ICS 35.020
L 04

团 体 标 准

T/DZJN 24—2020

数据中心基础设施智能运维技术通则

General technical principles for Artificial Intelligence Operations of Data Center infrastructure

2020-12-15 发布　　2020-12-30 实施

中国电子节能技术协会　发布

目　　次

前　言

本文件按照GB/T 1.1-2020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。

本文件由中国电子节能技术协会数据中心节能技术委员会提出。

本文件由中国电子节能技术协会归口。

本文件主要起草单位：华为技术有限公司、中国建筑标准设计研究院有限公司、中国石油天然气股份有限公司勘探开发研究院、中国电子节能技术协会数据中心节能技术委员会、上海天诚通信技术股份有限公司、上海热像科技股份有限公司、广东宇洪科技股份有限公司、中国人民银行清算总中心、中国工商银行股份有限公司数据中心、中国工程物理研究院动力部、中国电信股份有限公司北京分公司、中国移动通信集团设计院有限公司、中城建（北京）建筑设计有限公司、北京英沣特能源技术有限公司、北京科计通电子工程有限公司、宁波北仑华彬智慧通讯科技有限公司、恒华数字科技集团有限公司、南京佳力图机房环境技术股份有限公司、贵州翔明科技有限责任公司、科华数据股份有限公司、菲尼克斯（上海）环境控制技术有限公司、深圳市龙控智能技术有限公司、联想（北京）有限公司。

本文件主要起草人：李本强、赵勇祥、吕天文、李国强、于庆友、李小兵、姚建强、王新芳、王红峰、牛琳、吕晓丹、刘长龙、李刚、李润生、杨伟、杨志波、吴晓晖、邹元霖、张士蒙、张国峰、陆进军、陆明、姚远、顾剑涛、郭建伟、黄群骥、龚慧钦、黎镜锋。

引　言

0.1　总则

随着大数据、人工智能、云计算技术的日渐成熟和飞速发展，传统的运维技术和解决方案已经不能满足需求，智能运维已成为运维的热点领域。数据中心的运维工作从传统的人工运维，经历了数字化（运维数据采集数字化、运维流程电子化）、自动化的过程，正向着智能化的方向发展。

本文件提出的数据中心基础设施智能运维是指运用数字化、自动化、智能化的平台，高效组织运维工作的运维组织方式。平台除具备自动化和可视化的能力外，还能全部或部分具备能感知、会描述、可预测、会学习、会诊断、可决策的能力。

本文件提供建立、实现、维护和持续改进智能运维工作的要求。采用智能运维方式组织运维工作是数据中心组织的一项战略性决策。数据中心组织运维智能化的建立和实现受数据中心的需要和目标、安全要求、可采用的智能化技术和产品、规模和结构的影响。所有这些影响因素可能随时间发生变化。

本文件的制定是为数据中心及其相关组织共同促进数据中心智能化提供指导，同时可供相关国家和行业、地方法律法规贯彻实施提供支持。

0.2　智能化指南

本文件可作为组织推进智能化运维工作或开发智能化运维平台产品的起点。对一个组织而言本文件中的要求和措施并非全部适用。此外，很可能还需要本文件中未包括的另外的技术、措施。

0.3　生命周期的考虑

数据中心具有生命周期，他们被策划、设计、建造/开发、测试验证、投产、运行使用、维护改造，并最终退出服务进行处置。宜在每一个阶段考虑智能化需求。

0.4　与其他标准的兼容性

本文件参考了《信息技术服务 数据中心服务能力成熟度模型》（GB/T 33136），《数据中心基础设施运行维护标准》（GB/T 51314）、 COBIT（信息及相关技术的控制目标 Control Objectives for Information and Related Technology）、《信息技术服务 治理 第5部分 数据治理规范》（GB/T 34960.5）等标准和实践。应用本文件可有效支持上述标准和实践对应条款的要求。

数据中心基础设施智能运维技术通则

1 范围

本文件提出了数据中心基础设施全生命周期的智能运维要求，以及建立、实现、维护和持续改进智能运维工作的要求。

本文件可用于：

a） 数据中心组织、数据中心代维组织

1）组织开展智能运维工作；

2）评估自身智能运维工作条件和能力；

3）评估智能运维工具平台提供商提供的产品支持智能运维的能力，选择适合的工具平台；

4）评估设备系统供应商所提供的设备系统支持智能运维的程度，选择适合的设备系统。

b） 数据中心智能运维工具平台提供组织

1）为平台研发提供输入；

2）评估自身提供的平台支持智能运维的能力和水平。

c） 数据中心设备系统提供组织

1）将智能化要求融入其提供的设备系统；

2）评估自身所提供的设备支持智能运维的程度和能力。

d） 数据中心需方组织

1）评价数据中心供方智能运维的能力和程度，选择合适的供方。

e） 第三方评价和认定

1）评价数据中心组织、数据中心代维组织智能运维的能力和水平；

2）认定智能运维工具平台符合本文件的程度；

3）认定数据中心设备系统支持本文件的程度。

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 2887-2011 计算机场地通用规范

GB/T 33136-2016 信息技术服务 数据中心服务能力成熟度模型

GB/T 51314-2018 数据中心基础设施运行维护标准

ISO20000-1：2018 Information technology - Service Management -Part 1: Service management systems - Requirements

3 术语、定义和缩略语

3.1 术语和定义

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

3.1.1

数据中心 data center

由计算机场站（机房）、机房基础设施、信息系统硬件（虚拟与物理资源）、信息系统软件、信息资源（数据）和人员以及相应的规章制度组成的实体。

[改写GB/T 33136—2016，术语和定义3.1.1]

注1：数据中心场地、机房基础设施可参考GB/T 2887—2011。

注2：数据中心场地、机房基础设施、相关环境和人员的安全要求可参考GB 9361—2011、GB/T 24001—2016以及GB/T 28001—2011。

注3：数据中心可以是集中的，也可以是分散的，用于实现信息技术资源的统一配置和调度。

注4：数据中心提供业务系统基础运行环境以及物理或虚拟的网络、服务器等计算资源和存储资源保障，输出应用服务和数据服务。

3.1.2

基础设施 infrastructure

在数据中心内，为信息系统硬件提供运行保障的设施。

[改写GB/T 51314-2018，术语和定义2.0.2]

