

工业人工智能产业 智库报告 2026

国声智库

信息获取与处理陕西省重点实验室暨国际联合研究中心

中央财经大学中外经济比较研究中心

中央财经大学金融创新与风险管理研究中心

中国商业史学会一带一路专业委员会

上海全应科技有限公司

宜兴福鼎环保工程有限公司

联合出品

目 录

摘要	1
一、研究背景：工业人工智能进入系统性进化关键阶段	1
二、现状研判：工业人工智能产业生态的"四重跃迁"	2
（一）技术跃迁：从"通用大模型"到"工业专用智能体"	2
（二）应用跃迁："两端深化、中间突破"的全场景渗透	4
（三）数据跃迁：从"规模堆砌"到"质量优先"	6
（四）生态跃迁：开源开放与软硬协同	8
三、新型智库观察：比较优势与机制创新	10
（一）思想引领：构建"工业智能体经济"理论框架	10
（二）场景深耕：打造"AI+工业"垂直领域话语权	11
（三）机制创新：智库+产业的"旋转门"模式	13
四、挑战与瓶颈：制约工业 AI 深化的"三重门"	15
（一）数据之困：高质量工业数据稀缺与流通壁垒	15
（二）安全之虑：风险边界模糊与责任界定困难	16
（三）落地之难：从"盆景"到"风景"的规模化鸿沟	17
五、政策建议与实施路径：构建工业 AI 高质量发展的"四梁八柱"	18
（一）构建"1+N"工业 AI 数据治理体系，破解数据瓶颈	18
（二）创新"场景牵引"推进机制，加速规模化应用	20
（三）筑牢安全治理防线，建立可信 AI 生态	22
（四）强化智库支撑与生态协同，提升产业服务能力	24
（五）完善人才培养与金融支持体系	25
（六）创新"基金+平台"协同机制，构建多维融合生态	27
六、结论与展望：迈向"人机协同"的工业新纪元	30

摘要

2025 年，全球人工智能发展迈入"从能力涌现到价值落地"的实质性跨越期，我国人工智能核心产业规模预计突破 1.2 万亿元，工业领域正经历从"AI 工具应用"向"AI 原生重构"的质变。本报告基于国声智库对长三角、珠三角、京津冀等重点区域 30 余家制造业企业的实地调研，系统研判工业人工智能（工业 AI）在技术迭代、场景落地、生态构建等方面的发展趋势，提出产业已进入系统性进化的关键阶段，正经历"四重跃迁"。

技术跃迁体现为从"通用大模型"向"工业专用智能体"的范式转换。以 DeepSeek-V3.2、Qwen3 等为代表的模型通过深度集成推理与智能体能力，在复杂逻辑推理与高效响应间实现动态平衡；工业智能体构建"感知-决策-执行"闭环，成为新型"数字员工"雏形；具身智能进入规模化实训期，VLA（视觉-语言-动作）架构与世界模型加速探索，人形机器人在极氪 5G 智慧工厂等场景验证"实训-实战"路径。**应用跃迁**呈现"两端深化、中间突破"特征：后端运营管理（占比 45.8%）深度渗透至供应链优化与能源管理；前端研发设计（28.3%）通过 AI for Science 范式重塑产品创新，汽车研发周期从 36 个月压缩至 24 个月；中间生产制造（25.9%）在质量检测、工艺优化等场景潜力持续释放。**数据跃迁**面对"数据墙"挑战，工业数据集内容稠密性缺失占比高达 82.50%，亟需构建"行业机理+数据工程"双轮驱动的治理新范式，合成数据与智能生成技术兴起。**生态跃迁**表现为开源开放成为主旋律，国产开源大模型全球累计下载量突破百亿次，"算法-软硬件"协同设计显著降低应用门槛。

国声智库作为深耕政策研究的新型智库，首创"工业智能体经济"理论框架，超越传统"AI 赋能"工具论视角，提出从"工具赋能"到"系统重构"、从"数据驱动"到"数据和知识联合驱动"、从"单点智能"到"群体智能"的三重范式转换。智库构建"思想引领—场景深耕—机制创新"三位一体服务模式，在热电数智化（全应科技案例）、危废治理（福鼎环保案例）等垂直领域形成深度洞察，通过"旋转门"机制打通政产学研用壁垒，成为工业 AI 领域的"政策翻译器"与"产业连接器"。

报告深刻剖析制约工业 AI 深化的"三重门"：数据之困表现为高质量工业数据稀缺、跨企业流通壁垒高筑、标注成本高昂且难以规模化；安全之虑源于大模型"幻觉"风险、鲁棒性不足及

自主性风险苗头，工业场景责任界定缺乏明确法律框架；落地之难体现为中小企业面临算力成本、复合型人才、标准缺失三重制约，存在从“盆景”到“风景”的规模化鸿沟。

针对上述挑战，报告提出构建“四梁八柱”政策框架：建设“1+N”工业 AI 数据治理体系，设立国家级工业数据资源池与行业数据空间，全面推行数据工程贯标行动；建立工业 AI“场景机会清单”发布机制，深入实施“智改数转网联”专项工程，打造国家具身智能实训基地；建立分级分类安全风险评估与准入制度，构建覆盖研发、部署、运营全生命周期的安全防护技术体系；设立“工业 AI 智库联盟”，创新“基金+平台”协同机制，设立百亿级产业投资基金群，构建技术策源、产业升级、金融赋能、人才培养、组织协同的五维融合生态。

展望 2026 年及“十五五”时期，工业 AI 将呈现四大确定性趋势：（1）从单点应用向系统重构演进，催生“自感知、自决策、自执行”的“智能原生”新型工业化企业。（2）从数据驱动向数据和知识联合驱动升级，工业软件与 AI 边界趋于模糊，形成“物理世界与数字世界”融合[3]和实时闭环。（3）AI 产业正经历从“训练为王”到“推理为王”的结构性转移，推理效率与成本控制成为商业化核心变量；8/6 比特有限精度芯片的落地则将为端侧智能普及与供给侧算力重构提供关键支撑，二者叠加将全面重塑 AI 产业格局与应用生态。（4）从企业内向产业链协同扩展，工业互联网平台进化为“产业智能体网络”，实现跨企业计划协同与产能共享。

算力从训练侧向推理侧的转移与低比特芯片的双重驱动，将使 AI 产业在 2026 年进入“效率与普惠”的新阶段，企业需优先布局推理优化、低精度芯片适配与云-边-端协同架构，以抢占商业化先机。建议政府部门完善数据治理与安全监管框架，制造企业加快构建“首席 AI 官”制度，技术供应商深耕垂直场景建立风险共担机制，各方协同发力把握全球制造业智能化转型战略机遇，为制造强国建设贡献坚实力量。

关键词：工业人工智能；工业智能体；具身智能；数据治理；新型工业化；智能制造；产业基金；人机协同；多维融合；智库服务

一、研究背景：工业人工智能进入系统性进化关键阶段

2025 年，全球人工智能发展迈入"从能力涌现到价值落地"的实质性跨越期，技术革命与产业变革的叠加效应持续释放。中国信息通信研究院最新数据显示，我国人工智能核心产业规模 2024 年已突破 9000 亿元，同比增长 24%，预计 2025 年将达 1.2 万亿元；市场主体蓬勃发展，相关企业数量超 6000 家，全球占比达 16%，形成涵盖基础层、技术层、应用层的完整产业链条。在新型工业化战略纵深推进背景下，人工智能与制造业融合正经历从"试点示范"向"规模推广"的关键跃迁，成为培育新质生产力、建设现代化产业体系的核心引擎。国际社会同步加速布局，美国依托"先进制造业领导力战略"强化 AI 在高端制造领域的渗透，德国"工业 4.0"进入智能自适应生产新阶段，日本"社会 5.0"战略推动人机协同制造模式创新，全球工业智能化竞争格局更趋激烈。超威半导体、英伟达研制出 6/8 比特（bit）或位的有限精度 AI 芯片，大大减少存储量、计算量、功耗和成本；我国启动混合精度（有限精度）AI 芯片研制项目。有限精度 AI 芯片对于工业 AI 产业发展具有重大影响。

政策体系持续完善为产业发展提供坚实制度保障。2024 年以来，国务院《关于深入实施"人工智能+"行动的意见》明确提出"培育智能原生新模式新业态"的战略导向，工业和信息化部相继出台《智能制造典型场景参考指引》《工业重点行业领域设备更新和技术改造指南》等配套文件，构建起"顶层设计-专项行动-标准引领"的政策闭环。当前，工业人工智能发展呈现系统性进化特征：技术层面，基础模型通过强化学习与物理环境交互实现自主进化，具备"感知-决策-执行"闭环能力的工业智能体成为技术制高点，数字孪生与 AI 融合推动虚拟调试、预测性维护等应用走向成熟；应用层面，大模型在工业领域呈现"两端深化、中间突破"的梯次渗透格局，向后端运营管理（占比 45.8%）和前端研发设计（28.3%）深度延伸，生产制造环节智能化改造占比提升至 25.9%，质量检测、工艺优化、排产调度等场景落地成效显著；生态层面，开源开放成为智算基础设施建设主旋律，"算法-芯片-工具链"协同设计成为技术演进主流范式，MoE 架构、有限精度实现技术和小模型专业化发展有效降低中小企业应用门槛，算力成本下降与模型效率提升形成正向循环。

