

ICS 35.240.50
UNSPSC 43.23.15
CCS L 77



团 体 标 准

T/XXX XXXX—2024

工业互联网平台 IOT 管理系统技术规范

Technical specification for IOT management system of industrial Internet platform

(征求意见稿)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国联合国采购促进会 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 系统框架	1
5 功能要求	1
5.1 系统设置	1
5.2 IOT 设备管理	2
5.3 数据管理	3
5.4 智能分析与预测	4
5.5 可视化呈现	5
6 性能要求	5
6.1 数据处理性能	5
6.2 响应性能	5
6.3 可靠性和稳定性	6
6.4 可扩展性和兼容性	6
7 接口要求	6
7.1 设备接入接口	6
7.2 平台间接口	6
7.3 用户接口	7
8 安全要求	7
8.1 数据安全	7
8.2 网络安全	7
8.3 系统安全	7
9 运维管理	8
9.1 系统监控	8
9.2 故障处理	8
9.3 系统升级	8
10 评价改进	8

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。

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××××提出。

本文件由中国联合国采购促进会归口。

本文件起草单位：

本文件主要起草人：

引 言

为助力中国企业参与国际贸易,推动企业高质量发展,中国联合国采购促进会依托联合国采购体系,制定服务于国际贸易的系列标准,这些标准在国际贸易过程中发挥了越来越重要的作用,对促进贸易效率提升,减少交易成本和不确定性,确保产品质量与安全,增强消费者信心具有重要的意义。

联合国标准产品与服务分类代码(UNSPSC, United Nations Standard Products and Services Code)是联合国制定的标准,用于高效、准确地对产品和服务进行分类。在全球国际化采购中发挥着至关重要的作用,它为采购商和供应商提供了一个共同的语言和平台,促进了全球贸易的高效、有序发展。

围绕UNSPSC进行相关产品、技术和服务团体标准的制定,对助力企业融入国际采购,提升国际竞争力具有十分重要的作用和意义。

本文件采用UNSPSC分类代码由6位组成,对应原分类中的大类、中类和小类并用小数点分割。

本文件UNSPSC代码为“43.23.15”,由3段组成。其中:第1段“43”为大类,表示“信息技术广播和电信”,第2段为中类,“23”表示“软件”,第3段为小类,“15”表示“特定于业务功能的软件”。

工业互联网平台 IOT 管理系统技术规范

1 范围

本文件规定了工业互联网平台IOT管理系统技术规范（以下简称“系统”）的系统框架、功能要求、性能要求、接口要求、安全要求、运维管理以及评价改进。

本文件适用于系统的开发、运行和维护。

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 20270 信息安全技术 网络基础安全技术要求

GB/T 20988 信息安全技术 信息系统灾难恢复规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业设备 industrial equipment

工业企业所使用的设备、为生产设备和非生产设备两大类，生产设备指直接用于生产产品的设备，即将原材料到成品前整个全过程中所使用的设备；非生产设备指直接不直接用于产品生产的设备，即基本建设、科学试验和管理上所使用的设备。

