ICS 13.310
CCS A 91

中华人民共和国国家标准

GB/T 46364—2025

公共安全视频监控边界安全交互技术要求

Technical requirements for boundary security interaction system for video surveillance for public security

2025-10-05 发布　　2026-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

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。

本文件由中华人民共和国公安部提出。

本文件由全国安全防范报警系统标准化技术委员会(SAC/TC 100)归口。

本文件起草单位：国家信息中心、公安部第三研究所、杭州领信数科信息技术有限公司、杭州迪普科技股份有限公司、浙江宇视科技有限公司、深信服科技股份有限公司、公安部第一研究所、河南省政务大数据中心、广东省政务服务和数据管理局、浙江省大数据发展管理局、浙江省公安厅、水利部信息中心、云南省云上云中心、安徽省大数据中心、视联动力信息技术股份有限公司、北京天防安全科技有限公司、重庆市质量和标准化研究院、广州大学、北京网御星云信息技术有限公司、吉林省吉林祥云信息技术有限公司、华为技术有限公司、北京欣博电子科技有限公司、烁博信息科技(上海)有限公司、郑州信大捷安信息技术股份有限公司、新华三技术有限公司、招商局检测认证(重庆)有限公司、浙江大华技术股份有限公司、启明星辰信息技术集团股份有限公司、联通(广东)产业互联网有限公司、抚州中科院数据研究院。

本文件主要起草人：程子栋、罗海宁、任飞、樊志杰、杨乐好、张震宇、仇俊杰、吴参毅、赵彬琦、尹萍、宋潇潇、罗奇伟、焦迪、王鹏彪、田之泮、王瑚、夏海元、张潮、袁洪亮、朱典、陈凯、段伟恒、张旻旻、殷丽华、王斌、夏铭、孟凡辉、梁敏学、李志伟、刘相明、万晓兰、吴弘晨、张军昌、李轩、迟明辉、叶卫根、林迁、金梦然、朱雷、周豪、杨潍、周智增。

公共安全视频监控边界安全交互技术要求

1 范围

本文件规定了公共安全视频图像共享交换平台、部门/行业公共安全视频监控平台跨层级联及跨网互联的边界安全交互系统架构、安全等级划分和安全能力要求等。

本文件适用于公共安全视频图像共享交换平台、部门/行业公共安全视频监控平台的边界安全交互系统的规划设计、部署实施、检测验收和运行维护等。

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 2260 中华人民共和国行政区划代码

GB/T 20279—2024 网络安全技术 网络和终端隔离产品技术规范

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

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/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

GB 35114—2017 公共安全视频监控联网信息安全技术要求

GB/T 46356—2025 公共安全视频图像共享交换平台技术要求

GB/T 46361—2025 公共安全视频图像信息联网共享应用总体要求

GB/T 46363—2025 公共安全视频图像信息综合应用服务接口技术要求

3 术语和定义、缩略语

3.1 术语和定义

GB/T 46361—2025、GB/T 25724—2017、GB/T 22239—2019、GB/T 20279—2024 界定的以及下列术语和定义适用于本文件。

3.1.1

横向公共安全视频监控边界安全交互系统 horizontal boundary security interaction system for video surveillance for public security

公共安全视频图像共享交换平台与同级部门或行业公共安全视频监控平台互联时建立信息交互安全机制的软件与硬件。

3.1.2

纵向公共安全视频监控边界安全交互系统 vertical access security interaction system for video surveillance for public security

