

团 体 标 准

T/CAAMM xxxx—20xx

智能农机装备数字孪生系统

第 2 部分：技术要求

Digital twin system of intelligent agricultural machinery

part 2: Technical requirements

(报批公示稿)

202x-xx-xx 发布

202x-xx-xx 实施

中国农业机械工业协会 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 概述.....2

5 数字孪生系统总体技术要求.....2

6 数字孪生系统构成要素技术要求.....4

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》给出的规则起草。

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。

本文件由中国农业机械工业协会提出。

本文件由中国农业机械工业协会归口。

本文件起草单位：中国农业大学、北京农学院、洛阳智能农业装备研究院有限公司、北京市农林科学院智能装备技术研究中心、中国农业机械化科学研究院集团有限公司、洛阳拖拉机研究所有限公司、北京启维数字科技有限公司。

本文件主要起草人：杜岳峰、郭大方、宋正河、陈度、郭志强、黄胜操、尹彦鑫、周立明、陈凯康、王东青、高辽远、吴传鑫、栗晓宇、温昌凯、武秀恒、乔智、王林泽、吴志康、马若飞。

本文件为首次发布。

智能农机装备数字孪生系统 第2部分:技术要求

1 范围

本文件描述了智能农机装备数字孪生系统（以下简称“数字孪生系统”）应达到的技术要求。
本文件适用于数字孪生系统的规划、开发、管理、运维、评估和验收等工作。

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，仅该日期的对应版本适用于本文件；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 41723 自动化系统与集成 复杂产品数字孪生体系架构
- GB/T 43441.1 信息技术 数字孪生 第1部分：通用要求
- GB/T 2423 电工电子产品环境试验

