工业和信息化部人工智能标准化技术委员会
2025 年标准制定指南

根据工业和信息化部等四部委联合印发的《国家人工智能产业综合标准化体系建设指南（2024 版）》（以下简称《国家指南》）有关要求，工业和信息化部人工智能标准化技术委员会（以下简称“标委会”）第一次全体会议审议通过了《人工智能标准化技术委员会标准体系（2025 年）》，围绕基础共性、关键基础技术、产品服务、赋能应用、安全治理等 5 个方面，提出 2025 年标准制定工作指南（以下简称《工作指南》）。

一、基础共性

（一）工作范围

基础共性标准主要包括术语定义、测试评估、参考架构、运营运维管理、开源开放、可持续等标准。

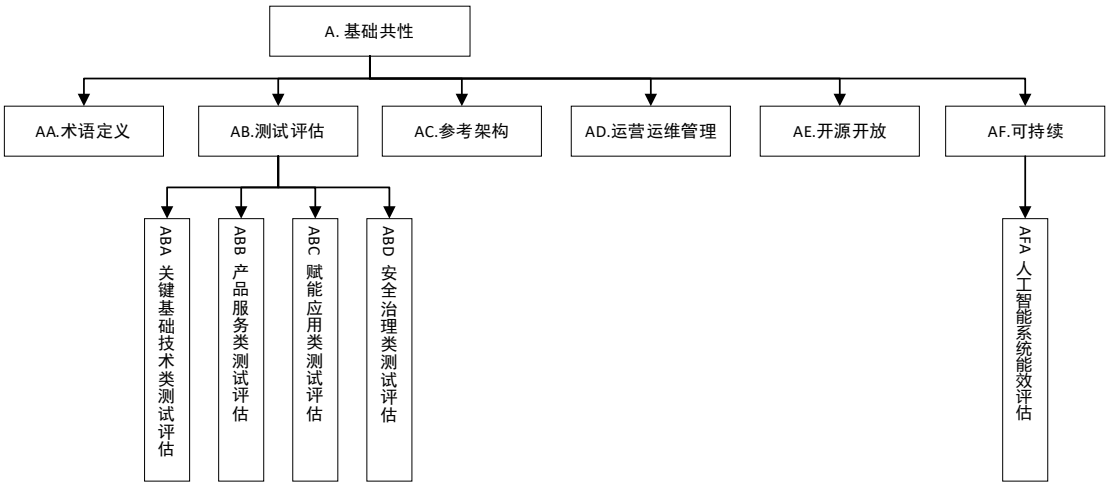


图 1 基础共性部分标准指南

1. 术语定义。规范人工智能相关技术、应用的概念定义，为其它标准的制定和人工智能研究提供参考，包括人工智能相关术语定义、范畴、实例等标准。

2. 测试评估。规范人工智能关键基础技术类、产品服务类、赋能应用类、安全治理类技术、产品和服务，包括性能测试、基准测试、评估方法、指标要求，制定相关应用的成熟度、就绪度、分类分级方法等标准。

3. 参考架构。规范人工智能相关技术、应用及系统的逻辑关系和相互作用，包括人工智能参考架构、人工智能系统生命周期及利益相关方等标准。

4. 运营运维管理。规范人工智能系统的运营运维管理流程，人工智能影响环境的技术框架、方法和指标，包括人员、系统、服务等组织管理、人工智能系统能效评价等。

5. 开源开放。规范开源人工智能模型、数据、工具、

平台、社区、生态等要求，包括开源开放程度定义、开源模型成熟度、开放接口定义、开源社区治理等标准。

6. 可持续。规范人工智能影响环境的技术框架、方法和指标，平衡产业发展与环境保护，包括人工智能系统能效评估等标准。

（二）2025 年拟制定标准

术语定义，拟制定人工智能新技术、新应用、新业态相关术语标准、人工智能产业边界界定相关标准，以及人工智能企业认定相关标准。**测试评估**，针对关键基础技术类，拟制定规范智算系统、基础数据服务、模型平台和具身智能的分类分级、基准测试方法与成熟度评估标准；针对产品服务类，拟制定数字人、模型即服务、智能化软件工程的的分类分级、性能测试方法与成熟度评估标准，针对赋能应用类，拟制定面向工业流程、应用赋能及其他行业的大模型基准测试及评估方法和智能化等级评估标准，针对安全治理类，拟制定面向数据隐私保护、模型鲁棒性、对抗性攻击防御、输出内容安全合规核心要求及检测技术标准。参考架构，拟制定人工智能系统参考架构等标准。运营运维标准，拟制定人工智能研发运营和企业组织管理等相关标准。**开源开放**，拟制定开源模型成熟度评估、开源社区规范等相关标准。