公共安全视频图像共享交换平台纵向级联时建立信息交互安全机制的软件与硬件。

3.1.3

逻辑隔离　logical isolation

采用技术方法将不同安全等级网络隔离从而避免入侵或信息泄露风险的技术手段，被隔离的两端仍然存在物理上数据通道连线。

3.2　缩略语

下列缩略语适用于本文件。

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

BSIS：边界安全交互系统（Boundary Security Interaction System）

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

ID：身份标识（Identity Document）

MAC：媒体访问控制（Media Access Control）

TCP：传输控制协议（Transmission Control Protocol）

UDP：用户数据报协议（User Datagram Protocol）

SIP：会话初始协议（Session Initiation Protocol）

NAT：网络地址翻译（Network Address Translation）

4　公共安全视频监控边界安全交互架构

4.1　公共安全视频监控边界安全交互总体架构

4.1.1　公共安全视频监控边界安全交互总体架构见图1。

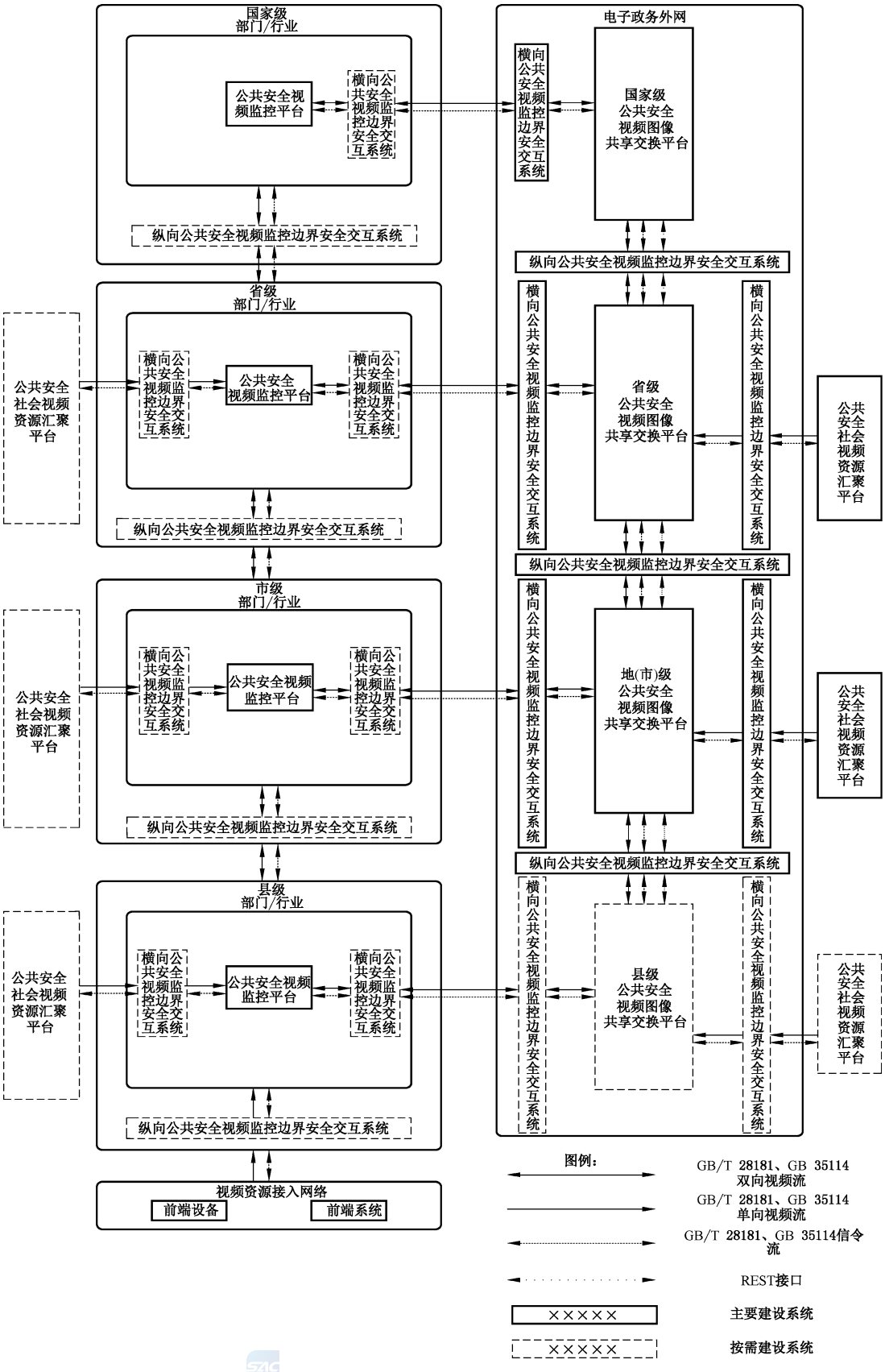

图 1　公共安全视频监控边界安全交互总体架构图

4.1.2 公共安全视频监控边界安全交互系统分为横向公共安全视频监控边界安全交互系统和纵向公共安全视频监控边界安全交互系统。

4.1.3 公共安全视频图像共享交换平台应设置横向公共安全视频监控边界安全交互系统，通过国家电子政务外网对接同级部门或行业公共安全视频监控平台，提供对横向视频交换的安全防护能力。支持对互联网、与互联网逻辑隔离网络、与互联网物理隔离网络等网络之间横向公共安全视频监控边界的安全接入。部门或行业公共安全视频监控平台横向级联宜参照国家电子政务外网安全架构建设横向公共安全视频监控边界安全交互系统。

4.1.4 上级公共安全视频图像共享交换平台应设置纵向公共安全视频监控边界安全交互系统，通过国家电子政务外网纵向级联下级公共安全视频图像共享交换平台，对跨级视频交换数据进行安全防护。部门或行业公共安全视频监控平台纵向级联宜参照国家电子政务外网安全架构建设纵向公共安全视频监控边界安全交互系统。

4.1.5 横向公共安全视频监控边界安全交互系统应符合 GB/T 28181—2022 的规定，宜符合 GB 35114—2017 的规定。

4.1.6 纵向公共安全视频监控边界安全交互系统应符合 GB/T 28181—2022 和 GB/T 46356—2025 中第 6 章的规定，宜符合 GB 35114—2017 的规定。

