中国工业互联网研究院
China Academy of Industrial Internet

工业智能体发展报告

中国工业互联网研究院智能化研究所
北京信息化和工业化融合服务联盟
中国科学院计算技术研究所

2026 年 9 月

特别声明

本报告由中国工业互联网研究院智能化研究所、北京信息化和工业化融合服务联盟、中国科学院计算技术研究所牵头编制，联合超聚变数字技术股份有限公司、北京神州光大科技股份有限公司、江苏慧工智能科技有限公司、中国电信集团有限公司、紫光云技术有限公司、福建工业互联网发展研究中心等共同参与完成。如果需要转载，须事先征得同意并注明“转载自中国工业互联网研究院智能化研究所、北京信息化和工业化融合服务联盟和中国科学院计算技术研究所”字样。

恳请各方批评指正，以及开展相关交流合作。

主　　编：顾维玺、闫同柱、程学旗

副 主 编：马戈、朱国伟、叶鸿儒、周河晓、何戍

编 写 组：刘永新、朱文友、朱鹰、谭学程、唐元武、姜宝正、李直儒、王骁、孙思齐、邱文瀛、傅冰飞、肖泽晓、李珏、魏常宁、李甲、刘晓慧、张宇宣、吕衎、李艳霞、段思祺、蒋泊辰、李优、廉润泽

主　　审：冯诀宵、黄自成、王青春、何思佳

校　　验：罗盈盈、李晨旭、陈超、和子然、陈悦、李婧妍、杨昱文、乔港

前 言

人工智能正从感知识别与内容生成向复杂推理、任务规划和行动执行拓展。制造业历经自动化、信息化、网络化与平台化的长期建设，已形成较为完备的工业软件、设备连接及数据资源基础。两股力量相互促进，使人工智能具备进入研发、生产、运维和服务等核心业务过程的工程条件，工业智能体因此成为人工智能赋能新型工业化的关键载体。

工业智能体不是对工业互联网平台、工业软件和控制系统的替代，而是面向清晰明确的工业任务，对现有数字能力的系统性重新整合。工业智能体以明确的工业任务目标为牵引，获取任务相关上下文信息，调用专业模型与工具形成实施方案，经由业务系统和现场装备开展受控执行，并依据确认回执对执行结果进行核验。在此背景下，制造业数字化智能化转型正呈现出三方面深刻转变：一是由系统功能驱动转向业务任务驱动，二是由单点优化转向跨系统协同，三是由信息辅助转向可验证、可接管的受控执行。评判工业智能体的发展水平，不能仅看模型是否先进，更要考察其能否在真实工况下完成任务并取得可核验的业务成效。

本报告是对工业智能体产业的系统研究成果，共分六章。第一章界定工业智能体的概念与战略意义；第二章从产业、功能、运行多个维度建立工业智能体体系架构；第三章按照数据、算力、模型、网络、安全与自进化六个层面阐述核心技术；第四章围绕研发设计、中试验证、生产制造、运维管理和营销服务五个环节

梳理产业实践；第五章聚焦工业智能体平台建设、一体机矩阵部署、工业智能体评测以及供需对接等重点工作进行讲解；第六章展望工业智能体由辅助工具向核心引擎演进的未来图景。

当前，工业智能体正处于由场景试点向规模应用过渡的关键阶段。本报告旨在为完善政策体系、推进应用场景建设、深化行业前瞻研究提供参考，也期待与产业各方共同探索符合工业特点、安全可信、渐进发展的智能体发展路径，为推进新型工业化、建设制造强国贡献力量。

目 录

第一章 工业智能体内涵、作用与定位 8
一、工业智能体内涵 8
二、工业智能体作用 9
三、工业智能体定位 10
第二章 工业智能体体系架构 14
一、产业体系 14
二、功能体系 19
三、运行体系 22
第三章 工业智能体核心技术 24
一、 数据：多源连接与语义底座构建 25
（一） 多系统与现场设备多源连接 26
（二） 统一事件模型构建 27
（三） 工业知识图谱 28
（四） 数字孪生映射 28
二、 算力：云边端协同部署 29
（一） 云侧：模型训练、数据治理与全局优化 29
（二） 边侧：低时延推理与现场编排 30
（三） 端侧：确定性执行与安全联锁 31
（四） 协同部署与弹性运维技术 32
（五） 工业智能体一体机 33
三、 模型：单智能体集成应用 34

（一） 感知：工业多模态感知与情境理解.....34
（二） 记忆：分层工业记忆体系.....35
（三） 推理：大模型与工业知识混合推理.....36
（四） 规划：约束感知的任务规划与动态重规划.....37
（五） 工具调用：工具标准化封装与安全调用.....37
（六） 策略约束与受约束决策生成.....38
四、 网络：多智能体协同编排.....38
（一） 领域智能体设置与编排.....39
（二） 任务分解与动态分配.....40
（三） 冲突消解机制.....40
（四） 一致性决策机制.....41
五、 安全：可信安全与治理.....41
（一） 身份与权限.....42
（二） 策略护栏.....42
（三） 全链审计.....43
（四） 故障降级.....43
六、 自进化机制：闭环验证与自演进.....44
（一） 感知与诊断：闭环起点与根因定位.....45
（二） 计划与仿真：改进策略生成与虚拟验证.....46
（三） 审批与执行：人工审批与安全下发.....46
（四） 反馈与持续演进：效果评估与迭代升级.....47
第四章 工业智能体产业实践.....48
一、 研发设计.....50
（一） 辅助设计与审查.....50

（二） 仿真与数字孪生 51
（三） 自动化工程开发 51
（四） 实验与配方筛选 53
二、 中试验证 53
（一） 工艺放大验证 54
（二） 试制与虚拟调试 56
三、 生产制造 56
（一） 生产计划调度 56
（二） 工艺优化控制 57
（三） 人机协同作业 58
（四） 质量检测改进 58
（五） 工厂协同优化 60
（六） 供应链风险管控 60
（七） 安全风险管控 61
四、 运维管理 61
（一） 设备诊断维护 62
（二） 无人巡检处置 63
（三） 能源系统优化 64
五、 营销服务 66
（一） 需求配置报价 66
（二） 售后技术服务 66
（三） 供需交易协同 67
第五章 重点任务 69
一、 建设通专融合工业智能体平台 69

二、 打造工业智能体一体机矩阵 69
三、 开展工业智能体评测 70
四、 推动工业智能体供需精准对接 71
第六章 未来展望 72
一、 从“辅助工具”向“核心引擎”的战略转型 72
二、 从“功能附加”向“智能原生”的业态重塑 72
三、 从“单点突破”向“集群聚变”的生态演进 73

第一章 工业智能体内涵、作用与定位

新一轮科技革命和产业变革纵深推进，人工智能正以前所未有的深度和广度重构生产要素、产业结构和治理模式。人工智能正处于从单点技术赋能向系统级智能跃迁的关键历史节点，以自主感知、自主决策、自主执行、自主迭代为核心特征的工业智能体，正在成为人工智能与制造业深度融合的核心落地载体。

一、工业智能体内涵

如图 1 所示，工业智能体是指面向明确工业目标和特定工业环境，融合工业数据、知识、模型与机理，具备环境感知、任务理解、规划决策、工具调用、协同交互、受控执行和反馈优化能力，能够在设定权限和安全边界内完成数字或物理工业任务的软件实体或软硬一体化智能系统。

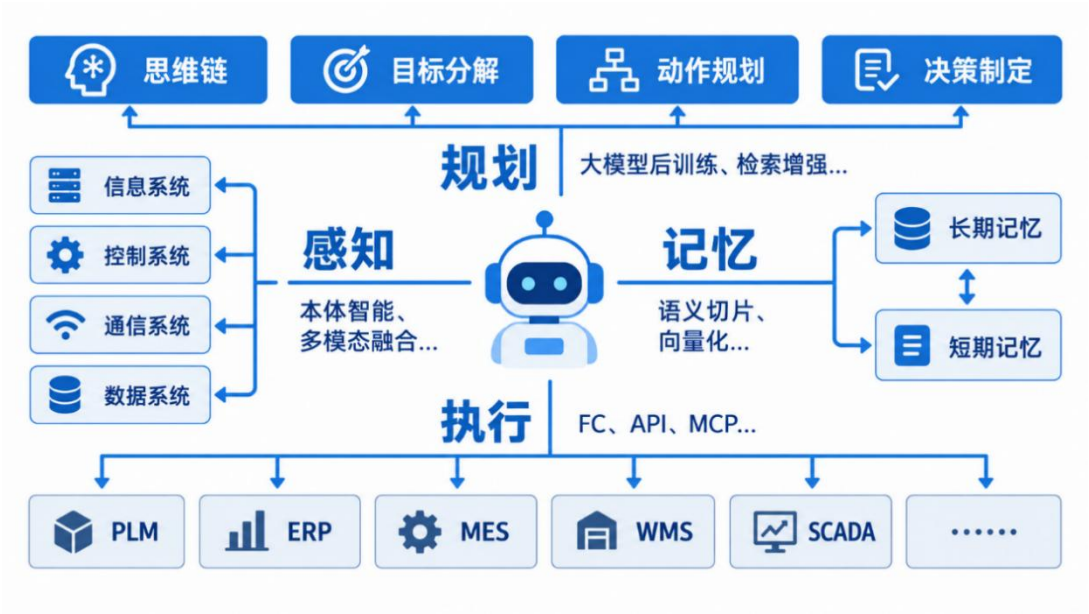

图 1 工业智能体

二、工业智能体作用

发展工业智能体，是顺应新一代人工智能技术演进趋势，推动人工智能与制造业深度融合的必然选择。国务院《关于深入实施“人工智能+”行动的意见》（国发〔2025〕11号）将“推进工业全要素智能化发展”列为重点任务，提出加快人工智能在设计、中试、生产、服务、运营全环节落地应用，到2027年新一代智能终端、智能体等应用普及率超70%。工业和信息化部等八部门印发的《“人工智能+制造”专项行动实施意见》（工信部联科〔2025〕279号）提出，到2027年推动3至5个通用大模型在制造业深度应用，推出1000个高水平工业智能体。工业智能体已成为推进制造业数智化转型、培育新质生产力、推进新型工业化的重要抓手。

第一，发展工业智能体可有效破解当前工业领域人工智能落地痛点。当前人工智能在工业领域的应用多停留在单点赋能、局部优化阶段，多数应用仅承担信息展示、方案建议等辅助性工作，难以直接对接工业核心业务流程完成闭环任务，落地成本高、价值变现周期长、规模化推广难等问题较为突出。工业智能体以完成明确工业任务为核心目标，能够打通数据、知识、模型与工业现场执行环节链路，推动人工智能从“能用”向“好用”、从“演示”向“落地”转变，切实提升人工智能在工业领域的应用效能。

第二，发展工业智能体可加速工业知识的沉淀、复用与创新。工业历经百年发展积累了海量知识，大量隐性知识仍留存于专家经验、纸质文档之中，存在传承效率偏低、复用

难度较大等问题。工业智能体通过数据挖掘、知识图谱构建等方式，将分散的工业知识转化为可调用、可迭代的智能化能力，实现了既有工业知识的高效传承，也可依托人机协同模式不断生成新的工业知识，为工业技术创新提供有力支撑。

第三，发展工业智能体能够为制造业数智化转型提供重要支撑。制造业智能化转型是覆盖研发、中试、生产、运维、营销等全链条的系统性变革，需要适配不同场景、承接不同任务的智能化载体予以支撑。工业智能体可根据不同场景需求灵活定制开发，既能够支撑单一生产环节智能化升级，也可通过多智能体协同实现全产业链智能化优化，为制造业全链条转型提供可复制、可推广的落地形态。

三、工业智能体定位

如图 2 所示，工业智能体是集成模型能力、软件工具与工业业务场景的任务组织和执行系统，正成为推动“人工智能+制造”规模化应用和产业化落地的重要载体。它的核心不在于形成更多模型输出，而在于完成产品设计优化、设备故障处置、质量异常处理、订单生产调度等工业任务。工业智能体基于任务对象、输入条件、约束规则、完成标准和责任主体等明确信息，获取必要上下文，调用专业模型、工业软件或设备能力形成策略方案，依据系统回执或现场状态核验结果，并将核验结论用于更新后续策略、模型参数或知识库。