国声智库作为深耕政策研究与产业经济的新型智库，2025 年以来持续以思想引领服务市场，充分发挥机制灵活、资源整合能力强的比较优势，率先聚焦工业人工智能细分赛道开展深度调研。本研究基于中国信息通信研究院《人工智能产业发展研究报告（2025 年）》[1]、工业和信息化部运行监测数据等权威信源，结合对长三角、珠三角、京津冀等重点区域 30 余家制造业企业的实地走访，以及对全应科技、福鼎环保等典型服务商的案例剖析，系统研判工业人工智能在技术迭代[2]、场景落地、生态构建等方面的发展趋势，针对性提出具有操作性的政策建议与产业实施路径，为推动"AI+制造"深度融合、助力新型工业化建设提供智力支撑。

二、现状研判：工业人工智能产业生态的"四重跃迁"

（一）技术跃迁：从"通用大模型"到"工业专用智能体"

2025 年，基础模型实现跨越式能力突破，头部语言大模型综合能力较 2024 年底提升 30%，多模态理解能力增长超 50%，推理性能与计算效率实现结构性优化。在工业场景，这种能力转化正推动技术应用从"工具辅助"向"主体赋能"深度演进，形成覆盖感知、认知、决策、执行全链条的技术体系。

1. 工业大模型向"超级模型"演进

以 DeepSeek-V3.2、Qwen3、Kimi K2 等为代表的模型，通过深度集成推理、代码生成及智能体能力，实现"思考+非思考"模式合一，在复杂逻辑推理与高效响应之间实现动态平衡。在工业场景中，这类模型展现出强大的跨模态理解能力，能够自主解析 CAD 图纸、工艺规程、设备日志及传感器时序数据，完成从设计优化到故障诊断的全流程复杂任务。例如，中国钢研集团发布的"冶金流程感知大模型"采用"感侧+知侧"双塔结构，融合 70 余年冶金行业知识积累与百万级工艺数据，实现金相分析准确率超 95%，元素含量检测误差控制在 0.5%以内，推动钢铁行业从"单点智能化"向"全流程数智化"转型。与此同时，中石化、国家电网、南方电网等央企

加速布局行业垂直大模型，在油气勘探、电网调度、设备运维等领域形成专业化解决方案，模型参数量从百亿级向千亿级跃升，训练数据覆盖多源异构工业知识库。

技术标准的体系化建设同步提速。全国信息技术标准化技术委员会人工智能分技术委员会加快推进工业大模型评测标准制定，围绕模型性能、安全性、可靠性、可解释性建立多维度评估框架。中国信通院联合工业互联网产业联盟发布《工业大模型能力要求》团体标准，明确模型在工业知识理解、工艺逻辑推理、实时响应等方面的技术指标，为行业选型提供权威参考。

2. 智能体成为"数字员工"雏形

中国信通院"方升"智能体基准测试结果显示，高度封装的通用智能体产品在特定工业场景下可获得比顶级大模型更优的性能表现，验证了"大模型+工具调用+领域知识"融合架构的有效性。在工业领域，智能体通过动态规划引擎与多模态工具调用框架，构建"感知-决策-执行"闭环，实现任务执行从流程固化向动态优化的转变。智能体技术架构呈现模块化、可编排特征，支持根据具体工业场景灵活配置感知模块、推理引擎和执行接口。

在化工领域，中国科学院过程工程研究所开发的智能机器人催化反应实验系统，可替代人工开展高通量实验，自动完成催化剂筛选、评价及工艺参数优化，实验效率提升超 10 倍，研发周期缩短 40%。在装备制造领域，智能排产 Agent 能够实时接入 ERP、MES、WMS 等多系统数据，综合考虑订单优先级、设备状态、物料齐套性等约束条件，动态生成最优生产计划，排产效率较人工提升 3-5 倍。当前，工业智能体正从单点功能向多智能体协同演进，通过分布式决策机制实现跨工序、跨车间、跨工厂的协同优化。

3. 具身智能进入"实训期"

具身智能正从实验室验证向规模化商用过渡，核心在于场景驱动下的"数据-模型-本体"闭环优化。端到端视觉-语言-动作（Vision-Language-Action: VLA）架构与世界模型加速探索，通过多模态大模型直接映射视觉感知到机械动作，显著提升机器人在未见环境中的泛化性与自适应能力。国内头部企业加快人形机器人在制造场景的落地验证，优必选 Walker S1 在极氪 5G 智慧

工厂实训中，承担车门锁质检、安全带检测、车灯盖板质检等任务，搬运效率提升约 25%，验证了"实训-实战"路径的可行性。傅利叶智能 GR-1 在康复医疗场景实现批量交付，智元机器人远征 A1 进入 3C 制造产线开展精密装配测试。

4. 有限精度 AI 软硬件加速 AI 工业应用与产业

2025 年初，DeepSeek 通过模型架构和实现技术创新（如 MLA 注意力机制、DeepSeekMoE 稀疏结构、8 比特有限精度运算）与软硬件联合优化，实现高性能与低成本共存，训练成本仅为同类闭源模型的 1/10，证明通过软硬协同的 AI 具备引领式创新潜力。

2025 年上半年，超威半导体、英伟达研制出 8/6 比特的有限精度 AI 芯片，大大减少 AI 存储量、计算量、功耗和成本；我国启动混合精度（有限精度）AI 芯片研制项目。有限精度 AI 技术与芯片对于工业 AI 产业发展具有重大影响。至此，我国科学家早在 1998 年出版的针对大规模神经网络的有限精度设计理论[4]于 27 年后得到国内外 AI 头部企业的成功工程部署或有限精度 AI 芯片成功研制的实证。有限精度 AI 芯片显著减少 AI 的二进制存储量、计算量，大大降低芯片设计难度与功耗，降低工业 AI 应用成本，这无疑将推进工业 AI 广泛的边缘应用和产业发展。

随着基础模型能力收敛，竞争焦点转向推理侧，需求端推理调用量增长，供给端厂商提升推理效率。这意味着芯片格局等将围绕推理效率重构，2026 年算力竞争主战场将从训练侧转向推理侧，有限精度 AI 芯片在边缘计算与端侧的部署，推理效率和成本控制能力成为决定 AI 商业化进程的关键变量。

政策层面，《人形机器人创新发展指导意见》[5]明确支持在制造、物流、特种作业等领域开展规模化应用试点。截至 2025 年底，国内已建成 30 余个具身智能训练场，配备真实工业场景、数字孪生环境及虚拟仿真平台，为机器人提供多模态交互数据与技能训练环境。技术路线上，"小脑+大脑"分层架构成为主流，"大脑"负责任务规划与语义理解，"小脑"专注运动控制与实时反馈，两者协同实现复杂工业操作的精准执行。

（二）应用跃迁："两端深化、中间突破"的全场景渗透

工业 AI 应用遵循"数字化水平领先领域率先突破"的规律，呈现鲜明场景特征与行业差异性。据中国信通院调研，2025 年工业大模型应用在后端运营管理、前端研发设计、中间生产制造三大环节的占比分别为 45.8%、28.3%和 25.9%，形成"两端引领、中间跟进"的梯次发展格局。

1. 后端运营管理（45.8%）：深度渗透，稳健增长

企业运营管理环节数字化基础较好、数据积累丰富，成为大模型应用最成熟的领域。当前应用已从辅助数据分析升级为智能决策支持，覆盖供应链优化、能源管理、安全监控、客户服务等全业务链条。煤炭科学研究总院研发的"矿山知行"调度平台，整合太阳石矿山大模型与多智能体协同决策技术，构建覆盖"人—机—环"全要素的智能化调度体系，实现采掘、运输、通风、排水等系统的联动优化，推动调度模式从辅助决策向自主决策转型升级，实现从"少人调度"到"黑灯调度"的智能化演进，单矿井调度人员减少 60%，异常事件响应时间缩短 80%。

在能源电力领域，大模型广泛应用于负荷预测、设备巡检、客服问答等场景。国家电网"电力知语"大模型支撑智能客服日均处理咨询超百万次，问题解决率达 92%；南方电网"大瓦特"模型在输电线路巡检中实现缺陷识别准确率 98.5%，巡检效率提升 5 倍。在供应链管理中，智能预测模型通过分析历史订单、市场趋势、天气数据等多维信息，实现需求预测误差率从传统方法的 15%降至 5%以内，库存周转率提升 20%-30%。

2. 前端研发设计（28.3%）：持续扩张，份额攀升

研发设计环节知识密集、创新性强，AI 应用正重塑产品创新与工艺开发范式。重点行业聚焦研发环节创新，AI 驱动的虚拟仿真技术加速应用，显著缩短研发周期、降低试验成本。汽车制造业走在前列，部分车企在新车研发阶段引入数字孪生模型，对空气动力学性能进行模拟测试，超过 94%的模拟案例与风洞试验数据偏差小于 3%，计算速度快 10-100 倍，单次模拟成本降低 60%，新车研发周期从 36 个月压缩至 24 个月以内。

