ICS 35.240.99
CCS L 77

T/CASME

中 国 中 小 商 业 企 业 协 会 团 体 标 准

T/CASME XXXXX—2023

空巢老人智能安全守护系统

Intelligent security guard system for empty-nesters

（征求意见稿）

2023－XX－XX 发布　　2023－XX－XX 实施

中国中小商业企业协会　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。

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。

本文件由中国中小商业企业协会提出并归口管理。

本文件主要起草单位：杭州极至科技有限公司。

本文件参与起草单位：杭州极兴物联有限公司 、杭州软信技术咨询服务有限公司。

本文件主要起草人：　王怡翔、蔡婧、强尊慧、孙钢宇、蔡祺、王薇、胡思兵。

空巢老人智能安全守护系统

1 范围

本文件规定了空巢老人智能安全守护系统的术语和定义、系统总体架构、功能要求、性能要求、云计算能力等技术规范。

本文件适用于居家单独生活的空巢老人的安全守护。

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 28448 《信息安全技术 网络安全等级保护测评要求》

GB/T 33745 物联网 术语

GB/T 35273 信息安全技术 个人信息安全规范

3 缩略语

下列缩略语适用于本文件。

VPN	虚拟专用网络	Virtual Private Network
ADE	自动体外除颤器	Automatic external defibrillator

4 术语和定义

GB/T 33745中界定的以及下列术语和定义适用于本文件。

4.1

智能安全守护系统(intelligent security guard system)

综合运用信息技术、大数据分析技术、物联网技术、智能红外感知技术，配合主动感知设备和触发式感知设备，监护老人的行为、位置、活动状况等数据，综合判断老人是否发生意外，并做出应急处理。

4.2

身份感知设备(sensing device)

通过读写设备对附加在对象(环境、设备等)上的身份信息进行识别和统一编码的能力，以实现采集或修改对象相关信息的设备。

4.3

位置感知设备（location perception device）

对设备、人员的位置信息进行采集的设备，包括出入感应器、人体红外探测器等。

4.4

环境感知设备（environment perception device）

采集与人体健康指数相关的基本环境状态信息的设备，包括水流传感器、火灾感应器、燃气感应器等。

4.5

跌倒感知设备（security perception device）

对人员安全信息、行为信息进行采集和上报的设备，包括跌倒传感器等。

4.6

安全控制设备（security control device）

对安全信息进行告警、通知、提示的设备，包括烟温火灾报警器、危险指示灯、声音报警器、语音提示器、视觉警告器等。

4.7

音视频感知设备 （audio and video information perception device）

环境、人员等进行音频、图像、视频采集，并进行数字化编码的设备，包括红外摄像头、视频摄像头等。

4.8

智能硬件设备（intelligent hardware device）

具备感知、联网、人机交互、后台服务支撑等功能的设备总称，包括智能门锁、智能灯具、智能开关、智能插座等。

4.9

健康监测设备（health monitoring equipment）

对人体基本生命体征参数和基本健康参数持续采集的设备，包括非接触红外传感器等。

4.10

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。

5 系统总体架构

空巢老人智能安全守护系统总体架构包括感知层、传输层、应用层三层架构设计（如图1），感知层主要完成数据采集处理，传输层将数据传输至应用层，应用层对家庭环境数据进行存储和分析，将数据上传至云数据库，进而实现独居老人环境的监测、电话、短信、微信小程序通知等。

图 1 空巢老人智能安全守护系统总体架构图

6 功能要求

6.1 信息管理

信息管理包含以下内容：

a) 包含老年人的基本信息、家庭情况、健康状况等基础信息；

b) 支持老年人基础信息的登记、变更、注销；

c) 可实现老人对应的监护人、网格员、物业、志愿者等信息的批量输入和绑定/解绑管理，有效实现不同层级的统一管理。

6.2 人数监测

通过红外感应设备和基于动态捕捉技术开发的人体活动目标检测网络，实时监测老人家中的人体活动，并将人数的活动数据实时发送至系统云平台。

6.3 位置监测

位置监测包含以下内容：

a) 采用独立式出入传感器，通过其智能红外感应无线监测老人的位置、活动状态等数据；

b) 由位置监测算法判断老人的位置、是否发生意外；

c) 将数据通过无线传输至系统云平台。

6.4 环境监测

环境监测包含以下内容：

a) 通过坐便器上的水流量传感器监测坐便器水流大小、水流时长；

b) 通过燃气传感器监测可燃气体含量；

c) 通过温度传感器监测灶台点火、熄火状态、锅具是否烧干状态；

d) 将数据通过无线传输至系统云平台。

6.5 跌倒监测及预警

跌倒监测及预警包含以下内容：

a) 通过智能红外的跌倒感应器和出入感应器收集空巢老人活动高度及范围数据，由跌倒监测算法判断老人是否跌倒；

b) 将判断结果通过无线网络传输到系统云平台；

c) 系统云平台按照预先设定的程序进行数据分析和应急处理；

d) 程序自动通过短信电话微信小程序消息等形式逐级通知其监护人、物业和社区。

6.6 健康状态监测

运用非接触红外感知等技术监护老人的居家活动状况，通过大数据分析老人日常活动行为，自动生成基本健康模型参数，综合比较近期活动数据后判断老人是否发生意外，可及时掌握老人的健康趋势情况，预防突发疾病。

