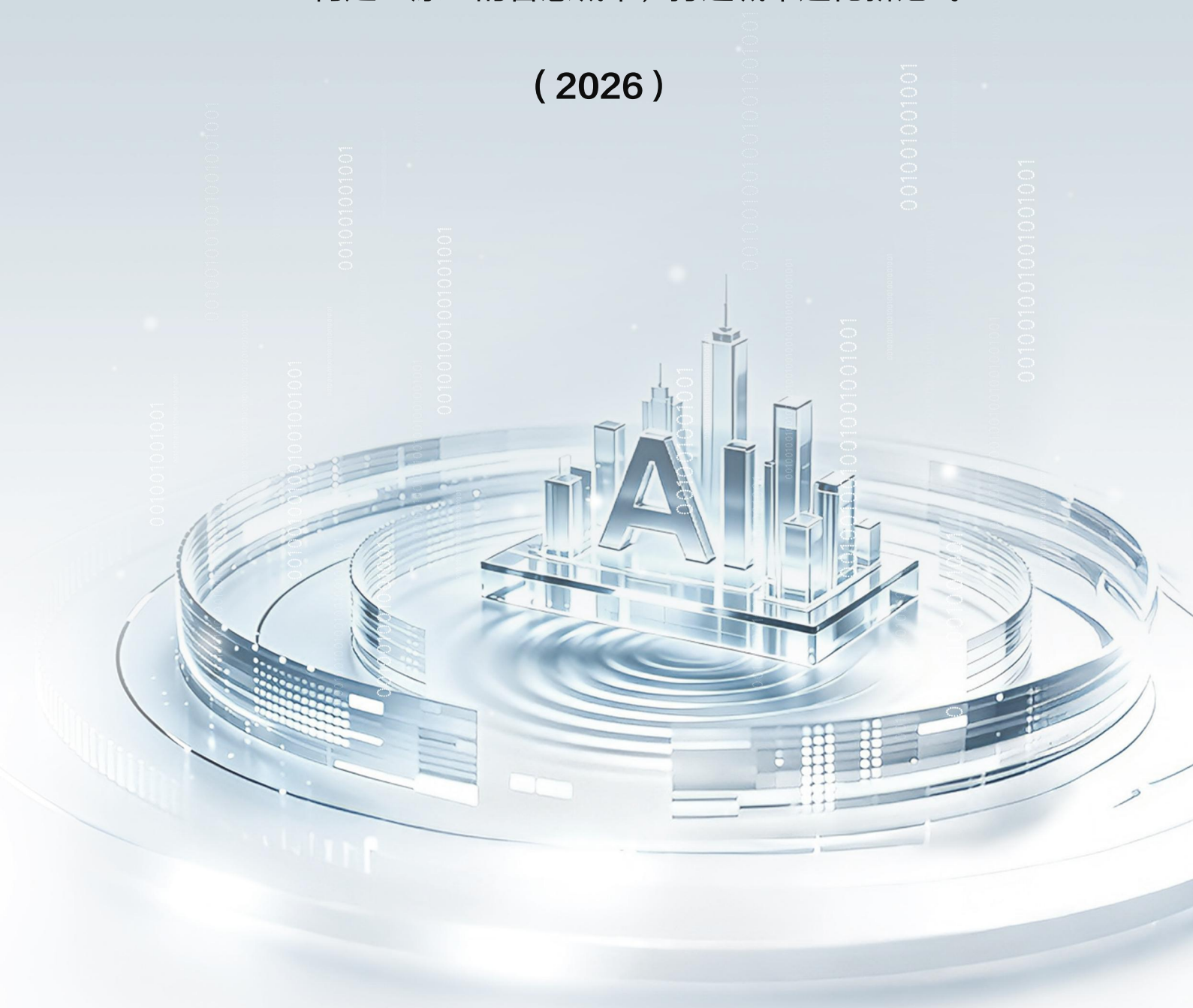


AI CITY发展研究报告

—— 构建AI原生的智慧城市，打造城市进化新范式

(2026)



编写委员会

(排名不分先后)

主编

单志广 周跃峰 杨瑞凯 吴 刚

专家顾问

胡玉海 孙承奎 肖 霏 曹 俊 赵英杰 王旭东 邹思轶 罗 杰

副主编

房毓菲 王丹丹 涂菲菲

李志强 周春燕 孔 砚

编委 (按姓氏拼音排序)

蔡旦旦 常苗苗 陈 栩 戴 彧 胡沐华 李春香 刘 殷 刘舒扬

舍日古楞 吴洁倩 徐清源 闫晓丽 张 岳 赵文景

白 霄 陈坚钦 陈 勇 崔 昊 杜 甫 郭文龙 韩 伟 韩 辉

黄文涛 华 璐 李 兵 李 倩 李 伟 李浩楠 李承羲 陆 晨

毛 瑞 沈 阳 沈放之 汤 凯 王艾军 吴著冠 邢云龙 余 琛

尉鹏程 赵永明 赵 峤 张守伟 郑建宇 郑志毅 钟福明 左 悦

特别鸣谢

武汉市城市运行管理中心

耿 峰

深圳市龙岗区政务服务和数据管理局

席 炜 叶 青

深圳市气象局 (台)

兰红平 陈训来 夏 昕

克拉玛依市数字化发展局

臧奕茗

武汉云计算科技有限公司

钟收成 孙 进

华智 (无锡) 人工智能科技有限公司

陈 卿 李 玮 谢 娟

主编单位

国家信息中心

华为云计算技术有限公司

序言

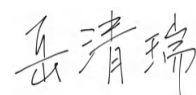
习近平总书记指出，要“运用大数据、云计算、区块链、人工智能等前沿技术推动城市管理手段、管理模式、管理理念创新”，要“以建设创新、宜居、美丽、韧性、文明、智慧的现代化人民城市为目标”，“顺应数智化趋势，创新治理理念、模式、手段，强化科技支撑，不断提升城市治理智慧化精细化水平”。

当前，人工智能技术演进重心正从“预测下一个词”的数字文本生成，升级为“预测世界下一个状态”的物理世界认知。技术发展从单点模型迭代走向全域落地应用，算力体系持续夯实、智能体技术日趋成熟，推动人工智能从数字对话工具，转变为赋能实体场景、驱动全域进化的核心技术底座。

历经多轮技术狂飙突进，人工智能正以不可逆的态势，重塑人类经济社会发展格局。在经济领域，全球 AI 产业竞争焦点脱离单一的大模型参数比拼，转向算力供给韧性、智能体落地深度、产业生态完备度与成本效率的综合实力角逐。智能技术渗透实体产业，持续重构生产、流通、服务全链条，加速产业提质增效与转型升级。在社会领域，人工智能从数字世界的交互工具，转变为改造物理世界的重要力量，催生出人机协同、虚实融合的全新社会运行模式。随着智能体技术的规模化落地，通过自主拆解复杂任务、联动调度各类工具、闭环完成执行与迭代优化，能够高效整合城市资源、串联碎片化场景、精准匹配多元需求。同时，智能体与人的主观决策、创新研判、人文服务能力形成深度互补，持续提升社会运行智能化水平。

当 AI 已成为产业变革的底层驱动力，当智能体拥有了改变现实世界的能力，城市的建设范式将会如何演进？AI CITY 理念给出的回答是：以 AI 原生逻辑重新审视城市的一切。它不是传统智慧城市的升级补丁，而是建设集约化、能力服务化、结果价值化、生态多样化、资产轻量化的系统性重构。这种重构关乎城市能否在 AI 时代持续释放创新活力，引领城市数智化转型的全新方向。

本报告紧扣全球新一代信息技术变革的时代背景，聚焦城市发展由“数字化”迈向“数智化”转型的核心课题，系统拆解 AI CITY 的核心架构、应用价值与生态体系，为我国城市落实“人工智能+”行动指明路径，擘画高质量发展蓝图。



中国工程院院士 北京科技大学城镇化与城市安全研究院院长

目录

第一章 战略形势： AI CITY 从“远景图”变为“施工图” 1

 (一) 政策导向：从全域转型到 AI 原生，AI 赋能城市进入落地新阶段2

 1、国家不断推进政策部署，全面加速 AI 赋能城市转型 2

 2、多地出台落地方案，推进城市智能化升级 8

 (二) 技术趋势：从联接智能到整体智能，全栈 AI 技术重构城市智能底层逻辑9

 1、智能体：重构人机协作的新一代交互入口 9

 2、城市公共云：承载智慧城市服务能力的核心载体 10

 3、算力网：从“东数西算大布局”到“以城市为核心”新转型 11

 4、端侧 AI 互联：城市全域智能协同的核心支撑 13

 (三) 发展需求：智慧城市走向高质量高价值智能服务新阶段 14

 1、智能社会新形态催生城市发展新要求 14

 2、传统智慧城市管理机制和建设运营模式面临挑战 14

 3、AI CITY 发展已进入实效比拼的阶段 15

第二章 概念模型： 城市进化新范式：AI 原生的高价值城市智能服务 16

 (一) AI CITY 核心理念：“城市超级智能体”提供 AI 原生的高价值城市智能服务 17

 (二) AI CITY 建设要点 19

 1、建设集约化 19

 2、能力服务化 19

 3、结果价值化 19

 4、生态多样化 20

 5、资产轻量化 20

第三章 体系架构： 全栈智能的 AI CITY 架构体系 21

 (一) 参考框架 22

 (二) 城市公共云体系 23

 1、功能定位 23

 2、部署形态 25

 3、技术架构 26

 (三) 数据体系 30

 1、功能定位 30

 2、多模态数据底座 31

 3、数据一站式开发治理平台 34

 4、可信数据空间 39

 (四) 模型体系 43

 1、功能定位 43

 2、模型分类 44

 3、MaaS 模型即服务 46

4、模型一站式训推平台	48
(五) Agent 体系	52
1、功能定位	52
2、智能体一站式开发与运行平台	53
3、多智能体协同	56
4、智能体监管	58
(六) 数智专业服务体系	61
1、功能定位	61
2、AI Infra 专业服务	62
3、数据专业服务	62
4、模型专业服务	63
5、智能体专业服务	64
(七) 保障体系	66
1、AI 安全	66
2、AI 运维	69
第四章 建设指引： 标准化、可迭代、可持续的 AI CITY 落地路径	74
(一) 分步推进策略	75
1、夯实基础支撑：筑牢算力、数据、模型三要素	75
2、突出关键能力：打造统一入口与城市级知识库	76
3、注重利旧衔接：做好与既有数字政府体系融合升级	77
(二) 生态建设指引	78
(三) 运营模式	82
1、优化综合服务运营	82
2、健全协同运营机制	82
3、创新 Token 运营	82
(三) 人才培养服务	83
(四) 标准体系	84
(五) 评价导向	84
1、基础能力评价导向	84
2、应用实效评价导向	85
第五章 华为落地实现	87
(一) 克拉玛依城市超级智能体	88
(二) 武汉超大城市治理智能体	93
(三) 上海国地中心具身智能实训场	100
(四) 无锡 AI CITY 具身智能与产业焕新	104
(五) 深圳龙岗“龙小二”AI 原生城市治理智能体	108
(六) 深圳市气象大模型	111
(七) 武汉医保影像云	115
结语	118

第一章 战略形势：

AI CITY 从“远景图”变为“施工图”



(一) 政策导向：从全域转型到 AI 原生，AI 赋能城市进入落地新阶段

1、国家不断推进政策部署，全面加速 AI 赋能城市转型

习近平总书记对人工智能赋能城市发展多次做出指示和部署，在 2018 年中央政治局集体学习时指出，要“推进智慧城市建设，运用人工智能提高公共服务和社会治理水平”；在 2020 年考察浙江时指出，“运用大数据、云计算、区块链、人工智能等前沿技术推动城市管理手段、管理模式、管理理念创新，从数字化到智能化再到智慧化，让城市更聪明一些、更智慧一些，是推动城市治理体系和治理能力现代化的必由之路，前景广阔”；在 2025 年中央城市工作会议上指出，要“建设创新、宜居、美丽、韧性、文明、智慧的现代化人民城市”，“坚持以城市居民需求为导向，顺应数智化趋势，创新治理理念、模式、手段，强化科技支撑，不断提升城市治理智慧化精细化水平”。

近年来，党中央、国务院出台多项有利于 AI CITY 建设与发展的政策，从城市数字底座、云服务、智能体、“人工智能+”应用等不同角度持续完善政策部署，提出了更加细化和实化的指引。

(1) 推动统筹集约建设城市数字底座

党中央、国务院持续强化人工智能与城市全域数字化转型的统筹部署。以城市智能中枢和城市数字底座为核心载体，统筹推进数字基础设施集约建设和一体化管理，强化城市算力网、城市智能感知终端、可信数据空间、城市大模型、CIM 等共性能力建设。

表 1 城市数字底座相关政策

时间	文件名称	相关内容
2024 年 5 月	国家发展改革委等四部门《关于深化智慧城市发展推进城市全域数字化转型的指导意见》（发改数据〔2024〕660 号）	构建统一规划、统一架构、统一标准、统一运维的城市运行和治理智能中枢，打造线上线下联动、服务管理协同的城市共性支撑平台。统筹推进城市算力网建设，实现城市算力需求与国家枢纽节点算力资源高效供需匹配，统筹部署泛在韧性的城市智能感知终端。

时间	文件名称	相关内容
2024 年 11 月	国家数据局《可信数据空间发展行动计划（2024—2028 年）》（国数资源〔2024〕119 号）	支持有条件的地区开展 城市可信数据空间 建设，发挥公共数据资源的引领作用，推动公共数据、企业数据、个人数据融合应用，构建城市数据资源体系，支撑城市建设、运营、治理体制改革。打造城市级 可信数据流通服务生态链 ，加快城市全域数字化转型。
2024 年 12 月	国家发展改革委、国家数据局、工业和信息化部《国家数据基础设施建设指引》（发改数据〔2024〕1853 号）	构建多元异构、高效调度、智能按需、绿色安全的高质量算力供给，鼓励创建 城市可信数据空间 ，支持基础好、有条件、意愿强的行业和城市，先行先试数场建设。
2025 年 3 月	《智慧城市城市智能中枢参考架构》（GB/T45402-2025）	“ 城市智能中枢 ”是综合应用新一代信息技术，融合城市多源数据资源，整合状态感知、建模分析、城市运行管理、应急指挥等功能，通过人机交互与协同，提供态势全面感知、趋势智能研判、协同高效处置、调度敏捷响应、平急快速切换等智能化服务，提升城市精准精细治理水平，支撑城市数字化转型的一种复杂系统。
2025 年 8 月	国务院《关于深入实施“人工智能+”行动的意见》（国发〔2025〕11 号）	开创社会治理人机共生新图景，有序推动市政 基础设施智能化 改造升级，探索面向新一代智能终端发展的城市规划、建设与治理，提升城市运行智能化水平。
2025 年 10 月	国家发展改革委等五部门《深化智慧城市发展推进全域数字化转型行动计划》（发改数据〔2025〕1306 号）	建设城市数字基础设施，集约建设感知、网络、算力等基础设施，实现城市“物联、数联、智联”。完善 城市智能中枢 。加强人工智能公共服务能力建设，探索集约构建多模融合的 城市大模型 ，打造 城市智能体 应用。鼓励超大特大城市有序推进 人工智能赋能全域转型 。
2026 年 5 月	国务院《城市更新“十五五”规划》（国发〔2026〕12 号）	城市全域数字化转型，建设城市信息模型（CIM）基础平台，打造集约统一、数据融合、高效协同的 城市数字底座 。完善 CIM 基础数据库和标准体系，丰富拓展“CIM+”在城市更新中的应用场景。

（2）积极发展智算云、公共云服务

党中央、国务院将智算云、公共云作为提升算力普惠供给能力、支撑人工智能规模化应用的重要抓手。通过统筹建设多层次算力设施，完善全国一体化算力监测调度和算电协同机制，积极发展标准化、可扩展的**智算云、公共云服务**。结合边缘算力和行业场景需求，逐步构建资源高效调度、供给弹性灵活、服务普惠便捷、云边端协同的云服务体系。

表 2 智算云、公共云服务相关政策

时间	文件名称	相关内容
2026 年 1 月	工业和信息化部等八部门《“人工智能+制造”专项行动实施意见》（工信部联科〔2025〕279 号）	开展 智算云服务 试点，推动大模型一体机、边缘计算服务器、工业云算力部署，提升智算资源供给能力。
2026 年 3 月	国务院《政府工作报告》（2026 年 3 月 5 日，十四届全国人大四次会议）	实施超大规模智算集群、算电协同等新基建工程，加强全国一体化算力监测调度，支持 公共云 发展。
2026 年 3 月	《中华人民共和国国民经济和社会发展第十五个五年规划纲要》	建设新一代超算、通算、智算设施体系，积极发展 公有云服务 。加快国家枢纽算力设施集群建设，支持有条件地区根据低时延场景需求适度发展算力，推进 云边端 协同发展。创新发展标准化可扩展的 智算云服务 。
2026 年 4 月	国务院《关于推进服务业扩能提质的意见》（国发〔2026〕7 号）	发展数据标注、认证等专业服务，探索建立分类分级的数据确权、评估、定价机制。有序推进算力布局与边缘算力建设，完善 智算云服务 体系。

(3) 鼓励打造领域智能体

党中央、国务院立足新一代人工智能发展全局，将智能体作为人工智能落地应用的核心载体与关键形态，坚持安全可控、规范有序、创新驱动、场景牵引的发展原则，聚焦民生服务、城市治理、数字经济等重点领域，持续推动智能体技术迭代、产品创新与场景落地，鼓励各行业打造专业化、场景化领域特色智能体，全面助力经济社会数智化转型。

表 3 领域智能体相关政策

时间	文件名称	相关内容
2024 年 7 月	工业和信息化部等四部门《国家人工智能产业综合标准化体系建设指南（2024 版）》（工信部联科〔2024〕113 号）	规范以 通用大模型 为核心的 智能体 实例和智能体基本功能、应用架构等技术要求，包括智能体强化学习、多任务分解、推理、提示词工程，智能体数据接口和参数范围，人机协作、智能体自主操作、多智能体分布式一致性等标准。
2025 年 8 月	国务院《关于深入实施“人工智能+”行动的意见》（国发〔2025〕11 号）	在软件、信息、金融、商务、法律、交通、物流、商贸等领域，推动 新一代智能终端、智能体 等广泛应用。
2025 年 10 月	国家发展改革委等五部门《深化智慧城市发展推进全域数字化转型行动计划》（发改数据〔2025〕1306 号）	加强人工智能公共服务能力建设，探索集约构建多模融合的城市大模型， 打造城市智能体应用 。

时间	文件名称	相关内容
2026 年 4 月	工信部办公厅、国家数据局综合司《关于联合实施 2026 年“模数共振”行动的通知》（工信厅联科函〔2026〕193 号）	通过行动牵引，推动产出一批推广价值高、技术可行性强的人工智能应用场景，攻关一批蕴含工业和信息化领域技术机理的行业模型、专用模型和特色智能体，构建一批行业通识和行业专识高质量数据集。
2026 年 5 月	国家网信办、国家发展改革委、工信部《智能体规范应用与创新发展实施意见》	重点围绕科学研究、产业发展、提振消费、民生福祉、社会治理等实际需求，发挥典型应用场景示范效应，先易后难、循序渐进，促进智能体技术验证、产品迭代、应用落地。

（4）支持政府采购 AI 基础服务

党中央、国务院将政府购买服务作为盘活市场化资源、提升公共服务质效、赋能政务数智化转型的重要制度抓手，持续完善政府购买服务机制，鼓励各地通过市场化采购方式引入优质社会服务资源，支持采购算力、大模型、智能体等 AI 基础服务，创新“企业运营、按需采购、按量付费”的服务模式。

表 4 政府采购 AI 基础服务相关政策

时间	文件名称	相关内容
2025 年 10 月	中央网信办、国家发展改革委《政务领域人工智能大模型部署应用指引》	加强政务领域人工智能大模型部署应用经费保障，引入市场化的产品和服务竞争机制，探索企业建设运营、政府购买服务、按使用情况结算费用的运作模式，营造高效、可持续的政务大模型生态。
2026 年 3 月	《中华人民共和国国民经济和社会发展第十五个五年规划纲要》	推进算力设施市场化建设运营，支持通过政府购买算力服务、算力租赁等多种方式满足算力需求。
2026 年 4 月	国务院《关于推进服务业扩能提质的意见》（国发〔2026〕7 号）	深入实施“人工智能+”行动，加快智能编程工具研发使用，支持采购大模型、智能体服务。

（5）丰富领域“人工智能+”应用

近年来，国家发展改革委、工信部、人社部、教育部、卫健委、交通运输部、国家数据局、国家能源局等多部委以国务院《关于深入实施“人工智能+”行动的意见》为总纲领，密集出台了分行业专项“人工智能+”落地政策或实施方案，以行业真实需求牵引技术落地，推动 AI 进入工业、农业、能源、交通、人社、教育、医疗等实体经济和公共服务领域，积极鼓励发展行业专用模型，打造人工智能新产品、新服务、新场景。

