

大连元利流体技术有限公司

MES 系统标准设计文档

System Design Specification

设计基线	内容
文档编号	YL-MES-DESIGN-001
系统版本	V1.1.0
文档版本	V1.1
基线日期	2026-07-24
设计性质	系统总体设计与详细设计基线
适用对象	架构、开发、实施、测试、运维和业务负责人

本文档描述 MES 系统的目标、边界、设计决策、业务域、数据模型、接口契约、状态机、非功能指标和验收基线。实现技术细节、现有过程名称和源码定位以《标准技术文档》为准。

1 设计总则

1.1 设计目标

以订单、物料、工艺、资源、任务、质量和工时为核心对象，形成可追溯的制造执行闭环。

将业务规则集中在服务端过程和领域边界内，前端负责交互、校验提示和视图编排。

通过角色、菜单、按钮和数据范围实现最小权限，所有关键变更可审计、可回退。

在不改变 SAP B1 主数据权威性的前提下，建立 MES 车间执行状态和异常反馈能力。

1.2 设计原则

原则	设计要求	验收证据
单一事实源	订单和物料以 SAP/接口主数据为源，执行事实以 MES 记录为源	主数据对账、字段映射表
状态可追溯	状态变更必须有前置状态、操作人、时间和来源	操作日志、状态流转测试
边界清晰	模块通过稳定对象和过程契约协作，不直接修改他域数据	依赖矩阵、接口清单
可恢复	数据库、文件、配置和发布包均有备份和回退路径	恢复演练记录
默认安全	服务端鉴权、参数校验、白名单和审计优先于前端限制	权限穿透测试、审计记录

1.3 范围与不在范围

范围	纳入内容	不纳入内容
纳入	MES Web、MESCommonBase、SQL Server、文件服务、SAP B1/TM/AGV/设备集成	MES 之外系统内部实现
纳入	生产计划、工艺、生产执行、质量、工时、设备、研发和看板	ERP 财务总账和人力资源主系统
约束	正式环境只按审批后的脚本和发布包变更	直接在正式库手工改业务数据

2 需求与业务域设计

2.1 业务域划分

业务域	职责边界	核心对象	输出
主数据与权限	人员、角色、菜单、工位、设备和基础参数	人员、角色、资源	可访问菜单和资源上下文
工艺工程	标准工艺、生产工艺、工序、图纸和工艺任务	工序、工艺版本、图纸	可下发的订单工艺路线
计划排产	按工艺和资源安排数量、工位、人员、日期	订单、工序任务、排产记录	未排产/已排产计划
生产执行	收料、开工、暂停、报工、送检、完工	任务、操作记录、报工记录	实时生产状态和完成数量
质量管理	检验标准、实测值、不合格处置和质量统计	检验任务、结果、处置单	合格/返工/让步/报废结论
工时与成本	操作工时、辅助工时、校验、修正、结算	工时记录、校验记录	可信工时和成本数据
集成与交付	ERP、库存、AGV、设备、文件和发货状态协同	接口消息、附件、交付状态	对账结果和交付视图

2.2 角色与责任

角色	允许的设计范围	关键责任
系统管理员	账号、角色、菜单、工位和基础配置	权限审批、账号生命周期、审计
工艺工程师	工序、标准工艺、生产工艺、图纸	工艺版本、启用状态、变更说明
计划员	排产、派工、计划时间和外协分组	资源冲突、计划冻结和调整原因
班组长/操作员	任务执行、报工、送检和异常说明	真实记录现场事实，不代录他人
质量人员	标准、检验、判定和不合格处置	检验结论、复检和质量追溯
运维/开发	部署、接口、数据库和故障处理	变更评审、备份恢复和技术支持

