ICS 29.240
CCS F21

团　　体　　标　　准

T/CERS 0096-2025

电网边缘侧智能终端操作系统技术要求

Technical requirements for Power Grid Edge Smart Device Operating System

2025-08-27 发布　　2025-08-27 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》给出的规则起草。

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这些专利的责任。

本文件由中国能源研究会提出。

本文件由中国能源研究会标准工作办公室归口。

本文件起草单位：四川中电启明星信息技术有限公司、重庆邮电大学、许昌许继软件技术有限公司、中能国研（北京）信息通信科技有限公司、中能国研(北京)电力科学研究院。

本文件主要起草人：郭正雄、吴大鹏、包伟、杨帆、何亮、温东旭、王汝言、高攀、李中锐、吴彦勇、周忠国、徐涛、黄宏程、颜涛、樊骥、李庆尧、阮正平、梁志琴、黄慕夏。

本文件为首次发布。

本文件在执行过程中的意见或建议反馈至中国能源研究会。

相关意见反馈联系方式：中国能源研究会标准执行办公室（E-mail: cers@cers.org.cn；电话：010-56284696）。

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参考体系架构、通用技术要求、边缘计算框架技术要求、安全技术要求、稳定性与可靠性技术要求、开源技术要求。

本文件适用于电网生产控制（如配电自动化 DA、馈线自动化 FA、继电保护信息管理）、运行监测（如变电站状态监测、线路在线监测）、用电信息采集、分布式能源监控、源网荷储协同控制等边缘侧核心业务场景的智能终端操作系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 36572-2018 电力监控系统网络安全防护导则

3 术语和定义

下列术语和定义适用于本文件。

3.1

操作系统 operating system

控制程序执行并提供资源分配、任务调度、输入输出控制及数据管理等服务的系统软件。

3.2

电网边缘侧智能终端操作系统 power grid edge smart device operating system（PEOS）

部署于电力系统边缘终端上的专用操作系统，北向通过电力通信网连接调度主站/云平台，南向通过工业总线或协议接入终端设备（如 FTU、智能电表等），并且具备本地化实时计算与控制能力。

3.3

硬件抽象层 hardware abstraction layer

位于操作系统内核与硬件驱动之间的技术层，通过标准化接口封装底层硬件差异，为上层提供统一的硬件访问服务，实现软件与硬件解耦。

3.4

容器 container

在操作系统层面实现的资源隔离单元，通过对 CPU、内存、存储等物理资源的划分与隔离，为应用程序提供独立的运行环境。

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

HAL：硬件抽象层（Hardware Abstraction Layer）

MQTT：消息队列遥测传输协议（Message Queuing Telemetry Transport）

NPU：神经网络处理器（Neural Processing Unit）

CPU：中央处理器（Central Processing Unit）

ECC：错误检查和纠正技术（Error Checking and Correcting）

AI：人工智能（Artificial Intelligence）

USB：通用串行总线（Universal Serial Bus）

SPI：串行外设接口（Serial Peripheral Interface）

I2C：I2C 总线（Inter-Integrated Circuit）
TCP：传输控制协议（Transmission Control Protocol）
UDP：用户数据报协议（User Datagram Protocol）
UDS：统一诊断服务（Unified Diagnostic Services）
SFTP：安全文件传输协议（Secure File Transfer Protocol）
SSH：安全外壳协议（Secure Shell）
GPIO：通用输入输出端口（General-purpose input/output）
UART：通用异步收发传输器（Universal Asynchronous Receiver/Transmitter）
PTP：精确时间协议（Precision Time Protocol）
NTP：网络时间协议（Network Time Protocol）
JSON：JS 对象简谱（Java Script Object Notation）
CoAP：受约束应用协议（Constrained Application Protocol）
SOE：事件顺序记录（Sequence of Events）
OTA：空中下载（Over the Air）
DA：配电自动化（Distribution Automation）
FA：馈线自动化（Feeder Automation）
HPLC：高速电力线载波通信（High - speed Power Line Communications）
RF：射频（Radio Frequency）

