ICS 45.020
CCS S73

团　　体　　标　　准

T/VSTR 027—2025

铁路视频安全隔离和信息交换网闸技术要求

Technical requirements for video security isolation and information exchange gateway of railway

2025-06-04 发布　　2025-07-01 实施

中关村轨道交通视频与安全产业技术联盟　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
3.1 1
3.2 1
3.3 1
4 缩略语 2
5 系统结构 3
6 功能要求 3
6.1 主要功能 3
6.2 安全防护 4
6.3 隔离交换 4
6.4 安全管理 6
7 性能要求 7
7.1 时延要求 7
7.2 视频并发输出路数要求 7
7.3 数据同步速率要求 7
7.4 可靠性要求 7
8 接口要求 7
8.1 隔离网闸与铁路综合视频监控系统的接口 7
8.2 隔离网闸与公安等外部专网的接口 7
8.3 隔离网闸与互联网相关系统的接口 8
9 时间同步要求 8
10 设备技术要求 8
11 运行环境要求 8
11.1 环境适应性 8
11.2 设备电源 8
11.3 电磁兼容 8
12 标志、包装、运输及贮存要求 9
12.1 标志 9
12.2 包装 9
12.3 运输 9
12.4 贮存 9
附　录　A （规范性） 云化服务要求 10
A.1 云化部署原则 10
A.2 云化平台功能要求 10
附　录　B （资料性） 典型铁路视频安全隔离和信息交换网闸应用 11
参考文献 12

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。

本文件由中关村轨道交通视频与安全产业技术联盟提出并归口。

本文件起草单位：北京浩瀚深度信息技术股份有限公司、北京全路通信信号研究设计院集团有限公司、北京铁路公安局、中国铁路济南局集团有限公司、河南蓝信科技有限责任公司、启明星辰信息技术集团股份有限公司、奇安信科技集团股份有限公司。

本文件主要起草人： 张跃、石蕊、洪波、许辉、吴昊、杨雪飞、戴亮、崔圣青、徐天涛、丁泉、陈文波、卢庆、刘少凯、李现强、胡京砾、刘新龙。

铁路视频安全隔离和信息交换网闸技术要求

1 范围

本文件规定了铁路视频安全隔离和信息交换网闸（以下简称“隔离网闸”）的系统结构、功能要求、性能要求、接口要求、时间同步要求、设备技术要求、运行环境要求、标志、包装、运输及贮存要求。

本文件适用于铁路综合视频监控系统隔离网闸的产品设计和制造，其他视频监控系统可参照执行。

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 8702 电磁环境控制限值

GB/T 9813.3-2017 计算机通用规范 第3部分：服务器

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 24338.5-2018 轨道交通第4部分：信号和通信设备的发射与抗扰度试验

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

GA/T 1400.4-2017 公安视频图像信息应用系统 第4部分：接口协议要求

YD/T 1099-2013 以太网交换机技术要求

3 术语和定义

GB/T 20279界定的以及下列术语和定义适用于本文件。

3.1

安全隔离 security isolation

通过物理或逻辑手段，将不同网络或同一网络不同安全域的信息系统进行有效的分隔，防止未经授权的访问、数据泄露和恶意攻击在不同区域之间传播。

3.2

信息交换 information exchange

数据在不同的信息实体之间进行交互的过程。

3.3

网闸 gap

指位于两个不同安全域之间,采用协议转换和信息摆渡技术实现网络隔离,只有安全策略允许传输的信息通过。

[来源：GB/T 20279-2024，3.9]