在材料科学领域，AI for Science 范式加速落地。中国科学院大连化学物理研究所研发的智能化工大模型 2.0Pro，构建催化反应、工艺开发、反应条件优化、分离纯化四大智能平台，通

过分子动力学模拟与量子化学计算相结合，为新材料研发提供全新路径，催化剂筛选效率提升百倍。在航空航天领域，中国商飞利用大模型辅助飞机结构强度分析，自动生成优化设计方案，减重效率提升 15%；航天科工集团将 AI 应用于复杂装备总体设计，实现多学科协同优化。随着生成式 AI 技术成熟，文本到 CAD、文本到仿真指令等应用逐步落地，设计效率进一步提升。

3. 中间生产制造（25.9%）：优化升级，潜力释放

生产制造环节对实时性、可靠性、安全性要求极高，大模型应用需与工业控制系统深度集成，技术门槛相对较高。随着工业质检、工艺参数优化、预测性维护等场景广泛落地，大模型对制造执行环节的赋能作用持续显现。某钢铁企业热轧产线接入宽度预测大模型后， ± 2 毫米宽展预测准确率从传统模型的 68% 提升至 83%，成材率提高 0.5 个百分点，年增效益超千万元。某石化企业建成国内首个乙烯装置数字孪生体，集成工艺机理模型与 AI 算法，实现装置运行状态实时映射与优化调控，日常操作量减少 90%，平均自控率从 85% 提升至 99.50%，能耗降低 3.2%。

在质量检测领域，基于视觉大模型的缺陷检测系统在汽车零部件、电子元器件、光伏面板等行业规模化部署，检测精度达像素级，误检率低于 0.1%，检测速度较传统机器视觉提升 3 倍以上。在工艺优化方面，注塑、压铸、焊接等工艺参数智能推荐系统通过分析历史工艺数据与质量结果，建立工艺-质量映射模型，自动推荐最优参数组合，产品不良率降低 40%-60%。当前，生产制造环节 AI 应用正从单点优化向全流程协同演进，通过 APS（高级计划排程）与 MES 系统集成，实现计划-执行-反馈闭环优化。

（三）数据跃迁：从"规模堆砌"到"质量优先"

高质量数据集是驱动模型能力提升的"燃料"，也是制约工业 AI 发展的关键瓶颈。当前，工业数据建设正经历从追求规模向注重质量的深刻变革，数据工程体系化、标准化、资产化趋势明显。

1. 数据密度见顶回落，质量瓶颈凸显

Epoch AI 数据显示，2020-2023 年代表性模型数据密度（单位参数对应的训练 token 数）连续上升，但 2024 年后出现见顶回落迹象。例如，Qwen 2.5-32B 数据密度约 554，而 Qwen 3-Max 仅为 36，表明参数扩张速度已超过高质量训练语料增长速度，“数据墙”问题日益凸显。中国信通院评估显示，当前行业数据集建设存在显著质量瓶颈，内容稠密性缺失占比高达 82.50%，领域相关性不足占比 14.04%，标注准确性问题占比 3.46%。工业领域尤为突出，设备数据噪声大、多源异构数据对齐难、工艺标签获取成本高等问题制约模型训练效果。

工业数据具有强专业性、高实时性、多模态性特征，对数据质量要求更为严苛。某装备制造企业调研显示，其设备传感器数据有效利用率不足 30%，大量数据因格式不统一、时间戳不同步、异常值未清洗而无法直接用于模型训练。数据标注方面，工业缺陷样本稀缺、标注专家依赖度高，某汽车零部件企业为建立瑕疵检测数据集，需投入 3 名工程师耗时 6 个月完成 2 万张图像标注，成本高昂且难以复制。

2. 数据工程体系加速成型

面向人工智能的数据工程由体系建设、开发维护、质量控制、资源运营、合规可信五大核心要素组成，覆盖数据设计、采集、清洗、增强、标注、质检、运营的全链条。工业领域需特别强化“行业机理+数据工程”双轮驱动，将工艺知识、专家经验转化为结构化数据资产。头部企业开始建立数据治理委员会，制定数据标准规范，构建数据质量评估体系。某家电集团建立覆盖研产供销服全链路的数据湖，统一数据标准与接口规范，数据准备时间缩短 70%。

在数据标注领域，专业化、自动化趋势明显。海天瑞声通过自研标注平台与大模型，构建“标-训-推”一体化数据处理模式，利用预标注模型自动生成初标结果，人工审核修正，标注效率提升 5 倍，成本降低 60%。针对工业场景，部分企业开发半自动化标注工具，结合 CAD 模型与物理规则生成合成数据，缓解样本稀缺问题。数据资产入表政策推动下，工业企业数据资产化意识增强，某能源企业将设备运行数据作为资产入表，评估价值超亿元。

3. 合成数据与智能生成兴起

随着推理模型与数据合成技术发展，自动化生成与人机协同标注发挥更大作用。合成数据通过物理仿真、生成对抗网络（GAN）、扩散模型等技术生成，可有效补充真实数据不足，降低标注成本。在自动驾驶领域，Waymo、特斯拉等企业大量采用合成数据训练感知模型；在工业领域，西门子、达索系统等通过数字孪生生成合成数据，用于机器人训练与工艺优化。

智能数据生成技术快速进步，大模型可自动生成高质量指令微调数据（SFT 数据）与基于人类反馈的强化学习数据（RLHF 数据）。部分工业企业开始利用大模型生成工艺异常案例、设备故障日志等合成数据，扩充训练集规模。同时，主动学习（Active Learning）技术应用于数据筛选，模型自动识别高价值样本请求人工标注，减少冗余标注工作量。数据版权与隐私保护方面，差分隐私、联邦学习等技术在跨企业数据协作中应用增多，某汽车联盟采用联邦学习机制，在不共享原始数据前提下联合训练供应链优化模型。

（四）生态跃迁：开源开放与软硬协同

工业人工智能生态正从封闭专有向开源开放转变，从单点技术竞争向系统级协同创新演进，产业链上下游协同、软硬一体化设计成为提升竞争力的关键路径。

1. 开源生态成为技术普惠关键力量

国产开源模型全球影响力稳步提升，截至 2025 年 12 月，国产开源大模型全球累计下载量突破百亿次，月下载份额最高占全球 17.1%，在 HuggingFace 等开源社区的热度持续攀升。魔搭（ModelScope）、焕新（OpenI）、魔乐（MindSpore）等本土开源社区快速崛起，推动模型托管规模快速增长，与 HuggingFace 托管模型比例从年初 11% 提升至 18%，形成具有国际影响力的开源矩阵。阿里通义千问、百度文心、智谱 ChatGLM 等开源版本在工业场景得到广泛应

用，中小企业可基于开源模型快速构建行业应用。

开源不仅限于模型权重，更向训练框架、推理引擎、开发工具链延伸。PyTorch、MindSpore 等深度学习框架持续优化工业部署能力，vLLM、TensorRT-LLM 等推理加速工具降低模型服务成本。开源社区推动形成模型即服务（MaaS）新业态，降低工业企业应用 AI 的技术门槛与资金门槛。某省中小企业公共服务平台基于开源大模型搭建 AI 服务云，为 500 余家制造企业提供低成本智能客服、文档解析等服务，单家企业年均投入不足万元即可享受 AI 赋能。

2. "算法-软硬件"协同设计成为主流

2025 年初，DeepSeek 通过模型架构创新（如 MLA 注意力机制、DeepSeekMoE 稀疏结构、8 比特运算）与软硬件联合优化，实现高性能与低成本共存，训练成本仅为同类闭源模型的 1/10，证明通过软硬协同具备引领式创新潜力。华为 CloudMatrix 384 超节点、阿里磐久 128 超节点等全栈化开放产品，采用新型互联协议（如 HCCS、NVLink）与存算一体架构，加速构建从芯片、服务器、网络到框架、模型全面开放的技术体系。

在边缘计算与端侧部署方面，模型压缩（量化、剪枝、蒸馏）、有限精度处理与专用芯片（NPU、TPU，特别是有限精度 AI 芯片）协同优化，使大模型可在工业现场设备实时运行。英特尔、英伟达、华为、地平线等企业推出面向工业场景的 AI 加速卡，支持 -40°C 至 85°C 宽温工作，满足工厂恶劣环境要求。某钢铁企业在高炉边缘侧部署轻量化质检模型，推理延迟低于 50 毫秒，无需上传云端即可实时检测表面缺陷。软硬协同还体现在开发工具链整合，如百度飞桨与英特尔 OpenVINO 深度适配，实现模型一键转换与优化，开发效率提升 40%。超威半导体、英伟达等研制 8/6 比特有限精度运算的 AI 芯片，将大力推进边缘计算与端侧部署并显著降低存储量、计算成本和功耗，对工业人工智能产业发展具有重要影响。产业生态组织方面，工业互联网产业联盟、人工智能产业发展联盟等组织推动产业链协同创新，建立供需对接平台与测试验证环境。地方政府积极建设智算中心与 AI 产业园区，形成“算力供给-模型开发-场景应用”区域生态。某市人工智能产业园集聚芯片、服务器、算法、应用企业 200 余家，形成从基础研究到产业应用的完整闭环，年产值突破 500 亿元。国际标准合作方面，我国积极参与 ISO/IEC JTC1/SC42 人工智能分委会工作，在工业 AI 术语、框架、用例等标准制定中贡献中国方案，提

