A14 基于 Agent 的流程工业建模数据智能优选与闭环寻优系统

项目概要介绍

2026 浙江省服务外包创新创业大赛 · 企业命题【和利时】

命题方向：智能计算 | 题目类别：应用类 | 产品名：ProcessPilot 工业辨识数据智能优选工作台

一、项目背景与行业痛点

流程工业（化工、炼化、电力、冶金、制药、造纸等）的先进控制（APC）已成为企业节能减排、提质增效的核心手段。然而 APC 策略的成功部署，高度依赖底层被控对象数学模型（系统辨识）的精度；而建模的成败，从根本上取决于输入数据的质量。面对真实工业场景中强噪声、多变量强耦合与复杂时滞并存的时序数据，传统依赖人工调参、缺乏即时反馈的预处理方式，已成为制约建模效率与精度的核心瓶颈。

- **有效样本被淹没：**工厂 90% 以上时间处于稳态运行，真正富含动态价值的有效辨识样本往往被海量无效的稳态平移段所淹没，工程师需手动从数月数据中"淘金"。
- **试错周期长：**预处理的好坏只能在最终建模后才能验证——清洗力度多大、截取哪段数据、时滞如何补偿，全部依赖工程师经验反复试错，单次迭代常以天计，且极难寻得全局最优。
- **企业诉求迫切：**命题企业杭州和利时自动化有限公司是国内唯一入选 ARC"全球自动化 50 强"的中国企业，每年承担 8000 余项智能化改造工程，对生产过程"安、稳、长、满、优"的诉求极为迫切，现场亟需把"数据→模型"这条路走通、走优。

二、产品定位：APC 前端加速器

本系统定位为 APC 前端加速器——不替代 APC，而是补上 APC 成功部署的前置缺口：在建模之前，自动完成"数据优选 + 闭环寻优"，交付高质量建模数据集与专业评估报告，让现场工程师从反复试错中解放出来。

- **无缝衔接现场：**OPC UA 连接器可直连 HOLLiAS DCS（只读不写，保障生产安全），成果可导出为和利时 MPC 组态格式（FOPDT 参数 + 阶跃响应 + 增益调度表），直接下装现场。
- **一键式自动化：**把"数据预处理 + 系统辨识 + 策略寻优"这一原本靠人反复试错的环节，变成由自然语言驱动的一键式自动化流水线，建模周期从"天级"压缩到"分钟级"。
- **可落地可验证：**所有核心数字均来自代码实测与金标准验证体系（21 数据集 / 133 项判定 / 8 缺陷闭环 / 留出集 8 组梯度泛化），而非纸面宣称。

三、核心思路：Agent 驱动的"一键式"闭环流水线

系统引入智能体（Agent）技术作为"智能中枢"：用户用自然语言下达指令，Agent 解析业务意图、自动编排并调度底层算法模块，再以辨识效果为反馈自动闭环寻优，最终自动生成专业报告与高质量数据集，形成"提问—编排—执行—反馈—交付"的完整闭环。

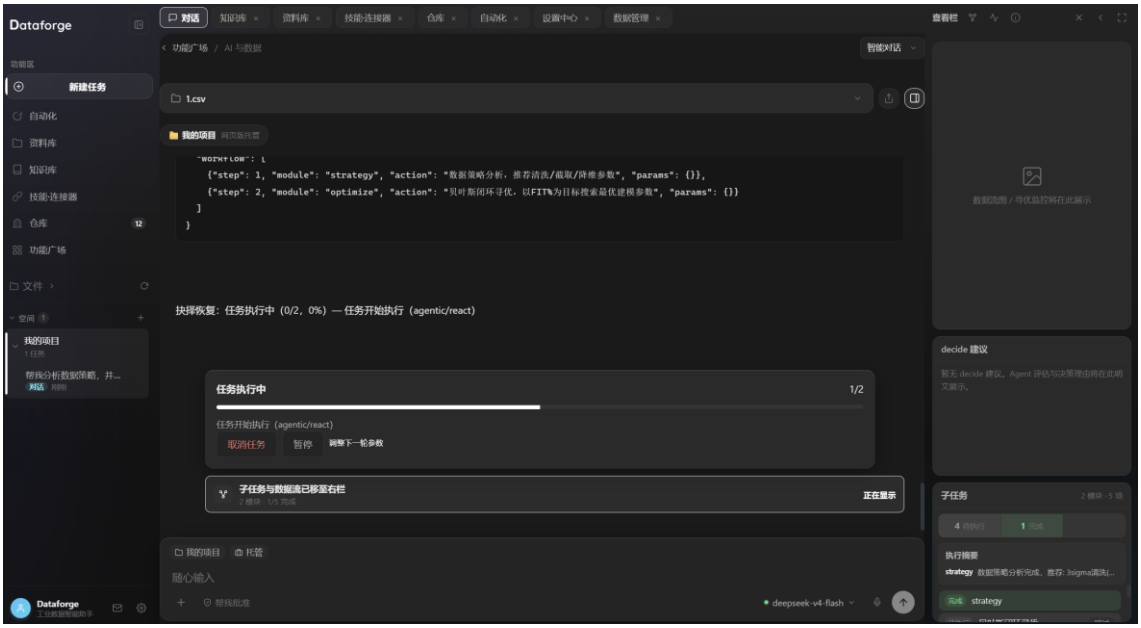
用户自然语言指令 → Agent 智能组装流水线 → 清洗 • 截取 • 时滞 • 降维 • 辨识 → 辨识效果反馈 → 不满足则自动调参循环 → 满足则输出最优数据集 + 图文报告

