ICS 35.240.50
CCS N10

团　　体　　标　　准

T/ZIUR XXXX—2026

机电装备智能协同控制技术规范

Technical Specification for Intelligent Collaborative Control of Electromechanical Equipment

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

浙江省产学研合作促进会　　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》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XXX提出。

本文件由浙江省产学研合作促进会归口。

本文件起草单位：XXX。

本文件主要起草人：XXX。

机电装备智能协同控制技术规范

1 范围

本文件规定了机电装备智能协同控制技术的术语和定义、总体架构、运行环境要求、数据互联互通、智能协同控制、智能优化、系统集成与测试、运维与安全保障。

本文件适用于工业领域各类机电装备智能协同控制系统的设计、集成、测试、运维和管理。

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 15969.3 可编程序控制器 第3部分：编程语言

GB/T 16656.1 工业自动化系统与集成 产品数据表达与交换 第1部分：概述与基本原理

GB/T 16656.52 工业自动化系统与集成 产品数据表达与交换 第52部分：集成通用资源：基于网格的拓扑结构

GB/T 17626（所有部分） 电磁兼容 试验和测量技术

GB/T 20988 网络安全技术 信息系统灾难恢复规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 30094 工业以太网交换机技术规范

GB/T 42127 智能制造 工业数据 采集规范

GB/T 43780 制造装备智能化通用技术要求

GB/T 45283.4 工业控制系统人机接口组态文件交互 第4部分：测试要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

机电装备 electromechanical equipment

由机械结构、电气控制、执行机构及辅助部件组成，能够实现特定工业生产、加工、搬运或控制功能的装备。

3.2

协同感知 collaborative perception

多台机电装备通过多传感器融合技术，共同采集自身运行状态、工作环境信息和任务需求信息，实现信息共享、时间同步和多源数据融合的过程。

3.3

协同调度 collaborative scheduling

基于决策规划结果，对多台机电装备的任务执行顺序、资源分配进行动态调整和优化，确保任务高效、有序完成的过程。

3.4

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239，3.1]

3.5

冲突消解 conflict resolution

实时检测机电装备间的空间、时间、资源和任务冲突，通过优先级调度、路径重规划等策略，及时解决冲突、避免安全事故的过程。

3.6

预测性维护 predictive maintenance

基于机电装备运行数据采集和分析，通过智能模型实现故障早期预警、故障类型识别和故障发生时间预测，提前制定维护计划的维护方式。

4 总体架构

4.1 系统组成

4.1.1 机电装备智能协同控制系统应包含感知层、控制层、协同层和接口层，各层应协同工作。

4.1.2 感知层应包含传感器、执行器等设备，负责采集机电装备运行状态、环境参数等各类数据，其性能指标应符合 GB/T 42127 的规定。

4.1.3 控制层应具备独立控制单台机电装备的能力，可接收协同层指令并执行，同时反馈装备运行状态，宜采用可编程控制器实现，符合 GB/T 15969.3 的规定。

4.1.4 协同层应作为系统核心，负责多装备协同决策、任务调度和冲突消解，宜采用分布式处理架构。

4.1.5 接口层应提供标准化的数据交互接口，支持与感知层、控制层及外部系统的数据通信。

4.1.6 系统各层之间的数据流应清晰可追溯，数据传输应具备完整性和安全性，可根据实际应用场景增设边缘计算节点。

4.2 拓扑结构

4.2.1 系统拓扑结构应根据机电装备的部署规模、分布范围和协同需求进行设计，宜采用分布式拓扑结构，兼顾灵活性和可扩展性，参考 GB/T 16656.52 的相关规定。

4.2.2 系统拓扑结构应支持星型、环形、总线型等子拓扑的混合部署，符合表 1 的要求。

表 1 系统拓扑结构

拓扑结构类型	适用场景	核心要求
星型拓扑	装备集中部署、数量较少（≤10台）的场景	中央节点无单点故障，通信延迟≤50ms
环形拓扑	装备线性部署、对可靠性要求高的场景	链路故障恢复时间≤100ms，支持冗余备份
总线型拓扑	装备分散部署、数据传输量适中的场景	总线负载率≤70%，抗干扰能力符合工业级要求
混合拓扑	装备规模大、分布复杂的场景	各子拓扑衔接顺畅，数据交互无冲突