表 5 领域“人工智能+”应用相关政策

时间	文件名称	相关内容
2025 年 9 月	交通运输部等七部门《“人工智能+交通运输”的实施意见》（交科技发〔2025〕92 号）	在交通运输领域构建人工智能创新链、产业链、资金链、人才链深度融合的工作机制，大力促进人工智能普及应用，助力实现“人享其行、物畅其流”的美好愿景。
2025 年 9 月	国家发展改革委、国家能源局《关于推进“人工智能+”能源高质量发展的实施意见》（国能发科技〔2025〕73 号）	拓展人工智能与能源领域深度融合应用场景。
2025 年 10 月	国家网信办《政务领域人工智能大模型部署应用指引》	有序推进人工智能大模型技术、产品和服务在政务领域的部署、应用和持续优化，充分发挥人工智能大模型在复杂语义理解与推理、多模态内容生成、知识整合与分析等方面的优势。
2025 年 10 月	国家卫生健康委等五部门《关于促进和规范“人工智能+医疗卫生”应用发展的实施意见》（国卫办规划发〔2025〕30 号）	促进人工智能在医疗卫生领域的规范应用，不断丰富应用场景，提升服务能力，保障服务安全，优化资源配置，创新预防、诊疗、康复、健康管理等全链条连续智能服务，更好地满足人民群众日益增长的健康服务需求。
2025 年 11 月	中国民用航空局《推动“人工智能+民航”高质量发展实施意见》（民航发〔2025〕24 号）	在安全、运行、出行、物流、监管、规划建设等重点领域，深入推进人工智能创新赋能行业发展，强化高质量数据集等核心支撑要素供给，深化行业、产业与人工智能深度融合。
2025 年 12 月	工业和信息化部等八部门《“人工智能+制造”专项行动实施意见》（工信部联科〔2025〕279 号）	促进人工智能科技创新与产业创新深度融合、人工智能技术与制造业应用“双向赋能”。
2025 年 12 月	工业和信息化部办公厅《工业互联网和人工智能融合赋能行动方案》（工信厅信管〔2025〕76 号）	形成一批面向原材料、高端装备、消费品、电子信息等重点行业的工业大模型，开发一批面向质量检测、智能控制、工艺优化、营销服务等应用场景的专用小模型。鼓励工业互联网平台企业探索开发工业模型互联接口，优化大模型与小模型间协同效率路径，助力形成“大模型夯基+小模型深耕”的人工智能工业应用模型体系。
2026 年 2 月	国家发展改革委等八部门《加快招标投标领域人工智能推广应用的实施意见》（发改法规〔2026〕195 号）	积极稳妥推进人工智能在招标投标领域的应用，改进招标投标范式，提升服务和监管的数智化水平，为保障公共资源公平高效配置、规范招标投标市场秩序提供有力支撑。

时间	文件名称	相关内容
2026 年 4 月	国家发展改革委等四部门《关于促进人工智能与能源双向赋能的行动方案》(国能发科技〔2026〕34 号)	充分发挥我国能源产业体系完备、数据资源富集、应用场景广阔等优势，促进能源、算力、场景、数据、模型等要素高效协同，助力抢占人工智能产业应用制高点，有力支撑能源高质量发展。
2026 年 4 月	教育部等五部门《“人工智能+教育”行动计划》(教科信〔2026〕1 号)	充分发挥人工智能赋能教育变革的引擎作用，推动智能技术与教育全要素融合、全过程贯通、全场景覆盖，加快构建人机协同、虚实结合、泛在可及的智慧教育新形态。
2026 年 5 月	国家数据局《2026 年数字社会工作要点》	在普及智能个性数字美好生活方面，推广数字家庭智能化应用，加快人工智能赋能交通出行场景创新，大力完善数字消费渠道，深化人工智能在“影视+文旅”模式中的创新应用。
2026 年 5 月	中央网信办、教育部、工业和信息化部、人力资源社会保障部《2026 年提升全民数字素养与技能工作要点》	提升全民人工智能素养，包括强化人工智能赋能教育、加快人工智能人才培养、深化人工智能普及应用。
2026 年 5 月	市场监管总局、国家发展改革委《人工智能计量体系和能力建设指引(2026 版)》	推动计量技术深度融入智能制造、智慧医疗、智慧交通等 14 个重点领域，围绕 AI 诊断算法可靠性等关键参数开展计量技术研究，助力解决产业数字化转型中质量评估难题。
2026 年 6 月	商务部等八部门《加快“人工智能+消费”发展的实施意见》(商建发〔2026〕89 号)	加快人工智能新产品新服务新场景示范应用，促进人工智能进千家万户、进千商万店，培育形成消费新增长点新动能，带动人工智能新技术新产品迭代升级，开辟人工智能新产业新赛道，更好满足人民美好生活需要。
2026 年 6 月	交通运输部等五部门《“人工智能+交通运输”典型应用场景创新行动方案》(交科技发〔2026〕60 号)	聚焦智能驾驶、智慧公路、智能铁路、智能航运、智慧民航、智慧邮政、智能建养、智慧出行服务、智慧货运、智能安全监管等重点方向，持续拓展人工智能技术在交通运输领域的应用广度与深度。
2026 年 6 月	人力资源社会保障部等四部门《加快推进“人工智能+人社”应用发展的实施意见》(人社部发〔2026〕40 号)	推动人工智能产业和人社工作协同优化，开拓创新人社行业领域人工智能应用场景，构建安全稳妥可持续的人工智能建设运行机制，实现人社工作数智化发展。
2026 年 7 月	国家发展改革委等部门《人工智能合作发展行动计划》	促进智能体规范应用与创新发展，推动人工智能在科学、制造、医疗、教育、农业、治理等领域应用赋能，以人工智能促进经济发展、改善社会治理和增进民生福祉。
2026 年 8 月	农业农村部《全国农产品产地市场体系发展“十五五”规划》(农市发〔2026〕2 号)	充分发挥大型农产品批发市场、“链主”企业、农业产业化龙头企业等作用，探索数字化集采集配、统仓统配等新模式，打造“人工智能+”农产品流通应用场景。

2、多地出台落地方案，推进城市智能化升级

随着人工智能技术快速迭代，智能体、智能中枢成为各地推进城市数智化转型的重要抓手。近年来，国内多地围绕全域数字化转型、“人工智能+”等出台政策文件，推动智能体作为数智赋能城市发展的重要应用载体，促进大模型、智能终端、机器人在基层治理、公共服务、科学研究等多种场景深度落地。

表 6 各省人工智能+城市相关政策

文件名称	相关内容
北京市《关于加快智能体引领发展的若干措施》(京发改〔2026〕1185号)	面向科学、医疗、教育、政务、制造、文化等重点领域，打造一批标杆场景并开展应用验证，形成可复制、可推广的智能体落地应用模式，不断提高智能体应用普及率。
上海市《关于人工智能“模塑申城”的实施方案》(沪府办发〔2024〕27号)	支持利用多模态大模型构建城市治理感知助手，支撑城市智慧决策。推动智能服务机器人、智能运载工具、智能终端等在城市治理中的应用，提高治理效率。
上海市《国家数字经济创新发展试验区（上海）实施方案》(沪府办发〔2026〕5号)	深化智能体赋能超大城市高效治理。
重庆市《推动“人工智能+”行动方案》(渝府办发〔2025〕60号)	打造超大城市现代化治理大模型，推动市政基础设施智能化改造，推动 AI 赋能“大综合一体化”城市治理，建设“城市交通拥堵促畅智治”“城市治理立体综合巡查”等“AI+”综合应用场景等。
江苏省《“人工智能+”行动方案》(苏政发〔2025〕108号)	打造政务大模型和虚拟政务服务大厅，开展大模型政务领域应用试点，推广政务助手、政务数字人和“智慧晓苏”政务智能体等一批“小巧灵”应用；推进大模型在公共资源交易场景中的应用；打造城市运行智能中枢，试点开展城市智能体应用。
广东省《推进城市全域数字化转型建设智慧城市行动方案》(粤政数〔2026〕16号)	完善城市智能中枢建设，打造城市共性技术能力支撑体系，分类推进有关数字孪生共性功能组件共享复用；加强人工智能公共服务能力建设，探索打造城市自进化综合智能体。
河南省《深化智慧城市发展 推进城市全域数字化转型实施方案（2025—2027年）》(豫发改数字〔2025〕569号)	按照统一规划、统一架构、统一标准、统一运维原则，推动各地在现有智慧城市框架基础上进行优化升级，构建全域感知、数据融通、能力共享、业务协同的城市运行和治理智能中枢平台。
四川省《加快推进“人工智能+”一号创新工程实施方案》(川办发〔2026〕14号)	深化人工智能在国土空间规划、城市建设、市场监管、城乡融合发展、生态环境领域应用；推动智能机器人、智能运载工具、智能终端等在城乡治理中的应用。
安徽省《“人工智能+万物”应用行动方案》(皖政办〔2025〕15号)	到 2027 年，新一代智能终端、智能体等应用普及率超 70%，到 2030 年，新一代智能终端、智能体等应用普及率超 90%。
贵州省《推进治理数智化转型三年行动方案（2026—2028年）》(黔府办函〔2025〕57号)	构建政务智能体中枢，推进与现有系统、平台、应用深度融合，加快高频共性智能化场景落地。

(二) 技术趋势：从联接智能到整体智能，全栈 AI 技术重构城市智能底层逻辑

1、智能体：重构人机协作的新一代交互入口

(1) 大模型与智能体形成能力互补关系

基础大模型与智能体在技术定位、能力边界与适用场景上具备清晰的层级互补关系。城市级大模型承担通用认知底座功能，提供自然语言理解、多模态感知、知识检索与内容生成等基础共性能力，支撑上层各类应用的通用认知需求。智能体则是面向特定任务的执行单元，基于大模型的基础认知能力，通过任务拆解、路径规划、工具调用与流程闭环实现完整的任务执行，是技术能力转化为业务价值的核心载体。在规则明确、流程标准化、目标可量化的封闭场景中，智能体凭借自主执行能力展现出显著的效率优势，可替代人工完成重复性、流程化的事务性工作。但在边界模糊、涉及价值判断与多方权衡的开放复杂场景中，智能体的综合研判、灵活处置与非结构化信息融合能力仍存在明显技术局限，无法替代人类的高阶认知与决策能力。从技术可信性维度看，智能体的稳定性、确定性与可解释性水平直接决定其应用边界。封闭标准化场景下智能体的运行可靠性与结果可校验性可满足业务需求，开放动态场景下仍存在输出偏差与逻辑不可控的风险，高风险场景下尚不具备脱离人类监督独立运行的技术条件。随着行业知识深度注入、可解释 AI 技术与安全管控机制的持续演进，智能体的可信应用边界将逐步拓展，但人类主导决策、智能体辅助执行的底层技术逻辑不会发生根本性改变。

(2) 智能体正在重塑人机协作新范式

智能体作为新一代交互入口，正在重构人与数字系统的协作模式，引领 AI 应用从工具调用阶段迈向人机深度协同的新阶段。在传统大模型阶段，AI 以被动工具的形态存在，人类需要通过明确指令逐步引导 AI 完成单点操作，本质上是人类适应技术系统的交互模式。进入智能体阶段后，人类只需提出目标诉求，智能体即可自主完成任务理解、路径规划、工具调用与结果交付，实现技术系统主动适配人的需求的范式转变。这种演进同时重构了智能体与智能体、人与智能体之间的协作关系，多领域专用智能体可通过统一的编排

调度实现信息互通与任务协商，共同完成跨领域的复杂任务，人类则在其中承担监督、决策与价值把控的核心角色，最终形成人机协同、多主体联动的交互范式。

(3) 轻量化端侧部署助力智能体规模化落地

模型压缩与端侧推理技术的快速成熟，推动智能体的部署架构从集中式云端向分布式端侧下沉，为智能体从试点验证走向城市级规模化部署扫清了技术障碍。端侧部署模式让城市中的海量感知节点从单纯的数据采集终端升级为具备就地分析与决策能力的智能单元，感知数据无需全量回传云端即可在本地完成处理、决策与响应。在此基础上形成的端云协同技术架构，由端侧智能体承担高频标准化场景的实时处理，云端大模型负责复杂事件研判、全局调度优化与模型迭代升级，二者形成能力互补的运行体系，为智能体向全域规模化覆盖提供了可行的技术路径。

2、城市公共云：承载智慧城市服务能力的核心载体

(1) 我国城市云服务正逐步向城市公共云转型

智能经济时代技术与应用迭代加速，传统线下自建的算力、算法、数据模式已无法满足智能应用对敏捷创新、弹性供给、普惠覆盖的要求，推动我国城市云加快向城市公共云演进。从发展基础看，我国超大型数据中心容量占全球 16.0%，智算规模占全球 14.6%，均位居全球第二；国产 AI 芯片年度出货量占比约为 41%¹，国产方案逐步形成规模化应用能力，为城市公共云建设筑牢硬件和自主可控发展根基。从供需驱动看，城市范围内大模型、多模态应用、智能体加速落地，模型训练、推理服务的算力需求增速高于供给增速，叠加能耗约束，传统分散自建模式存在投入高、利用率低等问题，倒逼城市算力供给向以城市云为核心的集约化建设、弹性化调度、服务化输出方向转型，通过云端统筹提升资源利用效率。从技术迭代看，芯片、大模型、智能体迭代周期大幅压缩，城市政务、产业主体依靠自建系统难以持续跟进芯片、框架、模型、工具链的快速更新，推动城市云从静态资源交付向全栈动态迭代的 AI 原生技术底座升级。

¹ 华为&罗兰贝格《先进公共云白皮书》

(2) 全栈系统能效成为 AI 时代算力竞争核心

AI 技术迭代和规模化落地催生爆发式算力需求，算力领域的竞争逻辑已发生根本转变。算力供给类型从传统通用 CPU 为主，拓展为 GPU、NPU 等多元异构算力，以匹配大模型训练、推理、数据预处理等差异化场景需求。竞争维度也从单一芯片的峰值算力、制程工艺单点比拼，升级为涵盖芯片架构、互联总线、散热技术、集群调度、算子库优化、编译工具链、算法适配的全栈系统能力竞争。单芯片算力不再是决定性指标，千卡/万卡级集群的线性加速比、有效算力利用率（MFU）、系统能效比，成为衡量算力竞争力的重要指标。针对地市、区县级地方云规模偏小、不具备超大规模集约效应的特点，城市公共云依托云原生弹性调度能力实现算力错峰复用，白天优先保障政务服务、产业生产的实时 AI 推理需求，夜间承接模型训练、离线分析等时延不敏感的任务，大幅提升算力利用率，以有限算力资源实现最大化产出效益。

(3) 城市公共云推动技术门槛降低与普惠创新

在算力资源层面，城市公共云通过集约化建设和专业化、绿色化运营，整合政府部门、产业园区、科研机构等分散算力资源，构建城市级统一智算资源池，从基建源头减少重复投入。在智能能力层面，城市公共云将大模型训练、智能体开发等高门槛技术能力封装为标准化公共云服务，把政务服务、城市治理、产业服务等通用场景能力沉淀为可复用组件，取代各单位独立开发、重复训练的模式，实现智能能力的全局共享与快速调用。这种集约化模式，一方面通过规模效应摊薄单位成本，从根源规避算力设备重复采购、智能应用重复开发的资源浪费；另一方面让政府机构与中小企业无需自建智算集群、无需组建专业 AI 团队，以按需调用、按量付费的轻量化模式即可获取匹配需求的智能能力，系统性降低 AI 技术应用门槛，激活全域普惠创新活力。

3、算力网：从“东数西算大布局”到“以城市为核心”新转型

(1) 全域算力资源整合夯实 AI CITY 算力根基

城市算力网以城市或都市圈为单元构建，通过整合城市智算、云计算、边缘终端等分散算力资源，构建统一集约、弹性可调的城市级一体化算力底

座，是支撑 AI 全生命周期的关键能力之一。传统城市数字化建设中，政府部门、园区、企业等算力建设分散，存在算力孤岛、资源闲置、重复建设、算力适配性差等问题，无法满足 AI 城市海量数据处理、大模型推理、全域智能感知的算力需求。城市算力网通过整合城市智算中心、云计算中心、边缘算力节点、终端算力等各类资源，构建全域统一、互联互通、弹性可调的一体化算力网络。一方面，统一纳管全域算力资源，实现算力统一调度、按需分配，解决传统算力忙闲不均、供给不足的痛点，为城市级 AI 大模型训练、全域数据研判、智能算法运行提供稳定、充足的算力支撑。另一方面，通过资源集约利用，降低城市数字化建设成本与能耗，统一算力接入、安全、运维标准，为 AI CITY 各类智能化系统稳定、持续运行筑牢底层硬件与资源基础。

(2) 端边云协同架构构建全域一体化智能体系

城市算力网与城市公共云、端侧 AI 深度联动，通过端、边、云协同实现全域智能资源的最优调配。端侧承接高频次、低时延、高安全的本地化场景任务，就地完成数据预处理、轻量化推理、实时事件处置，减少原始数据全量上云带来的带宽消耗与响应延迟，有效降低云端算力压力。边缘节点承接区域级终端调度、数据汇聚与中度算力推理任务，衔接端侧与云端能力。云端集约承载全局大模型训练、全域数据统筹、复杂场景研判、智能体全局调度等高阶任务。端边云协同架构既能发挥端侧分布式实时智能的优势，又能依托云端集约化算力与大模型能力弥补端侧算力规模不足、认知能力有限的短板，解决传统智慧城市“终端孤立、云端过载、响应滞后”的痛点，为城市全场景 AI 智能落地提供底层互联与协同支撑。

(3) 对接全国一体化算力网塑造协同发展格局

城市算力网是全国一体化算力网建设的核心抓手，从层级关系来看，全国一体化算力网负责全国范围内超大规模算力调度、跨区域数据协同、大型算力枢纽布局，侧重宏观统筹。城市算力网聚焦城市本地算力精细化调度、边缘算力落地、城市场景适配，是全国一体化算力网在城市维度的延伸与落地。依托城市算力网接入全国一体化算力网络，AI CITY 可共享国家枢纽节点的超算资源，弥补本地高端算力缺口，支撑超大规模城市模型训练、跨区域数据协同分析等高端应用。当前，1ms 城市算力网已从概念普及迈入规模化

落地新阶段，实现城市内算力 1 毫秒互联与用户 1 毫秒入算。城市算力网建设将丰富全国一体化算力网的节点布局，逐步形成“国家统筹、城市落地、全域协同”的算力发展格局。

4、端侧 AI 互联：城市全域智能协同的核心支撑

(1) 自主可控端侧操作系统筑牢城市智能终端底座

端侧操作系统作为城市海量终端智能化、互联化的最底层核心基座，是实现全域终端统一适配、智能赋能、安全可控的关键载体。现阶段城市终端设备品类繁杂、硬件架构差异化大，传统嵌入式系统普遍存在架构碎片化、AI 适配能力弱、功能固化、迭代滞后等问题，难以支撑城市级规模化、标准化的端侧智能应用落地。当前以华为鸿蒙为代表的国产 AI 原生端侧操作系统采用模块化、分布式原生架构，具备跨设备、跨硬件、跨场景的统一适配特性，可兼容城市感知终端、物联网设备、车载终端、民生智能设备等多元硬件形态，从底层解决终端碎片化难题，为城市海量异构终端提供统一纳管、统一适配、统一安全管控，支撑端侧 AI 能力规模化部署。

(2) 分布式高速智联技术实现异构终端极速组网协同

端侧设备互联正向无感自动组网、低时延高可靠、全域协同的分布式智联模式演进，是激活城市终端感知资源、实现设备协同智能的核心技术突破。传统城市物联体系连接流程繁琐、组网效率偏低、异构设备互通性差，设备间难以实现数据共享与指令联动，大量终端仅能完成基础数据采集，无法发挥协同智能价值。新一代分布式互联技术通过构建无中心自组网架构，具备设备自动发现、极简配网、毫秒级连接、高可靠传输的技术特性，可打破硬件、协议、场景壁垒，实现全域异构终端互联互通、资源共享、联合研判，构建起全域分布式智能节点网络，大幅提升城市感知响应效率与场景联动精度。例如，华为鸿蒙分布式软总线技术，凭借低时延、高稳定、大带宽的技术优势，实现城市各类异构终端的无感极速组网与跨设备协同联动，让城市中分散的摄像头、传感器、智能终端不再是孤立的数据采集单元，而是形成互联互通的分布式智能节点网络。

(三) 发展需求：智慧城市走向高质量高价值智能服务新阶段

1、智能社会新形态催生城市发展新要求

新一轮科技革命和产业变革深入演进，推动人类社会迈向人机协同、跨界融合、共创分享的智能时代。《国务院关于深入实施“人工智能+”行动的意见》提出积极构建更有温度的智能社会。相较于传统智慧城市以数据流转、线上办事为核心的建设模式，智能社会下的城市运行呈现三大全新特征：