2.3 关键业务规则

标准工艺是可复用模板，生产工艺是订单或物料的执行版本；只有通过启用和完整性检查的工艺才可下发任务。

同一订单工序的排产数量不得超过可计划数量；计划时间、工位和指派对象变更必须保留操作记录。

生产任务状态必须遵循状态机；已完成或已关闭任务不得通过普通编辑入口回退。

检验不合格必须进入处置分支，不能仅修改显示状态绕过返工、让步或报废流程。

3 总体架构设计

3.1 逻辑架构

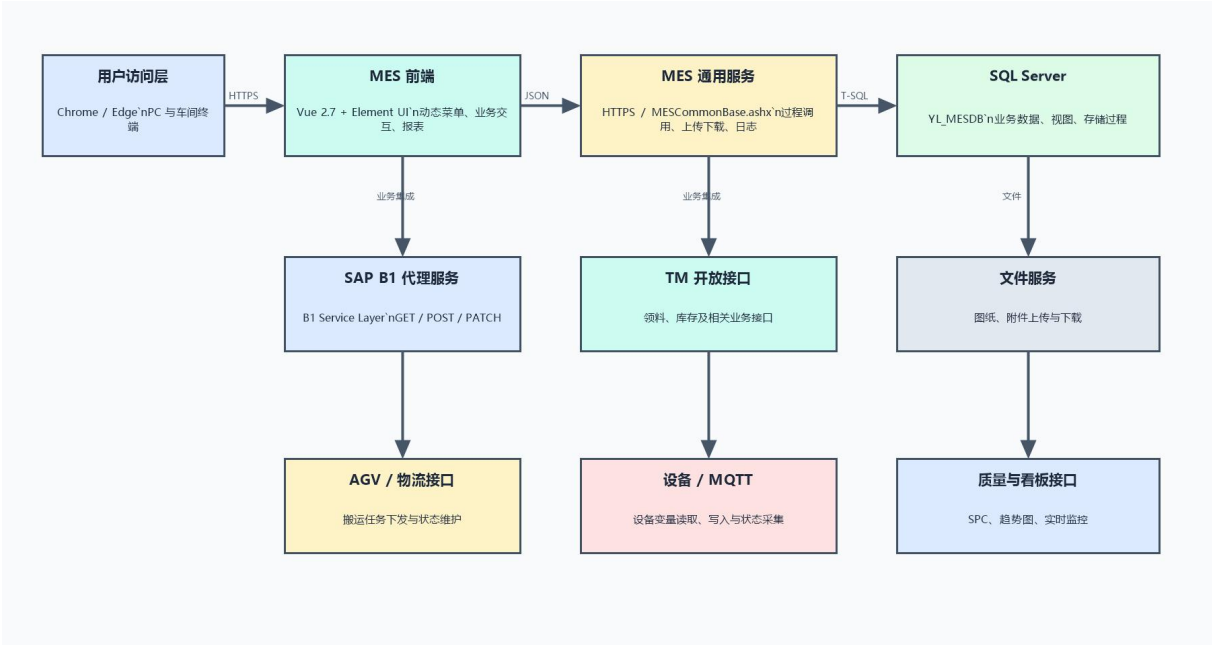


图 3-1 MES 逻辑架构

系统采用浏览器、MES Web 服务、统一数据库过程层和外部适配器分层。浏览器不直接连接数据库；业务请求携带用户和页面上下文，经服务端鉴权、参数处理和过程执行后返回结果。SAP B1、TM、AGV、设备和文件服务通过适配器隔离协议差异。

3.2 分层职责

层次	职责	禁止事项
表示层	页面、表格、弹窗、交互校验、分页和导出	不在前端伪造最终业务状态
应用服务层	身份上下文、请求编排、过程调用、异常和审计	不绕过权限直接暴露任意过程
领域过程层	状态转换、事务、校验、幂等、聚合查询	不依赖页面字段名称作为唯一契约
数据层	表、视图、索引、约束、日志和备份	正式环境手工修改业务表
集成适配层	SAP/TM/AGV/设备/文件协议转换与重试	把外部凭据下发到浏览器

3.3 设计决策记录

编号	决策	原因	影响
ADR-001	常规 MES 查询统一走过程调用	集中权限、事务和数据规则	需要维护过程契约和版本
ADR-002	外部系统通过适配器访问	隔离 SAP/TM/AGV 协议与凭据	需建设重试、超时和对账
ADR-003	附件采用元数据+文件实体	便于权限、版本和生命周期管理	禁止仅凭原始文件名定位
ADR-004	状态事实与统计视图分离	避免报表直接改生产状态	统计延迟和数据质量需监控