4 缩略语

下列缩略语适用于本文件。

AAC：高级音频编码（Advanced Audio Coding）
API：应用程序编程接口（Application Programming Interface）
CSV：逗号分隔值（Comma-Separated Values）
FTP：文件传输协议（File Transfer Protocol）
JPG：JPEG格式（Joint Photographic Experts Group）
MCX：关键任务通信服务（Mission Critical X-Service）
MTBF：平均故障间隔时间（Mean Time Between Failure）
NTP：网络时间协议(Network Time Protocol)
PNG：便携式网络图形（Portable Network Graphics）
PTZ：全方位移动及镜头变倍、变焦控制（Pan/Tilt/Zoom）
SAS： 串行连接SCSI接口（Serial Attached SCSI）
SATA：串行ATA(Serial Advanced Technology Attachment)
SDP：会话描述协议(Session Description Protocol)
SIP：会话初始协议(Session Initiation Protocol)
SMB：服务器信息块（Server Message Block）
TCP/IP：传输控制协议/因特网协议（Transmission Control Protocol/Internet Protocol）
XML：可扩展标记语言（eXtensible Markup Language）

5 系统结构

隔离网闸采用物理隔离、数据时分切换摆渡、协议转换等技术，实现跨域、跨网、跨协议系统间的安全隔离和信息交换。可向铁路综合视频监控系统提供路外系统授权后的视频、数据的安全接入；也可向路外系统提供铁路综合视频监控系统授权后的视频、数据的安全对接。路外系统包括公安等外部专网的视频监控系统和数据服务系统，以及互联网的视频监控系统和数据服务系统。公安等外部专网包括公安视频传输网、公安信息网以及平安城市、雪亮工程、护路办等，其中，根据公安业务需求，视频业务接入公安视频传输网的视频监控系统，人脸图像比对和违停抓拍等业务接入公安信息网的铁路公安数据服务系统。隔离网闸的系统结构及互联示意见图1。

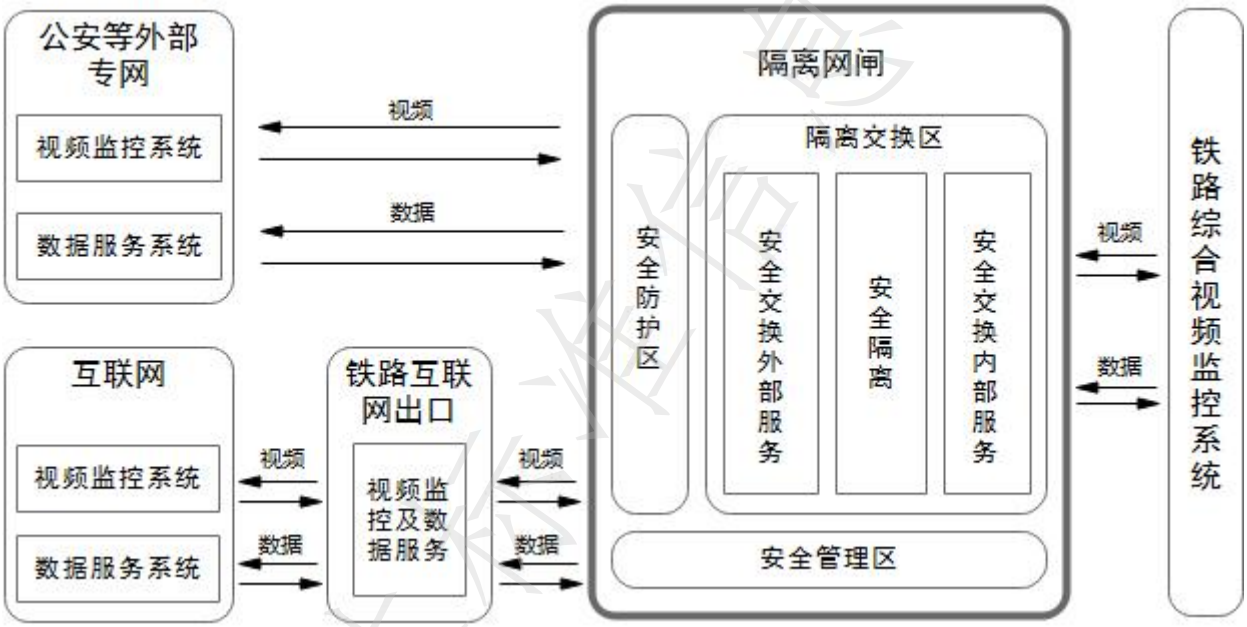

图 1 隔离网闸的系统结构及互联示意图

隔离网闸可部署在铁路综合视频监控系统的区域节点边界处，与公安等外部专网连接，或通过铁路互联网出口与互联网连接；还可部署在铁路综合视频监控系统的接入节点边界处，与公安等外部专网连接。隔离网闸宜采用云化部署，按附录A的要求部署。

