室分智能监测系统管理平台
技术规范书

广州市信息基础协会

2025年6月

目　录

1. 管理平台的技术指标

平台技术指标包括大屏端、WEB 端技术、通信接入服务。

1.1. 大屏端

支持大屏显示，经过数据清洗，通过图表等组态信息实时地展示，监控站点分布情况、实时告警列表、告警分类统计图表、监测对象统计等。

1.2. Web 端

1.2.1. 首页

包括区域站点信息统计图、告警统计图、站点报告分布图、站点健康统计图、采集设备统计图、设备共建共享情况分析图。

1.2.2. 站点管理

站点管理模块包括站点信息、绑定管理。

1. 站点信息

- 站点信息管理

站点信息管理，支持增加、删除、修改、查询、导入、导出站点，站点详情查看、站点报告查看、导出、打印。

站点信息包括：站址名称、站址编码、所属区域、经度、纬度、站点类型、维护人、备注等信息。

- 站点详情管理

包括站点拓扑图、站点告警管理、站点所属室分管理、感知终端列表管理、参数设置、站点信源管理、系统方案图管理。

2. 绑定管理

站点绑定室分天线信息，支持绑定、解绑操作。

1.2.3. 电子地图

电子地图实时显示站点 POI 信息、站点状态（异常、正常）。支持单击（显示站点概览信息）、双击事件（站点详情）。

1.2.4. 监测管理

监测管理包括站点监测、天线管理、感知终端管理、设备参数管理。

1. 站点监测

实时监测站点是否正常，站点相关的频段信息。

2. 天线管理

实时监测天线是否正常，支持天线录入绑定、详情查看、删除、编辑、查询、导出操作。

- 天线详情管理

包括天线频段管理、告警记录管理、所属感知终端管理、参数设置。

3. 感知终端管理

实时监测感知终端工作状态，告警状态和电量情况。

4. 设备参数

实时监测感知终端的参数变换情况及更新情况。

1.2.5. 告警管理

告警管理模块包括当前告警、历史告警、告警类型。

1. 当前告警

当前告警支持告警查询、过滤、告警确认、告警删除、导出、忽略告警和派发工单等操作。

2. 历史告警

历史告警管理，支持历史告警查询、删除、详情查看、导出功能。

3. 告警类型

告警类型支持编辑、修改、配置告警规则等功能。对已经设置好的规则进行编辑时，可设置自动确认、自动过滤、自动隐藏、自动清除、自动分发等功能。

1.2.6. 资源管理

1. 感知终端管理

自动生成设备信息，实时显示设备状态信息、所属站点信息，支持查询、修改、解绑、通信日志查看、远程升级等操作。

设备信息包括设备编号、电量、设备名称、设备型号、所属站点、设备状态（离线、在线）等。

2. 物联网卡管理

自动生成物联网卡信息，建立物联网卡与感知终端的关联关系，支持新增、编辑、删除、查询、导入、导出操作。

物联网卡信息包括：物联网卡号、ICCID、绑定感知终端 SN 等。

3. 区域管理

支持区域新增、修改、删除操作。

区域信息包括：区域编码、区域名称、所属父区域等。

1.2.7. 日志管理

日志管理模块包括登录日志、操作日志、通信日志功能。

1. 登录日志

支持日查询功能。

登录日志基本信息包括用户名、登录 IP、地区、浏览器信息、结果、备注、登录时间。

2. 操作日志

支持日查询、详情查看功能。

操作日志基本信息包括用户名、操作模块、操作内容、请求路径、登录 IP、地区、浏览器信息、结果、备注、操作时间。

3. 通信日志

支持日查询功能。

通信日志基本信息包括：终端名称、事件、产生时间、状态、更新时间、操作内容。

对于设置、升级操作，在未下发的情况下，可进行取消命令操作。

1.2.8. 系统管理

系统管理模块包括用户管理、角色管理、参数配置。

1. 用户管理

支持用户新增、删除、修改、重置密码、禁用、授权操作。

用户管理基本信息包括：登录账户名、用户名称、手机号码、状态、角色、部门等。

2. 角色管理

角色管理可设置功能权限、数据范围及成员列表。支持增加、修改、删除操作。

数据权限则限制用户的数据权限，员工列表可查看当前授权用户，同时可添

加、移除功能。

角色信息包括：角色编码、角色名称、创建时间、更新时间等

3. 参数配置

该参数配置为全局配置信息，设置将立即生效。支持查询、编辑操作。

全局参数信息包括：参数 Key、参数名称、参数值、备注信息等。

1.3. 通信接入服务

1.3.1. 通信协议支持

系统支持 TCP/IP、UDP 和 MQTT 通信协议，具体由平台设定接入方式，设备支持即可。

1.3.2. 数据接入安全策略

1. MQTT 协议使用 TLS/SSL 加密 MQTT 通信；
2. 使用 AES 加密消息内容；
3. 使用数字签名确保数据信息来源和完整性；
4. AES 加密和签名结合，保证消息的机密性和完整性。
5. 具体的安全策略由系统下发配置。

