

SZSD

数 字 山 东 工 程 标 准

SZSD 0025—2024

5G+智慧社区安防系统建设要求

Guidelines for the Construction of 5G+Smart Community Security System

2024 - 04 - 15 发布

2024 - 06 - 01 实施

目 次

1	范围	1
2	规范性引用文件	1
3	术语和定义	1
4	5G+智慧社区安防系统框架	2
5	基础设施层	3
5.1	物联感知设施	3
5.2	通信基础设施	3
5.3	计算和存储设施	3
6	系统层	3
6.1	IoT 物联接入	3
6.1.1	设备管理	3
6.1.2	规则引擎	3
6.1.3	流媒体服务	3
6.1.4	物模型	3
6.1.5	安全管理	4
6.1.6	场景联动	4
6.2	数据服务	4
6.3	数据库	4
6.4	应用支撑	4
7	应用层	4
7.1	社区人员管理	4
7.1.1	人员出入管理	4
7.1.2	周界防范	4
7.1.3	重点区域人员管理	4
7.1.4	特殊人群服务	4
7.2	社区车辆管理	5
7.2.1	车辆出入管理	5
7.2.2	车辆轨迹跟踪	5
7.2.3	停车场管理	5
7.3	社区事物管理	5
7.3.1	社区房屋管理	5
7.3.2	社区消防管理	5
7.3.3	防盗监控和报警	5
7.3.4	高空抛物管理	6
7.3.5	电梯安全	6
7.3.6	消防通道占用监管	6
7.3.7	充电桩安全监管	6
7.4	其他管理	6

7.4.1	报警管理	6
7.4.2	智能巡更	7
7.4.3	应急管理	7
7.4.4	社区网格化治理	7
7.5	安防综合服务	7
8	安全保障	7
8.1	网络安全	7
8.2	数据安全	7
8.3	物理安全	7
8.4	应用安全	8
8.5	信息安全	8
9	运行维护	8

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并归口。

本文件起草单位：中电信数智科技有限公司山东分公司、中国移动通信集团山东有限公司、联通（山东）产业互联网有限公司、利津县大数据中心、海纳云物联科技有限公司、中国移动通信集团设计院有限公司山东分公司、智耘（山东）城市运营科技有限公司、山东津跃智能科技有限公司、华高数字科技有限公司、山东高速建设管理集团、山东省新型智慧城市发展促进会。

本文件主要起草人：刘洋、田经师、吴文国、张泉、王玮、李海超、王巍、钟宸、宋文豪、张庆海、贾军超、李同国、赵树青、梁峰、朱铭果、周腾腾、房有策、薄纯光、张凯丽、丁磊、韩雪、杨林。

5G+智慧社区安防系统建设要求

1 范围

本文件规定了结合5G技术的智慧社区安防系统的建设框架、建设内容及要求等。
本文件适用于指导利用5G等新一代信息技术进行智慧社区安防系统建设工作。

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 22239-2019 网络安全等级保护基本要求
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/T 29245-2012 信息安全技术 政府部门信息安全管理基本要求
GB/T 37024-2018 信息安全技术 物联网感知层网关安全技术要求
GB/T 37300-2018 公共安全重点区域视频图像信息采集规范
GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧社区 smart community

指充分应用大数据、云计算、人工智能等信息技术手段，整合社区各类服务资源，打造基于信息化、智能化管理与服务的社区治理新形态。

3.2

物联网 internet of things; IoT

通过感知设备，按照约定协议，连接物、人、系统和信息资源，实现对物理和虚拟世界的信息进行处理并作出反应的智能服务系统。

注：物即物理实体。

[来源：GB/T 33745-2017 2.1.1]

3.3

数字孪生 digital twin

由物理资产、虚拟镜像和用户界面组成的混合模型。

[来源：GB/T 41723-2022 3.2]

3.4

时空基准 spatiotemporal datum

时间和地理空间维度上的基本参照依据和度量的起算数据。

[来源：GB/T 35776-2017 3.3]

3.5

网络安全/网络空间安全 cyber security

在网络空间中对信息保密性、完整性和可用性的保持。

[来源：GB/T 36643-2018 3.1]

3.6

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。
[来源：GB/T 37988-2019 3.1]