“AI+制造”产业图谱
行业应用
钢铁行业
宝钢股份 南京钢铁 首钢股份 河钢集团 沙钢集团 中国钢研
有色行业
中国铝业 江西铜业 紫金矿业 金川集团 云锡集团 南山铝业
石化行业
中国石化 中国石油 中国海油 恒力石化 荣盛石化 桐昆集团
化工行业
万华化学 华鲁恒升 湖北宜化 兴发集团 卫星化学 新疆天业
建材行业
中国建材 海螺水泥 华新水泥 北新建材 东方雨虹 中国巨石
机械行业
徐工集团 三一集团 中联重科 潍柴动力 柳工 山推股份
汽车行业
比亚迪 上汽集团 长安汽车 吉利汽车 理想汽车 小米汽车
电力装备行业
东方电气 上海电气 哈尔滨电气 特变电工 国电南瑞 金风科技
轻工行业
海尔智家 美的集团 格力电器 伊利集团 安琪酵母 波司登
电子行业
京东方 工业富联 立讯精密 中兴通讯 长飞光纤 海康威视
工业智能体
研发设计智能体
鼎捷数智 创新奇智 联想 羚数智能 浩辰软件 中望软件 和利时 中工互联
生产制造智能体
华为 微亿智造 远船智能 红壹科技 卡奥斯 中控技术 浪潮
中试验证智能体
镁伽科技 明珞装备 浪潮云洲 海辰储能 中汽智造 国机智能 国检集团 广电计量
运营管理智能体
云鼎科技 汉得信息 树根科技 神州光大 用友网络 美的集团 科大讯飞 顺丰科技
营销服务智能体
实在智能 黑湖科技 龙翼信息 迈富时 百度 亚信科技 爱动超越 纷享销客
智能体开发平台
百度智能云 阿里云 腾讯云 火山引擎 华为云 科大讯飞 智谱AI 京东云 来也科技 Dify
模型
传统模型
商汤科技 旷视科技 云从科技 依图科技 海康威视 大华股份 科大讯飞 云知声 思必驰 第四范式 竹间智能 格灵深瞳 Google Meta Amazon IBM
大模型
通用大模型
百度 阿里云 腾讯 华为 科大讯飞 智谱AI 深度求索 字节跳动 月之暗面 旷视科技 MiniMax 昆仑万维 商汤科技 美团 中国移动 面壁智能 OpenAI Google Anthropic Meta
行业大模型
宝信软件 羚羊工业互联网 创新奇智 南方电网 中冶赛迪 卡奥斯 京东方 中控技术 华为 华院计算 四川开物信息 中能拾贝 中国煤科 京东工业 Microsoft Siemens
技术框架
服务平台
百度 华为 阿里云 科大讯飞 智谱AI 360 腾讯云 竹间智能 九章云极 火山引擎 中国移动 联通数科 京东云 旷视 商汤 OpenAI AWS Microsoft Azure Hugging Face Meta Google Cloud
开发平台
百度 阿里云 腾讯云 联想 亚信科技 创新奇智 九章云极 中电金信 京东云 华为 Google Cloud AWS Microsoft Azure Dataiku DataRobot
通用框架
百度 一流科技 旷视科技 小米 华为 腾讯 阿里巴巴 Meta Amazon Google
专用框架
百度 腾讯 遥晨科技 淘天集团 Google Anyscale NVIDIA Preferred Networks Microsoft
基础支持
数据
数据采集与处理
海天瑞声 标贝科技 慧听科技 数据堂 觉醒向量 千机数据 云测数据 星环科技 中科闻歌 达观数据 拓尔思 百分点科技 Scale AI Gretel.ai Lionbridge Sama Labelbox 倍赛科技 Appen Snorkel AI V7 Databricks Unstructured TELUS Digital
数据确权
北京知识产权 北京国际大数据交易所 中国工业互联网研究院 人民数据 数权通（北京）科技有限公司 蚂蚁链
数据交易
北京国际大数据交易所 上海数据交易所 深圳数据交易所 贵阳大数据交易所 江苏大数据交易所 西部数据交易中心
芯片
训练芯片
华为 燧原科技 摩尔线程 天数智芯 壁仞科技 寒武纪 NVIDIA AMD Google Intel Microsoft Tesla
推理芯片
海光信息 寒武纪 沐曦 天数智芯 壁仞科技 燧原科技 昆仑芯 云天励飞 平头哥 摩尔线程 华为 NVIDIA Intel Meta Amazon Microsoft
服务器
联想 浪潮信息 中科曙光 新华三 华为 超聚变 宝德计算 宁畅 长城超云 Fujitsu Atos IBM Dell HPE
智算中心
商汤科技人工智能计算中心 鹏城云脑 腾讯智慧产业长三角智算中心 百度智能云·昆仑芯智算中心 张江智算中心 武汉人工智能计算中心 合肥先进计算中心 北京昇腾人工智能计算中心 深圳市智能计算中心 广州人工智能公共算力中心 昆明人工智能计算中心 贵安新区智算中心 西安未来人工智能计算中心 哈尔滨人工智能先进计算中心 中贝合肥智算中心 郑州人工智能计算中心 北京人工智能公共算力平台 北京数字经济算力中心
云服务
阿里云 腾讯云 百度智能云 金山云 天翼云 京东云 华为云 移动云 Microsoft Azure Google Cloud AWS CoreWeave
词元服务
硅基流动 PPIO派欧云 七牛云 Together AI Fireworks AI DeepInfra OpenRouter
安全
AI应用安全
奇安信网神 中国工业互联网研究院 安恒信息 360数字安全 天融信 启明星辰 深信服 绿盟科技 数美科技 亚信安全 网易易盾 顶象 腾讯安全 瑞莱智慧 君同未来 中科睿鉴 Adversa AI 长亭科技 Tenable Mindgard
模型安全
瑞莱智慧 奇安信网神 长亭科技 安恒信息 绿盟科技 深信服 数美科技 亚信安全 Microsoft Google Cloud NVIDIA Palo Alto Networks
开发框架安全
奇安信网神 360数字安全 安恒信息 绿盟科技 瑞莱智慧 Microsoft Google Cloud Cisco Trend Micro HiddenLayer
数据安全
阿里云 腾讯云 百度智能云 蚂蚁集团 瑞莱智慧 Microsoft Azure AWS Google Cloud
算力安全
海光信息 飞腾信息 华为 紫光同芯 华大电子 国民技术 紫光展锐 Intel AMD NVIDIA Arm IBM
数据来源：人工智能赋能新型工业化供需对接服务平台（https://ai-bridge.cn）
浅灰粉底：国外企业

图 2 “AI+制造”产业图谱

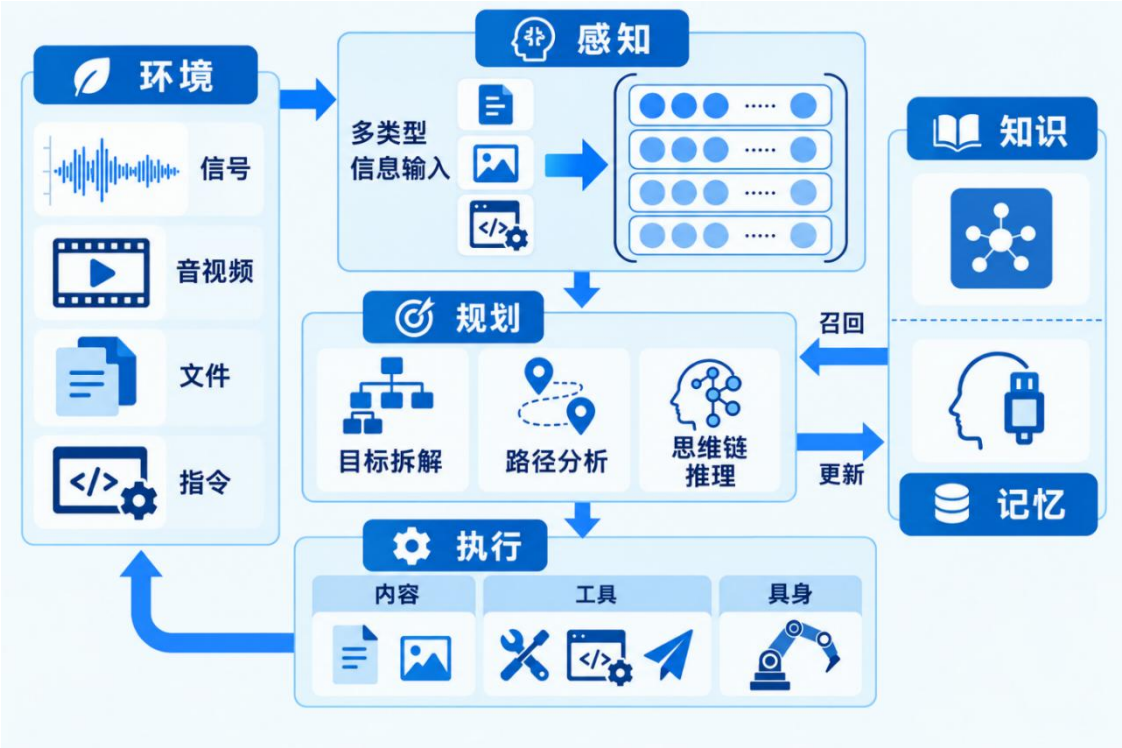

图 3 典型工业智能体运行模式

图 3 展示了工业智能体的典型运行模式，具体包括任务理解、规划决策、能力调用、执行反馈等环节。

工业智能体将迈进全自主协同与规模化应用的发展新阶段。**一是从应用进程看，**工业智能体由知识辅助向生产协同和受控闭环演进。当前工业智能体多承担知识检索、方案建议等辅助性功能，尚未直接融入生产控制环节。下一步，可完成闭环运行的工业智能体将直接对接工业生产各环节，输出可落地执行的任务结果。与传统工业自动化系统相比，工业智能体具备更强的环境适应能力与自主决策能力，能够在既定安全边界内适配多变的工业场景，解决传统程序难以

覆盖的不确定生产任务，同时保持任务推进过程可控，确保自主决策符合工业安全生产要求。**二是从产品供给看，**工业智能体将由单点应用向平台化、专业化、软硬一体化方向演进。随着技术底座的持续成熟，将涌现一批面向工业场景的基础平台，支撑不同行业、不同环节工业智能体的快速开发、灵活部署；同时将分化形成一批深耕细分领域的专业化工业智能体供应商，依托对行业知识和场景需求的深度积累，打造针对性更强、落地效果更优的产品，软硬一体化集成交付模式将进一步普及，有效降低工业企业应用门槛。**三是从生态构建看，**工业智能体将从单一主体开发向多主体协同共创方向演进。工业场景具有高度复杂性，单一主体难以覆盖全链条技术研发和需求响应。未来将逐步形成由底层算力提供商、基础模型开发商、工业知识服务商、系统集成商和终端工业企业共同参与的协同创新生态，各主体充分发挥自身优势，协同推进工业智能体的技术研发、测试验证与迭代优化，共同推动工业智能体在更大范围、更深层次实现落地应用。

第二章 工业智能体体系架构

工业智能体体系架构是人工智能深度融入制造业体系的顶层设计框架，其核心在于围绕订单、产能、质量、能耗、安全等生产目标与约束边界，明确智能体的作用层级、技术基座、协同机制、部署模式、演进路径及治理范畴。本章从产业、功能以及运行视角对工业智能体体系架构进行阐述，覆盖设备单元、产线、车间、工厂、企业、生态六个层级，清晰界定不同层级工业智能体的应用场域与功能定位，解析工业智能体的技术支撑体系与闭环运行机制。六层体系架构实现了工业智能体数据自生产现场向上逐层汇聚、知识沉淀动态更新、模型自上而下按需调度赋能、任务指令与执行反馈在层级间双向交互的协同运行模式。

一、产业体系

工业智能体产业体系按照制造组织和控制对象划分为一个自下而上、贯穿 OT（控制技术）与 IT（信息技术）的“六级架构”，图 4 展示了六个层级及其上下联动的总体运行关系。

图 4 工业智能体产业体系运行机理

L1 设备单元层位于端侧，承担终端执行，通过嵌入式 AI 实现单体设备的智能化。

L2 产线层位于边侧，侧重近端控制，实现产线级的协同与排产优化。

L3 车间层位于边侧，侧重边缘自治，实现车间内物料、人员、设备的智能调度。

L4 工厂层依托企业私有云，统筹工厂级资源，实现工厂级的全局资源优化与智慧运营。

L5 企业层依托企业公有云，打通研发、生产、供应链等数据，实现企业级的智能决策。

L6 生态层依托工业互联网平台，实现产业链上下游的高效协同与价值共创。

每一级均由数据、算力、模型、网络等构成场景赋能基础，并通过向上的数据汇聚和向下的模型调度形成层间联系，表 1 总结了六级体系在六类技术维度上的功能配置。

表 1 工业智能体六级体系功能配置

层级	数据	算力	模型	网络	安全	自进化
L1 设备单元	汇集设备运行、部件状态、仪表和传感器数据	配置智能传感器、边缘计算模块和嵌入式 AI 芯片，端侧终端执行采用低于 500 GFLOPS 的超小规模 AI 算力	部署端侧时序小模型、设备本体与机理模型、寿命预测模型，支撑故障诊断、寿命预测、工艺优化和微秒至毫秒级高频推理	采用工业总线、OPC UA、5G 专网、Wi-Fi 和设备标识解析	开展设备完整性校验、传感器加密和工业协议检测	设备与传感器反馈回流数据集，经训练微调更新端侧小模型和知识库
L2 产线	汇集控制系统、工艺参数、程序代码、日志和网络参数数据	配置云化 PLC/DCS、TSN 交换机和边缘控制器，边侧近端控制采用约 500 GFLOPS 至 10 TFLOPS 的小规模 AI 算力	部署视觉质检、多变量工艺映射、强化学习控制等小模型及边缘侧大模型，支撑异常检测、能耗计算、生产指令与产线工控代码生成和秒级自适应调控	采用工业以太网、TSN/DetNet 确定性网络和设备协同通信	实施指令加密传输、产线网络隔离、工控安全漏洞扫描和实时异常拦截	控制、代码、日志及网络参数向上汇聚，经训练微调更新产线小模型和边缘侧大模型
L3 车间	汇集产线管理、物料流转、生产计划和仓储库存数据	配置边缘云、智能仓储设备（如 AGV/AMR）、工业视觉和能耗监测终端，边侧自治采用约 500 GFLOPS 至 10 TFLOPS 的小规模 AI 算力	部署运筹优化、混合启发式排产、能效基线和车间数字孪生模型，支撑物料调度、工艺优化、计划排程和仓储优化	采用车间局域网、多协议网关和物料流转追溯网络	实施数据分级防护、作业权限管控、设备接入认证和操作行为审计	生产计划、物料及仓储反馈形成车间知识，经训练微调更新排程和优化模型

层级	数据	算力	模型	网络	安全	自进化
L4 工厂	汇集管理、工艺、作业过程、物料、生产计划、工业技术、安全环保和产品质量数据	建设企业云和数字孪生平台，以企业私有云承载约 10 TFLOPS 至 1 PFLOPS 的中规模 AI 算力	部署工厂级数字孪生、全局时序预测、多模态安防大模型和约束传播排产模型，支撑智能排产、云端大模型资源协同、仓储优化、产能调度和风险管控	采用算网控一体化网络、工业 PON 和 SD-WAN	实施零信任访问、工厂网络切片隔离、数据全生命周期加密和安全态势感知	工厂数据向企业层汇聚，工厂模型接受上层调度，并以场景运行结果持续更新知识库
L5 企业	汇集人力、财务、研发、采购、销售、成本和供应链数据	建设企业云、跨域大数据中台和 AI 原生生产平台，以企业公有云承载约 1 至 10 PFLOPS 的大规模 AI 算力	部署企业通用大语言模型、NLP 语义理解、供应链预测和企业分析知识图谱模型，结合小模型开展精准计算与数据校核，支撑经营策略、归因分析、利润预测、财务管理、供应链分配和协同决策	采用企业骨干网、跨互联网和供应链协同通信网络	实施数据分层保护、跨系统访问审计、隐私计算和核心数据脱敏	企业数据向生态层汇聚，企业模型接受生态层调度，并将经营反馈用于训练微调和场景赋能

层级	数据	算力	模型	网络	安全	自进化
L6 生态	汇集联合研发、协同策略、管理和碳排放数据	建设产业云和可信数据空间，支撑行业大模型训练及平台协同，配置 10 PFLOPS 以上超大规模 AI 算力	部署行业垂直大模型、生成式 AI 研发大模型（新材料、新药生成）、联邦学习和宏观市场预测模型，支撑供需匹配、供应链协同、产业链及碳排放管理	采用广域确定性网络、产业级标识解析和智能体交互协议	实施跨企业可信数据流通、智能体交互认证、产业级威胁情报共享和区块链存证溯源	协同数据形成生态知识库，训练微调行业大模型，并向企业层调度模型、向生态场景输出能力

二、功能体系

从功能视角来看，“六级架构”严格按照任务半径、响应时限及责任边界实施分层构建。其中，设备与产线层聚焦现场快速响应需求，车间与工厂层统筹生产资源配置，企业与生态层负责经营管理及产业协同；体系运行遵循“上下联动、权责清晰”原则，上层向下层输出目标任务、约束条件及模型支撑能力，下层向上层反馈运行状态、执行结果及风险信息。

