AI智能体在各行业的应用全景白皮书

17 大行业、核心业务链、典型智能体与企业落地路径

曾俊 | 北京硅基行动科技有限公司

研究截止日期：2026 年 9 月 5 日

目录

前言 4

执行摘要 5

如何使用这本白皮书 7

第一章 农业、林业、畜牧业与渔业 8

第二章 能源、矿业与公用事业 17

第三章 制造业 27

第四章 汽车、出行与交通服务 49

第五章 建筑、房地产与物业 60

第六章 消费品、食品与餐饮 70

第七章 零售与电商 79

第八章 物流、供应链与邮政 87

第九章 旅游、酒店与文旅 94

第十章 科技、互联网与软件服务 102

第十一章 电信 110

第十二章 媒体、营销、游戏与文娱 117

第十三章 教育与科研 123

第十四章 专业服务 130

第十五章 医疗、医药与生命科学 136

第十六章 金融服务 141

第十七章 政务、公共事业与非营利 147

结语 152

附录一：跨行业通用智能体图谱 153

附录二：企业 AI 智能体落地路线图 155

附录三：评测与验收框架 156

附录四：风险分级与人工控制 158

关于编制者

曾俊，北京硅基行动科技有限公司创始人，长期专注企业 AI 落地、AI 实战培训、企业 AI 诊断与咨询、智能体定制和 AI 转型推进。本白皮书面向中国企业老板、业务负责人、AI 转型负责人和普通企业员工，重点回答 AI 智能体可以进入哪些行业流程、如何落地以及如何验收。

前言：AI 智能体开始进入企业的业务链

过去几年，企业对 AI 的理解大多停留在“问一个问题，得到一个答案”。它可以写文案、总结文档、生成图片，也可以连接企业知识库回答制度和产品问题。这些能力已经创造价值，但它们仍然主要停留在信息生成层。

AI 智能体带来的变化，是 AI 开始进入企业的业务状态和动作链。它不只是回答“库存还有多少”，还可能持续监测安全库存、判断缺料风险、通知采购与计划人员、创建补货任务，并跟踪问题是否关闭；它不只是回答“设备为什么报警”，还可能读取报警代码、调用维修手册和历史案例、生成排查步骤、派发工单、回访维修结果，再把有效经验写回知识库。

这意味着，企业需要重新理解 AI 的应用单位。真正值得设计的，是一段可以被观察、被改造、被验收的业务流程；孤立的聊天入口很难形成持续价值。

不同行业的流程差异非常大。制造业关心质量、设备、产能和交付，金融业关心授信、欺诈、合规与资金风险，医疗行业关心临床安全、患者隐私与专业责任，零售行业关心商品、门店、库存和消费者体验。一个智能体能否落地，取决于它是否理解行业对象、业务规则、数据结构、系统权限和风险边界。

因此，本书不从技术平台出发，也不限定使用某一种通用智能体。企业可以使用垂直智能体、业务系统内置智能体、低代码平台、自研多智能体，也可以利用 Codex 等执行型 AI 工具完成研发、数据、文档和跨系统任务。关键问题始终是：它进入了哪一条业务链，解决了哪一个问题，采取了什么动作，最终如何验收。

真正的垂直化要求 AI 进入行业对象和责任链，远不止给通用聊天机器人更换一套行业提示词：医疗智能体要理解病历、药事、临床风险与专业责任；金融智能体要理解客户、交易、适当性、授信与监管口径；制造业智能体要连接图纸、BOM、工艺、设备、质量和生产状态；政务智能体则必须提供规则来源、纠错申诉和线下人工出口。

这本白皮书聚焦企业面对一条真实业务链时，哪些工作适合交给 AI，哪些动作必须由人保留，以及怎样证明一个智能体真正创造了价值。

执行摘要

一、AI 智能体的五种常见形态

为了避免把所有 AI 应用混为一谈，本书采用五种形态进行描述。

形态	核心能力	企业中的典型表现	是否一定属于完整智能体
AI 能力部件	识别、预测、分类、推荐、优化	OCR、语音识别、机器视觉、需求预测	否，通常是智能体调用的能力
知识与分析助手	检索、问答、摘要、报告、建议	制度问答、设备知识助手、投研助手	不一定，通常缺少业务动作与状态反馈
AI 增强工作流	模型判断嵌入固定流程	文档预审、异常分类、自动通知	具备部分智能体能力
受限执行型智能体	理解目标、选择工具、跨系统行动	创建任务、更新系统、追踪闭环	是当前企业较适合规模化的形态
多智能体或物理闭环	多角色协作，连接设备和现场动作	设备维修多智能体、仓储调度、机器人协作	是，但需要更严格的确定性与安全控制

二、判断一个 AI 应用是否真正进入业务

本书对重点智能体尽量补齐以下字段：

服务对象 → 触发条件 → 输入 → 判断与规划 → 调用工具 → 可执行动作 → 状态与反馈 → 人工控制点 → 业务结果 → 验收指标

判断一项 AI 应用是否真正进入业务，需要同时看清输入、动作、控制点、业务结果和验收方式，避免把单次演示等同于成熟落地。

三、17 个行业出现的共同规律

- AI 智能体的价值主要来自进入流程，而不是生成更多内容。
- 当前更稳妥的生产形态通常是“模型 + 企业数据 + 规则/专业工具 + 工作流 + 人工审批”。
- 行业垂直化的核心是对象、规则、系统、数据和责任，而不是名称中有没有“行业”二字。
- 越接近资金、生命健康、行政权益、产品放行和物理设备，越需要确定性控制、专业复核和人工接管。
- 多智能体不是天然更先进。只有任务确实需要分工、共享状态和互相校验时，多角色编排才有意义。
- 企业应先选一个可量化的业务问题建立基线，再决定使用通用智能体、垂直智能体、业务系统内置能力还是自研方案。
- 验收不能只看答案准确率，还要同时看业务结果、流程闭环、工程可靠性、持续使用和风险控制。

四、企业优先关注的四种机会

1. 高耗时的知识与文档工作

例如制度检索、合同或报告预审、设备手册查询、政策问答、病历摘要和投研资料整理。适合作为低风险入口，但必须保留来源和版本。

2. 多系统之间的状态追踪与任务闭环

例如供应商整改、维修工单、项目风险、客诉、贷后预警和政务派单。价值来自把“发现问题”推进到“责任到人、处理、回写和关闭”。

3. 专业模型与业务流程的组合

例如视觉质检、需求预测、排产优化、反欺诈、临床检验和能源调度。大语言模型负责理解、编排和解释，专业模型或确定性工具负责计算与约束。

4. 受控的跨系统执行

例如创建任务、更新字段、生成草稿、提交审批和运行代码。所有写入动作都需要最小权限、幂等、日志、回滚和人工接管。

如何使用这本白皮书

企业老板与业务负责人

先阅读对应行业章中的“核心业务链”和“智能体全景”，判断 AI 可以进入哪些经营环节，再选择一个有明确负责人、数据来源和结果指标的试点。

AI 转型负责人和信息化负责人

重点阅读“重点工作卡”“系统、数据与权限”“落地路线”和“评测验收”，将场景转化为需求清单、系统边界和验收方案。

业务部门和一线员工

重点查看每个智能体的服务对象、触发条件、输出动作和人工控制点，判断它是否真的减少重复工作、缩短处理时间或改善业务结果。

解决方案与服务机构

不要把行业章节当成标准产品清单。相同名称的智能体，在不同企业所需的数据、权限、系统接口和责任链可能完全不同。

第一章 农业、林业、畜牧业与渔业：AI 智能体连接自然生产、现场作业与供应链

农业、林业、畜牧业与渔业的 AI 智能体应用，主要集中在种植监测、农机作业、农产品质量、供应链追溯和经营支持，并正向育种、植保、畜牧、林业与渔业延伸。

本章核心结论

农业、林业、畜牧业与渔业共享三个特征：生产对象具有生命过程，经营结果受自然环境影响，许多关键动作发生在田间、圈舍、林区和水体。AI 智能体要产生业务价值，需要把遥感、气象、传感器、影像和经营数据转成可执行任务，再把人工或设备动作与生产结果写回同一条记录。

目前较成熟的应用集中在多源风险监测与农艺建议、农机作业与调度、农产品质量与供应链追溯、农业知识和经营支持。智能育种、植保治理和生鲜冷链也已出现项目探索，并逐步形成从监测、判断到任务执行和结果回写的业务链。

本行业的高风险边界十分清楚：农药和兽药使用、疫病处置、品种选育、正式质量定级、采伐捕捞、农机控制与交易结算都需要专业人员或授权主体确认。模型可以监测、诊断、排序、生成任务和记录结果，不能绕过资质、法规、安全联锁和现场责任人。

本章重点覆盖三个方向：

- 将智能育种从“品种知识问答”提升为独立的长周期科研链；
- 将农机从单机自动作业扩展到跨地块排程、共享服务、质量验收和结算；
- 将农产品追溯、温控预警、库存和销售协同纳入生产之后的经营闭环。

一、行业边界与子行业

本章保留一个上位行业簇，内部按照四条生产链和一条横向流通链展开。

1. 种植业

围绕种质、品种、地块、生育期、土壤、气象、水肥、病虫草害、农机、收获和质量分级展开，也是农业 AI 智能体应用较为集中的子行业。

2. 畜牧业

围绕种源、饲料、圈舍、动物个体或群体、疫病、出栏、运输、屠宰和食品安全展开，智能体可连接繁育、精准饲喂、疫病预警、采购、运输和肉品冷却。

3. 林业

围绕资源调查、育苗造林、抚育、防火、病虫害、采伐运输、生态服务和碳汇核算展开。遥感、无人机和预测模型是重要能力部件，相关完整执行型智能体仍处于探索与试点阶段。

4. 渔业

围绕苗种、水体、投喂、病害、生长、起捕、加工、冷链和销售展开，水质预测、投喂优化和机器视觉可作为感知与决策工具，连接“发现—处置—复检—经营结果”闭环。

5. 农产品供应链与经营

产地批次进入质检、分选、仓储、冷链、交易和销售后，会与食品制造、零售和物流交叉。本章关注农业特有的产地、品种、生产台账和批次追溯；仓内调度、门店经营和干线运输的通用能力分别在零售和物流章节展开。

二、核心业务链全景

资源与经营规划 → 种质与育种 → 生产计划 → 环境与生长监测 → 农事 饲喂 投喂与设施作业 → 病虫害 疫病与灾害处置 → 采收 出栏 起捕或采伐 → 质检 分级与追溯 → 仓储 冷链与运输 → 交易 销售与结算 → 经营复盘与知识回写

这条链在四个子行业中的业务对象不同。种植业关注地块和作物批次，畜牧业关注动物个体或群体，林业关注林班和生态资源，渔业关注养殖池、网箱、船舶和水产品批次。企业需要先统一对象标识，再谈跨系统智能。

环节	主要角色	输入与输出	典型瓶颈	AI 智能体机会
资源与经营规划	农场主、合作社、林场、养殖企业、政府服务部门	土地/水体/林地、历史产量、市场和政策 → 年度计划与预算	数据跨部门分散，计划依赖经验	政策研究、产销规划、投入测算智能体
种质与育种	育种专家、科研人员、试验站	基因型、表型、环境、文献、试验记录 → 候选组合和试验方案	长周期、多因素、知识分散	智能育种科研智能体
生产计划	农艺师、兽医、水产技术员、生产经理	品种、生育期、天气、产能、订单 → 农事/饲喂/投喂计划	计划与实时环境脱节	农业生产计划与决策智能体
环境与生长监测	农技人员、场站管理者	遥感、气象、土壤、水质、影像、传感器 → 风险定位与趋势	数据尺度不一，误报后无人处理	多模态监测与诊断智能体
现场作业	机手、一线人员、设备管理者	任务、地块、机具、药剂、人员 → 作业轨迹和结果	跨地块调度难，弱网和设备故障频繁	农机调度、植保治理、设施作业智能体
生物风险与灾害	农艺师、兽医、林业和水产专业人员	病征、影像、气象、流行病学和规则 → 处置建议与任务	漏报成本高，专业责任重	病虫害、疫病、火灾和水体风险智能体
采收与质量	生产、质量、采购	批次、成熟度、图像、检测值 → 采收/出栏和分级	标准不一，现场检验慢	成熟度、质量识别与定级辅助智能体
追溯与冷链	仓储、物流、质量、客户	生产台账、批次、温湿度、位置 → 追溯链和处置任务	数据断链，告警停在看板	追溯、冷链预警和异常闭环智能体
交易与经营	采购、销售、财务、管理层	行情、质量、合同、库存、订单 → 交易建议和经营分析	价格波动、损耗和履约难归因	采购、供需协同、销售经营智能体

三、逐环节业务流程与问题

1. 育种：模型建议必须回到田间试验

智能育种需要把种质资源、论文、基因型、表型、环境和历年试验记录放在同一研究上下文中。智能体可以检索相似材料、发现数据缺口、提出亲本或组合候选、生成试验设计，并跟踪试验状态。

真正的业务输出是可执行的试验计划和可追溯的候选依据。最终选育判断仍由育种专家负责，模型结果需要跨季节、跨试验地和跨品种验证。

2. 环境监测与风险诊断：从“一个指数”走向任务闭环

旱情、病虫害、水质、火情和圈舍环境通常依赖多源数据。卫星适合区域尺度，无人机和摄像头适合局部影像，地面传感器提供连续数值，人工巡查补充现场语义。智能体的任务是对齐时间、位置和生产对象，形成风险等级、原因候选和处置建议。

只有预警并不够。系统还要把任务派给农艺师、兽医或现场人员，记录是否采纳、何时执行、复检结果和最终损失。否则企业只能得到一个新的告警看板。

3. 农机与植保：调度层和控制层分开

农机任务编排涉及天气窗口、地块位置、作物阶段、机具能力、人员、道路和订单优先级。智能体可以生成排程、路线和改排方案，也可以跟踪轨迹、面积和作业质量。

车辆运动、植保飞行、药剂用量和现场停机由确定性控制器、专业规则和资质人员负责。无人机备案、禁飞区、药剂禁用规则、人工接管和异常上报需要先固化，再开放工具调用。

4. 质量、追溯与交易：识别结果需要对应正式标准

粮食质量识别、农产品分级和动物健康评估可以提高初检效率。企业需要同时保存原图、设备、模型版本、人工复核和正式检验结果，以判断误判是否影响价格、放行或争议。

追溯智能体则从地块、圈舍或水体开始，关联投入品、生产操作、质检、批次转换、仓储和运输。追溯链中任何一段缺失，召回范围和责任定位都会失真。

5. 冷链与供需协同：告警需要能改变损耗结果

冷链系统持续读取温湿度、位置、停留时间和设备状态。完整智能体在越界后会判断品类阈值和剩余时效，通知责任人、生成转仓或优先销售建议，并把最终报损和客户结果写回。

供需协同还需要读取订单、销量、库存、在途和保鲜期，输出采购、调拨或促销建议。采购承诺、价格和结算仍由授权人员确认。

四、AI 智能体全景图

业务链	代表智能体或相邻能力	主要动作
种质与育种	智能育种科研智能体	候选分析、试验设计、记录跟踪
生产规划	产销计划与投入测算智能体	生成情景计划和风险提示
环境监测	农业多模态监测—诊断智能体	风险定位、原因排序、任务移交
旱情与产量	旱情指数、作物健康和产量预测	预测和建议
病虫害与农技	农技知识和病害辅助智能体	带依据问答、识别和处置建议
农机作业	自主农业作业平台	感知、规划和物理作业
农机服务	农机任务编排与共享调度智能体	跨地块排程、改排、作业验收
植保治理	植保无人机作业治理智能体	备案草稿、任务、轨迹和台账
设施控制	温室照明、水肥和环境优化系统	预测、控制建议或设备动作
畜牧采购	生猪采购助手	推荐、合同草稿、验标和物流预警
质量分级	小麦 GeoAI 质量定级平台	图像识别和定级辅助
生产追溯	农产品生产追溯智能体	批次关联、异常定位、召回线索
冷链	生鲜冷链风险预警智能体	分级预警、派单和损耗回写
供需经营	生鲜供应链协同决策智能体	补货、调拨、优先销售建议
销售管理	海大销售 360/ 高管分身	客户全景、评分和业务辅导
林业	防火、病虫害、资源与碳汇智能体	监测、任务和核算
渔业	水质、投喂、病害和起捕智能体	预测、建议和现场任务

全景图中的预测模型、识别模型、控制系统和规则工作流都可能成为智能体工具。只有补齐目标理解、工具调用、动作、状态反馈和责任边界后，才进入完整执行型智能体。

五、重点智能体工作卡

1. 农业多模态监测与生产决策智能体

字段	内容
服务对象	农场经理、农艺师、合作社技术员和农业服务机构
触发条件	定时监测，或气象、土壤、影像、生长指标出现异常
主要输入	遥感、无人机、气象、土壤、水肥、作物影像、生产计划和农技规则
判断与规划	对齐地块和生育期，识别风险，生成原因候选、处置顺序和缺失信息
工具与系统	GIS、农业物联网、气象服务、农事台账、任务与通知系统
输出与动作	风险地图、处置建议、巡查或作业任务、复检提醒和结果记录
人工控制点	农艺师确认农药、水肥和重大生产调整；设备动作进入独立控制和安全规则
验收指标	风险提前量、漏报和误报、建议采纳率、任务关闭率、产量/损失和投入变化

2. 智能育种科研智能体

字段	内容
服务对象	育种专家、科研人员、试验站和种业企业
触发条件	新选育任务、亲本和组合筛选、试验设计或阶段性评价
主要输入	种质、基因型、表型、环境、文献、历年试验和专家标注
判断与规划	检索相似材料，提出候选组合和试验设计，标记证据和不确定性
工具与系统	种质资源库、试验数据库、科研文献、统计和生物信息工具
输出与动作	候选清单、试验方案、缺失数据、阶段报告和待办任务
人工控制点	专家决定组合与淘汰；试验结果按品种、地点和季节复核
验收指标	候选命中、专家修改率、试验设计完整性、跨季稳定性和知识可追溯

3. 农机任务编排与共享服务智能体

字段	内容
服务对象	农机合作社、农服平台、机手和农户
触发条件	新农事订单、天气变化、设备故障或作业延误
主要输入	农事窗口、地块位置、机具能力和状态、天气、人员、订单与道路
判断与规划	匹配机具，优化跨地块路线与时段，异常时滚动改排
工具与系统	农服订单、GIS/ 北斗、设备平台、气象、工单与结算系统
输出与动作	排程、路线、任务单、异常改排、作业验收和结算草稿
人工控制点	机手确认现场条件；运动和作业控制由设备安全系统执行；费用争议人工复核
验收指标	准时率、空驶、单位面积成本、改排次数、人工接管、返工和安全事件

4. 生鲜冷链风险与供应链协同智能体

字段	内容
服务对象	产地企业、仓储、物流、采购、门店和质量人员
触发条件	温湿度或时效越界、库存临期、在途延迟、需求偏差
主要输入	批次、品类阈值、质检、库存、订单、在途、温湿度、位置和保鲜期
判断与规划	判断影响范围和剩余时效，生成转仓、调拨、补货或优先销售建议
工具与系统	ERP、WMS、TMS、冷链物联网、门店 POS、质量和工单系统
输出与动作	分级预警、处置任务、追溯链、采购/调拨建议和损耗复盘
人工控制点	质量放行、报损、召回、价格和采购承诺由授权人员决定
验收指标	温控异常响应、追溯完整率、损耗、缺货、周转、误报和按期关闭率

六、代表案例

案例一：农业 AI 规模化项目组——把模型输出追到经营结果

目前，旱情预警、自主农业平台、粮食质量定级、设施农业照明和肉品冷却等应用已经进入项目实践。它们分属预测、机器视觉、优化和物理控制，共同呈现出农业 AI 的完整验收路径：现场数据进入模型，专业人员确认建议，设备或人员执行，再观察产量、质量、损耗、资源投入和经营结果。

农业项目的效果评估必须明确项目范围、对照基线、生产季节和计算口径，避免将天气、品种、管理和市场变化全部归因于 AI。



图：农业 AI 规模化应用原文配图

案例二：十字花科蔬菜智能育种大模型项目

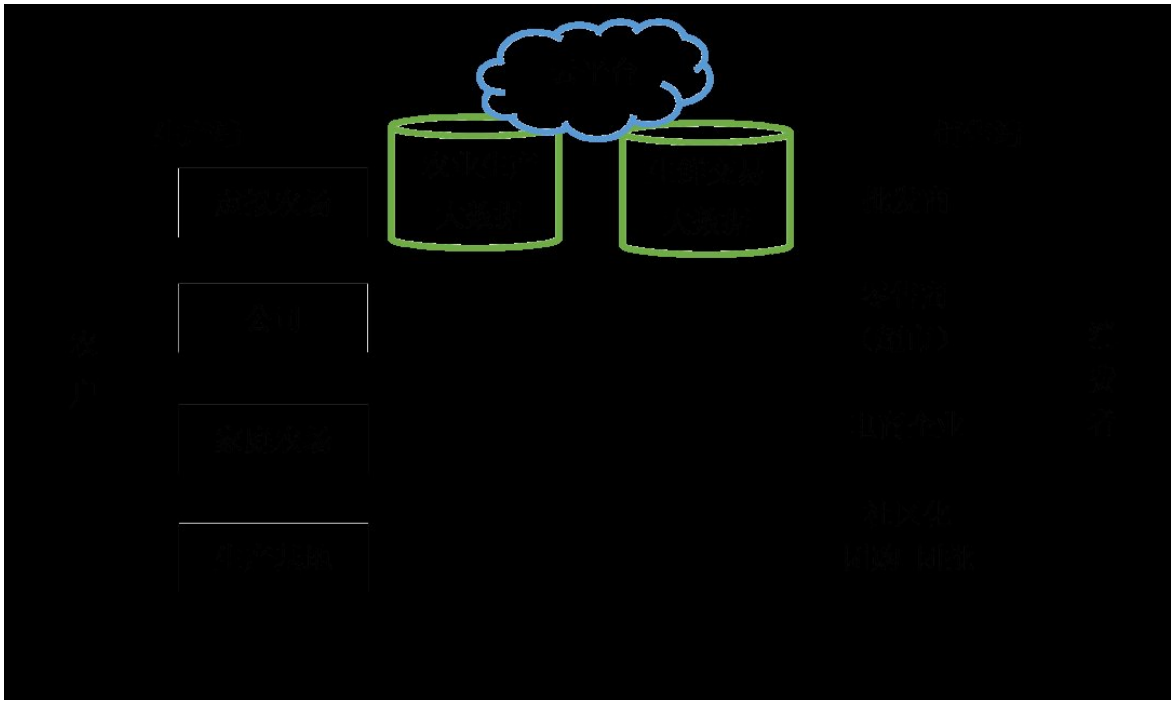
山东省重点研发计划相关公开信息可以确认项目已经启动，研究对象覆盖十字花科蔬菜智能育种。它适合用于说明种质、表型、基因型、环境、试验和专家知识如何构成一个长期科研链。

该项目已经启动，当前重点是建立育种数据、模型建议、田间试验和结果回写的闭环；育种成效应以完成验收后的田间结果和经营收益衡量。

案例三：生鲜农产品供应链智能化——追溯和冷链是基础层

相关材料将生产、质检、仓储、运输和销售串成连续链路。文中明确，运输和仓储环节以温湿度监测与预警保障货架期和保质期，生产端则依赖批次和过程信息形成追溯。

这类系统在加入派单、处置、复检和损耗回写后，才能形成完整的执行型智能体；实际成效应以冷链损耗、异常关闭时间和复检结果衡量。



图：生鲜农产品供应链智能化结构

案例四：海大销售 360——行业企业案例与农业生产案例分开

海大集团将 BI、CRM 和一线销售提交组织成客户全景、评分和业务辅导，展示了农牧企业销售经营智能体的应用方式。该智能体服务客户经营，与田间、圈舍或水体生产智能体属于不同业务链。

七、系统、数据与权限

1. 核心数据对象

- 种植：地块、品种、生育期、农事、投入品、设备和批次；
- 畜牧：动物个体/群体、种源、饲料、圈舍、检疫、用药和出栏批次；
- 林业：林班、小班、树种、蓄积、巡护、火情、病虫害和采伐许可；
- 渔业：池塘/网箱、水体、苗种、投喂、用药、船舶、起捕和加工批次；
- 供应链：质检、仓库、运输、温控、订单、价格、损耗和结算。

每个对象需要统一编码，关联时间、位置、责任人和版本。建议、批准、执行和结果要写入同一任务链。

2. 系统接口

常见接口包括农业物联网、GIS/ 北斗、遥感和气象服务、无人机与农机平台、农事台账、实验数据库、ERP、WMS、TMS、质量、合同、支付和协同系统。

弱网场景需要本地缓存和离线任务；设备接口需要状态校验、超时、重试和人工接管；跨农户和平台共享数据时需要明确权属和授权用途。

八、企业落地路线

阶段 0：选定生产对象和基线

从一个地块、一个温室、一类设备、一条冷链或一种高频问题开始。记录当前监测覆盖、处理时间、损失、投入和责任链。

阶段 1：只读知识与风险分析

先上线农技检索、试验资料整理、历史作业查询、风险报告和追溯查询。重点验证来源、版本、地域和品种适用性。

阶段 2：受控任务执行

允许智能体创建巡查、采样、维修和调度草稿，由人员确认后进入现场。同步验证弱网、重复任务、错误路由和回写失败。

阶段 3：有限闭环

低风险、规则明确的提醒、台账和任务流转可以自动执行。农药、兽药、疫病、设备运动、正式定级和交易保持人工闸门。

阶段 4：跨周期与规模复制

至少经过一个完整生产周期，再验证跨季节、跨地块、跨品种和跨基地迁移。复制时同时复制数据合同、专业规则、权限和验收方法。

九、评测与验收

场景	任务质量	业务结果	闭环与风险
风险监测	提前量、召回率、误报率、定位准确	损失、产量、水肥和响应工时	建议采纳、任务关闭、漏报升级
智能育种	候选命中、专家修改、证据完整	试验周期和有效候选率	跨季/跨地验证、错误淘汰复核
农机调度	计划兑现、改排、路线可执行	空驶、单位面积成本、准时率	安全冲突、人工接管和回退
植保治理	备案字段、轨迹与台账完整	作业覆盖和异常处置时间	禁飞/禁用阻断、资质确认
质量分级	与正式检验一致、漏检和误判	检验时间、争议、价格兑现	人工复核和错误放行
追溯与冷链	批次关联、预警有效、定位准确	损耗、缺货、周转和客诉	断链、篡改、超时升级和召回审批
知识助手	引用正确、版本正确、拒答质量	咨询和培训时间、问题解决率	高风险问题转专家、纠错回写

验收周期要覆盖真实季节和生产波动。单次演示或平均准确率无法替代跨地块、跨品种和边界工况测试。

十、风险边界

- 专业责任：农艺、兽医、水产和林业建议需要来源、版本和适用条件；模型不承担资质责任。
- 物理安全：农机、无人机、阀门和设施设备使用确定性控制与安全联锁，大语言模型不进入唯一控制链。
- 长期漂移：季节、区域、品种、病原、设备和经营模式变化会导致模型失效，需要持续复评。
- 数据权属：农户、合作社、平台和设备商之间明确采集、共享、训练、保存和删除范围。
- 成效归因：产量和损耗同时受天气、品种、管理和市场影响，需要对照基线，不能全部归因于智能体。

十一、来源索引

核心来源

- 农业 AI 如何从试验走向规模化应用
- 农业 AI 智能体成熟度评估体系
- 生猪采购助手行业方案
- 海大集团销售管理公开案例
- 中国人工智能学会农业大模型白皮书转载
- 农机制造业转型案例及启示
- 十字花科蔬菜智能育种项目启动信息
- 生鲜农产品供应链智能化探索

本章小结

农业智能体的关键能力，是把分散在自然环境、生命过程、现场设备和经营系统中的状态组织成任务。企业应先让风险可观察、建议可追溯、动作可确认、结果可回写，再逐步开放调度和设备接口。

现阶段，种植、农机和生鲜供应链已经形成清晰的应用路径。畜牧、林业和渔业可围绕繁育、饲喂、疫病、水质、投喂、防火和资源管理继续建设垂直智能体。

第二章 能源、矿业与公用事业：AI 智能体进入设计、生产、运维与安全闭环

能源、矿业与公用事业的 AI 智能体应用，已经进入电力工程知识、石化巡检、矿山安全和设备运维，并向发电运行、电网交易、油气生产和水气热运营延伸。

本章核心结论

能源、矿业与公用事业具有长资产周期、强实时数据和高安全责任。AI 智能体最现实的入口集中在工程知识与审查、设备诊断、巡检整改、风险预警和客户服务。它们可以读取图纸、规程、SCADA、DCS、视频和工单，生成建议、任务与证据包，并跟踪处理结果。

本章覆盖油气勘探解释、煤机预测维护、电力图纸识别与审核、矿山安全闭环、光伏远程诊断和排水项目审查。专业模型、预测算法、机器视觉、运筹优化和控制系统都是重要能力部件，只有加入目标、工具、动作、反馈和责任链后，才构成完整智能体。

本行业的核心边界是控制权。电网调度、交易报价、设备启停、工艺参数、井下安全和工程签字都可能造成重大后果。大语言模型适合理解问题、调用分析工具、组织证据和协调流程；连续控制、安全联锁、正式调度指令和专业签字必须留在确定性系统与授权人员手中。

一、行业边界与子行业

本章是一个基础设施行业簇，内部需要分别理解六条业务链。

1. 电力与综合能源

覆盖项目开发、设计建设、发电、储能、微电网、电网调度、资源聚合、电力交易、设备运维和客户能源服务。实时性、拓扑约束和供电可靠性决定了智能体只能分级进入生产系统。

2. 油气

覆盖勘探评价、钻完井、油气生产、集输管网、炼化加工、仓储贸易与安全环保。地震和测井解释已经形成明确应用，钻井、采输和管网调度可从专家辅助、风险预警和受控任务执行切入。

3. 煤炭与矿业

覆盖地质勘探、设计掘进、开采、井下运输、洗选、设备运维、安全和生态修复，当前应用重点集中在煤机健康和矿山安全监管。

4. 能源化工

覆盖配方与工艺、连续生产、质量、能耗、设备、安全和环保。它与流程制造交叉，本章关注能源化工专有知识、生产风险和高危设备，通用制造方法在制造业章节展开。

5. 水务、燃气与供热

覆盖水源/气源/热源、管网、泵站、调度、计量、漏损、抢修、收费和民生服务。只补到排水工程审查，生产运营材料仍然明显不足。

6. 能源设备制造与解决方案

储能系统、电气柜和能源工程产品属于制造业，但售前技术、方案设计和运维知识面向能源客户。本章保留海辰储能“小易同学”等行业知识案例，同时避免将设备制造链等同于能源运营链。

二、核心业务链全景

资源勘探与规划 → 投资与项目开发 → 设计 采购与工程建设 → 并网 投产或通气 → 生产运行与调度 → 交易计量与客户服务 → 巡检 运维与抢修 → 安全 环保与应急 → 资产改造 退役与复盘

环节	主要角色	输入与输出	典型瓶颈	AI 智能体机会
资源勘探与规划	地质、规划、投资人员	地震、测井、资源、市场和政策 → 目标与规划候选	多源解释耗时，经验分散	地震/测井解释、政策研究、选址智能体
投资与项目开发	投资、财务、工程、审批	资源、负荷、收益和风险 → 项目决策包	情景复杂，假设难追溯	投资测算、风险审查智能体
工程设计	设计院、工程师、审查人员	图纸、计算书、规范、设备参数 → 设计成果和审查意见	图文不一致，规范版本多	识图、设计生成、联合审核智能体
建设与投运	业主、总包、监理、设备商	进度、质量、调试、验收 → 投运资产	文档和现场状态割裂	工程资料、调试验收、项目风险智能体
生产运行	调度员、值长、运行人员	SCADA/DCS、拓扑、负荷、出力、工况 → 运行方案	实时性强，约束不可违反	运行分析、微网和资源聚合智能体
交易与计量	交易员、营销、财务	电价、负荷、规则、合同、计量 → 报价和结算	规则变化快，错单风险高	市场研究、报价建议、偏差风险智能体
巡检与运维	运维、设备、检修班组	告警、视频、传感器、手册、工单 → 诊断和检修	告警多、知识分散、闭环慢	巡检、预测维护、故障诊断和工单智能体
安全环保	安监、环保、应急、监管部门	人员、设备、环境、视频和制度 → 预警、整改、复核	漏报代价高，跨主体协调难	风险闭环、作业许可、应急辅助智能体
客户与公用服务	客服、抢修、运营、用户	报修、计量、管网和服务记录 → 工单和反馈	派单慢、现场信息不完整	客服、漏损、抢修和服务工单智能体

三、逐环节业务流程与问题

1. 勘探解释：专业模型需要专家复核与结果回写

地震解释和测井处理依赖高维数据、区域地质知识和专业软件。智能体可以调取资料、运行专业模型、比较历史解释、标记异常并生成候选报告。它的价值在于缩短资料准备和重复分析时间，并保留每条结论的依据。

井位和开发方案牵涉投资与安全。地质专家需要审查模型适用范围、置信区间和异常样本，后续钻探与生产结果再写回模型评测。

2. 工程设计：图纸、文档、规范和参数联合审查

电力工程设计包含一次图、二次图、设备表、设计说明和计算书。单纯 OCR 只能提取文字；设计智能体还需要理解图元、连接关系、设备参数和规范版本，并将问题定位到具体图纸和条款。

设计生成应在副本或版本分支中进行。注册工程师或具备相应资格的人员承担最终审查和签字责任，系统保存模型版本、问题清单、人工修改和审签记录。

3. 生产与调度：语言模型负责协调，专业求解器负责约束

发电、储能、微电网和配网调度同时面对负荷、出力、设备状态、拓扑和安全约束。智能体可以理解调度目标、读取实时数据、调用潮流计算、仿真和优化器，给出候选方案与风险解释。

生产控制和调度指令需要通过原有状态机、规程、双人确认和保护系统。试点阶段先采用影子模式，只生成建议并与调度员方案做历史回放比较。

4. 设备健康与故障诊断：从告警走到检修确认

煤机、光伏逆变器、泵组和石化设备会产生振动、温度、电流、油液、告警和维修记录。设备智能体对多模态状态进行健康评分和根因排序，调用手册与历史案例，生成检查步骤、备件建议和工单。

远程诊断有明确边界。它可以发现曲线异常、定位可能区域和安排优先级，无法完成绝缘测量、现场清洗、紧固、换件和高风险作业。最终结果由现场人员复检并回写。

5. 安全监管：识别、派单、整改、复核和归档

矿山和石化安全涉及人员、设备、环境和管理四类要素。机器视觉和传感器负责发现异常，规则与模型完成风险分级，工作流把问题派给责任人，整改证据进入复核和销项。

智能体不能把“识别准确率”当作全部价值。真正需要验收的是严重风险漏报、无效打扰、整改时效、复核完整率、应急升级和数据不可用时的降级能力。

6. 公用事业项目与客户服务：先从资料边界清楚的任务切入

排水项目审查具有清晰的输入、规则和输出：接收图纸、计算书和说明，检查完整性与参数，定位规范风险，生成审查意见草稿，最后由专家批准。

水务、燃气和供热运营可沿漏损监测、泵站诊断、客服报修和抢修工单建设智能体，先从只读分析和人工确认开始，再逐步连接工单闭环。

四、AI 智能体全景图

业务链	代表智能体或相邻能力	主要动作
油气勘探	地震解释专业模型/智能体候选	解释候选、目标识别和报告
油气开发	测井解释智能体候选	曲线处理、储层解释和异常提示
行业知识	能源化工专家知识智能体	检索、解释和方案辅助
解决方案	海辰储能“小易同学”	问答、方案草稿和技术偏差提示
电力设计	电力图纸识别智能体	图元、关系和参数结构化
电力设计	设计生成智能体	候选图纸、计算和设备选型
电力交付	设计审核与交付智能体	图文联合审核和审签包
配电知识	万榕“榕博士”	标准和历史方案问答
发储微网	微电网管理智能体	状态评估和运营建议
储能运营	EMS 智能调度系统	充放电优化和资源聚合
配网调度	配网调度智能体候选	异常识别和转供建议
电力交易	交易智能体候选	预测、报价和风险优化
石化巡检	东明石化智能巡检闭环	识图、通知和整改跟踪
煤机运维	煤机设备预警分析多智能体	健康评分、根因、工单
光伏运维	光伏远程故障诊断智能体	原因排序和现场任务
矿山安全	矿山安全风险闭环智能体	识别、派单、整改、复核
排水工程	排水项目审查智能体	完整性、规范和意见草稿
水气热运营	漏损、抢修和调度智能体	监测、派单与复检
充电运营	故障、工单和价格系统	预测、派单和建议

五、重点智能体工作卡

1. 电力图纸识别与设计审核智能体

字段	内容
服务对象	电力设计工程师、校核人员、项目负责人和审签人
触发条件	新设计、既有图纸数字化、版本变更或正式送审前
主要输入	一次/二次图纸、设备表、设计说明、计算书、规范和设备参数
判断与规划	识别图元与连接，核对参数、文图一致性、缺项和规范冲突
工具与系统	CAD/ 电力设计软件、计算引擎、设备库、规范库和审签系统
输出与动作	结构化图纸、设计草案、问题定位、依据和审签包
人工控制点	草案进入版本分支；注册工程师或授权人员终审签字
验收指标	图元识别、严重问题召回、误报、工程师修改率、错误放行和版本追溯