4.2 横向公共安全视频监控边界安全交互系统功能架构

4.2.1 功能架构图

横向公共安全视频监控边界安全交互系统划分为路由接入区、边界保护区、应用服务区、安全隔离区和安全监测与管理区，系统功能架构见图 2。

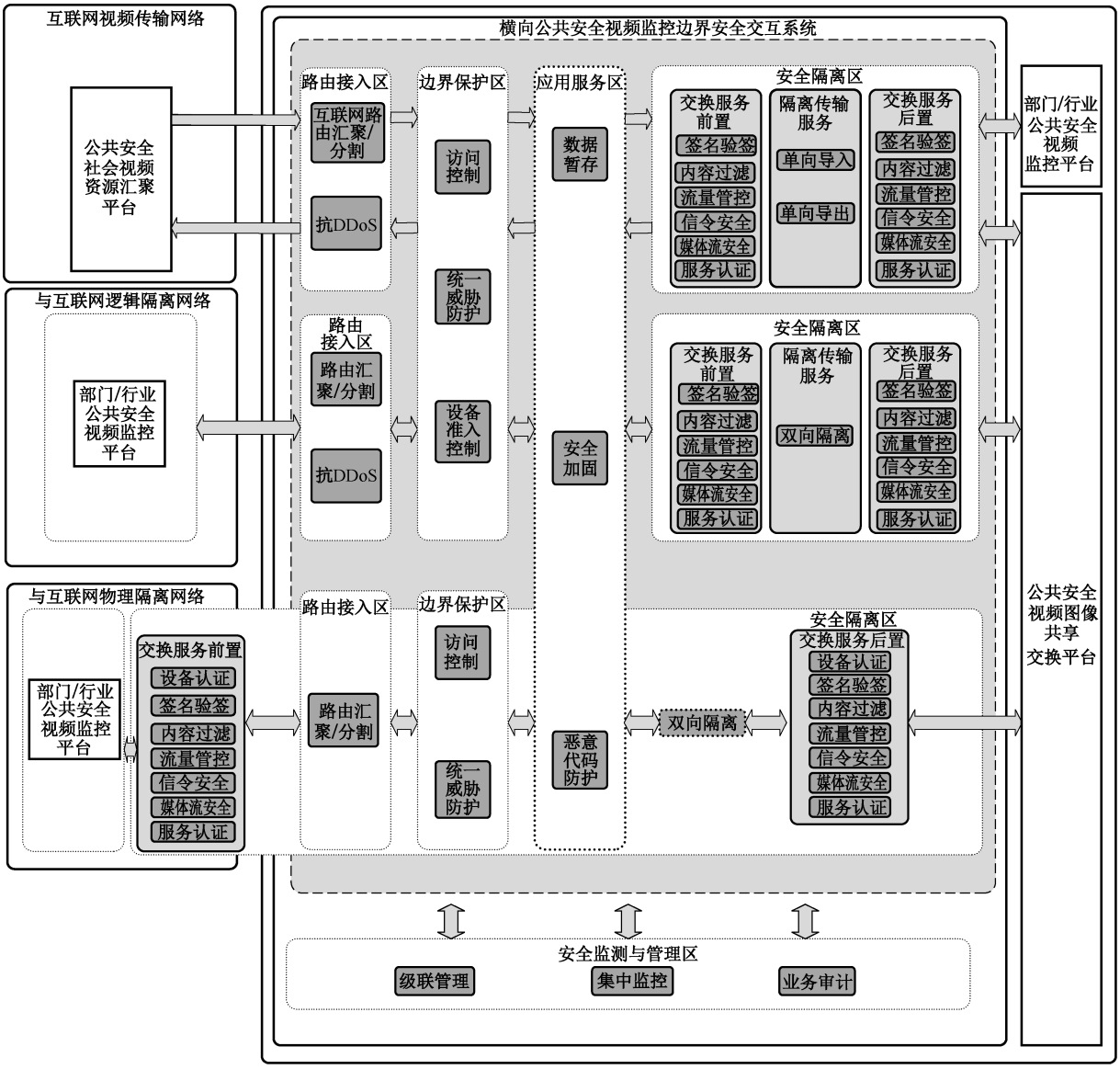

图 2　横向公共安全视频监控边界安全交互系统功能架构图

4.2.2　路由接入区

路由接入区主要实现横向公共安全边界安全交互系统的路由接入，应符合以下安全功能要求：

a）　针对互联网、与互联网逻辑隔离网络的路由接入区，支持路由汇聚与分割、抗 DDoS 防护功能；

b）　针对与互联网物理隔离网络的路由接入区，支持路由汇聚与分割功能。

4.2.3　边界保护区

边界保护区主要实现对横向公共安全边界安全交互系统的边界保护，应符合以下安全功能要求：

a）　针对互联网、与互联网逻辑隔离网络的边界保护区，支持访问控制、统一威胁防护、设备准入控制功能；

b）　针对与互联网物理隔离网络的边界保护区，支持访问控制、统一威胁防护功能。

4.2.4 应用服务区

应用服务区主要处理各类与应用相关的操作，是对外信息发布、信息采集和数据交换的中间区域，应支持数据暂存、安全加固、恶意代码防护等功能。在视频交换业务链路中，可建立应用服务区。

4.2.5 安全隔离区

安全隔离区主要实现公共安全视频图像共享交换平台与互联网、与互联网逻辑隔离网络、与互联网物理隔离网络内的公共安全视频监控平台之间的安全隔离与信息交换，应符合以下安全功能要求：

a) 针对与互联网视频接入和共享的安全隔离区，支持单向导入、单向导出、签名验签、内容过滤、流量管控、服务认证、信令安全、媒体流安全等功能，其中视频流采用单向传输的方式；
b) 针对与互联网逻辑隔离网络视频交换的安全隔离区，支持双向隔离、签名验签、内容过滤、流量管控、服务认证、信令安全、媒体流安全等功能；
c) 针对与互联网物理隔离网络视频交换的安全隔离区，支持设备认证、签名验签、内容过滤、流量管控、服务认证、信令安全、媒体流安全等功能。

4.2.6 安全监测与管理区

安全监测与管理区主要实现横向公共安全视频监控边界安全交互系统的业务审计、集中监控与级联管理等功能，应符合以下安全功能要求：

a) 针对各个安全设备的日志和交换业务日志进行采集；
b) 针对横向公共安全视频监控边界安全交互系统的资产信息、运行状态进行集中监控；
c) 向本级平台传输本级系统的数据。

