ICS

团 体 标 准

T/SDAAI 0002—2025

智慧校园安全平台架构建设指南

Guidelines for Constructing the Architecture

of a Smart Campus Security Platform

全国团体标准信息平台

2025-04-11发布 2025- 04-12实施

山东省人工智能学会发布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和缩略语 1
3.1 术语和定义 1
3.2 缩略语 1
4 总体架构 2
5 总体要求 3
5.1 基础设施 3
5.2 数据中心 3
5.3 应用平台 3
5.4 管理中心 4
5.5 终端门户 4
5.6 管理与保障体系 4
5.7 运行体系 5
参考文献 6

全国团体标准信息平台

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。

本文件由山东省人工智能学会提供、归口并组织实施。

本标准起草单位：山东大学、济南幼儿师范高等专科学校、济南亚爱特软件有限公司。

本标准主要起草人：张伟，王新程，李晓磊，池海，高杨，王坚，王瑞丰，宋然，程吉禹，夏伯慷，李伟，荐秋，亓振亿，戚舒蕾，张衍卿。

全国团体标准信息平台

智慧校园安全平台架构建设指南

1 范围

本文件规定了智慧校园建设中校园安全平台规划、搭建、运行和管理的基本原则、总体框架以及总体要求。

本文件适用于智慧校园建设中校园安全平台规划、搭建、运行和管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 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 29315 中小学、幼儿园安全技术防范系统要求

GB/Z 43444.1-2023 智能设备管理 第1部分：概念和定义

3 术语和缩略语

3.1 术语和定义

3.1.1

智能设备 smart device

具备通信、计算、感知与控制能力的终端硬件。

注：除具备上述能力外，智能设备也可具备一定的自主执行命令的能力。

3.1.2

校园安全平台 campus security platform

通过智能化和信息化理念，运用人工智能、智能设备控制、大数据分析等关键技术，实现智慧校园中校园智能安防的统一安全平台。

3.2 缩略语

下列缩略语适用于本文件。

PC：个人电脑（Personal Computer）

AI：人工智能（Artificial Intelligence）

GIS：地理信息系统（Geographic Information System）

GDPR：通用数据保护条例（General Data Protection Regulation）

HIPAA：健康保险流通与责任法案（Health Insurance Portability and Accountability Act 1996）

VPN：虚拟专用网络（Virtual Private Network）

4 总体架构

智慧校园安全平台总体架构包括：数据中心、应用平台和管理中心组成的智慧校园安全中枢系统，并且由管理与保障体系和运行体系负责整个安全平台的运行管理保障过程，基础设施部分为校园安全平台提供基础的硬件支撑，以及终端门户为安全平台提供用户类型和访问渠道。智慧校园安全平台总体架构如图1所示。

