

终端智能体协同发展标准体系框架

为深入贯彻落实党中央、国务院关于加快发展人工智能、推动人工智能与实体经济深度融合的战略部署，贯彻落实《国家标准化发展纲要》《全球人工智能治理倡议》《人工智能全球治理行动计划》，系统构建终端智能体协同发展的标准化生态，加快形成覆盖技术研发、场景应用、安全治理的全链条标准体系，切实提升智能体的互操作性、协同效率与可信水平，充分发挥标准对技术发展、产业协同、生态共建的引领作用，推动形成开放共享、安全可控的智能体协同发展新格局，编制本标准框架。

一、产业发展现状

通过将人工智能模型的强大能力与终端设备即时响应、环境感知等特性相结合，终端智能体全方位重塑人机交互模式，广泛应用于智能制造、智慧城市、智慧生活、智慧教育等重点领域，正逐步成为推动产业智能化升级和数字经济发展的核心载体。

终端智能体作为运行在各类终端设备上，基于终端设备计算、存储、安全等能力，感知环境信息，理解用户意图，通过智能算法和模型进行决策，并自主执行任务以满足用户需求的智能实体。近年来，我国终端智能体加速发展，软硬件性能持续提升，产业生态日益完善，应用场景深度拓展。



在硬件设备、运行环境、网络通信、数据资源以及大模型等核心要素的支撑下，终端智能体构建了从底层基础设施到上层应用服务的完整技术体系和产业生态，催生丰富多样的产品和服务形态，如智能家居设备、服务机器人等硬件产品，以及智能助手、数据分析系统等软件服务。面对人工智能与终端设备深度融合、单一功能向综合服务演进的技术趋势，亟需建立覆盖基础架构、能力组件、应用接口和安全保障的终端智能体标准体系，通过规范技术发展路径、提升系统互操作性、促进产业协同创新，为培育数字经济新质生产力提供关键支撑。

二、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大和二十届二中、三中、四中全会精神，坚持创新驱动和高质量发展理念，统筹发展和安全，以抢占人工智能产业发展制高点为目标，完善终端智能体标准化工作顶层设计。通过强化产业链标准协同，系统推进标准研制、实施应用和国际化进程，为终端智能体高质量发展提供坚实支撑。

推进过程中要重点把握：一是筑牢技术根基，强化标准对基础软硬件创新的引领作用，突破自主决策、多智能体协同等关键技术瓶颈；二是深耕行业应用，以标准为纽带推动终端智能体与实体经济深度融合，培育智能助手、智能家居

等示范产品和场景；三是优化产业生态，通过标准促进产业链上下游协同创新，构建开放共享的终端智能体发展共同体。

着力实现“三个突破”：一是在标准供给质量上实现突破，推动构建高质量终端智能体标准集群；二是在标准实施效能上实现突破，形成标准与产业互促共进的良性循环；三是在标准影响力上实现突破，推动标准体系成为未来终端智能体发展的重要参照。

三、建设思路

（一）终端智能体标准体系结构

终端智能体协同发展标准体系框架包括通用标准、基础支撑、核心能力、产品应用、服务场景、安全体系等六个部分，如图 1 所示。**通用标准**是明确终端智能体的术语定义、参考架构、基准测试、智能分级等基础要求。**基础支撑标准**是规范终端智能体硬件设施、运行环境、网络通信、数据资源、大模型等要求，夯实终端智能体运行的技术底座。**核心能力标准**是规范终端智能体感知、规划、执行、协作、记忆以及学习能力技术要求，推动终端智能体核心能力的优化和提升。**产品应用标准**规范终端智能体衍生的软硬件的产品和服务技术要求，推广终端智能体的创新和应用。**服务场景标准**聚焦交通出行、互联网销售、教育培训、医疗健康以及民生保障等典型场景，明确终端智能体服务场景应用要求。**安**

