工业大模型赋能制造业数字化转型的路径与对策

秦　峥[1]，李育涛[2]，郭淑芳[1]

（1. 国家工业信息安全发展研究中心，北京　100040；
2. 中国科学院大学，北京　100049）

摘　要：在全球制造业加速迈向数字化、智能化的背景下，工业大模型作为新一代智能技术，正成为推动制造业数字化转型的重要引擎。通过系统梳理工业大模型的概念、发展脉络和发展现状等基础理论，提出工业大模型赋能制造业数字化转型的理论框架，并详细阐述工业大模型在研发设计、生产制造、运维服务、经营管理和供应链管理等制造业典型应用场景的赋能作用。针对工业大模型在深度应用过程中所面临的高质量训练数据匮乏、工业场景分布碎片化、工业应用鲁棒性欠缺、关键场景风险需警惕和计算与系统能力不足等挑战，进一步探讨其赋能制造业数字化转型的方法路径，并从政策机制、示范引领、标准体系、自主创新、安全韧性和人才培养等多个维度提出对策建议，以期为工业大模型驱动制造业高质量发展提供有价值的参考和启示。

关键词：工业大模型；制造业；数字化转型；人工智能

中图分类号：TP391. 9　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 07. 006

引用格式：秦峥，李育涛，郭淑芳. 工业大模型赋能制造业数字化转型的路径与对策［J］. 网络安全与数据治理，2025，44(7)：36 - 42.

The path and countermeasures of empowering manufacturing digital transformation with industrial large models

Qin Zheng[1], Li Yutao[2], Guo Shufang[1]

(1. China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China;
2. University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Against the backdrop of the global manufacturing industry accelerating towards digitization and intelligence, industrial large models, as a new generation of intelligent technology, are becoming an important engine for promoting the digital transformation of the manufacturing industry. The concept, development context, and current status of the industrial large model are systematically reviewed, and a theoretical framework for empowering the digital transformation of the manufacturing industry with the industrial large model is proposed. The empowering role of the industrial large model in typical application scenarios of the manufacturing industry, such as research and development design, production and manufacturing, operation and maintenance services, business management, and supply chain management, is elaborated in detail. In response to the challenges faced by industrial large models in the process of deep application, such as the lack of high-quality training data, fragmented distribution of industrial scenarios, lack of robustness in industrial applications, vigilance against key scenario risks, and insufficient computing and system capabilities, this paper further explores the methods and paths to empower the digital transformation of the manufacturing industry, and proposes countermeasures and suggestions from multiple dimensions such as policy mechanisms, demonstration guidance, standard systems, independent innovation, safety resilience, and talent cultivation, in order to provide valuable reference and inspiration for industrial large models to drive the high-quality development of the manufacturing industry.

Key words: industrial large models; manufacturing; digital transformation; artificial intelligence

0 引言

当前，全球制造业正经历深刻的数字化与智能化变革[1]，工业大模型作为人工智能技术与制造业深度融合的核心技术，正在以前所未有的深度和广度重塑产业链、供应链及价值链体系[2]。依托深度学习、自然语言处理与多模态感知等前沿技术，工业大模型具备强大的数据处理、知识推理与智能决策能力，能够打破数据孤岛，构建跨企业、跨环节、跨场景的智能协同体系。工业大模型强大的泛化能力与自主学习特性，显著提升制造企业的生产效率与资源配置效率，助力其实现高效化、柔性化转型，增强整体竞争力[3]。

尽管工业大模型在制造业的应用前景广阔，但其发展仍面临诸多挑战[4-5]。制造业数据高度异构、复杂多样，实现高效整合与智能应用仍存在技术瓶颈。模型的可解释性、安全性和适用性亦亟待提升，以确保其在实际生产环境中的稳定性与可控性。同时，从政策和产业生态的角度来看，当前工业大模型的标准体系不完善、产业链协同机制不健全，也制约了其规模化推广[6-8]。

基于此，本文聚焦工业大模型赋能制造业数字化转型的路径，构建理论分析框架，系统梳理其典型应用场景与关键痛点问题，深入探讨赋能机制与落地路径，提出推动其规模化应用的政策与技术举措。旨在为工业大模型在制造业中的有效落地提供理论支撑与实践参考，助力制造业向智能化、绿色化、高质量方向发展。