4 系统框架

系统的总体架构见图1。

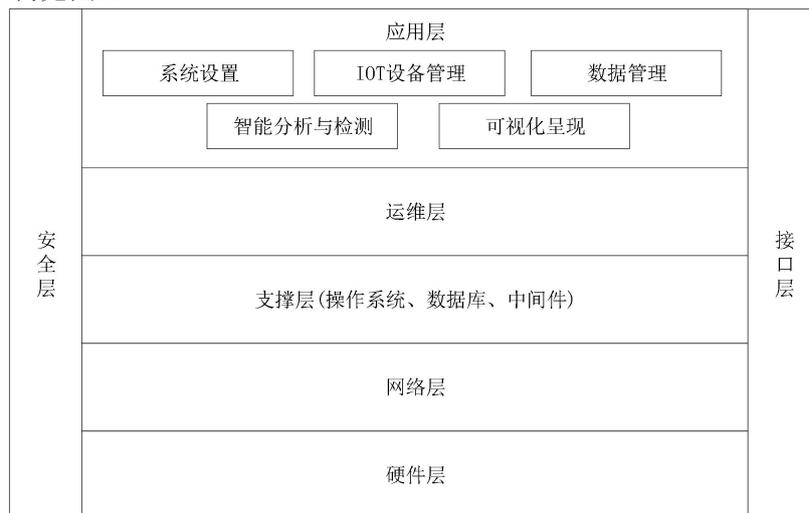


图 1 系统架构图

5 功能要求

5.1 系统设置

系统的设置符合以下要求：

- a) 应支持用户信息的查看、新增、修改和删除操作。用户信息包括但不限于用户名、姓名、联系方式等基本信息；
- b) 应具备权限管理体系，为用户分配不同的角色，一个用户可对应多个角色并实现复杂的权限组合；
- c) 应自动生成操作日志，记录系统内所有操作的相关信息，包括操作时间精确到秒、操作人员的准确标识、操作内容的详细描述；
- d) 应提供灵活的系统参数配置功能，可设置系统通知和警报的触发条件、通知方式（如邮件、短信、系统弹窗等）及系统管理员和相关人员能及时获取重要信息，信息内容包括但不限于：
 - 1) 设备故障警报、设备离线预警、设备维护提醒；
 - 2) 服务器资源过载警告、网络延迟异常通知；
 - 3) 系统资源异常通知等。

5.2 IOT 设备管理

5.2.1 接入与认证

系统的设备注册符合以下要求：

- a) 应支持记录设备的基本信息，信息内容包括但不限于：
 - 1) 设备编号：具有唯一性，精准识别和管理每台设备；
 - 2) 设备名称：应按设备的主要特征或用途命名；
 - 3) 设备类型：按设备的功能、所属领域或技术规格等进行分类；
 - 4) 设备位置：明确设备所处的地理位置或在工厂内部的具体安装位置，精确到车间、生产线等具体区域等信息。
- b) 应支持记录设备的生产日期、生产厂家、设备型号、设备规格等相关信息，为设备的全生命周期管理提供全面的数据基础。

5.2.2 远程监控与控制

5.2.2.1 应具备实时监控能力，能持续获取设备的各种状态信息，信息内容包括但不限于：

- a) 设备的运行状态，包括正常运行、停机、待机、故障停机等；
- b) 故障状态，包括及时准确地反馈故障类型、故障代码、故障发生时间等详细信息；
- c) 能耗数据，包括实时功率、累计能耗、能耗曲线等；
- d) 关键运行参数，包括如温度、压力、转速、流量等，根据设备类型和实际需求而定。

5.2.2.2 应支持多样化的筛选条件，能根据设备类型、设备位置、设备状态、运行时间、能耗范围等多个维度进行灵活筛选，快速定位目标设备。

5.2.2.3 系统对设备的远程控制符合以下要求：

- a) 应支持通过平台对设备进行精确操作，如远程启动、停止、暂停、重启设备；
- b) 应支持设备的运行参数调整，包括调整生产设备的加工速度、温度设定值、压力设定值等；
- c) 应支持远程校准、复位等操作，提高设备管理的便捷性和灵活性；
- d) 应实施操作权限管理机制，规定经过授权且具备相应权限级别的用户才能对设备进行特定操作，防止未经授权的非授权操作对设备造成损坏或影响生产安全；
- e) 应支持追溯操作过程，便于后续查询和分析。

5.2.3 生命周期管理

系统的生命周期管理符合以下要求：

- a) 采购环节应根据企业生产需求及设备性能标准，对市场上的设备进行综合评估与筛选；
- b) 安装环节应为安装人员提供详细的设备安装指导手册和视频教程，涵盖设备安装步骤、技术要点、安全注意事项等关键信息；
- c) 调试环节应用专业的测试工具和软件，对设备的各项功能进行全面检测与校准；
- d) 运行环节应利用测技术关注设备的运行状态。通过对设备关键性能指标（如温度、压力、转速、能耗等）的持续采集与分析，及时发现设备运行中的异常情况；