全体系标准规范终端智能体基本安全、交互安全、数据治理以及数据安全等要求，为终端智能体的发展提供安全保障。

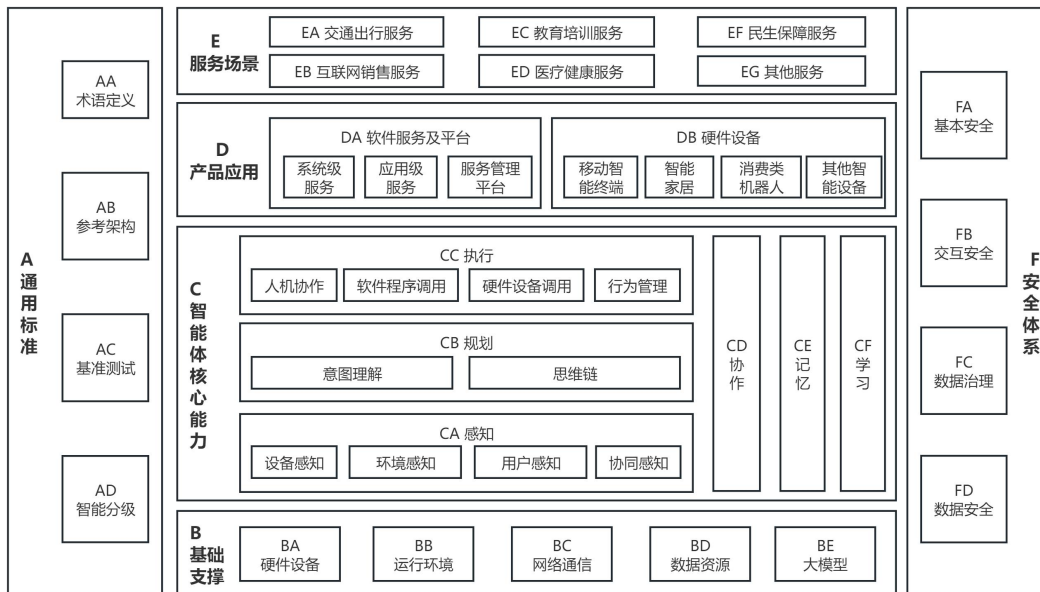


图 1 终端智能体标准体系结构图

(二) 终端智能体标准体系框架

终端智能体标准体系框架由通用标准、基础支撑、核心能力、产品应用、服务场景、安全体系 6 个部分组成，如图 2 所示。

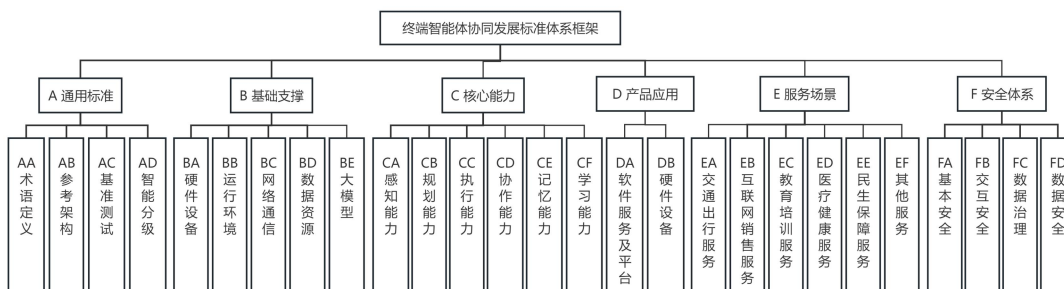


图 2 终端智能体标准体系框架图

四、重点方向

(一) 通用标准

通用标准主要包括术语定义、参考架构、基准测试、智能分级等。

1. 术语定义标准。明确终端智能体相关技术、应用的概念定义，为终端智能体的研究和其他标准的制定提供参考。

2. 参考架构标准。明确终端智能体相关技术、应用的系统逻辑关系和相互作用，包括终端智能体参考架构、生命周期及利益相关方等。

3. 基准测试标准。明确终端智能体核心指标、测试方法与评价规则，推动形成可对比、可验证、可感知的终端智能体基准评估体系。

4. 智能分级标准。明确终端智能体智能化分级要素、分级原则，以及不同等级智能体的技术要求。

(二) 基础支撑标准

基础支撑标准包括硬件设备、运行环境、网络通信、数据资源、大模型等。

1. 硬件设备标准。规范终端智能体底层芯片、传感器、计算设备等硬件的通用技术要求，包括技术架构、指令集、接口、协议、数据格式以及硬件性能指标等。

2. 运行环境标准。规范终端智能体运行环境的技术要求，包括软硬件编码器架构和优化方法、运行时资源管理、运行时库和调试工具、系统适配性和兼容性、计算性能等。

3. 网络通信标准。规范终端智能体的网络通信技术要

求，包括智能体网络拓扑结构、网络传输机制、通信协议支持、多智能体组网能力等。

4. **数据资源标准**。规范终端智能体的研发、测试、应用等过程中涉及的数据资源使用和管理的要求，包括数据采集、数据处理、数据隔离、数据更新、数据质量等。

5. **大模型标准**。规范终端智能体大模型相关技术要求，包括模型能力、模型更新、模型兼容性、模型能耗、模型伦理、智能体调度等技术要求。

（三）核心能力标准

核心能力标准包括终端智能体感知、规划、执行、协作、记忆以及学习能力等。

1. **感知能力标准**。规范终端智能体设备感知、环境感知、用户感知、协同感知等技术要求。

2. **规划能力标准**。规范终端智能体意图理解、多轮会话、思维链等决策能力技术要求，规范智能体从需求识别到需求响应的决策流程与评价指标。