4.3 纵向公共安全视频监控边界安全交互系统功能架构

4.3.1 功能架构图

纵向公共安全视频监控边界安全交互系统划分为安全防护区和安全监测与管理区，系统功能架构见图 3。

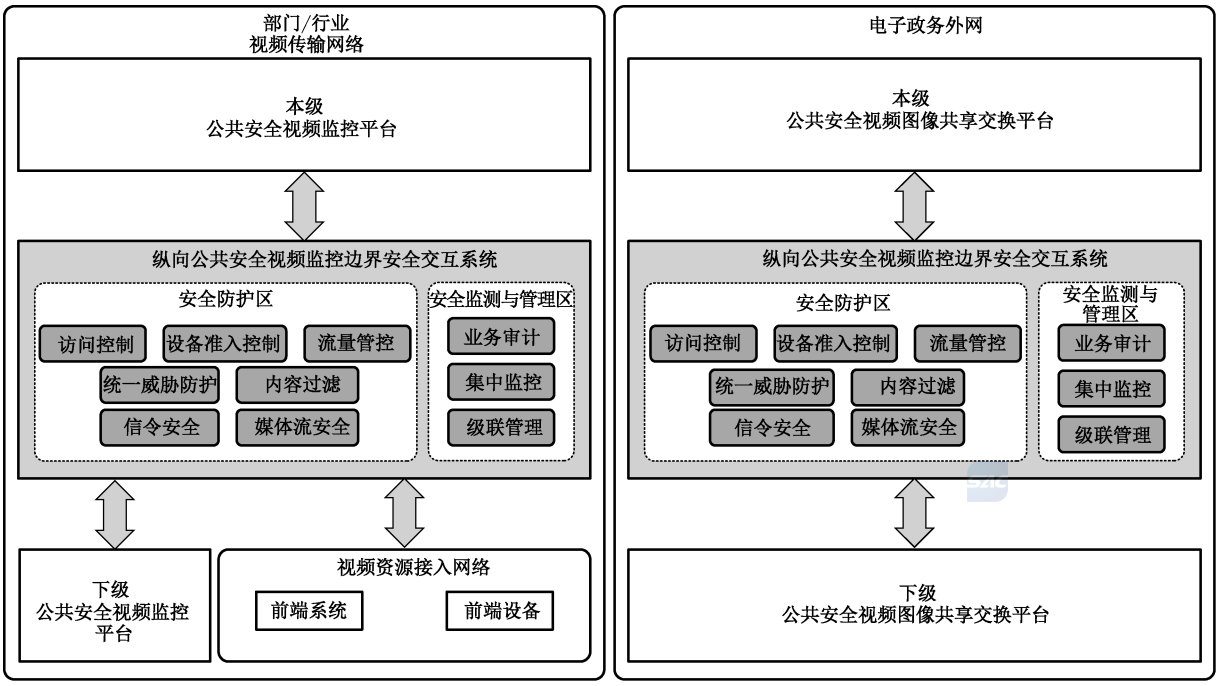

图 3　纵向公共安全视频监控边界安全交互系统功能架构图

4.3.2　安全防护区

安全防护区应支持下级公共安全视频图像共享交换平台与上级公共安全视频图像共享交换平台进行可控的信息交换。对下级公共安全视频图像共享交换平台，安全防护区应支持访问控制、设备准入控制、流量管控、统一威胁防护、内容过滤、信令安全和媒体流安全等功能，应符合 GB/T 28181—2022 和 GB/T 46356—2025 中第 6 章的规定，宜符合 GB 35114—2017 的规定。

4.3.3　安全监测与管理区

安全监测与管理区应支持纵向公共安全视频监控边界安全交互系统的业务审计、集中监控与级联管理等功能，可与横向公共安全视频监控边界安全交互系统共用，应符合以下安全功能要求：

a）　支持对各个安全设备的日志和交换业务日志进行采集；

b）　支持对纵向公共安全视频监控边界安全交互系统的业务审计、集中监控和级联管理功能；

c）　支持向上级平台级联上报本级系统的数据。

5　公共安全视频监控边界安全等级划分

5.1　横向公共安全视频监控边界安全交互系统安全等级

横向公共安全视频监控边界安全交互系统的安全等级由低到高分为基本级、增强级。横向基本级和增强级安全要求见表 1。

表 1　横向基本级和增强级的安全要求

序号	安全要求事项	基本级	增强级
1	访问控制	6.1	6.1
2	设备准入控制	6.2.a)～6.2.e)	6.2
3	统一威胁防护	6.3.a)	6.3
4	抗 DDoS 防护	6.4	6.4
5	安全加固	无	6.5
6	签名验签	6.6.a)	6.6
7	内容过滤	6.7.a)	6.7.a)
8	流量管控	6.8	6.8
9	服务认证	无	6.9
10	信令安全	6.10.a)	6.10
11	媒体流安全	6.11.a)	6.11
12	单向导入/导出	6.12	6.12
13	双向隔离	6.13	6.13
14	业务审计	6.14	6.14
15	集中监控	6.15	6.15
16	级联管理	无	6.16
17	路由汇聚/分割	6.17	6.17

5.2　纵向公共安全视频监控边界安全交互系统安全等级

纵向公共安全视频监控边界安全交互系统的安全等级由低到高分为基本级、增强级。纵向基本级和增强级安全要求见表 2。

表 2　纵向基本级和增强级的安全要求

序号	安全要求事项	基本级	增强级
1	访问控制	6.1	6.1
2	设备准入控制	6.2.a)～6.2.e)	6.2
3	统一威胁防护	6.3	6.3
4	流量管控	6.8	6.8
5	信令安全	6.10.a)	6.10
6	媒体流安全	6.11.a)	6.11
7	内容过滤	6.7	6.7

5.3　安全等级选择原则

安全等级选择遵循以下原则：

a） 含有敏感信息的公共安全视频图像共享交换平台应符合增强级的安全要求；
b） 其他部门/行业公共安全视频监控平台的边界安全交互系统安全等级可参照公共安全视频图像共享交换平台的边界安全交互系统安全等级进行选择。

6 公共安全视频监控边界安全能力

6.1 访问控制

应支持通过基于会话的防护规则实现网络访问控制。对不符合规则的访问，系统应进行拦截并发出告警，告警日志格式应符合附录 A 中表 A.1 的规定。

6.2 设备准入控制

设备准入控制符合以下要求：
a） 应支持对符合 GB/T 28181—2022 规定的协议的设备进行准入控制；
b） 应支持授权设备的 IP/MAC 地址绑定功能；
c） 应支持对接入资产类型、厂商、型号等信息进行准确识别；
d） 设备准入以及设备下线应支持日志发送，日志格式应符合表 A.2 的规定；
e） 应支持对设备私接、替换等行为进行阻断，并发出告警，告警日志格式应符合表 A.5 的规定；
f） 应支持对符合 GB 35114—2017 规定的协议的设备进行准入控制；
g） 宜支持对具有数字证书的设备进行准入控制。

