

01 检索业务知识

HUMAN GATE

现有实现：POST /api/search 的召回阶段

Purpose | 目的 从站点沉淀库与打包演示知识库召回相关条目，为后续判断提供可追溯证据；本动作本身不形成最终业务结论。

Input | 输入

必填：query (2-4000 字)。可选：product、category、order_type、case_notes、model；当前检索请求不接收案例号。

Precondition | 前置条件

服务、SQLite 与知识库可用；模型解析为启用项或默认项。demo-local 默认零外网；API 模式须另配 Key。

Role | 角色

业务角色：一线售后 / 维修人员。现状：检索接口未做用户身份或角色鉴权，仅适用于本地演示边界。

AI权限 | AI Authority

可分词、召回、精排并归纳；不得编造来源、维修参数、备件料号；不得回写工单、定责或自动执行处理。

Human Gate | 人工闸门

人工主动发起；使用前核对产品、来源、证据与风险。无匹配、跨机型或信息不足时，不得直接视为最终方案。

System Action | 系统动作

合并本地库与演示外部库候选，返回 matches / evidence / diagnosis / steps / verify，并写入一次检索埋点。

Audit | 审计

usage_logs 记录时间、action=search、产品、分类、耗时、命中数、模型调用 / 错误、客户端与模型；不记录 query 原文。

Failure | 失败处理

输入不合法返回 422；模型不可用时降级为关键词召回并带 llm_error；无候选时返回 no_match 与通用建议或空结果。

02 生成处理建议

HUMAN GATE

现有实现：与检索共用同一 /api/search 事务

Purpose | 目的 把案例上下文与候选证据转成结构化故障判断、操作步骤、资源和核实提示，供人工决策与沟通使用。

Input | 输入

沿用检索请求中的案例上下文，并使用召回候选。当前没有独立的“建议生成”业务接口；建议与检索结果一次返回。

Precondition | 前置条件

引用型建议须存在候选知识条目；无候选只能给明确标注的通用建议。模型与规则输出必须通过服务端清洗。

Role | 角色

业务角色：处理人员 / 技术支持。现状：系统未校验操作者资格，也未区分查看建议与采纳建议的权限。

AI权限 | AI Authority

可生成有序步骤、资源与风险提示；引用必须属于候选集。无依据内容只能标为“经验性建议”，不能作授权结论。

Human Gate | 人工闸门

人工逐条审阅。need_recheck、经验性步骤、机型差异、证据不足或高风险操作必须回源核实后方可采用。

System Action | 系统动作

白名单清洗字段与长度；校验步骤引用、剔除无效引用并降级；核验 evidence 来源后合成兼容的 answer。

Audit | 审计

沿用本次 search 埋点，仅留操作级指标。当前未留：完整提示词、建议全文、逐条采纳 / 拒绝决定与最终执行结果。

Failure | 失败处理

模型 / JSON 解析失败时保留关键词候选但不返回结构化步骤；虚构引用被清空并降级；失败不得触发任何自动执行。

03 提交 AI 审查质量反馈

HUMAN GATE

现有实现: POST /api/review/feedback (AI审查质量反馈)

Purpose | 目的 记录人工对 AI 案例审查的准确性评价与原因，形成质量反馈闭环。它不是最终工单裁决，也不会改变原审查结论。

Input | 输入

review_log_id≥0、review_uid、case_id、遗留 order_no；accuracy 必须为 accurate / partial / inaccurate；reason 最长 2000 字。

Role | 角色

业务角色：人工复核人员 / 处理人员。现状：提交接口无登录和角色鉴权；只有后台统计读取需要管理令牌。

Human Gate | 人工闸门

必须由人工点击并选择评价，可补充误报 / 漏报原因；案例号需人工核对，设备 SN 不得替代案例号。

Audit | 审计

记录时间、review_log_id、review_uid、case_id、遗留 order_no、accuracy、reason 与客户端；与模块 A 反馈表隔离。

Precondition | 前置条件

页面已获得一次审查结果并保留其标识。现状缺口：API 未校验被引用审查记录是否存在、是否属于当前操作者。

AI权限 | AI Authority

AI 对提交动作无权限：不得选择准确性、代写事实原因或自动提交。AI 仅提供被评价的审查输出。

System Action | 系统动作

写入 review_feedbacks 并返回 ok=true；成功后前端禁用本轮反馈按钮。不会回写工单，也不会自动改写 review_logs。

Failure | 失败处理

字段不合法返回 422；数据库 / 请求失败时前端提示并允许重试。当前无：幂等键、重复提交防护、引用完整性校验。

共同治理边界 | Shared Control Boundary

01 决策辅助

AI 输出是证据与建议，不是定责、放行或最终处理决定。

02 人工负责

检索采用、建议执行与质量反馈均由人工明确触发并承担判断责任。

03 本地演示

无工单系统回写；默认 demo-local 与虚构产品 / 演示知识库，不代表生产集成。

04 控制缺口

当前缺用户 / 角色鉴权、反馈关联校验与幂等、建议采纳及最终结果审计。