3.1.3

安全事件 security events

由于安全边界破坏、安全措施或安全设施失效，造成的安全等级下降或信息被非法盗用等数据中心利益被侵害的事件。

3.1.4

智能 Intelligence

智力和能力的总称。

3.1.5

人工智能 artificial intelligence; AI

已工程化（即设计并制造）的系统感知环境的能力，以及获取、处理、应用和表示知识的能力。

注：知识是通过经验或教育获得的事实、信息和技能。关注良性界定的任务，处置特定问题的人工智能。

[来源：ISO/IEC 22989 CD，定义3.2.02]。

3.1.6

智能运维 Intelligent operation and maintenance

使用人工智能的方法和成果，充分利用具备自动化和可视化的能力，能感知、会描述、可预测、会学习、会诊断、可决策的人工智能平台组织运维工作的运维组织方式。

3.1.7

虚拟与物理资源 Virtual and Physical Resources

采用虚拟化技术提供的服务器等资源，以及实际物理硬件资源。

3.2 缩略语

GB/T 33136中界定的以及下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）
API：应用开发接口(Application Programming Interface)
ATS：自动转换开关（Automatic Transfer Switch）
BAS：楼宇自动化系统 (Building Automation System)
CLF：制冷负载系数(Cooling Load Factor)
CMDB：配置管理数据库（Configuration Management DataBase）
CPU：中央处理器（Central Processing Unit）
DAAS：数据作为服务的云计算服务模式（Data as a service）
DDC：显示数据通道（Display Data Channel）
DDoS：分布式拒绝服务（Distributed Denial of Service）
EOP：应急作业规程（Emergency Operating Procedure）
EEUE：电能使用效率（Electric Energy Usage Effectiveness）
ETL，数据仓库技术 （Extract-Transform-Load）
HCI：超融合基础架构（Hyper-Converged Infrastructure）
IaaS：基础设施作为服务的云计算服务模式（Infrastructure as a Service）
IDC：互联网数据中心(Internet Data Center)
IoT：物联网（Internet of Things）
IP：互联网协议（Internet Protocol）
IPS：入侵检测防御（Intrusion Prevention System）
ISO：国际标准化组织（International Organization for Standardization）
ISP：因特网服务提供商（Internet Service Provider）
IT：信息技术（Information Technology）
KPI：关键绩效指标 (Key Performance Indicator)
MOP：维护作业规程（Maintenance Operating Procedure）
MTBF：两次故障间的平均时间（Media Time Between Faults）
MTOR：故障修复所需平均时间（Media Time of Repair）
NVT：网络虚拟终端（Network Virtual Terminal）
OLA：运营级别协议（Operational Level Agreement）
OLAP：联机分析处理 （On-Line Analysis Processing）
OLTP：联机事务处理 （On-Line Transaction Processing）
PaaS：平台作为服务的云计算服务模式（Platform as a Service）
PLF：供电负载系数(Power Load Factor)
QoS：服务质量（Quality of Services）
RAID：磁盘阵列（Redundant Arrays of Inexpensive Disks）
RPO：恢复点目标 （Recovery Point Objective）
RTO：恢复时间目标（Recovery Time Objective）
SaaS：软件作为服务的云计算服务模式（Software as a Service）
SAN：存储区域网络（Storage Area Network）
SAP：业务接入点（Service Access Point）

SCP: 机房配置规程（Site Configuration Procedures）
SDS：软件定义存储 （Software defined storage）
SDDC:软件定义数据中心 （Software defined Data Center）
SDN：软件定义网络 （Software defined network）
SLA: 服务级别协议（Service Level Agreement）
SLI: 服务级别指标 (Service Level Indicator)
SLO: 服务级别目标 (Service Level Objective)
SLR: 服务级别要求 (Service Level Requirement)
SOA：基于服务的架构 （Service Oriented Architecture）
SOE：事件顺序记录（Sequence Of Event）
SOP: 标准作业规程（Standard Operating Procedure）
SQL: 结构化查询语言（Structured Query Language）
SSI：服务器端包含（Server Side Include）
STM：同步传输方式（Synchronous Transfer Mode）
UC: 支撑合同（Underpinning Contract）
UPS: 不间断电源（Uninterrupted Power Supply）
VLAN: 虚拟局域网（Virtual Local Area Network）
VPN: 虚拟专用网（Virtual Private Network）
VRRP: 虚拟路由冗余协议 (Virtual Router Redundancy Protocol)
WAF: WEB应用防火墙 (Web Application Firewall)
WAN：广域网（Wide Area Network）
WRB：Web请求代理（Web Request Broker）
WWW：万维网（World Wide Web）
XML：可扩展标记语言(eXtensible Mark-up Language)
XSS: 跨站脚本攻击（Cross Site Scripting）
XXE：XML外部实体注入漏洞（XML ExternalEntity Injection）

4 基本要求

4.1 总体原则

数据中心基础设施智能运维应遵循“安全、稳定、可靠，快速、有序、有效，体验、效率、效益”的总体原则。运维的范围、内容和要求应满足GB/T 51314的要求和本数据中心的要求以及与客户SLA的要求，智能运维不能覆盖的部分，应保留非智能方式运维。

4.2 建立智能运维目标要求

数据中心基础设施智能运维应围绕体验、效率、效益、安全设定具体的（Specific）、可测量的（Measurable）、 有达成的（Attainable）、相关的（Relevant）且有明确截止期限（Time-bound）的目标，并应与数据中心的管理目标相一致。智能运维目标可依据组织智能运维管理的能力及成熟度进行分阶段设置，通过每阶段目标的达成，最终实现数据中心智能运维体验、效率、效益、安全的统一和平衡。

数据中心基础设施智能运维管理目标应至少包括在机房安全运行、业务高可用的要求下，将基础设施运维工作由以现场“人”运维转向以“智能平台”运维，减少对人力资源的依赖；通过平台化运营数

据中心，提高基础设施运维工作效率与质量，提升业务保障能力，优化运维成本，减少对各类资源的消耗，持续优化EEUE。

数据中心智能运维能力由感知力、分析力、决策力、执行力组成，应能够有效支撑智能运维目标的实现。

注1：感知力是指对运维对象及其相关内部及外部环境变化采集的数字化信息以及含义进行认知的水平，数据中心应根据运维目标制定策略以明确对变化的敏感程度和风险偏好，进而决定数据中心对变化实现自觉的感知力水平。

注2：执行力是指为实现预定运维目标通过自动化的手段对运维对象及内外部环境施加影响的行为和过程的能力。执行过程应有明确的目标、条件、方法、效果的定义，执行力应与感知力衔接，对运维对象及其内外部环境变化做出反馈和调节。

注 3：决策力是指为了实现确定的运维目标而对未来一定时期内的运维活动及方式进行智能化选择或调整的过程，由开放的提炼能力、准确的预测能力和准确的决断能力构成。决策过程应有数据、算法、模型、流程的支撑，并在设定的运维场景替代人工的判断和决策。决策力体现数据中心运维智能化程度和水平。