6.7 安全控制

通过火灾报警器、烟雾报警器、燃气泄漏报警器、SOS 一键呼救对安全信息进行告警，并将警告信息以微信、短信或电话的形式通知内设的多级救援联系人，通过操作信息、定位信息对预警处理进度实时跟踪，直至获得响应及相应救援。

6.8 一键呼救

通过安装一键呼救SOS按钮应对老人可能产生的突发情况，在来不及进行主动呼救时及时响应，无需复杂操作，按下按钮自动呼救，软件实时通过检测SOS感应器状态改变，立即通知其监护人或社区管理人员，做到及时救助响应。

6.9 紧急救援

当独居老人在家中发生意外时，以微信、短信或电话的形式通知内设多级救援联系人，通过操作信息、定位信息对预警处理进度实时跟踪，直至获得响应，救援结束。

6.10 急救设备地图

利用现代地图技术和实时数据采集分析技术，显示特定地区或城市急救设备（如AED设备）、急救资源的分布和实时使用情况的地图系统，实现当地应急救援。

6.11 智能钥匙托管

对有需要的住户选配智能钥匙盒，实现钥匙智能托管。

6.12 智能群组协同

当接到报警时，系统智能建群并接入相关监护人和救助人员，群组系统内共享救援信息，自由发送语音、文字、图片、视频等，永久追溯，实现闭环管理。

6.13 设备智能运维

设备及传感器定时自检，并上报设备状况，对功能性损坏、缺失和低电量进行智能提示，实现所属设备运维管理、自动化派单和分单管理、故障类型设置管理、流程模板管理、分单规则智能化设置等。

7 性能要求

7.1 硬件性能

a) 智能网关内置4G模块和物联网卡无需额外搭建网络；

b) 智能网关内置边缘计算程序，可以过滤部分大部分无效数据，和本地化应急响应处理；

c) 本地预警功能，发生火灾和燃气泄漏情况，设备上报数据同时本地会进行蜂鸣预警，提醒住户；

d) 硬件外壳采用压铸一体打造，具有基础防水防雨功能；

e) 传感类设备内置大容量电池，无需外接电源，可超长待机一年以上。

7.2 系统性能

7.2.1 响应时间

系统响应时间应满足以下要求：

a) Web 端各功能模块的访问页面加载时间应小于 0.5s；

b) 安卓移动端各功能模块的访问页面加载时间应小于 0.5s；

c) IOS 移动端各功能模块的访问页面加载时间应小于 0.5s。

7.2.2 所支持的并发接入量

平台并发数应满足以下要求：

a) 检查列表查询响应时间 7 秒内，并发要求 10s；

b) 二维码扫一扫响应时间 7 秒内，并发要求 10s；

c) 检查详情响应时间 7 秒内，并发要求 10s；

d) 登录并发响应时间 7 秒内，并发要求 10s。

7.3 网络性能要求

7.3.1 传输带宽

专用带宽不小于2MB。

7.3.2 网络延时

不大于500ms。

7.4 安全性

7.4.1 安全管理制度

安全管理制度应满足一下要求：

a) 应提供系统、健全的信息安全管理制度，并对信息安全管理制度中的主要部分进行披露；

b) 应提供安全管理制度的版本修订记录，并根据应用情况及时更新和完善安全管理制度。

7.4.2 访问安全

7.4.2.1 用户访问安全

用户访问安全应满足以下要求：

a) 应提供用户注册和注销机制：用户账号创建、激活、修改、审查、禁用和删除账号等机制；

b) 应提供用户权限管理机制：配置和修改账号权限；

c) 应提供用户密码管理机制：输入密码时隐藏显示；

d) 应提供用户权限管理机制：包含配置和修改账号权限，密码异常提示及修改，修改密码需用户验证、密码须满足一定的复杂度(长度在 16 字符内不少于 8 个字符,特殊符号、数字，字母等组合)；

