T/CECS×××-202×

中国工程建设标准化协会标准

Standard of China Association for Engineering Construction Standardization

公路机电设备操作系统技术规程

Technical Specifications for Operating System of Highway Electromechanical Device

（征求意见稿）

前　　言

根据中国工程建设标准化协会下达的《关于印发<2024 年第二批协会标准制订、修订计划>的通知》(建标协字[2024]28 号)的要求，由交通运输部公路科学研究院承担《公路机电设备操作系统技术规程》（以下简称“本规程”）的制定工作。

编制组在深入技术论证、国内外文献调研、工程经验总结和广泛征求意见的基础上，完成了本规程的编制工作。

本规程共分为 9 章，主要内容包括：1 总则、2 术语和符号、3 基本规定、4 内核层、5 系统服务层、6 框架层、7 应用层、8 安全要求、9 测试方法。

本规程的某些内容可能直接或间接涉及专利，本规程的发布机构不承担识别这些专利的责任。

请各有关单位在执行过程中，将发现的问题和意见，函告本指南日常管理组，联系人：谌仪（地址：北京市海淀区西土城路 8 号，邮编：100088；电话：010-82019616；传真：010-62370567；电子邮箱：chenyi@itsc.cn），以便修订时参考。

主 编 单 位：交通运输部公路科学研究院

参 编 单 位：深圳开鸿数字产业发展有限公司

河北高速公路集团有限公司

华为技术有限公司

中软国际有限公司

主　　编：李振华

主要参编人员：

主　　审：邹小春

参与审查人员：

目　　次

1 总则

1.0.1 为指导公路机电设备操作系统的设计、开发和使用，规范公路机电设备操作系统的技术架构、主要功能、安全要求和测试方法，制定本技术规程。

1.0.2 本规程规定了公路机电设备的操作系统总体技术架构，对操作系统内核层、硬件抽象层、系统服务层、框架层和应用层提出了技术要求，对操作系统相关安全要求和测评方法进行了规定。本规程适用于公路机电设备操作系统的设计、开发、应用部署和测试评价。

1.0.3 公路机电设备操作系统除应符合本规程的规定外，尚应符合国家和行业现行有关标准的规定。

2 术语和符号

2.1 术语

2.1.1 公路机电设备 highway electromechanical device

发挥公路运营管理和养护功能的主要辅助设备，包括监控、监测、收费、通信、供配电、照明等设备。

2.1.2 轻量系统类设备 mini system device

配备微控制器单元类处理器，提供多种轻量级网络协议、轻量级图形框架和物联网总线读写组件，内存容量至少为 128KiB 的通讯类模组、传感器设备、采集器等设备。

2.1.3 小型系统类设备 small system device

配备内存管理单元的应用处理器，具有高级别安全性能、标准化图形框架以及视频编解码多媒体功能，内存容量至少为 1MiB 的监控摄像机、路由器以及串口服务器等设备。

2.1.4 标准系统类设备 standard system device

配备应用处理器，提供增强的交互能力以及硬件合成能力、更多控件以及动效更丰富的图形能力、完整的应用框架，内存容量至少为 128MiB 的区域控制器、车道控制器、边缘物联网关等设备。

2.1.5 物模型 thing model

对一个物体的数字化描述。包括三层结构，分别是元素（包括属性、行为以及事件）、组件以及物模板。

2.1.6 应用元服务 application meta service

一种无需安装、即点即用、服务直达的应用程序形态。

2.2 符号

TCP/IP——传输控制协议/网际协议（Transmission Control Protocol/Internet Protocol）

HDI——硬件设备接口（Hardware Device Interface）

DFX——为了提升质量属性的软件设计，包含 DFR(Design for Reliability，可靠性)、DFT(Design for Testability，可测试性)。