3 术语和定义

GB/T 41723 和 GB/T 43441.1 界定的术语和定义适用于本文件。

3.1

多源数据 multi-source Data

来自不同感知设备、系统平台或外部环境（如农机、土壤、气象等）的数据集合。多源数据融合用于提升模型的精度和智能决策能力。

3.2

作业场景 operation Scenario

指农机装备在不同农业环节下的具体应用环境和任务情境，如耕整、播种、植保、收获等。作业场景是驱动建模、仿真、控制决策和优化分析的关键背景。

3.3

可视化 visualization

通过图形界面、三维模型、热力图、轨迹图等手段，将设备状态、作业数据和仿真结果进行直观展示，提升用户操作感知与系统透明度。

3.4

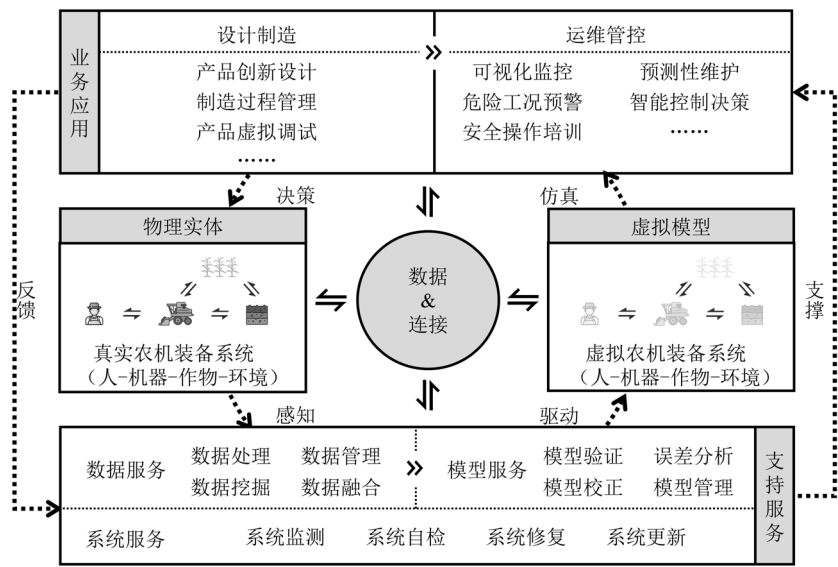
边缘计算 edge computing

指在靠近数据源（农机装备）的位置部署计算资源，对数据进行本地处理与预判断，减轻云端负

担，提高响应速度和可靠性。

4 概述

数字孪生系统由物理实体、虚拟模型、数据与连接、支持服务、业务应用五个核心要素组成，构成系统整体架构，如图 1 所示。



系统的技术要求涵盖功能、性能、用户体验、安全、运维五个维度，构成系统技术指标评价体系，如图 2 所示。

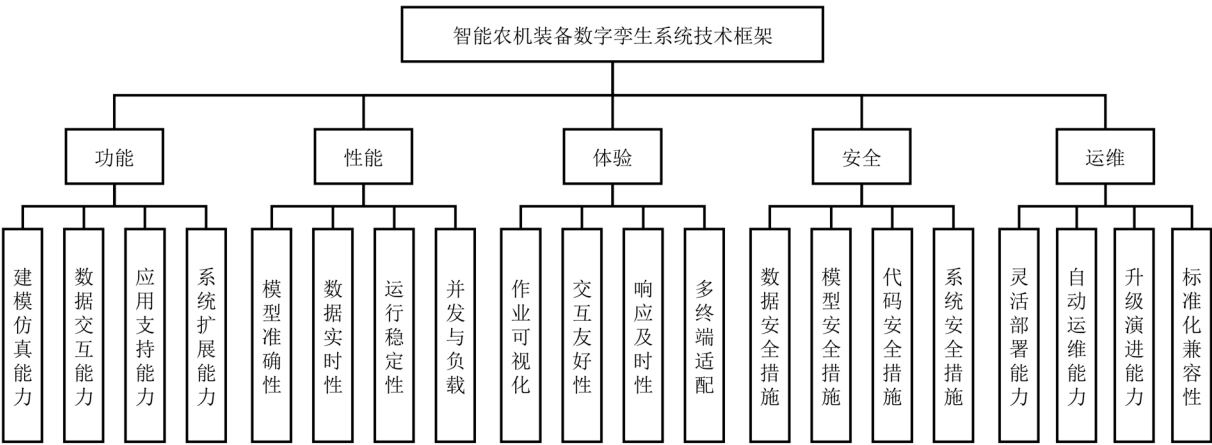


图2 系统技术指标评价维度

本标准中，首先从系统整体视角提出数字孪生系统在上述五个技术维度下的共性总体要求，然后面向构成系统的五个核心要素——物理实体、虚拟模型、数据与连接、支持服务、业务应用，分别提出其在上述五个维度的具体要求。

5 数字孪生系统总体技术要求

5.2 系统功能要求

系统功能性指标用于衡量系统应具备的技术与业务能力，目的是构建一个功能完整、场景驱动、灵活可扩展的数字孪生系统，具体要求包括：

- a) 建模仿真能力：应支持对智能农机装备的关键部件（如动力系统、传动系统、作业机构等）以及典型作业工况（如耕整、播种、植保、收获等）进行结构、行为和状态建模与仿真；
- b) 数据交互能力：支持农机装备与虚拟模型之间的实时或周期性数据采集、信息传输、状态映射、反馈控制，保证虚实同步；
- c) 应用支持能力：应支持多作业环节下的典型业务应用，涵盖产品设计制造与运维管理控制等方面，功能包括但不限于产品创新设计、制造过程管理、产品虚拟调试、可视化监控、危险工况预警、安全操作培训、预测性维护和智能控制决策等；
- d) 系统扩展能力：应具备良好的模块化结构、接口开放性与平台兼容性，支持与农机管理系统、农业生产系统、作业平台等外部系统集成。

5.3 系统性能要求

系统性能指标评估系统的运行精度、效率与可靠性，确保其在多变农田环境中的稳定适应性。具体要求如下：

- a) 模型准确性：虚拟模型应能精准反映农机装备实际状态，模型与实物的同步误差应控制在业务允许范围内；
- b) 数据实时性：系统应支持农机关键作业参数数据采集与反馈的低延迟处理。数据采集频率和时延由具体业务需求决定；
- c) 运行稳定性：系统应支持田间作业中的高强度连续运行，备高可靠性和容错能力，具备断点续传和边缘缓冲能力，避免因软件故障或硬件故障等问题导致的崩溃或卡顿；
- d) 并发与负载：支持至少多台农机设备同时接入，满足多台农机协同作业场景需求。

5.4 系统体验要求

用户体验指标衡量系统对用户群体的友好性与易用性，应充分适应农业场景下多样化使用环境，具体要求如下：

- a) 作业可视化：应提供基于农机装备的三维模型与作业数据的可视化功能，支持作业轨迹回放、工况状态监视、故障仿真与行为分析；
- b) 交互友好性：系统应具备图形化界面、简洁操作流程和多语言支持，满足基层用户快速上手和高频操作需求；
- c) 响应及时性：典型用户操作的系统响应时间和关键数据图表刷新周期应保障流畅的用户体验；
- d) 多终端适配：应支持个人计算机端、移动端、机载终端等多类型终端访问，适应田间、办公室等多场景使用。