4.2.3 关键控制节点宜采用环形拓扑，保障故障冗余能力，符合 GB/T 30094 中环网冗余要求。

4.2.4 拓扑结构设计应考虑未来装备扩容需求，预留不少于 20%的节点接口，接口类型应标准化。

5 运行环境要求

5.1 物理环境

5.1.1 温湿度要求

5.1.1.1 系统核心设备的运行环境温度应控制在 10℃～35℃，昼夜温差不宜超过 15℃。

5.1.1.2 运行环境相对湿度应控制在 40%～80%（非冷凝），当环境湿度超过 80%时，应采取除湿措施，防止设备内部结露损坏电子元件。

5.1.1.3 极端环境下，核心设备应采用工业级防护设计，温度适应范围可扩展至-30℃～65℃，湿度适应范围可扩展至 5%～95%（非冷凝）。

5.1.2 振动与粉尘要求

5.1.2.1 运行环境的振动加速度应≤0.5g（10～1000Hz），当振动超过限值时，应采取减震措施，保护设备硬件不受损伤。
5.1.2.2 环境粉尘浓度应≤0.1mg/m³，粉尘应无腐蚀性、无导电性，设备安装区域应定期清洁，避免粉尘堆积影响设备散热和正常运行。
5.1.2.3 腐蚀性环境中，设备应采用防腐外壳和密封设计，防止腐蚀性气体和粉尘侵入设备内部。

5.1.3 电磁环境要求

5.1.3.1 设备应具备良好的电磁兼容性，抗电磁干扰能力应满足工业级要求，避免因外部电磁干扰导致数据传输错误或设备误动作。
5.1.3.2 系统布线应区分强电和弱电线路，弱电线路应采用屏蔽线缆，布线间距不宜小于 30cm，减少电磁干扰对数据传输的影响。

5.2 网络环境

5.2.1 网络性能要求

5.2.1.1 系统网络应采用工业以太网，核心链路带宽应≥1000Mbps，终端设备接入带宽应≥100Mbps，满足多装备协同控制的数据传输需求。
5.2.1.2 网络传输延迟应≤50ms，丢包率应≤0.1%，抖动应≤10ms，确保协同控制指令和数据的实时传输，支持 IEEE 802.1AS 时钟同步协议。
5.2.1.3 网络应具备流量控制功能，优先保障协同控制指令的传输。

5.2.2 网络冗余要求

5.2.2.1 核心网络设备应采用双机热备模式，当主设备发生故障时，备用设备应在 50ms 内切换，保障网络连续运行。
5.2.2.2 关键链路应采用双链路备份设计，链路故障时应能自动切换至备用链路，切换时间≤100ms，确保数据传输不中断。
5.2.2.3 网络应具备故障自诊断功能，能够实时监测网络运行状态，当出现链路中断、设备故障等问题时，应及时发出告警信号。

5.2.3 网络布线要求

5.2.3.1 网络布线应采用工业级屏蔽线缆，线缆敷设应整齐规范，避免与强电线路并行敷设，减少干扰，布线距离应符合线缆传输特性要求。
5.2.3.2 室外布线应采用防水、防晒、抗老化的线缆，接头处应做好密封处理，防止雨水和灰尘侵入。
5.2.3.3 线缆标识应清晰明确，标注线缆用途、两端设备名称和编号。

6 数据互联互通

6.1 数据采集

6.1.1 采集对象与范围

6.1.1.1 数据采集应覆盖机电装备的运行参数、状态参数、环境参数和任务参数，采集范围应全面，满足智能协同控制和运维需求。
6.1.1.2 运行参数应包括转速、功率、电压、电流、压力、流量等，状态参数应包括设备运行状态、故障状态、负载状态等，环境参数应包括温度、湿度、振动等。
6.1.1.3 任务参数应包括协同任务类型、任务进度、任务优先级等，采集对象可根据装备类型和应用场景进行调整，确保采集数据的针对性。