DI——数字量输入（Digital Input）

DO——数字量输出（Digital Output）

AI——模拟量输入（Analog Input）

KB——千字节（Kilobyte）

MB——兆字节（Megabyte）

KiB——千位二进制字节（Kibibyte）

MiB——兆位二进制字节（Mebibyte）

3 基本规定

3.1 技术架构

3.1.1 公路机电设备操作系统的技术架构如图 1 所示，整体遵从分层设计，自下而上依次分为内核层、系统服务层、框架层和应用层。

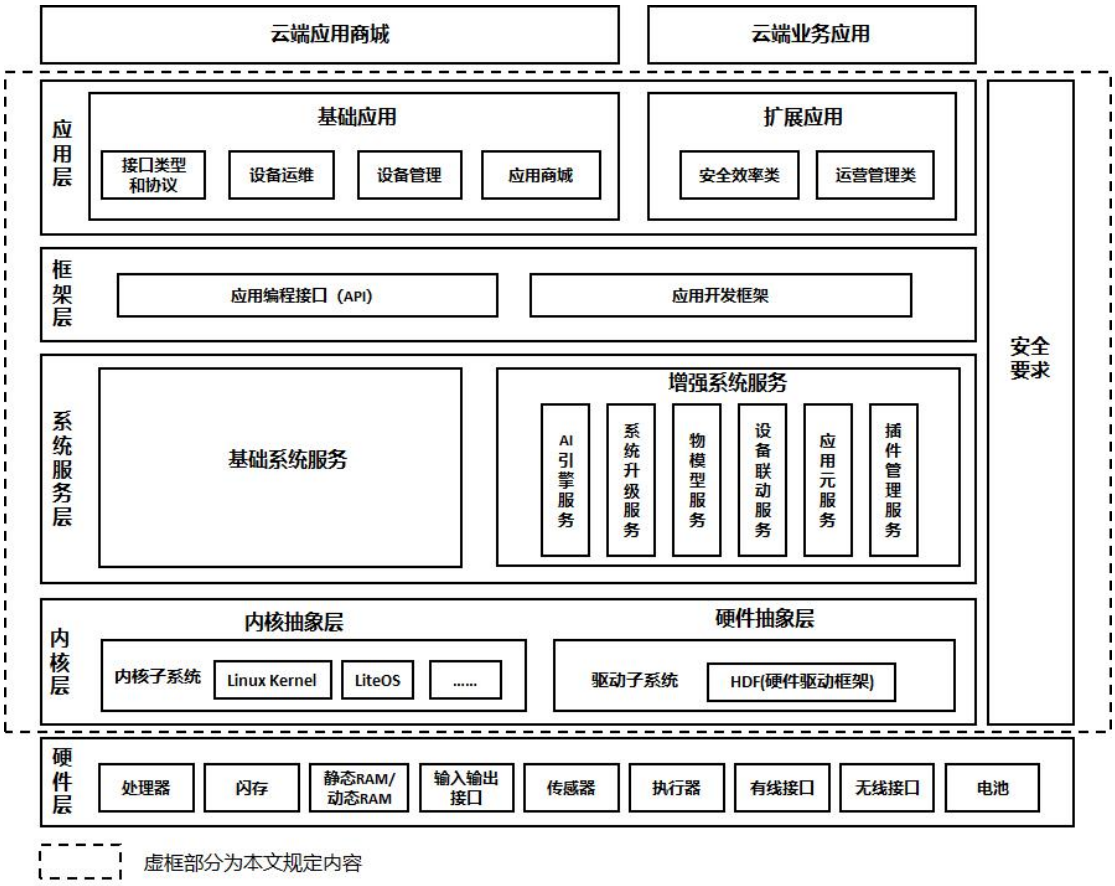

图 1 系统技术架构图

3.1.2 内核层包括内核抽象层和硬件抽象层两部分，其中内核抽象层屏蔽多内核差异，对上层提供基础的内核能力，包括进程/线程管理、内存管理、文件系统、网络管理和外设管理等。硬件抽象层提供硬件设备统一接口，支持系统服务层和应用层对于硬件驱动的操作。

3.1.3 系统服务层为应用开发提供统一的系统服务 API 接口。该层包含分布式管理服务、公共基础库服务、多模输入服务、图形服务、安全服务、事件通知

服务、电话服务、多媒体服务、DFX 服务、网络管理服务等基础系统服务，以及 AI 服务、升级服务、物模型服务、设备联动服务、近场感知服务、应用元服务、插件管理服务等增强系统服务。

3.1.4　框架层为应用开发提供了 C/C++/JS 多语言的用户程序框架和 API。

3.1.5　应用层包括基础应用和扩展应用。

3.2　总体要求

3.2.1　公路机电设备操作系统应支持功能模块化裁剪，根据设备 CPU、内存、存储等硬件能力按需组合必要模块，实现最小化系统部署。

3.2.2　操作系统软件所应适配内存容量大于 128KiB 的各类公路机电设备。

3.2.3　同一型号操作系统部署在新型号机电设备后，应支持原有应用程序。

3.2.4　公路机电操作系统根据设备资源差异提供三种系统类型：轻量系统、小型系统和标准系统。三者核心差异体现在硬件资源需求、内核选择、功能特性及适用场景上。具体区别请见表 1.