2. 适配性要求

2.1. 硬件适配性

2.1.1. 云原生多云支持

支持主流的云平台部署，如：铁塔云平台、运营商云平台、华为云、阿里云、腾讯云等多个云平台，实现快速部署，稳定运行。

- 前端应用模块（包括用户交互层、访问接入层等，如Web服务器）优先采用容器方式部署。后端应用模块优先使用容器方式部署，如后端应用处理逻辑复杂、性能需求高可视具体情况而定。
- 数据库模块根据规模选择部署方式，资源规模与性能要求高的中大型数据库可选择裸金属方式部署，其他中小型数据库选择虚拟机方式部署。

2.1.2. X86 和 ARM 服务器的混合部署的支持

同时支持X86 和 ARM服务器的混合部署架构。

支持机房集群内多可用区之间的混合部署，系统可部署于不同可用区内不同

CPU 架构的服务器之上。

2.2. 系统适配性

2.2.1. 操作系统支持

跨平台支持多种操作系统软件，支持 Solaris、Linux、Windows 和 FreeBSD 等操作系统。

2.2.2. 浏览器支持

Web 服务器支持 chrome、firefox、ie、safari 网络浏览器。

2.3. 自主可控要求

（1）自主可控服务器适配要求：应可适配国产服务器资源，包括但不限于鲲鹏、海光等；

（2）自主可控操作系统适配要求：应可适配国产操作系统，包括但不限于BC-Linux（龙蜥、欧拉版）、国内开源等各类操作系统；

（3）自主可控数据库适配要求：应可适配国产数据库，具备不依赖国外数据库产品的能力。

（4）中间件及通用组件适配要求：应可适配国产中间件，避免依赖国外商业软件产品。

（5）针对数据库的功能开发要严格遵从SQL92标准，禁止使用非标准功能，确保可以在不同的国产数据库中平滑迁移。

3. 平台能力

3.1. 性能要求

3.1.1. 响应时间

- 页面响应时间在3秒内。
- 接口响应时间500毫秒以内。
- 导出性能要求：

1万条数据，导出完成用时3s；

3万条数据，导出完成用时5s；

10万条数据，导出完成用时8s。

3.1.2. 并发用户数

≥500。

3.1.3. TPS

≥500TPS。

3.1.4. CPU 利用率

20%～60%。

3.1.5. 内存使用率

≤70%。

3.1.6. APP FPS

≥40帧/秒。

3.2. 二次开发能力

3.2.1. AI 模型指标自定义

提供灵活而可维护的方法来处理复杂的决策逻辑，AI模型指标的生成规则可配置，具备评估条件的能力，能够执行与规则指标相关联的动作。

3.2.2. 基站共建共享报告格式自定义

共建共享报告内容可进行自定义排版、编辑、发布，实现对数据展示子系统的自由组态，支持不同决策，呈现不同场景。

支持多源数据接入，可快速生报告基本要素，供可视化应用编辑器集成调用。

3.3. 自定义配置

3.3.1. 页面列表字段自定义配置

页面支持列表排列循序、显示宽度、排序自定义。

3.3.2. 界面自定义配置

系统支持换肤、菜单名称可配置、软件 logo 可配置、登录页面背景图片可配置。

4. 安全性要求

4.1. 平台通信安全

数据采集终端接入平台通信安全指平台与应用以及设备之间数据传输过程中的加密通信机制，主要目的是保障整个平台的数据在南北向传输过程中的数据

安全。

南向通信安全：在与设备通信过程中，平台应支持提供多种数据传输保护方式，保障数据传输的安全：

- 平台应具备端到端的安全体系能力；
- 平台应支持提供对终端认证、通道加密、数据加密的安全手段；
- 平台应支持对终端身份鉴别、访问控制、安全审计；
- 平台应支持设备通过TCP/IP、UDP和MQTT协议与平台通信；
- 平台应支持设备使用安全密钥（DeviceSecret）入网；
- 平台应支持设备使用数据安全密钥（SessionKey）通信；
- 平台应支持终端数据通过AES算法加密传输等。

4.2. 平台维护安全

应支持按用户分配账号，避免不同用户间共享账号；

在保证业务正常的情况下应支持增加、修改、删除账号功能；

在保证业务正常的情况下应具备限制账号登录功能，限制与设备运行、维护等工作无关的账号登录；

应支持按用户职责不同分配不同的界面权限；

应支持按用户不同分配不同的数据（站点）权限；

应支持用户同一时刻只能在一个客户端进行操作，保证用户登录状态安全；

密码保护应依照《中华人民共和国密码法》要求执行。

4.3. 平台数据安全

4.3.1. 数据存储

主要数据应具备数据指纹，防止恶意篡改；

关键数据应加密存储，防止泄露。

4.3.2. 数据备份

系统支持自动备份。

数据库日志及业务数据应支持本地备份，一旦数据遭到破坏，可恢复到破坏前的数据。本地备份应包括增量和全量备份，备份周期应支持自定义配置；

应提供完善的数据转储功能；

本地备份的数据应同时支持异地备份，应建立异地容灾机制，实时异地备份

日志数据和业务数据。

4.3.3. 数据审计

应建立专门的数据库审计用户；

应对审计记录有保护措施，定期备份，避免受到未预期的删除、修改或覆盖；

应提供安全审计功能模块，对重要用户行为和重要安全事件进行审计。