中国科学: 技术科学 2026 年 第 56 卷 第 3 期: 492 ~ 506
SCIENTIA SINICA Technologica techcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
评 述 厦门大学建校105周年航空宇航科学与技术学科专刊

工业智能体: 体系架构、关键技术与未来展望

任磊[1,2,3*†], 王海腾[1†], 董家宝[1], 张晶[1], 晏景衡[1], 曹志腾[1], 李世祥[1], 赖李媛君[1,2,3], 张霖[1,2,3], 李伯虎[1,3]

1. 北京航空航天大学自动化科学与电气工程学院, 北京 100191
2. 北京航空航天大学杭州国际创新研究院, 杭州 311115
3. 复杂产品智能制造系统技术全国重点实验室, 北京 100854
* E-mail: renlei@buaa.edu.cn
† 同等贡献

收稿日期: 2025-11-20; 接受日期: 2026-02-06; 网络版发表日期: 2026-03-02
国家杰出青年科学基金项目(编号: 62225302)、国家自然科学基金重大研究计划(编号: 92567303)和国家自然科学基金青年学生基础研究项目(编号: 623B2014, 624B2021, 625B2020)资助

摘要 随着工业大模型、具身智能等新一代人工智能技术的发展, 催生了面向Agentic AI的新一代智能体, 也为工业人工智能的发展提供了新的契机. 工业智能体作为新一代人工智能技术驱动的, 服务于工业产品全生命周期应用的新型智能体系统, 包括具身智能体和非具身(软件系统)形态, 具备面向工业场景的感知理解、知识记忆、规划决策、通信交互、自主执行、演化学习等核心能力, 能够为工业制造业研发设计、生产制造、试验测试、经营管理、运维服务等全业务链条提供智能化服务. 当前针对新一代工业智能体的系统化研究仍属空白. 本文给出了工业智能体的定义, 分析了其关键特征; 提出了工业智能体的体系架构, 包括工业智能体基座、工业智能体系统以及工业应用三个层次, 阐述了工业智能体的关键技术; 围绕工业产品全生命周期活动, 讨论了研发设计类智能体、生产制造类智能体、试验测试类智能体、经营管理类智能体、运维服务类智能体的未来典型应用场景; 最后展望了工业智能体的未来发展, 分析了工业智能体基座、工业世界模型、软硬协同的工业智能体、具备长期记忆的可信智能体、工业智能体内生安全、标准化等未来技术方向. 本文为新一代人工智能驱动的工业智能体理论与技术体系的构建、系统的研制以及产业应用的发展, 提供了一种体系化的参考.

关键词 工业智能体, 自主智能体驱动的人工智能, 多智能体系统, 工业大模型, 工业具身智能, 智能制造

1 引言

智能体(Agent)[1]理论自提出以来已历经多年发展, 产业界也开展了多方面探索, 例如基于多智能体的无人机集群协同、分布式电网调度等. 2023年以来, 大语言模型(large language model, LLM)的爆发推动智能体迈入了新的发展阶段. 新一代智能体(如Openclaw, Claude, QoderWork)展现出卓越的环境上下文认知能

引用格式: 任磊, 王海腾, 董家宝, 等. 工业智能体: 体系架构、关键技术与未来展望. 中国科学: 技术科学, 2026, 56: 492–506
Ren L, Wang H T, Dong J B, et al. Industrial agents: Architecture, key technologies, and future perspectives (in Chinese). Sci Sin Tech, 2026, 56: 492–506, doi: 10.1360/SST-2025-0364

© 2026 《中国科学》杂志社

力以及自主决策与执行能力. 同时, A2A协议及模型上下文协议(model context protocol, MCP)进一步确保了多智能体跨平台的互操作性, 推动着传统智能体向具备长程推理与分布式决策执行能力的自主智能体驱动的人工智能(Agentic AI)全面演进[2].

新一代智能体为未来工业人工智能[3]的发展提供了新的发展机遇. 然而, 当前工业界的实践仍多局限于“智能体+固定工作流”的初级阶段. 虽然欧美工业界已尝试利用多智能体系统进行制造单元调度或设备故障诊断, 但是面对工业生产环境的多变性、高度精确性要求以及实时性约束, 往往因缺乏对深层工业机理与工艺逻辑的深刻理解与可靠性保证, 仍难以直接承担生产工艺决策控制等核心任务[4]. 当前, 工业智能体主要面临以下挑战问题.

(1) 工业动态环境的自适应问题. 通用智能体通常部署于静态或半静态环境, 任务边界清晰, 而工业场景具有高度的动态性和不确定性[5], 例如市场需求波动、设备状态变化和资源约束调整. 智能体需要实时感知环境变化并调整行为, 但现有智能体缺乏长期学习和自适应能力, 难以在多变工业条件下自主进化适配. 导致这一问题的原因是多智能体系统的自主进化学习算法对工业数据漂移和场景迁移的泛化能力不足.

(2) 工业自主决策的可靠性问题. 通用智能体对于决策的准确性和鲁棒性缺乏统一的标准和规范约束, 能够容忍一定程度的误差和不确定性. 而工业应用要求极高的可靠性和安全性, 如自动化生产线的机械臂精准操控与设备故障风险调控. 现有智能体大多基于规则或浅层学习, 决策过程透明性差[6], 难以应对工业中的突发异常和复杂扰动. 导致这一问题的原因是智能体的自主决策机制尚未深入融合工业机理和领域知识约束, 使其难以确保稳定可靠的决策与执行.

(3) 工业多智能体的自组织协作问题. 通用智能体擅长处理独立、模块化的任务, 依赖于预设规则和工具辅助, 然而工业场景中多智能体系统需处理具有复杂关联流程的任务, 如跨产线生产调度、多工序质量控制和供应链协同管理, 涉及大量动态交互和关联关系. 工业多智能体协同中存在异质性和通信瓶颈, 例如不同智能体可能有不同的目标、数据模型和响应时间, 常面临信息不一致和决策冲突. 导致这一问题的原因是现有智能体缺乏对工业流程全局语境的理解, 缺乏支撑动态工作流的自组织协同机制.

(4) 工业场景中复杂长程指令的理解与执行问题. 通用智能体通常擅长处理定义清晰、步骤单一的原子任务, 而工业场景中的任务通常以冗长、抽象的自然语言指令下达, 其中隐含了复杂的子目标依赖关系和动态调整需求. 现有智能体在理解此类长程指令的深层意图、将其分解为有序可执行的子任务序列的能力仍达不到要求, 在执行过程中根据反馈的动态调整能力有限[7]. 导致这一问题的原因在于, 当前智能体任务规划与执行框架难以支撑长上下文工业流程的深度理解与任务规划, 难以支撑长期任务状态跟踪, 导致整体任务执行效率低下甚至发生错误中断.

从上述问题分析可见, 当前通用智能体难以满足工业复杂场景的应用需求, 亟需研究面向Agentic AI的工业智能体理论、方法与技术. 当前针对新一代工业智能体的系统化研究仍属空白. 本文旨在探讨工业智能体的定义、特征、体系架构、关键技术与典型应用, 并展望工业智能体的未来研究方向, 为新一代智能体赋能新型工业化提供理论与技术参考.

2 工业智能体: 定义与关键特征

工业智能体是以大模型、具身智能[8]等新一代人工智能技术驱动的, 服务于工业产品全生命周期应用的新型智能体系统, 包括具身智能体和非具身(软件系统)形态, 具备面向工业场景的感知理解、知识记忆、规划决策、通信交互、自主执行、演化学习等核心能力, 为工业制造业研发设计、生产制造、试验测试、经营管理、运维服务等全业务链条提供智能化服务. 工业智能体的关键特征如如图1所示.