6.1.2 采集精度与频率

6.1.2.1 数据采集精度应符合装备技术要求，数值型参数采集误差应≤±1%，状态型参数采集应准确无误，无误判和漏判。
6.1.2.2 采集频率应根据参数类型和控制需求设定：

a) 关键运行参数采集频率应≥10Hz；
b) 一般参数采集频率可设为 1～10Hz；
c) 环境参数采集频率可设为 0.1～1Hz。

6.1.2.3 采集频率应支持动态调整，当装备运行状态发生异常时，应自动提高对应参数的采集频率。

6.1.2.4 数据采集应采用自动采集方式，按设定的采集周期自动采集数据，采集参数可灵活设定，采集失败时应进行记录和告警。

6.2 数据预处理

6.2.1 数据预处理应在数据传输至协同层前完成，去除无效数据、修正异常数据，确保数据的准确性和完整性。

6.2.2 无效数据应包括缺失数据、重复数据和错误数据，缺失数据可采用插值法补充，重复数据应予以删除，错误数据应根据历史数据和装备特性进行修正。

6.2.3 异常数据识别应采用阈值判断法和趋势分析法相结合的方式，设定合理的异常阈值，当数据超出阈值或趋势异常时，应标记为异常数据并单独存储。

6.2.4 数据预处理应包括数据标准化处理，将不同格式、不同单位的数据转换为统一标准，便于后续数据交互和分析。

6.2.5 预处理后的数据包应添加时间戳和设备标识，数据应可追溯。

6.3 通信协议

6.3.1 系统数据通信应采用标准化通信协议，确保不同设备和系统之间的数据互联互通。

6.3.2 系统内部设备间通信宜采用 OPC UA 协议，支持设备间的实时数据交互和指令传输。

6.3.3 机电装备与控制层之间的通信可采用 Modbus、Profinet 等工业总线协议，协议应支持数据读写、指令下发和状态反馈。

6.3.4 通信协议应支持协议转换功能，当不同设备采用不同协议时，应通过协议转换器实现数据交互。

6.3.5 通信协议应具备错误检测和重传机制，当数据传输出现错误时，应自动重传，重传次数不宜超过 3 次，重传失败时应发出告警信号。

6.4 网络安全

6.4.1 身份认证

6.4.1.1 系统应建立完善的身份认证机制，所有接入网络的设备和用户均应进行身份认证，认证通过后方可接入系统，符合 GB/T 22239 的规定。

6.4.1.2 设备身份认证应采用硬件密钥或数字证书方式，用户身份认证应采用用户名+密码+动态验证码的方式，密码应定期更换，复杂度应符合相关安全要求。

6.4.1.3 系统应记录身份认证日志，包括认证时间、认证设备、认证结果等信息，日志保存时间应不少于 90 天，便于安全审计和故障追溯。

6.4.2 数据加密

6.4.2.1 数据传输过程中应采用加密方式，确保数据不被窃取、篡改和伪造，加密算法宜采用 AES-256 加密算法。

6.4.2.2 敏感数据应进行端到端加密，加密密钥应定期更新，密钥管理应符合保密要求，防止密钥泄露。

6.4.2.3 数据存储时应采用加密存储方式，对敏感数据进行加密处理，存储加密与传输加密可采用不同密钥，提升数据安全等级。

6.4.3 安全防护

6.4.3.1 应部署防火墙，对网络访问进行控制，禁止未授权访问，防火墙规则应根据系统需求定期更新，防范网络攻击。

6.4.3.2 应具备入侵检测功能，能够实时监测网络异常行为，发现异常时应及时发出告警并采取阻断措施。

6.4.3.3　应定期进行安全漏洞扫描，及时发现和修复安全漏洞，漏洞扫描周期不宜超过 3 个月。
6.4.3.4　应禁止使用弱密码、默认密码，定期对用户权限进行审计，清理无效用户和多余权限。