2. 煤机设备健康与预测维护智能体

字段	内容
服务对象	设备工程师、井下检修人员、生产调度和安全管理者
触发条件	定时健康评估、状态异常、报警或计划检修
主要输入	振动、油液、电流、温度、负荷、历史故障、检修和备件记录
判断与规划	健康评分、异常检测、根因回溯、案例比对和检修策略
工具与系统	工业互联网、边缘终端、EAM、设备知识库和工单系统
输出与动作	分级预警、根因候选、检查步骤、维修建议和工单草稿
人工控制点	检修人员确认诊断；停机、拆检和井下作业按规程审批
验收指标	漏报、误报、提前量、根因 Top-N 命中、误修、停机和工单关闭率

3. 矿山安全风险闭环智能体

字段	内容
服务对象	矿山企业安全部门、班组和监管监察人员
触发条件	视频/传感器异常、制度巡查、隐患逾期或应急事件
主要输入	视频、人员定位、设备和环境监测、隐患、规则和责任组织
判断与规划	风险识别、分级、责任匹配、处置时限和升级路径
工具与系统	安全监控、人员定位、工单、音视频会商和监管平台
输出与动作	预警、整改工单、复核任务、销项记录和应急会商通知
人工控制点	安全人员确认风险和停产处置；监管执法与应急指挥由法定主体负责
验收指标	严重风险召回、无效打扰、发现到派单时间、按期整改、复核销项和审计完整

4. 光伏远程故障诊断智能体

字段	内容
服务对象	光伏场站运营、远程监控中心和现场运维人员
触发条件	逆变器、组串、功率或环境数据出现异常
主要输入	SCADA、逆变器和组串曲线、告警、气象、设备台账与历史维修
判断与规划	判断数据质量，定位异常区域，排序原因，决定远程处置或现场检查
工具与系统	场站监控、气象、资产台账、EAM 和移动工单
输出与动作	根因候选、优先级、现场检查任务、备件建议和诊断报告
人工控制点	现场测量、清洗、紧固、换件和电气安全作业由持证人员执行
验收指标	远程解决率、误诊、现场复核、平均修复时间、故障复现和发电损失

六、代表案例

案例一：东明石化智能巡检——视觉识别进入整改链

东明石化公开案例将现场拍照、时间地点、液位温度等信息纳入巡检流程。系统识别风险点后通知责任人、跟踪整改，并向相关人员推送事故案例。其价值来自“识别—通知—整改—跟踪”的连续链条。

东明石化智能巡检将机器视觉、规则工作流和智能体判断组合起来。企业验收时应分别评估识别准确率、工单闭环效率和智能体判断的业务贡献。

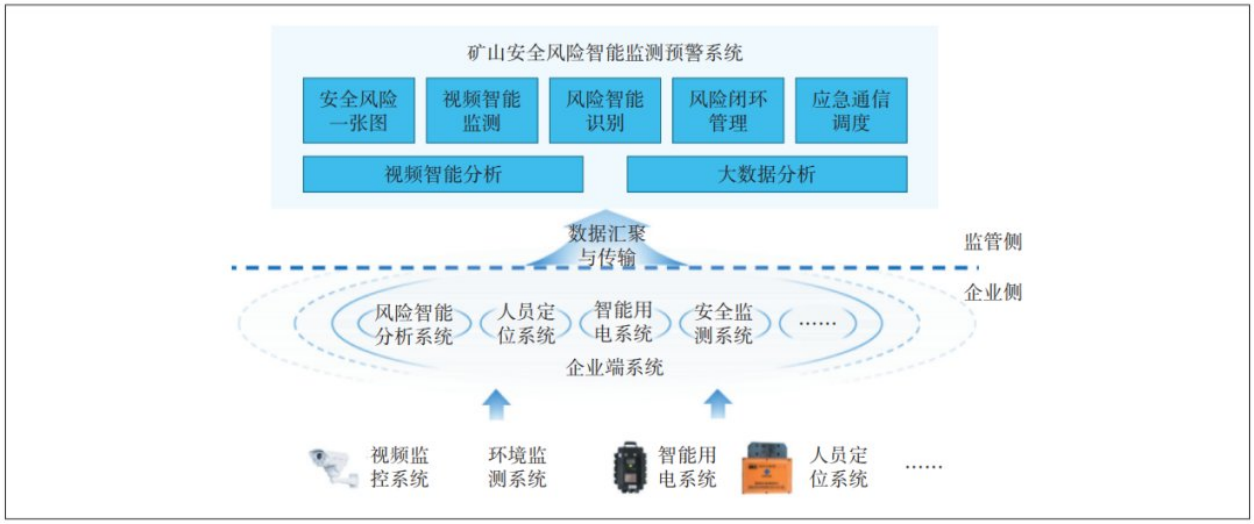


图：东明石化巡检案例图

案例二：矿山安全风险监测预警系统——监管闭环比单点识别更重要

研究材料把系统定位为视频智能分析与大数据分析的组合，覆盖风险识别、分级预警、整改反馈和政企应急联动。其核心价值是把“人、机、环、管”信息汇聚到同一监督链。

该类系统的正式验收应明确样本范围，并持续评估漏报、误报、现场整改闭环和长期运行稳定性。



图：矿山安全风险闭环定位示意

案例三：电力设计 AI——能生成还要能审查、追溯和签字

行业方案描述了识图、设计、计算、文档和双模态审核链。白皮书保留其中的工作机制：图纸和文档一起解析，问题定位到参数与规范，工程师最终审查并签字。

文中的效率、覆盖率和项目范围属于公开案例，当前不作为已验证成效。。



图：电力设计图文联合审核应用图

案例四：光伏远程诊断——明确“远程能做什么”

光伏运维材料把远程诊断限定在数据异常发现、区域定位、原因排序和任务准备。现场测量、清洗、维修和安全操作仍由运维人员完成。这种边界清晰的分工，比把远程平台包装成全自动运维更适合作为企业试点依据。

七、系统、数据与权限

1. 数据底座

- 实时数据：SCADA、DCS、EMS/BMS、IoT、保护和告警；
- 空间与资产：GIS、拓扑、线路、设备、井巷、管网和场站台账；
- 工程数据：图纸、计算书、BOM、规范、设计变更和竣工资料；
- 运维数据：巡检、缺陷、维修、备件、工单、工作票和停机记录；
- 经营数据：负荷、出力、电价、合同、计量、结算和客户服务；
- 风险知识：两票三制、作业规程、事故案例、应急预案和环保要求。

实时数据必须统一时间、设备标识和质量状态。智能体需要知道数据是否缺失、延迟、估算或失真。

2. 工具与系统

智能体可能调用专业解释软件、潮流计算、仿真、运筹求解、CAD、EAM、工单、市场交易、通知和文档系统。高风险系统采用只读、建议、受控写入和控制四级权限。

3. 权限与人工控制点

动作	默认控制方式
知识检索、数据汇总和报告生成	可自动执行，显示数据质量、引用和版本
创建低风险巡检、复核和资料任务	可自动执行，具备限频、去重和撤回
设计草案、诊断建议和交易方案	专业人员复核后进入下一环节
工作票、操作票、调度指令和正式报价	由授权人员按现有制度批准
设备启停、参数调整和网络拓扑变更	确定性控制系统执行，双人确认并保留人工接管
工程签字、监管执法和应急指挥	由法定责任主体承担

所有写入动作记录身份、输入、规则和模型版本、候选方案、批准人、执行结果、失败和回退。

八、企业落地路线

阶段 0：建立场景基线

选一个可量化问题，例如设备告警分诊、巡检整改、设计预审或光伏远程诊断。记录当前耗时、误报漏报、停机、人工复核和事故近失事件。

阶段 1：只读知识与分析

先做规程问答、历史案例检索、设计资料比对、设备状态报告和风险清单。验证引用、版本、权限和拒答质量。

阶段 2：影子运行与受控执行

智能体生成调度、交易、诊断或设计建议，与专家既有方案并行比较；允许创建工单和草稿，正式动作由人确认。

阶段 3：有限闭环

对低风险、规则明确的提醒、资料任务和常规工单开放自动执行。异常和高风险分支自动升级人工，系统具备超时、重试和回滚。

阶段 4：生产系统和规模复制

经过历史回放、仿真、故障注入和现场试点后，再连接生产系统。复制时按设备类型、工况、地域和组织重新验证，不能只复制提示词。

九、评测与验收

场景	任务质量	业务结果	工程与风险
工程知识	引用正确、版本正确、拒答质量	查询和方案准备时间	越权内容、专家转接和纠错回写
图纸审核	图元识别、严重问题召回、误报	审查周期和返工	错误放行、签字保留、版本追踪
设备诊断	提前量、根因 Top-N、误诊和漏报	修复时间、非计划停机、备件浪费	误修、高风险建议拦截和现场复核
安全闭环	严重风险召回、无效打扰	发现到处置、按期整改	复核销项、应急升级、审计完整
调度与交易	方案可执行、预测和收益偏差	供需平衡、偏差考核和收益	约束违反、错单、接管和最大潜在损失
公用事业工单	分类、路由和信息完整	响应、修复和客户满意	重复派单、重大事件转人工和隐私

高风险场景必须增加历史回放、数字孪生或沙箱、边界工况、接口故障、网络断开和模型不可用测试。

十、风险边界

- 实时与确定性：大语言模型不能成为毫秒级控制、保护和安全联锁的唯一决策者。
- 专业责任：工程签字、调度命令、工作票、监管执法和应急指挥由具备授权或资质的人员承担。
- 数据质量：传感器漂移、拓扑错误、时钟不同步和缺失数据会直接改变判断，必须显示质量状态。
- 网络与接口：生产系统需要隔离、白名单、最小权限、幂等、超时、重试、回滚和人工接管。

十一、来源索引

核心来源

- 东明石化工厂巡检公开案例
- 海辰储能解决方案管理公开案例
- 微电网管理智能体线索
- 新能源智能化运维平台线索
- 矿山安全风险智能监测预警系统研究
- 能源化工行业大模型及 18 个应用场景
- 煤机设备 AI 健康管家
- 电力设计识图、设计与审核
- 光伏远程故障诊断
- 排水项目审查智能体实践方法

本章小结

能源行业最值得建设的智能体，往往先出现在信息复杂、流程漫长、又能保留人工责任的环节：工程审查、设备诊断、巡检整改和风险协同。随着系统进入调度、交易和控制，治理要求会快速上升。

企业应以数据质量、专业规则和权限体系作为生产底座。智能体负责发现、解释和协调，确定性系统与授权人员负责高风险动作，才能把效率提升和安全责任放在同一套架构里。

第三章 制造业：AI 智能体进入研发、工艺、供应链、生产与质量全链路

制造业 AI 智能体已经覆盖研发、工艺、供应链、采购、生产、质量、设备、仓储、售后和经营管理等关键业务链。

本章核心结论

制造业不只有车间生产。一个制造企业从市场需求开始，要经历产品研发、工艺设计、供应商协同、采购、计划、生产、质量、设备、仓储物流、交付售后和经营管理。工艺路线、参数窗口、SOP 更新、CAD 操作、三单核验和采购比价，同样是制造业智能体的重要入口。

现阶段最容易产生确定价值的，不一定是让 AI 直接控制设备，而是让 AI 持续读取业务状态、发现异常、调用知识、生成任务、通知责任人并跟踪关闭。越接近 PLC、工艺参数、安全联锁和产品放行，越需要确定性规则、专业模型、人工确认和独立安全系统。

当前制造业 AI 智能体可以概括为六类：

- 监测预警智能体；
- 工业知识与诊断智能体；
- 审核与质量把关智能体；
- 计划与优化智能体；
- 跨系统流程执行智能体；
- 感知执行与多智能体闭环。

本章重点覆盖三块业务层：

- 工艺层：从“查 SOP”扩展到工艺路线生成、参数窗口建议、异常根因验证和工程变更后的文件联动；
- 工程软件层：从回答设计问题扩展到在 CAD 副本或分支中执行建模、修改和规则校核；
- 采购财务层：从供应商管理扩展到报价标准化、历史比价、合同/收货/发票三单核验和付款前风险拦截。

这些对象的共同边界是：智能体可以提出方案、生成草稿、调用工具和推动复核，但工艺发布、付款、产品放行和关键参数修改仍由授权人员负责。

一、行业边界：制造业共享一条骨架，但不是一种生产方式

制造业内部差异很大。钢铁、化工等流程制造关注连续工艺、能耗、装置稳定和安全联锁；汽车、装备和电子等离散制造关注 BOM、工艺路线、装配、供应商和质量追溯；食品、医药、日化等混合制造还需要同时处理配方、批次、保质期、卫生和法规要求。

本章先提炼制造企业共用的业务骨架，再在每个智能体中说明适用条件。垂直行业已经在本书单列的汽车、医药、食品等案例，以主营价值链确定主归属，同时保留“制造方法”作为交叉标签，避免重复统计。

1. 流程制造

典型行业包括钢铁、有色、石化、化工、建材等。核心对象是连续工艺、装置、配方、能耗和安全。适合重点关注过程监测、工艺异常、能源优化、设备预测和安全环保智能体。

2. 离散制造

典型行业包括汽车、机械装备、电子、航空航天等。核心对象是 BOM、零部件、工艺路线、工位、装配、供应商和项目交付。适合重点关注研发审核、供应商协同、排产、视觉质检、设备维修和交付服务智能体。

3. 混合制造

典型行业包括食品饮料、医药、日化、轮胎等。既有配方和批次连续过程，也有包装、装配等离散环节。智能体需要同时理解批次、配方、物料约束、设备状态和质量规则。

二、制造业核心业务链

市场与订单 → 产品与研发 → 工艺设计与工程文件 → 供应商与采购 → 采购结算与付款核验 → 产销协同与计划 → 生产执行 → 质量管理 → 设备与能源 → 安全与环保 → 仓储与物流 → 交付与售后 → 经营与持续改善

这条链不是简单的线性流程。质量问题会反向推动设计变更，设备状态会影响排产，客户投诉会追溯到批次、供应商和工艺参数，订单变化也会同时影响采购、库存和交付。

业务环节	核心流程	关键业务对象	常见问题	AI 智能体主要机会
市场与订单	市场洞察、线索、报价、投标、订单评审、需求预测	客户、产品、报价、合同、订单	信息分散、报价慢、订单变更传递不及时	市场情报、报价、投标、订单评审、需求预测智能体
产品与研发	需求、方案、CAD 设计、BOM、试制、测试、变更、交付物审批	需求、模型、图纸、BOM、标准、测试、变更单	标准检索慢、建模重复、设计错误复现、进度不透明	需求解析、设计知识、CAD 执行、设计校核、BOM 审核、变更影响智能体
工艺设计与工程文件	工艺路线、参数窗口、控制计划、SOP、工艺变更、现场知识	工序、设备、工装、参数、检验点、工艺文件	经验依赖强、工艺文件更新慢、异常难关联人机料法环测	工艺路线、参数推荐、异常分析、SOP 影响分析、工艺知识智能体
供应商与采购	寻源、准入、询比价、采购执行、来料、绩效、协同整改	供应商、物料、报价、历史价格、交期、质量	报价格式不一、主数据混乱、跨组织协同慢、风险发现晚	供应商预审、主数据治理、多维比价、采购执行、风险监测、委外质量智能体

业务环节	核心流程	关键业务对象	常见问题	AI 智能体主要机会
采购结算与付款	合同/订单、验收/入库、发票、付款申请和审批	合同、订单、收货、发票、税率、金额、付款状态	三单人工核对慢、重复付款、字段和审批口径不一致	三单核验、付款审核、异常证据整理和审批协同智能体
产销协同与计划	S&OP、主生产计划、物料计划、能力平衡、排产	需求、库存、产能、物料、交期	计划依赖经验、频繁插单、缺料、换型损失	S&OP 模拟、齐套分析、排产优化、瓶颈预测智能体
生产执行	派工、领料、报工、过程监测、异常、交接班	工单、设备、人员、工艺参数、批次	数据滞后、异常靠人发现、经验难复制	报工助手、过程监测、交接班、作业指导、异常分析智能体
质量管理	来料、过程、终检、放行、偏差、CAPA、追溯、客诉	检验标准、图片、测量值、缺陷、批次	漏检误报、问题闭环慢、追溯困难	视觉质检、质量审核、异常根因、8D/CAPA、追溯智能体
设备与能源	点检、保养、维修、备件、预测性维护、能源管理	设备、报警、振动、温度、能耗、维修记录	依赖老师傅、停机损失、维护被动	故障诊断、维修协同、预测性维护、备件、能源优化智能体
安全与环保	风险辨识、巡检、作业许可、隐患整改、排放监测、应急	人员、现场图片、危化品、排放、预案	违章识别晚、隐患跟踪断点、高风险动作不可容错	安环巡检、作业许可审核、隐患闭环、应急辅助智能体
仓储与物流	收货、上架、补货、拣选、盘点、装车、运输、运价	库位、库存、批次、车辆、路线、运价	库存不准、任务调度低效、异常响应慢	库存预警、仓内调度、装载校验、运输调度、运价监测智能体
交付与售后	安装、调试、服务、备件、保修、退换、召回	客户、设备、服务单、备件、故障、索赔	现场知识不足、响应慢、问题难回流研发	服务诊断、工单协同、备件建议、索赔审核、质量回流智能体
经营与持续改善	项目、成本、回款、绩效、精益、数据治理	项目、合同、成本、任务、指标、知识	多系统数据割裂、风险发现滞后	项目风险、经营报告、成本分析、精益改善、数据治理智能体

三、制造业 AI 智能体全景

1. 市场、订单与客户经营

AI 智能体	服务对象	主要任务与动作
制造业市场情报智能体	市场、战略、销售	汇总政策、产业、竞品和客户动态，生成机会与风险提示
客户需求解析智能体	销售、产品、研发	从会议、邮件、招标文件提取需求，形成结构化需求清单
方案与报价智能体	售前、销售、成本	调用产品配置、历史报价、成本与交期数据生成报价草案
投标智能体	售前、商务、法务	拆解标书、分派材料、检查响应完整性、生成投标文档
订单评审智能体	销售、计划、研发、采购	检查配置、产能、物料、交期和合同风险，发起会签
需求预测智能体	市场、计划、供应链	结合历史销量、促销、季节与外部变量输出预测和偏差解释
回款风险智能体	销售、财务、项目负责人	监测合同、开票、交付和回款节点，预警并创建催办任务

2. 产品与研发

AI 智能体	服务对象	主要任务与动作
产品需求管理智能体	产品、系统工程师	合并需求、识别冲突、建立需求到设计和测试的追踪关系
技术标准与设计知识智能体	研发、工艺	检索标准、图纸、历史方案和专家经验，给出可追溯答案
工业 CAD 设计执行智能体	研发、设计工程师	理解自然语言设计意图，在 CAD 副本中创建草图、特征或参数修改并返回执行记录
CAD 设计校核智能体	研发、工艺、质量	检查干涉、规则、可制造性和工程变更影响，定位问题并给出修订建议
方案生成与复用智能体	研发、售前	根据约束检索历史模块和相似项目，生成方案草案
BOM 一致性审核智能体	研发、工艺、采购	检查 BOM 版本、替代料、图纸和工艺文件的一致性
设计评审智能体	研发、质量	按标准和历史失效案例预审交付物，提示高风险项
工程变更影响分析智能体	研发、计划、采购、质量	分析变更对库存、供应商、工艺、测试和交付的影响
研发项目风险智能体	项目经理、研发负责人	聚合进度、采购、测试和问题数据，提前识别风险
测试分析与报告智能体	测试、研发	分析测试数据、发现异常模式、生成带引用的报告
IPD 交付物预审智能体	项目、质量、签审人	在提交前检查格式、标准、历史问题与完整性，保留人工签审
工艺路线生成智能体	工艺工程师、生产准备	结合产品结构、设备、工装和历史工艺生成候选工序、检验点和工时建议
工艺参数窗口智能体	工艺、质量、设备	关联过程参数与质量结果，调用专业模型生成参数窗口和试验建议
SOP 影响分析与更新智能体	工艺、文控、培训	识别工程变更影响的工序、设备、检验点和岗位，生成多角色文件草稿

3. 供应商与采购

AI 智能体	服务对象	主要任务与动作
供应商准入智能体	采购、质量、法务	收集资质、识别缺失和风险、生成预审意见
供应商技术预审智能体	研发、供应商质量	解析技术报告和尺寸链，标记关键风险供专家审核
供应商主数据治理智能体	采购运营、数据管家、IT	全量校验、异常分类、责任分派、复检并生成治理日报
采购多维比价智能体	采购、成本、业务部门	解析不同格式报价，结合历史价格、规格、交期、税运费和商务条件形成比选依据
三单核验与付款审核智能体	采购、仓库、财务	核对合同/订单、收货/验收和发票，标记金额、数量、税率与对象异常
采购执行智能体	采购、计划	创建或更新采购任务、跟踪确认函和交期、提醒异常
供应商风险监测智能体	采购、风控	监测经营、合规、交付、质量和舆情风险，触发复核
委外生产监控智能体	采购、制造、质量	统一收集供应商生产和良率数据，监测异常
委外异常分析智能体	供应商质量、工艺	识别良率波动、分析根因、生成异常单和 8D 任务
供应商绩效智能体	采购管理	汇总质量、交付、成本与整改表现，形成分层与改进建议

4. 产销协同、物料与排产

AI 智能体	服务对象	主要任务与动作
S&OP 情景模拟智能体	销售、计划、财务、供应链	模拟不同需求、产能、库存和成本情景，支持协同决策
物料齐套智能体	计划、采购、仓库	持续检查工单、BOM、库存和采购到货，预警缺料
库存安全线智能体	计划、仓库、采购	扫描库存和消耗速度，触发补货或风险提醒
产能瓶颈智能体	计划、生产	识别设备、人员、模具和工艺瓶颈，提出平衡建议
智能排产智能体	计划、生产	在交期、产线、换型、物料等硬约束下生成排产方案
插单影响分析智能体	销售、计划、生产	计算插单对现有订单、物料、换型和交付的影响
换型优化智能体	计划、工艺、生产	在满足交期的前提下减少换型次数和时间

5. 生产执行

AI 智能体	服务对象	主要任务与动作
语音报工智能体	一线员工、班组长	将语音转为结构化产量、工时、物料和异常记录
生产状态监测智能体	班组长、工艺、厂长	读取 MES 和现场数据，生成实时状态、趋势与风险提示
智能交接班智能体	班组、生产管理	汇总本班产量、参数、异常和未完任务，生成交接报告
作业指导智能体	一线员工、工艺	根据产品、设备和工序提供匹配版本的 SOP 与注意事项
生产异常分诊智能体	班组、工艺、质量、设备	根据异常类型路由责任人，推荐排查顺序并跟踪关闭
工艺偏差分析智能体	工艺、质量	结合参数、批次和历史偏差寻找可能原因
工艺参数建议智能体	工艺专家	在规则和机理约束下生成调整建议，必须由专业人员确认
生产异常多智能体分析系统	工艺、制造、工业工程、质量	将自然语言问题拆解为数据查询、假设生成、验证、图表和根因报告
生产任务协调智能体	生产管理	根据工单状态创建任务、催办、升级并回写执行结果

6. 质量管理

AI 智能体	服务对象	主要任务与动作
来料检验智能体	IQC、采购质量	根据物料风险和历史表现生成抽检建议、辅助判定异常
工业视觉质检智能体	质量、一线班组	读取图像，结合特征、字符、规则和工作流识别缺陷并告警
质量文件预审智能体	质量、项目、供应商	审核报告、记录和交付物是否符合标准与完整性要求
过程质量监测智能体	质量、工艺	监测 SPC、良率和过程参数，发现漂移并创建异常任务
质量异常根因智能体	质量、工艺、设备	聚合人机料法环测和历史案例，生成可验证的根因假设
8D/CAPA 协同智能体	质量、责任部门、供应商	生成问题单、分派措施、追踪证据、检查关闭条件
质量追溯智能体	质量、售后、生产	从客户问题反查批次、物料、设备、人员和工艺记录
客诉质量分析智能体	售后、质量、研发	聚类客户问题，识别高频失效并推动设计和工艺改进

7. 设备、备件与能源

AI 智能体	服务对象	主要任务与动作
设备知识智能体	维修工、设备工程师	检索手册、图纸、停工报告和历史维修案例
故障诊断智能体	维修工、设备工程师	读取报警、现象、语音和传感器数据，给出原因与排查步骤
维修工单协同智能体	设备管理、维修班组	接收告警、派发任务、跟踪维修、回访结果并回写知识
预测性维护智能体	设备、生产、计划	结合传感器、机理和历史故障预测风险，生成维护建议
保养计划智能体	设备、计划	根据运行时长、状态和生产计划调整保养窗口
备件智能体	设备、仓库、采购	预测备件需求、检查库存、推荐替代件并触发补货
OEE 损失分析智能体	厂长、生产、设备	分析停机、速度和质量损失，定位主要改善机会
能源监测智能体	能源、生产、设备	监测单耗、峰谷和异常用能，定位异常设备与班次
能源优化智能体	能源、工艺、计划	在产量、工艺和价格约束下生成用能优化方案

8. 安全与环保

AI 智能体	服务对象	主要任务与动作
现场违章识别智能体	安环、班组	分析现场图片和视频，识别违章并通知责任人
高危设备监测智能体	安环、设备	聚合巡检、设备和报警信息，诊断并跟踪隐患
作业许可预审智能体	安环、作业负责人	检查动火、受限空间、高处等许可材料和前置条件
隐患整改闭环智能体	安环、责任部门	生成整改任务、检查证据、逾期升级和复查
环境排放监测智能体	环保、生产	监测排放趋势和异常，关联生产批次与设备状态
应急辅助智能体	应急指挥、现场人员	检索预案、汇总态势、生成行动建议和信息通报

9. 仓储、物流与交付

AI 智能体	服务对象	主要任务与动作
库存异常智能体	仓库、计划、财务	识别账实差异、呆滞、超储、临期和安全库存风险
仓内任务调度智能体	仓库	编排收货、上架、补货、拣选、盘点和人员设备任务
装载与发运校验智能体	仓库、物流、质量	校验产品、数量、包装、标签、车辆和单证
运输调度智能体	物流、销售	根据订单、车辆、路线、时窗和成本生成调度方案
国际运价监测智能体	国际营销、物流	汇总航线运价、计算趋势、波动超阈值时按区域预警
交付异常智能体	销售、物流、客户服务	监测延迟、破损、拒收和缺件，路由责任人并跟踪处理

10. 售后与全生命周期服务

AI 智能体	服务对象	主要任务与动作
安装调试智能体	现场工程师、客户	根据设备型号和现场条件生成步骤、检查结果和报告
售后诊断智能体	服务工程师、客服	理解故障描述、图片和日志，给出排查与备件建议
服务工单智能体	客服、服务经理、工程师	分诊、派单、调度、跟踪 SLA 并回写结果
备件推荐智能体	服务、仓库、客户	根据设备、故障和库存推荐备件与替代件
保修与索赔审核智能体	售后、质量、财务	检查保修条件、证据和历史记录，生成审核建议
召回与质量追溯智能体	质量、售后、管理层	确定影响范围、生成客户清单、协调通知和处置
服务经验回流智能体	售后、研发、质量	从工单提炼失效模式和改进建议，写回产品知识

11. 经营、项目、精益与数据治理

AI 智能体	服务对象	主要任务与动作
项目经营智能体	项目经理、经营管理	聚合合同、进度、成本、工时、报销和回款，识别风险
经营报告智能体	管理层、财务、运营	跨系统取数、解释偏差、生成日报周报和经营分析
成本分析智能体	财务、工厂、产品	分析材料、人工、制造费用和质量损失，识别改善空间
付款异常证据整理智能体	财务、采购、审计	汇总三单差异、审批规则和历史重复付款线索，生成复核包并推动关闭
精益改善智能体	精益、一线员工、班组	识别现场改善点、检索历史改善、追踪提案项目
数据质量治理智能体	数据管家、业务、IT	全量体检、问题分派、规则更新、复检和质量报告
人员技能与培训智能体	人力、班组、工艺	根据岗位和任务推荐学习内容，模拟故障和考核
合规与审计准备智能体	质量、财务、内控	汇总证据、检查缺项、形成审计材料包

四、六类重点智能体及工作机制

1. 监测预警智能体：让问题主动找人

监测预警智能体持续读取生产、质量、设备、物料、供应商或物流数据。当指标越过阈值、趋势发生异常或多个条件组合成立时，它不只发送一条消息，还应确定责任对象、生成任务、设置截止时间并跟踪问题是否关闭。

典型链路：

业务事件 → 数据读取 → 规则/模型判断 → 风险分级 → 通知责任人 → 创建任务 → 处理反馈 → 关闭或升级

永卓控股高炉智能体、内江金鸿物料预警、临工重机运价预警和海信供应商数据治理都属于这一大类，但智能程度不同。有些主要依靠规则和自动化，有些加入了分析建议和持续反馈。

2. 工业知识与诊断智能体：把老师傅经验变成可调用能力

这类智能体连接设备手册、SOP、图纸、维修记录、停工报告和专家经验，根据现场的文字、语音、图片、报警代码或传感器数据给出排查建议。

知识问答只是第一步。更完整的诊断智能体需要知道设备型号、当前状态、维修历史和现场约束；当信息不足时主动追问；处理完成后回访结果，并把有效方案转成新的知识案例。

3. 审核与质量把关智能体：在问题进入下一环节前拦截

这类智能体依据标准、历史案例和风险规则，对研发交付物、供应商报告、质量记录、图片和生产结果进行预审。它适合承担高频、重复、规则明确的现有检查，把专家精力留给异常和高风险判断。

关键在于问题前置、依据可追溯，同时保留人工签审。

4. 计划与优化智能体：大语言模型不能替代运筹和机理约束

排产、能源、工艺参数等问题往往包含大量硬约束和优化目标。大语言模型可以理解业务目标、调用数据、解释方案和协调流程，但真正的求解通常仍需要运筹优化、规则引擎、仿真、机理模型或专用预测模型。

一个可靠的计划智能体，应把自然语言交互、约束检查、优化求解、方案解释、人工确认和执行反馈组合起来。

5. 跨系统流程执行智能体：把分析转成业务动作

这类智能体可以连接 ERP、MES、PLM、QMS、WMS、SRM、OA 和协同平台，读取状态、创建任务、更新字段、生成报告、通知责任人和追踪结果。

所有写入动作都需要明确鉴权、幂等、日志、超时、重试和回滚。涉及订单、付款、产品放行、工艺变更和安全操作时，应增加人工批准。

6. 感知执行与多智能体闭环：进入现场，但不绕过安全系统

机器视觉、传感器、边缘模型、知识智能体和流程智能体可以组成工业闭环。例如视觉模型识别异常，规则系统判断是否达到拦截条件，工作流通知质量人员并创建返工任务。

大语言模型不应成为毫秒级控制、PLC 逻辑或设备安全联锁的唯一决策者。物理执行必须服从确定性控制系统、工艺边界和安全标准。

7. 新增的四类重点工作卡

工艺路线生成智能体

字段	内容
服务对象	工艺工程师、生产准备、质量和设备人员
触发条件	新产品导入、产品变型、设备或工装变化、工艺重构
主要输入	图纸/模型、BOM、材料、工艺标准、设备与工装能力、历史工艺
判断与规划	识别制造特征，匹配相似产品，规划工序顺序、设备、检验点和候选工时
工具与系统	CAD/PLM、MES、设备与工装库、历史工艺库、规则或专业求解器
输出与动作	候选工艺路线、风险项、缺失信息和待试验参数，不直接发布正式路线
人工控制点	工艺工程师审核，必要时进行试制和能力验证；文控批准后生效
验收指标	路线可执行率、人工修改量、漏工序、试制问题、量产稳定性和版本一致性



图：工艺路线生成场景示意

工业 CAD 设计执行智能体

字段	内容
服务对象	机械设计、产品研发和工程变更人员
触发条件	新建模型、参数化修改、重复建模或规则校核
主要输入	自然语言设计意图、尺寸、约束、参考模型、标准件和设计规范
判断与规划	把需求转换为可执行的 CAD 操作序列，发现缺失约束并追问
工具与系统	CAD、PDM/PLM、几何约束求解器、标准件库和版本管理
输出与动作	可编辑模型、操作记录、错误信息和设计校核建议
人工控制点	在副本或分支中运行；工程师审查模型、图纸和变更影响后才能合并
验收指标	几何约束满足率、模型可编辑性、命令执行成功率、工程师修改率和回滚成功率

三单核验与付款审核智能体

字段	内容
服务对象	采购、仓库、业务验收、财务和审批人
触发条件	供应商提交发票或付款申请
主要输入	合同/采购订单、收货或验收单、发票、付款规则、供应商和历史支付记录
判断与规划	抽取并标准化字段，核对主体、金额、数量、税率、状态和审批条件
工具与系统	ERP、SRM、WMS、发票/财务系统和审批流
输出与动作	一致项、异常项、证据位置、付款建议和人工复核任务
人工控制点	智能体不拥有付款权；异常解释、供应商沟通和最终审批由授权人员完成
验收指标	异常召回、误拦截、重复付款、字段抽取准确、回写成功和审计可追溯

生产异常多智能体分析系统

字段	内容
服务对象	制造、工艺、工业工程、质量和工厂管理人员
触发条件	周期、良率、设备或工艺指标异常，需要跨维度根因分析
主要输入	IIoT/MES 数据、设备、SKU、介质、供应商、工艺与历史异常
判断与规划	理解问题、生成查询、提出根因假设、调用分析工具验证并形成证据链
工具与系统	数据仓库、IIoT 看板、统计分析、代码/图表工具、工业知识和权限系统
输出与动作	根因候选、证据、图表、处置建议和验证任务
人工控制点	专家确认分析口径和根因；参数调整、停机和工艺变更进入原有审批链
验收指标	根因 Top-N 命中、分析耗时、专家否决率、问题复发率、端到端延迟和错误图表

五、代表案例

案例一：永卓控股高炉智能体——从数据存储到生产洞察

钢铁高炉的原料投入和炉况变化存在时间差，传统交接班依赖纸质记录和工长经验。企业 MES 已经采集上千个数据点，但过去主要承担数据存储，风险仍然需要人自行分析。

高炉智能体将班次记录、生产数据和任务状态组合起来，自动生成基层交接报告，为组长提供风险调度信息，并向厂长输出决策建议。项目公开信息显示，交接班从 30 分钟缩短到 5 分钟，周报从 8 小时缩短到 0.5 小时，任务闭环效率提升 75%；企业应用时应以自身基线、运行周期和实际业务结果独立验收。



图：永卓控股高炉生产案例图

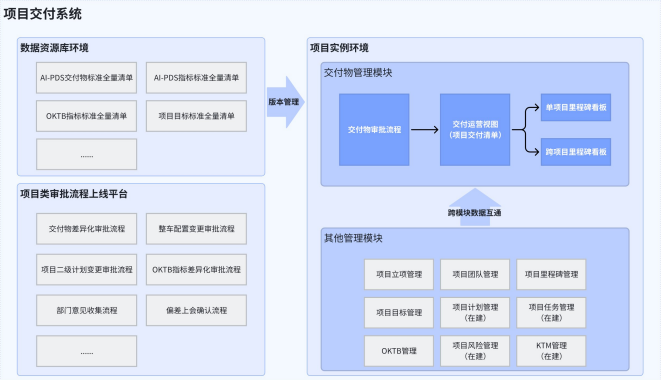
智能体工作卡

字段	内容
服务对象	炉前班组、工长、厂长
触发条件	班次交接、数据异常、日报周报周期
输入	MES 数据点、炉况、班次记录、任务状态
判断	状态汇总、趋势与风险识别、责任任务判断
输出与动作	交接报告、预警、任务、管理建议
人工控制点	工艺参数调整和生产控制由专业人员及控制系统负责
验收	交接用时、预警有效率、任务关闭率、误报漏报、生产稳定性

案例二：阿维塔 AI 虚拟质量工程师——先跑通 IPD，再把 AI 嵌进审签流

阿维塔的案例显示，AI 智能体并不是孤立的聊天入口。企业先把研发项目的交付清单、里程碑、目标、审批和版本管理放到统一流程中，再把 AI 预审核嵌入交付物提交和签审环节。

AI 负责检查格式和交付标准、检索历史问题、形成审核建议，人工签审责任仍然保留。公开案例显示，智能体嵌入业务流后累计调用超过 10 万次，覆盖 3,000 多人；相关效率与准确率均为案例公开口径。



图：阿维塔项目交付体系图

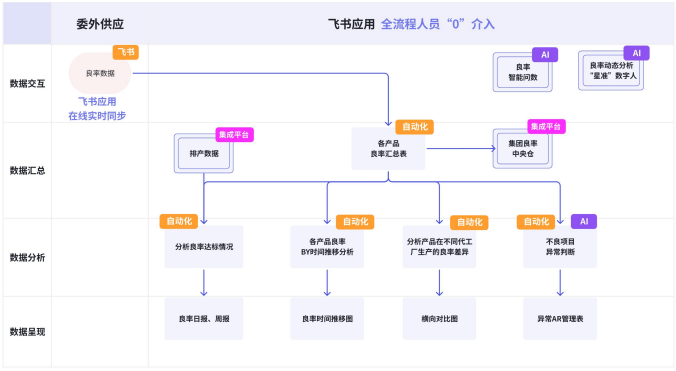
可复用启示

- 先统一交付清单、标准、版本和审批路径；
- AI 先做预检查，不直接替代专业签审；
- AI 意见与人工结论都需要留痕；
- 验收时同时看问题前置发现率、审核时间和错误放行数。

案例三：TCL 华星委外供应商多智能体——跨组织数据和异常闭环

委外供应商的难点不只在采购，而在跨企业的生产秩序。过去 40 多家供应商通过微信群、邮件和表格报送数据，数据流转滞后，良率异常需要人工识别和追踪。

案例将供应商数据收集、良率分析、异常单、8D 整改、绩效和知识沉淀放入统一平台，并设置监控、分析、建议和知识沉淀等角色。需要注意，其中自动催办、公式判断、仪表盘和数据流转主要属于规则和低代码能力；自然语言问答、异常分析和决策建议才是智能体相关部分。