2.1 从规则驱动到大模型驱动

大模型驱动是工业智能体在底层模型驱动机制方面的关键特征. 智能体系统由传统依赖显式规则库、阈值条件与固定工作流的确定性匹配执行, 演化为以语义理解与推理生成为核心的大模型主导决策. 工业智能体不再通过枚举人工预设规则来覆盖场景与异常组合, 而是将生产环境变量、制造任务、BOM、工艺文件、作业程序、检验规范与日志事件等多源信息进行语义对齐与分析理解, 将任务从规则触发的启动机制转化为目标与约束约定下的行动方案自主生成, 并

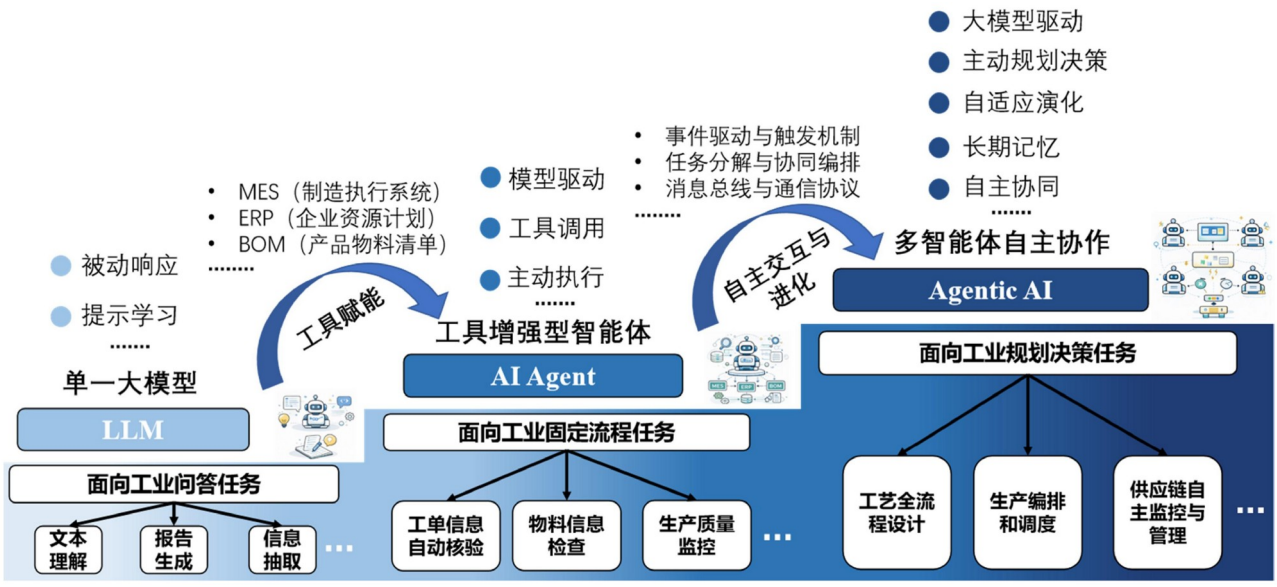


图 1 (网络版彩图)工业智能体核心能力演化趋势

Figure 1 (Color online) Evolution of industrial agents.

在工业机理与工艺规则的硬约束边界内完成一致性校验与可执行路径组织，使驱动逻辑从静态规则驱使转向动态推理与可验证思维决策.

大模型驱动在工业应用中的优势在于提升工业智能体复杂场景覆盖能力与跨域联动能力，尤其面对变更频繁、信息不完备与强约束耦合的制造环境时，能够主动补全信息缺口并生成可执行的任务分解与依赖编排方案，降低规则冲突与人工串联带来的决策滞后与局部最优风险. 通过联动检索、数据库查询、约束核验与优化求解等工具，并对接产品全生命周期工业软件系统完成查询、校核、下发、监控与回写等操作，工业智能体可以形成可校验的闭环运行并支持滚动重规划，同时将决策依据、工具调用轨迹与执行效果生成可追溯的版本化数据，从而在交期、成本、质量、资源与安全等多种约束条件下获得更稳定的全局一致性与工程可信度.

2.2 从被动响应到主动规划决策

主动规划决策是工业智能体在交互与决策模式方面的关键特征. 智能体系统由传统告警、指令或查询触发的反应式处置模式，演化为目标与状态驱动的主动规划决策. 工业智能体不再围绕单次输入指令进行反馈给出局部解释或建议，而是持续感知订单需求、产线工况、物料供给、设备运行与质量风险等工业运行状态，将任务从问答式响应或固定流程执行转化为包含目标、约束、资源与状态等多维要素的自主规划决策方案，并通过任务分解、依赖编排与回退策略生成可执行计划，在执行监控与偏差反馈作用下实现滚动式动态规划与一致性监测，从而将决策从单点反应升级为面向工业过程的自组织行动.

主动规划决策在工业应用中的优势在于工业智能体能够在强约束与多目标并存的条件下自主形成可执行的闭环方案，尤其在插单、缺料、停机、返工与质量问题等多扰动复杂场景中，可基于工业即时状态主动完成动态实时规划与冲突消解，降低人工串联导致的决策滞后与局部最优的风险. 同时具备主动联动ERP, MES, MOM, PHM, SCM, CRM等系统完成信息拉取、约束核验、下发执行、过程监控与结果回写等操作的能力. 在自主规划的结果和方案方面具备可验证与可追溯能力，能够支撑排产履约、资源利用、质量稳定性与运维保障等工业任务在同一约束框架下协同自主优化，从而显著提升复杂制造任务的韧性与鲁棒性.

2.3 从离线学习到自适应演化

自适应演化是工业智能体在学习与更新机制方面

的关键特征. 智能体系统由传统周期性离线训练与人工指导的被动静态学习, 演进为执行过程中可感知、可评估、可更新的动态策略学习演化. 工业智能体不再将模型参数与决策策略长期冻结在既定数据分布与工况假设下, 而是将人机物料法环等生产全要素多源运行数据纳入在线监测体系, 通过漂移检测、性能退化识别与触发式自主更新机制, 在约束边界内实现策略切换、参数自整定或增量更新等, 使学习从事后修补转向过程内的持续纠偏与迭代提升.

自适应演化在工业应用中的优势在于提升工业智能体对非平稳工况与长周期运行的灵活适应性, 尤其面对工艺变更、设备退化、材料批次差异、生产环境调整与供应商变化等生产状态转变引起的数据漂移与概念漂移时, 能够自适应学习与分析工业状态信息并进行有效决策, 进而抑制性能滑坡并维持决策质量. 通过将生产效率、产品良率、成本、缺料率、返工率等工业指标作为反馈信号进行在线自适应学习, 工业智能体可以形成在线评估与闭环优化路径, 将新的异常模式、缺陷形态与处置效果等工业信息转化可学习分析的数据, 支撑跨工况迁移与持续改进, 从而完成工业智能体的全局自适应学习和优化.

2.4　从短期记忆到长期记忆

长期记忆是工业智能体在知识承载与思维状态信息保持机制方面的关键特征. 智能体系统由传统依赖会话上下文与临时缓存的易失性记忆状态, 演化为可沉淀、可检索、可版本化的持久记忆体系. 工业智能体不再仅凭当前任务输入维持局部连贯, 而是将跨班次、跨工序、跨系统等关键事实与约束进行显式化处理并持续积累, 将BOM配置、工艺版本、参数设置、检验判据、设备履历、异常处置过程与决策轨迹等以结构化数据形式写入长期记忆, 使记忆从短时上下文扩展为可追溯的知识与经验底座.

长期记忆在工业应用中的优势在于能够显著增强工业智能体跨流程一致性、可追溯性与复用能力, 能够有效提升工业智能体在变更影响分析、异常根因追溯、跨工序约束校核与类似问题场景的快速处置能力, 进而避免因信息缺失与口径漂移造成的决策不一致问题. 通过对历史案例、约束核验结果、工具调用情况与处置效果等信息的有效积累, 工业智能体可以在型号切换、工艺变更与扰动频发等工业异常条件下快速召回有效策略并进行对照校验, 同时形成可追溯的证据链与策略思维链, 为质量追溯与持续改进提供支撑, 进而提升工业智能体在长程工业任务中的跨阶段一致性、决策前后逻辑贯通性与处置稳定性.