7　智能协同控制

7.1　协同感知

7.1.1　协同感知应基于多源异构数据融合技术，实现对机电装备运行状态、环境信息和任务需求的全面感知。
7.1.2　感知信息应包含装备状态信息、环境感知信息、任务指令信息和协同交互信息，信息维度应覆盖智能协同控制所需全部要素。
7.1.3　装备状态信息感知应包括位置、速度、加速度、负载、温度、振动等参数，感知精度应满足控制要求，数值型参数误差应≤±1%，状态型参数无误判漏判。
7.1.4　环境感知信息应涵盖工作区域内的障碍物、人员、其他装备等，宜采用视觉、激光雷达、超声波等多传感器融合方式。
7.1.5　感知数据应具备时间同步性，时间戳精度应≤1ms，支持多装备间的感知信息对齐，为协同决策提供统一时间基准。
7.1.6　协同感知应具备动态适应性，当装备数量、布局或任务发生变化时，感知范围和频率应自动调整。
7.1.7　感知数据应进行实时预处理，包括数据清洗、异常检测和数据融合。

7.2　决策规划

7.2.1　决策规划应基于感知信息和任务需求，生成多装备协同控制方案。
7.2.2　决策规划应采用分层决策架构，包括全局决策层、局部决策层和执行决策层，各层决策应协同一致。
7.2.3　全局决策层应负责任务分解、资源分配和协同策略制定，宜采用模型预测控制（MPC）算法，优化周期应≤1s，确保决策时效性。
7.2.4　局部决策层应负责单装备的路径规划和动作规划，支持动态障碍物规避。
7.2.5　执行决策层应负责控制指令的生成和执行，宜采用 PID、模糊控制等算法。
7.2.6　决策规划应考虑装备能力约束、任务优先级和时间窗口，生成的控制方案应具备可行性和最优性。
7.2.7　决策规划应支持动态调整，当任务变更、装备故障或环境变化时，应在≤500ms 内重新生成控制方案，保障协同控制的连续性。
7.2.8　决策结果应包含任务分配表、路径规划图和控制指令集，格式应标准化，便于装备间的数据交互和指令执行。

7.3　协同调度

7.3.1　协同调度应基于决策规划结果，实现多装备的任务分配和资源调度。
7.3.2　协同调度应遵循任务优先级原则，优先级分为紧急、高、中、低四个等级，紧急任务响应时间应≤1s，高优先级任务响应时间应≤3s。
7.3.3　协同调度应采用动态调度策略，支持任务的实时添加、删除和修改，调度周期应≤500ms，适应任务变化需求。
7.3.4　调度算法宜采用遗传算法、粒子群优化等智能优化算法，优化目标应包括任务完成时间最短、资源利用率最高和能耗最低。
7.3.5　协同调度应考虑装备间的协同约束，包括空间约束、时间约束和动作约束，避免装备间的碰撞和冲突。
7.3.6　调度结果应包含装备任务列表、执行顺序和时间节点，信息应清晰明确，便于装备执行和状态监控。
7.3.7　协同调度应具备负载均衡能力，避免单一装备负载过重，装备负载率应控制在 70%～80% 之间，提升系统整体效率。

7.3.8 调度过程应具备可追溯性，记录调度时间、调度人员、调度策略和调度结果，日志保存时间应不少于 90 天。

7.4 运动控制

7.4.1 运动控制应基于协同调度结果，实现机电装备的精确运动控制。
7.4.2 运动控制应支持单轴控制、多轴同步控制和多装备协同运动控制，控制精度应满足装备技术要求，定位精度应≤±0.01mm，重复定位精度应≤±0.005mm。
7.4.3 运动控制应采用标准化控制指令，支持不同厂商设备的互操作性。
7.4.4 多轴同步控制应支持电子齿轮、电子凸轮等功能，同步误差应≤±0.01mm，同步响应时间应≤10ms，满足高精度协同运动需求。
7.4.5 多装备协同运动控制应支持主从控制、等时同步控制等模式，协同运动误差应≤±0.02mm，协同响应时间应≤50ms。
7.4.6 运动控制应具备运动平滑功能，采用 S 曲线加减速控制，避免运动冲击，提升装备运行稳定性和使用寿命。
7.4.7 运动控制应支持运动参数的动态调整，包括速度、加速度、加加速度等，调整过程应平滑过渡，无明显冲击。
7.4.8 运动控制应具备安全保护功能，包括限位保护、过载保护、碰撞保护等。