- e) 维护环节应支持依据设备类型、使用频率、运行环境制定维护计划，设定如日、周、月、季、年等个性化维护周期，调整清洁、润滑等维护内容，安排并明确维护人员或团队，完整记录维护时间、执行内容、人员签名、问题及处理措施，且提前以弹窗、短信、邮件等方式向相关人员发送维护提醒。

5.3 数据管理

5.3.1 数据采集

系统的数据采集符合以下要求：

- a) 应具备多来源采集数据能力，保证数据来源的多样性和全面性，能满足不同业务场景和分析需求。来源包括但不限于：
 - 1) 各类工业设备，如传感器、仪器仪表、生产设备、智能终端等；
 - 2) 业务系统，如企业资源规划（ERP, Enterprise Resource Planning）、制造执行系统（MES, Manufacturing Execution System）、产品生命周期管理（PLM, Product Lifecycle Management）等；
 - 3) 外部数据源，如合作伙伴数据、行业数据库等。
- b) 应支持常见数据格式，格式包括但不限于：
 - 1) 结构化数据，逗号分隔值（CSV, Comma-Separated Values）、扩展标记语言（XML, Extensible Markup Language）、JavaScript 对象表示法（JSON, JavaScript Object Notation）；
 - 2) 半结构化数据，日志文件、XML 文档；
 - 3) 非结构化数据，图片、音频、视频等。
- c) 应兼容各类工业通信协议，包括 OPC 统一架构（OPC UA, OPC Unified Architecture）、Modbus、轻量级的消息传输协议（MQTT, Message Queuing Telemetry Transport）、超文本传输协议（HTTP, Hypertext Transfer Protocol）等；
- d) 应具备数据校验机制，对采集到的数据进行合理性检查和验证。如对于温度数据，出现超出正常工作温度范围（根据设备历史运行数据和设备手册确定合理范围）的数据点时，应自动识别并标记为可疑数据，同时启动数据复查或补充采集流程；
- e) 应建立完善的数据质量保障体系，在数据采集过程中对数据进行实时校验和清洗，校验和清洗内容包括但不限于：
 - 1) 数据完整性检查，保证关键数据完整；
 - 2) 数据准确性验证，通过算法比对、逻辑判断等方式剔除错误数据；
 - 3) 数据一致性处理，保证不同数据源同一数据的一致性；
 - 4) 异常数据识别与处理，如对超出合理范围的数据进行标记或修正。

5.3.2 数据传输

应具备对传输链路的实时监测和故障诊断能力，发现传输过程中的丢包、误码、链路中断等异常情况，自动采取切换传输链路、调整传输参数等恢复措施。

5.3.3 数据存储

系统的数据存储符合以下要求：

- a) 应支持根据数据的类型、规模、访问频率等特点，采用匹配的的数据存储方式，如关系型数据库、非关系型数据库以及分布式文件系统，实现数据的分类存储和优化管理，保证数据的长期保存和高效检索；
- b) 应制定合理的数据存储策略，包括但不限于：
 - 1) 数据分区，如按时间、地域、设备类型等维度进行分区存储，提高数据查询效率；
 - 2) 数据备份，定期对数据进行全量和增量备份，备份策略可根据数据重要性和业务需求设定，如每天全量备份关键数据，每小时增量备份实时数据，并将备份数据存储在地以外防止本地灾难导致数据丢失；
 - 3) 数据归档，对历史数据进行归档处理，降低存储成本，同时保证在需要时能快速恢复和查询；

