

团 体 标 准

T/CCUA LX006-2024

数据中心基础设施运维管理平台 技术要求

Data center infrastructure operation and maintenance management
platform-Technical requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

本稿完成日期：2025 年 8 月 18 日

20XX-XX-XX 发布

20XX-XX-XX 实施

中国计算机用户协会 发布

目次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 平台架构 1

5 规划设计要求 2

 5.1 设计原则 2

 5.2 规划要求 2

 5.3 技术要求 3

 5.4 能力要求 3

 5.5 性能要求 4

6 功能模块要求 5

 6.1 管理能力要求 5

 6.2 运营保障功能要求 5

 6.3 平台支撑功能要求 10

7 平台实施 11

 7.1 平台开发要求 11

 7.2 平台部署要求 11

8 测试与试运行要求 12

 8.1 一般规定 12

 8.2 功能测试 12

 8.3 试运行 12

9 平台升级要求 12

 9.1 代码更新要求 12

 9.2 版本升级要求 12

 9.3 系统扩容要求 13

 9.4 多站点多子系统接入要求 13

参考文献 0

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。

本文件由中国计算机用户协会提出并归口。

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。

本文件起草单位：

本文件主要起草人：

数据中心基础设施运维管理平台 技术要求

1 范围

本文件规定了数据中心基础设施运维管理平台的基本技术要求。

本文件适用于指导数据中心基础设施运维管理平台的规划设计、功能模块设置、平台实施、测试和升级的全生命周期过程，数据中心基础设施运维管理平台建设时可参照使用。

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 15532 《计算机软件测试规范》
- GB/T 33136 《信息技术服务 数据中心服务能力成熟度模型》
- GB 50174 《数据中心设计规范》
- GB 50462 《数据中心基础设施施工及验收标准》
- GB/T 51314 《数据中心基础设施运行维护标准》
- GB/T 51409 《数据中心综合监控系统工程技术标准》

3 术语和定义

GB 50174、GB/T 51314 和 GB/T 33136 界定的以及下列术语和定义适用于本文。

3.1

数据中心基础设施运维管理平台 data center infrastructure operation and maintenance platform

数据中心基础设施运维管理的数字化工作载体，通过监控基础设施设备，持续采集基础设施的资产、资源信息，以及各种设备的运行状态，构建业务完整、流程规范的运维服务管理体系，分析、整合和提炼有用数据，帮助数据中心运行维护人员管理运营数据中心，并提升数据中心的运维管理能力。

【来源：GB 50174-2017，2.0.43，有修改】

3.2

基础设施 infrastructure

在数据中心为保证电子信息设备安全、可靠、连续正常运行提供基本支持的空调与新风、电力与照明、防雷保护、系统接地、消防与安全保障、信息网络与布线、系统监控、给排水等设施。

【来源：GB 50462-2024，2.0.4】

4 平台架构

数据中心基础设施运维管理平台架构从下至上由采集接入层、管理应用层和展示交互层构成，如图1所示：

- a) 采集接入层用于进行基础数据采集，实现平台监控功能和各类系统的接入监控，支持包括电气系统、空气调节系统、安全防范系统、消防系统、智能化系统及其他平台，采集接入层的数据监控范围应满足 GB/T 51409 要求。
- b) 管理应用层用于支撑数据中心基础设施运维管理日常工作，提供规范化运维服务管理体系，包括管理能力、运营保障功能和平台支撑功能。其中管理能力宜包括人员管理、培训管理和计划管理等，运营保障功能宜包括监控管理、能耗管理和事件管理等，平台支撑功能宜包括系统管理、公告管理和数据管理等。
- c) 展示交互层用于多维度展示数据中心基础设施现场状态信息，支持提供移动端、可视化大屏、电脑端多种展示方式，支持不同用户不同层次内容展示，展示内容分为运维中心和监控中心，其中运维中心展示基础设施运行维护数据，涵盖值班日报、维护任务、巡检任务、应急工单和维保服务单等；监控中心展示基础设施现场状态数据，涵盖 2D 视图、3D 视图、告警数据、能耗数据和容量数据等。

