ICS 13.310
CCS A 91

团 体 标 准

T/CDAFXH 2—2026

公共安全防范系统智慧运维技术规范

2026－01－23 发布　　2026－01－23 实施

成都安全防范协会　　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。

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。

本文件由成都安全防范协会提出并归口。

本文件起草单位：成都市公安信息技术研究所、四川格瑞特科技有限公司、成都安全防范协会、成都市标准化研究院、厦门立林科技有限公司、成都合盛智联科技有限公司、成都宜泊信息科技有限公司、四川省人民医院、四川音乐学院 、中海物业管理有限公司成都分公司、四川司法警官职业学院、中国电信股份有限公司成都高新区分公司、中建西南院数字城市科技（四川）有限公司、四川省通信产业服务有限公司成都市分公司、四川省工业设备安装集团有限公司、四川华睿智讯科技有限公司、成都久信信息技术股份有限公司。

本文件主要起草人：赵敬千、尹砚、马骄、苟铭、赵靖、杨明奎、唐晶晶、蒋丽琼、陈旭、宋文杰、胡承志、孙尚东、张笑难、陈超、李道军、邓建勋、欧洋、余林俊、余训锋、胡江涛、敖天翔、宋金友、钟文豪、陈勇、文旭飞、陈积堉、贾林、宋常青、刘文勇、周雪梅。

引　言

公共安全防范系统是维护社会安全稳定的重要基础设施。随着安防系统规模不断扩大与技术快速迭代，传统运维模式在及时性、精准度和效率方面面临严峻挑战，难以满足全生命周期精细化管理的需求。智慧运维是一种通过引入人工智能、大数据、物联网等先进技术，实现从被动响应到主动预测、从单点处置到系统优化的转变的有效方法，是提升安防系统可靠性、保障其持续高效运行的重要手段和方式。

本文件旨在为公共安全防范系统的智慧运维的建设及既有安防系统的提质增效与智能化改造提供技术路径。通过智能感知、数据分析与AI决策等技术的应用，实现设备状态实时监测、故障智能诊断、工单自动流转及运维质量科学评价的全流程闭环管理；同时有效降低系统运维成本，及时发现和处置安全问题，提升安防系统的整体效能。

公共安全防范系统智慧运维技术规范

1 范围

本文件规定了公共安全防范系统智慧运维的总体要求、系统架构、硬件配置、性能要求、功能要求及安全保障要求。

本文件适用于既有、新建、改建、扩建和城市更新中的公共安全防范系统。

注：本文件中公共安全防范系统简称安防系统。

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 19582 基于Modbus协议的工业自动化网络规范
GB/T 22239 信息安全技术网络安全等级保护基本要求
GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求
GB/T 28827.2 信息技术服务 运行维护 第2部分：交付规范
GB/T 28181 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 39786 信息安全技术商用密码应用安全性评估指南
GB/T 45087 人工智能服务器系统性能测试方法
GB/T 46358 公共安全视频图像信息联网应用运维管理平台技术要求
GB 50174 数据中心设计规范
GB 50339 智能建筑工程质量验收规范
GB 50348 安全防范工程技术标准
GB 55029 安全防范工程通用规范
CJ/T 188 户用计量仪表数据传输技术条件
DL/T 645 多功能电能表通信规约
GA/T 1781 公共安全社会视频资源安全联网设备技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

公共安全防范系统 public security prevention system

运用实体防护、电子防护等技术构成的防范系统，通常包括视频监控、入侵和紧急报警、出入口控制、楼寓对讲、停车库（场）管理、电子巡查等子系统。

[来源：GB 50348—2018，有修改]

3.2

智慧运维 intelligent operation and maintenance

依托人工智能、大数据、云计算、物联网技术，实现公共安全防范系统设备状态监测、智能巡检、故障诊断、故障处置、订单管理、城市更新的提质改造及服务评价全流程智能化管理的运维模式，核心特征为“数据驱动、AI赋能、合规管控”。

