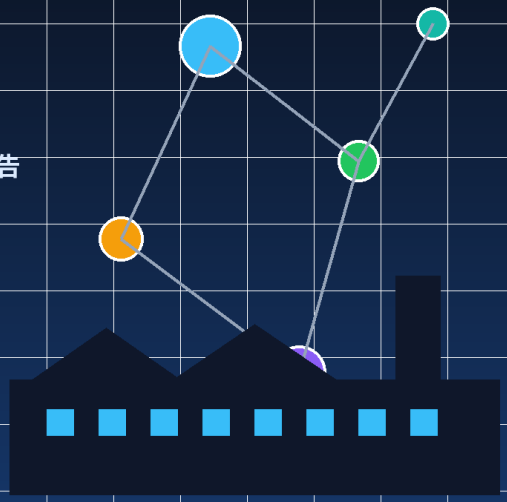
Agent First 理念下的

工业 AI 革命

基于 Hermes Agent 的制造业渐进式导入与商业闭环研究报告

优化排版版 · 2026年5月

上海达柒科技有限公司 | 战略研究部



文件定位：面向董事会、产业客户、政府孵化评审与试点企业的“可落地版”技术商业方案。

本版已完成：内容重组、错字与编码异常修正、图表重绘、章节节奏优化、色彩点缀与版面美化。

核心主张：不推倒重来，而是把 Hermes Agent 作为“跨系统智能操作层”叠加在既有 ERP / MES / SCADA / PLC 之上，先辅助、再协作、最终在安全边界内形成物理闭环。

Agent First	Computer Use	LLM Wiki
智能体优先	无 API 系统也可操作	知识资产自进化

执行摘要

当前工业数字化已进入深水区。传统以“系统集成”和“固定规则控制”为核心的工业 4.0 模式，正在面对系统异构、二次开发成本高、老旧软件缺乏 API、专家经验断层等瓶颈。大语言模型与智能体技术的成熟，使“Agent First（智能体优先）”从概念走向可落地的工业生产力。

达柒科技的 Hermes Agent 方案并不试图一次性替换既有 ERP、MES、SCADA 与 PLC 控制体系，而是在现有系统之上增加一个“跨系统智能操作层”：通过 LLM Wiki、数据中台、Computer Use 与 PLC Gateway 的协同，让企业先获得认知辅助，再进入工作流自动化，最终在安全边界内实现物理闭环优化。

核心理念	落地路径	技术抓手	商业结果
Agent First：以智能体作为跨系统中枢	三阶段：只读辅助 → 受控协作 → 自主闭环	LLM Wiki + 数据中台 + Computer Use + PLC	降本、增效、减碳、知识资产沉淀

目录

一、从 Tooling AI 到 Agent First

1.1 工业 AI 的关键转折

过去许多 AI 应用停留在“报表分析器”或“单点插件”层面，本质仍依附在既有系统中。Agent First 的差异在于：智能体不再只是工具，而是能够感知环境、理解上下文、规划任务并调用工具执行的“硅基劳动力”。它承担的是跨软件、跨数据、跨设备的协调角色。

这一转折对制造业尤其重要。制造现场的真实复杂性往往来自系统异构：ERP 管订单，MES 管排产，SCADA 管监控，PLC 管设备，而大量旧系统缺少现代 API。Hermes Agent 的价值，就是把这些碎片化系统重新组织为可被自然语言驱动、可被审计、可逐步授权的协同网络。

1.2 Computer Use 解决“最后一公里”

传统 API 集成	RPA 脚本自动化	Computer Use + Agent
依赖系统开放接口，二次开发成本高。	依赖固定坐标与流程，界面变化容易失效。	像工程师一样看屏幕、点按钮、读表单，并由大模型规划流程。
适合新系统、标准系统。	适合重复性强、变化少的流程。	适合旧版 ERP/MES、专用客户端、无 API 的遗留系统。
改造周期较长。	维护成本中等。	先以低侵入方式验证价值，再决定是否深度集成。

