

数 字 山 东 工 程 标 准

SZSD 0018—2024

公共视频监控 视图数据应用安全规范

Public video surveillance—Video and image data application security specification

2024 - 04 - 15 发布

2024 - 06 - 01 实施

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 安全组件..... 1

6 视图应用安全..... 2

6.1 应用访问控制..... 2

6.2 应用内容保护..... 2

6.3 应用攻击防护..... 2

6.4 应用脆弱性防护..... 2

6.5 应用日志审计..... 2

7 视图数据安全..... 3

7.1 数据签名和加密..... 3

7.2 数据访问控制..... 3

7.3 数据备份恢复..... 3

7.4 数据审计..... 3

7.5 其他数据安全措施..... 3

8 运行环境安全..... 3

8.1 终端安全..... 3

8.2 主机安全..... 4

8.3 云平台安全..... 4

参考文献..... 5

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由山东省大数据局提出、归口并组织实施。

本文件起草单位：山东省公安厅、山东大学、山东新一代标准化研究院有限公司、山东省大数据中心、泰山信息科技有限公司、山东华软金盾软件股份有限公司、山东省计算中心（国家超级计算济南中心）。

本文件主要起草人：程少龙、吴天柱、马辉、冯政、刘云、扈玮、张树强、陈翔、刘婉婷、赵硕。

公共视频监控 视图数据应用安全规范

1 范围

本文件规定了公共视频监控安全组件、视图应用安全、视图数据安全及运行环境安全等内容。
本文件适用于公共视频监控视图应用系统的安全规范。

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 25069—2022 信息安全技术 术语

GB 35114 公共安全视频监控联网信息安全技术要求

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

视图应用系统 view application system

提供视频图像信息采集、传输、存储、分析、处理、应用、联网共享、安全保护等功能的系统。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

DDoS：分布式拒绝服务（Distributed Denial of Service）

IP：网际互连协议（Internet Protocol）

5 安全组件

视图数据应用安全部署于各类视图应用系统的安全区域，主要包括视图应用安全、视图数据安全、运行环境安全，安全组件架构应符合图1的相关规定。

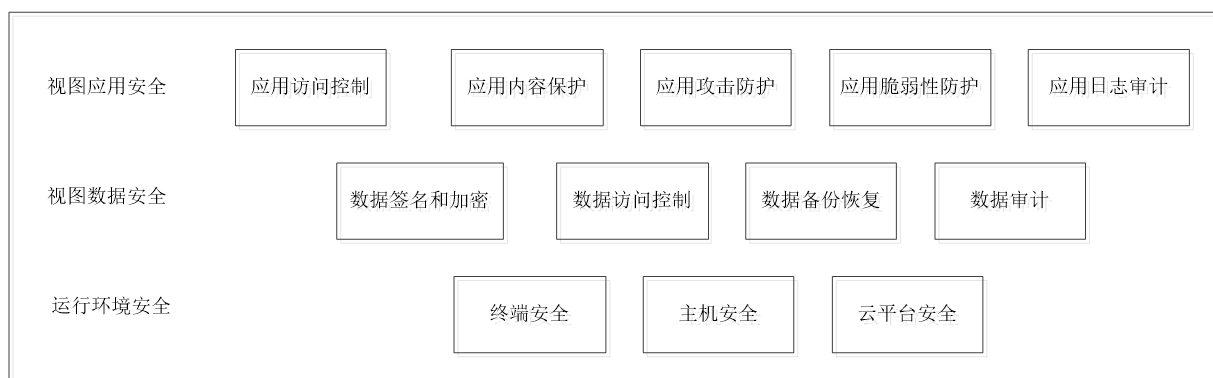


图 1 安全组件架构

6 视图应用安全

6.1 应用访问控制

应用访问控制要求，包括但不限于：

- 应对登录视图应用系统的用户进行身份鉴别，用户身份管理和认证管理由安全基础设施统一提供；
- 应对用户访问进行授权，并根据用户的不同角色、级别、所属机构、任务和场景进行鉴权、授权，实现功能级访问控制。

6.2 应用内容保护

应用内容保护要求，包括但不限于：

- 应根据业务需求对视图应用系统展示和导出的敏感视图、数据等信息进行脱敏处理；
- 应对应用内容的完整性进行保护，防止非授权修改；
- 应对视图应用系统应用内容进行安全防护，防止自动化工具攻击和数据爬取。

6.3 应用攻击防护

应用攻击防护要求，包括但不限于：

- 应对视图应用服务进行 Web 攻击防护，识别、防御恶意用户针对 Web 应用发起的攻击；
- 应对视图应用服务进行 API 攻击防护，检测、识别、拦截针对 API 接口的攻击；
- 应对视图应用服务进行应用层 DDos 攻击防护，阻断恶意发送大量合理请求、消耗目标系统服务资源的 DDos 攻击行为。

