ICS 35.240.01
CCS L 70

T/ZPP

团　　体　　标　　准

T/ZPP 145—2025

既有建筑安全物联网监测系统建设规范

Construction Specifications for the Internet of Things Monitoring System of Existing Building Safety

2025－06－27 发布　　2025－06－30 实施

浙江省品牌建设促进会　　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专利的责任。

本文件由杭州同杭云督信息科技有限公司提出。

本文件由浙江省品牌建设促进会归口。

本文件起草单位：杭州同杭云督信息科技有限公司、天坤营造（嘉兴）股份有限公司、浙大城市学院、嘉兴南湖学院、汇才企服（嘉兴）信息科技有限公司、中科华创（嘉兴）信息科技有限公司、嘉兴市软件行业协会。

本文件主要起草人：李晶晶、褚天云、丁杨、吴煜祺、谭君秋、张彭飞、应秀洁。

既有建筑安全物联网监测系统建设规范

1 范围

本文件规定了既有建筑安全物联网监测系统建设的术语和定义、系统架构要求、监测内容与指标、感知设备技术要求、数据管理系统、网络安全体系。

本文件适用于既有建筑安全物联网监测系统建设。

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 9254.1 信息技术设备、多媒体设备和接收机 电磁兼容 第1部分：发射要求

GB/T 10058 电梯技术条件

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB 50174 数据中心设计规范

GB 50292 民用建筑可靠性鉴定标准

GB/T 50452 古建筑防工业振动技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

既有建筑 existing buildings

指已建成并投入使用的建筑物，未经整体拆除重建或结构主体重大改造。

3.2

物联网 internet of Things

指通过信息传感设备按约定协议实现物与物、物与人的泛在网络互联与数据交互的技术体系。

4 系统架构要求

4.1 总体架构设计

4.1.1 既有建筑安全物联网监测系统应采用分层架构设计，由感知层、网络层、平台层及扩展应用层组成，各层级间应实现数据高效交互与功能协同。

4.1.2 系统架构设计应遵循模块化原则，支持功能扩展与设备兼容，且宜采用标准化协议接口，便于与既有建筑管理系统集成。

4.1.3 系统应满足实时性、可靠性与安全性要求，关键功能模块应具备冗余设计。

4.2 感知层设计要求

4.2.1 感知层应由传感器、数据采集终端及边缘计算设备组成，应具备物理量采集、数据预处理及本地存储功能。

4.2.2 传感器选型应符合下列要求：

——应适配既有建筑结构特征与环境条件，精度等级不应低于行业标准规定的限值；

——宜优先采用无线传输方式，若需有线部署，应避免对建筑结构造成二次损伤；

——在高温、高湿、振动等复杂环境下，传感器防护等级应达到 IP65 及以上。

4.2.3 数据采集终端应满足多源异构数据接入需求，支持 RS-485、LoRa、NB-IoT 等通信协议，且宜内置数据缓存机制，确保网络中断时数据不丢失。

4.2.4 关键监测部位的感知设备部署应冗余配置，单一设备故障不应导致监测功能失效。

4.3 网络层设计要求

4.3.1 网络层应实现感知层与平台层间的数据传输，并满足以下要求：
——应支持有线与无线混合组网方式，网络覆盖率应达到监测区域 95%以上；
——传输协议宜采用 MQTT、CoAP 等轻量级物联网协议，降低通信能耗；
——数据传输过程应加密，符合 GB/T 22239 中三级及以上安全标准。
4.3.2 无线网络部署时，应规避既有建筑中金属结构、电磁设备等干扰源，必要时宜采用多频段自适应技术。
4.3.3 网络层应具备链路自愈能力，单点故障恢复时间应小于 5 min。

