

人工智能标准化白皮书

(2018 版)

指导单位：国家标准化管理委员会工业二部

编写单位：中国电子技术标准化研究院

二零一八年一月

每日免费获取报告

- 1、每日微信群内分享**5+**最新重磅报告；
- 2、每日分享当日**华尔街日报**、金融时报；
- 3、每周分享**经济学人**
- 4、每月汇总**500+**份当月重磅报告
(增值服务)

扫一扫二维码

关注公众号

回复：**研究报告**

加入“起点财经”微信群。



编写单位（排名不分先后）

中国电子技术标准化研究院

中国科学院自动化研究所

北京理工大学

清华大学

北京大学

中国人民大学

北京航空航天大学

科大讯飞股份有限公司

华为技术有限公司

国际商业机器（中国）有限公司

阿里云计算有限公司

中国科学院计算技术研究所

中国电信集团公司

腾讯互联网加（深圳）有限公司

阿里巴巴网络技术有限公司

上海计算机软件技术开发中心

上海智臻智能网络科技股份有限公司

北京爱奇艺科技有限公司

北京有生志广科技有限公司

极限元（北京）智能科技股份有限公司

北京字节跳动科技有限公司（今日头条）

北京商汤科技开发有限公司

浙江蚂蚁小微金融服务集团有限公司

百度网络技术有限公司

英特尔（中国）有限公司

松下电器（中国）有限公司

重庆凯泽科技股份有限公司

海尔工业智能研究院有限公司

重庆中科云从科技有限公司

北京格灵深瞳信息技术有限公司

目录

1 前言	1
1.1 研究背景	1
1.2 研究目标及意义	2
2 人工智能概述	3
2.1 人工智能的历史及概念	3
2.1.1 人工智能的起源与历史	3
2.1.2 人工智能的概念	5
2.2 人工智能的特征	7
2.3 人工智能参考框架	8
3 人工智能发展现状及趋势	11
3.1 人工智能关键技术	11
3.1.1 机器学习	11
3.1.2 知识图谱	13
3.1.3 自然语言处理	14
3.1.4 人机交互	15
3.1.5 计算机视觉	17
3.1.6 生物特征识别	19
3.1.7 虚拟现实/增强现实	21
3.1.8 人工智能技术发展趋势	21
3.2 人工智能产业现状及趋势	22
3.2.1 智能基础设施	23
3.2.2 智能信息及数据	24
3.2.3 智能技术服务	25
3.2.4 智能产品	25
3.2.5 人工智能行业应用	27
3.2.6 人工智能产业发展趋势	31
3.3 安全、伦理、隐私问题	32
3.3.1 人工智能的安全问题	32
3.3.2 人工智能的伦理问题	33
3.3.3 人工智能的隐私问题	34
3.4 人工智能标准化的重要作用	35
4 人工智能标准化现状	37
4.1 国际标准化现状	37
4.1.1 ISO/IEC JTC 1	37
4.1.2 ISO	40
4.1.3 IEC	40

4.1.4 ITU	41
4.2 国外标准化现状	41
4.2.1 IEEE	41
4.2.2 NIST	41
4.2.3 其它	42
4.3 国内标准化现状	42
4.3.1 全国信息技术标准化技术委员会.....	42
4.3.2 全国自动化系统与集成标准化技术委员会.....	43
4.3.3 全国音频、视频和多媒体标准化技术委员会.....	43
4.3.4 全国信息安全标准化技术委员会.....	43
4.3.5 全国智能运输系统标准化技术委员会.....	44
4.4 人工智能标准化面临的问题和挑战	44
4.5 人工智能标准需求分析	45
4.6 人工智能标准化组织机制建设	46
5 人工智能标准体系	48
5.1 人工智能标准体系结构	48
5.2 标准体系框架	49
5.2.1 基础标准.....	51
5.2.2 平台/支撑标准.....	51
5.2.3 关键技术标准.....	51
5.2.4 产品及服务标准.....	53
5.2.5 应用标准.....	54
5.2.6 安全/伦理标准.....	56
5.3 近期急需制定标准	56
6 人工智能标准化工作重点建议	59
附件1 人工智能标准明细表	61
附件2 应用案例	71

1 前言

1.1 研究背景

人工智能概念诞生于 1956 年，在半个多世纪的发展历程中，由于受到智能算法、计算速度、存储水平等多方面因素的影响，人工智能技术和应用发展经历了多次高潮和低谷。2006 年以来，以深度学习为代表的机器学习算法在机器视觉和语音识别等领域取得了极大的成功，识别准确性大幅提升，使人工智能再次受到学术界和产业界的广泛关注。云计算、大数据等技术在提升运算速度，降低计算成本的同时，也为人工智能发展提供了丰富的数据资源，协助训练出更加智能化的算法模型。人工智能的发展模式也从过去追求“用计算机模拟人工智能”，逐步转向以机器与人结合而成的增强型混合智能系统，用机器、人、网络结合成新的群智系统，以及用机器、人、网络和物结合成的更加复杂的智能系统。

作为新一轮产业变革的核心驱动力，人工智能在催生新技术、新产品的同时，对传统行业也具备较强的赋能作用，能够引发经济结构的重大变革，实现社会生产力的整体跃升。人工智能将人从枯燥的劳动中解放出来，越来越多的简单性、重复性、危险性任务由人工智能系统完成，在减少人力投入，提高工作效率的同时，还能够比人类做得更快、更准确；人工智能还可以在教育、医疗、养老、环境保护、城市运行、司法服务等领域得到广泛应用，能够极大提高公共服务精准化水平，全面提升人民生活品质；同时，人工智能可帮助人类准确感知、预测、预警基础设施和社会安全运行的重大态势，及时把握群体认知及心理变化，主动作出决策反应，显著提高社会治理能力和水平，同时保障公共安全。

人工智能作为一项引领未来的战略技术，世界发达国家纷纷在新一轮国际竞争中争取掌握主导权，围绕人工智能出台规划和政策，对人工智能核心技术、顶尖人才、标准规范等进行部署，加快促进人工智能技术和产业发展。主要科技企业不断加大资金和人力投入，抢占人工智能发展制高点。2017 年，我国出台了《新一代人工智能发展规划》（国发〔2017〕35 号）、《促进新一代人工智能产业发展三年行动计划（2018-2020 年）》（工信部科〔2017〕315 号）等政策文件，推动人工智能技术研发和产业化发展。目前，国内人工智能发展已具备一定的技术和产业基础，在芯片、数据、平台、应用等领域集聚了一批人工智能企业，在

部分方向取得阶段性成果并向市场化发展。例如，人工智能在金融、安防、客服等行业领域已实现应用，在特定任务中语义识别、语音识别、人脸识别、图像识别技术的精度和效率已远超人工。

标准化工作对人工智能及其产业发展具有基础性、支撑性、引领性的作用，既是推动产业创新发展的关键抓手，也是产业竞争的制高点。当前，在我国人工智能相关产品和服务不断丰富的时候，也出现了标准化程度不足的问题。人工智能涉及众多领域，虽然某些领域已具备一定的标准化基础，但是这些分散的标准化工作并不足以完全支撑整个人工智能领域。另一方面，人工智能属于新兴领域，发展方兴未艾，从世界范围来看，标准化工作仍在起步过程中，尚未形成完善的标准体系，我国基本与国外处于同一起跑线，存在快速突破的机会窗口。只要瞄准机会，快速布局，完全有可能抢占标准创新的制高点，反之，则有可能丧失良机。因此，迫切需要把握机遇，加快对人工智能技术及产业发展的研究，系统梳理、加快研制人工智能各领域的标准体系，明确标准之间的依存性与制约关系，建立统一完善的标准体系，以标准的手段促进我国人工智能技术、产业蓬勃发展。

1.2 研究目标及意义

本白皮书前期在国标委工业二部和工信部科技司的指导下，通过梳理人工智能技术、应用和产业演进情况，分析人工智能的技术热点、行业动态和未来趋势，从支撑人工智能产业整体发展的角度出发，研究制定了能够适应和引导人工智能产业发展的标准体系，进而提出近期急需研制的基础和关键标准项目。

本白皮书并不预期成为人工智能领域的全面技术和产业综述，不求面面俱到，仅针对目前人工智能领域涵盖的技术热点和产业情况进行分析，研究提出人工智能标准体系。人工智能标准化工作尚处于起步阶段，本白皮书只作为人工智能领域技术、产业和标准化之间初始的连接纽带，并将在今后不断根据技术、产业和标准化的发展需求进行修订。本白皮书不过多地给出人工智能领域观点性的陈述，力求以较为浅显易懂的语言和方式进行阐述。

本白皮书的意义在于与业界分享人工智能领域的研究成果和实践经验，呼吁社会各界共同加强人工智能领域的技术研究、产业投入、标准建设与服务应用，共同推动人工智能及其产业发展。

2 人工智能概述

2.1 人工智能的历史及概念

2.1.1 人工智能的起源与历史

人工智能始于 20 世纪 50 年代，至今大致分为三个发展阶段：第一阶段（20 世纪 50 年代——80 年代）。这一阶段人工智能刚诞生，基于抽象数学推理的可编程数字计算机已经出现，符号主义（Symbolism）快速发展，但由于很多事物不能形式化表达，建立的模型存在一定的局限性。此外，随着计算任务的复杂性不断加大，人工智能发展一度遇到瓶颈；第二阶段（20 世纪 80 年代——90 年代末）。在这一阶段，专家系统得到快速发展，数学模型有重大突破，但由于专家系统在知识获取、推理能力等方面的不足，以及开发成本高等原因，人工智能的发展又一次进入低谷期；第三阶段（21 世纪初——至今）。随着大数据的积聚、理论算法的革新、计算能力的提升，人工智能在很多应用领域取得了突破性进展，迎来了又一个繁荣时期。人工智能具体的发展历程如图 1 所示。

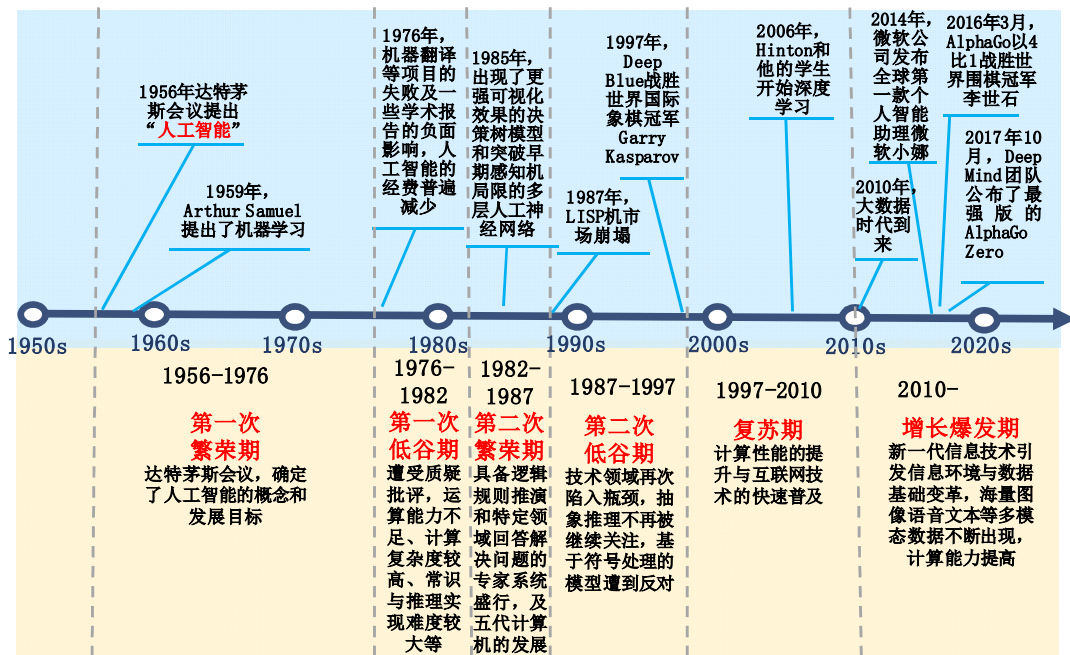


图 1 人工智能发展历史

长期以来，制造具有智能的机器一直是人类的重大梦想。早在 1950 年，Alan Turing 在《计算机与智能》中就阐述了对人工智能的思考。他提出的图灵测试是机器智能的重要测量手段，后来还衍生出了视觉图灵测试等测量方法。1956

年，“人工智能”这个词首次出现在达特茅斯会议上，标志着其作为一个研究领域的正式诞生。六十年来，人工智能发展潮起潮落的同时，基本思想可大致划分为四个流派：符号主义（Symbolism）、连接主义（Connectionism）、行为主义（Behaviourism）和统计主义（Statisticsism）（注：由于篇幅原因，本白皮书不对四个流派进行详细阐述）。这四个流派从不同侧面抓住了智能的部分特征，在“制造”人工智能方面都取得了里程碑式的成就。

1959年，Arthur Samuel 提出了机器学习，机器学习将传统的制造智能演化为通过学习能力来获取智能，推动人工智能进入了第一次繁荣期。20世纪70年代末期专家系统的出现，实现了人工智能从理论研究走向实际应用，从一般思维规律探索走向专门知识应用的重大突破，将人工智能的研究推向了新高潮。然而，机器学习的模型仍然是“人工”的，也有很大的局限性。随着专家系统应用的不断深入，专家系统自身存在的知识获取难、知识领域窄、推理能力弱、实用性差等问题逐步暴露。从1976年开始，人工智能的研究进入长达6年的萧瑟期。

在80年代中期，随着美国、日本立项支持人工智能研究，以及以知识工程为主导的机器学习方法的发展，出现了具有更强可视化效果的决策树模型和突破早期感知机局限的多层人工神经网络，由此带来了人工智能的又一次繁荣期。然而，当时的计算机难以模拟复杂度高及规模大的神经网络，仍有一定的局限性。1987年由于LISP机市场崩塌，美国取消了人工智能预算，日本第五代计算机项目失败并退出市场，专家系统进展缓慢，人工智能又进入了萧瑟期。

1997年，IBM深蓝（Deep Blue）战胜国际象棋世界冠军 Garry Kasparov。这是一次具有里程碑意义的成功，它代表了基于规则的人工智能的胜利。2006年，在 Hinton 和他的学生的推动下，深度学习开始备受关注，为后来人工智能的发展带来了重大影响。从2010年开始，人工智能进入爆发式的发展阶段，其最主要的驱动力是大数据时代的到来，运算能力及机器学习算法得到提高。人工智能快速发展，产业界也开始不断涌现出新的研发成果：2011年，IBM Watson 在综艺节目《危险边缘》中战胜了最高奖金得主和连胜纪录保持者；2012年，谷歌大脑通过模仿人类大脑在没有人类指导的情况下，利用非监督深度学习方法从大量视频中成功学习到识别出一只猫的能力；2014年，微软公司推出了一款实时口译系统，可以模仿说话者的声音并保留其口音；2014年，微软公司发布

全球第一款个人智能助理微软小娜；2014年，亚马逊发布至今为止最成功的智能音箱产品 Echo 和个人助手 Alexa；2016年，谷歌 AlphaGo 机器人在围棋比赛中击败了世界冠军李世石；2017年，苹果公司在原来个人助理 Siri 的基础上推出了智能私人助理 Siri 和智能音响 HomePod。

目前，世界各国都开始重视人工智能的发展。2017年6月29日，首届世界智能大会在天津召开。中国工程院院士潘云鹤在大会主论坛作了题为“中国新一代人工智能”的主题演讲，报告中概括了世界各国在人工智能研究方面的战略：2016年5月，美国白宫发表了《为人工智能的未来做好准备》；英国2016年12月发布《人工智能：未来决策制定的机遇和影响》；法国在2017年4月制定了《国家人工智能战略》；德国在2017年5月颁布全国第一部自动驾驶的法律；在中国，据不完全统计，2017年运营的人工智能公司接近400家，行业巨头百度、腾讯、阿里巴巴等都不断在人工智能领域发力。从数量、投资等角度来看，自然语言处理、机器人、计算机视觉成为了人工智能最为热门的三个产业方向。

2.1.2 人工智能的概念

人工智能作为一门前沿交叉学科，其定义一直存有不同观点：《人工智能——一种现代方法》中将已有的一些人工智能定义分为四类：像人一样思考的系统、像人一样行动的系统、理性地思考的系统、理性地行动的系统。维基百科上定义“人工智能就是机器展现出的智能”，即只要是某种机器，具有某种或某些“智能”的特征或表现，都应该算作“人工智能”。大英百科全书则限定人工智能是数字计算机或者数字计算机控制的机器人在执行智能生物体才有的一些任务上的能力。百度百科定义人工智能是“研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学”，将其视为计算机科学的一个分支，指出其研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。

本白皮书认为，人工智能是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。

人工智能的定义对人工智能学科的基本思想和内容作出了解释，即围绕智能

活动而构造的人工系统。人工智能是知识的工程，是机器模仿人类利用知识完成一定行为的过程。根据人工智能是否能真正实现推理、思考和解决问题，可以将人工智能分为弱人工智能和强人工智能。

弱人工智能是指不能真正实现推理和解决问题的智能机器，这些机器表面看像是智能的，但是并不真正拥有智能，也不会有自主意识。迄今为止的人工智能系统都还是实现特定功能的专用智能，而不是像人类智能那样能够不断适应复杂的新环境并不断涌现出新的功能，因此都还是弱人工智能。目前的主流研究仍然集中于弱人工智能，并取得了显著进步，如语音识别、图像处理和物体分割、机器翻译等方面取得了重大突破，甚至可以接近或超越人类水平。

强人工智能是指真正能思维的智能机器，并且认为这样的机器是有知觉的和自我意识的，这类机器可分为类人（机器的思考和推理类似人的思维）与非类人（机器产生了和人完全不一样的知觉和意识，使用和人完全不一样的推理方式）两大类。从一般意义来说，达到人类水平的、能够自适应地应对外界环境挑战的、具有自我意识的人工智能称为“通用人工智能”、“强人工智能”或“类人智能”。强人工智能不仅在哲学上存在巨大争论（涉及到思维与意识等根本问题的讨论），在技术上的研究也具有极大的挑战性。强人工智能当前鲜有进展，美国私营部门的专家及国家科技委员会比较支持的观点是，至少在未来几十年内难以实现。

靠符号主义、连接主义、行为主义和统计主义这四个流派的经典路线就能设计制造出强人工智能吗？其中一个主流看法是：即使有更高性能的计算平台和更大规模的大数据助力，也还只是量变，不是质变，人类对自身智能的认识还处在初级阶段，在人类真正理解智能机理之前，不可能制造出强人工智能。理解大脑产生智能的机理是脑科学的终极性问题，绝大多数脑科学专家都认为这是一个数百年乃至数千年甚至永远都解决不了的问题。

通向强人工智能还有一条“新”路线，这里称为“仿真主义”。这条新路线通过制造先进的大脑探测工具从结构上解析大脑，再利用工程技术手段构造出模仿大脑神经网络基元及结构的仿脑装置，最后通过环境刺激和交互训练仿真大脑实现类人智能，简言之，“先结构，后功能”。虽然这项工程也十分困难，但都是有可能在数十年内解决的工程技术问题，而不像“理解大脑”这个科学问题那样遥不可及。

仿真主义可以说是符号主义、连接主义、行为主义和统计主义之后的第五个流派，和前四个流派有着千丝万缕的联系，也是前四个流派通向强人工智能的关键一环。经典计算机是数理逻辑的开关电路实现，采用冯·诺依曼体系结构，可以作为逻辑推理等专用智能的实现载体。但要靠经典计算机不可能实现强人工智能。要按仿真主义的路线“仿脑”，就必须设计制造全新的软硬件系统，这就是“类脑计算机”，或者更准确地称为“仿脑机”。“仿脑机”是“仿真工程”的标志性成果，也是“仿脑工程”通向强人工智能之路的重要里程碑。

2.2 人工智能的特征

(1) **由人类设计，为人类服务，本质为计算，基础为数据。**从根本上说，人工智能系统必须以人为本，这些系统是人类设计出的机器，按照人类设定的程序逻辑或软件算法通过人类发明的芯片等硬件载体来运行或工作，其本质体现为计算，通过对数据的采集、加工、处理、分析和挖掘，形成有价值的信息流和知识模型，来为人类提供延伸人类能力的服务，来实现对人类期望的一些“智能行为”的模拟，在理想情况下必须体现服务人类的特点，而不应该伤害人类，特别是不应该有目的性地做出伤害人类的行为。

(2) **能感知环境，能产生反应，能与人交互，能与人互补。**人工智能系统应能借助传感器等器件产生对外界环境（包括人类）进行感知的能力，可以像人一样通过听觉、视觉、嗅觉、触觉等接收来自环境的各种信息，对外界输入产生文字、语音、表情、动作（控制执行机构）等必要的反应，甚至影响到环境或人类。借助于按钮、键盘、鼠标、屏幕、手势、体态、表情、力反馈、虚拟现实/增强现实等方式，人与机器间可以产生交互与互动，使机器设备越来越“理解”人类乃至与人类共同协作、优势互补。这样，人工智能系统能够帮助人类做人类不擅长、不喜欢但机器能够完成的工作，而人类则适合于去做更需要创造性、洞察力、想象力、灵活性、多变性乃至用心领悟或需要感情的一些工作。

(3) **有适应特性，有学习能力，有演化迭代，有连接扩展。**人工智能系统在理想情况下应具有一定的自适应特性和学习能力，即具有一定的随环境、数据或任务变化而自适应调节参数或更新优化模型的能力；并且，能够在此基础上通过与云、端、人、物越来越广泛深入数字化连接扩展，实现机器客体乃至人类主

体的演化迭代，以使系统具有适应性、鲁棒性、灵活性、扩展性，来应对不断变化的现实环境，从而使人工智能系统在各行各业产生丰富的应用。

2.3 人工智能参考框架

目前，人工智能领域尚未形成完善的参考框架。因此，本章基于人工智能的发展状况和应用特征，从人工智能信息流动的角度出发，提出一种人工智能参考框架（如图 2 所示），力图搭建较为完整的人工智能主体框架，描述人工智能系统总体工作流程，不受具体应用所限，适用于通用的人工智能领域需求。

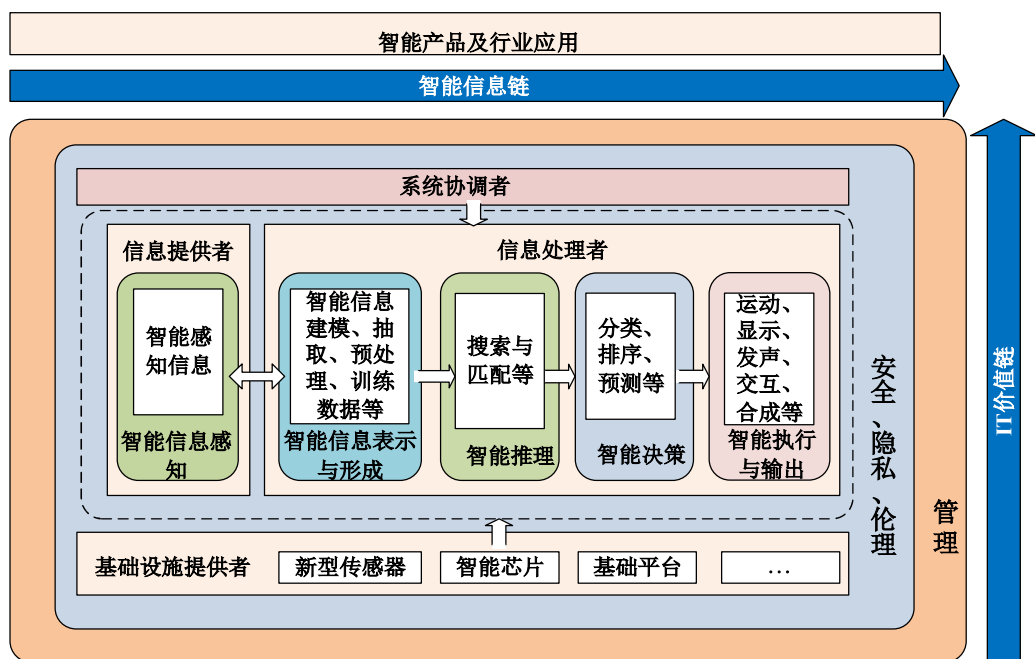


图 2 人工智能参考框架图

人工智能参考框架提供了基于“角色—活动—功能”的层级分类体系，从“智能信息链”（水平轴）和“IT 价值链”（垂直轴）两个维度阐述了人工智能系统框架。“智能信息链”反映从智能信息感知、智能信息表示与形成、智能推理、智能决策、智能执行与输出的一般过程。在这个过程中，智能信息是流动的载体，经历了“数据—信息—知识—智慧”的凝练过程。“IT 价值链”从人工智能的底层基础设施、信息（提供和处理技术实现）到系统的产业生态过程，反映人工智能为信息技术产业带来的价值。此外，人工智能系统还有其它非常重要的框架构件：安全、隐私、伦理和管理。人工智能系统主要由基础设施提供者、信息提供者、信息处理者和系统协调者 4 个角色组成。

（1）基础设施提供者

基础设施提供者为人工智能系统提供计算能力支持，实现与外部世界的沟通，并通过基础平台实现支撑。计算能力由智能芯片（CPU、GPU、ASIC、FPGA 等硬件加速芯片以及其它智能芯片）等硬件系统开发商提供；与外部世界的沟通通过新型传感器制造商提供；基础平台包括分布式计算框架提供商及网络提供商提供平台保障和支持，即包括云存储和计算、互联互通网络等。

（2）信息提供者

信息提供者在人工智能领域是智能信息的来源。通过知识信息感知过程由数据提供商提供智能感知信息，包括原始数据资源和数据集。原始数据资源的感知涉及到图形、图像、语音、文本的识别，还涉及到传统设备的物联网数据，包括已有系统的业务数据以及力、位移、液位、温度、湿度等感知数据。

（3）信息处理者

信息处理者是指人工智能领域中技术和服务提供商。信息处理者的主要活动包括智能信息表示与形成、智能推理、智能决策及智能执行与输出。智能信息处理者通常是算法工程师及技术服务提供商，通过计算框架、模型及通用技术，例如一些深度学习框架和机器学习算法模型等功能进行支撑。

智能信息表示与形成是指为描述外围世界所作的一组约定，分阶段对智能信息进行符号化和形式化的智能信息建模、抽取、预处理、训练数据等。

智能信息推理是指在计算机或智能系统中，模拟人类的智能推理方式，依据推理控制策略，利用形式化的信息进行机器思维和求解问题的过程，典型的功能是搜索与匹配。

智能信息决策是指智能信息经过推理后进行决策的过程，通常提供分类、排序、预测等功能。

智能执行与输出作为智能信息输出的环节，是对输入作出的响应，输出整个智能信息流动过程的结果，包括运动、显示、发声、交互、合成等功能。

（4）系统协调者

系统协调者提供人工智能系统必须满足的整体要求，包括政策、法律、资源

和业务需求，以及为确保系统符合这些需求而进行的监控和审计活动。由于人工智能是多学科交叉领域，需要系统协调者定义和整合所需的应用活动，使其在人工智能领域的垂直系统中运行。系统协调者的功能之一是配置和管理人工智能参考框架中的其他角色来执行一个或多个功能，并维持人工智能系统的运行。

（5）安全、隐私、伦理

安全、隐私、伦理覆盖了人工智能领域的其他 4 个主要角色，对每个角色都有重要的影响作用。同时，安全、隐私、伦理处于管理角色的覆盖范围之内，与全部角色和活动都建立了相关联系。在安全、隐私、伦理模块，需要通过不同的技术手段和安全措施，构筑全方位、立体的安全防护体系，保护人工智能领域参与者的安全和隐私。