6.3 统一威胁防护

统一威胁防护应符合以下要求：
a） 支持通过检测、阻断、限流、审计报警等防御手段，对蠕虫、后门、木马、间谍软件、Web 攻击等行为进行阻断，并发出告警，告警日志格式应符合表 A.3 的规定；
b） 具备通过恶意代码检查能力，对恶意代码进行高效检测和防御；
c） 支持细粒度分析与标识手段，实现统一威胁防护安全能力；
d） 支持病毒库、协议特征库、入侵特征库的更新。

6.4 抗 DDoS 攻击防护

系统应支持通过指纹特征识别、攻击源认证、智能协议分析等多种手段针对各种带宽型 Flood 攻击和连接型慢速攻击流量进行阻断，并发出告警，告警日志格式应符合表 A.4 的规定。

6.5 安全加固

系统应支持通过补丁修复、安装脚本、调整配置等方式增强系统的健壮性，防范或阻断恶意攻击，提升系统安全性。

6.6 签名验签

签名验签应符合以下要求：
a） 支持对无签名的视频信源进行拦截丢弃，并发出告警，告警日志格式应符合表 A.5 的规定；
b） 对带有签名的视频信源支持签名验签，对签名验签失败的视频信源进行拦截丢弃，并发出告警，告警日志格式符合表 A.5 的规定；
c） 数字证书格式符合 GB 35114—2017 中附录 A 的规定，非对称密钥及对称密钥的管理分别符合 GB 35114—2017 中 6.13 及 6.14 的规定。

6.7 内容过滤

内容过滤应符合以下要求：

a) 支持对指定协议的信令基于安全策略进行内容过滤，对含有敏感信息的信令进行阻断，并发出告警，告警日志格式应符合表 A.5 的规定；

b) 纵向公共安全视频监控边界安全交互系统支持对 API 请求/响应报文数据基于安全策略进行内容过滤，对含有敏感信息的 API 报文数据进行阻断，并发出告警，告警日志格式应符合表 A.6 的规定。

6.8 流量管控

系统应支持对视频流量进行监测，基于规则对流量异常实施控制，并发出告警，告警日志格式应符合表 A.5 的规定。

6.9 服务认证

服务认证符合以下要求：

a) 采用接口服务方式提供时，应支持通过鉴权方式对服务调用方进行身份认证，认证凭证包括数字证书、口令密码；

b) 采用接口服务方式提供时，应支持对服务调用方进行权限控制，确保最小授权；

c) 宜支持对服务提供注册、编目、查询、变更、注销等功能。

6.10 信令安全

信令安全应符合以下要求：

a) 支持对 GB/T 28181—2022、GB 35114—2017 指定协议的信令进行格式检查，对不符合格式的信令进行拦截丢弃，并发出告警，告警日志格式应符合表 A.5 的规定；

b) 支持采用国密加签保证信令协议自身安全，抵御信令被篡改、夹带、窃听等安全风险，并发出告警，告警日志格式应符合表 A.5 的规定。

6.11 媒体流安全

媒体流安全应符合以下要求：

a) 支持对指定协议的视频流按照 GB/T 28181—2022、GB 35114—2017 要求的格式进行检查，对不符合格式视频流进行拦截丢弃，并发出告警，告警日志格式应符合表 A.5 的规定；

b) 支持采用国家商用密码加签加密等手段保证媒体流协议自身安全，抵御媒体流被篡改、夹带、窃听等安全风险，并发出告警，告警日志格式应符合表 A.5 的规定。

6.12 单向导入/导出

单向导入/导出应符合以下要求：

a) 采用物理光通路建立单向传输通道，确保无任何反向通道；

b) 支持对视频流单向传输过程提供完整的日志记录；

c) 单向导入/导出设备支持通过标准管理接口、应用服务或协议，实现与第三方系统的级联与接入管理。

6.13 双向隔离

双向隔离应符合以下要求：

a) 按照 GB/T 20229—2015 的规定建立双向隔离传输通道；
b) 通过摆渡方式连接网络内外两侧，支持通过物理隔离方式断开内外部连接；
c) 支持对视频流双向传输过程提供完整的日志记录；
d) 双向隔离通道设备支持通过管理接口、应用服务或协议，实现与第三方系统的接入与级联管理。

6.14 业务审计

业务审计应符合以下要求：
a) 支持以 Syslog、FTP、API 接口等方式采集业务日志数据；
b) 支持将采集到的所有安全设备日志对外发送。

6.15 集中监控

集中监控应符合以下要求：
a) 支持边界安全交互系统相关的设备资产管理，资产信息包括设备类型、品牌型号、操作系统、版本、端口等信息，并支持资产注册功能，资产注册接口应符合附录 B 中 B.1.2 的规定，消息示例见附录 C 中的 C.1 和 C.5；
b) 支持边界安全交互系统运行状态监控，具备安全交互系统相关设备、链路、业务运行状态的监控能力，设备状态获取接口应符合 B.1.3 的规定，消息示例见 C.2 和 C.5；
c) 支持边界安全交互系统审计数据集中收集和存储，具备告警事件分析、追踪、溯源和处理等能力；
d) 支持通过管理接口、应用服务或协议与安全交互系统的相关安全设备进行对接及接入管理。

6.16 级联管理

系统应支持级联管理，具备管理数据报送、审批、通报等能力。级联注册接口应符合 B.1.4 的规定、级联注销接口应符合 B.1.5 的规定，消息示例见 C.3、C.4 和 C.5。