5.5 系统安全要求

系统安全指标用于确保数据、模型、平台与软件运行的全生命周期安全性，构建可信、可控、可追溯的系统安全保障体系。具体要求如下：

- a) 数据安全措施：应采用加密传输和存储技术，确保数据在采集、传输、存储过程中的安全性；
- b) 模型安全措施：应保障虚拟模型在构建、调用、部署、更新过程中的安全性，防止模型篡改、泄露或被恶意替换，重要模型应具备版本管理、完整性校验与访问控制机制；
- c) 代码安全措施：应对系统软件进行严格的安全测试和漏洞扫描，确保程序无漏洞、无后门，

防止漏洞或恶意代码的攻击；

- d) 访问权限控制：系统应支持多级权限划分与用户认证机制，防止非法访问与误操作；
- e) 系统防护能力：应具备入侵检测、防火墙、病毒防护等安全防护机制，防止外部攻击或内部泄密；
- f) 审计追溯机制：应记录用户操作、系统事件与异常行为日志，并支持日志审计、导出与追踪分析功能。

5.6 系统运维要求

运维保障指标评估系统在部署、运行、维护、升级等方面的持续运营能力，确保系统稳定可管、灵活可扩展、长期可用。具体要求如下：

- a) 灵活部署能力：支持标准化部署与快速上线，可适配云端、本地或混合部署环境，适应不同应用规模与网络条件；
- b) 自动运维能力：系统应支持自动监控、故障检测、资源调度、日志管理等自动化运维功能；
- c) 升级演进能力：应支持模块化架构和热更新机制，实现不中断业务情况下的系统迭代与版本升级；
- d) 标准化兼容性：系统应符合农业物联网通信协议、农机信息编码规范、行业数据接口标准，提升跨平台运行与设备兼容能力。

6 数字孪生系统构成要素技术要求

本节从物理实体、虚拟模型、数据与连接、支持服务、业务应用五个系统核心要素出发，分别提出其在功能、性能、体验、安全、运维五个维度下应满足的技术要求。各要素应在满足系统总体技术要求的基础上，具备面向农业装备作业场景的针对性能力。

6.1 物理实体技术要求

6.1.1 功能要求

a) 多维度感知能力

物理实体应具备覆盖“设备层-作业层-环境层”的多维感知能力，具体要求如下：

- 支持对应支持对关键运行参数（如位置、速度、姿态、作业深度、施药量、土壤湿度等）的实时、连续、准确采集；
- 重要传感器具备硬件冗余或软融合补偿机制，如 IMU+GPS 联合定位，保障感知精度连续性；
- 对于难以直接测量的物理量，建议通过软测量模型进行计算估算。

b) 传感器系统配置

- 所选传感器应具备工业级精度，良好抗干扰能力，能适应田间环境（如粉尘、高湿、震动等）；

c) 物理执行单元

- 关键执行部件应具备闭环控制能力，动作响应精准；
- 建议配备线控底盘等具备远程控制/无人化能力的装置；
- 控制系统应开放标准 API/SDK 接口，支持数字孪生系统平台实时调用与调度；
- 执行指令响应时间应控制在<100ms 范围内（视任务需求）；
- 执行单元支持多任务调度优先级管理机制，避免动作冲突。

6.1.2 性能要求

a) 数据采集性能

- 数据采集频率应根据作业模式自适应调整；
- 系统应提供采集频率配置功能，支持参数级个性化设置；
- 数据采集应具备时间戳校准机制，确保多源数据同步。

b) 执行控制性能

- 控制响应延迟建议小于 100ms，关键安全控制动作建议低于 50ms；
- 系统应具有抗干扰能力，指令信号应具备优先级调度与确认机制；
- 控制指令丢失率应小于 0.01%。

c) 环境适应性

- 感知与执行单元需符合 GB/T 2423 系列环境试验标准；

6.1.3 体验要求

状态可视化支持

- 系统应对执行状态、感知异常进行视觉/听觉提示，增强操作人员感知体验。

6.1.4 安全要求

a) 感知安全性

- 关键传感器应具备状态监测机制，可识别掉线、信号漂移、超限等异常情况；
- 关键感知数据（如位置、速度、姿态等）异常时，应触发降级运行机制或切换至人工控制模式；
- 建议对感知数据采用校验算法（如 CRC），防止传输误码导致虚拟模型状态漂移。