表 1 公路机电操作系统分类说明

类别	轻量系统（L0）	小型系统（L1）	标准系统（L2）
目标处理器	MCU（如 Arm Cortex-M、RISC-V 32 位）	应用处理器（如 Arm Cortex-A）	应用处理器（如 Arm Cortex-A）
最小内存要求	≥128 KiB	≥1 MiB	≥128 MiB
内核类型	LiteOS-M	LiteOS-A 或 Linux	Linux
图形能力	轻量级图形框架（如 GUI Lite）	标准图形框架（支持基础 GUI）	完整图形框架（支持 3D GPU、动效）
网络协议	轻量级协议（如 CoAP、MQTT）	完整协议栈（TCP/IP）	全协议支持（包括高性能网络）
多媒体支持	无或极简	视频编解码、音频处理	高级多媒体（如硬件编解码）
文件系统	轻量级文件系统（如 LittleFS）	完整文件系统（如 FAT、EXT4）	多文件系统支持（虚拟文件系统）
安全能力	基础加密机制	完整安全框架（如权限管理）	企业级安全（如 SELinux、可信执行）
典型应用场景	传感器、穿戴设备、连接模组	IP Camera、路由器、行车记录仪	手机、平板、智能显示屏

开发特性	低功耗、实时任务调度	平衡性能与功耗，支持多进程	完整应用框架、多用户多进程

条文说明

根据模块化裁剪、内存适配及向后兼容性要求，操作系统应支持功能模块化裁剪、按需适配大于 128KiB 内存容量及原有应用向后兼容功能，确保在硬件资源差异、内存容量范围及新旧设备替换情况下，公路机电设备业务功能运行不受影响。

4 内核层

4.1 内核抽象层

4.1.1 基础功能

4.1.1.1 内核层是公路机电设备操作系统的基础能力集合，应具备以下功能：

——上层服务组件及应用依赖的基础功能, 包括中断与异常管理、锁机制、任务管理、进程管理与调度、内存管理、定时器管理、时钟管理、能效管理或进程间通信能力等；

——基础网络协议栈功能，支持例如 TCP/IP 等通用网络协议。

4.1.2 增强功能

4.1.2.1 内核层根据不同级别终端的硬件资源需求，宜具备以下增强功能：

——多内核设计功能，根据终端硬件资源选择不同的内核，如资源占用较小的实时内核和资源占用较大的宏内核。

——根据硬件资源的丰富程度，具备维护测试服务以及多核管理等功能。

——文件系统功能，支持文件与文件夹的创建、移动、删除、权限查看与设定等操作。

——根据硬件指令集实际架构，具备多指令集架构兼容功能。

4.2 硬件抽象层

4.2.1 硬件抽象层主要由平台驱动和外设驱动共同提供设备驱动管理功能，宜提供硬件设备统一接口（HDI），支持系统服务层和应用层对于硬件驱动的操作，从而对内核和硬件进行解耦。

4.2.2 平台驱动应具备以下功能：

——设备驱动的安装与卸载功能。

——设备驱动的休眠/唤醒功能。

——设备驱动服务的查询功能。

4.2.3 外设驱动应具备以下功能：

——设备驱动的动态加载和按需加载功能，宜具备外部设备插入后驱动的自动侦测及加载功能。

——设备热插拔检测功能。

——对于由电源供电的泛终端设备，具备设备级电源管理功能。

5 系统服务层

5.1 基础系统服务

5.1.1 应具备分布式管理服务、公共基础库服务、多模输入服务、图形服务、安全服务、事件通知服务、电话服务、多媒体服务、DFX 服务、网络管理服务等能力。

5.1.2 应具备分布式管理能力，实现各类公路机电设备的互联互通、设备管理以及应用协同。

5.1.3 应提供包括常用的 C、C++、JS 开发增强 API，可被各业务子系统及上层应用所使用。

5.1.4 应提供统一的时间同步服务，支持利用网络时间协议（NTP）或卫星授时等手段与上位系统保持时钟同步。

5.1.5 应内置看门狗机制，对关键任务运行实施监测，当出现死机或卡死状况时能自动重启恢复。

5.1.6 应提供统一的用户身份认证和设备、应用授权接口，实现设备和数据的访问权限控制。

条文说明

C、C++是操作系统和高性能软件领域主流编程语言，具有高效率、高性能的优势，有利于系统功能开发。JS 是前端和轻量化应用领域主流编程语言，具有跨平台、高效和生态丰富的优势，这三者均有利于公路机电设备软件应用的开发和应用。