1 工业大模型的基础理论

1.1 工业大模型的基础概念与发展脉络

工业大模型是指基于深度学习、自然语言处理、多模态感知等人工智能技术，针对制造业领域构建的大规模预训练模型。工业大模型通过整合海量工业数据，包括设计图纸、传感器数据、设备日志、生产工艺参数等，形成具有行业知识理解、智能推理、优化决策能力的通用人工智能模型。与传统的工业智能系统相比，工业大模型具备更强的泛化能力、跨场景适应能力和自主学习能力，能够在复杂制造环境中实现智能优化、预测分析和自主决策，为制造业的数字化、智能化升级提供强大支撑。

工业大模型的发展可以追溯至人工智能在制造业的应用历程，经历了从基于专家系统的智能制造，到机器学习驱动的工业智能，再到大规模预训练模型主导的智能制造新时代的演进。早期的工业智能系统依赖于专家知识和规则推理，例如20世纪80年代的计算机辅助设计（CAD）与计算机集成制造（CIM）系统，主要基于逻辑规则和数学建模来优化生产流程。然而，这类方法存在知识获取瓶颈，难以适应复杂多变的制造环境。进入21世纪，随着大数据、物联网和云计算的发展，数据驱动的机器学习方法逐渐成为工业智能的主流。工业4.0浪潮推动了智能制造的发展，深度学习、强化学习等人工智能方法开始应用于制造过程优化、设备预测性维护、质量检测等领域，但仍然面临数据孤岛、模型迁移困难、缺乏通用性等挑战。

近年来，预训练大模型的快速发展为工业智能化注入了新的动能。以OpenAI的GPT、Google的PaLM，以及国内的DeepSeek、文心一言、通义千问等为代表，大模型技术正加速向工业领域延伸，深度融合推动了工业人工智能应用的跃升。在此背景下，全球主要工业强国正加快推进大模型在工业领域的垂直落地，加快工业大模型的研发与应用，推动制造业向智能化、自动化方向迈进，力图抢占未来智能制造的技术高地。表1详细列出了当前全球主流工业大模型的相关情况。

表1 全球主要工业大模型

序号	工业大模型	厂商	国家
1	Predix	GE	美国
2	盘古大模型	华为	中国
3	Industrial Copilot	Siemens	德国
4	DeepMind	Alphabet	美国
5	九天工业大模型	中国移动	中国
6	通义千问	阿里巴巴	中国
7	Joule	SAP	德国
8	COSMO-GPT	卡奥斯	中国
9	AbilityGenix	ABB	瑞士
10	Omniverse	NVIDIA	美国
11	Industrial Copilot	Microsoft	美国
12	根灵工业大模型	树根数联	中国
13	羚羊工业大模型	科大讯飞	中国
14	Autodesk Fusion 360	Autodesk	美国
15	Monitron	Amazon	美国

1.2 工业大模型与通用大模型的主要区别

在大模型技术迅速发展的背景下，通用大模型与工业大模型在架构设计、数据组织、语义建模、应用场景和部署方式等方面呈现出明显差异。通用大模型追求跨领域通用性与语言生成能力，其核心在于“理解自然语言+生成内容”；而工业大模型强调工业知识结构化、语义建模深度和与现场系统的深度融合，是制造业智能化转型的重要支撑技术，属于“AI+工业”的典型代表。两者主要区别体现在以下几个方面：

（1）技术架构侧重点不同

通用大模型依托大规模Transformer结构，强调模型规模、语料广度和跨领域能力，目标是实现“通用智能”，支持多任务、多模态理解与生成。而工业大模型则更关注领域适配与部署落地，通常在通用模型基础上引入工业知识图谱、微调模块和多源接口，强调低延迟、强稳定、可解释与业务嵌入，服务于具体的工业场景需求。

（2）数据来源与治理方式不同

通用大模型主要依赖海量网络文本，数据广泛但结构松散，治理方式偏重语料清洗与规模扩张。相比之下，工业大模型基于工业设备、传感器、工艺流程、行业标准等数据，具备高专业性与强结构化特征，需要构建面向工业场景的数据中台，重视数据时效性、一致性与安全性。