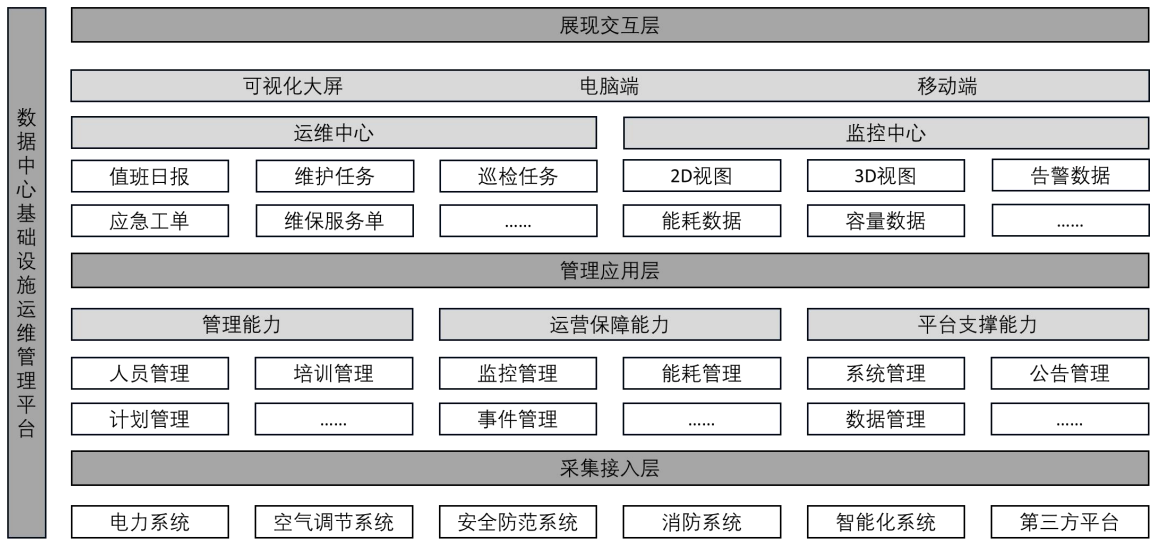


图 1 数据中心基础设施运维管理平台架构

5 规划设计要求

5.1 设计原则

平台设计应以实现基础设施运维管理核心诉求为目标，以数字化、自动化、智能化为核心，遵循标准化规范化的运维管理体系，统筹考虑运维人员操作需求及管理人员管理需求，定制化建立覆盖基础设施从正式投产、运维运营直至报废的全生命周期管理平台。

5.2 规划要求

平台发展规划应根据数据中心的建设等级、规模、功能、使用环境的要求进行，满足运行维护功能和性能指标的要求，遵循一次规划、分阶段设计实施的原则，结合业务实际情况，分阶段实现和应用部署：

- a) 初步规划和建设阶段聚焦核心架构和基础功能框架搭建，围绕数据中心基础设施运行维护和安全生产的核心工作展开，包括值班管理、巡检管理、监控管理、维护管理、应急管理等，功能满足基本使用需求，保证业务连续性，并应支持后期建设的升级改造条件，预留后期平台扩展相关接口。

- b) 功能扩展和优化阶段聚焦现有平台进行性能优化和迭代升级,提高系统的处理能力和响应速度,优化用户界面和交互设计,提升用户体验。完善现有功能模块,围绕数据中心基础设施运营和保障从多个渠道(如用户反馈、运维日志、故障报告等)收集改进需求,确保需求的全面性和准确性,对收集到的需求进行细致的分析和评估,确定需求的可行性、优先级以及改进方案,逐步增加新的功能模块使平台更加完善,包括人员管理、培训管理、容量管理、能耗管理等。
- c) 智能化应用和多站点集成部署阶段宜引入并应用自动化和人工智能技术,实现平台运维管理的智能化升级,宜支持多站点、多子系统及其他平台的接入,实现基础设施统一管理和监控,提供跨站点、跨系统和跨平台的数据分析、资源整合、数据展示功能。

5.3 技术要求

平台应采用高内聚、松耦合的模块化设计,实现功能模块的独立开发、部署与扩展,同时考虑业务未来发展需求具备灵活扩展和升级的基础。

应兼容不同操作系统,采用标准化的数据格式和开放性的通信接口,通信接口具备实现多工业通信协议兼容及扩展的能力,支持与动环监控系统,视频监控系统、楼宇自控系统和消防系统等其他智能化系统互联。

应采用冗余架构设计,容错机制等手段,关键系统异常时,自动触发故障隔离与恢复机制,单点故障不影响核心功能运行,确保系统能够稳定正常运行,不影响被监控对象的正常工作。

应支持 PC 端和移动端设备终端同时接入,终端设备宜具备足够的性能来支持运维管理平台的运行,采取安全措施防止数据泄露和恶意攻击。

宜支持机器学习、自然语言处理、大语言模型、图像识别、机器人等其他人工智能技术和自动化运维工具和技术的应用,提升平台在设备巡检、设备告警、故障应急、设备管理等运维能力的智能化程度。

5.4 能力要求

5.4.1 可视化能力

平台应具备可视化能力,支持基于基础设施架构建立 2D、3D 数字可视化模型,实时呈现机房现场、设备形态、系统架构,以及运行状态和数据。

5.4.2 感知与预警能力

平台应具备感知与预警能力,对基础设施系统设备内部及外部环境变化、状态变化、参数变化、配置变化、未授权操作等具备数据采集、监控和预警提示能力。宜对建筑漏水、设备异响、设备震动、非授权人员入侵等早期异常具备一定的探知能力。