L1 设备单元构成最小生产单元的感知与受控执行闭环。端侧配备智能传感器、边缘计算模块与嵌入式 AI 芯片，可用 AI 算力低于 500 GFLOPS，模型规模与推理时延均受超小规模算力约束。其以设备和传感器数据为依据，调用端侧小模型开展故障诊断、寿命预测与工艺优化，并由设备控制系统完成确定性执行。例如，某机加工设备的振动信号持续偏离正常区间，设备智能体综合当前转速与历史状态判断轴承劣化趋势，形成检修建议并触发维护任务；若需调整运行参数，仅在既定工艺窗口和安全联锁范围内执行。该层的职责是将设备真实状态转化为可用能力，而非以概率性判断取代现场控制。

L2 产线构建多设备、多工序的近端协同闭环。产线层汇集控制系统、工艺参数、程序代码及运行日志，依托云化 PLC/DCS、TSN 交换机与边缘控制器提供的 500 GFLOPS 至 10 TFLOPS 小规模 AI 算力，调用视觉质检、工艺映射、强化学习控制等小模型及边缘侧大模型，承担异常检测、生产

指令生成与产线自适应调控任务。例如，某装配线末端检测连续发现紧固偏差，产线智能体追溯前序工位参数与设备日志，生成节拍调整与代码修改建议，经校核后在局部工位试点实施，并持续跟踪后续质量结果。该层级的定位为围绕整线生产目标协调单机运行行为，避免单台设备最优运行造成整线生产失衡。

L3 车间构建多产线、多资源的边缘自治闭环。车间层整合生产计划、物料流转与仓储库存数据，依托边缘云以及AGV/AMR、工业视觉和能耗监测终端，在 500 GFLOPS 至 10 TFLOPS 的小规模算力范围内调用排程、能效和车间数字孪生模型，承担物料调度、工艺优化、计划排程和仓储优化任务。例如，某车间临时接入一批紧急订单，同时一台关键设备停机，车间智能体根据各产线生产能力、物料齐套情况与仓储位置重新排布生产任务，协调运输设备调整送料顺序，并将无法在当班内消化的产能冲突上报工厂层。该层级的定位为在完整工艺单元内平衡多项目标，赋予现场受约束的局部自治能力。

L4 工厂构建跨车间、面向订单交付的全厂协同闭环。工厂层汇集管理、工艺、作业过程、物料和生产计划等数据，以企业私有云和数字孪生平台为载体，依托 10 TFLOPS 至 1 PFLOPS 的中规模 AI 算力，调用工厂数字孪生、全局预测和排产模型，承担资源协同、能耗优化、产能调度和风险管控任务。例如，某工厂关键设备突发停机并影响一批重点订单，工厂智能体基于各车间负荷与物料状态生成转产方案，通过

数字孪生比对交期、产能和能耗影响，经审批后向相关车间下达增量调整任务。该层级的定位为形成全厂可执行的整体方案，同时接收车间和产线反馈的可行性意见。

L5 企业构建贯通经营与生产的企业级决策闭环。企业层汇集人力、财务、研发、采购、销售、成本和供应链数据，依托企业公有云、跨域大数据中台和 AI 原生生产平台配置的 1 至 10 PFLOPS 大规模 AI 算力，协同小模型与云端大模型开展精准计算、数据校核、经营策略分析和归因分析，承担利润预测、财务及供应链管理任务。例如，某企业核心原料供应周期突然延长，企业智能体整合库存、订单、采购成本和各工厂产能，比对替代采购、跨厂调拨和交付调整方案，经管理流程审定后向工厂分解生产约束要求。该层级的定位为将经营目标转化为制造任务，同时将生产状态转化为经营决策依据。

L6 生态构建跨企业、跨平台的产业协同闭环。该层级依托工业互联网平台，以产业云和可信数据空间为底座，配置 10 PFLOPS 以上的超大规模 AI 算力支撑行业大模型训练及平台协同，汇集经授权的联合研发、协同策略、管理和碳排放数据，调用行业大模型开展供需匹配、供应链协同、产业链管理和碳排放管理。例如，某区域出现关键材料阶段性短缺，生态智能体根据参与主体授权发布的需求、可用产能和物流条件形成供需匹配方案，协调各企业智能体确认交付承诺，各企业再在本单位系统内完成审批和执行。该层级的定

位为在保障各主体自主地位的前提下形成可验证协同，不直接越级控制企业内部生产设备。

三、运行体系

为保障六级智能体协同高效运转，需通过目标、状态、模型、事件四类核心要素在层级间的规范有序流转，统筹构建工业智能体运行体系。

目标与约束实行自上而下逐级分解。订单、产能、质量、能耗及安全等生产目标，由企业与生态层制定，向下逐步转化为可执行的具体任务。企业智能体将经营目标分解为各工厂的交付指标与成本红线，工厂智能体细化为各车间的资源调配策略与排产计划，车间智能体据此制定产线节拍与工单顺序，产线智能体将调整要求落地为具体工位的参数建议。

状态与知识实行自下而上逐级汇聚。设备运行状态形成产线能力画像，产线能力构成车间产能，车间产能汇总形成工厂交付能力，进而支撑企业经营研判与产业供需分析。状态向上汇聚的同时沉淀为各级知识：设备层积累故障类型与维护经验，车间层沉淀排程规则与工艺边界，企业层归纳成本结构与市场规律。知识库随运行持续更新，反向强化本级智能体的判断力。

模型与能力实行纵向双向调度。模型作为可调度的能力资源在“六级架构”内双向流动。生态层训练的大模型与企业层沉淀的经营分析模型面向场景向下部署，赋能工厂、车间具体业务；边端小模型运行产生的新样本与效果数据向上回流，推动上层模型持续迭代优化。模型配置与任务性质相匹

配：越贴近现场，模型规模越小、响应越快，侧重诊断与实时调控；越向上延伸，模型知识越综合，侧重推演、归因与策略生成。

事件与反馈实行逐级双向传递。日常运行中各层级闭环自治，层间交互主要由事件触发。设备劣化由设备智能体在工艺窗口内自行调整，超出范围则上交产线层评估；产线层无法在节拍内消解的偏差升级至车间层重排；车间层无法承接的产能冲突上报工厂层；工厂层难以化解的供应风险再传递至企业层统筹。事件沿层级逐级扩大处置范围，方案也随之逐级校验，涉及安全联锁和高风险变更的操作须报批后执行。

第三章 工业智能体核心技术

工业智能体的核心技术构成相互支撑、协同运行的工程体系。如图 5 所示，面向生产管控，技术体系以订单、产能、质量、能耗和安全为生产目标与约束，围绕数据、算力、模型、可信安全治理、网络和自进化组织技术能力贯穿全链条。工业数据、业务数据、设备数据和现场数据驱动体系运行，执行反馈回流数据侧形成业务闭环。

数据层按照“多源连接—事件统一—知识关联—虚实映射”组织语义底座，将分散数据转化为对象清晰、语义一致的可信事实。**算力层**依据时延、可靠性、能耗、数据域和风险等级，将训练与全局优化、低时延推理和确定性执行合理部署于云、边、端，通过容器化、弹性伸缩、断网自治和灰度发布保障运行。**模型层**遵循“认知可以概率化、执行必须

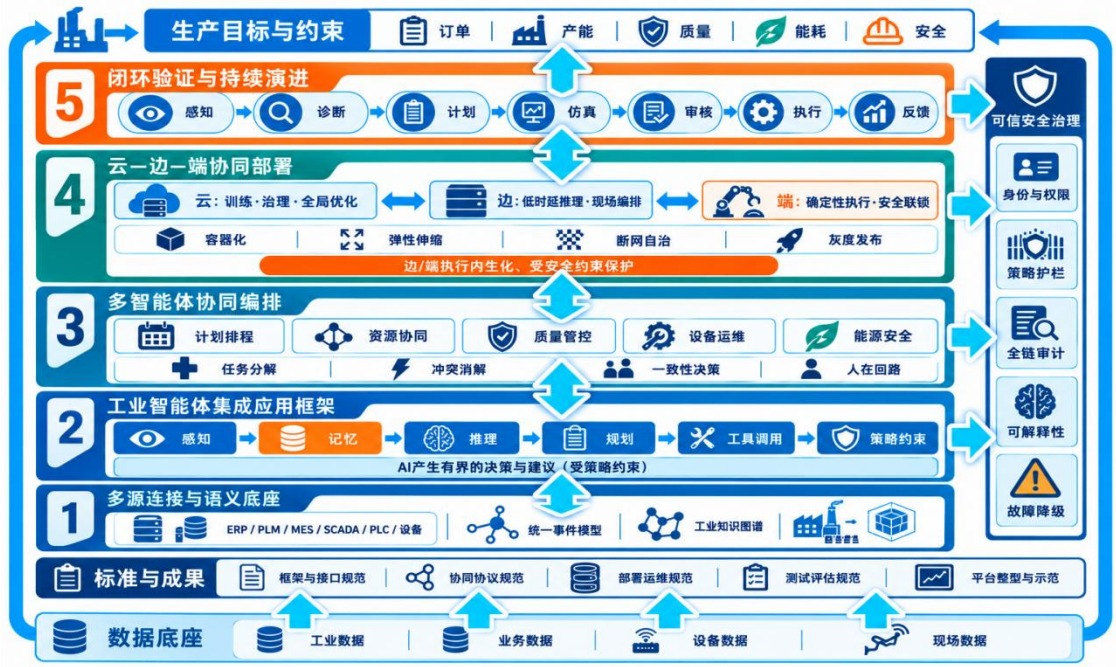

图 5 工业智能体技术体系

受约束”的原则，集成感知、记忆、推理、规划、工具调用和策略约束，将模型生成能力转化为具有输入依据、过程状态和调用边界的工业任务能力。**网络层**围绕计划排程、资源协同、质量管控、设备运维和能源安全五类专业智能体，通过任务分解、冲突消解、一致性决策和人在回路组织协同，在共同目标下明确分工、同步状态并落实责任。**安全层**以身份权限、策略护栏、全链审计、可解释性和故障降级贯穿全过程，使权限责任匹配，坚持安全与能力同步设计，将智能行为限定在可信边界内。**自进化层**按感知、诊断、计划、仿真、审批、执行、反馈组织验证改进，将仿真和审批置于计划与执行之间，隔离模型方案与真实生产动作，保障智能能力受控运行，模型和策略更新须验证，现场执行不得绕过确定性控制与安全联锁。

一、数据：多源连接与语义底座构建

数据是工业智能体的基础。多源连接汇聚系统与设备数据，统一事件模型提供一致的结构与语义表达，工业知识图谱建立语义关联，数字孪生融合数据与机理实现状态映射和仿真。四个环节相互衔接，将分散数据转化为机器可理解、可推理、可仿真的语义资产，为上层智能体提供统一的认知底座。图 6 表示了数据、知识、模型与机理之间的协同转换关系。

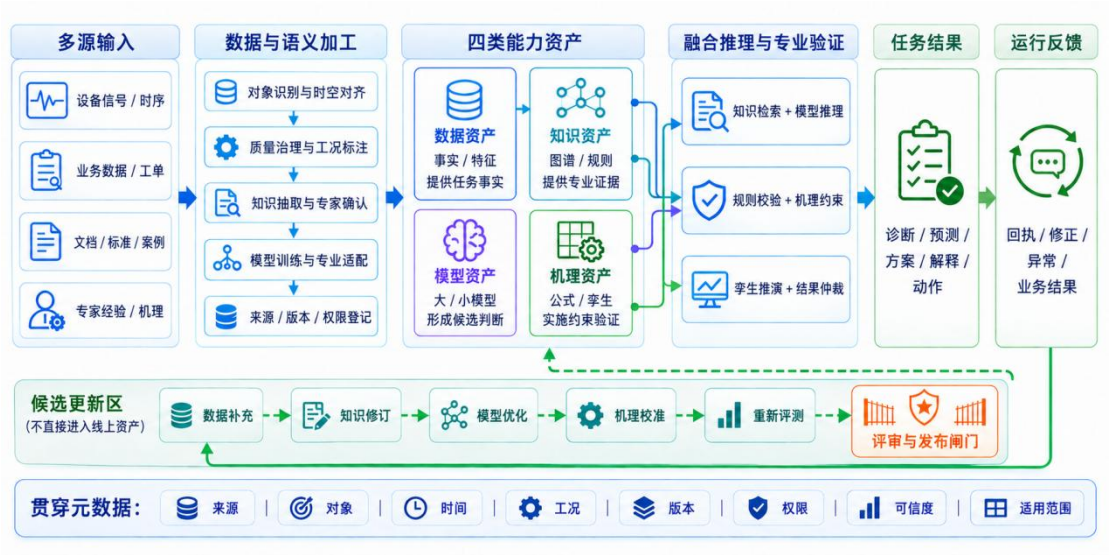

图 6 数据、知识、模型、机理协同转换

（一）多系统与现场设备多源连接

多源连接模块为工业现场与业务系统提供数据接入支撑。其中控制技术（OT）侧以边缘网关为核心枢纽，通过插件化组件完成对 OPC UA、Modbus 等各类工业协议的适配，并借助 MQTT 等通信通道实现实时数据的汇聚；信息技术（IT）侧则依托 API 网关完成业务接口对接，由消息中间件承担数据流转任务，通过变更数据捕获技术实时感知 ERP、PLM、MES 等系统中的记录变更，针对遗留系统则依托企业服务总线完成服务化对接。存储层面，采用时序数据库存储高频测点数据，依托数据湖留存原始数据，为后续的数据处理环节提供连续且可追溯的数据输入。

在工程实施阶段，首先完成设备资产梳理与统一编码，确保数据点均可追溯至对应的物理对象；对接入组件采用协议插件注册与版本管理机制，为审计与升级提供支持；针对采集链路，需实现断点续传、边缘压缩与异常值过滤功能，

针对接口配置限流与重连重试机制。系统运行阶段，以连接可用率作为核心监控指标，结合分级告警机制保障采集链路的稳定运行。

（二）统一事件模型构建

统一事件模型可为异构数据构建一致性业务表达框架，其技术核心为事件驱动架构，采用时间戳、对象标识、属性、值、事件源五元组完成事件描述，使异源数据具备统一的数据结构。依托 Flink CEP 等复杂事件处理引擎，可完成跨测点、跨时段的事件模式识别，将离散数据组织为具备明确业务含义的复合事件。事件模式注册中心实现事件定义与版本的集中管控，结合主数据管理完成语义标注，统一设备、物料、工单等对象的口径规范，为跨系统分析与协同提供支撑。

统一事件模型承接标准化数据流后，依次完成清洗对齐、语义标注与事件注册处理，随后发布至事件总线，为知识图谱与数字孪生提供数据输入，并向各智能体输出统一的事件表达。上层应用可通过事件订阅获取所需信息，无需对原始报文进行重复解析，即可在统一的对象标识与业务语义框架下开展任务处理。事件处理环节需完成统一时标对齐与钟差校正，解决多系统时钟不同步引发的时序错乱问题，同时建立设备、物料、工单的统一编码映射关系。事件按照设备级、工艺级、业务级三个层级开展分级管理，匹配差异化的处理优先级与消费对象。处理链路支持事件去重、保序与回放功能，配套版本管理机制，可保证事件定义的迭代更新不对现有消费方造成干扰。

