ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

算力监控平台建设技术规范

Clinical Auxiliary Examination Management Specifications

（工作组讨论稿）

（本草案完成时间：2026-4-22）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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，参照《团体标准管理规定》相关要求编制。

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专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

算力监控平台建设技术规范

1 引言

本标准的制定旨在规范算力监控平台的建设、部署、运行与维护，解决当前算力监控中存在的异构资源兼容不足、监测精度不够、智能化水平不高、数据互通不畅等问题，推动算力资源“可感知、可调度、可计量、可追溯”，助力全国一体化算力网建设，支撑数字经济高质量发展。本标准兼顾落地性与前瞻性，吸纳算力态势感知自动化监测最新实践，融入 AI 智能优化、非侵入式监测等创新技术，为各行业算力监控平台建设提供统一技术依据，适用于算力监控平台的规划、设计、开发、部署、验收及运维等全流程。

2 范围

本标准规定了算力监控平台（以下简称“平台”）的术语和定义、总体架构、技术要求、部署要求、安全要求、运维要求、验收要求及前瞻性技术布局。

本标准适用于各类算力基础设施（包括通用算力中心、智算中心、超算中心、边缘算力节点及多云异构算力资源）的监控平台建设，涵盖政府、企业、科研机构等各类算力使用及管理主体，可作为平台规划设计、开发实施、检验验收、运维管理的技术依据。

3 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 33745-2017 信息技术 云计算 参考架构

GB/T 37722-2019 信息技术 大数据 数据安全管理指南

TC609-6-2025-05 全国一体化算力网算力资源管理与调度技术要求

《全国一体化算力网监测调度平台建设指南》（草案）

《关于全面开展算力态势感知自动化监测工作的通知》（工信部办公厅，2026 年）

4 术语和定义

下列术语和定义适用于本文件。

4.1 算力 computing power

医综合数据处理能力，从处理能力的分类可划分为通算算力、智算算力、超算算力、量子算力等，包含硬件处理、软件处理及网络传输等综合能力。

4.2 算力监控平台 computing power monitoring platform

具备算力资源接入、数据采集、实时监测、智能分析、告警预警、可视化展示、数据交互等功能，能够实现对多源异构算力资源全生命周期监控与管理的一体化平台。

4.3 异构算力资源 heterogeneous computing power resources

不同架构、不同类型、不同来源的算力资源，包括 CPU 集群、GPU 集群、FPGA、ASIC、边缘计算节点、公有云算力、专有云算力、超算资源等。

4.4 非侵入式监测 non-intrusive monitoring

不侵入算力资源底层系统及业务流程，通过标准化接口、镜像采集、流量分析等方式实现算力数据采集与状态监测的技术方式，可避免对业务运行造成影响。

4.5 算力态势感知 computing power situation awareness

通过对算力资源的实时监测、数据挖掘与智能分析，全面掌握算力规模、负载状态、运行质量、能耗水平及发展趋势，为算力调度、资源优化提供决策支撑的能力。

4.6 调度引擎 scheduling engine

调度系统中负责执行调度策略的核心模块，能够基于业务类型、任务体量、资源状态、网络性能、能耗等多维因素，动态选择调度方案，实现任务的自动分发、资源部署与处理。

4.7 算力“一本账” computing power "single account"

通过算力态势感知自动化监测，构建统一的算力资源台账，全面、精准、动态掌握算力规模、

类型、分布、利用率等关键指标，形成覆盖监测范围的算力资源全景图。

5 总体架构

平台采用“分层架构、分布式部署、模块化设计”，遵循“统一标准、开放兼容、智能高效、安全可靠”的原则，整体分为5层，自上而下依次为：应用层、智能分析层、数据处理层、采集接入层、资源层，同时配套安全保障体系、运维管理体系和标准规范体系，支撑平台全生命周期稳定运行。架构设计兼顾当前落地需求与未来扩展，支持与国家级、省级算力监测平台互联互通，契合“1总+N分”的体系化贯通模式。

5.1 资源层

平台监测的核心对象，包括各类算力资源、网络资源、存储资源及配套基础设施，涵盖通用算力、智算算力、超算算力等多类型算力，公有云、专有云、边缘云等多来源算力，以及CPU、GPU、FPGA等多架构算力资源，是算力数据的源头。