（6）管理

管理角色承担系统管理活动，包括软件调配、资源管理等内容，管理的功能是监视各种资源的运行状况，应对出现的性能或故障事件，使得各系统组件透明且可观。

（7）智能产品及行业应用

智能产品及行业应用指人工智能系统的产品和应用，是对人工智能整体解决方案的封装，将智能信息决策产品化、实现落地应用，其应用领域主要包括：智能制造、智能交通、智能家居、智能医疗、智能安防等。

3 人工智能发展现状及趋势

依据参考框架中所涉及到的人工智能相关技术,本节重点介绍近二十年来人工智能领域关键技术的发展状况,包括机器学习、知识图谱、自然语言处理、计算机视觉、人机交互、生物特征识别、虚拟现实/增强现实等关键技术。

3.1 人工智能关键技术

3.1.1 机器学习

机器学习 (Machine Learning) 是一门涉及统计学、系统辨识、逼近理论、神经网络、优化理论、计算机科学、脑科学等诸多领域的交叉学科,研究计算机怎样模拟或实现人类的学习行为,以获取新的知识或技能,重新组织已有的知识结构使之不断改善自身的性能,是人工智能技术的核心。基于数据的机器学习是现代智能技术中的重要方法之一,研究从观测数据(样本)出发寻找规律,利用这些规律对未来数据或无法观测的数据进行预测。根据学习模式、学习方法以及算法的不同,机器学习存在不同的分类方法。

(1)根据学习模式将机器学习分类为监督学习、无监督学习和强化学习等。

监督学习

监督学习是利用已标记的有限训练数据集,通过某种学习策略/方法建立一个模型,实现对新数据/实例的标记(分类)/映射,最典型的监督学习算法包括回归和分类。监督学习要求训练样本的分类标签已知,分类标签精确度越高,样本越具有代表性,学习模型的准确度越高。监督学习在自然语言处理、信息检索、文本挖掘、手写体辨识、垃圾邮件侦测等领域获得了广泛应用。

无监督学习

无监督学习是利用无标记的有限数据描述隐藏在未标记数据中的结构/规律,最典型的非监督学习算法包括单类密度估计、单类数据降维、聚类等。无监督学习不需要训练样本和人工标注数据,便于压缩数据存储、减少计算量、提升算法速度,还可以避免正、负样本偏移引起的分类错误问题。主要用于经济预测、异常检测、数据挖掘、图像处理、模式识别等领域,例如组织大型计算机集群、社交网络分析、市场分割、天文数据分析等。

强化学习

强化学习是智能系统从环境到行为映射的学习，以使强化信号函数值最大。由于外部环境提供的信息很少，强化学习系统必须靠自身的经历进行学习。强化学习的目标是学习从环境状态到行为的映射，使得智能体选择的行为能够获得环境最大的奖赏，使得外部环境对学习系统在某种意义下的评价为最佳。其在机器人控制、无人驾驶、下棋、工业控制等领域获得成功应用。

(2) 根据学习方法可以将机器学习分为传统机器学习和深度学习。

传统机器学习

传统机器学习从一些观测（训练）样本出发，试图发现不能通过原理分析获得的规律，实现对未来数据行为或趋势的准确预测。相关算法包括逻辑回归、隐马尔科夫方法、支持向量机方法、K 近邻方法、三层人工神经网络方法、Adaboost 算法、贝叶斯方法以及决策树方法等。传统机器学习平衡了学习结果的有效性与学习模型的可解释性，为解决有限样本的学习问题提供了一种框架，主要用于有限样本情况下的模式分类、回归分析、概率密度估计等。传统机器学习方法共同的重要理论基础之一是统计学，在自然语言处理、语音识别、图像识别、信息检索和生物信息等许多计算机领域获得了广泛应用。

深度学习

深度学习是建立深层结构模型的学习方法，典型的深度学习算法包括深度置信网络、卷积神经网络、受限玻尔兹曼机和循环神经网络等。深度学习又称为深度神经网络（指层数超过 3 层的神经网络）。深度学习作为机器学习研究中的一个新兴领域，由 Hinton 等人于 2006 年提出。深度学习源于多层神经网络，其实质是给出了一种将特征表示和学习合二为一的方式。深度学习的特点是放弃了可解释性，单纯追求学习的有效性。经过多年的摸索尝试和研究，已经产生了诸多深度神经网络的模型，其中卷积神经网络、循环神经网络是两类典型的模型。卷积神经网络常被应用于空间性分布数据；循环神经网络在神经网络中引入了记忆和反馈，常被应用于时间性分布数据。深度学习框架是进行深度学习的基础底层框架，一般包含主流的神经网络算法模型，提供稳定的深度学习 API，支持训练模型在服务器和 GPU、TPU 间的分布式学习，部分框架还具备在包括移动设备、

云平台在内的多种平台上运行的移植能力，从而为深度学习算法带来前所未有的运行速度和实用性。目前主流的开源算法框架有 TensorFlow、Caffe/Caffe2、CNTK、MXNet、Paddle-paddle、Torch/PyTorch、Theano 等。

(3) 此外，机器学习的常见算法还包括迁移学习、主动学习和演化学习等。

迁移学习

迁移学习是指当在某些领域无法取得足够多的数据进行模型训练时，利用另一领域数据获得的关系进行的学习。迁移学习可以把已训练好的模型参数迁移到新的模型指导新模型训练，可以更有效的学习底层规则、减少数据量。目前的迁移学习技术主要在变量有限的小规模应用中使用，如基于传感器网络的定位，文字分类和图像分类等。未来迁移学习将被广泛应用于解决更有挑战性的问题，如视频分类、社交网络分析、逻辑推理等。

主动学习

主动学习通过一定的算法查询最有用的未标记样本，并交由专家进行标记，然后用查询到的样本训练分类模型来提高模型的精度。主动学习能够选择性地获取知识，通过较少的训练样本获得高性能的模型，最常用的策略是通过不确定性准则和差异性准则选取有效的样本。

演化学习

演化学习对优化问题性质要求极少，只需能够评估解的好坏即可，适用于求解复杂的优化问题，也能直接用于多目标优化。演化算法包括粒子群优化算法、多目标演化算法等。目前针对演化学习的研究主要集中在演化数据聚类、对演化数据更有效的分类，以及提供某种自适应机制以确定演化机制的影响等。

3.1.2 知识图谱

知识图谱本质上是结构化的语义知识库，是一种由节点和边组成的图数据结构，以符号形式描述物理世界中的概念及其相互关系，其基本组成单位是“实体—关系—实体”三元组，以及实体及其相关“属性—值”对。不同实体之间通过关系相互联结，构成网状的知识结构。在知识图谱中，每个节点表示现实世界的“实体”，每条边为实体与实体之间的“关系”。通俗地讲，知识图谱就是把所

有不同种类的信息连接在一起而得到的一个关系网络，提供了从“关系”的角度去分析问题的能力。

知识图谱可用于反欺诈、不一致性验证、组团欺诈等公共安全保障领域，需要用到异常分析、静态分析、动态分析等数据挖掘方法。特别地，知识图谱在搜索引擎、可视化展示和精准营销方面有很大的优势，已成为业界的热门工具。但是，知识图谱的发展还有很大的挑战，如数据的噪声问题，即数据本身有错误或者数据存在冗余。随着知识图谱应用的不断深入，还有一系列关键技术需要突破。

3.1.3 自然语言处理

自然语言处理是计算机科学领域与人工智能领域中的一个重要方向，研究能实现人与计算机之间用自然语言进行有效通信的各种理论和方法，涉及的领域较多，主要包括机器翻译、机器阅读理解和问答系统等。

(1) 机器翻译

机器翻译技术是指利用计算机技术实现从一种自然语言到另外一种自然语言的翻译过程。基于统计的机器翻译方法突破了之前基于规则和实例翻译方法的局限性，翻译性能取得巨大提升。基于深度神经网络的机器翻译在日常口语等一些场景的成功应用已经显现出了巨大的潜力。随着上下文的语境表征和知识逻辑推理能力的发展，自然语言知识图谱不断扩充，机器翻译将会在多轮对话翻译及篇章翻译等领域取得更大进展。

目前非限定领域机器翻译中性能较佳的一种是统计机器翻译，包括训练及解码两个阶段。训练阶段的目标是获得模型参数，解码阶段的目标是利用所估计的参数和给定的优化目标，获取待翻译语句的最佳翻译结果。统计机器翻译主要包括语料预处理、词对齐、短语抽取、短语概率计算、最大熵调序等步骤。基于神经网络的端到端翻译方法不需要针对双语句子专门设计特征模型，而是直接把源语言句子的词串送入神经网络模型，经过神经网络的运算，得到目标语言句子的翻译结果。在基于端到端的机器翻译系统中，通常采用递归神经网络或卷积神经网络对句子进行表征建模，从海量训练数据中抽取语义信息，与基于短语的统计翻译相比，其翻译结果更加流畅自然，在实际应用中取得了较好的效果。

(2) 语义理解

语义理解技术是指利用计算机技术实现对文本篇章的理解，并且回答与篇章相关问题的过程。语义理解更侧重于对上下文的理解以及对答案精准程度的把控。随着 MCTest 数据集的发布，语义理解受到更多关注，取得了快速发展，相关数据集和对应的神经网络模型层出不穷。语义理解技术将在智能客服、产品自动问答等相关领域发挥重要作用，进一步提高问答与对话系统的精度。

在数据采集方面，语义理解通过自动构造数据方法和自动构造填空题问题的方法来有效扩充数据资源。为了解决填充型问题，一些基于深度学习的方法相继提出，如基于注意力的神经网络方法。当前主流模型是利用神经网络技术对篇章、问题建模，对答案的开始和终止位置进行预测，抽取出篇章片段。对于进一步泛化的答案，处理难度进一步提升，目前的语义理解技术仍有较大的提升空间。

(3) 问答系统

问答系统分为开放领域的对话系统和特定领域的问答系统。问答系统技术是指让计算机像人类一样用自然语言与人交流的技术。人们可以向问答系统提交用自然语言表达的问题，系统会返回关联性较高的答案。尽管问答系统目前已经有了不少应用产品出现，但大多是在实际信息服务系统和智能手机助手等领域中的应用，在问答系统鲁棒性方面仍然存在着问题和挑战。

自然语言处理面临四大挑战：一是在词法、句法、语义、语用和语音等不同层面存在不确定性；二是新的词汇、术语、语义和语法导致未知语言现象的不可预测性；三是数据资源的不充分使其难以覆盖复杂的语言现象；四是语义知识的模糊性和错综复杂的关联性难以用简单的数学模型描述，语义计算需要参数庞大的非线性计算。

3.1.4 人机交互

人机交互主要研究人和计算机之间的信息交换，主要包括人到计算机和计算机到人的两部分信息交换，是人工智能领域的重要的外围技术。人机交互是与认知心理学、人机工程学、多媒体技术、虚拟现实技术等密切相关的综合学科。传统的人与计算机之间的信息交换主要依靠交互设备进行，主要包括键盘、鼠标、操纵杆、数据服装、眼动跟踪器、位置跟踪器、数据手套、压力笔等输入设备，

以及打印机、绘图仪、显示器、头盔式显示器、音箱等输出设备。人机交互技术除了传统的基本交互和图形交互外，还包括语音交互、情感交互、体感交互及脑机交互等技术，以下对后四种与人工智能关联密切的典型交互手段进行介绍。

（1）语音交互

语音交互是一种高效的交互方式，是人以自然语音或机器合成语音同计算机进行交互的综合性技术，结合了语言学、心理学、工程和计算机技术等领域的知识。语音交互不仅要研究语音识别和语音合成，还要研究人在语音通道下的交互机理、行为方式等。语音交互过程包括四部分：语音采集、语音识别、语义理解和语音合成。语音采集完成音频的录入、采样及编码；语音识别完成语音信息到机器可识别的文本信息的转化；语义理解根据语音识别转换后的文本字符或命令完成相应的操作；语音合成完成文本信息到声音信息的转换。作为人类沟通和获取信息最自然便捷的手段，语音交互比其他交互方式具备更多优势，能为人机交互带来根本性变革，是大数据和认知计算时代未来发展的制高点，具有广阔的发展前景和应用前景。

（2）情感交互

情感是一种高层次的信息传递，而情感交互是一种交互状态，它在表达功能和信息时传递情感，勾起人们的记忆或内心的情愫。传统的人机交互无法理解和适应人的情绪或心境，缺乏情感理解和表达能力，计算机难以具有类似人一样的智能，也难以通过人机交互做到真正的和谐与自然。情感交互就是要赋予计算机类似于人一样的观察、理解和生成各种情感的能力，最终使计算机像人一样能进行自然、亲切和生动的交互。情感交互已经成为人工智能领域中的热点方向，旨在让人机交互变得更加自然。目前，在情感交互信息的处理方式、情感描述方式、情感数据获取和处理过程、情感表达方式等方面还有诸多技术挑战。

（3）体感交互

体感交互是个体不需要借助任何复杂的控制系统，以体感技术为基础，直接通过肢体动作与周边数字设备装置和环境进行自然的交互。依照体感方式与原理的不同，体感技术主要分为三类：惯性感测、光学感测以及光学联合感测。体感交互通常由运动追踪、手势识别、运动捕捉、面部表情识别等一系列技术支撑。

与其他交互手段相比，体感交互技术无论是硬件还是软件方面都有了较大的提升，交互设备向小型化、便携化、使用方便化等方面发展，大大降低了对用户的约束，使得交互过程更加自然。目前，体感交互在游戏娱乐、医疗辅助与康复、全自动三维建模、辅助购物、眼动仪等领域有了较为广泛的应用。

(4) 脑机交互

脑机交互又称为脑机接口，指不依赖于外围神经和肌肉等神经通道，直接实现大脑与外界信息传递的通路。脑机接口系统检测中枢神经系统活动，并将其转化为人工输出指令，能够替代、修复、增强、补充或者改善中枢神经系统的正常输出，从而改变中枢神经系统与内外环境之间的交互作用。脑机交互通过对神经信号解码，实现脑信号到机器指令的转化，一般包括信号采集、特征提取和命令输出三个模块。从脑电信号采集的角度，一般将脑机接口分为侵入式和非侵入式两大类。除此之外，脑机接口还有其他常见的分类方式：按照信号传输方向可以分为脑到机、机到脑和脑机双向接口；按照信号生成的类型，可分为自发式脑机接口和诱发式脑机接口；按照信号源的不同还可分为基于脑电的脑机接口、基于功能性核磁共振的脑机接口以及基于近红外光谱分析的脑机接口。

3.1.5 计算机视觉

计算机视觉是使用计算机模仿人类视觉系统的科学，让计算机拥有类似人类提取、处理、理解和分析图像以及图像序列的能力。自动驾驶、机器人、智能医疗等领域均需要通过计算机视觉技术从视觉信号中提取并处理信息。近来随着深度学习的发展，预处理、特征提取与算法处理渐渐融合，形成端到端的人工智能算法技术。根据解决的问题，计算机视觉可分为计算成像学、图像理解、三维视觉、动态视觉和视频编解码五大类。

(1) 计算成像学

计算成像学是探索人眼结构、相机成像原理以及其延伸应用的科学。在相机成像原理方面，计算成像学不断促进现有可见光相机的完善，使得现代相机更加轻便，可以适用于不同场景。同时计算成像学也推动着新型相机的产生，使相机超出可见光的限制。在相机应用科学方面，计算成像学可以提升相机的能力，从而通过后续的计算处理使得在受限条件下拍摄的图像更加完善，例如图像去噪、

去模糊、暗光增强、去雾霾等，以及实现新的功能，例如全景图、软件虚化、超分辨率等。

（2）图像理解

图像理解是通过用计算机系统解释图像，实现类似人类视觉系统理解外部世界的一门科学。通常根据理解信息的抽象程度可分为三个层次：浅层理解，包括图像边缘、图像特征点、纹理元素等；中层理解，包括物体边界、区域与平面等；高层理解，根据需要抽取的高层语义信息，可大致分为识别、检测、分割、姿态估计、图像文字说明等。目前高层图像理解算法已逐渐广泛应用于人工智能系统，如刷脸支付、智慧安防、图像搜索等。

（3）三维视觉

三维视觉即研究如何通过视觉获取三维信息（三维重建）以及如何理解所获取的三维信息的科学。三维重建可以根据重建的信息来源，分为单目图像重建、多目图像重建和深度图像重建等。三维信息理解，即使用三维信息辅助图像理解或者直接理解三维信息。三维信息理解可分为，浅层：角点、边缘、法向量等；中层：平面、立方体等；高层：物体检测、识别、分割等。三维视觉技术可以广泛应用于机器人、无人驾驶、智慧工厂、虚拟/增强现实等方向。

（4）动态视觉

动态视觉即分析视频或图像序列，模拟人处理时序图像的科学。通常动态视觉问题可以定义为寻找图像元素，如像素、区域、物体在时序上的对应，以及提取其语义信息的问题。动态视觉研究被广泛应用在视频分析以及人机交互等方面。

（5）视频编解码

视频编解码是指通过特定的压缩技术，将视频流进行压缩。视频流传输中最为重要的编解码标准有国际电联的 H.261、H.263、H.264、H.265、M-JPEG 和 MPEG 系列标准。视频压缩编码主要分为两大类：无损压缩和有损压缩。无损压缩指使用压缩后的数据进行重构时，重构后的数据与原来的数据完全相同，例如磁盘文件的压缩。有损压缩也称为不可逆编码，指使用压缩后的数据进行重构时，重构后的数据与原来的数据有差异，但不会影响人们对原始资料所表达的信息产生误解。有损压缩的应用范围广泛，例如视频会议、可视电话、视频广播、视频

监控等。

目前，计算机视觉技术发展迅速，已具备初步的产业规模。未来计算机视觉技术的发展主要面临以下挑战：一是如何在不同的应用领域和其他技术更好的结合，计算机视觉在解决某些问题时可以广泛利用大数据，已经逐渐成熟并且可以超过人类，而在某些问题上却无法达到很高的精度；二是如何降低计算机视觉算法的开发时间和人力成本，目前计算机视觉算法需要大量的数据与人工标注，需要较长的研发周期以达到应用领域所要求的精度与耗时；三是如何加快新型算法的设计开发，随着新的成像硬件与人工智能芯片的出现，针对不同芯片与数据采集设备的计算机视觉算法的设计与开发也是挑战之一。

3.1.6 生物特征识别

生物特征识别技术是指通过个体生理特征或行为特征对个体身份进行识别认证的技术。从应用流程看，生物特征识别通常分为注册和识别两个阶段。注册阶段通过传感器对人体的生物表征信息进行采集，如利用图像传感器对指纹和人脸等光学信息、麦克风对说话声等声学信息进行采集，利用数据预处理以及特征提取技术对采集的数据进行处理，得到相应的特征进行存储。识别过程采用与注册过程一致的信息采集方式对待识别人进行信息采集、数据预处理和特征提取，然后将提取的特征与存储的特征进行比对分析，完成识别。从应用任务看，生物特征识别一般分为辨认与确认两种任务，辨认是指从存储库中确定待识别人身份的过程，是一对多的问题；确认是指将待识别人信息与存储库中特定单人信息进行比较，确定身份的过程，是一对一的问题。

生物特征识别技术涉及的内容十分广泛，包括指纹、掌纹、人脸、虹膜、指静脉、声纹、步态等多种生物特征，其识别过程涉及到图像处理、计算机视觉、语音识别、机器学习等多项技术。目前生物特征识别作为重要的智能化身份认证技术，在金融、公共安全、教育、交通等领域得到广泛的应用。下面将对指纹识别、人脸识别、虹膜识别、指静脉识别、声纹识别以及步态识别等技术进行介绍。

(1) 指纹识别

指纹识别过程通常包括数据采集、数据处理、分析判别三个过程。数据采集通过光、电、力、热等物理传感器获取指纹图像；数据处理包括预处理、畸变校

正、特征提取三个过程；分析判别是对提取的特征进行分析判别的过程。

（2）人脸识别

人脸识别是典型的计算机视觉应用，从应用过程来看，可将人脸识别技术划分为检测定位、面部特征提取以及人脸确认三个过程。人脸识别技术的应用主要受到光照、拍摄角度、图像遮挡、年龄等多个因素的影响，在约束条件下人脸识别技术相对成熟，在自由条件下人脸识别技术还在不断改进。

（3）虹膜识别

虹膜识别的理论框架主要包括虹膜图像分割、虹膜区域归一化、特征提取和识别四个部分，研究工作大多是基于此理论框架发展而来。虹膜识别技术应用的主要难题包含传感器和光照影响两个方面：一方面，由于虹膜尺寸小且受黑色素遮挡，需在近红外光源下采用高分辨图像传感器才可清晰成像，对传感器质量和稳定性要求比较高；另一方面，光照的强弱变化会引起瞳孔缩放，导致虹膜纹理产生复杂形变，增加了匹配的难度。

（4）指静脉识别

指静脉识别是利用了人体静脉血管中的脱氧血红蛋白对特定波长范围内的近红外线有很好的吸收作用这一特性，采用近红外光对指静脉进行成像与识别的技术。由于指静脉血管分布随机性很强，其网络特征具有很好的唯一性，且属于人体内部特征，不受到外界影响，因此模态特性十分稳定。指静脉识别技术应用面临的主要难题来自于成像单元。

（5）声纹识别

声纹识别是指根据待识别语音的声纹特征识别说话人的技术。声纹识别技术通常可以分为前端处理和建模分析两个阶段。声纹识别的过程是将某段来自某个人的语音经过特征提取后与多复合声纹模型库中的声纹模型进行匹配，常用的识别方法可以分为模板匹配法、概率模型法等。

（6）步态识别

步态是远距离复杂场景下唯一可清晰成像的生物特征，步态识别是指通过身体体型和行走姿态来识别人的身份。相比上述几种生物特征识别，步态识别的技

术难度更大，体现在其需要从视频中提取运动特征，以及需要更高要求的预处理算法，但步态识别具有远距离、跨角度、光照不敏感等优势。

3.1.7 虚拟现实/增强现实

虚拟现实（VR）/增强现实（AR）是以计算机为核心的新型视听技术。结合相关科学技术，在一定范围内生成与真实环境在视觉、听觉、触感等方面高度近似的数字化环境。用户借助必要的装备与数字化环境中的对象进行交互，相互影响，获得近似真实环境的感受和体验，通过显示设备、跟踪定位设备、触力觉交互设备、数据获取设备、专用芯片等实现。

虚拟现实/增强现实从技术特征角度，按照不同处理阶段，可以分为获取与建模技术、分析与利用技术、交换与分发技术、展示与交互技术以及技术标准与评价体系五个方面。获取与建模技术研究如何把物理世界或者人类的创意进行数字化和模型化，难点是三维物理世界的数字化和模型化技术；分析与利用技术重点研究对数字内容进行分析、理解、搜索和知识化方法，其难点是在于内容的语义表示和分析；交换与分发技术主要强调各种网络环境下大规模的数字化内容流通、转换、集成和面向不同终端用户的个性化服务等，其核心是开放的内容交换和版权管理技术；展示与交互技术重点研究符合人类习惯数字内容的各种显示技术及交互方法，以期提高人对复杂信息的认知能力，其难点在于建立自然和谐的人机交互环境；标准与评价体系重点研究虚拟现实/增强现实基础资源、内容编目、信源编码等的规范标准以及相应的评估技术。

目前虚拟现实/增强现实面临的挑战主要体现在智能获取、普适设备、自由交互和感知融合四个方面。在硬件平台与装置、核心芯片与器件、软件平台与工具、相关标准与规范等方面存在一系列科学技术问题。总体来说虚拟现实/增强现实呈现虚拟现实系统智能化、虚实环境对象无缝融合、自然交互全方位与舒适化的发展趋势。

3.1.8 人工智能技术发展趋势

综上所述，人工智能技术在以下方面的发展有显著的特点，是进一步研究人工智能趋势的重点。

（1）技术平台开源化

开源的学习框架在人工智能领域的研发成绩斐然，对深度学习领域影响巨大。开源的深度学习框架使得开发者可以直接使用已经研发成功的深度学习工具，减少二次开发，提高效率，促进业界紧密合作和交流。国内外产业巨头也纷纷意识到通过开源技术建立产业生态，是抢占产业制高点的重要手段。通过技术平台的开源化，可以扩大技术规模，整合技术和应用，有效布局人工智能全产业链。谷歌、百度等国内外龙头企业纷纷布局开源人工智能生态，未来将有更多的软硬件企业参与开源生态。

（2）专用智能向通用智能发展

目前的人工智能发展主要集中在专用智能方面，具有领域局限性。随着科技的发展，各领域之间相互融合、相互影响，需要一种范围广、集成度高、适应能力强的通用智能，提供从辅助性决策工具到专业性解决方案的升级。通用人工智能具备执行一般智慧行为的能力，可以将人工智能与感知、知识、意识和直觉等人类的特征互相连接，减少对领域知识的依赖性、提高处理任务的普适性，这将是人工智能未来的发展方向。未来的人工智能将广泛的涵盖各个领域，消除各领域之间的应用壁垒。

（3）智能感知向智能认知方向迈进

人工智能的主要发展阶段包括：运算智能、感知智能、认知智能，这一观点得到业界的广泛认可。早期阶段的人工智能是运算智能，机器具有快速计算和记忆存储能力。当前大数据时代的人工智能是感知智能，机器具有视觉、听觉、触觉等感知能力。随着类脑科技的发展，人工智能必然向认知智能时代迈进，即让机器能理解会思考。

3.2 人工智能产业现状及趋势

人工智能作为新一轮产业变革的核心驱动力，将催生新的技术、产品、产业、业态、模式，从而引发经济结构的重大变革，实现社会生产力的整体提升。麦肯锡预计，到 2025 年全球人工智能应用市场规模总值将达到 1270 亿美元，人工智能将是众多智能产业发展的突破点。

通过对人工智能产业分布进行梳理，提出了人工智能产业生态图，主要分为核心业态、关联业态、衍生业态三个层次，如图 3 所示。

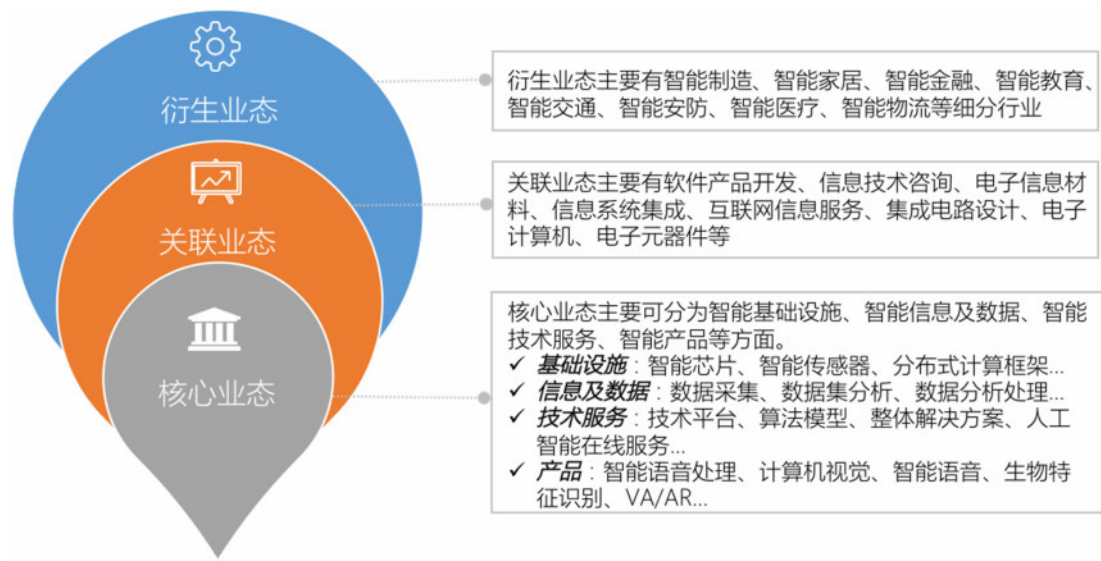


图 3 人工智能产业生态图

下面将重点对核心业态包含的智能基础设施建设、智能信息及数据、智能技术服务、智能产品四个方面展开介绍，并总结人工智能行业应用及产业发展趋势。

3.2.1 智能基础设施

智能基础设施为人工智能产业提供计算能力支撑，其范围包括智能传感器、智能芯片、分布式计算框架等，是人工智能产业发展的重要保障。

(1) 智能芯片

智能芯片从应用角度可以分为训练和推理两种类型。从部署场景来看，可以分为云端和设备端两步大类。训练过程由于涉及海量的训练数据和复杂的深度神经网络结构，需要庞大的计算规模，主要使用智能芯片集群来完成。与训练的计算量相比，推理的计算量较少，但仍然涉及大量的矩阵运算。目前，训练和推理通常都在云端实现，只有对实时性要求很高的设备会交由设备端进行处理。