3.7

应用安全 application security

智慧社区安防系统平台上提供的完成智慧安防应用功能的所有应用软件及相关组件的安全。
[来源：GB/T 34080.4-2021 3.1有修改]

4 5G+智慧社区安防系统框架

5G+智慧社区安防系统建设参考框架主要包括基础设施层、系统层、应用层、安全保障、运行维护五部分，框架见图1。

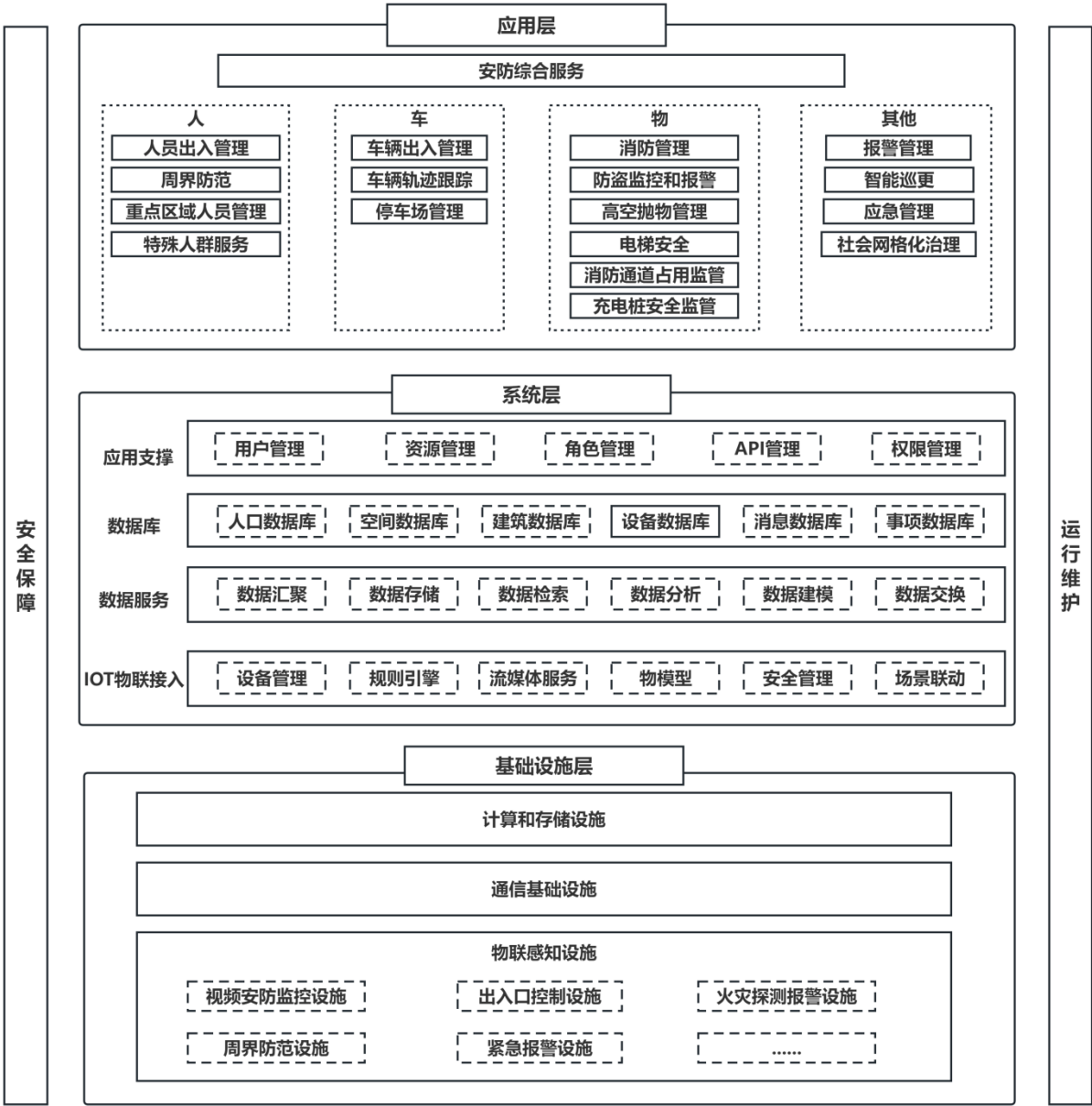


图1 5G+智慧社区安防系统框架图

5 基础设施层

5.1 物联感知设施

物联感知设施包括视频安防监控设施、出入口控制设施、火灾探测报警设施、周界防范设施、紧急报警设施等，设施要求除应符合GB/T 42455.1-2023要求外，还应符合下列要求：