4.3 赋能平台要求

数据中心基础设施智能运维应构建赋能平台。

a) 数据中心应构建、维护、持续优化数据中心统一的赋能平台以实现智能化运维；

b) 赋能平台应有效支撑基础设施的智能管控，并完整涵盖智能运维的规划设计、部署实施、例行管理、风险管控、服务支持、服务交付、监督改进全生命周期；

c) 赋能平台应通过数字化、自动化、智能化等功能模块有效支撑数据中心智能运维的感知力、控制力、决策力；

d) 应通过数据治理、数据管理提升赋能平台的感知力，实现运维管理数字化；

e) 应通过自动化、可视化能力的构建提升赋能平台的控制力，实现运维自动化；

f) 应通过能感知、会描述、会预测、会学习、会诊断、会决策的能力构建实现运维智能化；

g) 宜逐步实现与IT层智能运维全场景融合的一体化智能运维，即智能融合运维。

4.4 内外部环境要求

a) 数据中心应持续识别对智能运维目标的优化和内外部环境变化的影响，通过治理适时调整组织、策略、机制、文化，确保数据中心智能运维能力持续满足要求。内外部的环境变化包括：

1) 来自主管机构、监管组织提出的新的管理要求；

2) 来自风险管控组织或部门提出的管理要求；

3) 来自客户或业务部门提出的风险管理要求。

b) 组织应建立支持数据中心智能化转型的治理结构和管理组织，明确智能运维组织的职责及要求，落实智能运维相关的策划、实施、运行、改进工作，有效支撑智能化运维工作的持续优化；

c) 组织应明确数据中心智能运维能力建设的整体策略，并落实到对应的治理结构、管理组织、人员要求、技术实现、资源要求、管理机制、文化建设等方面；

d) 针对智能运维能力要素之间的结构关系和运行方式，组织应建立并运行评价、指导、监控以及沟通机制，以保证智能运维能力的管理、治理有效满足需求；

e) 组织应建立、培育、维护促进数据中心智能运维的精神文化。提升人员对智能运维和管理的认知、认可和认同，建设开放、共享、创新、持续改进的文化氛围。

5 组织要求

数据中心应设立能够支持基础设施智能运维的运维组织。

a)应设立专业的基础设施运维团队；

b)宜配置平台支撑管理的团队，负责管理智能运维平台运营，保证平台可用性；

c)宜设立专业技术团队，负责研究设施、系统智能化技术，以及智能运维平台及相关系统的技术、算法、模型、产品等开发；

d)应设立信息安全管理岗，或者将基础设施智能运维平台及其相关系统纳入上级组织信息安全管理团队的管理范围，以确保智能运维工作的信息安全，避免发生安全事件。

6 平台要求

数据中心应构建以运维数字化、运维自动化、运维智能化为核心的赋能平台，利用该平台提供统一的标准和规范，避免能力重复建设，提供开放的基础公共资源与服务，实现数据、流程及服务的互联互通。

数据中心智能运维应建设一个基于基础设施以及相关系统，具备对基础设施设备运行监测、控制，以及流程管理功能的智能运维系统。

智能运维系统应将电气系统、暖通系统、环控系统等进行统一管理，实时远程监视与控制；

智能运维系统应有能力将视频监控系统、门禁系统、安防系统、访客系统等统一管理，对数据中心环境进行实时监视与控制。

数据中心宜将消防系统互联到智能运维系统中；对消防系统包括火灾自动报警系统、消防联动系统、自动灭火系统等进行实时监视。

6.1 功能与性能要求

6.1.1 系统平台通用要求

a） 权限管理

应提供权限分级管理功能。

应支持以角色或组为单位进行批量授权。

应支持账户有效期设定。

应提供密码强度设定及提示功能，应具备定期提醒更换密码功能。

可采用电子证书（USBKEY）+密码双认证方式登陆。

b） 数据采集存储

平台应采集和存储各基础设施及系统的实时运行数据、运行状态、运行配置的参数；支持数据采集配置参数的在线修改；

平台应采用主流的数据库产品，应提供标准数据接口，应实现数据备份、灾难恢复、系统错误恢复、人为操作错误恢复等功能；

应实现用户标识与鉴别、存取控制、视图机制、审计和数据加密等安全控制机制功能。

c） 可靠性要求

平台应具备高可靠性和稳定性，实现 7X24 小时不间断地连续工作。

平台应采用冗余设计，局部故障不应影响整个系统的正常工作。

平台运行及故障时，应不影响监控对象的正常工作，不改变设备原有功能。

平台应具有自诊断和自恢复功能，对数据紊乱、通信干扰等可自动恢复；对软、硬件故障及通信中断等应能诊断出故障并及时告警。

6.1.2 性能要求

平台应识别不同厂家设备接入信号（数据）的差异，通过定义标准模型，为数字化管理提供统一的数据语言。

平台可接入各类设备数量、支持并发客户端访问的数量等应能满足本数据中心的当前要求和可预见的扩展要求。

告警数据数据采集延迟小于3s，实时监控数据采集延迟小于5s，控制命令在系统中的响应时间应小于 3s，设备状态变化信息响应时间应小于 3s。

系统数据应至少保存1年(其中视频数据不少于3个月），存储的数据量应能满足事后审计和模型训练的需要。

在产生告警风暴时，平台应不丢失任何告警信息，且平台运行正常。

平台应具备告警收敛功能，对于出现重大的事件时，突出呈现一条根因告警。

平台中集成的第三方子系统提供的告警信息，应可定位跟踪至设备层面，识别出故障设备。

平台应能实时监控设备的重要参数指标，且需提供UPS、空调、冷机等重要设备的运行原理图，数据刷新间隔须小于3s。

平台应提供温度云图功能，温度云图应可以3D化呈现房间、微模块的温度场分布情况，且温度云图的数据刷新时间间隔小于5s。

6.1.3 基础设施建模、展示功能要求

应采用组态功能对基础设施建模。采集组态主要包括协议、通道、设备、点表等信息，支持设备模板，可以通过设备模板快速生成单个、多个设备。

设施建模应建立各设施间的逻辑关联关系。

宜支持用户自定义建立设备管理视图。

应支持按区域或系统对设备进行分级管理、展示。

应具备基础设施及系统的 3D 可视化展示功能：

平台的3D视图需要根据虚拟仿真技术将数据中心所有设备按照实际设备的位置建模,还原数据中心全貌。

平台的3D视图应可显示楼层、机房、微模块、机柜、设备和主要设备管路、线缆路径，且3D视图可背景虚化，墙体可被设置为透明状态，突出呈现被查看的机房、微模块、机柜和设备。