一是社会主体多元化，智能体、数字人等非人类智能主体深度参与城市治理与民生服务，形成人类决策者与智能执行体共生的全新分工格局。

二是社会空间虚实一体化，数字孪生、元宇宙等技术推动物理城市与数字空间深度耦合，城市治理从单一实体管控转向虚实融合全域治理。

三是社会协作网络化，扁平化、平台化的新型社会组织形态，让跨部门、跨区域、跨主体的协同联动成为常态。

这种多元主体、虚实融合、协同共治的全新形态，打破了传统智慧城市的建设逻辑，对 AI CITY 的治理模式、服务体系、运行规则提出新要求，亟需建立适配人工智能、城市智能体落地的新型治理架构，明确人机共治的协同流程和运行规范，适配智能社会全新发展形态。

2、传统智慧城市管理机制和建设运营模式面临挑战

随着全国各地智慧城市建设进入全面落地阶段，技术应用、场景拓展与现有制度体系的矛盾日益凸显，各类机制短板成为制约智能化转型提质增效的核心瓶颈。

当前多数城市的智能化建设仍沿用传统信息化建设模式，算力成本较高、城市算力供需不均衡，存在数据融合不足、架构标准不统一、安全风险防范不足、无形资产采购机制滞后、运营模式不清晰等制度性障碍。数据壁垒尚未完全打破，数据确权、流通、应用等制度规范滞后，高质量城市数据缺乏，无法有效支撑大模型训练，导致城市专用领域模型供给不足，智能应用场景

落地困难。传统硬件采购的建设模式、固定资产核算的管理规则，与人工智能时代算法迭代、模型优化、智能体升级的轻量化、持续性建设需求不匹配，无形资产采购、数字能力运营的制度体系缺失。智能技术应用的标准体系、安全风险、伦理规范、隐私保护机制不完善，算法歧视、数据泄露等潜在风险难以管控，重建设轻运营现象依然存在，严重制约智慧城市发展。

3、AI CITY 发展已进入实效比拼的阶段

早期城市智能化建设的核心竞争力在于算力中心建设、数字底座搭建、头部企业落地等方面。而当前智慧城市建设已从工程思维向价值思维转变，城市管理者更加关注价值创造、风险管控、长效运营等问题。现阶段城市间硬件与技术资源逐步趋同，技术本身不再是发展瓶颈，应用实效成为拉开城市发展差距的关键。各地纷纷出台“人工智能+”发展专项政策，通过建设运营模式创新和发展生态优化，破解算力利用率低、智能场景落地难等难题，避免重蹈“重建设、轻运营”“有技术、无实效”的覆辙。

未来 AI CITY 的发展，将聚焦利用技术优化政府治理、提升民生服务质感、激活壮大产业，实现从“建成智慧城市”到“提供高价值的城市智能服务”的转变。



Ai

第二章 概念模型：

城市进化新范式：AI 原生的高价值城市智能服务

（一）AI CITY 核心理念：“城市超级智能体”提供 AI 原生的高价值城市智能服务

AI CITY 是国家信息中心与华为联合提出的人工智能时代的智慧城市发展新理念，是下一代智慧城市的底层逻辑变迁和发展模式升维。随着大模型、智能体、云原生技术的持续迭代，AI CITY 将城市从“数据驱动”推向“知识驱动”，并进一步向“城市超级智能体”跨越式升级。

发展理念：

AI CITY 是立足 AI 原生逻辑的高价值城市智能服务，以云服务为主要载体、以 AI 智能体为核心能力、以 RaaS（Result as a Service，效果即服务）为价值导向，整合全域软硬件资源，重构建设集约化、能力服务化、结果价值化、生态多样化、资产轻量化的城市建设运营范式。以 AI 原生思维重构业务流程、重塑治理体系、创新服务模式，建设 AI 就绪的社会底座，形成人机深度共治的城市运行新格局。



图 1 AI CITY 发展理念示意图

核心能力：

依托全域多模态感知，全天候采集空间、人流、设施等多元信息，完成对现实世界的立体感知，构成城市神经末梢。通过智能认知与决策，对海量数据深度理解推演，实现城市大脑自主思考研判。多智能体协作处置，各类城市智能单元协同联动，快速落地响应行动。同时，城市具备持续演进生长能力，系统在每次事件中不断学习，迭代优化，越用越聪明。以系统性的内生安全贯穿芯片、网络、数据、模型、智能体，筑牢底层屏障，抵御各类风险隐患。统一自然语言交互作为唯一入口，市民使用日常语言即可和城市智能系统对话，唤醒智能服务。AI CITY 将成为一个可感知、会思考、能行动、自迭代、高安全、易交互的“城市超级智能体”。



（二）AI CITY 建设要点

1、建设集约化

传统城市数字化建设中，各业务领域系统独立部署，硬件资源、算力资源、平台资源难以互通共享，造成大量建设资源浪费，且无法支撑城市全域智能化升级需求。AI CITY 通过统筹规划、统一纳管城市全域数字基础设施，构建普惠化、弹性化的云服务体系，打造分布式智能云底座与政务专属功能专区，实现算力、存储、网络等基础资源的集中管控、动态调度、按需分配和安全保障。通过集约化建设和普惠化供给，有效破解传统建设模式下重复建设、资源冗余、利用率低下等问题，保障城市各层级、各场景均可便捷调用基础数字资源，为全域智能化场景落地筑牢底层支撑。

2、能力服务化

数智技术迭代速度快、模型研发与算力部署成本高，传统数字化项目建设模式存在迭代滞后、成本高昂、适配性差等短板，难以支撑城市海量多元的智能化场景需求。AI CITY 构建与智能体适配的基础设施和云体系，打造覆盖 IaaS、PaaS、DaaS、MaaS 的全层级服务体系，将城市算力、模型、数据、智能体等各类数字资源，封装为标准化、模块化、可复用的云服务能力。基于一体化算力服务交付模式，城市数字资源从固定资产建设向动态服务供给转变，城市各类场景可实现智能化能力的灵活调用与快速落地。

3、结果价值化

以往智慧城市建设多聚焦于业务流程线上化、数字化，完成了城市治理与服务的形式升级，但是数据与技术无法直接转化为治理效能和民生服务价值，建设投入与实际产出不匹配。AI CITY 依托城市智能体构建全域闭环运行体系，打造全域感知、智能认知、自主决策、精准执行、持续迭代的全链路能力，可深度嵌入城市治理、民生服务、产业发展、应急管控等各领域场景，打破传统的流程局限。基于 RaaS（效果即服务）创新模式，AI CITY 不再单纯输出数据、流程等基础数字化产品，而是通过智能体等方式直接输出治理成效、服务成果、解决方案等高价值结果，真正实现数字技术服务城市发展的核心价值。

4、生态多样化

传统智慧城市建设中存在技术门槛高、标准不统一、产业链协同不足等问题，制约了城市 AI 产业与智能场景的规模化发展。AI CITY 以打造多元参与、协同共建、持续迭代的城市 AI 创新生态为目标，向算法企业、应用服务商、科研机构、初创企业等全产业链主体开放基础能力与资源，汇聚产业链上下游创新力量，打破技术壁垒与行业壁垒。通过统一标准化接口、模块化功能组件、可自由编排的智能体模板，各类市场主体与科研主体快速开展场景创新、算法优化、应用开发与方案迭代，持续丰富城市智能化应用供给，充分挖掘城市 AI 创新场景，为城市数智化发展提供源源不断的创新动力。

5、资产轻量化

以硬件设备、物理设施等固定资产为核心的投资模式，存在投入大、折旧快、复用难等问题，城市软硬件体系难以持续进化，后期运营运维乏力。AI CITY 以轻量化的无形资产投资替代重资产硬件投入，将建设重心从传统物理硬件的规模化堆砌，转向数字无形资产与软性核心能力的培育迭代。通过 AI 算法优化、智能体训练、数据资源激活、服务体系完善、治理规则迭代等软性能力建设，城市可以持续优化升级数智化建设服务能力，同时有效规避传统重资产建设的投入冗余、迭代僵化、运营成本高昂等问题，实现城市 AI 体系的动态进化、长效运营，保障 AI CITY 可持续发展。



图 2 AI CITY 建设要点示意图



第三章 体系架构：



全栈智能的 AI CITY 架构体系



（一）参考框架

AI CITY“123N”框架：

基于城市公共云部署 1 个安全可控 AI 数智底座, 依托多模态数据 (DaaS) 和主流大模型 (MaaS) 2 大创新引擎, 建设数据一站式开发治理平台、模型一站式训推平台、智能体一站式开发与运行平台 3 个使能平台, 打造 N 个 AI 创新应用场景, 以领域智能体专家规模化支撑场景应用, 构建全域自主可控的城市级 AI 操作系统。

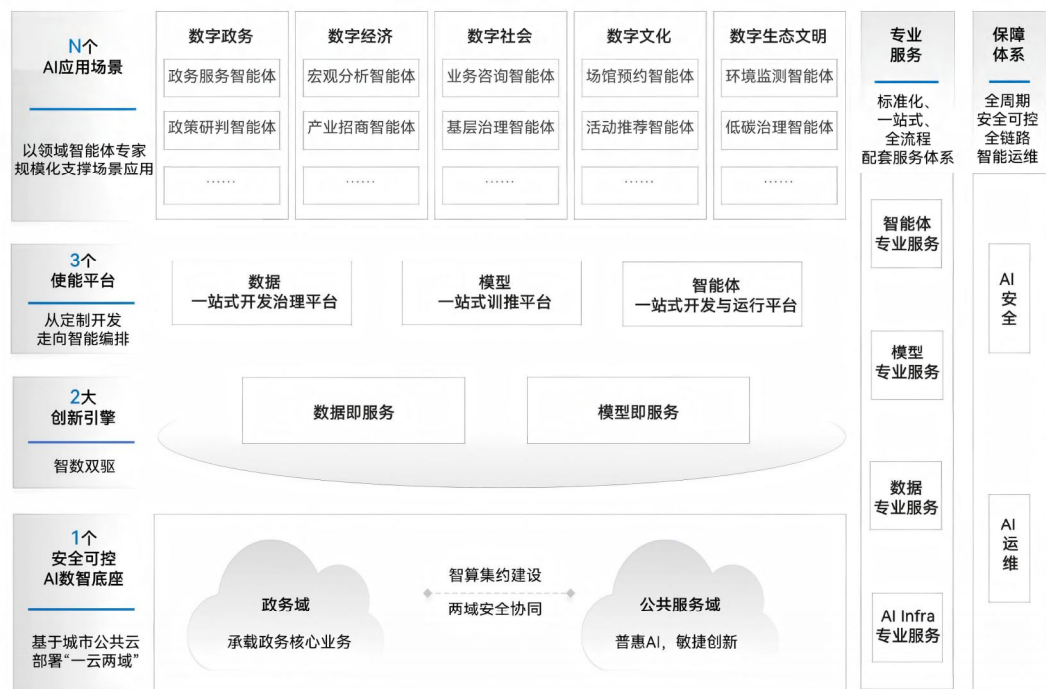


图 3 AI CITY 参考框架示意图

（二）城市公共云体系

1、功能定位

（1）现实需求

城市发展已全面进入数字化、智能化、集约化转型阶段，对城市云服务提出了算力供给、数据共享、智能渗透、普惠云端等方面的新需求。

一是智算资源供需矛盾加剧，要求云具备集约、弹性、安全可信的智算供给能力。大模型、生成式 AI、多模态应用和智能体快速发展，广泛应用于公共治理、普惠服务、生产经营和个人生活场景。传统分散的机房部署、独立的 IT 架构、碎片化的数据体系，缺乏高并发和弹性的算力资源，难以满足场景全域覆盖、实时响应、弹性供给和规模化协同的需求，已无法适配超大城市、大中型城市在服务提质、治理扩容、产业升级方面的发展需要。城市发展亟需构建统一的公共云底座，通过集约化建设、弹性化调度和服务化供给，实现资源按需调度、统一运维，降低城市数智化建设与运维成本，提升智算资源利用效率。

二是城市数据汇聚共享与融通，要求云具备统一数据归集、治理、共享、交换能力。AI CITY 的精细化治理高度依赖跨部门、跨层级、跨领域的数据共享与业务协同，要求对海量异构数据开展实时采集、统一治理、多模态融合与高效流通，支持跨系统、跨场景的持续联动。传统数据体系相对封闭割裂，数据难以归集、无法联动研判，难以满足海量场景下持续增长的推理与交互需求，无法支撑“一网统管”、“一网通办”、城市态势感知等新型治理场景，制约数据价值充分释放。城市发展亟需公共云提供统一的数据归集、治理、共享、交换能力，打通全域政务数据资源，推动城市治理由“被动处置”向“主动预判、精准治理”升级。

三是城市全场景智能升级，要求云具备支撑智能全域渗透的能力。智慧交通、智慧安防、智慧环保、智慧城管、智慧管网、数字孪生、物联感知等场景持续落地，城市每日产生海量物联数据、视频监控数据、城市运行数据，对大容量存储、实时算力、智能分析能力提出极高要求。传统本地服务器算力有限、扩容困难、智能化不足，亟需云服务提供弹性海量算力、AI 算法能

力、大数据分析能力，承载全域智慧场景稳定运行与持续迭代。

四是产业智能化转型升级，要求云能够提供普惠的云端服务。针对城市大量中小微企业数字化转型资金不足、技术薄弱、运维能力欠缺等痛点，公共云提供低成本、轻量化、普惠化的云端服务，将高门槛、高投入、高复杂度的 AI 能力转化为可调用、可组合、可规模化部署的服务，降低中小企业上云用云门槛，为行业智能化转型升级提供重要支撑。

(2) 主要功能

传统政务云向城市公共云升级，突破了固有云服务的定位边界，被赋予了更加丰富的功能内涵。

资源集约统筹，统一算力存储。AI CITY 需要的并非单一的云部署形态，而是能够全栈配置智能资源、广泛输出智能服务、稳定支撑智能闭环的公共性智能载体。城市公共云不是传统政务云的简单扩容，而是协同政务云、公有云、行业云等多种形态，构建面向全域的公共数字底座。通过对算力、存储、网络资源的统一池化调度，替代各部门分散自建机房、独立部署的传统模式，推动全城 IT 资源共建、共享、共用，破解重复建设、资源闲置、标准混乱等问题，夯实城市 AI 底座能力，以最大化公共利益、最优化资源共享，实现 AI 普惠。

数据汇聚共享，打通数据壁垒。作为城市数据资源的统一承载载体，城市公共云着力打破部门、层级、行业间的数据孤岛，承接跨部门、跨层级、跨区域的数据汇聚、清洗、整合、开放与共享工作。为城市大数据分析、智能决策、态势感知、协同调度提供稳定算力与平台支撑，充分盘活城市数据资源。支撑跨部门业务协同、联合审批、联动研判，为城市精细化治理场景提供核心数据能力支撑。

AI 场景赋能，提供海量智能算力。城市公共云承载城市海量物联、视频监控、环境监测、城市运行等数据的存储与实时运算，提供大数据分析、AI 智能研判、趋势预测、异常预警等智能化能力，推动城市治理从被动处置向主动预判、精准管控转型。通过统一资源调度与业务纳管以及标准化、模块化的云端服务，降低各类智慧应用的建设门槛，全面支撑智慧交通、智慧安

防、智慧环保、智慧城管、数字孪生城市等全域智慧场景快速部署、迭代升级，助力城市构建智能、韧性、高效的运行体系。

产业普惠赋能，助推数字经济发展。城市公共云将先进算力、模型、工具链和安全能力转化为可按需获取的公共服务，面向企业、产业园区、科创主体提供普惠性、低成本、轻量化的云服务，帮助企业更快获取最新技术、更高效利用智算资源，破解中小微企业数字化转型资金不足、技术薄弱、运维能力欠缺的问题。支持企业快速上云用数赋智，推动产业链数据协同、资源共享、业态创新，持续放大智算资源应用价值。

2、部署形态

城市智能应用场景加速扩展，智能化能力将广泛嵌入政务、金融、能源、医疗、教育、交通等关键行业，不同场景对部署形态、安全等级、时延性能和服务可及性提出差异化要求。城市公共云通过公有云、行业云、专属云、边缘云的深度协同，形成“公共云+本地政务云”协同的分布式政务云体系。依据业务类型、安全要求、运行特点，灵活选择业务部署形态；依托公共云弹性算力、共享组件能力，支撑政务数字化、智能化业务迭代发展，避免重复建设，提升城市算力资源统筹利用水平。

城市公共云以“最大化公共利益”“最优化资源共享”为目标，以统一架构同源技术、服务化按需供给、集中化统一运维为标准，推动云从单一部署模式走向公有云、行业云、规模化专属云和边缘云等多元云部署形态，适配不同应用场景和安全等级的管理要求，通过统一、开放和可拓展的服务体系，让政府与企业更安全、更经济地获取先进的算力和模型服务，支撑政府服务普惠化、城市治理现代化和产业数字化升级。

城市公共云通过规模化、标准化和服务化的智能能力供给，促进智能资源高效共享、智能技术普惠应用和全社会智能化水平的提升。



图 4 城市公共云部署形态示意图

3、技术架构

城市公共云采用“两域部署”的总体架构，统筹不同服务对象、业务属性和安全要求，形成架构统一、分域承载、能力协同、安全可控、持续运营的城市云服务体系。

（1）政务域

政务域是核心政务业务承载域，核心使命为“守底线，保安全”，面向党政机关内部业务承载政务智能体等政府核心业务系统与敏感数据，是政务运行的安全底座。以“主节点+同城节点+异地节点+县市区节点”的多地多中心分布式架构，保障全域业务高可用与容灾能力。部署上采用私有化模式，满足等保三级及以上安全防护要求，同时面向 AI 时代引入 Token 计量机制和 AI 能力，通过服务网关作为统一安全出入口对接公共服务域，在保障安全的前提下稳步提升政务智能化水平。

（2）公共服务域

公共服务域是城市公共云的服务主体与数据枢纽，核心使命为“促流通、保可信、强服务、促创新、推普惠”，面向公共服务机构、产业主体、基层治理组织、市民个人及政府对外服务，提供 AI 服务和可信数据支撑。部署上采

用公有云专区或联合共建的多厂商专区化模式，服务能力与公有云对齐、迭代同步，从而降低使用门槛、提升迭代效率，支撑全场景 AI 创新落地。

该域提供基础服务、MaaS 服务、智能体服务、AI 场景开发四层能力体系。

基础服务层提供计算、存储、网络等底层云资源，支撑全栈能力弹性调度。

MaaS 服务层通过专属接入区的多重防火墙保障接入安全，依托大模型资源池提供标准化模型服务与 Token 服务。

智能体服务层沉淀 Skill（AI 技能）、MCP（模型上下文协议）、Agent 模板等标准化 AI 资产，配套资产安全扫描、AI 数据安全等全链路防护能力。

AI 场景开发层提供代码智能体、办公智能体等开发工具，支撑各类 AI 场景快速构建。

(3) 两域安全协同

1) 统一的安全架构

统一基线标准：组件、身份、权限、配置、策略等同一套安全标准适用全场景，无异构问题。

统一安全策略：公共云/政务云采用统一安全防护策略，降低安全复杂性和运维成本。

2) 统一的安全运营

统一态势感知：安全数据、AI 资产风险、威胁态势统一归集展示、全局安全无盲区。

统一响应处置：安全告警规则与处置流程一致、事件处置时效缩短。

3) 统一的协同防护

威胁情报协同：利用公有云大量攻击样本进行实时分析，生成情报和特性库秒级同步到政务云。

数据流转协同：数据训、推、用全流程可视呈现不泄露。

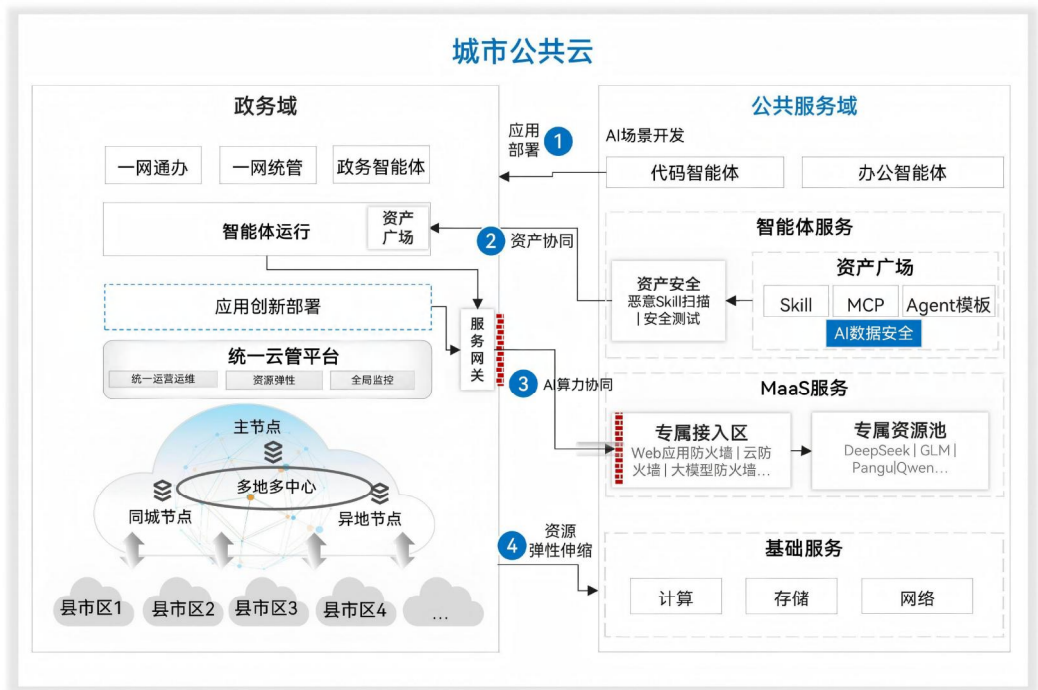


图 5 城市公共云技术架构

【规划案例】某市城市公共云规划：一云两域，快速获取弹性资源、先进 AI 算力、模型

某市城市公共云构建政务域与公共服务域“一云两域”协同体系，两域采用统一架构、同源技术，由统一团队统筹管理。其中，政务域以政务云为底座，采用主节点、同城节点、异地节点的多地多中心架构，由市云管平台实现全局监控、统一运维，覆盖全市各区算力资源。在政务域基础上拓展公共服务域，依托公有云/政务专区弹性扩展能力，快速补齐资源缺口，实现算力按需调度、弹性伸缩，可承载面向市民的政务服务，面向学校、医院、文体机构服务对象的数字公共服务，面向中小企业的 AI 赋能数字化转型服务等。