2.5　从单体智能到多智能体自主协同

多智能体自主协同是工业智能体在组织形态与决策机制方面的关键特征. 智能体系统由传统单一智能体支撑完成理解、推理与执行等任务的独立工作模式, 演进为面向角色分工与组织编排的自主协同式体系. 单体智能通常依托专用小模型完成特定工业任务, 其优势在于结构简单、决策链路短、工程可控性强, 适用于工艺边界清晰、目标明确、约束稳定的局部工业场景, 如单设备运行监测、单工序参数优化或局部异常诊断等. 然而, 在跨工序、跨系统与多目标耦合的复杂工业任务中, 单体智能需要在单一推理与决策链路中同时处理多源信息与复杂约束关系, 易受到推理深度、上下文容量与搜索空间扩张的限制, 从而暴露出推理瓶颈与局部最优等问题.

工业智能体将计划排产、工艺规划、质量工程、设备运维、物料调配等复杂工业拆分给多个子任务自主协作完成. 其核心在于将复杂工业任务由单点求解转化为可分解、可并行、可治理的协同求解过程, 即依据工业任务链路的功能边界与约束耦合关系, 将原本由单体承担的全流程工作拆分为多个职责清晰的专用智能体自主分析处理, 并在统一的组织编排下完成端到端闭环. 多智能体系统通过并行分工与协同调度, 能够将原本串行推进的决策流程解构为并行任务链与依赖图, 再通过依赖合并与冲突仲裁实现系统级方案收敛, 从而在强约束、多目标与高扰动并存的工业场景中显著提升整体决策效率与跨域一致性.

另外, 单体智能迈向多智能体自主协同, 并非简单的模型堆叠或通信连接, 而是在体系层面的迈进: 其一, 角色建模与职责划分, 需明确各智能体的能力边界、任务权限与协作关系, 避免功能重叠或责任冲突; 其二, 语义接口与状态共享, 需构建统一或可对齐的状态表示和信息交换规范, 支撑跨智能体理解一致性与协同决策; 其三, 协同一致性与冲突仲裁, 需依托任务编排与依赖建模, 确保多智能体决策在全局目标约束下可收敛、可控.

3 工业智能体体系架构

工业智能体是由工业大模型[4,9]驱动的自主智能系统, 是具备自主感知、认知、规划、决策、演化与行动执行能力的工业智能系统. 它能够在复杂工业场景中完成感知-认知-行动闭环, 实现人-机-环境的高效协同与智能演化, 同时能实现智能体间的高效协同与动态组织. 工业智能体体系架构如图2所示, 包含工业智能体基座、工业智能体系统以及工业应用三个层次.

3.1 工业智能体基座

工业智能体基座是整个工业智能体系统的认知计算内核与通用智能底座, 其设计目标在于突破传统工业自动化系统中基于规则的单一控制逻辑局限性, 通过深度融合海量异构多模态工业数据、复杂工业场景特征以及高保真工业世界模型, 构建一个能够理解规划、推演工业任务的认知基座. 该基座采用预训练-微调-强化学习的递进式训练范式: 首先基于大规模工业多模态语料进行预训练, 建立通用工业知识与逻辑基础; 随后通过特定工业场景与任务的监督微调, 实现对差异化工艺流程与设备特性的精准适配; 最终引入物理环境反馈的强化学习机制, 实现策略从数字仿真空间向真实物理空间的迁移以及与工业价值目标(如效率、质量、成本、安全等)的对齐. 这一多阶段训练路径使工业智能体基座能够具备感知理解、知识记忆、规划决策、通信交互、自主执行以及演化学习六大核心能力, 为上层工业智能体系统在动态、非结构化、高不确定性的工业环境中提供强泛化能力、高鲁棒性以及持续自进化能力的智能支撑.

3.1.1 基础设施及能力基础

工业智能体基座以工业数据+工业场景+工业世界模型为基础, 通过预训练-微调-强化学习的多阶段训练流水线实现能力学习与持续成长.

基座首先汇聚多源异构多模态工业数据, 例如行业专识、产品设计模型、工艺大纲、设备传感器时序信号、工业相机图像与音视频、产线日志等, 形成海量工业语料, 为预训练奠定丰富的通用知识基础, 同时为后续微调与强化学习提供针对性样本. 在此基础上, 基座融入产品全生命周期的典型工业场景特征, 涵盖研发设计、生产制造、试验测试、经营管理以及运维服务等作业环境与工艺流程. 通过场景特定的数据治理与标注, 实现模型对差异化工业任务的精准适配与跨场景泛化.

工业世界模型作为确保智能体高保真高可信运行的基础, 深度融合物理化学机理、工艺知识与专家经验, 严格遵循真实物理化学定律与约束条件. 它支持动态生成多样化训练场景与安全试错环境, 不仅扩展预训练的软性语料, 提供微调的仿真基准, 还为强化学习阶段构建高效的策略优化空间.

在训练流程上, 预训练阶段利用大规模多模态数据进行无监督或自监督学习, 建立通用感知、知识记忆与推理能力基础; 微调阶段基于特定场景数据开展监督学习与任务对齐, 显著增强智能操控、产品检测、异常诊断等细粒度任务能力; 强化学习阶段则在世界模型或真实环境中引入奖励反馈机制, 持续优化决策策略与执行控制, 实现与工业长期价值目标的对齐以及自适应进化.

这些核心要素与训练阶段紧密耦合, 共同构筑起基座的完整构建路径, 确保智能体能力从数字世界的数据驱动有效迁移至物理世界执行.

3.1.2 关键能力

通过多阶段训练赋能, 基座形成六大相互协同的核心能力, 支撑完整的认知-决策-执行闭环.

(1) 感知理解: 融合多模态传感数据, 实现对工业产品全生命周期各类应用场景的准确识别与语义理解.

(2) 知识记忆: 构建长短期工业知识存储与检索机制, 支持设计经验、工艺方案、机理规则与历史案例的快速调用与跨任务迁移.

(3) 规划决策: 结合生成式规划与运筹优化, 支持多约束不确定环境下的层次化任务分解规划与预测性决策.

(4) 通信交互: 支持多模态人-机/机-机间交互, 与传统工业软件及其他智能体高效协同, 实现动态自组织.

(5) 自主执行: 实现对机器人、机床、AGV等设备的精准控制, 以及对各类工业软件和外部工具软件的调用, 支持数字指令到物理动作的无缝映射及在线误差补偿.