4.4 平台层设计要求

4.4.1 平台层应包含数据管理、分析预警及可视化模块，并符合以下规定：
——数据管理模块应支持海量数据存储与快速检索，原始数据存储周期不应少于 5 年；
——分析预警模块应内置结构安全评估算法，实现多参数融合分析与分级预警；
——可视化模块应提供建筑三维模型动态展示、历史数据趋势分析及报表自动生成功能。
4.4.2 平台应支持分布式部署架构，核心服务器宜采用双机热备模式，确保系统连续运行可用性不低于 99.9%。
4.4.3 平台层应开放标准化 API 接口，支持与应急管理、城市信息模型（CIM）等外部系统数据交互。

4.5 系统兼容性与扩展性

4.5.1 系统应兼容既有建筑中已部署的监测设备，通过协议转换网关实现数据集成，避免重复建设。
4.5.2 系统设计宜预留不少于 20%的硬件扩展容量及软件功能接口，适应未来监测需求变化。
4.5.3 软件平台应支持模块化升级，功能扩展不应影响既有监测业务正常运行。

4.6 安全架构要求

4.6.1 系统应建立多层安全防护体系，涵盖设备认证、传输加密、访问控制及日志审计：
——感知层设备接入时应进行身份鉴权，非法设备禁止接入网络；
——网络层数据传输应使用 TLS 1.2 及以上加密协议；
——平台层用户权限管理应符合最小授权原则，操作日志保存时间不应少于 6 个月。
4.6.2 系统应定期进行漏洞扫描与渗透测试，高风险漏洞修复时间不应超过 24 h。

4.7 冗余与容灾

4.7.1 系统关键节点（如核心交换机、数据库服务器）应冗余部署，主备切换时间应小于 1 min。
4.7.2 数据存储宜采用本地与云端双备份机制，任一存储介质故障不应导致数据永久丢失。
4.7.3 网络层中断时，边缘计算设备应具备本地数据处理与告警能力，断网期间数据丢失率应小于 1%。

4.8 性能指标

系统应满足下列性能要求：
——数据采集终端至平台的数据传输延迟应小于 2 s；
——预警信息推送至相关责任人端的时间应小于 30 s；
——平台并发数据处理能力不应低于 1000 个监测点/秒。

5 监测内容与指标

5.1 一般要求

5.1.1 既有建筑安全物联网监测系统的监测内容应覆盖结构安全、环境风险、设备状态等核心维度，并应根据建筑类型、使用年限及风险评估结果确定监测重点。
5.1.2 监测指标的选取应符合 GB 50292 的要求，并宜结合建筑全生命周期管理需求动态调整。
5.1.3 监测数据采集频率、精度及传输时效性应与监测目标匹配，关键指标应实现连续或准实时监测。

5.2 结构安全监测

5.2.1 沉降与变形

5.2.1.1 应监测建筑整体沉降、差异沉降及基础变形，精度不应低于±1 mm。
5.2.1.2 对高层建筑、历史保护建筑或软土地基建筑，宜增设倾斜监测点，倾斜角分辨率不应低于 0.01°。
5.2.1.3 监测数据应与既有建筑竣工资料及历史检测记录进行对比分析。

5.2.2 裂缝与损伤

5.2.2.1 应重点监测承重墙、梁柱节点、楼板等关键部位的裂缝宽度、长度及发展趋势，裂缝宽度监测精度应达到±0.1 mm。
5.2.2.2 对已存在结构性损伤的建筑，宜采用分布式光纤或图像识别技术实现裂缝动态追踪。
5.2.2.3 裂缝扩展速率超过设计允许阈值时，系统应触发预警。

5.2.3 振动与动态响应

5.2.3.1 临近轨道交通、爆破施工区的建筑，应监测建筑振动加速度，频响范围应覆盖 0.1 Hz~50 Hz。
5.2.3.2 宜结合模态分析技术评估结构刚度退化，振动监测数据应满足 GB/T 50452 要求。
5.2.3.3 人员密集场所的楼盖振动监测指标宜满足舒适性规范要求。

5.2.4 荷载与应力

5.2.4.1 对大跨度钢结构、悬挑构件等应监测应力变化，传感器量程应覆盖设计荷载的 1.5 倍。
5.2.4.2 宜通过应变-应力转换模型推算构件实际受力状态，数据采样频率不应低于 10 Hz。

