新时期智慧园区安防体系研究

李恩庆
中国船舶集团有限公司第七一三研究所　河南　郑州　450015

摘　要：新时期智慧园区安防体系研究聚焦物联网、大数据、AI等技术融合，构建全域感知、智能预警、快速响应的立体化安防网络。通过高清智能监控、多模态生物识别、环境传感器等设备实现风险动态监测，结合边缘计算与云计算提升数据处理效率，推动门禁、消防、应急等子系统协同联动，形成“技防+人防”融合模式，显著提升园区安全管理精准度与应急处置能力。

关键词：新时期；智慧园区；安防体系

引言：随着物联网、人工智能与5G技术的深度融合，智慧园区建设正从单一功能优化向全场景智能化演进。安防体系作为园区安全运行的基石，面临传统模式响应滞后、数据孤岛、被动防御等痛点，难以应对非法入侵、网络攻击、灾害事故等复合型风险。新时期智慧园区安防需突破技术壁垒，构建全域感知、智能决策、多系统联动的主动防控体系，实现从“事后处置”向“事前预防”的范式转变，为园区高质量发展提供安全保障。

1 新时期智慧园区安防需求分析

1.1 智慧园区安全风险特征

（1）物理安全：园区物理空间安全隐患多元，包括非法入侵、翻越围墙等恶意闯入行为，火灾、燃气泄漏等灾害事故，以及电力设备、监控系统等关键设施故障，此类风险直接威胁园区财产与人员安全，具有突发性强、影响范围广的特点。（2）网络安全：随着园区智能化升级，物联网设备、管理系统广泛应用，数据泄露、系统攻击等网络风险凸显。园区内企业商业数据、人员身份信息等敏感数据易被窃取，监控系统、门禁系统等核心安防系统可能遭恶意入侵，导致安防体系瘫痪。（3）人员安全：园区人员流动频繁，应急疏散效率直接关乎人员生命安全，尤其在火灾、地震等突发事件中，需快速精准引导人员撤离；同时，人员异常行为如徘徊逗留、违规闯入禁区等，可能引发安全事故，需及时监测预警[1]。

1.2 传统安防体系的痛点

传统安防体系以被动防御为主，多依赖人工巡查和孤立设备监测，难以提前预判风险，往往在事故发生后才介入处理；各安防子系统如监控、门禁、消防等相互独立，缺乏协同联动机制，出现险情时无法快速响应、统筹处置；此外，系统运行产生的大量数据未得到有效挖掘利用，无法为安全管理决策提供数据支撑，安防效率和精准度不足。

1.3 新时期安防体系的核心需求

（1）全域感知与动态预警：构建覆盖园区物理空间、网络空间、人员活动的全域感知网络，整合视频监控、传感器、物联网设备等数据资源，通过智能算法实时分析风险隐患，实现对非法入侵、火灾苗头、网络攻击等风险的动态预警，变被动防御为主动防控。（2）多系统联动与智能决策：打破各安防系统信息壁垒，建立统一的安防管理平台，实现监控、门禁、消防、应急广播等系统的协同联动，险情发生时自动触发应急预案，精准调度资源；同时，依托大数据分析提供智能化决策建议，提升安防处置效率和科学性。（3）隐私保护与合规性要求：在推进安防智能化的同时，严格遵守数据安全相关法律法规，对人员身份信息、视频监控数据等敏感信息进行加密存储和规范管理，防止数据泄露滥用，平衡安防管控与个人隐私保护，确保安防体系建设与运营合法合规。

2 新时期智慧园区安防体系架构设计

2.1 总体架构设计原则

（1）模块化原则：按功能将安防体系拆解为感知、网络、平台、应用等独立模块，各模块边界清晰、接口标准化，便于单独部署、维护与升级；（2）可扩展性原则：预留充足的接口与扩展空间，支持后续新增安防设备接入、功能模块拓展及业务场景延伸，适配园区规模扩大与智能化升级需求；（3）安全性原则：从数据采集、传输、存储到应用全流程落实安全防护措施，采用加密传输、权限管控、安全审计等技术，抵御网络攻击与数据泄露风险；（4）用户体验原则：简化操作流程，设计直观的可视化管理界面，降低管理人员学习与操作成本，同时保障园区人员在安防管控中的便捷性，平衡安全管控与使用体验。