3.3

智慧运维管理平台 intelligent operation and maintenance management platform

包括数据采集、监控、分析、运维流程管理、决策支持等功能，用于对各类设备、系统及业务进行综合运维管控的信息化平台。

3.4

智能网关 intelligent gateway

通过采集和汇聚前端感知设备的数据，将各类协议数据转换为标准协议，从而实现与上级平台互联的设备。

3.5

时序数据 time series data

按时间顺序采集的系统运行指标数据，包括设备状态、监控参数、告警信息等。

4 缩略语

AI：人工智能（Artificial Intelligence）
PoE：以太网供电（Power over Ethernet）
SLA：服务级别协议（Service Level Agreement）
VLAN：虚拟局域网（Virtual Local Area Network）
AR:增强现实(Augmented Reality)

5 总体要求

5.1 智慧运维应实现全流程闭环、全数据驱动、全场景智能与全维度协同，符合 GB 55029、GB 50348 及 GB 50339 的相关要求。

5.2 应采用智慧运维技术措施，利用人工智能、大数据、云计算等先进技术，对各类设备和系统进行监控、分析预测和告警处置。

5.3 应遵循 GB/T 28181 与 GA/T 1781 的要求，构建开放协同、可独立部署、维护及升级的安防系统架构，支持跨层级、跨部门的数据共享与业务协同，具备纵向级联与横向互联功能，提升资源利用效率，避免重复建设。

6 系统架构

6.1 应采用“感知层-传输层-支撑层-应用层”的分层逻辑架构。

6.2 应实现“感知层设备异常、支撑层 AI 预警、应用层工单自动生成、支撑层智能调度、应用层处置进度跟踪”的端到端流程闭环，具体逻辑如下：

a) 感知层应由前端接入终端设备、物联感知设备、边缘数据采集设备或具有基础 AI 功能的相关设备进行故障或异常状态检测及分析；
b) 传输层应通过网络交换设备、智能网关采用加密协议实现各类数据的传输；
c) 支撑层应提供 AI 算力支撑，包括知识与数据库；
d) 应用层应整合包括运维总览可视化展示、智能巡检、工单管理、资源管理、智能问答以及监管评价功能的标准化、智能化应用。