（三）工业知识图谱

工业知识图谱通过本体建模、知识抽取与融合构建多源对象语义关联，为工业场景推理任务提供支撑。行业专家基于资源描述框架与 Web 本体语言定义设备、工艺、物料、工单、故障及应对措施等核心概念与关系模式；大语言模型从非结构化文档与事件流中抽取实体与关系，经规则校验满足本体约束；知识融合与实体对齐消除异名问题后，结构化知识存入图数据库。统一事件模型持续提供动态输入，推动生产事件沉淀为语义关联。工业知识图谱可实现关联推理，采用基于图结构的检索增强生成（GraphRAG）方法，并按场景结合图检索与向量检索，向大语言模型提供结构化知识，满足精确关系查询与语义匹配需求。

工业知识图谱采用“专家定本体、模型抽实例”的增量迭代路线构建，先经小范围高频场景验证，再逐步扩展至全厂。每条知识记录来源、置信度与时效性，低置信度知识，经人工复核方可作为决策依据。知识图谱采用增量更新与版本管理，保留完整知识变更记录，既保证检索与推理结果可追溯，也使图谱内容与生产过程变化保持同步。

（四）数字孪生映射

数字孪生融合现场监测数据、事件信息、工业知识与机理模型，可为工业系统提供物理状态映射与仿真验证能力。孪生体按几何、行为、规则维度分层建模，分别刻画装备结构空间关系、系统运行规律及操作约束边界。针对机理复杂、计算复杂度高的对象，可采用模型降阶与代理模型技术，平

衡模型保真度与计算实时性。运行阶段，孪生体以实时工业数据驱动状态更新，通过模型修正缩小仿真与实测偏差；对外以标准化 API 封装状态查询与方案推演服务，为工业智能体提供可调用的仿真验证能力。

统一事件模型为孪生对象提供动态状态更新，工业知识图谱补充对象关联与业务约束，机理模型支撑行为仿真，三者协同构建与物理生产过程耦合的数字映射，为决策闭环验证提供仿真环境，为规划模块提供方案试验条件，支撑“先仿真推演、后物理执行”的作业模式。孪生映射采用机理与数据双驱动校正，定期用实测数据完成精度验证。孪生体编码与统一事件模型对齐，保障事件准确映射至对应对象。孪生服务采用目录化管理与 API 化封装，明确输入输出规范、精度等级与调用配额，可供上层工业智能体按需调用。

二、算力：云边端协同部署

工业智能体的算力体系按云－边－端三级分层架构组织，依托容器化部署、弹性资源调度、断网自治与灰度发布支撑协同运行。云侧承载模型训练、数据治理与全局优化，边侧承担低时延推理与现场编排，端侧聚焦确定性执行与安全联锁管控。三个层级依任务时延、资源条件与风险等级分工，构建从模型训练到现场执行的任务链路，以边端执行稳定性与安全联锁保护为运行底线。

（一）云侧：模型训练、数据治理与全局优化

云侧是承载模型训练、数据治理与全局优化的核心中枢，训练基础设施以 GPU 集群为核心，依托数据并行、模型并行

等分布式技术支撑预训练与工业场景微调，将数据处理、参数优化、评测对比组织为标准化训练流水线。数据治理与标注平台加工语义底座汇聚的原始数据生成标准化训练集，通过人机协同平衡标注效率与质量。模型注册中心对训练的模型实行版本化管理，记录训练数据集、参数配置与评测结果。跨厂区多基地场景可采用联邦学习聚合各基地模型更新，在保障各基地数据本地留存的前提下完成全局模型优化。

云侧通过专用模型下发通道连接边侧，向边、端输出验证合格的模型与全局优化策略，基于各厂区回传数据滚动开展全局优化，校准产能分配、能耗配额等参数，保持优化结果与现场约束适配。训练数据全链路实行血缘管理，确保模型版本可追溯至原始数据来源与加工流程。模型需通过性能评测与安全验证方可发布，未通过验证的版本禁止上线。全局优化任务按预设周期滚动执行，优化策略投入执行前需在边侧完成合法性与本地约束校验，避免全局方案与现场冲突。

（二）边侧：低时延推理与现场编排

边侧是云侧能力与现场任务的衔接单元，承担低时延推理与现场编排的核心功能。为适配边侧有限硬件资源，模型需通过量化、剪枝、知识蒸馏等压缩算法完成结构优化，再由边缘推理引擎完成算子融合与执行性能优化，满足目标场景时延约束。边缘智能体运行时承担本地任务调度，可在云侧失联时维持现场编排能力。边缘一体机与多接入边缘计算节点为车间提供就近算力，模型规模与部署方案需根据计算负载、硬件资源条件以及系统可靠性要求适配调整。

边侧就近处理时延敏感型任务，可降低系统对远程网络传输的依赖，同时为端侧设备提供本地化决策支撑。云边任务划分综合时延约束、算力条件与安全需求：云侧集中承担模型训练与全局性计算，边侧在本地约束下完成推理计算与任务执行。模型可依据计算负载与时延敏感度做云边切分部署，时延敏感模块驻留边缘侧，其余模块依托云边协同计算。边侧将现场样本加工为增量训练数据，回流云侧支撑后续模型训练与性能评估。所有边缘节点纳入统一监控，以算力利用率与推理排队时延作为边缘侧容量规划的核心依据。

（三）端侧：确定性执行与安全联锁

端侧智能体承担就地感知、轻量化推理与受控任务执行功能，涉及实时控制与安全保护的动作由确定性控制系统与独立联锁机制保障。实时操作系统与工业控制器按确定周期执行指令，PLC 与 DCS 对接组件将上层决策转换为控制指令。安全仪表系统与硬件联锁独立于人工智能模型运行，智能体失效时按预设逻辑执行保护操作。指令下发配套回读校验，确认接收结果，结合现场反馈核验执行状态。

端侧仅执行经授权与策略校验的受控指令，高风险动作需满足审批要求。端侧权限范围与具体任务匹配，模型推理结果不得直接覆盖原有控制逻辑或安全联锁机制，保障现场执行稳定可靠。指令白名单与限值约束限定端侧可执行范围，越界指令直接拒绝执行。关键指令采用双通道比对，辅以看门狗技术监测，比对不一致时中止操作。联锁触发后系统进

入预定义安全状态，无需等待上层指令。运行阶段持续监测心跳、超时与抖动指标，异常波动及时告警排查。

（四）协同部署与弹性运维技术

云边端协同架构建立在分层异构硬件基础设施之上。**云侧**依托配有人工智能加速卡的计算集群完成模型训练与全局优化，通过高速互连与分布式存储支撑数据供给与集群调度；**边缘侧**通过车间附近的边缘计算设备或工业级服务器，满足就近推理与环境适配需求；**端侧**通过工业控制器、安全仪表系统等专用硬件保障控制确定性。三层架构按任务负载与运行约束配置资源，为模型与策略部署提供物理支撑。

容器化与编排技术在异构硬件之上构建统一应用交付与运维通道。Kubernetes 等编排框架结合边缘扩展组件，支撑云边侧应用部署；符合条件的端侧节点可采用容器化交付，确定性控制与安全联锁独立运行。编排系统通过资源标识与池化管理感知异构资源，按任务需求分配算力；弹性伸缩结合负载监测、节点扩缩与负载均衡，动态调整资源供给；断网自治依托本地环境与预设规则，云端失联时维持授权范围内现场任务运行，网络恢复后补传数据、核对状态；灰度发布采用分批上线、金丝雀或蓝绿切换策略，配合模型 A/B 测试管控更新风险；可观测性体系汇聚日志、指标与链路追踪数据，结合硬件健康状态生成统一运维视图，支撑模型、策略与配置的受控下发和稳定运行。云边端架构统一管理镜像与配置版本，降低环境漂移；通过健康检测、故障隔离与任务迁移管控节点失效影响。断网场景预设本地规则接管与降

产品类型	支持模型参数	应用场景
机房级一体机	支持Deepseek、ChatGLM、Qwen等系列 **800B级别**全精度模型	**L6：生态级智能体** □ 生态人才培训智能体 **L5：企业级智能体** □ 企业内部应用工具开发智能体 □ 生产经营分析智能体 □ 业财审计监管智能体
办公室/企业级一体机	支持Deepseek、ChatGLM、Qwen等系列 **1.6T级别**量化模型	**L4&L3：工厂/产线级智能体** □ 关键工艺参数调优智能体 □ 工程制图智能体 □ 物流物料调配智能体 □ 企业内部应用工具开发智能体
桌面/线边级一体机	支持Deepseek、ChatGLM、Qwen等系列 **200B级别**量化模型	**L2：产线智能体** □ 关键工艺参数调优智能体 **L1：设备单元智能体** □ 设备装备运维智能体 □ 通用电机与减速机故障预测与健康管理智能体

图 7 工业智能体一体机产品

级预案，网络恢复后核对数据与任务状态；版本发布采用分批灰度并保留回滚能力，发布流程与安全验证联动，确保新版本不绕过联锁验证直接投产。

（五）工业智能体一体机

聚焦工业企业智能体应用需求，工业智能体一体机在保证“数据不出域”的安全前提下，可实现开箱即用的本地化智能体调用。工业智能体应用场景横跨多行业、纵跨多层级应用需求，双维度定义工业智能体的承载形态与模型参数规模需求。如图 7 所示，市面上主流的一体机硬件形态分类为云侧、边侧、端侧三大类，对应集成不同参数规模的大模型本地化运行，支撑多种应用形态的工业智能体。

边侧一体机聚焦设备单元、产线以及部分车间级工业智能体的应用，支持关键工艺参数调优、设备装备运维等场景的智能体运行。该类一体机体积小，适合用于桌面或线边的场景，满足小参数规模、量化模型的本地化运行。

端侧一体机聚焦车间/工厂级，以及部分产线级和企业级的智能体应用，支持关键工艺参数调优、工程制图辅助、物

流物料调配、企业内部应用工具开发等场景的智能体运行。该类一体机体积适中，满足中度以上的智能体并发量，适用于办公室或企业级场景，通常无需专人维护，满足全参数规模、量化模型的本地化运行。

云侧一体机聚焦工厂级、企业级和生态级工业智能体应用，支持生态人才培训、生产经营分析、业财审计监管等场景的智能体运行。该类一体机的体积、功耗仅适合在专用机房中使用，支持高强度应用并发量和高精度模型应用，满足全参数规模、高精度模型的本地化运行。

三、模型：单智能体集成应用

单智能体是工业智能体体系的基本任务单元，内部集成感知、记忆、推理、规划、工具调用和策略约束六项能力。感知与记忆提供情境和经验，推理与规划形成方案，工具调用连接业务系统与现场设备，策略约束统一校验决策和动作，使任务在明确的权限与安全边界内运行。

（一）感知：工业多模态感知与情境理解

多模态大模型协同视觉模型与时序模型，处理文本工单、现场图像及设备时序数据等多源异构信息。工业视觉检测模块完成表面缺陷、装配完整性判定，时序异常检测模块提取识别测点时序曲线中的异常信号。感知模块从数据交互层获

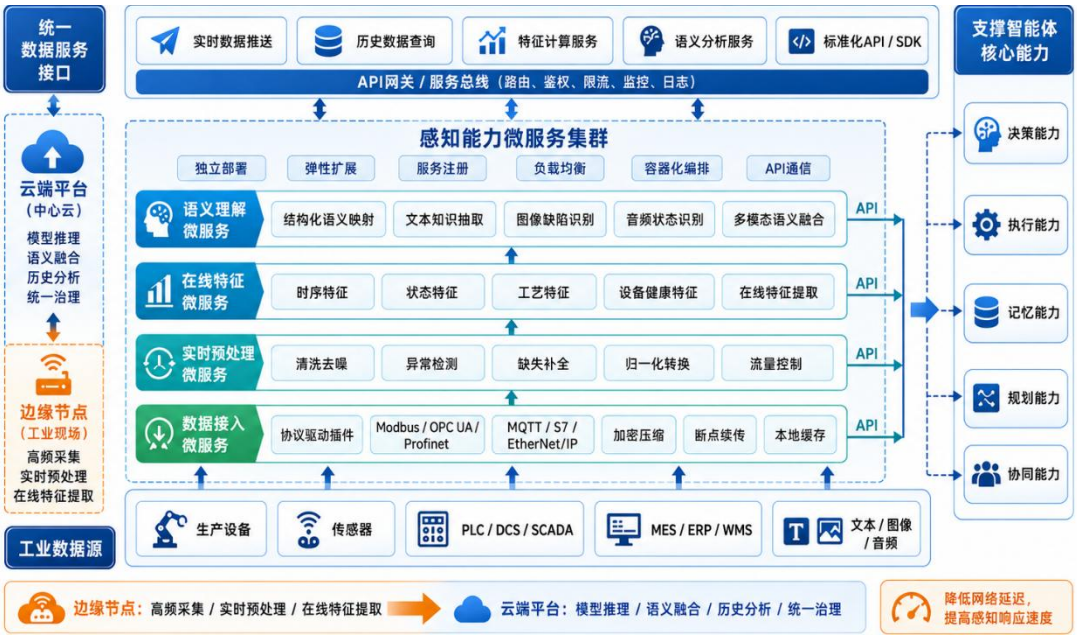

图 8 感知推理封装

取现场事件流与数字孪生状态信息，依托上下文工程按任务需求订阅信息，将多模态输入对齐至统一时空基准，生成结构化情境描述输出至记忆与推理环节。视觉数据由目标检测模型标注缺陷类别与位置，时序数据由嵌入模块编码为低维稠密特征向量，事件订阅结合注意力过滤突出任务相关信息特征。感知输出附带置信度标注，可为下游环节判断信息采信程度提供量化依据。图 8 展示了感知能力的封装及其与上下游能力模块的协同关系。

（二）记忆：分层工业记忆体系

跨工单、跨班次与跨场景的经验复用，依赖层级化组织的记忆体系。瞬时记忆承接当前任务输入，短期记忆依托上下文窗口与会话状态维持任务连续性，长期记忆采用向量库与知识图谱双存储架构，分别承载经验片段语义关联与实体精确关联关系。长期记忆按内容划分为情景记忆、程序记忆