5.3 环境风险监测

5.3.1 温湿度与腐蚀

5.3.1.1 对混凝土碳化敏感区域或钢结构建筑，应监测环境温湿度及氯离子浓度，温度测量误差应小于±0.5 ℃。
5.3.1.2 沿海或工业污染区建筑，宜增加大气腐蚀性气体（如 SO_2 、NOx）监测。

5.3.2 地下水位与土体变化

5.3.2.1 地下室、深基坑周边建筑应监测地下水位波动，水位监测精度应达到±10 mm。
5.3.2.2 对滑坡风险区域，宜增设土压力及孔隙水压力监测点。

5.3.3 风荷载与气象灾害

5.3.3.1 高度超过 100 m 的超高层建筑应监测风压分布及风速，风速量程宜覆盖 0 m/s~60 m/s。
5.3.3.2 台风多发地区建筑，宜将气象监测数据与结构响应数据关联分析。

5.4 设备设施监测

5.4.1 机电系统

5.4.1.1 应监测电梯运行振动、轨道偏移等参数，振动加速度阈值应符合 GB/T 10058 规定。
5.4.1.2 供配电系统宜监测电缆温度、漏电流等指标，温度监测精度应达到±1 ℃。

5.4.2 消防系统

5.4.2.1 应实时监测消防水管网压力、水箱水位及报警装置状态，压力监测误差应小于±0.01 MPa。
5.4.2.2 宜通过烟感、温感等多传感器融合技术提高火灾预警可靠性。

5.4.3 幕墙与围护结构

5.4.3.1 玻璃幕墙建筑应监测开启扇闭合状态、锚固件位移及玻璃应力，位移监测精度应达到±0.5 mm。
5.4.3.2 外立面装饰构件宜设置脱落风险监测，可采用加速度传感器检测异常振动。

5.5 数据指标要求

5.5.1 数据采集频率

5.5.1.1 结构安全类监测点采样频率不应低于 1 次/分钟，动态响应监测可提高至 100 Hz。
5.5.1.2 环境类监测数据采集间隔宜设为 5 min~30 min，灾害预警期间可调整为连续采集。

5.5.2 数据同步性

5.5.2.1 多传感器协同监测时，时间同步误差应小于 10 ms。
5.5.2.2 跨区域监测系统宜采用 NTP 或 PTP 协议实现时钟同步。

5.5.3 数据存储与质量

5.5.3.1 原始数据应全量存储，压缩存储时失真率应小于 0.1%。
5.5.3.2 数据缺失率超过 5%或异常率超过 3%时，系统应自动标记并启动复核机制。

5.6 扩展监测项

5.6.1 对特殊功能建筑（如医院、数据中心），可增加楼板微振动、电磁环境等定制化监测内容。
5.6.2 采用新型材料或改造加固的建筑，宜增设材料性能退化监测。
5.6.3 扩展监测项的指标设定应通过专家论证，并报主管部门备案后实施。

6 感知设备技术要求

6.1 设备选型

6.1.1 感知设备的选型应与监测内容、环境条件及长期稳定性要求相匹配，并应符合下列规定：
——传感器精度：结构安全监测用传感器精度等级不应低于 0.5 级，环境类传感器精度误差应小于满量程的±1%；
——环境适应性：在高温（＞60 ℃）、高湿（＞90%RH）、腐蚀性环境或振动区域部署的设备，防护等级应达到 IP67 及以上；
——长期稳定性：传感器年漂移量应小于满量程的 0.5%，且宜具备自诊断功能。
6.1.2 无线传感设备应满足以下要求：
——通信模块宜支持 LoRa、NB-IoT、ZigBee 等低功耗广域协议，空旷区域传输距离不应小于 200m；
——设备应具备抗同频干扰能力，在多节点部署场景下丢包率应小于 3%；
——电池供电设备续航时间不宜低于 3 年（按 1 次/分钟采集频率计）。