b) 执行安全性

- 执行单元应具备反馈闭环机制，确保执行后能及时反馈执行状态；
- 应设置执行动作超限报警机制，当发出错误或极限控制指令时，设备应具备指令校验与拦截机制；关键执行动作设定安全边界参数区间，模型控制不得突破边界，防止误操作带来设备损伤或作业失效；
- 对远程执行任务应设置两级操作确认机制，提高指令可靠性。

c) 虚实映射异常防护机制

- 系统应具备状态一致性监测功能，当虚实状态同步误差超过设定阈值应自动报警；
- 出现严重偏差时应中断控制联动，进入安全模式运行；
- 所有虚实交互操作（如模型下发控制参数、自动路径等）应具备日志记录与可追溯机制。

d) 安全通信与指令隔离

- 物理实体控制器应预留安全通信接口，支持状态传递、异常反馈与权限确认；
- 系统进行远程调试或参数修改时，应通过白名单机制对允许下发指令进行限制，避免误操作。

6.1.5 运维要求

a) 模块级维护便捷性

- 感知与执行部件应支持模块化更换与即插即用，缩短维护时间；
- 控制器配置应支持远程配置和本地按键调试。

- 应具备故障码上报机制与本地/远程诊断支持能力。
- b) 运行状态监控
 - 系统应具备设备运行状态远程监测、寿命评估与故障预警能力；
 - 建议支持边缘侧日志记录与历史数据上传功能，便于事后追溯。
- c) 兼容性与适配性
 - 控制器与传感器应支持多协议接入，可与主流农机品牌平台兼容；
 - 对于新增模块应具备自识别机制，快速适配与配置加载。

6.2 虚拟模型技术要求

6.2.1 功能要求

- a) 多物理场与多尺度建模能力
 - 应支持覆盖机械结构、电气系统、液压控制、机器-土壤-作物相互作用等多个物理域；
 - 应支持从部件级到系统级的多层级建模；
 - 应具备多学科建模统一接口标准(如 FMU)与耦合机制,支持联合仿真框架(Simulink、Modelica、AMESim、ANSYS 等)接入。
- b) 模型交互与作业场景适应能力
 - 应支持用户通过图形界面或 API 方式对模型进行加载、配置、运行与动态调整；
 - 应具备作业场景(如耕作、播种、收割等)的识别与模型自适应切换机制；
 - 输入参数应可通过任务驱动规则库自动适配不同仿真模式。
- c) 模型组件化设计与复用能力
 - 应采用模块化设计思想构建模型结构，支持参数模板与结构模板的快速复用；
 - 提供模型组件注册机制，支持组件版本控制、依赖关系管理与兼容性检查；
 - 支持多层级模型之间的耦合与联合仿真，如动力系统与控制系统协同建模。
- d) 数据驱动模型演化能力
 - 应支持融合多源数据对模型结构与参数进行自适应调整；
 - 推荐集成机器学习/深度学习模块用于构建数据驱动模型；
 - 模型更新过程应记录原始状态、训练过程、数据来源与版本编号，具备全过程可追溯性。

6.2.2 性能要求

- a) 仿真精度与验证机制
 - 模型整体仿真误差应满足实际业务需求；
 - 对关键性能指标(如路径跟踪误差、控制响应偏差)应设定单独误差阈值；
 - 应具备仿真精度动态自适应机制，根据场景切换仿真精度与响应速度。
- b) 高频响应与低延迟反馈能力
 - 模型输入—计算—输出闭环响应时间和仿真循环频率应满足实际业务需求；
 - 应具备状态缓存与异步处理能力，减少计算阻塞与卡顿现象。
- c) 资源效率与模型精简化能力
 - 建议支持多级模型配置(如轻量版、标准版、高精度版等)以适配不同计算资源；
 - 应具备模块启停与资源动态调度功能，提升系统整体计算效率；

- 建议采用稀疏矩阵、增量更新、代理模型等轻量算法结构，提高运行速度。

d) 边缘部署与同步机制

- 应支持在边缘计算节点部署轻量化模型，用于近场实时仿真或故障诊断；
- 模型同步应支持断点续传、差异化同步与版本回滚机制，确保边云一致性；
- 建议提供双向一致性校验机制，以保障模型同步过程的完整性与安全性。