系统采用五层技术架构（对应赛题"技术要求与指标"的 5 大模块），自上而下依次为：

架构层	核心能力
① 前端交互层	对话式输入框 + 多变量时序数据管理页 + 可视化展示区（Vue 3 + Element Plus + ECharts，30 个顶层视图 + 6 个向导步骤、31 条路由）
② Agent 智能中枢层	接入 DeepSeek / Ollama 等开源大模型，意图解析 + 两图 + 降级子图物理隔离调度（durable 确定性 / 降级子图 自主 / react 推理）+ 决策卡人机共审
③ 工业核心算法库	Python 构建 19 个算法模块：数据清洗 / 动态段截取 / 质量评分 / 时滞分析 / 共线性降维 / ARX • OE 辨识 / FOPDT 工程化 / 贝叶斯寻优，标准化参数接口

④ 流水线引擎与闭环反馈	执行 Agent 生成的工作流，捕获辨识 FIT% 指标，贝叶斯/TPE/遗传/网格四策略自动循环调整前置处理参数
⑤ 结果解释与报告层	结果回传大模型，生成工程视角自然语言报告 + 12 类可视化图表 + Word/PDF/PPTX 三格式导出

系统前端采用 Vue 3 + Element Plus + ECharts 构建，核心界面如下所示。用户通过对话式交互下达自然语言指令，Agent 实时展示思考过程与执行进度，右侧可视化区同步呈现数据波形与分析图表。



图：智能对话主界面（Agent 交互 + 流式输出 + 执行进度）

四、七大任务能力概览（对照赛题要求）

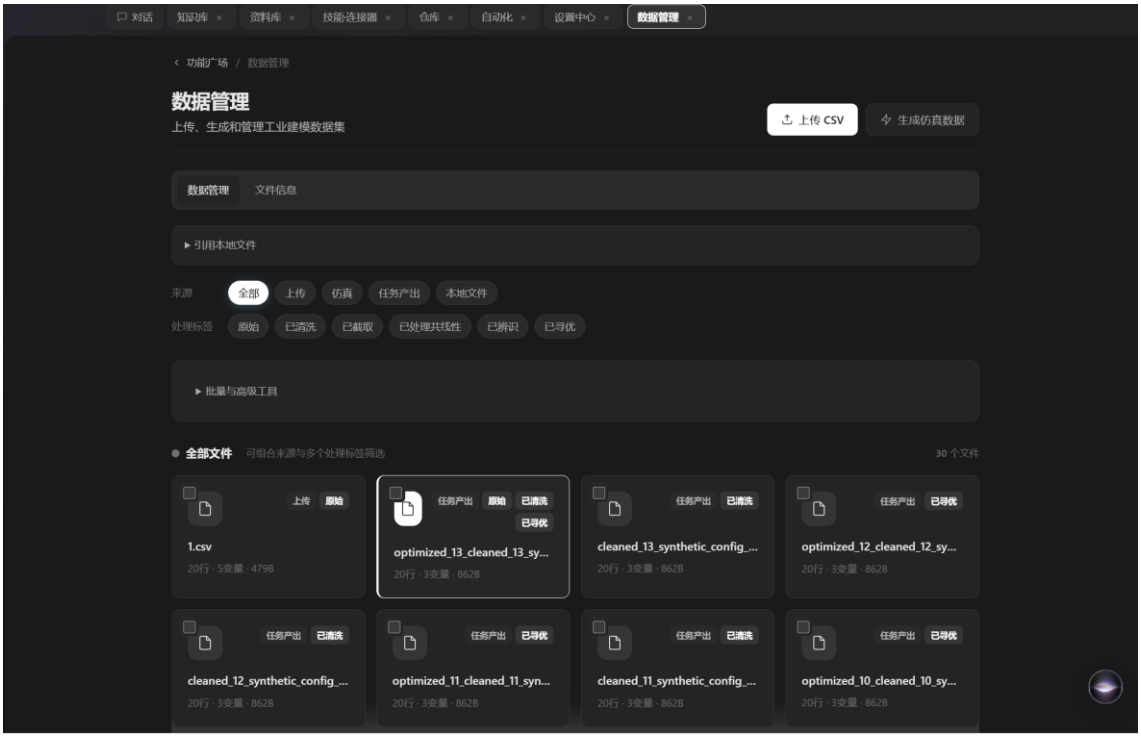
系统完整覆盖赛题全部 7 项任务清单，多项能力超出赛题基本要求：

赛题任务	实现情况与实测亮点
任务 1 数据文件管理	多变量 CSV 上传/查看/删除/管理 + 内置仿真测试集生成工具；超额支持 GB 级分片上传（实测 2.08GB 通过）、文件血缘链与版本回滚、413 预检中间件（拒收响应 6ms）
任务 2	异构数据重采样 / 时间戳对齐 / 3σ • IQR 异常剔除 / 缺失插补；守卫族 9