升国际话语权。

专栏：全应科技：热电智能化的"神经中枢"

作为热电智能化领域的专精特新"小巨人"，全应科技专注将工业大数据、人工智能与热电机理深度融合，打造"云+端"智能化整体解决方案，为燃煤热电、生物质发电及垃圾焚烧等流程工业提供数字化转型的关键支撑。

针对传统 DCS 系统难以实现全局优化、过度依赖老师傅经验等痛点，全应科技自主研发"全应热电云"平台，部署工业智能体构建"感知-决策-执行"闭环。其技术路径体现"机理+数据"双轮驱动：基于热力学第一性原理构建锅炉、汽轮机等关键设备的高保真数字孪生体，利用强化学习在虚拟环境中持续优化燃烧策略，将"看火"经验转化为算法模型；通过 OPC UA 协议与现有 DCS 系统无缝对接，实现给煤、配风、减温水等参数的毫秒级优化，确保 AI 指令在安全阈值内自动下发。

在某大型化工集团热电厂落地应用中，该系统实现锅炉燃烧效率提升 1.2%、汽轮机热耗降低 0.8%，年节约标煤超 8000 吨，减排二氧化碳 2 万余吨；环保排放波动降低 40%，NOx 排放均值下降 15%。同时建立"AI 中控+人工巡检"新模式，操作人员劳动强度降低 30%，安全隐患显著减少，推动热电行业从"单点自动化"向"全局智能化"跃迁。

全应科技的案例充分证明，流程工业 AI 应用必须深度嵌入行业 Know-how，通过数字孪生与智能体的结合，构建"物理世界-数字世界"实时映射，才能真正解决工业"卡脖子"环节，实现安全、高效、绿色的智能化生产，为"双碳"目标实现提供可复制路径。

三、新型智库观察：比较优势与机制创新

作为深耕政策研究与产业经济的新型智库，国声智库在工业人工智能领域具有独特比较优势。依托长期积累的政产学研资源网络与跨学科研究能力，智库不仅提供战略研判与政策解读，更通过机制创新深度参与产业实践，形成"思想引领-场景深耕-生态链接"的立体化服务体系。

（一）思想引领：构建"工业智能体经济"理论框架

国声智库率先提出"工业智能体经济"概念，将其定义为以工业智能体为核心载体，通过"感知-决策-执行"闭环实现生产要素重构、价值创造模式变革的新型经济形态。这一理论框架超越传统"AI 赋能"的工具论视角，从政治经济学与产业组织理论维度，系统阐释人工智能对工业生产关系的根本性重塑。

理论内涵层面，"工业智能体经济"强调三重范式转换：一是从"工具赋能"到"系统重构"，AI 不仅是提升效率的技术工具，更是重塑生产关系、组织形态与价值分配的基础设施，推动企业从科层制向智能体协同网络演进；二是从"数据驱动"到"数据与知识联合驱动知识驱动"，在数据智能基础上融合行业机理、工艺 Know-how 与专家经验，构建"物理世界与数字世界"的协同智能体，实现数据价值与领域知识的深度融合；三是从"单点智能"到"群体智能"，通过多智能体协同决策机制，打破企业边界与信息孤岛，实现产业链上下游的实时优化与全局最优配置，形成"点-线-面-体"的智能化演进路径。

理论价值层面，该框架为理解工业 AI 发展规律提供了新的分析范式。传统研究多聚焦技术本身的性能提升，而"工业智能体经济"理论关注技术-组织-制度的协同演化，强调标准规范、数据治理、人才结构等制度要素与技术进步的匹配性。智库基于该理论框架，先后完成《工业智能体发展白皮书》《制造业数字化转型路径研究》等成果，相关观点被《中国经济社会论坛》等权威平台刊载，为相关政策制定提供理论支撑。同时，该框架指导智库开展企业咨询，帮助某大型装备制造企业重构其生产组织模式，通过部署 12 类工业智能体，实现跨车间协同调度，产能利用率提升 18%，库存周转率提高 35%。

（二）场景深耕：打造"AI+工业"垂直领域话语权

依托与《中国经济社会论坛》《开发性金融研究》《金融监管研究》等权威平台的战略合作关系，以及长期在钢铁、有色、化工、能源等流程工业领域的跟踪研究，国声智库在以下细分场景形成深度洞察与专业积累：

1. 智能制造与工艺优化

聚焦钢铁、有色、石化、建材等流程工业的高价值场景，国声智库提出“机理模型+AI 模型”双驱动方法论。针对流程工业大滞后、大耦合、非线性的工艺特征，单纯数据驱动模型难以解释因果逻辑，而纯机理模型又难以应对工况波动。智库推动两者深度融合，在高价值设备智能运维、生产过程精准控制、能源优化调度等成熟模式基础上，提供从政策解读、技术选型到落地方案的全链条服务。

具体而言，在智能运维领域，智库团队深入调研 30 余家重点企业，构建“状态监测-故障诊断-预测性维护-备件优化”四级成熟度模型，帮助企业评估现状并规划升级路径。某千万吨级钢铁企业应用该模型后，高炉风机非计划停机时间减少 75%，年节约维护成本超 2000 万元。在工艺优化方面，针对轧钢加热炉燃烧控制、电解铝电流效率优化等痛点，智库联合科研院所开发“工艺机理约束下的强化学习”算法，在保证产品质量前提下降低能耗 3-5 个百分点。智库定期发布《流程工业 AI 应用成熟度指数》，建立行业对标基准，引导企业精准投资。

2. 具身智能与智能装备

国声智库前瞻布局具身智能领域，重点关注人形机器人、四足机器人、智能运载装备、协作机械臂在工业场景的应用落地。IDC 数据显示，2024 年全球四足机器人销售出货量约 2 万台，其中商用级占 27.9%，工业巡检场景成为最快增长点。智库联合产业链上下游主体，推动训练场建设与场景开放，加速技术从“实训”走向“实战”的跨越。

智库研究团队系统梳理具身智能在制造业的潜在应用场景矩阵，识别出物料搬运、质量检测、精密装配、设备巡检四大高优先级场景，并分析各场景的技术成熟度、投入产出比与实施难点。针对人形机器人应用，智库提出“场景分级-能力匹配-渐进导入”的实施策略，建议企业先在环境结构化程度高、任务标准化程度高的场景试点，逐步向复杂非结构化环境拓展。智库与某汽车制造企业合作开展人形机器人总装线应用试点，通过 3 个月实训优化，机器人完成车门装配、线束插接等任务的良品率从初期 72% 提升至 96%，单台机器人可替代 2 名工人，投资回收期约 2.5 年。智库发布的《具身智能工业应用指南》成为行业重要参考。

3. 工业数据治理与资产化

针对工业数据"孤岛化"、"沉睡化"、"低质化"的普遍问题，国声智库提出"数据工程体系"整体解决方案，帮助企业构建覆盖数据设计、采集、清洗、标注、存储、分析、运营的全生命周期管理体系，释放数据要素价值。智库强调，工业数据治理不仅是技术问题，更是组织变革与制度创新问题。

在数据架构设计方面，智库推动企业建立"数据湖+数据仓库+数据集市"的分层架构，统一数据标准与接口规范。某装备制造企业实施该方案后，数据准备时间缩短 70%，跨部门数据共享效率提升 5 倍。在数据质量管理方面，智库引入"数据可信度评级"机制，从完整性、准确性、一致性、时效性、可解释性五个维度建立评估体系，优先治理高业务价值数据。针对数据标注难题，智库推动建立"人机协同标注"模式，利用预训练模型自动标注，专家审核修正，标注成本降低 60%。在数据资产化方面，智库帮助企业完成数据资源盘点、质量评估、价值评估与会计入表，某能源企业在智库辅导下，将 20 年积累的设备运行数据作为无形资产入表，评估价值达 1.2 亿元，开辟数据资产融资新渠道。

（三）机制创新：智库+产业的"旋转门"模式

国声智库充分发挥社会组织机制灵活、资源整合能力强的比较优势，突破传统智库"研究-出版-影响"的线性模式，构建"政产学研用"深度融合的协同创新网络，形成智库与产业双向赋能的"旋转门"机制。

1. 政策翻译与标准研制

智库深度参与《国家人工智能产业综合标准化体系建设指南（2024 版）》《"人工智能+"行动计划》等政策文件的前期研究与后期解读，建立"政策文本-实施细则-操作手册"的三级翻译

机制，将部委文件的宏观导向转化为企业可理解、可执行的实施路径。智库定期举办"政策面对面"研讨会，邀请政策制定者、企业技术负责人、标准化专家共同研讨，消除政策理解偏差。

在标准研制方面，智库关注大模型评测、具身智能、工业高质量数据集、智能体互操作等重点方向，联合行业协会、龙头企业推动团体标准制定，并促进团体标准与行业标准、国家标准的互认与转化。智库牵头制定的《工业大模型应用能力评估规范》团体标准，已被多家央企采纳为供应商选型依据。智库还建立"标准试验验证"机制，在真实工业环境中测试标准适用性，确保标准的科学性与可操作性。