6.2.3 体验要求

a) 模型可视化与交互性

- 支持参数实时调整、结构模块启停、仿真结果可视对比等交互操作。

b) 操作简洁性与易配置性

- 模型加载、运行、切换过程应流程清晰、操作简洁，具备配置引导功能；
- 参数输入应支持模板化或自动化设置，减少人工配置成本。

6.2.3 安全要求

a) 调用审计与日志记录机制

- 模型调用应具备日志记录机制，至少包含时间、用户 ID、调用模块、输入参数、结果状态等内容；
- 日志应支持导出、分级查询与告警联动，保留时间不少于 180 天。

b) 模型数据加密与完整性保障

- 所有涉及模型的结构文件、配置文件、输入输出数据应采用 TLS 1.2 以上协议传输；
- 核心模型参数应采用 AES-256 加密存储，并具备权限控制机制；
- 应提供文件完整性校验机制（如 hash 签名）防止数据篡改。

c) 接口权限与风险控制机制

- 模型服务接口应基于 OAuth2.0 或同等级认证机制实现用户访问控制；
- 应支持接口访问频率限制（如每用户 60 次/分钟）防止滥用或恶意调用；
- 对高风险操作（如模型重置、强制更新等）应启用双因素验证或管理员授权机制。

6.2.4 运维要求

a) 模型生命周期管理

- 应支持模型的版本管理、状态标识、更新记录追踪与回滚机制；
- 所有模型的创建、修改、发布等操作应支持操作日志记录与权限控制。

b) 模型运行监控与自诊断

- 系统应提供模型运行状态监控界面，包括运行频率、响应时间、资源占用等指标；
- 应具备模型运行异常检测与自诊断机制，支持自动告警或切换备用模型。

c) 模型平台兼容与可扩展性

- 模型应兼容主流建模平台与仿真工具，支持标准模型接口格式（如 FMU 等）；
- 支持多模型并行运行、异构模型混合调用与横向扩展能力。

6.3 数据与连接

6.3.1 功能要求

- a) 多协议通信支持
 - 系统应支持 Modbus RTU/TCP、CAN、Ethernet 等主流工业通信协议；
 - 通信接口应具备自动识别与热插拔机制；
 - 通信驱动应采用模块化设计，支持插件化加载与自定义协议扩展。
- b) “农机装备—虚拟模型”数据联动机制
 - 应建立农机装备与虚拟模型的实时映射数据连接机制，实现动态驱动与状态同步；
 - 模型输出结果（如路径规划、参数优化等）应可反向传输并转化为控制指令下发；
 - 联动规则应支持用户自定义配置，形成“阈值-模型触发-反馈控制”的闭环联动模式。
- c) 外部数据源集成能力
 - 应支持通过标准化接口（RESTful API、WebSocket 等）接入农业气象、土壤监测等第三方数据源；
 - 系统应具备外部数据格式转换、时间同步、缺失补全等预处理能力；
 - 外部数据源应具备配置管理功能，包括数据源标识、更新频率、有效期与状态监控。

6.3.2 性能要求

- a) 动态采集与传输效率
 - 数据采集频率应支持按作业模式动态调整；
 - 支持双向数据并发传输，指令下发/上传响应时间应满足实际需求；
 - 所有数据包应包含时间戳，支持 JSON、XML 或二进制结构化格式；
 - 网络波动或高负载时，应优先保障关键数据刷新，自动延迟非核心数据更新。
- b) 边缘计算与预处理能力
 - 边缘节点应具备基础数据处理能力；
 - 推荐支持部署轻量化 AI 模型用于本地推理与判断；
 - 系统应支持“云+边”协同策略，根据带宽/任务动态切换处理重心。

6.3.3 体验要求

- a) 参数配置简便性
 - 通信频率、数据字段、采集策略等参数应支持模板化配置，并支持导入/导出操作；
 - 推荐提供图形化配置界面，便于非专业用户快速完成通信设置与参数调整；
 - 推荐支持自动推荐配置模板（如按设备类型自动匹配推荐通信参数）。
- b) 连接状态可视化
 - 系统应实时展示设备连接状态（在线/离线）、信号强度、数据传输速率等信息；
 - 应通过图标、颜色、图表等直观方式标识通信异常、链路断开、数据延迟等状态；
 - 应支持通过大屏/移动端快速查看当前连接总览与关键指标变化趋势。
- c) 数据交互友好性
 - 应支持采集数据的实时浏览、历史回放与关键字段筛选；
 - 数据展示应支持表格、图表、地图等多种视图切换，满足不同任务需求；
 - 推荐提供交互式过滤与时间轴操作，提升数据可读性与分析效率。
- d) 多终端一致体验
 - 应确保 PC 端、移动端、车载终端在通信设置与数据交互方面的一致性；