二、Hermes Agent 自进化工业智能体架构

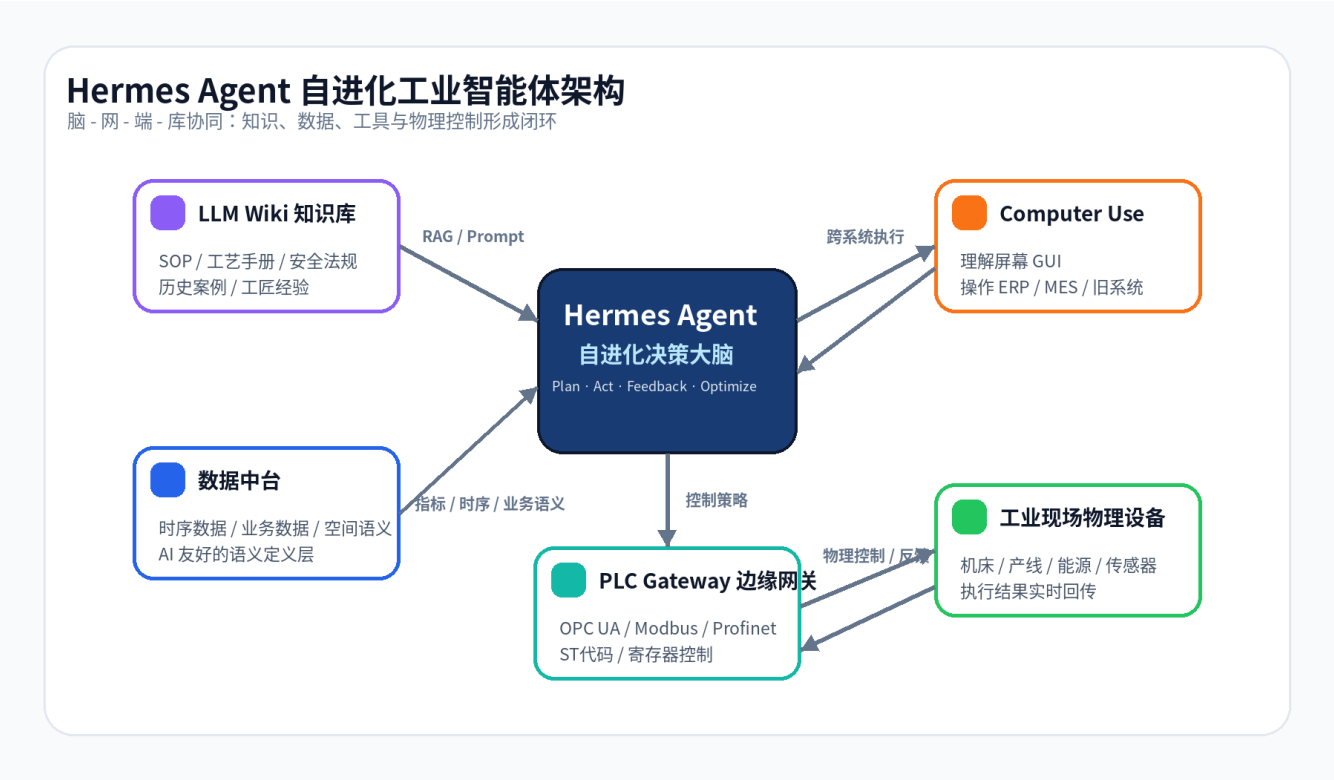


图 1 | Hermes Agent 的“脑-网-端-库”协同架构

2.1 四大基座组件

组件	角色定位	关键能力	落地价值
Hermes Agent	自进化决策大脑	任务规划、工具调用、反馈纠偏、记忆机制	把人找数、人调机升级为数找人、Agent 辅助调机
LLM Wiki	动态知识中枢	RAG 检索、SOP 语义化、案例沉淀	把老工匠经验与维修案例转化为可复用知识资产
数据中台	时序与业务语义层	汇聚 ERP、MES、传感器与能源数据	让 Agent 能理解停机损失、空转率、良率等业务指标
PLC Gateway	物理世界桥梁	OPC UA、Modbus、Profinet、ST 代码与边缘过滤	把高级策略转化为可执行的设备控制或微调指令