6 功能要求

6.1 主要功能

隔离网闸具有安全防护、隔离交换、安全管理等功能，安全防护功能包括访问控制、设备准入、身份认证以及威胁防护；隔离交换功能包括安全交换外部服务、安全隔离和安全交换内部服务；安全管理功能包括配置管理、集中监控、运维管理以及信息报送。其中，为保障交换行为可追踪和交换记录的安全性，由安全交换内部服务提供交换审计功能。隔离网闸功能框图见图2。

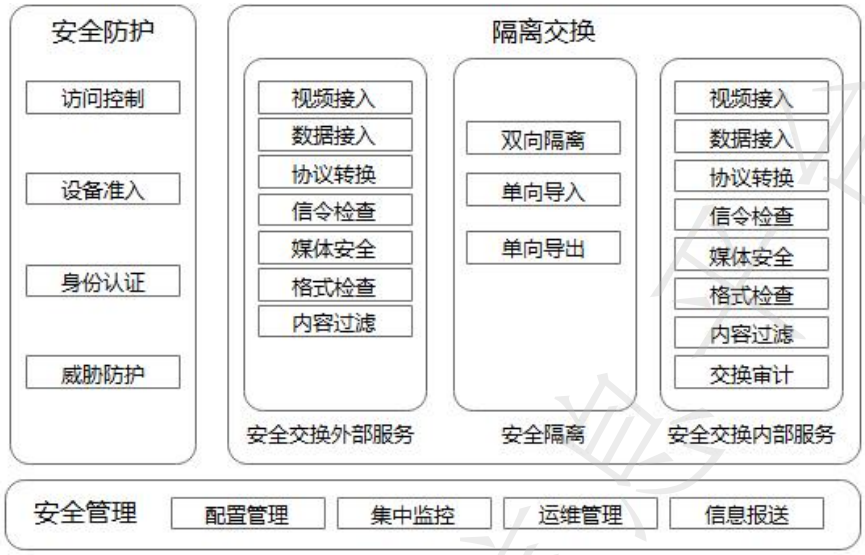

图 2　隔离网闸功能框图

6.2　安全防护

6.2.1　访问控制

访问控制应符合下列规定：

a)　支持网络应用和服务访问已授权的资源；

b)　根据最小权限原则，仅能访问执行任务所必需的资源。

6.2.2　设备准入

设备准入应符合下列规定：

a)　支持接入设备注册，注册信息包括设备 IP/MAC、设备 ID、设备属性等；

b)　支持对已注册设备提供资产编目、档案信息维护、设备更换以及设备下线等功能；

c)　支持向相关系统实时推送设备准入信息。

6.2.3　身份认证

身份认证应符合下列规定：

a)　支持采用口令和密码技术组合的鉴别技术对用户进行身份鉴别；

b)　支持对登录隔离网闸的用户进行身份标识和鉴别，身份标识具有唯一性；

c)　用户口令长度至少 8 位，至少包含数字、大小写英文字母、字符，初次登录时，强制修改厂商默认口令；

d)　支持账户口令定期更换，并设置提醒期限和失效期限。

6.2.4　威胁防护

威胁防护应符合下列规定：

a)　支持对网络流量进行采集和分析，发现攻击行为并进行阻断；

b)　支持对攻击行为进行引诱，分析攻击特征及攻击手法并进行反追踪。

6.3　隔离交换

6.3.1 视频接入

视频接入应符合下列规定：

a) 支持获取视频监控系统的视频资源，包括符合 GB 35114-2017 要求的视频资源；

b) 支持按照指定视频资源进行图像的实时浏览调用，支持多用户对同一图像资源的同时浏览调用；

c) 支持按照指定视频资源指定时间段的历史视音频文件进行检索、远程回放调用以及下载。

6.3.2 数据接入

数据接入应符合下列规定：

a) 支持接入关系型数据库、非关系型数据库以及异构数据库；

b) 支持接入 XML、CSV、TXT、JPG、PNG 等文件格式，可自定义接入文件格式；

c) 支持以 API 接口的形式提供服务，具体协议包括 SOAP、RESTful API 方式的接口访问。

6.3.3 协议转换

协议转换应符合下列规定：