6.3 智慧运维管理平台、数据传输与控制所使用的传输协议、接口协议及传输格式应符合相关国家标准与行业标准的规定。平台架构如图 1 所示。

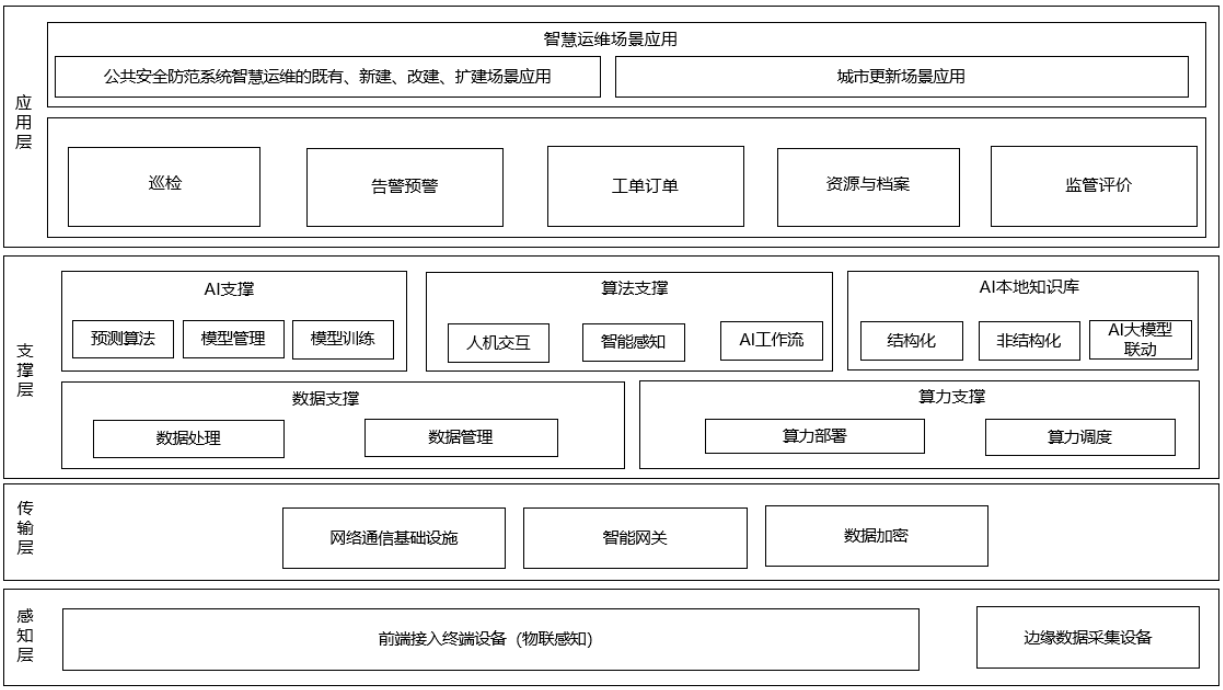

图1　系统智慧运维架构

7　硬件配置

7.1　配置原则

安防系统硬件设备在选型与配置时应遵循稳定可靠、智能适配、扩展兼容及安全可控的原则并满足以下要求：

a)　可靠性：核心硬件设备包括服务器、存储设备、网络交换机等，宜采用冗余设计。部署于户外的设备应具备相应的防雷、防水、防尘及抗老化能力，防护等级应满足安装环境要求；

b)　智能化：硬件设备宜内置状态传感器，能够实时采集电压、电流、温度、运行时长等关键运行数据，并支持远程状态监控与管理，具备 AI 辅助故障诊断能力；

c)　兼容性：硬件设备应符合安防行业及物联网相关标准协议。配置时应考虑未来设备扩展接入的能力，预留相应的接口与资源。在既有安防系统改造中，应优先选用或升级可兼容既有设备协议的硬件；

d)　安全性：软硬件选型应符合关键信息基础设施安全保护和安全可控原则，硬件设备应支持在全链路数据传输中采用符合国家相关规定的算法进行加密，同时设备管理应具备权限管控机制，对关键操作进行留痕。

7.2　感知层设备

7.2.1　感知层设备包括但不限于前端接入终端设备（视频监控摄像机、人脸抓拍摄像机、车辆识别摄像机、紧急求助设备、巡更设备、人脸识别门禁等）、物联网感知设备及边缘数据采集及运算设备。

7.2.2　前端接入终端设备应通过 GB/T 28181 规定的协议获取视频图像信息采集设备的视频流与在线状态，并支持通过该协议实现相关设备的管理与调用。

7.2.3　物联网感知设备应具备多协议转换能力，符合 GB/T 28181 及 GB/T 46358 的要求。

7.2.4　边缘数据采集设备应具备不少于 3 路 RS485 通讯接口和不少于 1 路 RJ45 网络接口，支持 RS485 与 LAN 连接，同时支持通过 LAN 接口或 4G 以及上无线网络进行本地或远程的配置与维护管理。

7.2.5　边缘数据采集设备应支持 Modbus TCP、OPC、HTTP 等通讯协议，并符合 GB/T 19582、DL/T 645 及 CJ/T 188 等相关标准的要求。

7.3　传输层设备

7.3.1 网络通信基础设备

7.3.1.1 核心交换机应采用冗余设计，背板带宽、包转发率等关键性能指标宜根据所承载的业务流量进行核算并留有余量。
7.3.1.2 接入交换机宜选择支持 PoE 供电、具备 VLAN 划分功能的可网管型交换机。

7.3.2 智能网关

7.3.2.1 应支持多协议转换，具备数据传输加密功能，能对采集的时序数据进行过滤、聚合和预处理。
7.3.2.2 网关处理器核心数宜不少于 4 核，主频应不低于 1.5GHz，宜支持轻量级 AI 推理模型部署。