2.2 关键技术支撑

（1）物联网（IoT）技术：通过部署各类智能传感器、RFID标签等终端设备，实现园区内安防设备的全面互联与数据实时采集，为安防管控提供基础数据支撑；（2）人工智能（AI）技术：核心应用于视频智能分析、人员行为识别与风险预测，可自动识别非法入侵、人员聚集、异常徘徊等危险行为，结合历史数据预判火灾、设备故障等风险，提升安防预警的精准度；（3）大数据技术：对感知层采集的视频数据、设备数据、人员数据等多源数据进行融合清洗与深度挖掘，提炼有价值的安全管理信息，为智能决策提供数据依据；（4）5G/边缘计算技术：借助5G低延迟、高带宽的传输优势，搭配边缘计算节点实现数据本地实时处理，减少云端传输延迟，保障安防指令快速响应，尤其适配应急处置等对实时性要求极高的场景[2]。

2.3 分层架构设计

（1）感知层：作为安防体系的“神经末梢”，全面部署智能传感器、高清摄像头、智能门禁、火灾探测器等终端设备，实现对园区物理环境、人员活动、设备状态的全方位感知与数据采集；（2）网络层：构建有线与无线融合的通信网络，采用以太网、WiFi、5G等多种通信协议，同时部署防火墙、入侵检测等安全设备，保障数据传输的稳定性与安全性，打通感知层与平台层的数据通道；（3）平台层：搭建数据中台、AI中台、业务中台三位一体的核心支撑平台，数据中台负责数据整合与管理，AI中台提供智能分析算法能力，业务中台承接各类安防业务逻辑，为上层应用提供统一的技术与数据支撑；（4）应用层：基于平台层能力，部署智能监控、应急指挥、访客管理、设备运维等核心业务模块，直接面向园区安全管理需求，实现风险监测、应急处置、日常管控等具体安防功能。

2.4 系统集成与协同机制

（1）跨子系统联动：打破传统安防子系统孤立运行的壁垒，实现消防、门禁、监控、应急广播等系统的深度联动，例如火灾发生时，系统可自动触发门禁解锁、应急广播启动、监控画面聚焦火灾区域等一系列联动操作，快速推进应急处置；（2）统一管理平台设计：构建一体化安防管理平台，整合各子系统数据与功能，实现对全园区安防状态的集中监控、统一调度与精准管理，平台支持可视化展示、智能告警、应急预案触发等功能，为管理人员提供全景式、智能化的管理工具，确保安防指令快速传达、资源高效调配。

3 新时期智慧园区安防核心功能模块实现

3.1 智能监控与预警系统

（1）基于深度学习的异常行为识别：通过部署搭载智能算法的高清摄像头，实时采集园区重点区域视频数据，算法可精准识别徘徊逗留、攀爬围墙、翻越栏杆等危险行为，一旦检测到异常，立即触发声光告警并将预警信息推送至管理平台，同时锁定事发区域监控画面，助力管理人员快速处置；（2）环境监测：在园区室内外关键点位部署温湿度传感器、气体泄漏探测器、烟雾传感器等设备，实时采集环境数据并上传至平台，当数据超出预设阈值（如烟雾浓度超标、燃气泄漏），系统自动发出预警，联动应急设备启动初步处置，如开启排风设备、关闭燃气阀门，为灾害防控争取时间。

3.2 应急响应与决策支持系统

（1）应急预案数字化管理：将火灾、地震、人员踩踏等各类突发事件的应急预案转化为数字化流程，录入系统数据库，明确应急组织机构、处置流程、责任分工及资源调配方案，支持预案快速检索、在线修订与全员推送，确保应急处置有章可循；（2）智能路径规划与疏散引导：结合园区地图数据与实时人员分布信息，突发事件发生时，系统通过AI算法快速规划最优疏散路线，规避危险区域，同时联动应急广播、指示灯牌等设备，精准推送疏散指引信息，同步向管理人员提供人员疏散进度、资源调配建议等决策支持，提升应急疏散效率与安全性[3]。

3.3 人员与车辆管理系统

（1）人脸识别/车牌识别无感通行：在园区出入口、楼栋单元门等关键点位部署人脸识别终端与车牌识别设备，内部人员录入人脸信息后可无感快速通行，外来车辆通过车牌识别自动登记信息，经管理人员审核后放行，有效杜绝无关人员与车辆闯入；（2）访客动态权限管理：搭建访客管理子系统，访客通过线上预约或现场登记录入身份信息，系统生成临时动态权限凭证（如二维码），可精准限定访客通行区域与停留时间，访客离开后权限自动失效，同时记录访客活动轨迹，便于后续追溯查询。