图：TCL 华星委外供应商优化后场景图

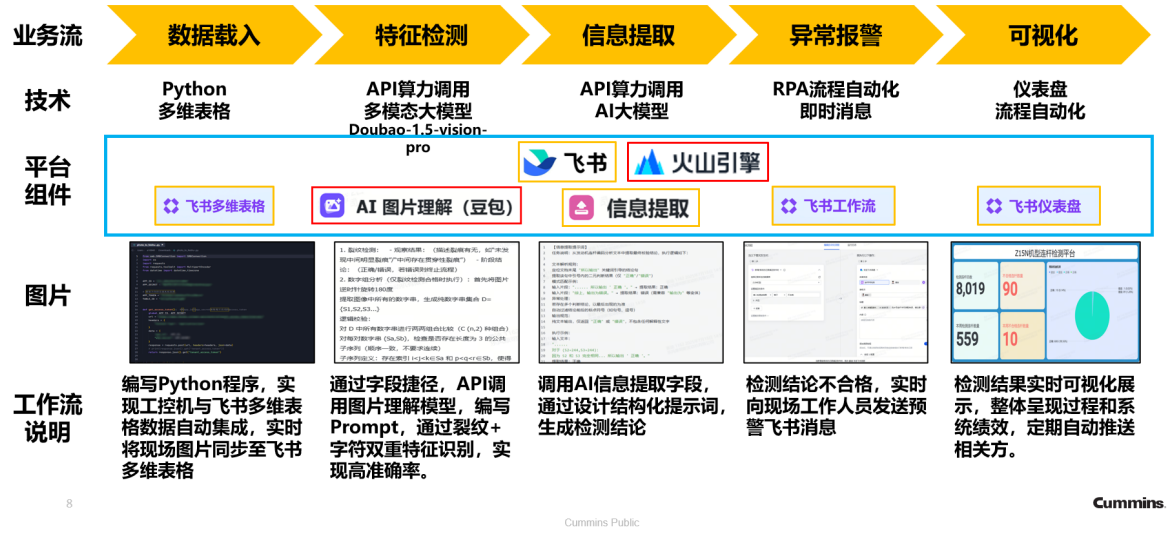
多角色分工

角色	主要任务
生产监控角色	持续读取供应商填报和生产实况
异常分析角色	识别良率波动并形成根因假设
决策建议角色	汇总风险、影响和行动建议
知识沉淀角色	将异常、措施和结果转成可复用案例

案例四：东风康明斯工业视觉质检——模型、规则和工作流组合

传统视觉在连杆配对码场景中受毛坯表面、字符清晰度和润滑脂影响，案例显示最初准确率无法满足现场要求。项目团队没有只依靠一次大模型识别，而是逐步组合裂纹检测、字符识别、模糊匹配、结论提取、异常告警和人工返工。

公开测试记录显示，最终一轮 3,000 张样本中出现 6 张错误，均为误报而非漏报。这个设计体现了工业质量的关键原则：不良漏检和良品误报的代价不同，不能只看一个整体准确率。



图：东风康明斯视觉质检架构

质检链路

产线相机采图 → 发动机号与图片写入 → 裂纹和字符双重识别 → 结构化结论 → 不合格告警 → 人工返工 → 结果可视化

验收重点

- 不良漏检率：应作为硬红线；
- 良品误报率：决定人工复核负担和停线影响；
- 单件推理延迟：是否满足生产节拍；
- 异常拦截成功率：告警是否真正到达现场并完成返工；
- 数据漂移：新产品、光照、相机和工况变化后是否失效。

案例五：东风奕派“设备大师”——从知识问答到五智能体闭环

设备维修常常依赖老师傅，故障处理记录散落在文件夹、群聊和个人经验中。设备大师的公开演进路线包括四步：经验数字化、报警直连与流程闭环、预测性维护、多智能体协作。

在多智能体形态中，前台由设备大师统一承接输入，后台由协调、认知、执行、跟踪和学习五个角色协作。故障修复后，系统主动回访并生成停工报告，再把处理经验写回知识库。

序号	输入源	需求类型	故障类别	Agent路径
001	1a人工	2A真实	3a短停	设备大师→协调→认知→执行→跟踪→学习
002	1a人工	2A真实	3b长停	设备大师→协调→认知→执行→跟踪→认知→学习（+停工报告+5why）
003	1a人工	2A真实	3c新发	设备大师→协调→认知→执行→跟踪→学习（+深度分析+类似故障提醒）
004	1a人工	2A真实	3d再发	设备大师→协调→认知→执行→跟踪→学习（+历史对比+对策有效性）
005	1a人工	2B假想	-	设备大师→协调→认知→学习（跳过执行）
006	1a人工	2C隐患	-	设备大师→协调→认知→执行→学习（提升风险等级）
007	1a人工	2D预防	-	设备大师→协调→认知→执行→跟踪→学习（+历史检修+备件）
008	1b PLC	2A真实	3a短停	设备大师→协调→认知→执行→跟踪→学习（+两次输入+自动报告）
009	1b PLC	2A真实	3b长停	设备大师→协调→认知→执行→跟踪→认知→学习（+两次输入+强制确认）
010	1b PLC	2A真实	3c新发	设备大师→协调→认知→执行→跟踪→学习
011	1b PLC	2A真实	3d再发	设备大师→协调→认知→执行→跟踪→学习（+历史对比）
012	1c预测	2C隐患	-	设备大师→协调→认知→执行→跟踪→学习（+规律分析+回传预测）
013	1d预防	2D任务	-	设备大师→协调→认知→执行→跟踪→学习（+周期提醒+备件）
014	1a图片	2A真实	-	设备大师(图片识别)→协调→认知→执行→跟踪→学习
015	事后跟踪	-	对策跟踪	执行→跟踪（超期提醒）

图：设备大师多智能体协同图

智能体角色	主要职责
协调智能体	判断输入来源和故障类型，选择处理路径
认知智能体	调用知识库分析原因，信息不足时向人追问
执行智能体	生成并下发维修方案，接收补充信息后重新分析
跟踪智能体	修复后主动回访，确认设备运行状态
学习智能体	生成停工报告，把有效经验更新回知识库

需要继续核验的内容包括：预测性维护覆盖哪些设备、预警提前量、漏报率、维修建议采纳率，以及停机损失的计算口径。

案例六：远星轮胎智能调度官——把老师傅经验变成硬约束

轮胎生产包含大量规格、设备、换型和交付约束。远星轮胎把十多年排产经验拆成规则、限制条件和优化目标，形成可计算的排产系统。项目公开信息显示，过去一天的排产工作可在 30 秒内完成，一期减少 10% 的换型时间；实际效果应结合订单结构和生产周期持续验收。

这个案例更接近“运筹优化系统 + AI 交互与调参”，不能只因为产品名称包含 AI 就认定为完全自主智能体。评估重点应是硬约束是否 100% 满足、方案是否可执行、人工改排次数、准交率、换型时间和异常恢复能力。

案例七：海信供应商数据治理——规则工作流也是智能体底座

海信案例将多套系统中的供应商数据汇入统一数据底座，使用字段校验规则进行全量体检，把异常分派给数据管家，并通过会议任务和工作流持续复检。

这类方案的核心价值主要来自数据治理、规则引擎和任务闭环，AI 智能体承担会议任务提取、分析和交互等部分。它提醒企业：智能体不能建立在错误、重复、责任不清的主数据之上。



图：海信供应商数据治理案例图

案例八：Apollo Tyres 生产异常分析——多智能体如何进入工业根因分析

Apollo Tyres 案例把智能体带进了一个更垂直的现场问题：乘用车子午线轮胎硫化环节的周期时间异常。旧流程虽然已经有 IIoT 描述性看板，但工程师仍要按设备、SKU、介质、供应商等维度逐层筛选，并组织制造、工艺、工业工程等专家共同判断。主要耗时来自分析起点不明确：不知道应该从哪个维度开始查，也难以快速验证多个假设。

Apollo Tyres 的系统把一句自然语言问题拆成数据查询、假设生成、工具验证、图表和根因报告，并通过多角色协作处理复杂分析。项目公开信息显示，复杂问题的分析时间从最长约 7 小时缩短到 10 分钟以内，人工分析投入减少约 88%；年度收益仍属于项目目标，企业应用时应以自身基线和财务口径独立验收。

这个案例最值得保留的是四条工程纪律：

- 模型不替代事实库，所有分析必须回到真实生产数据；
- 假设需要被工具和数据验证，不能只生成听起来合理的原因；
- 图表、代码和大数据处理本身也要纳入工程验收；
- 根因报告仍由专业人员确认，智能体不直接修改参数或控制设备。

六、制造业智能体的系统架构

一个可落地的制造业智能体通常由六层共同组成。

业务角色：销售 研发 计划 一线 质量 设备 管理层 → AI 智能体与多智能体编排 → 知识与约束：标准 SOP 图纸 手册 案例 本体 规则 → 工具与系统：ERP MES PLM QMS WMS SRM SCADA 协同平台 → 数据与现场：订单 物料 工艺 设备 图片 传感器 任务 → 人工控制：审批 复核 放行 调参 停机 安全责任 → 可观测与治理：日志 评测 权限 成本 告警 回滚

1. 数据层

- 订单、物料、供应商、设备、工艺、质量和项目主数据编码统一；
- CAD 模型、图纸、BOM、工艺路线、SOP 和工程变更之间能够按版本追踪；
- 合同、收货/验收、发票和付款记录能够关联同一订单与供应商；
- 时间戳、单位、版本、批次和责任人可追溯；
- 图片、报警、振动、温度和维修记录能够关联具体设备或产品；
- 保存失败样本、人工纠正和绕过系统的记录，而不只保存成功结果。

2. 知识与约束层

- 产品标准、SOP、设备手册、工艺窗口和安全联锁结构化；
- 老师傅经验通过维修报告、访谈、复盘和案例沉淀；
- 每项可执行动作记录前置条件、禁止条件、参数范围和后置检查；
- 知识版本绑定适用产线、设备型号、产品版本和生效日期。

3. 工具与系统层

根据场景连接 CAD/CAE、ERP、MES、PLM、QMS、WMS、SRM、财务/发票、SCADA、PLC 和协同平台。智能体不应默认获得所有系统权限，应按照最小权限、任务范围和操作风险进行授权。设计和工艺执行优先进入副本、沙箱或版本分支，确认后再合并；采购与财务写入则要经过订单状态、金额和审批权限的确定性校验。

4. 人工控制层

以下动作原则上不应由大语言模型独立完成：

- 修改 PLC 和安全联锁；
- 直接调整高风险工艺参数；
- 发布正式工艺路线、SOP 或工程变更；
- 产品最终放行；
- 供应商淘汰和重大采购承诺；
- 发起或批准实际付款；
- 自动停机、报废、召回或对外通知；
- 删除关键生产、质量和审计数据。

5. 工程可靠性与异常恢复

所有写入、派单、调参和删除动作需要鉴权、幂等、日志、超时、重试、回滚和人工接管。对于网络断开、模型不可用、接口失败和数据异常，应预先定义降级路径。

七、制造企业落地路线图

阶段 0：建立问题与基线

先选择一个具体问题，而不是先购买平台。例如“设备故障平均需要 10 分钟定位”“供应商良率数据晚两天”“质量报告审批平均需要一小时”。记录当前耗时、错误率、成本和责任链。

阶段 1：只读知识与分析

从检索、汇总、报告、数据查询和建议开始，不自动写入核心系统。重点验证答案依据、任务覆盖率和一线是否愿意使用。

适合场景：设备知识、标准检索、研发报告、工艺知识、历史报价分析、经营日报、市场情报。

阶段 2：受控流程执行

允许智能体创建草稿、任务和提醒，写入动作经过人工确认。重点验证权限、任务到人率、回写成功率和错误恢复。

适合场景：交付物预审、CAD 副本建模、工艺路线草稿、三单核验、异常分诊、供应商整改、维修工单、项目风险。

阶段 3：有限闭环

对于低风险、规则明确的动作，允许自动执行并持续监控；高风险分支自动升级人工。

适合场景：库存预警、数据治理、报告生成、常规催办、低风险工单流转。

阶段 4：工业现场与规模化复制

当模型、规则、工程和组织验收稳定后，再连接边缘设备、专业模型和现场系统，并将成熟模式复制到其他产线和工厂。复制的对象应是“场景、数据合同、权限和验收方法”，不是简单复制提示词。

八、试点选择方法

企业可以用五个问题筛选第一批场景：

- 业务问题是否高频且可以量化？
- 所需数据是否存在、可访问、可追溯？
- 智能体的错误是否能够被人发现和纠正？
- 是否能够在 4 至 8 周内形成一个真实闭环？
- 成功后能否复制到更多人员、产线或工厂？

推荐优先级

优先级	场景特征	代表场景
优先试点	高频、只读或低风险、数据现成、结果明确	报告、知识检索、历史比价、项目预警、数据治理、库存预警
条件成熟后试点	需要跨系统写入或专业判断，但可人工确认	CAD 副本操作、工艺路线草稿、三单核验、交付物审核、维修工单、排产建议
严格验证后试点	涉及产品质量、资金、设备动作、工艺和安全	付款、视觉质检、预测性维护、参数建议、停机与放行

九、评测与验收

通用验收框架

维度	核心问题	示例指标
业务结果	是否改善成本、交付、质量或停机	工时、准交率、库存周转、停机分钟、废品率、异常关闭周期
任务质量	判断是否可靠	漏报率、误报率、根因 Top-N 命中率、建议采纳率、人工修改率
流程闭环	是否真正进入业务流	自动触发率、任务到人率、按期关闭率、回写成功率、人工升级率
工程可靠性	是否能够稳定运行	端到端成功率、P95 延迟、接口失败率、重试成功率、单次成本
使用与组织	一线是否持续使用	活跃用户、任务覆盖率、绕过系统率、培训后独立完成率
风险控制	错误能否被发现和恢复	高风险动作人工确认率、审计日志完整率、回滚成功率、安全事件数

典型场景验收

视觉质检

不良漏检率、良品误报率、单件延迟、异常拦截率、人工复核量和不同工况下的数据漂移。

设备诊断

根因 Top-N 命中率、平均修复时间、错误维修建议数、预警提前量、非计划停机时间和知识回写质量。

智能排产

硬约束通过率、计划可执行率、准交率、换型时间、产能利用率和人工改排次数。

供应商预审

风险项召回率、专家复核通过率、审核周期、错误放行数和供应商整改关闭时间。

项目风险智能体

风险提前发现时间、有效预警率、无效打扰率、责任任务按期关闭率和数据完整性。

工艺路线与 SOP 智能体

路线可执行率、工程师修改量、漏工序、试制问题、影响对象召回率、版本一致性和旧版停用情况。

工业 CAD 设计执行智能体

命令执行成功率、几何约束满足率、模型可编辑性、工程师修改率、错误传播范围和回滚成功率。

三单核验与付款审核智能体

字段抽取准确率、异常召回率、误拦截率、重复付款数、审批绕过数、回写成功率和审计日志完整性。

生产异常多智能体分析

根因 Top-N 命中率、分析耗时、专家否决率、错误数据查询或图表数、行动建议采纳率和问题复发率。

十、风险边界

1. 概率模型与确定性控制的冲突

大语言模型适合理解、解释和协调，但工业控制需要确定性。毫秒级控制、设备安全联锁和不可逆动作不能把大语言模型放在唯一控制链路上。

2. 幻觉与错误依据

所有涉及标准、工艺、质量和维修的建议都应提供来源或规则依据。无法找到依据时，智能体应明确说“不确定”并升级人工，而不是补全一个看似合理的答案。

3. 数据版本和适用范围

同一份 SOP、图纸或维修方案可能只适用于某一设备型号和产品版本。知识检索必须带上版本、产线和生效日期。

4. 越权与错误写入

智能体连接多个系统后，风险从“回答错误”升级为“业务状态被错误修改”。CAD 和工艺智能体可能把错误传播到图纸、BOM 和 SOP，采购财务智能体可能影响供应商关系与资金安全。应采用最小权限、操作白名单、副本或分支、人工审批、审计日志和可回滚设计。

5. 公开案例数字的应用边界

不同企业的流程、数据、设备和组织基础差异较大，效率、准确率、节省金额和调用量不能直接迁移。试点应设置自身基线、对照范围、运行周期和财务口径。

十一、案例与来源索引

核心来源

- 永卓控股：高炉生产管理
- 山西鹏飞：高危设备监测

- 阿维塔：全生命周期质量管理与 AI 预审
- 内江金鸿：语音报工与物料预警
- 德马科技：研发项目管理
- 雅迪：精益改善与知识助手
- TCL 华星：委外供应商良率与多智能体
- 东风康明斯：工业视觉质检
- 海信：供应商主数据治理
- 四维图新：跨系统项目经营智能体
- 东风奕派：设备维修与预测性维护多智能体
- 远星轮胎：智能排产
- 赛力斯：供应商尺寸链预审
- 临工重机：国际运价监测与预警
- Apollo Tyres：生产异常多智能体分析
- 工业智能体：工艺智能体
- 工业 CAD 进入智能体时代
- 制造业三单核验与采购比价方案
- 工业智能体技术架构

本章小结

制造业 AI 智能体的应用全景，不应被缩成“车间里多了一个机器人”。它既可以工作在研发交付、CAD 和工艺设计，也可以进入供应商协同、采购付款、排产、生产监测、质量、设备、仓储、售后和经营管理。

真正的分水岭在于企业能否把数据、知识、规则、系统、权限和责任链组织起来，让智能体在可控范围内持续完成任务。

对于大多数制造企业，第一步应选择一个高频、可量化、可纠错的业务问题，让 AI 从“给建议”逐步走向“推动闭环”，暂不追求全自动工厂。

第四章 汽车、出行与交通服务：AI 智能体贯通研发、车端、售后与交通运营

汽车与交通行业的 AI 智能体已经进入研发制造、工厂执行、门店售后和车端服务；网约车、租赁、公交、公路、充换电和多式联运仍处于持续探索阶段。

本章核心结论

汽车行业已经出现从知识问答走向流程执行的 AI 智能体：研发侧可以检索和比对需求、生成工程文档草稿、操作工业软件和推动变更；工厂侧可以跨系统取数、派任务和开单；售后侧可以收集车辆上下文、辅助诊断、查询备件并生成工单；车端主智能体则负责理解用户目标并编排导航、补能、车控和内容能力。

汽车研发智能体已经从“万页需求检索”扩展到八类硬件研发模块，售后智能体也开始连接诊断、备件、技师、工位和预约调度。城轨供电运维已经出现试运行案例；船舶、港口和铁路协同则展示了多主体之间的消息、协商和异常级联设计。

本章必须保留三条边界。第一，自动驾驶感知、路线优化和动态定价属于专业算法系统，只有接入目标、工具和反馈后才构成完整智能体。第二，车控、高压维修、控制器刷写、城轨供电和运输调度不得绕过状态机、资质和人工确认。第三，汽车研发、制造、售后、座舱和交通运营属于不同价值链，不能用一个汽车助手概括全部场景。

一、行业边界与子行业

1. 汽车研发与制造

覆盖市场洞察、车型定义、需求工程、IPD、硬件与软件研发、供应商、试制量产、质量与安全。它与制造业共享 ERP、MES、质量和设备方法，同时具有 VIN、车型配置、车规标准、功能安全、软件版本和召回等专有对象。

2. 销售、交付与售后

覆盖销售线索、试驾、订单、交车、门店支持、车主咨询、保养、故障诊断、维修、质保、客诉与案例回写，当前应用主要集中在门店知识、客服、客诉和维修。

3. 智能座舱与车载服务

面向驾驶者和乘员，将语音、多模态、账户、车辆状态、导航、补能、内容和办公组织成端云协同服务。车载主智能体负责理解与编排，车辆控制器负责确定性执行。

4. 出行、租赁与车队运营

覆盖网约车供需匹配、司机与车辆调度、行程安全、费用结算，以及租赁车辆调拨、整备、维保、事故和残值。当前只有企业和平台线索，缺完整智能体案例。

5. 公共交通与交通基础设施

覆盖公交、地铁、铁路的线网、班次、乘务、站务、客流、票务、异常调度、设备维保和安全。当前应用覆盖城轨供电设备运维，但日常运营、客流和行车调度证据仍弱。

6. 充换电与多式联运

充换电覆盖站点、预约排队、设备、价格、维修与能源经营。多式联运横跨航运、港口、铁路和物流，本章关注交通主体协商，货物履约与供应链控制塔在物流章节交叉展开。

二、核心业务链全景

市场与产品定义 → 需求 架构与设计 → 试验 变更与供应商 → 试制 量产与质量 → 营销 销售与交付 → 车主服务 诊断与维修 → 质保 客诉与产品改进 → 车载服务与补能 → 出行 车队与交通运营 → 安全 结算与运营复盘

环节	主要角色	输入与输出	典型瓶颈	AI 智能体机会
产品与需求	产品、系统、法规、项目人员	市场、法规、需求、历史版本 → 需求基线	文档巨大、变更难追踪	需求检索、差异比对和变更智能体
硬件与软件研发	设计、嵌入式、测试、质量	参数、模型、代码、标准、测试 → 工程交付物	工具多、重复操作、追溯弱	选型、CAD、代码和测试智能体
工艺与供应商	工艺、采购、供应商质量	SOR、BOM、工艺、供应商报告 → 发包和成熟度	跨组织错版、进度风险	SOR、EWO、工艺和供应商预审智能体
生产与质量	工厂管理、一线、质量、安全	订单、生产、库存、图像、任务 → 产品和记录	系统割裂、异常发现晚	经营洞察、巡检、开单和质量智能体
销售与交付	销售、门店、交付专员	线索、订单、车辆、政策 → 交车和服务	车型政策多、问题重复	门店知识、交付支持和任务智能体
诊断与维修	车主、顾问、技师、调度	VIN、DTC、症状、手册、备件、排班 → 维修结果	误诊、错件、等待和重复进店	分诊、诊断、备件和工位调度智能体
质保与反馈	客服、质量、财务、研发	工单、客诉、索赔、故障 → 处置和改进	路由慢、问题难回流	客诉、质保审核和案例学习智能体
智能座舱	驾驶者、乘员、车企	语音、车辆状态、位置、账户 → 车内服务	意图跨域、弱网和安全限制	主智能体与专业能力群
出行与车队	平台、司机、车队、乘客	订单、位置、价格、车辆状态 → 行程和结算	实时供需、异常和公平性	司机助手、异常处置、车队运营智能体
公共交通	调度、站务、维保、安全	客流、班次、设备、事件 → 运输服务	多系统协同、故障影响大	运力、乘客服务和设备运维智能体
多式联运	船方、港口、铁路、货主	ETA、泊位、堆场、车皮、运单 → 协同计划	数据主权和计划冲突	船港铁协商多智能体

三、逐环节业务流程与问题

1. 需求与工程设计：每一步对应不同工具和责任人

车型研发从需求开始，进入架构、选型、详细设计、工程变更、工艺、试验和质量。不同阶段调用需求系统、PLM/PDM、CAD、仿真、试验和质量系统。一个可靠的智能体需要明确当前阶段、工程对象、版本和审批角色。

论文材料列出 DCS 选型、SOR 发包、EWO 填报、钣金建模、工艺手册、标准件选型、DVP 报告和 QA/ESO 审核八类模块。它们可以独立工作，也可以共享知识图谱和任务状态。论文方案试点数据需要保留研究口径，不能直接当作行业平均成效。

2. 汽车软件研发：Codex 类智能体进入隔离工程环境

编码智能体可以读取需求、ARXML、领域代码、接口和 MISRA C 规则，在隔离环境生成或修改低风险代码，运行静态分析、测试和缺陷定位。需求到代码、代码到测试、失败到修复都要可追溯。

安全关键模块、量产主干、测试基线和发布由工程师审核。企业要记录模型版本、代码差异、工具调用、测试结果、人工拒绝和回滚，防止错误在自动修复链中扩散。

3. 工厂执行：数据洞察必须能落到任务和系统动作

工厂智能体可以读取订单、生产、库存和质量数据，生成日报与异常建议，并在群内派任务、催办、复盘。涉及 SAP/ERP 开单时，它需要确认车型、工位、物料和数量，确保鉴权、幂等和回滚。

摄像头巡检、数据看板和规则催办都是能力部件。它们由统一任务状态连接起来后，才形成“发现—行动—反馈”的执行闭环。

4. 售后维修：DTC 只是诊断入口

售后智能体从车主描述开始，追问发生时间、频率、环境、仪表提示和近期维修。随后结合 VIN、车型配置、DTC、手册版本、召回公告和历史案例形成根因候选，并请求技师按步骤反馈测量结果。

诊断之后仍有一条资源链：查询备件库存与替代料，匹配技师技能和工位，生成预约或派单草稿，维修完成后复检、通知客户并写回案例。高压、制动、转向、控制器刷写和安全相关操作需要资质人员批准。

5. 智能座舱：主智能体编排专业能力

主智能体维护用户入口、上下文和账户权限，把目标拆给导航、补能、车控、内容和办公能力。端侧适合低延迟、隐私和离线任务，云端适合复杂知识与外部服务。

车窗、座椅、空调、充电和导航动作通过车辆状态机与确定性接口执行。驾驶状态下限制复杂交互，弱网时提供降级路径，外部智能体只获得完成任务所需的最小数据。

6. 城轨设备运维：工单和工作票连接诊断与现场

城轨供电运维从 PSCADA 和台账读取状态，发现风险后生成诊断候选、EAM 工单和工作票草稿，并结合行车计划、施工窗口、人员和备件安排检修。现场人员执行后，结果进入报告与复盘。

青岛地铁 6 号线材料属于具名试运行的公开案例。它可以说明链路，公开时效和效率数据仍需客户或联合验收材料核验。

7. 船港铁协同：多智能体解决跨主体计划冲突

船舶侧关注航速、气象和 ETA，港口侧关注泊位、岸桥、堆场和集疏运，铁路侧关注车皮、编组、运行图和卸车能力。三方只共享必要状态，通过提议、协商、确认和超时升级形成滚动计划。

该架构目前属于 行业方案。正式生产系统还需要 A2A 消息可靠性、身份与权限、商业责任、数据共享合同、死锁处理、人工仲裁和跨系统审计。

四、AI 智能体全景图

业务链	代表智能体或相邻能力	主要动作
需求工程	德赛西威“星舱知途”	需求检索、版本比对和追溯
项目管理	雅迪 IPD 助手与多角色预评审	周报、经验检索和多角色挑刺
方案选型	DCS 选型智能体	多目标比较和报告
需求发包	SOR 智能体	生成技术包、控版和跟踪
工程变更	EWO 工程更改智能体	填报、影响分析和流程推进
工业设计	钣金建模/空间优化智能体	调用 CAD 和仿真生成候选
工艺交付	工艺手册生成智能体	生成 PDM 工艺说明草稿
零件与试验	标准件选型、DVP 报告智能体	选型、数据汇总和缺项定位
质量审核	QA 分析与 ESO 审核智能体	设计风险和供应商试验审核
汽车软件	需求、领域代码和测试智能体	生成、执行测试和修复候选
工厂经营	北汽福田“长超小福”	跨系统取数、派单、巡检、SAP 开单
零部件协同	奇瑞捷途智控平台与提醒工作流	成熟度、风险和催办
门店知识	岚图“小岚”	问答、推荐和话题沉淀
客诉	新大洲本田客诉流转	集中、转发和看板
车主客服	一汽丰田智能客服	多轮问答和转人工
售后诊断	服务顾问、维修技师智能体	追问、诊断、检查和方案
售后调度	备件与维修工单调度智能体	库存、技师、工位和预约
智能座舱	NOMI、MBUX、博世端云编排	主入口和专业能力路由
城轨运维	城轨供电设备运维多智能体	预警、诊断、工单和工作票
多式联运	船舶、港口、铁路协同智能体	ETA、资源协商和异常级联
充换电	故障预测、派单、调价、占位识别	预测、工单和经营建议
出行与车队	司机助手、异常处置、车辆调拨	计划、服务和资产任务
自动驾驶	感知、预测、规划和控制	车辆运动控制

五、重点智能体工作卡

1. 汽车研发需求与变更智能体

字段	内容
服务对象	产品、系统、设计、项目、法规和质量工程师
触发条件	新需求、版本更新、设计变更或里程碑评审
主要输入	车型需求、法规标准、历史版本、设计参数、测试和问题记录
判断与规划	检索最新需求，识别差异和依赖，判断影响对象与评审角色
工具与系统	需求管理、PLM/PDM、ALM、知识图谱、任务与审签系统
输出与动作	差异表、变更草稿、影响清单、评审任务和状态跟踪
人工控制点	工程师确认需求基线、安全等级和正式变更；系统保留撤回与审计
验收指标	关键需求召回、差异漏检、影响漏项、退回率、人工修改和追溯覆盖

2. 硬件设计与工业软件执行智能体

字段	内容
服务对象	硬件、结构、工艺和试验工程师
触发条件	选型、参数化建模、空间优化、工艺或试验报告任务
主要输入	参数、安装边界、几何和性能约束、标准件、模型、试验数据
判断与规划	把自然语言目标拆成 CAD、仿真、检索和报告步骤，检查缺失约束
工具与系统	CAD/CAE、PLM/PDM、仿真、标准件库、试验管理和版本系统
输出与动作	可编辑模型、候选方案、工艺/试验草稿和执行日志
人工控制点	在副本或分支运行；工程师审查约束、可制造性和安全后合并
验收指标	约束满足、模型可编辑、工具成功、仿真复现、人工返工和回滚

3. 售后故障诊断与资源调度智能体

字段	内容
服务对象	车主、服务顾问、维修技师、备件和门店调度
触发条件	车主咨询、车辆入站、远程告警或维修复检
主要输入	VIN、配置、DTC、症状、车联网数据、手册、召回、库存和排班
判断与规划	补齐上下文，生成根因候选和检查步骤，匹配备件、技师与工位
工具与系统	DMS、车联网、诊断仪、知识库、ERP/WMS、排班和工单
输出与动作	初诊、检查任务、备件方案、预约/派单草稿、报告和案例
人工控制点	技师确认诊断和维修；高压、制动、转向、刷写等按资质与规程审批
验收指标	根因 Top-3、错换件、一次修复、重复进店、备件满足、错派和安全事件

4. 城轨供电设备运维智能体

字段	内容
服务对象	城轨供电调度、设备工程师、检修班组和安全管理者
触发条件	PSCADA 异常、设备预警、计划检修或故障事件
主要输入	实时状态、设备台账、图纸、故障、行车计划、施工窗口、人员备件
判断与规划	分析原因和影响，生成处置方案，协调工单、工作票和施工窗口
工具与系统	PSCADA、EAM、行车/施工系统、图纸知识库和移动工单
输出与动作	预警、诊断、工单、工作票草稿、计划和检修报告
人工控制点	调度命令、停送电和现场检修由持证人员按规程执行
验收指标	漏报、根因命中、处置时长、误工单、工作票错误和审计完整

5. 船港铁协同多智能体系统

字段	内容
服务对象	船公司、港口、铁路、货主与多式联运运营方
触发条件	新运输任务、ETA 变化、泊位冲突、设备故障或铁路运力变化
主要输入	AIS、气象、泊位/岸桥/堆场、车皮、运行图、运单和时间窗
判断与规划	三方生成候选计划，以最小必要数据协商，异常时级联调整
工具与系统	VTS/TOS、铁路系统、运筹求解器、事件总线、A2A 消息和审计
输出与动作	ETA、靠泊和疏运方案、确认消息、变更计划和人工仲裁任务
人工控制点	船长、港口调度和铁路调度保留法定权责；冲突与死锁升级人工
验收指标	ETA 误差、等泊、车皮空等、计划兑现、消息可靠、超时和规则合规

六、代表案例

案例一：端到端汽车研发硬件设计研究——八个模块共享工程状态

论文将硬件研发拆成八类智能体，覆盖选型、发包、更改、建模、工艺、标准件、试验和质量。系统采用“大模型统筹、小模型落地、知识图谱约束、仿真验证”的思路，并明确工程师保留最终审核权限。

论文中的数据量和试点指标属于作者自报。白皮书采用其业务划分和人机协同机制，企业范围、样本和成效仍需继续复核。



图：汽车研发硬件设计智能体全景

案例二：北汽福田“长超小福”——从日报到 SAP 开单

“长超小福”读取订单、生产、库存和质量数据，生成经营日报与调整建议，在群内派活、催办和复盘，还可调取监控进行安全巡检，并为装配工创建 SAP 缺件单。系统采用缓存与同步数据层、无人确认自动回退等工程策略。

北汽福田“长超小福”是汽车行业执行型智能体案例。正式评估应同时检查误开单、回滚、巡检漏报和长期运行稳定性，不能只看效率提升。



图：北汽福田长超小福整体方案

案例三：岚图“小岚”——门店知识与问题运营分开验收

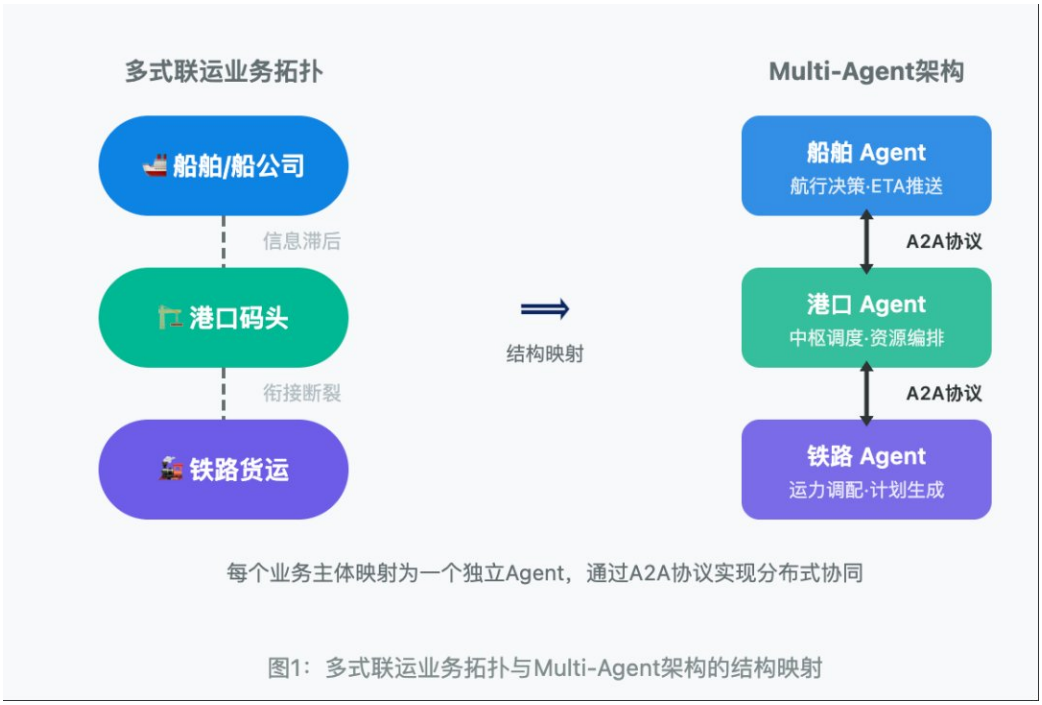
“小岚”服务门店一线，回答交车和售后问题并推荐案例；话题工作流记录问题、解决时间和参与人，用于分类与时效分析。知识问答、数据记录和流程自动化承担不同任务，验收时应分别计算正确率、一次解决率和问题关闭时间。



图：岚图小岚门店助手

案例四：船港铁多智能体——业务拓扑映射到角色协商

行业方案把船舶 ETA、港口泊位和铁路运力映射为三个业务角色。每一方保留自身数据与约束，通过标准消息交换必要状态，由监督/协商角色处理超时和冲突。



图：船港铁多智能体业务拓扑

七、系统、数据与权限

1. 数据与知识

- 研发：需求、法规、标准、车型、配置、零部件、图纸、代码、测试、变更和缺陷；

- 制造：订单、BOM、工艺、生产、库存、质量、设备和安全；
- 售后：VIN、DTC、车联网、手册、召回、工单、备件、技师、工位、质保和客诉；
- 车端：账户、位置、车辆状态、驾驶状态、偏好、语音和多模态输入；
- 出行交通：订单、司机/乘务、车辆、班次、客流、路线、票务和安全事件；
- 多式联运：AIS、ETA、泊位、岸桥、堆场、车皮、运行图和共享运单。

所有知识绑定车型、软件版本、地区、生效日期和责任人。保存误诊、漏报、错派、人工纠正、拒绝执行和回滚记录。

2. 系统接口

研发侧连接 PLM/PDM、ALM、CAD/CAE、代码库、CI/CD、测试台架和 QMS；制造侧连接 ERP、MES、WMS、SRM、SCADA 和协同平台；售后连接 CRM、DMS、车联网、诊断、配件、工单和结算；交通侧连接地图、订单、支付、调度、安全和资产系统。

3. 权限与人工控制点

动作	默认控制方式
检索、比对、生成报告和建议	可自动执行，显示来源、版本和不确定性
创建低风险任务和提醒	可自动执行，具备去重、限频和撤回
需求/模型/代码/工艺变更	进入评审与合并流程，不能直接改量产基线
SAP/ERP 开单、质保和费用	确认关键字段，强鉴权、幂等、日志和回滚
售后预约和备件建议	顾问或客户确认后执行
高压维修、刷写、制动转向与召回	由资质人员和授权主体批准
车控、城轨供电和运输调度	确定性系统执行，状态校验、二次确认和人工接管
自动驾驶运动控制	独立安全体系负责，语言模型不进入唯一控制链

