附件 2

制造业企业人工智能应用指南

人工智能与制造业全要素、全流程、全链条深度融合，是破解产业升级瓶颈、塑造国际竞争优势的重要途径。为加快推动人工智能与制造业深度融合，推动数字技术与制造优势更好结合，提升制造业企业应用人工智能的科学化、规范化水平，全面赋能新型工业化，制定本指南。

使用人工智能进行研发设计、生产制造、经营管理及开展延伸服务的企业适用本指南。

一、开展智能化评估和规划

（一）开展智能化水平诊断评估。综合运用数据管理能力成熟度、智能制造能力成熟度、数字化转型成熟度、两化融合管理体系等参考标准和制造业数字化转型通用评估指标体系，摸清企业数字化、网络化、智能化水平，找准转型升级瓶颈。结合经济性分析与风险评估，科学确定人工智能应用需求。

（二）制定人工智能应用规划。参考人工智能赋能新型工业化典型应用案例等，确定人工智能应用核心场景和技术导入优先级，合理设置应用目标。优先开展经营管理、研发设计等场景智能化升级，梯次布局中试验证、生产制造等环节改造升级。发挥工业互联网数字底座支撑作用，强化与企业数字化转型工作统筹衔接，确保人工智能应用精准支撑主营业务发展。

二、提升智能化基础能力

（三）升级硬件基础能力。对工业“哑设备”“哑岗位”实施数字化改造升级，构建统一技术底座和场景化应用套件相结合的硬件支撑体系。通过加装传感设备和智能仪器仪表、部署边缘计算设备、推动工业专网升级、应用数字化转型通用工具产品，全面提升各类场景信息感知、传输、决策、控制能力。通过计算、存储、网络优化升级，加快推动已有数据中心转型智算中心。

（四）提升软件智能化水平。加快工业实时操作系统等核心软件，制造执行系统、在线实时优化软件等控制优化软件，以及分布式控制系统、数据采集与监控系统等控制执行单元智能化改造升级，提升智能化支撑能力。优化基础软件内核，植入智能调度算法，提升资源分配效率，增强系统响应速度。部署集成数字孪生、大模型等数智技术的工业设计、生产控制、经营管理、服务保障等工业软件，强化工业软件原生智能基础。

三、构建高质量数据集

（五）建设数据资源平台。搭建企业专识数据库，形成覆盖研发设计、生产制造、供应链管理、经营决策管理等全业务场景的数据资源池。构建包含机理库（存储工业机理模型、技术文档、设计图纸等底层原理性知识）、仿真库（存储多学科仿真模型）、经验库（存储故障案例、最佳实践、操作技巧等实践性知识）在内的工业知识库，有效支撑企业人工智能数据集需求。建设企业数据管理一体化平台，支持多源异构数据的汇聚、处理、标注和质量评估，提高企业数据加工和利用能力，提高数据集质量。

（六）应用数据集处理工具链。加强数据处理工具使用，逐步覆盖数据汇聚、采集、清洗、增强、标注、合成、存储、传输、分析与应用等重点环节，为企业人工智能应用持续提供高质、高效、安全的数据集支持。重点加强智能标注、专家协同标注、融合机理与仿真数据合成、数据集质量评估、安全监测等方向工具的使用。

（七）建立数据管理体系。鼓励企业探索首席数据官制度，建立涵盖规划、实施、评价、改进的数据管理体系，加强数据标准化建设，推动各系统数据融合。建立企业数据集分类分层分级管理机制，综合考虑数据类型、数据系统、应用场景和安全等因素，保障企业数据集安全应用、有效流通。明确数据采集、预处理、数据标注、增强合成、数据集产品化等环节的关键步骤和质量要点，制定数据集质量评估标准，指导数据集质量提升和高效应用。