6.4 应用脆弱性防护

应用脆弱性防护要求，包括但不限于：

- 应对应用程序的安全漏洞、编码隐患进行安全扫描检测，发现潜在的安全问题和架构缺陷；
- 应对已经发现的应用漏洞通过修补程序或软件版本升级进行漏洞修复。

6.5 应用日志审计

应用日志审计要求，包括但不限于：

- a) 应记录视图业务应用的操作日志，操作日志应包含操作人、操作时间、操作终端、操作对象、操作条件、返回结果等；
- b) 应能够基于业务日志的行为发生源 IP 地址、行为发生时间范围、行为发生时间周期、行为结果等进行分析，发现用户异常行为；
- c) 应支持对异常应用行为进行告警，告警信息的内容包括但不限于告警类型、告警级别、事件时间、告警明细信息、处理建议等，并支持对审计日志以及告警信息进行人工和自动处置；
- d) 应由审计管理员查阅审计日志信息，审计管理员的查阅和审计操作需记录日志；
- e) 应提供应用日志存储能力，日志保存时间不少于 180 天。

7 视图数据安全

7.1 数据签名和加密

数据签名和加密要求，包括但不限于：

- a) 重要视频数据的签名和加密应符合 GB 35114 的相关规定；
- b) 应对其他重要的非视频数据在传输和存储过程中通过签名、加密等措施进行完整性和机密性保护。

7.2 数据访问控制

数据访问控制要求，包括但不限于：

- a) 应根据用户属性、数据属性、数据操作行为按最小权限原则配置数据访问权限策略；
- b) 结构化数据访问权限宜实现记录级权限管控。

7.3 数据备份恢复

数据备份恢复要求，包括但不限于：

- a) 应支持重要数据的本地备份与恢复；
- b) 应支持重要数据处理系统的热冗余；
- c) 宜支持异地备份。

7.4 数据审计

数据审计要求，包括但不限于：

- a) 应支持对视图应用系统中数据库和数据文件系统的操作行为进行审计，审计记录应包括日期、时间、用户、事件类型、操作是否成功及其他与审计相关的信息；
- b) 应支持发现并记录数据删除操作、敏感数据操作等异常数据操作；
- c) 应对视图信息的存储位置、使用交换过程、访问控制权限进行审计。

7.5 其他数据安全措施

应具备根据需求增加其他数据安全技术措施的能力。

8 运行环境安全

8.1 终端安全

终端安全要求，包括但不限于：

- a) 应对恶意代码进行实时检测、查杀或隔离；
- b) 应及时安装系统补丁，修复系统漏洞；
- c) 应对终端网络连接的端口、协议类型等进行有效管理，关闭高危端口，阻断未知协议；
- d) 应采用数字水印等方式对拍照、转发等视图数据泄露行为进行追踪溯源；
- e) 应对接入视频传输网的终端进行身份认证；
- f) 应对违规内/外联行为进行及时发现、阻断；
- g) 应通过采集、分析终端数据，发现存在风险和威胁的终端。

8.2 主机安全

主机安全要求，包括但不限于：

- a) 应能检查并调整物理主机操作系统的安全策略和配置；
- b) 应能扫描、分析物理主机上存在的安全漏洞，并提供修复建议；
- c) 应实时监控、识别针对物理主机的入侵和病毒攻击行为并阻断；
- d) 宜能通过裁剪物理主机操作系统内核、禁用不必要的系统服务等方式加固物理主机操作系统。

8.3 云平台安全

云平台安全要求，包括但不限于：

- a) 物理网络安全：应提供物理网络的安全访问控制，通过物理网络的安全威胁检测能力，保护云平台出口的物理网络；
- b) 虚拟化安全：应针对虚拟化漏洞的逃逸攻击进行检测和保护，对云计算资源进行隔离，保护宿主机和虚拟机的安全；
- c) 容器安全：应通过镜像完整性校验、资源安全隔离、文件访问控制、容器漏洞扫描、容器防逃逸、容器加固配置等机制，保障容器资源安全；
- d) 云主机安全：应通过对云主机进行基线核查、漏洞扫描、入侵检测、安全加固、安全迁移、恶意代码查杀，对镜像进行安全加固、漏洞扫描、访问控制、安全备份，提高云主机安全防护能力；
- e) 云网络安全：应对云平台流量进行安全访问控制，构建隔离的虚拟网络环境，针对网络流量进行威胁检测，及时阻断网络中存在的恶意威胁行为；
- f) 云存储安全：宜利用多副本冗余、数据一致性保障、虚拟化隔离等机制保障云存储安全可靠，宜对存储数据进行加密，防止存储数据泄露。

参 考 文 献

- [1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
 - [2] GB/T 28181—2022 公共安全视频监控联网系统信息传输、交换、控制技术要求
 - [3] GB/T 35273—2020 信息安全技术 个人信息安全规范
 - [4] GA/T 1788.1—2021 公安视频图像信息系统安全技术要求 第1部分：通用要求
-