八、企业落地路线

阶段 0：建立单场景基线

选择一类需求、一个车型项目、一组门店、一条售后工单或一类设备，记录现有周期、错误、返工和责任链。

阶段 1：知识与分析助手

先做需求检索、手册问答、报告生成和历史案例查询。重点验证版本、引用、权限和高风险转人工。

阶段 2：受控工程与流程执行

允许在副本中操作 CAD 或代码，创建变更、工单和预约草稿。所有写入前检查关键字段，人工确认后合并或提交。

阶段 3：有限闭环

对低风险提醒、话题记录、例行报告和常规派单开放自动执行。异常、安全和金额分支自动升级人工。

阶段 4：车端、现场与跨主体协同

经过仿真、故障注入、弱网和回滚测试后，再扩大到车端工具、城轨设备或多式联运。跨企业场景先签订数据、责任和仲裁协议。

九、评测与验收

场景	任务质量	业务结果	风险与可靠性
需求与变更	召回、差异漏检、影响漏项	评审周期、返工和退回	版本追溯、错误合并和撤回
工业软件执行	约束满足、模型可编辑、测试通过	工程师工时和交付周期	隔离、复现、越权和回滚
工厂执行	报告修改、异常有效、开单正确	问题关闭、停线和人工处理	重复开单、接口失败、回滚成功
门店知识	答案正确、来源覆盖、一次解决	响应和问题关闭	过期政策误答和转人工完整
售后诊断	根因 Top-3、错换件、检查完整	一次修复、重复进店、维修周期	高风险建议拦截和安全事件
智能座舱	意图、工具选择、端到端完成	任务完成和用户负担	误车控、驾驶分心和弱网降级
城轨运维	漏报、根因、工作票字段	故障处置和设备可用	误操作、持证确认和审计
多式联运	计划可执行、消息可靠、冲突解决	等泊、空等、延误和兑现	数据越界、死锁、超时和人工仲裁

汽车 AI 质量治理还需覆盖用例、数据、模型、验证、运行监控、变更和退役。引用的 VDA 黄皮书属于治理参考，不应表述为强制标准。

十、风险边界

- 工程安全：需求、代码、模型、工艺和试验结果必须可追溯、可复现、可审核。
- 车辆安全：车控和自动驾驶由状态机、功能安全体系与确定性控制器负责。
- 维修责任：远程或智能诊断不能替代技师测量、维修手册、资质和复检。
- 隐私与数据：位置、驾驶行为、车内语音图像、VIN 和维修记录按敏感等级最小化处理。
- 跨主体治理：船、港、铁协作要明确数据主权、消息标准、商业责任和人工仲裁。

十一、来源索引

核心来源

- 德赛西威 AI 需求专家
- 岚图“小岚”门店数字专家

- 雅迪研发营销协同
- 北汽福田“长超小福”
- 智能座舱多智能体协作行业研究
- 端到端汽车研发硬件设计智能体研究
- 汽车售后维修与工单调度方法
- 青岛智运城轨供电设备运维智能体
- 船港铁多智能体协同排程架构
- 汽车 AI 质量管理框架

本章小结

汽车和交通服务的智能体价值，来自把需求、工程工具、车辆上下文、备件资源和运输状态连接起来。研发、生产、售后、座舱和交通运营都需要自己的业务对象、知识和权限，无法靠一个通用聊天入口统一替代。

企业可以从需求比对、门店知识、报告和售后分诊等低风险场景开始，再进入工程软件、工单和车端工具。所有安全关键动作都应由确定性系统与授权人员负责，智能体承担理解、分析和协同。

第五章 建筑、房地产与物业：AI 智能体连接项目文件、工程现场与资产运营

建筑、房地产与物业的 AI 智能体应用，已经进入项目文档审核、规范问答、监理资料、工程造价、商业运营、物业客服和现场巡检。

本章核心结论

建筑、房地产与物业的共同底座是“项目和资产”，但三者的价值链差异很大。设计和施工关注图纸、规范、合同、进度、质量与安全；房地产开发关注投资、产品、营销、交付和资产回报；物业关注业主服务、设施、巡检、维修、收费和续约。AI 智能体必须进入对应业务链，才能从文档生成工具升级为业务系统的一部分。

当前最值得落地的环节包括项目文件与图纸预审、规范检索、监理资料、施工隐患闭环、全过程造价风险、材料询价、商业经营分析和物业工单。这些应用贯通设计、造价、施工安全和物业巡检，也必须处理弱网、版本、价格时效和法定责任等真实工程约束。

本行业的高风险控制点包括结构与消防结论、正式审图、危大工程、停工指令、合同放行、变更签证、计量支付、结算审计和物业安全。智能体可以发现问题、生成草稿、创建工单和组织证据，有资质或授权人员承担签字、定责、付款和放行责任。

本章重点覆盖三个方向：

- 建筑设计从效果图生成扩展到 BIM 深化、性能优化、规范校核和跨专业协同；
- 工程造价从单次询价扩展到预算、合同、进度、变更、付款和结算的动态风险链；
- 物业巡检从摄像头识别扩展到扫码到场、离线实拍、维修反馈和迎检台账。

一、行业边界与子行业

1. 勘察与建筑设计

覆盖客户需求、场地与测绘、概念方案、建筑/结构/机电深化、性能分析、规范校核、审图、变更与交底。生成可视化属于早期能力，真正交付还需要工程参数、规范和专业签审。

2. 工程建设与监理

覆盖投标、合同、项目策划、招采、施工计划、现场执行、进度、质量、安全、监理、资料、变更签证、验收、结算与维保。这里的核心对象会持续变更，智能体需要理解版本、责任主体和项目状态。

3. 房地产开发

覆盖投资研究、拿地、产品定位、设计管理、开发建设、成本融资、营销销售、交付和客户服务。施工智能体与开发经营智能体服务不同对象、调用不同系统，应分别设计和验收。

4. 商业地产与资产运营

覆盖招商、租户、客流、销售、活动、租赁、经营分析和资产管理。新城控股案例属于这一链路，不能代表住宅开发全过程。

5. 物业与设施服务

覆盖承接查验、业主入住、客服工单、安防、巡检、维修、收费、能耗、设施运维、社区服务和续约。老旧小区与高端商业综合体的设备、网络和人员条件差异显著，方案需要分层。

二、核心业务链全景

投资与项目策划 → 勘察与设计 → 造价 招采与合同 → 施工计划与现场执行 → 质量 安全与监理 → 变更 签证与计量支付 → 验收 结算与交付 → 营销 招商与租赁 → 资产与商业运营 → 物业 客服与设施服务

环节	主要角色	输入与输出	典型瓶颈	AI 智能体机会
投资与策划	投资、产品、规划、财务	土地、市场、规划、收益 → 项目判断	数据分散、假设难追溯	投资研究、定位和测算智能体
勘察与设计	建筑、结构、机电、设计管理	场地、需求、BIM、图纸、规范 → 设计成果	多专业冲突、版本混乱	方案生成、BIM 协调、规范审查智能体
造价与招采	造价、采购、商务、审计	清单、材料价、预算、合同 → 目标成本和采购依据	价格过期、口径不一	询价、清单审核、合同与造价智能体
施工执行	项目经理、总包、分包、班组	计划、人机料、现场状态 → 实体工程	信息滞后、跨主体协同慢	计划、资料、现场协调智能体
质量安全	质量、安全、监理、业主	方案、规范、影像、传感器 → 隐患与整改	漏报代价高、证据断裂	现场符合性、动态风险和整改智能体
变更与支付	商务、设计、监理、审计、财务	变更、签证、产值、付款 → 纠偏和支付	数据四张皮、超付难早发现	全过程造价风险预警智能体
验收与交付	业主、监理、施工、物业	竣工资料、缺陷、验收 → 交付和维保	文件与现场不一致	验收资料、缺陷和移交智能体
营销与招商	营销、销售、招商、客服	客户、房源/铺位、合同、活动 → 成交与入驻	线索和资产状态割裂	客户经营、招商和合同辅助智能体
商业运营	运营、租户、管理层	客流、销售、活动、租金、BI → 经营动作	异常发现晚、报告耗时	经营分析与责任推送智能体
物业与设施	客服、工程、保安、保洁、业主	报修、巡检、设备、收费 → 服务结果	派单错、弱网、维修证据缺失	客服、巡检、工单和设备能源智能体

三、逐环节业务流程与问题

1. 建筑设计：从概念生成到可签审成果

概念方案智能体可以根据场地、功能、风格、气候和规划指标生成多个候选；深化阶段需要解析 BIM 和专业模型，调用结构、采光、通风、能耗和材料工具，比较约束和性能。

施工图与审查要求更高。系统要核对图纸、说明、计算书和规范版本，定位跨专业碰撞、参数缺失与变更影响。建筑师和各专业工程师负责最终方案与签审，仿真结果需要可复现。

2. 项目文件与监理资料：动态任务和固定工作流分层

投标、RFI、提交文件、监理日志和报验资料包含大量 PDF、扫描件、表格和图纸。文件智能体需要建立项目记忆和文档关系，识别当前版本、缺项、冲突和责任人。

字段和步骤固定的监理表单适合确定性工作流；信息缺失、路径会变化的任务才需要动态智能体。正式文书生成前由监理人员核对事实，工具调用和版本记录完整留痕。

3. 施工安全：识别模型必须连接现场处置

施工现场使用摄像头、无人机、传感器、气象、人员定位和机械轨迹。危大工程符合性智能体把专项方案关键节点与现场画面或数据比对，发现支护、防护和作业偏差。

动态风险智能体则结合大风、高处作业、塔吊和交叉作业，生成停、改或复查建议。安全员和项目负责人按制度决定处置，法定责任不会因使用 AI 转移。

4. 全过程造价：预警要落到纠偏和支付

造价风险来自预算、合同、进度、产值、变更和付款之间的不一致。智能体需要贯通 BIM5D、成本、合同、PMS、审计和审批数据，识别超合同付款、大额签证未批、工期滞后和成本偏差，生成证据和责任工单。

预警只有进入责任人、时限、处置和关闭状态后才产生价值。计量、付款和结算由造价、审计和财务授权人员确认。

5. 材料询价：搜索只是第一步

询价智能体先识别清单材料，处理名称、规格、地区和日期，再按数据源回退链查询企业库、材价库、市场网站或搜索引擎。系统需要检查来源时效、规格映射、税运口径和异常价格。

企业还要管理数据源健康、限流、失败重试、Trace ID 和只追加价格版本。异常映射、替代材料和最终价格由造价或采购人员确认。

6. 商业运营：分析结果必须到达责任人

商业地产经营智能体连接业务系统、BI、多维表格和知识库，发现客流、销售、租户和活动异常，生成报告，并把问题推送给对应运营人员。

它的验收对象是数据一致性、有效异常、责任人响应和经营动作，不能只看报告生成速度。

7. 物业巡检与维修：低成本、弱网和证据链

老旧小区可以用二维码或 NFC 确认点位，以现场实拍证明到场，在弱网时本地缓存。发现隐患后生成工单，维修人员上传完工对比照片，项目负责人验收并导出台账。

图像识别、扫码和派单分别属于能力部件。完整闭环还要防代巡、重复工单、同步丢失、图片篡改和隐私越权。

四、AI 智能体全景图

业务链	代表智能体或相邻能力	主要动作
概念设计	建筑概念方案生成智能体	多方案生成和迭代
性能设计	建筑性能优化智能体/算法工作流	调用结构和能耗仿真
BIM 深化	BIM 跨专业协调智能体	碰撞、参数和变更闭环
项目文件	Trunk Tools 提交文件/图纸审查	跨文件核对和证据定位
项目澄清	RFI 智能体	生成问题并推动澄清
投标审查	投标文件审查智能体	响应完整性和冲突检查
规范知识	建筑装饰规范问答助手	条款检索、解释和建议
监理资料	监理日志动态智能体	缺项追问、起草和 Word 生成
合同商务	工程合同审核工作流	规则扫描、版本差异和风险提示
现场感知	无人机巡检/算量系统	采集、建模和缺陷识别
危大工程	现场符合性检查智能体	方案与现场比对、预警
动态安全	施工动态风险预测智能体	气象、人员、机械交叉研判
安全知识	隐患案例学习智能体	案例结构化和跨项目提示
全过程造价	造价风险预警智能体	偏差、证据、责任工单和关闭
材料询价	工程材料询价智能体	归一、采集、比价和询价表
询价治理	数据源治理/追踪子智能体	回退、版本、限流和追踪
商业运营	新城控股 AI+BI 系统	异常推送、报告和培训
物业客服	物业客服派单智能体	意图识别、回答和派单
物业巡检	离线巡检证据智能体/工作流	到场、实拍、缓存和台账
物业迎检	整改证据与迎检台账智能体	原图、工单、完工和验收关联
设施运维	楼宇设备和能源智能体	诊断、工单和调控建议

五、重点智能体工作卡

1. 项目文件与图纸审查智能体

字段	内容
服务对象	设计、项目、总包、监理、投标和 RFI 负责人
触发条件	新文件提交、版本变更、审查节点或现场问题
主要输入	PDF、图纸、扫描件、表格、规范、RFI、提交文件和项目历史
判断与规划	识别版本和对象关系，检查缺失、冲突、变更影响和不符合项
工具与系统	CDE/BIM、文档管理、OCR/ 视觉、规范库、RFI 和审签系统
输出与动作	问题定位、依据、审查清单、RFI 草稿和责任任务
人工控制点	专业人员确认结构、消防、规范和正式审查意见
验收指标	严重问题召回、误报、版本识别、证据定位、返工和错误放行

2. 施工隐患识别与闭环智能体

字段	内容
服务对象	项目经理、安全员、监理、班组和企业安全部门
触发条件	定时巡检、方案关键节点、气象变化或传感器越界
主要输入	专项方案、BIM、现场视频/照片、传感器、天气、人员和机械轨迹
判断与规划	识别执行偏差和交叉风险，分级，匹配责任人和处置时限
工具与系统	视频平台、智慧工地、BIM、实名制、机械物联网和工单
输出与动作	预警、证据、整改工单、复查任务和案例回写
人工控制点	安全员确认隐患；停工和应急处置按法定制度执行
验收指标	严重隐患漏报、误报、提前量、发现到处置、按期整改和复核销项

3. 全过程造价风险预警智能体

字段	内容
服务对象	业主成本、项目商务、造价、审计、监理和财务
触发条件	数据更新、阈值越界、变更、付款申请或月度结算
主要输入	目标成本、预算、合同、进度、产值、变更、签证和付款
判断与规划	计算偏差，识别超合同付款、未批签证和工期成本联动风险
工具与系统	BIM5D、成本/合同、PMS、审计、审批和财务系统
输出与动作	预警、证据位置、影响、责任工单、时限和关闭状态
人工控制点	计量、支付、审计结论和责任认定由授权人员确认
验收指标	有效预警、无效打扰、提前量、超付拦截、按期关闭和数据一致

4. 工程材料询价与价格治理智能体

字段	内容
服务对象	造价、采购、成本和项目商务人员
触发条件	清单询价、预算更新、材料替代或价格争议
主要输入	Excel/ 清单、材料名称和规格、地区、日期、历史价、税运口径
判断与规划	材料归一、数据源选择、失败回退、时效与异常价校验
工具与系统	企业价格库、材价/定额库、市场网站、采集器、数据库和日志
输出与动作	价格、来源、时间、异常提示、询价表和可回放 Trace ID
人工控制点	异常映射、替代材料和最终价格由造价或采购人员确认
验收指标	规格匹配、来源可追溯、价格过期、异常拦截、失败恢复和人工修改

5. 物业巡检与维修证据智能体

字段	内容
服务对象	物业项目经理、工程维修、安全巡逻和迎检人员
触发条件	巡检计划、现场扫码、隐患识别、维修完成或迎检任务
主要输入	点位、二维码/NFC、现场照片、人员时间、离线记录、工单和耗材
判断与规划	核验到场和图片，识别缺项，派单，关联维修与验收证据
工具与系统	移动端、离线缓存、物业工单、图片存储、台账和权限系统
输出与动作	巡检记录、隐患工单、漏巡提示、完工对比和迎检台账
人工控制点	高危隐患由专业人员确认；维修验收和责任认定由物业负责人完成
验收指标	到场可信、同步丢失、派单准确、按期完工、证据完整和抽查一致

六、代表案例

案例一：Trunk Tools——项目记忆与多智能体移交

行业研究将建筑项目 AI 分为感知、语义/图谱和智能体三层，处理 PDF、工程图、扫描件、表格、RFI 与提交文件。图纸审查智能体可以把问题移交 RFI 智能体，说明不同角色能够围绕同一项目状态协作。

公开效率和准确率来自二次翻译整理。。

案例二：全过程造价风险预警——数据贯通后才能提前纠偏

相关材料引用多个具名工程和平台案例，描述将 BIM5D、进度、成本、合同、变更和付款连接起来，通过看板和规则发现造价异常。白皮书采用“预警即工单、责任到人、处理后关闭”的机制。

案例中的准确率、节约率、争议下降和周期缩短均需回查原始报道，不能直接推广为行业收益。

案例三：材料询价智能体——六步循环与数据源回退

从业者实践把询价拆成感知、理解、规划、执行、反馈和学习六步。系统可识别清单、选择数据源、查询价格、遇到规格不明时追问，并输出带来源的询价表。后续还加入数据源限流、失败回退、版本和追踪。

该方案展示了完整工作流设计；进入企业生产环境还需要完成接口、安全、权限、稳定性和业务结果验收。

案例四：老旧小区低成本巡检——先解决到场、弱网和留证

厂商方案以扫码或 NFC 确认点位，现场实拍后生成巡检记录，弱网时离线缓存，恢复网络后同步。隐患进入维修工单，完工对比照片和验收结果生成迎检台账。

“咨询减少”“快速上线”等成效属于 宣传口径，白皮书只采用可验证的流程设计。



图：老旧小区巡检流程应用图

七、系统、数据与权限

1. 核心数据对象

- 项目：项目、标段、合同、单位工程、楼栋、楼层、构件和责任主体；
- 设计：场地、BIM/IFC、二维图纸、计算书、规范、审查和变更；
- 施工：计划、人员、设备、材料、影像、传感器、质量、安全和监理记录；
- 商务：清单、价格、预算、合同、签证、产值、付款和结算；
- 运营：商户、铺位、客流、销售、活动、租金和资产；
- 物业：业主、房屋、设备、点位、报修、工单、收费、能耗和服务评价。

每项数据保留来源、版本、生效时间、审批状态和责任人。项目、楼栋、构件、图纸、合同、变更和工单需要统一标识。

2. 系统接口

设计侧连接 GIS、BIM/CDE、CAD、仿真、规范和审签；施工侧连接 PMS、智慧工地、视频、物联网、监理和资料系统；商务侧连接成本、合同、采购、审计、审批和财务；运营侧连接 CRM、BI、招商、租赁、物业和设施系统。

3. 权限与人工控制点

动作	默认控制方式
检索、对比、报告和草稿	可自动执行，显示来源、版本和适用项目
创建低风险 RFI、资料和巡检任务	可自动执行，具备去重、限频和撤回
修改 BIM、图纸和设计参数	在副本或分支执行，专业人员审查后合并
安全预警和整改派单	可自动触发，停工与高危处置由责任人决定
合同、签证、计量和付款	法务、造价、监理、审计或财务授权人员确认
结构、消防、正式审图和工程签字	由具备资质的专业人员承担
楼宇设备控制	确定性 BMS 和安全联锁执行，保留人工接管

所有写入和工具调用记录输入、版本、动作、结果、失败、重试、批准人和回滚。

八、企业落地路线

阶段 0：选择一个项目对象和问题

从一类图纸、一种监理日志、一个造价风险、一条巡检工单或一个商业运营指标开始，建立周期、错误、返工和责任基线。

阶段 1：只读知识与审查

先做规范检索、项目文件查询、版本比对、报告和风险清单。重点验证证据定位、版本适用和高风险转专家。

阶段 2：受控文档与任务执行

允许生成 RFI、监理日志、询价表、整改或物业工单草稿，由人员确认后写入系统。同步验证弱网、重复任务和失败恢复。

阶段 3：有限闭环

低风险提醒、材料采集、例行报告和常规派单可自动执行。设计变更、停工、签证、支付和正式审查保持人工闸门。

阶段 4：跨项目和资产复制

把成熟场景复制到其他项目或资产时，重新校验地区规范、建筑类型、合同模板、组织权限和数据接口。复制对象包括数据合同、规则、角色和验收方法。

九、评测与验收

场景	任务质量	业务结果	风险与闭环
图纸/文件审查	严重问题召回、误报、版本和证据定位	审查周期、返工和 RFI 周期	错误放行、签字保留和审计
BIM 协调	碰撞召回、参数和变更影响	协调周期和现场返工	版本一致、复检销项和仿真复现
监理资料	字段完整、事实一致、人工修改	单份用时和退回率	正式成果确认和工具成功
施工安全	漏报、误报、提前量	隐患处置和事故近失	停工权限、复核销项和法定责任
全过程造价	有效预警、证据和数据一致	超付、成本偏差和结算周期	责任工单、人工审批和审计
材料询价	规格匹配、价格时效、来源可追溯	询价周期和采购偏差	异常价确认、数据合规和回放
商业运营	报告一致、异常有效、建议采纳	运营工时和经营指标	数据权限、无效打扰和责任关闭
物业巡检	到场可信、识别与派单准确	完工、投诉和巡检覆盖	弱网同步、图片隐私和证据完整

正式验收需要纳入项目阶段、地区规范、合同类型、建筑类型和设备差异，不能只使用一个平均准确率。

十、风险边界

- 专业签字：结构、消防、正式审图、监理和工程验收由具备资质的人员负责。
- 现场安全：视觉和预测只能辅助发现，停工、危大工程和应急处置按法定制度执行。
- 版本错误：过期图纸、规范、合同和价格会直接造成错误，所有输出显示来源和生效范围。
- 资金责任：签证、计量、支付和结算进入确定性规则与人工审批，不向模型开放最终付款权。
- 跨主体数据：业主、设计、总包、分包、监理和物业按项目、合同与角色隔离数据。

十一、来源索引

核心来源

- Trunk Tools 建筑项目智能体行业研究
- 监理智能体实践
- 路桥无人机与 AI 落地反思
- 新城控股购物中心运营公开案例
- AI 在建筑设计领域的应用现状
- 施工安全隐患识别与风险预警
- 全过程工程造价风险预警

- 造价询价智能体实践
- 老旧小区低成本数字化巡检方案

本章小结

建筑、房地产与物业的智能体机会贯穿图纸、规范、合同、进度、造价、现场和资产运营。最可行的起点是边界清楚、证据可追溯、能保留人工签审的任务，再逐步连接工单和项目系统。

项目行业的关键是版本、责任和资金。智能体负责发现问题、组织证据和推动闭环，专业人员负责签字与风险判断，授权主体负责支付和放行。只有把三类责任写进系统，AI 才能成为项目和资产运营的稳定能力。

第六章 消费品、食品与餐饮：从新品、食安到门店经营的智能体闭环

消费品、食品与餐饮行业已经形成从消费者洞察、新品研发、工厂质量到门店经营、食品安全和供应链协同的 AI 智能体应用链。

本章核心结论

消费品、食品与餐饮不是一个同质行业。本章重点覆盖食品饮料制造、连锁餐饮与现制饮品，并把品牌经营作为贯穿二者的横向链路；消费电子只保留交叉参照，不以少量案例替代其完整研发与售后链。

目前较成熟的是四类受约束闭环：工厂视觉巡检与整改、门店 QSC 与客诉闭环、食材效期与标签执行、渠道/VOC 信息汇总与任务路由。食品标签合规、菜单工程、排班、茶饮供应链、中央厨房追溯和咖啡具身服务也已出现应用实践。

这一行业的价值与风险都来自“短周期”：原料会过期，门店客流会波动，食品问题必须尽快处置，舆情和投诉也会迅速扩散。因此，AI 智能体不能只给建议，还要连接批次、门店、责任人和处理状态；但配方、标签、食品安全、停线复产、召回、报废、定价和赔付仍需专业人员批准。

一、行业边界与子板块

1. 食品与饮料制造

覆盖配方、原料、生产、质量、包装、短保库存、经销交付和批次追溯。通用设备运维、排产与质检可交叉制造业，但过敏原、食品标签、效期和召回必须保留行业规则。

2. 连锁餐饮与现制饮品

覆盖选址、菜单、中央厨房、采购、备料、制作、出餐、外卖、QSC、员工训练、单店经营与加盟网络。餐饮与零售共享门店、会员和库存，却多出现场制作、食安和即时履约责任。

3. 品牌经营与渠道运营

覆盖消费者洞察、新品上市、内容、经销、电商、团购、会员、VOC 与经营复盘。它是食品和餐饮的共同链路，不单独重复计数。

4. 消费电子与耐用消费品

安克、科沃斯等材料可用于说明全球品牌经营和 VOC 闭环，但其软硬件研发、固件、远程诊断、备件和召回不同于短保食品，本章不据此宣称已完整覆盖消费电子。

二、核心业务链与逐环节问题

1. 食品饮料制造链

消费者洞察 → 品类与新品 → 配方/小试 → 法规、过敏原与标签 → 原料和供应商 → 生产排程 → 加工包装 → 质量与食安 → 仓储冷链 → 渠道交付 → 客诉召回 → 产品改进

环节	典型问题	智能体切入点	必要控制点
消费者洞察	评论分散、多语种、问题反馈晚	汇聚评论、主题聚类、严重性识别、责任路由	噪声与水军过滤，不能把情绪当因果
新品与配方	试验资料难复用，成本、营养和稳定性冲突	检索历史试验，比较候选，生成小试计划	研发、法规和质控共同签审
标签合规	地区、法规版本和包装字段复杂	字段抽取、条文检索、缺失冲突提示、版本留痕	依据必须可追溯，法务/质控签发
原料采购	交期、品质、批次和价格分散	供应商预审、风险监测、异常任务	准入、换供与处罚人工批准
生产加工	短保和换线约束多，异常反馈慢	需求预测、排程建议、参数与异常分析	生产指令和工艺参数受确定性系统约束
质量食安	视觉漏检、巡检证据散、整改不闭环	视觉识别、人工复核、工单、复查和周报	放行、停线、复产、召回由责任人决定
仓储冷链	效期、温度、批次与库存同时变化	临期预警、FEFO 建议、冷链异常处置	传感器失效、错批次和重复任务需拦截
客诉召回	影响范围定位慢、跨部门协作长	批次追溯、证据包、候选影响清单	不自动公开结论或启动召回

2. 连锁餐饮与现制饮品链

商圈选址 → 菜单研发 → 供应商/中央厨房 → 门店预测与补货 → 排班备料 → 点单制作出餐 → 食品安全与效期 → 巡店整改 → 客诉服务 → 会员复购 → 单店复盘 → 标准复制

环节	典型问题	智能体切入点	必要控制点
选址与经营计划	商圈数据与品牌经验割裂	候选点研究、情景测算、风险解释	投资决策不交给模型
菜单工程	销量、毛利、评价和原料共用难同时判断	菜单四象限、组合/改价模拟	下架、改价和配方调整需审批与试验
预测补货	天气、活动、保质期导致波动	门店需求预测、仓配协同、缺货损耗预警	采购单、调拨和替代料人工批准
排班	客流波动、技能和劳动规则冲突	预测岗位需求、约束求解、替班建议	公平性、工时规则和员工确认
后厨效期	非标叫法、标签计算与打印易错	识别食材、匹配 SOP、算效期、打印和预警	错标签立即拦截，过期品由人员处置
巡店 QSC	图片多、标准多、假整改	识别问题、引用标准、派单、复查	重大食安问题人工复核与升级
客诉与舆情	响应慢、跨层级扯皮	情绪/风险分级、责任路由、超时升级	不自动判责、赔付或公开回复高风险事件
会员复购	粗放群发、归因失真	补货/沉默信号、个性化建议、结果回写	同意、退订、频控和对照组

三、AI 智能体全景

1. 消费者、品牌与新品

AI 智能体	服务对象	主要任务与动作
消费者/VOC 闭环智能体	产品、品牌、客服、质量	汇聚评论，翻译与聚类，识别高风险问题，路由并跟踪改进
渠道情报智能体	总部、区域、营业所	定时读取会议、铺货、竞品和库存信息，分层汇总与提醒
新品机会协同智能体	市场、研发、采购、产能、销售	形成机会卡，创建验证任务，追踪上市反馈
配方研发副驾驶	研发、法规、质量	检索原料与历史试验，比较成本、营养和感官结果
食品标签合规审查智能体	法务、法规、质量、包装	提取字段，检索标准，提示冲突，发起版本审批
食品电商视觉工作流	品牌、电商、设计	读取 SKU 和品牌规范，生成素材并送审

2. 供应链、生产与质量

AI 智能体	服务对象	主要任务与动作
短保需求与补货智能体	计划、采购、门店、仓配	预测需求，结合效期和交期生成补货/调拨草案
茶饮供应链协调智能体	总部、仓库、采购、门店	协调多门店、仓、供应商和配送约束
食品工厂巡检整改智能体	安环、质量、生产	图像识别、人工复核、派单、整改、复查、周报
包装视觉质检系统	质量、包装线	识别字符、外观和包装缺陷，触发复核或拦截
设备维修知识与工单智能体	维修、设备管理	查故障、识元器件、给步骤、生成工单总结并回写
中央厨房追溯调查助手	质量、供应链、门店	从批次追溯原料、工序、设备、人员和配送订单

3. 门店现场、人员与客户

AI 智能体	服务对象	主要任务与动作
门店知识与训练智能体	店员、店长、督导	按身份和门店返回有效 SOP，模拟训练并沉淀错题
QSC 巡店与整改智能体	店长、督导、总部	识别问题、引用标准、派单、超时升级与复核
后厨效期智能体	厨房、食安、巡检	识别食材、计算限用日期、打印标签与临期预警
菜单工程助手	产品、运营、财务	分析销量毛利与原料关系，模拟组合和改价
餐饮排班智能体	店长、人力、员工	预测客流，在技能工时约束下排班和替班
咖啡具身服务与远程运营智能体	顾客、门店运营、设备团队	接单、按配方制作、监测状态、触发补料和维修
团购报价与服务智能体	团购销售、客服	澄清数量预算，调用商品规则生成报价和改单建议

四、重点智能体工作卡

1. 食品标签合规审查智能体

字段	内容
服务对象	法规、法务、质量、研发和包装设计
触发条件	新品包装送审、配方变更、销售地区变化、标准更新
输入	配方、原料、营养、包装稿、宣称、目标地区、法规版本
判断与规划	抽取强制字段，匹配条文，识别缺失、矛盾、禁用和过期内容
工具与系统	PLM/PIM、配方库、法规标准库、包装资产、审批与版本系统
输出与动作	逐字段问题单、依据、修改建议、待确认项和审批草案
人工控制点	法务/法规与质控签发；模型不得给出最终合法性结论
验收	历史裁定集上的重大问题召回、误报、条文引用和版本一致性

2. 茶饮供应链协调智能体

字段	内容
服务对象	计划、采购、仓配、区域和门店
触发条件	周期补货、活动、天气突变、缺货或临期风险
输入	SKU 日销、活动、天气、库存效期、采购周期、仓配能力
判断与规划	预测需求，比较采购、补货与调拨方案，解释缺货和损耗权衡
工具与系统	POS、ERP、WMS、TMS、供应商协同、预测和运筹工具
输出与动作	补货/调拨/采购草案、风险清单、责任任务和回写记录
人工控制点	下单、换供、跨区调拨和促销清货按金额与风险批准
验收	缺货、报废、库存周转、预测误差、建议采纳和执行回写

3. 后厨效期与食安智能体

字段	内容
服务对象	厨师、店长、食安、督导
触发条件	食材入库、开封、加工、换容器、临期和巡检
输入	语音/图片/NFC、食材批次、SOP、温度、开封和加工时间
判断与规划	识别食材与状态，匹配规则，计算限用日期并监控临期
工具与系统	食材主数据、SOP、标签打印、库存、巡检和工单
输出与动作	标签、临期告警、处置任务、纠错样本与巡检记录
人工控制点	低置信必须确认；错标签作废；过期、报废和食安事件由人员处置
验收	食材识别、日期计算、标签字段、打印成功、漏报和人工接管

五、代表案例与图片

案例一：飞鹤“鹤巡”——视觉识别只有进入整改链才产生价值

公开材料给出了摄像头/无人机取图、点位规则、AI 识别、人工二次校验、工单、整改和周报。其价值在于把“看见问题”变成“问题有负责人、有状态、有复核”。公开的 98% 应理解为 AI 与人工二次校验口径，不是独立模型准确率。



图：飞鹤工厂智能巡检案例

案例二：亚朵后厨——从非标输入到物理标签

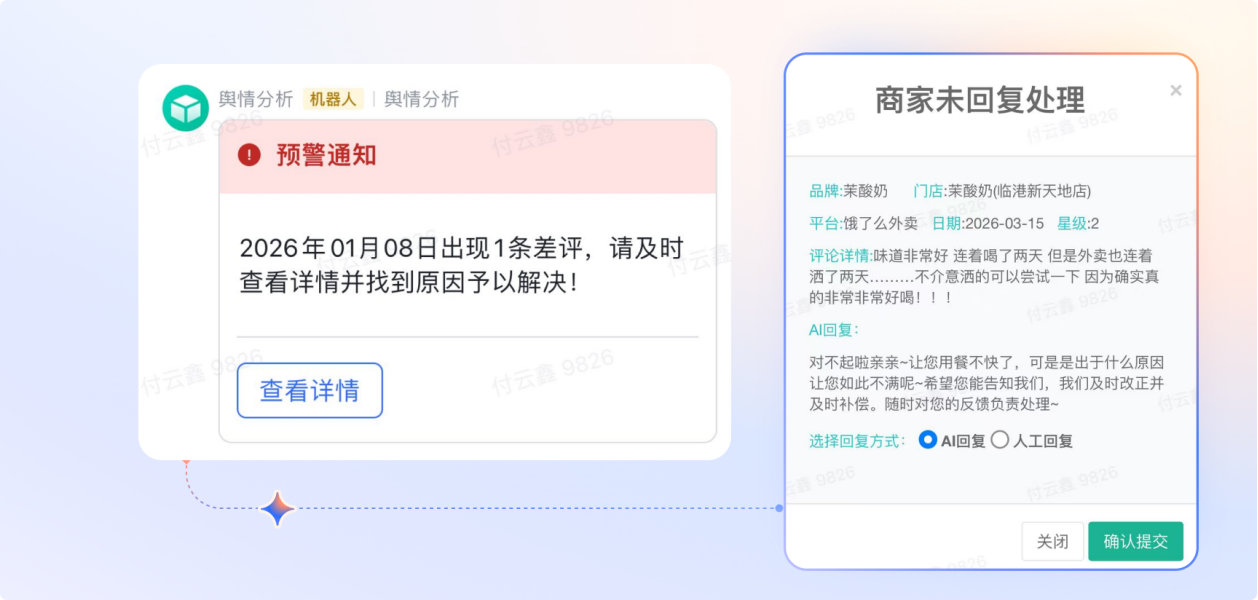
亚朵案例串联语音/图片识别、标准匹配、效期计算、标签打印、临期预警和一线纠错。它更像受标准约束的执行工作流，而非自由规划的高自治系统。验收必须覆盖方言、别名、照片模糊、打印失败、断网和错误标签撤销。



图：亚朵后厨效期管理案例

案例三：茉酸奶——差评不止要分类，还要形成组织动作

案例链路为外部评价或巡检进入系统，AI 分类并匹配责任人，建立整改任务，超时升级，处理后回复并沉淀记录。门店智能体的核心是把总部、区域、督导和店长连成责任链，并以闭环率、处理时效、复发率和顾客反馈验收。



图：茉酸奶门店问题闭环案例

案例四：康师傅——让总部听见一线，不等于 AI 自动经营

系统每日读取大量晨夕会内容，按渠道提取竞品、铺货、库存与动销信息，再逐级汇总反馈。它具备定时触发和信息穿透能力，但定价、铺货和营销调整仍由管理者决策。

六、系统、数据、权限与可靠性

1. 数据与知识

- 配方、原料、过敏原、法规、标签、批次、质检与召回数据必须统一版本；
- 门店、岗位、菜品、SOP、供应商、效期、活动和价格要带生效范围与时间；
- 评论、图片、语音和会议纪要保留来源、时间、主体与处理状态；
- 只有经人确认的纠错和策略才能回写正式知识库。

2. 业务系统

核心连接包括 PLM/PIM、ERP、MES、LIMS/QMS、WMS、TMS、POS、CRM/CDP、外卖与电商平台、协同任务、标签打印、IoT 和设备运维平台。智能体不应绕过这些系统建立第二套事实。

3. 权限与人工闸门

- 配方、标签、食品安全、质量放行、停线复产和召回由专业责任人批准；

- 采购、调拨、改价、促销、排班、赔付和对外回复按金额与风险分级；
- 顾客画像、录音、监控和营销触达遵守最小采集、用途限制、保存期限和退订；
- 写操作具备鉴权、幂等、回执、审计、撤销或补偿。

4. 异常恢复

断网、传感器离线、标签打印失败、库存延迟、平台接口限流、重复订单和模型低置信时，系统应停在安全状态并交给人工；不能为了“自动化率”继续执行不确定动作。

七、落地路线与试点选择

阶段 0：建立基线

选定一个门店群、工厂区域或品类，记录人工耗时、错误、缺货、损耗、投诉与整改周期。

阶段 1：只读助手

先上线知识检索、标签预审、VOC 聚类、经营报告和追溯证据整理，不写业务系统。

阶段 2：受控工作流

开放自动建任务、提醒、标签草稿和补货草案；所有高影响动作由人确认。

阶段 3：有限执行

对稳定、可回滚、低金额动作开放白名单执行，并持续比较人工与智能体结果。

阶段 4：多门店复制

按业态、地区、门店成熟度和系统版本分批扩展，保留本地规则与申诉渠道。

推荐优先顺序是：门店知识与巡检、VOC 路由、标签预审、追溯调查、后厨效期、补货协同，再到排班、菜单、生产优化和具身执行。

八、评测与验收

场景	任务质量	业务结果	风险与闭环
标签合规	重大问题召回、误报、依据与版本	审核周期、返工、上市延迟	专业复核、错版拦截、审计
工厂巡检	点位覆盖、漏检误报、图像鲁棒性	复核时间、隐患关闭、重复问题	假整改、摄像头离线、升级
后厨效期	识别、日期、标签和打印准确	操作时长、临期发现、报废	错标签、断网、人工接管
门店 QSC	分类、标准引用、责任匹配	覆盖、闭环、复发率	重大食安漏转、申诉、复核独立
VOC	标签、严重性、路由、聚类	发现提前量、整改周期、采纳	噪声、隐私、错误归因
补货	预测误差、约束满足、建议可行	缺货、损耗、周转、履约	重复下单、数据延迟、回滚
排班	覆盖、规则满足、人工修改率	加班、缺岗、员工稳定	公平性、劳动规则、紧急接管