5.4.3 学习能力

平台宜具备学习能力,能通过对基础设施系统设备的性能数据、容量数据、运行数据、日志记录数据等进行深度学习和挖掘总结,优化运维策略,提炼运维经验,获取知识或沉淀技能。

5.4.4 预测能力

平台宜具备预测能力,能基于基础设施系统设备的实时数据和历史数据,根据运维目标或结合算法建立计算模型,预测运维对象的状态。宜具备模拟仿真系统,具备对远程控制、重大变更等操作进行模拟仿真能力,提高远程操作可靠度。

5.4.5 判断能力

平台应具备判断能力，能基于预测结果、分析总结结果及模拟仿真结果对运维对象进行运行状态判断与风险评估。

5.4.6 决策能力

平台应具备决策能力，能基于运维数据、运维算法、逻辑模型进行信息搜集、加工与分析，提供智能决策或者辅助人工决策。

5.4.7 执行力

平台应具备执行能力，通过可视化场景对运维对象进行全部或部分的自动化远程控制、操作，减少人工干预。

5.5 性能要求

5.5.1 可用性

平台应支持实现 7*24 小时不间断地连续工作。

平台应具备自诊断能力，对数据紊乱、通信干扰等可自动恢复，对误操作或异常输入具备容错处理能力；对软、硬件故障及通信中断等应能诊断出故障并及时告警。

平台控制功能应具备断电自保持的能力。

平台宜支持客户端访问数量控制、接入对象数据流量控制与总量控制，防止平台出现流量与存储压力风险。

平台实时监控数据采集周期、采集延迟时间和控制命令响应时间宜满足管理要求。

5.5.2 安全性

平台应根据数据中心用户实际使用需求进行平台信息安全建设及管理。涉及的网络安全等级保护和涉密系统分级保护要求参见 GB/T 22239、GB/T 25070 以及《涉及国家秘密的信息系统分级保护管理办法》等。

平台应具有系统时间自动校准功能，应将平台接入生产时钟，统一授时。

平台应对传输和存储过程中的数据进行加密，并采取数据备份和恢复策略的措施，确保数据的机密性、完整性和可用性，数据存储时间和存储量宜满足平台各项功能需要及管理审计要求。

平台应限制非授权人员对运维管理平台的访问，确保操作仅由授权人员执行，宜采用网络层访问控制、协议层访问控制、应用层访问控制等网络架构安全技术，并结合多因素身份认证、细粒度权限控制、账号密码有效期管理等访问控制策略。

平台应在平台与外部网络之间部署防火墙，防止非法访问和恶意攻击；宜部署入侵检测系统，及时发现并应对潜在的安全威胁；应有防病毒措施。

平台宜部署安全审计系统，对运维操作进行实时监测与记录，生成审计报告，满足合规要求，防范内部安全威胁。

平台宜定期进行安全漏洞扫描，使用专业的安全扫描工具，及时发现并修复系统漏洞。

5.5.3 便捷性

平台应集中管理和展示各项运维活动的功能模块及操作界面，具备清晰、直观的用户界面并支持自定义，简便的操作流程，使得运维人员无需复杂培训即可进行日常操作。

平台应支持移动终端办公功能，移动终端支持远程查看数据中心基础设施运行数据、告警信息、统计数据，具备远程确认告警、任务推送功能等。

平台宜提供数据分析工具，支持对运行数据进行深入挖掘和分析，支持生成运维报告，辅助运维人员进行决策。

平台宜具备线上流程、远程操控平台与线下操作相互联动及校验等功能。

6 功能模块要求

6.1 管理能力要求

6.1.1 人员管理

平台人员管理应支持基础设施运维团队组织架构设计，包括整体组织架构及说明，岗位职责，工作内容，任职要求，能力要求，人员数量要求，职责矩阵及权限设置等，并支持自定义管理和展示组织架构，并与人员信息关联，能查看岗位配置的人员信息。

应支持人员信息的录入，包括姓名、专业方向、联系方式、所属组织、所属岗位、学历证照、工作年限等，并支持自定义人员信息字段展示、分级分权限管理，具备人员证照信息到期提醒功能。

宜支持根据数据中心基础设施管理需求划分团队，支持管理自身运维人员和第三方运维人员，支持对团队界别权限设定。

宜支持根据任务工作完成指标、培训考核通过率、平台操作记录、人员资质证照及自定义指标等方面对人员能力进行评定与展示。

6.1.2 培训管理

平台培训管理宜支持培训管理计划制定，包括基础设施在职员工培训计划，新员工培训计划，供应商培训计划等不同岗位不同专业培训计划。

宜支持对培训资源进行管理，包括培训材料、培训考题的上传、编制、查阅，支持在线考核，在线评阅。

宜支持对培训执行情况进行管理，包括培训评价、考核，培训结果分析展示，培训记录留存等，展示内容应包括培训计划的完成率、考核通过率、培训效果评价与建议，便于历史查询和统计分析。