5.2 采集接入层

平台的数据入口，负责各类算力资源、网络、存储及基础设施数据的采集与接入，支持多协议、多来源、多类型资源的接入与格式转换，采用侵入式与非侵入式相结合的采集方式，确保数据采集的全面性、实时性和准确性，构建“数据中心—平台—上级监测节点”的全链路自动采集与报送机制。

5.3 数据处理层

负责对采集到的原始数据进行清洗、转换、整合、存储与管理，建立统一的数据标准和数据模型，解决数据碎片化、格式不统一等问题，为上层智能分析和应用展示提供高质量的数据支撑，同时实现数据质量核查与异常修正。

5.4 智能分析层

平台的核心能力层，依托大数据、人工智能、机器学习等技术，实现算力负载分析、异常检测、趋势预测、能耗优化、调度辅助等功能，支持多因子综合分析，具备自学习、自优化能力，提升算力监控的智能化水平。

5.5 应用层

面向用户的交互层，提供可视化展示、告警预警、报表统计、权限管理、接口开放等功能，满足不同用户（管理员、运维人员、业务人员）的个性化需求，支持多终端访问，实现算力态势“一屏统览”。

5.6 配套体系

安全保障体系：涵盖数据安全、网络安全、应用安全、终端安全，落实网络安全等级保护要求，构建“平台安全+边界安全+数据传输链路安全”的一体化安全防护体系，保障平台及数据的安全可靠。

运维管理体系：建立平台部署、运行、维护、升级的标准化流程，实现运维工作的规范化、自动化，提升平台运维效率，降低运维成本。

标准规范体系：遵循本标准及相关国家、行业标准，建立数据接口、数据格式、监测指标、技术参数等方面的统一标准，确保平台的兼容性、可扩展性和互联互通性。

6 技术要求

6.1 采集接入技术要求

6.1.1 采集范围

采集范围应全面覆盖资源层所有对象，具体包括：

算力资源：CPU 利用率、内存使用率、GPU 负载、算力输出、任务执行状态、队列长度等；

网络资源：带宽利用率、时延、抖动、丢包率、端口状态、网络连接数等；

存储资源：存储容量利用率、IOPS、吞吐量、存储延迟、磁盘健康状态等；

基础设施：机房环境（温度、湿度、UPS 状态、供配电状态）、设备运行状态等；

业务数据：任务类型、任务优先级、任务执行时长、算力调度记录等。

6.1.2 采集方式

非侵入式采集：优先采用 API 接口、SNMP 协议、镜像采集、流量分析等非侵入式方式，适用于无法进行侵入式部署的第三方算力资源、核心业务节点，避免影响业务正常运行，构建非侵入式双向数据链路；

侵入式采集：对于自有算力资源、非核心业务节点，可采用部署采集代理、探针等方式，实现更精细、更实时的数据采集；

采集频率：支持自定义配置，核心指标（如 CPU 利用率、GPU 负载）采集频率不低于 1 次/分钟，普通指标采集频率不低于 1 次/5 分钟，可根据业务需求动态调整；

格式转换：支持多格式数据的接入与转换，包括 JSON、XML、CSV 等，实现异构数据的标准化处理，支持 20+数据格式识别与提取，自动修复编码错误、乱码字符，修复成功率不低于 90%。

6.1.3 接入兼容性

支持多类型、多架构、多来源算力资源的接入，包括但不限于：

架构兼容：x86、ARM、RISC-V 等多种 CPU 架构，GPU、FPGA、ASIC 等异构加速芯片；

平台兼容：公有云（阿里云、腾讯云、华为云等）、私有云、混合云、边缘计算平台、超算平台；

协议兼容：支持 SNMP、HTTP/HTTPS、SSH、Telnet、Modbus 等多种通信协议，支持自定义协议扩展；

资源适配：支持对所接入资源的信息校验、健康监控与状态同步管理，提供接入流程的可视化引导与日志审计。

6.2 数据处理技术要求

6.2.1 数据清洗与转换

清洗规则：能够自动识别并处理缺失值、异常值、重复值，采用“局部敏感哈希+分布式计算”方案实现近似去重，误判率控制在 0.5%以内；

数据转换：将不同格式、不同单位的原始数据转换为统一标准的数据格式和单位，确保数据的一致性；

数据校验：建立数据质量核查机制，采用元数据标注、智能校验等技术手段，对采集数据进行质量评估与异常检测，形成“数据回流”机制。

6.2.2 数据存储

存储架构：采用“时序数据库+关系型数据库+对象存储”的混合存储架构，时序数据库用于存储实时监测数据（如 InfluxDB、Prometheus），关系型数据库用于存储配置数据、用户数据等，对象存储用于存储历史数据、日志数据等；