4 业务流程与状态设计

4.1 订单到交付主流程

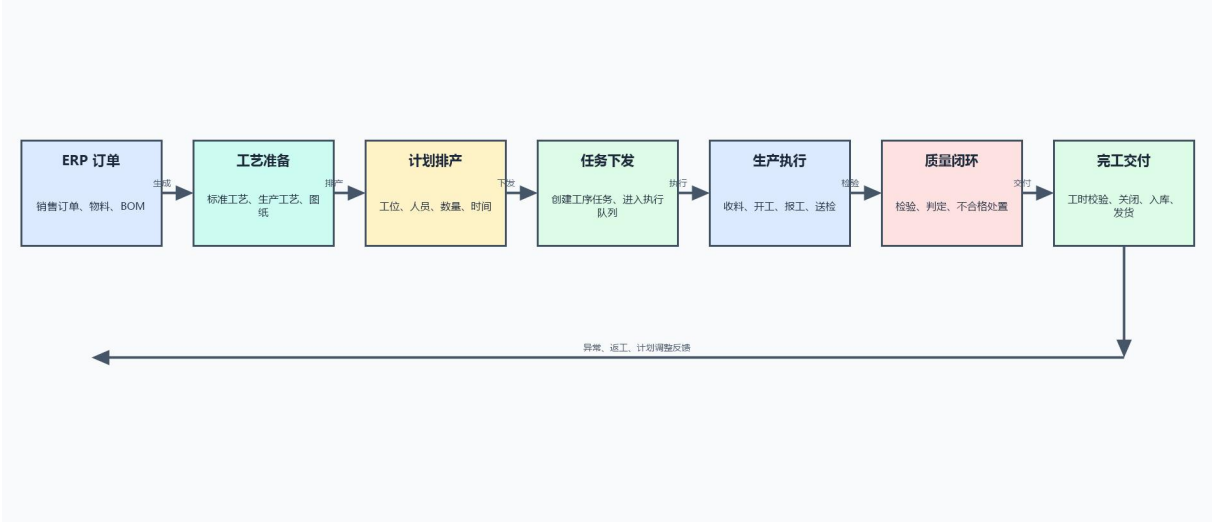


图 4-1 订单到交付业务主流程

- 接收订单和物料主数据，建立订单行、拆分内码及可视范围。
- 维护或选择标准工艺，生成订单生产工艺并校验工序顺序、数量和资源。
- 计划员为工序安排工位、人员、数量、计划开始和计划完成时间。
- 下发生产任务，任务进入可执行队列；执行过程中记录收料、开工、暂停、报工和送检。
- 质量结果和工时校验反馈任务状态，完成任务进入订单关闭、入库或发货协同。