所有业务成效必须用企业自身同口径基线验证。厂商公开的节时、准确率、闭环率或销售规模只用于提出试点假设。

九、风险边界

- 食品标签与配方涉及地区和时间有效性，静态知识库极易过期；
- 视觉识别会受遮挡、光照和场景迁移影响，不能跳过人工复核；
- 需求预测不等于可执行补货，效期、MOQ、仓容、配送和现金约束必须进入求解；
- 门店监控、顾客数据和精准营销存在隐私、歧视与骚扰风险；

十、案例与来源索引

核心来源

- 飞鹤“鹤巡”工厂智能巡检
- 亚朵酒店后厨管理
- 茉酸奶门店管理
- 益禾堂产品质检
- 康师傅会议与一线信息管理
- 思念食品新品研发
- 健力宝设备运维助手
- 海底捞知识问答
- 广州酒家电商客服
- 科沃斯用户洞察
- 瑞幸咖啡 AI 供应链
- 蒙牛乳业 AI 视觉质量检测
- 食品标签合规审查红线与新规解读
- 茶餐饮行业 AI 供应链核心技能图谱
- 具身智能咖啡服务案例
- 中央厨房 MES 生产管理系统解决方案
- 餐饮业 AI 管理：从库存预警到智能排班
- AI 驱动的肉食品行业跨部门协同

本章小结

消费品、食品与餐饮的智能体化，需要把消费者信号、食品标准、批次事实、门店状态和责任任务连接起来，并避免让一个模型包办品牌、工厂和门店。最可靠的路径是先让 AI 发现、解释和协调，再在确定性规则和人工签审之下开放有限执行。能否追到一张标签、一个批次、一家门店和一次整改结果，决定了它是演示工具，还是企业可验收的生产系统。

第七章 零售与电商：从商品、交易到履约和复购的智能体网络

零售与电商的 AI 智能体应用，已经贯通商品、门店、客户、订单、库存、内容、履约和经营分析，并持续向跨境供应链与全渠道运营延伸。

本章核心结论

零售与电商的核心，是围绕商品、门店、客户、订单、库存、平台账户和资金形成连续经营。目前较成熟的智能体集中在门店巡检、VOC 闭环、库存风险、经营诊断、订单写入和内容投放监控；意图购物、跨境供应商风险、复购运营、电商视频多智能体、即时零售配置、门店边缘设备运维和 AIGC 真实性审查也已进入探索与应用。

成熟应用往往是“模型判断 + 业务规则 + 系统接口 + 人工批准”。推荐、搜索、动态定价、销量预测、视觉识别和评论分类都很重要，但它们通常是智能体调用的能力，而不是完整智能体。只有当系统能持续观察、调用工具、改变任务状态、处理失败并用结果反馈时，才真正进入业务链。

一、行业边界

1. 实体连锁零售

以门店网络、商品、人员和现场履约为核心，重点包括选址、采购补货、陈列价格、排班服务、巡店、防损、会员和店效。

2. 品牌直营与全渠道

品牌同时经营门店、平台店铺、私域和经销渠道，核心是商品、库存、会员、订单、内容与服务的一致性。服饰、家纺、消费电子等企业的主行业仍可归消费品或制造业，本章记录其电商链路。

3. 平台电商与即时零售

平台承担商家治理、商品审核、搜索推荐、广告、交易支付、履约协调、售后争议和风险控制；即时零售还要处理门店实时库存、营业时段和履约半径。

4. 跨境电商

在国内电商基础上增加国家和平台规则、多语言、知识产权、税务、支付、跨境物流、本地化内容与售后。

5. 电商代运营与综合服务

其交付对象是客户店铺，必须处理多客户数据隔离、账号授权、服务 SLA、预算批准、交付计费和方法复用，不能把品牌内部工作流原样复制。

二、核心业务链与逐环节问题

市场洞察与选品 → 供应商与采购 → 商品建档 → 内容与上架 → 搜索推荐与投放 → 交易支付 → 库存与履约 → 客服售后 → 评价/VOC → 会员复购 → 经营诊断 → 平台与内容合规

业务环节	关键问题	智能体机会	人工控制点
洞察选品	趋势噪声大、抄竞品、需求不等于购买	趋势研究、竞品变化解释、反事实分析	选品和备货由经营者决策
供应商	只比报价，忽略质量、交期和退货	总落地成本、承诺兑现、Plan B 监测	样品、验厂、资质和换供确认
商品建档	参数冲突、版本多、客服知识滞后	事实卡编译、缺失冲突检测、版本审批	商品负责人批准后发布
内容上架	产能高但事实、版权和平台风险大	多角色脚本/分镜/生成/质检回打	发布前人审，实物一致和披露要求优先
搜索导购	用户需求模糊、实时信息变化	多轮澄清、商品研究、比较与交易草案	用户确认价格、数量、地址和退改规则
库存履约	多系统延迟、断货与积压并存	风险预测、补货/调拨建议、异常派单	调拨、停售、采购和替代品批准
客服售后	FAQ 会答但不会办事，容易乱承诺	查询订单、创建工单、事项处理、转人工	退款、补偿、高风险投诉分级授权
VOC	标签很多但不进入产品改进	严重性识别、责任路由、跟踪和回写	重大质量问题与公开回应人审
复购	群发骚扰、转化归因失真	补货/沉默信号、建议、人工确认、结果回写	同意、频控、退订和对照组
经营诊断	取数口径不一、相关性被误当因果	定时取数、下钻、报告、派单与策略沉淀	预算、改价、停投和目标由人决定

三、AI 智能体全景

1. 消费者与商品发现

AI 智能体	任务与动作
意图购物研究与交易协调智能体	澄清预算和用途，查询实时商品、库存与评价，比较候选并生成订单草案
多轮导购智能体	在推荐、搜索、比价和问答之间切换，解释选择并接受修正
商品事实卡编译智能体	从详情页、说明书和政策提取事实，识别冲突并生成版本化知识卡
AIGC 商品真实性审查智能体	比对实物、规格与生成内容，检查夸大、伪造和披露要求

2. 门店与全渠道运营

AI 智能体	任务与动作
门店知识与运营支持智能体	按身份、区域和门店调用知识，无法解决时转工单
巡店整改智能体	上报、分类、派单、整改、复核和报告
店效分析智能体	汇聚门店汇报和销售，比较计划与执行
门店边缘设备舰队运维智能体	统一注册、版本、分批更新、健康监测、告警归因和回滚
即时零售线上运营助手	检查商品、价格、库存、活动和履约配置并生成操作清单

3. 供应链、库存与订单

AI 智能体	任务与动作
供应商总落地成本助手	计算包装、检测、物流、关税、返工与延误成本，模拟风险
供应商承诺监测智能体	从沟通和合同抽取承诺，对照实际交付，触发备选验证
库存风险与调拨协同智能体	汇聚 ERP/WMS/ 平台数据，预测断货，创建调拨任务
群报单与 ERP 履约智能体	从群消息识别订单、拆单、校验和写入 ERP
退货风险干预助手	识别尺码、组合或商品风险，给出发货前提示

4. 客户、内容与增长

AI 智能体	任务与动作
VOC 与高风险客诉闭环智能体	聚类评论、识别严重性、路由责任部门并跟踪解决
客服复盘与预警助手	对大量会话分类、复盘和识别风险/意向
复购信号运营智能体	识别补货或沉默信号，经人工确认触达并回写结果
电商视频生产多智能体	洞察、脚本、分镜、素材、装配、质检与回打协作
内容与投放智能体	校验品牌事实、监控投放、建议加投或停损
跨境增长多智能体团队	市场、VOC、内容、社区、短视频角色协作

5. 经营与平台治理

AI 智能体	任务与动作
经营监控、诊断与派单智能体	定时取数、异常下钻、归因、责任派单和策略沉淀
多智能体滥用评测系统	在隔离环境模拟评论、舆论和交易操纵并发现监控盲区
平台风险调查智能体	聚合账户、设备、交易、评论关系和证据，提出处置建议

四、重点智能体工作卡

1. 意图购物研究与交易协调智能体

字段	内容
服务对象	消费者、平台导购、客服
触发条件	用户提出模糊购买目标或跨品类复杂需求
输入	用途、预算、偏好、实时商品、库存、价格、评价和服务规则
判断与规划	追问硬约束，研究商品事实，比较候选，识别冲突与风险
系统与工具	搜索推荐、PIM、库存价格、评价、试穿/试用、交易和履约
输出与动作	比较表、选择理由、购物方案和订单草案
人工控制点	下单前由用户确认关键字段；不得隐藏广告、利益排序或退改条件
验收	事实正确、约束满足、实时性、可购买率、用户成功率和失败恢复

2. 经营诊断与派单智能体

字段	内容
服务对象	店铺运营、品牌负责人、代运营团队
触发条件	每日/每周周期，或销售、流量、转化、库存、投放异常
输入	BI、店铺、广告、库存、活动、竞争和组织权责
判断与规划	校验口径，多层下钻，区分外部与内部因素，生成可验证假设
系统与工具	平台 API、ERP/WMS、广告、BI、任务与策略知识库
输出与动作	经营报告、异常证据、责任任务、采纳和关闭状态
人工控制点	不自动改预算、改价或停店；错误归因可申诉和否决
验收	取数正确、异常召回/误报、建议可执行、任务关闭和增量结果

3. 电商视频生产多智能体

字段	内容
服务对象	商品运营、创意、设计、合规与投放
触发条件	新品上架、活动批量生产、素材迭代
输入	商品事实、受众、平台规则、品牌资产、历史投放和版权信息
判断与规划	拆解洞察、脚本、分镜和制作任务，质检失败回打对应环节
系统与工具	PIM、DAM、生成模型、剪辑、审核、投放与效果平台
输出与动作	视频、质检报告、修改记录和送审任务
人工控制点	商品真实性、版权、广告披露和最终发布必须人审
验收	现有通过率、事实错误、版权风险、重做成本和增量投放效果

五、代表案例与图片

案例一：渝欧跨境——经营智能体的价值在闭环而非一张日报

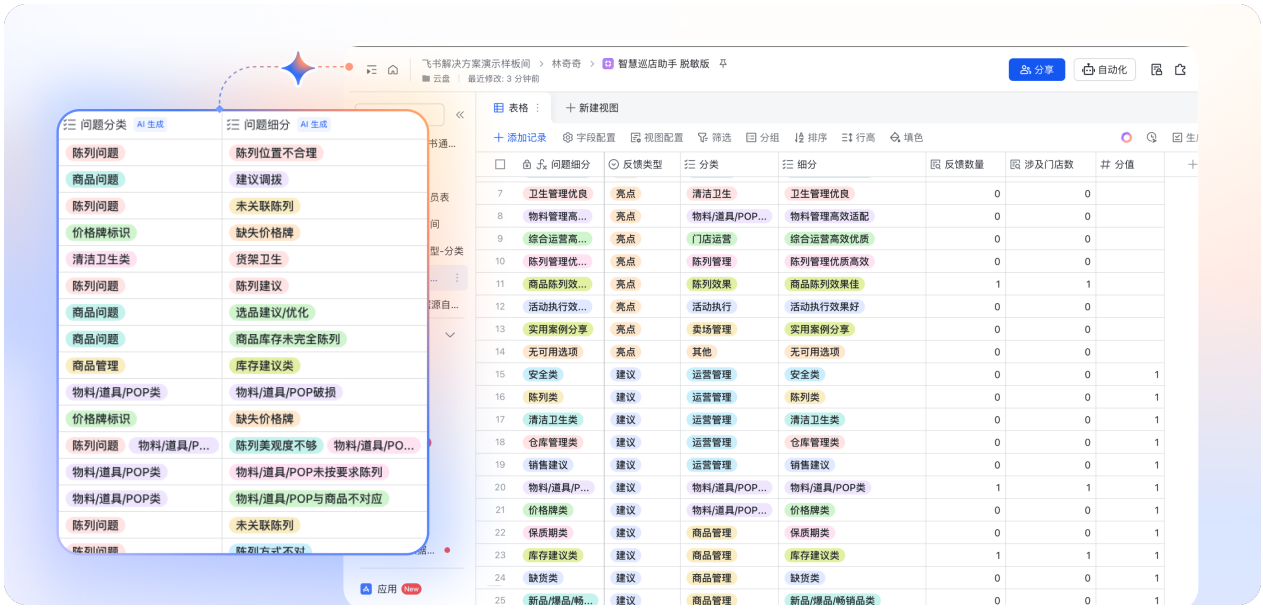
该应用覆盖数据抓取与清洗、昨日复盘、异常识别、外部竞争与内部执行归因、经营结论、责任派单和策略图书馆，比单次 BI 问答更接近持续经营智能体。企业验收应关注响应时间、风险识别金额、建议采纳率、任务闭环和人员效率。



图：渝欧跨境经营案例

案例二：名创优品——AI 分类加确定性流程形成巡店中枢

案例把问题上报、AI 打标分类、整改通知、处理、复核和报告串联起来。它强在任务状态和责任闭环，弱在动态自主规划，适合归为 AI 增强工作流。



图：名创优品智慧巡店案例

案例三：SKG——评论分析只有进入产品问题管理才构成闭环

方案覆盖多平台评论汇聚、打标、严重性识别、自动路由、跟踪解决和洞察报告。其关键是将问题分配给研发、物流、客服或品牌部门并留下结果。



图：SKG VOC 闭环方案

案例四：NEIWAI——预测、规则与任务要拆开验收

系统汇聚 ERP、WMS 和平台库存，计算健康指数、预判断货，并通知和创建调拨任务。材料未证明 AI 直接拥有调拨或停售权限，因此应分别验收预测误差、规则有效性、任务执行和人工审批。

六、系统、数据、权限与平台合规

1. 数据底座

统一商品/SKU、供应商、门店、渠道、客户、活动、库存、订单、退款和责任人主数据；评论、聊天、巡店图片与群消息保留来源、时间和处理状态。

2. 系统接口

连接 PIM、ERP、OMS、WMS、CRM/CDP、客服、广告、BI、内容资产和平台官方 API。浏览器自动化只能作为受控补充，不能假设页面、登录态和反自动化规则长期稳定。

3. 权限与人工控制

- 读写权限分离，改价、预算、退款、封禁、采购、调拨、停售、发布与私信分别授权；
- 先建议、后批准、再执行，结果必须回查；
- 金额、库存、账号、高价值客户和舆情设置硬阈值与双人批准；
- 跨境触达遵守同意、退订、频控、广告披露和当地个人信息规则。

4. 内容与平台安全

商品内容必须与实物一致，不能伪造效果、参数或消费者故事。TikTok Shop 等平台规则会持续变化。多智能体欺诈研究只能在隔离环境用于防护测试，不得对真实平台实施攻击。

七、落地路线

- 建立单门店、单渠道、单品类或单客户组基线；
- 先做知识卡、经营报告、VOC 聚类和巡店分析等只读任务；
- 再开放自动建单、派单、提醒和订单草稿；
- 在官方 API、幂等、回执和回滚完备后，开放低风险白名单写入；
- 通过 A/B 或对照组验证增量收益，再扩展到多平台、多门店和多客户；
- 规模化前测试峰值负载、账号风控、租户隔离、灾备、成本和人工接管。

优先顺序建议为：商品事实卡、门店知识、巡店整改、VOC 路由、经营诊断、复购试点、库存协同、订单写入，再到意图购物、内容多智能体和有限自动经营。

八、评测与验收

场景	任务质量	业务结果	风险与闭环
意图购物	事实正确、约束满足、库存价格实时	任务完成、转化、退货与满意度	利益披露、用户确认、失败恢复
巡店	分类、责任人、证据有效	覆盖、闭环、复发率	假整改、申诉、复核独立
经营诊断	取数、召回/误报、归因可复核	周期、采纳、任务关闭、增量利润	错误派单、预算越权、策略版本
库存调拨	预测误差、建议数量与时点	缺货、积压、周转、履约	重复动作、延迟、回滚
客服事项	意图、订单字段、答案和转人工	一次解决、处理周期、满意度	隐私、错误承诺、高风险漏转
复购	名单准确、话术事实、触达成功	对照组增量复购、毛利	退订、频控、骚扰投诉
内容投放	商品事实、品牌、版权、平台合规	审核通过、CTR/CVR、增量 ROI	虚假内容、预算越界、停损
ERP 写入	字段、拆单、幂等、回执	漏单错单、处理时间、履约	越权、重复提交、可回滚

九、风险边界

- 推荐和定价可能造成利益不透明、差异化待遇和消费者权益风险；
- 平台接口、账号和政策变化会让自动化突然失效；
- 经营诊断容易把相关性写成因果，错误派单会放大组织摩擦；
- 生成内容存在商品事实、版权、肖像、广告披露和文化风险；

- 跨境供应商与平台资料可能伪造，需按报价、样品、验货和历史订单逐级增权；

十、案例与来源索引

核心来源

- 渝欧跨境电商经营智能体
- 青木科技电商经营数字员工
- 名创优品智慧巡店管理中枢
- SKG 用户洞察
- NEIWAI 大促库存监控
- 美宜佳全渠道知识问答
- 全棉时代门店店效管理
- 爱回收智能客服
- 杰森娱乐销售助手
- 水星家纺内容与投放数字员工
- 京东用 AI 重做电商
- 跨境电商供应商筛选
- 电商客服 AI Skill
- 跨境电商视频多智能体
- 门店客户复购系统
- 即时零售线上运营
- 门店 AI 设备运维
- TikTok Shop 东南亚 AIGC 规则

本章小结

零售与电商智能体的真正价值，是把消费者意图、商品事实、库存、订单、客服、内容和经营动作连接起来。企业不应以“生成了多少内容”或“自动回复率”验收，而要检查事实是否正确、任务是否完成、结果是否回写、平台是否允许、失败是否可恢复，以及高影响动作是否仍在人类授权之内。

第八章 物流、供应链与邮政：跨组织、跨系统、跨运输方式的智能体协同

物流、供应链与邮政的 AI 智能体应用，已经进入客服、需求理解、仓储作业、运输调度和风险协同，并向多式联运、超大件运输与内河监管扩展。

本章核心结论

物流行业最适合 AI 智能体的原因，是一次订单天然跨越客户、承运商、仓库、司机、港口、铁路、关务和结算系统；最难的地方也正是跨组织数据不完整、责任分散、状态变化快。真正的价值不在于让大语言模型“算路线”，而在于理解事件、补齐上下文、调用预测或运筹工具、形成备选方案、推动授权、更新系统并追踪异常关闭。

目前已有 DHL 多任务客服、货拉拉需求理解与车型推荐、WMS 自然语言查询和写单等应用。船舶—港口—铁路多式联运、超大件运输、供应链风险控制塔、内河监管和小单拼载也正在形成新的应用方向。

一、行业边界

1. 独立物流、运输与邮政

包括快递包裹、第三方物流、合同物流、公路货运、国际货代、航运港口、铁路与多式联运、公共仓和邮政普遍服务。这些组织以物流服务本身作为收入来源或公共职责。

2. 企业内部供应链

制造、零售、餐饮和医药企业也有采购、库存、仓储和发货，但属于客户行业的内部职能。本章只借用通用磨坊、联影、致欧等材料解释方法，不重复主归属。

3. 物流智能体与相邻系统

ETA 预测、路径规划、装载、排程、视觉读码、OCR、RPA、AGV 和 PLC 都是重要能力或执行器。只有进入目标、状态、工具、动作、反馈与人工控制链后，才构成完整智能体。

二、核心业务链与逐环节问题

获客询价 → 订单/运单/订舱 → 提货揽收 → 入库与分拣 → 计划调度 → 干支线运输 → 港航铁路与多式联运 → 末端签收 → 在途异常 → 客服理赔 → 回单对账与结算 → 网络/运力经营 → 安全关务合规

环节	关键问题	智能体切入点	人工控制点
询报价	货物描述非结构化、计费约束多	提取货物字段、车型/线路候选、费用试算	客户确认货物与价格，危险属性人工核验
订单单证	邮件、提单、发票、报关字段不一致	文档抽取、差异定位、补件任务	报关申报、承诺和改单人工批准
仓内作业	库存口径、波次、人员设备冲突	自然语言查询、写单、任务编排、异常分流	写单幂等，机器人安全联锁独立

环节	关键问题	智能体切入点	人工控制点
运输调度	时间窗、车型、司机、路线与成本冲突	调用预测/运筹求解，生成备选和滚动重排	高价值改派、超载风险、危险品人工确认
多式联运	主体利益不同、系统协议不一、异常级联	多角色提议、协商、冲突升级与审计	数据最小共享，人工仲裁未决冲突
在途异常	温度、偏航、延误和港口事件影响难定位	识别事件、匹配订单、生成改线/改港方案	客户承诺、换承运商和额外费用审批
客服理赔	查询跨系统、证据散、重复沟通	多轮任务客服、工单和证据包	赔付、责任认定和高风险投诉转人工
对账结算	运单、回单、账单和合同口径不一	差异识别、费用归因、索赔/结算草案	付款、冲正、开票和核销由授权人执行
监管安全	AIS/ 视频、许可和现场事实需结合	候选事件识别、证据整理、核查任务	不自动作出行政处罚或安全关键指令

邮政另有网点/线上受理 → 验视计费 → 分拣封发 → 干线 → 投递 → 查询改退赔偿 → 普遍服务质量与安全监管。商业快递客服与邮政普遍服务的责任、系统和监管要求不同，应分别建设智能体。

三、AI 智能体全景

1. 客户、订单与单证

AI 智能体	主要任务与动作
快递多任务客服智能体	多轮收集参数，调用知识、计费和工作流处理寄收件与查询
货运需求理解智能体	提取货物名称、数量、尺寸、重量和运输方式
车型推荐协调智能体	调用车型和安全工具，解释推荐并推动用户确认
货代单证智能体	解析邮件、订舱、提单、发票和报关单，定位差异并归档
物流结算对账智能体	对照运单、回单、合同和账单，生成差异与核查任务

2. 仓储、运输与异常

AI 智能体	主要任务与动作
WMS 查询与写单智能体	查真实库存、创建入库单、回答仓储制度
仓内任务调度智能体	编排收货、上架、拣选、补货、盘点和设备任务
物流动态调度智能体	汇聚订单、车辆、司机、时窗和路况，调用求解器滚动重排
事件驱动异常处置智能体	从 WMS/TMS/IoT 事件定位影响，生成备选，经批准更新系统
小单协同拼载智能体	聚合小单，计算兼容性、容量、时间窗和成本分摊
超大件运输方案智能体	读取设备参数、道路桥梁和许可，生成路线与审批材料

3. 港航、铁路与供应链韧性

AI 智能体	主要任务与动作
多式联运协调智能体	协调船舶 ETA、泊位岸桥、堆场和铁路车皮，冲突升级
船舶 ETA 与准时到达助手	综合 AIS、天气、潮汐和泊位窗口，比较航速方案
港口资源协商智能体	调用运筹工具生成泊位、岸桥、堆场组合并记录协商
铁路车皮配置智能体	查询空车与运行图，生成装车、编组和路径候选
供应链风险协调智能体	从外部事件定位受影响订单，给改港、改线或库存建议并跟踪
内河违规证据整理助手	融合 AIS、视频和围栏生成候选事件与证据包

四、重点智能体工作卡

1. 多式联运协调智能体

字段	内容
服务对象	航运公司、港口、堆场、铁路和综合调度中心
触发条件	船舶 ETA 变化、泊位冲突、堆场拥堵、车皮不足或异常中断
输入	AIS、天气、潮汐、泊位岸桥、堆场、运行图、货种、优先级与 SLA
判断与规划	各主体生成提议，监督角色校验约束、协调冲突并限制协商轮次
工具与系统	VTS/AIS、TOS、堆场系统、铁路 TMIS、运筹求解器和消息协议
输出与动作	协同计划、确认消息、资源冲突、升级记录和版本差异
人工控制点	危险品、滞期费争议、未收敛冲突和跨主体责任由人仲裁
验收	约束满足、计划稳定、协商收敛、超时/死锁、数据最小化和接管



图：多式联运多智能体协同示意

2. 超大件运输方案智能体

字段	内容
服务对象	项目物流、工程、承运商、安全与审批人员
触发条件	超长、超宽、超高或超重设备运输项目
输入	尺寸重量、重心、道路桥梁、转弯、施工、天气、法规与历史项目
判断与规划	筛除硬约束不满足路线，生成候选、风险点、踏勘和许可清单
工具与系统	GIS、桥梁档案、BIM/ 图纸、仿真、法规许可和项目管理
输出与动作	路线候选、加固/护送建议、勘察任务和审批材料草案
人工控制点	现场踏勘、结构校核、承运方案与主管部门许可不可省略
验收	硬约束零遗漏、专家修改、方案时间、版本与现场偏差

3. 风险影响与异常处置智能体

字段	内容
服务对象	控制塔、运输、客户服务、采购和管理层
触发条件	港口关闭、极端天气、承运异常、供应商事件、温度或 ETA 超限
输入	外部风险、订单、路线、库存、客户 SLA 和承运资源
判断与规划	按地域、时间和运输方式匹配受影响订单，比较备选成本与时效
工具与系统	风险数据源、OMS、TMS、WMS、ERP、地图和承运商平台
输出与动作	风险分级、订单清单、改线/改港/库存方案、任务与复盘案例
人工控制点	对外承诺、额外费用、换承运商和高价值调度须批准
验收	预警提前量、影响匹配、方案可执行、关闭时间和损失口径

五、代表案例与图片

案例一：货拉拉车型推荐——把“对话”拆成需求理解和业务决策

官方技术材料把系统拆为 NLG 和 NLU 角色，并结合通用知识库、FAQ、长短期记忆、车型推荐、安全工具、敏感词和规则。公开的 90% 是内部测试集上的货物字段识别准确率，不等于车型推荐正确率或下单转化。其启示是：对话、字段抽取、专业推荐和用户确认必须分别验收。

案例二：DHL 任务型客服——服务事项比 FAQ 更接近业务

DHL 案例覆盖寄件、收件、查询和计费等多类任务，通过多轮对话补齐参数并调用工作流。公开解决率和转人工变化为厂商—客户口径。禁限寄、跨境合规和计费仍应调用确定性规则，不能由模型自由生成。

案例三：WMS 自然语言查询与写单——写入真实系统才暴露工程风险

仓储智能体可以通过聊天入口查询库存、创建入库单和调用仓储知识库。进入生产环境时，必须具备字段校验、鉴权、幂等、日志、状态回查和撤回机制。

案例四：物流智能调度——专业求解器与智能体各司其职

行业方案把订单、车辆、司机、时间窗、路况与异常重排组合起来。大语言模型适合理解目标、补齐参数和解释方案；路径、装载和排程应交给运筹或专业算法。



图：物流全链路作业应用示意

案例五：供应链风险控制塔——风险新闻必须落到受影响订单

控制塔只有完成“外部风险—订单/路线匹配—备选方案—执行跟踪—复盘”才从信息监测升级为流程智能体。只聚合新闻或打风险分数，仍是情报与预测系统。

六、系统、数据、权限与安全

1. 数据与语义

统一订单、运单、箱/托盘、库存、在途、ETA、路线、承运商、客户和 SLA；货物尺寸、重量、危险属性、温控、贸易条款、批次与责任主体可追溯。

2. 系统与协议

连接 CRM、报价、OMS、WMS、WCS、TMS、ERP、关务、客服、票税结算、IoT、AIS/VTS、TOS、铁路系统和承运商平台。跨组织协作应约定字段、时效、置信度、回执、重试和数据最小化。

3. 权限与人工控制

- 查询与写入分离；订舱、改派、调拨、报关、退款、结算分别授权；
- 车型、费用和路线建议由用户或调度员确认；
- 港航、冷链、危险品、超大件和邮政安全不得由大语言模型单点控制；
- 行政执法和责任判定必须人工核查；
- 外部邮件、网页和单证均视为不可信输入，防止提示注入。

4. 工程可靠性

所有写操作具备幂等、状态回查、超时、重试、补偿和审计。传感器离线、地图过期、数据冲突、协商不收敛、金额超限或低置信时自动转人工。

七、落地路线

- 先记录人工计划、异常处理、单证和客服基线；
- 用历史订单做离线回放，只生成建议；
- 进入影子模式，比较智能体与调度员方案；
- 开放只读查询、自动建单和通知；
- 对低风险、可回滚动作开放白名单写入；
- 经峰值、断网、重复事件和异常恢复测试后扩大线路或客户范围；
- 多式联运需先解决跨组织协议、数据权属和人工仲裁，再谈自动协商。

优先试点可选择任务型客服、单证核对、WMS 只读查询、异常证据整理和对账差异；动态调度、多式联运、超大件与监管应后置。

八、评测与验收

场景	任务质量	业务结果	安全与闭环
快递客服	意图/槽位、任务完成、计费正确	自助解决、转人工、处理时长	禁限寄升级、错误承诺、日志
车型推荐	字段提取、车型适配、纠错	转化、取消/改车型、客服介入	超载/不适装、用户确认
WMS 写单	查询正确、字段完整、写回成功	处理时间、错单、返工	越权、重复单、回滚
单证核对	字段准确、差异检出、依据	补件、退单、处理周期	低置信复核、错误自动补写为 0
动态调度	约束遗漏、可执行、稳定性	准时率、空驶、异常关闭、增量成本	人工接管、状态回查、补偿
多式联运	协议兼容、协商收敛、约束满足	等泊、转运、计划变更	死锁、数据泄漏、人工仲裁
风险控制塔	预警、影响订单匹配、方案质量	提前量、关闭时间、损失避免	错误改线、客户承诺、审计
监管助手	漏报误报、时空对齐、证据完整	发现到核查时间	人工执法、证据链、权限

九、风险边界

- 路线、调度和装载存在硬约束，语言模型不能替代运筹、仿真与安全计算；
- 跨组织智能体可能泄露客户、价格、运力和运营数据；
- 外部单证和邮件可能包含恶意内容，工具调用需隔离；

- 高频算法管理可能影响司机和一线员工公平性、休息与申诉；
- 空驶率、ROI、效率和人员投入变化应按企业自身基线、范围和运行周期评估。

十、案例与来源索引

核心来源

- 货拉拉 AI 客服选车助手
- WMS 仓储系统集成 AI 智能体
- 供应链与物流智能调度及异常预警
- 货代岗位应用
- 多智能体在多式联运中的应用架构
- 大模型驱动超大件设备运输方案
- 供应链风险控制塔
- 内河航运监管平台 AI 升级
- 小单供应链智能体
- AI 驱动的物流智能调度系统

本章小结

物流智能体的核心能力，是把跨系统事件转为可执行、可授权、可追踪的协同动作。越跨组织、跨运输方式和安全边界，越需要专业求解器、确定性控制、人工仲裁和完整审计。只有异常真正关闭、系统状态真正回写、失败真正可恢复，智能体才从“物流建议助手”进入生产链。

第九章 旅游、酒店与文旅：把灵感、交易与现场履约连接起来

旅游、酒店与文旅行业的 AI 智能体已经从内容推荐进入实时产品查询、行程规划、预订、住中服务、客诉处理和现场履约。

本章核心结论

旅游 AI 最容易做出“看起来很美”的攻略，也最容易在营业时间、路线、价格、库存、退改规则和安全信息上出错。真正有价值的 AI 智能体必须从灵感和内容生成走向实时产品、预订、住中服务、客诉、行中变化与人工接管。

目前已有华住住中服务协调、亚朵后厨效期、同程 DeepTrip 旅行规划与预订，以及去哪儿酒店售后问答等应用。飞猪多顾问旅行协调、酒店客诉分级、酒店采购、评论摘要安全、酒店应用网关安全与旅游规划任务评测也构成了重要实践方向。

本行业的共同原则是：动态事实必须实时查询，高风险事件必须快速转人工，付款和变更必须得到用户确认，生成内容必须保留来源和不确定性。一个能写行程的模型，不等于一个能承担旅行履约的智能体。

一、行业边界

1. 酒店与住宿运营

围绕房态房价、渠道、入住、住中客需、餐饮、设施、结算、评价、会员与单店经营。酒店地产开发归房地产，开业后运营归本章。

2. OTA 与旅行服务

OTA 承担商品、流量、交易、支付和平台服务；旅行社、地接社和定制游还承担资源确认、报价、合同、行前、行中和售后履约。二者共享交易链但责任不同。

3. 景区、目的地与文化场馆

围绕票务、客流、导览、演出、二次消费、设施、安全和目的地运营。客流预测与语音讲解本身不是完整智能体。

4. 会展与节事活动

是 B2B 项目制服务，包含招商招展、观众招募、议程、现场交付、商贸撮合和会后线索复盘，不能被普通旅游客服代表。

5. 邮轮与综合度假

同时组合交通、住宿、餐饮、娱乐、岸上活动和医疗安全。相关应用仍处于探索阶段，需要通过实际项目验证。

二、核心业务链与逐环节问题

1. 酒店运营链

定位筹开 → 房态房价 → 渠道获客 → 预订咨询 → 到店入住 → 住中客需 → 餐饮后厨 → 工程设施与安全 → 离店结算 → 客诉评价 → 会员复购 → 单店经营与标准迭代

环节	关键问题	智能体机会	人工控制点
预订售前	房型、价格、权益和政策动态变化	实时查询、比较、订单草案	下单、支付和特殊承诺用户确认
入住住中	一个请求常包含多个意图	场景切换、工单、机器人/人员调度	错房错物、身份和隐私校验
后厨食安	食材别名、效期和标签易错	识别、标准匹配、打印和预警	错标签拦截、过期品人工处置
工程设施	客房设备、能耗和工单分散	故障分诊、知识检索、派单与跟踪	高危维修和停用决定人审
客诉	情绪、证据、授权和舆情交织	风险分级、止血建议、升级与复盘	不自动判责、赔付、删帖或诉讼
收益经营	需求、渠道、房价和库存权衡	预测、优化、建议和复盘	定价政策、公平性和异常回滚

2. 旅行与 OTA 链

市场/目的地研究 → 供应签约 → 产品与线路 → 库存价格规则 → 搜索推荐 → 需求澄清 → 行程报价 → 预订支付 → 行前资料 → 行中变更/应急 → 退款投诉 → VOC 复购 → 供应商复盘

环节	关键问题	智能体机会	人工控制点
行程规划	目标开放、约束多、没有唯一答案	多顾问拆解、实时检索、冲突合并	重大冲突向用户确认
可预订性	攻略与真实库存价格脱节	实时机酒门票、营业与路线校验	付款和退改条款明确展示
销售	客户需求散、线路版本多	摘要、产品比较、报价条件与跟进	毛利、折扣、合同与承诺人工决定
行中服务	天气、延误、闭园等持续变化	监测影响、重排候选、通知和工单	医疗、安全、未成年人迅速转人工
售后退款	规则复杂、客户重复说明	订单上下文、自助事项、低置信转人工	例外退款和争议处理分级授权

3. 景区与会展链

景区链为产品活动 → 票务预约 → 入园 → 客流交通 → 导览演出 → 二消 → 现场服务与安全 → 评价复购；会展链为立项 → 招商招展 → 招观 → 议程/展位/物料 → 现场交付 → 商贸撮合 → 线索交付与续约。两类业务都需要实时状态、现场工单与安全升级，不能只做文案和推荐。

三、AI 智能体全景

1. 酒店服务与经营

AI 智能体	主要任务与动作
酒店住中服务协调智能体	多意图识别、知识查询、工单创建、机器人送物与完成回查
酒店售后问答与人工升级助手	区分可自助和必须人工事项，检索 FAQ、查询订单、生成转接摘要
酒店客诉分级与授权处置智能体	风险情绪分级、匹配授权和 SOP、跟踪整改与舆情
酒店食品效期助手	识别食材、匹配标准、打印标签、临期预警和纠错
酒店收益协同智能体	读取 PMS/CRS/ 渠道，生成价格与库存建议并复盘
酒店装修物料采购智能体	解析规格、搜料、比较总成本、生成询价与审批草案
酒店权限与诈骗预警智能体	监控网关、身份、支付和房客数据异常，升级安全事件

2. 旅行决策、交易与履约

AI 智能体	主要任务与动作
旅行咨询、规划与预订智能体	澄清日期人数预算，调用机酒、POI、地图和天气，形成可执行方案
飞猪旅行协调智能体	交通、酒店、预算和行程顾问协作，衔接平台实时产品
旅行社销售副驾驶	从客户摘要查询线路，比较候选，提示报价条件和跟进动作
行中变更协调智能体	监测天气、交通和供应变化，比较改签/替代方案并通知
旅游评价摘要安全审查智能体	将摘要与原评论对齐，强制保留卫生、治安、伤亡等高风险信息
旅游规划评测智能体	检查预算、路线、时间、人数、偏好和工具轨迹并比较方案

3. 景区、目的地与会展

AI 智能体	主要任务与动作
景区游客服务与现场任务智能体	回答票务演出，结合客流天气推荐路线并创建服务/救援任务
目的地运营智能体	汇聚搜索、客流、活动、消费和舆情，生成运营任务
会展销售研究智能体	研究目标企业、生成需求假设和触达草案，人工跟进后回写 CRM
会展项目协调智能体	维护展商、议程、展位、物料和现场问题状态