a) 支持对外部专网侧符合GB/T 28181规定的协议转换；

b) 支持对铁路侧符合铁路综合视频监控系统的协议转换。

6.3.4 信令检查

信令检查应符合下列规定：

a) 支持对视频控制信令类型、格式及内容等信息进行预注册；

b) 支持对传输协议和数据封装格式进行解析，支持对 GB 35114-2017 规定的信令进行独立解析，对不符合注册要求的内容进行阻断和报警。

6.3.5 媒体安全

媒体安全应符合下列规定：

a) 支持对不同视频设备的媒体传输协议和数据封装格式进行解析，支持对 GB 35114-2017 规定的 C 级视频设备的视频进行独立处理；

b) 支持识别实时流媒体数据是否被黑客入侵、窃取、篡改或者病毒攻击。

6.3.6 格式检查

格式检查应符合下列规定：

a) 支持对文件数据进行格式检查，对不符合预定义格式的文件进行拦截丢弃，记录日志并报警；

b) 支持对数据库进行格式检查，对不符合预定义格式的数据库数据进行拦截丢弃，记录日志并报警；

c) 支持对 API 报文进行格式检查，对不符合预定义格式的 API 报文进行拦截丢弃，记录日志并报警；

d) 支持对指定协议的信令和数据流进行格式检查，对不符合预定义格式的信令和数据流进行拦截丢弃，记录日志并报警；

e) 支持定期更新检查机制。

6.3.7 内容过滤

内容过滤应符合下列规定：

a） 支持对含有铁路行业敏感信息的文件进行拦截丢弃，记录日志并报警；

b） 支持对含有铁路行业敏感信息的数据库数据进行拦截丢弃，记录日志并报警；

c） 支持对含有铁路行业敏感信息的 API 报文进行拦截丢弃，记录日志并报警；

d） 支持对含有铁路行业敏感信息的信令和数据流进行拦截丢弃，记录日志并报警。

6.3.8 双向隔离

双向隔离应符合下列规定：

a）支持通过协议隔离方式断开内部 TCP/IP 连接，中断协议，剥离流量通信协议，还原为应用层信息；

b）支持根据预定义安全策略对协议头进行剥离和再生；

c）支持对数据摆渡传输过程记录日志。

6.3.9 单向导入、导出

单向导入、导出应符合下列规定：

a）支持在导入、导出及同向多个接入对象间采用传输隔离技术；

b）支持根据预定义的安全策略对协议头进行剥离及再生，进行物理单向导入、导出；

c）支持对导入、导出数据传输过程记录日志。

6.3.10 交换审计

交换审计应符合下列规定：

a） 支持对整个数据交换行为的完整审计，包括数据来源、发生时间、交换目标、交换内容、是否得到了授权、是否遵守交换规则、交换行为是否成功、不成功进行了几次尝试、交换结束时间等；