该模式形成四大核心协同价值：一是高并发业务弹性调度，面向公众的高并发业务可灵活部署上云，通过高峰扩容、低谷缩容精准匹配业务波峰波谷，持续优化资源利用效率。二是 AI 场景高效创新，依托码道（CodeArts）能力实现云上开发、本地部署，支持智能体本地运行、云上推理，大幅压缩

AI 应用开发周期。三是智能体资产安全共享，打通智能体资产协同通道，线上 300 余项插件与模板可按需取用，配套全程恶意资产扫描机制，全方位筑牢安全防线。四是前沿大模型安全接入，设置专属接入区并配套专属资源池，在保障线下访问安全、实现企业数据零泄漏的前提下，快速对接行业最新大模型，稳定获取先进 AI 技术能力。

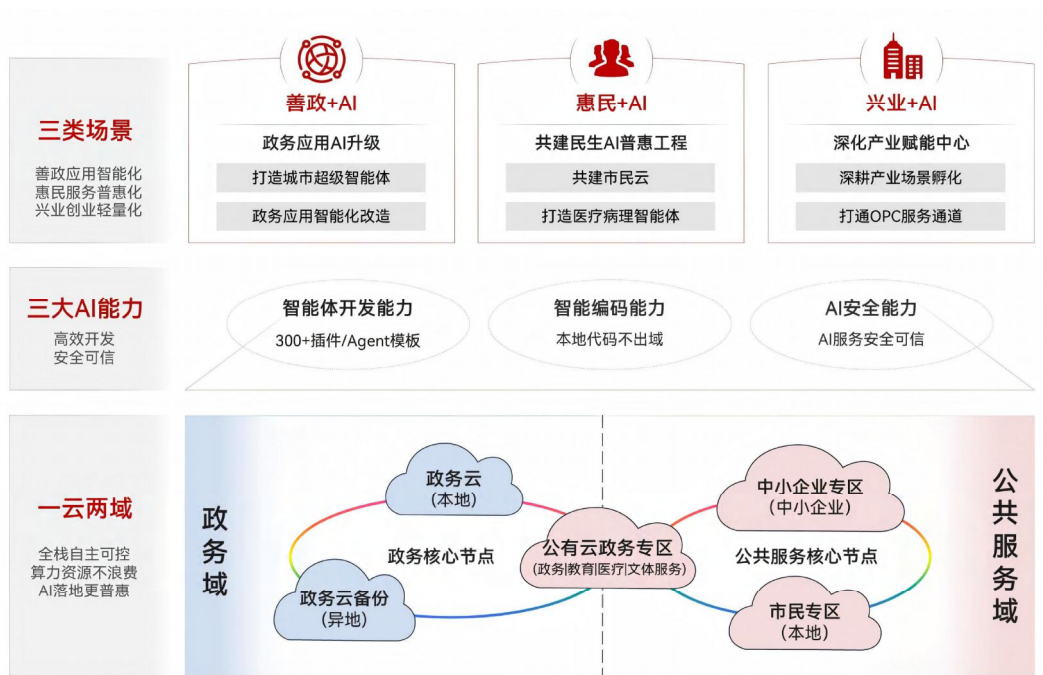


图 6 某市城市公共云规划架构示意图

（三）数据体系

1、功能定位

（1）现实需求

随着人工智能由大模型能力时代向智能体构建时代演进，数据正在由支撑城市数字化运行的基础资源，升级为驱动城市智能化发展的关键要素。传统模式下，城市数据体系主要服务于业务系统，多以结构化数据的采集汇聚、共享交换和辅助决策为使用链路。AI CITY 时代，数据需要持续支撑大模型训练、知识增强、智能体推理决策以及多智能体协同运行。城市数据的数据结构、建设重点等正在发生深刻变革。一方面，大模型训练和智能体构建需求下，推动城市数据需求从结构化数据向文本、图片、音频、视频、时空信息、物联网感知等多模态数据拓展，从静态数据查询向实时动态、敏捷响应的数据调用转变，对数据质量、语义关联和知识化水平提出更高要求。另一方面，数据建设的重点需要从“汇聚更多数据”加速转向“提供大模型和智能体可直接使用的高质量数据”，形成面向人工智能的数据语料、知识库和数据集体系。

数据功能升级还面临着两大难点。一是当前城市数据仍存在跨部门分散、数据标准不统一、非结构化数据利用不足、数据质量与人工智能需求不匹配等问题，大量已经汇聚的数据尚未真正转化为模型和智能体可理解、可调用的数据资源。二是随着人工智能应用由政务治理向医疗、交通、制造、公共服务等领域深入，仅依靠政府内部数据已难以满足复杂场景需求，公共数据、企业数据和社会数据融合利用仍然存在难点堵点。

（2）主要功能

立足发展实际，AI CITY 亟需构建面向人工智能的数据体系，以多模态数据底座实现城市全类型数据统一汇聚与组织，以数据治理智能体提升数据治理自动化和知识化水平，以高质量数据集和知识库持续支撑模型与智能体应用，以可信数据空间促进跨部门、跨行业、跨主体数据安全可信流通，推动城市数据体系从“面向业务的数据管理”向“面向人工智能的数据生产与供给”升级，为城市模型和智能体规模化创新提供良好的数据基础。



图 7 数据体系架构示意图

2、多模态数据底座

多模态数据底座是面向 AI 时代的智能数据平台，满足海量多模态数据的预处理需求，提供高性能的多模处理能力，支持文本、图像、音频、视频等多模态数据统一管理，兼容多样式格式，助力构建 AI 时代的数据竞争力。

（1）数据来源

多模态数据源：将城市各部门、各场景、各主体的数据进行接入。数据来源涉及网页、表格、文本、图片、音频、视频、日志服务、点云等。数据类型涉及结构化、半结构化、非结构化数据。

（2）数据全流程治理

数据加工预处理：依托标注平台、企业知识管理平台、模型训练平台等，完成原始数据初步治理。标注平台可完成智驾等垂类数据的标注处理，企业知识管理平台可完成非结构化数据挖掘抽取、大模型训练数据集预处理工作，模型训练平台可完成大模型预训练数据的加工。

数据开发：提供开发环境、任务管理、数据集成、数据治理等能力，对网页、表格、文本、音频、视频、点云等混杂的原始数据，开展清洗、转换、标注、格式规整、质量校验，剔除无效噪声数据，把零散原始素材加工为格式规范、质量可靠的可用数据集，为下层存储计算底座输出合格的数据原料。

大数据引擎：面向传统大数据业务，实现湖仓存储格式优化，支撑物理多租户环境下的实时增量计算分析，依托向量数据库提供语义向量存储检索能力，重点承载结构化、传统业务数据的离线统计、实时数仓分析业务。

智能数据湖：通过多模态数据处理引擎解析图片、音频、视频、点云等复杂数据，提供 AI 模型训练与推理算力，完成批流一体计算，专门服务多模态解析、模型训练、AI 挖掘类任务。

元数据管理：实施统一元数据管理和统一权限管理，实现对各类数据资源做集中访问管控，实现跨底座的数据可查、可管、可控，保障上层业务可以安全、高效调用数据资源。



图 8 多模态数据底座示意图

【方案案例】华为智能数据湖

智能数据湖是面向 AI 时代的智能数据平台，满足企业海量多模态数据的预处理需求，提供高性能的多模处理能力；支持文本、图像、音视频等多模态数据统一管理，兼容多样式格式，助力构建 AI 时代的数据竞争力。

智能数据湖提供多模数据引擎 Aura、AI 计算引擎 Ray、批处理引擎 Spark 和流处理引擎 Flink 四大核心计算引擎，聚焦多模数据处理、异构算力混合调度，开放湖仓处理，构建新一代多模湖仓架构，促进 Data+AI 协同创新。

智能数据湖（AI DataLake）以工作空间为载体，采用数据、资源、引擎三层解耦架构实现灵活高效的企业级数据管理：

数据与引擎解耦：所有引擎共享同一份数据，通过多模数据管理平台统一治理数据资产，避免数据孤岛和数据冗余，确保数据一致性。

资源与引擎解耦：支持多引擎共用资源池，细粒度管理通算、智算资源，通过资源的灵活配置和调度，提升资源利用率。

资源与数据解耦：数据跨智算与通算资源流通，灵活支撑交互式分析、多模分析、批处理、实时计算、AI 计算等多样化数据业务场景。

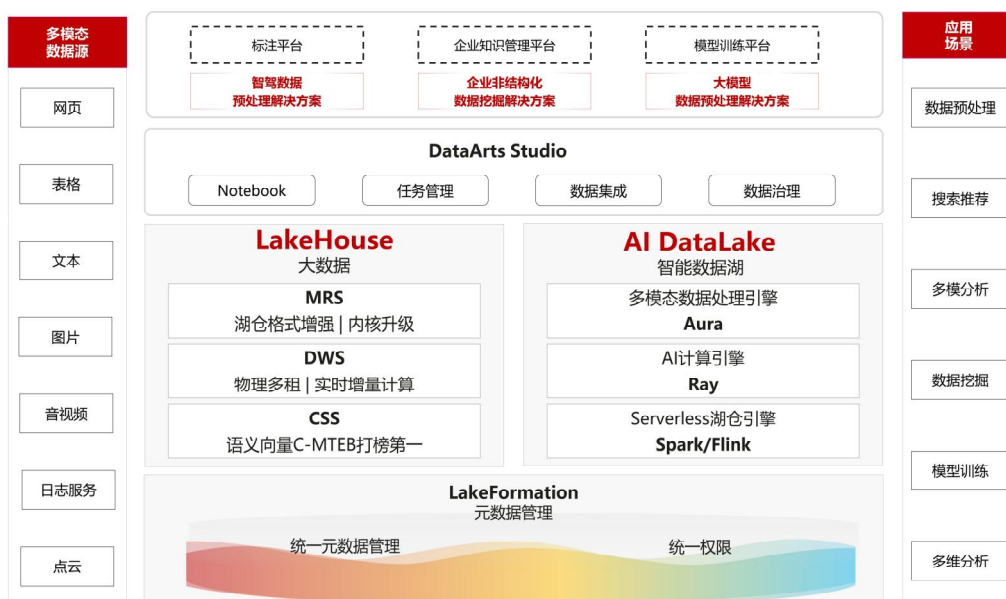


图 9 华为数据湖示意图

【应用案例】西安视频数据中枢

西安市视频资源整合共享平台,作为西安市公共支撑平台中的视频中枢,为西安市打造一个开放、共享的智能视频运营管理平台。通过汇聚、治理、共享全市视频资源,建立算法超市能力中心,为不同行业部门提供视频调阅、模型解析等支撑服务。

平台接入全市 16 万路以上的视频监控,整合公安、应急、城管、水务、秦岭保护、生态环境、区县等多部门视频资源,制定视频资源数据跨层级、跨部门的共享开放流程,推动视频数据建设、算法接入、联网汇聚、运行管理等多个规范标准编制,催化全市视频资源的规范建设。统筹西安市政务云昇腾算力资源,集约搭建共享开放的“算法超市”,在纳管各部门已建的算法技术上,针对公共安全、城市管理、民生服务等多领域,按需统筹规划视觉模型算法建设,实现算力算法资源集中建设、高效共享。除提供常态化视频共享支撑外,针对消防救援等部门的业务需求,在重点区域,搭建专属视频专题应用,有效识别现场情况,快速定位人员位置,实现视频能力与一线民生、应急业务深度融合。

3、数据一站式开发治理平台

数据一站式开发治理平台融合多模态数据底座和 AI 能力,打通多源异构业务数据,统一数据标准,提供数据集成、数据架构、数据质量、数据资产、数据安全、数据服务等功能,构建从数据接入到对外能力输出的端到端智能数据系统,实现数据从原始资源转变为可用数据资产的全生命周期管控,释放数据价值。

(1) 数据集成

全域数据集成: 实现政务业务、物联感知、空间地理、第三方、AI 衍生等多源异构数据统一汇聚,支持离线批量、实时流式多种采集方式,完成跨部门、跨设备数据接入,消除数据孤岛,为 AI CITY 提供完整数据输入来源。

统一链路监控: 对全部数据采集链路进行状态监控,实时监测连接状态、传输速率、异常报错,支持失败重试,及时发现接入故障,保障数据传输链

路稳定可靠。

自动分级分类:在数据接入环节,依据安全规范自动识别数据敏感等级,完成数据分级分类标记,为后续权限管控、隐私保护提供前置依据。

数据脱敏:接入阶段支持前置脱敏处理,对敏感字段进行屏蔽变换,在源头降低隐私泄露风险,输出合规的数据,支撑后续加工与 AI 使用。

(2) 数据架构

业务主题分组:按照城市业务域对数据进行主题域划分,如交通、安防、民生、网格等,实现数据按业务主题组织,便于业务理解、加工使用,适配 AI CITY 多业务场景。

数据标准管理:统一城市编码、字典、主数据等标准,规范字段值域、格式,解决多部门数据口径不一致问题,保障跨域数据融合,支撑 AI 实体识别与关联分析。

数据模型管理:统一管理逻辑模型、物理模型,支持模型导入导出、版本控制,对齐湖仓一体存储分层,规范库表结构,支撑 CHINER 元数建模工具对接。

业务指标设计:面向城市运营与 AI 研判,统一管理业务指标口径、统计逻辑,明确指标计算规则,保障业务报表、AI 态势分析指标统一。

发布审批管理:对模型、指标、主题的变更上线执行审批流程,管控架构变更,避免变更导致下游任务、AI 数据集异常,保障架构迭代可控。

(3) 数据质量

质量规则管理:维护数据完整性、唯一性、准确性、时效性、一致性质量规则库,支持自定义物联感知、政务表单、AI 样本的场景化校验规则。

质量作业配置:配置离线质检作业、实时质检作业,设置调度周期、脏数据处理策略,实现批量存量数据校验与实时流入脏数据拦截。

数据质量报告:自动生成质量统计报告,统计问题类型、问题数量、整改情况,用于评估业务数据、AI 数据集质量,为治理优化提供依据。

数据比对分析：支持跨源数据比对、历史版本比对，识别数据差异，发现数据不一致问题，用于台账核对、AI 样本正确性校验。

(4) 数据资产

数据地图：构建可视化数据资产地图，展示库表、API、数据集、时序资源，支持检索查询，展示业务释义、更新频率、质量评分，实现数据资产可查可用。

全链路血缘：构建从原始数据源、加工任务、数据资产、AI 应用的完整血缘，支持故障溯源、变更影响分析，快速定位指标、AI 推理异常根源。

实时元数据采集：自动实时采集库表、字段、接口、数据集元信息，动态更新元数据台账，保障数据资产地图、血缘信息与实际环境同步。

数据剖析：对数据做探查分析，统计字段值域、空值率、分布特征，辅助理解数据，为质量规则、模型设计、AI 样本筛选提供参考。

(5) 数据安全

统一权限配置：构建统一权限体系，权限细粒度到库、表、字段、数据集，区分运维、开发、业务、AI 算法账号，管控访问边界。

隐私数据保护：落实静态脱敏、动态脱敏，对个人敏感信息进行保护，输出脱敏数据集供 AI 训练，满足个人信息保护要求。

风险识别审计：识别越权访问、异常批量导出等高风险行为，留存完整审计日志，记录访问、修改、导出、模型读取行为，支持事后追溯。

数据使用申请：提供线上申请审批流程，业务、算法团队申请数据使用权限，完成审批后方可访问资产，实现数据使用流程化管控。

链路安全保护：对数据传输链路进行安全防护，加密传输，防止传输过程数据窃听篡改，保障 AI CITY 数据流转全链路安全。

(6) 数据服务

API 开发调试：支持数据 API 的开发、在线调试，将数据表、数据集封装

成接口，适配 AI 实时推理业务的低时延调用需求，也满足 AI CITY 模型训练场景大批量取数的业务需要。

API 审核发布：API 上线前执行审核流程，校验接口逻辑、安全策略，审核通过后正式发布，保障对外输出服务合规可靠。

API 授权流控：对调用方做授权管理，配置访问权限。设置限流、熔断策略，应对 AI CITY 高并发视频分析、多算法并行推理带来的大流量访问压力，对流量进行调度管控，防止服务崩溃、资源挤占，保障高并发场景下整套数据服务体系稳定弹性运行。

API 运行监控：监控接口调用频次、时延、成功率、报错信息，记录调用计量，便于运维定位服务异常，支撑各类城市智能化业务持续稳定运行。

数据共享交换：除 API 接口外，支持文件、数据集批量交付，实现跨部门、算法工厂的数据共享交换，兼顾 AI 训练大批量取数场景。



图 10 一站式数据开发治理平台示意图

【方案案例】华为数据治理中心平台（DataArts Studio）

数据治理中心平台(DataArts Studio)是数据全生命周期一站式开发运营平台，提供数据集成、数据开发、数据架构、数据安全、数据目录、数据服务等功能，支持行业知识库智能化建设，支持大数据存储、大数据计算分析引擎等数据底座，帮助企业快速构建从数据接入到数据分析的端到端智能数据系统，消除数据孤岛，统一数据标准，加快数据变现，实现数字化转型。分为标准版和铂金版两个版本，标准版只包含数据集成和数据开发功能，铂金版包含数据架构、数据质量、数据目录、数据地图、数据安全、数据服务高阶数据治理功能。

DataArts Studio 基于数据底座，提供数据集成、开发、治理等能力。DataArts Studio 支持对接所有华为云的数据湖与数据库云服务作为数据底座，例如 MRS Hive、数据仓库服务 DWS 等，也支持对接企业传统数据仓库，例如 Oracle、MySQL 等。



图 11 华为数据治理中心平台 DataArts Studio 示意图

【应用案例】海亮集团全域数据治理

海亮集团聚焦有色材料制造、教育服务事业、生态农业三大核心领域，布局 12 个国家和地区，营销网络辐射全球，连续四年上榜世界 500 强。海亮集团总系统业务 100+，但是数据分散在各产业的不同业务和系统中，协同分析需频繁迁移数据，易造成数据冗余，数据分析链路长，协同分析效率低。同时，数据无法复用，随着系统集成复杂度提升，开发维护成本递增。

为解决上述挑战，加速集团公司数字化转型，海亮集团基于华为云 DataArts 数据治理生产线，搭建了统一数据湖平台，将上百个重要系统、5000+张数据表单全部入湖，统一数据标准和口径，提升了数据质量，打通了数字工厂的全业务流程，实现全链路的数据管理、高效的数据流转。基于 DataArts Studio 提供的数据服务能力，实现成材率由 91%提高到 93%，单位产品综合能耗下降 300kwh，个别工序的劳动效率提高 3 倍。



图 12 海亮集团数据治理示意图

4、可信数据空间

可信数据空间作为 AI CITY 的关键可信协同基础设施，聚焦多主体之间数据安全流动与 AI 协同，保证数据流动可控、合规、可证。一方面打通多主体数据要素流转通路，为城市智能体的态势感知、推演决策提供高质量安全的数据供给。另一方面对数据使用目的、范围、行为进行全流程可控可证约束，满足数据安全、个人信息保护等合规要求。同时，依托多方安全计算(MPC)、