二、关键基础技术

（一）工作范围

关键基础技术标准主要围绕人工智能的核心技术领域展开，涵盖了智算系统、基础数据服务、模型平台、具身智能四个关键方向。

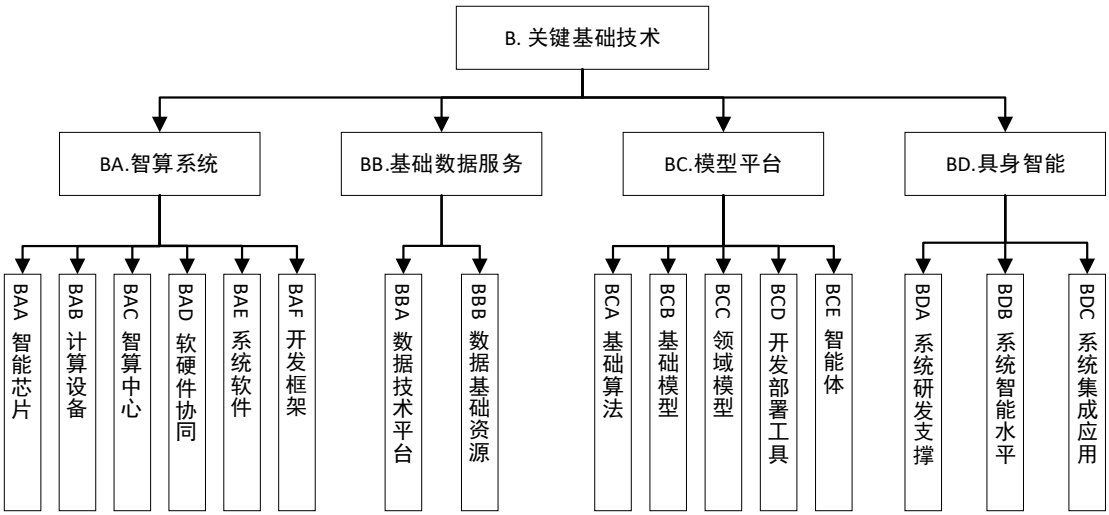


图 2 关键基础技术部分标准指南

1. 智算系统。一是规范智能芯片相关的通用技术要求，包括智能芯片架构、指令集、统一编程接口、芯片数据格式和协议等标准。二是规范人工智能加速卡、人工智能加速模组、人工智能服务器等计算设备，及使能软件的技术要求，包括人工智能计算设备虚拟化方法，人工智能加速模组接口协议和测试方法，及使能软件的访问协议、功能、性能、能效和运行维护要求等标准。三是规范面向人工智能的大规模计算集群、新型数据中心、智算中心、基础网络通信、算力网络、数据存储等基础设施的技术要求和评估方法，包括基础设施参考架构、计算能力、技术要求、稳定性要求和业务

服务接口等标准。四是规范智能芯片、计算设备等硬件与系统软件、开发框架等软件之间的适配要求，包括智能芯片与开发框架的适配要求、人工智能计算任务调度、分布式计算等软硬件协同任务的交互协议、执行效率和协同性能等标准。五是规范人工智能系统层的软硬件技术要求，包括软硬件编译器架构和优化方法、人工智能算子库、芯片软件运行时库及调试工具、人工智能软硬件平台计算性能等标准。六是规范人工智能开发框架相关的技术要求，包括开发框架的功能要求，与应用系统之间的接口协议、神经网络模型表达和压缩等标准。

2. 基础数据服务。规范人工智能研发、测试、应用等过程中涉及的数据技术平台和基础资源相关要求，包括数据采集、数据标注、数据治理、数据质量等标准。

3. 模型平台。一是规范人工智能基础算法的技术要求，包括网络架构、算法原理等标准。二是规范基础模型训练、推理、部署等环节的技术要求，包括文本、视觉、语音、多模态基础模型等标准。三是规范大模型能力要求，包括典型行业及细分领域大模型等标准。四是规范模型开发部署工具的技术要求和能力要求，包括面向传统机器学习、深度学习、大模型领域的工具链及软件平台等标准。五是规范以基础大模型为核心的智能体技术要求等标准，包括智能体架构、接

口及交互协议、多智能体协同机制、知识库等标准。

4. 具身智能。具身智能系统研发支撑，拟制定具身智能系统构建过程涉及到的必要支撑要素标准，如具身智能数据、仿真模拟等；**具身智能系统智能水平**，规范多模态主动与交互、自主行为学习、知识推理、具身导航等标准。**具身智能系统集成应用**，面向整机系统、群体具身智能等应用落地，以及系统软硬件集成过程涉及到的操作系统、智能传感系统、智能执行系统、高算力控制器等环节进行标准制定。