7.5 冲突消解

7.5.1 应基于协同感知和决策规划，实时检测并解决装备间的冲突。
7.5.2 冲突类型应包括：

a) 空间冲突；
b) 时间冲突；
c) 资源冲突；
d) 任务冲突。

7.5.3 冲突检测应实时进行，检测周期应≤50ms。
7.5.4 空间冲突消解应采用优先级调度和路径重规划相结合的方式，优先级高的装备优先通过，优先级低的装备暂停或重新规划路径。
7.5.5 时间冲突消解应采用任务调整和时间窗口优化的方式，调整任务执行顺序或时间，避免装备在同一时间执行冲突任务。
7.5.6 资源冲突消解应采用资源共享和资源分配优化的方式，合理分配有限资源，提高资源利用率，避免资源竞争。
7.5.7 任务冲突消解应采用任务优先级和任务分解相结合的方式，优先执行高优先级任务，对低优先级任务进行分解或延迟执行。
7.5.8 冲突消解应遵循安全优先原则，当冲突可能导致安全事故时，应立即停止相关装备运行，确保人员和设备安全。
7.5.9 冲突消解过程应记录冲突类型、冲突时间、冲突装备、消解策略和消解结果，日志保存时间应不少于 90 天，便于分析和优化。

8 智能优化

8.1 资源配置

8.1.1 资源配置应基于系统运行状态和任务需求，实现资源的优化分配和动态调整，符合 GB/T 43780 的规定。
8.1.2 资源类型应包括计算资源、存储资源、通信资源和装备资源，配置应综合考虑资源利用率、任务需求和系统性能。
8.1.3 计算资源配置应采用负载均衡策略，将计算任务分配到不同计算节点，计算节点负载率应控制在 60%～80%之间，避免节点过载。
8.1.4 存储资源配置应采用分层存储策略，将高频访问数据存储在高速存储设备，低频访问数据存储