四、重点智能体工作卡

1. 旅行规划与预订智能体

字段	内容
服务对象	游客、旅行顾问、OTA 客服
触发条件	用户提出跨交通、住宿、景点和预算的开放需求
输入	日期、出发地、人数、预算、偏好、特殊需求和实时产品
判断与规划	拆解子任务，调用实时工具，检查路线、营业、预算和预订冲突
系统与工具	机酒门票库存、地图 POI、天气、交通、价格、交易和订单
输出与动作	可执行行程、预算、来源、产品候选和预订草案
人工控制点	用户确认价格、退改和付款；重大冲突、健康与安全转人工
验收	事实正确、可预订率、路线可行、预算偏差、任务完成和失败恢复

2. 酒店客诉分级与授权处置智能体

字段	内容
服务对象	前台、值班经理、客服、运营、法务
触发条件	卫生、设施、服务、财物或安全投诉
输入	对话、订单会员、现场证据、授权额度、SOP 和历史记录
判断与规划	提取事实与诉求，按风险和影响分级，匹配止血与升级路径
系统与工具	PMS、CRM、工单、照片/监控、授权表、舆情与法务系统
输出与动作	处置建议、责任人、时限、升级、客户沟通草案和复盘
人工控制点	不自动判责、赔付、删帖或起诉；高风险立即交值班经理
验收	首次响应、现场闭环、升级漏失、重复来电、补救成本和满意度

3. 酒店售后问答与人工升级助手

字段	内容
服务对象	OTA 售后、酒店客服、宾客
触发条件	入住前后咨询、退款进度、发票、取消和订单问题
输入	用户问题、订单上下文、FAQ、会话历史与业务状态
判断与规划	识别意图，检索排序，判断能否自助、是否低置信或用户不满意
系统与工具	订单、售后、FAQ、客服工单和会话系统
输出与动作	答案、自助入口、置信度、转人工摘要和会话回写
人工控制点	规则外退款、入住失败、卫生安全和持续不满必须转人工
验收	召回排序、端到端解决、错误自助、转人工漏失、延迟与上下文完整

五、代表案例与图片

案例一：华住——从对话进入酒店工单和物理执行

公开材料描述宾客表达需求后，系统完成多意图识别、场景切换、MCP 对接酒店系统、生成工单并调用机器人送物。它具备真实工具调用和物理执行，但首字响应和回复准确率仍是厂商案例口径；错房、重复工单与机器人失败恢复应单独验收。

案例二：亚朵后厨——标准比生成更重要

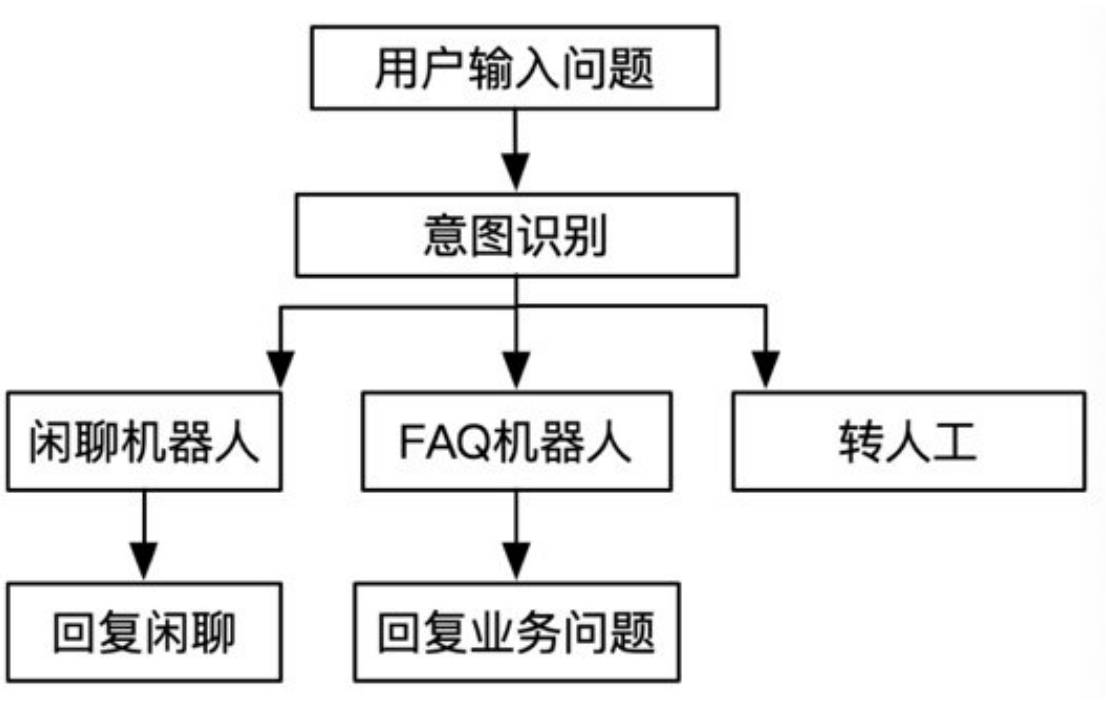
亚朵案例把语音/图片/NFC 输入、食材标准、效期计算、标签打印、临期预警和一线纠错连成短闭环。AI 负责理解非标输入，确定性规则负责效期，人员负责异常处置。



图：亚朵酒店后厨案例

案例三：去哪儿酒店售后问答——旧技术仍提供重要工程经验

技术实践覆盖意图识别、FAQ 召回与排序、多轮会话、可自助操作和人工转接。其数据来自 2020 年前后场景，不能代表当前大模型能力，却清楚说明客服不能只追求命中率，还要测转人工漏失和端到端解决。



图：酒店售后问答技术实践

案例四：旅游开放任务评测——没有唯一答案，也必须可检验

Open-Travel 与 ArenaRL 行业资料把预算、时间、人数、偏好、路线和工具调用纳入相对评测。它提醒企业：行程“看起来合理”不够，还要逐项检查硬约束和事实来源。

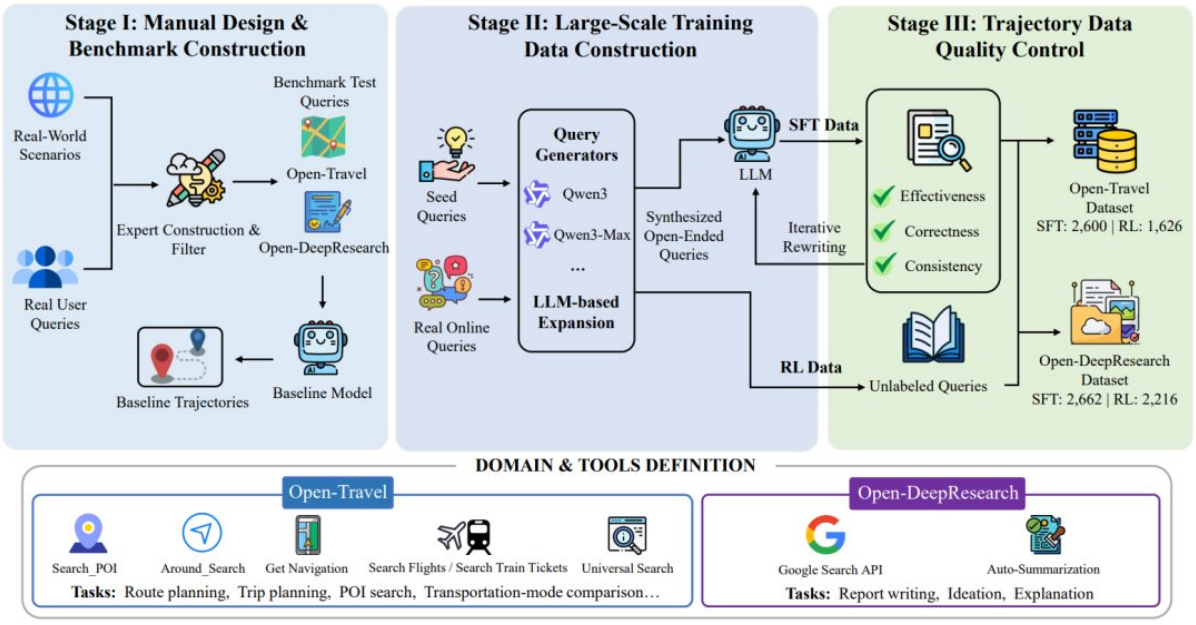


Figure 3: The construction process of Open-Travel and Open-DeepResearch benchmarks.

图：旅游开放任务评测材料

六、系统、数据、权限与安全

酒店侧连接 PMS、CRS、会员、房态房价、工单、餐饮库存、设备和机器人；旅行侧连接产品主数据、库存价格、订单、CRM、供应商、合同和退改；景区连接票务、地图、客流、设施、投诉和应急；会展连接 CRM、展商观众、展位、议程、证件和现场工单。

动态价格、库存、交通、天气和营业信息必须调用实时源。知识条目带状态、适用日期、门店/地区与负责人。一线纠错进入审核队列，不能直接修改正式 SOP。

支付、预订、改签、退款、升级房型、折扣、赔付、合同和高价值承诺分级授权；特殊健康需求、未成年人、公共安全、医疗救援和重大舆情快速转人工。酒店网关、机器人和第三方应用采用最小权限、密钥轮换、审计和隔离。

七、落地路线

- 建立客服、客诉、住中工单、行程规划和预订的人工基线；
- 先上线知识检索、客户摘要、行程草案和评价安全审查；
- 再连接实时库存价格与只读订单查询；
- 开放自动建工单、送审和低风险自助事项；
- 支付、变更、补偿和现场设备动作保持明确确认与回查；
- 经过历史回放、影子模式和单酒店/单线路试点后扩展；
- 对事故、断网、机器人失败、接口限流和价格跳变进行故障演练。

八、评测与验收

场景	任务质量	业务结果	风险与闭环
旅行规划	约束、事实来源、路线和预算	采纳、可预订、任务完成	幻觉、支付确认、取消和中断
住中服务	意图、房间、知识和工单字段	首响、一次解决、完成和满意度	错房错物、隐私、机器人失败
售后问答	召回排序、自助正确、转接摘要	解决率、处理时长、重复咨询	高风险漏转、过期规则、人工接管
客诉	风险分级、授权匹配、证据完整	现场闭环、重复来电、补救成本	错误判责、舆情升级、申诉
收益管理	预测、约束、建议可解释	RevPAR、ADR、入住与渠道成本增量	价格异常、公平性、回滚
景区服务	票务演出点位、多语种和路线	分流、等待、投诉和满意度	限流/安全错误、紧急升级
会展协同	线索、议程、物料和状态准确	到场、匹配会议、问题关闭、续约	错发、数据泄露、资源冲突

九、风险边界

- 行程和摘要会产生幻觉或粉饰，重大负面事实必须优先保留；
- 实时库存、价格、营业和交通变化会让正确答案迅速失效；

- 酒店系统接口可能产生越权、房客信息泄露和诈骗；
- 推荐与收益管理需处理利益披露、公平性和消费者知情；

十、案例与来源索引

核心来源

- 亚朵酒店后厨管理
- 旅行社 AI 销售助手与客服
- 腾讯文档 AI 旅行搭子
- 酒店售后智能问答实践
- 可信旅游 AI 应用
- 酒店客诉分级案例
- 酒店智能应用网关越权风险
- ArenaRL 开放域智能体评测
- Tripadvisor AI 摘要事件

本章小结

旅游与酒店智能体的分水岭，是能否从“生成灵感”进入实时事实、交易确认和现场履约。企业应把行程、房态、客诉和工单当作状态系统，而不是一次回答；把安全、隐私和人工接管当作产品能力，而不是上线后的补丁。只有用户真的订得到、住得上、办得成、出了问题有人接管，智能体才真正服务了旅行。

第十章 科技、互联网与软件服务：AI 智能体进入研发、运维、安全与客户成功

科技、互联网与软件服务行业的 AI 智能体，已经进入需求、编码、测试、发布、运维、安全、客服和客户成功等核心生产链。

本章核心结论

科技与软件行业是 AI 智能体最早进入生产工具的行业，但“代码生成比例”不等于交付价值。真正决定结果的是需求是否被理解、改动是否落在正确位置、测试是否覆盖风险、发布是否受控、故障是否能恢复、客户问题是否回到产品和研发。

目前已经出现测试智能体、仓库级编码智能体、客服分析预警和安全调查智能体，并覆盖遗留 AB 实验下线、Switch 开关治理、客服问题到轻量需求规格、自适应测试多智能体、代码审查编排，以及安全运营就绪度与动作分级。最可靠的研发智能体会受到仓库、规范、测试、发布和代码所有者的共同约束，不会自由写代码。

当前应用主要集中在研发与测试；SaaS 实施、客户成功、云成本、GPU 调度和生产级可观测闭环仍有较大拓展空间。

一、行业边界

1. 互联网平台

核心是用户、内容或交易供给、匹配推荐、客服争议、风险治理和增长。平台业务中的电商、广告和出行履约可与对应行业交叉，但平台治理仍属本章。

2. SaaS 与企业软件

不仅包含产品研发，还包括实施迁移、培训上线、支持、客户成功、续费扩容和生态集成。

3. 软件开发与 DevOps

既是本行业核心链，也是跨行业共同职能。本章聚焦智能体如何参与需求、编码、审查、测试、发布、运维和复盘。

4. 云服务与 AI 基础设施

围绕容量、资源供给、SLA、故障、成本、计费与安全。自动扩缩容和调度多为控制器/优化器，不自动等于智能体。

5. 网络安全

具有独立的资产、检测、调查、响应、恢复和合规链。生产隔离、封禁、删除和规则修改属于高风险动作。

二、核心业务链与逐环节问题

1. 软件研发交付链

客户/业务问题 → 需求澄清 → 产品与架构设计 → 编码 → 代码审查 → 测试 → 构建发布 → 可观测 → 故障响应 → 复盘与知识回流

环节	关键问题	智能体机会	人工控制点
需求	模糊、缺复现、边界和验收不清	追问上下文、生成轻量规格、关联日志和代码	产品、研发、测试确认完成定义
编码	找错文件、忽略架构、循环修改	仓库探索、计划、补丁、测试与修复	分支隔离、代码所有者审查
遗留治理	AB 实验和开关长期堆积	识别引用、依赖和环境差异，生成清理改动	灰度、上线和回滚由责任人批准
代码审查	上下文不足、意见重复、严重度失真	多专业角色并发检查，协调去重与证据定位	不拥有合并权，关键问题回查确定性工具
测试	用例跟不上变更、测试数据和多通道分散	风险生成、用例对抗、数据准备、执行与知识回流	高风险用例、失败归因和缺陷关闭人审
发布	生成代码通过但生产风险未知	发布计划、预检查、灰度监测和回滚建议	生产发布与扩大灰度分级批准
运维	告警风暴、根因跨系统	聚合证据、根因假设、预案和受控执行	配置、重启、扩缩容和回滚授权

2. SaaS 客户生命周期

线索与需求 → 方案演示 → 合同 → 实施迁移 → 配置集成 → 培训上线 → 支持工单 → 客户成功 → 续费扩容 → 产品反馈

智能体可做需求摘要、配置校验、迁移脚本、工单分诊、健康度解释、风险任务和续费材料，但租户数据必须隔离，商业承诺、折扣和续约决策由人负责。当前具名生产尚未形成成熟应用。

3. 云服务与运维链

容量预测 → 资源采购部署 → 调度供给 → 服务监控 → SLA 事件 → 故障处置 → 成本计费 → 安全合规 → 容量反馈

预测模型、调度器和自动扩缩容是工具层；智能体负责理解目标、调用工具、解释方案、协调批准和追踪结果。

4. 安全运营链

资产与暴露面 → 检测告警 → 聚合分级 → 调查取证 → 遏制 → 根除修复 → 恢复 → 复盘 → 规则与情报更新

安全智能体应从只读调查起步，以证据链和动作风险分级控制权限，不能因模型能调用工具就直接开放生产处置。

三、AI 智能体全景

1. 需求、编码与治理

AI 智能体	主要任务与动作
轻量需求规格协作智能体	从客服问题追问复现，关联日志/发布/代码，生成目标、边界与验收
仓库级编码智能体	探索仓库、修改文件、运行命令和测试、根据失败修复
遗留 AB 实验下线智能体	读取实验配置和代码分流，生成推全/下线改动并验证
Switch 开关治理智能体	识别配置、代码引用和环境差异，生成清理补丁与报告
多智能体代码审查编排	安全、性能、逻辑和工程角色并发检查，协调去重

2. 测试、发布与运维

AI 智能体	主要任务与动作
端到端软件测试智能体	探索产品、生成计划和用例、执行、报告并反馈修复
自适应测试多智能体系统	从需求与代码变更生成风险和用例，对抗融合，多通道执行和回流
硬件测试任务智能体	接收任务，调用上位机和云端分析，记录版本与报告
发布协同智能体	生成发布与回滚计划，监测灰度，异常时创建任务
AIOps 调查智能体	关联日志、指标、追踪、配置和变更，给根因与预案
云成本与容量智能体	解释资源浪费，比较扩缩容和购买方案并追踪

3. 客户、平台与安全

AI 智能体	主要任务与动作
客服数据分析与预警助手	对大量对话分类、复盘并发现风险与意向
SaaS 实施配置智能体	读取客户需求、版本和集成约束，生成迁移/配置任务
客户成功智能体	汇聚使用、工单、合同与健康度，触发干预任务
安全调查智能体	跨 SIEM、EDR、防火墙等只读查询，生成时间线和处置建议
安全运营就绪度与权限治理智能体	盘点数据、工具、知识和工作流，评估成熟度并配置动作等级
受控响应智能体	经批准调用 SOAR 隔离、封禁或改规则并验证结果

四、重点智能体工作卡

1. 遗留实验与开关治理智能体

字段	内容
服务对象	产品研发、平台治理、代码所有者和发布人员
触发条件	实验推全/下线、历史开关清理、配置一致性治理
输入	实验/开关清单、线上预发配置、代码、调用链和运行信息
判断与规划	搜索引用与依赖，识别环境差异，生成影响清单和改动计划
系统与工具	实验平台、配置中心、代码库、搜索/依赖工具、CI/CD 和观测
输出与动作	代码补丁、配置建议、构建测试结果、灰度和回滚草案
人工控制点	分支运行、代码所有者审查、发布批准和回滚不可绕过
验收	影响召回、编译/测试、人工修改、线上回退和遗留复发

2. 自适应测试多智能体系统

字段	内容
服务对象	测试、研发、产品与质量负责人
触发条件	需求、代码或配置变更，回归与发布准备
输入	需求、代码差异、配置、历史缺陷、用例、数据与环境
判断与规划	多角色生成与对抗风险/用例，准备数据，选择 UI/API/ 消息/监控通道
系统与工具	需求和代码库、测试平台、数据、环境、缺陷库与知识库
输出与动作	风险点、用例、执行轨迹、缺陷、改进建议与知识条目
人工控制点	高风险用例、失败归因、缺陷有效性和关闭由人确认
验收	用例准确率、漏测、执行成功、逃逸缺陷、人工接管和成本

阶段	经典测试范式	Agentic AI新测试范式
需求分析	通过不断评审对焦，测试同学仔细阅读和理解需求文档。 特点：多轮评审，但依然有部分问题被带到测试用例评审。	通过AI Agent快速解析需求文档，自动提取测试要点。 特点：自动发现对应风险点、待确定点，前置需求评审解决，对需求文档质量有较高要求
用例编写	基于经验手动编写测试用例 特点：人工编写时间长且依赖测试同学专业度，用例不易沉淀	通过AI Agent自动生成测试用例 特点：10min内生成，依赖领域知识库，稳定易沉淀。
测试执行	人工操作执行测试步骤 特点：虽有自动化辅助，但整体偏人工	AI Agent自动化执行测试用例 特点：10min中内并行完成各测试用例执行
结果记录&报告生成	手动记录测试结果、提报缺陷、整理数据生成测试报告 特点：整体偏人工，手工点点点。	AI Agent自动生成分析报告和优化建议 特点：Agent自动生成测试报告
研发时效	全流程一般 2~5天	全流程+人工结果校验约2.5小时

图：自适应测试多智能体材料

3. 安全调查与响应智能体

字段	内容
服务对象	SOC 分析师、事件响应、IT 与业务系统负责人
触发条件	告警聚合、疑似攻击、账号或资产异常
输入	SIEM、EDR、身份、网络、邮件、资产、情报和历史事件
判断与规划	建立实体和时间线，生成假设，调用只读工具验证并评估影响
系统与工具	SIEM/EDR/NDR、防火墙、IAM、威胁情报、SOAR 和工单
输出与动作	证据链、严重度、处置建议、审批任务和复盘材料
人工控制点	隔离、禁用、删除、改规则和公开漏洞按风险等级审批
验收	证据完整、严重度校准、MTTD/MTTR、误操作、接管和审计

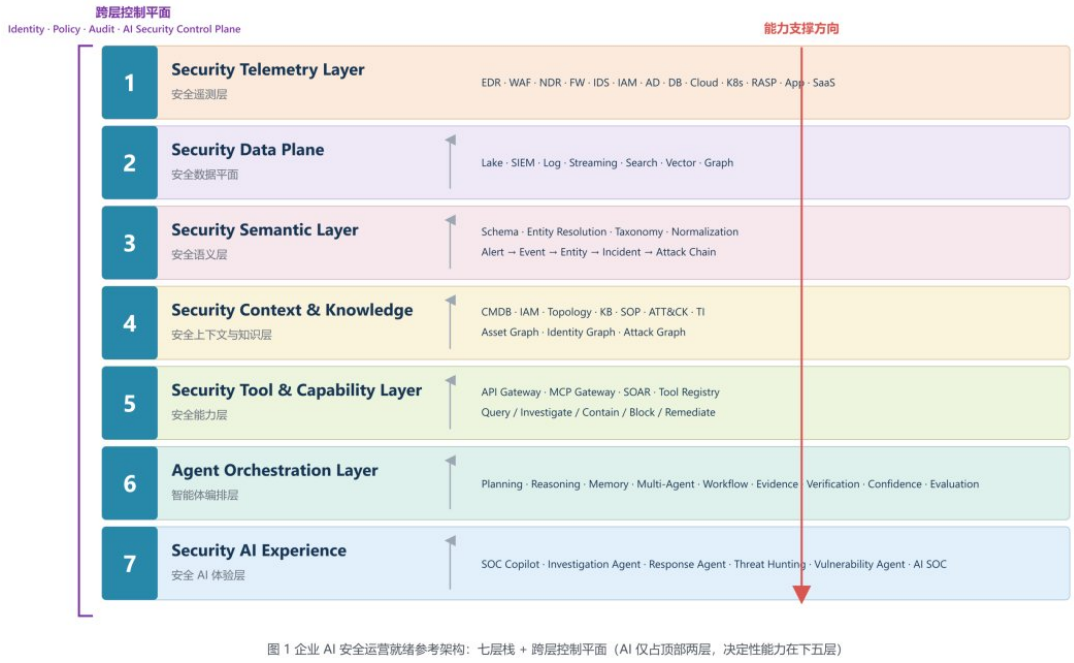


图 1 企业 AI 安全运营就绪参考架构：七层栈 + 跨层控制平面（AI 仅占顶部两层，决定性能力在下五层）

图：安全运营就绪度架构材料

五、代表案例与图片

案例一：大淘宝遗留 AB 实验治理——窄任务比通用写代码更易验收

技术团队把场景限制为实验推全与下线，接入实验配置、代码搜索、构建和测试，并通过坏例持续调整工作流。项目公开信息显示，任务成功率由不足 50% 提升至 92%。这类场景适合从高频、边界明确、验证链完整的任务开始。

案例二：淘工厂自适应测试——测试不是生成用例清单

系统把需求理解、代码配置、风险与用例对抗、数据准备、UI/API/ 消息/监控执行、结果核对和知识回流串成多角色闭环。验收应看漏测、执行成功、生产逃逸与人工接管，而非只看生成了多少用例。

案例三：客服问题到研发——智能体先修复信息流

团队实践把客服问题转为可复现信息和轻量需求规格，再进入编码、验收和知识沉淀。它提示企业：研发提效不只发生在 IDE，需求边界、日志、发布和验收同步往往更重要。

案例四：TestSprite——从生成测试到操作产品和反馈修复

测试智能体可以探索网站、生成计划与用例、执行测试并输出报告，也可通过 MCP 与编码工具形成修复循环。企业验收应以自身项目的缺陷发现率、生产逃逸、交付周期和人工投入为准。

六、系统、数据、权限与工程可靠性

统一需求、代码、提交、测试、构建、发布、告警、事件、工单和客户标识；补齐架构决策、依赖版本、历史事故和业务约束。日志、指标和追踪使用统一时间、服务、版本和 Trace ID。

查询与写入、分支与主干、测试与生产分别授权。代码改动必须经过分支保护、代码所有者、CI、扫描、灰度和回滚。外部 Issue、网页、工单、日志字段和工具返回均视为不可信输入，防止提示注入和密钥泄露。

运维与安全动作需具备幂等、超时、重试、状态回查、补偿与审计。核心数据库、身份权限、生产网络和安全控制面不允许模型单点决定。

七、落地路线

- 选择一个边界清楚、历史样本充足、可自动验证的任务；
- 在离线仓库或历史事件上回放，建立隐藏测试和失败分类；
- 只读分析与建议先进入影子模式；
- 开放分支写入、自动测试和报告，不开放合并与生产发布；
- 通过代码所有者、CI 和灰度后开放低风险白名单动作；
- 对生产故障和安全响应逐级从调查、建议、测试环境执行到有限生产动作；
- 持续保存失败、人工否决和回滚样本，避免只学习成功案例。

八、评测与验收

场景	任务质量	业务结果	安全与闭环
需求规格	复现信息、边界、验收完整	返工、交付周期、跨角色等待	错分类、敏感数据、人工确认
编码	隐藏测试、正确文件定位、一次修复	交付周期、返工、缺陷逃逸	越权写入、密钥泄露、回滚
代码审查	有效发现、严重漏报、重复意见	评审时长、线上缺陷	误阻断、证据、最终合并责任
测试	风险覆盖、用例有效、缺陷复现	回归周期、发布频率、逃逸缺陷	环境隔离、数据泄露、误改生产为 0
发布运维	异常识别、根因 Top-N、预案可行	失败率、MTTR、SLA 和成本	未批准发布为 0、状态回查与补偿
安全响应	证据完整、严重度、攻击链还原	MTTD、MTTR、重复事件	错误隔离、证据破坏、审计
客户成功	数据口径、风险解释、任务路由	上线、活跃、续费、扩容	租户隔离、错误商业承诺

九、风险边界

- 代码可运行不代表满足业务目标或架构约束；
- 智能体可能被仓库文件、Issue 或日志中的提示注入诱导；
- 自动测试会制造虚假覆盖，评测必须包含隐藏测试和生产逃逸；
- 安全智能体误隔离、删证据或改规则可能扩大事故；
- AI 生成代码比例不是交付效率、质量或商业价值；

十、案例与来源索引

核心来源

- 腾讯 WorkBuddy Bench
- 迈金科技测试自动化
- 爱回收客服分析与预警
- 企业 AI 安全运营就绪度参考架构
- 高准确率 AI Coding 工作流
- AI 团队全链路研发协作
- 淘工厂自适应测试系统
- AI 代码审查与智能体开发工具

本章小结

科技与软件行业的智能体化，需要重构从问题、代码、测试到发布和反馈的证据链，不能简化为把程序员换成一个聊天窗口。越接近生产、客户数据和安全控制面，越需要确定性工具、最小权限、人工签审和可回滚机制。能够在受控环境里做对事、证明做对了、失败时停下来，才是企业研发智能体的成熟标志。

第十一章 电信：从网络规划、故障诊断到客户服务与政企交付

电信行业的 AI 智能体已经进入网络规划、工程资料、故障诊断、客户服务、政企交付和安全治理；生产网络操作仍需严格受控。

本章核心结论

电信是最需要 AI 智能体、也最不能允许模型自由行动的行业之一。网络告警、拓扑、配置、变更、客户影响和故障知识跨多个专业域，适合智能体持续查询、建立证据、提出根因和协调任务；但网元配置、路由切换、重启和重大故障处置必须经过受控编排、变更审批、灰度、验证和回滚。

当前应用主要集中在客服坐席辅助、政企交付和行业治理，并已覆盖无线流量预测、Auto-RCA 基站故障诊断、通信工程图纸重构、中国联通“通通”多意图客服，以及运营商跨行业数据与智慧城市交付。公众网络生产闭环、计费和欺诈治理仍有较大拓展空间。

当前最值得优先落地的是只读网络调查、客服查询与工单、工程资料数字化和政企方案辅助；生产网络自动处置、费用调整和欺诈阻断应后置。

一、行业边界

1. 公众通信网络

覆盖无线、核心、传输、承载、接入、站点及资源的规划、建设、开通、运维、优化和退网。

2. 客户经营与 BSS

覆盖个人、家庭和中小企业的咨询、账单、套餐、故障、工单、投诉、订购、开通、计费、变更与退订。

3. 政企客户交付

覆盖行业研究、需求诊断、云网算力方案、投标合同、实施适配、测试验收、SLA 和续约复制。客户最终使用的医疗、制造或政务智能体应归客户行业；运营商保留交付能力。

4. 欺诈与收入保障

覆盖实名、SIM、设备、渠道、通联、支付、异常用量、调查处置和申诉。银行反欺诈不能替代电信欺诈证据。

5. 相邻对象

通信设备企业自身研发制造归制造业；通用企业 IT 运维不等于通信网络运维；GPU/RDMA 智算网络不等于公众无线或核心网；预测、图纸识别、告警聚类和 RPA 是智能体工具层。

二、核心业务链与逐环节问题

1. 网络规划建设链

覆盖与市场需求 → 流量容量预测 → 频谱/站址/路由规划 → 投资立项 → 工程设计采购 → 施工集成 → 开通优化 → 验收 → 扩容改造退网

环节	关键问题	智能体机会	人工控制点
流量容量	时间跨度和新区域缺历史数据	预测模型、方案比较与不确定性解释	预测不直接决定投资或节能参数
站址规划	GIS、覆盖、频谱、投诉和成本约束多	调用仿真与优化，生成候选和评审材料	无线规划专家和投资审批
工程图纸	纸/PDF 存量大、物料和几何难统计	视觉识别、人工纠错、矢量化和 CAD 重构	纠错后才能进入工程使用
开通验收	配置、资源、测试和文档不一致	前置校验、缺项清单、测试证据汇总	生产配置和验收签字由授权人完成

2. 网络运行维护链

多域监控 → 告警去重关联 → 业务影响 → 根因定位 → 预案 → 变更审批 → 受控执行 → 服务验证 → 复盘知识 → 容量性能能耗优化

环节	关键问题	智能体机会	人工控制点
告警风暴	多域、重复、顺序和拓扑关系复杂	事件聚合、拓扑关联和影响分析	保留原始告警与证据，不自动丢弃重大信号
根因定位	需跨告警、拓扑、配置、变更与历史案例	根因假设、验证查询、坏例迭代	工程师确认根因与处置
预案与执行	建议可能不适用当前网元和版本	生成预案、调用受控编排、验证 KPI	白名单、变更审批、灰度、回滚
优化节能	覆盖、容量、能耗和体验互相约束	调用预测/优化，比较方案和复盘	不以节能牺牲服务质量和应急能力

3. 客服、产品与计费链

客户认证 → 多意图咨询 → 账单/套餐/网络状态查询 → 诊断与办理 → 工单投诉 → 质检/VOC → 续约流失 → 推荐 → 客户确认 → 结果回查

环节	关键问题	智能体机会	人工控制点
坐席服务	一通电话频繁跨系统复制	转写、意图、知识、画像、查询、填单与摘要	坐席保留对话和办理责任
自助办理	多问题并发、资费规则复杂	分解意图，调用查询/办理工具，多模态答复	身份、费用、套餐和合约关键字段确认
账单争议	用量、资费版本、订购关系难追溯	证据汇集、规则解释和调查摘要	退款、冲正和计费修改人审
套餐顾问	推荐易忽略合约和总成本	比较真实用量、资格和总成本	客户同意，可撤销和投诉

4. 政企交付与欺诈链

政企链为客户研究 → 需求诊断 → 云网算力/AI 方案 → 成本报价 → 合同 → 实施适配 → 测试验收 → SLA → 续约复制。欺诈链为准入 → 行为监测 → 异常模型 → 关系证据 → 调查 → 人工处置 → 申诉恢复 → 规则更新。

三、AI 智能体全景

1. 网络规划建设

AI 智能体或能力	主要任务与动作
网络规划协同智能体	读取覆盖、流量、GIS、站点与投资约束，调用仿真并生成方案
无线流量预测与规划助手	预测短期、长期和无历史区域流量，支持选址、资源和节能方案
通信工程图纸识别重构系统	识别设备、物料、线路和标注，经人工纠错生成 CAD
工程资料预审智能体	检查设计、物料、配置和验收证据一致性

2. 网络运行维护

AI 智能体	主要任务与动作
多域告警与业务影响智能体	告警去重、拓扑关联，解释受影响区域、客户和业务
Auto-RCA 根因诊断智能体	关联告警、拓扑和故障知识，输出根因排序并用坏例自改进
故障协同智能体	建立事件上下文，生成验证步骤、协调专业人员和记录状态
网络变更与自愈执行智能体	在白名单和批准预案内调用编排器，验证并回滚
容量性能与能源优化智能体	调用预测和优化器，比较服务、成本与能耗方案

3. 客户、产品与计费

AI 智能体	主要任务与动作
客服坐席副驾	ASR 转写、意图情绪、知识检索、跨系统查询、填单和摘要
“通通”多意图客户服务智能体	一次对话分解多个问题，查询话费流量、办理业务并连续服务
自助服务事项智能体	认证、诊断、查询、建单、变更和结果确认
套餐与权益顾问智能体	比较用量、合约、终端和优惠，解释总成本并生成办理草案
计费争议调查智能体	追溯用量、资费版本、促销与调整项，生成证据

4. 政企与风控

AI 智能体或能力	主要任务与动作
政企售前与 FDE 交付智能体	需求诊断、方案组件、资源成本、实施计划和验收条目
通信—汽车联邦推荐系统	数据不出域建模，生成推荐、洞察和反欺诈线索
智慧城市视觉与算力调度能力	识别视频事件、分配算力、输出治理线索
电信欺诈调查智能体	聚合 SIM、设备、账户、渠道、通联和支付证据，规划调查
模型安全治理智能体	模型准入、风险测试、权限和审计

四、重点智能体工作卡

1. Auto-RCA 网络告警根因诊断智能体

字段	内容
服务对象	NOC、无线网优、设备与故障响应人员
触发条件	基站告警风暴、重复故障或根因不清
输入	告警、拓扑、配置、变更、故障知识和已标注案例
判断与规划	关联时序和拓扑，生成根因候选，评估坏例并迭代诊断逻辑
系统与工具	网管告警、拓扑/知识图谱、配置变更、案例库和评测版本库
输出与动作	根因排序、证据链、坏例分类和工程师核查任务
人工控制点	工程师确认；修复、切换和重启另行授权
验收	Top-N 根因、误导率、诊断时间、跨故障泛化和人工否决

2. 多意图客户服务智能体

字段	内容
服务对象	个人、家庭和中小企业客户，客服运营团队
触发条件	客户查询话费流量、咨询套餐或请求办理多个事项
输入	文字/图片、身份、产品、账单、网络状态和会话历史
判断与规划	分解多意图，选择查询或办理工具，生成文字/图片/卡片答复
系统与工具	CRM、计费、产品目录、订单、办理、认证、知识库和风控
输出与动作	多问多答、查询结果、办理确认、下一步建议和转人工摘要
人工控制点	强身份认证；费用、合约、停复机和敏感业务明确确认
验收	意图遗漏、查询正确、错办、幂等、结果回查、撤销和用户成功

3. 通信工程图纸识别与重构系统

字段	内容
服务对象	通信设计院、规划、工程和资产管理人员
触发条件	存量纸质或 PDF 图纸数字化、工程统计和改造
输入	扫描图/PDF、图例、设备物料规则和历史图档
判断与规划	识别线路、设备、文字和几何关系，关联物料
系统与工具	视觉/OCR、图例物料库、人工纠错界面、CAD 和图档系统
输出与动作	对象清单、矢量数据、物料表和可编辑 CAD
人工控制点	人工增删改和工程复核后才能用于设计、预算和施工
验收	分类别精度、人工修改量、几何物料一致和 CAD 可编辑性

五、代表案例

案例一：Auto-RCA——真实故障数据让根因诊断可被测量

材料基于中兴通讯与中国移动研究的公开研究，涉及真实基站故障场景，并通过评估、坏例分析、推理/代码和数据清理持续迭代。其价值是把“会解释告警”推进到可评测根因排序；但高指标不意味着可以自动修复网络。

案例二：中国联通“通通”——客服从单问答走向多事项

公开案例描述话费/流量查询、业务办理、多意图并行、多轮记忆和多模态输出。生产验收要把查询和办理分开，特别关注身份认证、错办、重复提交、结果回查和投诉撤销。

案例三：中国移动客服助手——部件组合不应被一个名称掩盖

一线实践将 RPA、ASR、语义分析、知识关联、画像、自动填派单、投诉提醒和质检组合起来，公开称每通节省一定时间。它说明坐席副驾的价值，也提醒企业分别验收转写、查询、填单和人工决策。

案例四：无线流量预测——模型服务规划，不代替规划责任

UoMo 公开研究覆盖短期、长期和无历史区域预测，可支持基站选址、资源分配和休眠节能。它本质是预测模型与优化器，只有进入方案、审批和反馈链后，才成为规划智能体的能力部件。

六、系统、数据、权限与组织

网络资源、网元、端口、链路、业务、客户和拓扑需要统一标识、版本和时间有效性；告警、性能、配置、变更、工单、投诉与客户影响关联同一事件。资费、产品、优惠、合约和计费规则保留地域、渠道和生效期。

