ICS 29.240
CCS F21

团　　体　　标　　准

T/××× ××××—××××

电网边缘侧智能终端操作系统技术要求

Technical requirements for power grid edge smart terminal operating system

××××－××－××发布　　××××－××－××实施

中国能源研究会　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。

本文件由中国能源研究会提出、归口管理。

本文件起草单位:四川中电启明星信息技术有限公司、国网信息通信产业集团有限公司、重庆邮电大学。

本文件主要起草人:郭正雄、杨帆、赵永生、李温静、郭文静、吴大鹏、王汝言、黄宏程、周忠国、颜涛、李庆尧。

本文件首次发布，自颁布之日起执行。

电网边缘侧智能终端操作系统技术要求

1 范围

本文件规定了电网边缘侧智能终端操作系统的相关技术要求，包括对操作系统架构、操作系统基本功能、操作系统边缘计算框架技术、操作系统边端互联技术，操作系统安全保障技术，操作系统安全升级技术的要求等。

本文件适用于电网边缘侧智能终端操作系统研发商、电网边缘侧智能终端设备生产企业、系统中间件厂商、应用软件研发厂商等电网边缘侧智能终端产业参与方，规范相关参与方进行操作系统研发的设计、开发和测试等工作。

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，仅注日期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 11457-2006　信息技术 软件工程术语

3 术语和定义

GB/T 11457-2006界定的以及下列术语和定义适用于本文件。

3.1 操作系统 operating system

控制各种程序的执行并可提供资源分配、调度、输入输出控制以及数据管理等服务的软件。

[来源:GB/T 11457-2006,2.1055,有修改]

3.2 电网边缘侧智能终端操作系统 power grid smart edge operating system

电网边缘侧智能终端操作系统 power grid smart edge operating system，简称PEOS，应用于电网边缘侧设备的操作系统，电网边缘侧设备定义为北向连接电网各种主站系统，南向连接各种终端设备的装置设备，包括但不限于输电网关、变电网关、配电网关、用采网关等设备。

3.3 硬件抽象层 Hardware abstract layer

硬件抽象层 Hardware abstract layer，简称 HAL，HAL 是一种软件层，它位于操作系统内核或运行时环境与硬件设备驱动之间，目的是隐藏具体的硬件驱动细节，为上层软件提供一致的接口，使得上层软件不必关心底层硬件驱动的实现细节，从而提高上层代码的可移植性和复用性。

3.4 可移植的操作系统接口 portable operating system interface

可移植的操作系统接口 portable operating system interface，简称POSIX，它最初由IEEE组织制定，目的是使不同的操作系统之间可以互相兼容。POSIX标准定义了一系列API（应用程序接口）和命令行工具，这些API和工具规定了操作系统应该提供哪些功能，并规定了这些功能的调用方式和行为。

3.5 容器 container

容器是一种在操作系统之上提供独立运行资源的虚拟化环境，能够通过对终端部分物理资源（CPU、内存、磁盘、网络资源等）进行划分和隔离，屏蔽本容器中应用程序与其他容器或操作系统的相互影响。