联邦学习（FL）、可信执行环境（TEE）、数据胶囊技术和数据交换空间，提供高效、安全的数据共享和协作能力，实现跨部门、政企、产业主体的数据联合分析、城市大模型联合微调与跨域智能计算，保障数据主权和隐私安全。

（1）连接器

异构系统对接：作为多方系统的接入适配单元，支持对接不同机构的业务平台、数据平台、AI 计算环境，屏蔽各方系统接口、协议差异，实现跨主体环境网络互通。

接入适配管理：统一管理各方接入端点，完成接入身份校验、链路连通性检测，维护接入对象台账，仅允许已授权主体建立数据通路。适配 AI CITY 各类本地数据源，如政务业务库、视频监控、产业数据库、业务 API 接口、物联感知数据、多模态城市感知数据等，实现城市域内异构数据的本地接入。

数据通路调度：根据业务申请，建立临时或持久化的数据交互通道，仅负责通路连通，不落地中转原始明文数据，为上层可信交换提供网络基础。

（2）策略管控

多维度控制策略配置：面向 AI CITY 城市业务生成定制化控制策略，针对业务明确约束数据的使用场景、调用频次、有效周期、敏感数据约束、城市大模型训练使用限制、禁止数据导出等规则。支持 AI 辅助风险校验能力，识别数字合约冲突、越权风险。数字合约作为跨部门协同的权威依据，将数据提供方、使用方、使用目的、使用范围、有效期、调用次数、计算方式、结果输出及禁止行为等约束形成机器可执行的策略规则，约束所有参与方的数据与 AI 行为，保障政务数据仅用于约定的城市业务。

运行时强制策略执行：统筹管控跨域数据交换行为，实时监测跨部门协同任务，识别超合约范围的访问行为并下发阻断指令。通过策略下发的方式，防范政务敏感数据违规流转。根据数据敏感等级和业务场景，支持“数据可控流通”和“数据不出域计算”两种可信协作模式；对高敏感数据通过隐私保护计算实现原始数据不出所属方环境，仅输出授权范围内的计算结果。

行为审计记录：汇聚城市所有接入连接器上报的全链路日志，机构身份

访问记录、数字合约执行记录、跨部门数据调用、城市 AI 任务运行、模型推理行为等。将关键业务证据上链存证，不可篡改。提供城市业务溯源查询能力，同时通过 AI 识别异常访问、违规调用行为，输出风险告警。满足政务监管、数据要素合规审计要求，保证城市跨主体数据协同行为全程可追溯、可举证。

权限与申请联动：和整体数据安全体系打通，依据数据使用申请审批结果动态加载对应控制策略，审批不通过则禁止发起数据交互。

(3) 数据胶囊

数据封装隔离：将待交互的数据、数据集、执行策略一同封装为数据胶囊，胶囊内部绑定数据权属标识、使用约束条件，胶囊外部无法直接解析原始数据内容。

跨域可信交换：胶囊在不同主体之间完成传输，传输过程中原始数据被隔离保护。接收方须按照胶囊内置的约束策略使用数据，无法脱离约束导出原始明文。

全生命周期跟踪：跟踪胶囊的分发、调用、销毁全生命周期，记录胶囊流转路径。结合可信执行环境、禁止使用方导出、复制等机制，任务结束后胶囊可自动失效销毁，降低数据被二次留存和违规复用风险。

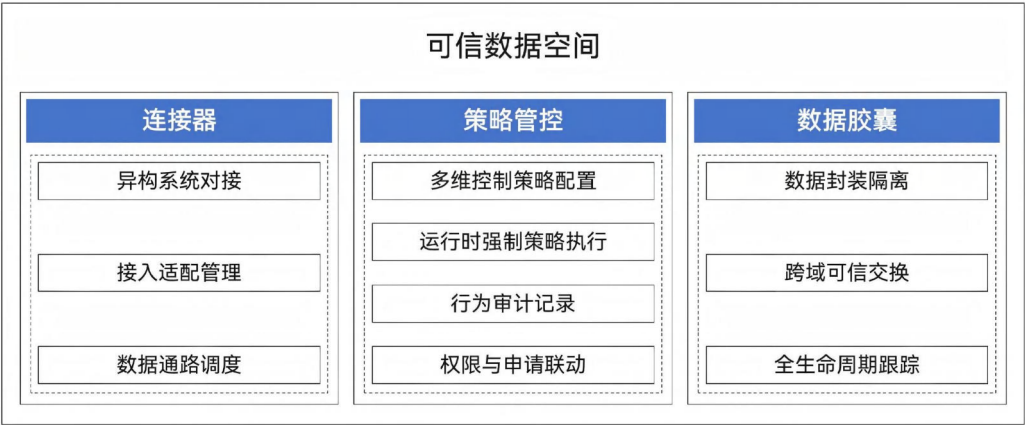


图 13 可信数据空间示意图

【应用案例】深圳南山区数据可信流通服务探索实践

南山区积极推进数据要素可信流通服务平台建设，在“数据要素×医疗”场景中，利用大数据、数据仓库、隐私计算、区块链等技术，打造“数据+平台+场景”一体化的医疗数据安全流通解决方案，可信流通服务平台连接南山医院等各方主体，实现了医疗健康领域的数据可信互联互通。依托医疗数据空间专区建设，激活了医疗健康行业数据，形成了可开发利用、可流通的高价值数据资产。

在医疗科研场景，医疗影像数据经过数据开发方的标注之后，形成高质量数据集，并基于可信数据空间实现数据集在医疗机构和科研机构间可控交换，辅助诊断模型训练效率大幅提升。

在医疗健康场景，基于医院的诊疗记录、住院结算费用等数据，在病人离院结算时，实现商业保险公司的直接赔付，借助合规开放就医数据，实现商保快赔平均 30 分钟内、商保直赔最快 3 秒内免材料赔付，降低保险公司理赔调查成本 50%以上。



图 14 南山区数据要素可信流通服务平台架构示意图

（四）模型体系

1、功能定位

（1）现实需求

当前，人工智能产业正从通用基础大模型的技术爆发阶段，加速向行业化、场景化、智能体化的纵深方向演进。构建多层次、多类型、可持续演进的 AI CITY 模型体系，是顺应技术趋势、破解落地痛点、支撑城市智能化升级的必然选择。

一是破解单一通用模型的垂直领域适配瓶颈。通用基础大模型的“通用化”属性，天然难以匹配城市垂直领域的专业规则、专属数据和精细化任务要求。在城市治理、公共服务、产业发展等核心场景中，差异化、专业化的智能需求持续升级，单一通用模型在领域知识深度、业务流程适配、任务精度达标等方面暴露出多重适配性问题，已成为制约城市 AI 规模化落地的核心瓶颈。

二是契合 AI 技术范式的行业共识转向。行业发展共识正从“追求单一模型参数规模”转向“构建分层协同的模型体系”。通过不同层级、不同类型模型的能力互补，能够实现 AI 能力的精准、高效、低成本供给。构建城市级模型体系，是顺应技术演进方向，将基础大模型的通用认知能力与城市专业知识、行业沉淀经验、场景任务要求深度融合的必由之路，能够为海量城市智能体和 AI 应用提供统一、灵活、高效的模型能力支撑，推动 AI 真正嵌入城市运行全链条。

三是扭转零散建设的资源浪费格局。传统“一个场景建一个模型”的零散建设模式，导致城市各部门、各领域模型重复建设、资源碎片化严重，同时抬高了人工智能应用的技术门槛。模型体系建设需面向城市人工智能应用全生命周期，统筹基础模型、行业模型、场景模型和端侧模型等多种模型资源，系统性降低城市各部门、行业企业和开发者使用人工智能的技术门槛。

四是支撑城市 AI 能力模式升级的底座需求。城市人工智能发展正经历两个关键转变，即 AI 能力供给从“单点模型建设”向“多模型协同供给”转变，应用模式从“拥有模型”向“使用模型服务”转变。构建开放兼容、统一管理、按需

服务的城市模型体系，是实现这两大转变的核心载体，能够为城市智能体规模化开发和 AI 应用创新提供公共模型能力底座，支撑城市 AI 可持续演进与全域赋能。

(2) 主要功能

当前城市 AI 建设普遍存在模型能力与业务需求适配性不足、资源分散建设重复、能力难以跨域复用等问题。单一通用基础大模型难以匹配城市垂直领域的专业规则与精细化任务要求，分散式的场景模型建设又陷入“一个场景建一个模型”的碎片化困境，既造成资源浪费，也无法支撑复杂城市治理任务的跨部门协同与规模化复用。

AI CITY 模型体系并非对现有模型资源与业务系统的简单替代或重构，而是建立在城市数字基础设施、公共数据平台、业务系统与各类 AI 能力之上的统一模型能力底座与协同供给层。其核心价值在于统筹多元模型资产、分层适配业务需求、统一服务供给标准，将基础大模型的通用认知能力与城市领域专业知识、场景任务要求深度融合，推动 AI CITY 能力供给从“单点模型建设”向“多模型协同服务”升级，从“重资产自建”向“轻量化复用”转型，为城市智能体规模化开发与全场景 AI 应用创新提供体系化支撑。

2、模型分类

(1) 基础底座模型

基础底座模型是整个模型体系的底层能力基座，主要涵盖**通用大语言模型、视觉基础模型、通用多模态大模型**等通用基础模型，核心作用是为 AI CITY 全类 AI 应用提供通用语义理解、视觉感知、多模态融合、逻辑推理等底层基础认知能力。该层级模型不直接面向具体业务场景输出定制化服务，而是作为公共能力源供上层各层级模型调用、微调与迭代，从源头保障 AI CITY 能力的统一底座供给，从根本上避免基础认知能力的重复建设与资源浪费。

(2) 通用认知与交互模型

通用认知与交互模型是城市级可共享的 AI 能力中台层，在基础底座模型的能力支撑下，面向城市跨部门共性业务需求提炼形成标准化通用认知能力，

主要包含三类模型。一是**城市垂类大模型**，覆盖政策解读、诉求工单研判、舆情分析、事件语义解析、咨询答复等城市通用政务与公共服务场景。二是**感知小模型**，涵盖图像识别、目标检测、OCR、行为识别、音频识别等通用感知处理能力。三是**知识推理模型**，支撑人、地、事、物、组织关联分析、知识图谱推理等通用知识应用需求。该层级模型不绑定单一部门的专属业务流程，可在多个委办局、多类业务场景中复用推广，是实现城市 AI 能力跨域共享、降低重复建设成本的核心中间载体。

(3) 城市业务域专用模型

城市业务域专用模型是模型体系对接具体城市业务的核心执行层，主要包含**领域大模型、专用小模型、业务机理模型**三类，按照城市治理、民生服务、产业经济、交通运行、市政管理等不同业务领域划分，分别对应对接各领域业务系统，聚焦处理各领域的具体城市任务，典型应用场景包括信号灯智能配时仿真、政务服务全流程智能办理、行业市场智能监管研判等。该层级模型在通用认知能力的基础上深度融合领域专业规则、专属业务数据与业务流程逻辑，在保证业务处理精度与性能的同时，兼顾部署成本与响应速度，是模型能力落地赋能具体业务场景的关键执行载体。

(4) 仿真推演与决策世界模型

仿真推演与决策世界模型是面向城市复杂治理决策的高阶模型层，主要包含**城市世界模型（City World Model）、城市混合仿真模型、决策推理模型**三类，核心作用是模拟、推演和预测城市运行的复杂动态变化，支撑城市突发事件推演、政策实施效果模拟、重大活动保障仿真、灾害连锁效应模拟等复杂决策场景。该层级模型整合多领域业务数据、城市空间地理数据与各层级模型能力，通过 AI 算法与传统机理模型的深度融合，构建城市数字孪生的智能内核，实现对城市运行态势的全景感知、动态模拟、趋势预判与方案优化，驱动城市治理从被动响应向主动预判、从经验决策向科学决策升级。

(5) 物理感知与执行模型

物理感知与执行模型是模型体系对接城市物理世界的感知触角与执行末梢，主要包含**轻量化感知小模型、边缘时序预测小模型、端侧简单推理模型**

等微型轻量化模型，部署运行在摄像头、传感器、燃气终端、水务设备、路口信号设备等各类城市终端设施之上。该层级模型聚焦前端物理场景的实时感知与即时执行需求，侧重低时延、轻量化、本地化的推理计算，负责前端数据采集、实时状态识别与简单指令响应，既保障了终端场景的响应效率，也可在本地完成基础数据处理以降低数据传输压力与隐私泄露风险。

上述五类模型并非孤立运行，而是通过“云-边-端”三级部署架构形成分层联动、协同互补的有机运行体系。云端集中承载计算密集型的基础底座模型、城市业务域大模型、仿真推演与决策世界模型等，负责全局知识沉淀、跨域资源调度、复杂决策推演与全域模型统筹管理。边缘端部署中等规模的领域专用模型与区域感知处理模型，承接云端能力下沉，处理区域级需要低延迟的本地实时任务，实现就近计算与快速响应。终端侧运行各类微型轻量化模型，负责前端物理世界的数据采集、即时感知与简单执行反馈。在该协同架构下，云端大模型可通过知识蒸馏、指令适配等方式指导边缘与终端小模型的迭代优化与能力提升，城市世界模型也可调用云端大模型的通用认知与跨域知识提升推演的全面性与精准度，最终形成“云端统筹、边缘协同、终端执行”的联动格局，实现模型资源的最优配置与城市 AI 能力的高效协同运行。

3、MaaS 模型即服务

针对当前大模型技术迭代快、种类激增带来的选型复杂度高、部署运维成本重、资源复用效率低等痛点，模型体系以 MaaS（Model as a Service，模型即服务）为核心服务载体，将不同来源、不同层级、不同类型的模型资源统一汇聚并进行服务化封装，转化为标准化、可按需调用的 AI 能力供给。MaaS 的核心价值是解决模型能力“高效复用、低成本落地”的问题，是降低政府部门、行业企业和开发者使用门槛，推动城市 AI 从“重资产自建模型”向“轻量化使用服务”转型的关键支撑，也是实现模型体系从“资产汇聚”到“价值释放”的核心枢纽。

MaaS 本质是以 AI 模型为核心的云化服务模式，通过对模型能力进行云化抽象与服务化封装，将基础大模型、行业模型、场景模型等各级能力封装为标准化 API/SDK 接口，支持按需调用、按量计费。其兼容公共云、专有云、

混合云等多种部署形态，用户无需从零构建和训练模型，可直接依托预训练模型开展推理调用或定制化微调，大幅压缩开发周期、降低技术投入与运维成本。围绕模型服务全链路，MaaS 具备六大核心能力。

一是统一模型广场与资源目录管理。汇聚主流基础大模型、多模态模型、行业领域模型及城市自研专属模型，构建开放共享的城市模型资源目录，明确模型能力边界、规格参数、性能指标与适用场景，实现模型资源的统一发现、统一检索、统一选型。支持预置模型开箱即用，并建立常态化接入机制，根据城市治理、公共服务、产业发展的实际需求持续引入主流通用模型与垂直专业模型，持续丰富城市模型供给池。

二是在线体验与智能选型支撑。提供多模型在线体验、参数调优与效果验证能力，支持开发者围绕具体业务任务开展横向能力比对、效果测试与成本测算，综合模型准确率、响应时延、调用成本、安全合规性等维度快速匹配最优模型，大幅降低前期选型验证的时间成本与试错成本，破解模型种类繁多带来的选型难题。

三是标准化 API 能力服务供给。将文本生成、代码生成、视觉理解、多模态生成、向量检索等各类模型推理能力封装为统一标准的 API 服务，面向城市各类应用与智能体提供统一调用入口。业务开发者无需关注底层模型部署架构、运行环境与基础设施运维，即可快速集成 AI 能力，将更多精力聚焦于业务逻辑创新与场景落地。

四是定制化调优与专属模型生成。针对政务服务、城市治理、产业发展等场景对专业知识与业务准确性的高要求，依托城市高质量公共数据与行业专属数据，提供全参微调、LoRA 轻量微调等多种模型优化能力，支撑通用大模型向城市专业模型、场景专属模型转化，沉淀可复用的领域化模型能力，实现通用能力与城市专业需求的深度适配。

五是弹性部署与高效推理服务。提供模型快速部署与在线推理服务，具备推理加速、弹性资源调度、实时运行监控等能力，保障模型服务的高性能与高可靠性。可根据不同应用的业务规模、时延要求与安全等级灵活配置推理资源，实现模型从开发成果到生产级服务的快速转化与平滑上线，匹配城

市不同场景的差异化运行需求。

六是全链路统一运营运维管理。建立覆盖模型资产、版本迭代、调用服务、运行状态的全链路统一管理机制，持续监测模型调用量、响应时延、准确率、服务可用性等核心指标，支撑模型版本迭代、服务更新与性能优化，保障城市模型能力持续迭代升级、稳定高效供给，实现模型服务的全生命周期闭环运营。

通过 MaaS 建设，模型从分散的技术资产转变为可统一汇聚、灵活选择、快速验证、按需调用、持续运营的城市公共 AI 服务，既打破了大模型应用的技术门槛与成本壁垒，也构建起连接“模型供给侧”与“城市 AI 应用侧”的核心服务枢纽，支撑模型体系价值的高效释放，推动城市 AI 能力规模化、普惠化落地。

4、模型一站式训推平台

模型一站式训推平台集“多模态数据管理、交互式协同开发、大规模推训一体、标准化模型评测、多形态灵活部署”等功能于一体，打通“数据准备-算法开发-模型训练-调优评测-部署上线-运维迭代”AI 应用开发全链路，满足不同行业、不同场景的差异化 AI 开发需求，降低 AI 开发门槛，缩短大模型开发上线周期，为各领域 AI 应用的规模化落地提供全生命周期工程化底座。模型一站式训推平台向下统筹多元算力基础设施，实现算力资源的灵活切分、弹性调度与高效运维。向上兼容业界各类主流基础模型，支撑通用大模型研发、行业垂直大模型应用和智能体应用开发。

(1) 模型开发

智能数据开发：面向 AI 大模型预训练与微调等数据生产场景，支持多源多模态数据接入与格式统一转换，集成智能清洗过滤、样本去重、自动标注、质量评估与样本增强合成等功能，输出适配大模型训练、微调的高质量数据集，打通大模型开发的数据工程全流程，解决行业大模型开发的数据预处理痛点。

模型训练：面向“高性能、高利用率、高易用、高可靠”大模型推训服务需求，支持万亿级混合专家 (MoE) 稀疏分布式训练、轻量化多领域微调 (Multi-

LoRA)、原生多模态早期融合预训练等先进训练能力，具备断点续训、全链路可观测等工程保障能力。

模型推理：面向 Agent 智能体应用场景，支持基于可验证强化学习技术的逻辑推理能力、原生多模态推理能力、百万 Token 超长上下文深度理解能力与长链路执行能力，满足复杂任务的高并发与深度思考需求。

模型测评：针对基座模型、行业模型开展自动化与人工相结合的综合评测，预置通用与行业领域评测数据集与多维度评价指标，从知识能力、逻辑推理、指令遵循、多模态理解、安全合规、生成质量等维度对模型进行量化打分，支持多模型、多版本之间的横向比对，支持样本溯源回流，输出完整可追溯的评测报告，为模型迭代优化、版本选型上线提供客观依据。

模型部署：支持训练与微调后的基座模型、行业定制模型快速封装上线，提供云服务推理、批量离线推理、边缘下发等多种部署形态，集成模型量化压缩、推理引擎适配、分布式调度、弹性扩缩容与流量流控等能力，支持“云-边-端”弹性部署，配套服务监控与故障恢复机制，实现各类大模型的工程化落地部署。

(2) 模型运营运维

智能运维：面向大模型推理业务，提供服务状态监控、性能指标观测、异常告警、日志全链路留存、流量管控、弹性扩缩容、模型版本灰度切换、访问权限与安全审计等功能，实时识别业务运行中的故障与风险点，结合业务反馈沉淀问题样本，支撑模型持续迭代，保障大模型服务稳定、安全、高效。

资产管理：实现基座模型、微调模型和多模态模型等各类模型资产的统一收纳管理，支持模型版本归档、元信息记录、来源溯源与权限分级管控，对接数据集、训练任务形成资产关联，支持模型资产的共享分发、重复利用与全生命周期档案管理，满足实验复现、安全审计和多项目协同开发的管理需求。