5 电网边缘侧智能终端操作系统参考体系架构

5.1 参考体系架构图

电网边缘侧智能终端操作系统（PEOS）的参考体系架构见图 1。

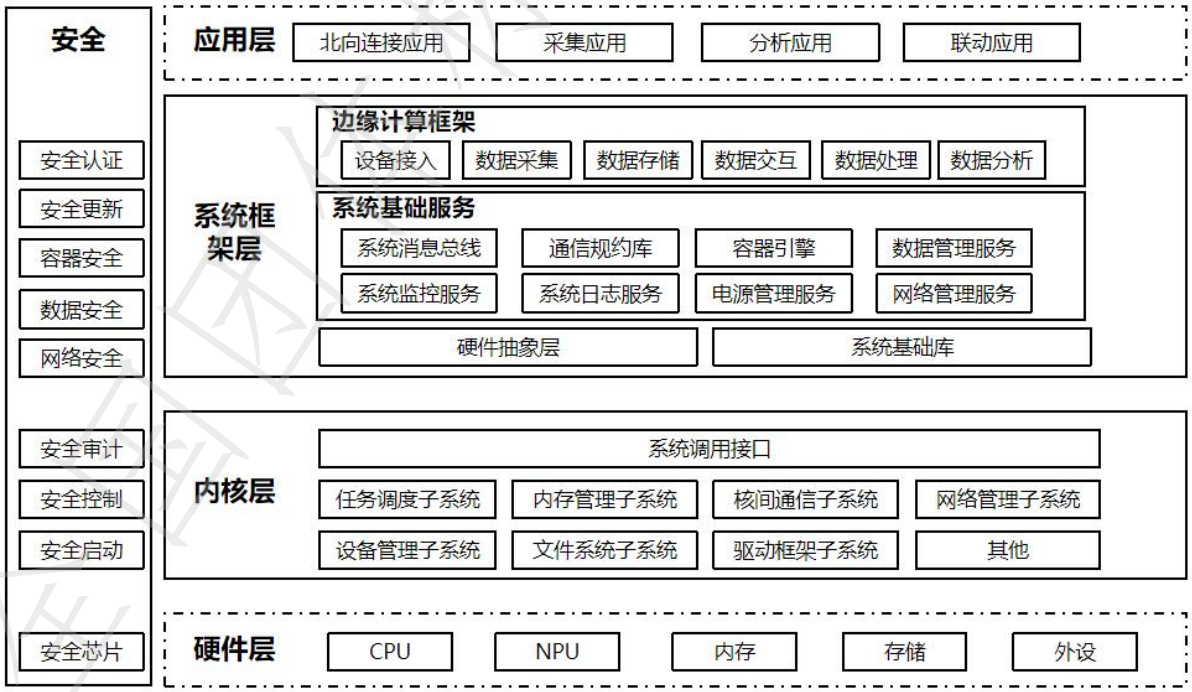

图1 电网边缘侧智能终端操作系统（PEOS）的参考体系架构

5.2 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。

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

分层架构	分层架构描述
硬件层	提供对相应硬件的支持，包含 CPU、内存、存储、NPU 人工智能加速单元及各种硬件外设。
内核层	提供任务调度管理子系统、内存管理子系统、网络管理子系统、设备管理子系统、文件管理子系统及驱动框架子系统等基础功能。提供满足电力实时控制业务需求的高精度时钟、低延迟中断响应和确定性任务调度能力。
系统框架层	提供系统基础服务以及边缘计算框架、面向电力边缘计算应用的专用服务支持以及提供应用编程语言需要的运行时及基础库，提供容器级安全隔离能力，实现不同安全等级业务应用的物理资源与运行时环境隔离。
应用层	支持符合电力安全分区要求的应用部署与隔离，支持各类业务应用（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，严格遵循 GB/T 36572 等电力监控系统安全防护规定，实现纵向加密认证、横向隔离、访问控制、安全审计等核心安全能力贯穿整个操作系统体系结构，覆盖应用层、系统框架层、内核层直至硬件安全芯片的全栈安全机制。