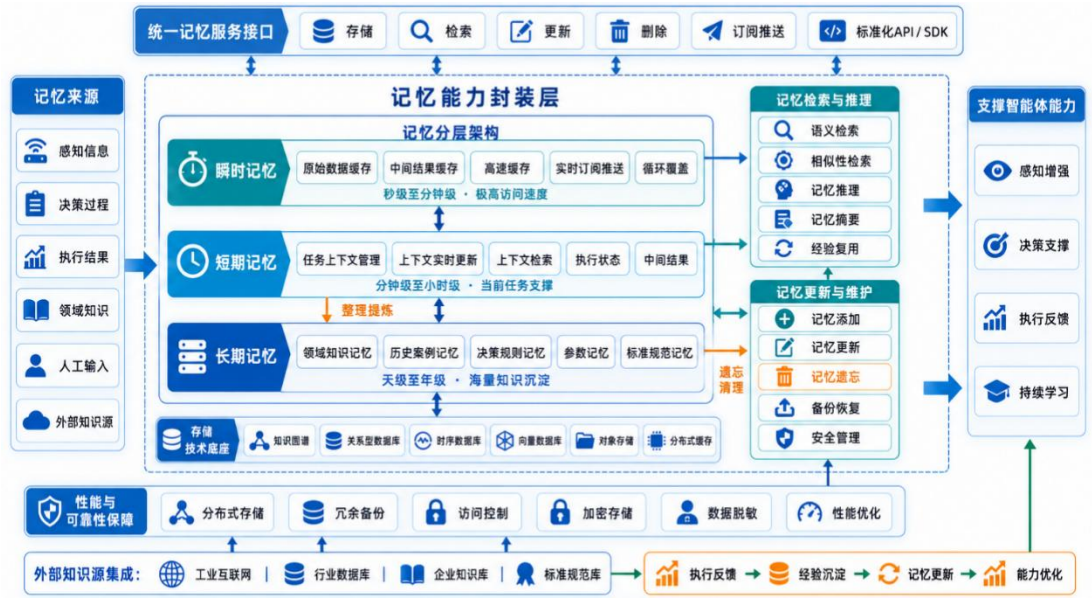

图 9 记忆能力封装

与语义记忆，配套巩固与遗忘机制动态控制存储规模。记忆模块接收感知输出的情境信息与任务结论，为推理环节提供经验支撑与背景知识，通过分片写入、索引管理及向量、图与关键词混合检索完成记忆调用，以重要性评分驱动记忆巩固、降权与更新。图 9 展示了分层工业记忆的组织、存储与调用关系。

（三）推理：大模型与工业知识混合推理

推理环节依托思维链与自反思构建多步分析，将知识图谱与文档库中的工业知识引入推理上下文，通过因果推理区分相关性与因果性，开展异常归因分析。机理模型为推理提供物理约束，校核违背运行规律的结论；不符合约束的判断需中止向规划环节传递，返回推理模块修正后重新校核，或转交人工复核。推理模块接收感知情境与记忆经验，完成归因分析与趋势判断后，将结论传递至规划环节。本模块采用 LoRA 领域微调与工业提示模板提升专业适配性，通过数据

与机理双轨校核验证结论，输出需标注证据来源、适用条件与校核结果，为后续任务规划与人工复核提供支撑。

（四）规划：约束感知的任务规划与动态重规划

规划环节以层次任务网络将高层目标分解为可执行子任务，通过多目标优化权衡产能、质量、能耗等指标，复杂排程与调度任务交由 APS 等专业排程工具和运筹求解器计算。规划模块承接推理结论，生成可调用的动作序列，输出方案需满足生产目标与约束，明确任务依赖与资源要求。本环节通过显式约束建模、方案评分与回溯剪枝筛选候选方案，在满足刚性约束的解集中择优。生产现场状态变更时，反馈信号触发动态重规划，通过滚动修正衔接长周期计划与现场执行。

（五）工具调用：工具标准化封装与安全调用

标准化工具调用模块将规划输出的动作方案映射为业务系统操作指令与现场执行动作，采用 MCP 等协议封装工业软件能力，通过 API 网关实现调用路由与治理，针对无开放接口的工业遗留系统用 RPA 适配对接。工具注册与描述模板明确定义工具功能、输入输出与适用边界，实现抽象动作序列到具体操作的映射。针对 MES、APS、SCADA 及 PLC 的操作接口设置权限管控，高风险动作需提前完成沙箱测试或仿真验证。工具调用全流程中，调用前完成授权与合规校验，调用中实施限流、幂等控制和满足前置条件的重试，调用后核验执行回执与现场状态。写操作设置回滚与安全预案，避免重复调用或执行偏差扩大风险。

（六）策略约束与受约束决策生成

策略约束模块可将企业操作规程与合规要求嵌入智能体决策生成与动作执行流程。该模块依托规则引擎与策略库承载约束条件，通过约束解码与输出校验缩小决策解空间，结合安全对齐机制降低违规决策风险，采用独立于大模型的硬联锁机制保障现场执行安全，可对感知、记忆、推理、规划与工具调用全环节的输出进行校验、修正或拦截，承接生产目标与既定约束，在涉及现场控制的工具调用前完成合规检查。约束分为硬、软两级：不满足硬约束直接阻断执行，偏离软约束则提示修正或触发重规划。违规输出按预案处置，约束命中与处理结果可追溯，为策略库迭代完善提供依据。

四、网络：多智能体协同编排

工业企业各专业领域在知识、工具、权责上边界明确，复杂生产任务覆盖研发、计划、生产、质量及供应链等多个环节，需要多智能体与人类协作完成。多智能体协同需围绕任务分工，明确各参与主体的能力范畴与交互规则。如图 10 所示，多智能体依靠专业分工、并行处理、交叉验证与动态协调组织任务。各智能体保持适度上下文隔离，跨域任务由编排机制衔接，关键结论由不同专业智能体交叉验证，环境变化时触发资源重协调。各主体基于本领域知识与工具输出专业决策，编排机制协调任务依赖与执行顺序，发挥并行优势同时维持清晰权责边界。协同编排统一管理身份、角色、能力、消息、状态与权限，保障各主体在共同目标下有序协作，同时管控通信、同步与协商的运行开销。

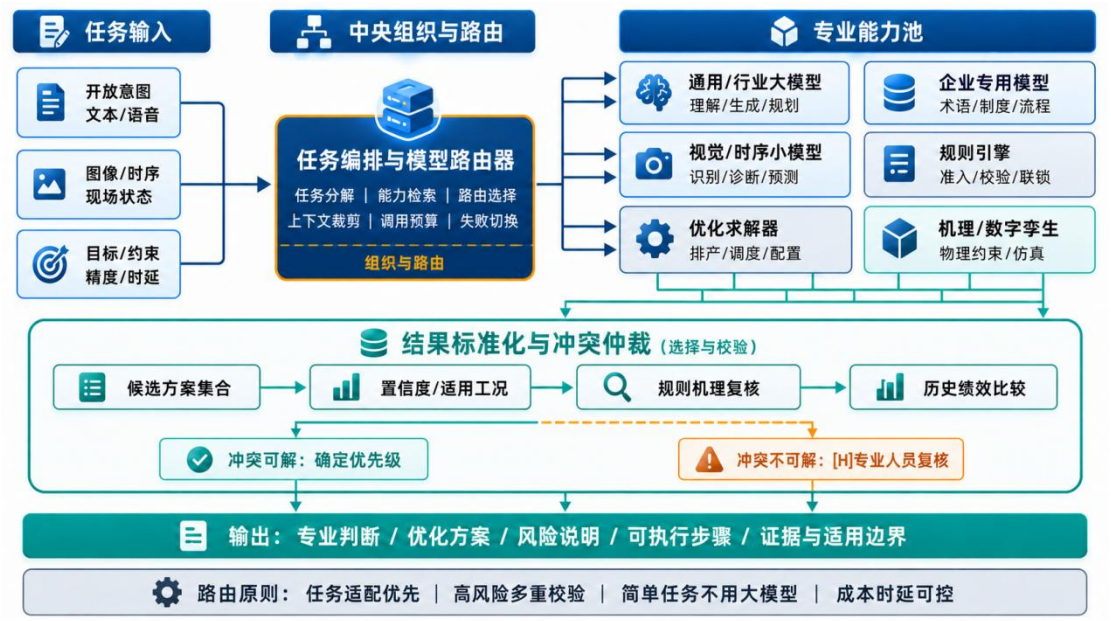

图 10 多智能体编排

（一）领域智能体设置与编排

多智能体编排可采用由编排器、共享黑板和契约网协商机制组成的混合架构：编排器调度任务流，黑板提供全局共享工作空间，契约网支撑协商分配。面向计划排程、资源协同、质量管控、设备运维和能源安全等场景的领域智能体，接入前需完成注册与发现，通过标准化能力描述声明可承接任务类型、职责边界与运行条件。各智能体经消息总线互联，依托 A2A 等协议交互结构化消息，通过接口适配与兼容性验证支撑跨框架协作。编排层承接上层生产目标，派发任务给对应智能体，依托云边端协同算力运行。编排流程可定义、可配置，通过能力画像选择执行主体，以状态同步与会话管理维持多主体协作一致性，提供故障恢复能力。

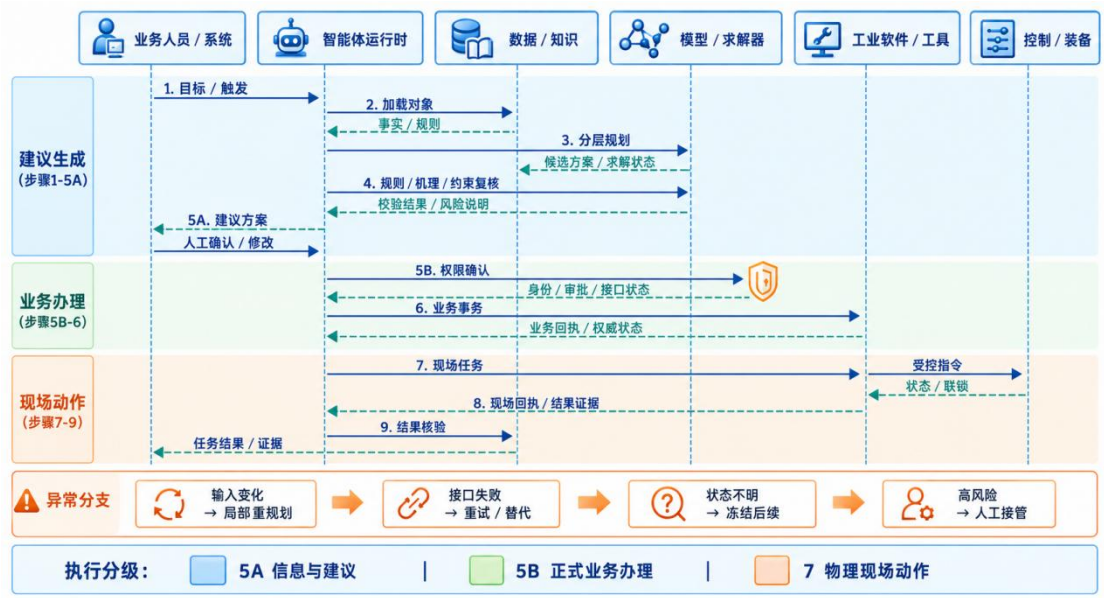

图 11 任务规划、专业求解与受控执行时序

（二）任务分解与动态分配

订单交付类全局任务先由层次任务网络按预设规则逐层拆解为子任务，再通过契约网协商分配。编排器发布任务需求，各领域智能体结合自身能力与当前负载响应，经能力匹配与负载均衡确定执行主体，明确任务输入与权责划分。成熟场景的分解方式沉淀为可复用模板库，支撑任务快速分解与动态调整。任务粒度需适配单个智能体处理能力，兼顾执行效率与协调开销。分配后需执行主体认领确认，超时未确认则重新派发；任务执行状态需持续同步，为后续协调与异常处置提供支撑。图 11 展示了任务从规划分解、专业求解到校验和受控执行的典型交互时序关系。

（三）冲突消解机制

多智能体并行决策可能产生资源争用或约束冲突。冲突消解机制通过约束检测识别资源、时间、规则的冲突，依托多属性效用评价支撑多主体协商让步，由优先级规则引擎执

行预设裁决流程。针对排产与能耗、检修与产能等冲突场景，优先识别不可突破的硬约束，比较各候选方案的综合影响。例如排程要求提升设备负荷而能源约束要求错峰生产时，可在满足安全与用能约束前提下调整生产安排。重大分歧交由仲裁机制按规则处理，协商超过预设轮次仍未达成共识的，应上报协调主体或转人工处置。冲突检测宜前置到方案生成阶段，让步依据、裁决逻辑与处理结果全程留痕归档。

（四）一致性决策机制

一致性决策是在各领域局部优化方案基础上，生成所有决策主体共同执行的全局优化方案的过程。投票机制与加权共识算法汇聚多主体意见，权重结合决策主体专业适用性与数据可信度设定。多主体分歧较大时，通过一致性协议组织多轮协商。方案评价以整体生产目标为核心依据，在满足安全、质量刚性约束前提下，采用多目标优化与 Pareto 优选方案，结合任务优先级权衡综合效益。一致性判断关注多主体目标取舍，校验资源占用与任务依赖一致性，最终生成可提交审批执行的统一方案。决策运行阶段需预设合理共识阈值与协商轮次，配置死锁规避与超限人工转接机制，避免协商无限循环。全局与局部目标的权衡过程完整留档，可作为后续调整决策评价规则的依据。

五、安全：可信安全与治理

可信安全治理贯穿数据、算力、模型、网络与自进化全流程，由身份与权限管理、策略护栏构建、全链路审计、决策可解释性与故障降级五大模块构成，各模块分别承担明确

行动主体、界定行为边界、留存过程记录、规范决策依据、落实失效处置等功能。可解释性嵌入决策生成与复核全环节，要求模型输出说明证据来源、适用范围、约束依据与验证结果，供业务人员判定决策适用性，相关内容可与审计记录印证。各机制协同实现权限控制、责任追溯与异常保护。

（一）身份与权限

身份与权限模块明确工业智能体的行动资格与职责范围，通过身份注册与统一认证为每个智能体生成可验证数字身份，遵循零信任原则持续验证调用身份与授权条件，内网访问不豁免检查。授权采用角色与属性结合的模式，按岗位职责划定基础权限，结合任务与环境细化授权条件：基于角色的访问控制绑定职责与权限，基于属性的访问控制引入调用对象、任务状态补充规则，支撑动态授权。权限设计遵循最小权限原则，区分读取、写入及联锁接口访问边界，禁止智能体获取绕过安全联锁的权限。统一身份与授权服务覆盖各层级智能体与人员，是跨层交互前置校验环节，岗位变动或任务结束及时回收权限，越权调用予以拦截，按既定流程处置。

（二）策略护栏

策略护栏依托安全策略库承载法规要求、行业标准与企业规程，硬性约束以独立规则或代码固化，不被模型输出覆盖。输入侧拦截违规指令与恶意提示，输出侧校验模型决策建议，规则引擎检查跨边界数据流与指令流。治理侧护栏与模型侧策略约束联动：模型侧生成时施加前置约束，治理侧

对输出与实际调用独立复核，协同管控越界风险。策略护栏同时检查输出内容与调用行为，模型生成的合规说明无法替代治理侧校验，现场安全联锁保持独立。护栏规则按法规、行业、企业、工序分级管理，则更新须完成验证并经授权后方可生效。违规拦截触发告警并记录处置结果，为规则优化、责任核查与运行改进提供支撑。