宜支持培训管理与平台工作分派关联，确保未参加培训或未考核通过人员无法接收平台的工作分派或任务推送。

6.1.3 计划管理

平台计划管理宜具备工作事项创建、计划制定、任务分配、进度追踪、定时提醒、回顾分析等管理功能。

宜支持邮件等第三方平台集成，实现数据互通。

6.1.4 报告管理

平台报告管理宜支持自定义报告模版，允许根据实际场景、空间位置、系统设备等划定运营数据的统计范围，以周、月、年为单位自动生成对应周期内的数据报告。

6.1.5 决策管理

平台决策管理宜支持创建标准决策模板，自定义决策流程并可视化，动态组建决策团队。

宜支持记录完整决策过程，包括评审意见及采纳修正情况、评审人的操作记录、评审时长等。

宜具备决策结果自动通知机制，包括站内链接或附件方式通知等。

6.2 运营保障功能要求

6.2.1 监控管理

平台监控管理应与采集接入层的各系统实现互联互通，应支持采集、存储基础设施系统的实时运行数据、历史运行数据、运行状态，支持图形，图表等形式展示。

宜建立不同层级的基础设施可视化模型、供电链路拓扑结构、制冷链路拓扑结构、网络连接拓扑结构、温度云图，真实还原基础设施系统设备间的现场实际情况和逻辑关系。

宜具备基础设施系统的 3D 可视化展示功能，支持显示数据中心楼宇结构、楼层房间分布、设备及主要设备线路管路。支持实时显示每台设备的简单资产情况、维修情况，支持与环境和设备监控系统、安防监控系统等联通，支持在 3D 场景中呈现设备实时监控数据、告警数据及现场安防监控实时画面等实时监控数据。当发生事件或演练时，可视化模型宜具备辅助指挥决策的能力。

6.2.2 告警管理

平台告警管理应具备配置告警模型和告警策略功能，支持接入第三方系统的告警，支持分类分级告警，告警收敛，告警根源确定，告警升级，告警定位，告警确认，告警分析，告警屏蔽，告警静默等功能。

应不丢失任何告警信息，应具备告警信息回顾分析功能。

宜具备声光、弹窗、邮件、短信、电话、移动端通知等多种告警通知方式，支持实时故障语音播报。

宜具备根据告警分级分类生成告警处置方案、告警策略异常分析能力。

6.2.3 值班管理

平台值班管理应具备制定值班计划、自动排班等功能，宜支持人员请假、调换班、工时统计等，值班计划宜能根据人员考勤情况自动更新，值班计划及考勤记录应能留存。

应支持根据值班计划，自动创建班次交接任务，具备交接班内容创建、录入，交接班次确认，信息同步功能。

平台派发的工单任务应与当班值班计划自动匹配，支持当前班次未完成的工单进行转移交接。

6.2.4 巡检管理

平台巡检管理应建立巡检计划、模板和内容，巡检内容应符合 GB/T 51314 要求，并允许运维人员根据设备运行状况以及历史故障数据等因素自定义巡检周期、时间和内容。

宜支持移动端电子化巡检，并预留巡检机器人的数据接入接口。移动端应支持离线巡检工作，包括预先下载巡检工单，无网环境下填写、修改、提交巡检记录，网络恢复后自动将本地数据上传至服务器。

宜自动生成巡检工单和派发，具备进度展示，定时提醒、催办功能。

宜支持巡检异常与事件关联，支持巡检异常快速建立事件工单。

宜具备巡检数据校验功能，确保运维人员提交的巡检数据与系统内数据保持一致。

宜支持巡检记录的存储和查询，具备巡检情况回顾分析能力，支持历史数据的导出、可视化对比分析、异常说明、自动化生成分析数据和报告。

宜采用近场通讯技术（NFC）、射频识别技术（RFID）或二维码识别等技术，保证运维人员到达指定巡检区域后方可执行巡检工作。

6.2.5 维护管理

平台维护管理应支持建立维护计划和维护项，维护内容应符合 GB/T 51314 要求，并允许运维人员根据设备类型、运行状况、历史故障数据、运维工作安排等因素，自定义调整维护计划和内容。

宜自动生成维护任务和派发，包括维护计划审批与变更，维护任务的派发、接单、执行、评价及关闭等流程，具备定时提醒、催办功能，能自动跟踪计划的执行情况，允许延期/提前执行维护计划。