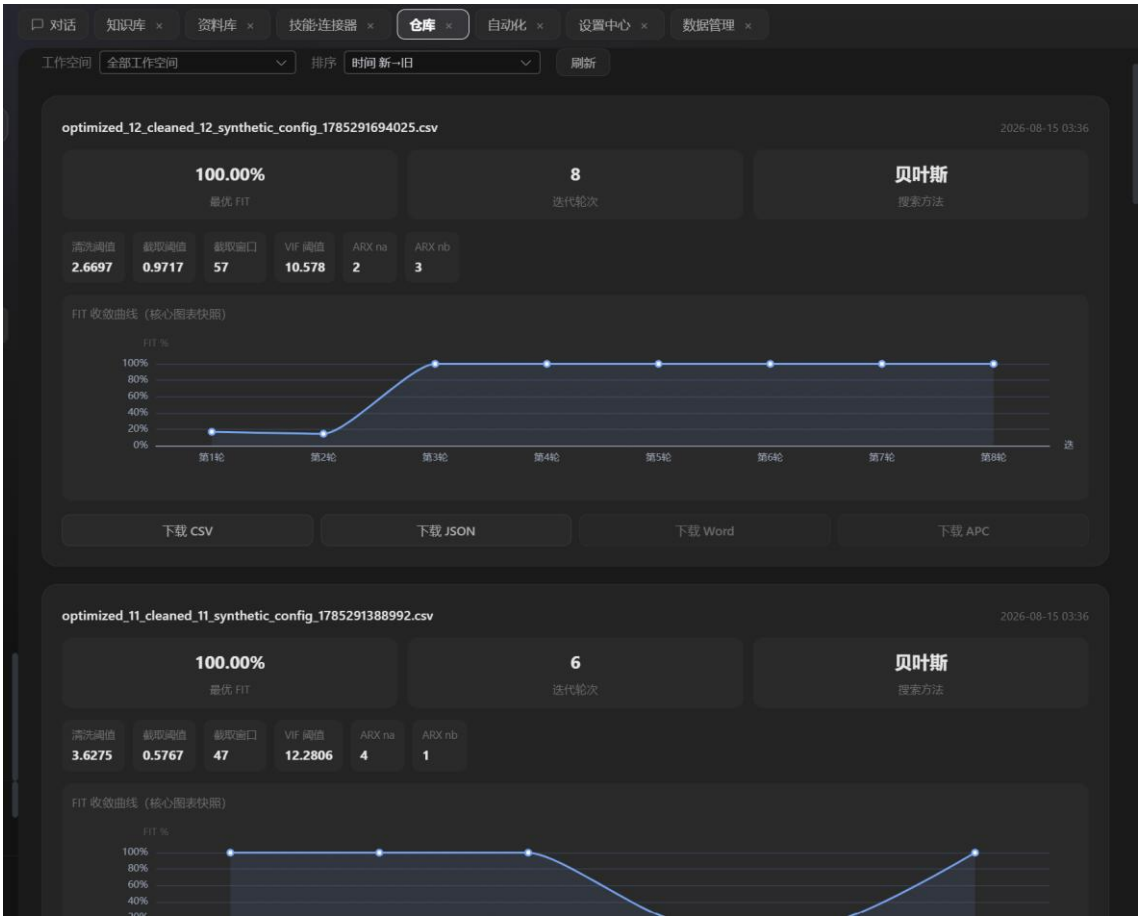
智能规整与清洗	件，每件对应一个真实缺陷闭环——HAI attack 攻击标记逐字符级零改写、UCI 相关系数从 +0.886 恢复为物理正确的 -0.574
任务 3 高信噪比筛选 ⭐	Rhinehart 稳态/瞬态自动识别（IEEE ACC 2013 方法）+ 三维质量评分（SNR + 动态丰度 + 平稳性）排序；反例法论证：全量建模 K 偏差 9 倍、τ 偏差 72 倍，截取动态段后 K 误差仅 1.2%
任务 4 时滞与共线性解耦	互相关函数法时滞估算 + 时滞矩阵 + 自动补偿；VIF 方差膨胀因子检测 + 冗余变量剔除 + PCA 降维；FOPDT 一阶加纯滞后模型工程化交付（跨任务交付物，承接任务 5 辨识结果）
任务 5 一键闭环寻优 ⭐	以辨识 FIT% 为目标函数，贝叶斯（GP Matern 2.5 + EI）/ TPE / 遗传 / 网格四策略自动寻优；辨识结果自动转换为 FOPDT 工程化模型（增益 K / 时间常数 τ / 纯滞后 θ）；实测合成数据 K 回收率从 49.2% 提升至 81.09%，UCI FPE 改善 227→409 倍
任务 6 专家级图文报告	12 类图表（清洗对比 / 动态段高亮 / 相关热力图 / 时滞矩阵 / 收敛曲线 / 预测对比 / AB 对比 / 响应面 3D 等）+ LLM 智能选图撰写 + Word / PDF / PPTX 三格式导出
任务 7 高质量数据导出	一键导出优选数据集（CSV/Parquet）+ 工作流 Manifest + Trial 历史 + 模型指标；超额支持和利时 APC 组态包导出（apc_params.csv 15 列 FOPDT 参数 + 200 点阶跃响应 + 增益调度表）