（三）全链审计

全链路审计对感知、推理、决策与执行全链路行为生成可追溯记录。审计日志遵循统一字段规范，依托哈希链等机制降低篡改风险，支持跨系统聚合分析、追溯查询与合规报告生成。统一格式可关联不同系统同一任务行为，支撑还原决策、审批与执行时序逻辑。异常行为检测可识别越权操作与异常模式，为安全处置提供线索。审计覆盖不同层级与场景，记录行动主体、时间、任务依据、操作与结果，关联决策证据与执行回执，为事故复盘、责任认定与合规检查提供依据。审计日志按重要程度分级存储，依据行业合规要求明确保存期限。审计发现问题由责任主体按期处置，经复核确认整改有效性。

（四）故障降级

故障降级机制基于失效模式与影响分析，预先识别工业智能体各运行环节的失效模式与后果，设计对应故障接管路径与安全处置方案。AI 失效时，先由规则控制系统接管；规则控制无法满足要求则切换为人工处置；不具备接管条件时，系统按预案进入安全状态。故障降级机制可与联锁保护、安

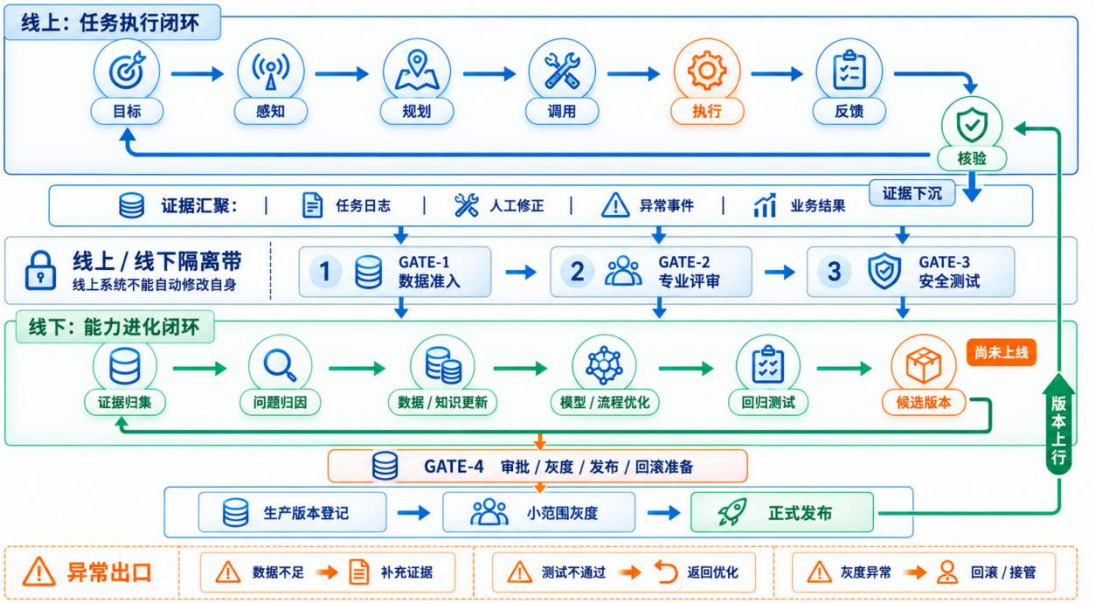

图 12 任务执行与能力进化双闭环自进化

全仪表系统协同，管控故障影响范围，避免异常向生产过程扩散。针对模型异常、通信中断、传感失效等典型场景，该机制明确分级触发阈值、接管主体与操作流程，保留一键降级与紧急停机能力。接管路径依据失效类型与影响范围差异化设置，衔接异常检测、权限切换与联锁保护环节。需定期演练检验预案可用性，恢复运行前完成状态核验与安全验证，不满足条件不得重新投入运行。

六、自进化机制：闭环验证与自演进

工业智能体依托运行反馈与验证迭代实现能力持续优化。任务执行闭环面向单次任务，核心要求为目标清晰、过程可控、状态一致、结果可核验；能力进化闭环面向模型与策略的后续版本，核心要求为问题可归因、离线可优化、验证充分、发布规范。如图 12 所示，两个闭环在数据、知识、

模型与经验层面衔接，在运行时序与权限管理层面严格隔离，避免生产侧运行反馈未经合规审查直接变更线上运行策略。

任务执行闭环以目标输入与环境感知为起点，依次经过任务理解、计划生成、能力调用、方案验证，最终进入受控执行并输出结果反馈，由任务对象、完成标准、时间约束与风险边界共同限定执行过程。其中，环境感知采集关联设备、物料与工况的实时状态；任务理解将业务事件与告警转化为结构化任务；计划生成明确执行步骤、资源、依赖关系与约束条件，同时构建正常执行路径与异常处置路径。能力演进以运行偏差与反馈证据为基础，依照“感知—诊断—计划—仿真—审批—执行—反馈”链路优化，将仿真验证与审批发布作为更新模型、知识与运行策略的必要前置环节。业务运行为能力优化提供依据，验证通过的成果作用于后续任务，形成运行与优化衔接的双闭环迭代架构。

（一）感知与诊断：闭环起点与根因定位

感知与诊断以目标偏差或重要异常事件为触发条件。感知环节复用语义底座指标与事件订阅能力，实时监测订单达成率、产能利用率、产品质量指标、能源消耗及安全运行状态等关键指标与状态，通过异常检测区分正常生产波动与显著状态偏离。诊断环节依托数字孪生比对仿真输出与实际测量结果，确定偏差位置与程度；以因果图、故障树承载的工程逻辑约束大模型根因分析，在故障传播链路中核验证据，输出可人工复核的根因诊断结论。诊断结果作为后续改进方

案生成的输入，其证据完整性与置信水平直接决定改进方向与处置方式。

诊断结论以结构化格式输出，涵盖异常现象、根因定位、证据链与候选处置建议，需按置信度分级：置信度满足阈值的进入后续计划环节，置信度较低的转人工研判。进入计划环节仅代表启动候选方案生成，不替代后续仿真验证与审批。诊断结论及关联证据沉淀入样本库，为根因分析模型后续训练与性能评估提供数据支撑。

（二）计划与仿真：改进策略生成与虚拟验证

针对已确认的根因，计划环节由大模型结合策略库生成候选改进方案，覆盖工艺参数、排程安排、控制策略等调整对象。仿真环节依托数字孪生开展虚拟验证，影子系统在与实际产线并行的环境中复核方案性能。验证覆盖常规工况、安全边界工况与极端工况，评估方案在不同条件下的有效性与潜在风险，为后续审批提供决策依据。

候选方案通过虚拟验证后方可进入审批。仿真前明确控制变量、工况组合与观测指标，验收判据与生产目标一致：在满足安全、质量等刚性约束前提下，依据任务优先级综合评价方案对产能、交付周期、能源消耗的影响。未通过验证的方案记录失效原因，返回计划环节修正后重测；多次未通过或存在重大不确定性的，转人工处理。

（三）审批与执行：人工审批与安全下发

通过虚拟验证的候选方案进入分级审批，高风险调整动作经授权后方可现场执行。电子审批流程与风险等级匹配：

常规参数调整由工艺责任人确认，涉及质量标准变更需追加质量责任人签批，涉及安全事项由安全责任人终审，审批主体、时间、意见全程留档。获批方案灰度下发至边缘端，由执行编排引擎按预设顺序与执行窗口编排动作，与安全联锁系统联动；触发联锁条件时中止操作、按预案处置，明确人机协同责任边界。

（四）反馈与持续演进：效果评估与迭代升级

执行完成后，效果评估体系围绕订单达成率、产能利用率、质量稳定性、能耗强度和安全运行状态，对比实际运行结果与预设基线，核验改进方案是否达标，厘清目标改善与其他指标波动的关联。验证有效的案例转化为训练样本，支撑大模型微调与对齐迭代，优化结论形成策略库、知识图谱的候选更新，验证后发布。系统通过能力评测基准定期检验各环节能力与适用边界，识别改进引发的性能变化。评估结果反馈业务运行，为下一轮优化提供依据，保障系统能力演进基于可核验效果。

第四章 工业智能体产业实践

当前制造业人工智能应用正由单点智能化向业务流程的综合智能化发展。工业智能体的产业价值不在于单纯增加模型交互能力，而在于能否融入企业实际业务流程，围绕具体工业任务形成稳定、可验证的业务闭环。如图 13 所示，本章围绕研发设计、中试验证、生产制造、运维管理和营销服务等关键环节，梳理工业智能体在制造业典型场景中的应用实践，分析其对提升研发效率、优化生产过程、增强设备可靠性和促进产业协同带来的影响。

总体上看，不同环节的任务数字化程度、执行风险和工程集成要求存在差异。研发设计和营销服务以数字任务为主，专业人员可以在提交、审批和发布环节进行有效把关，适合较快推广；生产制造和运维管理需要与 MES、SCADA、设

图 13 工业智能体全生命周期应用全景

备控制和现场装备衔接，工程可靠性要求更高；中试验证处于研发与生产之间，既需要人工智能提高探索效率，又必须保持计量、试验和安全责任的完整性。表 2 汇总了各环节的典型应用场景及代表性案例。

表 2 工业智能体典型应用场景与案例汇总

产业环节	典型场景	案例名称	案例主体	国家
研发设计	辅助设计与审查	慧工智能图纸审核智能体	慧工智能	中国
	仿真与数字孪生	Cadence AuraStack 多物理场设计智能体	Cadence	美国
	自动化工程开发	西门子 Eigen 工程智能体	西门子、CASMT	德国 中国
	实验与配方筛选	Golab 物质科学研发智能体	上海科学智能研究院	中国
中试验证	工艺放大验证	武汉先进院材料中试智能体	武汉先进院	中国
	试制与虚拟调试	百事产线数字孪生验证智能体	百事公司	美国
生产制造	生产计划调度	华工赛百智能排程智能体	华工赛百	中国
	工艺优化控制	霍里斯特矿石分选智能体	霍里斯特	中国
	人机协同作业	智元精灵 G2 质检协作智能体	智元机器人、龙旗科技	中国
	质量检测改进	Pegatron 装配指导智能体	Pegatron	中国
	工厂协同优化	友达光电 AgentX 智能体集群	友达光电	中国
	供应链风险管控	美的跨境供应链智能体	美的集团	中国
	安全风险管控	NVIDIA Halos 机器人安全智能体	NVIDIA、KION	美国
运维管理	设备诊断维护	重庆机电设备运维智能体	重庆机电	中国
	无人巡检处置	国网淮安立体巡检智能体	国网淮安供电	中国
	能源系统优化	中国电信空压节能智能体	中国电信	中国
营销	需求配置报价	鼎捷数智装备报价智能体	鼎捷数智	中国
	售后技术服务	Regal Rexnord 客户服务智能体	Regal Rexnord	美国

服务	供需交易协同	联想集团跨企业供应链智能体	联想集团	中国

一、研发设计

研发设计决定产品性能、成本与后续制造复杂度，是人工智能较早形成高价值任务闭环的环节之一。其代表性应用不以模型替代工程师完成全流程设计，而是连接需求、规范、历史项目、CAD/CAE/EDA 等专业软件与评审流程，减少信息检索、重复建模、跨专业等待和方案试错。从产业竞争力角度，研发智能体的核心意义在于提升企业对工业软件、工程知识与高端研发资源的组织效率，推动研发服务由单一软件采购向知识、模型、工具与工程服务协同供给转变。

（一）辅助设计与审查

辅助设计与审查面向需求解析、方案论证、参数化建模、工程出图、规范校核和图纸审查等任务。工业智能体可将客户需求、标准条款和历史设计转化为结构化约束，调用知识库、CAD 及规则校核工具形成候选方案，并在提交评审前检查尺寸、公差、材料、接口和规范符合性。其价值不在于替代工程师，而在于减少跨文档检索、重复建模和人工逐项审图，使工程师把更多精力用于关键方案判断。例如，慧工智能构建图纸审核智能体，形成“AI 全量初筛—专家复核定夺—过程数据沉淀”的人机协同审图闭环。智能体装载标准规范，对全量图纸逐张识别逻辑、核对规格与标注，圈出疑点并生成修改意见；专家对候选意见进行复核，系统同步记录采纳、驳回和修正结果，持续沉淀审核规则。在某机械设备项目中，智能体对 340 余张已多轮审核的图纸进行复核，对

约 180 张提出修改意见，经专家逐项确认后，最终采纳 135 张图纸的修改建议；单张电气系统图的识读与清单提取由数小时压缩至分钟级，效率提升约 10 倍。

（二）仿真与数字孪生

仿真与数字孪生面向产品和装备在设计定型前的性能、可靠性与安全性验证，涵盖结构、流体、热、电磁、振动等多学科计算。工业智能体可根据设计目标自动拆分仿真任务，组织几何模型、参数、求解器和算力资源，并根据中间结果调整下一轮计算，从而把原本由不同专业人员串行衔接的流程转化为面向目标的协同迭代。例如，Cadence 发布的 AuraStack AI Super Agent 已将这一模式应用于 PCB 和先进封装设计：系统可在规划、实现以及电、热、机械等多物理场分析之间协调专业智能体和工具，并依据分析结果持续迭代设计。Cadence 披露，AuraStack 可实现最高 15 倍的生产力提升，并将产品上市速度最高提升 2 倍。

（三）自动化工程开发

自动化工程开发面向 PLC 程序、HMI 画面、驱动与设备配置、测试逻辑和工程文档等任务。工业智能体能够读取设备拓扑、变量命名、客户标准和历史项目，调用自动化工程软件生成代码、配置和测试内容，并辅助完成项目迁移与一致性检查。相比单纯代码生成，其核心增量在于理解完整工程上下文，并将生成结果直接纳入正式工程工具链。例如，西门子 Eigen Engineering Agent 与 TIA Portal 连接，可读取完整项目上下文，支持 PLC 工程、HMI 画面、驱动配置、硬件

设置和自动测试生成。在与中国自动化企业 CASMT 开展的机电制动（EMB）概念验证中，团队在不到两个月内完成了将 30 至 50 个工位功能集成到单一演示设备的首版构建；西门子披露，该智能体在相关测试中可实现 2 至 5 倍更快的任务执行，并使工程效率提升约 50%。

专栏 1：应用开发智能体
应用场景： 针对企业数智化转型研发面临的需求理解周期长、协同成本高、重复性编码占比大、知识复用不足等挑战，超聚变数字技术股份有限公司构建面向软件开发全流程的应用开发智能体，围绕需求分析、代码生成、测试构造、问题定位等环节提供上下文感知的智能支持，构建覆盖“需求—开发—测试—修复—沉淀”的人机协同研发体系。
技术方案： 该智能体以大模型能力为底座，以研发知识和项目上下文为支撑，由四层组成。能力底座层以大模型为核心，提供代码生成补全、问题分析、文档生成等通用智能服务；知识与数据层接入需求文档、技术规范、缺陷库等企业知识，通过检索增强提升输出准确性；智能体编排层将能力封装为需求解析、代码助手、测试助手等任务单元，通过流程编排实现任务流转与结果回写；应用集成层与开发环境、代码仓、测试平台等对接，研发人员在原有工作流中即可调用。
实际成效： 人均代码产出提升 897%，研发任务交付周期明显缩短；转测缺陷密度下降 17.7%，版本质量进一步增强；方案设计、历史代码理解等个人经验转化为组织级可共享能力。该应用已形成“研发任务进入