5.1.4 应支持触控、键盘和鼠标等输入能力，支持多设备协同输入。

5.1.5 应提供屏幕显示管理、图形界面管理、图形绘制、图形编辑、图形转换和界面自适应布局功能。

5.1.6 应具备事件监控、事件处理、通知队列、事件订阅和日志记录等功能，

宜提供事件定义扩展机制。

5.1.7　应支持音频、视频和图形服务功能。

5.1.8　应提供记录流水日志、设备状态信息、CPU、存储能力信息，以及记录系统崩溃或者程序异常的信息、信息导出和测试框架等功能。

5.1.9　应提供至少一种数据网络服务，如 WLAN 服务、蓝牙服务、以太网服务、星闪接入服务等，支持常用网络协议和无线接入协议，宜提供网络连接管理、联网策略管理、热点网络共享等服务。

5.2　增强系统服务

5.2.1　AI 引擎服务

对于具备边缘 AI 算力的标准系统类设备，符合以下技术要求：

——应提供统一的、开放的 AI 引擎服务，支持 MindSpore Lite、RKNN 等推理框架，并具备可扩展性以兼容其他主流 AI 计算框架。应支持 PyTorch、TensorFlow、ONNX 等 AI 模型格式。

——应提供统一的硬件驱动抽象层，屏蔽底层 NPU/GPU/DSP/FPGA 等异构硬件差异，为上层应用提供硬件加速能力。

——应提供 AI 算法模型全生命周期管理能力，支持 AI 算法模型的下发、动态更新和订阅。

——应建立 AI 算法模型资产安全保护机制，提供 AI 算法模型加密存储、签名验证、权限管控等能力。

——宜支持 AI 能力的分布式调用，允许机电设备根据业务需求，协同调用网络内其他设备的 AI 算力与模型，实现分布式推理与 AI 能力共享。

条文说明

MindSpore Lite、RKNN 等推理框架是端侧 AI 推理领域主流，具有轻量化、高性能，并能与操作系统生态深度融合或充分利用硬件加速能力的优势，有利于在资源受限的公路机电设备上高效部署和执行 AI 算法。

PyTorch、TensorFlow、ONNX 等 AI 模型格式是 AI 算法开发与部署领域主流标准，具有生态成熟、兼容性强、易于转换的优势，有利于算法模型的快速迁移、部署应用到公路机电设备上。