注：⭐ 标记为赛题核心技术得分点。

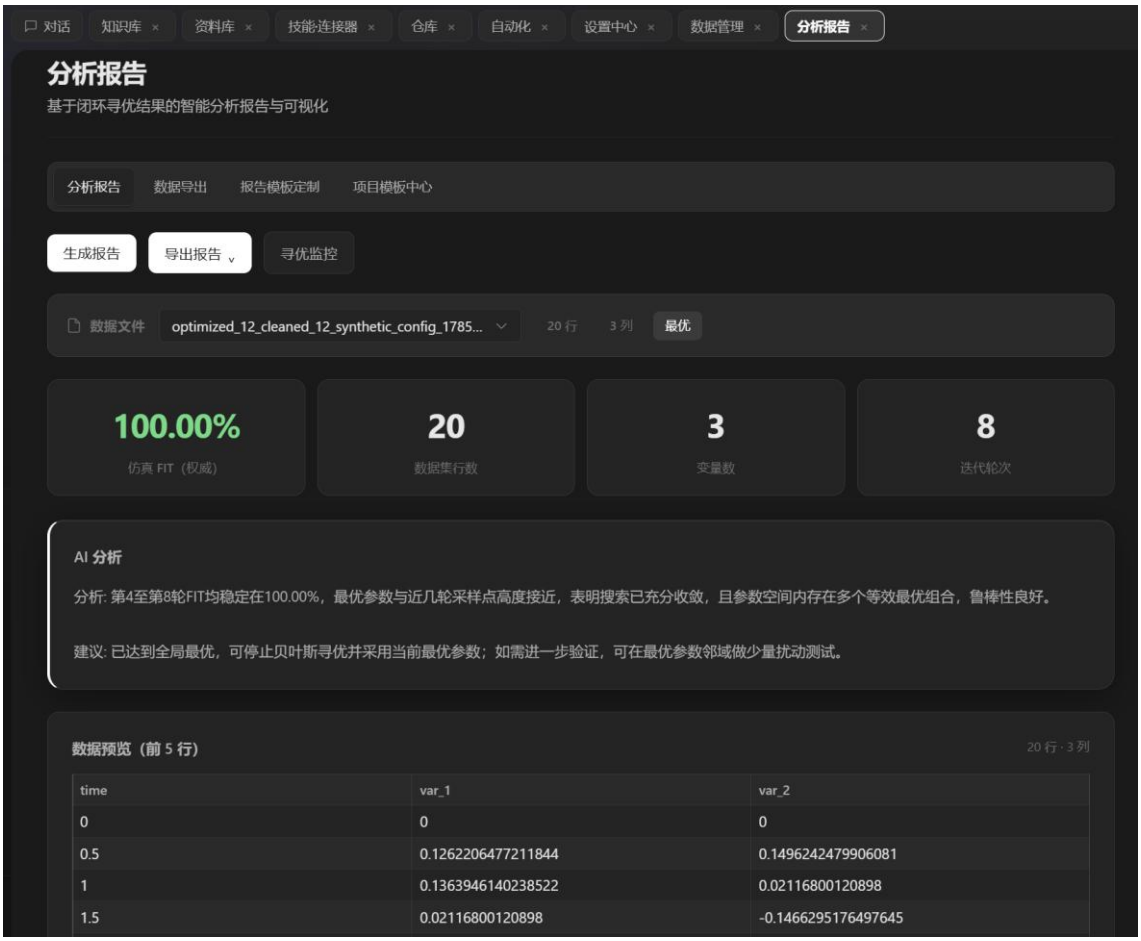
以下为系统核心功能界面展示，覆盖数据管理、闭环寻优、智能报告三大关键场景：



图：数据管理界面（CSV 上传 + 文件列表 + 仿真数据生成 + 数据预览）



图：闭环寻优监控界面（FIT% 收敛曲线 + 参数迭代表 + 最优结果高亮）



图：智能分析报告界面（12 类图表 + LLM 分析结论 + 多格式导出）

五、关键技术创新点

- **两图 + 降级子图物理隔离的 Agent 调度架构：**durable（确定性规则编排，908 行）/ 降级子图（LLM 自主规划，714 行）/ react（推理型 ReAct，1625 行）三张状态图物理隔离互不复用，根据任务复杂度自动分发，兼顾开放性与可靠性；配套决策卡 D1-D6 人机共审机制。
- **守卫族 9 件的工业级鲁棒清洗：**从金标准验证战役中逼出的 9 个数据守卫（标签列排除、哨兵检测、分隔符守卫、索引列排除、累积列保护、身份序列排除、事件段保护、PRBS 护栏等），每件对应一个真实缺陷的闭环修复，确保工业数据"不改坏"。

- **反例法论证的动态截取精度：**不空谈算法先进性，用"全量建模 vs 截取后"对照说话：全量数据 K 偏差 9 倍、τ 偏差 72 倍，截取动态段后 K 误差仅 1.2%，直接证明动态截取是建模精度的保障。
- **FOPDT 工程化交付 + 增益调度：**辨识结果不止停留在 ARX 参数，而是自动转换为 APC 工程师直接可用的一阶加纯滞后（FOPDT）模型（增益 K / 时间常数 τ / 纯滞后 θ），并支持按负荷操作点分桶的多模型增益调度，解决流程工业非线性。
- **金标准验证体系：**21 个公开/工业数据集、133 项判定（其中 86 项带代码锚点可追溯）、8 个缺陷闭环、留出集 8 组梯度泛化验证；所有核心数字来自代码实测（v0.1.43），单元测试 2597 passed + 3 failed（已知环境敏感：CRLF×2 / 文件监听×1）+ 2 skipped；前端 857 例（844 通过 / 13 存量失败）。
- **诚实边界（差异化王牌）：**101+ 轮出现负 FIT 均如实标注零粉饰；credibility 自动降档机制；constant_test_target 退化标注；主动披露架构评审 68/100 与 VIF 剔除无物理保护等边界——把"弱点"转化为"可信度王牌"。