6 通用技术要求

6.1 硬件层要求

6.1.1 CPU 架构要求

为满足电力边缘侧终端多业务并发处理需求，PEOS应支持符合下列要求的CPU架构：

a) 应支持 X86_64、AArch64、AArch32、MIPS、RISC-V、LoongArch、SW64 等指令集架构的CPU，CPU 配置应至少包含 2 个物理处理核心，且每个核心的基础运行频率不低于 1.0 GHz；

b) 应具备电力实时业务处理需求的强实时性和确定性计算能力，并兼顾低功耗特性。

6.1.2 内存要求

PEOS应支持符合下列要求的内存：

a) 应支持最低 512 MB 大小的内存；

b) 应具备强电磁干扰环境下的数据完整性保护能力；

c) 宜支持错误校验与纠正技术（ECC）能力。

6.1.3 存储要求

PEOS应支持符合下列要求的存储：

a) 用于安装和运行的最小持久化存储空间应不少于 2 GB；

b) 宜采用工业级存储介质，具备抗振动、宽温适应性和高耐用性（擦写次数）。

6.1.4 神经网络处理器要求（NPU）

PEOS宜支持符合下列要求的神经网络处理器：

a) 宜支持 NPU 硬件驱动加载及 INT8 等量化模型推理；

b) 宜支持电力设备状态识别（如图像、声音）、异常检测、负荷预测等典型 AI 模型的加速推理。

6.1.5 外设接口要求

PEOS外设接口应满足以下要求：

a) 应支持各类终端外设接口，如 USB、SPI、I2C、RS485、GPIO、CAN、以太网、串口等各种外设总线接口；

b) 应支持 HPLC、RF 等电力专用通信模块的驱动适配；

c) 应具备防误插拔、防静电、浪涌保护等特性，以便满足电力现场安装和接线要求。

6.2 操作系统基本功能要求

6.2.1 进程调度管理要求

进程调度管理应符合以下要求：

a) 应支持进程管理功能，包括查询进程状态、控制进程（重启、中断、终止进程等）、监控进程、进程间通信及进程优先级设置等；

b) 应提供线程/进程的管理与调度能力，进程切换时间应不超过 10 毫秒；

c) 进程调度管理宜支持对电力关键业务进程进行分级调度：

1） 保护控制级（如继电保护、FA 动作）：响应时间应小于 5 毫秒，CPU 核心应独占绑定；

2） 实时监测级（如 SOE 记录、故障录波）：响应时间应小于 20 毫秒；

3） 分析计算级（如负荷预测）：可抢占资源优先级应最低。

6.2.2 内存管理要求

操作系统应支持以下内存管理功能：

a） 内存分配与释放；

b） 内存使用监控与优化；

c） 内存映射文件。

6.2.3 文件系统要求

文件系统应满足以下要求：

a) 应支持 Ext2、Ext3、Ext4、FAT32、NTFS、XFS 等主流文件系统类型；

b) 应支持掉电保护机制或日志型文件系统，以防止电力中断导致文件系统损坏或关键数据（如配置、事件记录）丢失。

6.2.4 网络协议要求

网络协议应满足以下要求：

a) 应支持 TCP、UDP、UDS、MQTT、SFTP、SSH 等网络协议；

b) 应支持 IEC 61850 GOOSE/SV、IEC 104 等电力通信协议。

6.2.5 系统信息查询要求

系统信息查询应满足以下要求：

a) 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；

b) 应支持查询关键外设（如通信模块、加密模块）的运行状态（如在线/离线、工作正常/故障）及资源使用情况（如缓存、队列深度）等。

6.3 系统框架层要求

6.3.1 系统基础服务

系统服务需保障电力业务高可用性，应支持以下功能：

a) PEOS 基础服务应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；

b) 应支持电池/超级电容后备电源管理，确保在主电源中断时能完成关键数据保存、状态上报及安全关机流程；

c) 应支持对电力关键业务进程/服务状态、关键通信链路状态、资源使用阈值（CPU、内存、存储、 网络带宽）的实时监控与告警。

