

科创之声

人工智能安全要从娃娃抓起

破

智

困

本报记者

郭静原

日前,市场监管总局批准发布《人工智能 智能体互联》系列7项国家标准,系统性搭建起智能体“身份标识—能力描述—供需发现—协同交互—工具调用”全覆盖、闭环式标准规范体系,有效补齐领域标准空白。

“随着智能体规模化落地、多场景普及应用,海量智能体跨平台、跨场景、跨领域互联互通成为产业发展的必然趋势。”市场监管总局标准技术司司长朱美娜介绍,智能体爆发式增长的背后,产业深层次矛盾也日益凸显:一方面,不同厂商智能体之间接口、协议不统一,形成“智能体孤岛”,严重制约了规模化协同应用;另一方面,智能体缺乏统一的身份认证与追溯机制,跨境交互面临身份仿冒、数据泄露等安全风险。此外,缺乏通用的交互与描述规范,导致企业重复建设,系统集成适配成本高昂。

此次标准的发布,对重塑人工智能产业生态意义何在?中国电子技术标准化研究院副院长范科峰介绍,智能体互联系列标准为人工智能技术研发和产业应用划定了基础原则和能力准入门槛,将原本封闭的智能体系统转化为可互联互通的节点,推动形成网络化的智能生态。同时,通过统一的描述与发现机制,能够大幅降低中小企业技术门槛,使其融入主流生态,激发长尾创新活力。

值得关注的是,该系列标准以国家标准化指导性技术文件发布,是产业培育阶段采取的一次敏捷标准化安排,能够最大限度兼容多条技术路线、快速凝聚全行业共识,为技术创新预留充足试错空间。“我们推动技术攻关、标准编制、落地转化同步部署,适配智能体迭代速度快、新业态新模式持续涌现、产业动态演化特征显著的现实特点。”朱美娜说,后续将适时推进身份码相关标准向强制性国家标准转化,同步加快智能体审计、智能体交易等细分领域标准研制,为智能体能力共享、价值流转搭建起合规高效、安全可信的规则体系。

人工智能产业飞速发展,急需逐步完善的标准加以规范。2025年年底,市场监管总局会同工业和信息化部等共同实施“人工智能百项国家标准建设专项行动计划”,统筹推进146项人工智能国家标准项目,涵盖算力、大模型、具身智能、智能体、终端等重点方向。

截至目前,一系列重点标准的发布实施正推动人工智能技术从单点突破走向体系化迭代。此次智能体互联系列国家标准将依托北京市海淀区等创新高地,有序开展标准验证、贯标试点和示范引领工作,培育标准化、可推广的优质智能体产品和高价值应用场景。中关村科学城管委会副主任、海淀区副区长唐超表示,将依托辖区千亿级AI原生生态、万亿级信软业产业规模优势,汇聚海量智能体创新主体,为智能体互联互通的适配、测试、协议优化提供充足的产业样本和空间。

打造开源生态,共享智能互联。工业和信息化部科技司一级巡视员范斌告诉记者,随着标准的发布,工信部指导发起《智能体协议共建共享倡议书》,依托开放原子开源基金会壮大开源社区。目前,已有百余家行业头部企业参与共建共享倡议,50多家企业正开展试点应用工作,稳步加速智能体互联生态落地。

朱美娜透露,市场监管总局将坚持体系前置布局、前沿预研先行、产学研用协同、流程提质增效,动态完善适配产业发展的智能体国家标准矩阵,以多层次标准供给引领产业规范创新。“未来,我们计划进一步聚焦产业管理与人工智能落地评价,推动人工智能企业智能化成熟度评估、人工智能高价值应用场景评价等重点标准出台发布。同时,继续统筹人工智能基础通用、核心技术、行业应用、安全治理全链条标准布局,充分发挥标准引领作用。”朱美娜说。

本版编辑 孟飞 李苑美 编夏祎 来稿邮箱 jrbgzb@163.com

市场监管总局批准发布《人工智能 智能体互联》系列7项国家标准,系统性搭建起智能体“身份标识—能力描述—供需发现—协同交互—工具调用”全覆盖、闭环式标准规范体系,有效补齐领域标准空白。