六、应用价值与实测成效

- **经济价值：**建模周期从"天级"压缩到"分钟级"，工程师从反复试错中解放，APC 项目交付质量与效率双提升；对齐和利时 MPC 组态格式，可直接下装现场，降低部署门槛。
- **实测成效：**合成数据 K 回收率 49.2% → 81.09%；DMC 闭环仿真验证 K 误差 0.139%、超调 15.8%（"控得住"的直接证明）；UCI 数据集 FPE 改善 227 → 409 倍；Rieth 40 万行数据 1599 段自适应截取。
- **工程质量：**PyPI 0.1.43 发布，安装态严格验证（90 依赖一次解析成功）；GB 级数据支持（2.08GB 分片上传 + OE 辨识向量化 45 倍提速）；Docker 一键部署；self-RAG 知识库沉淀案例。
- **质量底线：**管线参数 ≠ 操作参数（"寻优"指建模管线自整定，非工艺操作参数，对标诚实）；101+ 轮负 FIT 如实标注零违例；所有验证数据可追溯至代码锚点与测试报告。

七、应用对象与应用环境

本系统面向流程工业 APC 建模与数据预处理场景，核心应用对象包括：

- **现场控制工程师：**负责 DCS 日常运维与 APC 投运，需要从海量历史数据中快速筛选高质量建模数据，降低对资深辨识专家的依赖。
- **APC 项目实施团队：**和利时等自动化公司的工程实施人员，需在有限项目周期内完成多装置建模，一键式流水线可显著提升交付效率与质量。
- **企业数字化与工艺部门：**关注节能降耗与工艺优化，需要可信的模型与数据支撑 APC 投运决策，系统的诚实边界与可追溯验证满足工程审计要求。
- **科研与教学场景：**高校与科研机构的系统辨识教学与研究，仿真数据生成 + 金标准验证体系可作为实验教学平台。

应用环境：

- 操作系统：Windows 10/11 / Linux（Ubuntu 20.04+）/ macOS
- 运行环境：Python 3.10+ / Docker 20.10+ / Node.js 18+（前端开发）
- 数据接口：CSV 文件导入 / OPC UA 直连 HOLLiAS DCS（只读）
- LLM 接入：DeepSeek API（云端）/ Ollama 本地部署（数据不出厂）
- 部署方式：Docker Compose 一键部署 / PyPI 安装（ai4industry 命令）/ 源码运行

八、技术栈与交付形态

维度	技术选型
算法 / 数据	Python 3.10+（pandas / NumPy / SciPy / scikit-learn / matplotlib）+ 自研工业算法库（19 模块）
智能体框架	LangGraph 两图 + 降级子图物理隔离（确定性编排（durable）/ ReAct（含 react_fallback 降级子图）+ 工具治理三级白名单（A 级直连 / B 级需确认

	/ C 级不可达） + DeepSeek / Ollama 双 LLM 接入
后端 / 前端	FastAPI（16 个路由模块）+ Vue 3（30 个顶层视图 + 6 个向导步骤）+ Element Plus + ECharts；OPC UA 连接 HOLLiAS DCS；Docker 沙箱安全执行
交付形态	Web 应用 + 图文报告（Word / PDF / PPTX）+ 和利时 APC 组态包；PyPI 0.1.43 可安装 CLI（ai4industry 命令）
团队分工	数据 / 算法 / Agent / 前端 / 测试模块化协作，详细分工与过程文档见《项目详细方案》

九、结语

ProcessPilot 工业辨识数据智能优选工作台，致力于解决流程工业 APC 建模中"高质量数据获取难、人工调参试错成本高"的核心痛点。我们不追求"大而全"的平台叙事，而是聚焦"数据→模型"这一关键前置环节，把工程师从反复试错中解放出来，让建模周期从"天级"压缩到"分钟级"。

我们相信，工业 AI 的价值不在于概念炫技，而在于每一个数字可追溯、每一步取舍有依据、每一条边界敢披露。守卫族 9 件的鲁棒清洗、反例法论证的截取精度、金标准验证体系的 133 项判定、以及 101+ 轮负 FIT 零粉饰的诚实边界——这些不是营销话术，而是代码实测出来的工程质量。

对齐和利时 HOLLiAS DCS 与 MPC 组态格式，让成果可直接下装现场；开放 PyPI 与 Docker 部署，让更多工程师用得上、用得稳。我们希望 ProcessPilot 成为 APC 工程师的"前置加速器"，让每一次建模都站在高质量数据的起点上。

注：本文档为项目概要介绍，核心技术细节、代码锚点与完整验证数据见《项目详细方案》及配套答辩思维导图。所有实测数字均来自代码 HEAD=v0.1.43 的实跑验证。

