ICS 91.060
CCS Q62

团　　体　　标　　准

T/ZIUR XXXX—XXXX

建筑新材料全流程物联网管理通则

General Rules for Whole-process IoT Management of New Building Materials

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

浙江省产学研合作促进会　　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××××提出。

本文件由浙江省产学研合作促进会归口。

本文件起草单位：

本文件主要起草人：

建筑新材料全流程物联网管理通则

1 范围

本文件规定了建筑新材料全流程物联网管理的术语和定义、总则、物联网总体架构、标识与信息采集规范、全流程物联网管控、数据管理与交互、网络与数据安全管理、运维管理。

本文件适用于各类建筑新材料从生产、仓储、运输、施工现场应用、余料回收至报废处置的全生命周期物联网数字化管控工作。

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 21740 基础地理信息城市数据库建设规范
GB/T 22081 网络安全技术 信息安全控制
GB/T 22239 信息安全技术 网络安全等级保护基本要求
GB/T 33474 物联网 参考体系结构
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
GB/T 35319 物联网 系统接口要求
GB/T 36478.3 物联网 信息交换和共享 第3部分：元数据
GB/T 36605 物联网标识体系 Ecode解析规范
GB/T 36626 信息安全技术 信息系统安全运维管理指南
GB/T 37032 物联网标识体系 总则
GB/T 37973 信息安全技术 大数据安全管理指南
GB/T 38619 工业物联网 数据采集结构化描述规范
GB/T 38662 物联网标识体系 Ecode标识应用指南
GB/T 38853 用于数据采集和分析的监测和测量系统的性能要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

物联网 internet of things(IoT)

基于感知控制设备，通过通信网络，使物理实体、人、系统和信息资源相连接，响应和处理物理和虚拟世界信息的基础设施。

[来源：GB/T 33745，3.1.1]

3.2

建筑新材料 new building material

具备节能、环保、高性能、多功能等特性，用于建筑工程的新型材料、制品及部品部件。

3.3

感知层 perception layer

物联网体系结构中，由传感器、执行器、RFID标签、摄像头等感知设备组成，实现信息采集与物理对象状态感知的层级。

3.4

标识 identification

通过使用属性、标识符等特征唯一识别一个实体的过程。

[来源：GB/T 33745，3.4.1]