6.3.2 轻量级容器技术的支持

6.3.2.1 轻量级容器引擎

PEOS应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，应满足如下规格要求：

a) 容器基础镜像应小于 32 MB；

b) 容器基础镜像应提供标准 C 库等基础库。

6.3.2.2 容器管理

PEOS 应支持通过管理通道执行以下操作：

a) 安装与卸载容器；

b) 启动与停止容器；

c) 修改容器的 CPU 占用率、内存占用率、存储资源占用率的告警门限值；

d) 查询容器的 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、版本号、CPU 占用率、内存占用率、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。

6.3.2.3 容器微应用管理

PEOS 应支持通过管理通道执行以下容器微应用管理操作：

a) 安装与卸载微应用；

b) 启动与停止微应用；

c) 使能与去使能微应用；

d) 修改微应用的 CPU 占用率及内存占用率告警门限值；

e) 查询微应用的 CPU 占用率及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、版本号、运行状态、CPU 占用率、内存占用率、最近一次的启动时间等；

g) 召回微应用日志。

6.3.3 HAL 技术要求

6.3.3.1 HAL 模块化设计要求

HAL 模块化设计应符合以下要求：

a) HAL 应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 等），且每个模块应提供标准化接口函数，以便于 PEOS 和应用程序调用；

b) 应支持电力专用硬件模块（如加密芯片、专用通信芯片、合并单元接口）。

6.3.4 系统基础库要求

PEOS 应提供一系列的基础库，构建支持的应用运行的环境，包括但不限于标准 C 库、OpenSSL 库等。

6.3.5 系统升级要求

PEOS 应支持系统升级功能，具体要求如下：

a) 支持 OTA 空中下载或从本地存储卡读取的方式安装升级包；

b) 支持对升级包实施签名验证；

c) 支持 A/B 分区升级机制；

d) 升级过程应保证电力业务的连续性或控制中断时间在最小范围内；

e) 升级失败应具备安全回滚机制，确保系统可恢复至可用状态。

6.3.6 电力规约与数据模型支持要求

电力规约与数据模型应满足以下要求：

a) 应内嵌支持电力行业规约协议栈，包括 IEC 61850、IEC 101、IEC 104、DL/T 645、Modbus RTU、Modbus TCP 等；

b) 内嵌协议栈应符合高性能、低资源占用的技术要求；

c) 应原生支持 IEC 61850(MMS、GOOSE、SV) 、IEC 104/101、DL/T 645（及各地规约）、Modbus RTU/TCP 等；

d) 应提供统一的数据访问接口、接口符合 IEC 61970/61968 CIM 或电力行业通用模型；
e) 应支持电力行业标准的时间同步协议（如 PTP，NTP）及高精度时钟保持。

6.4 系统应用层要求

6.4.1 编程语言的支持

PEOS 应支持多种编程语言，以满足不同开发者的需求及不同类型应用的开发需求，包括：
a) C/C++；
b) Java；
c) Rust；
d) Go。

6.4.2 编程开发接口的支持

PEOS 应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) 提供网络编程接口和库，支持常见网络协议和通信方式，如 Socket、HTTP、MQTT 等；
e) 应提供访问电力规约栈和统一数据模型的专用 API；
f) 提供的 API 和安全库应便于开发者构建符合电力安全防护规定的应用。