平台的3D视图应可实时显示每个微模块、每个机柜的告警数量和告警等级，每个机柜的电量、冷量、承重、空间容量信息。

平台的3D视图需可集中展示温湿度传感器、摄像头、门禁等设备的监控状态和设备信息。

6.1.4 拓扑结构展示要求

配电链路呈现供电链路的全局拓扑结构，关键设备的电流、电压、功率和转换效率等核心指标，当出现告警时，供电链路做出提示；

制冷链路呈现制冷系统的全局拓扑结构，关键设备的运行功率、负载率等指标，同时提供各个节点上的温度、流量、压力等指标；

应能呈现运维网络拓扑结构；

系统需可通过大屏展示数据中心的重要监控信息，展示内容展示背景可以自由定义，且具备轮流播放功能，定时切换不同的展示内容，轮播规则可自由设置。

6.1.5 能效管理要求

应按照不同的管理域（数据中心、楼栋、机房等）配置和统计 EEUE、pPUE 数据。

应提供机柜级能耗数据的配置功能。

应提供能效数据（EEUE、CLF等）、设备的运行工况可视（能耗、功率、负载率、转速等运行状态的实时数据的监控）。

应提供EEUE调优能力，根据实时工况数据给出当前工况下最优的调优参数，并提供自动/手动下发能力。

应支持多种类型制冷设备（水冷、风冷等）和多场景（电制冷、预冷、自然制冷等）的节能调优。

应能根据数据中心的制冷系统实际运行情况，提供场景参数在线配置能力，在线选择制冷模式，配置制冷设备工程参数，从而充分适配不同数据中心差异化环境。

应能提供节能分析报告，对节能效果进行总结分析。

6.1.6 设备监视与告警管理要求

平台应具备对各基础设施及系统的监视功能，并具备多级监视功能；

应可通过操作平台的设备可视化模型，监视设备实时数据、实时状态、实时曲线、历史曲线；

平台应具备基础设施及系统的告警功能；

平台应具备告警模型、告警策略的配置功能；

平台应对基础设施及系统进行分级告警；

平台应具备基于模型或规则的收敛的功能，不会对关键报警进行收敛。告警发生时，系统应自动识别告警的源头，对其余关联告警进行收敛；

平台应具备告警多级的升级功能；

平台应具备多种告警通知方式。包括且不限于平台人机界面声光等多媒体、短信、电话、邮件、微信、手机 APP 等；

6.1.7 设备控制功能要求

平台应具备对基础设施及系统的远程、本地控制功能。运维人员可通过智能运维系统下发设施操作指令，修改设施的运行参数、策略配置参数等，实现远程控制操作；

平台宜支持运维人员的单席控制、双席位控制；

平台宜支持设备独占控制操作，防止多人或并发同时操作同一设备。

平台宜支持控制权逻辑管理，支持三级控制权位置控制；

所有的远程控制操作数据都应在系统记录；

远程控制操作应支持操作票功能，包括开票、审核确认、打印输出、操作票存档等功能。

6.1.8 预测能力要求

应具备基于大数据分析进行故障预测的能力。

应支持电池容量预测、在线养护，提前识别异常电池规避运维风险。

应支持对UPS、配电柜、母线槽等配电设备的端子、开关等温度趋势预测能力，提前诊断识别温度异常规避运维风险。

应具备对机电系统设备运行数据和信号进行采集、分析，并结合设备运行的寿命期统计规律和历史数据，预测设备运行情况的能力，以便提前采取有针对性的维护活动。

应具备基于大数据分析进行故障预测的能力。

电气系统应具备基于整定值、电流、电压、温度等参数进行电气系统或电气链路的故障预测能力。其中：

1）应支持电池寿命和容量、后备时间的预测、在线养护，提前识别异常电池规避运维风险；

2）应支持对UPS、配电柜、母线槽等配电设备的端子、开关等温度趋势预测能力，提前识别温度异常规避运维风险；

3）应支持对柴发带载能力、后备时间的预测；

4）应支持对高压直流设备模块故障的预测；

5）应支持对变压器带载能力、使用寿命的预测。

暖通系统应具备基于温度、压力、流量等参数进行暖通系统或专业设备的故障预测能力。其中：

1） 应支持基于蓄冷罐容量、负载率等参数预测机房距温升设定值的剩余时间；

2） 应支持基于室外环境温度、负载率、冷却水回水温度等参数预测冷塔工作可靠性；

3） 应支持基于负载率、压缩机吸气和排气压力等参数预判冷机运行可靠性；

4） 应支持基于电流、进水和出水压力、噪音、轴承温度、振动、同轴度等参数来预判水泵运行可靠性；

5） 应支持基于小温差来预判板换可靠工作时间；

6） 应支持基于供回水压差和温差来预判室内机运行可靠性。

宜具备对异常声响、气味、震动、活动和危险物质等特殊信息的感知与分析能力，预判风险。

6.1.9 资产与配置管理要求

平台应提供资产管理功能，对基础设备、IT设备等设备进行管理，且可以批量导入资产信息，应对设备入库、上架、变更、维修、退库等资产全生命周期进行管理。

平台的资产管理功能应可以自定义添加设备的资产属性。

平台应自动识别资产状态，应能展示实时的资产整体信息，应展示资产运行状态，应展示资产可用性状态。应能根据资产历史数据，输出资产折旧报告。应能根据资产历史数据以及运行数据，输出资产报废建议方案。

应自动启动资产审计活动；应自动化生成审计报告；宜具备资产审计全流程可视化能力；应具备审计结果多维度展示的能力；应具备资产审计异常判断能力。

数据中心正式运维前，应建立配置管理数据库。基于配置信息采集表或监控信息，自动完成配置管理数据库初始化。

基于配置管理数据库信息，自动生成逻辑拓扑和物理拓扑。逻辑拓扑和物理拓扑应采用可视化的方式呈现。

应实现配置数据与业务流程的关联，通过流程自动完成配置数据的修改。

应能够通过业务流程及监控数据自动校验配置信息，生成对账单。

与数据中心裁撤业务流程关联，自动将配置项状态标记为“已裁撤”。

6.1.10 容量管理要求

宜在智能化平台配置各类设施容量管理模型，以及容量基线，通过自动化流程管理设施容量。应采集各设施或者系统的运行数据，基于设施资源需求分析能力，分析设施运行状态。平台应提供容量配置功能，可以对数据中心电力、冷量、空间、承重、水、网络连接等关系进行编辑管理。

平台应自动监测管理容量信息；应自动识别容量影响范围，包括基础设施以及it业务。应实时采集设施运行数据或者状态；应能展示实时的容量数据，展示容量预警信息；宜通过历史数据、运行数据，输出合理容量模型以及基线；应根据设施运行数据、历史数据、业务数据，做出容量变化趋势，预警容量；应根据运行数据预测容量影响的业务范围与程度。

平台应可智能管理各个U位上的设备，自动识别U位的资产信息与变更信息。

平台应可管理计划变更的IT设备，包括待上架设备、待下架设备、待移动位置源、待移动目的地，对于计划变更的设备应可生成计划变更工单，包括上下架任务、任务流程关系，且应具备指导施工能力，宜具备控制自动上（下）架机器人工作的能力。