（3）工业语义建模能力要求更高

通用模型擅长自然语言处理，但在逻辑推理、因果建模方面仍有局限，难以满足工业场景中的高可靠性需求。工业大模型强调对设备行为、工艺逻辑、工况边界等的语义建模，常嵌入机理模型、规则引擎与专家系统，提升故障诊断、过程优化等任务的准确性与可控性。

（4）应用场景与价值实现路径不同

通用大模型广泛应用于内容生成、对话交互、编程辅助等领域，重在人机协同与信息获取，其价值主要体现在办公效率与知识服务。而工业大模型紧贴制造业核心流程，聚焦设备预测性维护、工艺推荐、生产调度、质量控制等高价值场景，直接服务于“提质、降本、增效”目标，价值实现路径更具行业深度。

（5）工程化与部署形态差异显著

通用大模型多采用标准化云服务部署，接口统一、便于调用。工业大模型则需嵌入 MES、SCADA、ERP 等系统中，部署形态多样，如本地部署、边缘计算与模型轻量化推理等，强调实时响应、安全隔离和长期运维能力，工程集成要求高。

1.3 主要国家工业大模型的发展比较

在全球范围内，工业大模型的核心参与者既包括传统工业软件与自动化企业，也涵盖科技巨头与人工智能领军企业。它们依托在工业控制、软件系统与 AI 算法方面的深厚积累，积极推动工业大模型的研发与落地。

美国在工业大模型领域走在前列，代表性企业包括 OpenAI、GE 等。其发展策略强调“芯片 + 算法 + 数据”的三位一体协同，聚焦底层算力、通用模型和基础算法的领先优势，构建起全球工业大模型的“技术金字塔”。欧洲以德国为代表，更注重标准体系建设与工业系统集成。依托深厚的工业 Know-How，通过机理模型嵌入、工程闭环设计和生态协同，实现了工业大模型在汽车制造、精密仪器与化工制药等高端制造领域的深度应用。其发展强调模型的可解释性、安全性与合规性，形成稳固的技术护城河。

中国拥有完整的工业体系和丰富的制造场景，在政策推动与市场需求的双重驱动下，工业大模型发展迅速。尤其在流程制造、装备制造等领域，积累了大量复杂工况与工业数据，为模型训练与验证提供了坚实基础。近年来，国内企业加快工业大模型研发步伐，成果不断涌现。如盘古大模型在电子产品与汽车设计中缩短研发周期；卡奥斯的 COSMO-GPT 已落地工业指标优化、知识生成等多类应用；羚羊工业大模型基于讯飞星火认知能力，集成文本生成、问答理解、代码生成与多模态分析功能，助力制造企业实现智能升级。这些探索正推动中国构建多元化的工业大模型生态体系，助力制造业向高质量发展迈进。

总体来看，中、美、欧在工业大模型的发展路径、技术重点与应用策略上各具特色，形成了各自优势互补、差异化竞争的全球格局。中、美、欧工业大模型的路径与重点应用领域对比见表 2。

表 2 中、美、欧工业大模型发展路径与重点应用领域对比

比较维度	中国	美国	欧洲
发展路径	政策引导 + 龙头企业牵引，强调产学研融合、自主安全，依托国家级制造平台试点推动落地	由科技巨头和工业龙头主导，市场驱动为主，注重 AI 与工业软件深度融合	以“工业 4.0”为核心，注重标准化、互操作性和安全合规性，政府支持与企业协同并重
技术重点	多模态感知、垂直行业微调、自研工业知识图谱与物理模型融合	通用大模型微调为主，融合边缘计算与云平台能力，强调可扩展性与通用性	强调语义建模、数字孪生与控制逻辑一体化，推动智能制造架构标准化
基础优势	数据规模大、应用场景多，算力资源日益完善	算法创新领先、AI 基础模型生态成熟	工业软件优势明显，系统建模与控制理论基础扎实
重点领域	智能质检、预测性维护、产线优化、工业机器人、数字孪生工厂	智能制造操作系统、工业边缘智能、故障诊断与预测、流程制造优化	智能工厂标准建设、高端装备制造、能源管理、智能物流与协同制造
标准与规范	标准体系初步建立，尚缺国际影响力	拥有 ISA、NIST 等权威机构，标准成熟	强调标准统一（如 Industrie 4.0 框架），强调隐私和合规性
发展挑战	工业数据质量与共享机制不足，模型通用性与迁移能力需提升	成本高、安全隐私与跨领域通用性挑战	数据孤岛、跨国标准整合难度大、中小企业智能化转型门槛高