2. 场景对接与生态链接

智库建立"需求方-技术方-资本方"三方高效对接机制，通过深度调研识别高价值应用场景，定期发布《工业人工智能高价值场景清单》（涵盖智能质检、预测性维护、工艺优化、智能排产、能源管理等 12 大类 58 个细分场景），降低供需双方信息不对称。清单不仅描述场景需求，还附技术成熟度、投资回报周期、实施难点等关键信息，为企业决策提供参考。

针对中小企业"不会转、不敢转、不能转"的痛点，智库联合技术服务商开发"轻量化、模块化、低成本"的 AI 解决方案，提供"咨询诊断-方案设计-试点验证-规模推广"的全流程陪伴式服务。智库发起成立"工业 AI 中小企业服务联盟"，整合算力、算法、数据、人才等资源，以云服务模式降低中小企业应用门槛，使年费 5 万元以下的中小企业也能享受 AI 赋能。智库建立的"场景-技术-资本"对接平台，已促成 50 余个工业 AI 项目落地，拉动投资超 10 亿元。

3. 国际视野与本土实践结合

智库设立国际技术跟踪团队，持续监测全球工业 AI 发展动态，特别是欧美"主权 AI"战略、数据跨境流动规则、AI 出口管制政策等对产业链的影响，为企业提供出海合规咨询与本地化策略。针对欧盟《人工智能法案》对高风险 AI 系统的合规要求，智库编制《工业 AI 出海合规指南》，帮助企业识别合规风险并建立治理体系。

同时，智库将依托“一带一路”国际智库合作网络，推动国产工业 AI 解决方案在东南亚、中东、非洲等沿线国家的应用推广。智库组织国内 AI 企业与当地制造企业对接，提供“技术+标准+培训”的综合服务包，助力中国智造“走出去”。在某东南亚国家钢铁产业园项目中，智库协调国内企业与当地合作伙伴共建智能工厂，输出中国工业 AI 标准与最佳实践，项目建成后成为当地智能制造标杆，年产能提升 30%，能耗降低 15%，彰显中国工业 AI 技术的国际竞争力。

专栏：宜兴福鼎环保：AI+危废治理的“安全卫士”

宜兴福鼎环保工程有限公司作为国家高新技术企业，深耕危险废弃物焚烧处置领域，是全应科技“AI+环保”重点合作企业，代表传统环保装备企业向“AI 原生”转型的创新实践。

针对危废成分复杂、热值波动剧烈导致的“工况波动大、污染物排放难控制、人工干预依赖度高”等行业痛点，福鼎环保开发基于大模型的智能燃烧控制系统（AICS）。该系统构建多智能体协同控制架构：通过红外热成像、激光光谱等多模态传感器实时感知炉内三维温度场与烟气成分；利用 Transformer 时序预测模型提前 300 秒预判工况波动；采用“双系统架构”——慢系统负责燃烧策略规划，快系统负责毫秒级给料、配风控制，确保稳定性与响应速度平衡；并设置“物理不可逾越”的安全护栏，确保炉温不低于 850℃、负压波动在±50Pa 范围内。

在江苏某危废处置中心运行数据显示，二噁英排放浓度稳定控制在 0.05ng-TEQ/m³ 以下，优于国标 50%，达到欧盟标准；焚烧热效率提升 5%，吨处置综合能耗降低 8%，年节约运营成本超 200 万元；人工干预频次降低 70%，实现“黑灯工厂”连续稳定运行。

该案例证明，环保装备智能化必须守住“安全底线”与“环保红线”。福鼎环保“安全护栏+智能优化”的技术路线，为高危复杂工业场景提供了可靠的 AI 应用范式，正推动行业从“经验驱动”向“模型驱动”转型。

四、挑战与瓶颈：制约工业 AI 深化的“三重门”

尽管工业人工智能发展势头强劲，技术迭代与场景落地取得显著进展，但向规模化、深层次应用推进过程中，仍面临数据、安全、落地三个维度的结构性制约，形成制约产业高质量发展的“三重门”。

（一）数据之困：高质量工业数据稀缺与流通壁垒

工业数据具有多源异构、高噪声、强机理耦合、时序依赖等显著特征，与消费互联网数据

存在本质差异。首先，工业数据来源复杂，涵盖传感器时序数据、CAD 图纸、工艺规程、设备日志、质检报告等多模态信息，数据格式不统一、时间戳不同步、采样频率差异大，数据清洗与对齐成本极高。中国信通院评估显示，当前行业数据集建设存在显著质量瓶颈，内容稠密性缺失占比高达 82.50%，领域相关性不足占比 14.04%，标注准确性问题占比 3.46%，高质量训练数据呈现严重“饥渴”状态。

其次，数据共享与流通面临制度性障碍。工业数据涉及工艺参数、配方比例、设备状态等核心商业秘密，企业“不愿共享、不敢流通、不会定价”现象突出，形成严重的数据孤岛。调研显示，85%以上的制造企业将生产数据视为核心资产，仅允许内部使用，跨企业数据共享缺乏信任机制与利益分配模式。即便在集团内部，不同子公司间的数据壁垒依然显著，某大型央企拥有数十家工厂，但数据互通率不足 30%，严重制约大模型的跨场景泛化能力。

再次，工业数据标注成本高昂且难以规模化。与图像识别等通用场景不同，工业缺陷样本稀缺（正样本占比通常不足 1%），且需要具备深厚工艺知识的专家进行标注。某汽车零部件企业为建立瑕疵检测数据集，需投入 3 名高级工程师耗时 6 个月完成 2 万张图像标注，单张标注成本超 50 元，且标注质量高度依赖专家经验，难以复制推广。此外，工业数据具有强时效性，设备老化、工艺调整后历史数据可能失效，需持续投入更新维护，进一步加剧数据供给压力。

（二）安全之虑：风险边界模糊与责任界定困难

工业 AI 应用面临现实风险与前沿风险交错的复杂挑战，安全风险边界与事故责任界定尚未明晰，制约技术推广信心。

现实风险层面，大模型的“幻觉”问题在工业场景可能引发严重后果。模型可能生成看似合理但实际错误的工艺参数建议，若未经过严格验证直接下发至控制系统，可能导致产品质量批次报废甚至设备损坏。2025 年行业测试显示，主流工业大模型在处理未见过的工艺异常时，错误率高达 15%-20%。同时，模型的鲁棒性不足，面对传感器噪声、数据分布偏移（如原料成分

波动)时,输出结果可能出现剧烈抖动,而工业控制系统要求极高的稳定性与可预测性。此外,推理思维链的暴露可能泄露企业工艺秘密,某化工企业测试发现,大模型在解释决策逻辑时可能间接暴露关键工艺参数。

前沿风险层面,部分先进大模型已展现出"拒绝关闭"、"策略欺骗"等自主性风险苗头。2025年权威测试显示,Claude Opus 在高压测试场景下,为规避被替代风险,产生高达 84%的策略欺骗行为,试图隐藏真实能力或规避监控。虽然当前工业 AI 系统尚未达到此智能水平,但随着智能体自主性增强,可能出现目标错位、工具滥用等不可预测行为。工业场景对安全性要求极高,化工、能源等领域的单次误判可能引发爆炸、泄漏等重大安全事故,造成巨大经济损失与人员伤亡。

责任界定方面,当 AI 系统参与决策并导致事故时,责任在算法开发者、系统集成商、设备制造商与最终用户之间的划分缺乏明确法律框架。现行《产品质量法》《安全生产法》主要针对传统机械设备,对 AI 系统的"黑箱"特性与自主决策行为缺乏适应性条款,企业担心承担不可预估的法律风险,采取保守观望态度。

(三) 落地之难:从"盆景"到"风景"的规模化鸿沟

当前工业 AI 应用多处于试点示范阶段,呈现"点状开花、面状稀疏"特征,规模化推广面临成本、人才、标准三重制约,存在从"盆景"到"风景"的转化鸿沟。

成本门槛方面,中小企业难以承担 AI 转型的全链条投入。算力基础设施方面,训练行业垂直大模型需采购或租用高性能 GPU 集群,单次训练成本动辄数百万元;模型微调与部署需持续投入算法工程师团队,年人力成本超百万元;更关键的是系统集成成本,将 AI 模型与现有 PLC、DCS、MES 等工业控制系统深度集成,需改造通信协议、重构数据流,某中型制造企业实施 AI 质检项目,软硬件投入仅占 40%,系统集成与产线改造费用高达 60%,且需停产配合,机会成本高昂。

人才缺口方面，既懂工业机理又懂 AI 算法的复合型人才极度稀缺。传统 IT 工程师缺乏热力学、材料学、化工原理等领域知识，难以理解工艺约束；而工艺专家虽熟悉生产流程，却缺乏数据科学与算法建模能力。教育部数据显示，全国高校人工智能专业毕业生年均不足 2 万人，具备工业背景的不足 10%，人才供需比达 1:10 以上。企业面临“招不到、养不起、留不住”的困境，某地方调研显示，工业 AI 算法工程师平均年薪较普通软件工程师高 40%，且流动率高达 25%，中小企业难以承受。