3.6 消息队列遥测传输 message queuing telemetry transport

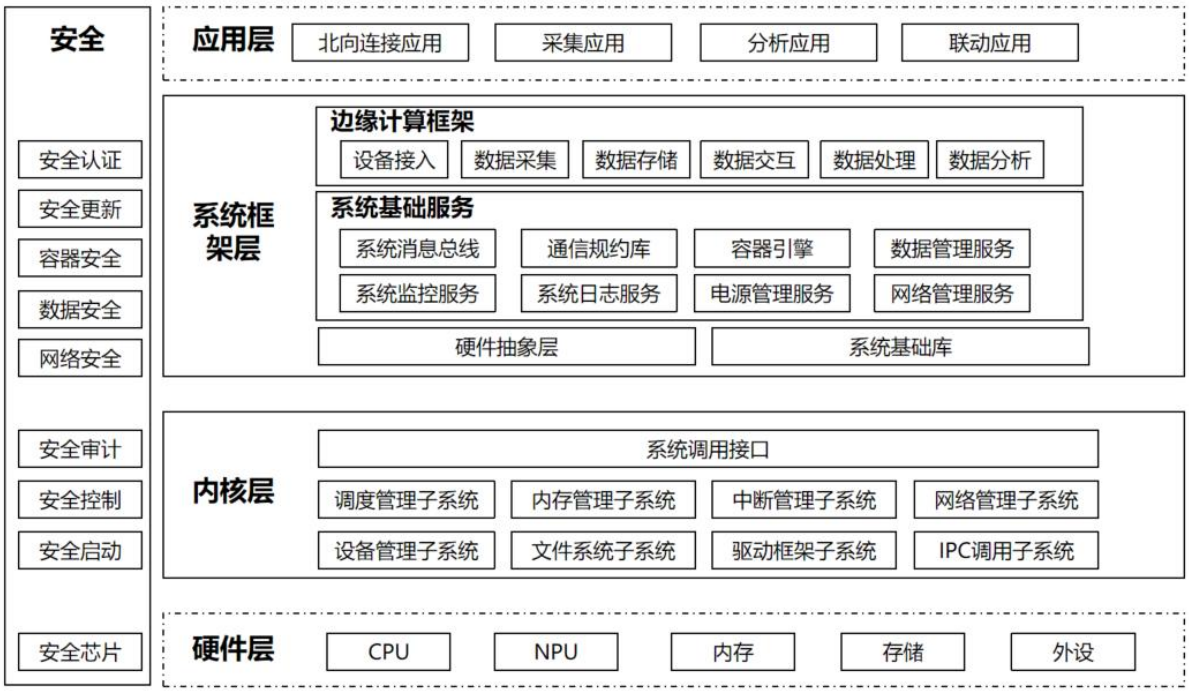
消息队列遥测传输 message queuing telemetry transport，简称 MQTT，是 ISO 标准（ISO/IEC PRF 20922）下基于发布订阅范式的消息协议。它工作在 TCP/IP 协议之上，是为硬件性能低下的远程设备以及网络状况糟糕的情况下而设计的发布/订阅型消息协议。

4 电网边缘侧智能终端操作系统参考体系架构

4.1 参考体系架构图

电网边缘侧智能终端操作系统PEOS的参考体系架构如图1：

图1 电网边缘侧智能终端操作系统PEOS的参考体系架构



4.2 参考体系分层架构描述

PEOS 参考体系架构中的分层架构描述见表 1。

分层架构	分层架构描述

内核层	提供调度管理子系统、内存管理子系统、中断管理子系统、网络管理子系统、设备管理子系统、文件管理子系统、驱动框架子系统、驱动框架子系统等基础功能。
系统框架层	提供系统基础服务以及边缘计算框架，以及提供应用编程语言需要的运行时及基础库。
应用层	各种业务应用，包含原生应用与容器化的业务应用
安全层	完整的安全体系，贯穿整个操作系统体系结构，从应用到系统框架到内核到安全芯片

表1　电网边缘侧智能操作系统参考体系架构中的分层架构描述

5　通用技术要求

PEOS应该采用模块化架构，将操作系统的功能分成多个独立的模块，如内核、网络栈、安全模块、设备驱动等，便于定制和扩展。PEOS提供一系列的编程接口，支持插件和扩展机制，使开发者能够轻松添加新的功能或改进现有功能。

5.1　硬件规格要求

PEOS应用在电网边缘侧智能终端设备之上，为了保障PEOS能够正常运行，满足电网边缘侧业务的需求，PEOS对硬件规格的CPU算力，内存，存储有下列要求。

5.1.1　CPU 架构要求

PEOS应该支持X86、AMD64、ARM/ARM64、MIPS、RISC-V，LongArch，申威等指令集架构的CPU，CPU需要最低2个核心数，主频需要最低1.8 GHz。

5.1.2　内存要求

PEOS应该支持最低512 MB大小的内存，推荐支持ECC功能的内存，提高系统稳定性。

5.1.3　存储要求

PEOS应该支持最低2 GB大小的存储。

5.1.4　外设接口要求

PEOS应该支持各类终端外设接口，如USB、SPI、I2C、RS485、串口等各种外设总线接口。

5.2　操作系统基本功能要求

PEOS操作系统内核层应该采用宏内核/微内核设计，应该需要具备包括进程/线程管理、内存管理、文件系统、网络管理和外设管理等能力，并且能够支持标准的POSIX接口。