按技术架构来看，智能芯片可以分为通用类芯片（CPU、GPU、FPGA）、基于 FPGA 的半定制化芯片、全定制化 ASIC 芯片、类脑计算芯片（IBM TrueNorth）。另外，主要的人工智能处理器还有 DPU、BPU、NPU、EPU 等适用于不同场景和功能的人工智能芯片。

随着互联网用户量和数据规模的急剧膨胀,人工智能发展对计算性能的要求迫切增长,对 CPU 计算性能提升的需求超过了摩尔定律的增长速度。同时,受限于技术原因,传统处理器性能也无法按照摩尔定律继续增长,发展下一代智能芯片势在必行。未来的智能芯片主要是在两个方向发展:一是模仿人类大脑结构的芯片,二是量子芯片。智能芯片是人工智能时代的战略制高点,预计到 2020 年人工智能芯片全球市场规模将突破百亿美元。

(2) 智能传感器

智能传感器是具有信息处理功能的传感器。智能传感器带有微处理机,具备采集、处理、交换信息等功能,是传感器集成化与微处理机相结合的产物。智能传感器属于人工智能的神经末梢,用于全面感知外界环境。各类传感器的大规模部署和应用为实现人工智能创造了不可或缺的条件。不同应用场景,如智能安防、智能家居、智能医疗等对传感器应用提出了不同的要求。未来,随着人工智能应用领域的不断拓展,市场对传感器的需求将不断增多,2020 年市场规模有望突破 4600 亿美元。未来,高敏度、高精度、高可靠性、微型化、集成化将成为智能传感器发展的重要趋势。

(3) 分布式计算框架

面对海量的数据处理、复杂的知识推理,常规的单机计算模式已经不能支撑。所以,计算模式必须将巨大的计算任务分成小的单机可以承受的计算任务,即云计算、边缘计算、大数据技术提供了基础的计算框架。目前流行的分布式计算框架如 OpenStack、Hadoop、Storm、Spark、Samza、Bigflow 等。各种开源深度学习框架也层出不穷,其中包括 TensorFlow、Caffe、Keras、CNTK、Torch7、MXNet、Leaf、Theano、DeepLearning4j、Lasagne、Neon 等等。

3.2.2 智能信息及数据

信息数据是人工智能创造价值的关键要素之一。我国庞大的人口和产业基数带来了数据方面的天生优势。随着算法、算力技术水平的提升,围绕数据的采集、分析、处理产生了众多的企业。目前,在人工智能数据采集、分析、处理方面的企业主要有两种:一种是数据集提供商,以提供数据为自身主要业务,为需求方提供机器学习等技术所需要的不同领域的数据集;另一种是数据采集、分析、处

理综合性厂商，自身拥有获取数据的途径，并对采集到的数据进行分析处理，最终将处理后的结果提供给需求方进行使用。对于一些大型企业，企业本身也是数据分析处理结果的需求方。

3.2.3 智能技术服务

智能技术服务主要关注如何构建人工智能的技术平台，并对外提供人工智能相关的服务。此类厂商在人工智能产业链中处于关键位置，依托基础设施和大量的数据，为各类人工智能的应用提供关键性的技术平台、解决方案和服务。目前，从提供服务的类型来看，提供技术服务厂商包括以下几类：

(1) 提供人工智能的技术平台和算法模型。此类厂商主要针对用户或者行业需求，提供人工智能技术平台以及算法模型。用户可以在人工智能平台之上，通过一系列的算法模型来进行人工智能的应用开发。此类厂商主要关注人工智能的通用计算框架、算法模型、通用技术等关键领域。

(2) 提供人工智能的整体解决方案。此类厂商主要针对用户或者行业需求，设计和提供包括软、硬件一体的行业人工智能解决方案，整体方案中集成多种人工智能算法模型以及软、硬件环境，帮助用户或行业解决特定的问题。此类厂商重点关注人工智能在特定领域或者特定行业的应用。

(3) 提供人工智能在线服务。此类厂商一般为传统的云服务提供厂商，主要依托其已有的云计算和大数据应用的用户资源，聚集用户的需求和行业属性，为客户提供多类型的人工智能服务；从各类模型算法和计算框架的 API 等特定应用平台到特定行业的整体解决方案等，进一步吸引大量的用户使用，从而进一步完善其提供的人工智能服务。此类厂商主要提供相对通用的人工智能服务，同时也会关注一些重点行业和领域。

需要指出的是，上述三类角色并不是严格区分开的，很多情况下会出现重叠，随着技术的发展成熟，在人工智能产业链中已有大量的厂商同时具备上述两类或者三类角色的特征。

3.2.4 智能产品

智能产品是指将人工智能领域的技术成果集成化、产品化，具体的分类如表

1 所示。

表 1 人工智能的产品

分类	典型产品示例	
智能机器人	工业机器人	焊接机器人、喷涂机器人、搬运机器人、加工机器人、装配机器人、清洁机器人以及其它工业机器人
	个人/家用服务机器人	家政服务机器人、教育娱乐服务机器人、养老助残服务机器人、个人运输服务机器人、安防监控服务机器人
	公共服务机器人	酒店服务机器人、银行服务机器人、场馆服务机器人和餐饮服务机器人
	特种机器人	特种极限机器人、康复辅助机器人、农业（包括农林牧副渔）机器人、水下机器人、军用和警用机器人、电力机器人、石油化工机器人、矿业机器人、建筑机器人、物流机器人、安防机器人、清洁机器人、医疗服务机器人及其它非结构和非家用机器人
智能运载工具	自动驾驶汽车	
	轨道交通系统	
	无人机	无人直升机、固定翼机、多旋翼飞行器、无人飞艇、无人伞翼机
	无人船	
智能终端	智能手机	
	车载智能终端	
	可穿戴终端	智能手表、智能耳机、智能眼镜
自然语言处理	机器翻译	
	机器阅读理解	
	问答系统	
	智能搜索	
计算机视觉	图像分析仪、视频监控系统	
生物特征识别	指纹识别系统	
	人脸识别系统	
	虹膜识别系统	
	指静脉识别系统	
	DNA、步态、掌纹、声纹等其它生物特征识别系统	
VR/AR	PC 端 VR、一体机 VR、移动端头显	
人机交互	语音交互	个人助理
		语音助手
		智能客服
	情感交互	
	体感交互	
	脑机交互	

随着制造强国、网络强国、数字中国建设进程的加快，在制造、家居、金融、教育、交通、安防、医疗、物流等领域对人工智能技术和产品的需求将进一步释放，相关智能产品的种类和形态也将越来越丰富。

3.2.5 人工智能行业应用

人工智能与行业领域的深度融合将改变甚至重新塑造传统行业，本节重点介绍人工智能在制造、家居、金融、交通、安防、医疗、物流行业的应用，由于篇幅有限，其它很多重要的行业应用在这里不展开论述。

(1) 智能制造

智能制造是基于新一代信息通信技术与先进制造技术深度融合，贯穿于设计、生产、管理、服务等制造活动的各个环节，具有自感知、自学习、自决策、自执行、自适应等功能新型生产方式。智能制造对人工智能的需求主要表现在以下三个方面：一是智能装备，包括自动识别设备、人机交互系统、工业机器人以及数控机床等具体设备，涉及到跨媒体分析推理、自然语言处理、虚拟现实智能建模及自主无人系统等关键技术。二是智能工厂，包括智能设计、智能生产、智能管理以及集成优化等具体内容，涉及到跨媒体分析推理、大数据智能、机器学习等关键技术。三是智能服务，包括大规模个性化定制、远程运维以及预测性维护等具体服务模式，涉及到跨媒体分析推理、自然语言处理、大数据智能、高级机器学习等关键技术。例如，现有涉及智能装备故障问题的纸质化文件，可通过自然语言处理，形成数字化资料，再通过非结构化数据向结构化数据的转换，形成深度学习所需的训练数据，从而构建设备故障分析的神经网络，为下一步故障诊断、优化参数设置提供决策依据。

(2) 智能家居

参照工业和信息化部印发的《智慧家庭综合标准化体系建设指南》，智能家居是智慧家庭八大应用场景之一。受产业环境、价格、消费者认可度等因素影响，我国智能家居行业经历了漫长的探索期。至 2010 年，随着物联网技术的发展以及智慧城市概念的出现，智能家居概念逐步有了清晰的定义并随之涌现出各类产品，软件系统也经历了若干轮升级。

智能家居以住宅为平台，基于物联网技术，由硬件（智能家电、智能硬件、安防控制设备、家具等）、软件系统、云计算平台构成的家居生态圈，实现人远程控制设备、设备间互联互通、设备自我学习等功能，并通过收集、分析用户行为数据为用户提供个性化生活服务，使家居生活安全、节能、便捷等。例如，借

助智能语音技术，用户应用自然语言实现对家居系统各设备的操控，如开关窗帘（窗户）、操控家用电器和照明系统、打扫卫生等操作；借助机器学习技术，智能电视可以从用户看电视的历史数据中分析其兴趣和爱好，并将相关的节目推荐给用户。通过应用声纹识别、脸部识别、指纹识别等技术进行开锁等；通过大数据技术可以使智能家电实现对自身状态及环境的自我感知，具有故障诊断能力。通过收集产品运行数据，发现产品异常，主动提供服务，降低故障率。还可以通过大数据分析、远程监控和诊断，快速发现问题、解决问题及提高效率。

（3）智能金融

人工智能的飞速发展将对身处服务价值链高端的金融业带来深刻影响，人工智能逐步成为决定金融业沟通客户、发现客户金融需求的重要因素。人工智能技术在金融业中可以用于服务客户，支持授信、各类金融交易和金融分析中的决策，并用于风险防控和监督，将大幅改变金融现有格局，金融服务将会更加地个性化与智能化。智能金融对于金融机构的业务部门来说，可以帮助获客，精准服务客户，提高效率；对于金融机构的风控部门来说，可以提高风险控制，增加安全性；对于用户来说，可以实现资产优化配置，体验到金融机构更加完美地服务。人工智能在金融领域的应用主要包括：智能获客，依托大数据，对金融用户进行画像，通过需求响应模型，极大地提升获客效率；身份识别，以人工智能为内核，通过人脸识别、声纹识别、指静脉识别等生物识别手段，再加上各类票据、身份证、银行卡等证件票据的 OCR 识别等技术手段，对用户身份进行验证，大幅降低核验成本，有助于提高安全性；大数据风控，通过大数据、算力、算法的结合，搭建反欺诈、信用风险等模型，多维度控制金融机构的信用风险和操作风险，同时避免资产损失；智能投顾，基于大数据和算法能力，对用户与资产信息进行标签化，精准匹配用户与资产；智能客服，基于自然语言处理能力和语音识别能力，拓展客服领域的深度和广度，大幅降低服务成本，提升服务体验；金融云，依托云计算能力的金融科技，为金融机构提供更安全高效的全套金融解决方案。

（4）智能交通

智能交通系统（Intelligent Traffic System, ITS）是通信、信息和控制技术在交通系统中集成应用的产物。ITS 借助现代科技手段和设备，将各核心交通元素联通，实现信息互通与共享以及各交通元素的彼此协调、优化配置和高效使用，

形成人、车和交通的一个高效协同环境，建立安全、高效、便捷和低碳的交通。例如通过交通信息采集系统采集道路中的车辆流量、行车速度等信息，信息分析处理系统处理后形成实时路况，决策系统据此调整道路红绿灯时长，调整可变车道或潮汐车道的通行方向等，通过信息发布系统将路况推送到导航软件和广播中，让人们合理规划行驶路线。通过不停车收费系统（ETC），实现对通过 ETC 入口站的车辆身份及信息自动采集、处理、收费和放行，有效提高通行能力、简化收费管理、降低环境污染。

ITS 应用最广泛的地区是日本，其次是美国、欧洲等地区。中国的智能交通系统近几年也发展迅速，在北京、上海、广州、杭州等大城市已经建设了先进的智能交通系统；其中，北京建立了道路交通控制、公共交通指挥与调度、高速公路管理和紧急事件管理等四大 ITS 系统；广州建立了交通信息共用主平台、物流信息平台 and 静态交通管理系统等三大 ITS 系统。

（5）智能安防

智能安防技术是一种利用人工智能对视频、图像进行存储和分析，从中识别安全隐患并对其进行处理的技术。智能安防与传统安防的最大区别在于智能化，传统安防对人的依赖性比较强，非常耗费人力，而智能安防能够通过机器实现智能判断，从而尽可能实现实时地安全防范和处理。

当前，高清视频、智能分析等技术的发展，使得安防从传统的被动防御向主动判断和预警发展，行业也从单一的安全领域向多行业应用发展，进而提升生产效率并提高生活智能化程度，为更多的行业和人群提供可视化及智能化方案。用户面对海量的视频数据，已无法简单利用人海战术进行检索和分析，需要采用人工智能技术作专家系统或辅助手段，实时分析视频内容，探测异常信息，进行风险预测。从技术方面来讲，目前国内智能安防分析技术主要集中在两大类：一类是采用画面分割前景提取等方法对视频画面中的目标进行提取检测，通过不同的规则来区分不同的事件，从而实现不同的判断并产生相应的报警联动等，例如：区域入侵分析、打架检测、人员聚集分析、交通事件检测等；另一类是利用模式识别技术，对画面中特定的物体进行建模，并通过大量样本进行训练，从而达到对视频画面中的特定物体进行识别，如车辆检测、人脸检测、人头检测（人流统计）等应用。

智能安防目前涵盖众多的领域，如街道社区、道路、楼宇建筑、机动车辆的监控，移动物体监测等。今后智能安防还要解决海量视频数据分析、存储控制及传输问题，将智能视频分析技术、云计算及云存储技术结合起来，构建智慧城市下的安防体系。

（6）智能医疗

人工智能的快速发展，为医疗健康领域向更高的智能化方向发展提供了非常有利的技术条件。近几年，智能医疗在辅助诊疗、疾病预测、医疗影像辅助诊断、药物开发等方面发挥重要作用。

在辅助诊疗方面，通过人工智能技术可以有效提高医护人员工作效率，提升一线全科医生的诊断治疗水平。如利用智能语音技术可以实现电子病历的智能语音录入；利用智能影像识别技术，可以实现医学图像自动读片；利用智能技术和大数据平台，构建辅助诊疗系统。

在疾病预测方面，人工智能借助大数据技术可以进行疫情监测，及时有效地预测并防止疫情的进一步扩散和发展。以流感为例，很多国家都有规定，当医生发现新型流感病例时需告知疾病控制与预防中心。但由于人们可能患病不及时就医，同时信息传达回疾控中心也需要时间，因此，通告新流感病例时往往会有一定的延迟，人工智能通过疫情监测能够有效缩短响应时间。

在医疗影像辅助诊断方面，影像判读系统的发展是人工智能技术的产物。早期的影像判读系统主要靠人手工编写判定规则，存在耗时长、临床应用难度大等问题，从而未能得到广泛推广。影像组学是通过医学影像对特征进行提取和分析，为患者预前和预后的诊断和治疗提供评估方法和精准诊疗决策。这在很大程度上简化了人工智能技术的应用流程，节约了人力成本。

（7）智能物流

传统物流企业在利用条形码、射频识别技术、传感器、全球定位系统等方面优化改善运输、仓储、配送装卸等物流业基本活动，同时也在尝试使用智能搜索、推理规划、计算机视觉以及智能机器人等技术，实现货物运输过程的自动化运作和高效优化管理，提高物流效率。例如，在仓储环节，利用大数据智能通过分析大量历史库存数据，建立相关预测模型，实现物流库存商品的动态调整。大数

据智能也可以支撑商品配送规划，进而实现物流供给与需求匹配、物流资源优化与配置等。在货物搬运环节，加载计算机视觉、动态路径规划等技术的智能搬运机器人（如搬运机器人、货架穿梭车、分拣机器人等）得到广泛应用，大大减少了订单出库时间，使物流仓库的存储密度、搬运的速度、拣选的精度均有大幅度提升。

3.2.6 人工智能产业发展趋势

从人工智能产业进程来看，技术突破是推动产业升级的核心驱动力。数据资源、运算能力、核心算法共同发展，掀起人工智能第三次新浪潮。人工智能产业正处于从感知智能向认知智能的进阶阶段，前者涉及的智能语音、计算机视觉及自然语言处理等技术，已具有大规模应用基础，但后者要求的“机器要像人一样去思考及主动行动”仍尚待突破，诸如无人驾驶、全自动智能机器人等仍处于开发中，与大规模应用仍有一定距离。

（1）智能服务呈现线下和线上的无缝结合

分布式计算平台的广泛部署和应用，增大了线上服务的应用范围。同时人工智能技术的发展和产品不断涌现，如智能家居、智能机器人、自动驾驶汽车等，为智能服务带来新的渠道或新的传播模式，使得线上服务与线下服务的融合进程加快，促进多产业升级。

（2）智能化应用场景从单一向多元发展

目前人工智能的应用领域还多处于专用阶段，如人脸识别、视频监控、语音识别等都主要用于完成具体任务，覆盖范围有限，产业化程度有待提高。随着智能家居、智慧物流等产品的推出，人工智能的应用终将进入面向复杂场景，处理复杂问题，提高社会生产效率和生活质量的新阶段。

（3）人工智能和实体经济深度融合进程将进一步加快

党的十九大报告提出“推动互联网、大数据、人工智能和实体经济深度融合”，一方面，随着制造强国建设的加快将促进人工智能等新一代信息技术产品发展和应用，助推传统产业转型升级，推动战略性新兴产业实现整体性突破。另一方面，随着人工智能底层技术的开源化，传统行业将有望加快掌握人工智能基础技术并

依托其积累的行业数据资源实现人工智能与实体经济的深度融合创新。

3.3 安全、伦理、隐私问题

历史经验表明新技术常常能够提高生产效率，促进社会进步。但与此同时，由于人工智能尚处于初期发展阶段，该领域的安全、伦理、隐私的政策、法律和标准问题值得关注。就人工智能技术而言，安全、伦理和隐私问题直接影响人们与人工智能工具交互经验中对人工智能技术的信任。社会公众必须信任人工智能技术能够给人类带来的安全利益远大于伤害，才有可能发展人工智能。要保障安全，人工智能技术本身及在各个领域的应用应遵循人类社会所认同的伦理原则，其中应特别关注的是隐私问题，因为人工智能的发展伴随着越来越多的个人数据被记录和分析，而在这个过程中保障个人隐私则是社会信任能够增加的重要条件。总之，建立一个令人工智能技术造福于社会、保护公众利益的政策、法律和标准化环境，是人工智能技术持续、健康发展的重要前提。为此，本章集中讨论与人工智能技术相关的安全、伦理、隐私的政策和法律问题。

3.3.1 人工智能的安全问题

人工智能最大的特征是能够实现无人干预的，基于知识并能够自我修正地自动化运行。在开启人工智能系统后，人工智能系统的决策不再需要操控者进一步的指令，这种决策可能会产生人类预料不到的结果。设计者和生产者在开发人工智能产品的过程中可能并不能准确预知某一产品会存在的风险。因此，对于人工智能的安全问题不容忽视。

与传统的公共安全（例如核技术）需要强大的基础设施作为支撑不同，人工智能以计算机和互联网为依托，无需昂贵的基础设施就能造成安全威胁。掌握相关技术的人员可以在任何时间、地点且没有昂贵基础设施的情况下做出人工智能产品。人工智能的程序运行并非公开可追踪，其扩散途径和速度也难以精确控制。在无法利用已有传统管制技术的条件下，对人工智能技术的管制必须另辟蹊径。换言之，管制者必须考虑更为深层的伦理问题，保证人工智能技术及其应用均应符合伦理要求，才能真正实现保障公共安全的目的。

由于人工智能技术的目标实现受其初始设定的影响，必须能够保障人工智能

设计的目标与大多数人类的利益和伦理道德一致，即使在决策过程中面对不同的环境，人工智能也能做出相对安全的决定。从人工智能的技术应用方面看，要充分考虑到人工智能开发和部署过程中的责任和过错问题，通过为人工智能技术开发者、产品生产者或者服务提供者、最终使用者设定权利和义务的具体内容，来达到落实安全保障要求的目的。

此外，考虑到目前世界各国关于人工智能管理的规定尚不统一，相关标准也处于空白状态，同一人工智能技术的参与者可能来自不同国家，而这些国家尚未签署针对人工智能的共有合约。为此，我国应加强国际合作，推动制定一套世界通用的管制原则和标准来保障人工智能技术的安全性。

3.3.2 人工智能的伦理问题

人工智能是人类智能的延伸，也是人类价值系统的延伸。在其发展的过程中，应当包含对人类伦理价值的正确考量。设定人工智能技术的伦理要求，要依托于社会和公众对人工智能伦理的深入思考和广泛共识，并遵循一些共识原则：

一是人类利益原则，即人工智能应以实现人类利益为终极目标。这一原则体现对人权的尊重、对人类和自然环境利益最大化以及降低技术风险和对社会的负面影响。在此原则下，政策和法律应致力于人工智能发展的外部社会环境的构建，推动对社会个体的人工智能伦理和安全意识教育，让社会警惕人工智能技术被滥用的风险。此外，还应该警惕人工智能系统作出与伦理道德偏差的决策。例如，大学利用机器学习算法来评估入学申请，假如用于训练算法的历史入学数据（有意或无意）反映出之前的录取程序的某些偏差（如性别歧视），那么机器学习可能会在重复累计的运算过程中恶化这些偏差，造成恶性循环。如果没有纠正，偏差会以这种方式在社会中永久存在。

二是责任原则，即在技术开发和应用两方面都建立明确的责任体系，以便在技术层面可以对人工智能技术开发人员或部门问责，在应用层面可以建立合理的时间和赔偿体系。在责任原则下，在技术开发方面应遵循透明度原则；在技术应用方面则应当遵循权责一致原则。

其中，透明度原则要求了解系统的工作原理从而预测未来发展，即人类应当知道人工智能如何以及为何做出特定决定，这对于责任分配至关重要。例如，在

神经网络这个人工智能的重要议题中，人们需要知道为什么会产生特定的输出结果。另外，数据来源透明度也同样非常重要。即便是在处理没有问题的数据集时，也有可能面临数据中隐含的偏见问题。透明度原则还要求开发技术时注意多个人工智能系统协作产生的危害。

权责一致原则，指的是未来政策和法律应该做出明确规定：一方面必要的商业数据应被合理记录、相应算法应受到监督、商业应用应受到合理审查；另一方面商业主体仍可利用合理的知识产权或者商业秘密来保护本企业的核心参数。在人工智能的应用领域，权利和责任一致的原则尚未在商界、政府对伦理的实践中完全实现。主要是由于在人工智能产品和服务的开发和生产过程中，工程师和设计团队往往忽视伦理问题，此外人工智能的整个行业尚未习惯于综合考量各个利益相关者需求的工作流程，人工智能相关企业对商业秘密的保护也未与透明度相平衡。

3.3.3 人工智能的隐私问题

人工智能的近期发展是建立在大量数据的信息技术应用之上，不可避免地涉及到个人信息的合理使用问题，因此对于隐私应该有明确且可操作的定义。人工智能技术的发展也让侵犯个人隐私（的行为）更为便利，因此相关法律和标准应该为个人隐私提供更强有力的保护。已有的对隐私信息的管制包括对使用者未明示同意的收集，以及使用者明示同意条件下的个人信息收集两种类型的处理。人工智能技术的发展对原有的管制框架带来了新的挑战，原因是使用者所同意的个人信息收集范围不再有确定的界限。利用人工智能技术很容易推导出公民不愿意泄露的隐私，例如从公共数据中推导出私人信息，从个人信息中推导出和个人有关的其他人员（如朋友、亲人、同事）信息（在线行为、人际关系等）。这类信息超出了最初个人同意披露的个人信息范围。

此外，人工智能技术的发展使得政府对于公民个人数据信息的收集和使用更加便利。大量个人数据信息能够帮助政府各个部门更好地了解所服务的人群状态，确保个性化服务的机会和质量。但随之而来的是，政府部门和政府工作人员个人不恰当使用个人数据信息的风险和潜在的危害应当得到足够的重视。

人工智能语境下的个人数据的获取和知情同意应该重新进行定义。首先，相

关政策、法律和标准应直接对数据的收集和使用进行规制，而不能仅仅征得数据所有者的同意；其次，应当建立实用、可执行的、适应于不同使用场景的标准流程以供设计者和开发者保护数据来源的隐私；再次，对于利用人工智能可能推导出超过公民最初同意披露的信息的行为应该进行规制。最后，政策、法律和标准对于个人数据管理应该采取延伸式保护，鼓励发展相关技术，探索将算法工具作为个体在数字和现实世界中的代理人。这种方式使得控制和使用两者得以共存，因为算法代理人可以根据不同的情况，设定不同的使用权限，同时管理个人同意与拒绝分享的信息。

本章节所涉及的安全、伦理和隐私问题是人工智能发展面临的挑战。安全问题是让技术能够持续发展的前提。技术的发展给社会信任带来了风险，如何增加社会信任，让技术发展遵循伦理要求，特别是保障隐私不会被侵犯是亟需解决的问题。为此，需要（制订）合理的政策、法律、标准基础，并与国际社会协作。在制订政策、法律和标准时，应当摆脱肤浅的新闻炒作和广告式的热点宣传，必须促进对人工智能技术产品更深层地理解，聚焦这一新技术给社会产生重大利益的同时也带来的巨大挑战。作为国际社会的重要成员，中国对保障人工智能技术应用在正确的道路上、基于正确的理由得到健康发展担负重要的责任。

3.4 人工智能标准化的重要作用

当今，经济全球化和市场国际化深入发展，标准作为经济和社会活动的主要技术依据，已成为衡量国家或地区技术发展水平的重要标志、产品进入市场的基本准则、企业市场竞争力的具体体现。标准化工作对人工智能及其产业发展具有基础性、支撑性、引领性的作用，既是推动产业创新发展的关键抓手，也是产业竞争的制高点。人工智能标准的先进与完善与否，关系到产业的健康发展、以及产品国际市场竞争力的强弱。

美国、欧盟、日本等发达国家高度重视人工智能标准化工作。美国发布的《国家人工智能研究与发展战略规划》，欧盟发布的“人脑计划”，日本实施的“人工智能/大数据/物联网/网络安全综合项目”，均提出围绕核心技术、顶尖人才、标准规范等强化部署，力图抢占新一轮科技主导权。