网络侧连接 OSS、EMS/NMS、SDN/NFV 编排、拓扑、配置、变更、性能、告警、工单、GIS 和仿真；客服侧连接 CRM、计费、产品目录、订单、认证和诊断；政企侧连接商机、报价、合同、项目、云网资源、模型平台和 SLA；风控侧连接 SIM、设备、渠道、通联、位置、支付、案件和申诉。

网元配置、路由、切换和重启只能通过受控编排器，必须预检查、变更审批、灰度、回滚和业务验证。欺诈限制、黑名单和费用调整保留人工裁决及申诉恢复。重大故障由人工指挥，智能体只做辅助。

七、落地路线

- 建立告警、定位、修复、客服和计费的人工基线；
- 用历史故障和账单构建固定测试集，离线回放；
- 先开放知识、摘要、根因建议和工程资料识别；
- 进入影子模式，对比工程师判断，不写生产系统；
- 开放自动建单、只读查询和测试网执行；
- 低风险动作通过白名单编排、小范围灰度和回滚验证；

- 生产规模化前完成峰值告警、状态冲突、工具失败和重大故障演练；
- 计费、欺诈和客户办理单独建立授权、纠错与申诉机制。

八、评测与验收

场景	任务质量	业务结果	安全与闭环
网络规划	约束识别、引用、方案可行、仿真通过	迭代、返工、投资偏差	不自动立项采购或下配置
告警影响	压缩准确、拓扑关联、影响识别	有效告警、首次定位	重大告警漏失、证据保留
根因诊断	Top-N 命中、误导率、证据	定位时间、MTTR、重复故障	工程师确认、修复另授权
网络执行	预检查、动作成功、业务验证	恢复时间、SLA	未批准动作 0、回滚和审计
客服办理	意图、答案、字段、转人工	一次解决、时长、投诉	身份、错办、撤销、隐私
计费争议	规则版本、账单解释、证据	调查周期、重复咨询	冲正退款人审、可申诉
政企交付	需求遗漏、方案复用、验收条目	周期、一次通过、SLA	不承诺未经验证效果
欺诈调查	召回误报、证据、关系还原	每案时间、损失与恢复	误伤、时限、申诉和漂移

九、风险边界

- 网络拓扑、配置和知识快速变化，过期依据可能造成错误处置；
- 大语言模型不具备通信协议和安全控制的确定性，不能直接下网元命令；
- 客服多意图和套餐办理涉及身份、资费、合约与消费者权益；
- 跨行业联邦模型仍可能有成员、梯度和用途泄露风险；
- Auto-RCA 论文指标、联通公开案例和跨行业效益需确认样本、范围和口径。

十、案例与来源索引

核心来源

- AI 客服助手在电话客服中的应用
- 中国电信 AI 治理实践
- 运营商 FDE 团队
- MWC 2026 AI 企业应用趋势
- UoMo 无线网络流量预测
- Auto-RCA 电信网络故障诊断
- 通信行业工程图纸智能识别与重构

- 中国联通“通通”智能体
- 天津联通智慧城市应用

本章小结

成熟的电信智能体能够在复杂拓扑和严格权限中找到证据、协调专业域、提出可验证方案，并把所有生产动作交给受控编排和责任人。客服同样不能只看应答率，而要确认事项办对、账单说清、结果可撤销。高可靠网络需要智能体，但更需要人类指挥、确定性控制和审计边界。

第十二章 媒体、营销、游戏与文娱：从内容生成走向资产、投放与运营闭环

研究截止：2026 年 9 月 3 日。本章把“会生成”与“能交付”分开：生成文字、画面或音频，不等于已经进入策划、权利、审核、发行、投放和结算。

本章核心结论

- 当前较成熟的应用集中在素材检索、批量初稿、多工具制作、版本审片、翻译审校、投放盯盘和项目协同。
- 两条业务链尤其关键：广告制作要保留洞察、创意、审美、真实性和版权责任；投放智能体要受预算、阈值、账户权限和结果回查约束。
- 山海星辰短剧案例展示了 IP 评估、剧本、制作、翻译、审核、投流和 PMO 的完整业务链。多智能体是否能够稳定协作，应通过任务成功率、返工率、交付周期、投放结果和异常接管进行验收。
- 游戏 NPC、AI 短剧工作台和小团队创作正在形成新的生产方式，规模化应用仍需经过项目运行与业务验收。

一、行业边界

子行业	核心产出	不能混淆的责任
新闻出版与知识内容	可核验的公共信息和内容产品	事实核查、主编责任、更正与档案
广告营销与创意制作	策略、创意、物料、投放和归因	多客户隔离、品牌安全、媒介账户和预算
影视、短剧与流媒体	可发行内容和 IP 资产	版权、角色连续性、主创审批和平台审核
游戏研发、发行与运营	可运行软件和长期在线服务	引擎、性能、版本、反作弊和未成年人保护
音乐、艺人和现场演出	作品、授权、现场履约与分账	词曲/录音/表演者权利、票务和公共安全

甲方企业内部的营销案例可以证明能力可复用，但不能自动作为广告代理机构的主营业务案例。推荐、竞价、生成模型和内容分类器默认是 AI 能力部件；只有进入任务状态、工具调用、审核、异常恢复与交付链，才更接近 AI 智能体。

二、核心业务链

洞察/选题 → 策略与创意 → 内容和资产生产 → 事实、品牌、版权与合规审核 → 发布、发行或投放 → 互动与在线运营 → 商业化/结算 → 效果复盘 → 内容与 IP 资产回流

游戏还包含“策划—开发—引擎集成—构建测试—版本上线—长期服务”；音乐演出还包含“权利—场次—票务—现场安全—分账”。

三、逐环节业务流程与问题

环节	参与角色与输入输出	典型问题	智能体切入点
洞察与选题	编辑、策略、IP 负责人读取平台、受众、竞品和权利数据，形成候选方向	来源分散、热度替代价值、版权状态不清	可追溯研究、选题比较、补证任务
策略与创意	策略、编剧、导演、创意与客户把 brief 变成脚本/分镜	目标模糊、多方反复、模型输出同质	约束澄清、版本比较；不接管核心创意
内容与资产生产	制片、美术、剪辑、技术美术、本地化交付可审片/可测试版本	多工具切换、人设漂移、版本断链	生成、修复、增强、任务和资产编排
审核	主编、品牌、法务、客户和平台复核原始素材、规则和授权	规则变化、证据断链、误杀漏检	事实、红灯区、版权和平台规则预审
投放与发行	媒介、增长、发行人员管理账户、预算、素材和渠道	多账户、夜间异常、归因偏差、超预算	监控、报告、预警和受限止损
互动与运营	社区、客服、游戏运营读取用户行为、世界状态和工单	海量对话、人设破坏、滥用、延迟成本	NPC 受限行为、工单分诊、异常升级
商业化与复盘	财务、版权、客户成功汇总投放、付费、票务和版税	权利口径复杂、增量难归因	证据归集、差异解释和人工结算待办

四、AI 智能体全景

智能体或能力形态	位置	边界
多模态素材检索与采编助手	素材—编辑	必须带时间码和来源，不自动发布
短剧 IP、剧本、制作、翻译、审核、投流和 PMO 智能体组	短剧全链	命名对象不等于高自治协同
广告创意制作编排智能体	策略—审片	核心洞察、创意、审美和客户定稿归人
广告 AI 红灯区审查助手	品牌治理	预审不替代品牌和法务判断
多账户投放监控与止损智能体	投放运营	预算、阈值和写权限预配置
营销物料 1→N 加工智能体	内容运营	适合作为试点方向
AI 短剧数字制片工作台	剧本—成片	成效需通过客户业务结果验收
游戏资产生成与引擎验证助手	游戏研发	原型可用不等于正式资产合格
游戏 NPC 对话—行为智能体	游戏互动	限制可见状态、动作、成本与安全
游戏运营预测与结算工作流	供需/结算	预测加规则自动化不当然是完整智能体
音乐版权与演出履约智能体	授权/现场	版权、安全和资金动作必须人工批准

五、重点智能体工作卡

1. 广告创意制作编排智能体

字段	内容
服务对象	策略、创意、导演、美术、后期和客户团队
触发条件	brief 与核心创意经人工确认后进入制作
主要输入	brief、分镜、品牌/产品资产、渠道规格、授权状态
判断与规划	选择生成、修复和增强工具，拆分镜头与版本，识别待审项
工具与系统	数字资产库、多模型工具、项目/版本管理、在线审片
输出与动作	候选镜头、可审片版本、修改记录和素材来源卡
人工控制点	创意、审美、真实性、版权和客户定稿
验收指标	brief 一致、可用镜头率、修改轮次、交付周期、品牌偏差、权利溯源

2. 多账户投放监控与止损智能体

字段	内容
服务对象	媒介优化师、广告主和客户负责人
触发条件	消耗、转化、频控或成本达到预设阈值
主要输入	账户、预算、消耗、曝光/点击/转化、归因与止损规则
判断与规划	区分正常波动与异常，选择提醒、停投、重启或升级
工具与系统	媒体 API、多账户平台、归因仓库、规则引擎和审计日志
输出与动作	总览、报告、预警、受限停投/重启和复盘证据
人工控制点	预算、阈值、账户写权、高消耗活动和策略改动
验收指标	异常召回、误停、超预算、状态回查、恢复时间和真实增量

3. 短剧数字制片智能体

字段	内容
服务对象	编剧、制片、导演、美术、剪辑和审核
主要输入	剧本、分镜、角色/场景/风格资产、任务与成本约束
工具与系统	剧本/分镜画布、资产库、生成模型、任务、版本和审片
输出与动作	分镜、镜头、任务状态、版本和审片意见闭环
人工控制点	IP/ 肖像/声音授权、主创决策、平台审核与发行
验收指标	角色连续性、资产齐套、版本溯源、返工、平台通过和成本

4. 游戏 NPC 对话—行为智能体

字段	内容
服务对象	玩家、叙事/策划、客户端、服务端和安全团队
主要输入	人格、世界知识、玩家行为、受限世界状态和记忆
判断与规划	检索知识、保持角色，从动作白名单中选择对话或行为
工具与系统	RAG/ 记忆、行为树、游戏引擎、语音动画、安全与评测
输出与动作	对话、表情、语音和受限游戏动作
人工控制点	世界观、敏感内容、动作权、成本、灰度和紧急关闭
验收指标	人设与记忆正确、越权动作、安全、延迟、成本和长对话退化

六、代表案例

案例一：山海星辰短剧全链路

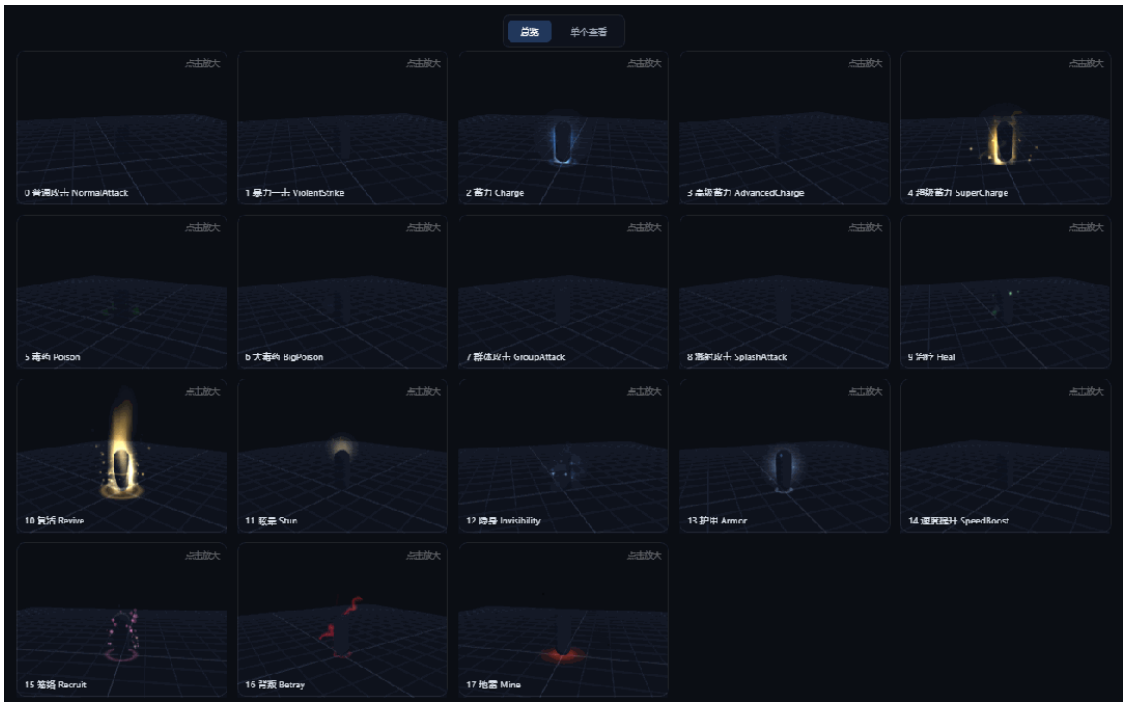
联合案例公开了 IP 评估、剧本、制作、翻译、审核、投流和 PMO 七类对象，证明短剧是一条项目链而非一次生成。但工具权限、任务间动态协商、失败恢复和最终放行人没有被完整披露；相关产能和收益均按案例公开口径理解。

案例二：广告公司访谈

F5、BU 蓝昊和耀火的访谈共同指出：策略和核心创意仍由人负责，AI 适合进入分镜、生成、修复、增强和版本制作。公益、真实受助者、产品功能实证等红灯区，不宜让生成内容替代真实证据。

案例三：游戏美术工作流

行业实践展示 UI 图层拆分、技能特效、白模、Shader、动作生成和引擎导入自检。它能证明“生成—验证—报错”可组成工具工作流，但正式资产仍需通过美术、性能、版本、兼容和版权验收。



图：游戏美术工作流原始配图

七、系统、数据与权限

层	必要能力	治理要求
资产与数据	原始素材、时间码、角色/品牌卡、授权、投放与互动数据	客户/项目隔离；素材来源、肖像和声音授权可追溯
知识与规则	编辑/品牌规范、平台规则、世界观、术语和版权规则	标注版本、地域、有效期与责任人
生产工具	生成模型、数字资产库、引擎、任务与审片	只读获授权资产；登记外部模型留存/训练条款
发布与商业系统	CMS、投放账户、应用商店、票务、版税和结算	默认只读；发布、预算、结算和下架分级审批
运行治理	状态、超时、重试、幂等、回滚、日志和成本	可暂停、可接管；“已提交”不能当“已交付”

八、企业落地路线

- 阶段 0：选一个栏目、客户、剧集或资产类型，建立交付周期、返工、可用率、违规和人工责任基线。
- 阶段 1：先做只读检索、初稿和预审，不连接发布、预算和结算写权限。
- 阶段 2：进入制作与审片，让智能体创建任务、调用工具、记录版本和发起审核，对外产出仍由人放行。
- 阶段 3：只对明确阈值开放停投、重试、内部派单等低风险动作，要求结果回查、幂等和回滚。
- 阶段 4：按客户、项目、语种和渠道复制，建立统一素材权利台账、评测集和成本看板。

九、评测与验收

场景	任务质量	业务结果	风险与闭环
采编检索	时间码、来源、引用和事实准确	检索时间、稿件采用、返工	错引、幻觉、版权漏标、发布前人审
广告制作	brief、品牌、授权、渠道规格	周期、合格版本率、修改轮次	肖像/音乐/商标、虚假宣传、客户误发
投放止损	指标口径、异常识别、状态回查	超预算、无效消耗、响应时间	误停、账户越权、归因偏差、回滚
短剧生产	角色连续、资产齐套、术语、审核	交付周期、返工、可用率	IP 侵权、平台合规、主创确认
游戏 NPC	人设、记忆、动作正确和延迟	留存/体验需受控实验	有害内容、作弊、未成年人、紧急关闭

验收不能只看产量。任何效率、收益、曝光或成本数字都应绑定同口径基线、试点范围、人工复核、失败样本与观察周期。

十、风险边界

- 新闻事实、公共事件、对外发布和更正必须由编辑体系负责。

- 生成内容不能替代产品功能、公益对象和真实事件的证据；AI 标识、广告法和平台规则需按时点核验。
- 对外发布、投放预算、游戏经济、票务、版税和结算都是写操作，必须最小权限、审批、日志、回查和撤销。

十一、案例与来源索引

核心来源

- 山海星辰短剧全链路智能体
- 游戏美术 AI 工作流
- 游戏本地化质量
- 螃蟹游戏业务管理
- 三家广告公司的 AI 创意实践
- 网易智选 AI 广告投放
- 生成式 AI 营销内容运营
- AniShort AI 短剧工作台
- 大模型驱动的游戏智能 NPC
- 前《原神》主创的 AI 游戏创业实践

第十三章 教育与科研：把 AI 智能体放进学习反馈、校务运营和可复现实验

研究截止：2026 年 9 月 3 日。教育的目标不是“多生成一份答案”，科研的目标也不是“多写一篇综述”；两者都要把过程证据、专业判断和人的责任留在链路中。

本章核心结论

- 教育端最清楚的落地链是教学设计、互动辅导、作业反馈、成长观察、教务咨询和教师复核；学生成绩、升学和权益决定不能交给模型。
- 当前应用已经覆盖高校教务教学矩阵、科研软件部署、实验设备编排，以及预算、资产、设备和能耗等校务运营链。
- Deploy-Master 证明“找到工具—理解仓库—构建—最小命令验证—注册”的科研基础设施价值；MHS 仍是研究预览，不宜表述为实验室规模化自主运行。
- 教育效果必须看学习增益、错误纠偏、公平性和教师工作变化；科研效果必须看证据、复现、参数、失败记录和专家驳回，而不是只看生成速度。

一、行业边界

本章覆盖 K12、幼教、高校、职业与成人教育、教培服务、校务后勤、科研机构和实验室。招生营销与一般 CRM 只作交叉能力；科学计算工具、文献模型和设备驱动也不因“自动化”自动升级为完整智能体。

教育与科研共享知识、评价和人才培养，但业务结果不同：教育面对学生发展和公平，科研面对可证伪、可重复和学术诚信；物理实验还增加设备、样品和人员安全责任。

二、核心业务链

教育链：招生/入学 → 教学设计 → 学习互动 → 作业与评价 → 学情干预 → 教务服务 → 家校沟通 → 校务后勤 → 质量改进

科研链：研究问题 → 文献与数据 → 假设 → 工具发现与部署 → 实验设计 → 模拟/物理实验 → 分析 → 复现与同行核验 → 知识沉淀

三、逐环节业务问题

环节	输入与角色	典型问题	智能体机会
教学设计	教师、课程标准、学情、资源	备课重复、目标与评价脱节	项目/课程设计助手、课件和题目草拟
学习互动	学生书写/语音、课程内容	只给答案、不识别思路与卡点	多模态互动辅导、分步提示和再练习
作业评价	作业、Rubric、历史反馈	批改负担、反馈不一致	批阅草稿、证据定位、易错点汇总
教务服务	校规、课程、学籍和办事流程	政策更新快、入口分散	有出处问答、工具入口和转人工
成长与家校	观察、作品、照片、发展指标	数据零散、报告主观	结构化观察、报告草稿、教师确认
校务运营	预算、合同、采购、资产、维修、能耗	重复采购、闲置、维护晚、异常难归因	预警、调拨/维护/节能建议
科研准备	文献、仓库、依赖、工具说明	工具找不到、部署失败、环境不可复现	科研工具搜索与部署智能体
物理实验	方案、样品、设备能力和状态	接口异构、动作风险、记录断链	受控设备编排、异常阻断和日志

四、AI 智能体全景

智能体或形态	业务位置	应用边界
项目制课程设计助手	教学设计	探月学校已应用；课程目标、内容和评价由教师审定
英语写作辅导/教师分身	作业与个辅	北京中学已应用；评分依据可解释，学习效果持续评估
幼儿成长观察与报告助手	成长档案	东方悦稚已应用；儿童数据最小化，报告由教师确认
多模态互动辅导智能体	学习闭环	学而思 材料；L3 是厂商自定义
高校教务咨询智能体	教务服务	西建大 学校官方上线材料
高校教学工作智能体矩阵	备课、出题、批阅、学情	西安建筑科技大学已应用；教师负责最终评价
高校科研服务智能体	文献、查新、知识库、学术追踪	西安建筑科技大学已应用；引用和研究判断由研究者负责
科研全周期伙伴型智能体	假设—实验—分析	可协助检索、假设、实验设计和分析，科学判断由研究者负责
科研软件搜索与部署智能体	科学计算基础设施	Deploy-Master 技术材料
实验设备编排智能体	物理实验	MHS 展示设备编排路径；必须配置动作白名单与急停
预算与重复采购预警智能体	校务运营	识别重复采购和预算异常，采购决定由授权人员作出
资产与预测维护智能体	校务运营	连接资产台账、报修和设备状态，维护计划由责任部门确认
能耗异常与节能调度助手	后勤	先建立能耗基线，再评估异常识别和节能结果
独立英语工作室教学交付智能体	教培	支持备课、练习、反馈和家校沟通，教师负责教学质量
教育集团 AI 项目孵化机制	组织采用	属于智能体孵化与治理机制，用于组织场景筛选和复制

五、重点智能体工作卡

1. 多模态互动辅导智能体

字段	内容
服务对象	学生、教师和家长
触发条件	学生书写、语音作答、连续错误或停滞
主要输入	手写/语音、题目、课程内容、学习历史和教学策略
判断与规划	识别思路与错误类型，选择追问、提示、讲解或练习
工具与系统	学习平台、多模态识别、课程知识库、题库和学情系统
输出与动作	分步提示、讲题、练习推荐和学情更新
人工控制点	错误答案、长期卡住、敏感心理/健康信息和重要评价转教师
验收指标	错误识别、提示有效、学习增益、依赖性、教师接管和不同群体公平性

2. 高校教务教学智能体矩阵

字段	内容
服务对象	学生、教师、教务与教学管理人员
主要输入	校规、培养方案、课程、作业、教学资源和学习行为
工具与系统	门户、教务、课程平台、知识库、题库与人工工单
输出与动作	有出处咨询、课件/题目草稿、批阅建议、学情报告和转人工
人工控制点	学籍、成绩、奖惩和教师最终评价
验收指标	政策时效、引用正确、问题解决率、错转、教师修改量和学生申诉

3. 科研软件搜索与部署智能体

字段	内容
服务对象	科研人员、科研平台和计算环境管理员
触发条件	研究任务需要寻找并运行新的科研软件
主要输入	研究目标、仓库、文档、依赖、许可和算力限制
判断与规划	搜索候选，理解仓库，由双模型评审构建方案，执行最小命令验证
工具与系统	代码仓库、容器、构建工具、算力调度、工具注册与日志
输出与动作	可调用容器、注册信息、验证结果、依赖和失败分类
人工控制点	环境隔离、许可/安全审查、资源限额和结果科学有效性
验收指标	部署成功、最小命令通过、复现、失败归因、依赖污染和资源消耗

4. 实验设备编排智能体

字段	内容
服务对象	实验人员、平台工程师与安全负责人
主要输入	实验方案、样品、设备能力/状态、动作权限与异常规则
工具与系统	标准设备描述、驱动、机械臂/移液器/读板机、监控和日志
输出与动作	受控动作序列、执行记录、异常阻断和待人工任务
人工控制点	动作白名单、样品确认、异常阻断、急停和人工批准
验收指标	动作正确、设备状态回查、样品错配、异常拦截、复现和接管时间

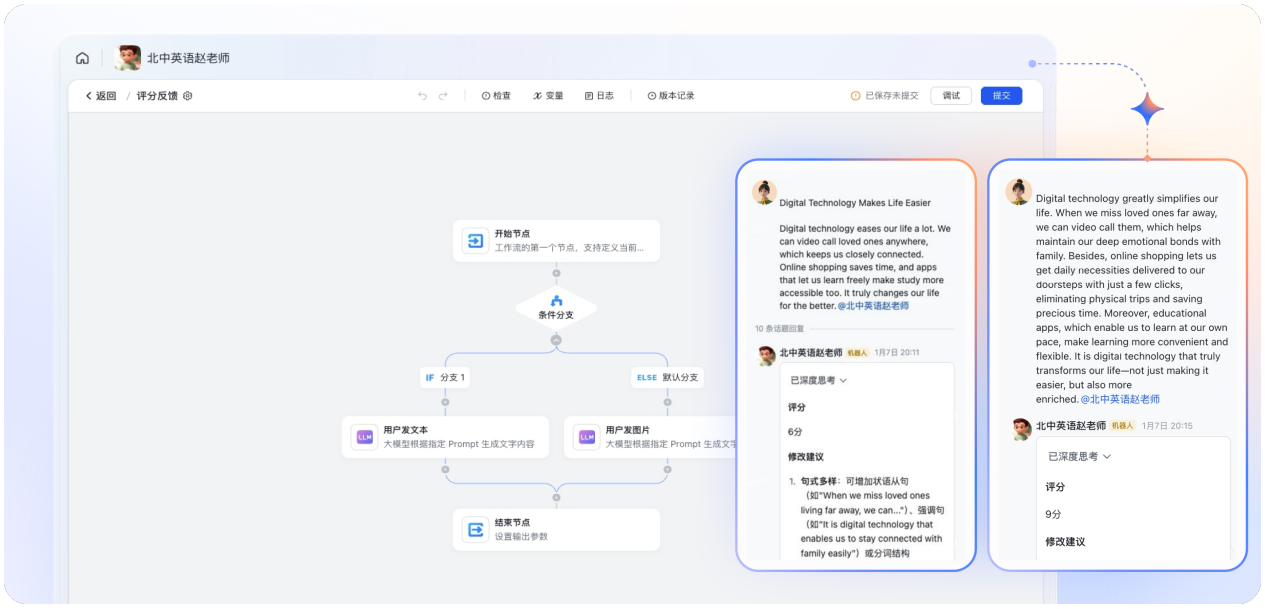
六、代表案例

探月学校的 PA 项目设计助手通过分步提问、资源匹配和结构诊断形成课程草稿，说明智能体可以把课程设计方法嵌入教师工作流；最终目标、活动和评价仍由教师确认。



图：探月 PA 助手案例原图

北京中学的应用形成了“作文提交—打分与解释—多轮修改—班级易错点汇总”链路。学校应持续评估评分偏差、教师否决率和长期学习效果。



图：北京中学英语写作辅导案例原图

西建大官方材料呈现了教务、教学和科研服务的学校级矩阵。Deploy-Master 和 MHS 则说明科研智能体正从“读文献”走向“部署工具”和“受控操作设备”，但风险等级随执行深度快速上升。

七、系统、数据与权限

- 教学侧连接课程平台、题库、作业、教务、学情与人工工单；成绩写入、学籍和奖惩必须审批并提供申诉。
- 成长档案包含儿童个人信息、照片和行为记录，应最小化采集、区分教师/家长权限并设置留存期限。
- 校务侧连接预算、合同、采购、库存、资产、维修、课表、门禁、人流与能耗；调拨、采购、处置和设备控制由授权人员批准。
- 科研侧保存文献版本、数据许可、代码提交、依赖、容器、参数、随机种子和实验日志；外部工具不得获得超出任务的网络、文件或设备权限。
- 物理设备采用动作白名单、前置检查、互锁、超时、急停和人工接管，智能体不能绕过设备自身安全控制。

八、落地路线

- 先选一个课程、教务事项或科研工具建立错误、工时、复现和人工复核基线。
- 从只读问答、资料整理和草稿开始，建立来源、版本和转人工机制。
- 再接入作业、学情、工单或容器执行，只开放低风险写入并保存完整日志。
- 物理实验先做影子运行和模拟器验证，再逐项开放动作白名单和急停演练。
- 跨课程、院系和实验室复制前重测人群公平性、知识差异、设备差异和运维成本。

九、评测与验收

场景	核心验收
互动辅导	错误识别、提示有效、学习增益、依赖、教师接管和公平性
教务咨询	引用与政策时效、真实解决率、错导办、人工转接和申诉
作业批阅	Rubric 一致、关键错误漏检、教师修改和成绩争议
校务运营	预警有效、重复采购/闲置/故障变化、节能基线和收益归因
科研部署	可复现、依赖/许可、安全、失败分类和最小命令验证
设备编排	动作/样品正确、异常阻断、急停、日志和人工接管

十、风险边界

- AI 不得独立决定成绩、升学、学籍、奖惩或资源资格；教师和学校提供复核、解释与申诉。
- 学生和儿童数据不用于超出教育目的的画像或训练；需要访问控制、脱敏、留存期限和删除机制。
- 生成答案可能造成过度依赖与学术不端，应区分辅导、代做和正式评价。
- 科研智能体的文字流畅不等于科学正确；引用、假设、参数、统计与实验结果必须由研究者复核并可复现。

十一、来源索引

核心来源

- 探月学校项目设计助手
- 北京中学英语写作智能分身
- 东方悦稚幼儿成长记录
- 华图教育产品教研平台
- 学而思新一代 AI 教师
- 西建大智慧校园教学服务 AI 助手
- 西建大智慧校园科研服务 AI 助手
- Deploy-Master 科研软件部署智能体
- 实验室设备编排智能体
- 学校预算、资产、设备与能耗智能体
- 科研智能体漫游指南

第十四章 专业服务：AI 智能体进入专业交付，但责任仍由持牌与签字人员承担

研究截止：2026 年 9 月 3 日。本章覆盖法律、知识产权、会计审计税务、咨询、工程设计和人力服务。专业服务的价值不只在文档，而在委托关系、专业判断、签字责任和结果可解释。

本章核心结论

- 当前应用主要集中在合同审查、法务协同、知识产权检索、设计变更和招聘流程；会计师事务所、税务师事务所、管理咨询、检测认证和翻译本地化仍有较大拓展空间。
- 合同审查形成“解析—类型/主体—范本/清单/法规/案例比对—风险分级—红线稿—律师复核”的完整链，也补出 AI 原生律所按合同或结果计价的服务模式。
- 专利检索、OA 答复、FTO 和 Claim Chart 可以分别成为专业智能体，但新颖性、侵权、答复策略和正式意见必须由专利律师或代理师确认。
- 任何 AI 输出都不能自动成为法律意见、审计结论、税务申报、设计签章或用工决定；客户知情、人工复核、申诉、停止和审计是交付组成部分。

一、行业边界与核心业务链

专业服务共同链：获客与委托 → 冲突/独立性/资格检查 → 信息收集 → 专业检索 → 分析或审查 → 方案与交付 → 持牌/签字责任 → 项目复盘 → 客户经营

法律和知识产权重证据、期限与执业责任；会计审计税务重独立性、底稿和鉴证；咨询重假设、访谈和实施结果；工程设计重规范、版本、现场变更和签章；人力服务重候选人权益、偏差和跨系统推进。相似的 RAG 或文档生成不能抹平这些差异。

二、逐环节问题

环节	业务问题	智能体机会	必须保留的人
委托与准入	客户冲突、授权、涉密和服务范围不清	材料收集、冲突线索和缺口清单	项目负责人决定是否承接
专业检索	法规/准则/专利/规范版本多、证据难定位	可追溯检索、引用和有效期核验	专业人员判断适用性
审查与分析	合同、财务、技术材料量大且上下文复杂	风险定位、假设、证据包和修订草稿	律师、审计师、工程师复核
交付与签字	初稿易规模化，但错误也会规模化	版本、送审、补件和交付状态跟踪	持牌/签字人员承担结论
项目执行	群聊、邮件、图纸、底稿和工单分散	问题归集、任务、期限和变更协同	项目经理及专业负责人
复盘与客户经营	反馈难沉淀、知识易跨客户泄露	经批准的模板/案例沉淀与提醒	客户隔离和知识审批

三、AI 智能体全景

智能体或形态	位置	应用边界
客户上下文合同审查工作区	法律服务	律师实践；现有对象
企业级合同审查工作流智能体	合同审查	执行条款定位、风险比对、修订和协同，法务终审
Crosby AI 原生律所合同交付系统	法律服务	AI 批量处理合同初稿，持牌律师复核、签字并承担责任
一人律所经营智能体	律所经营	二次产品方案
专利现有技术检索智能体	知识产权	自动构造检索式、聚类文献和定位依据，检索范围由专业人员确认
OA 答复智能体	知识产权	分析审查意见、检索依据并生成答复草稿，正式答复由代理师签发
FTO 初筛与 Claim Chart 智能体	知识产权	执行权利要求拆解和初步比对，不直接给出侵权结论
审计分录异常与调查智能体	审计	识别异常分录、组织调查任务和留痕，审计判断由注册会计师负责
咨询研究与方法论助手	管理咨询	执行检索、访谈整理、分析和报告草拟，外部事实逐条核验
设计院现场问题归集与变更协同智能体	工程专业服务	归集现场问题、关联图纸并协同变更，设计签章由专业人员负责
招聘触达、初筛、排期与回访智能体	人力服务	支持触达、初筛、排期和回访，持续检查偏差并保障候选人申诉
智能体治理审计智能体	内部审计	检查权限、日志、模型与流程控制，独立审计结论由审计人员作出

四、重点智能体工作卡

1. 企业级合同审查工作流智能体

字段	内容
服务对象	企业法务、外部律师、业务和审批人
主要输入	合同、主体信息、范本、审核清单、历史案例、法规和客户偏好
判断与规划	解析/OCR、识别类型与主体，逐条比对并按风险分级
工具与系统	合同系统、OCR、法规/案例库、企业信息、审批与版本管理
输出与动作	风险报告、证据定位、红线稿、谈判要点和补件任务
人工控制点	法规与主体回查、风险取舍、对外意见和最终签署
验收指标	关键风险召回、误报、引用有效、红线可用、修改量和错误放行

2. 专利智能体组

字段	内容
服务对象	专利工程师、代理师、律师和研发团队
主要输入	技术交底、专利库、分类号、权利要求、审查意见、产品证据
判断与规划	扩展检索路径，拆解区别特征，组织 OA、FTO 和 Claim Chart 任务
工具与系统	全球专利库、法律状态、项目空间、检索/比对工具和日志
输出与动作	现有技术、答复策略草稿、权利要求映射和风险初筛
人工控制点	检索范围、新颖性/创造性、法律状态、侵权和正式答复
验收指标	召回、证据可追溯、法律状态时效、映射正确和专家驳回率

3. 设计院现场问题与变更协同智能体

字段	内容
服务对象	项目经理、各专业负责人、现场与经营部门
主要输入	群聊、邮件、联系单、图纸、合同、版本和现场问题
判断与规划	归集分类，区分答疑/变更，检查多专业影响和合同外服务
工具与系统	协同平台、图档/文控、项目管理、合同与工时系统
输出与动作	问题台账、技术回复草稿、变更清单、签收和边界提醒
人工控制点	专业负责人审签；经营部门确认合同外工作
验收指标	问题遗漏、响应时间、错版、影响漏检、签收和额外服务留痕

4. 智能体治理审计智能体

字段	内容
服务对象	内审、风控、信息安全和业务责任人
主要输入	智能体清单、身份、访问权、行为权、审批、工具日志和第三方合同
判断与规划	追踪授权链，抽查越权/绕批，检视日志、责任与停止机制
输出与动作	风险证据、整改建议、复测任务和审计底稿草稿
人工控制点	独立审计判断、责任认定、整改验收和紧急停止
验收指标	盘点完整、权限漂移、日志缺口、问题复现和整改关闭

五、代表案例与图片

现有的合同材料说明：合同风险不只来自条款文本，还来自客户、交易地位、主体、履约历史和谈判偏好。材料覆盖范本、清单、法规、案例和红线稿工作流。Crosby 案例则提示商业模式变化：AI 完成批量初稿，持牌律师复核与签字，服务可从按工时转向按合同或结果计价；其服务范围、责任保险和效率仍需一手材料。



图：法律 AI 报告文章配图

Thrive Holdings/Current 税务材料更接近生产线索，但税表数量、准备时间和准确率来自二次文章，缺少完整样本与复核定义，不宜表述为 AI 独立报税或签字。

环节	传统工作	AI/自动化后	对 EBITDA 的影响
税务准备	人工录入、核对、计算	自动抽取、分类、计算、生成初稿	**人工成本下降**
Bookkeeping	凭证、分类、对账	自动分类、自动 reconciliation	**交付成本下降**
Audit	抽样、凭证检查、工作底稿	文档分析、异常识别、全量检查	**审计效率提高**
Document processing	PDF、Excel、邮件人工读取	OCR/LLM抽取与结构化	**低价值工时下降**
Review	senior逐项复核	AI预审、异常提示	**高级人员 leverage 提升**
Billing	工时、开票、催收	自动 billing/workflow	**后台成本下降、DSO改善**
Client service	邮件、常见咨询	AI助手生成答案/材料	**客户容量提高**
Advisory	人工搜集分析资料	AI辅助分析、报告、预测	**高毛利收入增加**

图：Thrive 会计服务文章配图

设计院相关材料把施工配合写成可验收链：多渠道问题归集—分类—专业影响检查—版本与签收—合同外服务留痕。这比单纯规范问答更接近主营交付。

六、系统、数据与权限

- 客户与项目空间必须隔离；合同、底稿、专利、候选人和设计资料按事项授权，禁止跨客户记忆污染。
- 法规、准则、专利法律状态和工程规范标注发布机构、地域、版本、生效/失效时间及引用位置。
- 核心系统包括合同/案件、专利检索、审计底稿、财税、项目/图档、ATS/CRM 和工单；默认只读，写入、提交、签发和对外发送逐级授权。
- 每次工具调用、人工修改、模型版本、检索来源和最终采纳都要留痕；对外部模型明确数据留存、训练、删除和分包方责任。

七、落地路线

- 从单一合同类型、专利任务、项目问题台账或招聘环节建立基线和金标准。
- 先做只读检索、材料整理和初稿，逐条展示依据和不确定项。
- 接入项目空间、版本和审批流，只开放建任务、存草稿、送审等可撤销动作。
- 在专业人员持续复核下扩大任务类型，分别统计低风险自动通过和高风险强制升级。
- 跨客户复制前重新验证权限隔离、规则版本、责任保险/合同和质量复核体系。

