

DIRECTOR · 工作内项目 · 参与/协助

Director：内容生产工作台 的边界、迭代与真实失败

模型、知识库与执行器都不稳定时，生产系统如何继续工作？

01 问题

旧流程：人在多个工具之间搬运上下文

短视频编导的工作流大致是：找选题 → 查历史脚本与热点 → 写大纲 → 生成脚本 → 改稿 → 交付。在没有系统之前，这些步骤分散在文档、表格、聊天窗口和若干 AI 工具之间。

这带来三类真实问题：

- **上下文丢失**：每次换工具都要重新描述需求，版本之间无法比较。
- **失败不可见**：模型调用失败、RAG 检索为空、知识库同步失败都被包装成“成功”，生成出低质脚本。
- **无法追溯**：为什么选用某个选题、某段引用来自哪里、V2 改了什么，都没有记录。

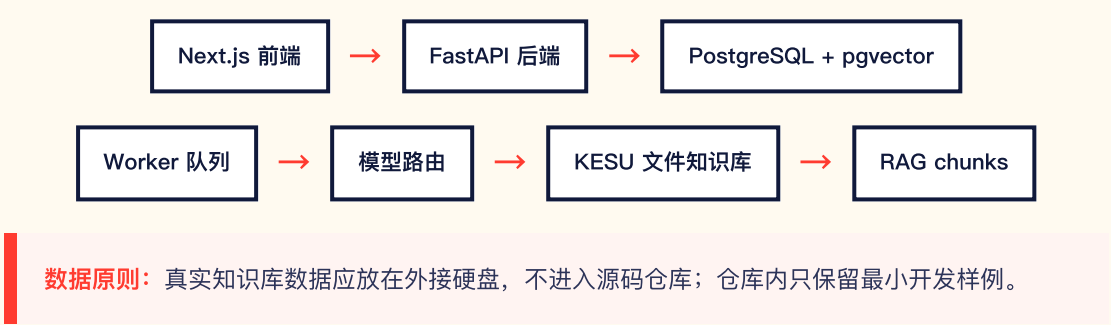
Director 的目标不是让 AI 替编导写完，而是把“生成—编辑—反馈—沉淀”变成可追溯、可回退、可审计的流程。

本地单机 MVP，不是公开 SaaS

Director 是公司内部短视频编导 Agent 系统的本地单机 MVP。它明确不服务外部用户，数据不外流，真实知识库通过外接硬盘挂载。

在范围内	不在范围内
脚本大纲确认、脚本生成、AI 改稿、revision 版本、知识提案审批、参考视频拆解、单机 worker 队列、pgvector 检索。	公网部署、多租户、实时协作、自动发布到平台、替代编导最终判断、无人值守自动执行。

技术栈



22 个路由，6 条核心调用链

根据 PROJECT_RUNTIME_MAP 的只读审计，后端 22 个路由全部注册并活跃，六大能力调用链完整：

- generate script: 脚本生成器 → 模型路由 → LLM provider
- knowledge proposal: AI 知识提案 → 审核 → Relay → 知识库
- revision: 版本历史自动落库
- feedback: 脚本反馈
- pilot event: 行为事件记录
- script session: 会话管理

模型路由

按任务类型选择 provider: 缺 key 时返回明确标记的失败回退 (fallback=true)，而不是静默假数据。
Phase 2.8 后，真实模型全部不可用时会抛异常，不再存“成功”脚本。

知识提案 governance

Remote AI 不能直写知识库。所有回传知识走 Knowledge Proposal: Pending Review → Approve → Admin submit → Relay → skill_iteration → Knowledge Base。

Director 2.0：从“找功能”到“说需求”

在原有 V1 继续生产的同时，我在旁侧提出 2.0 方案：一个对话式入口，员工直接说需求，系统拆解任务并显示进度。



方案原型：首页对话式入口 + 常用任务快捷按钮

一次完整任务：找选题 → 查知识库 → 写稿 → 改稿



方案原型：员工说需求后，系统按任务步骤推进并显示当前状态

说明：以上两页为改造方案原型，不是真实生产界面。真实生产界面包含客户与业务数据，已脱敏，不对外展示。

从“静默成功”到“有证据的健康状态”

PHASE 2.8

消除静默成功

model_router 4 处失败分支由“返回占位假数据”改为抛异常；生成失败不再存 status=generated 假脚本；知识同步失败不伪装 applied。

PHASE 2.9

让系统自己报告健康状态

发现 model_call_logs 已约 95% 建成；补齐 fallback 语义与聚合查询端点，失败路径也写入日志。

PHASE 6.2

Pilot 数据指标

基于 generated_scripts、script_revisions、pilot_events 定义 DAU、日生成/修改/接受/拒绝量，不新增埋点。

能力存在 ≠ 用户可用

前端真实生成入口断裂 PROJECT_RUNTIME_MAP 记录：前端 product_brief_id 为空时返回 422，生成链路实际不可达。	迁移系统缺失 无 alembic、无自建迁移文件、无 Base.metadata.create_all；schema 漂移对代码不可见。
应用内无调度 知识提案重试、周期性任务依赖外部 cron 主动调端点，否则静默不跑。	死代码 pilot_event 三个 list 函数、knowledge_proposal 两个 405 桩、部分前端组件零调用。

2026-07-19 E2E 验收结果

真实搜索触发抖音安全验证，系统按设计停止并熔断设备。结论为“风控路径通过、成功结果路径受平台阻断”，不能标记完整 E2E 通过。

07 我的角色

参与，而非主导

我在 Director 中的参与范围可核实的包括：

- 需求梳理与业务流程讨论；
- 技术决策方案撰写（docs/18_TECH_DECISIONS_AND_TRADEOFFS.md：Skill+API 结合、母包+子包、Markdown 权威源、退修后人工审核等）；
- Director 2.0 改造方案与原型图（prototype_home.png / prototype_flow.png）；
- 生成工作流测试、验收记录与 Pilot 指标体系梳理。

边界：客户名、账号、密钥、内部 URL 与真实业务数据已遮盖。页面与 PDF 中不写“Director 由我主导”。仓库元数据无法给出逐提交署名，因此只写“参与/协助”。