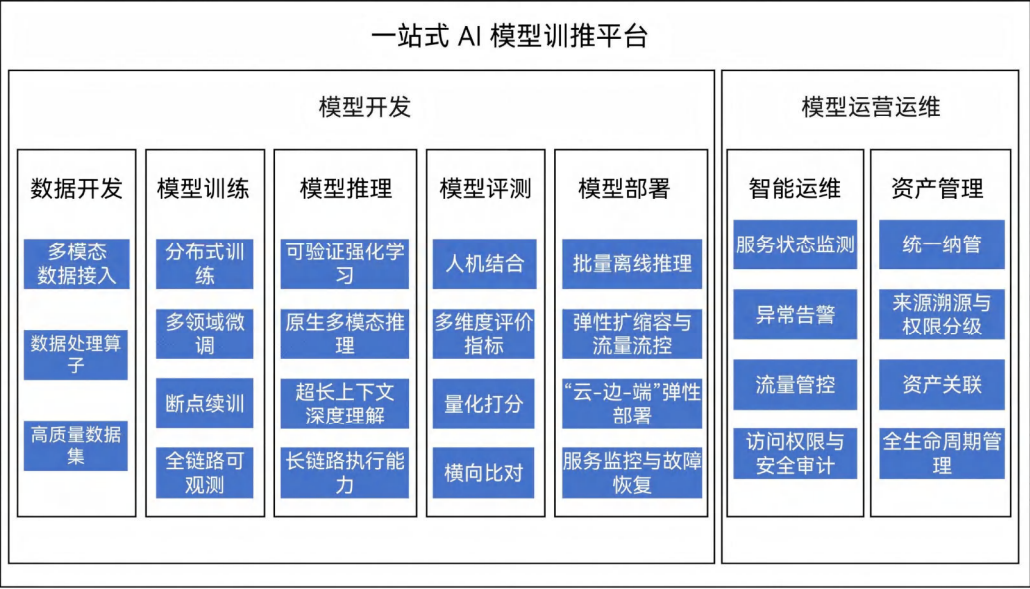


图 15 模型一站式训推平台示意图

【方案案例】华为魔坊（ModelArts）模型训推平台

ModelArts 是面向开发者的一站式 AI 开发平台，为机器学习与深度学习提供海量数据预处理及半自动化标注、大规模分布式训练、自动化模型生成，及端-边-云模型按需部署能力，帮助用户快速创建和部署模型，管理全周期 AI 工作流。平台提供算法开发、模型训练、部署上线、资源管理的全生命周期工具链，旨在显著降低 AI 应用开发的技术门槛与时间成本，让开发者能更专注于业务创新本身。同时，ModelArts 底层兼容多种异构计算资源，并提供多元化的资源调度能力，并全面支持 MindSpore、TensorFlow、PyTorch、Ascend-vLLM、LLamaFactory、Verl 等主流框架，使开发者无需深究底层基础设施，即可灵活调用强大算力。



图 16 华为一站式训推平台 ModelArts 示意图

【应用案例】国产化智驾解决方案研发场景

针对大模型迭代更新速度慢、大量数据资源治理难等痛点问题，某车企采用一站式训推平台构建高性能、低成本、高稳定性的国产化智驾解决方案。一站式训推平台能够处理 PB 级路采多模态数据，支持图像、点云数据的批量处理、智能标注与数据集版本管理。平台支持感知、预测、规控类自动驾驶模型的分布式训练、评测迭代与端侧部署。平台具备断点续训、训练全链路监控能力，支持“云-边-端”部署链路，支持训练模型实时下发、模型评测与问题样本回流，构建起“数据处理-模型训练-仿真验证-迭代优化”的研发闭环，有效提升数据生产与模型训练全流程研发效能，降低智驾模型工程化落地门槛，助力自动驾驶技术加速落地。



图 17 国产化智驾解决方案研发示意图

（五）Agent 体系

1、功能定位

（1）现实需求

城市业务具有事项流程复杂、参与主体多、数据分散、系统异构、跨部门协同频繁等特点。现有 AI 应用大多以单点场景和独立系统建设为主，普遍存在能力分散、重复建设、业务流程割裂、跨部门任务协同难、AI 能力规模化复制难等问题。特别是面对复杂城市治理任务，依靠单一模型或单一应用难以完成从需求理解、任务拆解、资源调用到跨部门协同执行的全过程。随着城市业务复杂度上升以及人工智能技术更新迭代，城市需求从鼓励人工智能试点应用逐步向推动智能体普及应用、加快高价值场景落地、形成可复制样板扩展。

与此同时，随着智能体进入城市核心业务场景，城市对智能体发展的要求从“能用”向“好用、可信、可控”转变，关注重点从“能不能执行”向“能否安全、可靠、持续地执行”转变，更加突出“发展与治理并重”。例如智能体在进入政务核心业务流程的同时，需要同步建立身份、权限、审计、评测、风险控制和责任追溯机制。

（2）主要功能

当前，人工智能发展从技术突破和能力验证阶段，加快进入以场景应用、规模普及和规范治理为重点的新阶段，Agent 技术正在形成“连接—协同—专业化—自主执行—经验沉淀—工程治理—持续进化”的发展路径。其核心变化是，人工智能不再只是被动响应请求，而正在成为能够连接城市数据、系统和设备，理解复杂业务目标，组织多个专业能力协同执行，并在运行过程中持续学习优化的新型数字执行主体。这为人工智能可控可靠地解决复杂城市业务问题、实现跨部门协同执行提供了技术基础，为城市智能体规模应用提供了现实可能。

AI CITY 需要构建统一、协同、可信的城市级 Agent 体系，以智能体作为连接“人、模型、数据、系统、设备”的新型数字化执行单元，形成覆盖智能体

开发、运行、协同、治理和运营的统一体系。通过城市级智能中枢统筹调度、业务智能体协同编排、委办局专业智能体执行，将传统以系统和数据为中心的数字化架构，进一步演进为以任务和智能协作为中心的新型城市智能架构。

Agent 体系并非是对现有业务系统的简单替代，而是建立在现有数字基础设施、数据平台、业务系统和 AI 能力之上的智能化协同层。其核心价值在于理解业务意图、组织已有数字能力、驱动业务流程执行，并通过多智能体协同实现跨系统、跨部门、跨层级的任务闭环，从而推动城市智能化由“单点智能”向“群体智能”、由“辅助决策”向“协同执行”持续演进。

2、智能体一站式开发与运行平台

面向城市智能体规模化建设和持续运营需求，构建统一的智能体一站式开发与运行平台，提供覆盖智能体设计、开发、调试、部署、运行、评测和运营运维的全生命周期能力，支撑城市智能体统一生产、统一运行、统一资产管理和统一运营。为各业务部门和生态伙伴快速构建专业智能体提供标准化工具和运行环境，降低各部门智能体建设门槛，同时保障智能体在复杂业务环境下的安全运行、高效运维与精准资产调用。助力城市智能体从分散开发、单点试用向统一建设、规模应用演进，为城市级多智能体协同体系建设提供统一技术基础。

（1）智能体开发

模型、知识与工具：面向不同业务场景统一接入大语言模型、多模态模型、向量模型等模型服务，并通过知识库和检索增强等方式，将政策文件、业务规则、专业知识和历史案例转化为智能体可理解、可检索、可调用的知识资源，为智能体开展专业分析、推理和任务执行提供支撑。将既有业务系统、数据服务、算法能力及各类数字工具封装为智能体可发现、可调用的工具能力，形成统一的工具注册、管理和调用体系，使智能体能够根据任务需要动态调用外部能力。

开发支持：提供低代码、高代码和自然语言辅助构建等多种开发模式，支持智能体、工作流、多智能体及复杂业务应用的灵活编排。开发过程中可按需组合模型、提示词、知识、记忆、工具和业务流程，既支持业务人员快

速搭建，也满足专业开发人员复杂业务逻辑和深度定制需求。

（2）智能体运行

安全与隔离：构建面向城市业务的智能体运行环境，为模型调用、工具执行、代码运行和复杂任务处理提供安全隔离、弹性调度和可靠运行保障。提供安全隔离的代码执行环境，支持代码执行、文件管理、系统命令执行等复杂任务，支持智能体安全可控地自动化执行。

记忆与协同：通过上下文管理、短期记忆和长期记忆等机制保持任务状态和业务上下文联通，支撑长流程、多步骤和复杂业务任务持续执行。在多种身份认证与网络管控保障下，支持智能体与存量业务的数据联通，支持安全合规开展智能体外部调用。

（3）智能体运营运维

自动观测与评估：构建覆盖开发态和运行态的智能体标准化、自动化评估体系，对用户交互、模型推理、知识检索、工具调用、任务执行等全过程进行链路追踪和轨迹分析。建立离线评估与在线评估相结合的质量评价机制，通过测试数据、真实运行数据和典型问题数据持续评估任务成功率、准确性、稳定性、效率、安全性及业务效果，结合智能评判、问题归因和典型数据回流机制，形成智能体质量持续改进的数据基础。

自优化：基于智能体运行过程产生的会话轨迹、任务结果、用户反馈和业务评价，建立“运行数据回流—效果评估—问题诊断—能力优化—重新验证”的持续优化闭环。在模型层，可结合高质量交互数据和客观奖励信号，对特定模型能力进行持续训练和优化。在智能体应用层，可在不改变基础模型权重的情况下，对 Prompt（提示词）、Skill、工具描述、调用规则和记忆等关键组成要素进行单项或联合优化，持续提升复杂任务成功率、执行效率和资源使用效率。

统一资产管理：建设城市智能体资产体系，开展智能体统一注册管理，支持智能体共享和复用。将成熟的智能体模板、模型、提示词、知识库、工作流、MCP 服务、插件和 Skill 等沉淀为标准化资产，逐步形成可复制、可推广的城市智能体资产库。各部门可基于已有资产快速组合形成新的业务智能

体，减少重复建设。

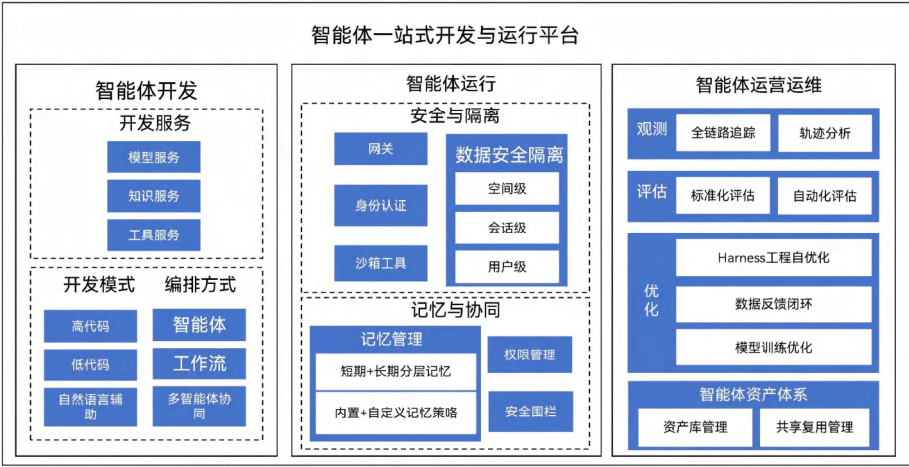


图 18 智能体一站式开发与运行平台示意图

【方案案例】华为智果（AgentArts）企业级智能体平台

随着企业大模型应用从“原型试验”走向“核心生产场景”，如何保障智能体在复杂业务环境下的安全运行、高效运维与精准资产调用，成为企业规模化部署的挑战。为此，华为面向企业级核心业务场景打造华为智果（AgentArts）智能体平台。平台基于 Harness 最佳实践构建标准化的开发与治理框架，专注于解决智能体在企业复杂环境下落地难、运行不可靠、运维无抓手等痛点，致力于降低应用门槛，助力企业将 AI 能力与实际业务深度融合，实现规模化落地。平台兼容业界主流开源大模型，提供安全可靠的企业级运行底座、长短期记忆、海量行业资产精准调用与全链路运营运维体系，帮助企业快速组建高可信的 AI 数字员工团队，助力大模型真正转化为企业核心生产力。



图 19 华为智果（AgentArts）企业级智能体平台示意图

3、多智能体协同

传统单智能体通常面向单一任务或单一部门，能够完成知识问答、信息查询、流程辅助等局部任务，但面对跨部门、跨系统、跨领域的复杂业务时，容易受到能力边界、数据边界和职责边界限制，难以独立完成从需求理解、任务拆解、资源组织到协同执行和结果汇聚的全过程。面向城市治理和公共服务中的复杂业务场景，需要构建城市级多智能体协同体系。通过多智能体协同，将复杂业务任务拆解为多个专业子任务，并由具备不同职责和能力的智能体协同完成，推动城市人工智能从单点智能向群体智能演进。

城市级多智能体协同体系包含安全可信云底座、城市级智能调度与协同中枢、核心引擎、专业智能体，形成“**城市统一统筹、业务协同编排、部门专业执行**”的多层次智能协作体系。

安全可信云底座：依托城市公共云基础设施、城市数据底座等为多智能体体系提供统一的算力、存储、网络、模型、安全和信创适配能力，通过身份认证、权限控制、运行隔离、日志审计、数据安全和可靠性保障机制，为多智能体在城市核心业务场景中的持续稳定运行提供基础支撑。

城市级智能调度与协同中枢：依托城市级智能调度与协同中枢，统一承接城市治理和政务服务需求，负责复杂业务意图理解、任务拆解、能力匹配、协同调度、过程统筹和结果汇聚等。针对跨领域、跨部门复杂诉求，城市智能中枢能够将整体业务目标拆解为可执行任务，动态组织相关专业智能体协同完成，实现从统一受理到协同执行的城市级任务闭环。

多智能体协同引擎：负责复杂意图识别、任务拆解、智能体发现、能力匹配、跨域编排、状态管理和协同调度，解决多个智能体之间“如何发现、如何分工、如何协作”的问题。

单智能体执行引擎：负责专业任务规划与执行，以及对模型、知识、数据、工具、API 和业务系统的调用，解决单个智能体“如何完成专业任务”的问题。双引擎协同形成“统一调度—任务分解—专业执行—结果反馈”的完整业务闭环。

专业智能体：围绕不同委办局职责和城市运行专业业务领域构建专业智

能体，将部门业务规则、专业知识、数据资源、业务流程和现有信息系统能力进行智能化封装。专业智能体既可独立完成本部门业务任务，也可接受城市智能中枢的协同调度，与其他专业智能体共同完成跨部门任务。在协同过程中，优先通过能力调用和结果交换实现协作，减少原始数据跨域流转，在保障数据安全和部门职责边界的基础上实现业务协同。

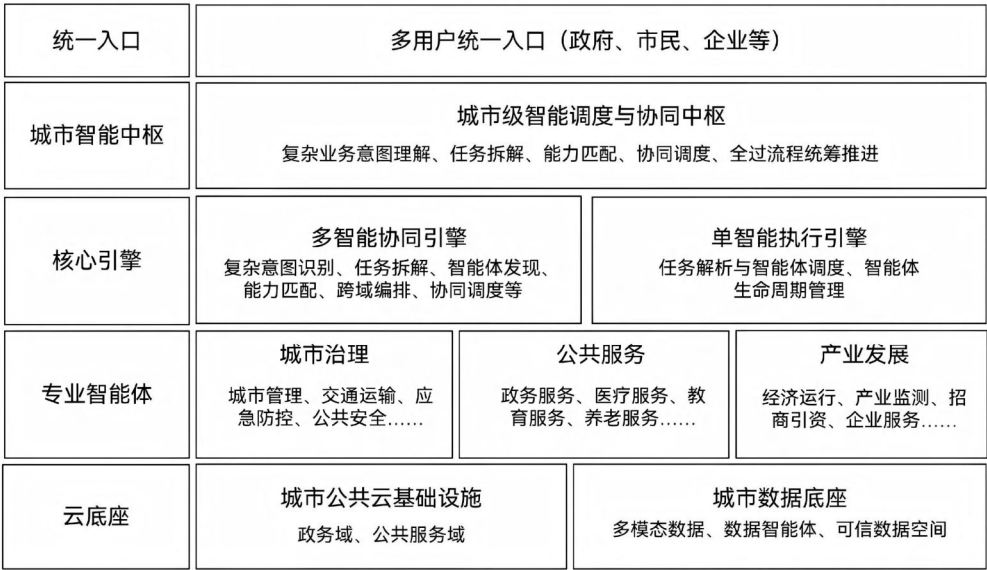


图 20 多智能体协同总体架构示意图

【应用案例】克拉玛依城市超级智能体建设

克拉玛依市以跨部门复杂业务场景为切入，探索开展“城市统一统筹、业务协同编排、委办局专业执行”的多智能体协同模式建设，通过构建城市级智能中枢，对复杂业务诉求进行统一理解、任务拆解和协同调度，并按业务需要调用不同委办局专业智能体完成具体任务，形成跨部门、跨系统的智能协同闭环。

技术流程方面，城市级智能中枢接收业务诉求后，按照业务目标拆解形成多个专业核查任务，并协同调度相关委办局智能体。各委办局智能体依托本部门职责、业务规则、数据资源和系统能力完成专业分析与核查，再将结果返回城市中枢，由中枢进行汇总、校验和综合研判，形成面向业务人员的统一结果，形成“中枢-业务-委办局”多智能体治理架构。该模式改变了传统跨部门业务依赖人工逐部门协调、逐系统查询的处理方式，将原本分散在不

同部门和系统中的专业能力以智能体形式组织起来，通过统一调度实现跨部门业务协同。在保障各部门职责边界和数据安全的前提下，重点实现“能力协同、结果协同”，提升复杂业务场景的协同效率和可控性。

目前克拉玛依市在民生服务等多领域初步形成了“城市中枢统一调度、委办局智能体专业履职、多智能体协同完成复杂任务”的城市超级智能体实现路径，为后续扩展至城市治理、政务服务、应急处置、经济运行等更多跨部门场景，推动城市智能体规模化建设和统一治理提供了实践基础。



图 21 克拉玛依市城市智能体总体架构示意图

4、智能体监管

智能体快速发展背后，治理体系滞后、风险隐患凸显等问题不容忽视。一是数字身份缺失。智能体未与所有者法定身份有效绑定，无法将智能体行为精准归至对应责任主体，攻击者可以轻易创建仿冒的智能体进行诈骗或散布虚假信息，单个智能体的劳动成果、交易历史和信誉无法被量化和记录，多个智能体之间的可信交互与协同也难以保障。二是执行链路不明。智能体的决策依赖于大模型的动态推理和记忆上下文，其操作链条复杂且隐蔽，决策和执行过程为“黑箱”操作，导致其行为难以被有效追踪和审计。目前普遍缺乏对提示词、工具调用、中间决策等关键环节的结构化日志记录，使得追溯智能体“何时、何地、做了什么”变得极其困难。三是责任边界难定。智能体

的行为涉及基础模型开发者、技能插件开发者、部署平台以及最终用户，当智能体自主决策造成损害时，导致“监管找不到主体，追责分不清责任”。且智能体具有极强的跨场景性，可能同时涉及网信、工信、公安等多个部门都有管辖权，导致监管重叠与监管真空并存。

区块链技术具有多中心、防篡改、透明性、可追溯等特征，可以弥补智能体应用面临的身份、行为、监管等非可信难题。需面向智能体深化与区块链技术的融合应用，构建智能体可信监管体系，主要包括智能体可信身份监管、执行链路全过程监管和安全监管。

智能体可信数字身份监管：基于国内区块链公共设施平台（如国家信息中心牵头的区块链服务网络 BSN）建立“中心化签发、分布式认证”的 AI 智能体数字身份管理体系。有关监管部门作为法定签发方统一注册、审核并签发 AI 智能体的数字身份凭证，明确所属企业、职责范围、权限边界、人类监护人等关键信息，确保身份来源的权威性与合法性，实现身份确权与全生命周期管理。进一步利用区块链构建分布式节点网络进行身份验证，满足海量数字身份高并发验证需求，确保智能体身份可验证、主体可辨识、责任可界定。

智能体执行链路全过程监管：基于区块链智能合约和不可篡改特性，开展智能体行为约束和操作行为存证监管。一是将智能体的行为边界、操作权限、风险控制策略等规则以“智能合约”的形式编码上链，智能体的所有操作都必须通过这些预设规则的校验才能执行，实现“代码即法律”的硬约束，有效防止其越权或做出有害行为。二是将智能体的所有操作行为上链，确保行为的可追溯性和不可抵赖性，监管机构作为节点接入区块链，实现对智能体行为的实时、穿透式监管。三是建立智能体信用评级体系，基于智能体完成任务的质量、效率、协同和合规情况，动态评价其信誉情况，设计动态激励与惩罚机制，打造智能体经济良好发展生态。

智能体安全监管：建立智能体协同管理机制，制定面向智能体行为监管的行业规范，建立安全认证和备案机制，通过多重安全检测、数字签名认证等手段，防范恶意插件注入风险，规范技能供应链安全。推进智能体分级管理，根据智能体所需的系统权限和操作范围，将其划分为低风险、中风险、高风险等级别。对高风险智能体，实施强制性的安全认证和备案制度，强制