7 边缘计算框架技术要求

7.1 边缘计算框架数据采集要求

PEOS 的边缘计算框架对南向设备的数据采集应满足以下要求：
a) 应支持接入各类南向终端设备，包括智能电表、FTU、DTU、TTU、继电保护装置、合并单元、智能传感器（温度、局放、图像）、逆变器、充电桩等设备；
b) 应支持多种通信协议，如 HTTP、MQTT、CoAP、Modbus、OPC-UA、IEC61850(MMS、GOOSE、SV）、IEC104/101、DL/T645、Modbus、DNP3.0 等电力主流协议，以确保能够从各类设备采集数据；
c) 应提供设备注册、配置、监控及管理功能，确保设备能够被有效地集成和管理。并具备可扩展性，以支持新设备与新协议的快速接入；
d) 应实现数据的快速采集，对保护动作信号（SOE）、故障录波、实时遥测等关键数据的采集延迟应严格满足业务要求，宜控制在 20 毫秒的延时以内，并能处理大量设备与数据流，检测类数据采集宜控制在 200 毫秒以内；
e) 应支持使用统一的数据模型来表示采集到的数据，便于后续处理和分析，支持统一的数据格式（如 JSON）。

7.2 边缘计算框架数据传输要求

PEOS 的边缘计算框架对采集数据的传输应满足以下要求：
a) 应支持多种数据传输模式，包括发布/订阅模式（MQTT）和请求/响应模式（HTTP），事件驱动的架构实时推送数据到订阅者，并支持多方订阅；
b) 应保证数据采集过程中的传输安全，支持 TLS/SSL 等加密协议，并提供细颗粒度的访问控制，确保仅被授权的设备与用户可采集和访问数据；
c) 北向与业务主站/业务平台通信需支持符合电力安全要求的加密通道（如纵向加密）及认证机制。

7.3 边缘计算框架数据存储要求

边缘计算框架数据存储应符合以下要求：
a) 应支持在边缘节点本地存储采集数据；

b) 对于网络不稳定或断联的场景，应提供数据缓存功能；

c) 应支持存储关键事件记录（SOE）、故障录波数据、设备运行状态历史、电能质量数据等，并保证其断电不丢失；

d) 存储格式应便于后续分析，且符合电力规范，如 DL/T 860 等。

7.4 边缘计算框架数据计算要求

PEOS 的边缘计算框架对采集数据的处理满足以下要求：

a) 应支持在边缘节点对数据进行预处理（如过滤、聚合、转换），减少传输数据量及中心处理负担；

b) 应支持流式数据处理及实时分析，能够在边缘节点执行复杂的数据分析与人工智能分析任务；

c) 应提供规则引擎，基于预定义规则对数据进行处理和筛选。

8 安全技术要求

8.1 安全技术描述

PEOS 应具备完整的安全要求体系和技术要求，应符合 GB/T 36572、GB/T 22239 规定，确保电网边缘侧智能终端设备计算环境中数据与应用的安全性、隐私性及可靠性。同时，PEOS 须在分布式和资源受限的边缘环境中提供强有力的安全保障，保护数据和应用免受各类威胁和攻击。

8.2 安全国密算法要求

PEOS 应支持 SM2/SM3/SM4/SM9 等国密算法，生产控制大区业务严禁使用非国密算法。

8.3 安全启动与固件加密要求

PEOS 应采用安全启动机制（如 UEFI Secure Boot 或同等级别的安全启动机制），确保电网边缘侧智能终端设备仅能启动经认证的可信固件及操作系统。并且对固件实施数字签名和验证，以防止未授权的固件修改或安装。