5.2.2 系统升级服务

——应支持在线升级和本地存储升级服务（如 U 盘、SD 卡），宜支持 pull+差分和 push+差分等多种方式。

——针对隧道、收费站等关键业务场景，应支持静默升级、预约升级和断点续传功能。

——应支持升级后业务数据不丢失。

5.2.3 物模型服务

——应提供统一的物模型管理服务，采用标准化的数据格式（如 JSON）对机电设备的属性、服务和事件进行统一描述。

——物模型应具备可扩展性，支持公路行业不同类型机电设备的自定义物模型描述。

——应基于物模型提供标准的数据交换和设备控制接口。

——应支持主流机电设备物模型，如射流风机、车道指示器、照明、交通信号灯、可变情报板、限速标识、线圈车辆检测器等。

5.2.4 设备联动服务

——应提供设备联动服务框架，使用统一的数字化抽象描述语言，对不同机电设备的硬件能力（如摄像头、传感器、车道指示器、照明、车辆检测器）和软件能力进行抽象和封装。

——应提供软总线服务框架，使用统一的通信软总线接口，对不同通信方式能力（如有线和无线方式）进行抽象和封装。

——应支持机电设备硬件资源共享，允许同一网络内的不同机电设备按需发现、组合并调用。

——应支持根据预设的业务逻辑（如事件触发、时间策略），自动编排和调度一种及以上机电设备能力。

——宜支持分布式空间计算能力。

条文说明

星闪技术是新一代近距离无线连接技术，具有低功耗、速度快、低时延、连接稳、覆盖广、组网大等优势，有利于公路机电设备间互联互通。

5.2.5 近场服务感知

——应支持蓝牙、Wi-Fi、星闪等一种及以上的通信技术，提供统一的设备发现、安全配对、连接管理和数据传输 API。

5.2.6 应用元服务

——应支持应用元服务的多种启动方式，如用户手动点击、特定事件触发（如设备靠近）、API 调用等。

——应支持元服务的即用即走或仅执行轻量化的首次加载。

——应建立元服务的统一分发和生命周期管理机制。

——应支持元服务的跨设备流转能力，允许用户将当前设备上的服务无缝迁移至另一台设备上继续执行。

5.2.7 插件管理服务

——应提供标准化的插件管理服务框架，支持动态加载和硬件驱动及功能模块管理。

——应支持插件的即插即用，提供插件发现、安装、启用/禁用、更新和卸载机制。

——应对插件的运行环境进行沙箱隔离，并权限控制。

6 框架层

6.1 基础功能

6.1.1 应为上层应用开发提供 C/C++/JS 等多语言的用户程序框架和 Ability 框架。

6.1.2 应为上层应用开发提供统一的系统服务 API。

6.1.3 应为不同硬件平台提供适配接口，确保框架层服务在不同平台行为一致。

6.1.4 应支持按需裁剪子系统及功能模块。

6.2 增强功能

6.2.1 应支持根据设备裁剪程度动态调整支持的 API 范围，确保接口与硬件能力匹配。

6.2.2 应提供分布式 UI 框架，支持界面元素跨设备显示与交互。

7 应用层

7.1 基础应用

7.1.1 接口类型和协议接入应用

应能根据公路行业要求及使用场景提供机电设备接入 SDK 应用服务，SDK 应用服务应符合如下要求：

——应提供一组 API，以供第三方应用调用 DI、DO、AI、RS485、RS233、Modbus 类机电设备。

——应支持多种通用的通信协议，包括但不限于 TCP/IP、MQTT、UDP、CoAP、HTTPS 等通信协议；应支持 Modbus-RTU、DL/T645、GB28181 等现场控制协议，宜支持 C-V2X 等车路协同通信协议。

——宜支持机电设备无码接入，根据接入机电设备类型定义设备接入无码配置协议，主要包括接口、协议、设备数据结构、数据类型、设备能力等。

条文说明

DI、DO、AI、RS485、RS233、Modbus 等接口类型是公路机电设备常见接口，提供对应的 API 服务有利于相关应用开发调用。RS485、RS233 参考国际标准 TIA-485-A 执行；Modbus 参考参考《基于 Modbus 协议的工业自动化网络规范 第 1 部分:Modbus 应用协议》（GB/T 19582.1-2008）执行。

TCP/IP、MQTT、UDP、CoAP、HTTPS、Modbus-RTU、DL/T645、GB28181 等通信协议是公路机电设备常见的通信协议，提供对应的协议支持，有利于机电设备应用快速接入和调用。

无码接入是指通过无代码平台实现公路机电设备的数据接入。通常借助系统中预定义的物模型、标准化协议以及可视化配置界面，用户可通过控制台完成产品模型定义与设备注册，无需编写代码即可实现物理设备与云端服务的无缝对接，将设备接入周期从数周缩短至小时级，大大缩短公路机电设备集成工期。