4.2 生产任务状态机

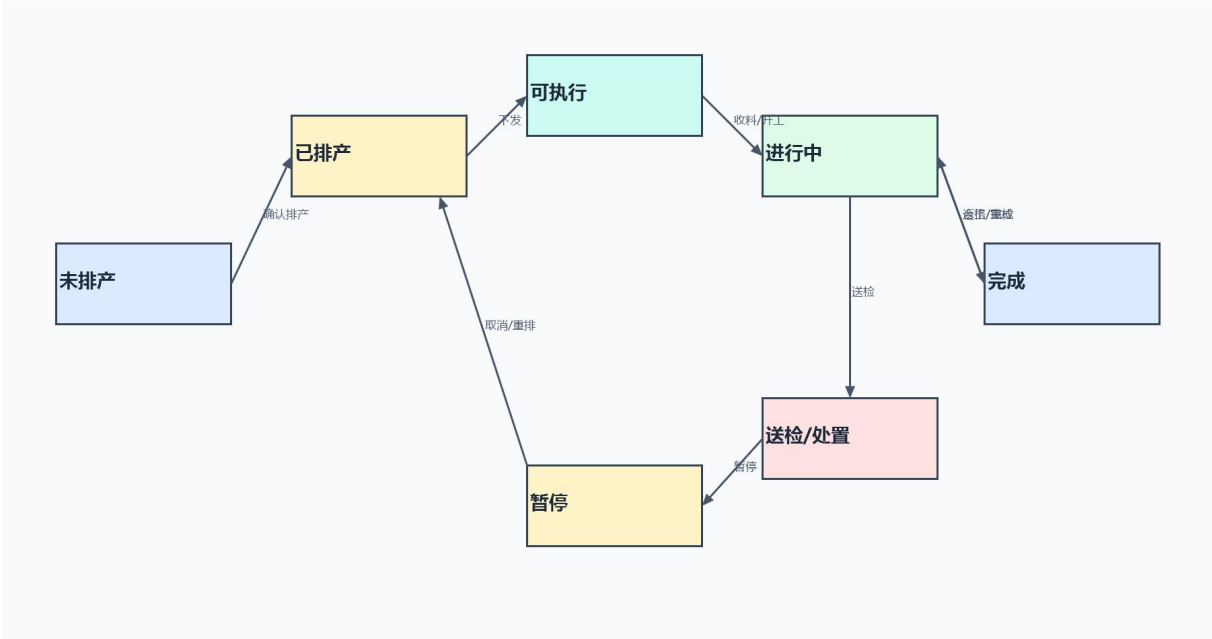


图 4-2 生产任务状态机

状态	允许前置	触发动作	允许后续
未排产	新建/计划调整	保存排产信息	已排产、取消
已排产	未排产	确认排产/派工	可执行、重排
可执行	已排产且工艺下发	收料或开工	进行中、异常
进行中	可执行/暂停	开始、恢复、报工	暂停、送检、完成
暂停	进行中	暂停并填写原因	进行中、取消
送检	进行中/报工完成	提交检验任务	完成、返工、让步、报废
完成	检验合格/无需检验	完成确认	关闭/入库

4.3 质量与工时闭环

生产事实、检验事实和工时事实分别记录，再由状态规则和统计视图汇总。工时结算不得直接把页面显示值当作事实；必须使用可校验的开始/结束记录、报工数量、辅助工时和修正原因。质量不合格结果必须保留检验依据及处置结论。

5 数据设计

5.1 核心实体关系

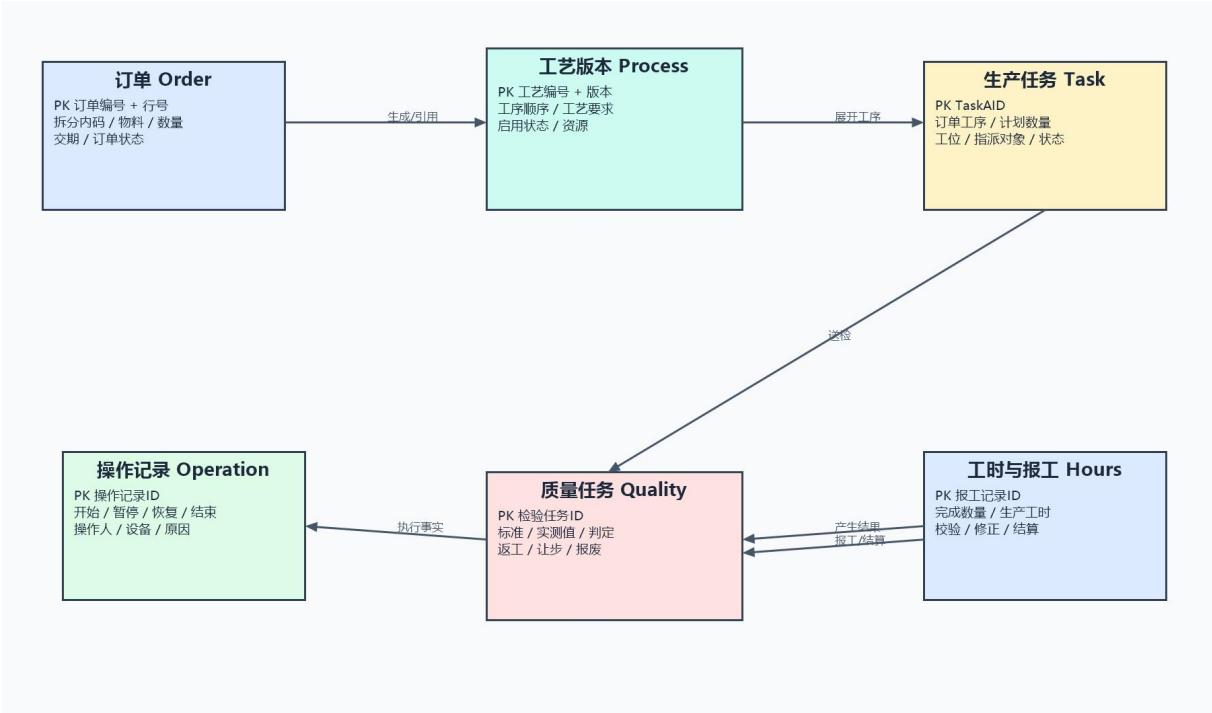


图 5-1 MES 核心实体关系图（ER）

实体	主标识	关键关系	生命周期
订单	订单编号+订单行号+拆分内码	包含物料、工艺和任务	接收、执行、关闭
工艺版本	工艺编号/版本/启用状态	由多个工序组成	草稿、启用、停用
生产任务	任务标识+订单工序	关联工位、人员、计划和报工	未排产至完成
操作记录	记录标识	关联任务和操作人	开始、暂停、恢复、结束
质量任务	检验任务标识	关联任务、标准和结果	待检、检验、处置、关闭
附件	文件标识/哈希	关联订单、物料、工艺或检验	上传、启用、归档