5.2.1　进程调度管理的要求

PEOS操作系统进程调度管理应该支持以下功能：

a)　支持查询进程状态、控制进程（重启、中断、终止进程等）、监控进程、进程间通信、进程优先级设置等进程管理功能。

b)　操作系统应该提供线程/进程的管理与调度能力，进程切换时间不超过 20 微秒。

5.2.2　内存管理的要求

PEOS操作系统应支持内存映射文件、分配内存、释放内存等内存管理要求。

5.2.3 文件系统要求

PEOS操作系统应支持Ext2、Ext3、Ext4、FAT32、NTFS、XFS等文件系统类型。

5.2.4 网络协议要求

PEOS操作系统应支持TCP、UDP、UDS、MQTT、SFTP、SSH等网络协议。

5.2.5 系统信息查询要求

PEOS操作系统应支持查询系统信息，包括操作系统版本、内核版本、CPU使用率、内存使用率、存储使用率、系统启动时间、系统当前时间、系统运行时长等信息。

5.3 系统框架层要求

PEOS框架层应该为保障系统运行提供基础的服务。并且通过标准基础库以及容器引擎为上层应用程序提供基础的运行环境以及访问操作系统内核能力的接口。

5.3.1 系统基础服务

PEOS基础服务应该为整个系统运行提供基础的保障服务。包括系统消息总线、通信规约库、电源管理服务、网络管理服务、系统监控服务、系统日志服务、升级管理子系统等。

5.3.2 轻量级容器引擎

PEOS应该支持轻量级容器引擎，支持行业应用及边缘计算框架组件在容器中运行，提供安全隔离的运行环境，同时为边缘计算引擎提供基础。需满足如下规格要求：

a) 容器基础镜像应该小于 32 MB；
b) 容器基础镜像应该提供标准 C 库等基础库。

5.3.3 容器管理

PEOS 操作系统应支持通过管理通道执行以下操作：

a) 安装和卸载容器；
b) 启动和停止容器；
c) 修改容器内 CPU 占用率、内存占用率、存储资源占用率的告警门限值；
d) 查询容器内 CPU 占用率、内存占用率、存储资源占用率的告警门限值；
e) 查询容器状态：包括容器运行状态、容器版本号、容器内 CPU 占用率、容器内内存占用率、容器内存储资源占用率、创建时间、最近一次的启动时间等；
f) 召回容器日志；
g) 升级基础容器镜像。

5.3.4 容器微应用管理

PEOS 操作系统支持通过管理通道执行以下容器微应用管理操作：

a) 安装和卸载微应用；
b) 启动和停止微应用；
c) 使能和去使能微应用；
d) 修改微应用的 CPU 占用率和微应用内存占用率告警门限值；

e) 查询微应用的 CPU 占用率和微应用内存占用率告警门限值；

f) 查询微应用状态：包括微应用名称、微应用版本号、微应用运行状态、微应用的 CPU 占用率、微应用内存占用率、微应用最近一次的启动时间等；

g) 召回微应用日志。

5.3.5 HAL 技术要求

硬件抽象层（Hardware Abstraction Layer, HAL）接口规范旨在提供一种标准化的方式，让操作系统和应用程序能够与底层硬件进行交互，而无需了解具体的硬件实现细节。以下是PEOS系统HAL接口规范的关键技术要求，通过遵循这些技术规范，HAL接口可以实现硬件抽象和标准化，简化上层软件的开发，提高系统的可移植性和维护性。

5.3.5.1 HAL 模块化设计的要求

PEOS操作系统的HAL应该由多个独立的模块组成，每个模块负责特定类型的硬件设备（如GPIO、UART、I2C、SPI、ADC、PWM等）。且每个模块需要提供标准化的接口函数，以便于PEOS系统和应用程序调用。

5.3.6 系统基础库要求

PEOS应该提供一系列的基础库构建成支持应用运行的环境，包括但不限于标准C库，OpenSSL库等。

5.3.7 系统升级要求

PEOS需要支持系统升级功能：

a) 支持在线下载安装升级包或者从本地存储卡安装升级包；

b) 支持对升级包进行签名验证；

c) 支持 A/B 分区升级机制。

5.3.8 电力协议规约要求

PEOS需要内嵌支持电力行业规约协议栈,包含IEC 61850、IEC 101、IEC 104、DL/T 645、Q/GDW 1376.15、Q/GDW 1376.3、Modbus RTU、Modbus TCP等。