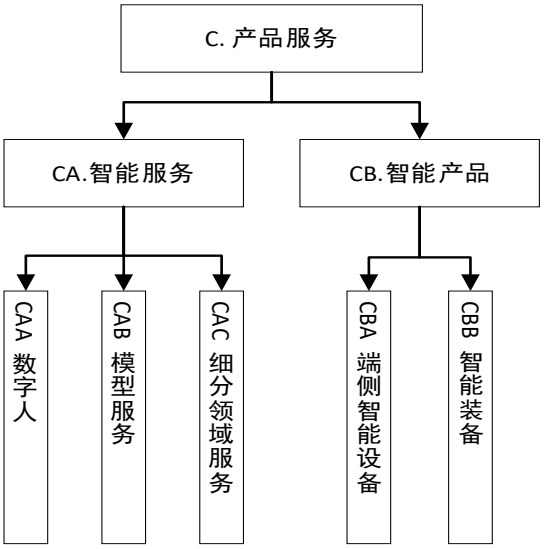
（二）2025 年拟制定标准

智算系统，拟制定面向大模型训练推理需求的智算系统领域标准，包括智能芯片、计算设备、智算中心等软硬件系统能力；互联互通、异构混训、兼容适配、算子库、加速框架等协同技术。**基础数据服务，**拟制定人工智能及大模型数据关键技术、工具平台、数据集的技术要求、质量评估方法等标准。**模型平台，**一是拟制定面向云侧、边缘侧等不同场景，文本、视觉、语音等不同模态，金融、电信等不同领域的大模型开发部署工具技术要求等标准；二是拟制定面向文本、视觉、语音、多模态等不同模态的基础模型技术要求，面向端侧、代码等不同场景，金融、电信、科学等不同领域的大模型能力要求等标准；三是拟制定多模态智能体，接口及协议，多智能体协作，知识库架构，交互协议与多知识库

组织管理以及与智能体、大模型协同等标准。**具身智能**，一是拟制定训练数据全流程规范，明确系统架构技术要求及跨本体平台通用能力；二是拟制定智能化分级和多模态交互、感知决策技术要求及评价方法；三是拟制定人形机器人、家庭陪伴及装配制造等具身智能系统的技术能力要求，推动多场景应用。

三、产品服务

（一）工作范围



产品服务标准主要包括智能服务和智能产品等标准。

1. 智能服务。一是规范数字人的外形、动作生成、语音识别与合成、自然语言交互等技术要求，包括数字人基础能力评估、多媒体合成渲染、基础数据采集方法、标识和识别方法等标准。二是规范基于大模型、自然语言处理、智能语音、计算机视觉等人工智能技术提供的服务，包括模型即

服务平台技术要求等标准，以及面向特定场景的人工智能应用服务，如智能软件开发、智能设计等标准。

2. 智能产品。规范人工智能应用在移动终端和智能装备等领域的技术要求，包括图像识别、人脸识别、智能语音交互，以及智能移动终端涉及的信息无障碍、适老化等标准。

（二）2025 年拟制定标准

智能服务，拟主要制定基于大模型的数字人、模型即服务、基于人工智能的软件研发技术要求和能力要求标准。**智能产品，**拟主要制定面向智能端侧设备和智能装备领域的新产品、新应用制定技术要求和能力要求。