存储性能：支持高并发写入，实时数据写入延迟不超过 100ms，查询延迟不超过 500ms；

数据留存：实时监测数据留存至少 3 个月，历史数据留存至少 1 年，支持数据归档与备份，备份周期不超过 24 小时，备份数据留存至少 6 个月；

数据加密：对敏感数据（如用户信息、算力调度数据）进行加密存储，采用 AES-256 加密算法，确保数据安全。

6.2.3 数据管理

数据建模：对算力资源、网络、存储等数据进行标准化建模，明确数据字段、数据类型、数据约束，支持 TOSCA、YANG 等建模语言，实现资源的抽象与标准化描述；

数据目录：建立统一的数据目录，实现数据的分类管理、检索与溯源，支持数据血缘分析；

数据同步：支持与外部系统（如算力调度平台、政务数据平台、行业业务系统）的数据同步，支持实时同步与定时同步两种模式，同步延迟不超过 5 分钟。

6.3 智能分析技术要求

6.3.1 算力负载分析

实时分析：实时分析各算力节点的负载状态，包括 CPU、内存、GPU 等资源的利用率，识别负载过高、负载过低、负载波动过大等异常情况；

趋势分析：基于历史数据，采用时间序列分析、机器学习等技术，预测算力负载的变化趋势，提前预警负载峰值，支撑算力调度决策；

负载均衡建议：根据负载分析结果，自动生成算力负载均衡建议，指导算力资源的动态调整与调度，提升资源利用率。

6.3.2 异常检测与告警

异常检测：采用 AI 算法（如孤立森林、LSTM、异常检测模型），结合规则引擎，实现对算力资源、网络、存储等异常情况的自动检测，包括设备故障、资源过载、网络中断、数据异常等，异常检测准确率不低于 95%；