—智能辅助执行—结果校验—经验沉淀—持续优化”的业务闭环，具备工业智能体应用的典型特征。
经验与可复制性： 一是场景驱动，聚焦高频、刚需、可量化的研发场景形成价值闭环；二是人机协同，智能体承担标准化、高重复性任务，关键决策由专业人员把关；三是知识增强与治理并重，建立权限控制、输出校验等配套机制；四是模式可迁移至技术服务、运营支持、方案设计等知识密集型场景，通过“知识底座+流程编排+智能协同”快速复制推广。

（四）实验与配方筛选

实验与配方筛选面向材料、化学、生物、食品等领域的新材料、新分子和新配方。工业智能体可根据研发目标和已有数据生成试验组合，调用计算模型、自动化制备和检测设备执行实验，再依据结果选择下一轮变量，使“提出假设—实验验证—数据回流—再规划”形成闭环。例如，上海科学智能研究院 Golab 物质科学研发智能体以“计算—实验—数据回流—再规划”的方式组织研发流程，依据研发目标设计试验，调用计算模型与自动化仪器完成制备和检测，再根据实验结果规划下一轮任务。上海市经济和信息化委员会公开信息显示，针对一项公开的难成药靶点，相关系统将候选分子筛选时间由传统数月缩短至一两天；在与华谊集团开展的高分子材料合成规划项目中，研发效率提升约 30%。

二、中试验证

中试验证承担实验室成果到规模化生产的关键转换功能，长期面临试验成本高、参数空间大、放大规律复杂、专

业人才稀缺等问题。本节将与中试紧密衔接的量产前工程验证纳入考察范围，观察智能体在正式量产前降低实体试错和工程变更风险的作用。工业智能体在该环节的价值，不是单纯增加自动实验数量，而是通过更合理的试验选择、高效设备组织、完整数据回流和充分虚拟验证，提升单位试验与工程验证资源转化为有效知识和工艺证据的效率。

（一）工艺放大验证

工艺放大验证承担实验室方案向规模生产工艺转换的关键任务。设备尺度变化后，传热传质、流动状态、混合效率、控制精度和原料波动都会改变，小试参数往往不能直接复制。工业智能体可综合实验数据、中试数据、设备能力和机理模型，识别影响放大的关键变量，设计试验顺序、推荐参数窗口，并利用每轮中试结果持续校准模型。例如，武汉先进院依托 MARS 材料创制大模型和实体中试线探索材料中试智能体，将实验数据、设备能力和工艺机理组织到同一任务链中，用于参数推荐、试验设计和实体中试验证。武汉市科技创新局公开资料显示，其新材料中试验证效率提升 50%、成本降低 60%；截至相关报道发布时，中试基地已累计提供 60 余项研发及中试服务，24 项科技成果实现产业化。

专栏 2：图纸审核智能体

应用场景：

在离散制造企业，设备漏油、物料占道、5S 违规等一线问题长期靠“人盯人”处理，整改通知分散在微信群及表格中，难以说清“哪些问题没改、谁负责、是否完成”，同类问题反复发生。慧工智能探

索将“发现问题→派单协调→现场整改→验收关闭→复盘改进”沉淀为有台账、可追溯、自动分派的业务闭环，让智能体承担“理解语义、判断归属、智能派单”工作，让人专注处置与决策。
技术方案: 系统以 AI 智能体中台为核心，构建“感知→理解→协调→执行→复盘”闭环架构。在**感知入口层**，一线员工通过扫码、拍照、自然语言对话即可上报，对接巡检、设备与质量数据源，形成统一入口；在 **AI 理解与分拣层**，大模型从口语化描述中自动抽取地点、对象、责任人并打类别标签；图像评分由人定规则、AI 全量执行；在**智能派单层**，按区域、职责、兜底规则自动分派到责任人，高风险或超期问题升级为整改单（含红牌机制），整改后复检验收；在**复盘洞察层**，全程留痕，自动沉淀问题台账、区域热力、闭环时效，反向指导改进。
实际成效: 在某机械设备项目中，340 多张经专家多轮审核的机械加工图纸，AI 复核后对约 180 张提出修改意见，经专家逐项复核（AI 意见仅作候选），最终 135 张图纸的意见被接受。单区域巡检由约半小时压缩至 5 分钟内，问题整改闭环率提升至 80%，高风险问题错判率为 0，分拣准确率达 90%以上，实现“上报→派单→整改→验收”全程可追溯。
经验与可复制性: 核心经验：闭环的关键是“语义理解+智能派单+升级机制+数据复盘”四位一体，把靠人盯的隐性协调工作标准化为可执行动作。落地从“小而硬”场景切入，一至两周形成首个可验收闭环，验收由人工负责、AI 承担识别与留痕。同一引擎已在齐套缺料、比价采购、安

全培训等场景复制落地，为制造企业提供“单点切入、逐步铺开、低成本起步”的路径。

（二）试制与虚拟调试

试制与虚拟调试主要服务于新产线建设、设备导入、产线改造和物流重构。工业智能体可在数字孪生环境中组织设备布局、节拍、物流路线、人员路径和控制逻辑仿真，在真实设备安装或停机改造前发现冲突、瓶颈和控制问题，并根据验证结果持续修正方案，从而降低现场返工和试错成本。例如，百事公司与西门子、NVIDIA 合作，将 AI 智能体嵌入数字孪生验证流程，借助 Siemens Digital Twin Composer、NVIDIA Omniverse 和计算机视觉，在物理改造前模拟、测试并优化设备、输送、托盘路线和人员路径等变化。百事公司披露，初期部署最多可提前识别 90%的潜在问题，并实现 20%的吞吐量提升，同时推动资本性支出降低 10%至 15%。

三、生产制造

生产制造是工业智能体价值最集中、约束最复杂的应用环节。生产计划、设备、物料等各类生产状态持续变化，单一系统难以完成全局协调。工业智能体的核心增量，是在 ERP、APS、MES 等各类系统与现场装备之间建立面向任务的组织层，实现异常快速识别、影响范围计算、专业工具调用，并将最终动作和状态回写到系统。生产现场的安全和实时控制要求决定了智能体必须坚持受控执行。

（一）生产计划调度

生产计划调度需要在订单交期、物料齐套、设备能力、工装、人员、维护窗口和在制品等多重约束下形成可执行计划。工业智能体可理解自然语言目标和业务规则，把订单与现场状态转化为求解条件，调用 APS、数学规划或启发式算法生成方案，并对结果进行解释和业务办理。其增量价值尤其体现在插单、缺料、设备故障等异常发生后的动态重调度。例如，华工赛百的智能排程智能体可读取订单、物料、设备和工艺路线等状态，将生产目标转化为约束条件并调用优化求解器生成排产方案，在插单、缺料或设备异常发生后重新规划。企业披露，其方案可在 20 分钟内完成十万级任务排程，齐套率提高 10%以上，库存周转率提升 15%以上。

（二）工艺优化控制

工艺优化控制面向产量、收率、质量稳定性、能耗和生产节拍等目标。工业智能体可持续读取原料、设备、工艺参数和在线测量数据，结合机理模型、时序模型和优化算法识别偏差原因，形成候选参数区间或操作建议，再通过专业控制系统和人员按权限验证执行。流程制造侧重连续工况优化，离散制造则更多关注加工参数和节拍。例如，霍里斯特通过对 PLC、DCS、HMI 等工业控制系统智能化改造，构建生产控制智能体，实现“振动给料-皮带加速-成像识别-喷吹分离”四大环节智能协同，保障分选设备高速运转、有效识别、精准分离，矿石通过量提高至每秒 1200 颗，提升总经济效益超 2000 万元。中国石油在炼化装置运行优化中部署智能体，将炼化时序大模型与工艺机理结合进行预测和异常识别，再由

优化算法形成参数调整建议，并通过运行优化智能体组织业务流程，模型预测准确度达到 95%以上；现场初步验证中，单炉乙烯收率提高 0.373%，单炉升温时长缩短 35%以上。

（三）人机协同作业

人机协同作业面向搬运、上下料、装配、检测、分拣等现场任务，重点提升多品种、小批量和频繁换型条件下的生产柔性。工业智能体可依据产品型号、工艺路线和设备状态组织机器人技能和物流资源，上层负责理解任务和编排，中间层将搬运、抓取、检测等能力封装为标准技能，底层控制器继续负责轨迹、速度、力矩和安全保护。例如，龙旗科技南昌工厂在平板质检产线部署多台智元“精灵 G2”机器人，与测试装备、传输轨道协同完成质检工序，并依据生产节拍连续执行上下料、检测和分流任务。科技日报公开报道显示，相关真实产线直播累计作业时长超过 64 小时，产线累计产量 17625 件，机器人作业成功率达到 99.99%。

（四）质量检测改进

质量检测改进是在机器视觉基础上进一步连接制造上下文和质量处置流程。工业智能体不仅识别缺陷，还可关联物料批次、设备参数、工艺条件和历史案例，辅助开展根因分析、批次追溯和纠正预防，使质量管理从“发现异常”延伸到“解释异常并组织处置”。例如，Pegatron 利用视觉 AI 智能体强化装配过程，将视频和现场信息用于异常识别、操作分析和质量改进。客户案例显示，相关智能体应用使单条产线人工成本降低 7%、缺陷率下降 67%；在同一技术体系

下，Pegatron 客户 Kinsus 进一步将图像分析与制造数据结合开展缺陷根因分析，分析准确率由 76%提升至接近 95%。

专栏 3：工业图纸 AI 引擎智能体
应用场景： 传统机械质检存在两个问题：一是依赖人工识图、手动找点、人工比对，流程繁琐耗时，无法适配流水线节奏，易造成质检拥堵；二是设计数据与质检数据割裂，图纸数据无法直接驱动质检设备，无法自动生成测量坐标、规划检测路径，难以形成“设计—检测—整改—归档”数字化闭环。
技术方案： 紫光云研发的工业图纸 AI 引擎智能体采用大小模型协同机制，搭配工业特殊符号识别、图样尺寸检测等垂类模型，依托自主研发的 4 层分解算法（图纸分页—分块—图元分类—元素提取），对 DWG、PDF、图片等图纸全要素解析，精准识别标题栏、技术要求、形位公差、轮廓坐标等核心信息，实现图纸数据结构化提取，并通过图纸解析、质检单生成、坐标系定位等智能体与检测设备及企业研发、生产、质检系统集成，实现基于工业图纸的自动化检测。
实际成效： 1.图纸处理整体效率提升 80%，图纸信息提取准确率达 95%以上，人工误差率降低 90%，实现降本、提质、增效； 2.图纸数据数字化沉淀，构建企业专属图纸知识库，激活存量数据资产； 3.设计数据直接驱动定位检测，构建“图纸解析－坐标定位－自动检测－尺寸核验－数据归档－质量分析”全数字化质检闭环。

经验与可复制性：

首创工业图纸大小模型协同架构，经上万套图纸微调，破解工业符号复杂、图文混排、尺寸高精度提取等难题，模型可基于企业私域数据持续迭代优化。方案适配非标装备、机械加工、计量设备等多行业，可复制到研发、生产、质检、供应链全环节，为制造业“人工智能+”转型提供可落地的标杆方案。

（五）工厂协同优化

工厂协同优化面向排产、设备、质量、物流、能源和人员等多专业目标之间的协调。工业智能体可在 APS、MES、WMS、QMS 和能源管理等系统之上建立任务组织层，根据全厂目标汇集状态、调用专业能力并比较方案，避免各系统只优化局部指标而造成物流拥堵、质量波动或资源冲突。例如，友达光电苏州工厂构建了由多个 AI 智能体组成的集群矩阵，并形成 AI 虚拟助理 AgentX，用于连接现场数据、分析任务和生产管理。苏州工业园区公开资料显示，该工厂设备综合效率（OEE）提升 15%，不良率下降 6.3%。

（六）供应链风险管控

供应链风险管控面向供应商、库存、在途物流、订单和生产状态的持续监测。工业智能体可从多源数据中识别可能影响交付的节点，评估风险传播范围，并调用采购、库存、物流和生产计划系统形成替代供应、调拨或排产调整建议，使风险管理由人工逐级追踪转向事件驱动的主动处置。例如，美的泰国家用空调工厂构建跨境供应链 AI 智能体，对 35 个核心节点开展实时监控和风险预警，并围绕库存、物流和生

产计划组织异常处置。公开资料显示，相关应用使异常处理闭环由 48 小时缩短至 12 小时以内，原材料准时达率稳定在 96%以上。与此同时，该工厂通过 72 个 AI 应用和 13 大智能体的协同应用，推动端到端订单前置时间整体减少 43%。

（七）安全风险管控

安全风险管控面向人员行为、危险区域、设备状态、作业票证和应急预案等信息，是工业智能体治理要求最高的场景之一。智能体可利用视频、传感器和文本信息识别风险事件，匹配安全规则和历史案例，形成风险提示、整改任务和闭环跟踪，并在多人多机协作区域组织更及时的安全响应。例如，NVIDIA Halos“由外向内”安全方案通过安装在设施内的摄像头扩大机器人感知范围，将低延迟目标检测、安全监测与决策逻辑结合，在人员或物体进入保护区域时触发机器人减速或停止，并在区域恢复安全后允许恢复运行。NVIDIA 与 KION 等企业正在围绕自动叉车装载、移动机器人分区等场景开展验证，相关实践仍处于持续工程化和功能安全验证阶段。

四、运维管理

设备运维具备状态数据连续、任务边界清晰、业务收益可量化的特点，是工业智能体易从分析建议进入流程执行的领域。传统预测性维护通常仅停留在健康评分或故障预警，工业智能体可进一步连接状态监测、诊断知识、工单、备件、人员和生产窗口，将异常转化为维修任务，并在维修后核验

设备状态，相关能力还可扩展到电力、能源等多领域设施运维，形成跨行业的状态监测与任务闭环能力。

（一）设备诊断维护

设备诊断维护面向机床、压缩机、泵、风机和生产装备的状态监测、故障诊断和维修执行。工业智能体可关联振动、温度、电流、报警与维修历史，调用诊断模型和故障知识识别风险，再结合生产计划、备机能力、备件和人员安排生成维修建议或工单，实现从故障预警到维修资源协同的端到端闭环。例如，重庆机电依托络钉工业互联网平台开发设备运维智能体和设备绩效分析智能体，将设备状态、维修历史、备件信息和工单流程连接起来。重庆日报公开报道显示，该系统自 2025 年下半年上线后已陆续接入集团内外 3000 多台设备；在盟讯科技应用后，原本通常需要 1 至 2 小时的维修响应时间缩短至半小时以内。某家电企业，基于大数据分析与 AI 决策模型，建立运维智能体，自动完成运维指标计算；建立可视化监控体系，快速定位运维问题，进行异常指标溯源，并沉淀运维知识库，运维管理决策效率提升 30%以上。