5.4 系统应用层要求

PEOS应用层应该包含以下功能。

5.4.1 应用开发接口支持

5.4.1.1 编程语言的支持

PEOS系统需要支持多种编程语言：

a) C/C++；

b) Java；

c) Rust；

d) Go。

满足不同开发者的需求和不同类型应用的开发需求。

5.4.1.2 编程开发接口的支持

PEOS系统需要提供以下标准的开发接口：

a) 提供安全开发工具和库（如安全的加密库、认证和授权框架），帮助开发人员编写安全的应用程序；

b) 提供多线程和并发编程接口，帮助开发人员创建高效的多线程应用程序；

c) 提供对各种数据库（如 SQLite）和文件系统（如 NTFS、EXT4）的支持，方便数据的存储和管理；

d) 提供丰富的网络编程接口和库，支持各种网络协议和通信方式，方便开发网络应用。

6 边缘计算框架技术要求

边缘计算框架的技术要求旨在确保高效、安全、可靠地在边缘环境中处理数据和运行应用程序，PEOS边缘计算框架应该包含数据采集、传输、存储和计算四大基本功能，且边缘计算框架应该采用微服务架构，支持容器化部署，并且提供高效的资源管理与编排工具，能够自动发现，配置和管理边缘设备和资源。

6.1 边缘计算框架数据采集的要求

PEOS的边缘计算框架对南向设备的数据采集有以下要求：

a) PEOS 边缘计算框架应该支持电网边缘侧智能终端设备需要支持的各种类型的设备，包括传感器，执行器和智能设备；

b) PEOS 边缘计算框架应该支持多种通信协议，如 HTTP、MQTT、CoAP、Modbus、BACnet、OPC-UA 等，以确保能够从各种设备采集数据；

c) PEOS 边缘计算框架需要提供设备注册、配置、监控和管理功能，确保设备能够被有效地集成和管理。并且需要具备可扩展性，方便对新设备与新协议的支持；

d) PEOS 边缘计算框架需要快速采集数据，需要做到 20 ms 的延时以内。并且能够处理大量设备与数据流；

e) PEOS 边缘计算框架需要支持使用统一的数据模型来表示采集到的数据，方便后续处理和分析。支持统一的数据格式（如 JSON）。

6.2 边缘计算框架数据传输的要求

PEOS的边缘计算框架对采集数据的传输有以下要求：

a) PEOS 边缘计算框架需要支持多种数据传输模式，如发布/订阅模式（MQTT）和请求/响应模式（HTTP）。并且支持事件驱动的架构，实时推送数据到订阅者。需要同时支持多方订阅；

b) PEOS 边缘计算框架需要支持在数据采集过程中需要保证数据的安全传输，支持 TLS/SSL 等加密协议。并且提供细颗粒度的访问控制，确保只有被授权的设备和用户能够采集和访问数据。

6.3 边缘计算框架数据存储的要求

PEOS边缘计算框架需要支持在边缘节点本地存储采集的数据，以应对网络不稳定或断连的情况。并且提供数据缓存功能，以优化数据传输和处理性能。

6.4 边缘计算框架数据计算的要求

PEOS的边缘计算框架对采集数据的处理有以下要求：

a) PEOS 边缘计算框架需要支持在边缘节点对数据进行预处理，如过滤、聚合和转换，减少传输数据量和中心处理负担。可以提供规则引擎，可以基于预定义规则对数据进行处理和筛选；

b) PEOS 边缘计算框架需要支持流式数据处理和实时分析，能够在边缘节点上执行复杂的数据分

析和人工智能分析任务。

7 安全技术要求

7.1 安全技术描述

PEOS应该具备一套完整的安全要求体系技术要求，旨在确保在电网边缘智能终端设备计算环境中数据和应用的安全性、隐私性和可靠性。以下是PEOS的一些关键安全技术规范要求，通过实施这些安全技术规范要求，PEOS能够在分布式和资源受限的边缘环境中提供强大的安全保障，保护数据和应用免受各种威胁和攻击。

7.2 安全国密算法的要求

PEOS应该支持SM1/SM2/SM3/SM4/SM9等国密算法。

7.3 安全启动与固件加密的要求

PEOS应该采用安全启动机制（如UEFI Secure Boot），确保电网边缘智能终端设备只能启动经过认证的可信固件和操作系统。并且对固件进行数字签名和验证，以防止未授权的固件修改和安装。