3.5

标识编码 identifier coding

为对象分配具有唯一识别性的代码，用于身份识别、信息关联与追溯管理。

3.6

智能管控 intelligent management and control

基于物联网、大数据、人工智能等技术，实现对建筑新材料状态、位置、数量、质量等的自动监测、预警与控制。

4 总则

4.1 基本原则

建筑新材料全流程物联网管理的基本原则应包括以下：

——合规性原则：管理工作应遵守国家现行法律法规，契合物联网、建筑建材领域相关标准规范，保证管理活动合法合规；

——全周期管控原则：管控范围应覆盖建筑新材料生产、仓储、运输、现场应用、余料回收及报废处置全生命周期，实现全程闭环可追溯；

——实用先进原则：技术选型与系统搭建应贴合实际应用场景，选用成熟可靠的技术方案；宜结合行业发展趋势预留升级拓展空间；

——安全可控原则：应建立完整的安全防护体系，保障终端设备、网络链路、业务数据安全，落实风险预警与应急处置要求；

——开放兼容原则：系统接口、数据格式、通信协议应执行通用标准，支持多设备、多平台互联互通；宜满足后期功能迭代与跨系统对接需求；

——绿色高效原则：宜依托数字化管控减少材料损耗，提升资源利用效率，助力行业绿色低碳发展。

4.2 总体管控要求

4.2.1 应搭建一体化管控体系，统一标识编码、信息采集、数据交互、运行运维等管理要求，实现全流程数字化、可视化管理。

4.2.2 物联网各层级架构应布局合理、功能适配、运行稳定，满足不同场景下建筑新材料动态监测与业务管控需求。

4.2.3 全流程业务数据应做到采集真实、传输及时、存储完整，严禁数据篡改、丢失，保障数据可用于质量核查、责任追溯与监督管理。

4.2.4 各参与主体应打通信息壁垒，实现数据共享与业务协同，构建跨环节、跨单位的联动管控机制。

4.2.5 系统运行期间宜设置异常识别与智能预警功能，对各类问题及时处置，提升整体管控精细化水平。

4.3 主体职责

4.3.1 生产企业应完成建筑新材料身份赋码、生产信息采集与数据上传，确保产品信息完整、标识唯一。

4.3.2 生产企业应配合后续环节开展信息核验与溯源查询。

4.3.3 物流服务商应布设物联网感知设备，实时采集运输轨迹、材料状态等数据并上报，保证运输过程全程可追踪、数据可留存。

4.3.4 施工单位应落实材料进场核验、现场存储、领用使用、余料管理等环节的数据采集工作，履行施工现场数字化管控主体责任。

4.3.5 平台运维机构应保障物联网平台稳定运行、接口合规、数据安全，按要求开展日常巡检、故障处理、版本维护及台账记录工作。

4.3.6 行业管理部门可依据本文件开展行业监督与标准宣贯；宜利用平台数据开展行业监管、态势分析等工作。

5 物联网总体架构

5.1 架构构成

5.1.1 建筑新材料全流程物联网系统应遵循分层架构设计，整体由感知层、网络传输层、平台应用层三部分组成，各层级边界清晰、功能独立、衔接顺畅。

5.1.2 各层级之间应按照统一协议完成数据交互与指令传递，形成自上而下、互联互通的整体运行体系。

5.1.3 系统整体架构应符合 GB/T 33474 规定的物联网通用参考模型，适配建筑新材料全流程管控业务场景。具体架构图见图 1 所示。

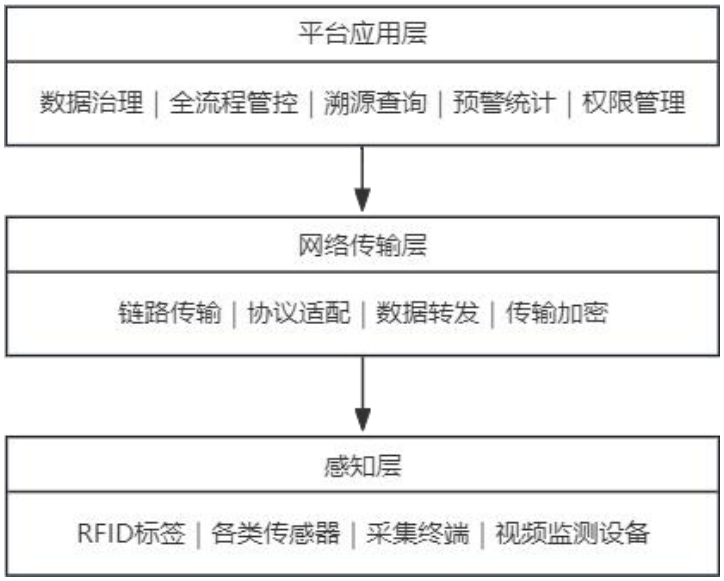

图 1 架构示意图

5.2 感知层设备要求

5.2.1 感知层设备应包含电子标识标签、物联网传感器、智能采集终端、视频监测设备等，应满足建筑多场景长期稳定工作要求。

5.2.2 设备识别精度、采集频率、响应性能应符合建材管控业务需求，保证材料数据采集真实、有效、可复用。

5.2.3 露天、工地、仓储潮湿等复杂工况下使用的设备，宜具备防尘、防水、抗干扰、宽温工作性能。

5.2.4 感知设备数据输出格式、通信规约应适配网络传输层通用标准，保障即插即用、快速入网。

5.2.5 设备布设点位应覆盖材料流转关键节点，无采集盲区，满足全流程动态监测要求。

5.3 网络传输层通信规范