b） 支持主键追踪功能，发现违规记录并进行预警；

c） 支持文件和审计日志的变更查询。

6.4 安全管理

6.4.1 配置管理

配置管理应符合下列规定：

a）支持用户对业务资源进行参数许可配置；

b）支持用户对业务资源进行权限配置，可标注自定义属性；

c）支持对业务资源进行传输配置以及下发安全策略，并根据业务类型，配置不同的网络传输通道；

d）支持对业务资源状态进行控制，如禁用、恢复等。

6.4.2 集中监控

集中监控应符合下列规定：

a）支持对隔离网闸设备运行状态进行监控及异常告警；

b）支持对隔离网闸业务运行状态进行监控及异常告警；

c）支持隔离网闸流量和流速异常告警；

d）支持进行集中统计分析和可视化展示。

6.4.3 运维管理

运维管理应符合下列规定：

a）支持 telnet、https、SNMP 等运维协议，支持单点登录和密码托管；

b）支持根据不同运维场景分配用户角色权限，应支持对运维操作进行录像；

c）支持记录登陆、角色授权、访问会话等日志信息，以及对运维操作录像进行回放。

6.4.4 信息报送

信息报送应符合下列规定：

a）支持对隔离网闸运行状态信息进行定时上报；

b）支持对隔离网闸接入业务进行实时上报；

c）支持对隔离网闸使用单位信息、配置管理日志以及日常用户操作日志进行定时上报。

7 性能要求

7.1 时延要求

时延应符合下列规定：

a）视频调用经过隔离网闸的时延不应大于 100 ms；

b）数据传输经过隔离网闸的时延不应大于 80ms。

7.2 视频并发输出路数要求

视频并发输出路数应符合下列规定：

a）在每路平均码率为 2 Mbit/s 时，单套隔离网闸应支持同时并发输出路数不应小于 256 路；

b）在每路平均码率为 4 Mbit/s 时，单套隔离网闸应支持同时并发输出路数不应小于 128 路；

c）在每路平均码率为 8 Mbit/s 时，单套隔离网闸应支持同时并发输出路数不应小于 64 路。

7.3 数据同步速率要求

数据同步速率应符合下列规定：

a）文件吞吐量不应小于 600 Mbit/s；

b）数据库同步速率不应小于 5000 条/s。

7.4 可靠性要求

可靠性要求应符合下列规定：

a）断电发生时，系统自动保存正在记录的信息，系统自动启动，自动启动时间不应大于 10 min；

b）隔离网闸系统的 MTBF 不应小于 5×10^4 h。

8 接口要求

8.1 隔离网闸与铁路综合视频监控系统的接口

隔离网闸与铁路综合视频监控系统的接口应符合铁路综合视频监控系统相关接口要求。

8.2 隔离网闸与公安等外部专网的接口

隔离网闸与公安视频传输网相关系统的接口应符合GB/T 28181-2022中的第9章和GB 35114-2017规定的协议接口。应用要求见附录B;

隔离网闸与公安信息网相关系统的接口应符合FTP协议、SMB协议、GA/T 1400.4-2017协议、SOAP接口及RESTful API接口。应用要求见附录B;

隔离网闸与平安城市、雪亮工程、护路办等外部专网相关系统的接口应符合GB/T 28181-2022中的第9章和GB 35114-2017规定的协议接口、SOAP接口、RESTful API接口。应用要求见附录B。