我国高度重视人工智能标准化工作。在国务院《新一代人工智能发展规划》

中将人工智能标准化作为重要支撑保障，提出要“加强人工智能标准框架体系研究。坚持安全性、可用性、互操作性、可追溯性原则，逐步建立并完善人工智能基础共性、互联互通、行业应用、网络安全、隐私保护等技术标准。加快推动无人驾驶、服务机器人等细分应用领域的行业协会和联盟制定相关标准”。工信部在《促进新一代人工智能产业发展三年行动计划（2018-2020年）》中指出，要建设人工智能产业标准规范体系，建立并完善基础共性、互联互通、安全隐私、行业应用等技术标准；同时构建人工智能产品评估评测体系。

我国虽然在人工智能领域虽然具备了良好基础，语音识别、视觉识别、中文信息处理等核心技术实现了突破，也具有巨大的应用市场环境，但整体发展水平仍落后于发达国家，在核心算法、关键设备、高端芯片、重大产品与系统等方面差距较大，适应人工智能发展的基础设施、政策法规、标准体系亟待完善。

综上分析，更应重视人工智能标准化工作对于促进技术创新、支撑产业发展具有的重要引领作用：

（一）标准化工作有利于加快人工智能技术创新和成果转化。现阶段人工智能技术发展迅速，市场上逐步出现了可规模化、可商业化的产品和应用，需要以标准化的手段固化技术成果，实现快速创新推广；

（二）标准化工作有助于提升人工智能产品和服务质量。如市场上出现的人脸识别系统、智能音箱、服务机器人等产品，质量残次不齐，需要标准的统一规范，并配合以开展符合性测试评估的方式，提升产品和服务质量；

（三）标准化工作有助于切实保障用户安全。例如自动驾驶领域的“电车难题”伦理难题、苹果手机指纹泄露用户隐私等问题，引起了人们的广泛关注。如何保护用户权益是难点也是重点，这需要通过建立以人为本的原则，制定相关安全标准规范，确保智能系统遵从并服务于人类伦理，并确保信息安全；

（四）标准化工作有助于营造公平开放的人工智能产业生态。当前，行业巨头以开源算法、平台接口绑定等方式，打造自有深度学习框架等生态体系，造成用户数据信息较难迁移。这需要统一的标准实现厂商之间的互操作与协同工作，防止行业垄断、用户绑定，形成良性的产业生态。

4 人工智能标准化现状

近年来，在国际标准化组织、国外标准化组织、以及国内标准化组织都在研究人工智能问题，并进行相关技术的标准化工作。

4.1 国际标准化现状

4.1.1 ISO/IEC JTC 1

ISO/IEC JTC 1（国际标准化组织和国际电工委员会第一联合技术委员会）在人工智能领域的标准化工作已有 20 多年的历史。前期，在人工智能词汇、人机交互、生物特征识别、计算机图像处理等关键领域，以及云计算、大数据、传感网等人工智能技术支撑领域，ISO/IEC JTC 1 均已开展了相关标准化工作。

在词汇领域，ISO/IEC JTC 1 词汇工作组发布了 ISO/IEC 2382-28:1995《信息技术 词汇 第 28 部分：人工智能基本概念与专家系统》、ISO/IEC 2382-29:1999《信息技术 词汇 第 29 部分：人工智能语音识别与合成》、ISO/IEC 2382-31:1997《信息技术 词汇 第 31 部分：人工智能机器学习》、ISO/IEC 2382-34:1999《信息技术 词汇 第 34 部分：人工智能神经网络》等 4 项标准。目前，上述标准已经废止，相关术语收录在 ISO/IEC 2382:2015《信息技术 词汇》标准中。

在人机交互领域，ISO/IEC JTC 1/SC 35（用户界面分技术委员会）开展了语音交互、手势交互和情感交互等标准项目。语音交互方面有 ISO/IEC 30122-1《信息技术 语音命令 第 1 部分：框架和通用指南》、ISO/IEC 30122-2《信息技术 语音命令 第 2 部分：构建和测试》、ISO/IEC 30122-3《信息技术 语音命令 第 3 部分：翻译和本地化》、ISO/IEC 30122-4《信息技术 语音命令 第 4 部分：语音命令注册管理》等四个标准项目，其中第 2 和 3 部分已经发布；手势交互方面正在进行 ISO/IEC 30113-1《信息技术 用户界面 跨设备基于手势的界面和方法第 1 部分：框架》等 3 个项目；情感交互正在进行 ISO/IEC 30150《信息技术 情感计算 用户界面框架》1 个项目。

在生物特征识别领域，ISO/IEC JTC 1/SC 37（生物特征识别分技术委员会）已发布了共计 121 项标准，包括数据交换格式、应用程序接口、样本质量、性能

测试等方面。代表性的标准有 ISO/IEC 19794-2:2005《信息技术 生物特征识别 数据交换格式 第2部分：指纹细节点数据》、ISO/IEC 19784-1:2006《信息技术 生物特征识别 应用程序接口 第1部分：BioAPI 规范》、ISO/IEC 29794-6:2015《信息技术 生物特征样本质量 第6部分：虹膜样本质量数据》、ISO/IEC 19795-1:2006《信息技术 生物特征识别 性能测试和报告 第1部分：原则与框架》等，涵盖了指纹、人脸、虹膜、静脉、数字签名、声纹等模态，形成了较为完备的标准体系。

在计算机图像处理领域，ISO/IEC JTC 1/SC 24（计算机图形、图像处理和环境数据表示分技术委员会）和 ISO/IEC JTC 1/SC 29（音频、图像编码、多媒体及超媒体信息分技术委员会）负责开展标准化工作。ISO/IEC JTC 1/SC 24 正在研制 ISO/IEC 8632-1《信息技术 计算机图形 存储和传送图形描述信息的元文卷 第1部分：功能规范》、ISO/IEC 8632-3《信息技术 计算机图形 存储和传送图形描述信息的元文卷 第3部分：二进制编码》、ISO/IEC 18039《信息技术 混合和增强现实参考模型》等标准。ISO/IEC JTC 1/SC 29 正在研制及发布的标准有 ISO/IEC 15938-13《信息技术 多媒体内容描述接口 第13部分：图像搜索用简洁描述符》、ISO/IEC 24800-3《信息技术 JP 搜索 第3部分：查询格式》等。

在云计算领域，ISO/IEC JTC 1/SC 38（云计算和分布式平台分技术委员会）主要研制了云计算通用基础标准、互操作标准、可移植标准、云服务、应用场景、案例分析、云安全等规范。其中对人工智能技术起到支撑平台作用的国际标准有 ISO/IEC 19941《信息技术 云计算 互操作和可移植》、ISO/IEC 19944《信息技术 云计算 数据和跨设备与云服务的数据流》等。

在大数据领域，ISO/IEC JTC 1/WG 9（大数据标准工作组）主要开展大数据领域通用性标准研制，正在研制及发布的标准有：ISO/IEC 20546《信息技术 大数据 概述与术语》、ISO/IEC 20547-3《信息技术 大数据 参考架构 第1部分：框架与应用》、ISO/IEC 20547-3《信息技术 大数据 参考架构 第2部分：用例和需求》、ISO/IEC 20547-3《信息技术 大数据 参考架构 第3部分：参考架构》、ISO/IEC 20547-4《信息技术 大数据 参考架构 第4部分：安全与隐私》、ISO/IEC 20547-5《信息技术 大数据 参考架构 第5部分：标准路线

图》。

在传感网领域，ISO/IEC JTC 1/SC 41 开展了物联网架构、物联网互操作、物联网应用、可信物联网、工业物联网、边缘计算、实时物联网等方面研究，正在开展 ISO/IEC 29182-2:2013《信息技术 传感器网络：参考体系结构（SNRA） 第 2 部分：术语和词汇》、ISO/IEC 20005:2013《信息技术 传感器网络 智能传感器网络协同信息处理支撑服务和接口》等国际标准研制工作。

在安全方面，ISO/IEC JTC 1/SC 27 开展了个人隐私保护、大数据安全、物联网安全、云计算安全等标准研究，包括 ISO/IEC 29100《信息技术 安全技术 隐私框架》、ISO/IEC 29101《信息技术 安全技术 隐私参考体系结构》、ISO/IEC 29190《信息技术 安全技术 隐私能力评估模型》、ISO/IEC 29134《信息技术 安全技术 隐私影响评估方法学》等标准。

ISO/IEC JTC 1 研究范围涵盖的人工智能技术领域有很多，许多分技术委员会（SC）和工作组（WG）工作受到人工智能的影响。从 2017 年 7 月 29 日到 8 月 31 日，JTC 1 通过在线调查，了解其部分 SC/WG 开展的工作与人工智能标准化相关联的程度，具体情况如表 2 所示：

表 2 与人工智能标准化相关联的各 SC 及其关联程度

JTC 1	SC	SC	SC	SC	SC	SC	SC	SC	SC	SC	SC	SC	WG
议题	7	17	22	24	27	28	29	36	37	40	41	9	
可互操作性				◆		◆	◆			◆	◆	◆	
社会安全		◆			◆			◆	◆	◆		◆	
可用性				◆		◆		◆		◆	◆	◆	
隐私		◆			◆			◆		◆		◆	
范围及领域				◆				◆		◆	◆	◆	
系统性能							◆	◆	◆	◆		◆	
软件工程	◆							◆	◆	◆		◆	
度量指标								◆	◆	◆		◆	
生产安全								◆		◆		◆	
可追溯性								◆		◆		◆	
其它			◆					◆		◆			
风险分析								◆		◆			
伦理道德								◆		◆			

对此，ISO/IEC JTC 1 认为，需要成立一个新的标准组织开展人工智能标准化工作。2017 年 10 月，在 ISO/IEC JTC 1 第 32 届全会上批准成立了 JTC 1/SC 42

人工智能分技术委员会，将围绕基础标准（Foundational standards）、计算方法（Computational methods）、可信赖性（Trustworthiness）和社会关注（Societal concerns）等方面开展国际化工作。“人工智能概念与术语”（NP 22989）和“运用机器学习的人工智能系统框架”（NP 23053）两项新工作项目提案也已通过国际标准投票，后续将在 SC 42 开展。SC 42 第一次全会将于 2018 年 4 月 18 日至 20 日在中国北京召开，会上将进一步讨论明确工作范围及重点研制的标准项目。

4.1.2 ISO

国际标准化组织（International Organization for Standardization, ISO）主要在工业机器人、智能金融、智能驾驶方面开展了人工智能标准化研究。

在工业机器人方面，ISO/TC 299（机器人技术委员会）开展了 ISO 11593:1996《工业机器人 末端执行器自动更换系统 词汇和特征表示》、ISO 9946:1999《工业机器人 特性表示》、ISO 14539:2000《工业机器人 抓握型夹持器物体搬运 词汇和特性表示》、ISO 9787:1999《工业机器人 坐标系和运动命名原则》、ISO 8373:2012《机器人与机器人装备 词汇》等标准的研制。

在智能金融方面，ISO/TC 68（金融服务技术委员会）从事金融标准化工作，主要负责银行、证券及金融业务相关标准的制定，共出台发布智能金融相关标准 58 项，其中与人工智能相关的有 ISO 19092:2008《金融服务 生物特征识别 安全框架》、ISO 14742:2010《金融服务 密码算法及其使用建议》和 ISO 19038:2005《银行业务和相关金融服务 TDEA 运算模式 实施指南》等。

在智能驾驶方面，ISO/TC 22（道路车辆技术委员会）负责制定道路车辆相关基础标准，正在开展智能网联汽车相关标准化研究。

4.1.3 IEC

国际电工委员会（International Electrotechnical Commission, IEC）主要在可穿戴设备领域开展了人工智能标准化工作。

IEC TC100（音频、视频、多媒体系统和设备分技术委员会）针对可穿戴设备领域开展了标准化工作，建立了由 SS8 研究小组负责的“可穿戴设备使用场

景”议题，研制可穿戴设备包括虚拟现实的标准化工作。IEC TC 124（可穿戴技术分技术委员会）负责开展与可穿戴相关的电工、材料、人身安全相关的技术标准研制工作。

IEC 市场战略委员会（MSB）于 2017 年 8 月启动了“人工智能跨垂直行业的应用”白皮书编写工作，计划于 2018 年年中发布。

4.1.4 ITU

国际电信联盟（International Telecommunications Union, ITU）从 2016 年开始开展人工智能标准化研究。2017 年 6 月，ITU 和 XPRIZE 基金会共同举办了“人工智能优势全球峰会”。ITU-T 提出了对于人工智能建议的草案，包括 ITU-T Y.AI4SC 人工智能和物联网以及 ITU-T Y.qos-ml 基于机器学习的 IMT-2020 的服务质量要求。

4.2 国外标准化现状

4.2.1 IEEE

电气和电子工程师协会（Institute of Electrical and Electronics Engineers, IEEE）主要聚焦人工智能领域伦理道德标准的研究。2017 年 3 月，IEEE 在《IEEE 机器人与自动化》杂志发表了名为“旨在推进人工智能和自治系统的伦理设计的 IEEE 全球倡议书”，倡议建立人工智能伦理的设计原则和标准，帮助人们避免对人工智能技术产生恐惧和盲目崇拜，从而推动人工智能技术的创新。IEEE 批准了 7 个 IEEE 标准项目，包括 IEEE P7000《系统设计期间解决伦理问题的模型过程》；IEEE P7001《自主系统的透明度》；IEEE P7002《数据隐私处理》；IEEE P7003《算法偏差注意事项》；IEEE P7004《儿童和学生数据治理标准》；IEEE P7005《雇主数据治理标准》；IEEE P7006《个人数据 AI 代理标准》。

4.2.2 NIST

美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）在人工智能数据采集分析工具、未来专家系统、基于人工智能的集体生产质量控制、高通量材料发现和优化应用的机器学习方面有一定的研究基础，但

目前为止，还没有在研或发布相关的标准。

4.2.3 其它

此外，欧洲电信标准化协会(European Telecommunications Standards Institute, ETSI)在人工智能标准化方面重点关注认知技术，并将人工智能纳入 ETSI 技术路线图。国外知名企业 Alphabet、亚马逊、Facebook、IBM 和微软的相关研究人员正在开展人工智能道德标准研究。

4.3 国内标准化现状

4.3.1 全国信息技术标准化技术委员会

全国信息技术标准化技术委员会(SAC/TC 28)对口 ISO/IEC JTC 1 工作，人工智能方面主要在术语词汇、人机交互、生物特征识别、大数据、云计算等领域开展了标准化工作。

在术语词汇领域，目前发布了《信息技术 词汇 第 28 部分：人工智能基本概念与专家系统》《信息技术 词汇 第 29 部分：人工智能语音识别与合成》《信息技术 词汇 第 31 部分：人工智能机器学习》《信息技术 词汇 第 34 部分：人工智能神经网络》四项基础国家标准。

在人机交互领域，全国信标委用户界面分技术委员会成立了语音交互、体感交互、脑机交互等工作组，开展智能语音、体感交互等标准研制。目前发布了《中文语音识别系统通用技术规范》《中文语音合成系统通用技术规范》《自动声纹识别(说话人识别)技术规范》《中文语音识别互联网服务接口规范》《中文语音合成互联网服务接口规范》五项语音交互标准，正在开展《信息技术 中文语音识别终端服务接口规范》《信息技术 智能语音交互系统》等系列标准、《智能客服语义库技术要求》等国家标准的研制。同时，积极将国内研究成果贡献国际，于 2017 年向 ISO/IEC JTC 1/SC 35 提交了《信息技术 情感计算用户界面框架》国际提案并取得立项。

在生物特征识别领域，全国信标委生物特征识别分技术委员会开展了《指纹识别设备通用技术要求》《人脸识别设备通用技术要求》《信息技术 生物特征样

本质量 第 4 部分：指纹图像数据》《信息技术 生物特征样本质量 第 5 部分：人脸图像数据》等指纹、人脸、虹膜等标准研制。

在计算机图形图像处理及环境数据领域，全国信标委计算机图形图像处理及环境数据分技术委员会开展了《信息技术 增强现实 第 1 部分：术语》等图形图像基础标准研制。

另外，全国信标委大数据标准工作组、云计算标准工作组、物联网标准工作组、国家传感器网络标准工作组也在开展相关领域基础标准的研制，为人工智能相关技术及应用提供支撑。

4.3.2 全国自动化系统与集成标准化技术委员会

全国自动化系统与集成标准化技术委员会（SAC/TC 159）下设 SC 2 机器人装备分技术委员会工作范围主要涉及工业机器人整机、系统接口、零部件、控制器等领域，制定了《工业机器人 末端执行器自动更换系统 词汇和特征表示》《工业机器人 特性表示》《工业机器人 抓握型夹持器物体搬运 词汇和特性表示》《工业机器人 坐标系和运动命名原则》《机器人与机器人装备 词汇》等标准。

4.3.3 全国音频、视频和多媒体标准化技术委员会

全国音频、视频和多媒体标准化技术委员会（SAC/TC 242）主要围绕音视频、智慧家庭医疗健康产品开展相关标准化研究。目前正在开展《虚拟现实 音频主观评价方法》《智慧家庭 健康管理腕式可穿戴设备技术要求》《智慧家庭健康养老产品分类及描述》《智慧家庭 健康养老服务平台参考模型》《智慧家庭老人手环（手表）技术规范》等标准研制。

4.3.4 全国信息安全标准化技术委员会

全国信息安全标准化技术委员会（SAC/TC 260）在生物特征识别、智慧城市、智能制造等领域开展了相关安全标准化研究工作。在生物特征识别领域，开展了《信息安全技术 基于可信环境的生物特征识别身份鉴别协议》《信息安全技术 指纹识别系统技术要求》《信息安全技术 网络人脸识别认证系统安全技术要求》《信息安全技术 虹膜识别系统技术要求》等标准研制；在自动驾驶领

域，开展了《信息安全技术 汽车电子系统网络安全指南》标准研制；在智能制造领域，开展了《信息安全技术 工业控制网络安全监测安全技术要求及测试评价方法》《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》《信息安全技术 工业控制系统产品信息安全通用评估准则》等标准研制。

4.3.5 全国智能运输系统标准化技术委员会

全国智能运输系统标准化技术委员会（SAC/TC 268）主要在智能交通领域开展了标准化工作，制定了《合作式智能运输系统专用短程通信 第1部分：总体技术要求》《合作式智能运输系统专用短程通信 第2部分：媒体访问控制层和物理层规范》《智能交通数据安全服务》《智能交通数字证书应用接口规范》《车路协同专用短程通信 第3部分：网络层和应用层》《车路协同专用短程通信 第4部分：设备应用》等标准。

4.4 人工智能标准化面临的问题和挑战

目前，人工智能标准化工作虽然具备一定的基础，但仍面临一系列现实问题，困难和挑战如下：

（1）人工智能技术、产品还在快速发展中，业界对人工智能的概念、内涵、应用模式、智能化水平等尚难达成共识，现有标准化工作基础较为薄弱；

（2）人工智能标准涉及共性技术领域较多，涉及不同的标准化技术委员会，其在人工智能领域的标准化工作边界有待进一步明晰，需要加强人工智能标准化顶层设计，避免标准化工作交叉重复；

（3）人工智能作为国内外关注的前沿技术，行业巨头正在加快谋篇布局，我国在人工智能领域创新能力有待进一步提升，机器学习、自然语言处理等标准化工作需要国内技术研发机构和产业的有力支撑；

（4）人工智能各类技术在不同领域的融合应用，涉及部门、领域、厂商众多，工作协调难度大；

（5）相关伦理道德、安全标准往往滞后于技术的发展，将会引发更多分歧和争议，对标准制定工作带来新的挑战。

4.5 人工智能标准需求分析

通过以上内容，分析国内外人工智能的发展现状，可以初步得到以下标准化需求分析：

(1) 界定人工智能需要研究的范围。人工智能从实验室研究转向各应用领域的实用系统，呈现快节奏增长的态势，这需要通过统一的术语进行界定，明确人工智能的内涵、外延和需求的核心理念，引导产业界正确认识和理解人工智能技术，便于大众广泛使用人工智能技术；

(2) 描述人工智能系统的框架。用户和开发者在面对人工智能系统的功能和实现时，普遍将人工智能系统看作是一个“黑盒子”，但有必要通过技术框架规范来增强人工智能系统的透明度。由于人工智能系统应用范围广泛，可能很难给出通用的人工智能框架，更现实的方式是在特定的范围和问题中给出特定的框架。例如，目前以机器学习为基础的人工智能系统是主流技术，并依赖于包括云计算和大数据在内的技术资源，可以以此为基础构建一个基于机器学习的人工智能系统框架，并对其中组件的功能进行界定；

(3) 评价人工智能系统的智能等级。按智能程度对人工智能系统进行划分一直存在争议，给出一个标杆来衡量它的智能等级是困难且具有挑战的工作。随着不同的应用场合对智能等级评价需求的进一步明确，需要标准化工作来逐步解决该问题；

(4) 促进人工智能系统的互操作性。人工智能系统及其组件有一定的复杂性，不同的应用场景涉及到的系统及组件不同。系统与系统之间，组件与组件之间的信息交互与共享，需要通过互操作性来保证。人工智能互操作性也涉及到不同的智能模块产品之间的互用性，达到数据互通，也就是不同的智能产品需要有标准化的接口。标准化工作保证人工智能系统的应用程序接口、服务及数据格式，通过标准和兼容接口，定义可互换的组件、数据和事务模型；

(5) 进行人工智能产品的评估。人工智能系统作为工业产品，需要在功能、性能、安全性、兼容性、互操作性等多方面进行评估，才能确保产品的质量和可用性，并为产业的可持续发展提供保障。评估工作一般包括测试、评价等一系列活动，评估对象可以是自动驾驶系统、服务机器人等产品，按照规范化的程序和

手段，通过可测量的指标和可量化的评价系统得到科学的评估结果，同时配合培训、宣贯等手段推进标准的实施；

(6) 对关键技术进行标准化。对已经形成模式，并广泛应用的关键技术，应及时进行标准化，防止版本碎片化和独立性，确保互操作性和连续性。例如，深度学习框架绑定的用户数据，应当通过明确神经网络的数据表示方法和压缩算法，确保数据交换，且不被平台绑定，保障用户对数据拥有的权益，其它如人机交互技术、传感器接口、基本算法等基础标准也需要尽快制定；

(7) 确保安全及伦理道德。人工智能从各种设备、应用和网络中收集了大量的个人、生物或者其它特征数据，这些数据并不一定从系统设计之初就能够很好地组织管理并采取恰当的隐私保护措施。对人类的安全和生命安全有直接的影响的人工智能系统，可能会对人类构成威胁，需要在这类人工智能系统得到广泛应用之前，就通过标准化等手段对系统进行规范和评估，保障安全性；

(8) 针对行业应用特点的标准化。除了共性技术外，在特定行业中实施人工智能还存在个性化的需求与技术特色，典型的如家居应用、医疗应用、交通应用等，需考虑特定设备的功能性能特征、系统组成结构和相互关系等。

4.6 人工智能标准化组织机制建设

目前我国在人工智能关键技术领域虽然已具备一定的标准化基础，已制定多项产品和技术规范，但还缺乏从人工智能的角度进行顶层设计，在基础、支撑技术、产品和行业应用间存在多技术委员会归口，各技术委员会的研究工作仅限于自身领域范围，标准化工作尚未形成统筹推进的机制，不利于技术创新与产业化应用的协同推进。因此，急需建立人工智能领域标准化统筹协调机制。

2018年1月，国家标准化管理委员会批准成立国家人工智能标准化总体组、专家咨询组。总体组在人工智能标准化中承担统筹协调、规划布局的角色，负责开展人工智能国际国内标准化工作，拟定我国人工智能标准化规划、体系和政策措施；协调人工智能相关国家标准的技术内容和归口，统筹相关标准化组织、企业及研究机构，建立人工智能基础共性标准与行业应用标准的传导机制；以关键技术为核心，以行业应用为导向，构建兼容性好、开放性强的标准体系；开展人工智能国家标准试点示范、应用实施、宣贯培训等工作，组织参与人工智能国

际标准化工作并开展国际标准化交流合作。总体组秘书处设在中国电子技术标准化研究院。总体组可根据标准化工作的需要下设专题组，负责某一方面的专项工作。

专家咨询组由国内人工智能领域知名专家学者组成，负责为总体组提供我国人工智能标准化规划、体系和政策措施等方面的咨询，对人工智能领域国际国内标准研制、试点、应用实施、标准传导机制建立等提出意见建议，对国家人工智能标准化总体组的工作进行指导。

5 人工智能标准体系

人工智能涉及跨领域的多技术融合，人工智能标准之间存在着相互依存、相互制约的内在联系。因此，人工智能标准化工作需要统筹协调，以系统科学的理论和方法为基础，运用标准化的工作原理，不断优化标准之间的关系，避免标准间不配套、不协调及组成不合理等问题。

5.1 人工智能标准体系结构

人工智能标准体系结构包括“**A 基础**”、“**B 平台/支撑**”、“**C 关键技术**”、“**D 产品及服务**”、“**E 应用**”、“**F 安全/伦理**”等六个部分，主要反映标准体系各部分的组成关系。人工智能标准体系结构，如图 4 所示。



图 4 人工智能标准体系结构图

具体而言，A 基础标准包括术语、参考架构、数据和测试评估四大类，位于人工智能标准体系结构的最底层，支撑标准体系结构中的其它部分；B 平台/支撑标准是对人工智能硬件、软件、网络和数据的综合集成，在人工智能标准体系

结构中起承上启下的作用；C 关键技术标准主要针对自然语言处理、人机交互、计算机视觉、生物特征识别和 VR/AR 等领域，为人工智能实际应用提供支撑；D 产品及服务标准包括在人工智能技术领域中形成的智能化产品及新服务模式的相关标准；E 应用标准位于人工智能标准体系结构的最顶层，面向行业具体需求，对其它部分标准进行细化和落地，支撑各行业推进人工智能发展；F 安全/伦理标准位于人工智能标准体系结构的最右侧，贯穿于其它部分，提供安全标准，支撑人工智能发展。