8 性能要求

安防系统的智慧运维性能要求应符合表1。

表1 安防系统智慧运维性能要求

序号	具体内容	要求值	应用场景
1	基础算力要求	见附录 A	1)视频质量监测，包括丢帧检测、完整性验证、分辨率与帧率分析； 2)设备故障预测； 3)异常检测； 4)日志智能分析；
2	运维日志留存	≥3 年	-
3	视频质量自动化检测覆盖率	≥99%	-
4	故障识别率	≥98%	1)预防性维护； 2)运维效率评价。
5	故障识别准确率	≥95%	1)故障处置； 2)技术性能评价。
6	与授时服务器的时间进行一致性检测	安防系统内的时间偏差应不大于 5s,安防系统时钟与北京时间偏差应不大于 30s。	时钟检测

9 功能要求

9.1 业务功能

9.1.1 巡检

9.1.1.1 应具备系统预警、计划、执行、处置、反馈等主动式巡检功能。
9.1.1.2 应具备获取感知层设备、传输层网络设备、支撑层设备以及应用层运行数据的能力。
9.1.1.3 巡检完成后应自动生成包含覆盖率、异常率等信息的报告。

9.1.2 告警、预警管理

9.1.2.1 应实行告警分级管理，并与故障处置流程绑定，支持告警的合并、抑制与关联分析。
9.1.2.2 应具备基于设备运行数据的预警能力，能够预测设备健康度与故障风险，并触发预防性维护流程。

9.1.3 工单、订单管理

9.1.3.1 应实现运维工单与服务订单的统一管理。安防系统应支持服务请求的自动创建与分类，并根据预设规则自动分派工单，支持人工转派、升级与多级审批。
9.1.3.2 服务请求应关联相关设备资产、合同与历史记录，全过程应可跟踪、记录并上传佐证材料。
9.1.3.3 应实现服务环节的成本核算与全流程归档，并支持按多条件对记录进行检索与统计分析。

9.1.4 资源与档案管理

9.1.4.1 应对合同、备件、运维项目及用户权限等运维资源进行数字化与全生命周期管理，并建立权责清晰的多级用户体系。
9.1.4.2 应建立集中、完整的电子档案库。为所有设备建立全生命周期档案，并自动归档全部工单、订单及相关记录。

9.1.5 质量评价

9.1.5.1 应能基于巡检、故障处理、设备资产、工单、订单等数据自动生成合规性评价报告与服务态势分析报告。
9.1.5.2 应能基于 SLA 等指标，自动对项目整体、运维团队、人员及供应商进行月度、季度、年度等多维度考评。
9.1.5.3 应支持自定义配置多维度分析，按需自动生成、导出与推送月度、季度、年度运维报告、合规性报告及巡检报告等。

9.2 AI 赋能

9.2.1 巡检分析

9.2.1.1 可利用计算机视觉等 AI 技术、算法，对摄像机在线/遮挡/噪点状态、交换机状态、存储设备工作状态及视频质量（缺失、偏色等）进行自动分析与故障识别。
9.2.1.2 在有毒有害、高温高压等特殊或高危环境下，应支持采用巡检机器人或无人机完成自动化巡检任务。
9.2.1.3 应支持通过 AR 眼镜或移动终端，为现场人工巡检叠加设备参数与维修指引等增强信息。
9.2.1.4 应对巡检数据进行分析，支持多维度可视化展示，并辅助生成巡检报告。

9.2.2 智能问答

9.2.2.1 应提供基于中文自然语言交互的智能化信息检索与对话支持，覆盖故障咨询、政策查询、指令下达、方案与技术指引、故障诊断与提质升级建议等多种场景。
9.2.2.2 应具备多轮对话与模糊查询能力，可输出文本、图表、链接或自动生成工单等结构化结果。

9.2.3 多模态 AI 大模型管理

9.2.3.1 用于运维的 AI 大模型训练的训练数据应纳入故障案例库，支持模型的持续迭代优化、在线升级以及 AI 大模型的本地化部署。
9.2.3.2 应实时监控模型的运行状态、性能指标（如诊断准确率、响应时间），当性能低于设定阈值时自动告警。