2.2 自进化机制：PAFO 闭环

图 2 | PAFO：规划、执行、反馈与优化的自进化闭环

工业场景容错率低，因此 Agent 必须从一开始就具备“可审计、可回滚、可验证”的反思机制。建议把每一次执行都记录为结构化事件：输入数据、决策依据、调用工具、操作结果、人工审批记录、异常处理与最终 KPI。通过这些事件沉淀，LLM Wiki 不只是问答库，而会逐步成为企业的工业知识资产库。

三、工业 Agent 循序渐进导入路线

图 3 | 三阶段渐进式导入路线：由只读到闭环

工业控制系统不能采用“一次性替换”的激进方式。达柒科技的导入原则是：大处着眼、小处着手、渐进迭代。先让客户感受到认知辅助价值，再通过低风险流程自动化建立信任，最终在明确的安全边界内逐步开放物理控制权限。

阶段	核心目标	系统部署	典型动作	安全边界
阶段一 认知辅助	建立信任，打通知识与数据流	上线 LLM Wiki 与数据中台	自然语言问数、异常解释、SOP 推荐	只读不写，不修改业务系统与设备
阶段二 跨系统协作	降低人工操作成本，实现流程自动化	引入 Computer Use，有限授权 PLC 写入	备件申请、派工、报表上传、参数微调	Human-in-the-loop，人审与双签
阶段三 物理闭环	形成降本增效与节能减排闭环	安全边界内开放自主策略	工艺自优化、能效削峰填谷、集团知识共享	Safe-RL Boundary、沙盒验证、审计与回滚

四、核心应用实例与商业闭环

图 4 | 从技术动作到经营结果的商业闭环

应用场景	原始痛点	Agent 介入方式	可量化结果
设备预测性维护	阈值报警误报率高，故障排查依赖老师傅经验。	PLC Gateway 采集 10 kHz 振动与电流数据，Hermes Agent 结合维修手册推理故障，自动跨 MES/ERP 查排产、查库存、建工单。	非计划停机时间降低约 40%；备件资金占用降低约 15%；OEE 提升约 3%-5%。
工艺自适应优化	SOP 静态，原料批次与反应过程变化快，良率波动大。	Agent 读取原材料光谱、温度与流量数据，通过 PLC Gateway 动态微调 PID 与投料比例。	一次良品率由 91.2% 提升至 96.5%；原材料利用率提升约 2.8%。
多能互补调度	分时电价、光伏、储能与生产	Agent 结合天气、电价、光伏功率与车间负荷，规划储能充	综合电费降低约 15%-22%；光伏自发自用率提升约 18%；支