- a) 在消防重点区域应配置具有火灾探测和报警功能的视频监控系统；
- b) 在建筑物内部应配备电动车非法进入监测系统；
- c) 应具备安全措施，包括加密通信、身份验证、数据保护等，以确保数据安全；
- d) 应具备可扩展性，能够支持更多设备的接入和管理，同时可以方便地升级和扩展功能；
- e) 应与其他设备和系统互联互通，实现数据的共享和交互；
- f) 应具备简单易用的操作界面，能够方便地进行设备管理和控制；
- g) 应具备低功耗的特点，以延长设备的使用寿命和降低能源消耗；
- h) 应具备合理的成本；
- i) 应具备智能化的特点，能够自动地执行任务和进行数据分析，以提高设备的效率和智能化水平；
- j) 应具备可定制性，能够根据用户的需求和场景进行定制和调整；
- k) 物联网平台提供端到端安全认证机制，支持对接入平台的设备进行鉴权、接收设备上报的数据。

5.2 通信基础设施

智慧社区安防通信基础设施除符合GB/T 42455.1-2023要求外，还应符合下列要求：

- a) 支持各种网络接入模式；
- b) 应实现 5G 信号全覆盖，或为 5G 信号全覆盖预留条件；
- c) 物联网应满足社区安防系统中涉及的安防物联设备完全接入；
- d) 物联网中各种摄像头、传感器等物联设备应尽量以非侵入式和零拉线方式完成部署；
- e) 物联网建设应使用开放的弹性架构，能实现后期网络规模的无限扩展；
- f) 宜在条件允许时，搭建卫星通信设施或布置 6G 通信技术网络。

5.3 计算和存储设施

计算和存储设施应符合GB/T 42455.1-2023中6.3计算和存储设施的相关要求。

6 系统层

6.1 IoT 物联接入

智慧社区安防系统IoT物联接入包含但不限于设备管理、规则引擎、流媒体服务、物模型、安全管理、场景联动等内容。

6.1.1 设备管理

除满足GB/T 28181-2022 中7控制要求、GB/T 37300-2018中6采集设备要求中的相关要求，还应具备设备注册管理、设备接入管理、设备状态监控、设备升级管理等功能。

6.1.2 规则引擎

应具备用户自定义功能，基于条件、事件、时间等因素触发各类规则。

6.1.3 流媒体服务

除满足GB/T 28181-2022 中第5章、第6章、第9章的相关要求，还应支持H.264、H.265等标准视频编解码协议，应支持HTTP、RTMP等视频流传输协议。

6.1.4 物模型

应对设备的物理属性、功能属性、数据类型、传感器信息、执行器信息、运行状态等进行详细描述。

6.1.5 安全管理

除满足GB/T 28181-2022 中第8章的相关要求，还应提供数据加密和保护、身份认证和访问控制、安全监控和日志管理、物理安全等安全防护。

6.1.6 场景联动

应具备场景分析、任务规划、数据集成、通信建立、控制执行等功能。

6.2 数据服务

数据服务要求应符合GB/T 42455.1-2023中7.1数据服务相关要求。

6.3 数据库

数据库要求应符合GB/T 42455.1-2023中7.2数据库相关要求。

6.4 应用支撑

应用支撑应符合GB/T 42455.1-2023中7.3应用支撑相关要求。

7 应用层

7.1 社区人员管理

7.1.1 人员出入管理

人员出入管理应该包括但不限于业主出入管理和访客出入管理，应满足但不限于以下要求：

- a) 针对社区访客，应支持通过社区人脸抓拍、摄像头等监控设施，进行访客人脸信息、目的地、行为轨迹的收集、查询和回放；
- b) 应支持对快递员/车的出入管理功能，如出入登记，宜实现快递员/车的轨迹跟踪、查询；
- c) 宜支持对社区进入人口目的地智能分析，对进入无人房屋的外来访客进行重点关注。

