接状态、录像状态、码流信令状态、网关在线状态。
9.9.2　应具备对视频图像质量进行巡检分析功能，包括雪花噪声、信号缺失、画面冻结、色彩丢失、遮挡、模糊、移位、彩条、偏色、亮度异常。

9.10　用户管理

9.10.1　应具备用户注册、身份认证等用户管理功能。
9.10.2　应具备权限管理、访问控制等权限控制功能。

10　性能要求

10.1 视频性能

10.1.1 系统应基于国产化操作系统部署且稳定运行。
10.1.2 视频接入和准入路数应不低于 50 路。
10.1.3 视频转发数应不低于 16 路实时视频流。
10.1.4 视频调阅并发路数应不低于 16 路。

10.2 设备身份认证性能

应符合GB 35114—2017中7.1的规定。

10.3 稳定性要求

在正常工作条件下，设备应支持 7×24 小时连续工作，并且不出现电路、机械或设备装载操作系统的故障。

10.4 日志流程时间

日志留存时间应不少于180天。

参 考 文 献

[1] GB 37300 公共安全重点区域视频图像信息采集规范
[2] GB 50395 视频安防监控系统工程设计规范
[3] GB/T 50636 城市轨道交通综合监控系统工程技术标准
[4] GA/T 367 视频安防监控系统技术要求
[5] GA/T 1788 公安视频图像信息系统安全技术要求
[7] GA/T 1781 公共安全社会资源安全联网设备技术要求