- 4) 数据生命周期管理，根据数据的价值随时间的变化规律，自动对数据进行迁移、删除等操作。
- c) 应采用冗余存储技术，如独立磁盘冗余阵列（RAID, Redundant Array of Independent Disks）、数据备份与恢复机制等；
- d) 数据的恢复时间目标（RTO, Recovery Time Objective）不应超过 2 h，恢复点目标（RPO, Recovery Point Objective）应为最近一次成功备份的时间点；
- e) 应具备数据一致性保障机制，数据一致性的验证成功率不应低于 99.99%，在数据写入、更新和读取过程中不同副本之间的数据应具有有一致性。

5.3.4 数据分析

系统的数据分析符合以下要求：

- a) 应集成多种先进的数据分析算法和工具，为用户提供全面的数据分析能力，支持从简单的数据统计到复杂的预测性分析等多种分析任务。工具包括但不限于：
 - 1) 数据挖掘算法，如分类算法、聚类算法、关联规则挖掘等用于发现数据中的潜在模式和规律；
 - 2) 机器学习算法，如回归分析、神经网络、深度学习等用于预测设备故障、优化生产过程等；
 - 3) 统计分析方法，如均值、方差、相关性分析等用于数据描述和基本统计推断；
 - 4) 数据可视化工具，如 Echarts、Tableau 等用于直观展示分析结果。
- b) 应支持实时数据分析，能对实时采集的数据进行即时处理和分析，及时反馈设备运行状态、生产过程中的异常情况关键信息，为实时决策提供支持；
- c) 应具备离线分析能力，能对历史数据进行深度挖掘和批量处理，用于长期趋势分析、业务流程优化、战略决策制定等场景，满足企业不同层次和时间尺度的分析需求；
- d) 应具备数据分析结果可解释性，能通过可视化展示、通俗易懂的报告生成等方式，帮助用户理解分析结果背后的业务含义和潜在影响。

5.4 智能分析与预测

5.4.1 故障预测与诊断

系统的故障预测与诊断符合以下要求：

- a) 应通过实时监测设备的关键运行参数，如温度、压力、振动频率等，结合设备的历史运行数据和故障案例库，构建故障预测模型；
- b) 各运行数据出现异常波动或趋近于历史故障数据模式时，系统应提前发出精准的故障预警，并提供详细的故障诊断信息，包括可能的故障原因、故障部位以及推荐的维修措施。

5.4.2 设备性能分析

系统的设备性能分析符合以下要求：

- a) 应对设备的各项性能指标进行实时监测和长期跟踪，如生产效率、产品质量参数、能耗数据等；
- b) 应采用优化算法对设备的工艺参数进行优化调整，例如响应曲面法、遗传算法等，提高设备的生产效率和产品质量，同时降低能耗；
- c) 应支持对设备的能耗数据进行详细分析，识别能耗异常的时间段和操作环节；
- d) 应开展预测性维护工作，根据设备的磨损程度、关键部件的剩余寿命等信息，安排设备维护计划。

5.4.3 生产优化分析

系统的生产优化分析符合以下要求：

- a) 应整合来自设备、生产计划、供应链等多方面的数据，运用生产调度模型、流程模拟技术等手段，对生产计划进行优化调整；

- b) 应对生产过程中的质量数据进行分析，识别质量问题的根源，并提出改进措施，提升产品的整体质量。

5.5 可视化呈现

5.5.1 设备可视化

系统的设备可视化符合以下要求：

- a) 应通过 3D 建模、拓扑图等技术手段，呈现设备的物理结构和运行状态；
- b) 可视化界面应支持用户对设备进行远程操作，如启动、停止、调整参数等，操作过程中应有相应的动画效果和提示信息。

