

T/CASME

中国中小商业企业协会团体标准

T/CASME XXXX—2023

智慧物业与物联网平台建设要求

Intelligent property and IOT platform construction requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

中国中小商业企业协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 建设原则 1

5 总体要求 2

6 网络要求 2

7 设备要求 3

8 数据要求 4

9 应用要求 4

10 其他要求 6

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××××提出。

本文件由××××归口。

本文件起草单位：××××

本文件主要起草人：××××

智慧物业与物联网平台建设要求

1 范围

本文件规定了智慧物业与物联网平台建设的术语和定义、建设原则、总体要求、网络要求、设备要求、数据要求、应用要求和其他要求等内容。

本文件适用于智慧物业与物联网平台建设。

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 33905.2 智能传感器 第2部分：物联网应用行规
- GB/T 34068 物联网总体技术 智能传感器接口规范
- GB/T 34069 物联网总体技术 智能传感器特性与分类
- GB/T 34070 物联网电流变送器规范
- GB/T 34071 物联网总体技术 智能传感器可靠性设计方法与评审

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧物业 smart property

是指以现代科学技术特别是信息技术、移动技术、语音技术为主要支撑，建立在传统物业服务基础上的新的商业模式、服务方式和管理方法的物业服务企业。

3.2

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.3

消息队列遥测传输 message queue telemetry transmission (MQTT)

是ISO标准（ISO/IEC PRF 20922）下基于发布/订阅范式的消息协议（以下简称MQTT）。它工作在TCP/IP协议族上，是为硬件性能低下的远程设备以及网络状况糟糕的情况下而设计的发布/订阅型消息协议，为此，它需要一个消息中间件。MQTT是一个基于客户端-服务器的消息发布/订阅传输协议。

3.4

CoAP 协议 the constrained application protocol

是一种计算机协议，应用于物联网，基于REST架构。

4 建设原则

4.1 先进性

系统设计及平台建设应采用先进的技术、方法和设备。既应反映当今先进技术水平，又应具备发展潜力。

4.2 可靠性

系统设备应保证连续可靠运行，当某一现场设备发生故障时，不影响整个系统的可靠运行。

4.3 便捷实用性

系统设计及平台建设应面向需求，实用主导；系统的操作和维护应简便、易掌握，并具有友好的、直观的用户界面。

4.4 经济性

在实现系统先进、可靠的前提下，还应考虑系统投资的经济性，使系统具有较高的性价比。系统配置除考虑建设时的一次性投资外，还应充分考虑系统的运行成本，并使之达到最小化。

5 总体要求

- 5.1 物联网建设应符合 GB/T 33905.2、GB/T 34068、GB/T 34069、GB/T 34070、GB/T 34071 的规定。
- 5.2 物业管理中的物联网通信应符合低功耗、远距离、大量连接等要求。
- 5.3 应提供相应的技术措施，保证物联网安全。
- 5.4 应结合智能控制系统的建设情况，合理部署感知设备，并保证感知设备有效接入物业物联网，实现设备、网络 and 系统之间的互联互通。
- 5.5 应支持智慧物业管理，包括但不限于物业服务、安全监控、设备管理、能源管理等功能。
- 5.6 应具备高可用性、高扩展性、高安全性等特点，确保系统能够长期稳定运行。
- 5.7 应支持多种终端设备接入，包括但不限于传感器、智能家居设备、智能门禁等。
- 5.8 应支持数据采集、存储、处理和分析，提供实时监测、预警和决策支持等功能。

6 网络要求

6.1 网络架构设计

6.1.1 可靠性

- 6.1.1.1 网络架构应具备高可靠性，能够保障系统的稳定运行。
- 6.1.1.2 应采用冗余设计、备份设备和链路，以确保网络的可靠性和容错能力。

6.1.2 扩展性

- 6.1.2.1 网络架构应具备良好的扩展性，能够满足未来系统功能和规模的扩展需求。
- 6.1.2.2 应采用模块化设计、可扩展的网络设备和协议，以便系统的持续发展和扩展。

6.1.3 安全性

- 6.1.3.1 网络架构应考虑系统的安全性需求，包括网络防火墙、入侵检测与防御系统等安全措施。
- 6.1.3.2 应采用加密技术和身份认证机制，保护网络通信和数据的安全。

6.1.4 带宽与延迟

- 6.1.4.1 网络架构应根据系统的需求和数据流量，合理规划和配置网络带宽，以确保系统的数据传输和响应效率。
- 6.1.4.2 应控制网络延迟，提供良好的用户体验。

6.2 网络设备选择与配置

6.2.1 路由器与交换机

- 6.2.1.1 应选择高性能、可靠的路由器和交换机设备，能够提供高速的数据传输和稳定的网络连接。
- 6.2.1.2 应根据网络规模和需求，合理配置路由器和交换机的数量和位置。