8.3 隔离网闸与互联网相关系统的接口

隔离网闸与互联网相关系统的接口应符合GB/T 28181-2022中的第9章和GB 35114-2017规定的协议接口、FTP协议。应用要求见附录B。

9 时间同步要求

隔离网闸应支持NTP协议，具有自动同步功能。

10 设备技术要求

设备技术要求应符合下列规定：

a）CPU 不应低于 6 核 12 线程；

b）内存不应低于 32GB；

c）网卡不应低于 4 个 GE 口；

d）系统盘 SSD 单盘容量不应低于 240 GB 或 SAS 单盘容量不应低于 500 GB；

e）支持适配国密加密芯片；

f）隔离交换应支持电子开关控制或以光介质传输；

g）支持远程管理、远程配置以及远程启停机；

h）支持 SNMP 协议，采用其他协议时应开放接口；

i）具备冗余电源。

11 运行环境要求

11.1 环境适应性

室内设备在下列环境下应正常工作：

a）工作温度：0 ℃～45 ℃；

b）相对湿度：10 %～95 %不凝结；

11.2 设备电源

设备采用交流220 V供电或采用直流-48 V供电，并应符合下列规定：

a）隔离网闸设备电源应符合 GB/T 9813.3-2017 中 4.5 的规定；

b）网络设备电源应符合 YD/T 1099-2013 中 13.1 的规定。

11.3 电磁兼容

设备电磁兼容性应符合下列规定：

a）系统设备电磁兼容性要求符合 GB/T 24338.5-2018 的规定；

b）系统中与操作人员直接靠近或接触的设备的对外电磁辐射功率应符合 GB 8702 的规定。

12 标志、包装、运输及贮存要求

12.1 标志

12.1.1 设备标志

在设备明显的位置装有铭牌，铭牌应清晰，易于识别，不易磨损。
铭牌应标明下列信息：
a）产品名称、型号；
b）出厂编号；
c）制造日期；
d）制造商名称。

12.1.2 外包装标志

设备包装箱外应采用不易褪色涂料，清晰地标出下列信息：
a）正面：产品名称、型号、数量、重量、外包装尺寸，到站，收货、发货单位名称和地址等；
b）侧面：“易碎物品”、“向上”、“怕雨”及发站、制造商名称等。

12.2 包装

包装应符合下列规定：
a）设备包装应能防止其正常运输过程中遭受损坏；
b）随机应提供产品的用户手册、产品合格证、装箱单、专用安装工具。

12.3 运输

设备在搬运过程中，应轻拿轻放，避免摔碰，不应无包装运输。

12.4 贮存

设备贮存条件应符合下列规定：
a）贮存处应有防雨、雪和水浸的措施，不应在露天存放；
b）贮存处应远离高温、高热、高湿的环境；
c）贮存处不应有有毒或腐蚀性气体，不应与有毒或带有腐蚀性的酸、碱、盐等物品一起存放。

附 录 A
（规范性）
云化服务要求

A.1 云化部署原则

隔离网闸云化部署应符合下列规定：

a) 安全防护区的安全能力包含访问控制、设备准入、身份认证及威胁防护。其中，访问控制用于控制访问安全策略，应采用物理设备，其他能力宜采用云化部署；

b) 隔离交换区的安全能力包含安全交换外部服务、安全隔离及安全交换内部服务。其中，安全隔离内的双向隔离和单向导入、导出应采用物理设备，其他能力宜采用云化部署；

c) 安全管理区的管理能力包含集中监控、资源管理、信息报送及运维管理，宜采用云化部署；

隔离网闸云化部署示意图见图A.1。

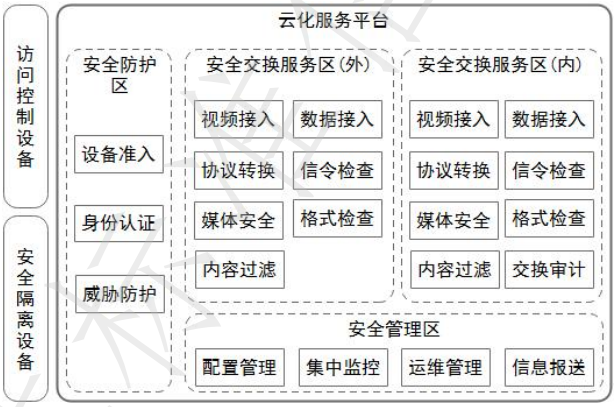

图 A.1 隔离网闸云化部署示意图

A.2 云化平台功能要求

弹性自动化扩缩容、故障恢复及灾备要求应符合下列规定：

a) 要求平台具备自动化扩缩容能力，以应对不同负载情况下的资源需求变化；

b) 需要能够实时监测各项资源的利用率，包括CPU、内存、存储和网络带宽等指标，根据监测到的数据预测未来负载变化；

c) 支持定义自动化扩缩容的触发条件和规则，例如CPU利用率超过80%持续10 min，或者请求响应时间超过阈值等；系统应能够根据预设的触发条件自动扩展计算资源，包括增加虚拟机实例、容器实例或其他计算资源，且需要考虑资源分配、负载均衡和高可用性，确保新加入的资源能够有效地参与负载处理。