四、赋能应用

（一）工作范围

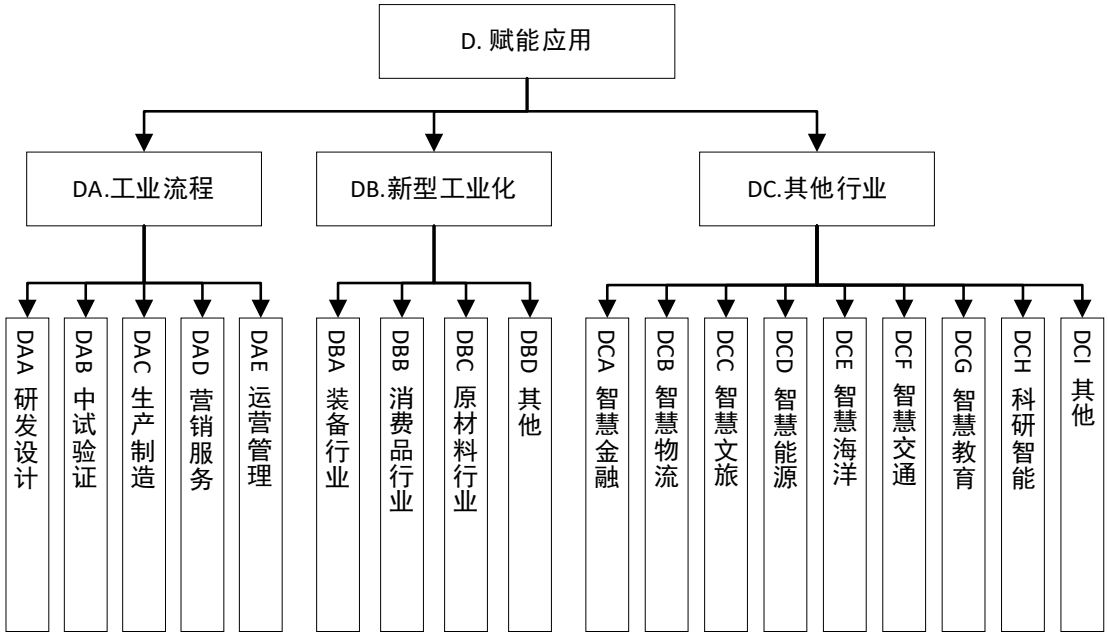


图 4 赋能应用类标准指南

赋能应用标准主要规范人工智能技术赋能工业全流程

智能化以及重点行业智能化升级的技术要求，主要包括工业流程、新型工业化和其它行业等组成部分。

1. 工业流程。制定人工智能赋能研发设计、中试验证、生产制造、营销服务、运营管理等环节的相关标准。

2. 新型工业化。围绕原材料行业，开展大模型畅联产线数据、优化在线监测调控和工艺改进等标准制定。围绕消费品行业，开展需求预测、个性化定制等标准制定。围绕装备行业，制定智能装备感知、交互、控制、协作、自主决策等标准。

3. 其他行业。开展智慧金融、智慧物流、智慧文旅、智慧能源、智慧海洋、智慧交通、智慧教育、科研智能等领域标准研究。

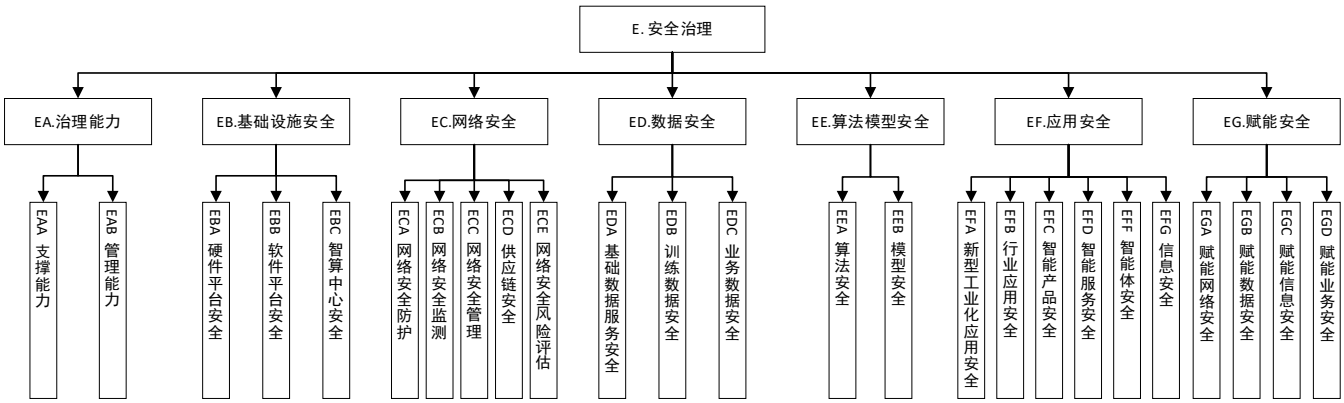
（二）2025 年拟制定标准

工业流程，拟主要制定基于人工智能的装备和软件研发技术要求和能力要求标准。**新型工业化，**拟主要制定基于人工智能技术，面向装备制造、原材料、消费品、能源、航空航天和轻工业等领域的新产品、新应用制定技术要求和能力要求。**其他行业，**拟主要对金融、文旅、传媒、电力等多个行业的大模型技术能力和成熟度等开展标准研究。