5.2 数据一致性设计

- 所有跨域写入必须由一个明确的业务过程完成，过程内控制事务边界和失败回滚。
- 查询结果必须明确粒度；一对多关联用于展示时要通过聚合、去重或明确版本条件避免任务行膨胀。
- 工艺库、任务表和统计视图应定义当前启用记录规则，禁止仅按订单号和工序号无条件关联多个版本。
- 接口重试必须具备业务幂等键，避免重复创建任务、重复发料、重复报工或重复检验。
- 删除优先采用停用、关闭或归档，保留历史记录和审计链。

5.3 数据字典基线

数据域	必须定义的字段	质量规则
订单	订单编号、行号、拆分内码、物料、数量、交期	组合标识唯一，数量非负
工艺	工艺编号、顺序、工艺要求、资源、启用、版本	同一范围仅一个当前启用版本
排产	计划数量、工位、指派对象、开始/完成时间、排产状态	计划数量不超可计划量，时间先后合法
执行	收料、开工、暂停、报工、完成数量	状态与操作记录一致
质量	检验类型、标准、实测值、判定、处置	结果可追溯至任务和人员
审计	用户、角色、页面、动作、参数摘要、结果、时间	禁止记录密码和敏感凭据

6 接口与集成设计

6.1 订单到任务接口时序

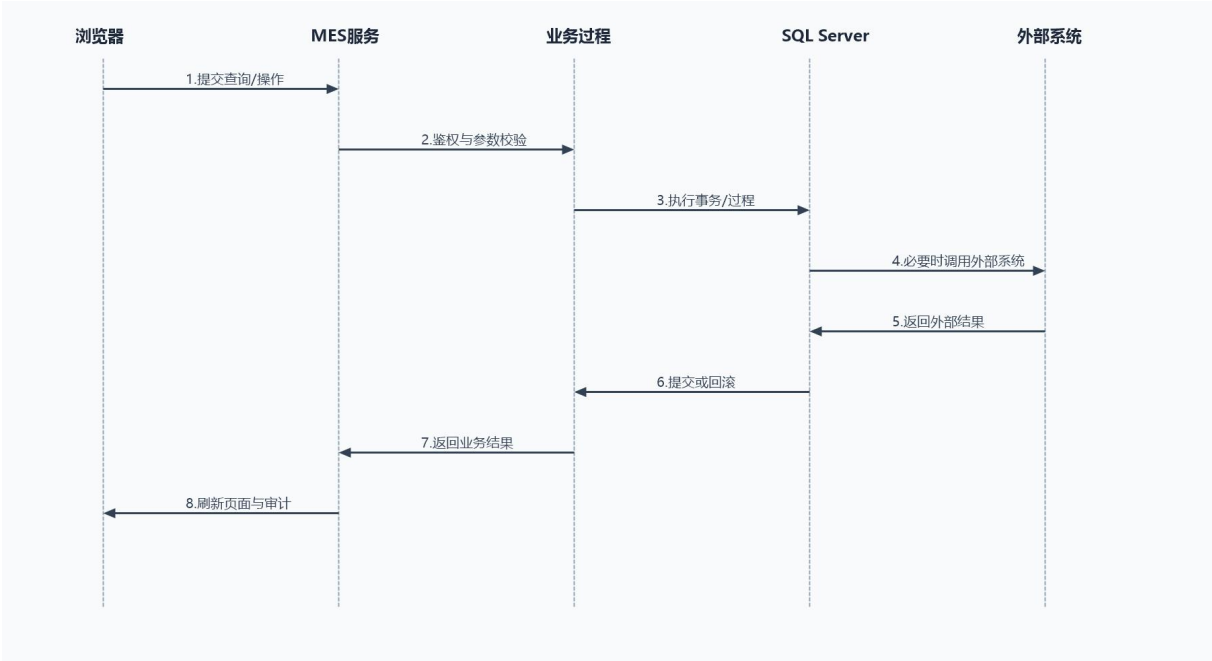


图 6-1 订单到生产任务的接口时序图

6.2 MES 通用接口契约

部分	设计约束	失败处理
请求上下文	用户标识、页面模块、动作类型、过程名、参数和分页信息	缺失身份或模块上下文直接拒绝
查询响应	数据、总数、错误码、错误消息和关联标识	分页总数必须与结果粒度一致
写入响应	成功标识、业务主键、状态和可重试提示	失败回滚并记录原因