八、评测与验收

场景	任务质量	业务结果	风险控制
合同审查	关键风险召回、引用、红线正确	周期、返工、谈判准备	漏检、过期法规、错误外发、律师终审
专利任务	现有技术召回、特征映射、状态时效	检索/答复周期、专家修改	侵权误判、期限、正式签发
审计调查	异常、证据完整、底稿可追溯	调查时间、问题关闭	独立性、重大错报漏检、签字责任
设计变更	问题归集、影响和版本准确	响应、变更关闭、额外服务留痕	错版、漏专业、无授权变更
招聘流程	信息准确、排期/回写成功	候选人推进和响应	偏差、隐私、拒绝理由与申诉

九、风险边界

- 法律意见、诉讼策略、税务申报、鉴证结论、设计签章和用工决定不得由模型独立作出。
- 生成内容必须展示来源和有效期；来源缺失时只能标不确定，不能补写“合理”依据。
- 人力场景需要检查性别、年龄、地域、口音和残障等差异影响，并为候选人提供人工渠道。

十、来源索引

核心来源

- AI 合同审查进阶指南
- AI 合同审查落地实践
- Crosby AI 原生律所合同交付
- Harvey 知识产权 AI 产品
- 一人律所法律 AI 智能体
- 设计院现场服务与设计变更闭环
- AI 智能体治理审计

第十五章 医疗、医药与生命科学：从信息辅助到受控临床与科研工作流

研究截止：2026 年 9 月 3 日。本章所有诊疗、用药、检验、药物警戒和临床研究输出均定位为辅助材料或受控动作；医生、药师、检验人员、科研人员和法定责任主体保留最终判断。

本章核心结论

- 医疗智能体不应只写“问诊”。数据治理、导诊、病历质控、随访慢病、药事、科研工具、药物警戒和院内供应链同样决定能否进入生产。
- 研发情报、药物安全和医疗多智能体已经形成基本应用链；广州发布的场景清单也呈现出数据治理、临床服务、科研和运营等大量具体需求。
- OriBench 展示了药研智能体应有的形态：专业工具连接、长任务、中间产物、证据溯源、失败恢复和人工复核。
- 医疗验收不能只看答案正确率，还要看急症漏分、错误建议、人工接管、真实使用、审计、跨院复制和患者申诉。

一、行业边界与核心业务链

本章覆盖医疗服务、生物医药、生命科学、医疗器械和医药流通。健康科普、医院信息系统、传统预测模型、机器人和自动化设备均可能是智能体部件，但不能因带 AI 名称就视为完整智能体。

医疗服务链：健康咨询 → 预问诊/导诊 → 医生接诊 → 检验检查 → 诊疗与用药 → 病历质控 → 随访/慢病 → 转诊与申诉

医药链：文献/组学 → 靶点与分子 → 实验/临床 → 工艺与生产 → 质量与安全 → 药物警戒 → 流通追溯

院内供应链：采购 → 入库 → 二级库 → 领用配送 → 使用核销 → UDI 追溯 → 结算 → 效期与召回

二、逐环节问题

环节	典型问题	智能体切入点	高风险闸门
数据治理	字段异构、血缘不清、用途和权限复杂	数据元、数据源、映射和关系探查	数据管理员、伦理与用途审批
导诊接诊	信息重复、科室错配、急症风险	预问诊摘要、风险分层、医生副驾驶	急危重症升级、医生判断
病历与检验	漏项、逻辑冲突、危急值	病历草稿/质控、检验审核线索	医生/检验师签发
随访慢病	失访、多病计划冲突、依从性差	外呼、风险分层、任务编排	身份核验、医生/药师处置
药物研发	工具分散、长任务不可追溯	工具发现、编排、中间证据和复现	科研人员决定假设与实验
药物警戒	多源个例、编码和信号调查量大	去重、信号线索、证据包和报送草稿	因果判断与法定报送审批
SPD/UDI	库存、效期、批号和领用断链	预警、补货、追溯和召回任务	采购、用药、召回人工批准

三、AI 智能体全景

智能体或形态	位置	应用边界
医疗数据元、数据源、映射和表关系探查智能体	数据治理	自动探查数据关系，人工审核后写入数据目录
数字家庭医生智能体	基层连续服务	提供健康咨询、随访和服务协调，不独立诊断或处方
预问诊与导诊智能体	门诊前	采集症状并匹配科室，急症漏分必须作为红线指标
病历生成与质控智能体	门诊/住院	产品功能材料；医生签署
临床检验推荐与报告审核智能体	检验	提供检验建议和报告预审，不得自动加检或签发
随访与失访追踪智能体	诊后/公卫	应用场景；区分固定外呼和动态编排
慢病多病共管智能体	基层健康管理	应用场景；临床责任归团队
药房库存与连续用药监测智能体	药事	应用场景；不自动改处方
AI 医院多专业服务编排智能体	健康入口	协调多专业服务与资源，预约和服务结果必须可确认
循证检索与证据分级智能体	临床/科研	检索、分级并生成摘要，引用由临床或科研人员逐条核验
OriBench 与 OriGene 专家智能体群	药物研发	支持药研任务评测与专家协作，生产效果按真实研发任务验收
药物警戒候选智能体	制药安全	辅助信号识别、病例聚合和报告草拟，正式信号与报送由专业人员负责
SPD 效期与 UDI 追溯候选智能体	院内供应链	连接效期、库存和 UDI 追溯，可与规则、视觉和工作流组合

四、重点智能体工作卡

1. 预问诊与病历质控智能体

字段	内容
服务对象	患者、接诊医生和病案质控人员
输入	主诉、病史、历史病历、检验检查、科室/号源、模板与规则
判断与工具	追问和风险分层；连接患者端、HIS/EMR、LIS/PACS 和质控规则
输出	预问诊摘要、科室建议、急症提示、病历草稿和质控问题
人工控制点	急症立即升级；医生确认诊断、医嘱、病历与签名
验收	急症漏分、科室命中、虚构/漏项、医生修改、响应与回填失败

2. 随访与慢病共管智能体

字段	内容
输入	患者名单、随访计划、诊断指标、用药、依从性和联系方式
工具	随访/公卫平台、EMR、呼叫/企微、预约和家庭医生系统
输出	结构化记录、风险分层、失访清单、复诊/转诊和人工任务
人工控制点	身份、拒访、急症、用药冲突和临床处置
验收	触达之外看风险漏报、转人工时延、任务关闭和计划冲突

3. 药物研发工具编排智能体

字段	内容
输入	研究目标、文献、组学/分子数据、工具参数与算力约束
判断与工具	选择 OrigeneMCP 等专业工具，编排长任务并保存中间状态
输出	计划、中间产物、候选靶点/分子/方案、活动与证据记录
人工控制点	假设、参数、实验设计、结果解释和是否进入下一阶段
验收	工具成功、参数正确、来源、复现、失败恢复和专家驳回

4. 药物警戒智能体

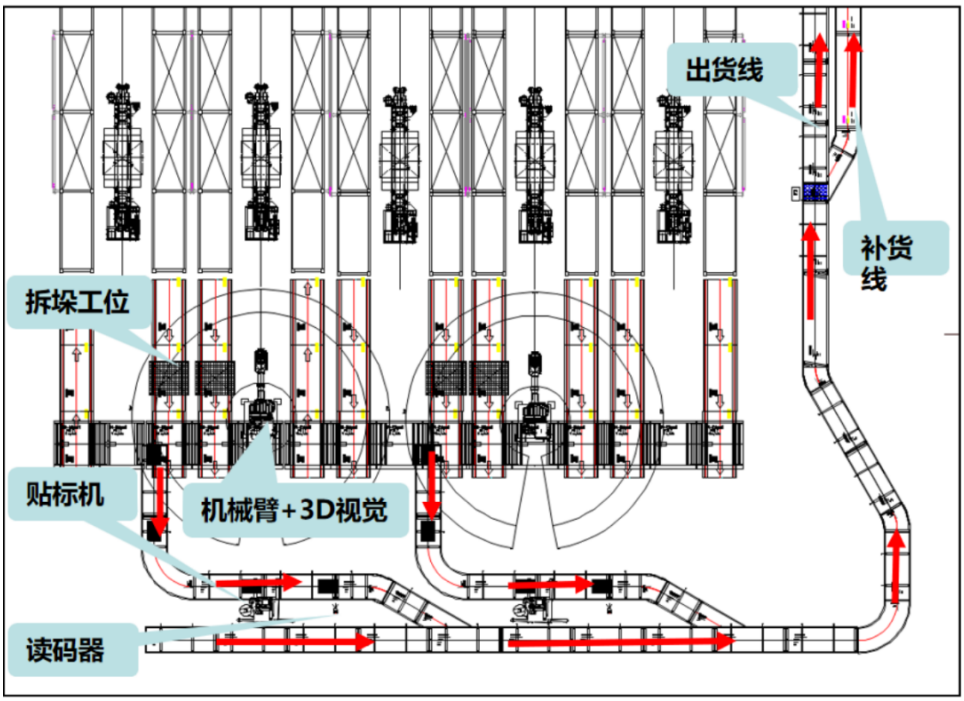
字段	内容
输入	个例报告、文献、投诉、临床/上市后数据、质量与法规
工具	药物警戒系统、安全库、医学编码、文献/监管库和工作流
输出	去重与编码建议、信号线索、证据包、调查和报送草稿
人工控制点	医学复核、因果判断、信号确认、风险措施和法定报送
验收	个例漏检、重复合并、编码、时限、证据完整和错误信号

五、代表案例与图片

医疗多智能体材料区分 MDT 圆桌、流水线和教学式协作，适合解释责任结构；文中的示例时长属于说明性故事，不能当医院实测。

扬子江靶点调研机器人连接会议、公共数据库和内部知识库，抽取适应症、风险、基因、临床数据和候选药物参数，形成研发情报报告。相关效率为联合案例公开口径，科研人员仍负责假设与实验。

医药物流材料展示机械臂、AGV、视觉复核与 WMS/EIS/WCS 追溯，其核心是确定性自动化和视觉算法，不应包装为大语言模型智能体。



图：医药物流原文配图

六、系统、数据与权限

- 临床系统：HIS、EMR、LIS、PACS、处方、预约、随访和区域健康档案；按角色、患者关系和用途授权。
- 科研与药企：文献/组学/分子库、ELN/LIMS、算力、质量、临床试验和药物警戒；数据许可与试验版本全程留痕。
- 供应链：SPD、WMS、批号效期、UDI、配送与结算；补货、采购、召回和支付均需审批。
- 所有模型输出保存来源、时间、版本、置信与人工修改；敏感健康数据最小化、脱敏、限期保存并支持撤回/删除。

七、落地路线与验收

- 从病历质控、随访记录、科研工具部署或效期预警等可回顾验证场景起步。

- 先只读影子运行，与医生/药师/科研人员金标准对比，建立急症和高风险强制升级。
- 再开放草稿回填、预约/随访任务和内部工单；诊疗、用药、报告签发和法定报送不自动执行。
- 通过固定测试集、真实运行、失败演练和患者申诉后再扩科室/病种/机构。

验收同时覆盖临床/科研质量、业务周期、人工修改、真实使用、系统可靠性、隐私、安全、接管和审计。跨院复制必须重新评估人群、设备、流程和知识版本。

八、风险边界

- 模型不能独立给出诊断、处方、检验签发、药物因果结论或患者权益决定。
- 低置信、急危重症、儿童/孕产妇等高风险人群必须升级专业人员，并保留线下通道、接管和申诉。
- SPD、机器人和视觉系统有价值，但需与生成式智能体的贡献分开验收。

九、来源索引

核心来源

- 广州卫生健康领域 AI 应用场景
- 京东健康探索研究院访谈
- OrigeneMCP 与 OriBench
- 医药工业数智化转型
- 华山医院 SPD 供应链管理
- 诊疗助手产品升级
- AI 医疗生成式大模型平台
- 医疗 AI 商业化与持续付费
- 医疗领域 DeepSeek 与安诊儿大模型

第十六章 金融服务：把 AI 智能体放进证据链，而不是放上最终决策席

研究截止：2026 年 9 月 3 日。授信、核保、理赔、投资、交易、支付、反洗钱与监管报送均为高风险活动；智能体可以调查、计算、核验和编排，但最终责任、授权、签发、申诉与审计必须归人。

本章核心结论

- 金融智能体正从客服问答扩展到客户经营、对公风控、反洗钱调查、资产负债核验、保险条款/理赔、财富研究和监管报送。
- AlphaMo 说明特征、模型和策略可拆成协作智能体；ICBCBench 说明“会写报告”不等于“会做金融研究”，必须考计算、日期、监管口径、证据和建议。
- 最重要的变化，是把对公风控还原为贷前尽调、审查、贷中监测、贷后预警和风险处置，而不是让大模型给一个授信分数。
- 金融智能体的效果必须结合具体任务、样本范围、运行周期和人工复核结果进行验收。

一、行业边界与核心业务链

本章覆盖银行、保险、证券、资产管理、财富管理、支付与金融科技。推荐模型、OCR、反欺诈评分、规则引擎和 RPA 是重要部件，但只有在权限、任务状态、工具调用、人工闸门和结果回查完整时，才构成执行型智能体。

银行链：客户识别/KYC → 产品与适当性 → 授信 → 交易运营 → 持续风险 → 处置/催收 → 合规报送

保险链：需求与条款 → 核保定价 → 承保 → 保全服务 → 报案/定损 → 理赔 → 反欺诈 → 再保与合规

投资链：研究 → 组合构建 → 交易前合规 → 执行 → 监控 → 归因与再平衡

二、逐环节问题

环节	典型问题	智能体机会	人工闸门
客户经营	信息分散、产品与客户约束难对齐	客户摘要、需求线索、方案草稿和服务回写	适当性、承诺和推荐
贷前/审查	工商、财务、流水和外部风险难穿透	多源核验、矛盾证据、补件和审查清单	现场调查、批准/拒绝、额度与定价
贷中/贷后	静态报表滞后、风险传导难解释	时序状态、预警剧本和核查任务	限额、冻结、收贷与法律处置
反洗钱	预警多、关联证据拉取耗时	交易图谱、证据包和调查报告草稿	EDD、可疑定性与报送
保险产品/理赔	条款复杂、材料多模态、欺诈与误伤并存	条款原子化、配置校验、定损和反欺诈线索	核保、条款签核、拒赔与支付
投研与组合	口径、日期、计算和引用易错	深度研究、计算核验、组合偏离与情景比较	投资建议、交易和再平衡
监管报送	规则版本多、字段和勾稽复杂	取数、校验、草稿、复核任务与回执	复核、签发、更正和问责

三、AI 智能体全景

智能体或形态	业务位置	应用边界
网点制度与流程助手	网点运营	回答制度与流程问题并展示出处，复杂事项转后台
客户经理服务副驾驶	客户经营	汇总客户信息并生成服务建议，不擅自推荐或承诺收益
AlphaMo 特征/模型/策略智能体	风控工程	专业材料；策略不等于自动审批
贷前尽调与授信审查智能体	对公信贷	执行多源核验和审查准备，保留现场核验与人工签批
贷中监测、贷后预警与风险处置智能体	持续风险	监测风险并发起处置建议，关键处置必须授权
反洗钱调查智能体	AML	综合材料；不自动定性/报送
客服摘要与工单智能体	客户服务	多银行研究
银行研发编码与测试智能体	金融科技	二次案例；代码审查/发布不绕过
LCR/IRRBB 核验智能体	资产负债	ICBCBench 评测映射；不是生产部署证明
保险条款智造与产品配置智能体	保险产品	二次企业案例；法务/精算/合规签核
车险理赔材料理解与图像反欺诈智能体	理赔	线索；不得据评分直接拒赔
财富顾问副驾驶与研究核验智能体	财富/证券	辅助研究和客户服务，所有建议由持牌人员复核
组合监控与再平衡候选智能体	资管	监控组合并生成再平衡建议，不自动交易
支付反欺诈协作与监管报送候选智能体	支付/合规	应用方法

四、重点智能体工作卡

1. 对公信贷全周期智能体组

字段	内容
输入	工商股权、财报、流水、税务、订单/物流、征信、司法舆情、合同和担保
判断与工具	主体穿透、交叉核验、时序风险、契约检查；连接信贷、评级、押品、交易和外部数据
输出	矛盾证据、补件、审查清单、风险剧本、核查和处置方案草稿
人工控制点	客户验真、授信批准/拒绝、额度、定价、提款限制、冻结、收贷和诉讼
验收	证据完整、复算、预警提前量、误报漏报、处置闭环、偏差与申诉

2. 反洗钱调查智能体

字段	内容
输入	KYC、交易流水、账户关系、名单、历史预警和规则
工具	AML 平台、核心/支付、客户主数据、图数据库、名单和案例库
输出	交易脉络、风险点、证据包、补充调查与报告草稿
人工控制点	PEP/ 受益所有人/资金来源核验、EDD、可疑定性和报送
验收	证据召回、误关联、调查时长、引用、人工修改、审计和客户申诉

3. 保险条款智造与配置智能体

字段	内容
输入	原始条款、模板、医学/保险知识、监管和公司规则
工具	条款库、产品工厂、核心保险、核保/理赔规则、审批与版本
输出	原子条款、字段、冲突、配置草稿、测试与写入记录
人工控制点	法务、合规、精算逐级签核；未经审批不得上线
验收	字段/规则映射、冲突召回、回归测试、错版、回滚和签核

4. 金融研究与证据核验智能体

字段	内容
输入	研究任务、财报/公告、行情、监管文本、内部研究和日期
判断与工具	拆题、检索、确定性计算、口径/日期核验和引用支持检查
输出	底稿、计算、逐条引用、报告、冲突和不确定项
人工控制点	研究结论、评级/建议、对客材料和任何投资交易
验收	标准答案、计算可复算、日期/规则版本、引用支持度和专业 Rubric

五、代表案例与图片

中信百信银行 AlphaMo 把特征挖掘、模型开发和策略寻优拆成协作链。公开效率和风险预测数字均为案例公开口径，仍需核验测试集、基线、时间窗和生产范围。



图：AlphaMo 智能风控工程体系

银行投入产出材料记录交通银行公开的场景/智能体数量和四维价值评估，但数量未逐项定义，不能等同于完整智能体数量。更可复用的经验是：业务部门承担真实成本，小范围试点以运行数据决定扩大。



图：银行 AI 投入产出研讨会现场

反洗钱实践演示企查查 MCP 拉取工商、股权、司法和关联关系数据并草拟报告；单一商业数据源不足以完成合规定性。

以往作业模式	企查查MCP解决方案
信息收集以"客户身份基本信息"为主，难以快速并高度概括客户风险全貌	AI自动聚合工商、司法、舆情等多维数据，一键生成客户风险画像
对受益所有人的最终穿透及风险状况判断，耗时且易遗漏	股权穿透自动计算，精准识别25%以上持股的自然人
高风险客户特征点难以精准定位	司法风险、经营异常、行政处罚等18类风险标签自动标注
难以实施针对性的强化尽职调查（EDD）	风险标签直接指向EDD触发点，指导下一步尽调重点

图：反洗钱尽调流程应用示意图

六、系统、数据与权限

- 核心系统包括 CRM/KYC、核心交易、信贷、评级、押品、AML、保险核心/理赔、投研/组合/订单、支付风控、监管数据集市。
- 数据按客户、账户、产品、机构和用途授权；敏感数据脱敏，外部模型不得获得不必要的交易明细。
- 读、建议、建任务、改字段、发起交易、资金划转和报送签发分级授权；所有写操作幂等、回查、可撤销并留审计日志。
- 模型、规则、名单、监管口径和产品版本都要可追溯；高风险输出展示依据、反方证据和人工采纳/否决。

七、落地路线与验收

- 先选网点问答、客服摘要、研究核验或贷后材料归集等可回顾验证场景，建立金标准和损失基线。
- 影子运行并与人工结论对比，检查不同客户群体、产品和周期的偏差。
- 开放内部建单、补件和草稿回写；授信、拒赔、投资、交易、支付和报送仍人工签批。
- 以小额度、白名单和双重确认试点低风险动作，演练超时、数据缺失、误操作、回滚和人工接管。
- 规模化前持续监测漂移、投诉/申诉、人工修改、业务结果和单位成本。

验收同时覆盖任务正确、业务结果、流程闭环、系统可靠、使用率、偏差、越权、申诉与审计；不能只看模型准确率或处理量。

八、风险边界

- 大模型不能作为授信、核保、拒赔、投资、交易、冻结、扣款或可疑报送的唯一决策者。
- 对客户产生不利影响时，必须给出可理解理由、人工复核和申诉渠道。

九、来源索引

核心来源

- 银行 AI 的新拐点
- AI 重做对公风控
- 19 家上市银行大模型应用
- ICBCBench 金融大模型评测
- 中华财险 AI 转型
- 大模型赋能客服中心与远程银行
- 证券公司财富管理数智化
- 支付反欺诈与反洗钱
- 平安智能理赔助手

第十七章 政务、公共事业与非营利：让智能体辅助办事与治理，不替代法定权力

研究截止：2026 年 9 月 3 日。行政决定、执法、采购评审、福利资格、劳动争议和应急指挥均由有权人员依法作出；系统必须保留规则来源、人工复核、申诉、线下通道、接管与审计。

本章核心结论

- 政务当前最成熟的应用集中在政策知识运营、导办预审、12345 摘要/归口/派发、机关办公预审和内部协同，自动审批不在成熟范围。
- 当前应用已经覆盖知识清洗与增量运营、政府采购表单和跨系统操作、政务智能体安全治理、基层巡查与仿真实训。
- 呼和浩特和湘桥已经上线政务知识、热线和机关办公相关应用，成效应按照事项准确率、办理时限、人工接管和群众反馈进行验收。
- 公共事业可从污水巡检等场景切入；非营利组织则可围绕捐赠、志愿者、项目管理和服务转介建设独立应用，不能直接套用政务流程。

一、行业边界与核心业务链

本章覆盖政务服务、机关办公、12345 热线、政府采购、城市和基层治理、市政公共事业、社会工作与非营利组织。政策问答、OCR、分类派单、RPA、驾驶舱、预测模型和设备控制都是相邻能力，不能自动算作完整 AI 智能体。

政务服务链：政策知识 → 群众诉求 → 意图识别 → 导办/材料预审 → 受理/审批 → 派单处置 → 回访/申诉 → 运营分析和政策改进

政府采购链：需求预算 → 文件/表单 → 合规检测 → 多系统录入/发布 → 评审辅助 → 合同/履约 → 留痕审计

基层治理链：视频/无人机/居民上报 → 事件识别 → 网格派单 → 现场核查处置 → 反馈与风险沉淀

公共事业链：设备/路线 → 传感与巡检 → 异常识别 → 告警/工单 → 运维复核处置；连续控制与应急指挥另设安全系统。

二、逐环节问题

环节	典型问题	智能体机会	人工/法定边界
政策知识	表格难解析、有效期与废止难维护	清洗、脱敏、QA/ 要素化、反馈更新	入库、废止和敏感知识审核
导办预审	群众不会表达、材料反复补	意图、事项匹配、补正和依据提示	正式受理、审批和权益结论
12345 热线	长诉求、错派、跨部门和热点难分析	摘要、归口、派发、回访和周报	模糊/重大/跨部门人工调度
机关办公	公文、合同、立项、采购材料量大	校对、预审、知识和项目辅助	签发、立项、采购和审批责任
政府采购	异构表单与平台、操作留痕难	字段抽取、校验、跨系统执行	金额、主体、公告、评审和合同
基层治理	视频/无人机事件多、误报影响权益	识别、派单、进度和风险模式	现场核查、执法与救助
公共事业	巡检危险、数据多源	机器人/无人机采集、异常和工单	连续控制、停产、应急指挥
社会工作/非营利	个案复杂、资源与伦理约束强	仿真实训、资料整理和转介候选	个案评估、危机、资格和隐私

三、AI 智能体全景

智能体或形态	业务位置	应用边界
政务知识清洗与增量运营智能体	知识后台	裕安 实践；入库人工审核
政策文件问答化预审智能体	12345 知识库	呼和浩特 官方材料
12345 诉求总结—归口—派发智能体	热线	呼和浩特和湘桥已应用；错误归口可转人工纠正
政务导办—预审—代办—协同智能体	政务服务	无锡 二次分析；正式审批归人
政府采购表单处理智能体	采购前台	行业实践
政府采购跨系统操作智能体	采购执行	专业媒体；高风险发布确认
政务平台场景智能体矩阵	机关办公	湘桥 官方材料
政务智能体安全态势感知与治理系统	安全治理	行业实践
基层无人机/视频巡查智能体	城市治理	专业报道；现场核查
社区工作者仿真实训智能体	人才培养	专业报道；不替代督导
污水处理厂巡检候选智能体	公共事业	厂商方案；不接管连续控制
非营利项目/志愿者/捐赠智能体	非营利	当前应用不足，不列已落地

四、重点智能体工作卡

1. 政务知识运营智能体

字段	内容
输入	政策、事项、表格、有效期、废止信息、热线反馈
判断与工具	解析、清洗、脱敏、摘要/QA/ 要素化、有效期监测
系统	政策库、事项库、12345 知识库、版本和审核平台
输出	可溯源知识条目、冲突、待审更新和反馈周报
人工控制点	新增、废止、敏感脱敏、部门口径和正式入库
验收	引用、时效、冲突召回、问答命中、错误扩散和更新时长

2. 12345 工单智能体

字段	内容
输入	语音/文本诉求、政策、事项目录、历史工单、部门职责
工具	ASR、知识库、分类/归口、工单、回访和分析平台
输出	摘要、归口、派单、补充问题、回访和热点/地域分析
人工控制点	模糊、重大、群体性、跨部门和紧急事项人工调度
验收	关键信息完整、错派/退单、办理时长、回访、重复投诉和人工可达

3. 政府采购跨系统操作智能体

字段	内容
输入	项目、预算、文件、表单、时点和系统规则
工具	文档/OCR、备案、公告、专家抽取、结果公示和档案系统
输出	标准字段、缺失/冲突、操作草稿、截图、状态和审计记录
人工控制点	金额、主体、公告发布、专家/评审、合同和投诉答复
验收	字段准确、平台状态回查、重复提交、时限、接管和全程留痕

4. 基层治理巡查智能体

字段	内容
输入	无人机/摄像头、居民上报、GIS、网格和事件规则
工具	视觉识别、网格工单、地图、消息和处置反馈
输出	违建/焚烧/违停/垃圾/跌倒/聚集线索、派单和进度
人工控制点	现场核查、执法、救助、权益影响和紧急指挥
验收	分场景误报漏报、定位、派单、到场、闭环和申诉

六、系统、数据与权限

- 知识层保留政策原文、摘要、QA、要素、有效期、部门口径和版本；答案必须回链原文。
- 业务层连接事项、一网通办、OA、公文、合同、采购、12345、网格和公共设施平台；按场景隔离读写权限。
- 群众身份、健康、社保、救助和影像数据最小化使用；按用途、角色、地域和留存期控制。
- 高风险写操作采用双重确认、实时暂停、人工接管、幂等、截图/回执和不可抵赖日志。
- 建立事前准入、事中监测、事后审计、熔断降级、模型/规则版本和第三方安全评估。

七、落地路线与验收

- 从政策问答、材料预审、热线摘要或采购表单等可回顾验证任务建立基线。
- 先做只读与草稿模式，验证引用、时效、错导办、错派和人工可达。
- 开放内部建单、预填、提醒和状态查询；提交、发布和审批保持人工确认。
- 对跨系统操作采用白名单、最小权限和影子运行，演练界面变化、超时、重复提交、回滚和接管。
- 扩大前同时看办成率、补件、纠错、申诉、线下通道、公众公平性和单位运维成本。

场景	核心验收
知识问答	引用、政策有效期、冲突、错误答案和更新时长
导办预审	事项命中、补件、办成率、错导办和申诉
12345	摘要完整、错派/退单、办理、回访和重复投诉
政府采购	字段、规则、发布确认、回执、时限和审计
基层巡查	误报漏报、现场核查、处置闭环和权益申诉
公共事业	异常发现、现场复核、工单、接管和安全事件

八、风险边界

- AI 不得替代行政许可、执法、采购评审、福利资格、劳动争议、应急指挥等法定权力。
- 群众必须知道如何转人工、纠错和申诉；自动化不能成为拒绝线下服务的理由。
- 污水巡检只能辅助发现和派单，不能替代连续控制、安全联锁和现场处置。

九、来源索引

核心来源

- 裕安区政务服务智能化实践
- 呼和浩特 12345 与 DeepSeek 融合
- 湘桥政务 AI 平台

- 政府采购表单智能处理
- OpenClaw 驱动政府采购智能化
- 政务领域 AI 智能体安全治理
- 人工智能优化基层治理
- AI 污水处理厂智能巡检
- 无锡政务智能体应用
- 政务服务热线智能化转型

结语：从“AI 能做什么”回到“企业要完成什么”

17 个行业的材料放在一起，会看到一个很清楚的变化：企业采用 AI 的单位，正在从一段文字、一个模型能力或一个聊天入口，转向一段可分工、可执行、可追踪的业务流程。

智能体并不会让行业差异消失。恰恰相反，越往业务深处走，行业对象、专业规则、系统接口和责任边界越重要。制造业的图纸、工艺、质量和设备，医疗行业的病历、药事与临床责任，金融行业的交易、适当性与监管，政务场景的法定程序、申诉与公共责任，都不能被一套通用提示词替代。

这也是本书坚持先讲业务链、再讲 AI 智能体的原因。只有先说明谁在什么情况下处理什么对象、需要调用哪些系统、最终对什么结果负责，企业才能判断 AI 应该停留在知识助手，还是可以进入受控执行；也才能判断一个方案究竟是演示、试点，还是已经具备规模化条件。

对于多数企业，真正可行的路线并不是一步走向“全自动公司”。更现实的路径是：先让 AI 看懂资料和状态，再让它形成建议和草稿；随后允许它在受控范围内创建任务、更新系统和追踪闭环；只有经过真实业务验收，才逐步扩大动作范围和复制规模。

未来最有价值的智能体，可能不再以一个独立产品的形式出现。它会嵌入 ERP、MES、HIS、核心银行系统、政务平台、CRM、办公协同、研发工具和现场设备中，成为业务流程里一段受约束的能力。企业真正要建设的，也不只是一个智能体，而是一套可以让智能体安全工作的数据、知识、工具、权限、评测和责任体系。

附录一：跨行业通用智能体图谱

1. 知识与证据类

通用对象	适用行业	核心输入	核心输出	主要边界
制度/政策/标准知识智能体	全行业	文件、法规、标准、FAQ	带引用回答、适用版本、待核验项	来源、版本和权限
专业检索与研究智能体	科技、教育、医疗、金融、专业服务	研究问题、数据库、内部资料	检索式、证据集、分析报告	引文准确与专业复核
文档预审智能体	制造、建筑、金融、政务、法律	报告、合同、申请、规则	缺项、冲突、风险、修改建议	不替代正式签字和决定
知识运营智能体	全行业	新旧文件、反馈、使用日志	清洗、拆分、问答、有效期和更新任务	入库、废止和敏感信息审核

2. 分析与决策支持类

通用对象	适用行业	核心任务	需要组合的专业能力	主要边界
异常根因分析智能体	制造、能源、物流、电信、软件	汇总状态、提出并验证原因	时序分析、统计、图谱、日志检索	根因和处置由专家确认
风险预警智能体	金融、供应链、项目、政务	监测变化、分级、创建复核任务	规则、预测、图模型、外部数据	预警不等于最终定性
计划与调度智能体	制造、物流、能源、交通、酒店	理解目标、调用求解器、解释方案	运筹优化、仿真、预测、硬约束	不能让大模型替代求解和安全约束
经营分析智能体	零售、餐饮、制造、服务业	跨系统取数、解释偏差、生成行动建议	指标体系、BI、财务与业务规则	口径一致和归因边界

3. 流程与执行类

通用对象	典型动作	系统要求	人工控制点
工单与任务闭环智能体	分类、派发、催办、升级、回写、关闭	工单、协同、SLA 和责任目录	模糊、高风险和跨部门事项
客户服务智能体	意图识别、知识回答、摘要、建单、跟进	CRM、客服、订单与知识库	承诺、补偿、敏感投诉与监管事项
采购与供应商协同智能体	询比价、准入预审、交期、整改、绩效	ERP、SRM、合同、质量与库存	定标、重大承诺和付款
项目协同智能体	里程碑、风险、会议任务、资源和交付物	项目、合同、工时、财务和文档	范围、预算、对外承诺和验收
跨系统操作智能体	查询、录入、提交、截图、回写	稳定 API 或受控界面、身份权限、审计	发布、删除、付款、审批和不可逆动作

4. 感知与物理执行类

通用对象	感知/动作	典型场景	必要安全设计
视觉巡检智能体	图像识别、定位、派单	工厂、物业、农业、城市治理	漏报/误报分开验收，现场复核
设备诊断智能体	报警、传感器、手册、维修记录	制造、能源、交通、公用事业	设备型号和版本匹配，维修人员确认
机器人/设备编排智能体	调用机械臂、移动机器人或实验设备	仓储、制造、实验室、巡检	动作白名单、联锁、急停、隔离和接管
现场控制辅助智能体	参数建议、方案模拟、风险提示	能源、化工、制造、水务	不进入毫秒级安全回路，确定性控制优先

附录二：企业 AI 智能体落地路线图

阶段 0：问题定义与基线

先定义一个真实问题：当前谁在做、多久发生一次、耗时多少、错误和延迟造成什么影响。没有基线，就无法判断智能体是否创造价值。

最小输出包括：业务流程图、责任人、触发条件、输入输出、当前指标、不可接受错误和试点范围。

阶段 1：只读知识与分析

智能体可以检索、摘要、查询、分析和形成建议，但不能写入核心系统。重点验证依据、覆盖率、专业人员修改量和真实使用率。

适合场景包括制度问答、标准检索、设备知识、研究资料整理、经营报告和政策导办。

阶段 2：受控草稿与任务执行

智能体可以生成正式流程之前的草稿，或创建待确认任务。所有写入先经过人工确认。

适合场景包括合同预审、病历草稿、采购比价、三单核验、工单分派、项目风险和客户服务摘要。

阶段 3：有限自动闭环

对于低风险、高频、规则明确的分支，允许智能体自动执行；低置信度、异常和高风险分支自动升级人工。

这一阶段必须具备：最小权限、操作白名单、幂等、超时、重试、回滚、日志、人工接管和线上监控。

阶段 4：规模化复制与多智能体协作

在单场景稳定后，再复制到更多部门、产线、门店、机构或地区。复制时应同步迁移场景定义、数据合同、工具权限、评测集、责任链和运维机制，单独复制提示词不足以支撑规模化。

多智能体只在任务确实需要专业分工、共享状态和交叉验证时使用。角色越多，通信、状态一致性、权限和失败恢复越复杂。

附录三：评测与验收框架

1. 业务结果

根据场景选择成本、周期、交付、质量、收入、风险或公共服务结果。任何收益数字都应说明基线、时间范围、样本、对照和归因方法。

2. 任务质量

- 检索与问答：答案正确、引用准确、版本适用、拒答和转人工；
- 识别与预警：漏报、误报、提前量和高风险召回；
- 生成与审查：完整性、专业错误、人工修改、采纳和错误放行；
- 规划与优化：硬约束、可执行性、人工改排和异常恢复；
- 工具执行：成功率、幂等、错误写入、回滚和权限越界。

3. 流程闭环

验证智能体是否真正进入业务：自动触发率、任务到人率、按期关闭率、回写成功率、人工升级率、重复问题和跨系统状态一致性。

4. 工程可靠性

记录端到端成功率、P95 延迟、接口失败、重试、降级、单次成本、峰值容量、模型/知识版本和故障恢复时间。

5. 使用与组织

观察真实活跃、任务覆盖、员工修改、绕过系统、培训后独立完成和使用负担。登录人数或调用次数不能单独证明业务价值。

6. 风险控制

高风险动作人工确认率、审计日志完整率、回滚成功率、越权访问、敏感数据泄漏、偏差与歧视、申诉处理和安全事件必须单独统计。

7. 评测证据组合

- 确定性检查：字段、格式、计算、权限、接口和硬约束；
- 专家评测：医疗、金融、法律、工艺、工程等专业判断；
- 模型裁判：只处理经过人工校准的窄任务，不能替代最终责任人；

- 真实轨迹：用户请求、检索、工具调用、状态、输出、人工修改、执行和回滚；
- 业务指标：连接真实经营或服务结果，防止只优化离线分数。

附录四：风险分级与人工控制

风险级别	典型任务	建议自动化范围	必须保留的控制
低风险	内部检索、摘要、报告草稿	可自动生成与推荐	来源、权限和人工抽检
中风险	工单派发、材料预审、报价与排产建议	可创建任务或待确认写入	人工确认、回滚和异常升级
高风险	授信、核保、诊疗、许可、付款、放行、停机	以影子模式和决策辅助为主	有权人员批准、双人复核、审计和申诉/接管
生命/公共安全	手术/用药、应急指挥、连续控制、物理设备动作	不由大语言模型独立执行	确定性系统、联锁、急停、演练、冗余和现场责任人

高风险场景仍可使用 AI，但必须改变系统设计和验收方式。越接近不可逆动作，越需要把建议、决定和执行拆开，并明确每一步的责任主体。

—— 完 ——

关于编制者

曾俊，北京硅基行动科技有限公司创始人，长期专注企业 AI 落地、AI 实战培训、企业 AI 诊断与咨询、智能体定制和 AI 转型推进。本白皮书面向中国企业老板、业务负责人、AI 转型负责人和普通企业员工，重点回答 AI 智能体可以进入哪些行业流程、如何落地以及如何验收。

联系与交流

微信：ZF1235813266

公众号：曾俊 AI 实战笔记



微信二维码