宜支持维护工单的全流程电子化管理，确保维护记录的完整性和可追溯性。运维人员可通过平台随时查阅历史维护记录，了解设备的维护历史和运行状况。

宜与事件管理、变更管理、人员管理、值班管理、设备管理、知识管理、供应商管理相关联。具备维护异常与事件、变更关联，维护人员为当班值班人员、供应商人员或其他资质信息满足要求的人员，且数量满足管理要求，维护工作质量与人员能力评定关联，维护记录与设备信息同步，维护过程中的工具及备件信息可调用设备管理的数据，维护操作流程存放于知识库，供应商维护应关联产生供应商服务记录等功能。

宜具备维护情况回顾分析能力，支持历史数据的导出，可视化对比分析，异常说明，自动化生成分析数据和报告，评估设备健康度，给出维护建议。

宜具备维修管理流程，支持维修申请发起，维修工单派发，维修过程记录，维修记录查阅。维修记录应与设备信息关联，同步设备维修信息，动态更新备件信息。

6.2.6 作业许可管理

平台作业许可管理宜具备作业电子化申请、安全风险评估、多级审批、执行记录、关闭全流程管理功能。

宜支持录入作业票模板，并支持作业票填写检验。

宜与人员管理、设备管理联动，支持验证作业人员资质，匹配运维工具。

宜内置安全作业风险库，依据作业内容提示作业过程中的潜在风险并给出防护措施。

6.2.7 应急及演练管理

6.2.7.1 应急管理

平台应急管理宜支持制定应急策略与应急方案、应急场景手动触发、应急方案自动匹配和关联展示，并派发至移动端，以便运维人员在演练和实际应急响应中快速参考和执行。

宜支持展示应急处理流程的进行情况，能判断应急流程的执行准确率，并能全程动态展示应急操作对象及现场的状态，基础设施系统的运行数据或状态，及时识别异常、判断异常。

宜具备应急处理的回顾分析能力，支持应急过程记录的导出，异常或偏差说明，自动化生成应急处理报告，应急方案的优化建议等。

宜具备特定应急场景辅助识别、应急处理建议等功能。

6.2.7.2 演练管理

平台演练管理宜具备定义演练模板、设定演练周期、设置演练内容、演练计划提醒、演练总结功能。

宜与值班管理联动，支持演练任务派发至当班值班人员。

宜支持标准作业程序和标准应急操作流程的上传和录入。

宜支持演练过程记录，具备演练全流程可视化，评定演练结果，优化演练预案功能。

6.2.8 供应商管理

平台供应商管理应具备供应商信息管理功能，支持建立人员信息台账，包括供应商名称、联系人、联系方式、资质证书、供应商服务范围、服务级别协议（SLA）和服务周期等关键信息。

宜支持建立供应商维保计划，并支持自定义调整。

宜支持自动生成服务记录单，详细记录供应商服务过程，包括服务时间、服务内容、服务人员、服务评价等，并支持对服务过程进行统计和分析。

宜具有供应商评价功能，建立评价模型，包括单次评价和服务周期内的总体评价等，定期更新评价结果。

宜与设备管理关联，供应商服务内容应与设备管理信息互相关联，自动化更新设备维保信息。

6.2.9 设备管理

平台设备管理宜建立设备的全生命周期计划和设备台账清单，包括设备核心组件，设备投产时间、设备规划使用时间、设备替换时间等。

宜支持在 3D 可视化视图中对设备的运行状态、告警信息、维护信息、维修信息、维保信息、设备投产时间等内容进行记录并集中关联展示。

宜能根据设备的历史运行数据，进行设备状态评估和故障预测，生成设备更新、设备优化或设备报废建议报告。

宜支持对维护工具和备品备件日常管理，包括建立备件及工具清单，出入库管理，实时跟踪备件及工具的库存情况和使用状态，定期发布库存盘点任务等流程，流程宜全过程线上记录。

宜能根据备件及工具库存情况，工具校验情况，进行预警提醒，并根据历史数据给出建议。

6.2.10 配置管理

平台配置管理宜能实时监测基础设施设备的重要配置参数，支持自定义、集中展示基础设施设备的实时运行状态，配置参数，支持以设备为标签查看设备配置参数，支持展示设备对应的上下游关系。

宜建立配置管理流程，配置参数变化应严格按照流程执行。

宜与变更管理、维护管理关联，及时更新配置状态。

6.2.11 容量管理

平台容量管理应能监测管理容量信息，并支持自定义展示。

宜建立数据中心不同物理层级（数据中心、机房、列、机柜、所有基础设施和 IT 设备）的容量信息模型，容量管理信息可包括空间、承重、供电、制冷、电口、光口、网口等，支持分级进行容量信息的监测、查询、配置、预警、统计、展示等管理。