5.2 标准体系框架

结合人工智能国内外技术、产业以及标准化现状，形成人工智能标准体系框架，由基础、平台/支撑、关键技术、产品及服务、应用和安全/伦理六个部分组成，如图 5 所示。

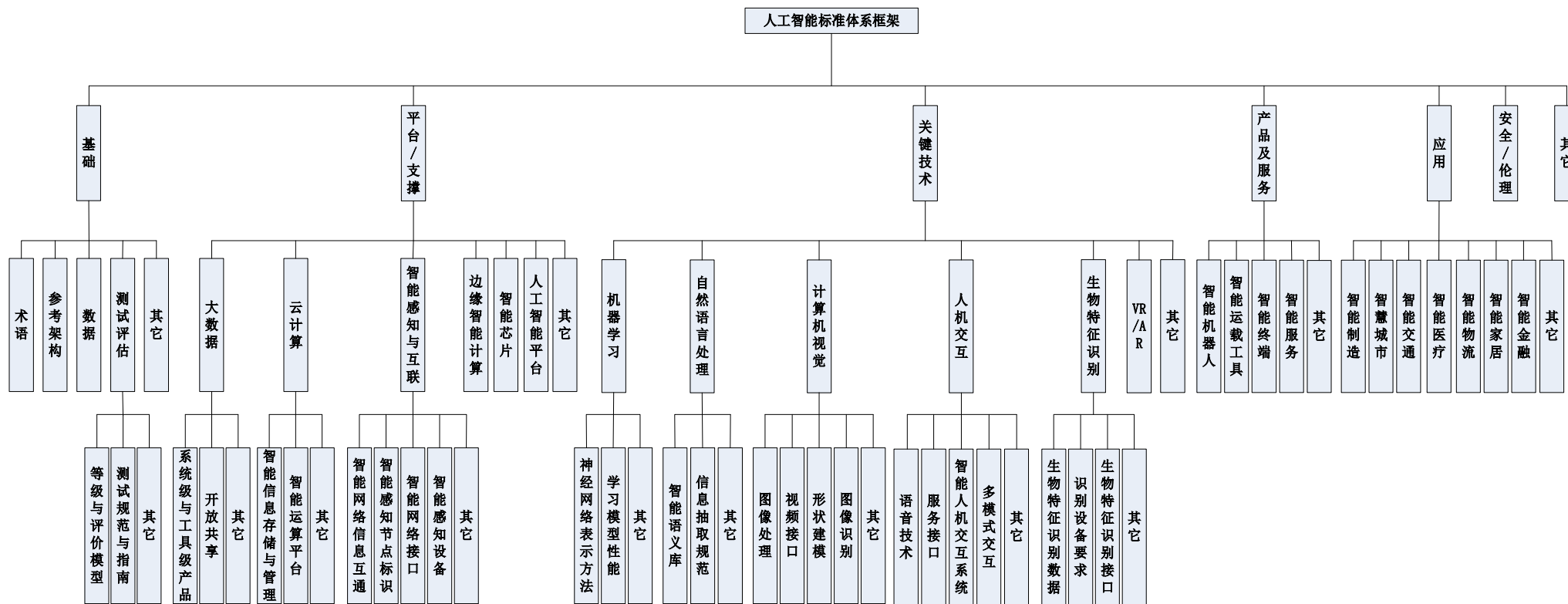


图5 人工智能标准体系框架

5.2.1 基础标准

该类标准主要针对人工智能基础进行规范，包括术语定义、参考架构、数据、测试评估等。

针对已有人工智能术语相关标准，围绕人工智能发展现状开展标准制修订工作；深入研究人工智能相关技术及产业链，开展人工智能参考架构等标准研制工作；结合人工智能领域发展需求，开展用于数据训练的数据格式、标签、数据模型、质量要求等数据资源相关标准的研制；针对人工智能技术、行业发展较为成熟的领域，提取测试评估的共性需求，开展人工智能通用性测试指南、评估原则以及智能等级分级要求等标准研制。

5.2.2 平台/支撑标准

该类标准主要针对人工智能底层平台和支撑进行规范，包括大数据、云计算、智能感知及互联、边缘智能计算、智能芯片及人工智能平台等。

用于支撑人工智能的大数据、云计算、智能感知及互联等标准化工作已具备一定的基础。大数据方面，重点研制系统级和工具级产品、数据开放共享等标准；云计算方面，重点研制面向人工智能的异构计算等虚拟和物理资源池化、调度和管理标准；智能感知与互联方面，重点开展高精度传感器、新型 MEMS 传感器相关标准制定，为人工智能的硬件发展提供标准支撑；边缘智能计算方面，重点研制参考架构、轻量级运行环境要求等标准；智能芯片方面，开展芯片性能测试要求等标准研制；人工智能平台方面，重点研制人工智能计算框架、人工智能算法任务调度等通用功能要求，以及支持机器学习、知识图谱等不同计算模式的通用计算能力要求等相关标准。

5.2.3 关键技术标准

该类标准主要针对人工智能相关技术进行规范，包括机器学习、自然语言处理、计算机视觉、人机交互、生物特征识别以及 VR/AR 等关键技术。

在机器学习方面，开源在人工智能中有重要的影响，开源软件和开源社区往往由于其实验性、灵活性而领先一步，需要开展开源与标准化协调发展研究。同

时，神经网络表示方法与模型压缩、机器学习算法性能评估等标准也是后续标准化工作的重点方向。

在自然语言处理方面，国内外自然语言处理技术及产业发展处于起步阶段，下一步可以开展以下标准化工作：语义库方面，包括语义库的结构、数据规范、接口规范等；信息提取规范方面，包括词性标注及其描述规范等；文本内容分析方面，包括内容相关度分析的准则和描述、使用方法，以及文本内容正确与否的判断准则及其相关性能评估规范等。

在计算机视觉方面，国内已开展计算机视觉术语标准的研究。由于不同应用场景对采集设备有着不同的要求，采集设备对于计算机视觉算法的开发有着很大的影响，需要规范数据采集设备的类型及对应参数要求；视觉采集数据与计算机视觉算法输出的结果（元数据）都是多种多样，如数据的格式、计算机视觉数据库（例如采用单一还是多种数据形式）、多类数据形式等，定义数据的格式、构建计算机视觉数据库（例如采用单一还是多种数据形式）、关联多类数据形式等都是亟待规范的问题；不同应用场景对于计算机视觉提出了不同的要求，如量化和规范不同行业对于计算机视觉的衡量方法也有着很大的标准化需求。

在人机交互方面，国内外已具备一定的标准化成果，主要集中在语音交互和手势交互方向。后续继续开展语音合成、识别等技术和接口相关测试标准研制，搭建智能语音交互系统标准符合性评估平台；研制手势识别等技术规范和服务接口规范等；进一步丰富智能人机交互的系统规范，如智能教育领域的基于多模式交互系统标准规范等。

在生物特征识别方面，标准化工作主要围绕图像数据、应用接口、系统应用以及性能测试四个方向进行。目前国内已完成对诸如指纹、人脸、虹膜等典型模态的识别设备通用规范、数据交换格式、样本质量等标准的研制，同时还建立了指纹检测平台，可依据已制定的符合性测试方法相关标准完成对指纹识别产品的标准符合性测试。随着 DNA、步态等新兴模态识别技术的发展以及互联网金融等应用场景的增多，亟需制定 DNA 数据质量、呈现攻击检测、安全评估及安全防范等标准，支撑生物特征识别产业发展。

在 VR/AR 方面，国内 VR/AR 领域目前已经开展了场景建模信息表示、增强

现实术语、头戴式显示设备通用规范以及舒适度和安全测试方面的标准，但是VR/AR的一些技术要求已超出了目前已有的一些配套行业的技术要求，针对目前我国虚拟现实内容制作、设备制造、领域应用存在的问题，需要开展框架、编解码标准、感知与交互、设备、应用、安全与健康、舒适等标准，形成分层次、结构化的统一标准体系。

5.2.4 产品及服务标准

产品及服务标准包括智能机器人、智能运载工具、智能终端以及智能服务等人工智能现有的产品和服务标准。

在智能机器人方面，结合《国家机器人标准体系建设指南》工作部署，围绕服务机器人，重点攻克核心零部件、专用传感器技术标准，完善服务机器人硬件接口、安全使用以及多模态交互模式、功能集、服务机器人应用操作系统框架、服务机器人云平台通用要求等标准；围绕工业机器人，重点在工业机器人路径动态规划、协作型机器人设计规范、工业检测图像识别标定等开展标准化工作。

在智能运载工具方面，重点在智能网联汽车方面开展标准化工作。目前面临的主要问题是汽车智能化涉及的高性能协同传感技术、车载互联及通信技术、汽车智能化与网联化安全技术等。结合《国家车联网产业标准体系建设指南（智能网联汽车）》工作部署，重点开展先进驾驶辅助系统（ADAS）术语定义、汽车驾驶自动化分级、车载信息交互系统信息安全技术要求等标准制定工作。

在智能终端方面，建立智能终端的标准化和测试验证平台是提高智能终端产业规范发展的有效途径，为满足产业发展需要，亟需建立设备互联接口、内容服务接口、应用程序开发接口、系统安全技术、测试及评价等方面的标准，推动设备间的数据格式和标准协议的开放共享，推进产品和系统间的互联互通。

在智能服务方面，既包括图像识别、智能语音、自然语言处理、机器学习算法等人工智能模块通过 SaaS 服务方式向行业提供综合性解决方案，也包括利用人工智能技术改变传统 IT 服务。与之相应的标准化需求正在兴起，如不同商家的同一种服务在功能集、服务接口、通信交互协议、服务获取方式等方面存在较大差别，需求方选择服务时花费成本较高，急需标准化的规范和统一。下一步重

点加强人工智能服务能力成熟度评价、智能服务参考架构等标准制定工作。

5.2.5 应用标准

应用标准包括智能制造、智慧城市、智能交通、智能医疗、智能物流、智能家居、智能金融等领域。

在智能制造领域，我国智能制造标准化工作的快速推进为人工智能在智能制造中的应用探索提供了良好的基础。下一步，围绕《智能制造标准体系建设指南》要求部署，结合人工智能技术在智能制造中的应用，重点开展个性化定制、SCADA 数据分析、智能在线监测、预测性维护、高级排产和工艺优化、智能机器人、基于 VR/AR 的维修保养等标准研究。

在智能家居领域，结合《智慧家庭综合标准化体系建设指南》文件要求，建议根据产业发展现状和技术发展，联合智能家居产业链上下游企业广泛参与共同构建并完善智能家居标准体系，重点制定智能家居主要应用领域关键技术、产品和服务标准，适时启动并参与若干重点标准的国际标准化进程。

在智能金融领域，智能金融未来将通过人工智能技术对信息进行预判、决策、行动，使得金融投资、分析变得更加精准，有利于打造标准化、模型化、智能化的风险控制系统，从而推动金融的发展。因此，结合金融领域应用，使用深度学习技术，基于机器学习技术构建金融知识图谱，从金融数据中自动发现模式，建议在人工智能金融数据标准化、金融征信标准化工作、金融风控标准化等开展研究工作。

在智慧城市领域，新型智慧城市已有标准化工作集中在基础通用类标准，具体应用领域相关标准仍需完善，下一步将结合人工智能在城市基础设施智能化、设施管理和运营、城市运行和管理等层面的应用情况，加强支撑人工智能技术与城市规划、建设、运行、服务、管理等方面深度融合的技术标准研究，开展人工智能应用成效动态评估指标工作。

在智能交通领域，国内已具备一定的标准化基础，下一步信息数据平台及综合管理系统是人工智能交通标准化工作的方向，重点开展智能交通数据信息平台、车辆与路网通信、电子车牌识别等标准，形成多维的智能交通监控、管理的一体

化服务系统。

在智能医疗领域，国内已具备一定的标准化基础，但是还存在数据质量、数据和模型的隐私性、数据模型建立困难等问题，下一步重点开展生理监测、医疗监管智能化、医疗信息交换、数据平台接口、医疗数据质量评价等标准制定工作。

在智能物流领域，我国在智能物流技术及产业方面发展迅速，国内已具备一定的标准化基础，下一步相将重点针对智能物流中的物流智能规划规范、智能识别通用要求、智能仓储调度规范、结合供应链的物流配置要求等方面开展标准化工作。

在智能农业领域，智慧农业产业日趋成熟，虽然已经制定了一些传感网相关标准，但是由于农业应用环境复杂、应用场景多样，还亟需制定智能传感器、窄带物联网、病虫害预测数据模型、数据平台接口等相关标准。

在智能健康养老领域，从智能健康养老的发展规划来看，智能健康养老标准体系优先制定适用于个人、家庭和社区的血压、血糖、血氧、心律和心电五大类常用生理健康指标智能检测设备产品及数据服务标准，完善智能健康养老服务流程规范和评价指标体系，推动智能健康养老服务的规范化和标准化。

在智能政务领域，电子政务技术及产业发展不断创新，新兴技术不断涌现，根据我国《“十三五”国家信息化规划》建设要求，下一步将重点针对数据共享、业务协同、政务信息资源开放等方面开展标准化工作。

在智能环保领域，针对传统环保领域的标准已比较全面，然而，与人工智能相关的环保标准尚未发布，下一步重点开展人工智能与环保领域相结合的标准研究及制定，主要聚焦在环境监测技术；资源能源消耗、环境污染物排放的智能预测数据模型；环境智能监控大数据分析平台；信息共享的智能环境监测网络等。

在智慧法庭领域，智慧法庭的建设和应用需要依托于智能大数据分析、语音识别、图像视频分析等多项人工智能技术的支撑，从而实现案情要素的分析、庭审语音识别自动转写、庭审行为视频分析、庭审视频流媒体转发与调度等功能。因此，为实现法院审判体系和审判能力智能化，需要研制庭审数据格式统一规范、庭审数据深度分析等规范，利用深度学习算法对多元化数据进行挖掘分析，进而

提升庭审效率。

5.2.6 安全/伦理标准

安全/伦理标准包括与人工智能安全、伦理、隐私保护等相关的标准规范。

人工智能安全/伦理标准，从广义来说涉及人工智能本身、平台、技术、产品和应用相关的安全标准，以及伦理、隐私保护规范。目前，人工智能安全与伦理标准主要集中在生物特征识别、自动驾驶等部分领域的应用安全标准，以及大数据安全、隐私保护等支撑类安全标准，而与人工智能自身安全或基础共性相关的标准还比较少。

人工智能安全与伦理标准研究，一方面要加强人工智能基础标准研究，重点开展人工智能安全的参考架构、安全风险、伦理设计、安全评估等标准研究，提出人工智能算法、产品和系统的安全要求和测评方法。另一方面要继续深化应用领域标准化工作，针对已有标准完善智能安全要求，并继续开展网络安全领域的人工智能应用安全、智能机器人安全、自动驾驶安全、智能安防、智能交通安全、智能物流安全、智慧城市安全等领域的标准研究。

例如，在智慧城市领域，可重点开展公共安防、安全管理体系、数据安全、安全监测预警等标准研制工作；在智能物流领域，可重点针对深度感知智能仓储系统、智能物流公共信息平台 and 指挥系统、产品质量认证及追溯系统、智能配货调度体系的数据安全管理及评测等开展标准化研究；在智能金融领域，可重点针对金融行业的智能客服、智能监控等技术和装备，金融风险智能预警与防控系统的数据安全管控，后台数据滥用等开展标准制定工作。

5.3 近期急需制定标准

根据人工智能标准体系与人工智能标准化需求分析，形成人工智能近期急需研制的标准明细表，如表3所示：

表3 人工智能近期急需研制的标准明细表

序号	一级分类	二级分类	标准名称	采用标准号及采用程度	状态
1.	基础	术语	信息技术 人工智能 术语	——	拟研制

序号	一级分类	二级分类	标准名称	采用标准号及采用程度	状态	
2.		参考架构	信息技术 人工智能 参考架构	---	拟研制	
3.		测试评估	信息技术 人工智能 等级要求及评估指南	---	拟研制	
4.	平台/ 支撑	人工智能平台	信息技术 人工智能 平台任务调度及资源管理能力要求	---	拟研制	
5.			信息技术 人工智能 基本服务接口规范	---	拟研制	
6.			信息技术 人工智能 平台计算框架能力要求	---	拟研制	
7.			信息技术 人工智能 平台通用要求	---	拟研制	
8.		边缘智能计算	边缘智能计算参考架构	---	拟研制	
9.		智能芯片	智能芯片性能评估指南	---	拟研制	
10.		关键技术	机器学习	信息技术 神经网络表示与模型压缩	---	拟研制
11.	信息技术 学习模型性能评估规范			---	拟研制	
12.	计算机视觉		信息技术 计算机视觉 术语	---	拟研制	
13.			智能监控 结构化视频 数据交换格式	---	拟研制	
14.			智慧传媒 智能分析元数据规范	---	拟研制	
15.			视频图像身份识别系统技术要求	---	拟研制	
16.	人机交互			信息技术 智能语音交互系统 第1部分：通用规范	---	拟研制
17.				信息技术 智能语音交互评测 第1部分：语音处理	---	拟研制
18.				信息技术 智能语音交互评测 第2部分：识别	---	拟研制
19.				信息技术 智能语音交互评测 第3部分：语义理解	---	拟研制
20.				信息技术 智能语音交互评测 第4部分：合成	---	拟研制
21.				信息技术 智能语音交互评测 第5部分：语音评测	---	拟研制
22.				信息技术 语音交互应用 第1部分：通用系统规范	---	拟研制
23.		信息技术 智能音箱评估指南		---	拟研制	

序号	一级分类	二级分类	标准名称	采用标准号及采用程度	状态
24.		VR/AR	信息技术 虚拟现实头戴式显示设备舒适度测试方法	---	拟研制
25.			信息技术 虚拟现实头戴式显示设备安全测试方法	---	拟研制
26.			增强现实人脸结构定位与特效数据格式规范	---	拟研制
27.	产品	机器人	智能客服机器人通用技术规范	---	拟研制
28.	应用/服务	智能家居	信息技术 智能家居通信交互协议规范	---	拟研制
29.				信息技术 智能家居人机交互界面要求	---
30.			智能医疗	医学影像辅助诊断系统技术要求	---
31.		安全	信息技术 人工智能 安全态势感知技术要求	---	拟研制

6 人工智能标准化工作重点建议

人工智能标准化建设是我国人工智能产业发展的关键因素之一，是保证我国人工智能产业在全球竞争中抢占先机、获得优势的重要手段。结合人工智能产业发展现状和需求，对照现有标准化工作情况，提出我国机器人标准化工作近期重点工作如下：

（一）加强人工智能标准化顶层设计

人工智能关键技术及产业应用范围涉及到众多部门和标准化技术组织，建议在国家人工智能国家标准化总体组、专家咨询组的统筹规划下，集聚好业界主流产学研单位资源，营造良好标准化氛围。同时，梳理人工智能产业生态体系脉络，把握产业未来重点发展方向，以“基础统领、应用牵引”为原则，建立完善标准体系。

（二）加强人工智能核心关键技术研究

突破人工智能基础理论及关键核心技术瓶颈，以算法为核心，以数据和硬件为基础，以人工智能安全可控为导向，实施重大关键技术攻关工程，制定人工智能通用技术发展路线图，重点提升感知识别、知识计算、认知推理、运动执行、人机交互能力，形成开放兼容、稳定成熟的技术体系，梳理标准化需求，以技术突破带动核心技术标准突破。

（三）推进人工智能重点标准研制

落实《新一代人工智能发展规划》《促进新一代人工智能产业发展三年行动计划》等政策文件标准化部署和要求，围绕人工智能标准化需求，按照“急用先行、成熟先上”的原则，开展术语、参考框架、算法模型、技术平台等重点急需标准的研制；推动人工智能国际化工作，集聚国内产学研优势资源参与国际标准研制工作，提升国际话语权。

（四）搭建标准符合性测试公共服务平台

加快建设人工智能关键标准的符合性测试平台，开展标准化应用验证，统一测试评估标准，加强测试公共服务平台建设。提高公共服务平台的测试与评价能力。依托标准引导企业尝试开发人工智能在典型行业的解决方案，联合投融资机

构进行孵化。

（五）完善安全、伦理和隐私等相关标准法律政策

人工智能的发展带来各种社会问题，应充分考虑人工智能开发和部署过程中的责任和过错问题，制定完善相关安全法规；依托社会公众对人工智能伦理的广泛共识，设定人工智能技术的伦理要求；从数据的收集和使用开始进行规制，对个人数据管理应该采取延伸式保护，保护公众隐私。在此过程过程中，完善安全、伦理和隐私等相关标准、法律、政策。

附件 1 人工智能标准明细表

根据人工智能标准体系框架，对已发布、在研及拟研制的人工智能相关标准进行整理，形成人工智能标准明细表，如表 4 所示：

表 4 人工智能标准明细表

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
1.	基础	术语	GB/T 5271.28-2001	信息技术 词汇 第 28 部分：人工智能基本概念与专家系统	---	已发布
2.			GB/T 5271.29-2006	信息技术 词汇 第 29 部分：人工智能语音识别与合成	---	已发布
3.			GB/T 5271.31-2006	信息技术 词汇 第 31 部分：人工智能机器学习	---	已发布
4.			GB/T 5271.34-2006	信息技术 词汇 第 34 部分：人工智能神经网络	---	已发布
5.				信息技术 人工智能 术语	---	拟研制
6.		数据	GB/T 31916.5-2015	信息技术 云数据存储和管理 第 5 部分：基于键值（Key-Value）的云数据管理应用接口	---	已发布
7.			20141179-T-469	信息技术 系统与软件工程系统与软件产品质量要求和评价（SQuaRE） 第 12 部分：数据质量模型	---	在研
8.			2010-2210T-SJ	信息技术 服务外包 第 4 部分：非结构化数据管理与服务规范	---	在研
9.		参考架构	20141190-T-469	信息技术 大数据 技术参考模型	---	在研
10.			GB/T 32399-2015	信息技术 云计算 参考架构	---	已发布
11.			---	信息技术 人工智能 参考架构	---	拟研制
12.		测试评估	---	信息技术 人工智能 等级要求及评估指南	---	拟研制
13.	平台 / 支撑	大数据	20160598-T-469	信息技术 大数据存储与处理平台技术要求	---	在研
14.			20171081-T-469	信息技术 大数据 存储与处理系统功能测试规范	---	在研
15.			20160597-T-469	信息技术 大数据分析系统基本功能要求	---	在研
16.			20171065-T-469	信息技术 大数据 分析系统功能测试规范	---	在研
17.			20171067-T-469	信息技术 大数据 开放共享 第 1 部分：总则	---	在研

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
18.			20171068-T-469	信息技术 大数据 开放共享 第2部分：政府数据开放共享基本要求	---	在研
19.			20171069-T-469	信息技术 大数据 开放共享 第3部分：开放程度评价	---	在研
20.			20171066-T-469	信息技术 大数据 面向应用的基础计算平台基本性能要求	---	在研
21.			20171084-T-469	信息技术 大数据 系统通用规范	---	在研
22.		智能感知及网络	GB/T 33905.1-2017	智能传感器 第1部分：总则	---	已发布
23.			GB/T 33905.2-2017	智能传感器 第2部分：物联网应用行规	---	已发布
24.			GB/T 33905.3-2017	智能传感器 第3部分：术语	---	已发布
25.			GB/T 33905.4-2017	智能传感器 第4部分：性能评定方法	---	已发布
26.			GB/T 33905.5-2017	智能传感器 第5部分：检查和例行试验方法	---	已发布
27.			20120545-T-469	传感器网络标识解析和管理规范	---	在研
28.			20141553-T-469	信息技术 传感器网络 第903部分：网关：逻辑功能接口技术规范	---	在研
29.			20171073-T-469	物联网 感知控制设备接入 第1部分：总体要求	---	在研
30.			20150049-T-469	物联网 感知对象信息融合模型	---	在研
31.			云计算	GB/T 31915-2015	信息技术 弹性计算应用接口	---
32.		GB/T 31916.1-2015		信息技术 云数据存储和管理 第1部分：总则	---	已发布
33.		GB/T 31916.2-2015		信息技术 云数据存储和管理 第2部分：基于对象的云存储应用接口	---	已发布
34.		20153697-T-469		信息技术 云数据存储和管理 第3部分：分布式文件存储系统应用接口	---	在研
35.		20153674-T-469		信息技术 云计算 云存储资源管理技术规范	---	在研
36.		20153703-T-469		信息技术 云计算 分布式块存储系统总体技术要求	---	在研
37.		20153698-T-469		信息技术 云计算 虚拟机管理通用要求	---	在研
38.		20153707-T-469		信息技术 云计算 云服务运营通用要求	---	在研
39.		20120544-T-469		PaaS 平台参考架构	---	在研

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态	
40.		人工智能平台	---	信息技术 人工智能 平台任务调度及资源管理能力要求	---	拟研制	
41.			---	信息技术 人工智能 基本服务接口规范	---	拟研制	
42.			---	信息技术 人工智能 平台计算框架能力要求	---	拟研制	
43.			---	信息技术 人工智能 平台通用要求	---	拟研制	
44.		边缘智能计算	---	边缘智能计算参考架构	---	拟研制	
45.		智能芯片	---	智能芯片性能评估指南	---	拟研制	
46.		关键技术	机器学习	---	信息技术 神经网络表示与模型压缩	---	拟研制
47.	---			信息技术 学习模型性能评估规范	---	拟研制	
48.	计算机视觉		---	信息技术 计算机视觉 术语	---	拟研制	
49.			20141209-T-469	信息技术 形状建模信息表示 第1部分：框架和基本组件	---	在研	
50.			20141210-T-469	信息技术 形状建模信息表示 第2部分：特征约束	---	在研	
51.			20141203-T-469	信息技术 形状建模信息表示 第3部分：流式传输	---	在研	
52.			20141204-T-469	信息技术 形状建模信息表示 第4部分：存储格式	---	在研	
53.			---	智能监控 结构化视频 数据交换格式	---	拟研制	
54.			---	智慧传媒 智能分析元数据规范	---	拟研制	
55.			---	视频图像身份识别系统技术要求	---	拟研制	
56.			自然语言处理	20151549-T-469	智能客服语义库技术要求	---	在研
57.			人机交互	20171072-T-469	信息技术 手势交互系统 第1部分：技术要求	---	在研
58.	20171075-T-469			信息技术 手势交互系统 第2部分：系统接口	---	在研	
59.	20141231-T-469			信息技术 中文语音识别终端服务接口规范	---	在研	
60.	GB/T 21023-2007			中文语音识别系统通用技术规范	---	已发布	
61.	GB/T 21024-2007			中文语音合成系统通用技术规范	---	已发布	
62.	SJ/T 11380-2008			自动声纹识别（说话人识别）技术规范	---	已发布	
63.	GB/T 34145-2017	中文语音合成互联网服务接口规范		---	已发布		
64.	GB/T 34083-2017	中文语音识别互联网服务接口规范		---	已发布		

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
65.			---	信息技术 智能语音交互系统 第1部分：通用规范	---	拟研制
66.			20153685-T-469	信息技术 智能语音交互系统 第2部分：智能家居	---	在研
67.			20153686-T-469	信息技术 智能语音交互系统 第3部分：智能客服	---	在研
68.			20153687-T-469	信息技术 智能语音交互系统 第4部分：移动终端	---	在研
69.			20153688-T-469	信息技术 智能语音交互系统 第5部分：车载	---	在研
70.			2014-0419T-SJ	信息技术 智能电视语音识别测试方法	---	在研
71.			2014-0420T-SJ	信息技术 智能电视语音识别通用技术要求	---	在研
72.			---	信息技术 智能语音交互评测 第1部分：语音处理	---	拟研制
73.			---	信息技术 智能语音交互评测 第2部分：识别	---	拟研制
74.			---	信息技术 智能语音交互评测 第3部分：语义理解	---	拟研制
75.			---	信息技术 智能语音交互评测 第4部分：合成	---	拟研制
76.			---	信息技术 智能语音交互评测 第5部分：语音评测	---	拟研制
77.			---	信息技术 语音交互应用 第1部分：通用系统规范	---	拟研制
78.			---	信息技术 智能音箱评估指南	---	拟研制
79.		生物特征识别	GB/T 26237.1-2010	信息技术 生物特征识别 数据交换格式 第1部分：框架	ISO/IEC 19794-1: 2006 修改	已发布
80.	GB/T 26237.2-2011		信息技术 生物特征识别 数据交换格式 第2部分：指纹细节点数据	ISO/IEC 19794-2: 2005 修改	已发布	
81.	GB/T 26237.3-2011		信息技术 生物特征识别 数据交换格式 第3部分：指纹型谱数据	ISO/IEC 19794-3: 2006 修改	已发布	
82.	GB/T 26237.4-2014		信息技术 生物特征识别 数据交换格式 第4部分：指纹图像数据	ISO/IEC 19794-4: 2005 修改	已发布	
83.	GB/T 26237.5-2014		信息技术 生物特征识别 数据交换格式 第5部分：人脸图像数据	ISO/IEC 19794-5: 2005 修改	已发布	