7.1.2 设备运维应用

应能根据公路行业要求及使用场景提供机电设备自身运维应用服务，运维应用服务应满足如下要求：

——应支持密码管理功能，运维应用访问须有用户名密码校验，处于同一网络的所有机电设备的密码应统一，并支持统一设置。

——应支持监听机电设备接入状态，状态变化（接入<—>离线）时及时上报。

——应支持监听机电设备接入数据采集成功与指令下发状态，轮询类设备可设置采集频率，异常时及时上报。

——应支持远程调试诊断功能，包括远程日志提取、故障定位和系统调试接口。

——宜提供跨设备的应用调用接口，以供第三方应用调用，实现跨设备运维功能。

——对于视频类设备，宜支持对视频流、AI 算法（若有）、云控制台（若有）等功能进行调试与配置，支持视频流拉取到第三方应用。

7.1.3 设备管理应用

应能根据公路行业要求及使用场景提供机电设备自身设备管理应用服务，设备管理应用服务应满足如下要求：

——应支持对不同的账号角色等设置不同的权限，对设备数据查看、设备控制、参数配置、升级等权限进行管理。

——应支持便捷的网络参数配置界面，支持对 IP 地址、子网掩码、网关、DNS 等进行静态或动态配置。

——对于支持主备机模式的机电设备，应支持主备机模式的配置、状态监控及故障自动切换。

7.1.4 应用分发服务

应支持应用分发服务，作为获取、管理和更新各类应用的统一入口。应用分发服务应满足如下要求：

——应支持对应用、设备插件、行业标准协议库、AI 模型等资源的分类展示、搜索和下载。

——应支持应用管理功能，包括版本管理、更新日志管理、应用信息管理等。

——应支持应用的自动更新、手动更新、计划更新。

7.2 扩展应用

针对公路机电系统中控制类设备（例如区域控制器、车道控制器、边缘智能网关等）的操作系统，应具备本地自治管理功能，实现各类机电设备之间的应用协同，在公路典型应用场景中的应用满足如下要求：

7.2.1 安全效率类应用

——应支持应急预案的本地化部署、更新和执行。在与上层业务平台断连等极端情况下，能够根据本地预案，自主或协同周边相关设备执行应急联动指令。

——应支持可移动设备近场运维，近场无线通信应满足公路无线安全通信相关要求。

——宜支持环境感知类应用（如能见度监测、道路积水检测等），实现对异常天气和路况的本地监测报警及联动处理。

7.2.2 运营管理类应用

——应支持对照明类设备、监控类设备、光亮度传感器等机电设备的联动规则部署、更新和执行。能根据预设时间策略、车流量、环境光照度等条件，实现照明系统的智能调光和分组控制。

——宜支持 AI 算法的按需加载、运行和停止。AI 算法包括行人入侵监测、火情识别、烟雾识别、车辆停驶、车辆拥堵、车辆事故、路面障碍物识别等常用算法。

8 安全要求

8.1 系统安全

8.1.1 权限管理及访问控制

在轻量系统类设备和小型系统类设备上满足如下要求：

——应具备权限管控和安全访问策略功能。

——宜具备身份认证功能。

在标准系统类设备上满足如下要求：

——应具备自主访问控制能力。文件权限由文件拥有者来决定其他角色的访问权限。

——应具备强制访问控制能力。定义进程间交互以及与系统资源进行交互的权限。

——应具备确保非授权用户无法进入恢复出场模式等功能。

8.1.2 安全隔离

——具备进程间的内存隔离和进程间的存储空间隔离功能。

——提供沙箱机制，应用程序在沙箱中运行。

8.2 数据安全

应符合《物联网 泛终端操作系统总体技术要求》（GB/T 45082—2024）的相关要求。

8.3 设备认证安全

8.3.1 终端设备应使用预置对称密钥作为设备初始化信任凭据；预置对称密钥宜在设备生产阶段安全写入。

8.3.2 硬件资源较小的终端设备应采用共享对称密钥模式进行设备身份认证；应使用预置对称密钥直接作为共享对称密钥进行设备身份认证。

8.3.3 硬件资源较大的终端设备应采用数字证书模式进行设备身份认证；应使用预置对称密钥作为数字证书在线申请的信任凭据。

8.3.4 预置密钥体系、数字证书体系应由交通运输行业密钥管理和电子认证机构统一规划、生成和管理，以支持跨区域互信。

8.3.6 应支持设置白名单功能；对于非白名单的设备拒绝接入。

8.4 应用安全

对于存在扩展应用的机电设备，应提供应用安全机制，并符合如下要求：

8.4.1 应支持定制应用签名。

8.4.2 应用安装时，对应用进行签名校验。

8.4.3 应提供数据传输和控制指令的合法性校验能力。

8.5 安全升级

8.5.1 应具备升级包的完整性校验和安全签名验证机制。

8.5.2 应提供升级回滚机制，当升级失败或出现严重兼容性问题时，系统能自动或手动恢复至升级前的稳定版本。

8.6 系统日志

8.6.1 应提供日志本地存储、日志输出级别实时变更、系统日志定制化、系统日志导出等功能。

8.6.2 应提供日志本地存储的策略及产品级特性配置开关，包括日志可读权限、日志自动存储相关配置。

8.6.3 应提供系统日志的访问和接入功能，宜提供告警上报功能。

9 测试方法

9.1 测试环境要求

9.1.1 硬件环境要求

应搭建包含目标机电设备、必要的调试工具（如串口调试工具、CAN 调试工具等）、网络交换机、服务器、PC 机以及必要的公路专用设备（如传感器、控制器等）的典型硬件测试环境。