8.4 安全应用要求

PEOS 应采用应用安全启动机制，具备对应用安装/启动进行安全验签的能力，确保安装运行的应用程序安全可信。

8.5 禁用默认超级用户要求

为防范未授权特权操作风险，应具备以下能力：

a) 应禁止默认超级用户远程登录及常规用户切换超级用户权限的操作；

b) 执行必要特权操作时，应通过安全审计的专用管理接口或结合本地物理访问强认证机制。

8.6 内存安全保护要求

PEOS 应具备内存安全保护机制，对程序运行加载时的入口地址、栈地址以及堆地址实施随机化处理。

8.7 安全数据加密要求

安全数据加密应具备以下功能：

a) 应具备安全的密钥管理机制，确保加密密钥的安全存储和使用；

b) 应支持在数据传输及存储过程中实施加密（如 TLS/SSL 传输加密、SM4 存储加密），以保障数据的机密性；

c) 应支持基于数字证书的设备身份认证；

d) 网络配置应遵循安全分区原则，不同安全区之间须通过符合电力行业要求的逻辑或物理隔离装置实施访问控制；

e) 应支持纵向加密认证装置或具备同等功能。

8.8 设备和网络安全要求

设备和网络安全应满足以下要求：

a) 应具备设备认证与安全配置能力，确保边缘设备的安全性，防止未经授权的设备接入网络；

b) 应采用防火墙、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。

8.9 安全更新和补丁管理要求

安全更新和补丁管理应满足以下要求：

a) PEOS 应具备自动更新及补丁管理能力，能够及时修复安全漏洞与缺陷，确保系统持续处于最新且安全的状态；

b) PEOS 应对应用更新及补丁进行验证，以保障其完整性与来源的可信性。

8.10 容器安全要求

8.10.1 容器安全基础要求

PEOS 应实施容器镜像签名验证、运行时行为监控及资源隔离策略，确保容器间攻击面最小化。

8.10.2 容器安全分级隔离要求

容器安全分级隔离要求应满足以下要求：

a) PEOS 应根据电网业务应用的差异，对容器实施安全等级分类，生产控制大区业务容器与管理信息大区容器应具备不同的安全等级；

b) 管理信息大区容器应禁止直接访问生产控制大区的容器资源；

c) 生产控制大区容器宜禁止任何南向 HTTP/RESTful API 暴露，仅允许 IEC 61850、Modbus TCP 等电力规约通信。

8.10.3 容器安全运行时安全防护要求

容器安全运行时安全防护要求应满足以下要求：

a) 应支持系统调用过滤功能，如生产控制区容器禁用 ptrace、mount 等高危系统调用；

b) 应支持文件系统保护功能，如 power_config 等关键目录设置为只读挂载；

c) 应恶意行为监测功能，如 iptables 修改等敏感操作触发审计日志。

8.11 边缘智能和 AI 模型安全要求

边缘智能和AI模型应满足以下要求：

a) 应具备边缘 AI 模型的机密性与完整性保护能力，防止模型被盗取或恶意篡改；

b) 电网边缘侧智能终端设备上运行的 AI 推理过程应保障安全，且具备抵御恶意输入引发推理错误或攻击的防护能力。

8.12 安全控制要求

8.12.1 身份鉴别

主要包括以下要求：

a) 用户登录操作系统前，应先进行身份标识；

b) 操作系统用户标识应采用用户名和 UID 组合方式；

c) 采用口令进行身份鉴别，且鉴别需在用户登录系统及系统重新连接时执行；

d) 口令在存储和传输时应进行安全保护，确保不被非授权访问、修改或删除；

e) 口令长度应至少包含 8 位字符，并混合使用大小写字母、数字及特殊符号；

f) 应具有身份鉴别失败处理功能，预先定义鉴别尝试次数及时间阈值，并支持限制非法鉴别次数、连接超时自动退出等能力；

g) 应具备登录失败处理功能，支持配置对连续登录失败的同一用户账号实施锁定及锁定时长设置。

8.12.2 自主访问控制要求

自主访问控制应支持授权用户以自身身份规定并控制对客体文件的访问权限，同时阻止非授权用户对客体文件的访问。