6.2.2 网络安全设备

应选择适当的网络安全设备，如防火墙、入侵检测与防御系统等，保护网络免受恶意攻击和未经授权访问。

6.2.3 网络存储设备

应根据系统的数据存储需求，选择可靠的网络存储设备，提供高容量和可扩展的存储空间。

6.3 网络监控与管理设备

6.3.1 网络安全要求

6.3.1.1 访问控制

应实施严格的访问控制机制，包括身份认证、授权和权限管理，确保只有授权的用户才能访问系统和数据。

6.3.1.2 数据加密

应采用加密技术保护网络通信和数据传输的安全性。对敏感数据和用户隐私进行加密存储和传输，防止数据泄露和篡改。

6.3.1.3 安全审计与监控

应建立安全审计和监控机制，对网络和系统进行实时监测和日志记录，及时发现和响应安全事件和威胁。

6.3.1.4 安全培训与意识

应开展安全培训和意识提升活动，加强员工和用户对网络安全的认识 and 意识，防范社会工程学攻击和用户疏忽导致的安全风险。

6.4 网络性能监测与优化

6.4.1 性能监测

应建立网络性能监测系统，实时监测网络带宽利用率、延迟和丢包率等关键指标，及时发现和解决网络性能问题。

6.4.2 带宽管理与优化

应合理规划和管理网络带宽，通过流量控制、带宽分配和负载均衡等措施，优化网络带宽的使用效率。

6.4.3 延迟优化

应通过网络设备配置和优化，减少网络传输的延迟，提升系统的响应速度和用户体验。

6.4.4 故障恢复与备份

应建立网络故障恢复和数据备份机制，确保在网络故障和数据丢失时能够及时恢复系统功能和数据。

7 设备要求

7.1 智能设备选择与集成

7.1.1 设备类型

应选择符合系统需求的智能设备，包括传感器、执行器、智能终端等，能够获取物业环境信息、控制设备操作和与用户进行交互。

7.1.2 通信协议

设备应支持常用的物联网通信协议，如MQTT、CoAP等，以实现设备之间的互联和数据传输。

7.1.3 兼容性

设备应具备良好的兼容性，能够与平台和其他设备进行无缝集成和通信。确保设备能够与不同厂商和型号的设备进行互操作。

7.1.4 可靠性与稳定性

选择具备高可靠性和稳定性的设备，能够长时间稳定运行，抵抗恶劣环境和干扰。

7.1.5 安全性

设备应具备安全功能和机制，包括数据加密、身份认证和访问控制等，保障设备和系统的安全性。

7.1.6 数据质量与准确性

设备应提供准确可靠的数据，通过校准和数据校验等手段，确保数据的质量和可信度。

7.2 设备安装与调试

7.2.1 安装位置与布局

应根据设备的功能和要求，合理选择安装位置和布局，确保设备能够有效获取数据和实施控制。

7.2.2 连接与配置

应正确连接设备的电源、通信线路和传感器等，进行设备的配置和参数设置，确保设备能够正常工作 and 与平台通信。

7.2.3 故障排除与修复

应针对设备安装过程中可能出现的故障和问题，进行及时排除和修复，保障设备的正常运行和性能。

7.2.4 调试与校准

应对设备进行调试和校准，确保设备输出的数据准确可靠，与实际环境相匹配。

7.3 设备管理与监控

7.3.1 设备信息管理

应建立设备信息管理系统，对设备进行统一管理和维护，包括设备的基本信息、配置参数和状态监测等。

7.3.2 运行状态监测

应实施设备的运行状态监测和故障预警，及时发现和解决设备故障和异常情况，确保设备的正常运行。

7.3.3 远程监控与控制

应通过物联网平台实现对设备的远程监控和控制，包括数据采集、设备状态查询和远程操作等，方便管理和维护人员对设备进行远程管理。

7.3.4 维护与保养

应建立设备维护和保养计划，定期对设备进行检查、清洁和维护，延长设备的使用寿命和保持其正常运行。

8 数据要求

8.1 应支持数据的实时采集、存储和处理，确保数据的准确性和实时性。

8.2 应支持数据分析和挖掘，包括但不限于数据建模、数据可视化、数据挖掘等，为智慧物业管理提供数据支持和决策依据。

8.3 应支持数据的隐私保护和安全存储，确保个人隐私和敏感信息不被泄露。

9 应用要求

9.1 功能需求

9.1.1 物业管理

应提供全面的物业管理功能，包括楼宇管理、设备维护、安全监控、资源调配等，以提高物业管理的效率和质量。

9.1.2 能源管理

应支持能源消耗的监测和分析，优化能源使用，减少能源浪费，实现能源的可持续利用。

9.1.3 环境监测