- 移动端应支持弱网环境下的本地缓存与自动补传机制，保障使用连续性；
- 界面布局与操作逻辑应符合终端分辨率与操作习惯的差异化适配设计。

6.3.4 安全性要求

a) 网络通信安全防护能力

- 系统应部署防火墙策略，具备 IP 白名单、端口过滤、协议限制等功能；
- 支持网络入侵检测与异常行为识别（如流量洪泛、指令异常等）；
- 可联动安全事件告警模块，实现实时通知与快速处置。

b) 数据加密与完整性保护机制

- 所有数据传输应基于 TLS 1.2 或更高协议加密；内部数据推荐使用 AES-256 标准加密；
- 所有通信链路应附带完整性校验（如 hash 签名、CRC 码等）防止数据被篡改。

c) 断点续传与本地缓存保障机制

- 网络中断时，系统应自动启动本地缓存机制，缓存时间不少于 24 小时；
- 传输应具备 ACK 确认机制与丢包重发策略；
- 数据重传后应自动触发完整性校验与虚拟模型状态更新。

6.3.5 运维要求

a) 数据链路状态监控

- 系统应实时监测各设备连接状态、通信延迟、数据丢包率、异常事件等指标，支持图形化展示与告警推送。

b) 通信驱动热更新机制

- 新增通信协议或设备类型时，应支持驱动热加载、插件式扩展，无需整体系统重启。

c) 接口兼容与标准对接能力

- 系统应兼容主流农机与农业物联网通信协议，支持统一 API 接口规范与开放平台对接能力，确保数据流通与互操作性。

d) 备份与恢复能力

- 系统应配置多级备份策略：边缘端日备份，云端周备份；
- 系统应具备数据恢复操作界面，可按时间点、数据类型、设备 ID 等精细化恢复；
- 所有关键数据应支持异地容灾备份与加密存储，保留时间 ≥ 180 天；
- 恢复操作应支持按时间点、设备 ID、数据类型等精细化选择，并具备回滚机制。

6.4 支持服务技术要求

6.4.1 功能要求

a) 数据服务能力

- 支持结构化、半结构化、非结构化数据采集与预处理，包括清洗、补全、标准化等操作；
- 具备数据治理功能，如元数据管理、血缘追踪、权限配置、生命周期管理等；
- 支持多源异构数据融合能力；
- 据挖掘模块应提供聚类、回归、预测、频繁项挖掘等算法支持，并具备插件扩展接口。

b) 模型服务能力

- 支持模型的验证、校准、残差分析与可视化对比等功能，提升模型可信度；

- 支持模型参数辨识算法、优化算法等，实现自适应调参；
- 应具备版本化管理能力，支持差异对比、回溯发布、标签管理与生命周期管理（注册、审核、上下架等）。
- c) 系统支撑能力
 - 应支持运行状态实时监控，覆盖服务响应、任务队列、资源使用等关键指标；
 - 具备容错管理机制，如自动重试、故障转移、副本热备等；
 - 支持接口治理功能，包括限流、黑白名单、调用频控、异常熔断等；
 - 支持第三方插件或服务集成生命周期管理（启停、升级、卸载）。
- d) 接口标准化与互操作能力
 - 系统所有接口应符合 RESTful 规范，并基于 HTTP/HTTPS 协议；
 - 应提供符合 OpenAPI 3.0 标准的接口文档，支持自动化测试工具（如 Swagger、Postman 等）；
 - 应提供多语言 SDK 示例（至少包含 Python、Java、C#）与异常处理、错误码说明文档；
 - 接口访问应具备 OAuth2.0 等权限控制机制，支持统一认证接入。

6.4.2 性能要求

- a) 高效数据处理能力
 - 系统应支持数据流处理能力，满足多农机、多维参数的并发处理需求；
 - 实时数据流延迟满足场景需求，支持主流处理框架的无缝集成；
 - 应提供数据处理策略选择功能，根据数据类型或任务场景自动加载预设模板。
- b) 数据质量与监测能力
 - 应支持自定义质量指标阈值（延迟率、缺失率、重复率等）并实时检测；
 - 应以图表、趋势线、热力图等形式展示数据质量状态与历史演变；
 - 支持按数据源、时间段、设备类别等维度进行多层次统计与异常告警。
- c) 系统稳定性与负载能力
 - 应支持多节点分布式部署与统一资源监控，保障横向扩展能力；
 - 支持图形化监控大屏，展示系统运行状态与资源瓶颈预警。
- d) 性能降级与服务熔断能力
 - 系统负载接近设定阈值时，应自动限制非关键功能调用频率；
 - 出现调用异常比例超过 10% 时，应自动触发服务熔断机制并隔离故障实例；
 - 健康服务实例状态恢复后，应自动恢复熔断服务，并保证调用不中断。