在低速存储设备。

8.1.5 通信资源配置应采用流量控制和优先级调度策略，优先保障控制指令和关键数据的传输，通信带宽利用率应控制在 70%～90%之间。

8.1.6 装备资源配置应采用任务匹配和能力评估策略，将任务分配给最适合的装备，装备能力利用率应≥80%。

8.1.7 资源配置应支持动态调整，当任务变化或资源状态改变时，应在≤1s 内重新配置资源，适应系统动态变化需求。

8.1.8 资源配置应具备可扩展性，支持新增资源的接入和配置，无需对原有系统进行大规模改造。

8.1.9 资源配置效果应进行定期评估，评估指标包括资源利用率、任务完成时间和系统能耗，评估周期应≤1 个月。

8.2 能耗管理

8.2.1 能耗管理应基于数据采集和分析，实现机电装备的能耗监测、分析和优化。

8.2.2 能耗监测应覆盖机电装备的全部能耗环节，包括驱动系统、控制系统、执行系统等，监测参数应包括电压、电流、功率、能耗。

8.2.3 能耗分析应采用数据挖掘和机器学习技术，分析能耗数据的趋势、规律和异常，识别能耗浪费环节。

8.2.4 能耗优化应采用智能控制和调度策略，优化装备运行参数和运行模式，降低能耗，优化目标应包括单位产品能耗最低和综合能耗最低。

8.2.5 驱动系统能耗优化应采用变频控制、软启动等技术，根据负载变化调整驱动参数，驱动系统能效比应≥0.9。

8.2.6 控制系统能耗优化应采用低功耗设计和动态功耗管理技术，控制系统待机功耗应≤10W，运行功耗应≤50W。

8.2.7 执行系统能耗优化应采用轻量化设计和高效执行机构，执行系统能耗应降低 10%～30%，提升能源利用效率。

8.2.8 能耗管理应具备能耗预测功能，预测未来一段时间的能耗情况，预测精度应≥90%，为能源管理提供决策支持。

8.2.9 能耗管理应建立能耗基准，定期对比实际能耗与基准能耗，分析能耗差异原因，持续改进能耗管理策略。

8.3 故障预测

8.3.1 应基于数据采集和分析，实现机电装备故障的早期预警和预测。

8.3.2 故障预测应覆盖机电装备的关键部件和系统，包括电机、轴承、减速器、控制系统等，预测参数应包括振动、温度、电流、电压等。

8.3.3 应采用数据驱动和模型驱动相结合的方法，数据驱动方法包括机器学习、深度学习等，模型驱动方法包括故障树分析、失效模式与影响分析等。

8.3.4 故障预测模型应具备自学习能力，能够根据新的故障数据不断优化模型参数，提升预测准确率，模型更新周期应≤1 周。

8.3.5 应具备多故障类型识别能力，能够识别机械故障、电气故障、控制系统故障等，故障识别准确率应≥90%。

8.3.6 应输出故障类型、故障位置、故障概率和故障发生时间，预测结果应清晰明确，便于维护决策。

8.3.7 故障预测预警应分级，分为预警、告警和紧急告警三个级别，预警响应时间应≤10s，告警响应时间应≤5s，紧急告警响应时间应≤1s。

8.3.8 应与维护管理系统集成，根据预测结果自动生成维护计划，维护计划应包括维护时间、维护内容和维护人员。

8.3.9 故障预测结果应进行验证和评估，评估指标包括预测准确率、误报率和漏报率，评估周期应≤1 个月，持续优化预测模型。

9 系统集成与测试

9.1 集成要求

9.1.1 系统集成应遵循模块化、标准化和开放性原则，确保各子系统间的兼容性和互操作性，符合 GB/T 16656.1 的规定。

9.1.2 系统集成应采用分层集成架构，包括设备层集成、控制层集成、协同层集成和应用层集成，各层集成应独立进行，便于测试和维护。

9.1.3 设备层集成应支持不同厂商、不同型号机电装备的接入，接入接口应标准化，符合 OPC UA、Modbus 等工业通信协议要求。

9.1.4 控制层集成应支持可编程控制器、运动控制器等控制设备的集成，控制逻辑应标准化。

9.1.5 协同层集成应支持协同控制算法和决策模型的集成，集成平台应具备分布式处理能力，支持多装备协同控制。

9.1.6 应用层集成应支持人机界面、数据管理系统、维护管理系统等应用系统的集成，集成接口应标准化，便于数据交互和功能扩展。

9.1.7 系统集成应具备可扩展性，支持新增设备和系统的接入，无需对原有系统进行大规模改造。

9.1.8 系统集成应进行兼容性测试，测试内容包括设备兼容性、软件兼容性和数据兼容性，测试通过率应≥99%。

9.2 硬件测试

9.2.1 硬件测试应覆盖系统所有硬件设备，包括：

a) 传感器；
b) 执行器；
c) 控制器；
d) 交换机；
e) 服务器。

9.2.2 硬件测试应包括：

a) 功能测试；
b) 性能测试；
c) 可靠性测试；
d) 环境适应性测试；
e) 安全性测试。

9.2.3 功能测试应验证硬件设备的基本功能是否正常，包括数据采集、指令执行、通信功能等，功能测试通过率应≥99.9%。

9.2.4 性能测试应验证硬件设备的性能指标是否满足要求，包括响应时间、处理能力、传输速率。

9.2.5 可靠性测试应采用加速寿命测试和耐久性测试，验证硬件设备的平均无故障运行时间（MTBF），MTBF 应≥20000 小时。

9.2.6 环境适应性测试应包括温度、湿度、振动、冲击等环境因素的测试。

9.2.7 安全性测试应验证硬件设备的电气安全、机械安全和电磁兼容性，符合 GB/T 17626 系列规定。

9.2.8 硬件测试应记录测试过程和测试结果，测试报告应包括测试设备、测试方法、测试数据和测试结论。

9.2.9 硬件测试不合格的设备应进行整改或更换，整改后应重新测试，直至测试合格。

9.3 软件测试

9.3.1 软件测试应覆盖系统所有软件，包括嵌入式软件、控制软件、协同软件和应用软件，测试应符合 GB/T 15532 的规定。

9.3.2 软件测试应符合以下要求：

——单元测试：应验证软件模块的功能和性能，测试覆盖率应≥90%，单元测试通过率应≥99%；
——集成测试：应验证软件模块间的接口和交互，测试内容包括接口兼容性、数据传输正确性和功能协同性，集成测试通过率应≥99%；
——系统测试：应验证软件系统的整体功能和性能，测试内容包括功能完整性、性能指标、安全性和可靠性；