2　工业大模型赋能制造业数字化转型的理论框架

工业大模型正在成为驱动制造业迈向智能化和高质量发展的核心引擎，但其价值实现并非自发发生，而是建立在特定场景牵引、能力支撑、挑战应对与路径选择的系统逻辑之上。为此，本文构建“场景—能力—挑战—路径”的理论分析框架，明确工业大模型的应用场景需求、关键支撑能力、面临的现实挑战以及相应的赋能路径，以期从宏观视角厘清工业大模型赋能制造业数字化转型的运行机制，揭示其落地推广的内在逻辑。工业大模型赋能制造业数字化转型的理论框架如图 1 所示。

2.1　场景：复杂制造场景的智能化转型需求

在制造业高质量发展背景下，工业大模型被广泛期望部署于研发设计、生产制造、运维服务、经营管理、供应链协同等关键环节，以提升生产效率、优化决策质量和强化系统韧性。具体而言，不同行业中分散的工业场景呈现出碎片化、非结构化、异构化等特征，亟需统一、泛化的智能模型进行认知融合与任务适配。

2.2　能力：工业大模型的底层支撑与功能实现

工业大模型的有效部署依赖于三类基础资源的系统集成：工业知识（包括通用知识与私有知识）、计算资源（如训练设备、传输设备、边缘计算设备）和工业数据（包含结构化实时数据、文本文档、图像视频等）。在此基础上，通过多模态训练、机理微调、智能体交互等核心技术，工业大模型逐步实现如智能问答、场景认知、异常识别、路径规划、内容生成、辅助设计、工艺建模与工艺生成等关键功能，支撑复杂工业任务的执行。

2.3　挑战：关键工业任务场景的瓶颈与风险

尽管工业大模型潜力巨大，但在实际应用中仍面临多重挑战，主要包括：高质量训练数据的缺乏，导致模型泛化能力受限；工业场景碎片化严重，模型难以复用和迁移；工业知识表征能力不足，尤其是隐性知识难以结构化表达；关键任务场景中风险预警能力薄弱，影响模型在生产现场的安全性与可靠性；算力与系统性能不足，成为大模型落地的现实约束。这些挑战是制约工业大模型规模化部署的主要瓶颈。

2.4　路径：从需求到部署的闭环赋能机制

针对上述挑战，本文提炼出“需求分析与验证—数据采集与处理—模型开发与训练—系统集成与测试—产品部署与优化”五阶段赋能路径。该路径以工业痛点需求为起点，依托多源数据融合与知识抽取构建基础模型能力，进而通过持续训练与系统验证，向目标场景实施功能化部署。最终形成一个可持续演进的智能系统闭环，推动工业大模型从技术研发走向场景落地。

3　工业大模型在制造业数字化转型中的典型应用场景

典型应用场景是指围绕特定业务需求进行业务数字化、模型化运行的参与主体、行为活动、资源条件及数据要素等构成的组合，是数字化活动中不可分割的业务单元，也是数字化转型水平与价值呈现的基础载体。工业大模型专注于满足制造业需求，并通过独特的架构与训练方法，提供具有行业特色的应用场景，支撑制造业企业在多个关键环节实现智能化跃升。