标准缺失方面，工业 AI 产品服务缺乏统一评价标准与互操作规范，用户选型困难且风险高企。当前市场上大模型产品性能参差不齐，但缺乏权威第三方评测体系，企业难以评估模型真实能力；智能体接口标准不统一，不同厂商系统难以互联互通，形成新的“软烟囱”；数据格式、通信协议、安全规范的差异导致“数据孤岛”向“模型孤岛”演变。此外，工业 AI 项目的投资回报评估缺乏标准方法论，企业难以量化测算效率提升与成本节约，影响投资决策信心。这些制约因素相互交织，导致工业 AI 应用呈现“大企业试点热、中小企业观望冷”的分化态势，亟需通过政策引导、模式创新与生态培育打破瓶颈，推动产业从示范走向普及。

五、政策建议与实施路径：构建工业 AI 高质量发展的“四梁八柱”

基于前述分析，工业人工智能发展已进入由“技术验证”向“规模应用”转段的关键期，亟需通过系统性制度创新破解数据瓶颈、安全顾虑与落地难题。结合国声智库在政策研究、产业咨询与生态构建方面的专业积累，提出构建以数据治理为基、场景牵引为要、安全可信为先、生态协同为重、要素支撑为实的“四梁八柱”政策框架，推动工业 AI 从“试点示范”迈向“全面赋能”。

（一）构建“1+N”工业 AI 数据治理体系，破解数据瓶颈

数据是工业 AI 发展的核心生产要素，针对当前高质量工业数据稀缺、流通壁垒高筑的痛点，建议构建“1 个国家级资源池+N 个行业数据空间”的治理体系，打通数据供给与流通的“任督

二脉"。

1. 建设国家级工业数据资源池与行业数据空间

依托国家数据局统筹协调职能，在钢铁、石化、汽车、能源、电子信息等重点行业，分阶段建设高质量工业训练数据集与行业级数据空间。采取"政府引导+企业共建+市场化运营"的多元化建设模式：政府负责顶层设计与标准制定，提供初期建设资金与政策支持；龙头企业贡献脱敏后的高质量工艺数据、设备运行数据与质量检测数据，享有数据使用权与收益权；第三方专业机构负责技术运营，通过隐私计算、联邦学习、可信执行环境（TEE）等技术实现"数据可用不可见、数据可控可计量"。

参考中国信通院 ADAQ（人工智能数据质量）评估体系，建立工业数据质量五级分类认证标准，从数据完整性、准确性、一致性、时效性、可解释性五个维度设定量化指标，对入库数据进行严格质检与分级标注。建立数据贡献激励机制，对提供高质量数据的企业给予税收抵扣、项目申报优先支持等政策奖励。力争到 2027 年，建成覆盖 10 个以上重点行业、数据规模超 10PB 的国家级工业数据资源池，形成支撑千亿参数级工业大模型训练的数据底座。

2. 全面推行"数据工程"贯标行动

制定并发布《工业人工智能数据工程实施指南》国家标准，明确工业数据全生命周期管理的技术规范与最佳实践。引导企业建立覆盖数据设计（Data Design）、数据采集（Data Collection）、数据清洗（Data Cleaning）、数据标注（Data Annotation）、数据增强（Data Augmentation）、数据存储（Data Storage）、数据运营（Data Operation）的"7D"管理体系。

实施"工业数据治理成熟度评估"专项行动，对标 CMMI（能力成熟度模型集成）体系，建立五级成熟度模型，对达到三级以上企业给予数字化改造补贴。鼓励龙头企业发挥"链主"作用，通过工业互联网平台向上下游中小企业开放脱敏数据接口，构建产业级数据共享生态。支持中小企业通过数据信托（Data Trust）、数据空间（Data Space）等新型基础设施参与数据流通，降低数据入池门槛。建立工业数据资产登记确权制度，探索数据资源持有权、数据加工使用权、

数据产品经营权"三权分置"的产权运行机制，为企业数据资产入表、质押融资、交易流通提供制度保障。

3. 大力发展合成数据与智能生成技术

针对工业场景数据采集成本高、危险性大、隐私敏感等痛点，支持基于世界模型（World Model）、物理仿真、生成式 AI 的合成数据生成技术研发。在航空航天、核工业、深海探测等高风险、高成本领域，建立"虚实融合"的数据生成工厂，通过高保真数字孪生环境生成涵盖正常工况、边界条件、异常状态的海量训练数据。

设立合成数据技术研发专项，支持企业开发基于扩散模型（Diffusion Model）、神经辐射场（NeRF）的工业场景生成工具，生成带精确标注的典型缺陷样本、工艺参数组合与设备故障案例。建立合成数据质量评估标准，确保合成数据与真实数据的分布一致性（Distribution Alignment）与物理合理性（Physical Plausibility）。探索"真实数据+合成数据"的混合训练模式，在保障核心工艺秘密前提下，将合成数据比例提升至训练集的 30%-50%，显著降低对真实数据的依赖，缩短模型开发周期。

（二）创新"场景牵引"推进机制，加速规模化应用

应用场景是技术迭代的催化剂与价值实现的载体。针对当前工业 AI"试点热、推广冷"的现状，建议建立"场景清单牵引、供需精准匹配、成本合理分担"的推进机制，加速技术从"盆景"向"风景"转化。

1. 建立工业 AI"场景机会清单"发布机制

建议工业和信息化部联合中国钢铁工业协会、中国石油和化学工业联合会、中国机械工业联合会等行业协会，按年度编制发布《工业人工智能高价值场景目录》。目录编制遵循"技术成

熟度可行、经济效益可量化、实施风险可控"原则，聚焦研发设计、中试验证、生产制造、质量管控、营销服务、运营管理、安全生产等全价值链环节，筛选识别出 50-80 个高价值应用场景。

每个场景明确技术需求规格（如模型响应延迟、预测准确率、可解释性要求）、数据基础条件（数据量、数据质量、接口标准）、预期经济效益（投资回收期、成本降低率、效率提升幅度）与实施难点提示。搭建"揭榜挂帅"线上对接平台，组织技术供给方（AI 企业、科研院所）与场景需求方（制造企业）精准匹配，对成功落地且成效显著的项目给予专项资金支持。建立场景应用效果第三方评估机制，定期发布《工业 AI 场景应用成效报告》，形成示范引领效应。

2. 深入实施"智改数转网联"专项工程

设立工业人工智能应用专项基金，规模建议不低于 100 亿元，重点支持中小企业"智能化改造、数字化转型、网络化联接"。对中小企业购买 AI 云服务、智能体解决方案、轻量化工业 APP 给予 30%-50%的购置补贴，对采用"模型即服务"（MaaS）模式按调用量给予用算补贴。推广"轻量化、模块化、微服务化"部署模式，支持企业通过低代码平台快速构建 AI 应用，降低对 IT 基础设施的一次性投入。

实施"工业 AI 万企赋能"行动，力争到 2027 年，规模以上工业企业 AI 应用渗透率达到 50% 以上，其中中小企业 AI 应用普及率达到 30%以上。建立"智改数转"城市试点，支持苏州、宁波、佛山等制造业基础好的城市开展全域智能化改造，形成可复制推广的经验模式。推动工业互联网平台与 AI 大模型深度融合，打造 100 个以上"平台+AI"创新应用示范，实现从设备级智能到工厂级智能的跃升。

3. 打造国家具身智能实训基地与场景开放矩阵

在京津冀、长三角、粤港澳大湾区、成渝地区双城经济圈建设 4-6 个国家级具身智能训练场与实训基地，面向汽车制造、电子装配、物流仓储、危险作业等行业开放真实工业场景。基地配备多形态机器人（人形机器人、四足机器人、协作机械臂）、多模态感知设备（视觉、力觉、触觉传感器）与数字孪生训练环境，为机器人企业提供"数据采集-技能训练-场景验证-性能

评测"的全链条服务。

推广"机器人即服务"（RaaS）商业模式，支持企业通过租赁方式使用具身智能装备，按作业量或时间付费，降低企业应用具身智能的初期投入门槛。建立人形机器人、四足机器人等新型智能装备的准入测试标准与认证体系，制定《工业环境用机器人安全要求》强制性国家标准，设置机械安全、电气安全、功能安全、网络安全四维检测指标，确保装备在复杂工业环境下的安全可靠运行。到 2027 年，建成 30 个以上万人级机器人训练场，培育 100 家以上具身智能示范应用企业。

（三）筑牢安全治理防线，建立可信 AI 生态

安全是工业 AI 规模化应用的生命线。针对模型幻觉、对抗攻击、自主性风险等挑战，建议构建覆盖研发、部署、运营全生命周期的安全防护体系与治理框架。

1. 建立工业 AI 安全风险评估与准入制度

参照中国信通院"方升"大模型安全基准测试框架，制定《工业人工智能系统安全评估规范》国家标准与行业标准。建立分级分类安全评估机制：对应用于一般辅助决策场景的 AI 系统，实行企业自评估与第三方备案；对应用于关键基础设施、高危作业环节（如化工反应控制、高压电网调度、核电设备运维）的 AI 系统，实施强制性第三方安全测评与行政许可。