告警分级：将告警分为紧急告警、重要告警、一般告警三个级别，明确各级告警的触发条件、处理流程和响应时限；

告警方式：支持短信、邮件、钉钉、企业微信、平台弹窗等多种告警方式，支持告警接收人、告警频率的自定义配置，支持告警升级机制；

异常溯源：支持异常事件的溯源分析，定位异常发生的原因、影响范围和持续时间，提供异常处理建议。

6.3.3 能耗优化分析

融入绿色算力理念，实现能耗的实时监测与优化分析：

能耗监测：实时采集算力设备、机房的能耗数据，计算算力能效比（PUE），监测能耗变化趋势；

优化建议：基于能耗数据与算力负载数据，采用 AI 算法生成能耗优化建议，如设备启停调整、负载迁移、机房环境优化等，助力降低 PUE，实现绿色算力；

能效评估：定期对算力资源的能效进行评估，生成能效报告，为算力基础设施的绿色升级提供依据。

6.3.4 调度辅助分析

支撑算力资源的高效调度，提供多维度调度辅助分析：

多因子分析：支持基于算力类型、性能、能耗、延迟、位置等多因子的综合分析，为调度决策提供

数据支撑；

调度策略适配：支持对多调度因子设置权重排序，适配不同业务场景的调度需求，如低延迟优先、高性价比优先等；

AI 调度优化：支持基于强化学习等 AI 算法进行调度优化，实现多任务并发调度、依赖控制，提升调度效率与资源利用率。

6.4 应用层技术要求

6.4.1 可视化展示

全景展示：提供算力资源全景视图，包括算力规模、分布、负载状态、能耗水平、告警信息等，实现“一屏统览”；

个性化展示：支持根据用户角色（管理员、运维人员、业务人员）自定义展示内容，支持多维度数据钻取、筛选与对比；

终端适配：支持 PC 端、移动端（手机、平板）访问，适配不同屏幕尺寸，确保展示效果清晰、操作便捷；

实时更新：可视化数据实时更新，更新频率与采集频率同步，确保数据的实时性。

6.4.2 报表统计

报表类型：支持生成算力负载报表、能耗报表、告警报表、资源利用率报表、调度报表等多种类型报表；

自定义报表：支持用户自定义报表模板、统计维度、统计周期（日、周、月、季度、年）；

报表导出：支持报表导出功能，导出格式包括 Excel、PDF、CSV 等，方便数据归档与分析。

6.4.3 权限管理

角色分级：支持基于 RBAC（基于角色的访问控制）模型，设置超级管理员、管理员、运维人员、普通用户等不同角色，明确各角色的权限范围；

权限分配：支持精细化权限分配，可针对具体功能模块、数据范围分配权限，确保数据安全与操作规范；

操作审计：记录用户的所有操作行为，包括登录、查询、修改、删除等，形成操作日志，日志留存至少 6 个月，支持日志查询与追溯。

6.4.4 接口开放

接口类型：提供 RESTful API、WebSocket 等多种类型接口，支持外部系统（如算力调度平台、业务系统、上级监测平台）的接入与数据交互；

接口规范：制定统一的接口规范，明确接口参数、请求方式、返回格式、调用频率限制等，确保接口的兼容性与可扩展性；

接口安全：对接口调用进行身份认证与权限控制，采用 Token 认证、IP 白名单等方式，防止非法调用，确保接口安全。

7 部署要求

7.1 部署架构

分布式部署：支持分布式部署架构，可根据算力资源的分布情况，部署多个采集节点、处理节点和应用节点，实现负载均衡，提升平台的可靠性与扩展性；

集群部署：核心组件（如数据处理、智能分析、应用服务）采用集群部署方式，支持节点故障自动切换，确保平台连续运行，无单点故障；

边缘部署：对于边缘算力节点，支持边缘采集节点的本地化部署，实现边缘算力数据的本地采集与初步处理，减少网络传输压力，提升实时性，契合“中心—区域—国家”三级监测架构。

7.2 硬件要求

服务器：根据平台规模选择合适配置的服务器，CPU 不低于 8 核，内存不低于 16GB，硬盘容量不低于 1TB，支持虚拟化技术；核心节点服务器 CPU 不低于 16 核，内存不低于 32GB，硬盘容量不低于 2TB；