“随着智能体规模化落地、多场景普及应用,海量智能体跨平台、跨场景、跨领域互联互通成为产业发展的必然趋势。”市场监管总局标准技术司司长朱美娜介绍,智能体爆发式增长的背后,产业深层次矛盾也日益凸显:一方面,不同厂商智能体之间接口、协议不统一,形成“智能体孤岛”,严重制约了规模化协同应用;另一方面,智能体缺乏统一的身份认证与追溯机制,跨境交互面临身份仿冒、数据泄露等安全风险。此外,缺乏通用的交互与描述规范,导致企业重复建设,系统集成适配成本高昂。

此次标准的发布,对重塑人工智能产业生态意义何在?中国电子技术标准化研究院副院长范科峰介绍,智能体互联系列标准为人工智能技术研发和产业应用划定了基础原则和能力准入门槛,将原本封闭的智能体系统转化为可互联互通的节点,推动形成网络化的智能生态。同时,通过统一的描述与发现机制,能够大幅降低中小企业技术门槛,使其融入主流生态,激发长尾创新活力。

值得关注的是,该系列标准以国家标准化指导性技术文件发布,是产业培育阶段采取的一次敏捷标准化安排,能够最大限度兼容多条技术路线、快速凝聚全行业共识,为技术创新预留充足试错空间。“我们推动技术攻关、标准编制、落地转化同步部署,适配智能体迭代速度快、新业态新模式持续涌现、产业动态演化特征显著的现实特点。”朱美娜说,后续将适时推进身份码相关标准向强制性国家标准转化,同步加快智能体审计、智能体交易等细分领域标准研制,为智能体能力共享、价值流转搭建起合规高效、安全可信的规则体系。

人工智能产业飞速发展,急需逐步完善的标准加以规范。2025年年底,市场监管总局会同工业和信息化部等共同实施“人工智能百项国家标准建设专项行动计划”,统筹推进146项人工智能国家标准项目,涵盖算力、大模型、具身智能、智能体、终端等重点方向。

截至目前,一系列重点标准的发布实施正推动人工智能技术从单点突破走向体系化迭代。此次智能体互联系列国家标准将依托北京市海淀区等创新高地,有序开展标准验证、贯标试点和示范引领工作,培育标准化、可推广的优质智能体产品和高价值应用场景。中关村科学城管委会副主任、海淀区副区长唐超表示,将依托辖区千亿级AI原生生态、万亿级信软业产业规模优势,汇聚海量智能体创新主体,为智能体互联互通的适配、测试、协议优化提供充足的产业样本和空间。

打造开源生态,共享智能互联。工业和信息化部科技司一级巡视员范斌告诉记者,随着标准的发布,工信部指导发起《智能体协议共建共享倡议书》,依托开放原子开源基金会壮大开源社区。目前,已有百余家行业头部企业参与共建共享倡议,50多家企业正开展试点应用工作,稳步加速智能体互联生态落地。

近日,联合国儿童基金会发布的一份声明引发关注。通过对10个国家最新数据的分析,儿基会估计全球至少有2000万名儿童已经使用过人工智能,且青少年采用该技术人数的增长速度是成年人的3倍多。这一数据令人且喜且忧。喜的是,人工智能为儿童教育带来了前所未有的机遇;忧的是,在儿童快速拥抱AI的同时,相应的安全防护措施却未跟上。人工智能安全,已经到了必须从娃娃抓起的紧迫时刻。

人工智能为儿童打开了一扇充满可能性的窗口。它可以打破地域与师资壁垒,成为个性化的学习助手;可以成为情感倾诉的出口,为性格内向或存在社交障碍的孩子疏导负面情绪。智能语音交互、实时翻译工具还能帮助残障儿童或非母语儿童跨越沟通障碍,平等参与学习与社交活动。合理运用人工智能,能让儿童的成长更具多元可能性。

然而,机遇的另一面是同样不容忽视的风险,AI对心智尚未成熟的儿童构成多重安全挑战。

视点 中国新闻奖名专栏

工业机器人出海“卖方案”

工业机器人的研发、制造、应用是衡量一个国家科技创新和高端制造业水平的重要标志。海关总署数据显示,4月,我国工业机器人单月出口量正式突破2.5万台,同比增长近90%,相较今年一季度42%的增速进一步加快。中国工业机器人正从“世界工厂”的配件供给者,变成全球智能制造的方案输出者。

苦练内功:从能造到造得好

海关总署数据显示,2025年我国工业机器人出口同比增长48.7%,出口规模首次超越进口,实现净出口的历史性突破。这标志着中国工业机器人产业从进口依赖向出口驱动转型,“走出去”步伐正在提速,本土企业不仅能满足国内市场需求,更具备了参与全球市场角逐的实力。