e) 支持用户访问权限审查：未登录时，应提供及时调整用户访问权限的功能。

7.4.2.2 网络访问安全

网络访问安全应满足以下要求：

a) 具有入侵检测功能，一旦发现可疑连接、非法访问等，针对入侵采取的措施包括实时报警、自动阻断通信连接或执行用户自定义的安全策略；

b) 具备定期安全漏洞检查功能；

c) 应提供网络隔离机制：与外部网络连接的地方、以及内部与其他信息系统之间，应设置网关或防火墙来保障网络隔离；

d) 应提供网络连接控制机制：根据业务应用的要求，限制用户连接到内部网络的能力；

e) 平台可部署防病毒软件且具备病毒查杀、 病毒库自动更新功能；

f) 提供平台操作日志记录功能， 日志保存时间不少 6 个月。

7.4.3 系统安全

系统安全防护应满足以下要求：

a) 应提供防火墙、漏洞扫描、病毒防治和入侵检测等安全防护。

b) 应制定适用于应用系统与安全设备配置的安全规范或软件安全开发规范，并且承诺能够对相关系统的 Web 应用服务和相关协议及时修复已公布的漏洞。

c) 应提供详细的云端数据操作日志，包括:上传、修改、删除、下载、恢复改等变更操作，并确保操作记录可以被追溯。

7.4.4 数据安全

7.4.5 数据管理及存储安全

数据管理及存储安全应满足以下要求：

a) 确保用户数据、 用户信息等存储与管理遵循国家相关规定；

b) 确保数据存储和数据迁移中具有完整性保护措施；

c) 具有对敏感数据进行加密存储、加密使用的功能；

d) 数据库应具备审计功能，并进行定期审计，审计周期不得超过 6 个月，审计日志保存时间不少于 6 个月；

e) 用户终止服务时，除非有特殊约定，平台应立即将用户数据彻底删除。

7.4.6 数据传输安全

数据传输安全应满足以下要求：

a) 应对重要数据进行加密传输；

b) 传输过程中应对敏感数据进行加密；

c) 对数据传输过程中的业务数据进行完整性校验。

7.4.7 身份验证安全

身份验证安全应满足以下要求：

a) 支持密码登录，且密码支持加密传输；

b) 支持身份认证、短信验证登录方式（可选）；

c) 支持用户权限管理，通过用户权限的设置来实现用户隐私安全和数据安全。

7.4.8 用户隐私安全

用户隐私安全应满足以下要求：

a) 对系统中敏感数据范围进行说明的文档资料；

b) 对患者的基本信息、病例资料与影像数据采取隔离措施，实现分别存储；

c) 支持创建患者信息，并进行一一验证；

d) 建立用户个人信息收集保护及用户授权告知制度；

e) 满足个人信息主体授权同意的目的所需的最少个人信息类型和数量,检查用户的个人信息，包括个人敏感信息、 社会关系信息、位置信息、发布的信息及使用业务行为信息；目的达成后，应及时删除个人信息；

f) 在数据分析和挖掘过程中，应对数据脱敏。

7.5 可靠性

可靠性应满足以下要求：

a) 支持每周 7 天，每天 24 小时的服务；

b) 应具备数据容灾备份机制，保障系统自动转移并恢复负载均衡的能力；

c) 应具备故障实时监测、异常报警、故障自恢复机制，保证系统正常运行；

d） 应支持根据数据的重要性和数据对系统运行的影响，确定数据的备份和恢复策略。

7.6 兼容性

兼容性应满足如下要求：

a） 浏览器版本 IE 8 以上

b） 支持数据的输入、传输、保存等；

c） 符合保存图像不可用有损压缩的方式保存、传输或调阅；

d） 网页内容在主流操作系统或浏览器下运行正常，并支持现有的辅助工具和其他用户代理。

8 云平台服务能力

8.1 云服务可用性

云服务可用性要求如下：

a） 平台系统支持 7*24 小时自动化运维；

b） 支持海量物联网设备及数据高并发处理。

8.2 云服务开放性

云服务的开放性要求如下：

a） 支持不同格式不同长度的设备通讯协议通讯；

b） 支持二次开发能力；

c） 支持数据系统的本地化私有化部署；

d） 支持 AIGC 生成式人工智能个性化响应和服务；

e） 支持第三方公众号，小程序对接；

f） 支持第三方数据融合提供数据迁移和数据清洗服务。

8.3 网络架构要求

网络架构要求如下：

a） 实现不同云服务客户虚拟网络之间的隔离；

b） 具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

c） 提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；

d） 支持第三方公众号，小程序对接。

8.4 云服务安全性

云服务安全性应符合 GB/T 28448《信息安全技术 网络安全等级保护测评要求》中规定内容。

8.5 云服务故障恢复能力

云服务故障恢复能力要求如下：

a) 具有运维管理系统，可自动产生报表和运维报告，定期自动发送给用户，故障报警信息可通过邮件/短信即时发送；

b) 具备容灾备份能力；

c) 具备故障管控机。