6.17 路由汇聚/分割

路由汇聚/分割应符合以下要求：
a) 支持静态路由与动态路由两种路由方式实现路由汇聚，动态路由协议如开放最短路径优先(OSPF)等；
b) 路由接入区支持逻辑隔离，通过 NAT 技术实现链路互通，NAT 转换方式包括源 NAT、目的 NAT、一对一 NAT 等。

附 录 A
（规范性）
数据日志格式

A.1 基本要求

边界安全交互系统所使用的设备应至少兼容 Syslog 日志传输方式。

日志数据格式描述方法除了标识符采用蛇形命名方式之外，其他方法应符合 GB/T 46356—2025 中 6.4.1 的规定。

表中约束条件 M＝Mandatory，表示必选字段；O＝Optional，表示可选字段；可选时，字段不含或者值为空。

A.2 访问控制告警日志

访问控制告警日志数据格式应符合表 A.1 的规定。

表 A.1 访问控制告警日志特征属性

序号	名称	标识符	格式	约束条件	备注
1	发送设备 IPv4	device_addr	string(..16)	M	发送设备 IPv4，如“192.168.2.1”
2	设备厂商名称	vendor	string(..32)	M	可识别名称
3	日志类型	log_type	string(..16)	M	如“ACL”
4	日志时间	log_time	string(..32)	M	YYYY-MM-DD HH:MM:ss
5	源 IPv4	src_ipv4	string(..16)	O	IPv4 与 IPv6 地址二选一
6	源 IPv6	src_ipv6	string(..48)	O	
7	源端口	src_port	string(..5)	M	访问请求的源端口，如“5060”
8	目的 IPv4	dst_ipv4	string(..16)	O	IPv4 与 IPv6 地址二选一
9	目的 IPv6	dst_ipv6	string(..48)	O	
10	目的端口	dst_port	string(..5)	M	访问请求的目的端口，如“5060”
11	响应动作	action	string(..16)	M	响应动作 allow/deny
12	协议	protocol	string(..16)	M	取值为 IP、ICMP、TCP、UDP 等
13	策略编号	security_policy_id	string(..64)	O	日志对应的安全策略编号
14	策略名称	security_policy_name	string(..255)	O	策略名称
15	策略描述	description	string(..255)	O	策略描述

A.3 设备准入控制日志

设备准入日志数据格式应符合表 A.2 的规定。

表 A.2　设备准入控制日志特征属性

序号	名称	标识符	格式	约束条件	备注
1	发送设备 IPv4	device_addr	string(..16)	M	发送设备 IP 地址，如“192.168.2.1”
2	设备厂商名称	vendor	string(..32)	M	可识别名称
3	日志类型	log_type	string(..16)	M	如“asset_access”
4	日志时间	log_time	string(..32)	M	YYYY-MM-DD HH:MM:ss
5	资产类型	asset_type	string(..32)	M	如“IPC”
6	资产 ID	asset_id	string(..32)	M	如“34020000002000000131”
7	资产 IPv4 地址	asset_ipv4	string(..16)	M	IPv4 与 IPv6 地址二选一
8	资产 IPv6 地址	asset_ipv6	string(..48)	M	
9	准入动作	access_action	int32	M	1——准入成功； 2——资产下线； 3——准入失败

A.4　统一威胁防护告警日志

统一威胁防护告警日志数据格式应符合表 A.3 的规定。

表 A.3　统一威胁防护告警日志

序号	名称	标识符	格式	约束条件	备注
1	发送设备 IPv4	device_addr	string(..16)	M	发送设备 IPv4，如“192.168.2.1”
2	设备厂商名称	vendor	string(..32)	M	—
3	日志类型	log_type	string(..16)	M	“IPS”
4	发生时间	log_time	string(..32)	M	2021-04-21 18:01:39
5	响应动作	action	string(..10)	M	0——deny； 1——allow
6	事件主类型	event_type	string(..32)	O	事件一级类型，漏洞利用类；其他
7	事件子类型	sub_event_type	string(..32)	O	事件二级类型
8	事件名称	event_name	string(..255)	O	攻击事件名称，如“(123140913) Microsoft Windows NetBIOS 共享访问控制”
9	厂商事件 ID	event_id	string(..12)	O	123140913
10	威胁等级	severity	int32	O	—
11	源 IPv4	src_ipv4	string(..16)	O	IPv4 与 IPv6 地址二选一
12	源 IPv6	src_ipv6	string(..48)	O	
13	源端口	src_port	string(..5)	M	访问请求的源端口，如“13092”

表 A.3　统一威胁防护告警日志（续）

序号	名称	标识符	格式	约束条件	备注
14	目的 IPv4	dst_ipv4	string(..16)	O	IPv4 与 IPv6 地址二选一
15	目的 IPv6	dst_ipv6	string(..48)	O	
16	目的端口	dst_port	string(..5)	M	访问请求的目的端口，如“443”
17	CVE 编号	cve	string(..255)	O	如“CVE-2014-6277”“CVE-2014-6278”
18	报文负载内容	payload	string(..4096)	O	—
19	日志严重级别	priority	int32	M	日志等级，严重性 0-7
20	协议	protocol	string(..32)	M	网络连接协议