亮眼数据的背后,是产业链多年“苦练内功”的厚积薄发。从政策层面看,2023年17部门联合发布《“机器人+”应用行动方案》,到2026年8部门联合发布《“人工智能+制造”专项行动实施意见》,政策持续聚焦场景应用,加快制造业智能化、绿色化、融合化发展,促进人工智能技术与制造业应用双向赋能。

在机器人技术不断突破的同时,行业也迎来资本化加速期。今年以来,多家机器人企业推进上市流程,资本市场也聚集了众多产业链企业。

在零部件端,苏州绿的谐波传动科技股份有限公司、深圳市汇川技术股份有限公司等布局伺服电机赛道,苏州敏芯微电子技术股份有限公司等深耕传感器领域,机器人核心零部件国产化率快速攀升;在整机制造端,宇树科技股份有限公司、南京埃斯顿自动化股份有限公司等一批企业已形成产业集群,将多年技术积累转化为新产品形态,并加速向更多应用场景渗透。

在珠三角、长三角,已经形成了高度集聚的机器人产业集群。张江具身智能机器人有限公司副总经理王涛介绍,张江机器人谷内的机器人企业上下游、形成覆盖研发、测试、制造的产业链生态,企业生产出的机器人产品还有专门的展示对接中心,使企业得以更加专注于研发与生产。

“公司关键原材料和零部件约95%为国内采购,在保证技术性能的前提下形成更高的成本效率,因此能够向海外客户提供‘国际品质+更优TCO(全生命周期成本)’的价值方案。”成都卡诺普机器人技术股份有限公司副总经理邓世海认为,成本优势是敲门砖,技术能力和可靠服务才是长期合作的基础。

这种“不靠低价靠价值”的理念,正成为中国工业机器人企业出海共识,也推动工业机器人从“能造”向“造得好”升级。清华大学基础工业训练中心副教授周晋指出,工业机器人出口呈现强劲增长态势,是全产业链协同形成的系统性竞争力,具体体现在4个维度:核心零部件国产替代重构了成本基础;规模化生产与精益管理大幅降低了产品制造成本;工程师红利与本地化服务形成了独特的服务价值;客户侧具备显著的全生命周期使用吸引力。

系统出海:技术+方案+服务

在制造业升级进程中,工业机器人是实现自动化、智能化转型的关键装备。通过替

代人工完成重复性、高强度、高精度、高风险作业,工业机器人推动生产模式从人工主导向机器主导转变。

欧美和亚太地区电商、零售、第三方物流行业发展多年,数字化基础扎实,在人力成本高企背景下,仓储自动化需求已从选配变为标配,客户为技术付费的意愿强、付费能力高。东南亚、中东等新兴市场的自动化基础设施也逐渐完善,正处于工业化升级的关键窗口期,相较于其他国家的产业,中国工业机器人产品性价比优势突出,成为当地企业自动化投入的优先选项。

“在工业机器人这个赛道上,竞争从来不是单一产品输出,而是技术方案与服务标准的综合比拼。”湖南中南智能装备有限公司党总支委员、长沙长泰机器人有限公司董事长高狄表示,技术的独特性是中国工业机器人的名片,如中南智能的具身智能焊接机器人,因为搭载具身智能系统,产品能够给出最优的焊接建议,不需要复杂的产线调试,而是自动适配生产需求,这既有别于传统的工业机器人,也是中国工业机器人的特色。

高狄介绍,他们出口的工业机器人中,很大一部分是具身智能机器人,出口模式也转型为“技术+方案+服务”的综合输出。随着全球机器人产业竞争焦点已从传统自动化效率转向智能协同与多场景应用,中南智能的具身智能机器人产品快速放量,在海外市场站稳了脚跟。

邓世海认为,海外客户更关注的是焊缝一致性、轨迹精度、设备稳定性以及长期运行可靠性,而不是只盯着采购价格。工业机器人行业与消费电子行业最大的区别在于,客户购买的不是设备,而是一个持续运行10年以上的生产系统。卡诺普正在以“售前规划—项目交付—工艺优化—生命周期运维”的全流程服务体系,通过“本土伙伴+技术赋能”模式,适配不同区域的工艺需求与产业特性。

在全球制造业绿色化、智能化升级的背景下,中国工业机器人企业持续推进技术创新与新产品研发,不断完善全流程服务能力,在夯实国内市场长期稳健发展根基的同时,积极拓展海外市场,逐步打造出第二增长曲线。