安全测评重点检测四大类指标：一是模型幻觉率（Hallucination Rate）与事实准确性，确保工艺参数建议的物理合理性；二是对抗攻击鲁棒性（Adversarial Robustness），检测在传感器噪声、数据污染情况下的输出稳定性；三是极端场景可靠性（Edge Case Reliability），验证在设备故障、原料异常等边界条件下的 fail-safe 机制；四是供应链安全（Supply Chain Security），审查训练数据来源、模型组件依赖与开源代码漏洞。建立工业 AI 系统"安全护照"制度，只有通过测评的系统方可进入政府采购与央企采购目录。

2. 构建全生命周期安全防护技术体系

研发阶段：实施"负责任的人工智能开发"（Responsible AI Development）准则，加强训练数据治理，剔除偏见数据与有害内容；采用价值对齐（Value Alignment）技术，通过 RLHF（基于人类反馈的强化学习）与 Constitutional AI（宪法 AI）方法，确保模型行为符合工业安全规范与伦理要求。

部署阶段：建立"安全护栏"（Guardrails）机制，在 AI 模型与工业控制系统之间设置安全隔离层，对模型输出进行物理约束检查与逻辑验证；部署实时监测与异常检测系统，利用可解释 AI（XAI）技术追踪模型决策逻辑，及时发现"黑天鹅"行为；推行 AI-SBOM（人工智能软件物料清单）制度，实现从训练框架、基础模型、微调数据到推理引擎的全供应链安全可追溯。

运营阶段：建立人机协同的异常处置机制，在关键决策环节保留“人在环”（Human in the Loop）暨人类专家的审核权与否决权，设置"一键熔断"机制，在检测到异常风险时立即切换至人工模式；建立持续学习与模型更新机制，定期用新采集的工业数据对模型进行微调，防止模型性能退化；建立安全事件应急响应体系，制定 AI 系统故障应急预案，定期开展攻防演练。

3. 完善数据安全与隐私保护合规机制

严格落实《生成式人工智能服务管理暂行办法》《人工智能生成合成内容标识办法》《数据安全法》《个人信息保护法》等法规要求，在工业 AI 系统中嵌入不可见数字水印与隐式标识技术，确保 AI 生成的设计图纸、工艺方案、检测报告可追溯、可鉴别。建立工业数据分类分级保护制度，将工艺配方、核心参数、客户信息列为核心数据，实行本地化存储、私有化部署与加密传输；将一般性设备运行数据列为重要数据，实行严格访问控制；将公开的行业标准、市场信息列为一般数据，允许适度共享。

建立工业 AI 系统的数据跨境流动安全评估机制，对涉及关键行业数据的出境活动进行安全审查。推行"隐私计算+边缘计算"架构，在设备侧完成敏感数据处理，减少原始数据上传。建

立 AI 安全责任保险制度，鼓励保险公司开发"工业 AI 产品责任险""算法故障险"等新型险种，分散企业应用风险。

（四）强化智库支撑与生态协同，提升产业服务能力

智库是连接政策、学术与产业的桥梁。建议发挥高端智库在政策研究、标准研制、生态链接方面的独特作用，构建多层次、网络化的产业服务体系。

1. 设立"工业 AI 智库联盟"与协同研究网络

筹划由国声智库联合中国信息通信研究院、中国电子信息产业发展研究院（赛迪研究院）、国家工业信息安全发展研究中心、中国科学院自动化研究所等权威机构，发起成立"工业人工智能智库联盟"。联盟设立战略研究、技术标准、产业经济、国际治理四个专业委员会，建立常态化协同研究机制。

联盟重点开展三方面工作：一是前瞻性政策研究，围绕工业智能体经济、AI 驱动的生产关系变革等前沿议题开展储备性研究，每季度发布《工业 AI 政策动态与趋势研判》；二是标准体系研究，编制《工业人工智能产业发展白皮书》《工业智能体应用指南》《工业 AI 伦理准则》等系列成果，打造权威发布平台与行业"风向标"；三是评估评价服务，建立工业 AI 企业竞争力评价模型与区域产业发展指数，为政府决策与企业对标提供参考。

2. 创新"智库+产业"深度协同机制

建立智库专家与制造业企业的"旋转门"制度，推动研究人员深入工厂一线开展长期驻点调研，将论文写在车间里，将研究成果转化为解决方案。支持智库联合龙头企业共建"联合创新中心"，在工艺优化、质量检测、预测性维护等场景开展联合技术攻关、标准研制与人才培养。建立"智库咨询+工程实施"的一体化服务模式，智库负责顶层规划与方案设计，合作技术企业负责

系统集成与实施交付，形成从战略到执行的闭环服务。

设立"工业 AI 观察员"制度，聘请一线工程师、技术专家、企业管理者担任智库特约研究员，及时捕捉产业痛点与技术趋势，增强研究的实践针对性。建立智库研究成果的转化应用机制，对具有政策价值的建议通过内参渠道报送决策部门，对具有市场价值的方案通过孵化器转化落地。

3. 构建开源开放的技术生态体系

大力支持国产开源社区建设，推动魔搭（ModelScope）、OpenI 启智、Gitee 等本土平台发展，鼓励企业将非核心工业大模型、行业数据集、开发工具链开源开放。建立"开源贡献积分"制度，对贡献高质量代码、数据集、评测工具的企业和个人给予税收优惠、项目申报加分、人才评定倾斜等激励。

设立工业 AI 开源基金会，参照 Apache 基金会、Linux 基金会的治理模式，吸纳华为、阿里、百度、DeepSeek 等龙头企业作为白金会员，制定开源项目的知识产权规则、伦理审查流程与安全治理规范。定期举办工业 AI 开源大赛，围绕特定工业场景（如轴承故障诊断、焊接缺陷检测）发布开源任务，吸引全球开发者参与，提升国产开源项目的技术水平与国际影响力。建立开源软件的供应链安全监测机制，及时修复漏洞，防范安全风险。

（五）完善人才培养与金融支持体系

人才与资金是工业 AI 发展的关键要素。建议构建"产教融合育人才、多元金融强支撑"的保障体系，破解制约产业发展的要素瓶颈。

1. 实施"工业 AI 工匠"培育计划与教育体系改革

建议教育部联合工业和信息化部、人力资源和社会保障部，在高等职业院校、应用型本科高校开设"工业人工智能"微专业与交叉学科方向，设计"工业机理+AI 算法+工程实践"三位一体的课程体系。核心课程涵盖工业大数据分析、工艺机理建模、机器学习应用、工业软件开发、智能装备运维等模块，强化学生的跨学科能力。

推行"现代产业学院 2.0"建设，支持高校与龙头企业（如宝钢、中石化、海尔、格力）、专精特新"小巨人"企业（如全应科技、福鼎环保）共建产业学院，实行"双导师制"（学校导师+企业导师）与"二元制"培养（在校学习+企业实训）。学生在三年级即进入企业真实场景完成毕业设计 with 项目实践，实现"入学即入岗、毕业即就业"的订单式培养。

支持企业开展在岗职工的"AI+技能"转岗培训，将智能体使用、数据标注、Prompt 工程、基础算法调优等纳入职业技能等级认定范围，对取得相应等级证书的职工给予培训补贴。设立"工业 AI 技能大师工作室"，评选表彰既精通传统工艺又掌握 AI 技术的复合型高技能人才，弘扬工匠精神。力争到 2027 年，培养工业 AI 复合型技术人才 10 万人以上，培训在岗职工 100 万人次以上。

2. 创新科技金融支持与商业模式

开发"AI 技改贷""智改专项债""工业 AI 融资租赁"等专属金融产品，支持企业通过贷款、发债、租赁等多元化方式融资，用于 AI 设备购置、系统开发与集成改造。对工业 AI 技改项目给予贷款贴息支持，降低企业融资成本。

探索"按效果付费"（Outcome-based Pricing）的商业模式创新，鼓励 AI 技术服务商与制造企业签订对赌协议，共担实施风险、共享收益成果。例如，在节能降耗场景中，按实际节约的能源费用比例收取服务费；在质量检测场景中，按漏检率降低幅度与效率提升幅度收取费用。这种模式既降低了企业的初期投入风险，又激励服务商确保应用效果。

引导国家制造业转型升级基金、国家中小企业发展基金、地方产业引导基金加大对工业 AI"硬科技"企业的投资力度，重点支持拥有自主知识产权的工业软件、智能装备、核心算法企业。

支持符合条件的工业 AI 企业上市融资，在科创板、北交所开辟绿色通道。建立工业 AI 产业投融资服务平台，定期举办项目路演与资本对接会，提高投融资效率。

（六）创新"基金+平台"协同机制，构建五维融合生态

当前工业 AI 发展面临"技术孤岛化、产业碎片化、金融泛化化"的结构性矛盾，亟需构建以技术策源、产业升级、金融赋能、人才培育、组织协同为支柱的五维融合范式，打通从实验室到生产线的"最后一公里"。

1. 设立国家级工业人工智能产业投资基金群

建议由国家制造业转型升级基金、中国国有企业结构调整基金（国调基金）、国家集成电路产业投资基金（大基金）等国家级基金发起，联合地方引导基金、产业龙头企业、金融机构，设立工业 AI 产业母基金（目标规模 100-200 亿元），采用"母基金+区域子基金+行业子基金"的立体架构：