智能体开发企业披露模型的基本原理、训练数据来源、潜在风险及应对措施。

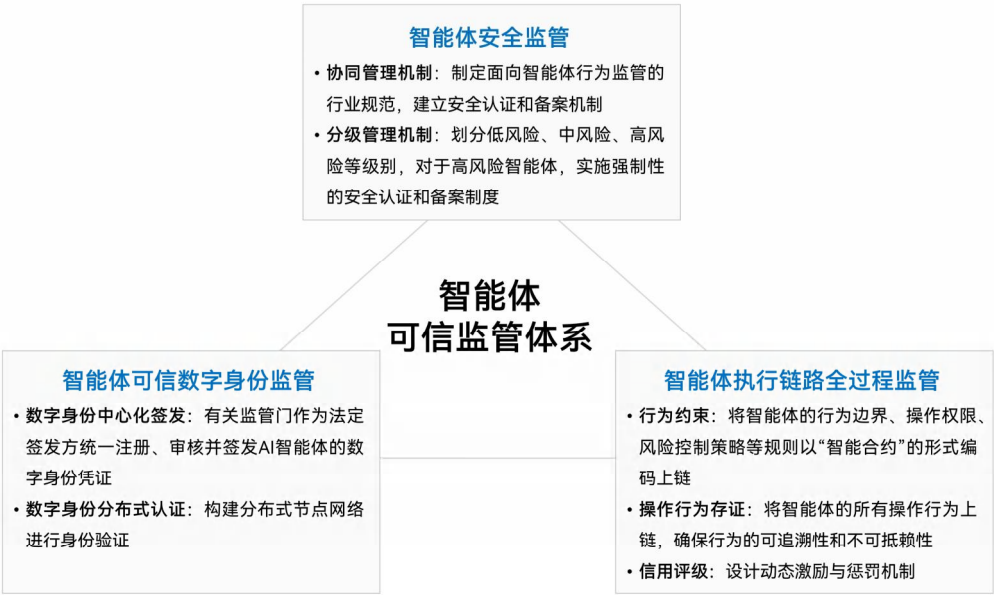
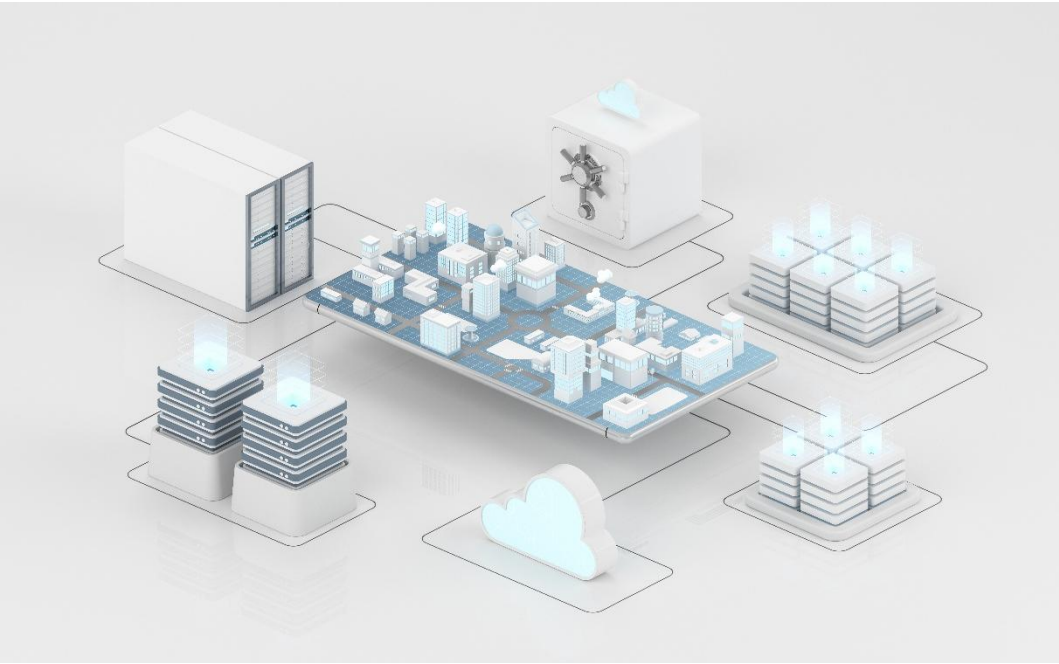


图 22 智能体可信监管体系示意图



(六) 数智专业服务体系

1、功能定位

(1) 现实需求

算力、数据、模型、智能体等技术能力建成后，如果缺乏标准化、一站式、全流程的配套服务体系，会导致底座复用率低、落地门槛高、技术与业务脱节、迭代成本高，技术能力难以快速转化为实际应用价值。需要一套覆盖 AI CITY 建设运营全环节全流程的专业服务体系，保障其健康可持续运行。

(2) 主要功能

数智专业服务体系作为贯穿 AI CITY 整体架构的落地保障能力，覆盖城市公共云、数据、模型、智能体四大核心板块，以“轻量化接入、低门槛使用、全生命周期运维、可快速迭代”为核心目标，构建标准化、通用化、普惠化的 AI 全栈服务能力。数智专业服务体系具体包括四方面专业服务，AI Infra 规划设计与集成实施服务助力打造安全、智能底座，数据专业服务助力数据治理、发挥数据价值，模型专业服务提升模型能力与落地效率，智能体专业服务助力 AI CITY 实现智能化应用的快速构建与迭代。通过系统化的 AI Infra、数据、模型和智能体专业服务，打通技术底座与城市业务场景的衔接壁垒，降低政府部门、行业单位、开发者的 AI 应用建设成本，实现各类 AI 能力开箱即用、快速部署、持续优化，保障城市 AI 体系长效运营、规模化落地。

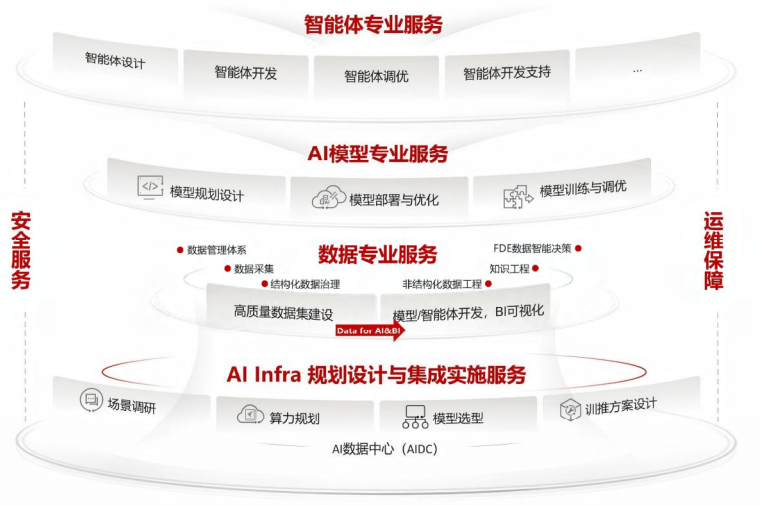


图 23 数智专业服务体系示意图

2、AI Infra 专业服务

AI Infra 专业服务聚焦 AI 基础设施全流程建设与落地，围绕算力、存储、网络等底层资源，提供从前期规划、方案设计、建设实施、监控、调优等一体化专业服务。核心目标是为城市打造安全稳定、资源集约、Token 效率最优的 AI 基础设施，支撑上层数据、模型、智能体全链条能力运转。

在具体服务内容上，AI Infra 专业服务紧扣基础设施落地全流程，通过统一规划城市 AI 算力、存力、网络资源，实现算力集约化建设与弹性调度，解决传统基础设施分散建设、资源利用率低、训推脱节、峰值资源不足等问题。同时依托专业化集成部署能力，打通云、边、端基础设施资源壁垒，为城市 AI 场景创新、模型训练推理、智能体持续运行提供高可用、高性价比、可扩展的底层硬件与算力服务支撑。



图 24 AI Infra 专业服务示意图

3、数据专业服务

数据专业服务的核心定位是构建 AI-Ready 的高质量数据集，为大模型训练、智能体场景应用提供适配业务的高质量数据支撑。数据服务帮助建立标准化、规范化、安全可控的 AI 数据集全生命周期服务体系，解决城市数据质量参差不齐、标准缺失、模型适配度不足、安全共享困难等核心问题。

数据专业服务覆盖数据采集获取、多模态加工处理、数据集治理、质量管控、标准规范建设、安全共享、场景应用全链路。服务支持文本、图片、

音频、视频等城市数据全模态，配套完善的 AI 数据集管理政策、分类规范、质量管理机制与安全共享机制。通过人机协同模式，完成数据标准化、血缘梳理、质量稽核、资产沉淀等，形成可直接用于模型训练、智能体推理的优质语料与知识库，让城市数据深度适配 AI 业务场景，实现数据价值高效释放。



图 25 数据专业服务示意图

4、模型专业服务

模型专业服务主打全栈低门槛服务能力，让非专业业务团队也可快速落地大模型应用。服务覆盖模型设计、训练、调优、部署、运维全生命周期，依托标准化服务体系降低城市垂类模型的开发落地门槛，最大化挖掘模型场景价值，适配城市各类 AI 业务创新需求。

模型专业服务分为四大标准化核心模块：一是模型规划设计服务，依托需求调研、场景评估完成训推方案设计与模型精准选型。二是模型训练与调优服务，通过数据适配、微调训练、效果验证、迭代优化等，提升模型场景适配精度。三是模型部署与集成服务，完成模型适配改造、业务系统对接、线上落地部署，打通模型与业务应用壁垒。四是模型运行支持和监测运维服务，提供全流程监控、故障诊断、持续迭代，保障模型服务长期稳定输出，实现模型能力可持续赋能城市业务。



图 26 模型专业服务示意图

5、智能体专业服务

智能体专业服务以业务为核心牵引，提供智能体全生命周期专业化服务，推动 AI 智能体深度嵌入生产、治理、服务流程，转化为城市新质生产力。整套服务包含规划设计、集成实施、运行优化、安全治理四大核心方面，适配城市全场景智能体建设运行调度需求。

具体服务内容包括：**一是行业智能体规划设计**，针对细分场景，定制专属智能体建设方案。**二是全流程集成实施**，依托智能体平台能力，完成资源接入、智能体编排、功能评测、系统对接、上线部署，实现业务流程闭环贯通。**三是常态化运行优化**，通过全链路监测、故障快速定界、自动化评估、持续调优，提升智能体实战能力。**四是全维度安全治理**，覆盖合规校验、风险防控、安全审计、跨平台迁移适配，依托专业智能体平台筑牢安全防线，支撑城市 N 类领域智能体规模化落地、常态化运营。



图 27 智能体专业服务示意图

（七）保障体系

大模型与智能体加速融入城市运行，攻防逻辑与运维生产关系同步重构，传统集中式防护与被动式运维已难以适应分布式、高动态的智能环境。亟需围绕安全与稳定两条主线，构建 AI 安全和 AI 运维一体化保障体系。

安全侧坚持统一安全、协同共治，从 AI 基础设施、智能体基础设施、模型、智能体四个层次筑牢纵深防线，构建准则统一、节点协同的体系，实现可感、可追溯、可审计的内生安全。

运维侧以确定性运维为核心，构建确定性恢复、动态风险治理、作业可信、主动运维、运维 Agent 平台五项能力，以 AI 赋能运维增效，以确定性约束 AI 安全边界。

1、AI 安全

（1）功能定位

一是技术新趋势。大模型借助工具调用、代码执行、外部接口等途径获得实际操作能力，智能体则具备自主感知、记忆、决策与执行能力，可围绕复杂目标自主规划并连续完成任务，应用规模快速扩大。与此同时，大模型训练与推理高度依赖海量多源数据，训练数据、用户交互数据、知识库数据等数据资产已成为驱动 AI 能力持续演进的核心要素，数据的规模性、流动性和敏感性显著上升，AI 数据安全性的重要性日益凸显。

二是安全新风险。AI 大模型与自主智能体的广泛应用，并非简单的技术升级，而是深刻改变了攻防逻辑，传统安全体系面临三重挑战。第一，失控风险易发多发，智能体的自主决策使行为边界难以预先划定，越权操作、指令注入、工具滥用等问题频发。第二，不确定性加剧，人工智能以概率为基础的输出特性，使传统规则匹配式防御难以覆盖模型内生潜在安全风险，模型幻觉、误导性输出等可能直接传导至业务决策环节，易导致风险由内容层向行为层扩散，概率性输出放大不确定性。同时，训练数据投毒、样本污染等针对数据供应链的攻击手段隐蔽性强，数据来源仿冒、知识库污染等风险在数据采集与流转环节持续累积，可能导致模型在训练阶段即被植入偏差或

后门，风险向下游传导路径更加隐蔽。第三，信任域边界模糊，跨模型、跨系统、跨服务的复杂协同，使原有以边界划分为基础的防护失效，数据在多方协同中频繁跨域流转，敏感信息在训练和推理过程中面临逆向提取与泄露风险，威胁路径更加隐蔽。

三是建设新需求。传统依赖安全大脑集中管控的模式，在分布式、高动态的智能体环境中面临响应延迟、单点失效等局限，难以适应新的攻防态势，新的 AI 安全形势对 AI 安全体系建设提出了新要求。从业务层面看，人工智能深度融入城市运行后，系统连续性和数据资产安全的重要性显著上升，亟须防范数据泄露、模型窃取、知识库污染等风险，需贯穿数据采集、传输、存储、使用、共享到销毁的全生命周期构建数据治理能力，运用隐私计算、联邦学习、数据脱敏与差分隐私等技术手段，保障训练数据与推理数据的真实性、完整性和隐私安全，保障核心业务稳定运行。从能力层面看，安全治理模式需要由“中心集中决策”转向“统一安全、协同共治”，中心负责制定准则、释放智能交互的边界，打造可控的自主系统。各智能体、模型服务与基础设施节点在统一准则框架内，各智能体与节点在准则框架内自主决策、协同治理。通过体系化的建设可有效抵御传统网络威胁和新型 AI 安全风险，实现意图驱动的内生安全，做到可感、可追溯、可审计。



图 28 AI 安全解决方案理念示意图

(2) AI 基础设施安全

AI 基础设施是人工智能运行的底座，是所有大模型训练推理、多智能体协同、智能应用落地的前提与根本保障，其安全状况直接决定上层模型和智

能体的可信程度。AI 基础设施安全面向算力集群、分布式存储、容器编排、开发框架、训练平台和推理服务等全栈环节，通过机密计算、异构计算环境下的可信保护等技术，保障训练和推理过程中的数据与模型不被窃取或篡改，并与云基础设施自身安全相衔接，为上层应用提供可信的运行根基。

(3) 数据安全

AI 数据安全聚焦人工智能全流程中的数据资产保护，贯穿训练数据、推理数据、知识库数据等关键数据要素的采集、传输、存储、使用、共享与销毁全生命周期。在数据采集与准备环节，重点防范数据投毒、样本污染、数据来源仿冒等风险，确保训练数据的真实性、完整性和可追溯性。在训练与推理环节，运用隐私计算、联邦学习、数据脱敏与差分隐私等技术手段，防止敏感信息在模型训练和推理过程中被逆向提取或泄露。在数据共享与流转环节，建立数据分类分级、访问控制与跨境流转审查机制，防范知识库污染、数据越权访问和跨系统数据滥用。通过全生命周期数据治理与隐私保护体系，实现 AI 数据资产底数清晰、流转可审计、风险可溯源，为 AI 安全提供坚实的数据安全底座。

【方案案例】华为数据安全屋

数据安全屋面向云上数据安全，实现资源强隔离、数据全密态，区内数据流转可视可控、数据离区即失效。

网络、资源强隔离：网络默认封闭，本地信任域的安全延伸；资源物理多租，逻辑隔离，多租互不影响。

全密态，密钥可控：开源加密 SDK，数据上云自动加密，客户密钥自持，云厂商无法窥探数据，加密策略可配置，专钥专用。

AI 模型保护：模型混淆推理模型可用不可见，资产零外泄。

数据离域即失效：数据胶囊，数据仅在专区内可用，离开专区使用，数据自动失效，数据管控策略，数据区内定向使用。

全程透明可观测：数据接入轨迹化，数据入云完整、干净，数据存储可视化，权限清晰，没有越权，训练任务拓扑化，无窃取、无后门。

(4) 智能体基础设施安全

智能体基础设施安全面向多智能体的运行环境,为智能体从创建、调度、通信、工具调用到销毁的完整生命周期提供防护。其核心在于防范身份仿冒、越权协作、工具劫持、指令篡改、数据外泄和决策被操纵等针对智能体运行机理的新型攻击,确保各类智能体在可信环境中执行任务,是保障多智能体协同可靠运行的基础支撑。

(5) 模型安全

模型安全着眼于模型从生产到应用的全过程。在模型生产环节,防护覆盖数据采集、清洗、标注、训练、微调、评估和发布各步骤,重点拦截训练数据投毒、后门植入、样本污染和知识产权流失等风险。在模型应用环节,围绕部署后的运行环境与对外交互,重点应对对抗样本攻击、模型窃取、推理数据泄露和恶意指令注入等威胁。通过分层、闭环的防护机制,推动模型运行由不确定走向安全可控。

(6) 智能体安全

智能体安全是多智能体系统运行的可信保障,从资产安全、运行安全、执行安全三个维度构建防护能力。资产维度,对智能体身份凭证、模型权重、专属知识库、工具权限和配置策略等关键资源实施全生命周期保护。运行维度,覆盖智能体创建、调度、通信直至销毁全过程,运用内存与微隔离、运行态监控和异常检测等手段,抵御身份伪造、越权、进程劫持和恶意代码注入等攻击。执行维度,面向智能体与外部环境的交互,通过工具白名单、指令校验、决策审计和结果验证等机制,防范指令注入、工具滥用、有害行为执行和决策结果篡改等风险。尤其是提升 Agent 意图威胁检测能力,保障智能体应用安全可靠运行,实现智能体资产与漏洞底数更清晰,智能体恶意和算力恶意消耗类行为可防可控。

2、AI 运维

(1) 功能定位

随着数字化转型深入推进,云环境、混合云、微服务、容器化等新技术

广泛应用，IT 基础设施规模呈指数级增长，系统架构与依赖关系日趋复杂，传统以人工经验为主的运维模式在被动监控、告警风暴、根因分析依赖个人经验、知识难以沉淀等方面日益难以应对，运维理念与模式的根本性变革成为必然趋势。一是应对复杂性与规模挑战，基础设施指数级增长、微服务与容器化架构复杂化、混合云与多云环境管理、数据爆发性增长以及安全威胁日益复杂，已超出人工分析与处理的能力边界，而 AI 能够有效处理此类复杂性。二是提升运维效率与质量，通过智能告警、自动化根因分析与智能诊断、预测性维护与自愈修复、资源智能调度，显著减少人工干预、缩短问题解决时间，实现从被动响应向主动预测、从事后处置向事前预防的转变，全面提升服务可用性与用户体验。

确定性运维将 AI 工程化纳入运维体系，构建覆盖确定性恢复、动态风险治理、作业可信、全生命周期主动运维、运维 Agent 平台的一体化能力体系，既以 AI 赋能运维提质增效，又以确定性约束 AI 安全边界，实现从被动运维向主动治理的跃迁，以 AI 解决 AI 带来的质量难题，为云上业务稳定、安全、高效运行提供根本保障。

（2）确定性运维

确定性恢复：确定性恢复能力建立在覆盖智能告警、智能故障定位、自动恢复、确定性恢复四个紧密衔接环节的全生命周期主动运维体系之上。告警环节基于指标、日志、调用链多源数据，依托算法模型完成噪音抑制与根因收敛。故障定位环节将人工经验沉淀为可复用的诊断推理链路。自动恢复环节由预案引擎按故障模式触发相应处置动作，将识别、定位、修复的过程压扁为秒级闭环。确定性恢复环节以确定性失效率、确定性恢复时长、确定性爆炸半径三项指标作为质量目标，使运维结果可衡量、可预期。

动态风险治理：动态风险治理以智能治理系统为中枢，将治理逻辑抽象为物理世界、数字孪生和自主智能体三层架构，由系统基于状态感知与知识进行自主决策评估，输出确定的恢复动作，实现从被动运维到主动治理的范式跃迁。基于人因风险理论模型，将不安全行为划分为无意行为（如疏忽、遗忘、错误等）与有意行为（如破坏、欺诈、盗窃等）两类，据此从作业授权、命令白名单、参数校验、人机回路审批等环节设计前置防控，把事后追

责转化为事前约束、事中拦截、事后审计的纵深防护。在面向外部运营环境一侧，构建舆情感知大脑、智能分析、处置助手的舆情管理闭环，实现全域多模态实时感知解析、大模型深度语义理解、智能风险预警、AI 深度洞察与归因、全自动报告生成等能力。