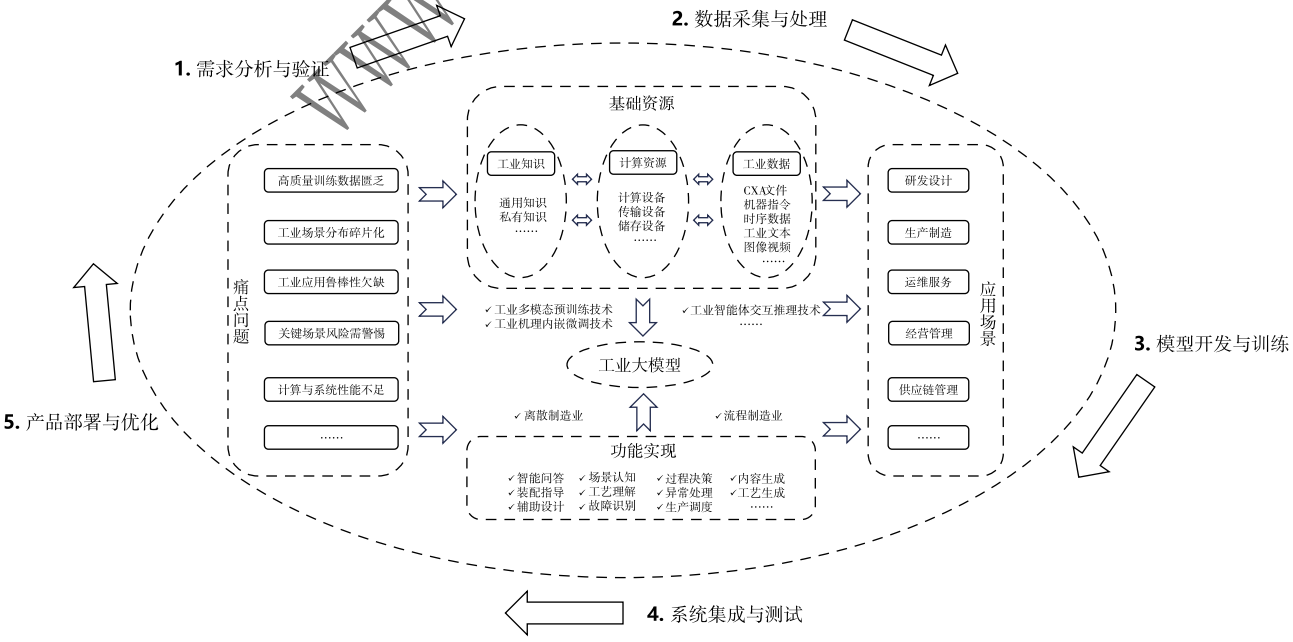

图 1　工业大模型赋能制造业数字化转型的理论框架

3.1 研发设计

（1）需求开发。借助市场数据、用户行为反馈和销售历史等信息，工业大模型可捕捉潜在需求变动趋势，通过语义理解与聚类分析，提炼功能痛点与用户偏好，支持产品定义与定位策略优化，从而加速市场响应和新品成功率。

（2）产品设计。工业大模型集成虚拟仿真与知识图谱能力，对多种设计方案进行多维评估，涵盖结构强度、工艺约束与用户体验等指标，有效筛选高潜力方案，缩短研发周期，减少物理样机依赖。

（3）工艺设计。通过分析历史工艺参数与质量结果之间的关联，工业大模型自动推荐优化路径，识别瓶颈环节并提出调整建议，提升良率与过程稳定性，支撑柔性与精益并重的生产模式。

（4）测试验证。工业大模型结合数字孪生平台进行虚拟测试，预测产品在多场景下的性能表现与可靠性风险，为工程师提供迭代建议，减少物理试错次数，强化产品可靠性验证。

3.2 生产制造

（1）生产管理。工业大模型融合实时产线监测数据与历史排产记录，动态优化设备配置与任务分配，识别生产异常并及时预警，提高产线负载平衡与响应速度。

（2）制造执行。借助对生产现场数据的高频采集与模型推理，工业大模型可实现生产参数的自适应调节与流程动态重构，增强制造弹性，提升单位产出稳定性。

（3）质量管理。工业大模型基于生产中采集的工艺数据与检验结果，建立缺陷预测模型，实现缺陷成因溯源与过程修正路径推荐，减少批量质量波动，增强预防性质量控制能力。

（4）设备管理。工业大模型利用传感器数据对设备运行状态进行建模，识别关键指标的变化趋势，预测设备寿命与潜在故障时点，实现计划性维护替代被动抢修。

3.3 运维服务

（1）市场营销。通过融合电商平台评论、用户画像与竞争产品情报，工业大模型可自动识别目标客群特征与购买行为模式，支持营销渠道细分与内容个性化，提升客户触达与转化效率。