（八）构建多样化数据集。聚焦工业领域研发设计、生产制造、经营管理等环节，打造覆盖企业工艺设计优化、过程控制、故障诊断、智慧运营等场景的多模态工业高质量数据集。鼓励制造业企业联合第三方开展合成数据集、工业领域深度思维链数据集、跨学科跨领域知识图谱等数据集建设，打造高质量行业数据集，探索数据集产品化、支持复杂场景工业人工智能应用。

四、合理规划布局算力资源

（九）科学规划算力规模。按照国家总体部署，结合企业发展实际，制定阶段化、梯度上升的算力部署规模，鼓励优先

选择可实现瞬时响应、可扩缩容的算力服务。

（十）合理配置算力资源。鼓励优先采用云计算服务快速构建智能化基础服务能力，降低技术投入成本。具备良好数字化基础且对数据安全要求较高的企业，可依托自有算力基础设施建设智算资源，部署人工智能应用，实现资源集约化利用。

（十一）加强算力资源协同调度。鼓励企业基于业务特征实现云边端算力协同，整合多元异构芯片资源，云侧实现模型训练、微调、量化和蒸馏等任务，边缘端侧实现模型轻量化部署以满足工业低延迟需求。深挖算力使用需求和应用场景，深化算力供需对接和算力资源高效调度运营。

五、开展模型选型与调优

（十二）科学确定应用场景。聚焦解决企业在制造全流程中的关键技术或工艺难题，选取对生产力有明显带动作用的高价值场景，开展人工智能技术研发和应用落地，在以下五类场景中重点布局人工智能应用。研发设计类重点推进智能辅助设计、创意图纸快速生成等；中试验证类重点开展仿真模型智能构建、测试数据智能生成等；生产制造类深化应用智能排产调度、工业视觉智能检测等；营销服务类重点突破个性化推荐、定制化售后等；运维管理类着力实施设备预测性维护、能效优化分析、辅助经营决策支持等。

（十三）量化场景关键指标。结合场景特征和业务目标，设定模型选型所用的可量化指标，以此评估场景应用效果，为模型选型和调优提供依据。研发设计类场景重点衡量单位时间内设计迭代次数、设计方案生成数量、方案采纳比率等；中试

验证类场景重点考核仿真建模效率、测试指标覆盖程度等；生产制造类场景着重监测综合优化效率、生产合格率以及漏报率、误报率等；营销服务类场景重点检查营销转化率、响应时效等；运维管理类场景重点关注故障预测准确率、维护成本降低幅度等。

（十四）结合业务选定模型。基于业务场景需求，结合算力基础设施建设情况，开展模型评测选型。综合考虑模型、开发框架、编译器、推理部署工具链之间的兼容性、可靠性及易用性，优先选用经行业实践验证的成熟方案。鼓励面向制造业细分业务场景研发智能体产品，构建智能化解决方案。把安全作为模型选型的重要考虑，综合考量模型来源、漏洞缺陷、安全防护机制等，优先选择安全可信度高的模型底座。鼓励企业打造产、供、销全链条模型协同能力，提升各环节联动效率。

（十五）采用提示词工程与检索增强调优。构建涵盖工业常规问题、边缘案例的提示词库，建立语法正确性、语义完整性、用户满意度等多维度指标。针对市场分析、新技术应用等高频知识更新场景，对接行业数据库及资讯平台，实施数据源权威性评价与内容监测机制，确保信息真实性。

（十六）利用模型微调适配典型场景。质量检测与缺陷识别场景，重点开展基于预训练模型的小样本标注缺陷数据微调，强化模型对复杂微小特征提取能力；生产调度场景，重点根据产线历史数据全参数微调时序预测模型，动态分配资源提升核心任务效率；设备故障诊断场景，重点利用时序数据、音频数据等多模态数据开展实时监测预测，优化故障预测模型。

（十七）结合实际开展混合调优。鼓励企业根据实际情况，优先采用提示词工程及检索增强技术，逐步尝试参数高效微调、全参数微调，提升模型能力。结合实际建设多模态模型候选库，综合采用参数微调、架构搜索、大小模型协同等手段，确定最优解决方案。