——验收测试：应验证软件系统是否满足用户需求，测试内容应基于用户需求规格说明书，验收测试通过率应≥99%。

9.3.3 应采用自动化测试工具，提高测试效率和测试准确性，自动化测试覆盖率应≥70%。

9.3.4 应记录测试缺陷，缺陷应分级管理，包括致命缺陷、严重缺陷、一般缺陷和轻微缺陷，致命缺陷和严重缺陷应100%修复。

9.3.5 应生成测试报告，报告应包括测试范围、测试方法、测试结果和缺陷分析。

9.4 联调测试

9.4.1 联调测试应在硬件测试和软件测试合格后进行，验证整个系统的协同工作能力，符合GB/T 45283.4的规定。

9.4.2 联调测试应符合以下要求：

——设备联调：应验证机电装备与控制设备的通信和控制功能，测试内容包括指令下发、数据上传和状态反馈，设备联调通过率应≥99%；

——子系统联调：应验证控制子系统、协同子系统和应用子系统的协同工作能力，测试内容包括数据交互、功能协同和故障处理，子系统联调通过率应≥99%；

——全系统联调：应验证整个系统的功能和性能，测试内容包括任务执行、协同控制、故障预测和能耗管理，全系统联调通过率应≥99%。

9.4.3 应模拟实际运行场景，包括正常工况、异常工况和故障工况，测试系统在不同场景下的适应性和稳定性。

9.4.4 应记录测试数据，包括响应时间、执行效率、能耗数据和故障处理时间，测试数据应符合设计要求。

9.4.5 应生成联调测试报告，报告应包括测试环境、测试内容、测试结果和问题分析，便于系统优化和改进。

9.4.6 联调测试不合格的部分应进行整改，整改后应重新测试，直至测试合格。

10 运维与安全保障

10.1 状态监控

10.1.1 状态监控应覆盖系统所有设备和软件，实时监测运行状态和性能指标。

10.1.2 状态监控应包括设备状态监控、软件状态监控、网络状态监控和系统性能监控，监控内容应全面，符合以下要求：

——设备状态监控：应监测设备的运行参数、故障状态和健康状态，监控频率应≥1Hz，异常检测响应时间应≤10s；

——软件状态监控：应监测软件的运行状态、资源占用和功能执行情况，监控频率应≥1Hz，异常检测响应时间应≤10s；

——网络状态监控：应监测网络的带宽利用率、传输延迟、丢包率和抖动，监控频率应≥1Hz，异常检测响应时间应≤10s；

——系统性能监控：应监测系统的任务完成时间、资源利用率和能耗数据，监控频率应≥1Hz，性能分析周期应≤1h。

10.1.3 应具备可视化功能，通过图表、曲线等方式展示监控数据。

10.1.4 应具备异常告警功能，告警方式包括声音告警、灯光告警和短信告警，告警响应时间应≤5s。

10.1.5 状态监控数据应存储在数据库中，存储时间应不少于1年。

10.2 日志管理

10.2.1 日志管理应记录系统所有操作和事件，包括用户操作、设备运行、软件执行和异常事件。

10.2.2 日志类型应包括操作日志、运行日志、异常日志和安全日志，日志内容应完整，记录时间、对象、内容和结果，符合以下要求：

——操作日志：应记录用户的登录、退出、配置修改等操作，日志记录应准确，时间戳精度应≤1ms；

——运行日志：应记录设备和软件的运行状态和性能指标，日志记录频率应≥1 次/分钟，确保运行过程可追溯；

——异常日志：应记录设备故障、软件错误和网络异常等事件，日志应包括异常类型、异常时间、异常位置和异常描述；

——安全日志：应记录安全事件，包括身份认证失败、未授权访问和恶意攻击等，日志应包括事件类型、事件时间、事件源和事件结果。

10.2.3 日志存储应采用分级存储策略，重要日志应加密存储，存储时间应不少于 90 天，普通日志存储时间应不少于 30 天。