6.4.3 体验要求

- a) 服务状态与运行透明性
 - 支持仪表盘形式展示各类服务运行状态、接口健康度、任务执行进度等信息；
 - 应支持操作日志实时查询，关键服务应具备进度条、状态标签等视觉反馈；
 - 建议对告警、资源瓶颈、更新计划等系统事件提供弹窗或通知提醒。
- b) 配置灵活性与个性化管理
 - 支持用户根据角色定制仪表板、常用功能菜单与参数视图；
 - 应支持接口调用统计、模型调用频次、任务执行记录等视图的过滤、排序、自定义保存；
 - 可提供用户偏好存储功能，支持自动加载用户上次使用习惯（如时间范围、筛选项、工作台

布局等)。

6.4.4 安全要求

a) 漏洞防护与访问权限管理

- 应接入自动漏洞扫描工具，扫描频率不少于每周一次；
- 应具备完整的漏洞补丁管理体系，包括灰度部署、快速回滚、影响范围评估等；
- 用户权限控制应基于细粒度 RBAC 模型，精确控制模块、接口与数据字段的访问权限。

b) 日志审计与行为追溯机制

- 审计日志应覆盖操作人、时间、来源 IP、操作内容、影响范围等字段；
- 日志应至少保存 180 天，并支持快速索引与检索分析；
- 所有关键行为（如登录、权限变更、模型调用、数据导出等）必须记录。

c) 安全发布与回滚机制

- 应支持蓝绿部署、金丝雀发布与分阶段灰度上线等方式，降低上线风险；
- 应支持 10 分钟内完成系统版本快速回滚；
- 所有发布与回滚操作应生成完整日志，支持异常时自动恢复到上一个稳定版本。

d) 容器化与资源隔离安全保障

- 容器部署环境应启用 Liveness/Readiness 探针，保障服务持续健康运行；
- 应对容器设置资源上限与配额，避免单容器资源过载影响整体系统；
- 应支持网络、存储空间的隔离机制，确保容器间资源安全（如 Kubernetes namespace/volume 隔离策略）。

6.4.5 运维要求

a) 用户权限与组织管理能力

- 支持用户按角色（如管理员、运维人员、使用人员、外部人员等）配置权限；
- 限粒度可精确至数据维度、操作类型、时间段；
- 支持用户批量导入与企业统一认证系统（如 LDAP、SSO 等）集成。

b) 系统维护与数据备份机制

- 支持每日增量+每周全量+每月快照的三级数据备份策略；
- 有备份支持断点续传与模块级恢复，提升系统可用性与数据安全性；
- 系统日志支持模块化、时间范围与关键字检索，支持压缩归档导出。

c) 设备管理与远程诊断功能

- 具备设备登记、分类管理、状态监控与全生命周期管理功能；
- 支持远程日志收集、历史数据对比与规则匹配分析；
- 支持部署模型预测算法（如 RUL、故障树分析等）提升运维前瞻性。

d) 故障预警与远程处置能力

- 支持 CPU/内存/IO/延迟等多指标综合故障判断与分级告警机制；
- 统应具备自动恢复能力，如容器自愈、热重启、副本切换等；
- 支持远程运维操作，如固件升级、参数下发、配置同步，并具备访问审计与快速回滚能力。

6.5 业务应用技术要求

6.5.1 功能要求

a) 核心业务模块能力

- 作业可视化：应支持农机装备作业状态、作业轨迹、传感器数据、地图信息等多源信息融合展示，并提供作业回放与视频流嵌入能力；
- 仿真交互：应支持基于数字孪生模型的虚拟操作与调参测试，支持仿真与实机状态联动；
- 路径规划：应支持自动路径生成、避障优化与多机协同路径策略；
- 故障与工况预测：应支持基于规则与人工智能的工况异常预警与故障预测；
- 决策推荐：应基于作业历史与环境参数推荐作业时机、作业策略与参数组合；
- 培训教学：应提供虚拟操作考核环境、任务评分反馈机制与用户考核模式。