	负荷缺乏统一调度。	放电和非紧急负载调节。	持 ESG 审计。

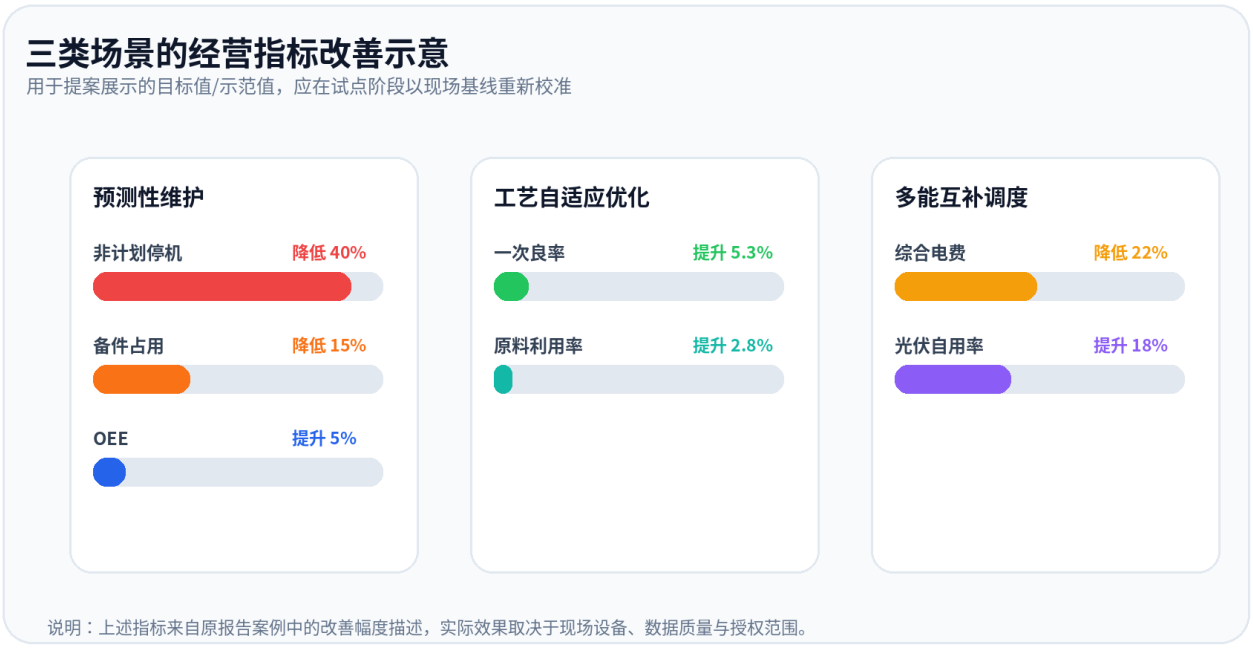


图 5 | 三类典型场景的 KPI 改善示意

五、安全治理与试点实施计划

5.1 安全治理原则

原则	说明
最小权限	Agent 默认只读，只有在明确授权后才能写入业务系统或 PLC。
人机协同	关键工艺变化、设备启停、能源调度等动作必须通过人工确认或双签。
沙盒先行	新策略先进入数字孪生或仿真沙盒验证，再逐步释放到真实产线。
全链路审计	记录每个提示词、数据来源、工具调用、审批人、执行结果与回滚动作。
可回滚机制	任何控制策略都必须具备一键回退到人工或固定规则模式的能力。

5.2 12 周试点推进建议

周期	重点任务	交付物	验收指标
第 1-2 周	场景盘点、数据源清单、权限边界确认	试点蓝图、KPI 基线表、风险清单	明确 1-2 个高价值场景

第 3-5 周	LLM Wiki 建库、SOP/手册/历史工单结构化	可检索知识库、知识质量评分	问答准确率与引用可追溯
第 6-8 周	数据中台接入与语义层建模	设备、工单、能耗与产线指标看板	关键数据延迟与完整率达标
第 9-10 周	Computer Use 流程自动化试运行	自动派工/报表/审批 Demo	人工节省时间、误操作率下降
第 11-12 周	受控闭环演示与 ROI 复盘	试点报告、扩展路线、预算建议	KPI 改善与可复制性评估

六、商业化复制与结语

6.1 建议商业模式

收入模块	客户购买理由	交付内容
咨询与诊断	帮助企业识别最适合 Agent First 的高 ROI 场景。	流程盘点、数据成熟度评估、试点蓝图。
平台订阅/私有化许可	建设企业内部可持续进化的工业智能体底座。	Hermes Agent、LLM Wiki、数据语义层、权限审计。
系统集成与场景包	把方案快速落到产线、设备与业务流程。	Computer Use 流程包、PLC Gateway 接入、看板与告警。
效果分成/托管优化	降低客户一次性投入压力，与客户共同承担结果。	能效优化、OEE 提升、良率提升等绩效型服务。

6.2 结语

Agent First 不是对工业现场的颠覆式替换，而是一种更现实的渐进式增强：先让知识流动起来，让数据被自然语言理解；再让繁琐的跨系统流程自动化；最后在可验证、可回滚的安全边界内，把 AI 的决策能力连接到真实设备与能源系统。

对达柒科技而言，Hermes Agent 的长期价值不只在于降本增效，更在于沉淀企业级工业知识资产：把经验、案例、参数、工艺与安全规则转化为可检索、可复用、可进化的智能体能力。通过一个个小场景的稳健试点，最终形成可复制的“工业 AI 升级包”，帮助制造企业走向自主、自进化、低碳的智能工厂。