（2）履约交付。工业大模型整合订单状态、产能与库存数据，预测交付风险与延误节点，自动调整排产与物流路径，实现订单履约的时间精准性与客户满意度同步提升。

（3）售后服务。借助售后维修记录与用户行为数据，工业大模型可识别故障发生的前置信号，为用户推送主动服务建议，构建以用户为中心的服务闭环体系。

3.4 经营管理

（1）战略决策。工业大模型融合企业经营指标、行业情报与政策动态，通过多场景仿真与敏感性分析，为企业提供多元化战略路径评估，支持中长期资源配置与风险管理。

（2）财务管理。工业大模型可对现金流、营收周期与成本结构进行智能分析，识别资金占用异常与流动风险点，辅助制定更具前瞻性的资金调度与投资策略。

（3）人力资源管理。通过分析员工绩效数据、岗位履历与组织网络，工业大模型可以发现关键岗位风险与人才发展路径瓶颈，支持人员流动优化与培训资源配置。

（4）办公管理。工业大模型可融合任务协同平台数据与员工行为模式，实现流程瓶颈定位与会议效率评估，辅助精简流程，提升组织响应力。

3.5 供应链管理

（1）采购管理。工业大模型整合原材料价格、供应商履约记录与地缘风险数据，评估采购成本变动趋势与供应商可靠性，支持动态采购计划与风险缓释措施制定。

（2）订单管理。借助订单履历、物流反馈与客户画像，工业大模型可精准预测订单波动及潜在延迟风险，实现订单排产与供应链节奏协调，提升履约稳定性。

（3）仓储物流。工业大模型利用库存流转记录与区域销售动态，优化库位分布与补货策略，实现库存压缩与响应速度提升的双重目标。

（4）销售管理。通过融合终端销售数据、渠道信息与竞品走势，工业大模型可实现客户需求预测与渠道激励优化，辅助企业制定精准促销与价格策略，提升销售闭环效率。

4 面向制造业的工业大模型应用痛点问题与挑战

4.1 高质量训练数据匮乏

工业大模型应用面临的首要难题是高质量训练数据的缺乏。一是数据采集不全面。受制于技术、设备和管理水平，许多制造企业尚未实现关键生产数据的系统化采集，即使已部署传感器和物联网技术，所采集数据仍存在精度低、干扰多、噪声大、缺失值多等问题。二是数据缺乏准确标注。部分企业虽拥有大量历史数据，但大多未进行高质量标注，难以满足模型训练要求，特别是在故障诊断和质量控制等关键场景，标注不足严重影响模型性能。三是行业专有数据集稀缺。如特定传感信号、工业文档、机器指令等模态数据资源有限，导致模型难以全面理解行业特性，降低了训练效果与实际适应性。

4.2 工业场景分布碎片化

制造业涵盖研发、生产、运维、服务等多个环节，

系统平台异构、数据标准不一，易形成“信息孤岛”等因素，严重制约了工业大模型的泛化能力。一是数据标准不统一。标准不统一阻碍数据整合与共享，不同系统之间在数据格式、管理方式上缺乏协调，影响模型全流程优化。二是系统架构差异大。控制系统、设备协议种类繁多，缺乏统一接口，导致数据流通不畅，模型难以跨系统学习和部署，限制其在复杂工业环境中的推广。

4.3 工业应用鲁棒性欠缺

工业环境复杂多变，设备老化、传感器漂移、工况波动等不确定性使得现有工业大模型在应对异常工况时表现不稳定。一是异常识别机制薄弱。模型对传感器异常、操作误差等识别能力不足，异常数据易混入训练和推理过程，降低预测准确性，甚至造成误判。二是自适应能力有限。当前模型普遍缺乏在线学习和动态调整能力，无法快速响应突发情况，影响决策时效与系统稳定。三是缺乏可解释性。工业场景对决策透明度要求高，然而深度学习模型“黑箱”特性使错误预测难以追溯，影响故障排查和生产安全。