b) 多终端接入与同步能力

- 应支持多端访问统一接入；
- 移动端应具备离线数据采集、模型浏览与历史查询能力，支持断网重连自动同步机制；
- 地图服务应支持高德、百度、天地图、离线地图等多源切换，保障终端兼容性。

c) API/SDK 与开放能力

- 应提供标准 RESTful API，覆盖数据查询、模型调用、状态上报、控制下发等功能；
- 应提供多语言 SDK 包（至少支持 Python、Java、C#），具备调用样例、错误码说明等文档；
- 支持 Webhook 推送机制，将预警、告警、控制指令推送至第三方平台；
- 应提供开发者控制台，支持密钥管理、调用统计、接口权限配置。

d) 模块集成与动态更新能力

- 应基于微服务架构设计，支持模块级热更新，避免系统整体重启；
- 应支持模块注册、版本控制与参数配置接口，便于模块扩展与集成；
- 支持沙箱机制接入第三方模块，隔离运行环境，保障系统稳定与安全。

6.5.2 性能要求

a) 访问响应与查询性能

- 页面首次加载时间应 ≤ 3 秒，用户操作响应时间 $\leq 500\text{ms}$ ；
- 数据查询接口应具备分页、模糊查询与缓存功能，平均查询响应 $\leq 200\text{ms}$ ；
- 应支持预加载机制，实现页面进入前异步加载关键数据。

b) 高可用与容错能力

- 应支持主备双活或多节点部署架构，切换时间 ≤ 15 秒；
- 应配置健康检查机制（如 K8s Liveness Probe）自动剔除失效服务；
- 系统异常时，应支持服务熔断与性能降级，保障关键功能持续可用。

c) 高并发处理与可扩展能力

- 系统应支持多用户并发访问，支持容器级横向弹性扩展；
- 应使用异步任务队列（如 Kafka、RabbitMQ）处理耗时操作，避免阻塞主线程；
- 所有微服务应具备容器部署支持（如 Docker + Kubernetes 架构）。

6.5.3 安全要求

a) 权限管理与角色隔离

- 应基于 RBAC 模型建立权限体系，支持角色分级（管理员、维护员、作业员、开发者等）；
- 各业务模块权限应可独立配置（如路径模块仅限高级用户访问）；

- 权限配置应可视化展示，并支持导出备份。
- b) 加密通信与身份校验机制
 - 所有数据传输应基于 HTTPS（TLS 1.2 以上）；
 - 终端用户应强制身份认证，支持 OAuth 2.0、JWT 等机制；
 - 对高风险操作（如远程控制）应启用双因素认证或操作确认机制。
- c) 日志审计与行为追踪机制
 - 所有用户操作（如查询、修改、导出等）应记录操作对象、参数、结果、时间与 IP；
 - 审计日志保留周期 ≥ 180 天，支持检索、筛选、导出分析；
 - 应自动识别行为异常（如短时间高频操作、越权访问等），并触发封锁或告警。
- d) 终端安全与访问防护机制
 - 应支持终端唯一绑定机制，限制非授权设备访问业务系统；
 - 可设置终端访问白名单，限制数据暴露面；
 - 应根据终端风险等级配置访问权限，如公共终端只读、认证终端读写等差异化策略。

6.5.4 体验要求

- a) 多终端一致性体验保障
 - 个人计算机、移动、车载等终端应保持核心功能一致，保障跨端体验完整性；
 - 所有终端应支持自适应布局与响应式界面，适配 $\geq 1280 \times 720$ 屏幕；
 - 移动端应具备离线缓存、断点续传、网络切换等弱网优化能力。
 - b) 界面交互设计友好性
 - 操作界面应以图形化方式展现流程，支持拖拽、滑动、点选等直觉交互操作；
 - 动效应控制在帧率 $\geq 30\text{fps}$ ，避免视觉疲劳，突出操作重点；
 - 应统一颜色、图标、字体风格，保障在户外高光环境下可视性。
 - c) 用户学习曲线优化
 - 所有术语应通俗易懂，贴合农业操作人员使用习惯；
 - 初次登录应提供引导界面、悬浮说明、操作提示；
 - 建议提供“新手模式”与“专家模式”切换，适配不同层级用户。
 - d) 界面可定制与个性化能力
 - 应支持仪表板组件拖拽、快捷入口自定义与功能收藏机制；
 - 用户可配置个性化场景模板、仿真策略与路径规划方案；
 - 应支持主题（浅/深色）、字体大小、模块布局等 UI 参数的自定义配置。
-