5.5.2 数据可视化

系统的数据可视化符合以下要求：

- a) 应提供丰富多样的可视化组件，包括但不限于：
 - 1) 各类图表，如柱状图、折线图、饼图、散点图、雷达图等用于展示不同类型的数据分布和趋势；
 - 2) 仪表盘，将关键指标以直观的表盘形式展示，实时反映设备状态、生产进度、质量指标等重要信息；
 - 3) 地图，用于展示设备地理位置分布、物流路径等基于地理信息的数据；
 - 4) 数据大屏，可定制化的大屏幕展示，适用于监控中心、指挥调度等场景，集中展示多个关键数据和分析结果。
- b) 应支持用户根据自身需求灵活配置可视化内容和样式，如选择不同的图表类型、自定义坐标轴标签、设置颜色主题、调整图表布局等，实现个性化的数据展示；
- c) 应具备交互功能，能通过鼠标点击、缩放、过滤、钻取等操作探索数据细节，如在图表上点击某个数据点查看其详细信息、对数据进行时间范围筛选、从总体数据钻取到具体设备或业务环节的数据等，提高数据可视化的实用性和用户体验。

6 性能要求

6.1 数据处理性能

6.1.1 系统的采集性能符合以下要求：

- a) 应支持根据设备类型、数据重要性及业务需求，灵活配置数据采集频率。如高精密制造设备的加工精度参数、化工生产中的关键反应温度和压力等，采集频率应不低于每秒 1 次；
- b) 应具备自动提高采集频率的能力，针对具有突发数据特征的设备，如故障检测设备在异常发生时，能从常规频率瞬间提升至最高每秒 10 次，并记录故障发生前后的关键数据；
- c) 应根据预设规则在故障稳定后恢复至原采集频率；
- a) 应符合设备本身的技术精度指标要求。对于高精度测量设备，如电子秤、激光测距仪等，数据采集的误差范围为在设备标称精度的 $\pm 0.5\%$ ；
- b) 可疑数据的误判率应低于 5%。

6.1.2 系统的传输性能符合以下要求：

- a) 设备端到工业互联网平台的数据平均传输延迟不应超过 500 ms；
- b) 对于实时性要求极高的控制指令类数据传输，如自动化生产线上的设备紧急制动指令、高精度加工设备的实时参数调整指令等，延迟应在 100 ms 内；
- c) 通过广域网（如互联网）进行数据传输时，应根据网络带宽和质量的实际情况，数据传输延迟的平均值不应超过 2 s；
- d) 成功率不应低于 99.99%；
- e) 故障恢复时间不应超过 10 s。

6.2 响应性能

系统的响应性能符合以下要求：

- a) 执行常规操作（如登录、查询数据、发送控制指令等）时，平均响应时间应不超过 2 s；
- b) 执行复杂的业务操作（如涉及大数据量的统计分析、多设备协同控制等），响应时间应不超过 10 s；
- c) 在系统执行自动化任务或对设备状态变化做出响应时，应在 1 s 内给出反馈信息；
- d) 应支持实时数据推送功能，将设备的关键数据变化实时推送给用户，推送延迟不超过 500 ms；
- e) 对于实时数据处理任务，系统应在数据到达后的 1 s 内完成初步的分析和处理；
- f) 对于复杂的数据分析算法，如基于机器学习模型的设备故障预测、生产流程优化分析等，处理时间不应超过 10 min；
- g) 应具备高效的数据索引和检索能力，在 3 s 内响应常见的数据查询请求，如根据设备编号、时间范围、数据类型等条件进行数据检索；
- h) 应具备并行处理能力，同时处理多个数据处理任务，随着硬件资源的增加，如核心数增加、内存扩展等，数据处理性能应呈线性提升。

6.3 可靠性和稳定性

系统的可靠性和稳定性符合以下要求：

- a) 应具备高可靠性，平均无故障时间（MTBF, Mean Time Between Failures）应不低于 5000 h；
- b) 对于关键业务模块，MTBF 不应低于 8000 h；
- c) 应具备快速的故障恢复机制，在出现硬件故障、软件错误、网络中断等异常情况时，能在 5 min 内自动切换到备用系统或采取相应的恢复措施；
- d) 高负荷运行条件下，应保持稳定的性能表现，各项性能指标（如响应时间、吞吐量、数据准确性等）的波动范围应控制 $\pm 10\%$ ；
- e) 应能连续稳定运行至少 72 h 且无异常错误和故障发生。