7.1.2 周界防范

周界防范的范围应包括但不限于社区/小区和单元楼字的周界围墙、栅栏、与外界相通的水域、易攀爬管道等，应满足但不限于以下要求：

- a) 通过部署和安装摄像头、电子围栏等，实现对社区/小区的周界入侵防范；
- b) 可支持报警与周界电子地图联动，发生报警时，能在电子地图的对应位置显示出报警区域；
- c) 可支持报警与视频监控联动，发生报警时，可在监控中心屏幕上调阅对应区域的视频图像。

7.1.3 重点区域人员管理

重点区域人员管理应包括但不限于以下范围：

- a) 物业办公区、公共活动场所；
- b) 单元楼字的重要通道和要害部位；
- c) 公共场所的无人值守的变(配)电房、供水泵房、电梯机房等部位出入口。

应满足但不限于以下要求：

- a) 通过部署和安装摄像头、电子围栏等，实现对重点区域的人员监控；
- b) 可支持报警与社区电子地图联动，发生报警时，能在电子地图的对应位置显示出报警区域；
- c) 支持报警与视频监控联动，发生报警时，可在监控中心屏幕上调阅对应区域的视频图像；
- d) 可支持人流统计、人群聚集报警、移动侦测报警、遮挡报警等视频智能分析报警。

7.1.4 特殊人群服务

特殊人群包括但不限于独居老人、残疾人、精神异常人员、刑满释放人员等。

特殊人群服务符合下列要求：

- a) 可支持通过社区监控对特殊人群出入轨迹及时间的监控；
- b) 可支持电子地图与智能分析联动，对特殊人群异常行为警报，并在地图上进行实时显示；

- c) 可支持与智能手环、智能水表、智能电表等设备进行对接,对设备异常进行警报,并在地图上进行实时显示,同时推送给网格管理人员。

7.2 社区车辆管理

7.2.1 车辆出入管理

车辆出入管理符合下列要求:

- a) 应支持对业主车辆以及访客车辆分类管理;
- b) 针对访客车辆,应支持建立实时档案,记录车牌号、进出社区时间及目的地。

7.2.2 车辆轨迹跟踪

车辆轨迹跟踪符合下列要求:

- a) 可通过公共区域视频监控,针对访客车辆及重点车辆,如厢式货车、大型货车进行监控,记录运行轨迹,并支持查询和回放;
- b) 可重点关注夜晚进入社区车辆,通过社区监控及智能识别建立重点关注车辆档案;
- c) 可实时定位重点关注车辆,对异常行为进行报警;
- d) 可灵活设定社区车辆进出规则,对异常行为进行报警;
- e) 应支持提供面向第三方系统的标准化数据共享接口,同步设备信息和告警信息。

7.2.3 停车场管理

停车场管理应符合下列要求:

- a) 停车场安全管理建设区域应包括但不限于:社区/小区内的地上停车场、地下停车场、公共场合的停车场等。
- b) 停车场安全管理应满足但不限于以下要求:
 - 1) 停车场出入口应设置车牌抓拍摄像机,应能清晰抓取进出车辆的车牌号;
 - 2) 具备出入道闸自动控制、车辆出入识别、视频监控、停车场状况信息显示等功能;
 - 3) 应支持按 GA/T 1400.4 规定的的数据服务接口与其他信息系统进行数据交换;
 - 4) 停车场宜配备智能消防监控,具体要求见 7.3.1。

7.3 社区事物管理

7.3.1 社区房屋管理

社区房屋、财产管理应符合GB/T 42455.1-2023中8.1.3房屋管理相关要求。

7.3.2 社区消防管理

智慧社区消防监控区域应包括但不限于:

- a) 居民房屋内;
- b) 社区/小区的出入口、楼栋楼层、主要公共区域;
- c) 单元楼宇的出入口、重要通道、电梯厅及电梯轿厢等要害部位;
- d) 公共场所的出入口、重要通道、电梯厅及电梯轿厢、电梯机房等要害部位。

消防管理应包含火灾探测报警、消防设施监测、电动车进楼监测、消防通道占用监测。应满足但不限于以下要求:

- a) 应支持提供面向第三方系统的标准化数据共享接口,同步设备信息和告警信息;
- b) 应支持告警联动功能,与小区监控室实现声光报警联动,也应与地区消防主管部门建立消防联动报警机制,实现警民联动;
- c) 应支持报警自动消除功能;
- d) 可支持通过物联网技术或 AI 技术,检测消防通道占用、消火栓状态、消防门开闭、电动车进楼等情况;
- e) 消防隐患管理服务应满足 GB/T 42455.1-2023 中 8.1.10 消防安全隐患管理相关要求。

7.3.3 防盗监控和报警

防盗监控安装位置应包括但不限于以下位置：

- a) 社区内公共活动区域；
- b) 社区内人群聚集区域；
- c) 居住区域一楼出入口附近区域；
- d) 居住区域水、电、热、气、通信等设备间；
- e) 居住区域楼梯通道及电梯进出口；
- f) 非封闭式社区的进出通道及封闭式社区的出入口。

防盗监控和报警符合下列要求：

- a) 应支持对公共区域物品进行信息化管理，分类创建相应档案；
- b) 应支持对无人居住房屋及重点防盗区域周边进行重点监控，对附近异常停靠车辆进行监测报警并推送给相关安保人员；
- c) 可支持非法入侵报警，非法打开入户门窗时立即联网推送警示信息，实现警民联动。

7.3.4 高空抛物管理

应支持通过社区视频监控等系统对高空抛物位置进行识别、监控及定位，支持事件相关信息查询和监控追溯。

7.3.5 电梯安全

电梯安全管理应符合下列要求：

- a) 应支持对小区内所有电梯进行信息化管理，设置相应档案；
- b) 应支持根据电梯检修档案以及电梯运行情况设置检修提醒，并将提醒信息推送给相关人员；
- c) 应支持对电梯运行情况进行实时监控，针对异常情况及时报警；
- d) 应支持对电梯内信息的监控，并对电动车入电梯实现及时报警；
- e) 宜通过监控及 AI 智能识别的相互连动，识别影响电梯设备运行以及破坏电梯设备的行为，及时进行提醒并将报警信息推送给相关人员；
- f) 宜通过电梯刷卡等方式，实现电梯门禁和刷卡直达功能，同时支持访客乘梯、临时乘梯等。

7.3.6 消防通道占用监管

消防通道占用监管应符合下列要求：

- a) 应支持对消防通道实时监控，对占用消防通道行为及时报警，并发送报警信息至相关人员；
- b) 应支持对造成消防隐患人员的识别与建档，允许对事件相关信息的查询。

7.3.7 充电桩安全监管

充电桩安全监管符合下列要求：

- a) 应支持对充电桩相关监控设备统一管理；
- b) 应支持根据充电桩检修及使用情况设置实时档案，及时发送检修信息及检修提醒至相关人员；
- c) 应支持智能识别与自动报警联动，自动识别充电桩危险状态并及时报警；
- d) 可通过人脸识别对破坏充电桩行为进行监控，记录事件相关信息并允许查询；
- e) 可支持对充电桩进行远程控制。

7.4 其他管理

7.4.1 报警管理

入侵和报警建设应满足但不限于以下要求：

- a) 应通过部署和安装摄像头、电子围栏等，实现对社区/小区的周界入侵防范；
- b) 可支持报警与周界电子地图联动，发生报警时，能在电子地图的对应位置显示出报警区域；
- c) 可支持报警与视频监控联动，发生报警时，可在监控中心屏幕上调阅对应区域的视频图像；
- d) 应具备过载保护、漏电保护、过热保护、欠压保护等功能，支持电能监测、故障诊断和异常报警；
- e) 可支持人流统计、人群聚集报警、移动侦测报警、遮挡报警等视频智能分析报警。

7.4.2 智能巡更

智能巡更服务应满足但不限于以下要求：

- a) 支持对警民联防工作人员巡查行为进行实时监控和记录；
- b) 支持获取警卫巡更点信息，巡更时间和路线可根据需要设定和修改；
- c) 支持显示、统计和查询巡更人员相关信息；
- d) 条件允许的社区，宜配备无人巡更车或无人巡更飞行器，实现 24 小时不间断巡更。