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
84.			GB/T 26237.6-2014	信息技术 生物特征识别 数据交换格式 第6部分：虹膜图像数据	ISO/IEC 19794-6: 2005 修改	已发布
85.			GB/T 26237.7-2013	信息技术 生物特征识别 数据交换格式 第7部分：签名/签字时间序列数据	ISO/IEC 19794-7: 2007 修改	已发布
86.			GB/T 26237.8-2014	信息技术 生物特征识别 数据交换格式 第8部分：指纹型骨架数据	ISO/IEC 19794-8: 2006 等同	已发布
87.			GB/T 26237.9-2014	信息技术 生物特征识别 数据交换格式 第9部分：血管图像数据	ISO/IEC 19794-9: 2007 修改	已发布
88.			GB/T 26237.10-2014	信息技术 生物特征识别 数据交换格式 第10部分：手型轮廓数据	ISO/IEC 19794-10: 2007 等同	已发布
89.			20080532-T-469	信息技术 生物特征识别 数据交换格式 第14部分：DNA数据	---	在研
90.			SJ/T 11607-2016	指纹识别设备通用规范	---	已发布
91.			SJ/T 11608-2016	人脸识别设备通用规范	---	已发布
92.			20151546-T-469	信息技术 生物特征识别 指纹处理芯片通用规范	---	在研
93.			20160129-T-469	信息技术 生物特征识别 指纹识别设备通用规范	---	在研
94.			20152000-T-469	信息技术 虹膜识别设备通用规范	---	在研
95.			GB/T 33767.1-2017	信息技术 生物特征样本质量 第1部分：框架	ISO/IEC 29794-1: 2009 等同	已发布
96.			20141198-T-469	信息技术 生物特征样本质量 第4部分：指纹图像数据	ISO/IEC 29794-4: 2010 等同	在研
97.			20141199-T-469	信息技术 生物特征样本质量 第5部分：人脸图像数据	ISO/IEC 29794-5: 2010 等同	在研
98.			20153692-T-469	信息技术 生物特征样本质量 第6部分：虹膜图像数据	ISO/IEC 29794-6: 2015 等同	在研
99.			GB/T 28826.2-2014	信息技术 公用生物特征识别交换格式框架 第2部分：生物特征识别注册机构操作规程	ISO/IEC 19785-2: 2006 修改	已发布
100.			GB/T 33844-2017	信息技术 生物特征识别用于生物特征十指指纹采集应用编程接口 (BioAPI)	ISO/IEC 29141: 2009 等同	已发布

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
101.			GB/T 32629-2016	信息技术 生物特征识别应用程序接口的互通协议	ISO/IEC 24708: 2008 等同	已发布
102.			GB/T 33842.2-2017	信息技术 GB/T26237 中定义的生物特征数据交换格式的符合性测试方法 第2部分: 指纹细节点数据	---	已发布
103.			GB/T 33842.4-2017	信息技术 GB/T26237 定义的生物特征数据交换格式的符合性测试方法 第4部分: 指纹图像数据	---	已发布
104.			20151550-T-469	信息技术 GB/T26237 定义的生物特征数据交换格式的符合性测试方法 第5部分: 人脸图像数据	ISO/IEC 29109-5: 2014 修改	在研
105.			20141196-T-469	信息技术 生物特征识别 多模态及其他多生物特征融合	ISO/IEC 24722: 2007 修改	在研
106.			20153999-T-469	信息技术 移动设备生物特征识别 第1部分: 通用要求	---	在研
107.		VR/AR	20130388-T-469	信息技术 增强现实 第1部分: 术语	---	在研
108.			20171076-T-469	信息技术 虚拟现实头戴式显示设备通用规范	---	在研
109.			20172574-T-469	信息技术 虚拟现实应用软件基本要求和测评方法	---	在研
110.			---	信息技术 虚拟现实头戴式显示设备舒适度测试方法	---	拟研制
111.			---	信息技术 虚拟现实头戴式显示设备安全测试方法	---	拟研制
112.			---	增强现实人脸结构定位与特效数据格式规范	---	拟研制
113.	产品	机器人	GB/T 33267-2016	机器人仿真开发环境接口	---	已发布
114.			GB/T 29825-2013	机器人通信总线协议	---	已发布
115.			GB/T 33266-2016	模块化机器人高速通用通信总线性能	---	已发布
116.			GB/T 33262-2016	工业机器人 模块化设计规范	---	已发布
117.			GB 11291.2-2013	机器人与机器人装备 工业机器人的安全要求 第2部分: 机器人系统与集成	ISO 10218-2: 2011 等同	已发布
118.			GB/T 29824-2013	工业机器人 用户编程指令	---	已发布
119.			GB/T 12642-2013	工业机器人 性能规范及其试验方法	---	已发布
120.			GB/T 20868-2007	工业机器人 性能试验实施规范	---	已发布

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态	
121.			GB/T 33261-2016	服务机器人模块化设计总则	---	已发布	
122.			GB/T 34454-2017	家用干式清洁机器人性能测试方法	---	已发布	
123.			GB/T 33265-2016	教育机器人安全要求	---	已发布	
124.			---	智能客服机器人通用技术规范	---	拟研制	
125.		智能终端	GB/T 30284-2013	移动通信智能终端操作系统安全技术要求（EAL2级）	---	已发布	
126.			GB/T 32927-2016	信息安全技术 移动智能终端安全架构	---	已发布	
127.			GB/T 33776.4-2017	林业物联网 第4部分：手持式智能终端通用规范	---	已发布	
128.			GB/T 34132-2017	智能变电站智能终端装置通用技术条件	---	已发布	
129.			SJ/T 11592-2016	智能电视 概念模型	---	在研	
130.			2014-0421T-SJ	智能电视 智能化技术评价方法	---	在研	
131.			2014-0418T-SJ	智能电视 手势识别技术要求及测试方法	---	在研	
132.			2015-1604T-SJ	智能电视 娱乐操控编码规则及测量方法	---	在研	
133.			智能运载工具	JB/T 5063-2014	搬运机器人通用技术条件	---	已发布
134.				SJ 20569-1996	无人侦察飞机综合无线电系统通用规范	---	已发布
135.		GB 10827.1-2014		工业车辆 安全要求和验证 第1部分：自行式工业车辆（除无人驾驶车辆、伸缩臂式叉车和载运车）	---	已发布	
136.	应用/服务	智能家居	GB/T 30246.1-2013	家庭网络 第1部分：系统体系结构及参考模型	---	已发布	
137.				GB/T 30246.2-2013	家庭网络 第2部分：控制终端规范	---	已发布
138.				GB/T 30246.3-2013	家庭网络 第3部分：内部网关规范	---	已发布
139.				GB/T 30246.4-2013	家庭网络 第4部分：终端设备规范 音视频及多媒体设备	---	已发布
140.				GB/T 30246.5-2014	家庭网络 第5部分：终端设备规范 家用和类似用途电器	---	已发布
141.				GB/T 30246.6-2013	家庭网络 第6部分：多媒体与数据网络通信协议	---	已发布
142.				GB/T 30246.7-2013	家庭网络 第7部分：控制网络通信协议	---	已发布
143.				GB/T 30246.8-2013	家庭网络 第8部分：设备描述文件规范 XML 格式	---	已发布
144.				GB/T 30246.9-2013	家庭网络 第9部分：设备描述文件规范二进制格式	---	已发布

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
145.			GB/T 30246.11-2013	家庭网络 第 11 部分：控制网络接口一致性测试规范	---	已发布
146.			---	信息技术 智能家居 通信交互协议规范	---	拟研制
147.			---	信息技术 智能家居 人机交互界面要求	---	拟研制
148.		智能物流	GB/T 32404-2015	基于 M2M 技术的移动通信网物流信息服务总体技术框架	---	已发布
149.	GB/T 32405-2015		移动通信网面向物流信息服务的 M2M 协议	---	已发布	
150.	GB/T 32406-2015		移动通信网面向物流信息服务的 M2M 平台技术要求	---	已发布	
151.	GB/T 32407-2015		移动通信网面向物流信息服务的 M2M 通信模块技术要求	---	已发布	
152.		智能制造	20170053-T-339	工业互联网总体网络架构	---	在研
153.			20170057-T-469	智能制造 对象标识要求	---	在研
154.			20170054-T-339	智能制造 标识解析体系要求	---	在研
155.			20170039-T-604	数字化车间通用技术要求	---	在研
156.			20170038-T-604	数字化车间机床制造信息模型	---	在研
157.		智慧城市	GB/T 33356-2016	新型智慧城市评价指标	---	已发布
158.			GB/T 34678-2017	智慧城市 技术参考模型	---	已发布
159.			20151993-T-469	智慧城市 领域知识模型 第 1 部分：核心概念模型	---	在研
160.			20151994-T-469	智慧城市 数据融合 第 2 部分：数据编码规范	---	在研
161.			20151995-T-469	智慧城市 数据融合 第 1 部分：数据概念模型及描述规范	---	在研
162.			20151996-T-469	智慧城市 信息与服务公共支撑平台 第 2 部分：目录管理与服务要求	---	在研
163.			20151997-T-469	智慧城市 信息系统运维指南	---	在研
164.			20151998-T-469	智慧城市 顶层设计指南	---	在研
165.			GB/T 34680.1-2017	智慧城市 评价模型及基础评价指标体系 第 1 部分：总体框架及分项评价指标制定的要求	---	已发布
166.			20130390-T-469	智慧城市 评价模型及基础评价指标体系 第 2 部分：信息化应用和服务	---	在研

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
167.			GB/T 34680.3-2017	智慧城市 评价模型及基础评价指标体系 第3部分：信息资源	---	已发布
168.		智能交通	GB/T 31024.1-2014	合作式智能运输系统 专用短程通信 第1部分：总体技术要求	---	已发布
169.	GB/T 31024.2-2014		合作式智能运输系统 专用短程通信 第2部分：媒体访问控制层和物理层规范	---	已发布	
170.	20130075-T-469		车路协同专用短程通信 第3部分：网络层和应用层	---	在研	
171.	20130076-T-469		车路协同专用短程通信 第4部分：设备应用	---	在研	
172.	GB/T 24466-2009		电子健康记录体系架构需求	---	已发布	
173.		智能医疗	20161920-T-469	智慧城市 智慧医疗 第1部分：框架及总体要求	---	在研
174.	20152350-T-339		智慧城市 智慧医疗 第2部分：移动健康	---	在研	
175.	20150079-T-361		医疗健康物联网 感知设备数据命名表 第1部分：总则	---	在研	
176.	20150081-T-361		医疗健康物联网 感知设备数据命名表 第2部分：体温计	---	在研	
177.	20150076-T-361		医疗健康物联网 感知设备数据命名表 第3部分：血氧仪	---	在研	
178.	20150074-T-361		医疗健康物联网 感知设备数据命名表 第4部分：心电测量仪	---	在研	
179.	20150075-T-361		医疗健康物联网 感知设备数据命名表 第5部分：血压计	---	在研	
180.	20150073-T-361		医疗健康物联网 感知设备数据命名表 第6部分：血糖仪	---	在研	
181.	20150077-T-361		医疗健康物联网 感知设备数据命名表 第7部分：能量监测仪	---	在研	
182.	20150078-T-361		医疗健康物联网 感知设备数据命名表 第8部分：位置标识	---	在研	
183.	2017-0289T-SJ		智慧家庭 健康管理腕式可穿戴设备技术要求	---	在研	
184.	2017-0290T-SJ		智慧家庭 健康养老产品分类及描述	---	在研	
185.	2017-0291T-SJ		智慧家庭 健康养老服务平台参考模型	---	在研	
186.	2017-0292T-SJ		智慧家庭 老人手环（手表）技术规范	---	在研	
187.			---	医学影像辅助诊断系统技术要求	---	拟研制

序号	一级分类	二级分类	国家/行业标准编号/计划号	标准名称	采用标准号及采用程度	状态
188.		智能金融	JR/T0093.1-2012	中国金融移动支付 远程支付应用 第1部分：数据元	---	已发布
189.	JR/T0093.2-2012		中国金融移动支付 远程支付应用 第2部分：交易模型及流程规范	---	已发布	
190.	GB/T27912-2011		金融服务生物特征识别安全框架	---	已发布	
191.		安全	20141145-T-469	信息安全技术 物联网 感知层接入通信网的安全要求	---	在研
192.	20151593-T-469		信息安全技术 物联网 安全参考模型及通用要求	---	在研	
193.	20152012-T-469		信息安全技术 物联网 数据传输安全技术要求	---	在研	
194.	20152014-T-469		信息安全技术 物联网 感知层网关安全技术要求	---	在研	
195.	20152007-T-469		信息安全技术 物联网 感知设备安全技术要求	---	在研	
196.	20171113-T-469		信息安全技术 信息系统等级保护安全设计技术要求 第4部分：物联网	---	在研	
197.	GB/T 31167-2014		信息安全技术 云计算 服务安全指南	---	已发布	
198.	GB/T 31168-2014		信息安全技术 云计算 服务安全能力要求	---	已发布	
199.	20170565-T-469		信息安全技术 基于可信环境的生物特征识别身份鉴别协议	---	在研	
200.	---		信息技术 人工智能安全态势感知技术要求	---	拟研制	

附件 2 应用案例

根据人工智能应用场景，本白皮书选编了 10 个典型应用案例，限于篇幅，每个案例仅是简要介绍，感兴趣的读者可以联系案例单位获取进一步信息。

案例一：城市大脑在城市公共资源优化配置的创新实践与应用

应用领域：城市治理

应用场景：交通态势评价与信号灯控制优化、城市事件感知与智能处理、公共出行与运营车辆调度、社会治理与公共安全

案例提供者：阿里云计算有限公司

（1）客户需求和方案简介

中国的信息化建设已经到达一定阶段，积累了海量数据。但现状是各部门正在运行的各类交通管理信息化系统和平台都是以传统的信息化模式建设的，建设标准和运行模式不一样，各自独立运行，不能互通和协同。传统的信息化建设模式导致信息孤岛的产生，各类数据资源相互割裂，数据的共享和开放程度低。另外针对海量数据的存储及计算，没有领先的大数据、云计算及 AI 能力，很难把数据的价值很好的挖掘和利用起来。

城市大脑是支撑未来城市可持续发展的全新基础设施,其核心是利用实时全量的城市数据资源全局优化城市公共资源，即时修正城市运行缺陷，实现以下三个突破：

①城市治理模式突破

以城市数据为资源，提升政府管理能力，解决城市治理突出问题，实现城市治理智能化、集约化、人性化。

②城市服务模式突破

更精准地随时随地服务企业和个人，城市的公共服务更加高效，公共资源更加节约。

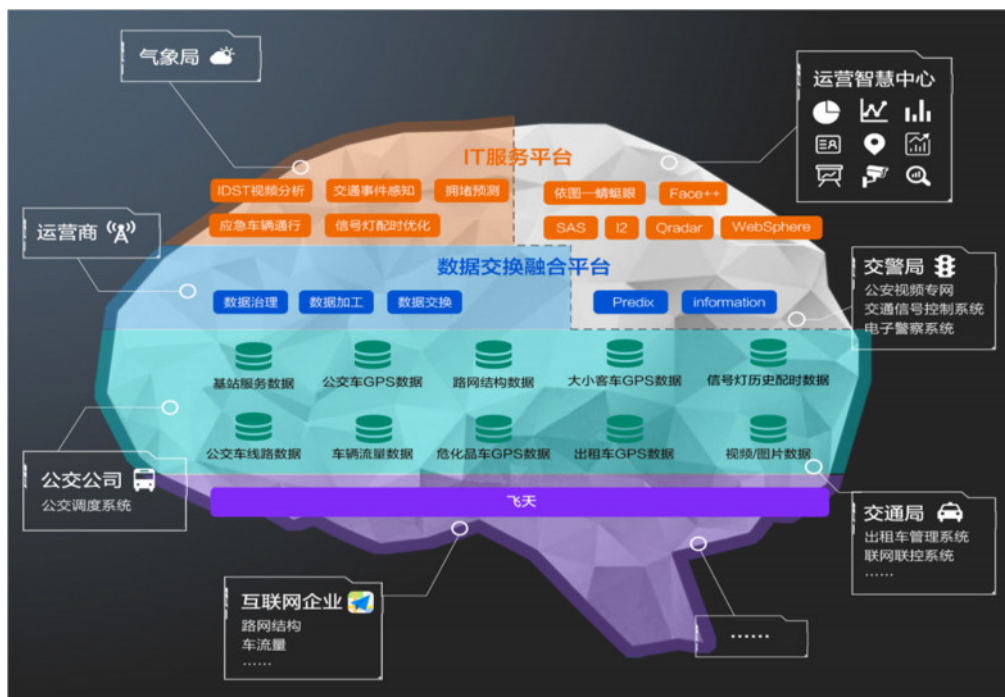
③城市产业发展突破

开放的城市数据资源是重要的基础资源，对产业发展发挥催生带动作用，促进传统产业转型升级。

（2）具体解决方案介绍

ET 城市大脑是在依托阿里云大数据一体化计算平台基础上，通过阿里云数

据资源平台对包括企业数据、公安数据、政府数据、运营商等多方城市数据的汇集，借助机器学习和人工智能算法，面向城市治理问题打造的数据智能产品。通过 ET 城市大脑，可以从全局、实时的角度发现城市的问题并给出相应的优化处理方案，同时联动城市内各项资源调度，从而整体提升城市运行效率。



从上面的城市大脑总体架构图可以看到，城市大脑分为三层，最下层为阿里云飞天计算平台，中间为阿里云城市大脑数据资源平台，最上层为阿里云城市大脑 IT 服务平台。其中数据资源平台和 IT 服务平台为开放平台，可以承载其他厂商产品。

一体化计算平台：为城市大脑提供足够的计算能力，具备极致弹性，支持全量城市数据的实时计算。EB 级存储能力，PB 级处理能力，百万路级别视频实时分析能力。

数据资源平台：全网数据实时汇聚，让数据真正成为资源。保障数据安全，提升数据质量，通过数据调度实现数据价值。

IT 服务平台：开放的 IT 服务平台，繁荣产业生态。通过数据资源的消耗换来自然资源的节约。



城市大脑子产品子系统图展示了智能数据应用各个子系统模块的内容，具体包含以下几个子系统：交通态势评价、信号灯控制策略优化、城市事件感知、应急车辆优先通行、公交调度优化、重点车辆监控。

(3) 方案实施后的价值或成果

在交通领域，全球首个互联网+联信号灯平台在广州成功推出并取得实战结果（试点路口失衡指数下降 26%，拥堵指数下降 19%）；在杭州，首次通过球机视频分析，实现交通异常事件的自动巡检，交通事故实现秒级实时报警，识别准确率 92%以上，同时联合信号灯智能调控，部分区域通行时间缩短 15.3%；在萧山，实现救护车弹性绿波带，救护车到达时间缩减 50%，为每一个等待拯救的生命亮起绿色信号灯。城市大脑，城市治理的前瞻性实践，陆续在中大型及特大型城市成功登陆，包括苏州、衢州、澳门等。通过数据的汇聚，实现对整个城市的实时数据分析和研判，有效调配和优化公共资源，不断修正城市运行中的缺陷，突破城市治理和服务模式。

案例二：医疗 AI 影像的成功应用

应用领域：医疗影像

应用场景：临床医疗影像辅助诊断

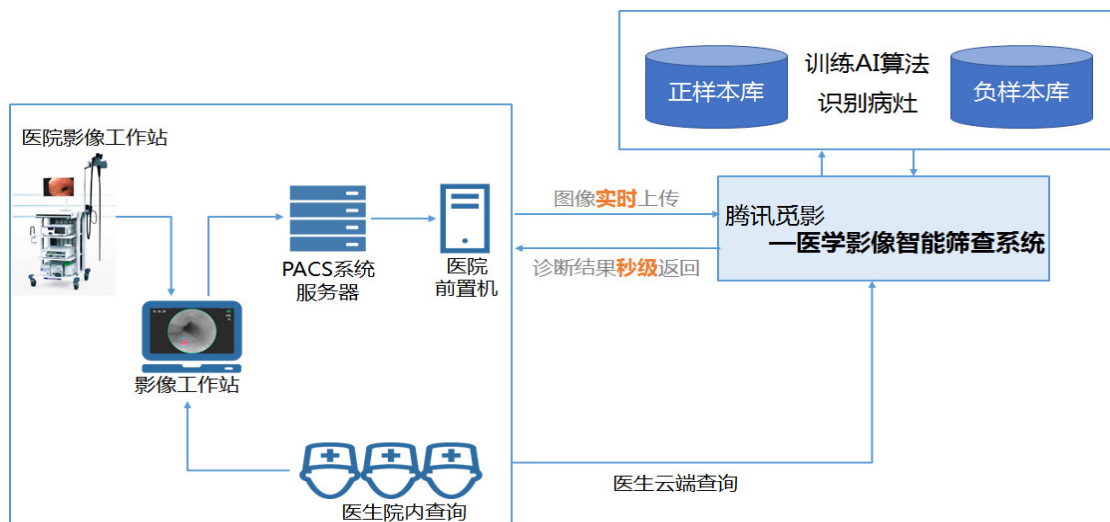
案例提供者：腾讯互联网加（深圳）有限公司

（1）客户需求和方案简介

随着医学成像技术的不断进步，近几十年中 X 光、超声波、计算机断层扫描（CT）、核磁共振（MR）、数字病理成像、消化道内窥镜、眼底照相等新兴医学成像技术发展突飞猛进，各类医学图像数据也爆炸性增加。在传统临床领域，医学图像的判读主要是由医学影像专家、临床医生实现，日益增长的图像数据给医生阅片带来极大的挑战和压力。随着计算机技术的不断突破，计算机辅助医学图像的判断成为可能，并且在临床辅助诊断中所占比重逐年增大。相比于人工判读图像，计算机辅助诊断可以有效提高阅片效率，避免人工误判，降低医生工作量和压力。

（2）具体解决方案介绍

依托国际领先的图像识别技术，腾讯开发了医学影像智能筛查系统，实现了对早期食管癌、早期肺癌、早期乳腺癌、糖尿病性视网膜病变等疾病的智能化筛查和识别，辅助医疗临床诊断。腾讯医学影像智能筛查系统由“食管癌早期筛查子系统”、“肺癌早期筛查子系统”、“糖网智能分期识别子系统”、“乳腺癌早期筛查子系统”构成，支持食管癌良恶性识别、肺结节位置检测、肺癌良恶性识别、糖网识别、糖网分期、乳腺癌钙化和肿块检测、乳腺癌良恶性识别等临床需求。



(3) 方案实施后的价值或成果

腾讯医学影像智能筛查系统目前已经在全国多个省市的数十家三甲医院中进行了广泛应用，并获得了医生高度认可。例如，浙江省温州市中心医院上线食管癌早期筛查系统 2 周即发现 2 例医生未发现的早期食管癌患者，最终这 2 位患者确诊后，进行早癌手术。早发现早治疗，大大提高了患者生存率，降低治疗费用，保障术后生活质量。

地区	医院	应用
广东	中山大学附属肿瘤医院	食管癌早期筛查系统
广东	南山区人民医院	食管癌早期筛查系统 肺癌早期筛查系统 眼底糖网筛查系统
广东	广东省第二人民医院	肺癌早期筛查系统 食管癌早期筛查系统
浙江	浙江省人民医院	食管癌早期筛查系统
浙江	温州市中心医院	食管癌早期筛查系统
广西	广西壮族自治区人民医院	眼底糖网筛查系统 食管癌早期筛查系统
江苏	苏州科技城医院	肺癌早期筛查系统
四川	四川省中医二院	肺癌早期筛查系统
陕西	西安第四医院	眼底糖网筛查系统

利用基于人工智能的腾讯医学影像智能筛查系统进行辅助医学图像诊断相对于医生独立通过人工诊断具有显著的优势：统一的问题，使得影像诊断更加客观；人工智能诊断可以大幅度大规模提高人工阅片的速度，降低医生的工作量，提高效率；人工智能诊断能比人工阅片更快更精准的发现病灶，防止医生漏诊和误诊，给医生诊断加上了一层安全保障，是未来的发展趋势；人工智能诊断可以辅助重大疾病早期筛查，降低人工筛查的人力成本和工作量，大大提高我国重大疾病早期筛查的普及率和准确率；人工智能诊断通过辅助基层医生诊断让低年资医生快速的积累诊断经验，降低学习成本，从而能大大缓解我国患者多，医生资源不足的情况。

案例三：语音评测在英语听说考试的成功应用

应用领域：教育考试

应用场景：中考、高考中的英语听说测试

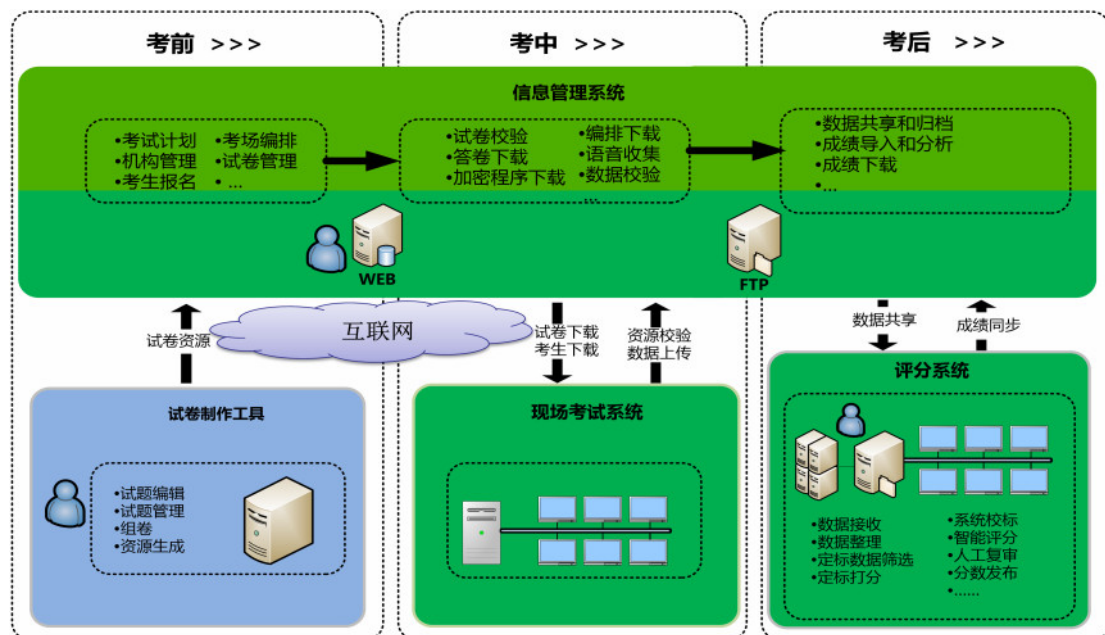
案例提供者：科大讯飞股份有限公司

(1) 客户需求和方案简介

随着国际交流的日益增多，英语交际能力越来越重要。虽然国家、社会、学校都很重视英语教学工作，但是由于缺乏有效的评估和教学手段，“哑巴英语”、“洋泾浜英语”等现象仍然大量存在。中国青年报统计，我国有 56% 的学生“大部分”时间花在英语学习上，但是真正具备沟通能力的仅有 10%。全国绝大多数省份都已开展了高考英语听力考试和口语加试，广东、江苏等越来越多的省市已经把英语口语考试成绩计入到高考、中考绝对分。实践表明，开展英语听说考试可以显著促进英语教学的发展。中高考英语听说考试已经是大势所趋。

(2) 具体解决方案介绍

依托国际领先的智能语音评测技术，科大讯飞开发了英语听说智能测试系统，实现了英语听说考试全过程的自动化与智能化。讯飞英语听说智能测试系统由“命题制卷子系统”、“考务管理子系统”、“现场考试子系统”、“阅卷评分子系统”构成，支持短文朗读、情景反应、角色扮演、口语表达、话题复述所有主流题型。