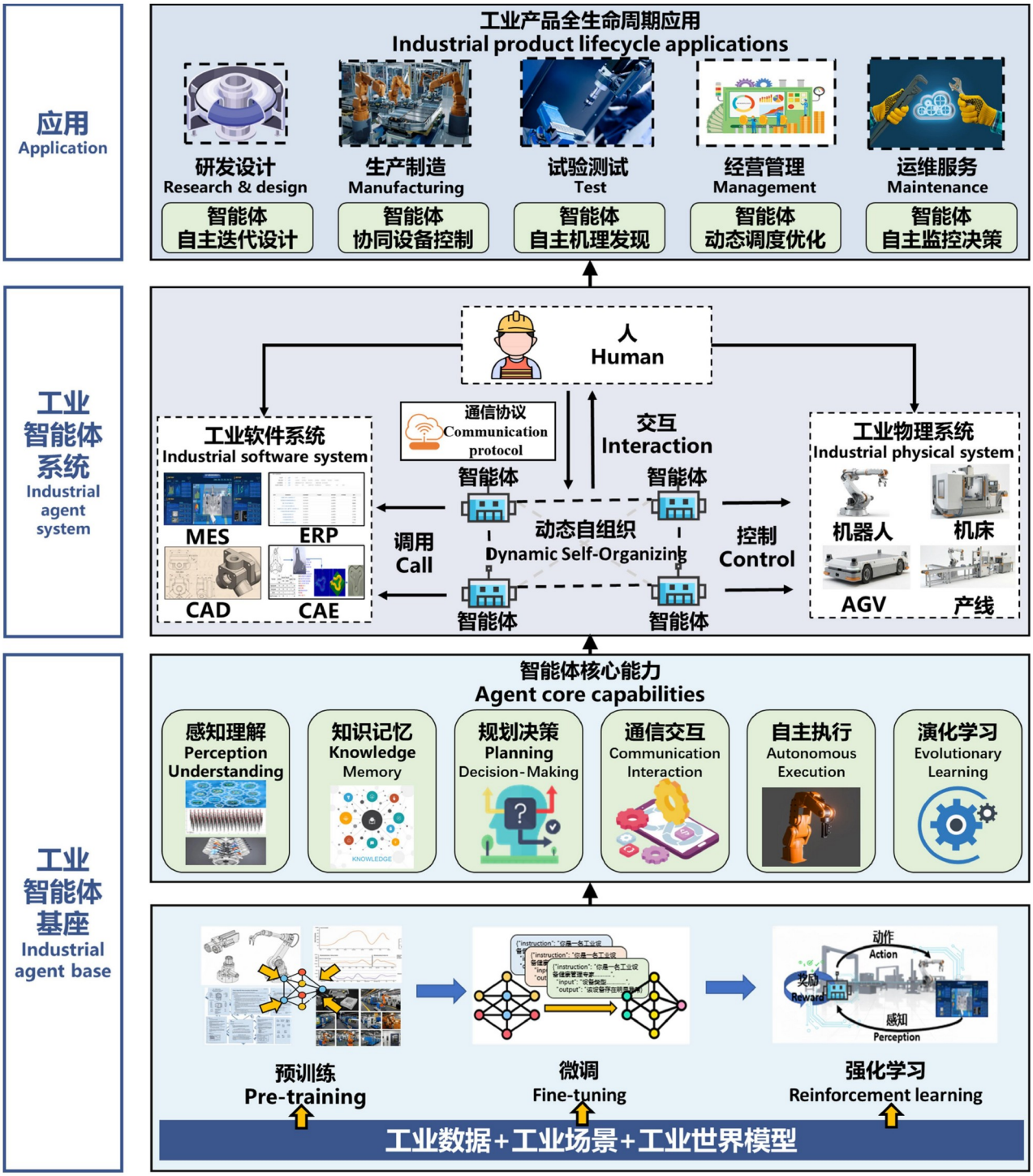


图 2　(网络版彩图)工业智能体体系架构

Figure 2　(Color online) Architecture of industrial agents.

(6) 演化学习: 集成在线强化、元学习与模仿学习机制, 基于实时反馈持续优化策略, 实现终身学习与能力自进化.

六大能力紧密耦合，为工业产品全生命周期应用

提供通用、可扩展的智能基础.

3.2 工业智能体系统

工业智能体系统作为连接数字域与物理域的中枢, 以动态自组织机制为核心, 构建异构工业智能体集群, 实现复杂工业场景的柔性适应与高效协同.

首先, 工业智能体间基于语义互操作实现动态自组织网络构建. 不同于传统分布式系统中预设的刚性通信链路, 工业智能体系统依托于标准化的智能体通信协议与共享的上下文空间, 支持异构智能体在缺乏先验知识的情况下进行自主发现、能力握手与任务协商. 在这一机制下, 智能体集群能够根据复杂的工业任务需求, 演化出串行协作、中心化调度或分布式网状等多种拓扑结构, 通过任务分解与角色的动态分配, 形成具备弹性的协作生态; 这种深度的社会化交互不仅能解决单一模型在长序列推理中的能力瓶颈, 还使得系统在面对生产扰动时能够通过多方博弈与共识达成, 涌现出超越个体总和的系统级鲁棒性与解决复杂问题的群体智能.

其次, 工业智能体系统通过构建感知工业环境的物理-数字接口, 实现智能体对工业赛博系统及物理系统的集成交互与闭环控制. 在软件环境侧, 工业智能体通过封装各类工业软件(如ERP, MES, MOM, PHM, CRM, SCM, CAD, CAE等)的API接口, 赋予智能体工具调用能力, 使其能够跨越系统壁垒获取全生命周期数据并下发业务指令; 在物理环境侧, 智能体具有明确的智能体具身化路径, 通过实时交互协议将决策指令映射为机器人、数控机床及AGV等执行机构的物理动作, 完成对物理世界的精准操控; 更为关键的是, 工业智能体系统保证人员在环的高阶环境交互维度, 将人类专家的认知反馈作为关键的环境信号纳入决策闭环, 从而构建起一个涵盖软件数据流、硬件控制流与人类认知流的混合增强交互场, 确保智能体行为与复杂的工业现场环境保持高度的对齐与适应.

3.3 工业应用

工业应用层实现工业智能体的业务价值落地与全生命周期赋能, 通过将工业智能体深度融入研发设计、生产制造、试验测试、经营管理及运维服务等业务环节, 打破传统工业价值链的数据孤岛、流程割裂与单点辅助局限. 相较于传统智能体仅能提供孤立的工具型支持(如单次查询、局部参数调整或静态数据分析), 工业智能体凭借自主规划、工具调用、跨模态理解、长链条任务执行及闭环自治能力, 实现从被动单步辅助向全流程自治执行的跃迁.

在研发设计与试验测试环节, 工业智能体超越传统辅助工具范畴, 通过端到端自主迭代设计、全流程自治测试以及在线机理推理能力, 在虚拟仿真与物理验证的双重循环中显著加速产品创新, 提升方案质量并深化复杂物理规律探索; 在生产制造与经营管理环节, 依托工业智能体及智能体集群的实时感知、动态优化与跨系统协同机制, 生产系统能够主动响应订单波动、设备扰动与供应链约束, 实现从刚性自动化向敏捷柔性、智能预测性运营的跨越; 在运维服务环节, 工业智能体通过构建设备全生命周期健康管理与预测性维护闭环, 将故障处理从被动响应升级为主动规划防御, 并将运维洞察持续反哺至上游研发与设计环节, 从而形成贯穿“研-产-试-管-服”全流程的自适应、自优化与持续进化决策体系, 推动工业体系向高自律、强泛化与自主进化的新型工业化形态迈进.

4 工业智能体关键技术

工业智能体的体系架构描述了宏观功能框架, 关键技术则是将该框架落地为可运行系统的具体路径. 本节围绕工业智能体构建中涉及的关键技术, 从三个维度具体阐述: 一是作为工业智能体核心的基座关键技术; 二是工业智能体核心功能模块关键技术; 三是基于基座与核心模块能力的系统组织编排技术. 这些技术共同支撑工业智能体从理论概念转化为实际工业应用的智能实体.

4.1 工业智能体基座关键技术

4.1.1 工业智能体预训练

在工业智能体基座构建过程中, 预训练是奠定模型通用能力的关键步骤. 工业智能体基座的预训练不仅要完成语言、图像或动作等通用能力的学习, 还需通过跨模态建模和与工业相关的领域专业学习, 使模型具备理解工业设备特性、工艺流程及操作语义的能力.

工业智能体基座的预训练通常采用大规模自监督

预训练范式, 典型方法包括掩码预测[10]、自回归序列建模[11]以及跨模态对齐学习, 使模型能够在设备日志、工业文本、时序传感数据及多模态感知数据中学习通用表征, 为故障诊断、运行状态理解与复杂决策提供基础能力. 针对工业场景中对安全性、可靠性与专业知识的高要求的特点, 预训练阶段进一步引入领域知识增强机制[12], 如通过融合工业知识图谱、工程规则约束和标准化技术文档, 使模型具备符合物理规律与行业规范的行为能力.

通过预训练得到的工业智能体基座可以作为后续指令微调与强化学习的基础, 为构建具有工业语义理解、多工业场景适配与工具调用能力的智能体提供核心支撑.

4.1.2　工业智能体指令微调

工业智能体指令微调主要通过大量结构化任务指令、专家示范与真实操作样本, 使模型掌握任务执行规范、工业场景逻辑以及与工具交互的方式, 是将预训练模型适配到具体工业任务的重要环节.

在工业场景中, 指令数据通常涵盖操作流程描述、异常处置规范、设备调试步骤、工艺规划指令以及多回合任务交互等, 其主要来源包括制造手册、企业SOP、历史工单记录以及专家构造的示范数据. 在训练策略上, 为增强模型在复杂工况和多约束环境下的泛化与推理能力, 通常引入思维链(chain-of-thought)[13]、工具调用轨迹以及包含错误修正的反事实指令样本[14], 使模型显式学习工业任务中的推理过程、工具调用方法与失败边界. 对于需要与仿真系统或真实设备接口交互的任务, 还需通过工具API调用驱动的指令微调, 使模型能够在遵循安全约束与权限控制的前提下, 准确完成外部功能调用与系统级协同操作.