宜支持对机房容量的可视化管理，在 3D 可视化环境中支持对机房内机柜的容量信息查询和直观展示，并可支持自定义容量视图展示。

宜能根据设备上架信息进行容量资源评估，自动匹配上架位置，出具部署方案，提出上架建议，辅助运维人员决策，实现资源的合理使用。

宜具备容量预测趋势分析能力，根据基础设施设备运行数据、历史数据、IT 设备部署情况，做出容量变化趋势，容量预警，容量优化建议等。

6.2.12 能耗管理

平台能耗管理应能通过监控系统实时采集数据中心的能耗数据，包括电力、水、柴油等能源消耗情况。

宜支持可视化展示数据中心不同物理层级（数据中心、机房、列、机柜、所有基础设施和 IT 设备）的能耗情况，包括实时功耗数据，历史能耗数据，能耗占比。

宜支持统计、计算能源相关数据，包括 PUE、WUE、能源成本、碳排放等，能耗测量计算方法见 GB 40879 要求。

宜提供能耗视图，支持根据用户自定义进行能源消耗不同时间跨度的趋势分析，对比分析，高能耗设备识别，能耗超限预警等，并支持生成能耗报告。

宜支持设定节能目标，根据运行数据和环境数据生成节能建议和优化方案，执行、跟踪和记录节能目标的完成情况和预警功能。

6.2.13 事件管理

平台事件管理应建立完整的事件记录与分类、事件分派与受理、事件调查与诊断、事件升级、事件解决、事件观察、事件关闭的事件流程，应按照管理要求设置审批节点和时间节点，并支持全过程线上记录。

宜支持与配置管理、知识管理、变更管理、问题管理、应急管理、设备管理相关联，支持事件的快速解决。

宜能将事件信息、事件处理实时流程状态以标准化格式通知相关人员。

宜对事件处置过程进行实时监控，支持远程协作，多地联动。

宜具备事件回顾分析能力，包括总结事件数量、类别，判断遗留事件影响范围，总结事件处理经验纳入知识库，对基础设施系统运行状态进行预测，生成事件分析报告等，并支持事件回顾分析结果多维度展示。

宜支持对设备告警及故障信息的辅助识别、汇总分析功能，结合预设规则评估事件影响范围、提供事件根因建议性分析、分类，可生成事件工单模板，关联知识库、应急方案、历史事件获取解决方案，通知运维人员，进行全流程的记录、分派和流转。

宜具备事件审计功能，对事件处理流程的不同节点进行审计，识别偏差，并能输出审计报告。

6.2.14 变更管理

平台变更管理应建立完整的变更申请、变更计划评估、变更实施评审、提交变更材料、变更实施、变更回退、变更观察、变更关闭等变更流程，应按照管理要求设置审批节点和时间节点，并支持全过程线上记录。

应能将变更类型、变更通知、变更实施的流程状态以标准化格式通知相关人员。

宜支持建立变更计划，进行合理排期。

宜对变更实施过程进行实时监控，收集变更数据，监测设备状态，识别异常，必要时启动变更调整或回退流程，支持远程协作，多地联动。

宜支持与事件管理、配置管理、知识管理、问题管理、应急管理、设备管理相关联，保证变更的顺利实施。

宜具备变更验证和观察能力，对变更前后的基础设施系统状态进行重点监测，辅助评估变更是否成功。

宜具备变更回顾分析能力，对变更过程及结果数据进行收集，分析，多维度展示，生成变更总结分析报告，总结变更方案或经验教训纳入知识库。

宜具备变更实施影响分析、变更方案可行性分析、变更回退方案可行性分析、变更成功率预测能力，提出风险或建议等，辅助变更决策。

宜具备变更管理审计能力，对变更流程的不同节点进行审计，识别偏差，并能输出审计报告。

6.2.15 问题管理

平台问题管理应建立完整的问题识别、问题准入审批与分派、问题调查诊断、问题处置方案审批、问题处置、问题观察、问题关闭的问题流程，应按照管理要求设置审批节点和时间节点，并支持全过程线上记录。