(3) 方案实施后的价值或成果

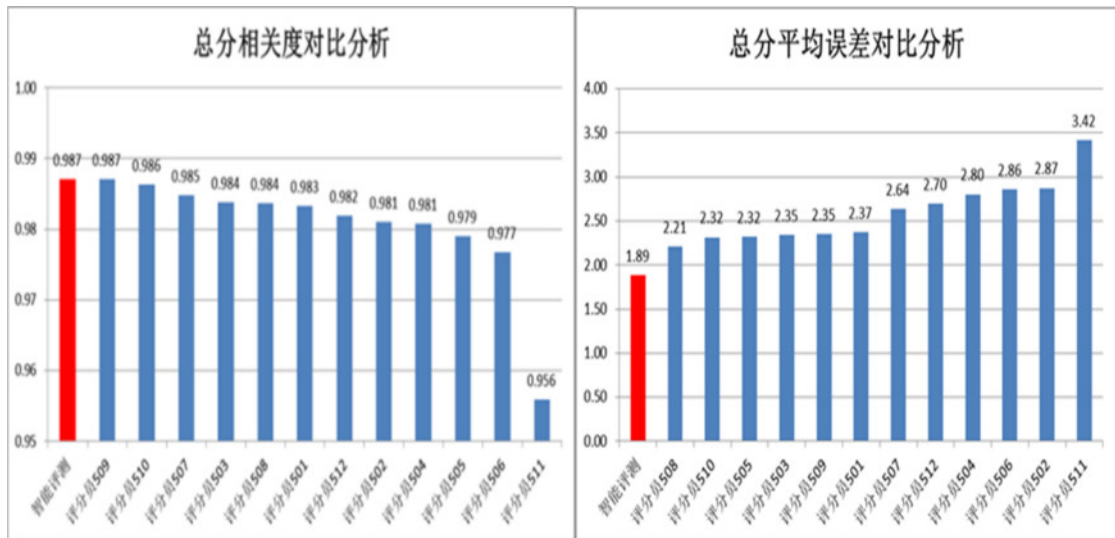
科大讯飞英语听说智能测试系统目前已经在全国 23 个省市地区的中、高考中进行了广泛应用，包括北京中、高考、上海高考、广东高考、江苏中考、深圳中考等，年测试人数达 230 万人次，累计测试人数达 1900 万人次。

科大讯飞英语听说智能测试系统的具体应用情况，如下所示：

地区	考试类型	考试成绩作用
广东	高考	英语听说考试总分 15 分，直接计入高考总分
	中考	广州、深圳、东莞、江门、中山等 9 个地市开展，成绩直接计入中考总分
北京	中考	北京市中考从 2018 年起，英语总分 100 分，其中 60 分为卷面考试成绩，40 分为听力、口语考试，与统考笔试分离，学生有两次考试机会。
	高考	北京市高考，从 2017 年起，英语听力分值 30 分，采用计算机化考试，与统考笔试分离，一年两次考试，取听力最高成绩与笔试成绩一同组成英语科目成绩计入高考总分，从 2021 年起，英语增加口语考试，口语加听力考试共计 50 分，英语科目满分 150 分。
上海	高中学业水平考试	作为高考外语相关专业录取参考分
	高考	从 2017 年 1 月份起，上海高考全面启动英语听说口语考试，采用一年两考的形式，考试成绩计入高考总分，总分 10 分
重庆	高职单招	英语学科不再进行纸笔考试，听说考试成绩直接作为高职院校招生录取成绩
	中考	綦江、江津、黔江等区县开展，总分 30 分，直接计入中考总分
江苏	中考	总分 30 分，直接计入中考总分
浙江	中考	2010 年，温州正式开始测试，总分 30 分，直接计入中考总分
安徽	中考	总分 30 分，直接计入中考总分，目前合肥开展
山东	中考	口语成绩 30 分，直接计入中考总分，目前青岛、淄博、威海开展
青海	中考	总分 30 分，直接计入中考总分，目前西宁开展
贵州	高考	高考加试，2014 年全省全面应用
湖北	高考	高考加试
福建	中考	口语成绩 10 分，中考录取参考分，目前三明正式开展
沈阳	中考	总分 20 分，15 年正式考试，16 年直接计入中考总分

随着人工智能技术的快速发展，基于自然语言理解、机器学习等人工智能技术的智能语音技术得到了长足的进步，已经在多个行业进行了广泛的应用。

在 2012 年广东省科技鉴定中，科大讯飞智能语音评测技术的计算机评分相关度超过所有专家，平均误差低于所有专家，整体效果方面全面超过人工。



注：相关度是衡量评分者对考生打分排序合理性的指标，反映了评分的公平性。介于0-1之间，越接近1越好；平均误差是衡量评分者评分准确程度的一种指标，平均误差越小表示评分准确度越高。

利用基于人工智能技术开发设计的英语听说智能测试系统开展考试，相对传统的人工考试具有显著优势：

①智能语音评分技术可以彻底解决人工阅卷主观性强、评分标准不统一的问题，使英语口语考试更加公平、公正。

②智能语音评测技术可大幅提高大规模口语考试的阅卷速度，降低口语考试阅卷的成本及实施难度，促进口语考试的发展。

③智能语音评测技术能够从发音标准度评估、发音缺陷检测、口语应用能力评估等多个维度进行详细的测评，能够客观全面的反应学生的口语能力。

④考试现场应用人工智能技术进行在线实时评分，使自适应考试成为可能。自适应考试由于更加准确的评估考生水平，是未来考试的发展趋势。

⑤智能语音质量检测技术应用于考试端，能够在考生口语采集环节避免设备故障或人为原因造成录音失败的情况，大大提高口语考试的成功率。

案例四：智能供应链设计系统

应用领域：制造领域

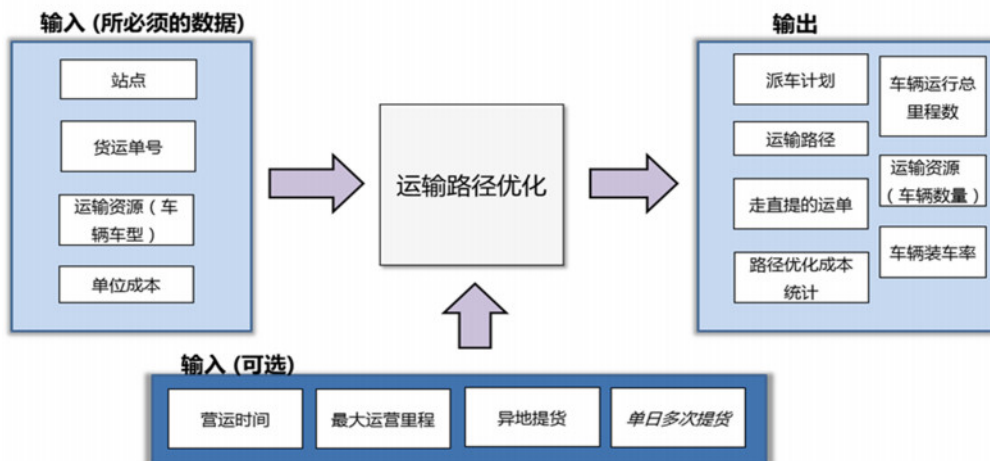
应用场景：供应链路径优化

案例提供者：华为技术有限公司

(1) 用户需求和方案简介

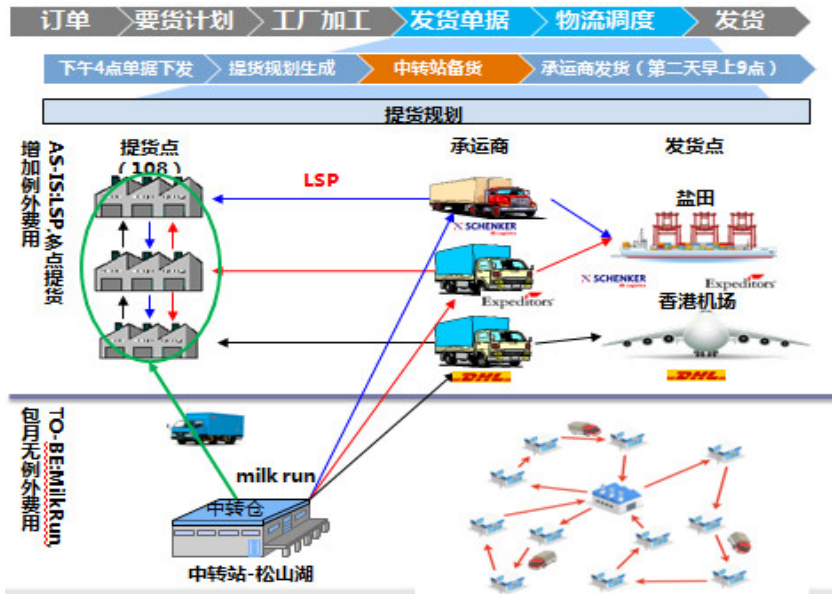
当前华为供应链物流供应商（LSP）单车提货每增加一个提货点，就多增加一次例外费用，导致多点提货费用高，需要根据发货单据，人工的方式拆分给承运商，进行发货，每年的例外费用高达 1200 多万人民币。

之前人工方式效率低，成本高，无法实现实时、快速设计最为合适的供应链物流方案，而采用智能供应链设计系统之后，能够大量减少人力投入，快速实现供应链路径优化。



(2) 具体解决方案介绍

智能系统自动识别是选择直提物流模式还是选择中转仓模式，自动优化并推荐给用户车辆数。按天输出派车计划，解决多订单、多工厂映射关系下的组合路径优化问题，目标达到月运输成本最优。10 分钟之内完成给出物流配车和路线规划。



华为人工智能系统的路径优化解决方案聚焦于降低物流运输成本，包含三个模块：

自动识别运输方案	假设有 M 个订单，其中有 m 个订单采用中转仓的方式，其余采用原来直提的运输方式。通过 0-1 动态规划技术，自动识别，确定走中转仓的货运单数 m。
智能路径优化技术	通过聚类 KNN 模型对 m 个订单的对应的工厂进行聚类找出相邻距离最小的点。然后根据聚类结果，进一步采用 Dijkstra 算法计算遍历最短路径计算派车计划、运输路径。
成本优化统计	基于每天最佳配车方案，按月统计输出节省的总运输成本、车辆运行总里程数、运输所需车辆数、装车率等。

构建智能分布式优化算法库，包含业务模型层、数学模型层/各种规划问题、基础优化算法层；通过 0-1 动态规划技术，自动识别并确定走中转仓的货运单数；通过聚类 KNN 模型对订单的对应的工厂进行聚类找出相邻距离最小的点。然后根据聚类结果，进一步计算派车计划、运输路径。

(3) 方案实施后的价值或成果

通过提货规划，减少例外费用，提升发货效率。以天为单位，合理分配租赁车辆并对提货路线进行优化，利用中转仓（MilkRun）尽可能提高车辆满载率、减少出行次数，减少提货的例外费用。根据 2016 年 1-6 月的历史数据进行优化，每个月的运输成本降低 30% 以上。基于平台能力，优化算法高效率，按天输出派车计划，只需要 10s 左右。

案例五：百度机器翻译

应用领域：机器翻译

应用场景：不同语种间的转换

案例提供者：百度网络技术有限公司

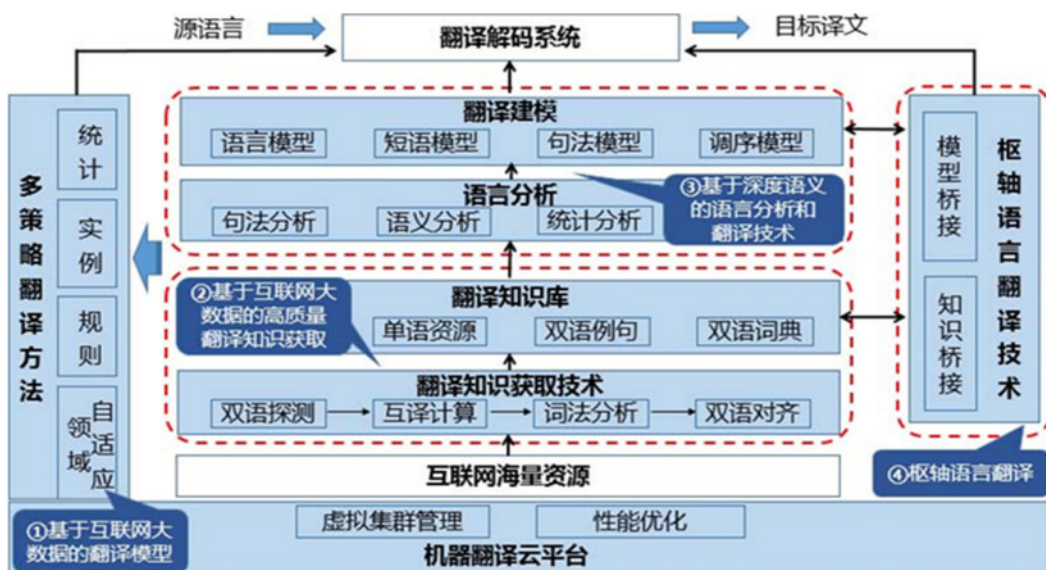
(1) 客户需求和方案简介

机器翻译是利用计算机将一种语言自动翻译为另外一种语言。早在 1946 年第一台现代计算机诞生之初，美国科学家 W.Weaver 就提出了机器翻译的设想。机器翻译涉及计算机、认知科学、语言学、信息论等学科，是人工智能的终极目标之一，研究机器翻译技术具有重要的学术意义。

在互联网和全球化背景下，大国之间的网络博弈趋于白热化，网络信息安全面临前所未有的挑战。研发具有完全自主知识产权的机器翻译系统，实时准确地获取多语种政治、经济、文化、军事等信息，是我国信息安全的重要基础保障，对于保障国家安全、发展国民经济和实施国际化战略具有重要意义。

(2) 具体解决方案介绍

互联网大数据给机器翻译研究带来新的机遇和挑战，使得海量翻译知识的自动获取和实时更新成为可能，传统翻译模型和方法亟待创新。本项目在海量翻译知识获取、翻译模型、多语种翻译技术等方面取得重大突破，解决了传统方法研发成本高、周期长、质量低的难题，实时准确地响应互联网海量、复杂的翻译请求，使我国掌握了互联网机器翻译的核心技术，占据了该领域的技术制高点。基于大数据的互联网机器翻译核心技术如下：



①提出了基于互联网大数据的翻译模型。在此模型指导下，提出了自适应训练和多策略解码算法，突破了多领域、多文体的翻译瓶颈；实现了翻译云平台与算法的充分优化与融合，实时响应每天来自全球过亿次复杂多样的翻译请求。

②研发了基于互联网大数据的高质量翻译知识获取技术。突破了传统翻译知识获取规模小、成本高的瓶颈；制订了语言内容处理领域的国际标准。项目积累的高质量翻译知识规模是权威国际机构 NIST 发布的数据规模的 100 倍。

③提出了基于深度语义的语言分析和翻译技术。突破了机器翻译中公认的消歧和调序世界难题，在国际上首次提出了基于树到串的句法统计翻译模型，有效利用源语言句法信息解决短语泛化和长距离翻译调序问题。

④提出了基于枢轴语言的翻译知识桥接和模型桥接技术。突破了机器翻译语种覆盖度受限的瓶颈，使得资源稀缺的小语种翻译成为可能，并实现了多语种翻译的快速部署，11 天可部署 1 个新语种。目前系统支持 28 种语言，756 个翻译方向。

(3) 方案实施后的价值或成果

以上技术应用于国家多个重要部门和百度、华为、金山等超过 7000 个企业和第三方应用，此外，百度的机器翻译项目，曾获得 2015 年度的国家科技进步二等奖，百度机器翻译典型的应用如下：

①基于以上研究成果，实现了“多语言信息采集处理与分析系统”，支持英语、日语、德语、法语、朝鲜语、阿拉伯语和土耳其语等外国语，及藏语、维吾尔语和蒙古语等我国少数民族语言，共 10 多种语言文本的自动采集、翻译和分析系统。该系统成果应用于中国人民解放军总参谋部第五十五研究所等国家重要部门，有效支撑了相关单位核心事业的发展，为维护国家安全和社会稳定、推动多语言情报翻译和分析事业的发展发挥了重要作用。

②研究成果应用于“百度翻译”，支持了汉语、英语、日语、韩语、泰语等 28 种语言和 756 个翻译方向，形成了支持多语言高质量翻译的市场竞争优势，覆盖全球超过 5 亿用户，每日响应过亿次的翻译请求。根据第三方评测，“百度翻译”在当时上线的 32 个翻译方向中，有 28 个翻译方向超越谷歌翻译。在中国电子学会组织的科技成果技术鉴定中，院士专家一致认为：“在翻译质量、翻译语种方向、响应时间三个指标上达到国际领先水平”。

③翻译技术应用于百度搜索，帮助用户更加便捷地获取多语言信息，找到所求。2014年7月习近平总书记和百度CEO李彦宏共同启动葡萄牙语搜索引擎，为用户提供跨语言搜索服务；该技术也应用于百度的阿拉伯语、泰语搜索引擎中。近三年，取得直接经济效益10.94亿元。

④“百度翻译”开放平台为超过7000个第三方应用提供免费服务，促进了国民经济的发展，助力中国企业的国际化；为大量中小企业提供翻译平台服务，降低了创业创新门槛，带动了相关产业的繁荣与发展。华为将翻译服务集成到其Ascend Mate手机的摄像头翻译应用中，提升了该手机的市场竞争力，带有翻译功能的手机被销往法国、德国、俄罗斯、西班牙、英国等30多个国家和地区。

“金山词霸”使用以上翻译技术，实现从字词查询到句篇自动翻译的跨越，增强了其产品的价值，装机量4660万套，合计产值4561万元。B2B跨境电子商务平台“敦煌网”使用“百度翻译”进行跨境贸易，服务超过100万家国内供应商，帮助其将商品销往全球224个国家和地区，促进了我国对外贸易的发展。

案例六：小i机器人智能客服机器人系统

应用领域：智能人机交互

应用场景：自动客服、呼叫中心、智能人机交互

案例提供者：上海智臻智能网络科技股份有限公司（小i机器人）

（1）客户需求和方案简介

客服机器人是一种全新的智能工具，可以24小时在线实时回复用户提问，因此将客服机器人作为人工客户服务的补充，其为公众服务的能力相较传统的纯人工客服可以得到明显提高。

智能客服机器人可透过一定的载体，如WEB、IM、WAP/SMS等，结合图片、文字甚至音视频等媒体给用户最完整的回复，让用户在交流中解决问题。在客户服务中心已经高度发达的欧美国家，相当多的企业已经实施了智能客服机器人服务系统，采用人工智能技术为企业和政府的客户提供便捷、准确和高质量的服务，有效地配合客户服务中心，增加了客户满意度。

将人工智能技术应用于互联网实时通信领域和无线通信领域，在针对当前具有大规模智能需求的企业，如电信、金融、电力以及政府客户服务中心等市场进

行深入研究之后，基于机器人智能引擎系统推出了面对企业和政府的各类智能客服机器人及解决方案，可以在低投入的基础上为企业的用户提供优质高效的服务。

(2) 具体解决方案介绍

智能客服机器人基本架构图如下所示。



该基本架构图主要包括以下模块：

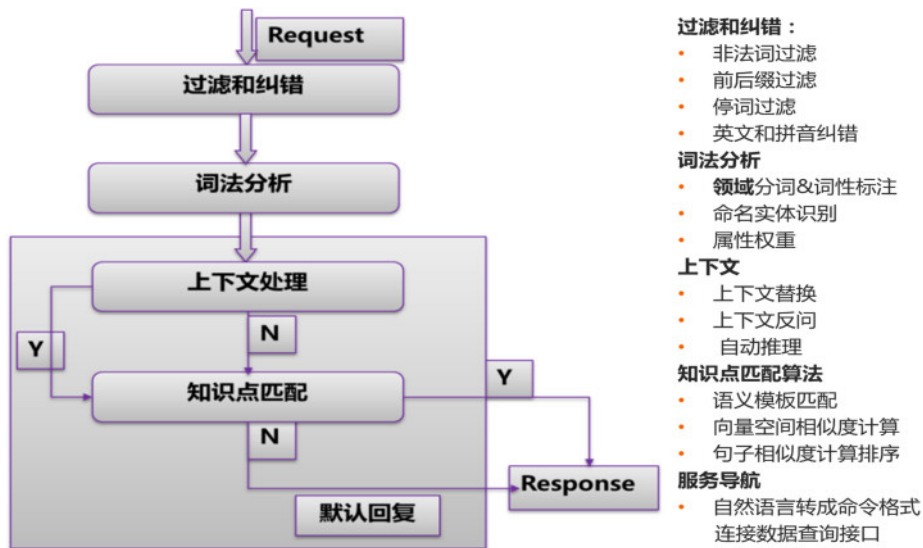
机器人核心模块及运行框架：

包括通讯控制模块、服务接口模块、交换业务逻辑及二次开发框架等组成部分。该平台主要实现全渠道终端与后端智能服务引擎及第三方服务系统（如人工客服系统）的通信接口服务，并且能够针对各渠道不同业务逻辑提供二次开发的接口。包括用户使用智能机器人系统的所有前端用户交互和表现功能，以及负责机器人的登陆验证，响应调度，负载均衡等。

智能服务引擎 AI

智能服务引擎是处理自然语言和集成各种专业处理引擎的基础平台，包括引擎核心模块、智能分词引擎、语义分析引擎、聊天对话引擎以及场景上下文处理模块、知识索引管理等模块。智能服务引擎相当于机器人的“大脑”，是机器人表现是否智能的关键，它的智能性、准确度、并发性能等各方面都会对整个系统产生关键影响。

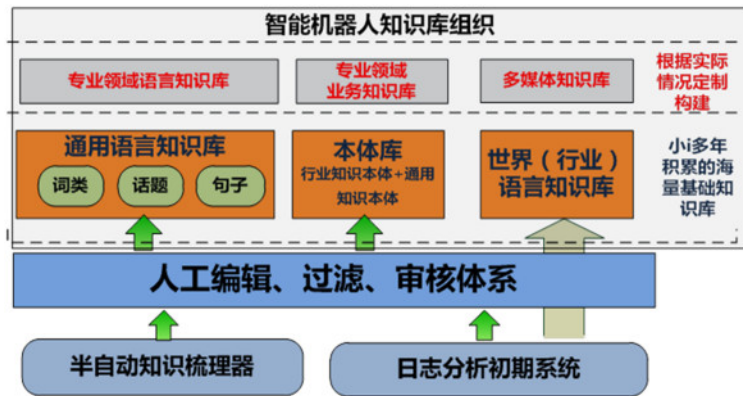
智能服务引擎的主要作用包括：文本处理，句法分析，语义分析，对话管理，句子匹配，答案渲染等。不同业务模型和应用场景可能会对智能服务引擎的处理过程及模块参数做调整，引擎的一般处理流程如下：



统一管理平台

通过智能服务引擎及机器人前端平台提供的 API，对机器人进行统一的管理及维护。包括知识管理、服务管理、渠道管理、语音管理、运维管理（日志和报表）和系统管理。

从工程化角度来看，支持智能客服应用的知识结构可分为业务知识库和语言知识库两个部分：通过语言知识库来理解以客户化语言组织的输入问题，通过业务知识库来定位理解后的问题所对应的答案内容。语言知识库包括通用词类、通用句型短语、领域专业词类、语义规则模板（集），以及语法停词、敏感词汇等辅助内容；业务知识库包括业务知识文档，如产品说明、业务介绍、营销活动规则，以及常见问题解答 FAQ 等。业务和语言知识库通过知识本体基类的属性进行关联，这两部分知识库缺少任一部分或构建不完善，都会影响到前端机器人的智能体验及问题解决率。知识组织结构如下图所示：



智能客服机器人可以通过多种渠道进行呈现和交互，包括微信、QQ、网页（Web）、手机 App（iPhone、Android）、电话等多种渠道，还可以通过标准接口（API）可以把语义理解能力提供给更多的人机交互渠道，语义库中的维度可以对应不同渠道接入的代码，可以同时支持不同渠道对回复内容的具体要求。



(3) 方案实施后的价值或成果

2015 年中国建行官方数据显示，由小 i 机器人提供技术支持的“小微”服务能力已经相当于 9000 个人工座席的工作量，远超 95533、400 人工座席的服务量总和。在招行，每天上百万次的交互量原来大约需要 2000-3000 人来服务，而引入 i 小机器人的智能客服机器人系统后，现在只需要 10 个左右的工作人员，且大部分工作是在提升客户粘性的创意工作上。

案例七：重点人群身份识别系统

应用领域：社会公共安全

应用场景：交通枢纽、商场、医院等公共场所

案例提供者：重庆凯泽科技股份有限公司

(1) 客户需求和方案简介

经过近 20 多年的建设，我国社会安全体系初具规模，较好地维护了我国的社会安定，但由于受到各种主客观因素的制约，治安防控体系建设还不能完全适应社会发展需要。众所周知，人口管理是我国社会管理的基础，公民身份的唯一性、准确性、权威性涉及国家各层面的安全。一些不法分子利用这些管理上的漏

洞，编造虚假身份信息从事不法行为或通过假冒信息躲避法律制裁，严重干扰了法律秩序，威胁着公众安全。为了维护社会稳定和国家安全，迫切需要有先进的高科技技术手段来快速、准确核实与鉴别相关人员的信息。同时公安人员在对通缉犯进行人工排查时如大海捞针，成功率极低，效果也不明显。主要有如下实际问题：首先，由于罪犯群体不断扩大，要在数以百万计的人员照片库中找出犯罪嫌疑人，不仅费时费力，还有可能造成遗漏等情况，破案的效率大打折扣；其次，目前公安机关侦察案件大多数仍然依靠事后追查和通缉，对已经发生的案件造成的损失很难有效弥补；最后，如果在案发的同时能防患于未然，就能第一时间将损失控制在最小范围内。

采用高效的人脸监控和比对系统，第一可帮助公安侦查人员快速识别并辨别特定人员真实身份，把过去难以想象的千万级的海量照片库比对需求变成现实，从而有效的为公安视频侦查、治安管理、刑侦立案等工作提供实战上的有效帮助和解决方法。第二可帮助公安侦查人员办案时候追查和通缉，真正从打变为防，能够极大的减少警力资源浪费和事故发生概率。

(2) 具体解决方案介绍

按照“统一规划、统一标准、统一平台、统一管理”的建设思路，在信息中心搭建软硬件运行平台，整合利用现有数据资源，采用业界先进成熟的人像比对识别技术，建立人像特征库，在信息中心建设面向全警的公安人像识别应用平台，并以分级授权、提供接口的方式，供全局各警种使用。