经过指令微调后的模型能表现出更强的任务执行能力、更高的可控性及更规范的行动结构, 这为后续强化学习阶段奠定行为基线.

4.1.3　工业智能体强化学习

工业智能体强化学习是在模型具备基础认知与执行能力之后, 用于进一步提升工业智能体行为对齐、策略优化与安全约束收敛的能力的关键技术.

强化学习[15]通用框架基于马尔科夫决策过程, 核心是通过智能体与环境的交互试错优化策略, 其一般方法围绕“交互-反馈-更新”闭环展开. 主要学习方法有策略梯度优化: 通过调整策略参数最大化累积奖励期望直接优化策略函数(如PPO[16], GRPO[17]等); 价值函数方法: 先学习价值函数, 再基于价值函数推导最优动作(如Q-Learning[18], DQN[19]等); 偏好优化方法: 无需显式奖励函数, 直接利用偏好数据优化策略(如DPO[20], KTO[21]等). 工业智能体强化学习让工业智能体突破静态能力局限, 从“被动生成”升级为“主动决策”, 如通过RL学习多步决策轨迹, 让智能体具备规划决策能力, 又如使用RL推动内部自我监督和改进, 让智能体具备学习演化能力等.

通过强化学习, 模型可以逐步掌握复杂工艺流程的多步骤规划能力, 提高在动态环境中的自适应性, 并增强其在稀疏奖励、长时依赖任务中的表现.

4.2　工业智能体核心能力模块关键技术

4.2.1　感知理解模块

感知理解模块的功能是将异构、含噪的工业现场数据转化为机器可理解的高维语义信息.

该模块的核心在于构建鲁棒的多模态融合能力以应对工业现场的异构噪声数据. 首先基于跨模态Transformer的特征对齐与融合架构, 将来自多源传感器的特征进行统一表示; 再引入物理约束神经网络(physics-informed neural networks, PINNs[22]), 将工业系统的动力学或物理方程作为训练正则化条件; 最后, 采用特征级多传感器融合方法, 通过特定融合策略实现视觉、深度、惯性等模态之间的协同感知.

4.2.2　知识记忆模块

知识记忆模块负责决定工业智能体应存储的信息、何时检索知识以及如何遗忘过时或低价值内容.

该模块采用分层记忆架构, 短期记忆用于缓存当前任务上下文与中间状态, 长期记忆用于存储稳定的工业知识与经验模式. 短期记忆多通过上下文窗口管理实现, 支持多步推理与连续决策; 长期记忆则结合向量数据库与检索增强生成(retrieval-augmented generation, RAG[23])进行语义化存储与按需检索. 同时, 引入记忆重要性评估与持续学习约束, 实现对低价值或过时知识的遗忘与更新, 以保持记忆系统的有效性与安全性.

4.2.3 规划决策模块

规划决策模块负责将工业生产目标转化为可执行的方案, 实现复杂任务组织与系统优化.

该模块采用“全局规划-局部决策-动态调整”架构: 全局规划基于工业任务目标与约束, 通过任务分解与多步推理生成整体行动框架; 局部决策结合实时工况数据, 采用启发式搜索与序列建模优化单步动作选择; 动态调整机制通过环境反馈与轨迹评估, 实现计划重规划与冲突消解. 同时, 引入不确定性建模应对工况波动, 确保复杂场景下的决策稳健性.

4.2.4 自主执行模块

自主执行模块负责将规划决策输出的动作序列转化为工业场景中的可执行操作.

该模块采用指令解析、动作执行、状态反馈、异常修正的架构: 指令解析通过工业协议适配将抽象动作转化为设备可识别指令; 动作执行集成工具调用引擎与设备控制接口, 支持API调用、参数调节等复合操作; 状态反馈通过传感器数据实时采集与语义化解析, 同步操作结果与环境变化; 异常修正机制结合工业规则库与故障诊断模型, 实现执行偏差校正、故障降级处理.

4.2.5 通信交互模块

通信交互模块负责实现工业智能体与操作人员、其他智能体以及外部工业系统交互协同.

该模块应支持工业以太网、MCP、A2A等主流协议, 实现设备指令与多智能体消息的标准化转换; 通过工业语义对齐与意图识别, 精准解析跨模态交互内容; 基于分布式通信机制与冲突消解规则, 协调多智能体任务分工, 同步共享工况与决策信息. 同时, 融入通信加密与容错机制, 应对工业环境干扰, 确保数据传输安全与交互连续性.

4.2.6 学习演化模块

学习演化模块保障系统在长期运行过程中能够持续学习、动态适应、自主迭代, 实现可持续智能演化.

该模块采用“经验学习-策略优化-能力演化”三层架构: 采集涵盖工业场景离线数据与在线交互轨迹数据, 提取设备故障、工艺优化等关键模式, 为自改进提供基础素材; 知识更新结合工业知识图谱与实时工况数据, 通过增量学习实现知识迭代; 策略评估引入过程监督与结果反馈, 结合自我反思与错误修正机制, 验证决策逻辑适配性; 模型增量训练采用微调与强化学习技术, 融入自训练与协同优化策略, 避免灾难性遗忘; 版本化部署支持模型迭代后的安全上线与回滚, 保障演化稳定性.

4.3 工业智能体系统组织编排技术

工业智能体系统通过动态自组织或特定的组织编排技术来协调各单元的行为, 以满足不同工业场景对灵活性、稳定性或规范性的要求, 如图3所示.

自组织智能体系统是一种去中心化多智能体架构, 其核心特征是在缺乏全局控制与统一调度的条件下, 各工业智能体仅基于局部感知、邻域通信与内在行为规则自主决策, 并通过持续交互在系统层面涌现出协调一致的生产与控制行为. 该范式在设备高度异构、生产状态频繁变化或集中控制存在单点失效风险的工业环境, 如柔性制造系统、自适应车间调度、工业机器人群体协作、分布式能源管理以及大规模工业物联网等场景, 能够显著提升系统的鲁棒性与扩展能力.

自组织工业智能体系统通常以局部自治决策+分布式协同机制为核心: 一方面, 通过分布式约束优化[24]或基于博弈的协调模型, 使设备智能体在仅掌握局部工况与资源约束的条件下完成工序分配与负载均衡; 另一方面, 引入工业多智能体强化学习, 如独立Q-learning、协作型策略梯度或基于邻域奖励分解的方法, 使智能体能够在动态生产环境中持续学习协同策

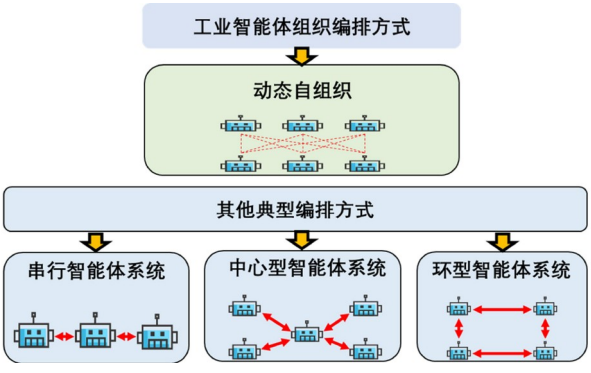


图 3 (网络版彩图)工业智能体系统组织编排

Figure 3 (Color online) Orchestration of industrial agents.

略. 在通信层面, 系统采用局部广播、Gossip或事件驱动交互机制, 结合基于规则的行为模板与工业知识约束, 引导群体行为朝安全、稳定的方向演化. 但由于系统行为依赖局部交互的叠加, 其也存在整体性能难以精确预测与形式化验证, 且在规模扩大时可能出现协同效率下降或通信开销上升的问题.

除自组织智能体系统外, 智能体系统常用的编排方式还有以下三种.

(1) 中心型智能体系统: 中心型架构以“中央决策单元”作为系统大脑, 对所有智能体组件、工具调用以及环境交互进行统一调控[25]. 该架构适用于工业自动化产线控制、集中式生产调度、工艺参数统一优化以及安全约束严格、流程高度规范化的场景, 能够实现全局最优规划与一致性控制. 但中心型架构对中央节点的计算能力与可靠性依赖较强, 在设备规模扩大或环境高度动态的工业场景中, 其灵活性与鲁棒性相对受限.

