ICS 13.310
CCS A 91

DB34

安 徽 省 地 方 标 准

DB34/T 4659—2024

医院智慧安防建设指南

Guidelines for intelligent security construction of hospital

2024－01－11 发布　　2024－02－11 实施

安徽省市场监督管理局　　发 布

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这些专利的责任。

本文件由合肥市公安局提出。

本文件由安徽省公安厅归口。

本文件起草单位：合肥市公安局、安徽省公安厅治安警察总队、安徽省公安厅科技信息化处、合肥市卫生健康委员会、上海天跃科技股份有限公司、安徽省安全技术防范行业协会、四创电子股份有限公司、讯飞智元信息科技有限公司、安徽电信规划设计有限责任公司、合肥市伟丰电子有限责任公司、中星微技术股份有限公司、安徽金蓓检测认证股份有限公司、中国科学技术大学附属第一医院（安徽省立医院）、安徽医科大学第一附属医院、合肥市第一人民医院、合肥保安智能科技有限公司、安徽康姆电子科技有限公司、安徽创和建筑集团有限公司、安徽中恺保安服务有限公司。

本文件主要起草人：舒萍、童映升、史哲桢、徐丹丹、苏增亮、杨柳、彭华、杜勇、胡健、王瑞、陶东、金成城、梁昌岭、孙欣、马志强、李琳、王树林、岳勇、田峰、金炜、陈孝谋、孙方德、钱捷、方菲、徐道广、任义康、梁楠、张佳佳。

医院智慧安防建设指南

1 范围

本文件规定了医院智慧安防系统建设的总则、系统构成、系统建设和系统安全。

本文件适用于医院的智慧安防系统建设。

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 信息安全技术 网络安全等级保护基本要求

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 31458 医院安全技术防范系统要求

GB/T 32581—2016 入侵和紧急报警系统技术要求

GB 35114 公共安全视频监控联网信息安全技术要求

GB/T 37078—2018 出入口控制系统技术要求

GB 37300 公共安全重点区域视频图像信息采集规范

GB 50348—2018 安全防范工程技术标准

GB 55029 安全防范工程通用规范

GA/T 1400 公安视频图像信息应用系统（所有部分）

YD/T 1171—2015 IP网络技术要求网络性能参数与指标

3 术语和定义、缩略语

3.1 术语和定义

GB 50348—2018 界定的以及下列术语和定义适用于本文件。

3.1.1

智慧安防系统 intelligent security system

以安全为目的，应用大数据、云计算、物联网等新一代信息技术，利用各类数据资源辅助科学决策，提升风险感知、延迟和处置能力，实现预防、延迟、阻止入侵、盗窃、抢劫、破坏、爆炸、暴力袭击等事件发生的电子防护系统。

3.2 缩略语

下列缩略语适用于本文件。

QoS：服务质量（Quality of Service）

SMART：自我监测分析与报告技术（Self-Monitoring, Analysis and Reporting Technology）

4 总则

4.1 应坚持“统筹协调、创新引领、安全可靠”的基本原则。
4.2 应具备多院区、多层级、多部门数据共享、业务协同的系统支撑能力。
4.3 应满足基于安防数据实现风险预警、辅助决策和应急处置的安全防范管理要求。
4.4 应符合 GB 55029、GB 50348、GB 37300 和 GB/T 31458 的相关规定。

5 系统构成

5.1 医院智慧安防系统由智慧安防管理平台（以下简称管理平台）和各子系统构成。子系统包括但不限于：

——入侵和紧急报警；
——视频监控；
——出入口控制；
——停车场（库）安全管理；
——防爆安全检查；
——电子标签；
——语音识别；
——监控中心动力环境监测。