5.3.1 网络通信方式可根据应用场景选用以太网、无线局域网、移动通信、低功耗广域网等形式，通信协议应符合国家现行物联网通信相关标准。

5.3.2 数据传输过程应保证实时性、完整性，关键管控数据传输延迟宜控制在业务允许范围内，不出现丢包、乱码现象。

5.3.3 跨区域、跨主体数据传输链路应做好链路冗余设计，提升网络运行可靠性。

5.3.4 通信数据报文格式、交互规则应参照 GB/T 35319 执行，保障不同链路、不同设备间数据互通。

5.4 平台应用层功能架构

5.4.1 平台应用层应具备数据接收、数据解析、数据存储、状态监测的基础能力。

5.4.2 平台应搭建全流程管控模块，实现材料生产、仓储、运输、现场应用、报废全链条可视化管理。

5.4.3 平台应具备溯源查询、数据统计、台账生成、异常记录功能，满足工程核查与监管需求。

5.4.4 平台宜配置智能预警功能，对材料异常滞留、状态异常、数据断连等情况主动提示。

5.4.5 平台权限体系应分级配置，满足多主体、多角色差异化操作需求。
5.4.6 平台界面与功能逻辑宜贴合建材行业应用习惯，便于现场落地使用。

5.5 架构兼容与拓展要求

5.5.1 系统架构、通信协议、数据接口应采用通用开放式设计，兼容行业主流物联网系统与智能建造平台。
5.5.2 架构设计宜预留功能拓展接口，可适配新材料品类、新管控场景、新智能设备接入。
5.5.3 系统升级、功能迭代应兼容历史数据与原有业务流程，保障系统平稳过渡运行。

6 标识与信息采集规范

6.1 身份标识编码规则

6.1.1 物联网对象应分配全局唯一身份标识，编码规则应符合 GB/T 37032 及 GB/T 36605 要求，确保标识唯一性、兼容性与可解析性。
6.1.2 标识编码宜采用分段结构化设计，包含前缀码、主体码、校验码及扩展码，编码长度与格式应适配行业应用需求，支持全生命周期追溯。
6.1.3 设备类标识应嵌入硬件不可篡改区域，物料类标识可采用 RFID、二维码等载体，编码数据格式应符合 GB/T 38662 中的编码结构依据。
6.1.4 标识编码应预留版本与类型字段，支持跨系统、跨平台兼容解析，编码生成与分配应建立台账记录，确保可追溯、可审计。

6.2 信息采集内容标准

6.2.1 基础信息采集应包含对象身份信息、状态信息、环境信息、位置信息四大类，数据元与格式应符合 GB/T 38619 中的数据结构要求。
6.2.2 身份信息采集内容应包括编码标识、型号规格、生产厂商、出厂日期、唯一序列号等，确保对象身份可精准识别。
6.2.3 状态信息采集应覆盖运行参数、工作状态、故障告警、能耗数据等，关键参数采集精度、频率应满足业务管控与溯源需求。
6.2.4 环境与位置信息采集应包含温湿度、气压、光照、地理位置、布设点位等，格式应符合 GB/T 21740 要求。
6.2.5 采集数据应遵循最小必要原则，涉及个人隐私或敏感数据时，应符合 GB/T 35273 规定，采取脱敏与加密措施。

6.3 采集设备要求

6.3.1 采集设备，包括传感器、RFID 读写器、智能终端、视频设备等的性能、接口、环境适应性应符合 GB/T 38853 规定。
6.3.2 设备识别精度、响应时间、采集频率应满足业务需求，数据输出格式、通信协议应适配网络传输层，支持即插即用与快速入网。
6.3.3 复杂工况下的设备，应具备防尘、防水、抗干扰、宽温工作能力，防护等级不低于 IP65。
6.3.4 设备应支持本地数据缓存与断点续传，具备低功耗、长续航特性，关键设备应支持远程升级、故障自诊断与状态监测。
6.3.5 设备接口应采用通用标准，兼容行业主流协议，电磁兼容性（EMC）应符合国家相关标准，避免干扰其他设备正常运行。

6.4 多场景信息采集规范

建筑新材料在全生命周期各流转场景下，应根据场景作业特点、环境条件及管控需求，制定差异化信息采集规则，保障各环节数据采集完整、精准、有效。各场景采集要求如下：

——生产场景：应针对新材料生产工序、产出状态开展数据采集，覆盖生产批次、工艺参数、质量检测结果、出厂赋码信息等内容，采集频率适配生产节奏，确保生产源头数据真实可溯；