网络设备：支持千兆及以上网络带宽，配备交换机、路由器等网络设备，确保网络连接稳定、高速，支持网络冗余；

采集设备：根据采集需求，配置合适的采集探针、传感器等设备，确保数据采集的准确性与稳定性；

备份设备：配置专用的备份服务器、存储设备，确保数据备份的安全性与可用性。

7.3 软件要求

操作系统：支持 Linux（CentOS、Ubuntu 等）、Windows Server 等主流操作系统，优先选择开源、稳定、安全的 Linux 操作系统；

数据库：支持 InfluxDB、Prometheus、MySQL、PostgreSQL 等主流数据库，确保数据存储与查询的高效性；

中间件：支持 Kafka、RabbitMQ 等消息中间件，用于数据传输与缓冲，提升平台的并发处理能力；

开发语言与框架：支持 Java、Python、Go 等主流开发语言，采用 Spring Boot、Django、Flask 等成

熟框架，确保平台的可维护性与可扩展性；

安全软件：配备防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、杀毒软件等安全软件，保障平台安全。

7.4 部署环境

机房环境：机房温度控制在 18-25℃，湿度控制在 40%-60%，配备 UPS 不间断电源、空调、消防设施等，确保设备正常运行；

网络环境：网络连接稳定，延迟不超过 50ms，丢包率不超过 0.1%，支持网络冗余，避免网络中断；

安全环境：部署在安全可控的网络环境中，隔离外部不安全网络，落实网络安全等级保护要求，至少达到二级及以上防护水平。

8 安全要求

8.1 网络安全

边界防护：部署防火墙、IDS/IPS 等边界安全设备，明确网络边界，限制非法访问，设置安全策略，过滤不安全的网络流量；

网络隔离：将平台网络与外部网络、内部业务网络进行隔离，采用 VLAN 划分、子网隔离等方式，减少安全风险；

加密传输：平台内部数据传输、平台与外部系统的数据传输采用 HTTPS、SSL/TLS 等加密协议，确保数据传输过程中的安全，防止数据被窃取、篡改；

网络监控：实时监测网络流量、网络连接状态，及时发现网络异常行为，如端口扫描、DDoS 攻击等，并进行告警与处置。

8.2 数据安全

数据分类分级：对平台数据进行分类分级管理，明确敏感数据（如用户信息、算力调度数据、能耗数据）的范围，采取针对性的安全保护措施；

数据加密：敏感数据采用加密存储、加密传输，采用 AES-256、RSA 等加密算法，确保数据的机密性；

数据备份与恢复：建立完善的数据备份与恢复机制，定期对数据进行备份，备份数据存储在安全的位置，支持数据的快速恢复，应对数据丢失、损坏等情况；

数据脱敏：对涉及隐私、敏感信息的数据进行脱敏处理，如隐藏用户姓名、身份证号等，确保数据使用的安全性与合规性；

数据访问控制：严格控制数据访问权限，只有授权用户才能访问相应的数据，实现数据的精细化访问控制，防止数据泄露。

8.3 应用安全

身份认证：采用用户名密码、短信验证、人脸识别、Token 认证等多种身份认证方式，确保用户身份的真实性，防止非法登录；

权限控制：基于 RBAC 模型，实现精细化的权限分配，明确各用户的操作权限，防止越权操作；

漏洞防护：定期对平台应用进行漏洞扫描与修复，及时修补安全漏洞，防止被黑客利用；支持漏洞自动化扫描，扫描频率不低于每月 1 次；

操作审计：记录用户的所有操作行为，形成操作日志，支持日志查询、追溯，便于安全事件的排查与处理；

防注入攻击：采取参数过滤、输入验证等措施，防止 SQL 注入、XSS 跨站脚本等注入攻击。

8.4 终端安全

终端准入：对访问平台的终端设备进行准入控制，检查终端设备的安全状态（如是否安装杀毒软件、是否存在漏洞），不符合安全要求的终端禁止访问平台；

终端管理：对接入平台的终端设备进行统一管理，包括终端设备的注册、注销、配置管理等，及时发现并处置终端安全隐患；

终端加密：对终端设备中的敏感数据进行加密存储，防止终端设备丢失、被盗导致数据泄露。

8.5 安全管理

安全制度：建立完善的安全管理制度，包括网络安全、数据安全、应用安全、终端安全等方面的管理制度，明确安全责任；

安全培训：定期对平台运维人员、用户进行安全培训，提升安全意识与安全操作能力；

安全审计：定期对平台的安全状况进行审计，排查安全风险，形成安全审计报告，及时整改安全隐患；

应急处置：建立安全应急处置机制，制定安全应急预案，应对网络攻击、数据泄露、设备故障等安全事件，确保事件发生后能够快速响应、妥善处置，降低损失。

9 运维要求

9.1 运维组织与职责

建立专门的运维团队，明确运维负责人、技术运维人员、安全运维人员等角色的职责，确保运维工作有序开展；

运维团队负责平台的日常运行监测、故障排查、设备维护、软件升级、数据备份与恢复、安全防护等工作；

建立运维工作流程，规范运维操作，确保运维工作的标准化、规范化。

9.2 日常运维

运行监测：实时监测平台各组件、各节点的运行状态，包括服务器、网络设备、数据库、应用服务等，及时发现运行异常；

故障排查：建立故障排查机制，接到故障告警后，及时排查故障原因，采取针对性的处置措施，确保故障快速解决，核心故障响应时间不超过 30 分钟，一般故障响应时间不超过 1 小时；