平台应能统计各IT设备的功耗，如最大功率，平均功率，功率趋势等。

智能平台应具备自动提出容量优化方案的能力；宜具备容量的自动优化能力；宜具备容量优化后自动验证能力。宜具备容量优化的全流程可视化能力，优化过程实现全程动态、实时、多维度可视化展示。应具备感知容量优化实施过程中设备、系统的状态能力，通过采集变更过程中相关设施或者系统的实时运行数据，描述容量状态；可通过平台控制设施运行状态，进行容量调拨以及优化；应具备容量优化总结能力；宜基于容量优化实施，形成容量优化方案知识库；应具备容量优化异常判断能力；应具备判断容量优化结果的能力。

平台应具备最佳机位搜索功能，结合电力、冷量、空间、网络、承重等因素为需要上架的设备提供推荐方案，搜索条件要求至少包括：按照设备型号，按照预留连续空间/预留电力，按照机柜规格/功率/范围等。

6.1.11 运维巡检要求

平台宜具备根据基础设施资源库的信息自动生成巡检对象能力，应能够依据GB/T 51314、本数据中心要求、SLA要求，自动生成巡检计划，包括远程线上巡检、巡检机器人巡检、人工现场巡检等方式，实现巡检内容全覆盖。

应具备巡检作业关联人员管理、排班管理、事件管理、基础设施设备资源库等模块能力。平台应支持自定义巡检视图，自定义项包括任务名称、责任人、任务周期、日期、状态、完成时间、备注等内容，并且视图可以随意选择上述项目进行筛选查看巡检任务。

可展示巡检作业计划的一览表，包括所有的巡检对象、内容、周期、人员。

应具备根据现场巡检计划，自动生成巡检工单能力。应具备对现场巡检情况进行电子化记录，异常情况自动上报（转事件工单）能力。智能巡检机器人应具备根据设定的计划和线路，定期自动完成巡检任务的能力。宜具备巡检线路可视化导航能力。宜能对巡检情况进行视频、图片记录和回放。员工携带和现场部署的各类传感器、摄像头、智能巡检机器人等应具备感知和采集基础设施和机房环境各类数据的能力，包括不限于各类温湿度、电压电流、运行状态等。

应具备根据线上巡检计划，自动生成巡检工单能力。平台应能自主执行远程巡检。应具备对线上巡检情况进行电子化记录，异常情况自动上报（转事件工单）能力。应具备对线上巡检情况自动生成报告能力。应具备线上巡检进度展示能力。应具备线上巡检结论图形化展示能力。应具备对线上巡检的总体情况进行概括总结能力。应具备对线上巡检异常情况进行详细描述能力。宜对设备运行数据分析，与历史数据进行纵向对比，判断是否有突变、波动等异常情况；与不同厂家型号进行横向对比，看哪种型号有较多异常情况。对系统级的数据分析，宜具备同一系统不同设备（如配电系统的高压、低压和PDU设备）之间的关联参数，分析出系统是否出现异常的能力。

平台应具备巡检数据校验功能，巡检人员/设备系统提交的巡检数据须与系统内的数据保持一致，以防止巡检人员数据造假现象并对监控系统数据进行校验。

应具备根据现场巡检和线上巡检情况，自动生成总体巡检报告的能力。应以各类文档文件（WORD、PDF）、网页浏览、短信、邮件等方式自动发送到相关人员。应具备总体巡检结论图形化报告生成、展示能力。宜从历史巡检结论学习到基础设施设备和系统的运行规律（健康度）等。宜从学习到的规律以及现有的运营状态，对未来可能发生的事件进行推断预测，并发出预警。

6.1.12 知识库管理要求

平台应具备知识库的管理功能，知识包括设计方案、施工方案、运维方案、事件、问题、故障、投诉解决方案、模板、SOP、MOP、EOP、自动化作业脚本等知识文档和经验，具备进行创建、更新、历史变化记录、分类、分享、审批等功能。

平台应能根据业务场景排序案例，根据应用频次进行排序，筛选出价值高的案例。

平台支持知识库功能具有收藏视图，视图只展示个人收藏过的案例，个人可对收藏过的案例进行查看，删除等。

平台应支持知识库功能具有分享视图，视图只展示个人分享过的案例，个人可对分享过的案例进行查看，删除等。

平台应支持对知识库进行更新。

6.1.13 监控与事件管理要求

通过达成6.1.6和6.1.11要求，实现预警异常事态，通过对事件的处理，保障数据中心高可用。

应能判断测点数据完整性、可靠性；宜具备检测数据基础分析能力，判断设备的生命周期阶段的能力；宜具备设备关联系统协同分析能力，可分辨变更情况下的监控数据变化；宜具备异常情况发起自检的能力，通过多个数据反复验证测点数据的准确性。

应具备自动化部署告警策略的能力，能够图形化展示告警策略，应能感知告警策略的异常；应具备根据设备运行情况，自动改变告警阀值的能力，应具备根据设备的环境数据及历史告警数据，预测设备健康度的能力，应具备复杂策略的演进能力，预测设备检查和维修处理，宜根据已发生告警的处理结果反馈，生成合理的复杂策略，并进行部署。宜具备策略异常分析的能力，如该策略在一定时间内从未出现的情况下，应进行的修订或检查工作。

应具备根据告警自动创建、派发、转派、跟催、升级、恢复确认、结单的功能。

宜具备事件自动化远程控制、处理操作，实现自愈的功能；宜具备处理方法学习能力。

6.1.14 应急管理要求

智能运维平台应能够制定与配置应急策略、应急方案。应能够建立设施应急模型；应具备设施应急方案的配置功能；应具备制定变更回退方案的能力；宜具备展示各设施的应急方案功能；宜具备应急方案模拟展示功能；宜具备判断应急方案可行性的能力。

应具备应急演练管理功能。应具备自动演练的能力；宜具备关联系统分析能力，分析演练影响范围，应自动识别演练影响范围；宜自动生成演练计划，下发演练计划与方案；宜具备演练全流程步骤可视化功能；应记录演练过程中设备运行数据；应记录演练步骤及质量；宜具备演练质量分析能力，提出问题点；宜具备应急演练操作模拟功能；应具备判断演练成功率、演练质量的功能。

应具备应急事件处理自动流程；宜具备应急处理后业务的验证能力；应具备应急处理全流程可视化能力；应急处理过程实现全程动态、实时、多维度可视化展示；应具备获取、记录应急处理实施过程中设备、系统运行数据能力，描述设施或者系统的运行状态；应具备应急处理的评估能力；宜具备应急处理方案优化建议能力；应具备应急处理异常情况判断能力；宜具备实时判断应急处理效果的能力；应具备判断产生二次事件的能力。

应能够根据应急案，以及实际应急操作，自动生成应急处理报告；宜能回顾应急处理实施情况，及时发现与管理目标之间的偏差，分析原因；宜结合现状与管理目标，给出后续措施建议，持续优化改进。