——仓储场景：应采集材料入库、在库、出库全流程数据，同步采集仓储环境温湿度、堆放状态、库存变动信息；宜支持批量识别、快速盘点，保障仓储材料状态可控、账物相符；
——运输场景：应采集新材料运输轨迹、运输时段、车载状态、环境参数等动态信息，实现运输全程实时追踪；关键运输节点应固定采集记录，杜绝流转断档；
——施工现场场景：应采集材料进场核验、堆放存储、领用消耗、现场应用、工序匹配等信息，适配工地露天、多干扰、移动式作业环境，保障现场材料管控数据闭环；
——回收与报废场景：应采集余料回收数量、存储状态、回收时间及报废材料核验、处置去向、注销登记等信息，实现末端环节数据留存与闭环管控。

6.5 信息核验管理

6.5.1 采集信息应建立设备自核验、前端核验、平台核验三级核验机制，明确配套核验规则与处置流程。采集数据三级核验要点应符合表 1 规定。

表 1 采集数据三级核验表

核验级别	核验主体	核心要求
设备自核验	采集终端	校验数据完整性、合理性
前端核验	边缘节点	剔除重复、错误数据
平台核验	管控平台	校验数据一致性、时效性

6.5.2 采集数据上传前，设备应自动校验数据完整性、格式正确性、取值合理性，异常数据标记并重新采集。
6.5.3 边缘节点或采集终端应对数据进行二次核验，核对标识与数据关联性，剔除重复、错误、异常数据。
6.5.4 平台应建立数据质量规则库，对采集数据进行一致性、完整性、时效性核验，异常数据预警并启动复核流程。
6.5.5 核验记录应全程留痕，包含核验时间、人员、结果、处理措施等，建立数据质量台账，定期开展质量评估与优化。
6.5.6 核验通过的数据可入库与应用，未通过数据应分类存储、限期整改，整改后重新核验，确保数据真实、准确、有效。

7 全流程物联网管控

7.1 生产环节动态监测管控

7.1.1 建筑新材料生产工序关键节点应布设物联网感知设备，实时采集生产工艺参数、设备运行状态、生产批次、产品规格等核心数据，实现生产过程动态监测。
7.1.2 生产过程中出现的工艺偏差、设备故障、生产异常等情况应实时上传管控平台，自动触发预警提示，保障生产质量可控。
7.1.3 产品成品下线后应完成一物一码唯一标识赋码，将生产数据、质检数据、批次信息与标识编码绑定关联。
7.1.4 外协生产、代加工的建筑新材料宜对接供方生产管控系统，实现源头生产数据同步归集、统一溯源。
7.1.5 生产环节所有监测数据、操作记录、异常处置记录应分类归档留存，满足质量核查与行业监管要求。

7.2 仓储智能管控

7.2.1 仓储环节应依托物联网设备实现建筑新材料入库、在库、出库全流程智能管控，实时监测仓储环境与材料堆放状态。
7.2.2 仓储智能管控内容应包含库存数量、存放位置、环境温湿度、出入库时间、材料状态等关键信息，宜实现自动盘点、库存预警、超期预警功能。
7.2.3 仓储管理应遵循以下管控要求：

——材料入库时应完成标识识别、信息核验、数据绑定，杜绝无码、错码材料入库；
——在库期间应持续监测存储环境，对温湿度超标、堆放异常、长期滞留等情况及时预警；
——材料出库应自动记录出库批次、数量、流向、领用单位，确保账物匹配、流转有据。

7.3 运输全程追踪管控

7.3.1 运输设备装配与调试

7.3.1.1 建筑新材料运输前，应完成定位终端、环境传感器、数据传输设备的安装与调试，确保设备工况正常、网络稳定。
7.3.1.2 常规建材短途转运可采用局域无线传输方式，长途干线运输宜采用蜂窝移动通信方式保障数据连续传输。
7.3.1.3 易损、恒温、防潮类特殊新材料应加装震动、温湿度感知设备，全程监测运输储存条件。