权限	服务端校验菜单、按钮和数据范围	前端隐藏不等于授权
幂等	请求号或业务组合键可重复提交而不重复落库	重复请求返回原结果或明确冲突

6.3 外部集成边界

系统	方向	数据	设计要求
SAP B1	SAP→MES 为主	订单、物料、BOM、采购和库存	明确主数据权威方、同步窗口和对

系统	方向	数据	设计要求
			账
TM/库存	双向按场景	领料、库存、拣配和搬运	超时重试、幂等和人工补偿
AGV	MES→AGV 并回传	ContainerTransportOrder 及任务状态	避免重复下发，记录外部任务号
设备/MQTT	设备→MES, 受控写入	变量、状态和设备命令	Tag 白名单、范围校验和审计
文件服务	MES↔ 文件服务	图纸、工艺附件、检验附件	权限一致、哈希校验、版本化

6.4 超时、重试和对账

同步查询和写入采用分类超时；外部调用失败不得直接伪造成功状态。可重试错误使用指数退避和幂等键，业务不可重试错误进入人工处理队列。每日对订单、任务、库存、AGV 和文件实体执行数量及状态对账，差异生成可关闭的问题单。

7 安全与权限设计

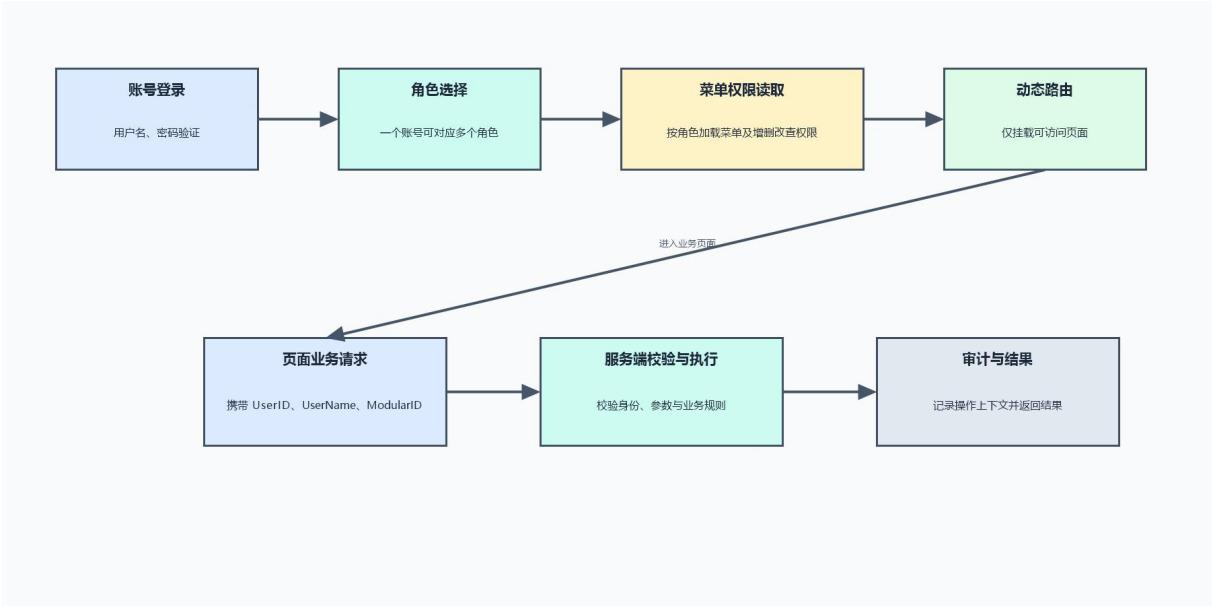


图 7-1 身份与权限设计

7.1 权限模型

控制点	设计
身份认证	账号、密码、会话和登录失败控制；禁止共享账号
角色授权	用户可关联多个角色，权限取角色授权集合并按数据范围收敛
菜单/按钮	菜单决定入口，按钮决定动作；查询、编辑、确认、删除分别授权
数据范围	按组织、工位、班组、订单或资源限制可见和可操作数据
审计	记录登录、权限变更、关键写入、接口调用、设备写入和异常