六、模型部署与集成

（十八）验证模型性能。在实际生产环境中进行试运行验证，确保模型能够在真实场景中有效运行。综合考虑各类模型的资源分配、数据安全性、实时性、稳定性、响应能力以及系统的扩展性等要求，使用微服务架构、API 接口、中间件等技术，基于业务特征将模型集中部署或云边端协同部署。

（十九）提升模型易用性。根据业务需求，开发具体的模型应用接口、低代码组件等，基于业务需求实现数据接入灵活配置和模型分析结果展示。

七、持续提升应用成效

（二十）评估应用能力水平。组建专业团队开展专项评估，定期分析改进。从模型准确率、算力利用率、推理时延、投入成本、安全稳定等方面，评估人工智能在企业应用中的问题。

（二十一）推动迭代优化升级。定期分析应用人工智能对企业运营决策水平提高、业务处理效率提升、产品生产质量改进、经营效益改善等方面的影响。结合企业发展战略和人工智能技术趋势，制定下一阶段应用目标与实施方案。强化集约管控，推动智能化与绿色化深度融合，实现可持续发展。

（二十二）深化技术融合创新。联合高校科研机构攻关模

型在工业应用过程中的实时性、端侧部署和可靠性等关键技术。结合应用成效，推动二次创新，将行业大模型深度嵌入研发设计、中试、生产和运营等全流程。强化参数优化与知识推理能力，孵化智能软件开发、智能运维等工业智能软硬件工具和产品，构建以人工智能为驱动的新质生产力。

（二十三）鼓励优秀方案输出。具备技术优势的行业领军企业，通过开放平台接口、开源通用模型及工具链、共享高性能算法模型、研制标准规范等方式，向产业链上下游输出整体技术解决方案，促进产业链协同创新。

八、做好人工智能应用安全防护

（二十四）强化数据安全防护。贯彻落实《数据安全法》《工业和信息化领域数据安全管理办法（试行）》等法律政策，根据行业领域数据特点，组织开展数据分类分级、全生命周期安全防护、风险监测预警、风险评估等工作，为各行业人工智能应用提供数据安全保障。面向数据标注、汇聚、训练、合成等环节，强化数据校验、检测评估、身份认证和权限管理，提升数据安全风险防范水平。

（二十五）防范应用安全风险。面向研发设计、中试验证、生产制造、营销服务和运营管理等人工智能典型应用场景，鼓励企业定期对工业大模型幻觉、准确性、鲁棒性等开展安全测试评估。建立人工智能应用输入输出双端过滤安全监控能力，加强恶意指令输入、异常推理输出等风险防范。强化人工智能应用供应链安全管理，将上下游供应商的安全能力纳入合作方管理要点，构建完善供应链安全治理能力。

（二十六）提升网络安全防护水平。推动网络安全贯穿制造业企业人工智能规划、部署、应用等各环节，落实《网络安全法》《工业互联网安全分类分级管理办法》，开展自主定级、信息登记、分级防护、符合性评测、安全整改等工作，健全企业网络安全管理和防护体系，加强工业控制系统网络安全能力，提升人工智能应用过程中的风险防范水平。

九、加强组织保障

（二十七）压实企业主体责任。系统制定企业数智化转型升级管理制度，强化企业资源保障力度，高效、稳妥推动人工智能应用逐步深入。

（二十八）加强复合人才培养。加强产学研用协同，鼓励高校和企业依托国家人工智能产教融合创新平台、示范性特色学院等，支撑人工智能拔尖创新人才培养，健全企业人工智能人才引进、评价和激励机制，营造良好人才发展环境，培养兼具行业认知与技术实操能力的复合型人才。

（二十九）积极参与生态共建。及时归纳总结成功经验，积极共享人工智能解决方案，打造行业应用标杆，推动提升制造业智能化水平。