设备维护：定期对服务器、网络设备、采集设备等硬件设备进行维护，包括清洁、检查、更换等，确保设备正常运行；

软件升级：定期对平台的操作系统、数据库、中间件、应用软件等进行升级，修复安全漏洞，提升平台性能与功能，升级前需进行测试，确保升级不影响平台正常运行；

数据备份与恢复：按照数据存储要求，定期进行数据备份，定期测试数据恢复功能，确保备份数据的可用性。

9.3 运维监控

建立运维监控体系，实时监测平台的运行状态、资源使用情况、告警信息等，实现运维工作的可视化、智能化；

设置运维告警机制，对平台运行异常、设备故障、安全事件等进行告警，确保运维人员及时知晓并处置；

定期生成运维报告，包括平台运行状态、故障处置情况、资源使用情况、安全状况等，为运维决策提供依据。

9.4 运维考核

建立运维考核机制，明确考核指标，包括故障处置效率、平台可用性、数据安全性、运维响应时间等；

定期对运维团队及运维人员进行考核，考核结果与绩效挂钩，激励运维人员提升运维工作质量与效

率；

持续优化运维流程与运维策略，根据考核结果、平台运行情况，不断提升运维水平。

10 验收要求

10.1 验收前提

平台已完成部署、调试，所有功能模块正常运行；

平台已完成数据采集、处理、分析等功能的测试，测试结果符合本标准要求；

运维团队已组建，运维管理制度已建立，运维人员已完成培训；

提供完整的验收资料，包括平台设计方案、部署文档、测试报告、运维手册、安全评估报告等。

10.2 验收内容

10.2.1 架构验收

检查平台的总体架构是否符合本标准第 4 章的要求，分层架构、分布式部署、模块化设计是否落实，配套体系是否完善，是否支持与上级监测平台互联互通。

10.2.2 功能验收

采集接入功能：检查采集范围、采集方式、接入兼容性是否符合本标准第 5.1 节的要求，数据采集的实时性、准确性是否达标；

数据处理功能：检查数据清洗、转换、存储、管理等功能是否符合本标准第 5.2 节的要求，数据质量是否达标；

智能分析功能：检查算力负载分析、异常检测与告警、能耗优化分析、调度辅助分析等功能是否符合本标准第 5.3 节的要求，分析结果的准确性、可靠性是否达标；

应用层功能：检查可视化展示、报表统计、权限管理、接口开放等功能是否符合本标准第 5.4 节的要求，操作便捷性、兼容性是否达标。

10.2.3 部署验收

检查平台的部署架构、硬件配置、软件配置、部署环境是否符合本标准第 6 章的要求，平台运行是否稳定，无单点故障。

10.2.4 安全验收

检查平台的网络安全、数据安全、应用安全、终端安全、安全管理是否符合本标准第 7 章的要求，

安全防护措施是否落实，安全风险是否可控，是否达到规定的网络安全等级保护水平。

10.2.5 运维验收

检查运维组织、运维职责、日常运维、运维监控、运维考核是否符合本标准第 8 章的要求，运维工作是否有序开展，运维能力是否满足平台运行需求。

10.3 验收标准

所有验收内容均符合本标准的要求，无重大缺陷；

平台运行稳定，连续运行 72 小时无故障，核心功能可用率不低于 99.9%；

数据采集准确率不低于 98%，实时数据写入延迟不超过 100ms，查询延迟不超过 500ms；

异常检测准确率不低于 95%，告警响应时间不超过 5 分钟；

安全防护措施到位，无安全漏洞与安全风险，通过安全评估；

验收资料完整、规范，符合要求。

10.4 验收流程

建设单位提交验收申请及完整的验收资料；

验收小组（由发起单位、参与单位、第三方专家组成）对验收资料进行审核；

验收小组对平台进行现场测试、核查，检查平台的功能、部署、安全、运维等情况；

验收小组根据测试、核查结果，形成验收报告，明确验收结论（合格、不合格、整改后重新验收）；

对于验收不合格的，建设单位需在规定期限内完成整改，整改完成后重新提交验收申请；

验收合格后，验收小组签署验收报告，平台正式投入使用。

11 前瞻性技术布局

为适应算力产业的快速发展，平台建设应兼顾前瞻性，预留技术扩展接口，布局以下前沿技术，确保平台的可持续发展与竞争力，支撑全国一体化算力网建设的长远需求。

11.1 量子算力监测技术

预留量子算力资源的接入与监测接口，研究量子算力的监测指标、采集方式与分析方法，适应量子算力发展趋势，实现对量子算力资源的有效监测与管理，为量子算力与传统算力的协同调度提供支撑。

11.2 AI 大模型融合应用

融入 AI 大模型技术，提升平台的智能分析与决策能力，实现算力态势的深度分析、异常事件的精准预测、调度策略的智能优化，打造“AI+算力监控”的智能化模式，提升平台的运维效率与决策水平。

11.3 边缘智能监测技术

深化边缘计算与算力监控的融合，部署边缘智能监测节点，实现边缘算力数据的本地实时分析、异常告警与自主决策，减少对中心平台的依赖，提升边缘算力监控的实时性与可靠性，适配边缘计算快速发展的需求。

11.4 算力区块链技术应用

探索区块链技术在算力监控中的应用，实现算力数据的不可篡改、可追溯，提升数据可信度，支撑算力交易、算力计量的公平公正，构建可信的算力监控体系，助力算力要素市场化配置。

11.5 跨域协同监测技术

研究跨区域、跨行业、跨平台的算力协同监测技术，实现不同区域、不同类型算力监控平台的数据互通、资源共享与协同调度，支撑全国算力“一本账”、监测“一张网”的建设目标，提升全国算力资源的整体利用效率。