五、安全治理

（一）工作范围

人工智能安全治理标准体系规范人工智能安全标准体系框架，明确标准体系的总体架构、分类和关键标准领域，为行业提供基本的安全规范和技术指导。



1. 治理能力标准主要规范人工智能支撑能力和管理能力，为安全治理标准体系奠定基础底座。

2. 基础设施安全标准主要规范硬件平台、软件平台和智算中心等方面安全，为人工智能提供基础运营环境安全保障。

3. 网络安全标准主要规范人工智能网络安全要求，包括网络安全防护、网络安全监测、网络安全管理、供应链安全等，明确人工智能网络安全要求。

4. 数据安全标准主要规范训练数据、业务数据、基础数据服务等方面安全，明确人工智能数据安全要求。

5. 算法模型安全标准主要规范算法、模型等方面安全，保障人工智能技术创新及安全可控。

6. 应用安全标准结合新型工业化，主要规范智能网联

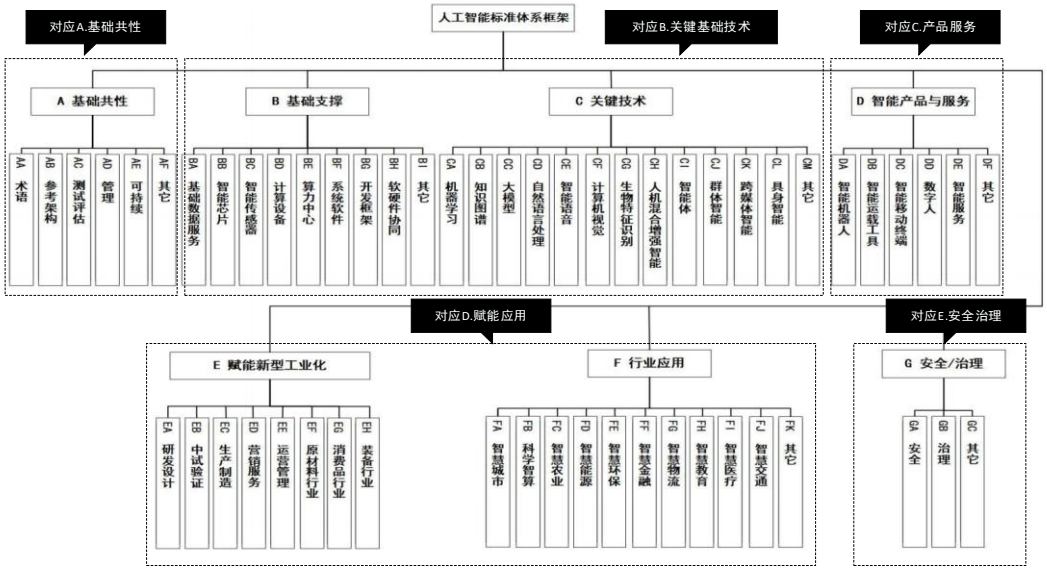
汽车、生成式人工智能、生物特征识别、智能体等典型应用，提出新型工业化应用安全、行业应用安全、智能产品应用安全、智能服务应用安全，以及智能体安全等新产品形态安全的要求和评估方法。

7. 赋能安全标准主要规范人工智能赋能网络、数据、信息、业务和其他安全等方面的要求。

（二）2025 年拟制定标准

治理能力标准拟主要制定大模型安全基准测试、人工智能生成合成内容追溯技术等支撑能力要求，以及人工智能可信研发、风险管理、风险评估、用户权益保障等管理能力要求相关标准。**基础设施安全标准**拟主要制定人工智能算力中心安全相关标准。**网络安全标准**拟主要制定人工智能平台供应链安全相关标准。**数据安全标准**拟主要制定电信和互联网人工智能数据安全、生成式人工智能服务用户数据安全相关标准。**算法模型安全标准**拟主要制定电信和互联网领域算法安全标准、人工智能模型开发框架、部署安全相关标准。**应用安全标准**拟主要制定生成式人工智能检测、深度合成信息服务标识、人脸识别系统安全、大模型检索增强知识库安全、智能体安全、大模型一体机安全等相关标准。**赋能安全标准**拟主要制定网络安全大模型、人工智能赋能恶意流量检测等相关标准。

附件：《国家指南》与《工作指南》的对应关系说明



《工作指南》的工作范围与《国家指南》的重点方向全面对标对表：《工作指南》A.类基础共性与《国家指南》A.类基础共性对应；《工作指南》B.类关键基础技术中 BA.智算系统和 BB.基础数据服务对应《国家指南》B.基础支撑；《工作指南》BC.模型平台和 BD.具身智能对应《国家指南》C.关键技术；《工作指南》C.产品服务对应《国家指南》D.智能产品与服务；《工作指南》D.赋能应用对应《国家指南》E.赋能新型工业化和 F.行业应用；《工作指南》E.安全治理对应《国家指南》G.安全/治理。