3.4 网络安全防护体系

（1）数据加密与访问控制：对安防系统采集的视频数据、人员身份信息、设备运行数据等敏感数据，采用AES加密算法进行传输与存储，同时建立精细化访问控制体系，按岗位层级分配数据访问权限，落实“最小权限”原则，通过账号密码、动态口令等多重认证方式，防止数据泄露与非法访问；（2）入侵检测与主动防御机制：部署网络入侵检测系统（IDS）与入侵防御系统（IPS），实时监测网络流量与系统运行状态，精准识别恶意攻击、病毒入侵等网络威胁，一旦发现异常，立即触发防御策略，

如阻断攻击源、隔离受感染设备，同时生成安全告警与分析报告，助力管理人员及时排查安全隐患，保障安防系统网络稳定运行。

4 新时期智慧园区安防建设的挑战与对策建议

4.1 技术挑战

（1）数据隐私与安全风险：安防系统运行过程中会采集海量人员人脸、身份信息及园区敏感空间数据，此类数据在传输、存储和使用环节，易遭受黑客攻击、非法窃取或滥用，既侵犯个人隐私，也可能泄露园区核心安全信息，引发安全隐患。（2）多源异构数据融合难题：园区安防系统涵盖视频、传感、网络、人员车辆等多类型数据，不同数据格式、标准差异较大，缺乏统一的数据融合规范，导致数据难以高效整合关联，无法充分挖掘数据价值，影响智能决策的准确性。（3）算法鲁棒性与适应性不足：当前安防依赖的AI算法易受环境因素干扰，如恶劣天气、光照变化、遮挡物等都会降低行为识别、风险预测的精准度，且不同园区场景差异较大，通用算法难以快速适配个性化需求，存在误报、漏报问题。

4.2 管理挑战

（1）跨部门协同机制缺失：园区安防涉及安保、物业、消防、IT等多个部门，各部门权责划分不够清晰，缺乏常态化协同沟通与联动处置机制，出现安全问题时易出现推诿扯皮、响应滞后的情况，无法形成安防管控合力。（2）人员技能与意识不足：一方面，现有管理人员多缺乏智能化设备操作、数据解读及系统运维的专业技能，难以充分发挥智慧安防系统的功能优势；另一方面，部分人员安全防范意识薄弱，存在违规操作设备、泄露系统权限等行为，人为增加了安防体系的运行风险。

4.3 对策建议

（1）完善政策标准与监管体系：结合数据安全法、个人信息保护法等法律法规，制定智慧园区安防数据采集、使用、存储的专项标准规范，明确各主体责任；建立常态化监管机制，加强对安防系统运行及数据安全的监督检查，严厉打击数据滥用等违法行为，筑牢制度保障防线。（2）加强产学研合作推动技术落地：鼓励园区运营方与科研院校、科技企业开展深度合作，聚焦数据融合、算法优化等核心技术难题联合攻关，开发适配多场景的鲁棒性算法和统一数据融合平台；同时加快技术成果转化应用，通过试点示范推动成熟技术在园区落地，提升安防技术水平[4]。（3）构建“技术+管理”双轮驱动模式：技术层面持续优化安防系统功能，提升系统稳定性与智能化水平；管理层面健全跨部门协同机制，明确权责清单，建立定期会商与联动处置流程；同时加强人员培训，开展智能化技能与安全意识专项培训，提升管理人员专业能力，规范操作行为，实现技术赋能与管理提质的有机结合。

结束语

新时期智慧园区安防体系的建设，是技术革新与管理升级的深度融合。通过物联网、人工智能与大数据技术的协同应用，安防体系已实现从被动防御到主动预警、从单点防控到全局联动的跨越。未来，需持续优化算法鲁棒性、强化数据隐私保护，并完善跨部门协同机制，推动安防体系向智能化、人性化、可持续化方向演进。唯有技术赋能与制度保障双轮驱动，才能构建安全、高效、韧性强的智慧园区新生态，为城市数字化转型提供坚实支撑。

参考文献

[1]沈翰文.人工智能嵌入下视频图像大数据综合感知与智能应用[J].软件,2024,45(8):34-38.

[2]林瑜.基于人工智能视频图像数据分析的机器人远程监测系统设计[J].自动化与仪器仪表,2025(7):155-159.

[3]张旭阳,叶光红,杨建波,等.基于智能视频分析的智慧安防技术优化与可用性评估[J].互联网周刊,2024(10):46-48.

[4]卞桂平,王莉.基于人工智能的中小幼校园智慧安防系统实践研究[J].电脑知识与技术,2025,21(12):15-17.