6.2 安装与部署

6.2.1 传感器安装应符合既有建筑保护要求，且应避免对结构承载性能造成影响：
——承重构件安装应采用无损固定工艺，不应随意钻孔或焊接；
——隐蔽空间设备应设置检修通道，检修口尺寸不应小于 300 mm×300 mm；
——外露设备应增加防破坏保护措施。
6.2.2 设备布设位置与密度应符合下列原则：
——结构关键部位（如跨中、支座、裂缝处）应布置冗余监测点，冗余度不宜低于 20%；
——振动传感器宜避开空调机组、电梯井等持续振动源，水平安装偏差应小于±2°；
——温湿度传感器部署高度宜距地面 1.5 m，且避开阳光直射与通风死角。

6.3 数据采集与传输

6.3.1 数据采集终端应满足多类型信号接入需求：
——应支持模拟量、数字量及无线信号混合接入；
——采样频率可调范围应覆盖 0.1 Hz~1 kHz，分辨率不低于 16 位；
——宜集成边缘计算功能，可对原始数据进行滤波、降噪及特征提取。
6.3.2 数据传输应满足以下性能要求：
——网络正常时，数据从采集终端到平台层的端到端延迟应小于 5 s；
——断网期间，本地应缓存不少于 72 h 数据，网络恢复后优先补传；