A.5　抗 DDoS 防护告警日志

抗 DDoS 防护告警日志数据格式应符合表 A.4 的规定。

表 A.4　抗 DDoS 防护告警日志

编号	名称	标识符	格式	约束条件	备注
1	发送设备 IPv4	device_ipv4	string(..16)	M	发送设备 IPv4
2	设备厂商名称	vendor	string(..32)	M	可识别名称
3	日志类型	log_type	string(..16)	M	“DDoS”
4	事件发生时间	log_time	string(..32)	M	YYYY-MM-DD HH:MM:ss
5	日志严重级别	priority	int32	M	日志等级，严重性 0～7
6	目的 IPv4	dst_ipv4	string(..16)	O	IPv4 与 IPv6 地址二选一
7	目的 IPv6	dst_ipv6	string(..48)	O	
8	目的端口	dst_port	string(..5)	M	日志的目的端口
9	开始时间	start_time	string(..32)	M	异常流量记录开始时间
10	结束时间	end_time	string(..32)	M	异常流量记录结束时间
11	总字节流量	total_byte_flow	int32	M	时间间隔内攻击流量的总字节数
12	峰值字节流量	peak_byte_flow	int32	M	攻击开始后流量的峰值字节数
13	总包流量	total_package_flow	int32	O	时间间隔内攻击流量的总包数
14	峰值包流量	peak_package_flow	int32	O	攻击开始后流量的峰值包数
15	攻击类型	attack_type	string(..200)	M	攻击所属类型
16	丢弃流量	discard_flow	string(..16)	M	丢弃的流量统计

A.6　通用告警日志

签名验签、内容过滤、信令安全、媒体流以及流量管控日志应符合表 A.5 的规定。

表 A.5　通用告警日志

序号	名称	标识符	格式	约束条件	说明
1	发送设备 IPv4	device_addr	string(..16)	否	发送设备 IPv4，如“192.168.2.1”
2	设备厂商名称	vendor	string(..32)	M	可识别名称
3	日志类型	log_type	string(..16)	M	未认证设备：“Unauth_ERROR” 设备被替换：“Replace_ERROR” 内容过滤：“SCI” 信令安全：“SIP_ERROR” 媒体流：“MEDIA_ERROR” 签名验签：“SIGNA_ERROR”
4	日志时间	log_time	string(..32)	M	YYYY-MM-DD HH:MM:ss
5	发送端 ID	src_id	string(..32)	M	如“34020000002000000131”，发送端设备 SIP-ID
6	接收端 ID	dst_id	string(..32)	O	如“34020000002000000131”，接收端设备 SIP-ID
7	源 IPv4	src_ipv4	string(..16)	M	IPv4 与 IPv6 地址二选一
8	源 IPv6	src_ipv6	string(..48)	M	
9	源端口	src_port	string(..5)	M	访问请求的源端口，如“5060”
10	目的 IPv4	dst_ipv4	string(..16)	M	IPv4 与 IPv6 地址二选一
11	目的 IPv6	dst_ipv6	string(..48)	M	
12	目的端口	dst_port	string(..5)	M	访问请求的目的端口，如“5060”
13	协议	protocol	string(..16)	M	取值为 TCP、UDP、ICMP
14	内容描述	description	string(..256)	O	敏感信息内容、错误信息、错误媒体流内容

附 录 B
（规范性）
接口定义

B.1 基本接口

B.1.1 通则

边界安全交互系统提供的接口基于 REST，接口协议应符合 GB/T 46363—2025 中 4.2 的规定，REST 与 RESTful 服务规则应符合 GB/T 46363—2025 中附录 A 的规定。

边界安全交互系统提供系统内资产设备向系统资产注册服务、系统向系统内资产设备查询设备状态服务、下级系统向上级系统注册和注销服务。基本接口对照关系应符合表 B.1 的规定。

表中约束条件 M＝Mandatory，表示必选字段；O＝Optional，表示可选字段；C＝Conditional，表示特定条件下必选，其他可选。可选时，字段不含或者值为空。

表 B.1 基本接口对照关系

序号	功能	对应接口消息章节	执行方法	说明
1	资产设备注册	B.1.2	POST	边界安全交互系统内资产设备主动向系统进行资产注册
2	资产设备状态查询	B.1.3	GET	边界安全交互系统向具体某个资产设备查询设备状态
3	系统注册	B.1.4	POST	下级边界安全交互系统主动向上级系统注册
4	系统注销	B.1.5	POST	下级边界安全交互系统主动向上级系统注销

B.1.2 资产设备注册

资产设备注册接口应符合表 B.2 的规定。

表 B.2 资产注册接口

URI	/BSIS/AssetRegister		
功能	资产设备主动向边界安全交互系统进行资产注册		
方法	查询字符串	请求消息体	响应消息体
POST	无	＜AssertRegister＞	＜Response＞
注释	1.＜AssertRegister＞应符合 B.2.1 的规定，示例见 C.1； 2.＜Response＞应符合 B.2.5 的规定，示例见 C.5		

B.1.3 资产设备状态查询

资产设备状态查询接口应符合表 B.3 的规定。

表 B.3　资产设备状态查询接口

URI	/BSIS/DeviceStates/＜device_ip＞		
功能	边界安全交互系统查询其他设备的状态		
方法	查询字符串	请求消息体	响应消息体
GET	无	无	＜Response＞
注释	1. 参数＜device_ip＞为资产设备的 IPv4/IPv6 地址； 2. ＜DeviceStates＞应符合 B.2.2 的规定，示例见 C.2； 3. ＜Response＞应符合 B.2.5 的规定，示例见 C.5		

B.1.4　系统注册

边界安全交互系统注册接口应符合表 B.4 的规定。

表 B.4　系统注册接口

URI	/BSIS/Register		
功能	下级边界安全交互系统向上级边界安全交互系统主动注册		
方法	查询字符串	请求消息体	响应消息体
POST	无	＜Register＞	＜Response＞
注释	1. ＜Register＞应符合 B.2.3 的规定，示例见 C.3； 2. ＜Response＞应符合 B.2.5 的规定，示例见 C.5		

B.1.5　系统注销

边界安全交互系统注销接口应符合表 B.5 的规定。

表 B.5　系统注销接口

URI	/BSIS/UnRegisters		
功能	下级边界安全交互系统上上级边界安全交互系统主动注销		
方法	查询字符串	请求消息体	响应消息体
POST	无	＜UnRegister＞	＜Response＞
注释	1. ＜UnRegister＞应符合 B.2.4 的规定，示例见 C.4； 2. ＜Response＞应符合 B.2.5 的规定，示例见 C.5		