宜支持与变更管理、配置管理、知识管理、事件管理、风险管理、设备管理相关联，满足管理模块的信息流转，保持一致。

宜具备问题回顾分析能力，对问题过程及结果数据进行收集，分析，多维度展示，形成问题总结分析报告，总结问题解决办法纳入知识库。

宜具备问题影响分析、问题根因分析、问题临时解决方案建议、问题解决方案可行性分析等辅助分析能力，提出风险或建议等，辅助问题解决。

宜能根据基础设施设备告警数据、运行数据，辅助识别问题。

宜具备问题管理审计能力，对问题流程的不同节点进行审计，识别偏差，并生成审计报告。

6.2.16 风险管理

平台风险管理应支持风险项发现、指派、评估、审批、过程监控、风险解决全流程管理。

宜具备风险预警能力，能够根据监控数据和告警信息判断并报告风险，进行风险信息共享与同步。

宜支持与事件、变更管理相关联，支持从事件、变更流程的风险信息接转入。

宜支持对已识别的风险进行量化分析和等级划分，包括风险的威胁性、脆弱性和影响系数等。

宜具备风险管理回顾分析能力，对风险处理过程及结果数据进行收集，分析，多维度展示，形成总结分析报告。

宜接入成熟的风险库和专家决策，提出有效的风险应对措施建议，辅助人工决策。

6.2.17 知识管理

平台知识管理应建立完整的知识的识别、分类、评审、录入知识库、更新知识库、知识发布、知识使用分享等流程，应按照管理要求设置审批节点，并支持全过程线上记录。

宜与运维管理、事件管理、变更管理及问题管理、设备管理关联，支持知识的联动更新和获取。

应建立知识库，收录数据中心设计及建设方案、施工图纸、竣工材料、设备清单等基础资料并支持各类型知识文件上传，同类型知识的归纳合并，知识库宜支持可视化展示、浏览、自定义收藏或分享，支持知识以设备为便签查看及其他方便检索筛选的方式。

知识库宜支持动态更新，确保数据的时效性和准确性，同时宜利用机器学习和数据分析等人工智能技术，构建运维自动化决策模型，提供智能化的故障预测和修复建议。

6.3 平台支撑功能要求

6.3.1 系统管理

平台系统管理应对用户权限进行多层多级的权限配置，支持按照区域、部门、职能等业务模式进行灵活的组合，支持机房级、设备级、菜单级、数据级等多种权限设置。应将权限相同的用户放置于同一个组内，进行集中的权限管理。

宜支持对用户的系统首页界面个性化定制，根据用户职务或用户关注与其相关的系统进行自定义配置。

宜支持按照多维度（包括但不限于空间维度、设备维度、页面维度、菜单维度和操作维度等）进行权限授权。

6.3.2 移动运维终端

平台应支持移动终端登录并适配界面。

平台移动端应支持查看告警信息，查看待处理、已处理等与运维相关的工单任务列表与详情，包括巡检、维护及演练等，同时具备对工单的领取、提醒、拒绝、处理、审批、转发、上传提交、验证功能、搜索等能力。

宜支持查看设备列表、设备测点列表、测点历史运行曲线等运行数据，支持查看及操作运维流程工作，包括设备进出、备品备件出入库、人员进出、设备上下架等，宜具备发起事件能力。

宜支持通过移动端进行设备盘点任务，支持查看盘点任务列表与详情，具备扫描设备标签（条形码/二维码）快速定位设备能力，具备按区域、按设备类型查看设备统计图功能。

平台可通过在基础设施区域部署无线局域网（WiFi）为移动终端提供专属网络，接入到运维管理平台内，网络应采用白名单记录方式，仅白名单内设备可以接入网络。网络传输速率应满足移动终端数据

传输要求，宜不低于 15MB/s。无法布置无线局域网（WiFi）时，平台可根据用户实际使用和管理需求选择移动端接入方式，平台与移动端之间的数据传输安全应满足平台整体安全等级要求。