——无线传输误码率应小于 10^{-6}，重传机制触发次数不应超过 3 次。

6.4 电源与功耗

6.4.1 设备供电方式选择应遵循下列原则：

——固定监测点宜采用市电供电，电源线路应设置浪涌保护与漏电保护装置；

——无线设备可采用电池或能量收集（如太阳能、振动发电）供电，电池容量衰减至 80%时应预警；

——关键节点设备应配置 UPS 后备电源，续航时间不应小于 30 min。

6.4.2 低功耗设计应满足以下要求：

——无线传感设备在休眠模式下功耗应小于 10 μA；

——动态功耗调节功能宜根据监测需求自动切换工作模式（如定时唤醒、事件触发）；

——能量收集设备应能在典型环境条件下满足日均能量供需平衡。

6.5 校准与维护

6.5.1 设备应定期校准，且符合下列规定：

——结构类传感器校准周期不应超过 12 个月，环境类设备不应超过 6 个月；

——现场校准应采用标准仪器比对法，校准结果不确定度应小于传感器允许误差的 1/3；

——校准记录应上传至平台并保存至设备报废后至少 2 年。

6.5.2 维护管理应满足以下要求：

——设备状态应实时监测，异常状态应在 1 h 内推送告警；

——户外设备宜每季度进行清洁、紧固等预防性维护；

——设备更换时应保证新旧数据时序连续性，且不得影响系统整体运行。

6.6 兼容性与扩展性

6.6.1 感知设备应支持协议兼容性扩展：

——新接入设备宜采用 Modbus、MQTT 等通用协议，私有协议需提供标准化转换接口；

——同一监测点的多品牌设备输出数据应满足量纲一致性，平台可自动归一化处理；

——设备固件应支持远程升级，升级失败时能自动回滚至稳定版本。

6.6.2 系统设计宜预留扩展能力：

——单个数据采集终端可接入传感节点数不应小于 32 个；

——无线网络应支持至少 50%的节点密度扩展；

——设备 ID 编码空间应满足 10 万级规模部署需求。

6.7 安全要求

6.7.1 设备硬件安全应符合以下规定：

——外壳材料应阻燃、耐腐蚀，金属部件应做接地处理；

——电路板应具备防雷击、防静电保护；

——线设备发射功率应符合 GB/T 9254.1 要求。

6.7.2 数据安全应满足：

——敏感数据存储应加密，加密算法强度不低于 AES-128；

——设备身份认证应采用双向验证机制，证书有效期不超过 2 年；

——固件更新包应进行数字签名，哈希值校验失败时不应安装。

7 数据管理系统

7.1 系统架构与功能

7.1.1 数据管理系统应基于模块化架构设计，包含数据采集、存储、处理、分析及可视化功能模块，并支持与外部系统互联互通。

7.1.2 系统应实现监测数据的全生命周期管理，覆盖数据采集、清洗、存储、分析、共享至归档的全

流程，且宜采用分布式技术提升处理能力。

7.1.3 核心功能模块应冗余部署，单点故障不应导致系统服务中断超过 5 min。

7.2 数据采集与预处理

7.2.1 数据采集应符合以下要求：

——应支持多源异构数据接入，包括传感器实时数据、人工巡检记录及历史档案数据；

——数据采集终端与平台间的通信协议宜采用 MQTT、HTTP/HTTPS，传输间隔可配置为秒级至小时级；

——断网场景下，边缘节点应缓存至少 72 h 数据，网络恢复后自动补传并标记断网时段。

7.2.2 数据预处理应包括：

——应自动剔除明显异常数据，清洗规则可自定义；

——宜对原始数据进行标准化处理），确保多传感器数据融合一致性；

——预处理后的数据应添加质量标签。

7.3 数据存储与管理

7.3.1 存储架构设计应满足：

——采用分层存储策略，实时数据存入时序数据库，历史数据可转存至对象存储或冷备份介质；

——原始数据全量保存周期不应少于 5 年，分析结果数据保存周期不宜少于 10 年；

——存储系统应支持横向扩展，容量预留不应低于当前需求的 50%。

7.3.2 数据管理应实现：

——建立元数据目录，明确数据来源、采集时间、设备 ID 等属性，支持多维检索；

——敏感数据（如建筑位置、结构参数）应单独加密存储，访问权限应分级控制；

——数据归档操作应记录操作人员、时间及归档路径，确保可追溯性。

7.4 数据分析与模型应用

7.4.1 数据分析功能应包括：

——应内置结构安全评估模型，模型输入参数可配置；

——宜采用机器学习技术实现异常检测，训练数据集应涵盖正常工况与典型故障场景；

——分析结果应以置信度区间形式输出，供运维人员参考决策。

7.4.2 模型管理应符合以下要求：

——算法模型应定期验证，准确率下降超过 10%时需重新训练或替换；

——用户自定义模型宜通过容器化技术部署，避免影响系统核心服务；

——模型版本应统一管理，回滚操作不应导致数据丢失。

7.5 数据可视化与报警

7.5.1 可视化界面应满足：

——应提供建筑三维模型与监测数据叠加显示，支持缩放、剖切及动态数据图层切换；

——历史数据曲线对比分析时间范围可设置为日、周、月、年，分辨率自适应调整；

——宜集成 GIS 地图功能，实现多建筑群监测状态宏观展示。

7.5.2 报警管理应符合：

——应支持多级预警，阈值可动态调整；

——报警信息应通过短信、邮件、平台弹窗等多通道推送，响应延迟应小于 30 s；

——报警处理流程应闭环管理，包括确认、处置、反馈及记录，未确认报警需逐级升级。

7.6 数据安全与隐私保护

7.6.1 数据安全防护应涵盖：

——传输数据应使用 TLS 1.2 及以上协议加密，存储数据加密强度不低于 AES-256；

——访问控制应符合 RBAC 模型，操作日志保存周期不应少于 2 年；

——外部数据共享应脱敏处理，去除可识别建筑身份的特征字段。

7.6.2 隐私保护应满足：

——含个人信息的数据应经匿名化处理，且单独存储；
——数据跨境传输应遵守《网络安全法》《数据安全法》相关规定；
——系统应定期开展数据安全风险评估，高风险漏洞需在 48 h 内修复。

7.7 系统接口与兼容性

7.7.1 接口设计应符合：
——应提供标准 RESTful API，支持 JSON、XML 等数据格式交互；
——与物联网平台对接时，宜采用 OPC UA、Modbus TCP 等工业协议；
——接口调用需身份认证，每秒最大并发数不应低于 500 次。
7.7.2 兼容性要求包括：
——应兼容主流数据库，数据迁移时格式转换损失率应小于 0.1%；
——宜支持与第三方分析工具对接，提供 SDK 开发包；
——系统版本升级应保证向下兼容，旧版本数据接口至少保留 3 年。