专栏 4：面向复杂工业 IT 环境的智能运维智能体

应用场景：

传统企业 IT 运维面临双重挑战：一是监控、日志、资产、工单数据分散在多系统，告警多、关联难；二是故障诊断依赖资深工程师经验，知识难以沉淀。神州光大建设企业 IT 智能运维智能体，构建“监控告警—故障研判—知识检索—工具调用—处置执行—工单闭

环—知识沉淀”核心链路，推动运维向“智能分析、工具协同、人机共治”转变。
技术方案： 神州光大研发的智能运维智能体采用“统一交互入口+智能体编排中枢+领域智能体+知识与数据服务+基础设施”分层架构：用户以自然语言交互，由 Lead Agent 理解意图、分解任务，调度知识库、告警、资产、日志等领域智能体协同处理；以 MCP 标准连接企业既有数据源、云平台和运维工具，无需重建运维系统。故障分析时，告警智能体关联资产配置、运行指标及日志，知识智能体通过 RAG 检索处置知识，再结合 MCP 工具调用获取的实时结果，形成故障判断和处置建议。
实际成效： 项目已形成智能运维闭环，实现告警到资产、指标、日志及审计信息的关联分析，全过程留痕，形成可追溯的运维证据链。经测试，RAG 检索召回率达 98.7%，通用 IT 问题解决准确率超 97%，复杂故障诊断准确率超 90%，实现故障秒级根因定位；整体运维响应效率提升 60%，人力成本降低 30%，知识复用率提升 50%。
经验与可复制性： 以“Lead Agent 统一编排、领域智能体专业分工、MCP 标准化工具接入、RAG 知识增强”的方式，将 AI 嵌入原有运维体系而非替代既有系统，降低改造成本与实施风险；系统分层解耦、模块化设计，新增能力可通过 Skill、MCP Server 或领域智能体扩展，具备规模化推广价值。

（二）无人巡检处置

无人巡检处置适用于巡检对象多、空间分散、环境危险或人工难以持续覆盖的场景。工业智能体可统一调度固定摄像头、无人机、轮式或四足机器人、红外和声学设备，根据任务规划路线，融合多源感知结果识别仪表、温升、泄漏和外观异常，并将结果关联设备台账和工单系统形成后续处置。例如，国网淮安供电在 220 千伏武黄变电站构建“无人机+高清视频+四足机器人”的立体智能巡检体系，并通过统一平台组织任务派发、协同巡视、智能分析、报告生成和结果回传。新华社公开报道显示，该体系在单座变电站每年可替代 120 多次人工巡检，降低 80%的人工巡检工作量，设备自主巡检和研判准确率超过 95%。

（三）能源系统优化

能源系统优化面向电、气、蒸汽、压缩空气、制冷等公辅系统，通过关联生产负荷和设备工况持续寻找较优运行方式。工业智能体可预测能源需求，调用群控、优化和数字孪生模型形成设备启停与负荷分配方案，并依据执行结果滚动调整，减少设备空载、低效运行和人工经验造成的能耗浪费。例如，中国电信在空压系统中部署节能管控智能体，持续读取多品牌设备状态和生产排班，预测用气需求，调用群控策略生成设备启停与负荷分配方案，并根据执行结果持续优化。在大型制造企业应用后，年节电超百万千瓦时，节能率 7.7%，异常响应速度提升 90%。

专栏 5：节能管控智能体
应用场景： 空压系统是制造企业公辅能源核心设施，也是高能耗、节能潜力突出的环节。企业空压站普遍存在设备机型繁杂、用气负荷波动大、调度依赖人工经验等痛点，系统综合能耗居高不下。中国电信研发的节能管控智能体落地空压站智能群控解决方案，构建“感知—预测—优化—执行”全流程管控体系，推动运行从经验驱动转向数据驱动，在保障供气安全稳定的前提下降低系统能耗。
技术方案： 方案依托翼智企采控一体化平台，搭建数据感知、智能规划、监督决策、控制执行四层协同架构：感知层完成设备全量参数采集与清洗，构建运行特征库；规划层通过用气需求预测模型输出最优开机台数与机组分配方案；决策层将策略转化为调度指令并内置安全保护机制；执行层采用模型预测控制算法实现毫秒级闭环调节。系统打通采集到执行完整闭环，无需大规模改造原有控制系统。
实际成效： 该方案已在大型制造企业空压站落地：年节约电量超百万千瓦时，整体节能率达 7.7%；系统异常响应速度提升 90%，泄漏修复周期缩短 60%；打通多品牌设备数据壁垒，实现站房运行全局可视、精准可控，供气稳定性显著增强。
经验与可复制性： 用气预测、机组群控算法策略可跨品牌、机型、站房规模快速复用，并可延伸至冷站、循环水、蒸汽等公辅系统，支撑园区级多能源

协同优化。方案对现场硬件改动小、落地成本低，契合工业节能与“双碳”政策导向，具备规模化复制推广能力。

五、营销服务

营销服务是制造企业连接市场需求与内部制造能力的重要接口。相较于通用客服，工业智能体在此领域的核心价值，是打通客户需求、产品配置、报价规则、订单、产能和设备服务数据，让前端履约承诺建立在真实产品与产能基础上，并将客户使用阶段问题反馈至研发和生产环节，同时也是服务型制造转型的重要支撑。

（一）需求配置报价

需求配置报价面向非标装备、工业零部件和多配置产品从客户需求到商务方案形成的过程。工业智能体可解析图纸和文字需求，匹配产品型号、BOM、历史报价与成本数据，生成配置和报价草案，并连接库存、计划和供应链信息校验交期，使销售、技术、采购和生产之间的大量串行沟通转化为任务协同。例如，鼎捷数智面向装备制造业推出报价专家智能体，将客户需求、产品配置、BOM、成本和历史报价等信息组织到报价流程中，用于配置匹配、成本核算和方案生成。新华网公开报道显示，该类智能体可使报价人力投入减少 80%，报价利润达成率提升 15%。

（二）售后技术服务

售后技术服务涵盖技术咨询、故障诊断、远程支持、现场维修和备件保障。工业智能体可识别客户问题和产品身份，查询手册、知识库、设备状态和历史工单，形成排查步骤，

并根据服务等级、人员技能、区域和备件情况组织后续服务，使分散在不同工程师和系统中的经验转化为可持续复用的企业能力。例如，Regal Rexnord 基于 Microsoft Copilot Studio 构建客户与员工服务智能体，连接企业知识源和 ServiceNow 等系统，识别问题、检索信息并将复杂事项转交后续服务流程。微软客户案例显示，其企业级员工智能体每月处理超过 2000 次咨询，预计每年节省约 2400 小时；面向客户的智能体每周服务超过 1000 名用户。

（三）供需交易协同

供需交易协同面向工业 B2B 中的询价、规格匹配、库存核对、报价、合同准备、物流和结算等任务。工业智能体可持续处理聊天、订单和商品信息，抽取规格与数量需求，匹配库存和供应商，形成报价和合同草稿，并将确认结果写入交易和履约系统，从而减少大量非结构化沟通和人工内勤衔接。例如，联想集团通过对供应链生产、采购、物流等数据开展智能监测分析，搭建供应链智能体，可为多级供应商动态实时共享数据，同步供应链上下游企业的供求信息，实现从需求预测到零部件交付，从生产制造到物流交付的全链路多智能体协同，工作效率提升 20%，订单交货及时率提升 5%，制造和物流成本降低 20%。找钢网将 AI Agent 体系嵌入 B2B 交易流程，用于理解产业对话、识别需求并支撑询报价和供需匹配。找钢网集团公开资料显示，截至 2025 年底，其自研 SaleMatch 交易引擎日均处理消息量超过 1600 万条，解析准

确率达到95%以上；对于合同、价格和交付等责任性事项，仍以正式交易系统和人工确认作为最终依据。

第五章 重点任务

一、建设通专融合工业智能体平台

工业智能体通用能力与工业知识、专业工具衔接不足，平台重复建设、接口不统一、跨层级协同困难，制约其规模化发展。建设通专融合工业智能体平台，可汇聚行业知识、专业模型、工业软件、设备接口和业务系统等能力，提供数据接入、任务编排、工具调用、协同调度和安全治理等公共服务，形成支撑工业智能体开发、运行、协同和治理的公共底座。

促进通用大模型与行业模型、机理模型、专业小模型融合应用，坚持“认知可以概率化、执行必须受约束”，将模型生成能力转化为具有输入依据、过程状态和调用边界的工业任务能力。吸纳工业互联网平台企业、基础模型厂商、工业软件企业、系统集成商、科研院所和行业龙头企业等各方资源，联合建设平台，开放标准化接口和开发工具，降低工业智能体开发、测试、部署和运维门槛，支撑其从单点应用向规模化、集群化应用演进。

二、打造工业智能体一体机矩阵

企业应用工业智能体，常面临环境适配复杂、系统集成成本高、数据不出域要求强、现场时延和安全约束严格等现实难题。布局覆盖云侧、边侧、端侧的工业智能体一体机矩阵，集成模型、算力、平台软件、行业应用和安全治理能力，采用软硬一体交付方式，并按任务规模、时延要求、安全等

级和部署条件提供适配产品，满足不同层级、不同场景的本地化运行需求。

依托一体机矩阵，引导工业智能体由项目定制向产品化、标准化、规模化供给转变，降低工业企业应用门槛，增强数据安全、低时延和开箱即用能力。同时，与工业现场控制系统、安全联锁机制协同，确保智能体行为受控、可验证、可接管，符合工业安全生产要求。联动整机厂商、芯片厂商、模型厂商、平台企业和行业集成商等资源，构建覆盖不同层级和应用场景的产品谱系，提高软硬一体化交付能力。

三、开展工业智能体评测

当前，工业智能体能力评价与实际业务效果衔接不够紧密，产品选型缺乏统一依据，安全责任边界尚不清晰，亟需构建面向工业场景的工业智能体评测体系。

评测应立足具体工业任务，围绕任务理解、规划决策、工具调用、行业知识运用、多智能体协同、受控执行和安全治理等能力展开，并结合任务完成质量、业务成效、责任边界和可验证结果，实行分级分类评价。重点考察工业智能体能否在真实工况下完成任务并取得可核验的业务成效，能否在权限和安全边界内受控执行，能否在异常情况下安全降级并实现人工接管等问题。

通过评测，引导产业从关注“模型是否先进”转向关注“任务能否完成、业务是否有效、安全是否可控”，为企业选型、政府采购、行业监管和产品迭代提供依据。

四、推动工业智能体供需精准对接

针对工业智能体技术供给与企业场景需求匹配不足、需求描述不规范、验收指标不清晰、无效试点风险偏高等问题，推动工业智能体供需精准对接，有利于促进智能体结合业务场景落地应用。

系统梳理重点行业、重点环节的场景清单、能力清单和产品目录等，明确业务需求、验收指标、适用条件、接口要求和交付方式，提高对接效率，降低落地成本。联合央企、行业龙头企业、产业园区和中小企业等开放典型场景，组织开展联合攻关和试验验证，优先推进任务边界清晰、数据基础较好、风险可控、成效可量化的场景。建立应用反馈和迭代机制，促进产品持续优化和案例推广，以场景开放带动产业供给，以应用反馈促进产品迭代，推动工业智能体从单点突破向集群聚变演进。

第六章 未来展望

一、从“辅助工具”向“核心引擎”的战略转型

近年来，人工智能在工业领域应用主要集中于局部分析和辅助决策，与生产经营核心流程的衔接仍有提升空间。随着大模型技术与工业知识融合，以及工业智能体体系化能力形成，人工智能打破应用边界，从“后台辅助”走向“前台引领”，成为拉动工业效率变革、产品创新、商业模式重构的核心引擎。工业智能体已逐步贯穿企业研发、生产、管理、服务全链路，成为驱动业务体系运转的关键载体。部分制造企业的生产现场中，工业智能体已承担核心调度、动态决策任务，依托全链路实时数据完成自主决策、执行与优化。这种转型重构了生产组织逻辑，将数据转化为制造业核心生产要素，让智能能力成为制造企业核心竞争力。大量制造企业已将工业智能体技术纳入整体战略布局，不再将其视为局部业务补充，而是面向全流程全链条重塑智能能力，融入业务核心环节，成为决定企业生产效率与市场竞争力的关键内核。未来，随着工业智能体技术成熟落地，战略转型进程将持续加快，更多企业将完成从“用智能补短板”到“靠智能谋发展”的思路转变，推动制造业智能化进入全新发展阶段。

二、从“功能附加”向“智能原生”的业态重塑

以往工业领域智能化改造是在原有生产业态基础上叠加智能化功能，通过开展老旧设备数智化改造、对既有流程进行智能优化，实现有限提效，并未从根本上变革传统生产

业态逻辑。随着工业智能体技术逐步成熟，越来越多制造企业在新建工厂和新增产能的规划阶段，就将工业智能体设计开发嵌入产业规划、厂房建设、设备部署全流程，按照“智能原生”逻辑搭建生产体系，使智能能力成为新增产能的原生属性。这类业态重塑，大幅降低后期智能化改造的适配成本，释放工业智能体的技术潜能，为全链路自主决策、全场景智能协同预留了发展空间，推动制造业业态沿着“传统生产+智能补丁”向“原生智能驱动生产”方向实现深度变革。

三、从“单点突破”向“集群聚变”的生态演进

当前，工业智能体仍以单点场景应用为主，存在数据互联互通不足、标准不统一、跨系统协同能力弱等问题，难以释放跨环节、跨主体系统性价值。从单点到集群升级，不是智能体数量简单叠加，而是产业组织形态和运行模式的深层次变革。在集群协同模式下，各智能体分工协作，通过多源校验、动态协商形成整体决策能力，实现单体智能体无法达成的系统优化效能。工业智能体集群协同分为三个层面：企业层面，构建覆盖全价值链的协同网络，实现流程贯通与资源优化配置；企业间层面，围绕订单、库存、产能开展跨主体协同，推动产业链向智能化网络升级；区域层面，依托工业互联网平台建设公共智能体服务体系，为企业提供低成本的智能服务。在智能体的支撑下，工业体系将实现系统级跃升，人工智能将如同历史上的蒸汽机与电力，全面融入工业生产各环节，成为驱动新型工业化的核心动力。

版权声明：

本报告版权属于中国工业互联网研究院智能化研究所、北京信息化和工业化融合服务联盟、中国科学院计算技术研究所，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国工业互联网研究院智能化研究所、北京信息化和工业化融合服务联盟、中国科学院计算技术研究所”。违反上述声明者，编者将追究其相关法律责任。

联系人：

智能化研究所

李老师：17614059751（同微信）

周老师：15025366513（同微信）