区域子基金：聚焦京津冀、长三角、粤港澳大湾区、成渝双城经济圈等制造业集聚区，与"具身智能实训基地"联动布局，形成"基金投资+基地建设+产业集聚"的闭环生态，重点支持本地化"智改数转"项目与区域特色产业集群的智能化升级。

行业子基金：针对钢铁、石化、化工、环保、能源等细分垂直领域，投资具有高价值场景解决方案能力的"专精特新"企业，重点支持如全应科技（热电智能化）、福鼎环保（危废处置 AI）、天准科技（工业视觉）等已在细分领域建立优势的企业的跨区域复制、产业链纵向并购与技术迭代升级。实行"投早投小投硬科技"的宽容失败机制，建议设定 20% 的容错率，允许因技术路线探索失败导致的合理投资损失。

创新退出与循环机制：探索 REITs（基础设施领域不动产投资信托基金）模式在工业 AI

领域的应用，将智能工厂、AI 训练场、智算中心等重资产项目资产证券化，盘活存量资产，形成"投资-建设-运营-证券化退出-再投资"的良性循环，提高资本周转效率。

2. 构建"概念验证-中试熟化-产业应用"的高校技术转化体系

突破单一人才培养视角，强化高校作为工业 AI 技术策源地的核心功能：

建设工业 AI 概念验证中心（PoC Center）：在清华大学、哈尔滨工业大学、浙江大学、上海交通大学和西北工业大学等工科强校设立校级概念验证平台，由政府引导基金、产业子基金、龙头企业共同出资，配备工程化团队与试验场地。针对实验室阶段的算法原型，开展工厂级可行性验证、工艺适配性测试与经济性评估，弥合"论文-产品"之间的鸿沟，降低技术转化的早期风险与不确定性。

建立中试熟化基地：依托国家大学科技园、高新技术产业开发区，建设专业化中试基地，为高校科研成果提供工程化开发、产品化定型、小批量试制的全链条服务，解决"中试空白"难题。

深化"旋转门"人才流动机制：允许高校教师保留基本编制参与产业基金投资评审或入企担任首席科学家、技术顾问，允许企业资深工程师到高校担任产业教授、兼职博导，打破体制内外身份壁垒，促进理论知识与工程实践的双向流动与深度融合。

3. 发挥行业社会组织"生态枢纽"与治理功能

将分散的行业协会、学会、产业联盟升级为制度化、实体化的生态协同平台：

成立中国工业人工智能产业联盟：由国声智库联合中国信通院、中国钢铁工业协会、中国石油和化学工业联合会、中国循环经济协会、中国智能制造系统解决方案供应商联盟等共同发起，设立标准推进、安全伦理、数据治理、产融合作四个专业委员会，对应本报告数据治理、安全监管、金融支持等核心内容，形成政策传导、标准制定、行业自律的"超级节点"。

设立工业 AI 开源基金会与数据信托机构：参照 Linux 基金会模式，吸纳产业链上下游企业为会员，治理开源模型的知识产权与伦理风险；由行业协会作为受托人发起设立工业数据信托，管理成员企业的工艺数据资产，建立"数据托管-收益分配-风险隔离"的合规流通机制，解决"数据不愿共享、不敢流通"的制度性难题，为工业大模型训练提供可持续的高质量语料供给。

建立行业自律与伦理审查机制：制定《工业人工智能伦理公约》，设立伦理审查委员会，对涉及安全生产、就业替代、环境影响等重大问题的 AI 应用进行伦理评估，引导产业健康发展。

【专栏】产业基金与协同创新平台——工业 AI 生态的"连接器"

工业 AI 的产业化不仅需要技术突破，更需资本、人才、组织的系统耦合。国声智库建议构建"基金引导+平台运营+场景落地"的协同范式，打造连接政策、技术、产业、金融、高校的"旋转门"。

产业基金方面，建议设立工业 AI 场景创新基金，采用"政府引导出资 20%+社会资本 80%"结构，重点投向两类标的：一是如全应科技般的"机理+数据"双驱动解决方案商，支持其从单点示范向跨区域复制扩张；二是具身智能、工业软件等"卡脖子"环节的早期项目。基金实行"赛马机制"与"对赌豁免"，允许技术路线试错，通过"优先股+可转债"组合设计平衡风险与收益。针对福鼎环保等环保装备企业，探索"绿色 AI 基金"定向支持，将碳减排收益与基金回报挂钩。

平台组织方面，建议依托全应科技、福鼎环保等龙头企业，联合中国节能协会、中国电力企业联合会等行业组织，共建"AI+流程工业"产业创新共同体。该共同体由智库提供政策与标准支撑，高校负责算法研发与人才培养，基金提供融资与并购服务，形成"技术攻关-中试验证-规模推广"的闭环。例如，针对福鼎环保的危废焚烧场景，共同体可组织高校环境工程系优化燃烧算法、基金公司提供智能设备融资租赁、行业协会制定 AI 安全运行标准，实现从单点示范到行业标配的跃迁；针对全应科技的热电场景，可通过共同体对接高校热动专业共建数字孪生实验室，对接产业基金支持其"热电云"平台的行业垂直整合。

此类平台将成为连接本报告所述"政策翻译器"与"产业连接器"的生态枢纽，通过"技术-产业

-金融-高校-社会组织"多维协同，加速工业 AI 从"盆景"向"风景"的规模化扩散，为制造强国建设提供可持续的生态系统支撑。

六、结论与展望：迈向"人机协同"的工业新纪元

工业人工智能正站在从"技术可用"到"价值兑现"的关键拐点，产业演进呈现加速跃迁态势。据中国信息通信研究院预测，2026 年我国人工智能核心产业规模将突破 1.5 万亿元，工业互联网平台普及率将超过 45%，工业 AI 应用将从当前的试点探索全面转向规模化推广。随着 DeepSeek-V3、Qwen3 等国产大模型在工业场景的深度适配，以及 30 余个具身智能训练场的网络化布局，技术供给与产业需求的"剪刀差"正在快速收敛。这一历史性窗口期，要求政策制定者、制造企业、技术供应商与智库机构形成高度共识与协同行动，把握全球制造业智能化转型的战略机遇，在新一轮科技革命与产业变革中占据制高点。

展望 2026 年及"十五五"时期，工业人工智能将呈现三大确定性趋势：一是从单点应用向系统重构演进，AI 将超越工具属性，深度融入企业战略规划、组织架构重塑与商业模式创新，催生具备"自感知、自决策、自执行"能力的"智能原生"新型工业化企业，预计将有超过 30% 的规模以上工业企业建立 AI 驱动的决策中枢，工业智能体成为企业新型"数字员工"；二是从数据驱动向数据与知识联合驱动跃迁，基于 MoE 架构的行业大模型与物理信息"小模型"将深度融合工艺机理与数据智能，VLA 端到端架构推动具身智能在装配、搬运等场景规模化落地，形成"物理世界与数字世界"的协同与实时闭环，工业软件与 AI 的边界趋于模糊，"AI+工业软件"一体化解决方案成为主流，8/6 比特有限精度 AI 芯片显著降低 AI 应用成本和功耗必将推进工业 AI 广泛的边缘应用；三是从企业内向产业链协同扩展，通过多智能体协同决策机制与区块链赋能的信任体系，实现跨企业的计划协同、产能共享与库存优化，工业互联网平台进化为"产业智能体网络"，供应链响应速度预计提升 40% 以上，资源配置效率实现质的飞跃，产业集群整体竞争力显著增强。

新型智库将持续发挥思想引领、服务市场、机制灵活的比较优势，聚焦工业人工智能前沿趋势与落地实践，打造高端智库品牌。建议政府部门加强顶层设计，完善"1+N"数据治理体系与安全监管框架，加大"智改数转"专项基金对中小企业的倾斜力度，建立工业 AI 安全评估与准入的强制性标准；建议制造企业把握历史机遇，加快构建"首席 AI 官"制度，推动 AI 应用从生产辅助环节向核心工艺环节渗透，培育内部 AI 工程化能力，建设企业级数据资产管理体系；建议技术供应商深耕垂直场景，摒弃"技术万能论"，提供符合行业安全标准、可解释、可审计的"能用、好用、敢用"解决方案，建立与客户共担风险、共享收益的长期合作机制，推动商业模式从"卖软件"向"卖服务"转型。各方协同发力，共同推动我国工业人工智能产业高质量发展，为制造强国、网络强国、数字中国建设贡献坚实力量。

- [1] “《工业人工智能技术与产业发展趋势报告》发布，助力民营经济数智化转型”。新华网，2025 年 12 月 24 日
- [2] “人工智能与数智能源创新发展研讨会暨工业人工智能实验室筹备会议”，2025-01-14
- [3] 何明一，保铮.《神经网络与信号处理系统: 有限精度设计理论》，西北工业大学出版社，1998
- [4] 《人工智能产业发展研究报告（2025 年）》，中国信息通信研究院. 2026-02-03
- [5] 《人形机器人创新发展指导意见》，工业和信息化部，工信部科〔2023〕193 号