系统架构（代码实证 · v0.1.43）

以下架构与数字均以当前代码为准（2026-09-15 实核）。

一、两种运行模式（react_enabled 唯一分叉）

ReAct 模式（默认）：LLM 真工具循环，A 级 9 工具直连 + 提交式 2 工具（optimize_submit / task_status）+ send_mail / 知识检索；轮次 10 / 硬顶 20、token 100k、墙钟 30 分钟三重预算；同参重复限 2；C 级同步工具确定性拒绝。

确定性编排（durable）：规则栈执行，LLM 仅输出叙事文本、不参与业务决策；react_enabled 关闭后并入本分支；主链为清洗 / 分段 / 共线 / 辨识 / 寻优五步。

降级子图：已退役为 react_fallback 专属降级子图，仅在 Function Calling 不可用或写操作被拒需救赎时自动重入，用户不可直选。

二、任务执行链（durable）

task_runner（线程池 TASK_WORKERS=2，重启恢复）→ task_executor（按 run_type 分派）→ agentic_runner（ReAct / agentic 执行体）；图状态持久化（graph_state 白名单）支持断点续跑；任务事件经 SSE 推送（内存环缓冲 + DB 尾部窗口补发）。

三、能力面

工具 18 个（tools.py:2964）+ 参数 Schema 护栏；算法 19 模块（清洗含审计 / Rhinehart 分段 / VIF 共线 / ARX-OE 辨识 / 贝叶斯与 TPE 寻优等）。

API：routes.py 聚合 14 个子路由 + main.py 直挂 workspaces 与 fs，共 16 个 routes_*.py；门禁：路由层禁直连 DB（gate1=12 存量）、测试裸 drop_all 须带 _db_guard（gate2=1 存量），增量零新增。

四、前端

Vue3 工作台：31 条路由（30 个顶层视图 + 6 个向导步骤）；右栏为「寻优子任务 / 寻优监控 / 抉择卡」；图表 ECharts（统计）+ D3（关系与结构，6 组件）。

五、质量基线

后端全量 2597 passed + 3 failed（已知环境敏感：CRLF×2 / 文件监听×1）+ 2 skipped；前端 857 例（844 通过 / 13 存量失败）；双 AST 门禁零新增。