6.1.15 变更管理要求

应通过智能化的变更管理过程，提高变更的风险评估能力，降低变更风险；提高变更效率，缩短变更中断时间，减少业务受影响时间；提高变更质量，加强变更记录、跟踪和评估的精细化管理程度，并持续改进。提高平台对变更的辅助决策、自动执行能力，降低人工风险；

应具备自动需求收集、自动生成标准变更的变更方案的能力；应具备制定变更回退方案的能力；宜具备基础设施资源需求分析能力，分析设施运行状态；宜具备变更涉及的监控运维工具；宜具备关联系统协同分析能力，形成与关联系统间的变更协同方案。宜具备可行性评估能力和平台脆弱性分析能力；宜具备技术保障安排能力，根据变更级别制定保障方案。

应具备自动化变更风险评估能力，自动生成变更评估；应自动识别变更影响范围，包括基础设施以及IT业务。宜具备关联系统分析能力，分析关联系统数量、关联事项及任务；宜具备变更回退分析能力，分析变更回退方案的可行性。宜对变更方案通过模拟仿真系统进行模拟仿真（包括回退方案），可视化展示设备或者系统的变更操作；平台根据模拟仿真变更方案，智能输出变更评估报告；应自动识别变更影响范围，包括基础设施以及IT。宜具备变更准入决策能力，辅助运维人员决策可行性。

应具备变更自动化实施能力；宜具备变更后业务的自动化验证能力。应根据变更操作，在变更窗口时间内自动屏蔽变更产生告警信息；应具备变更全流程可视化能力，变更过程实现全程动态、实时、多维度可视化展示。应具备感知变更实施过程中设备、系统的状态能力，通过采集变更过程中相关设施或者系统的实时运行数据，描述运行状态；应具备变更总结能力，确认变更结果；应具备变更后监控学习能力，监控指标部署或调整应在变更后同步生效，基线自适应；应具备识别关联运维对象并进行验证的能力。应具备变更异常判断能力。对变更异常应会分析具体原因、启动应急方案。宜具备实时启动变更沟通、调整、回退流程能力，实时监测、适时启动变更的业务影响沟通、变更调整与回退。

应根据变更方案，自动完成变更流程；生成变更报告；宜具备分析回顾能力，及时分析变更情况，形成变更质量报告；宜具备变更总结能力，自动总结变更方案、变更实施过程中的经验教训等内容形成知识。宜回顾变更管理情况，及时发现与管理目标之间的偏差，分析原因。宜结合变更现状与管理目标，给出后续措施建议，持续优化改进。

6.1.16 维保管理要求

平台应具备维保基础信息管理的功能。应具备自动化更新能力，设备的维保周期，维保厂家，服务要求等信息可根据维保合同信息关联更新。设备基础信息在基础设施数据库自动化维护。应具备自动化提醒能力，预警合同的时效性情况。应具备维保基础信息的可视化能力，合同信息、设备信息等实现周期性、多维度可视化展示。宜具备维保合同续签策略分析能力，根据同类型设备、同维保厂家合同、服务要求的执行情况，给出合同续签调整分析。

应具备维保策略自动化实施能力，维保策略与合同、设备信息能自动化实现匹配。应具备维保策略优化能力，为调整维保策略提供支撑。

应能根据设备运行和维护维修数据以及备件库存数据，自动生成备品备件补充计划。

应具备设备维保生命周期自动化管理能力，维保需求审批、采购合同、执行验收、付款实现自动化线上管理。应具备设备维保生命周期管理全流程可视化能力，实现全程动态、实时可视化展示。

应具备维保计划自动化生成能力。应具备维保计划自动化调整能力。应具备维保作业计划、执行的可视化能力。维保作业计划、维保作业执行量化指标等实现周期性、多维度可视化展示。应具备维保作业成本的统计能力，形成维保成本模型。

应具备计划性维保自动化执行能力，针对设备软件设置、操作类等维保作业，可运用批处理等方式自动化远程操作完成。宜具备维修自动化执行能力，设备重启，参数调整等可远程操作的故障恢复手段，可自动化远程操作完成。应具备维保实施的可视化能力，对维保实施各环节能动态，实时进行展示。应具备感知维保实施情况能力，收集当前及历史执行数据，帮助描述系统运行状态。实时监测、适时启动维保实施对业务影响沟通、调整与回退。

应具备供应商评估自动化操作能力，通过维保管理模块能自动关联获取量化数据，对各服务商进行评估打分，并通过模块能自动将评估结果进行报批，公布。宜具备服务商评估结果分析能力，提供服务商合作选择的数据支撑。

6.1.17 优化、节能管理要求

平台应具备建立设施或者系统节能优化数字模型的能力；应具备优化模型的策略远程配置的能力；应能获取设施及系统的实时运行数据；应能获取相关设施以及运行环境的运行数据；宜具备设备优化方案可视化功能。

应具备对优化、节能实施方案的分析能力；输出设施优化方案可行性报告；应自动识别优设施优化操作的影响范围，包括基础设施以及IT。

应具备优化自动化实施能力，可远程控制、改变设施运行参数、状态；应具备优化方案自动化验证能力。宜具备优化操作全流程可视化能力，对优化过程实现全程动态、实时数据、变化进行多维度展示。应具备感知优化实施过程中设备、系统的状态能力，采集过程中相关设施或者系统的实时运行数据或者运行状态；应具备实时计算优化方案的实施状态能力；应具备诊断优化结果能力；分析优化实施结果与目标的差距；宜具备优化异常实时判断能力。对异常应会分析具体原因、启动应急方案或者预警；

应根据优化方案、实际优化数据，生成优化实施报告；宜具备分析回顾能力，及时分析变更情况，形成变更质量报告；宜具备通过分析实施过程数据，分析与管理目标之间的偏差，以及原因。应具备判断优化实施结果的能力。

6.1.18 物理安全管理要求

平台应具备安全管理策略的系统配置功能；包括监控策略、门禁权限，巡视策略等；应具备异常预警配置功能；应采集各安全管理的区域、设施等运行数据。

应具备安全事件应急处理自动流程；宜具备安全异常的预警能力；应根据安全级别，自动触发应急处理；应具备安全现状的可视化能力；安全事件的应急处理过程实现全程动态、实时、多维度可视化展示。应具备获取、记录物理安全管理的设备、系统运行数据能力，描述区域、系统安全状态；应具备安全事件处理的评估能力；应具备安全事件影响面的评估能力；宜具备安全存在风险的识别能力；应具备应急处理异常情况判断能力；应具备安全状态的判断能力；应具备实时判断安全事件状态，启动应急处理的能力。

应能自动生成数据中心安全运行报告；宜回顾安全处理实施情况，及时发现与管理目标之间的偏差，分析原因。通过分析安全类运行数据、事件，形成安全优化方案建议。

6.2 数据要求

6.2.1 数据治理要求

数据中心数字化转型是实现智能运维的前提，数据治理是数字化转型的重要内容。应建立持续、有效的数据治理过程，持续进行数据到资产的转化，实现数据的价值。

应做好数据资产管理的规划、监控和执行，在制度层面明确数据相关方的责权利，在流程层面形成端到端的闭环负反馈，协调数据相关方达成数据利益一致，促进数据相关方协同工作，实现数据资产价值最大化。