8.12.3 标记和强制访问控制要求

标记和强制访问控制应具备以下能力：

a) 操作系统应具备强制访问控制机制，对操作系统内核、关键系统服务、系统配置文件等客体实施强制访问控制；

b) 电力角色配置与强制访问控制策略应依据电力业务角色和安全等级进行配置，所有角色权限需符合最小权限原则。

8.12.4 高危漏洞管理要求

高危漏洞应满足以下要求：

a) PEOS 发布前，应经过严格的安全漏洞扫描和评估，不存在已知高危漏洞（包括但不限于 CVE、CNNVD 等漏洞库收录的漏洞）；

b) 应建立针对电力行业已知高危漏洞（如工控系统特定漏洞）的快速响应与修复机制。

8.12.5 远程端口管理要求

远程端口功能应满足以下要求：

a) PEOS 在面向生产网络或非安全分区的接口上，应仅开放业务必需且经过安全加固的端口，禁止开启 Telnet、FTP 等不安全协议端口；

b) SSH 访问应使用强密码或密钥认证，并限制访问源 IP 地址。

8.13 日志与监控要求

日志与监控功能应满足以下要求：

a) 应详细记录系统和应用的安全事件与操作日志，为审计和追踪依据；

b) 应具备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；

c) 应完整记录所有用户操作（重点为特权操作）、关键系统事件（如启动、关机、升级、故障）、安全事件（如登录成功/失败、访问拒绝、策略变更）及关键业务事件（如保护动作、控制命令下发）；

d) 应包含精确时标（同步于电力统一时钟），并具备防篡改能力；

e) 日志保存期限应不少于 180 天；

f) 应支持将关键安全日志及告警实时上报至业务主站安全审计平台；

g) 日志需满足 GB/T 36572 要求，记录关键操作（如保护动作、控制命令下发）并支持与主站安全审计平台对接。

9 稳定性与可靠性技术要求

9.1 运行稳定性

应在指定参考硬件平台上，模拟电力典型业务负载（含峰值冲击场景），满足 7x24 小时连续运行要求，并通过不少于 168 小时（7 天）的连续高负荷压力测试与稳定性测试。

9.2 恢复出厂设置

PEOS 应具备将系统还原至出厂设置状态的功能。

9.3 故障恢复

故障恢复应满足以下要求：

a) PEOS 应在断网、断电等突发故障恢复后，能够快速恢复并稳定运行，同时确保系统日志、系统配置等关键系统数据的完整保存；

b) 网络中断恢复后，应自动同步中断期间的电力关键数据（如 SOE、故障录波），且数据时标准确（与主站时钟校准）。

9.4 异常处理

PEOS 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) 应支持异常状态持续一段时间后自动重启操作系统的功能。重启前应保存现场信息，确保重启不会导致状态混乱或设备误动；

d) 异常重启前，宜优先保存继电保护定值、当前遥信状态等关键数据，重启后自动恢复业务（无需人工干预）。

10 开源技术要求

PEOS 在开发与使用过程中涉及的第三方开源软件，应严格遵守其对应开源许可证（如 GPL、LGPL、Apache、MIT 等）的规定，履行相应的义务（如源码提供、版权声明、许可证文本包含等）。

参 考 文 献

[1] GB/T 5271 信息技术词汇
[2] GB/T 45082-2024 物联网 泛终端操作系统总体技术要求
[3] GB 18030-2022 信息技术-中文编码字符集
[4] GB/T 11457-2006 信息技术-软件工程术语
[5] DL/T 634.5104-2009 (IEC 60870-5-104) 远动设备及系统 第 5-104 部分：传输规约
[6] ISO/IEC 9945-1:2003 信息技术.可移植操作系统接口（POSIX）.第 1 部分:基本定义
[7] ISO/IEC 20922:2016 信息技术.消息队列遥测传输（MQTT）v3.1.1
[8] ISO/IEC TR 30144:2020 信息技术-边缘计算-术语和用例