7.2 安全基线

正式凭据只保存在服务端配置或密钥系统，前端包、日志和文档不得出现密码。

SQL、文件路径、设备 Tag、外部命令和过程调用采用白名单与参数化策略。

图纸和附件下载必须经过业务权限校验，不能依赖公开目录地址。

设备写入、AGV 下发、订单关闭和质量处置属于高风险动作，应二次确认并记录前后值。

安全事件按账号、请求号、页面、时间、IP 和业务主键关联，支持追溯。

8 部署与运行设计

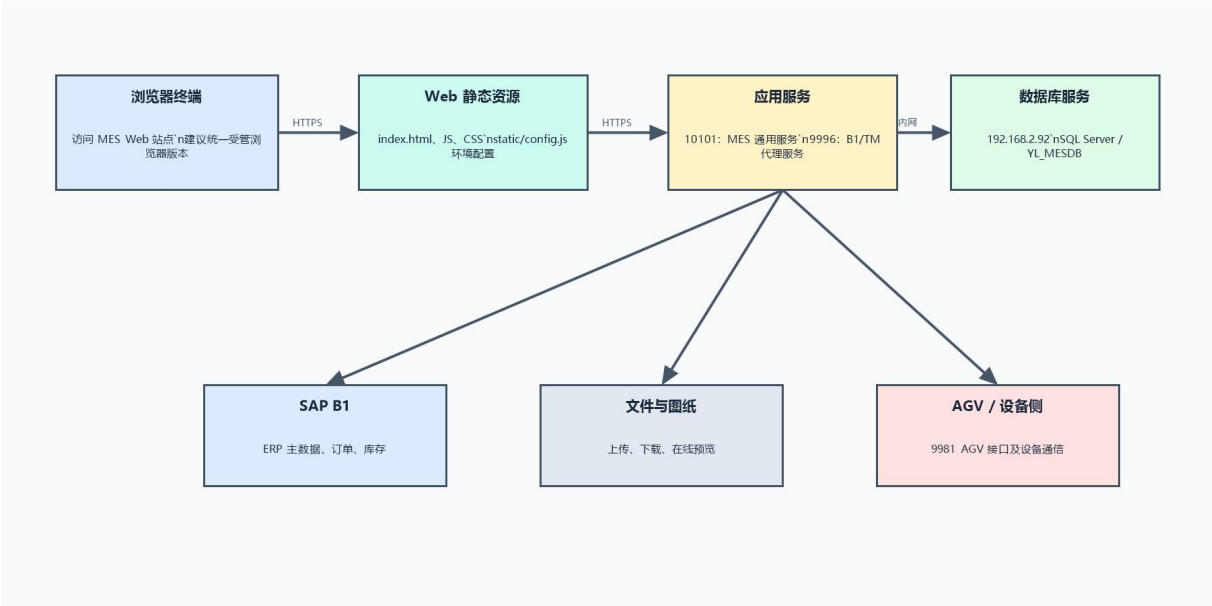


图 8-1 正式环境部署拓扑

8.1 环境划分

环境	用途	数据策略	发布要求
开发	功能开发和单元调试	脱敏或模拟数据	允许快速迭代
测试/预发布	集成、回归、性能和权限验证	接近正式结构的测试数据	必须有版本化构建包
正式	生产执行和经营数据	正式备份、审批和审计	变更窗口、回退包和 应急联系人齐备

8.2 发布设计

构建阶段锁定依赖、生成版本号和校验文件；发布包包含 dist、运行时配置模板和回退包。

数据库脚本先在测试库执行并验证，再按审批顺序执行正式脚本；脚本必须可重复检查、可审计。

发布前备份数据库、配置、文件索引和当前前端包，发布后执行登录、查询、关键写入、外部接口和回退冒烟。

发布失败时先停止继续变更，依据故障范围选择前端回退、脚本回退或数据补偿，并保留现场日志。

8.3 可用性和恢复目标

指标	设计基线	验证方式
RPO	核心数据库按备份策略可恢复；日志和附件纳入备份范围	备份恢复演练
RTO	按故障等级定义恢复时限，关键生产入口优先	故障演练记录
查询性能	常用列表在目标数据量下满足页面交互时延	代表性数据压测
并发控制	同一任务的排产、报工、关闭和质量处置避免并发覆盖	冲突测试、版本校验
容量	每月记录数据库、附件、日志和核心表增长率	容量趋势报告