(2) 串行式智能体系统: 串行式架构将工业智能体系统拆分为具有明确功能边界的模块, 如“感知→理解→规划→执行”, 或采用多个分工明确的子智能体顺序完成任务[26]. 该架构适用于工业流程清晰、任务阶段划分明确且对可解释性要求较高的场景, 如工业文档审查、设备故障诊断流水线、工艺参数分析与决策支持系统, 能够降低系统设计复杂度并便于模块化维护与验证. 但由于决策链路较长, 串行式架构在实时性要求高或环境快速变化的工业场景中容易产生响应延迟, 且早期阶段的误差可能沿链路累积放大, 限制了系统整体鲁棒性与并行效率.

(3) 环路型智能体系统: 环路型架构通过构建“执行-评估-反思-再训练”的持续循环, 使智能体具备自我提升能力. 其适用于工业过程控制、设备健康监测、质量检测与参数自整定等需要持续校正与迭代优化的场景, 能够通过反馈回路提升决策稳定性与控制精度. 但因其对反馈时延与稳定性高度敏感, 若回路设计不当, 易引发振荡或收敛缓慢问题; 同时, 多重反馈环叠加会增加系统分析与调试难度, 在复杂工业系统中建模与验证难度大.

5　工业智能体典型应用

面向工业产品全生命周期实际需求, 传统工业智能体多以“单步任务辅助”为主要能力, 缺乏对跨环节知识的理解, 无法持续跟踪上下文并执行长链条任务. 而工业智能体通过自主规划、自主调用工具、跨模态理解、长期记忆等能力, 能够自主决策并执行工业任务, 主要应用如图4所示.

5.1　研发设计类智能体应用

研发设计环节的工业智能体可整合工业软件工具链, 并结合AIGC生成式人工智能, 辅助开展高度专业化的产品设计、仿真分析、工艺优化等任务, 可形成CAD模型设计智能体、CAE仿真分析智能体、工业软件代码生成智能体、CAM工艺优化智能体等, 促进产品研发提质增效, 缩短周期, 为个性化、高效化的智能化产品设计提供支撑.

例如, 在航空精密零部件研发场景中, CAD模型AIGC智能体可针对研发设计的模型构建核心任务, 解析航空零部件的尺寸公差、材料特性等设计标准, 精准拆解三维特征建模、装配约束定义、工程图标注等细分任务, 整合CAD工具链自动生成符合工艺要求的零部件三维模型, 同时适配不同设计模块的接口需求, 实现模型的跨环节复用与协同修改, 输出标准化的CAD模型文件与设计关联文档; 在新能源汽车车身结构研发场景中, CAE仿真分析智能体可围绕车身轻量化与抗冲击性的研发目标, 拆解静力学仿真、碰撞工况模拟、模态分析等核心任务, 整合CAE仿真工具调用对应的分析模块, 自动导入CAD模型并配置边界条件、材料力学参数, 完成多工况下的性能仿真计算, 针对仿真结果中出现的应力集中、变形超标等问题, 迭代输出结构优化、材料选型调整等建议, 推动设计方案的迭代, 缩短仿真验证周期.

5.2　生产制造类智能体应用

生产制造环节的工业智能体具备设备/车间/工厂/企业/供应链产业链级全局协同与动态调控能力, 统筹工序规划与排产调度, 调控各类生产资源. 可形成生产状态问答智能体、工艺调参智能体、排产调度智能体、机器操控智能体等, 为传统生产模式被动响应、资源配置失衡等问题的解决提供支撑.

例如, 在精密五金冲压生产场景中, 生产工艺调参智能体解析冲压件的尺寸精度、表面平整度等核心质量要求, 实时感知冲压机的压力输出、冲程频率、模

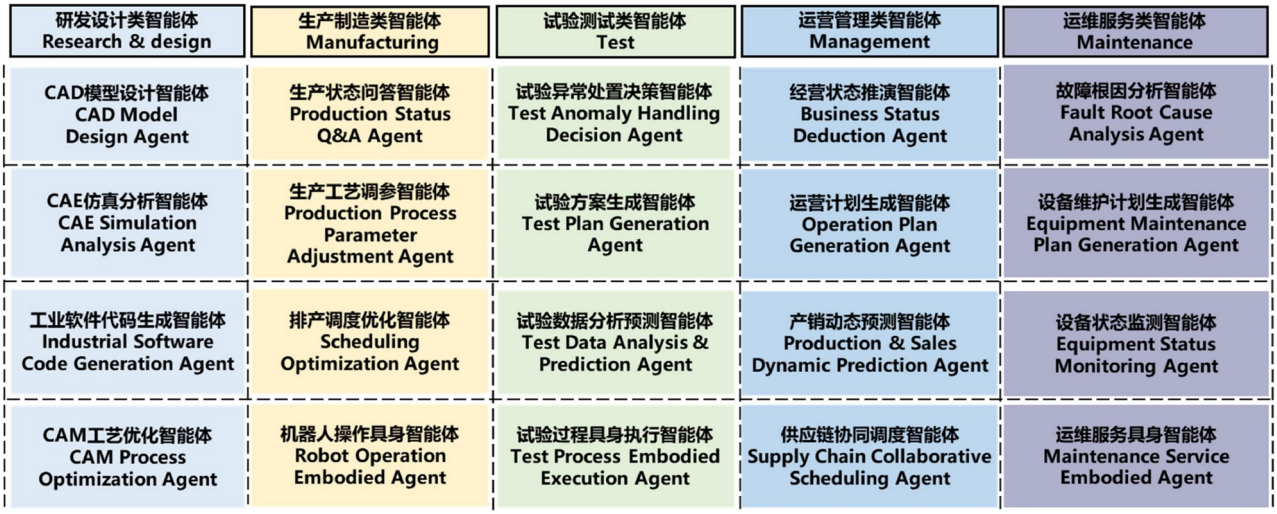


图 4 (网络版彩图)工业智能体典型应用

Figure 4 (Color online) Application of industrial agents.

具工作温度等工艺参数, 同时同步采集产品质检环节的毛刺、形变数据, 针对冲压件尺寸偏差超标、表面毛刺过多等问题, 动态优化冲压压力阈值与模具冷却周期, 整合MES系统与质检数据平台完成工艺参数的全流程闭环调控, 在保障冲压件质量达标的同时, 提升设备运行稳定性与生产节拍; 在汽车车身焊接生产场景中, 机器人智能操控具身智能体紧扣车身焊接的一致性要求, 统筹多台焊接机器人的工位协同, 实时感知机器人焊枪的姿态轨迹、焊接电流强度、工位物料的定位精度, 针对焊接偏位、熔合不良等问题, 自适应调整机器人的运动路径与焊接参数, 同时整合焊接设备管理系统与物料输送线资源, 优化机器人的工序衔接节奏, 显著提升车身焊接效率与焊缝质量.

5.3 试验测试类智能体应用

试验测试环节的工业智能体聚焦标准化与自动化测试落地, 解析测试标准, 生成测试方案, 自动化执行测试, 形成全流程自治闭环, 突破传统测试模式依赖人工、过程碎片化的局限, 可形成试验异常处置决策智能体、试验方案生成智能体、试验数据分析预测智能体、试验过程具身执行智能体等, 为测试效率与可靠性的提升提供支撑.

例如, 在电机耐久性测试场景中, 试验异常处置决策智能体提取国家标准核心指标, 通过工具接口调用传感器, 监测模块启动测试, 实时接收设备数据; 检测到异常时, 调用台架控制, 冷却系统接口执行处置动作, 闭环完成测试并通过接口输出报告; 在中试验证场景中, 试验数据分析预测智能体查阅历史试验方案, 制定试验计划, 通过接口调用测试系统, 采集终端启动测试, 并通过时序AIGC方法模拟难以测试的极端工况数据[27~29]; 以专用算法分析数据, 预测衰减拐点, 通过接口反馈至系统调整参数.