6.3.3 公告管理

平台应具备通知公告管理功能，支持授权用户自定义通知公告内容、时间及发布范围，支持多种文件、图片上传格式，实现信息内部共享。

6.3.4 日志管理

平台应对管理人员在系统内的操作都以日志形式进行保存，提供统一的日志查询界面，根据操作人、操作时间、操作类型等条件查询追溯。

日志内容应包括用户操作日志、系统运行状态日志、报警日志。所有日志可以根据查询条件生成报表，并可打印。

日志文件大小和记录的时间应可配置。日志应设定不可被任何人修改。

平台日志保存时间应不少于 6 个月。

6.3.5 数据管理

平台应能自动保存历史数据，核心数据保存时间宜不少于 3 年，应支持历史数据的定期清理。

平台宜具有按数据库容量和时间设定条件，提示将数据进行备份的功能。

平台宜支持自定义分组统计，多种形式的历史数据查询，并支持定义时间段。

平台宜支持数据导出多种文件格式，应支持用户自定义报表。

7 平台实施

7.1 平台开发要求

平台开发过程中应选用经过市场验证和广泛使用且自主可控的技术架构。

宜采用具有自主可控的安全系统、工具、数据库、算法等进行开发。

应采用持续集成和持续部署的方法，确保代码在开发过程中得到及时的测试和部署。

应使用版本控制系统对代码进行版本管理，确保代码的可追溯性和可管理性。

应优化代码质量，确保系统在高并发、大数据量等场景下仍能稳定运行。

平台代码编写应清晰、简洁、易读，遵循编码规范和最佳实践，包括代码的可读性、模块化设计、注释和文档等方面。应具有良好的可维护性，方便后续的开发和运维工作。

应建立完善的日志系统和监控机制以及及时发现和定位问题。

宜采用零代码/低代码开发平台等技术，支持业务系统的快速搭建与敏捷迭代和灵活拓展。

7.2 平台部署要求

7.2.1 硬件设备

应根据数据中心的规模、业务需求以及未来扩展计划，选择合适的平台硬件设备，满足包括但不限于以下要求：

- a) 应配备防止数据泄露和网络攻击的安全设备，以确保平台的网络信息安全宜配备具有多核中央处理器（CPU）、大内存和高速存储性能，支持多节点冗余架构（N+1 或 2N）的高性能计算服务器，以确保数据处理的高效性和稳定性。
- b) 在满足数据安全的前提下，宜采用云平台部署。

- c) 宜配备大容量、高可靠性、高可用性和高扩展性的存储设备，以满足不断增长的数据存储需求。
- d) 宜配备具备高带宽、低延迟和高可靠性的网络设备，包括交换机、路由器、防火墙和负载均衡器等，以满足实时数据传输需求。

7.2.2 部署环境

平台硬件安装物理环境和采集接入层监控系统应根据现行国家标准 GB 50174、GB/T 51409 要求以及用户实际需求设计建设。

平台硬件物理安全的设计参见 GB/T 21052 要求。

硬件设备应支持双电源供电，应采用不间断电源为设备供电。应对设备进行初步的配置和测试，确保设备能够正常启动和运行。

应为平台搭建独立的网络并绘制网络拓扑图，根据网络拓扑图配置网络设备，确保网络连接的正确性和稳定性。

8 测试与试运行要求

8.1 一般规定

平台建设工程项目的综合测试应符合 GB 50462 和 GB/T 51409 的有关规定。

测试阶段应不影响现场基础设施设备正常运行。

8.2 功能测试

平台软件功能测试应根据现行 GB/T 15532 要求，分阶段进行单元测试、集成测试、系统测试、验收测试。

软件功能测试应搭建独立的测试环境，模拟实际运行场景，确保测试结果的准确性。软件功能测试文档应包括测试计划、测试说明、测试报告、测试记录、测试问题报告。在此基础上，还应满足如下要求：

- a) 平台的硬件配置、软件配置、网络地址配置、所使用的操作系统、数据库、网络通信协议、计算性能、存储性能及网络带宽等测试结果应满足设计要求。
- b) 应对系统进行安全测试，确保系统能够抵御常见的网络攻击和病毒威胁。
- c) 应采用分层级测试，分别对单独功能模块的功能、关联功能模块的功能和平台性能进行测试并满足设计要求。
- d) 应对集成子系统进行全面测试，集成子系统联动功能应满足设计要求。

8.3 试运行

试运行阶段应试用各功能模块是否满足设计要求，单个模块试运行时间不宜少于 3 个月。

9 平台升级要求

9.1 代码更新要求

平台新代码应与现有系统代码兼容，并进行严格的测试，包括单元测试、集成测试和系统测试，避免因引入新的漏洞或性能问题，确保更新后系统能够正常运行。

平台应建立有效的回滚机制，确保在更新出现问题时能够迅速恢复到更新前的状态。

9.2 版本升级要求

平台应使用版本控制系统来管理代码的版本，确保每次升级都有明确的版本记录和升级说明。

平台新版本应在测试环境中进行充分的测试，包括功能测试、分层测试、全面测试等，确保新版本的功能和性能符合预期。

平台应具备版本升级提示功能，包括升级时间、目的和可能的影响，以使用户做好相应的准备。

平台应具备版本升级前自动备份相关数据功能。

9.3 系统扩容要求

平台的硬件设备和软件配置宜支持扩容需求。

在扩容后，平台宜合理配置负载均衡策略，以确保系统的性能和稳定性。

9.4 多站点多子系统接入要求

应制定统一的接口标准，确保不同站点和子系统之间的数据交换和通信能够顺利进行。

在多站点多子系统接入时，应加强网络安全防护，防止数据泄露和攻击。

不同站点和子系统之间的数据应实现实时同步，以保持数据的一致性和完整性。

在多站点环境中，平台应建立有效的故障自动切换机制，以便在主站点出现故障时能够迅速切换到备用站点。

参 考 文 献

- [1] GB/T 21052 《信息安全技术 信息系统物理安全技术要求》
- [2] GB/T 22239 《信息安全技术 网络安全等级保护基本要求》
- [3] GB/T 25070 《信息安全技术 网络安全等级保护安全设计技术要求》
- [4] GB 40879 《数据中心能效限定值及能效等级》
- [5] 《涉及国家秘密的信息系统分级保护管理办法》（国保发[2005]16号）