9 测试与验收设计

9.1 测试层次

层次	对象	通过标准
单元/过程测试	校验、状态转换、计算和异常分支	规则边界和回滚正确
接口测试	MES 通用、SAP/TM、AGV、设备和文件接口	契约、超时、重试和幂等通过
集成测试	订单→工艺→排产→执行→质量→交付	主链路和失败链路可追踪
权限测试	角色、按钮、数据范围和越权路径	无越权、无水平或垂直越权
性能/恢复	并发、慢查询、备份恢复和发布回退	达到指标且演练可重复
用户验收	计划员、工艺、班组、质量、管理人员场景	关键岗位签字确认

9.2 核心验收场景

订单导入后生成标准工艺和生产工艺，验证保存、启用、下发、编辑和版本边界。

机加件和装配件分别排产，验证工位、人员、数量、计划时间、外协分组和已/未排产查询粒度。

执行收料、开工、暂停、恢复、报工、送检和完成，验证状态机、数量和工时记录。

质量合格、不合格、返工、让步和报废分别验证下游状态和追溯。

外部接口成功、超时、重复提交和部分成功分别验证重试、对账和人工补偿。

权限矩阵逐角色验证查询、编辑、确认、删除、设备写入和附件下载。

9.3 验收交付物

交付物	内容	责任方
设计基线	架构、数据、接口、状态和非功能要求	架构/产品
测试证据	用例、结果、缺陷、性能和恢复记录	测试/运维
变更证据	版本号、审批、脚本、备份和回退记录	开发/实施
运行证据	监控、告警、权限、审计和对账结果	运维/业务

10 设计风险与演进路线

优先级	设计风险	影响	演进动作
P0	前端上下文不足或服务端权限不强制	越权和审计失效	统一服务端鉴权、权限穿透测试和审计关联
P1	过程与页面字段耦合，缺少版本化契约	升级回归和接口兼容风险	建立接口契约、过程版本和自动化回归
P1	工艺版本一对多关联导致任务结果膨胀	计划数量、报表和排产判断失真	明确当前启用版本，查询按版本去重并建立数据质量检查
P1	外部接口缺乏统一幂等与补偿	重复任务或状态不一致	统一请求号、对账任务和人工补偿队列
P2	大页面和大过程维护成本高	变更影响面大	按业务域拆分服务、查询和前端页面
P2	统计和事实数据边界不清	报表与现场状态不一致	建立数据产品层和指标口径管理

10.1 分阶段演进

阶段	重点	完成标志
阶段一：基线治理	权限、凭据、过程契约、工艺版本和备份恢复	风险项有负责人和验证记录
阶段二：稳定性提升	接口幂等、对账、监控、慢查询和自动化回归	关键链路可观测、可恢复
阶段三：领域演进	按业务域拆分、统一状态服务、数据产品和容量治理	新功能不依赖跨域直接改表
阶段四：智能优化	负荷预测、异常推荐、设备分析和工艺成本优化	模型结果可解释且不绕过业务审批

附录 A 设计追踪矩阵

需求/目标	设计章节	实现/验证对象	验收证据
订单可追溯	2、4、5	订单、任务、操作、质量和附件	全流程主键追踪
工艺可复用	2、4、5	标准工艺、生产工艺、启用版本	工艺生成和版本测试
计划可执行	4、5	工序任务、资源、计划时间	排产冲突和状态测试
生产可核算	4、5	操作记录、报工、工时校验	工时计算和修正记录
质量可闭环	4、5、6	检验任务、结果、处置和交付	不合格处置链路
系统可运营	7、8、9、10	权限、日志、监控、备份和回退	演练、审计和验收清单

附录 B 设计输入与输出

类别	输入	输出
业务输入	订单、工艺、资源、质量和交付规则	业务域模型、状态机和流程
技术输入	前端源码、服务接口、数据库对象、运行配置	分层架构、接口边界和部署拓扑
运营输入	权限矩阵、备份策略、监控和应急要求	安全、恢复、运维和验收设计
变更输入	缺陷、需求、数据质量和容量趋势	ADR、风险项和演进路线