7.8 性能指标

系统应满足以下性能：
——数据入库吞吐量不低于 10000 条/s，查询响应时间小于 2 s；
——可视化界面刷新延迟应小于 1 s，三维模型加载时间不超过 5 s；
——系统可用性不低于 99.9%，年度计划外停机时间累计小于 8 h。

8 网络安全体系

8.1 总体要求

8.1.1 既有建筑安全物联网监测系统的网络安全体系应遵循“分层防护、主动防御、动态管控”原则，覆盖物理环境、网络通信、数据存储及业务应用全流程。
8.1.2 系统网络安全等级保护应不低于 GB/T 22239 的有关规定，并根据业务重要性实施差异化管理。
8.1.3 网络安全防护应与系统建设同步规划、同步实施、同步运维，定期开展风险评估与合规性审计。

8.2 安全物理环境

8.2.1 核心网络设备、服务器应部署在专用机房，具备防火、防水、防电磁干扰措施，温湿度控制应符合 GB 50174 的规定。
8.2.2 边缘计算节点、通信柜等户外设备应达到 IP65 防护等级，并安装防拆报警装置。
8.2.3 机房出入口应设置门禁系统，访问记录保存时间不应少于 180 天。

8.3 安全通信网络

8.3.1 应划分逻辑安全域，域间通过防火墙隔离，非授权不应跨域访问。
8.3.2 无线通信应采用 WPA3 或商用加密协议，有线网络宜部署 VLAN 技术隔离广播域。
8.3.3 网络设备应关闭非必要端口与服务，SNMP 等管理协议需启用强认证机制。
8.3.4 感知层至平台的数据传输应使用 TLS 1.2 及以上协议加密，密钥长度不低于 256 位。
8.3.5 敏感指令（如设备控制、固件升级）应双向认证，且采用一次性令牌（OTP）防重放攻击。
8.3.6 网络流量异常（如 DDoS 攻击、高频扫描）应实时监测并自动限流。

8.4 安全设备与终端

8.4.1 设备固件应具备防篡改机制，启动时进行数字签名验证，非法固件不应加载。
8.4.2 无线传感器节点应支持设备唯一标识，非法节点接入应触发隔离。
8.4.3 设备密钥应定期轮换，存储时采用硬件安全模块保护，明文不应存储。
8.4.4 终端操作系统应启用最小化服务，定期更新安全补丁，补丁滞后时间不超过 30 天。
8.4.5 远程维护需通过 VPN 接入，会话超时时间应小于 10 min。
8.4.6 终端日志应本地加密存储，容量不足时自动上传至平台并清空。

8.5 数据安全与隐私保护

8.5.1 存储数据应加密，结构化数据采用字段级加密，非结构化数据使用 AES-256 算法。
8.5.2 数据共享前应脱敏处理，去除可关联至具体建筑或个人的敏感信息。
8.5.3 数据销毁应通过覆写或物理破坏，确保不可恢复。
8.5.4 涉及人员定位、身份信息的数据需获取明确授权，且保留期限不超过 1 年。
8.5.5 数据跨境传输前应通过安全评估，并向主管部门备案。
8.5.6 系统应提供隐私数据查询、撤回及删除接口。

8.6 安全监测与应急响应

8.6.1 部署入侵检测系统实时分析网络流量，高风险行为应自动阻断。
8.6.2 日志审计范围应覆盖设备操作、用户行为及系统事件，日志记录保存时间不少于 6 个月。
8.6.3 每月生成安全态势报告，包含威胁分析、漏洞统计及处置建议。
8.6.4 制定网络安全事件分级预案，明确Ⅰ级（重大）、Ⅱ级（严重）、Ⅲ级（一般）事件处置流程。
8.6.5 Ⅰ级事件响应时间应小于 15 min，系统恢复时间目标不超过 4 h。
8.6.6 每年至少开展 1 次网络安全攻防演练，演练记录保存至下次演练后销毁。