10 安全保障

10.1 核心服务器、网络及存储设备的建设与运行环境应符合 GB 50174 的要求，具备防火、防水、防电磁干扰、防雷、温湿度控制、门禁管理和视频监控等基础物理防护措施。
10.2 安防系统网络架构与防护措施应符合 GB/T 22239 中规定的第三级或以上网络安全等级保护技术要求。
10.3 密码技术的应用应符合 GB/T 39786 中第三级或以上的商用密码应用安全性评估要求。

11 更新维护

11.1 基本要求

11.1.1 更新维护应涵盖问题发现、智能诊断、故障定位、自动处置及人工核验等环节，形成人机协同、流程闭环的运维保障机制。
11.1.2 应建立完整的更新维护管理制度，明确更新范围、审批流程、实施方案（含回滚预案）、测试验证及记录归档要求。
11.1.3 更新维护前应对系统性能、业务连续性与数据安全进行评估；更新后应开展功能验证、性能测

试及安全检测。

11.2 硬件更新

11.2.1 硬件更新原则应符合本规范 7.1 的要求，优先选用兼容既有系统协议、符合行业最新标准的设备。

11.2.2 前端感知设备固件更新应符合设备制造厂标准及 GA/T 1788 等相关要求，更新前应备份配置。

11.2.3 网络传输层设备宜定期进行硬件健康状态检测，出现部件老化、性能下降或故障时及时更新替换，冗余设备更新应采用先备后主的方式进行。

11.3 软件更新

软件更新应包括系统补丁、功能模块升级、AI模型迭代等，符合GB/T 22239及GB/T 39786的相关要求。

11.4 服务确认

11.4.1 更新维护完成后，应按 GB/T 28827.1 及 GB/T 28827.2 的要求开展服务确认，确认工作应包括：

a) 核心功能完整性与业务流程连续性验证；
b) 系统性能指标核查；
c) 安全防护措施有效性检测；
d) 涉及工程整改的更新服务，其验收应按 GB 55029、GB 50348 及 GB 50339 等相关标准执行。

11.4.2 服务确认过程应形成书面报告，相关记录纳入运维档案管理。

附 录 A
（资料性）
基础算力配置

安防系统中 AI 基础算力的配置应与其承担的智能分析任务规模及场景复杂度相匹配，实际配置时应以满足第 8 章性能指标及具体功能要求为准，算力配置参考表 A.1。

表A.1 基础算力配置表

序号	复杂度描述	AI算力需求（FP16）	支撑能力
1	轻量AI任务	8～20TFLOPS	单路或少量视频流实时分析。
2	并行处理多类AI任务	20～50TFLOPS	支持多路视频实时分析、多种故障模型并行处理。
3	大规模、多模态AI模型	80～150TFLOPS或集群化部署	支持高并发、低延迟的智能分析与预测，满足大型场所全局管控需求。

参 考 文 献

[1]《公共安全视频图像信息系统管理条例》（国务院令第799号）
[2] GB/T 21741 住宅小区安全防范系统通用技术要求
[3] GB/T 28827.3 信息技术服务 运行维护 第3部分：应急响应规范
[4] GB/T 31000 社会治安综合治理基础数据规范
[5] GB/T 32581 入侵和紧急报警系统技术要求
[6] GB 35114 公共安全视频监控联网信息安全技术要求
[7] GB/T 36951 网络安全技术 物联网感知终端应用安全技术要求
[8] GB 37300 公共安全重点区域视频图像信息采集规范
[9] GB/T 45402 智慧城市 城市智能中枢 参考架构
[10] GB 55024 建筑电气与智能化通用规范
[11] JGJ/T 454 智能建筑工程资料监测标准
[12] GA/T 1043 道路交通技术监控设备运行维护规范
[13] GA/T 1081 安全防范系统维护保养规范