a) 要求单台服务器故障不会中断业务的正常运行，计算资源可以自动调度到其它机器上执行，且数据可正常访问；

b) 要求云存储支持EC校验或者多副本容错方式，多节点或磁盘故障不会造成数据丢失和不一致，且可在后台自动进行数据的恢复；

c) 要求具备完备的故障发现和告警监控工具；

d) 要求在故障恢复过程中不影响业务的正常运行，且在故障恢复后自动进行资源的重新调配。

附 录 B
（资料性）
典型铁路视频安全隔离和信息交换网闸应用

路外系统经隔离网闸接入铁路综合视频监控系统，不同接入对象的业务类型、交换形式、隔离措施及参考依据见表B.1。

表 B.1 部署场景典型应用要求

接入对象	业务类型	业务交换形式	交换通道类型	参考依据
公安视频传输网	视频交换	双向交换	双向或单向	GB 35114-2017 公共安全视频监控联网信息安全技术要求；GA/T 1788.1 公安视频图像信息系统安全技术要求 第 1 部分：通用要求；GA/T 1788.2 公安视频图像信息系统安全技术要求 第 2 部分：前端设备；GA/T 1788.3 公安视频图像信息系统安全技术要求 第 3 部分：安全交互；GA/T 1788.4 公安视频图像信息系统安全技术要求 第 4 部分：安全管理平台。
公安信息网	数据交换	单向导出	单向	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；GA/T 1400.2-2017 公安视频图像信息应用系统 第 2 部分：应用平台技术要求；GA/T 1400.3-2017 公安视频图像信息应用系统 第 3 部分：数据库技术要求；GA/T 1400.4-2017 公安视频图像信息应用系统 第 4 部分：接口协议要求；遵守公安部相关安全规范。
	接口服务	双向交换	双向或单向	
平安城市、雪亮工程	视频交换	单向导出	单向	GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求；Q/CR 783.4 铁路通信网络安全技术要求 第 4 部分：综合视频监控系统；GA/T 1788.1 公安视频图像信息系统安全技术要求 第 1 部分：通用要求 ；GA/T 1788.2 公安视频图像信息系统安全技术要求 第 2 部分：前端设备；GA/T 1788.3 公安视频图像信息系统安全技术要求 第 3 部分：安全交互；GA/T 1788.4 公安视频图像信息系统安全技术要求 第 4 部分：安全管理平台。
	数据交换	单向导出	单向	
	接口服务	双向交换	双向或单向	
护路办	视频交换	双向交换	双向或单向	
	接口服务	双向交换	双向或单向	
互联网	视频交换	双向交换	单向	GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求；Q/CR 783.4 铁路通信网络安全技术要求第 4 部分：综合视频监控系统。
	数据交换	双向交换	单向	

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] 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] GA/T 1400.2-2017 公安视频图像信息应用系统 第2部分：应用平台技术要求
[4] GA/T 1400.3-2017 公安视频图像信息应用系统 第3部分：数据库技术要求
[5] GA/T 1788.1 公安视频图像信息系统安全技术要求 第1部分：通用要求
[6] GA/T 1788.2 公安视频图像信息系统安全技术要求 第2部分：前端设备
[7] GA/T 1788.3 公安视频图像信息系统安全技术要求 第3部分：安全交互
[8] GA/T 1788.4 公安视频图像信息系统安全技术要求 第4部分：安全管理平台
[9] Q/CR 575-2022 铁路综合视频监控系统技术规范
[10] Q/CR 783.1 铁路通信网络安全技术要求 总体技术要求
[11] Q/CR 783.4 铁路通信网络安全技术要求第4部分：综合视频监控系统