7.3.2 运输过程动态监测

7.3.2.1 运输途中应实时采集车辆位置、行驶轨迹、行驶速度、车载环境等数据，定时上传管控平台。
7.3.2.2 出现路线偏离、长时间滞留、环境参数超标等异常情况，系统应自动预警，相关责任人应及时处置。

7.3.3 运输闭环核验

7.3.3.1 材料抵达施工现场后，收货方应扫码核验材料信息，确认货物完好、信息一致后完成线上签收。
7.3.3.2 签收完成后平台应自动更新材料流转状态，完成运输环节管控闭环。

7.4 现场应用管控

7.4.1 施工现场应落实新材料进场核验、现场堆放、领用登记、工序应用的全过程物联网管控。
7.4.2 现场应用数据应实时采集、同步更新，确保材料进场数量、使用消耗量、剩余库存量数据真实一致。
7.4.3 现场异常情况应及时录入平台，形成问题记录、整改处置、复核销号的闭环管理流程。
7.4.4 施工现场材料应用管控应满足以下细则要求：
——进场核验：应通过标识扫码完成材料溯源核验，核对规格、批次、生产信息，不合格、信息不全材料禁止进场；
——堆放管控：应根据新材料存储要求定点堆放，实时监测现场堆放环境，规避受潮、暴晒、破损风险；
——领用管控：应实行扫码领用登记，做到用料可查、消耗可统计、责任可追溯；
——工序应用：宜关联施工工序，实现材料应用与施工进度联动管控，提升精细化管理水平。
7.4.5 每日施工结束后，作业结余新材料应及时清点、分类登记、归库存放，更新平台库存数据。
7.4.6 现场管控数据宜按月汇总分析，为材料采购计划、施工用料优化提供数据支撑。

7.5 剩余材料回收管控

7.5.1 施工现场剩余建筑新材料应统一开展回收登记、分类存放、状态复核与数据归档。
7.5.2 余料回收时应重新核验标识信息、剩余数量、完好状态，更新平台库存数据，避免数据脱节、账物不符。
7.5.3 可二次利用余料宜单独建档标记，优先用于后续配套施工，提升材料资源利用率。

7.6 报废闭环管控

7.6.1 出现破损、过期、性能衰减、检测不合格的建筑新材料应及时判定报废，严禁私自复用、随意丢弃。
7.6.2 材料报废判定过程应留存现场影像、检测报告等佐证资料，在管控平台更新材料状态为报废注销。
7.6.3 委托第三方机构处置报废材料时，应完整录入处置单位、处置时间、处置方式等关键信息。

7.6.4 报废审核、处置、归档全流程数据应加密长期留存，实现全生命周期溯源闭环。
7.6.5 批量新材料集中报废时，宜履行内部报备流程，完成线上审批后开展处置工作。

8 数据管理与交互

8.1 数据分类与格式规范

8.1.1 建筑新材料物联网管控数据应按照业务属性、数据类型开展标准化分类管理，统一数据字段、数据精度、数据单位，保障数据规范性与通用性。
8.1.2 全流程管控数据分类应包含以下类别：
——基础静态数据：包含材料编码、规格型号、生产厂家、出厂参数、资质文件等固定不变的基础信息，数据格式应符合 GB/T 36478.3 数据元规范要求；
——动态监测数据：包含生产工艺、仓储环境、运输状态、现场应用、温湿度、定位轨迹等实时变动数据；
——业务管理数据：包含出入库记录、领用台账、核验记录、回收报废、异常处置、审计追溯等业务流转数据。
8.1.3 所有对外交互数据应统一字段格式、统一编码规则、统一数据精度，杜绝自定义非标格式，保障跨主体、跨系统数据互通。
8.1.4 涉密及敏感业务数据宜单独分类标识，采用脱敏格式输出，满足数据安全管理要求。