9.1.2 软件环境要求

测试 PC 应安装必要的测试工具、日志分析工具和模拟器软件，如 hdc_std 命令行工具、ssh 登录工具、网络协议分析工具等。

测试服务器应安装必要的云端应用模拟平台软件，如平台软件、机电设备云端应用组件等。

9.1.3 网络环境要求

应构建可模拟公路现场网络条件的测试网络，支持模拟网络延迟、丢包、带宽限制等不稳定情况。

9.1.4 文档要求

所有测试活动应具备完整的测试计划、测试用例和测试报告。

9.2 启动过程测试

9.2.1 启动时间测试

通过外部计时或系统日志，记录设备从通电到进入正常工作状态所需时间，验证其是否满足设计要求。

9.2.2 启动一致性测试

重复执行冷启动和热启动操作，检查系统内核、核心服务和基础应用是否每次都能正确加载和运行。

9.2.3 异常启动测试

模拟异常断电后再次上电的场景，验证系统的自恢复能力和文件系统的完整性。

9.3 基本管理测试

9.3.1 系统性能测试

通过命令行及性能测试软件工具，检查 CPU 利用率、内存使用率等性能指标。

9.3.2 DFX 功能验证

通过命令行或运维界面，验证系统日志、应用和系统事件的查询与导出、设备性能（CPU、内存）和故障监控数据的准确性。

9.3.3 配置管理验证

通过设备管理应用，对网络配置、时间同步、主备配置等功能进行设定，重启设备后检查配置是否生效并持久化。

9.3.4 升级服务验证

执行一次完整的 OTA 升级流程，包括差分包和整包升级，验证升级包校验、安装过程，并模拟升级失败场景，检验回滚机制是否正常工作。

9.4 入网和组网测试

9.4.1 设备入网测试

验证设备接入网络，并能成功连接到指定的云端模拟平台，完成注册和数据上报。

9.4.2 分布式组网测试

将至少两个测试设备置于同一局域网内，验证设备间的自动发现、安全认证和设备联动的构建过程。

9.4.3 跨设备协同测试

通过一台设备调用另一台设备的硬件能力（如摄像头）或软件服务，验证设备联动和资源共享功能。应模拟网络延迟和丢包，并验证在跨设备协同操作后，所有相关设备的关键数据和状态是否达到预期的一致性。

9.5 应用层功能测试

9.5.1 基础应用功能验证

——协议接入：验证设备能否通过 MQTT/HTTP 协议与云端模拟平台进行双向通信。

——设备运维：验证设备运维应用的各项功能，如远程登录、状态监测、设备控制等是否符合 8.1.2 章节要求。

——应用商城：验证从应用商城下载、安装、更新和卸载应用、插件和 AI 模型的功能流程。

9.5.2 扩展应用功能验证

——场景模拟：通过模拟器输入异常环境数据（如低能见度），验证环境监测应用能否正确上报和告警。

——联动测试：模拟交通事件触发条件，验证应急管理应用能否按预案执行本地设备间的联动控制。

9.6 安全能力测试

9.6.1 权限隔离测试

使用不同权限的账户登录运维应用，验证其操作和访问范围是否受到正确限制。

9.6.1 数据安全测试

检查系统存储的关键配置文件和用户数据是否以加密形式存放。

9.6.3 应用安全测试

尝试安装未签名或签名无效的应用程序包，验证系统是否会拒绝安装。

9.6.4 端口与服务扫描

使用网络安全工具扫描设备开放的端口，检查是否存在不必要的、有风险的服务。

本规程用词用语说明

1　本规程执行严格程度的用词，采用下列写法：

1）表示很严格，非这样做不可的用词，正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况下均应这样用词，正面词采用“应”，反面词采用“不应”或“不得”；

3)表示允许稍有选择,在条件许可时首先应这样做的用词,正面词采用“宜”,反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的用词，采用“可”。

2　引用标准的用语采用下列写法：

1）在标准总则中表述与相关标准的关系时，采用“除应符合本标准的规定外，尚应符合国家和行业现行有关标准的规定”。

2）在标准条文及其他规定中，当引用的标准为国家标准和行业标准时，表述为“应符合《×××》（×××）的有关规定”。

3）当引用本标准中的其他规定时，表述为“应符合本标准第×章的有关规定”、“应符合本标准第×.×节的有关规定”、“应符合本标准第×.×.×条的有关规定”或“应按本标准第×.×.×条的有关规定执行”。