角色升级:发力中高端市场

业内专家表示,中国工业机器人的出海,本质上是中国制造的一次“角色升级”——从全球产业链的参与者,变成规则的参与者和方案的定义者。

短期来看,全球制造业成熟市场存量改造需求叠加新兴市场增量建设需求,仍在持续释放中。中长期看,中国机器人技术持续迭代,全链路服务能力不断完善,全球市场份额有提升空间,尤其是工业机器人的高附加值综合解决方案占比会越来越高,整个产业逐步向全球价值链中高端攀升。

但这个过程中也有相应的挑战。部分机器人企业表示,高端芯片、部分核心零部件仍依赖进口,这不仅推高了产品成本,更让企业在产品研发设计和规模化生产中感受到了压力。

“中国工业机器人企业与国际领先水平相比还存在差距,还是要发力中高端市场。”北京物联网智能技术应用协会副会长顾阳表示,国际工业机器人市场上,ABB集团、德

15日起施行。该办法严禁向未成年人提供虚拟亲属、虚拟伴侣等虚拟亲密关系服务,要求设置未成年人模式和时长限制。这是全球范围内针对AI情感交互服务实施监管的重要一步。在此基础上,未来,我们还应进一步将儿童权利全面纳入人工智能治理体系。

加大研究是认知基础。关于AI对儿童认知发展、情绪健康及潜在伤害的影响,相关证据才刚刚开始浮出水面。需加大对这一领域的研究投入,系统地评估不同类型的AI应用对不同年龄段儿童的具体影响,为精准施策提供科学依据。

源头治理靠安全设计。AI产品要在设计之初就引入儿童安全影响评估,不能等上市后再修补漏洞。在数据收集和处理的遵循最小化原则,要获得父母或监护人知情同意。在功能设计上体现克制,要设计家长授权机制,少占用屏幕时间,少进行社交刺激。

长远之计需提升素养。学校和家庭应将AI素养教育融入日常。家长要为孩子划



求真

食用油开封两月就不能吃了吗

中国经济网记者 朱晓倩

近期,网络上流传“食用油开封两个月就变质”的说法,引发不少家庭关注。很多人习惯参考包装上18个月的保质期,认为食用油耐储存,更倾向于购买大容量包装。那么,开封两个月后,食用油真的就不能吃了吗?

记者求证发现,2025年发表于《中国油脂》杂志的《家庭食用油条件下食用植物油的氧化酸败研究》一文中,通过模拟家庭用油,监测亚麻籽油、葵花籽油、大豆油、花生油(1升和5升包装)63天的氧化酸败情况。结果显示:酸值均未超标;过氧化值因油种和包装而异——5升装亚麻籽油在42天、葵花籽油在49天、大豆油在56天、花生油在63天超标;1升装亚麻籽油在28天、花生油在56天超标。因此,文章建议5升桶装油42天内、1升装28天内用完。

不过,也有专家指出,该实验是在特定温光条件和开闭频率下进行的,不同地区、不同季节、不同使用习惯(如开盖频率、存放位置)都会影响实际氧化速度,因此研究给出的时间节点属于参考性建议,并不适用于所有家庭场景的硬性标准。

科信食品与健康信息交流中心副主任、中华预防医学会健康传播分会委员阮光锋表示,实验数据具有参考价值,提醒消费者开封后尽快食用确有一定道理,但“时间上不必过于刻板”。他建议,家庭应

根据实际用油量选购包装规格;如果人口较多,一日三餐均在家烹饪,一大桶油可能1个月左右就用完,完全不必担忧;若人口少或不常做饭,则优先选择小瓶装,避免久存带来的品质下降。即便略超建议时间,只要油品未出现明显的哈喇味、浑浊或沉淀,通常仍可安全使用,不必因“到期”而盲目丢弃,造成不必要的浪费。

想要延长食用油开封后的新鲜度,科学的储存方法至关重要。业内人士介绍,首先,油脂与氧气接触会加速自动氧化,因此每次使用后务必立即拧紧瓶盖,减少空气进入。其次,光照会促进氧化反应,应将油瓶放在橱柜等避光处,远离窗边等阳光直射的位置。再次,灶台旁的高温环境会显著加快氧化速率,因此不宜将油瓶长期置于炉灶附近。最后,对于大桶油建议分装至深色小瓶中,日常取用小瓶,大桶密封后置于阴凉干燥处,减少整桶油反复开启暴露于空气中的次数。这些简单使用习惯能有效延缓油脂劣变,保持其风味和营养。



更多

扫码