8.2 数据采集上报机制

8.2.1 物联网终端采集数据应遵循实时采集、按需上报、断点续传的原则，保障数据上报连续、完整、不缺失。
8.2.2 数据上报应根据业务优先级执行差异化上报机制，具体要求如下：
a) 预警类、异常类关键数据应实时上报，无延迟、无积压，确保风险快速处置；
b) 常规监测类数据可按照固定频次定时上报，采集周期适配场景管控需求；
c) 台账统计类、归档类数据宜按日或按批次汇总上报，保障业务台账完整闭环。
8.2.3 网络断连、设备离线等异常场景下，终端应具备本地缓存能力，网络恢复后自动补传离线数据，不得遗漏历史数据。
8.2.4 数据上报前应完成基础校验，剔除乱码、超量程、重复无效数据，提升上报数据质量。
8.2.5 各主体上报数据应实行专人负责制，明确数据审核、上报、复核岗位职责，杜绝错报、漏报、迟报现象。
8.2.6 平台宜建立数据上报质量考核机制，对长期数据异常、上报不及时的点位及主体进行统计预警。

8.3 数据传输接口标准

8.3.1 通用接口规范

8.3.1.1 系统内外数据交互接口应符合 GB/T 35319，采用标准化通用接口协议，支持多设备、多平台互联互通。
8.3.1.2 接口调用、数据请求、数据返回格式应统一标准化定义，支持接口鉴权、报文校验、日志留痕。
8.3.1.3 新建对接接口宜预留拓展字段，适配后续业务迭代与新增数据类型接入。

8.3.2 跨系统传输要求

8.3.2.1 平台与感知终端、企业管理系统、行业监管平台的数据交互应采用加密传输方式。
8.3.2.2 跨主体数据共享传输应设置权限管控，按需开放接口访问权限，杜绝数据越权调取。

8.4 存储与备份

8.4.1 数据存储规范

8.4.1.1 全流程物联网管控数据存储应符合 GB/T 22081 存储安全通用要求，保障数据存储安全、稳定、持久。

8.4.1.2 结构化数据、非结构化数据、影像资料应分区分类存储，建立标准化数据存储目录。
8.4.1.3 原始采集数据应原封不动留存，不得随意篡改、覆盖，保障数据原始性。
8.4.1.4 业务中间运算数据宜设置留存时效，到期后按制度审批清理，节约存储空间。

8.4.2 数据备份要求

8.4.2.1 系统应建立自动备份机制，实现数据定时全量备份与增量备份。
8.4.2.2 关键业务数据应采用异地备份、多副本存储模式，规避数据丢失、硬件损坏风险。
8.4.2.3 备份完成后宜定期开展数据恢复测试，验证备份文件有效性。

8.4.3 数据容灾恢复

8.4.3.1 系统应搭建基础容灾体系，针对服务器故障、链路中断、硬件损毁等突发情况制定容灾预案。
8.4.3.2 发生数据异常或系统故障时，运维人员应依据预案快速启动容灾恢复操作，最大限度缩短系统停运时长。
8.4.3.3 容灾恢复完成后应核对数据完整性、一致性，确认系统功能正常后方可恢复正常业务运行。

8.5 归档与溯源

8.5.1 业务周期结束后的全流程数据应统一归集、整理、归档，形成完整的材料全生命周期数据档案。
8.5.2 归档数据应关联材料唯一标识编码，实现一键溯源、全链查询。
8.5.3 数据归档溯源管理应满足以下要求：

a) 归档数据应长期留存，保存期限满足工程质量追溯、行业监管、审计核查要求；
b) 溯源查询应完整展示材料生产、仓储、运输、应用、回收、报废全链条数据记录；
c) 归档操作、查询操作、数据调取记录应全程留痕，可审计、可追溯、可追责。

8.5.4 过期归档数据宜按照规范流程统一清理、销毁，清理记录同步归档留存。

9 网络与数据安全管理

9.1 网络安全防护

9.1.1 边界安全防护

9.1.1.1 物联网系统网络边界应部署防火墙、入侵检测、入侵防御等安全设备，严格管控网络访问权限，防范非法访问、网络攻击行为，网络边界防护整体要求符合 GB/T 22239 相关规定。
9.1.1.2 外网与内网、业务网与设备感知网之间应设置安全隔离机制，禁止跨区域无防护直通访问。
9.1.1.3 所有网络端口应实行最小化开放原则，关闭无用端口、闲置服务，定期开展端口安全扫描排查。
9.1.1.4 网络边界防护策略应定期更新优化，适配新型网络攻击防护需求。