5.4 经营管理类智能体应用

经营管理环节的工业智能体整合跨部门数据, 预测潜在风险, 优化决策方案, 可形成经营状态推演智能体、运营计划生成智能体、产销动态预测智能体、供应链协同调度智能体等, 改变传统运营管理数据割裂、决策依赖经验的被动局面, 优化企业资源配置, 辅助提升企业运营决策科学性和效率.

例如, 在航空零部件工厂生产管理场景中, 运营计划生成智能体基于计划自主分解任务, 获取工业软件中产能负荷、订单优先级等核心数据, 构建产能适配模型, 整合跨部门系统数据生成运营计划, 实现计划制定与执行全闭环; 在汽车零部件供应链场景中, 供应链协同调度智能体围绕供需协同调度任务, 实时监控供应商产能、库存及物流状态, 预测供需偏差, 拆解资源调配、跨节点协同等任务, 整合供应链系统资

源制定调度策略, 降低供需失衡风险.

5.5　运维服务类智能体应用

运维服务环节的工业智能体可用于产品的远程服务, 例如装备全生命周期健康保障, 监测状态, 预测劣化趋势, 制定维修策略, 替代传统被动响应模式. 可形成故障根因分析智能体、设备维护计划生成智能体、设备状态监测智能体、运维服务具身智能体等. 推动运维模式向主动预测转型, 保障设备稳定运行, 降低运维成本与停机损失, 实现产品与装备全生命周期高效管理.

例如, 在数控机床运维场景中, 故障根因分析智能体调用振动分析仪、电流检测仪等工具采集数据, 定位故障点位并深挖核心根因; 事后总结同类故障规律与处置经验, 迭代优化根因分析模型, 提升后续故障研判精准度, 结合生产计划制定修复方案, 完成运维闭环; 在风电设备运维场景中, 设备维护计划生成智能体调用备件管理系统, 人员排班工具整合资源, 预判劣化趋势并制定分级维护计划, 定期总结计划执行效果与资源适配性, 优化计划生成算法实现自我进化, 合理规划维修计划, 减少故障停机时间.

6　未来技术方向展望

尽管当前智能体已在部分垂直场景实现了点状突破, 但在面对非结构化、高不确定性的开放工业环境时, 其泛化推理与群体协同能力还存在显著瓶颈. 面向未来, 工业智能体的发展将深度融合工业大模型与具身智能技术, 进一步突破物理世界与数字空间的认知壁垒. 通过在基座算力、世界模型、软硬协同及可信安全等维度的系统性重塑, 工业智能体将最终完成从“自动化工具”到“自主化伙伴”的转变, 推动工业人工智能进入全新发展阶段. 未来发展方向展望如下.

6.1　工业智能体基座

未来工业智能体基座将不再仅依赖于通用大语言模型微调, 而是向工业领域专业知识驱动的多模态工业大模型底座发展. 关键在于构建多模态融合及多工具调用能力的新型工业神经网络, 突破单一文本模态的限制, 原生地理解工业领域的时序信号、三维点云、热成像及多物理场仿真数据[5]. 未来的工业智能体基座将内嵌物理化学方程与工业控制逻辑, 使神经网络具备因果推理能力, 而非单纯的概率拟合. 同时, 基座支持在线增量学习, 能够在不遗忘旧知识的前提下, 实时吸收产线产生的新数据与新工艺, 成为一个能随工业生产系统共同演化的工业大脑, 为上层应用提供持续的智能算力与认知支撑.

6.2　工业世界模型驱动的智能体

工业世界模型将是确保未来工业智能体符合真实工业世界运转规律的关键支撑. 未来通过数字族谱[30,31]等技术将构建工业生产涉及的人机物料法环全要素世界模型, 形成大规模多样化工业具身/非具身训练场. 在工业世界模型支持下, 将从静态的数字仿真模型转向一个可交互、可推演、符合物理定律的生成式动力学系统. 通过在潜在空间中进行状态演化建模与推理验证, 智能体可在低成本环境下完成策略评估与方案筛选. 这意味着, 在执行复杂工业操作或危险动作前, 智能体已在世界模型中推演了数百万次, 预判了可能的边界条件与长尾故障. 这种能力有望改变工业试错成本高昂的现状, 实现从基于经验的被动响应到基于模型的超前预测的范式转移, 让智能体真正具备对工业物理世界的直觉与预判能力.

6.3　软硬协同的工业智能体

工业智能体的终极形态之一是软硬深度融合的具身智能系统. 未来工业智能体将朝着端侧大模型与感知执行硬件深度融合的方向演进. 技术上, 这将推动大模型轻量化压缩技术的极限突破, 使百亿参数级的智能体能够运行在功率受限的嵌入式芯片上. 同时, 通信机制将从高延迟的应用层协议下沉至底层的实时网络, 实现毫秒级/微秒级的推理与控制同步. 通过模型压缩与量化技术、低时延通信机制以及具备感算一体能力的新型传感与执行硬件, 智能体有望在端侧实现更紧耦合的感知、推理、执行闭环. 这种软硬协同将消除感知与执行之间的时延壁垒, 使得各种工业机器从预编程的自动化机器装置进化为手眼脑协调的智能工匠.

6.4　具有长期记忆的可信智能体

随着智能体接管核心控制权, 黑盒模型带来的不确定性将成为工业界一大担忧. 未来的核心保障是建

立一套可验证的信任机制. 这要求技术上实现从端到端黑盒推理, 向神经符号融合等新机制的转型, 例如可将深度学习的感知能力与符号逻辑的推理过程结合, 确保智能体的每一个决策都有明确的逻辑链路可追溯. 同时, 可考虑引入形式化验证技术, 用数学方法证明智能体在极端工况下的行为边界, 确保其绝对不会违背安全约束. 此外, 价值对齐将成为必选项之一, 确保智能体的目标函数始终与人类工程师的安全规范和伦理标准保持一致, 让智能体既具备自主性, 又符合安全与伦理约束.

6.5 内生安全的工业智能体

面对日益复杂的网络空间威胁与对抗攻击, 工业智能体的安全范式正从外挂式防御向内生安全体系深度演进. 未来的工业智能体将集成鲁棒性增强技术, 在训练阶段引入扰动建模与对抗训练, 使模型具备对传感器噪声及恶意对抗样本的识别与过滤能力, 从根源上防范因数据投毒引发的决策偏差. 在系统架构层面, 可融合零信任架构与分布式可信计算, 通过动态身份认证与指令完整性鉴权, 确保多智能体协作流的可信受控. 可引入基于物理规律的语义一致性监控, 通过将物理先验知识嵌入判定逻辑, 使智能体具备实时校验决策行为是否符合物理常识的能力, 构建起应对黑盒模型不可解释性的逻辑熔断机制. 针对工业敏感数据的保护需求, 可集成联邦学习、同态加密及安全多方计算等隐私计算技术, 支撑智能体在不泄露原始工艺参数与核心数据的前提下实现群体知识共享与模型协同演进. 这种覆盖算法鲁棒性、架构可信性与数据隐私性的立体化防御体系, 将为工业关键基础设施和各类工业智能体应用的安全运行提供内生安全保障.

6.6 工业智能体标准化规范化

工业智能体在产业界的规模化落地, 亟需标准规范的制定. 产学研各界需要对新一代人工智能背景下的新型工业智能体的定义与内涵形成共识, 形成工业智能体系统体系架构的统一标准, 并对工业智能体的核心技术要求进行规范. 同时, 异构互操作性问题一直是工业界面临的问题, 未来的异构工业智能体如何交互集成, 涉及各类交互协议与集成接口的标准化问题. 在面向工业产品全生命周期应用时, 工业智能体如何与当前的制造业信息化系统、各类工业软件进行集成, 也需要制定规范化的流程和指南. 对于开发者而言, 如何开发具身/非具身工业智能体系统, 也需要一套新的开发方法论与标准化流程. 工业智能体国际/国家/行业多层次标准体系的制定, 是引领和推动工业智能体应用落地的基础性支撑.