4.4 关键场景风险需警惕

工业大模型在关键环节虽提升了智能化水平，但同时也带来放大化、系统性的新型风险。一是感知偏差或推理错误可能引发安全事故。例如在冶金、化工等行业，模型误判可能导致温压失控、设备损毁等严重后果。二是识别精度波动导致质检失效。质检识别错误导致出现次品漏检或优品误剔，影响客户满意度和品牌信誉。三是模型脆弱性带来网络安全风险。工业大模型依赖云平台和开放接口，易受到对抗样本、模型投毒等攻击，可能引发控制系统瘫痪、数据泄露等重大安全事件。

4.5 计算与系统性能不足

工业大模型对计算资源和系统性能提出极高要求，许多企业尚不具备相应支撑能力。一是算力不足。传统制造企业 IT 架构陈旧，难以支撑大模型在训练、推理和实时控制等场景的高性能需求，影响效率。二是云边协同薄弱。现有架构无法满足边缘侧快速响应与云端高效计算协同的需求，实时性不足。三是数据存储与传输受限。随着数据量激增，企业在高效采集、存储与调用数据方面存在明显短板，进一步限制了模型性能的充分发挥。

5 工业大模型赋能制造业数字化转型的方法路径

5.1 需求分析与验证：明确数字化转型的应用场景与目标

数字化转型的首要任务是明确企业面临的核心问题与转型目标。制造业普遍存在生产效率低、质量控制难、设备故障频发、资源浪费等问题，成为推动转型的关键动力。工业大模型的应用应聚焦于具体场景，如生产调度优化、预测性维护、质量检测和供应链优化等。企业需结合现有流程与业务模式，深入识别瓶颈环节，厘清模型介入的切入点。例如，钢铁行业可重点部署于设备预测性维护，而汽车制造则更适用于智能调度与自动化质检。准确识别需求将为后续模型开发和系统集成奠定清晰基础。

5.2 数据采集与处理：构建高质量的数据基础

数据是工业大模型的基础。企业需从设备、生产流程中采集运行状态、工艺参数、质量指标等多维数据。高质量数据不仅依赖于采集过程，更需要在预处理环节控制数据质量，包括去噪、填补缺失值、剔除异常点等，确保进入模型的训练数据具有高度的准确性和可用性。同时，对图像等非结构化数据，也需借助图像处理与特征提取技术生成有效输入。数据标准化同样重要，确保不同系统、设备间的数据可互联互通。随着数据体量与复杂度增长，企业应借助大数据平台和云计算技术，实现高效的数据存储、管理与调用，为模型提供坚实的数据支撑。

5.3 模型开发与训练：从数据到智能决策的关键环节

工业大模型需结合行业特性进行深度定制，难以照搬通用模型路径。制造业中，不同行业、产线需求差异显著，模型开发必须贴近工艺实际，捕捉关键变量与潜在规律。模型训练通常依赖云平台的大规模算力，对数据建模能力和算法性能提出更高要求。训练过程要适应生产动态变化，并在多个场景中进行定制化微调。同时，模型需持续迭代优化，响应设备升级、工艺调整和市场需求变化。企业可通过交叉验证、误差修正等手段评估模型表现，提升其实用性与稳定性。

5.4 系统集成与测试：确保大模型与现有系统的高效融合

工业大模型训练完成后，系统集成是实现其价值的关键。工业大模型需与企业现有信息系统（如 MES、ERP）深度融合，确保数据实时对接与反馈响应。在集成过程中，应特别关注系统兼容性、运行稳定性和响应效率。集成完成后，还需开展全面测试，包括功能测试、性能测试与稳定性测试。以设备故障预测为例，测试应验证模型能否及时识别异常并生成预警；在生产调度场景中，则应评估其决策速度与准确性。通过测试，企业可规避部署风险，保障模型在复杂工业环境中的可靠运行。

5.5 产品部署与优化：实现持续的生产效益提升

工业大模型的部署应结合实际场景灵活选择，如对实时性要求高的，可采用边缘计算部署至生产现场；对数据处理要求高的，可依托云平台实现集中计算。部署

仅是起点，更重要的是后续的持续优化。企业应建立实时监控与反馈机制，对模型进行动态评估与迭代更新。随着数据不断积累，模型可在反馈中自我优化，持续提升预测准确率和决策能力。通过不断调整和优化，工业大模型将助力企业在提升效率、降低成本、保障质量等方面实现可持续的数字化转型成果。