9.1.2 传输链路安全

9.1.2.1 物联网终端与平台、跨系统、跨主体之间的数据传输应采用加密传输方式，符合网络安全等级保护传输安全要求。
9.1.2.2 无线通信链路应启用加密认证机制，防范数据窃听、篡改、伪造、重放攻击等风险。
9.1.2.3 关键业务传输链路宜设置链路冗余，避免单点故障导致网络中断、数据断传。

9.1.3 设备网络安全

9.1.3.1 物联网感知终端、传输设备应设置初始密码强制修改机制，禁止使用弱口令、通用默认密码。
9.1.3.2 接入网络的终端设备应进行入网安全校验，非法设备、未知设备禁止接入系统网络。
9.1.3.3 设备网络访问行为应全程留痕，支持安全审计与异常追溯。

9.2 数据安全管控

9.2.1 系统全生命周期数据安全管控应覆盖数据采集、传输、存储、使用、共享、归档、销毁全环节，落实分级分类安全管理要求，全流程管控规范契合 GB/T 37973 管理准则。

9.2.2 平台存储的原始业务数据、监测数据、台账数据应禁止私自篡改、删除、覆盖，保障数据原始性、真实性、不可篡改性。

9.2.3 涉及企业经营、工程建设的敏感数据应单独加密存储，设置专属访问权限，严防数据泄露。

9.2.4 数据销毁应采用合规销毁方式，过期、失效数据销毁前应履行审批流程，销毁记录长期归档留存。

9.2.5 数据安全全流程管控应遵循以下要求：

a) 采集环节：应保障采集数据真实完整，禁止非法采集、超范围采集业务数据；

b) 使用环节：应实行按需调用、最小权限使用原则，严控数据导出、复制、外传行为；

c) 共享环节：跨主体数据共享应经过安全审核，敏感数据宜采用脱敏、脱密处理后对外交互。

9.3 用户权限分级管理

9.3.1 系统用户权限应实行分级授权、分岗管控机制，按照岗位职能匹配对应操作权限，落实最小权限原则。

9.3.2 系统用户权限应严格落实专人专岗管控模式，杜绝权限滥用、账号共用等违规问题。

9.3.3 用户账号应实行专人专号管理，禁止共用账号、转借账号，离职、调岗人员应及时注销或冻结账号权限。

9.3.4 系统用户角色划分及权限配置应遵循以下要求：

——超级管理员：负责系统整体权限配置、角色管理、安全策略设置，仅限核心运维人员持有；

——运维管理员：负责系统巡检、故障处置、数据运维，无核心权限修改与批量删除权限；

——企业操作员：负责本单位数据上报、台账维护、设备管理，仅可操作本主体业务数据；

——监管查看员：仅具备数据查看、统计查询权限，无数据修改、删除、导出权限。

9.3.5 账号登录应开启密码复杂度校验、异地登录校验、多次失败锁定功能，提升账号安全等级。

9.3.6 所有用户操作行为应全程日志留痕，支持权限审计、操作追溯与责任认定。

9.3.7 系统用户权限分级配置应符合表 2 的要求，严格落实最小权限原则，确保各角色权限与岗位职责匹配，杜绝权限滥用、越权操作等违规行为。

表 2 系统用户权限分级配置表

用户角色	权限等级	核心操作权限
超级管理员	一级	系统配置、权限管理
运维管理员	二级	设备运维、故障处置
企业操作员	三级	数据上报、台账维护
监管查看员	四级	数据查询、溯源查看