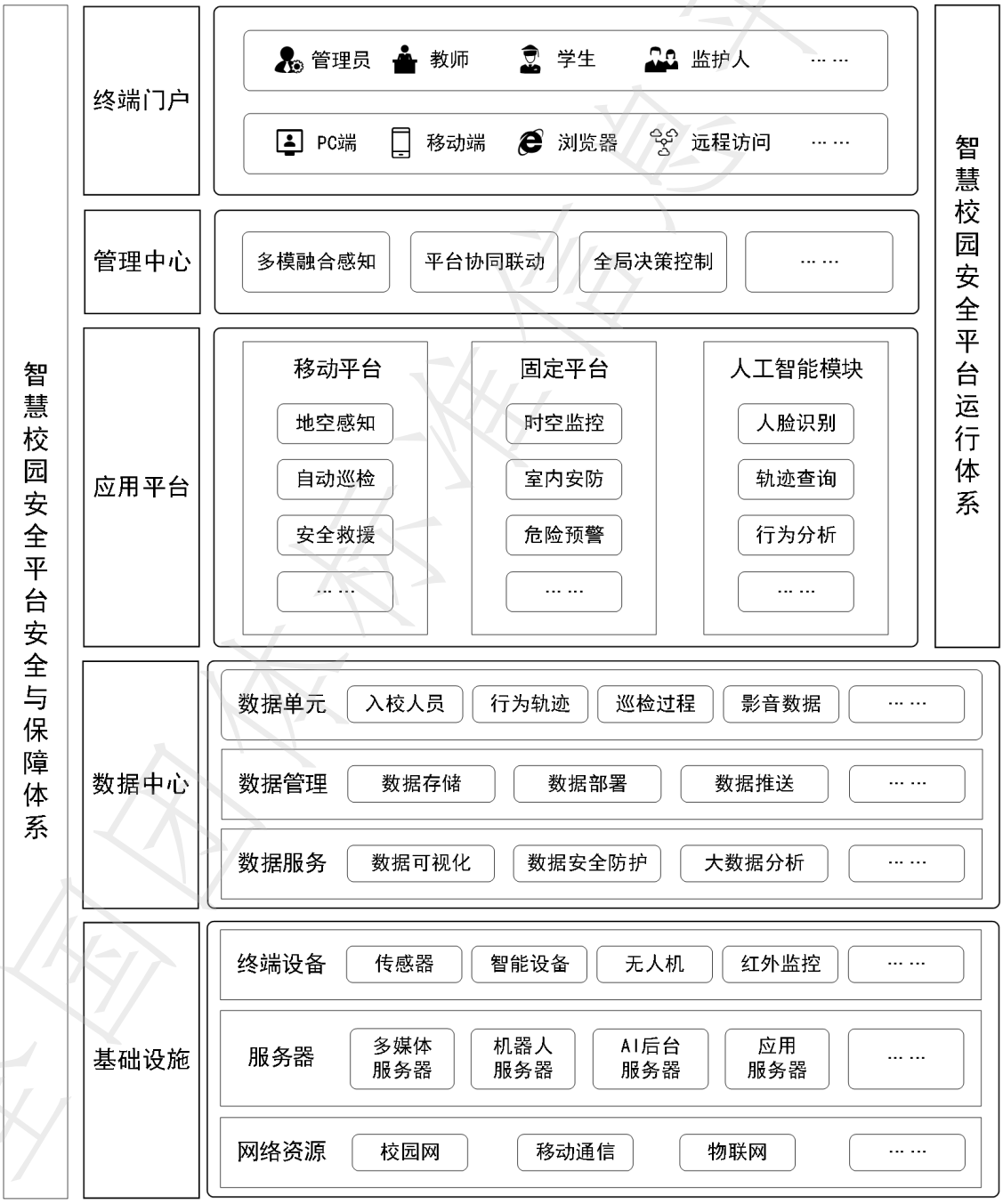

图 1　智慧校园安全平台总体架构

5 总体要求

5.1 基础设施

由终端设备、服务器和网络资源等校园数字化信息化基础设施组成，在维持设施稳定、安全、可控的前提下，支撑整个智慧校园安全平台的各种业务类型。应实现的功能包括但不限于：

a) 终端设备：通过各类传感器、监控摄像头、智能设备等硬件设备，为校园安全平台提供感知和行动能力，实现对校园中人员、行为、物品等元素进行感知与交互，并应符合 GB/Z 43444.1-2023 的要求；

b) 服务器：通过多媒体服务器、机器人服务器、AI 后台服务器、应用服务器等服务器设施，为校园安全平台提供算法决策、应用支撑以及各类数据的存储；

c) 网络资源：通过校园网、移动通信、物联网等传输网络基于设施，为校园安全平台提供传输网络、联通硬件设备的能力，实现各种数据的有效传输，并应符合 GB/T 28181 的要求；

5.2 数据中心

为校园安全平台提供数据流的组织和管理，促进各种数据的收集、存储、处理、分析和可视化过程。应实现的功能包括但不限于：

a) 数据单元：由入校人员、行为轨迹、巡检过程、预警警报等类型的信息构成校园安全平台的基础数据结构，为平台提供所需的基础数据；

b) 数据管理：经过数据存储、数据部署、数据推送等环节的操作可对数据进行必要的管理行为，为校园安全平台的数据提供完整周期的数据流治理能力；

c) 数据服务：包括数据可视化、数据完全防护、大数据分析等重要的数据处理行为，为校园安全平台的数据组织和管理过程提供支撑；

5.3 应用平台

5.3.1 移动平台

移动平台主要负责校园室外场景下的人与事件的监控、交互行为，是保障校园安全的关键点之一。应实现的功能包括但不限于：

a) 地空感知：主要利用摄像头、声音采集器、无人机等终端设备对人与物从地面视角以及空中俯视视角进行全方位的感知，收集数据便于后续应用平台处理；

b) 自动巡检：由机器人等智能设备负责的自动化定期巡检校园行为，并进行视频监控、检测异常行为与发送报告。其有助于提高学校的安全性与应急响应能力；

c) 安全救援：通过智能设备可实现紧急通信、现场勘察、物品运输等救援行为，在事故或灾难场景下，为学生和教职员工提供必要的救援；

5.3.2 固定平台

固定平台主要负责校园室内场景下的监控与通信行为，是保障校园安全的另一个关键点。应实现的功能包括但不限于：

a) 时空监控：在室内场景下通过终端设备利用时间和地理位置数据监控各种活动和事件，为校园安全平台提供更全面的安全管理和监控手段；

b) 室内安防：通过视频监控系统、门禁系统、紧急通信系统等措施确保校内各个室内区域的安全和管辖，防止不法入侵、监测学生和工作人员的安全，并应符合 GB/T 29315 的要求；

c) 危险预警：对视频监控、声音监控等多源数据进行智能检测、分析，一旦检测到异常或潜在安全风险，可自动触发警报，并向学校管理人员、安保团队和相关负责人员发送通知；