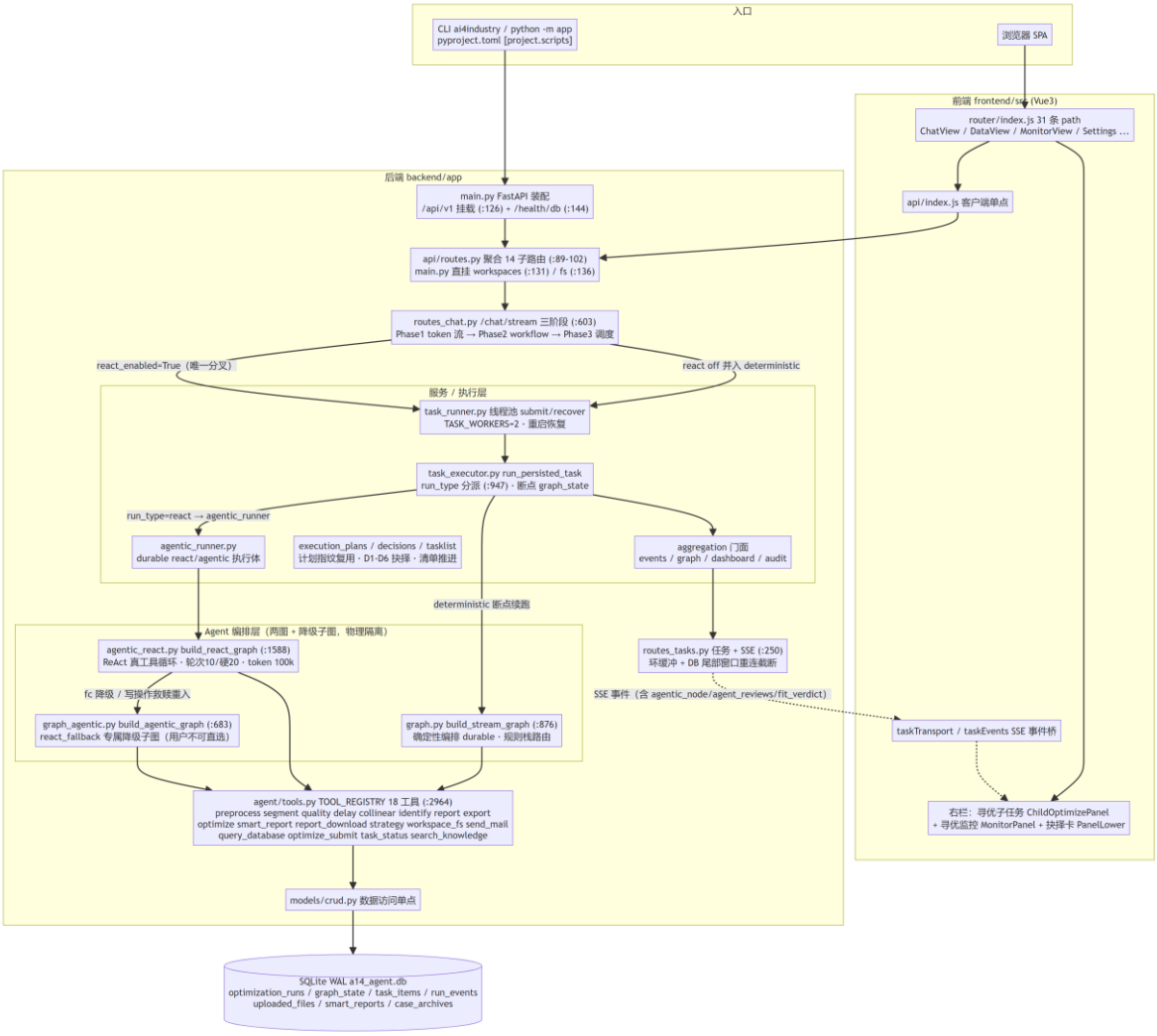


图 1 系统架构全景图（入口 / API / 编排 / 服务 / 工具 / 数据 + 前端右栏）

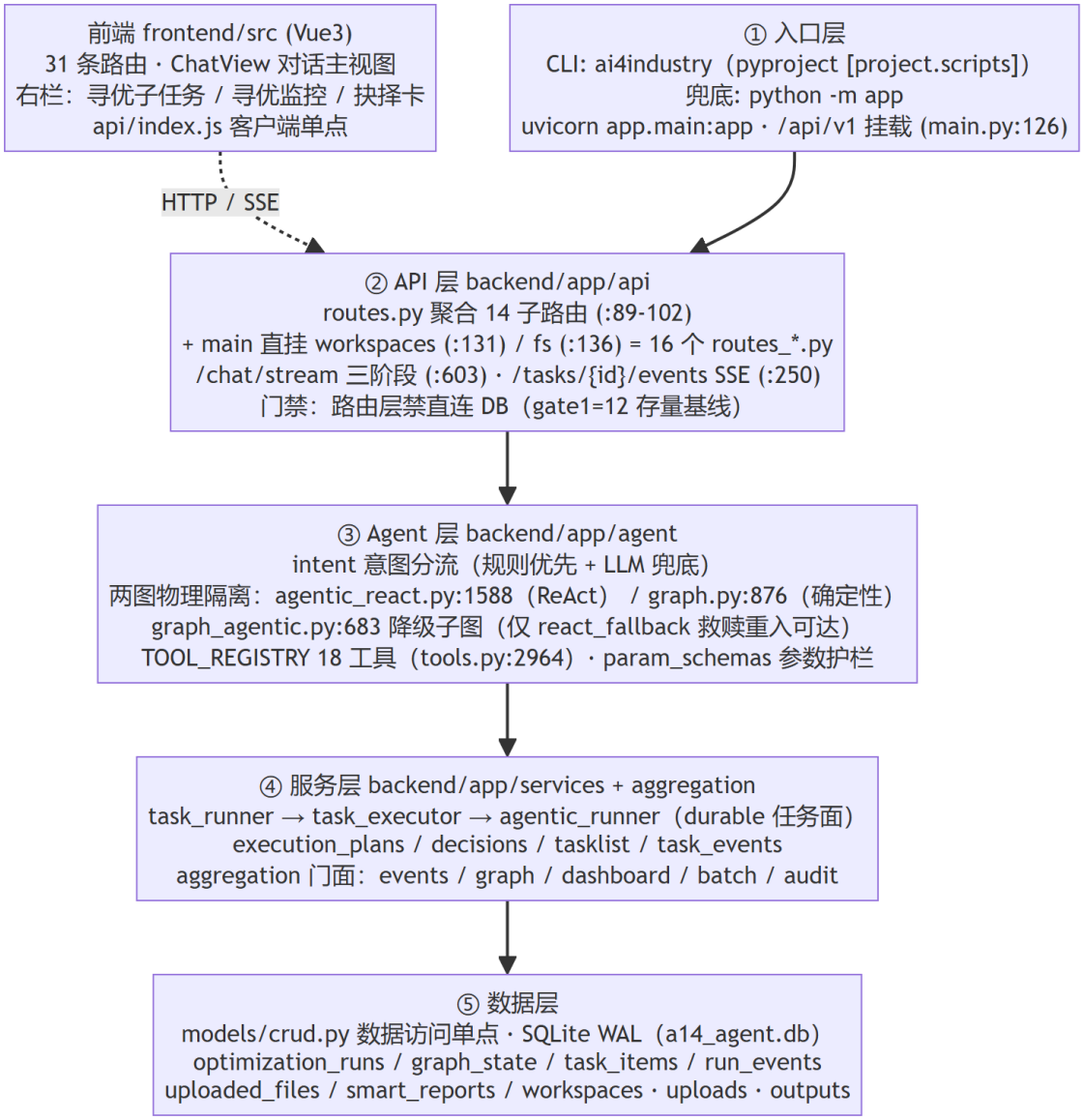


图 2 五层功能地图（入口 / API / Agent / 服务 / 数据）

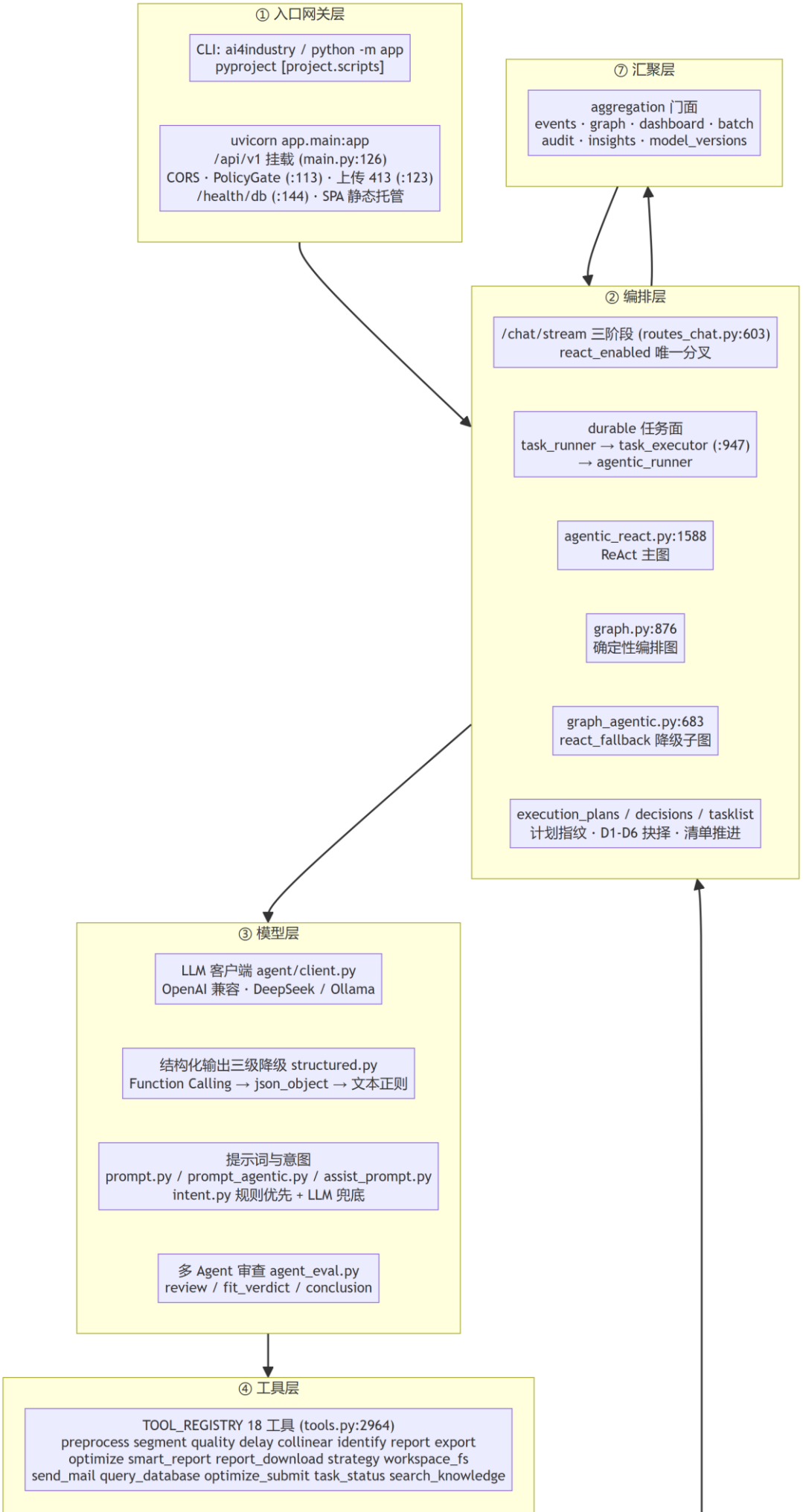

① 入口网关层
CLI: ai4industry / python -m app
pyproject [project.scripts]
uvicorn app.main:app
/api/v1 挂载 (main.py:126)
CORS · PolicyGate (:113) · 上传 413 (:123)
/health/db (:144) · SPA 静态托管
⑦ 汇聚层
aggregation 门面
events · graph · dashboard · batch
audit · insights · model_versions
② 编排层
/chat/stream 三阶段 (routes_chat.py:603)
react_enabled 唯一分叉
durable 任务面
task_runner → task_executor (:947)
→ agentic_runner
agentic_react.py:1588
ReAct 主图
graph.py:876
确定性编排图
graph_agentic.py:683
react_fallback 降级子图
execution_plans / decisions / tasklist
计划指纹 · D1-D6 抉择 · 清单推进
③ 模型层
LLM 客户端 agent/client.py
OpenAI 兼容 · DeepSeek / Ollama
结构化输出三级降级 structured.py
Function Calling → json_object → 文本正则
提示词与意图
prompt.py / prompt_agentic.py / assist_prompt.py
intent.py 规则优先 + LLM 兜底
多 Agent 审查 agent_eval.py
review / fit_verdict / conclusion
④ 工具层
TOOL_REGISTRY 18 工具 (tools.py:2964)
preprocess segment quality delay collinear identify report export
optimize smart_report report_download strategy workspace_fs
send_mail query_database optimize_submit task_status search_knowledge

图 3 七层功能地图（入口网关 / 编排 / 模型 / 工具 / 算法 / 记忆 / 汇聚）

多 Agent 审查（代码标准）：按模块映射为 4 类专业 Agent——数据 Agent（preprocess / segment / quality / export / strategy）、分析 Agent（delay / collinear）、建模 Agent（identify / optimize）、报告 Agent（report / smart_report / report_download），共覆盖 12 个模块；由 agent_eval 统一并行审查并给出 FIT 权威结论。