7.4 安全应用的要求

PEOS应该采用应用安全启动机制，应该具备对应用安装/启动进行安全验签的机制，确保安装运行的是安全可信的应用程序。

7.5 禁用默认 root 用户的要求

PEOS 操作系统应禁止 root 用户登录，且不允许切换为 root 用户。

7.6 内存安全保护的要求

PEOS 操作系统应具备内存安全保护机制，应对程序运行加载时的入口地址、栈地址以及堆地址进行随机化处理。

7.7 安全数据加密的要求

PEOS应该支持安全的密钥管理机制，确保加密密钥的安全存储和使用。支持在传输和存储过程中，对数据进行加密（如TLS/SSL加密传输、SM4存储加密）以保护数据的机密性。

7.8 设备和网络安全的要求

PEOS应该支持设备认证和安全配置，确保边缘设备的安全性，并防止未经授权的设备接入网络。并且采用防火墙、入侵检测和预防系统（IDS/IPS）等网络安全措施，保护边缘网络免受攻击和入侵。

7.9 安全更新和补丁管理的要求

PEOS应该支持自动更新和补丁管理，及时修复安全漏洞和缺陷，确保系统始终处于最新和安全的状态。对应用更新与补丁能够进行验证以确保其完整性和来源的可信性。

7.10 容器安全的要求

PEOS应该支持对容器进行安全配置，确保容器之间的安全隔离，防止跨容器的攻击。

7.11 边缘智能和 AI 模型安全的要求

PEOS应该支持保护边缘AI模型的机密性和完整性，防止模型被盗取或篡改。同时确保在电网边缘侧智能终端设备上运行的AI推理过程是安全的，并防止恶意输入导致的推理错误或攻击。

7.12 安全控制的要求

安全控制需要满足以下要求：

7.12.1 身份鉴别

主要包括：

a) 用户登录操作系统前，应先进行标识；
b) 操作系统用户标识应使用用户名和 UID；
c) 采用口令进行身份鉴别，并在每次用户登录系统和系统重新连接时进行鉴别；
d) 口令在存储和传输时应进行安全保护，确保其不被非授权的访问、修改和删除；
e) 口令复杂度满足数字、字母和特殊字符三种或三种以上组合，口令长度 8 位以上；
f) 应具有身份鉴别失败处理功能，对身份鉴别尝试测试和时间的阈值进行预先定义，并具备限制非法鉴别次数、连接超时自动退出等功能；
g) 应具备登录失败处理功能，对连续 5 次登录失败的同一用户，锁定账号 2 小时。

7.12.2 自主访问控制

自主访问控制应允许授权用户以用户的身份规定并控制对客体文件的访问，并阻止非授权用户对客体文件的访问。

7.12.3 标记和强制访问控制

操作系统应具备强制访问控制机制，对系统命令具有强制访问控制能力，强制访问控制机制在系统启动后生效，系统中所有命令都应遵循强制访问控制机制。

7.12.4 高危漏洞

PEOS 操作系统发布时应不存在 CVE、CNNVD 库中包含的高危漏洞。

7.12.5 远程端口

PEOS 操作系统应关闭所有非必要的远程端口。

7.13 日志与监控的要求

PEOS应该详细记录系统和应用的安全事件和操作日志，以便于审计和追踪。同时应该实施实时监控和告警机制，及时发现和响应安全事件和异常行为。

8 稳定性与可靠性技术要求

8.1 运行稳定性

PEOS 操作系统应具备连续稳定可靠运行的能力。

8.2 恢复出厂设置

PEOS 操作系统应提供还原到出厂设置状态的功能。

8.3 故障恢复

PEOS 操作系统应在断网、断电等故障恢复后正常运行。操作系统应支持在故障恢复后保持系统日志，系统配置等关键系统数据。

8.4 异常处理

PEOS 操作系统应在存储资源不足、内存不足、CPU 占用率过高等异常情况下提供以下处理机制：

a) 应在异常发生时记录告警日志；
b) 应在异常发生时上报告警；
c) 应可配置在异常状态持续一段时间后自动重启操作系统。

9 开源合规要求

PEOS 操作系统应遵循开源许可协议。

参 考 文 献

[1] GB/T 1.1-2020 标准化工作导则

[2] GB/T 13000-2010 信息技术-通用多八位编码字符集

[3] GB/T 14246.1-1993 信息技术-可移植操作系统界面

[4] GB/T 15272-1994 程序设计语言C

[5] GB/T 5271 信息技术词汇

[6] GB/T 45082-2024 物联网 泛终端操作系统总体技术要求

[7] GB 18030-2022 信息技术-中文编码字符集

[8] GB/T 30284-2020 信息安全技术-操作系统安全技术要求