5.3.3 人工智能模块

AI模块主要负责人工智能算法部分的实现，作为整个智慧校园安全平台的核心之一，是产生系统决策的重要支撑。应实现的功能包括但不限于：

a) 人脸识别：平台可以使用面部识别技术，识别学生、教职员工和访客，确保只有授权人员能够进入校园或特定区域，是实现校园安全系统中角色管理落实的关键；
b) 轨迹查询：基于时空监控和 AI 识别功能可对人员进行历史轨迹和事件的追溯和查询，便于对可疑人员的轨迹进行快速检索，提高追查效率；
c) 行为分析：基于时空监控、AI 数据分析、AI 异常检测等智能算法对多源数据中的特定人员行为进行分析、判断、预测是否发生危险或存在潜在危险行为；
d) 灾情检测：通过 AI 识别功能对固定平台和移动平台中的视频画面进行烟雾、火灾以及地面塌陷等灾情的检测并进行及时的消息推送；

5.4 管理中心

管理中心主要负责智慧校园安全平台中全局的感知、决策、控制，对全部平台进行一个总体协调、指挥的中心组织。应实现的功能包括但不限于：

a) 多模融合感知：利用各种感知技术，包括视觉、声音、 温度、气象、GIS 信息、入侵检测传感器等来获取不同类型的信息，并且将收集的多源数据整合到统一校园安全平台内，以便进行综合分析；
b) 平台协同联动：具备对校园平台内的多个应用平台进行统一调度、联动控制和快速协作。并且支持一定范围内的不同平台的数据资源互联互通，共享和交换；
c) 全局决策控制：构建完整校园安全状态的分析、研判与预警的综合决策控制中心，实现校园安全平台的智能化管理与科学化指挥；

5.5 终端门户

终端门户为校园内学生、教职员工、监护人和其他相关人员提供安全方面信息和服务的平台门户，通过计算机页面浏览器、移动端系统、远程访问等方式接入访问以获取资源和相关服务。应实现的功能包括但不限于：

a) 获取安全信息：各个用户可在校园安全平台上了解发布的通知和公告，了解校园内的安全信息、紧急事件和安全政策的更新，以提高用户的安全知识和意识；
b) 获取用户轨迹：可为监护人以及教职员工等用户提供学生的一段时间内的活动轨迹并且通过平台可以提供给用户权限内的学生的多源数据信息，让更多人参与到校园安全活动中以增强校园安全性；
c) 提供信息：用户可在校园安全平台上报告校内的危险点信息或者遇到危险在平台上进行呼救，平台接收用户的信息并给予及时的反馈与帮助，加强了用户对校园安全的参与度；

5.6 安全与保障体系

在考虑平台安全、稳定运行的基础上，为智慧校园安全平台系统构建统一的安全与保障系统，应实现的功能包括但不限于：

a) 数据安全：确保学生和教职员工的个人数据和隐私得到充分保护，遵守相关法律和法规的要求，如 GDPR 或 HIPAA 等；

b) 访问安全：实施强大的身份验证和访问控制措施，以确保只有授权用户能够访问特定信息和功能，并且校外访问只能通过特殊 VPN；
c) 网络安全：加强网络安全措施，包括防火墙、入侵检测系统、反病毒软件等，以防止网络攻击和数据泄露，并应符合 GB/T 22239-2019 的要求；
d) 物理安全：对服务器和数据中心实施物理安全措施，以保护服务器和存储设备免受未经授权的访问；

5.7 运行体系

构建校园安全运行管理体系，保证安全平台的有序运行，并规范平台的运行体系，明确各方职责。应实现的功能包括但不限于：

a) 制度管理：应制定详细的校园安全平台运行体系管理制度、平台维护制度等明确职责和运行管理流程，并且定期检查平台安全问题；
b) 人员管理：应明确平台管理人员的职责、工作范围、资源权限、数据安全，并且制定对应的人员储备计划、考核计划、保密计划等；
c) 运行管理：应对校园安全平台进行日常的系统检测、安全检查、备份等活动，并且建立应急机制，制定多种应急预案，保障系统在任何场景下都能安全、稳定的运行；
d) 监管管理：应建立多层次、多维度的监管机制、多级预警机制和问题反馈机制，确保平台的运行透明、合规和高效以及用户人员能上报问题并得到解决；

全国团体标准信息平台

参 考 文 献

[1]GB/T 36342-2018 智慧校园总体框架
[2]DB43/T 1669-2019 校园安全技术防范系统建设规范

全国团体标准信息平台