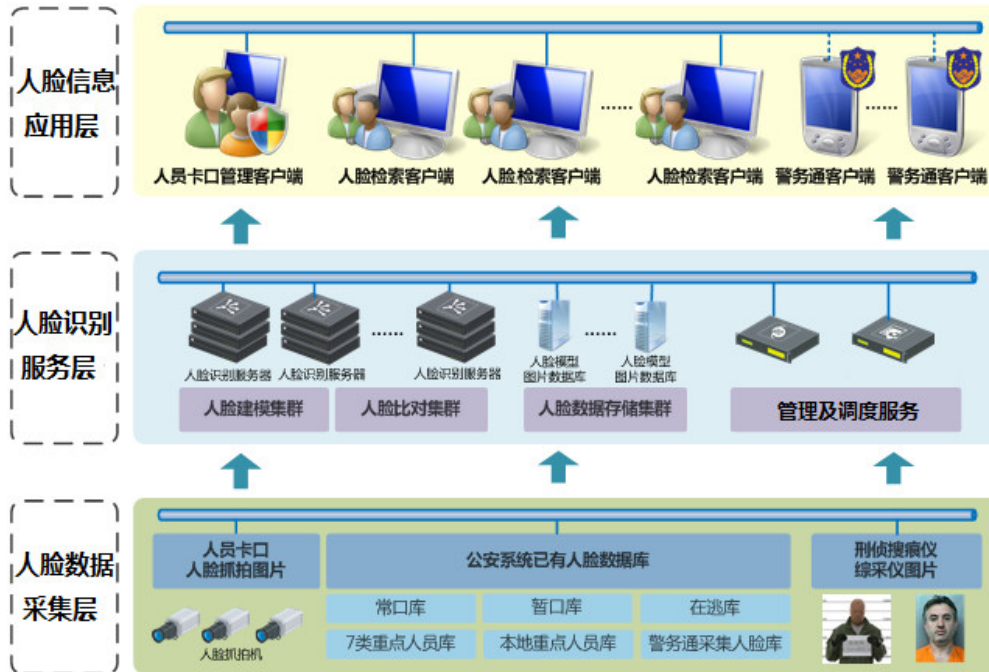
①设计一套高清人脸采集系统，实现高质量的人脸自动抓拍、自动识别、自动比对、自动报警、轨迹回放等功能，做到“人过留像、留特征、留轨迹”，实现“由像到人”、“由人到案”业务模式的改变和创新。

②在城市各主要场所人员进出通道合理设置高清人员卡口监控点，形成覆盖全部区域人员监控，实现严密的监控覆盖，全面记录城市出入及内部通行人员。

③依托公安图像传输专网，运用成熟的 SOA 体系框架，搭建人脸信息综合应用平台，实现全市人脸卡口数据的实时转发、统一存储、深入分析、深度应用。

④人脸信息综合应用平台与公安业务信息库建立连接，提供人脸布控及动态比对预警、人员轨迹追踪查询、人员身份鉴别查询等实战应用功能，为公安治安防控、刑侦破案、反恐防暴等工作提供有力支持。

系统主要包括人脸数据采集层、人脸识别服务层、人脸信息应用层。系统设备主要为前端摄像机、人脸检测服务器、人脸识别服务器、存储设备、人脸数据库、人脸识别系统平台六类设备。



硬件结构：



(3) 方案实施后的价值或成果

目前人脸抓拍比对系统主要应用在以下几个方面：

公安治安人员黑名单比对实时报警：

针对一些人员密集区域的关键出入口、通道等卡口位置布置人员卡口，后端对重点关注人员、打防控人员进行黑名单布控，通过实时视频流比对布控黑名单，

实现人脸比对识别。

不明身份人员身份确认：

治安人员在日常巡逻、人员身份验证过程中，避免肢体接触和冲突，使用前端摄像机或手机进行抓拍，后端通过数据库进行人员信息比对分析，达到人员身份确认的应用。

治安或刑侦人员对流动性人口中的无合法有效身份证件、无固定住所、无正当职业或合法经济来源的人员进行非接触性身份确认。

重要点位重点人员身份排查：

针对一些重要管控的区域，如大型保障活动，政府、公安出入口等布置前端摄像机对现场进行人脸抓拍，每日安排公安人员人工进行重点人员筛选排查。

案例应用成果 1：

①重庆市北城天街商业中心区域。

②由于商业中心区域人员聚集密度高，流动性大，期间可能面临各种个人或公共财物被盗窃的风险。因此，公安机关在现场对每个活动人员做人脸抓拍比对识别。

③将本地在逃人员、吸毒人员、有盗窃前科人员导入布控库，并启用人脸动态比对预警功能。

④通过人脸实时比对报警和人工确认，现场成功捕获并拦截了黑名单中的多名吸毒人员和有盗窃前科人员，有效提高了区域的安全级别。

案例应用成果 2：

①2014年12月5日7时20分XX便利店（A地点）发生盗窃案。

②2014年12月15日16时19分XX小区（B地点）发生入室盗窃案。

③通过分析两起案件，初步判断属于连环案，是同一伙人作案。

④通过调取A地点与B地点的人脸抓拍图片，进行区域碰撞分析，系统自动按相似度依次展示两个案发地点出现的相同人员。

⑤辅以人工筛选，发现张某某、李某某在案发时间期间都出现在案发现场附近，从而锁定确认了该犯罪团伙。

案例应用成果 3：

XX派出所接到精神病人走失报警，通过家属提供的身份信息和清晰数码照片，通过凯泽重点人群身份识别系统进行时空轨迹重现。

案例八：智能网络视频云服务平台

应用领域：互联网传媒产业

应用场景：视频识别、视频推荐、社交传播、视频营销

案例提供者：北京爱奇艺科技有限公司

（1）客户需求和方案简介

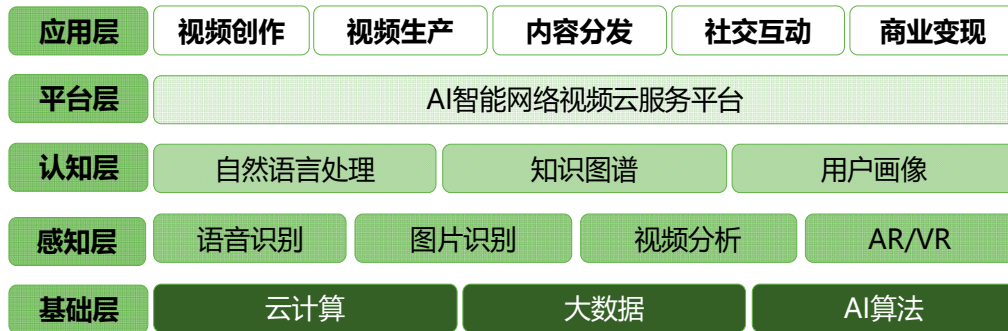
近年来，互联网视频产业发展迅猛，成为用户规模最大的网络服务。据中国互联网信息中心 CNNIC 第 40 次中国互联网统计报告，中国网络视频用户达到 5.65 亿，占网民总数的 75%。随着用户数目逐年增长，视频内容数量呈指数级增长。作为国内最大的网络视频分享平台，爱奇艺每天处理上万小时的新增视频，产生千亿条的用户日志。海量信息内容孕育着更多的价值，也为网络视频行业发展提出新的挑战。首先，面对海量的内容，视频平台急需优化生产和审核流程，提高内容生产的效率，为用户提供更加便捷、流畅的内容服务。其次，用户面对过载的信息海洋，选择成本太高，平台需要挑选和推荐用户最感兴趣的优质内容。再次，粗放投放为企业带来高额营销成本，迫切需要精准的广告投放和精细化的商业运营。

本项目依托爱奇艺在互联网视频行业的深厚积累，上线功能比较完备的智能网络视频云服务系统，可自动对视频进行智能识别处理，大幅度提高生产效率；并通过智能算法对用户行为大数据进行分析，产生用户画像，提供精准的个性化搜索推荐；最后，系统支持商业合作伙伴进行精准营销和广告投放，通过闪植和随视购技术，创新性地打通了电商系统和视频系统，实现“视频内物品所见即所买”的精准投放。

（2）具体解决方案介绍

爱奇艺智能网络视频云服务平台架构包括基础层、感知层、认知层、平台层和应用层。基础层提供 AI 服务所需的算力、数据和基本算法，极大地降低了对本地硬件设备和软件系统的要求，运维成本和风险。感知层模拟人的听觉、视觉，实现语音识别、图片识别、视频分析，AR/VR 配准渲染等功能。认知层模拟大脑的语义理解功能，实现自然语言处理、知识图谱的记忆推理和用户画像分析等功能，构成爱奇艺大脑。平台层通过开放服务接口，为视频创作、视频生产、内容分发、社交互动、商业变现等上层应用赋能。其中最主要的应用系统为智能视

频生产系统，智能内容分发系统和智能商业变现系统。爱奇艺智能网络视频云服务平台架构图，如下所示。



智能视频生产系统

智能视频生产系统依托音、视频智能识别技术，实现基于内容的视频拆条、视频标注和视频审核。爱奇艺自主研发 CNN 卷积神经网络深度学习技术进行高精度明星识别、情感识别、物品识别、场景识别，基于 BLSTM 网络的视频字幕识别、语音识别，获得视频编目的语义标注和封面图。

不断增加的海量视频内容，对审核速度和准确性都提出了更高的要求。智能审核系统研发了基于音视频指纹的快速版权检测，基于黑白名单、CNN 网络的情色检测等关键技术。通过对视频中文字、人体、露点、枪声、烟火、人群聚集等自动检测功能，利用深度学习加强对非法广告、黄色、暴力图片的训练和识别，极大地提高人工审查的效率，维护了健康良好的视频环境。

智能分发系统

在智能传媒时代，每个用户既是内容的消费者，也成为了内容的创造者。这些海量的内容在满足了用户需求的同时，也使寻找所需内容更加困难。在这种情况下，智能分发系统应运而生。智能分发系统是在大数据分析和人工智能技术的基础上，通过研究视频内容和用户的兴趣偏好，进行个性化推荐；通过社交网络宣发和热点发掘，给用户提供更高质量的个性化内容，解决信息过载问题，更好的服务用户的需求。

爱奇艺智能推荐系统的各个模块作用如下：

①用户画像：包含用户的人群属性、历史行为、兴趣内容和偏好倾向等多维度的分析，是个性化的基石；

②特征工程：包含了视频类别属性、内容分析、人群偏好和统计特征等全方位的描绘和度量，是视频内容和质量分析的基础；

③召回算法：包含了多个通道的召回模型，比如协同过滤、主题模型、内容召回和 SNS 等通道，能够从视频库中选出多样性的偏好内容；

④排序模型：对多个召回通道的内容进行打分排序，选出最优的少量结果。

除此之外，推荐系统还兼顾了推荐结果的多样性，新鲜度，深度和惊喜度等多个维度，更能够满足用户多样性的需求。

此外，爱奇艺开创了视频社交的先河，研发爱奇艺泡泡社区聚拢相似爱好的用户群体“圈子”分享互动，并宣发内容。圈子的类型有多种（明星圈、视频圈、兴趣圈、游戏圈、漫画圈、图书圈等等），不同类型的圈子也有不同的玩法，比如明星圈可以做积分任务、追踪明星的行程信息等；视频圈里面可以直接看视频等。每个圈子下面汇集了用户自发、编辑运营的相关内容（Feed 流），以及相关圈子的周边信息。通过用户的观看、分享和评论数据，可以智能分析舆情、发掘热点事件，进一步在不同的用户群体中，宣发用户感兴趣的相关内容。

智能商业变现系统

智能商业变现系统利用人工智能技术充分挖掘视频内容价值，包括闪植广告、随视购广告、智能票房预测等系统。通过大数据分析，对于用户浏览、点击、购买等行为进行统计和监测，可以进行用户群体定位和商品的流行性预测，更好的指导商家用户生产市场用户需要的流行商品，及时调整广告的投放策略，促进电商交易。

闪植是首创的视频植入营销方式。根据影视场景进行内容植入，充分保障植入物品的摆放位置、角度、光照等视觉效果，并保持原场景的一致性。随视购是爱奇艺基于视频内容相关的广告推荐系统。该系统通过视频解析技术检测视频镜头和关键帧，然后使用先进的 CNN 卷积神经网络深度学习技术自动检测和识别视频内的物品场景，为视频打上带时间的物品或场景标签。最后通过基于知识图谱的关键字映射推导和统计过滤，输出稳定可靠的广告物品标签。这样，当互联网用户观看影视剧时，广告推送引擎能够自动的将与当前视频内容相关的角标广告以动态的方式展示到视频画面中，吸引用户关注和购买。例如，基于内容关联的爱奇艺随视购广告可识别电视剧画面并推送同款的女包商品和利用 OCR 字幕识别技术推送电视剧台词相关的手游商品等。

智能票房预测系统利用深度学习技术，根据剧集信息、演员、搜索指数和社交关注等数据，预测电影和电视剧的收视率和票房，辅助投资者在版权采购和内

容创作中进行精准判断，降低前期投入风险，并提高投资回报率。

(3) 方案实施后的价值或成果

智能视频生产系统极大提高了视频生产效率，视频数量从 2014 年到 2017 年增长了约 20 倍，但员工人数仅增长约 2 倍。爱奇艺精彩片段的剪辑通过 AI 技术的生产效率提升 2.5 倍。封面图生成通过 AI 技术实现全自动生成，每天为几十万 UGC 视频(用户生成视频)自动生产封面图。情感识别技术则首次将 C3D 和 RNN 模型应用到情感识别领域中，准确地捕捉表情时序变化，协助发掘视频中的精彩片段。

智能内容分发系统建立了精准的用户画像，使用 AI 技术赋能个性化搜索推荐，进行高效内容分发。爱奇艺全网搜索涵盖高达 5 亿全网视频内容，是业界领先的全网视频搜索引擎。目前高峰搜索量突破 3 亿，整体日导流量突破 4 亿。智能推荐整体导流超 6 亿，占总流量约 30%，长视频猜你喜欢、短视频联播效果达到行业第一。爱奇艺泡泡社区是中国最大的视频社交平台，目前高峰 DAU 接近 7 千万。

智能商业变现系统打通了内容生产、人机交互和电商服务的各个层面，增加了爱奇艺作为网络视频平台的广告和商业价值。爱奇艺基于机器学习的多时间窗口预测中，电影票房预测，提前半年方差准确率高达 77%；电视剧流量预测方面，提前半年到一年的方差准确率高达 88%，为投资采购、广告、营销提供有力支持。闪植和随视购广告在《虎妈猫爸》《老九门》《中国有嘻哈》等剧集中大量播出，在不影响用户观看的同时，精准投放了视频内容相关的广告，实现文化产业和电商的共同增长，促进文化与科技的深度融合。

总结来看，本案例逐步探索基于人工智能+传媒产业的新模式，对整个网络视频行业的发展有着良好的示范作用。基于智能识别的互联网视频云服务系统，为内容生产方、用户、商业合作伙伴提供强大的服务平台，引领网络视频行业进入一个健康、可持续发展的新时代。

案例九：中移动人证比对实名认证

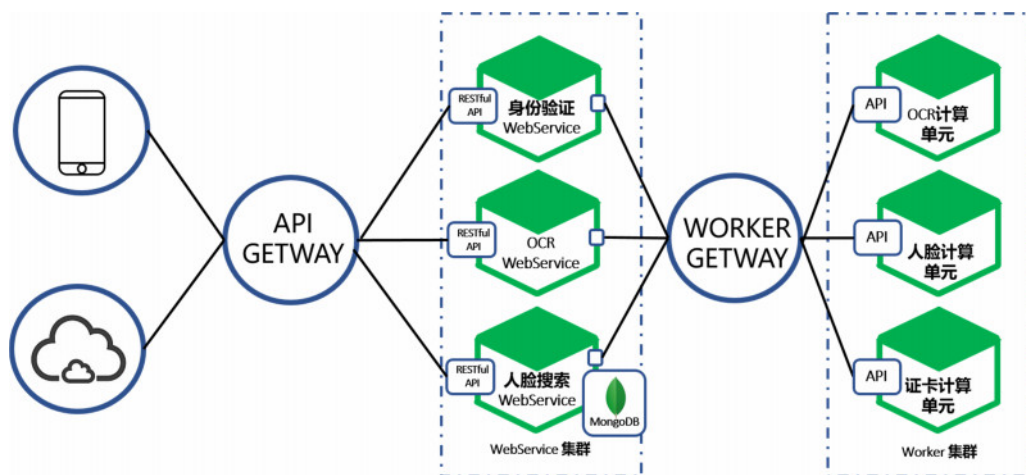
应用领域：用户实名化，自动人证对比人证

应用场景：大规模人脸识别，人证对比，OCR 识别

案例提供者：商汤科技开发有限公司

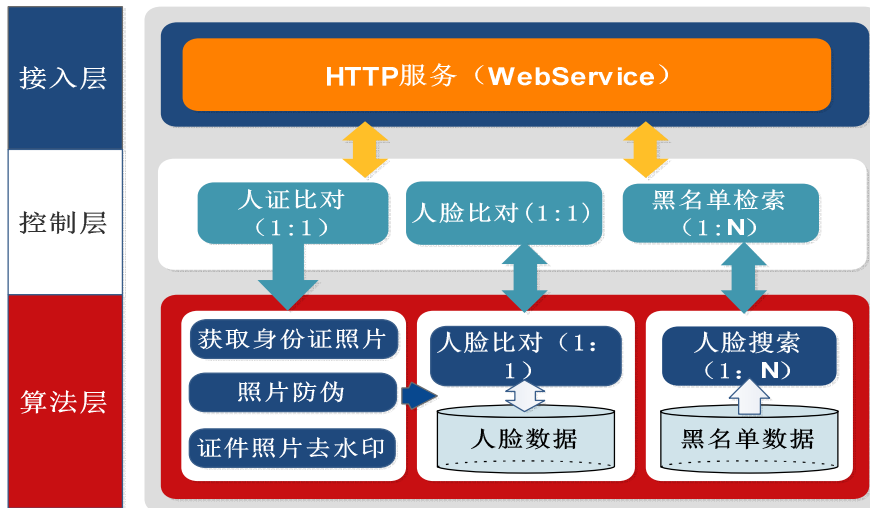
(1) 客户需求和方案简介

在中国移动 8 亿用户进行账户注册或者首次进行重要业务之前，需要用某种途径对用户身份进行核实，以保证产品操作者所关联的实际个人身份真实无误且确实对应实际用户本人，并将此作为保障后续业务展开的基础。用户在进行实名认证时，需要提供本人的照片，个人身份信息（身份证号/姓名等）以及其他相关信息供业务后台进行核对。同时后台需要基于身份信息获取其他权威信息（比如公安部照片），并对各类照片信息进行交叉核验。由于用户数量众多（8 亿），所以身份核验中的所有步骤都需要自动进行，包括人脸识别和身份证 OCR 识别，以代替人工核验人脸和手工录入身份证，软硬件架构图如下所示。



(2) 具体解决方案介绍

前端身份证识别并采集自拍照，在私有云服务做人脸比对和身份核验，支撑移动的在线实名制补登记业务，覆盖全国 8 亿用户以及大多数线上线下渠道。人脸验证后端服务架构图如下。



项目实施过程中，提供了图片预处理组件、人脸检测组件、人脸比对组件以及身份证 OCR 组件，评测后的性能指标均大大超过合同原定目标。以手持证件照判断组件为例，通常合同上要求鉴别准确率达到 90%，而商汤科技研究员根据实际业务数据两次优化后的算法，准确率达到了 97.3%。身份证号的识别正确率（整行号码，而不是单个字符）高达 99.6%。

(3) 方案实施后的价值或成果

商汤科技为中国移动在线服务公司提供的人证比对系统，通过人工智能技术识别用户身份证信息，并判断用户上传带头像与用户证件照片是否为同一人。在项目招标过程中，商汤科技在核心组件性能、整体技术方案以及支撑能力等方面从众多供应商中全面胜出，成为该运营商选择的合作对象。其中商汤科技的人脸识别与认证方面的技术指标更是遥遥领先市场同类产品。同时，商汤科技在系统中配套提供了自主研发的基于深度学习的图像处理技术，对照片进行自动朝向纠正、质量增强，以及对环境、光照、成像质量等干扰因素智能处理，并提供专有的证件照清晰化处理技术，保障了识别的高准确性。该系统上线运行以来，覆盖了全国 28 个省的移动用户，将中国移动实名制登记业务中核验用户人证一致性的百分之九十以上的工作交由机器自动处理，并将之前人工审核每分钟只能核对约一人的处理效率提升了上百倍。

案例十：COSMOPlat 工业互联网平台-人工智能与制造业融合创新

应用领域：工业制造领域

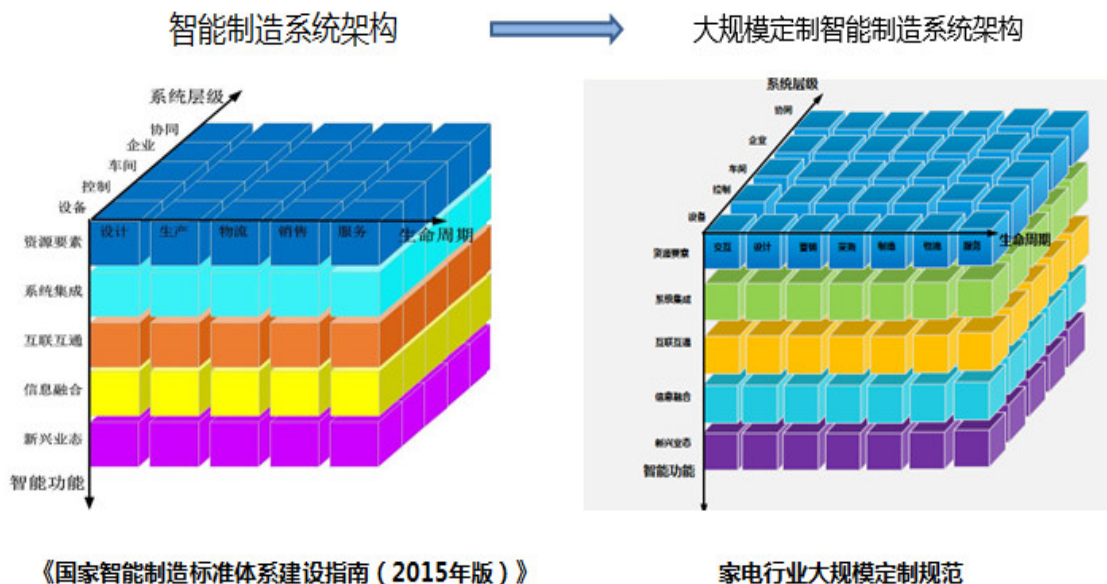
应用场景：智能制造、智能产品

案例提供者：海尔工业智能研究院

(1) 客户需求和方案简介

在中国制造 2025 的战略指引下，海尔自主创新，打造了具有自主知识产权的工业互联网平台—COSMOPlat，是物联网模式下以用户为中心的共创共赢的多边平台。海尔 COSMOPlat 平台可以为离散型制造企业提供智能制造和资产管理解决方案。通过物联网技术，实现人机物的互联协作，包括设备、人员、流程、工厂数据的接入和监测分析，满足不同企业信息化部署、改造、智能升级需求，实现大规模定制的高精度与高效率。海尔 COSMOPlat 平台通过设备资产数据的实时采集，对资产在线实时监测和管理，并根据资产模型和运行大数据，优化资产效率。例如可采集设备实时数据，结合设备机理分析和建模，实现了预测性维护，提升效率降低成本。

下图为海尔大规模定制智能制造系统架构。



(2) 具体解决方案介绍

海尔 COSMOPlat 平台智能制造解决方案运用了各种智能化技术，构建了用户交互、研发、采购、制造、物流、服务等 7 个应用模块，实现高精度的产品创新服务和高效率的智慧生产服务。COSMOPlat 平台中的所有服务依托海尔提出的互

联工厂实现以用户个性化需求为中心的家电产品的混合柔性生产。海尔互联工厂以 COSMOPlat 平台为核心，采用智能化、数字化、柔性化的设计理念，通过与 COSMOPlat 平台的无缝连接，不仅实现了冰箱、洗衣机等网器产品从个性化定制、远程下单到智能制造的全过程，同时也实现了智能产品和智能制造全流程的无缝连接。

海尔智能化互联工厂

海尔智能化互联工厂包含用户定制、模块智能拣配、柔性装配、模块装配、智能检测、定制交付等多个智能单元，集成了 COSMOPlat 平台、虚实融合双胞胎系统、RFID、智能相机、双臂机器人、AGV、网络安全等多种智能技术。用户可以应用众创汇、HOPE 等在线交互设计平台，自主定义所需产品，平台整合需求并达到一定需求规模后，形成用户订单，同时引进一流资源在线开展虚拟设计，订单可直达工厂与模块商，驱动全流程并联，自动匹配所需模块部件，通过工厂 AGV 与空中积放链等智能物流系统实现模块立即配送和按需配料，并全流程追溯和可视化制造过程信息数据（制造过程数据及网器大数据），针对 VIP 和紧急用户订单还提供智能插单功能。此外，虚实融合双胞胎系统既可以离线仿真所有生产流程，也可实时动画显示现场设备的运行状态和订单数据。

海尔产品智能化

海尔 U+智慧家庭平台打造了全球首个物联网智慧家庭领域行业解决方案，以海尔智慧家电产品为载体，通过底层及应用层协议打通，以及接口的开放，提供了多入口、全场景的智能家居解决方案，海尔 U+智慧家庭平台是一套智能操作系统，能够理解用户需求、主动提供服务，以家庭用户为中心，串联“人”、“家电”、“服务”三张网，赋能家电，为终端用户提供全场景智能服务。例如，海尔智能物联网洗衣机，能自动辨别衣物面料、添加和购买洗涤剂，用户仅需要将脏衣物放入洗衣机，洗衣机便可以智能判断、自动完成整个洗衣流程；海尔智能冰箱不但可以与手机实时无缝互联，也可以通过门外的触摸屏，查看冰箱内部存储的食材，浏览图片，观看视频、查找食谱等，还可以与其它家电产品互通互联，比如买回一块牛排，可以为用户提供烹饪菜谱，并发送到燃气灶具，用合适的温度进行烹饪，烟机随着灶具自动控制风量大小，烹饪全程无需人工干预，让用户更专注于烹饪过程，洗碗机也自动选择合适的程序和水温对用餐后的餐具进行清洗。海尔的智能家电产品还包括智能控制浴室的浴霸、排风扇、灯光等多个

设备，用户开门进入/关门走出浴室后，浴室的灯会自动开启/熄灭；当检测到浴室温度低于洗浴所需的舒适温度时，就会提前启动浴霸；当检测到浴室内水汽过多时，就会自动开启排风扇等。海尔 U+智慧家庭平台已经在家电、家具、家装、医疗、安防、机器人、通讯等七大领域实现推广落地，推动企业从“硬件制造”到“硬件+软件+服务”的物联网生态转型，为物联网时代下的创新变革带来新模式。

(3) 方案实施后的价值或成果

海尔用户场景大数据与制造数据融合，促进了产品迭代和体验提升。用户数据与生产数据互联互通，实现智能化生产。例如，COSMOPlat 云平台搜集微博、微信、搜索引擎及其他途径的用户需求，发现用户对所有品牌空调的各类需求问题，通过数据分析挖掘分析出空调声音为主要问题。空调声音主要包括噪音和异音，噪音可通过分贝辨别，而异音有千万种，COSMOPlat 平台依托大数据和人工智能技术自主学习辨别异音和自动管控，提升辨别的精准度，聚焦噪音问题后，可追溯生产过程，通过生产过程大数据，分析出导致异音的原因（包括空调风扇安装不良、电机安装不良或者骨架模块毛刺等原因），进而总结出改善异音的关键措施，提前预防，改善用户体验。

海尔 COSMOPlat 平台旨在推动企业智能化转型升级和人工智能与制造行业融合创新，构建新型企业组织结构和运营方式，形成制造与服务智能化融合的业态模式，实现大规模定制。在 COSMOPlat 平台的效应下，产品生产效率和产品不入库率得到了提升。同时 COSMOPlat 是“企业和智能制造资源最专业的连接者”，在服务内部互联工厂的同时，也为制造业企业转型升级提供解决方案和增值服务，让企业自身具备持续提升大规模定制的能力，满足用户的最佳体验。



START YOUR FINANCE



起点财经，网罗天下报告