5.2 各子系统应提供联网所要求的硬件接口和软件通讯协议等，与管理平台实现信息传输、交换、控制。

6 系统建设

6.1 入侵和紧急报警子系统

6.1.1 应具备记录功能，内容包括但不限于：

——报警人员；
——报警位置；
——报警时间；
——报警类型。

6.1.2 应具备识别翻越、穿越、挖凿等行为的周界报警功能。

6.2 视频监控子系统

6.2.1 应支持在单一画面上同时抓拍、识别多个人脸，抓拍、识别数量可在 2 个至 30 个或以上的范围设置。

6.2.2 应支持通过人脸特征数据，判断目标对象的性别、年龄段、是否戴口罩、是否戴眼镜等。

6.2.3 应支持以下视频实时智能分析功能，包括但不限于：

——入侵检测；
——绊线检测；
——人员聚集检测；
——人员离岗检测；
——物品搬移检测；
——遗留物检测；
——人数统计；

——密度检测。

6.2.4 宜采用不可逆方式从人脸样本中提取生物特征数据。

6.2.5 宜支持识别跌倒、扭打、烟雾、明火、吸烟等异常现象。

6.3 出入口控制子系统

6.3.1 应具备复合识别功能，并至少支持以下 1 种人体生物特征识别功能：

——人脸；

——指纹；

——掌纹；

——指静脉；

——掌静脉；

——虹膜；

——声纹。

6.3.2 重要场所出入口的人体生物特征识读装置应具备活体检测功能。

6.4 停车场（库）安全管理子系统

6.4.1 应支持识别通行车辆的类型、颜色、号牌等特征。

6.4.2 应具备车辆通行权限设置、异常报警和道闸联动功能。

6.4.3 应具备停车引导和寻车功能。

6.5 防爆安全检查子系统

6.5.1 应具备实时显示、记录和报警功能。

6.5.2 宜支持非接触式扫描，并生成图像。

6.6 电子标签子系统

6.6.1 应具备对标识物进行信息采集和信息远程维护功能。

6.6.2 应具备对标识物信息进行识别、跟踪和异常状态实时告警功能。

6.7 语音识别子系统

6.7.1 应具备关键词识别功能。

6.7.2 应具备语音转文字功能。

6.7.3 应具备关键字检索功能。

6.8 监控中心动力环境监测子系统

6.8.1 应支持对监控中心的市电供电、UPS 设备和蓄电池状态进行实时监测。监测数据包括但不限于：

——市电供电：电压、电流、功率因数；

——UPS 设备：电压、电流、频率、负载率；

——蓄电池：剩余电量、电池温度。

6.8.2 应支持对监控中心的温湿度、漏水情况、电缆温度进行实时监测。

6.8.3 当监测数据阈值超出限值时，应实时告警。

6.9 管理平台

6.9.1 配置管理

6.9.1.1　应支持对防护对象、各子系统和设备的名称、位置、属性/类型、管理要求等参数进行管理任务和处置预案配置。

6.9.1.2　配置管理任务，应包括但不限于：

——任务名称；

——任务执行要求；

——任务执行人。

6.9.1.3　配置处置预案，应包括但不限于：

——告警信号/事件信息；

——视频联动；

——电子地图联动；

——人员分工；

——处置流程；

——保障措施。

6.9.2　运行管理

6.9.2.1　应支持在规定时间自动发送管理任务至相应的任务执行人，并记录任务执行过程。

6.9.2.2　应支持同时接收和处理各子系统的系统状态、告警信号/事件信息，并根据设定的规则，自动判别警情的类型、级别。

6.9.2.3　应支持警情发生后自动发送处置预案规定的处置流程、保障措施至相应的任务执行人。

6.9.2.4　应支持按照处置预案自动切换监控图像和数据可视化展示。出现异常情况时，支持手动控制。

6.9.2.5　应支持对警情处置过程进行全程记录，对处置记录进行检索、回放。

6.9.2.6　应具备按照处置预案自动执行视频巡查功能，对巡查过程进行全程记录，对巡查结果进行检索、回放。

6.9.2.7　应具备管理任务执行情况、告警信号/事件信息统计和态势分析功能。

6.9.2.8　应具备安防监控中心值守排班功能。

6.9.2.9　宜支持实时追踪和刻画人员和车辆轨迹，并建立档案。

6.9.3　数据共享

6.9.3.1　应支持向公安机关和相关管理部门推送信息。

6.9.3.2　宜支持与医院信息管理系统、火灾报警系统和信息导引系统共享数据。

6.9.4　运维管理

6.9.4.1　应支持自动监测各子系统设备在线与离线状态、故障状态。

6.9.4.2　应支持自动检测视频质量、录像数据丢失和录像天数不足。

6.9.4.3　应具备自动校时功能。

6.9.4.4　检测到故障时，应支持自主生成和派发报修工单，并跟踪处置过程。

6.9.4.5　应支持自主生成设备运行分析报告和运维质量报告。

6.9.4.6　宜支持监测设备硬盘 SMART 信息。

6.9.5　数据可视化

6.9.5.1　应支持对告警信号/事件信息的数据进行总结、归纳及趋势分析并形成可视化展示，内容包括但不限于：

——发生时间；

——发生地点；
——等级；
——数量；
——处置时长；
——处置结果；
——处置率；
——处置及时率；
——分布态势。

6.9.5.2 应支持系统对运维数据进行总结、归纳及趋势分析并形成可视化展示，内容包括但不限于：
——故障发生时间；
——故障地点；
——设备类型；
——设备品牌；
——维保单位；
——故障数量；
——维修时长；
——故障类型分布；
——故障发生趋势。

6.9.5.3 应支持图表方式展示。

6.9.6 移动应用

6.9.6.1 应支持在移动端处置告警信号/事件信息和维修工单,包括但不限于：
——接收推送信息；
——上报处置结果；
——查询处置记录。

6.9.6.2 应支持通过移动端进行事件上报，内容包括现场视音频、事件描述和位置等。

6.9.6.3 应支持通过移动端实施预案演练和安保巡更，并记录过程。

7 系统安全

7.1 应具备容错机制和可扩展能力。

7.2 应具备数据传输加密功能。

7.3 应具备数据脱敏和防篡改功能。

7.4 入侵和紧急报警系统的安全等级应不低于 GB/T 32581—2016 中规定的 2 级要求。

7.5 视频监控系统联网信息安全要求应符合 GB 35114 的相关规定。

7.6 出入口控制系统的安全等级应不低于 GB/T 37078—2018 中规定的 2 级要求。

7.7 系统网络性能应符合 YD/T 1171—2015 中网络 QoS 类别 1 的相关规定。

7.8 智慧安防管理平台联网接口应符合 GB/T 28181 的相关规定，向公安机关推送视频图像数据应符合 GA/T 1400 的相关规定。

7.9 网络安全等级保护应符合 GB/T 22239 的相关规定。

参 考 文 献

[1] GB/T 37036.1—2018 信息技术 移动设备生物特征识别 第1部分：通用要求
[2] 关于推进医院安全秩序管理工作的指导意见（国卫医发〔2021〕28号）
[3] 关于进一步加强医院安全秩序管理工作的通知（皖卫医秘〔2022〕106号）