6 对策与建议

6.1 完善政策体系，强化机制保障

政府应将工业大模型纳入重点发展领域，制定专项政策，设立资金支持计划，通过科技资助、税收优惠等方式降低企业尤其是中小企业的技术转型成本。同时，健全监管机制，确保大模型技术在合规、透明的环境中安全应用，避免技术滥用。

6.2 推动示范引领，促进行业协同

加快典型应用场景的示范项目布局，在研发设计、智能制造、供应链管理等环节推广试点应用，总结经验、形成示范。鼓励龙头企业和行业组织分享实践成果，推进跨行业协同与产学研合作，建设联合创新平台，助推行业整体升级。

6.3 统一标准体系，确保数据安全

加快构建涵盖数据格式、接口协议、模型应用等方面的工业大模型标准体系，解决数据孤岛和系统割裂问题。同步加强数据安全和隐私保护，推动企业落实数据加密、访问控制等措施，构建安全、可信的数据生态。

6.4 鼓励自主创新，推动技术突破

支持企业加大对大模型关键技术的研发投入，重点突破数据处理、算法优化和模型训练等核心环节。推动跨学科协作，深化人工智能与制造工艺的融合，提升自主安全能力。鼓励技术成果转化，完善知识产权保护机制，构建创新驱动发展格局。

6.5 引入约束机制，提升安全韧性

企业应为大模型部署建立多层次安全保障机制，包括设置高风险工况下的人工干预与决策门槛、构建异常检测与多模态校验机制、设定模型容错区间和故障恢复策略等，从而提升系统整体鲁棒性与安全性。

6.6 加强人才培养，促进跨学科发展

高等院校应开设智能制造与人工智能交叉课程，培养复合型人才。企业要加强技能培训，提升员工对工业大模型的开发和应用能力。推动高校与企业联合攻关，打造产教融合的人才培养新模式。

7 结束语

工业大模型以其强大的感知、认知和决策能力，正加速推动制造业向智能化转型。本文从赋能路径出发，系统分析其应用挑战，并提出政策、示范、技术、标准、安全、人才等方面的对策建议，旨在为其健康发展提供理论支持与实践指南。未来，随着大模型技术的不断发展和应用场景的日益丰富，制造业的数字化转型将迎来更多机遇，如何进一步提升工业大模型的可解释性、可靠性和产业适配性，将是值得深入研究的重要方向。

参考文献

[1] 肖静华，曹望华，夏正豪. 制造业企业数字化转型的适应性变革：跨越与强基双路径［J］. 中国工业经济，2024（12）：136－154.

[2] 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［J］. 中国科学：信息科学，2024，54（11）：2606－2622.

[3] 周云杰. 推进新型工业化，用好工业大模型的“超级大脑”［J］. 数字化转型，2025，2（3）：10－13.

[4] 李诗婧，赵爽. 生成式人工智能应用于制造业的网络安全风险及对策研究［J］. 信息通信技术与政策，2025，51（1）：20－24.

[5] 栾燕，孟祥曦. 人工智能大模型与新型工业化融合的路径与挑战［J］. 信息通信技术与政策，2025，51（1）：76－82.

[6] 秦峥，刘帅，李育涛. 数据要素驱动下的工业互联网平台创新发展与应用研究［J］. 网络安全与数据治理，2024，43（11）：1－6.

[7] 陈小平. 大模型的逻辑增强与人工智能驱动的行业创新［J］. 技术经济，2024，43（12）：1－9.

[8] 刘冀辰，李金星，吴佳，等. 大模型技术在电力行业的应用展望［J］. 图学学报，2024，45（6）：1132－1144.

（收稿日期：2025－04－23）

作者简介：

秦峥（1989－），女，博士，工程师，主要研究方向：工业互联网平台、制造业数字化转型、知识产权法、反不正当竞争法等。

李育涛（1998－），男，博士研究生，主要研究方向：工业大模型、新型工业化、风险管理等。

郭淑芳（1994－），通信作者，女，硕士，工程师，主要研究方向：竞争政策、制造业数字化转型等。E-mail：guoshufang@infoip. org。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部