6.4 可扩展性和兼容性

系统的可扩展性和兼容性符合以下要求：

- a) 应采用模块化、分布式设计，能在不影响现有系统正常运行的情况下扩展系统功能和规模；
- b) 应支持通过添加服务器节点、扩展存储容量、增加网络带宽等方式，线性提升系统的处理能力和存储容量；
- c) 应能兼容市场上主流的工业设备，包括但不限于：
 - 1) 各类传感器，如温度传感器、压力传感器、位移传感器等；
 - 2) 执行器，如电机、阀门、继电器等；
 - 3) PLC（可编程逻辑控制器）、DCS（集散控制系统）、智能仪表等；
 - 4) 通信接口，如 RS-232、RS-485、以太网、Wi-Fi、蓝牙等；
 - 5) 通信协议，如 Modbus、OPC UA、MQTT、CoAP。
- d) 应兼容其他企业级软件，如 ERP 系统、MES、PLM 系统等。

7 接口要求

7.1 设备接入接口

系统的设备接入接口符合以下要求：

- a) 应具备多种的通信协议接口，支持各类工业设备的接入，如工业通信协议 Modbus RTU/TCP、OPC UA、MQTT、CoAP 和智能仪表等设备；
- b) 对于特定行业或企业自定义的通信协议，应提供可扩展的接口开发框架，根据实际需求进行协议适配和定制开发；
- c) 应在设备接入过程中自动进行数据格式的转换和统一；
- d) 应具备连接稳定性和可靠性机制。采用心跳检测、自动重连等技术手段，设备意外掉线、网络波动等情况下，能迅速恢复连接。

7.2 平台间接口

系统的平台间接入接口符合以下要求：

- a) 应提供标准化的数据交互接口，支持超文本传输协议（HTTP, Hypertext Transfer Protocol）和超文本传输安全协议（HTTPS, Hypertext Transfer Protocol Secure）协议；
- b) 应实现数据的双向交互，从本平台向其他平台推送设备实时数据、状态信息、分析结果等，接收来自其他平台的指令、配置信息等，实现跨平台的业务协同和信息共享；
- c) 应具备高度的安全性保障措施。采用身份认证、授权访问、数据加密等技术，防止数据在传输过程中被窃取、篡改或非法访问；
- d) 应具备良好的兼容性和可扩展性。适应不同平台的版本升级和功能扩展，在接口设计上遵循松耦合的原则，降低接口与具体平台实现的依赖关系；
- e) 应采用版本控制机制，接口的升级不应影响已有的对接平台的正常使用。

7.3 用户接口

系统的用户接口符合以下要求：

- a) 应支持可视化展示功能接口，将复杂的数据以直观的图表（如柱状图、折线图、饼图、地图等）、图形（如设备布局图、工艺流程模拟图等）、仪表盘等形式呈现给用户；
- b) 应支持用户根据自己的需求自定义可视化展示的内容、布局和样式，选择性展示数据指标、设置图表的颜色和坐标轴范围等；
- c) 应支持并发用户访问，根据系统的设计规模和预期用户量，在高并发情况下（同时有 100 个以上用户进行操作），系统的性能不应出现明显下降。

8 安全要求

8.1 数据安全

系统的数据安全符合GB/T 20270和GB/T 20988的相关规定，并符合以下要求：

- a) 应采用安全的加密算法，如高级加密标准（AES, Advanced Encryption Standard），对数据进行加密，防止数据被窃取或篡改；
- b) 存储在平台数据库中的数据应进行加密存储，减少数据泄露风险；
- c) 应建立完善的数据备份策略和机制，定期对平台数据进行备份，并将备份数据存储安全可靠的位置，与原数据存储位置相互隔离；
- d) 备份数据应具有完整性和可恢复性，定期进行恢复演练，验证备份数据的有效性，保证在数据灾难发生时能快速恢复数据。