9.4 安全风险识别与预警

9.4.1 风险常态化识别

9.4.1.1 运维单位应定期开展网络风险、数据风险、设备风险、权限风险的排查识别，形成风险排查台账。

9.4.1.2 针对网络攻击、数据异常、设备离线、越权操作等风险应建立常态化识别机制。

9.4.1.3 每季度宜开展全面安全风险评估，及时识别潜在安全隐患。

9.4.2 智能预警管控

9.4.2.1 系统应配置安全预警功能，对异常登录、批量数据导出、设备异常离线、网络流量异常等行为自动预警。

9.4.2.2 预警信息应精准推送至对应运维及管理人员，明确预警处置责任人与处置时限。

9.4.2.3 所有预警记录应留存归档，形成预警、处置、复核闭环管理台账。

9.5 应急处置流程

9.5.1 运维单位应编制网络安全、数据泄露、系统瘫痪、设备故障等突发事件的应急处置预案。

9.5.2 运维单位应结合系统安全风险特点，制定分级处置机制，规范突发事件处置流程。

9.5.3 发生安全突发事件时，应按以下流程闭环处置：

——快速研判：第一时间判定故障类型、影响范围、风险等级，锁定问题源头；

——紧急处置：及时采取断网隔离、权限冻结、数据保护等措施，遏制风险扩大；

——复盘整改：事件处置完成后开展复盘分析，优化安全策略与应急预案。

9.5.4 重大安全事件应及时上报行业管理部门，不得瞒报、漏报、迟报。

9.5.5 运维单位宜每半年组织一次安全应急演练，提升突发事件处置能力。

9.5.6 所有应急处置记录、演练记录应长期归档留存，作为安全考核依据。

10 运维管理

10.1 日常巡检规范

10.1.1 设备巡检

10.1.1.1 运维人员应定期对感知终端、传输设备、供电设备开展现场巡检，核查设备在线状态、运行工况、安装固定情况，日常设备巡检流程符合 GB/T 36626，巡检内容按表 3 执行。

表 3 物联网设备日常巡检项目表

设备类型	巡检项目	判定要求
感知终端	在线、采集、供电	正常运行
传输设备	联网、链路、信号	通信稳定
采集设备	识别、上传、防护	数据有效

10.1.1.2 户外布设设备应重点检查防水、防尘、抗干扰性能，及时清理设备遮挡、积尘、破损问题。

10.1.1.3 巡检发现设备老化、性能衰减问题应提前报备并安排更换维护。

10.1.2 平台巡检

10.1.2.1 每日应核查平台服务器运行状态、数据库负载、数据推送情况，确保平台稳定运行。

10.1.2.2 应定期检查接口连通性、数据交互有效性，及时修复接口异常、数据断传问题。

10.2 故障排查修复

10.2.1 系统及设备发生故障后，运维人员应第一时间接收故障工单，开展故障定位与排查工作。

10.2.2 一般性设备离线、数据异常故障应在 24 h 内完成排查修复，重大系统故障应立即启动应急处置。

10.2.3 故障修复后应测试设备、系统、数据运行状态，确认功能恢复正常后方可闭环销号。

10.2.4 所有故障问题应记录故障现象、原因、处置过程、修复结果，形成故障处置台账。

10.3 系统版本迭代

10.3.1 系统功能优化、漏洞修复、性能升级等版本迭代工作应制定迭代方案，明确迭代内容、测试流程、上线时间。

10.3.2 版本更新前应完成数据全量备份，避免迭代过程造成数据丢失、系统异常。

10.3.3 版本上线后应开展试运行测试，核查功能完整性、系统稳定性、数据交互准确性。

10.3.4 系统迭代升级应兼容历史数据与原有业务流程，保障业务不间断运行。

10.3.5 迭代更新记录应归档留存，包含版本号、更新内容、测试记录、上线说明。

10.4 运维台账与考核

10.4.1 运维单位应建立完整的运维台账体系，台账内容应包含巡检记录、故障处置、版本迭代、应急演练、设备维护等信息。

10.4.2 运维台账应做到记录真实、内容完整、更新及时，支持随时核查与审计追溯。

10.4.3 运维考核应遵循以下管理要求：

a) 按照运维规范考核巡检完成率、故障处置及时率、系统在线率、数据完好率；

b) 对运维疏漏、处置滞后、数据异常等问题应定期通报整改；

c） 考核结果宜作为运维工作评价、服务优化的重要依据。

10.4.4 运维台账资料应长期归档保存，保存期限满足行业监管及工程追溯要求。