10.2.4 应具备日志查询和分析功能，支持按时间、类型、对象等条件查询，分析日志数据的趋势和规律。

10.2.5 应具备日志备份功能，备份周期应≤1 天，备份数据应存储在安全位置。

10.3 权限控制

10.3.1 权限控制应基于最小权限原则，为不同用户分配不同权限，确保系统安全。

10.3.2 用户角色应分为系统管理员、运维人员、操作人员和访客，不同角色权限应明确区分，避免权限交叉，符合以下要求：

——系统管理员：应具备最高权限，负责系统配置、用户管理和安全管理，权限应严格控制，仅授权给必要人员；

——运维人员：应具备设备维护、软件更新和故障处理权限，权限应限于运维工作所需，不得越权操作；

——操作人员：应具备任务执行和状态监控权限，权限应限于操作工作所需，不得修改系统配置；

——访客：应具备只读权限，仅能查看系统状态和公开信息，不得进行任何操作。

10.3.3 应采用基于角色的访问控制（RBAC）模型，权限分配应通过角色进行。

10.3.4 应具备权限审计功能，记录权限分配和使用情况，审计日志保存时间应不少于 90 天。

10.3.5 应支持权限动态调整，当用户角色变化时，应及时调整权限，防止权限滥用。

10.4 容灾备份

10.4.1 容灾备份应保障系统在发生故障或灾难时的数据安全和业务连续性，符合 GB/T 20988 的规定。

10.4.2 容灾备份应包括数据备份、系统备份和业务备份，备份内容应全面，符合以下要求：

——数据备份：应采用全量备份和增量备份相结合的方式，全量备份周期应≤1 周，增量备份周期应≤1 天；应采用异地备份策略，备份数据应存储在不同地理位置的备份中心，防止数据丢失；

——系统备份：应包括操作系统、数据库和应用程序的备份，备份周期应≤1 个月；

——业务备份：应采用冗余设计，关键设备和链路应具备备份，当主设备或链路故障时，备用设备或链路应在≤50ms 内切换。

10.4.3 应具备恢复测试功能，定期测试备份数据和系统的恢复能力，恢复测试周期应≤1 个月。

10.4.4 应制定灾难恢复计划，明确灾难恢复流程、责任人和恢复时间目标（RTO），RTO 应≤1h。

10.4.5 应定期更新备份策略和灾难恢复计划，适应系统变化需求，确保容灾备份有效性。

10.5 安全审计

10.5.1 安全审计应覆盖系统所有安全相关活动，包括用户操作、权限变更、安全事件和系统配置，符合 GB/T 22239 的规定。

10.5.2 安全审计应采用自动化审计工具，提高审计效率和准确性，审计覆盖率应≥99%。

10.5.3 安全审计应包括操作审计、权限审计、安全事件审计和配置审计，审计内容应全面，符合以下要求：

——操作审计：应记录用户的所有操作，包括登录、退出、数据访问和配置修改，审计日志应包括操作时间、操作对象和操作结果；

——权限审计：应记录权限分配和变更情况，包括用户角色变更、权限添加和权限删除，审计日志应包括变更时间、变更人和变更内容；

——安全事件：审计应记录安全事件的检测、响应和处理情况，包括事件类型、事件时间、事件源和处理结果；

——配置审计：应记录系统配置的变更情况，包括网络配置、安全配置和系统参数，审计日志应包括变更时间、变更人和变更内容。

10.5.4 应定期生成审计报告，报告应包括审计范围、审计结果、安全风险和改进建议，审计周期应≤1 个月。

10.5.5 安全审计发现的安全问题应及时整改，整改完成后应进行复查。

10.5.6 应遵循保密原则，审计数据应加密存储，仅授权人员可访问，防止审计数据泄露。