7.4.3 应急管理

应急管理除应符合GB/T 42455.1-2023要求外，还应满足但不限于以下要求：

- a) 应支持住户的燃气泄漏报警。发生水火燃气等警情时，能触发报警并自动将报警信息推送到住户手机、紧急联系人或物业，处理记录可供查询；
- b) 应支持信息化应急管理功能，提供应急预案管理、应急演练管理等功能。

7.4.4 社区网格化治理

智慧社区网格化管理服务除符合GB/T 42455.1-2023的要求外，应实现对网格员管理工作的支撑，如安防信息采集、安防事件处理、警情科普宣传、疫情防控等。

7.5 安防综合服务

基于智慧社区安防系统平台汇集的数据，可视化展现社区安防综合服务状态，如：

- a) 支持智慧社区安防动态“一张图”管理，实现全区域动态实时呈现，时间、空间统一管理；
- b) 提供智慧社区安防系统相关场景应用的统一入口；
- c) 支持智慧社区安防相关设备设施的统一监控和管理；
- d) 提供智慧社区安防系统涉及的人、车、物等相关对象的信息可视化展示及分析；
- e) 支持安防系统相关预警、报警信息和消息推送提醒。

8 安全保障

8.1 网络安全

智慧社区安防系统网络安全建设需保障整体网络架构的安全性，应满足GB/T 22239-2019中相关要求，同时应满足以下要求：

- a) 安防信息系统网络与其他公共信息网络应实行逻辑隔离，也可实行物理隔离；
- b) 涉及政府部门的网络边界防护应遵循GB/T 29245-2012相关要求；
- c) 应对网络设备和安全事件进行监测、监控及审计；
- d) 涉及网络安全中使用的商用密码技术，应遵循国家密码管理部门相关规范标准；
- e) 在部署基础安全防御组件的基础上加强实时监测，检测到威胁后进行有效响应，从而形成集防御、检测、响应于一体的闭环安全。

8.2 数据安全

智慧社区安防系统的数据安全应符合GB/T 42455.1-2023中9.4数据安全相关要求，同时，应满足以下要求：

- a) 数据安全应覆盖数据流转的各个环节。在数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等各个环节实现全生命周期的安全防护；
- b) 可基于AI和大数据分析技术快速定位数据泄露源头，实现数据安全事件定责有据，保障数据安全可溯；
- c) 应确保社区所有数据的处理与存储设备位于中国境内。

8.3 物理安全

智慧社区安防系统物理安全应满足GB/T 42455.1-2023和GB/T 22239-2019中相关要求，同时应满足以下要求：

- a) 建设中物联网感知层网关，应遵循 GB/T 37024-2018 相关要求；
- b) 所需密码设备，应采用国家密码管理局行政审批的品种和型号；
- c) 系统建设中所采用其他设备，应确保供应链安全。

8.4 应用安全

智慧社区安防系统应用安全应满足GB / T 22239-2019中相关要求，同时应满足以下要求：

- a) 针对智慧社区安防系统建设中涉及到的上层应用，应全流程保障其整体安全；
- b) 针对应用访问过程，首先实现身份鉴别，保障接入用户身份的安全性；
- c) 进行访问控制，设置访问规则，保障各用户访问权限的最小化，避免非授权访问；
- d) 在访问应用的过程中，需进行日志留存，实现审计回溯；
- e) 在访问中需保障应用的安全管理，做到针对应用的定期更新以及核心应用和数据的定时备份；
- f) 应通过零信任等身份鉴别系统实现应用的精细化权限访问管理，建设应用边界防护措施，如Web应用防火墙、下一代防火墙等实现应用边界访问控制。

8.5 信息安全

智慧社区安防系统信息安全宜参考 GB/Z 28828-2012 的要求，同时应满足以下要求：

- a) 应对相关工作人员采用访问控制模式，进行操作和接触人员身份认证和识别；
- b) 系统宜采用数字摘要、数字时间等技术保护信息的完整性；
- c) 非必要情况下，智慧社区安防系统内涉及到的居民个人信息不得外传及拷贝；
- d) 智慧社区安防系统中采集到的车辆轨迹等信息，不得外传及拷贝；
- e) 如必要情况下需数据及信息拷贝时，应对数据再存储和运输过程中进行加密。

9 运行维护

智慧社区安防系统的运行和维护应符合智慧社区信息系统整体运行维护的要求，符合GB/T 42455.1-2023中10运行维护相关要求。