3. **执行能力标准**。规范终端智能体人机协作、软硬件调用、行为管理等技术要求。

4. **协作能力标准**。规范终端智能体在感知、决策、执行等环节中软硬件交互及协作的技术要求。

5. **记忆能力标准**。规范终端智能体在感知、决策、执行中的记忆能力分类、记忆隔离、记忆控制等技术要求。

6. 学习能力标准。规范终端智能体自主进化、个性化适应、知识库更新等技术要求。

(四) 产品应用标准

产品应用标准包括软件服务及平台、硬件设备等。

1. 软件服务及平台标准。规范终端智能体系统级软件服务、应用级服务和服务管理平台的技术要求，包括产品类型、服务场景、技术架构、功能接口以及服务管理平台框架与功能、智能体注册、审核等。

2. 硬件设备标准。规范终端智能体在智能终端、智能家居、消费类机器人等硬件产品的技术要求，包括产品类型、技术架构、资源调度、端云协同、交互接口、感知能力、决策能力、协作能力、运动控制等。

(五) 服务场景标准

服务场景标准包括交通出行服务、互联网销售服务、教育培训服务、医疗健康服务、民生保障服务以及其他服务标准，主要规范不同服务场景中的服务设计、服务开发、服务接入、数据管理、用户权益保障等技术要求。

(六) 安全治理标准

安全治理标准包括基本安全、交互安全、数据治理以及数据安全等。

1. 基础安全标准。规范终端智能体的基本安全要求，包括算力安全、模型安全、组件安全、资源安全、安全管理服

务、安全测试评估等。

2. 交互安全标准。规范终端智能体交互过程的安全技术要求，包括交互过程中的身份认证、协议安全、数据保护、行为控制等。

3. 数据治理标准。规范终端智能体数据全生命周期的管理技术要求，包括数据分类分级、数据采集合规、数据质量评估、数据使用审计、数据共享机制等标准。

4. 数据安全标准。规范终端智能体数据保护的技术要求，包括数据处理的端云协同安全机制、敏感数据匿名化处理、数据传输与存储加密技术、隐私计算技术应用、安全漏洞与威胁检测响应等标准。

五、保障措施

（一）打造协同创新平台。联合芯片厂商、设备制造商、模型提供商、算力提供商、产品服务提供商等产业链核心力量，建立技术研发、标准制定、产业应用三位一体的协同机制，加速创新成果标准化进程。

（二）建设标准验证基地。联合行业企业开展终端智能体标准试点示范，为新技术、新产品提供标准符合性测试环境，促进标准与产业实践的良性互动。

（三）建立动态更新机制。建立终端智能体标准动态评估体系，设立技术演进跟踪小组，定期评估标准适用性，确保标准体系与技术创新保持同步。