8.2 网络安全

系统的网络安全符合以下要求：

- a) 应实施网络访问控制策略，通过防火墙、虚拟局域网（VLAN, Virtual Local Area Network）划分、访问控制列表（ACL, Access Control List）等技术手段，限制对平台的网络访问，仅授权的设备、用户和网络流量进入平台内部；
- b) 应部署入侵检测系统（IDS, Intrusion Detection System）和入侵防御系统（IPS, Intrusion Prevention System）系统，实时监测网络流量，及发现并阻止各类网络攻击行为，如分布式拒绝服务攻击（DDoS, Distributed Denial of Service）、端口扫描、恶意软件入侵等；
- c) 应定期更新 IDS/IPS 的特征库，适应不断变化的网络攻击手段和技术；
- d) 应建立定期的网络安全漏洞扫描和修复机制，使用专业的漏洞扫描工具对平台网络进行全面检测，及时发现操作系统、网络设备、应用程序等存在的安全漏洞。

8.3 系统安全

系统的系统安全符合以下要求：

- a) 应采用多因素认证（如密码、短信验证码、数字证书、指纹识别等）方式，保证用户和设备的身份真实性和合法性；

- b) 应建立安全审计系统，对平台上的所有用户操作、设备行为、系统事件等进行审计记录，包括操作时间、操作人、操作内容、操作结果等详细信息；
- c) 应支持跟踪和获取操作系统、数据库、应用程序等系统组件的安全更新和补丁信息，进行更新和部署。

9 运维管理

9.1 系统监控

系统的监控符合以下要求：

- a) 应对关键性能指标进行实时监测，包括但不限于中央处理器（CPU, Central Processing Unit）使用率、内存占用率、磁盘（I/O, Input/Output Rate）速率、网络带宽利用率、数据处理延迟、设备连接数等；
- b) 应设置性能阈值，当性能指标超出阈值时，及时发出警报通知运维人员；
- c) 应进行长期存储和分析，识别系统性能的变化趋势和潜在问题，存储时间不应少于 1 年；
- d) 应实时监控接入平台的各类设备的运行状态，包括设备的在线离线情况、故障信息、电量状态（对于移动或电池供电设备）、工作温度等关键参数；
- e) 应建立安全事件监测机制，对系统的网络攻击、数据泄露、非法访问等安全事件进行实时监控和预警。

9.2 故障处理

系统的故障处理符合以下要求：

- a) 应制定应急响应预案，系统遭受严重故障、安全事件或自然灾害等紧急情况下的应急响应流程和措施应具备快速准确的故障诊断能力；
- b) 通过对系统日志、性能数据、设备状态信息等多源数据的综合分析，定位故障发生的根本原因；
- c) 应建立故障知识库，对常见故障类型和解决方法进行记录和整理；
- d) 应根据故障诊断结果，制定相应的故障修复方案，及时采取措施进行修复；
- e) 应记录故障修复步骤和操作记录，包括修复时间、修复人员、使用的工具和方法等信息，用于后续的审计和问题追溯。

9.3 系统升级

系统的系统升级符合以下要求：

- a) 应支持根据系统的发展需求、技术演进趋势以及用户反馈，制定系统升级规划，升级规划内容包括但不限于升级的目标、内容、时间安排、风险评估等；
- b) 在系统升级过程中，应采用灰度发布、版本回滚等技术手段，减少升级过程对业务的影响；
- c) 应对升级后系统进行验证与优化，通过功能测试、性能测试、兼容性测试等手段，使系统满足升级后的预期目标和业务需求。

10 评价改进

依据第5章~9章规定的要求，定期开展系统的功能、性能、接口、安全和运维管理方面的评价，审查不合格项，并有针对性地采取纠偏措施并持续改进。