7 结论

以大模型为代表的新一代人工智能催生的新型智能体为未来工业智能化升级提供了新的驱动引擎. 本文探讨了在这一新时代背景下, 工业智能体的定义、关键特征、体系架构与关键技术, 围绕工业产品全生命周期活动讨论了未来典型应用场景, 并分析展望了工业智能体未来的技术发展方向. 本文为新一代人工智能驱动的工业智能体理论与技术体系的构建、系统的研制以及产业应用的发展, 提供了一种体系化的参考.

参考文献

1 Russell S, Norvig P. A modern approach. Artif Intell, 1995, 25: 79–80

2 Sapkota R, Roumeliotis K I, Karkee M. AI Agents vs. Agentic AI: A Conceptual taxonomy, applications and challenges. Inf Fusion, 2026, 126: 103599

3 Ren L, Jia Z, Laili Y, et al. Deep learning for time-series prediction in IIoT: Progress, challenges, and prospects. IEEE Trans Neural Netw Learn Syst, 2023, 35: 15072–15091

4 Ren L, Wang H, Dong J, et al. Industrial foundation model. IEEE Trans Cybern, 2025, 55: 2286–2301

5 Ren L, Wang H T, Dong J B, et al. Industrial foundation model: Architecture, key technologies, and typical applications. Sci Sin Inform, 2024, 54: 2606–2622 [任磊, 王海腾, 董家宝, 等. 工业大模型: 体系架构、关键技术与典型应用. 中国科学: 信息科学, 2024, 54: 2606–2622]

6 Liu X, Yu H, Zhang H, et al. Agentbench: Evaluating llms as agents,. arXiv: 2308.03688

7 Nayak S, Morrison Orozco A, Have M, et al. Long-horizon planning for multi-agent robots in partially observable environments. Adv Neural Inf

Process Syst, 2024, 37: 67929–67967
8 Ren L, Dong J, Liu S, et al. Embodied intelligence toward future smart manufacturing in the era of AI foundation model. IEEE ASME Trans Mechatron, 2025, 30: 2632–2642
9 Ren L, Wang H, Wang Y, et al. Foundation models for the process industry: Challenges and opportunities. Engineering, 2025, 52: 53–59
10 Ghazvininejad M, Levy O, Liu Y, et al. Mask-predict: Parallel decoding of conditional masked language models,. arXiv: 1904.09324
11 Bautista D, Atienza R. Scene text recognition with permuted autoregressive sequence models. In: Proceedings of the European Conference on Computer Vision. 2022. 178–196
12 Peters M E, Neumann M, Logan R, et al. Knowledge enhanced contextual word representations. In: Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP). 2019. 43–54
13 Wei J, Wang X, Schuurmans D, et al. Chain-of-thought prompting elicits reasoning in large language models. Adv Neural Inf Process Syst, 2022, 35: 24824–24837
14 Glossop C, Chen W, Bhorkar A, et al. Cast: Counterfactual labels improve instruction following in vision-language-action models,. arXiv: 2508.13446
15 Kaelbling L P, Littman M L, Moore A W. Reinforcement learning: A survey. J Artif Intell Res, 1996, 4: 237–285
16 Yu C, Velu A, Vinitsky E, et al. The surprising effectiveness of PPO in cooperative multi-agent games. Adv Neural Inf Process Syst, 2022, 35: 24611–24624
17 Shao Z, Wang P, Zhu Q, et al. Deepseekmath: Pushing the limits of mathematical reasoning in open language models,. arXiv: 2402.03300
18 Watkins C J C H, Dayan P. Q-learning. Mach Learn, 1992, 8: 279–292
19 Osband I, Blundell C, Pritzel A, et al. Deep exploration via bootstrapped DQN. Adv Neural Inf Process Syst, 2016, 29: 4033–4041
20 Rafailov R, Sharma A, Mitchell E, et al. Direct preference optimization: Your language model is secretly a reward model. Adv Neural Inf Process Syst, 2023, 36: 53728–53741
21 Ethayarajh K, Xu W, Muennighoff N, et al. Kto: Model alignment as prospect theoretic optimization,. arXiv: 2402.01306
22 Cai S, Mao Z, Wang Z, et al. Physics-informed neural networks (PINNs) for fluid mechanics: A review. Acta Mech Sin, 2021, 37: 1727–1738
23 Lewis P, Perez E, Piktus A, et al. Retrieval-augmented generation for knowledge-intensive nlp tasks. Adv Neural Inf Process Syst, 2020, 33: 9459–9474
24 Fioretto F, Pontelli E, Yeoh W. Distributed constraint optimization problems and applications: A survey. J Artif Intell Res, 2018, 61: 623–698
25 Jin B, Collins T J, Yu D, et al. Controlling performance and budget of a centralized multi-agent llm system with reinforcement learning,. arXiv: 2511.02755
26 Zhang Y, Sun R, Chen Y, et al. Chain of agent: Large language models collaborating on long-context tasks. Adv Neural Inf Process Syst, 2024, 37: 132208–132237
27 Wang H, Ren L, Li Y, et al. MetaIndux-TS: Frequency-aware AIGC foundation model for industrial time series. IEEE Trans Neural Netw Learn Syst, 2025, 36: 18062–18074
28 Ren L, Wang H, Laili Y. Diff-MTS: Temporal-augmented conditional diffusion-based AIGC for industrial time series toward the large model era. IEEE Trans Cybern, 2024, 54: 7187–7197
29 Ren L, Wang H, Li J, et al. AIGC for industrial time series: From deep-generative models to large-generative models. IEEE Trans Syst Man Cybern Syst, 2025, 55: 7774–7791
30 Ren L, Dong J B, Zeng X C, et al. Digital genealogy: Driving the world model of industrial embodied intelligence. Sci Sin Inform, 2025, 55: 1748–1765 [任磊, 董家宝, 曾宪超, 等. 数字族谱: 驱动工业具身智能世界模型. 中国科学: 信息科学, 2025, 55:1748–1765]
31 Ren L, Dong J, Zeng X, et al. Digital genealogy: AIGC-driven evolution of digital twin for future smart manufacturing. IEEE Trans Automat Sci Eng, 2026, 23: 3525–3535

Industrial agents: Architecture, key technologies, and future perspectives

REN Lei[1,2,3], WANG HaiTeng[1], DONG JiaBao[1], ZHANG Jing[1], YAN JingHeng[1], CAO ZhiTeng[1], LI ShiXiang[1], LAILI YuanJun[1,2,3], ZHANG Lin[1,2,3] & LI BoHu[1,3]

[1] *School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China*
[2] *Hangzhou International Innovation Institute, Beihang University, Hangzhou 311115, China*
[3] *State Key Laboratory of Intelligent Manufacturing System Technology, Beijing 100854, China*

The advancement of new-generation artificial intelligence technologies, such as industrial foundation models and embodied AI, has catalyzed the emergence of new agents oriented towards Agentic AI, presenting fresh opportunities for the development of industrial artificial intelligence. As novel agent systems driven by these cutting-edge technologies and serving the full lifecycle of industrial products, industrial agents encompass both embodied and non-embodied (software system) forms. They possess core capabilities tailored to industrial scenarios, including perception and understanding, knowledge memory, planning and decision-making, communication and interaction, autonomous execution, and evolutionary learning. Consequently, they provide intelligent services across the entire business chain of industrial manufacturing, including R&D, manufacturing, testing, management, and maintenance. Currently, systematic research regarding new-generation industrial agents remains a gap in the field. This paper defines the concept of industrial agents and analyzes their key characteristics. It proposes an architecture for industrial agents comprising three layers: the industrial agent base, the industrial agent system, and industrial applications, while also elucidating the associated key technologies. Centering on industrial product lifecycle activities, the paper discusses typical future application scenarios for agents in R&D, manufacturing, testing, management, and maintenance. Finally, the paper provides an outlook on the future development of industrial agents, analyzing prospective technical directions such as the industrial agent foundation, industrial world models, software-hardware synergetic agents, trustworthy agents with long-term memory, endogenous security, and standardization. This work provides a systematic reference for the construction of theoretical and technical frameworks, system development, and industrial application of industrial agents driven by new-generation AI.

industrial agents, Agentic AI, multi-agent systems, industrial foundation models, industrial embodied AI, intelligent manufacturing

doi: 10.1360/SST-2025-0364