应实时监测室内外环境参数，包括温度、湿度、空气质量等，提供环境数据分析和预警功能，改善居住和工作环境。

9.1.4 安全与保障

应提供安全监控、入侵检测、火灾报警等功能，保障居民和工作人员的安全与生命财产安全。

9.1.5 智能控制

应实现对设备和系统的智能控制和调节，包括照明控制、空调控制、门禁控制等，提升生活和工作的便利性和舒适性。

9.1.6 数据分析与决策支持

应对采集的数据进行分析和挖掘，提供决策支持和预测功能，帮助管理者优化资源配置和制定合理的决策策略。

9.2 用户界面与交互体验

9.2.1 界面设计

界面应具备直观、简洁和易用的特点，符合用户习惯和操作习惯，提供友好的用户体验。

9.2.2 多终端适配

应支持不同终端设备的适配，包括PC、手机、平板等，确保在不同设备上都能够正常访问和使用。

9.2.3 交互方式

应提供多种交互方式，包括触摸屏、语音识别、手势控制等，方便用户进行操作和控制。

9.2.4 个性化定制

应支持用户个性化的界面定制和设置，满足不同用户的需求和偏好。

9.3 数据隐私与安全

9.3.1 数据隐私保护

应确保用户的个人信息和隐私数据得到有效的保护，采取数据加密、权限管理等措施，防止数据泄露和滥用。

9.3.2 安全认证与访问控制

应建立严格的安全认证和访问控制机制，确保只有经过授权的用户才能访问系统和相关数据。

9.3.3 数据备份与恢复

应建立数据备份和恢复机制，定期对数据进行备份，确保在数据丢失或系统故障时能够及时恢复数据。

9.3.4 安全审计与监控

应建立安全审计和监控机制，对系统和用户的操作进行实时监测和日志记录，及时发现和响应安全事件和威胁。

9.4 智能化与创新性

9.4.1 智能算法与学习

应应用智能算法和机器学习技术，对数据进行分析和学习，提供智能化的决策和优化功能。

9.4.2 人工智能与自动化

应引入人工智能和自动化技术，实现自动化控制和智能化服务，提高效率和便利性。

9.4.3 创新应用场景

应探索和创新各类应用场景，满足不同用户的需求，提供个性化和差异化的服务。

9.4.4 互联互通与生态整合

应实现不同应用系统之间的互联互通，打造开放的生态系统，促进资源共享和协同创新。

10 其他要求

10.1 兼容性与互操作性

10.1.1 硬件兼容性

平台应与不同厂商和型号的硬件设备进行兼容，确保平台能够与各类设备无缝集成和通信。

10.1.2 软件兼容性

平台应与不同软件系统进行兼容，支持与其他应用系统的集成和数据交换。

10.1.3 数据格式与协议兼容性

平台应支持多种数据格式和通信协议，以便与其他系统进行数据交换和共享。

10.1.4 互操作性

平台应与其他物联网平台或系统进行互操作，实现跨平台的数据共享和协同操作。

10.2 可扩展性与灵活性

10.2.1 硬件扩展性

平台应支持灵活的硬件扩展，能够方便地添加新的设备和模块，满足未来的功能扩展需求。

10.2.2 软件扩展性

平台应支持软件功能的扩展和定制，通过插件或模块化的方式，方便地添加新的功能模块。

10.2.3 系统配置与定制

平台应支持系统配置和定制，根据实际需求进行灵活的配置和定制化开发，满足不同用户的特定需求。

10.2.4 灵活部署与管理

平台应支持灵活的部署和管理方式，包括云端部署、边缘计算等，根据实际情况选择合适的部署方案。

10.3 持续改进与优化

10.3.1 性能优化

应不断优化平台的性能，提高数据处理和响应速度，提升用户体验和系统效率。

10.3.2 功能更新与升级

应根据市场需求和用户反馈，及时更新和升级平台的功能，引入新的技术和特性。

10.3.3 安全漏洞修复

应定期对平台进行安全漏洞扫描和修复，确保平台的安全性和稳定性。

10.3.4 用户培训与支持

应提供系统培训和技术支持，帮助用户熟练使用平台，并解决遇到的问题和困难。

10.4 法律与合规要求

10.4.1 数据隐私与保护

应遵守相关的数据隐私法律法规，保护用户的个人隐私和数据安全。

10.4.2 信息安全与防护

应建立完善的信息安全管理制度，采取有效的安全措施，防止信息泄露和网络攻击。

10.4.3 知识产权保护

应尊重知识产权，不侵犯他人的版权、专利等知识产权。

10.4.4 合规运营

应遵守当地相关法律法规，合规运营平台，并及时跟进和遵守相关法规的更新和调整。