数据治理应考虑数据的机密性，完整性，可用性；应保证数据质量；应规范数据接口。

6.2.2 数据管理要求

应做好数据管理，建立数据标准，提高数据质量，要考虑数据架构、数据模型与设计、数据存储与操作、数据安全、数据集成与互操作性、文件和内容、参考数据和主数据、数据仓库和商务智能、元数据、数据质量等。

应关注数据的访问，应监视数据的存储，应控制数据处理系统中的输入输出操作。

数据应以接口访问形式，自底向上逐级开放读取、写入、收集、筛选、分组和事件订阅等功能。

数据采集，根据运维目标不同，应以指标化方式确定数据采集方式；应明确采集工具的资源消耗，应以指标化方式确定采集工具的性能指标；

数据传输，应参数化方式确定消息队列集群中保存期限，应就网络、磁盘等资源的存量和用量制定方案；

数据加工，应明确数据分类，状态和数据使用权限，制定管理流程；

数据分析，应有效管理数据分析使用的模型和参数，建立相应的数据管理规范、工具，保护分析成果；

应明确定义数据分析结果的评价指标；应分离数据分析环境和应用环境；

数据应用，应建立数据分析成果转化的持续改进流程；应对作业平台的资源用量有明确规划；

数据审计，审计数据应作为一个数据分类，按流程使用和管理。

6.3 模型要求

应对数据中心全部基础设施设备建立数字化模型，通过智能运维平台可视化展示基础设施构成与运行状况，并可实施各类设施或者系统的运维管理与操作；

数据中心基础设施数字化模型，应可视化展示（通过终端、移动端、大屏等途径）；

数据中心基础设施数字化模型宜具备运维管理操作的功能；

数据中心基础设施数字化模型，可分为静态数字化模型与动态数字化模型。

基础设施静态数字化模型，应准确记录各类基础设施属性数据，以及设施之间逻辑关系。

基础设施动态数字化模型应记录设备或者系统的实时运行数据、历史运行数据、历史维护操作类数据、历史告警、异常数据等运行、运维数据，展示基础设施实时动态以及状态；

智能设备以及系统应具备在远程控制逻辑中互斥、互锁功能；

宜建设面向对象的设施生命周期管理模型，模型宜包括设备自身属性数据、运行数据、历史操作数据、设备标准操作规定等。

6.4 信息安全要求

a) 系统应采用高安全设计，对操作系统、数据库、管理软件进行加固，管理软件与采集器之间传输通道必须采用加密传输，对于敏感数据和密码等应加密保护，可有效防御窃听、伪造、篡改、越权访问、病毒、网络入侵等危害动作，避免管理系统安全成为用户网络中的安全短板；

b)平台在系统设计阶段，应进行威胁建模，分析理解系统中潜在的安全威胁、明确风险，降低系统的攻击面，并建立相应的消减机制。系统应包括但不限于以下安全维度对系统进行威胁建模分析：仿冒(Spoofing)、篡改(Tampering)、抵赖(Repudiation)、信息泄露(Information Disclosure) 、拒绝服务(DoS)、特权提升(EoP)；

c)对于来自客户端、第三方系统等外部实体的数据请求，在使用这些数据之前都需要根据业务场景进行严格的校验，确保数据符合业务规则，基础的校验包括语法验证、数据类型、数据长度等；

d)平台应具备防注入攻击能力，包括：

1)应对所有输出到前台的不可信数据采取防XSS攻击的防范措施；

2)应支持防SQL注入处理。对于所有来自客户端、第三方系统等外部实体的数据不可信数据，进行防护处理，同时对于不可信数据进行校验；

3)应对所有来自客户端、第三方系统等外部实体的数据进行校验和处理，防止命令注入；

4)应对外部输入XML数据进行校验，并禁止外部实体解析，防止XXE注入；

5)应对每个请求都应进行校验，防止跨站请求伪造；

6)防数据泄露（数据安全传输）：在系统间传递敏感数据时，采用安全传输通道保护，如SSL、FTPS、SSH、HTTPS、IPSec等；

7)防数据泄露（数据安全存储）：配置文件等重要数据AES-CBC的加密存储。敏感数据采用强对称加密算法对其进行加解密；

8)防身份仿冒（身份验证）：使用白名单识别合法用户身份重要参数修改时进行二次身份认证；用户登录时，进行多因素认证；

9)防DOS、DDOS攻击（资源配额限制)：在单个访问请求上做资源配额限制、流量控制；使用进程白名单监控流程进程。

e)平台应进行防目录跨越处理，限制上传文件的大小，对文件头特征码进行校验，确保上传的文件类型在预期范围内，上传的文件不允许放到WEB内容目录下，具有垃圾文件清理机制。对于压缩包文件（如ZIP文件），进行压缩包文件炸弹处理；

f)平台应对于与用户绑定的数据进行横向越权校验，防止合法登录用户之间的横向越权；

g)在密码不需要还原的场景下，平台应使用业界公认安全的不可逆加密方式对密码进行加密；在密码需要还原的场景使用对称加密算法进行加密。密码不应明文保存或显示。应使用强密码策略与密码修改策略，如长度限制、字符组合及弱密码检测等，用于防止密码攻击；

h)平台应具有对口令防暴力破解能力，登录失败三次以上，宜要求输入验证码。登录失败五次以上，宜锁定IP；

i)平台应对敏感数据进行保护，包括：

1)敏感数据不允许明文存储在认证端的系统中，使用安全的加密算法加密保护。在不需要还原敏感数据的场景下，必须使用不可逆算法加密；

2)敏感数据传输需要通过加密通道或者数据加密后传输；

3)敏感数据的访问需要要有认证、授权；

4)敏感数据不允许存储在应用程序的内存中；

5)敏感数据不允许使用私有加密算法。

j)平台需具备数字签名功能，防止软件安装包和升级包被篡改，在版本安装和升级时自动进行软件完整性签名验证，签名验证过程遵循RFC3161规范；

k)平台应提供个人数据说明，只收集业务范围需要使用的数据，对个人数据加密进行保存，在浏览器显示时进行部分匿名化处理，手机APP在收集或使用个人数据前，明确提示用户，并获得用户的明示同意；

l) 日志管理：日志需包含安全日志、系统日志和操作日志，涵盖系统内所有的用户活动和操作指令，且不允许删除。对系统的安全事件、系统情况、操作动作等都做到有迹可循，可查，可诊。用户活动包括但不限于：