B.2　接口信息对象

B.2.1　资产注册信息对象

资产注册信息对象(＜AssertRegister＞)应符合表 B.6 的规定。

表 B.6　资产注册信息对象

序号	名称	标识符	格式	约束条件	说明
1	资产 IPv4 格式	asset_IPv4	string(..15)	M	—
2	资产 IPv6 地址	asset_IPv6	string(..39)	O	—
3	资产 MAC 地址	asset_mac	string(..17)	M	—
4	资产类型	asset_type	string(..32)	M	—
5	资产厂商	asset_factory	string(..100)	M	—
6	资产型号	asset_model	string(..100)	M	—

B.2.2　设备状态信息对象

设备状态信息对象(＜DeviceState＞)应符合表 B.7 的规定。

表 B.7　设备状态信息对象

序号	名称	标识符	格式	约束条件	说明
1	CPU 利用	device_cpu	float	O	如 25.25％表示为 25.25
2	设备运行状态	device_runState	string(..2)	O	值为“OK”或“NO”
3	内存利用率	device_ram	float	O	如 30.12％表示为 30.12
4	硬盘利用率	device_hardDisk	float	O	如 34.34％表示为 34.34
5	链路运行状态	device_link	string(..2)	O	值为“OK”或“NO”，NO 代表设备有异常丢包

B.2.3　系统注册信息对象

系统注册信息对象(＜Register＞)应符合表 B.8 的内容。

表 B.8　系统注册信息对象属性表

序号	名称	标识符	格式	约束条件	说明
1	下级边界安全交互系统标识	platform_id	string(20)	M	应符合 GB/T 28181—2022 中附录 E 的规定
2	下级监控平台 IPv4 地址	platfrom_IPv4	string(..15)	M	—
3	下级级监控平台 IPv6 地址	platform_IPv6	string(..48)	O	—
4	下级级平台描述	platfrom_des	string(..256)	M	—
5	下级级平台所在行政区域	platfrom_area	string(6)	M	采用 GB/T 2260 中的六位数字代码
6	下级级平台管理机构	platform_unit	string(..256)	M	—

B.2.4 系统注销信息对象

系统注销信息对象(＜UnRegister＞)应符合表 B.9 的内容。

表 B.9 系统注销信息对象属性表

序号	名称	标识符	格式	约束条件	说明
1	下级边界安全交互系统标识	platform_id	string(20)	M	应符合 GB/T 28181—2022 中附录 E 的规定
2	本机监控平台 IPv4 地址	platfrom_IPv4	string(..15)	M	—
3	本机监控平台 IPv6 地址	platfrom_IPv6	string(..39)	O	—
4	上级监管平台 ID	s_platform_id	string(20)	M	应符合 GB/T 28181—2022 中附录 E 的规定

B.2.5 应答信息对象

应答信息对象(＜Response＞)应符合表 B.10 的内容。

表 B.10 应答信息对象

序号	名称	标识符	格式	约束条件	说明
1	状态码	status_code	int32	M	—
2	应答数据	data	＜D＞	M	—
2.1	应答消息	D. msg	string(..256)	M	success——成功； fail——失败
2.2	上级监管平台 ID	D. s_platform_id	string(20)	C	下级边界安全交互系统向上级边界安全交互系统注销时必选； 应符合 GB/T 28181—2022 中附录 E 的规定
2.3	设备状态	D. device_state	＜DeviceStatus＞	C	查询设备状态应答时必选，＜DeviceStatus＞应符合 B.2.2的规定

附 录 C
（资料性）
消息实体

C.1 资产设备注册信息对象

资产设备注册信息对象见示例。

示例：

```
{
    "data":{
        "asset_IPv4":"192.168.1.1",
        "asset_IPv6":"",
        "asset_MAC":"11::22:33:44:55:66",
        "asset_type":"IPC",
        "asset_factory":"厂商简称",
        "asset_model ":" IPC6126-WDL-F "
    }
}
```

C.2 资产设备状态信息对象

资产设备状态信息对象见示例。

示例：

```
{
    "data":{
        "device_cpu":"25.25",
        "device_runState":"OK",
        "device_ram":"30.12",
        "device_hDisk":"34.34",
        "device_link":"OK"
    }
}
```

C.3 系统注册信息对象

系统注册信息对象见示例。

示例：

```
{
    "Data": {
        " platform_id ": "34020000002000000131",
        " platfrom_IPv4": "192.168.2.1",
        " platfrom_IPv6": "",
        " platfrom_des ": "××××集中监控平台",
        " platfrom_area ": "××省××市××县",
        " platfrom_unit ": "×××大数据局"
    }
}
```

C.4 系统注销信息对象

系统注销信息对象见示例。

示例：

```
{
    "data": {
        " platform_id ": "34020000002000000131",
        " platfrom_IPv4": "192.168.2.1",
        " platfrom_IPv6": "",
        " s_platform_id ": "34020000002000000131"
    }
}
```

C.5 应答信息对象

应答信息对象见示例 1、示例 2、示例 3。

示例 1：

```
{
    "status_code": 200,
    "data": {
        "msg": "success"
    }
}
```

示例 2：

```
{
    "status_code": 200,
    "data": {
        "msg": "success",
        " s_platform_id ": "34020000002000000131"
    }
}
```

示例 3：

```
{
    "status_code"：200，
    "data"：{
        "msg"："success"，
        "device_state"：{
            "device_cpu"："25.25"，
            "device_runState"："OK"，
            "device_ram"："30.12"，
            "device_hDisk"："34.34"，
            "device_link"："OK"
        }
    }
}
```