登录和注销；

增加、删除用户和用户属性（帐号、口令等）的变更；

用户的锁定和解锁，禁用和恢复；

角色权限变更；

系统相关安全配置（如安全日志内容配置）的变更；

重要资源的变更，如某个重要文件的删除、修改等。

操作指令包括但不限于：

对系统配置参数的修改；

对系统进行启动、关闭、重启、暂停、恢复、倒换；

对业务的加载、卸载；

软件的升级操作，包括远程升级和本地升级；

对重要个人数据的创建、删除、修改；
所有帐户的命令行操作命令。

m)平台所在服务器的操作系统应部署防病毒系统，自动更新病毒库，并更新系统补丁，能够发现并抵制外来软件（病毒或非法用户）的攻击；

n）操作系统、数据库、管理软件加固：系统应对操作系统、数据库、软件使用各种加固手段进行加固。如限制和禁用不安全的服务、限制登录次数和登录时间、限制连接数和连接时间、限制内存大小、限制访问路径、限制操作权限等；

o）用户鉴权：系统应对用户进行登录认证，必须先登录才能访问，对每一个需要授权访问的请求都应核实用户的会话标识是否合法、用户是否被授权执行此操作。对于多次登录失败的，应锁定账号IP；

p）安全访问协议：系统应使用业界公认标准安全的协议来登录后台服务器或访问设备，安全协议参考SSHv2、HTTPS、FTPS、SNMPv3、TLSv1.1、TLSv1.2。

6.5 运维对象智能化要求

数据中心基础设施的设备以及系统应满足智能化功能要求，开放运行数据、运行参数、API，支持本地、远程的被监测、被控制、SOE等功能；

数据中心智能基础设备应采用行业主流协议，与智能运维系统平台互联实现监测与控制功能；

数据中心应配置时钟同步系统或设备，完成对设备时钟同步监视与控制，保证数据中心范围内各基础设施设备以及相关系统的时钟同步。

电气接口应具备安装便捷、稳定、可靠等特性。

线缆应具备抗干扰、阻燃等特性。

通讯协议应具备双向信息传输能力，应具备定义清晰、通讯距离长、兼容性好、易扩展、开发难度低等特点，宜具备纠错机制。

7 人员要求

7.1 职责要求

在制定运维制度和建立运维流程时，应根据人机协作情况，确定人员的运维职责。

数据中心宜配置智能运维系统平台运维团队，负责：

a）通过智能平台对基础设设备及系统进行远程监测、控制操作与管理；

b）负责智能平台运营管理，包括平台可用性、平台优化等管理；

数据中心应明确平台运维团队、现场维护团队的职责与界面；形成远程运维与现场运维的综合运维能力；

数据中心平台运维团队宜配置监控岗、管控岗。平台远程控制操作应得到监督、复核，即操作过程应有监管，操作结束有确认。

7.2 能力要求

数据中心运维人员应具备相关能力证明，对于特殊岗位应具备相关管理部门或者组织的授予资质证书，以满足操作规范以及安全性。

设施运维的智能运维平台的设备控制操作人员，应具备相关管理要求的操作能力认可，宜具有上岗证；

数据中心应定期对运维人员进行技术、管理类培训、考核和优化，提高组织的运维能力。

8 流程管控要求

运维流程，应清晰界定人机界面，充分发挥智能化优势。

运维流程以及相关业务流程宜在智能运维平台运行，应支撑各设施运维场景。

运维流程引发数据变更时，应及时对变更数据进行更新、保存，并应满足后期审计要求。

运维流程管理宜具有流程的OLA管理、流程预警、流程分析报表等功能。

数据中心应根据智能运维流程与设备智能化水平、智能平台成熟度情况、业务场景等因素，定期评估、优化流程以及相关管理要求。

数据中心运维远程操作应建立操作票管理机制，管理操作风险。

9 资源投入要求

数据中心应站在数字化转型、战略发展的高度，认识智能运维的必要性与紧迫性，获得组织高层的认同与支持，在人力、财力、物力等方面保障充足的投入。应优先保障数据治理和赋能平台建设。

注：数据治理是数字化转型的前提，是智能化运维的基础，赋能平台则是数据中心企业级智能平台，是智能运维的核心能力。

数据中心应对基础设施设备及系统、智能运维平台的建设、运维投入资源研究；宜对设施智能化能力和水平进行评估，提出设备的智能化功能要求；应持续对智能运维平台的模型、算法等进行开发，满足运维需求；应持续提升平台自身运行质量与能力，保障平台高可用性。

10 基础设施全生命周期管理过程对智能运维的支持要求

数据中心基础设施的全生命周期管理是面向设施设备及系统的管理方法论，涉及规划设计、建设测试、运营及退役四个阶段。智能化运维不只是运营阶段的目标，更应在全生命周期的前期做完整和精确的规划和设计，并作为项目的全生命周期关键目标贯穿始终。

10.1 规划设计阶段

在设计数据中心硬件架构（配电架构、制冷架构）同时，应在智能运维平台上开始数据模型的构建，其中关键要素是容量设计和拓扑关系设计，应在数据模型中准确定义。

a)在数据中心关键设施设备层面，应选择符合自动化、智能化要求和接口标准定义的设施设备；设备与设备间连接的电缆或管道（包括相关联的开关及阀门），宜使用空间信息的模型进行描述和定义；

b)在数据中心功能设计层面，应全面考虑全面支持自动化运维的场景，重点在于基于ECC的远程监控和操作功能的实现。

10.2 建设和验证测试阶段

在正常的数据中心硬件的工程建设和测试的同时，智能运维平台的功能开发及软硬件联调工作应并行开展。平台功能应能提供包含配电和制冷系统等完整统一的监、管、控、智平台，应整合设备厂家原有的BA自控系统，并与消防自控系统形成联动。应严格遵循软件测试流程和方法对平台进行功能性测试和验证，应特别关注平台接口采集设备的遥测数据的质量，以及设备遥控功能的可靠性。

10.3 运营阶段

运营管理的业务需求相关流程（监控、事件、变更、问题、变更、巡检、演练、维保等）应与智能化的操作平台紧密结合，线上流程、远程操控平台应与线下操作相互联动及校验。

应建立以设备管理为核心的管理模型以及相关大数据分析平台，将设备的固有属性信息、动态运行数据、运行相关操作逻辑以及运营管理相关业务场景做全方位的记录、聚合及联动分析，为对设备下一步的调整或操作提供必要的决策依据。

应建立以数据中心整体系统为对象的运行管控平台与机制，在数据中心投运、加载、降载、运行调整与优化、事件及故障处理、应急处理等，实时性高、直接影响可用性的运行操作，应以运行中心远程操控为主、现场人工备用。

10.4 退役阶段

应对设施设备建立健康管理档案库、历史记录及运营健康度模型，并对设施设备运行状态进行准实时的记录和评估，在结合可靠性影响及综合风险评估，对设备的退役做预先的规划和计划。