作业可信：作业可信体系以开发态一次做对和运行态实时防错为双轮驱动，构建 AI 主导的四层校验与人机协同变更稽查机制。开发态由 AI 自动识别告警处理、巡检处理、变更操作、故障处理等研发、运维、测试全生命周期等 SOP 文档，从中提炼流程经验并辅助生成业务代码。代码经四层校验，第一层硬性语法、第二层软性规范、第三层业务逻辑、第四层流水线集成，AI 同时在定位环节自动生成行号与修正建议、提取引用关系图、编写时实时校验并给出修复建议，实现即时校验。运行态聚焦变更方案书写、评审、实施、稽查全流程，由 AI 辅助风险识别与异常监测，实现潜在风险显化、可追溯，提升变更作业的安全性与可信度。

全生命周期主动运维：故障发生前识别潜在风险，从被动响应转向主动预见，让设备保持最佳状态运行。构建覆盖硬盘、SSD 卡、服务器、网络四类对象的四层硬件风险前置能力，硬盘层面通过 SMART 信息、UNC 错误、慢盘与坏块监测精准定位亚健康盘，启用读修复功能预先修复故障并对故障盘执行预重构与移除。SSD 卡层面监测高温故障、电容失效、擦写次数超过亚健康阈值等指标，提前告警并隔离故障节点。服务器层面针对 CPU 资源耗尽、CPU 频率降低、内存故障等亚健康症状精准定位并隔离。网络层面覆盖网卡失效/降速、链路丢包/降速、端口故障/闪断/丢包等场景，支持超过阈值即精确定位亚健康、提前告警，启用双健康网口主备切换保障连通性。

运维 Agent 平台：运维 Agent 平台以三个阶段梯次演进，重塑运维生产关系。第一阶段为工具智能化，AI 支撑人完成运维活动，通过变更作业、监控恢复、主动运维、客户运维等平台将 AI 能力嵌入运维工具链。第二阶段为 AI 代替人（当前阶段），AI 代替人完成运维活动，构建租户运维、客户服务与保障、变更、运营、知识问答、事件与告警等系列运维 Agent，覆盖资源管理、故障诊断、变更决策、数据分析等核心场景。第三阶段为系统自治，AI 消除运维活动，实现异常自助诊断、故障修复方案、智能监控优化、风险

治理、故障快恢与演练等无人值守能力。



图 29 确定性运维体系示意图

【应用案例】AlertSeek 告警数据智能分析 Agent

1、业务架构

采用三层分层架构，整体覆盖用户交互、Agent 核心处理、数据与知识全链路。最上层为用户层，基于前端对话界面，支持信息实时推送与自然语言交互。中间层为 Agent 核心层，包含 IntentHandler 意图路由引擎理解用户意图并路由，SkillEngine 技能执行引擎编排技能执行，12 个专业工具执行原子操作，LLMService 大模型服务提供意图理解、技能理解、结果生成能力，规则降级在 LLM 不可用时切换规则引擎保障系统可靠性。最底层为数据与知识层，由缓存数据库、告警原始数据、业务规则、专家经验构成数据底座，支撑上层 Agent 能力。

2、核心能力

指标查询、多维分析、报告生成、数据管理四大功能协同运作。指标查询支持告警降量率、自动化率和 11 项运营指标查询；多维分析支持服务域对比、时间趋势和 TopN 深度分析等；报告生成支持月度报告、综合分析报告自动生成；数据管理支持数据上传和缓存管理。

功能特点方面，具备支持任意时间范围（日/周/月/季度/自定义）、任意服务域组合查询和通过自然语言交互零学习成本。

效率提升方面，通过自然语言一句话查询指标数据，秒级完成响应；一键生成月报，30 秒自动生成 7 章节月报（含趋势图和环比分析），报告内容包括运营指标达成情况、告警工单上报情况分析、告警处理效果分析、告警优化情况分析、人力负载情况分析、问题跟踪与改进建议、趋势分析与环比变化。



图 30 AlertSeek 告警数据智能分析 Agent 示意图

第四章 建设指引：

标准化、可迭代、可持续的 AI CITY 落地路径

（一）分步推进策略

1、夯实基础支撑：筑牢算力、数据、模型三要素

在 AI CITY 建设中应注重算力、数据和模型的一体规划、分层推进。可按照盘活存量、按需供给、适度新建、绿色集约的原则统筹推进建设，防止碎片化投入。

（1）城市算力体系

城市算力体系建设应注重多级协同、统筹集约，从三方面统筹推进：

一是摸清家底、统一纳管，全面盘点城市已经形成的政务云等公共基础设施，充分利旧使用。

二是积极融入全国一体化算力网，对接国家算力枢纽节点和统一调度平台按需采购资源。

三是逐步构建“政务智算公共云+城市智算中心+边缘算力+区域协同算力”的多层次算力供给体系，满足不同时延智能应用需要，同时推进全市算力统一调度、统一计量、统一结算，从源头避免算力“孤岛”与闲置浪费。

（2）城市数据体系

城市数据体系建设应注重汇聚共享、分级授权，从以下方面分步推进：

一是目录先行，建立城市统一数据资源目录和“一数一源”责任清单，明确归集主体与更新机制。

二是归集汇聚，依托城市数据底座汇聚政务数据、公共数据，推动与社会数据融合。

三是治理提质，推进数据分级分类管理，提升数据质量。

四是共享开放，以数据应用需求为导向，深化政务数据共享、有序推进公共数据开放，加强公共数据授权运营与城市可信数据空间建设探索。全程注重做好数据安全管理和个人隐私保护，保障数据合规流通使用。

(3) 城市模型体系

城市模型体系建设应注重统一底座、分层适配，坚持“一城一底座”。基于集训练、推理、调度、评测、运营于一体的统一模型服务底座，支撑各部门、各层级按需调用通用模型，防止重复采购。在此之上，面向政务服务、城市治理、产业发展等场景，分层分类培育行业模型和场景模型，实现“通用模型打底、领域模型适配”。同步建立模型备案、安全评测、内容审计、更新退出等机制，确保自主可控、可用可信。

2、突出关键能力：打造统一入口与城市级知识库

在底座建设的基础上，为解决 AI CITY“好用、管用”的关键问题，需着力打造两大核心能力，一是基于智能体的统一智能交互入口，二是支撑超级智能体运转的城市级知识库。

(1) 统一智能交互入口

统一智能交互入口作为 AI CITY 从“能力供给侧”通向“用户需求侧”的总门户，在前端表现为服务体验的重构，背后体现的是 Agent 编排能力。

第一步可在现有政务 APP、网站、小程序、12345 热线等既有服务渠道之上叠加统一入口，基于一套知识体系，实现多渠道服务统一智能应答。

第二步可按需轻量化开发智能体，为“智能问答”向“智能经办”做好准备。

第三步基于多智能体协同，真正实现基于统一入口的精准识别需求、主动规划服务、全程智能办理，支撑“一件事”高效办成。

(2) 知识库

知识库是智能体顺畅运转的必要支撑，其质量决定了 AI CITY 智能水平的上限。为支持城市级超级智能体运转，需要构建城市级知识库。

搭建全市统一的知识库平台，与统一智能交互入口、智能体开发平台无缝集成，按“先高频后低频、先急用后缓用”原则，分类、分源、分批推进知识入库，避免重复采集、多头建设。

在迭代完善阶段，一方面从应用反馈中反查知识缺口，不断补充完善，

另一方面在交互中反哺更新迭代知识库,达到“越用越全、越用越准”的效果。

3、注重利旧衔接：做好与既有数字政府体系融合升级

AI CITY 不是另起炉灶,而是对既有城市数字化系统的智能化升级。要坚守“能利旧不新建、能叠加不替代、能演进不推倒”的原则,做好与政务云、城市大脑、“一网通办”系统、“一网统管”系统、“一网协同”系统等既有平台的衔接。

政务云:可通过扩容升级叠加智算、模型服务能力,推动算力统一纳管、统一调度,避免另建机房、重复投资。

城市大脑(智能中枢):可复用既有感知体系与治理机制,把大模型、智能体作为“新引擎”叠加嵌入,构建基于智能中枢的多级贯通智能化平台,推动监测预警、事件流转、指挥调度、决策支持等能力整体跃升。

“一网通办”系统:可将 AI 导办、智能预审、智能审批、智能客服嵌入既有办事流程,推动高频事项“高效办成”,实现“好办、易办、智办”。

“一网统管”系统:可推动依托智能中枢的多级贯通智能化平台,提升智能感知、预测预警、智能分拨能力,助力城市管理从“事后处置”向“事前预警、事中干预”转变。

“一网协同”系统:可推动 AI 赋能公文办理、督查督办、辅助决策、跨部门协同等场景,实现跨系统、跨层级、跨部门业务协同与流程再造。

（二）生态建设指引

AI CITY 建设是场景共创、能力共建、资产共用、价值共享的持续过程，构建生态是 AI CITY 从“建成”走向“用好”的必由之路。为促进 AI CITY 健康可持续发展，形成覆盖场景开放、数据供给、技术论证、平台建设、产品验证、能力沉淀、复制推广的闭环，应加快推动 AI CITY 从“建平台”向“建生态”转变。

一是要坚持政府引导、市场主导，做到政府搭台不越位，市场主体唱戏不缺位。

二是要坚持场景牵引、应用为王，以真实需求定方向、以落地成效论英雄。

三是要坚持开放共建、成果共享，推动数据开放与资产复用并重，实现一地创新、多地复用。

四是要坚持安全可控、底线思维，以合规安全为前提促进繁荣发展。

【应用案例】华为云“行业 AI 梦工厂”

“行业 AI 梦工厂”是华为云推出的一项核心战略，目标是聚焦行业实际需求打造基于华为云的行业 AI 赋能平台，帮助行业解决普遍存在的“不会转、不敢转、转不起”难题。通过平台化模式汇聚资源、打破壁垒、共建生态，聚合产业组织、客户、开发者和生态伙伴等多方力量，持续围绕行业场景沉淀模型、数据集、工具链和应用能力，开发行业应用和解决方案，降低 AI 在垂直行业中的应用门槛，推动 AI 技术与实体行业的深度融合，加速 AI 在实体行业的规模化落地。

发展定位：华为云“行业 AI 梦工厂”以生态共建为核心定位，以“能力沉淀”为主线，向伙伴、客户和开发者开放模型能力、数据样例、智能体技能（Skill）等原子能力，推动形成“华为提供技术底座、伙伴提供专业技术和行业知识、客户提供业务问题与生产环境”的共建闭环，加速行业 AI 能力规模化沉淀与复用。

创新实践：以政务领域实践为例，随着人工智能由基础大模型迈向智能

体应用新阶段，传统政务应用在敏捷开发、改造升级、迁移适配等方面面临现实挑战，迫切需要加快沉淀行业 AI 能力。华为云联合政府客户与生态伙伴，依托“行业 AI 梦工厂”共同打造“政务智能应用超市”，通过聚合应用实践提炼行业知识（Know-how），开发各类政务应用智能体和 Skill，形成可复用的行业场景能力，有效降低 AI 应用开发门槛，推动城市数智生态共建共赢。这种从“单点能力建设”走向“生态体系共建”的转变，正成为未来 AI CITY 行业领域实现 AI 应用落地的新模式。面向善政、兴业、惠民等领域不同场景应用，“行业 AI 梦工厂”可基于城市智能底座，以政务资产广场提供的 Skill、数据集、MCP 等“标准件”原料，通过政务智能体平台的 AI 编排、多 Agent 协同，将通用能力“装配”成为适配场景的 AI 应用并交付使用。将运行产生的数据回流至资产广场与 AI CITY 底座，进行反哺沉淀和迭代升级，形成“越用越多、越用越准”的自我强化循环。

应用成效：目前，华为云依托“行业 AI 梦工厂”已经沉淀形成政务场景应用模板 10 余个、政务应用 20 余项、通用办公 MCP 资产 50 余个、政务应用开发 Skill 6 余项、政务行业数据集超过 5 个，并已经在政务服务、机关办公、城市治理、产业经济等领域落地应用。政务服务类覆盖智能客服、政务热线、智能咨询、智能填单，机关办公类覆盖政务办公、智能审校、智慧公文，城市治理类覆盖智慧警务、辅助决策，产业经济类覆盖产业招商、产业链分析、数据治理。



图 31 华为云“行业 AI 梦工厂”政务领域应用

【应用案例】数字深圳联合创新中心

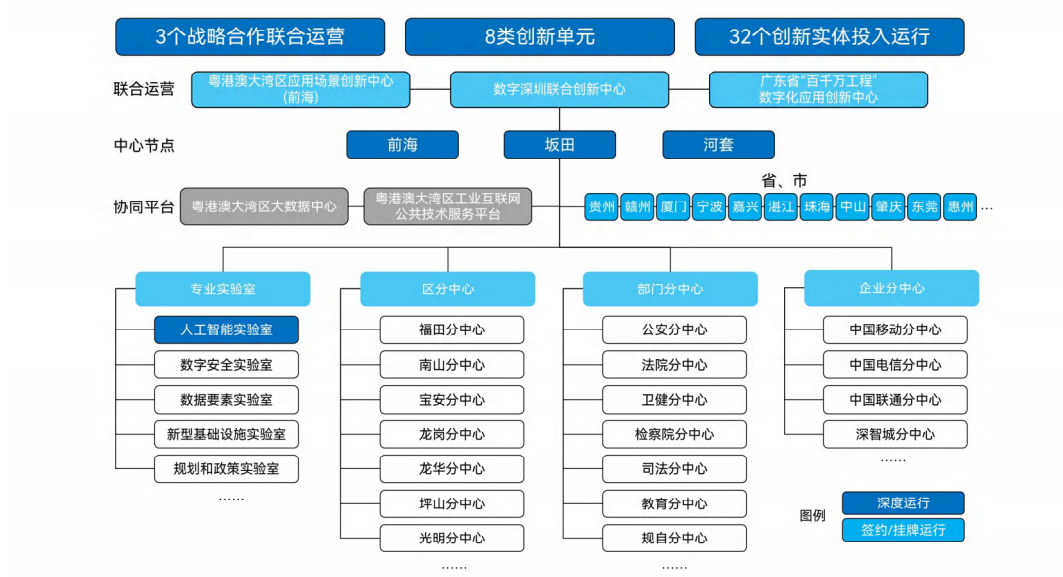
数字深圳联合创新中心由深圳市政务服务和数据管理局牵头建设，针对传统政务信息化“先立项后建设”模式周期长、试错成本高、建成易落后、需求匹配度不足等痛点，创新构建“先实验、再实战”的联创机制，打通技术与政务场景的衔接通道，打造场景孵化器、产品转化器与产业加速器。

发展定位：构建“政产学研用资”多元协同创新载体，联动粤港澳大湾区应用场景创新中心、广东省“百千万工程”数字化应用创新中心协同运营，立足深圳、辐射粤港澳大湾区，探索政府信息化项目建设新模式，实现“一地创新、多地复用”，为数字城市建设输出可复制的深圳实践方案。打破技术与政务场景割裂现状，以场景开放牵引技术创新，通过低成本前置实验降低项目试错风险，提升数字化项目建设成功率。统筹算力、数据、模型、工具等创新要素，培育一批贴合政务真实需求的数字化产品，形成全流程闭环、全要素支撑、全方位推广的“三全”创新体系，激活数字生态活力。

创新实践：一是搭建多元生态组织，汇聚政府、企业、科研院所、专家智库、投资机构、交易服务机构六类主体，布局专业实验室、区级分中心、部门分中心、企业分中心等创新单元，已有 32 个创新实体投入运行。二是创新六环节实验流程，遵循“开放场景—方案遴选—创新研发—试用验证—成果认定—落地推广”路径，政府开放真实业务场景，企业揭榜参与，经多维度测试验证后，成熟成果再转为正式项目落地推广。三是建设三大支撑平台，创新要素业务平台实现从“创意”到“产品”应用场景全生命周期业务支撑。AI 公共支撑平台纳管 274P 算力，提供基础与精调模型、通用算法等工具。数字安全质量检测平台完成功能、性能、安全合规检测，为创新实验提供“拎包入住”式全要素保障。四是持续运营品牌活动，打造“一周一活动、两周一发布、一月一主题”常态化机制，发布 100 个“AI CITY”场景，覆盖辅助决策、社会治理、机关办公、政务服务、民生服务五大领域。

应用成效：数字深圳联合创新中心已孵化多个标杆 AI 应用。“深小 i”AI 政务助手归集 9 万余个政策文件、68 万余条问答数据，政务问题应答率达 97.7%，问答精准率达 94.3%，实现政务秒级智能服务，在政务服务智能化领

域的综合能力居于行业领先水平。深圳中院 AI 辅助审判基于历年沉淀的裁判文书与法规，对立案、审理、判决等全流程 85 个核心办案节点进行精准拆解，复杂案件审理周期平均缩短 50%，2025 年深圳法院法官人均结案 744 件，同比增加 249 件，高出全省平均水平 261 件，显著提升司法服务效能。电动车安全隐患治理智能体打通十余个部门，实现隐患感知、策略生成、工单派发、复盘迭代全链路自治，打造城市安全智能体样板。机制层面，通过实验前置有效压低试错成本，滚动遴选验证让成果贴合业务实际，促进技术成果迭代复用。创新成果可通过数交所上架，实现跨地域复用推广，为全国数字城市建设提供实践参考。



（三）运营模式

1、优化综合服务运营

城市公共云运营是贯穿规划、建设、使用全过程的系统工程，核心在于推动运营主体由“云资源运营”向“价值运营”转型。随着 2026 年政府工作报告明确提出支持公共云发展，各地以集约统一、安全可信的城市公共云为底座，加快破解部门数据壁垒、降低数字化建设成本，运营模式也随之从以算力、存储等资源交付为主，升级为覆盖应用开发、智能运营、产业赋能的综合服务运营。运营公司将与政府、能力型伙伴共同围绕政务高效履职与城市数字经济发展，构建“建设、使用、运营”一体化闭环，实现技术可行、商业可持续的良性运营格局。

2、健全协同运营机制

运营模式的落地，有赖于政府、运营公司、能力型伙伴共同参与的多方协同运营机制。一方面由运营公司结合本地场景定制化能力，打通场景落地的“最后一公里”。另一方面通过联合创新、能力共享等方式，持续升级运营主体的核心能力，推动运营公司向综合服务型组织转型。有条件的地方可探索发起“城市公共云合伙人”等行动，通过聚合应用实践、沉淀可复用资产，形成政策护航、伙伴深度参与、能力型伙伴联合创新的运营生态，为 AI CITY 的可持续运营提供制度保障。

3、创新 Token 运营

Token 作为大模型信息处理的计量单位，已成为 AI CITY 价值计量、资源调度与结算的核心载体。应依托公共服务平台搭建 Token 运营能力，对异构算力与多厂商大模型统一计量、统一调度、统一结算，破解接口割裂、计费不统一等痛点，实现按业务消耗获取 AI 服务。同时支持根据不同业务性质可灵活调用互联网公共云、政务外网公共云、本地智算中心的政务 Tokens 服务。一方面，探索政府 Token 券、创新券等补贴模式，面向中小微企业发放 Token 额度补贴，降低 AI 应用门槛、拉动场景落地。另一方面，健全分级配额、套餐订阅、按量计费相结合的商业机制，对政务、医疗、教育、工业等行业企业设置差异化配额、消耗阈值与超支管控策略，实现用量可审计、成

本可追溯，推动运营从“卖算力资源”向“交付智能业务价值”升级，构建可持续运营闭环。

（三）人才培养服务

人才培养服务以实战能力为核心牵引，向政务人员提供云通用基础、数据和人工智能理论、AI 智能体应用等全周期培养服务，推动 AI 智能体深度嵌入日常办公、审批办理、决策辅助、公共服务等政务场景，转化为政务队伍新质履职能力。整套服务包含课程规划、教学实施、实训演练、能力评估四大核心环节，适配各级政务部门智能化转型与人才梯队建设需求。

具体服务内容包括：一是分层课程规划设计，针对不同岗位层级与业务条线，提供针对性培养方案，覆盖基层人员基础赋能、业务骨干实操进阶。二是全流程教学实施，依托专业培训平台与师资力量，完成理论授课、案例研讨、工具操作、场景模拟等，实现从知识输入到技能转化的闭环贯通。三是常态化实训演练，通过真实业务场景嵌入、任务驱动式实操、问题导向式复盘、持续迭代式训练，提升政务人员智能体协同应用实战水平。四是全维度能力评估，覆盖知识测评、技能考核、场景应用评价、岗位胜任度认证，依托专业化评估体系量化培养成效，支撑各级政务部门智能化人才规模化培养、常态化赋能。



图 33 人才培养服务体系示意图

（四）标准体系

面向城市全域 AI 建设统筹需要，探索建立 AI CITY 标准体系、AI CITY 顶层设计标准、AI CITY 政务 Token 远程调用标准等，为不同发展基础、不同规模城市推动 AI CITY 建设与发展提供可参考的范式指引。引导各地结合自身城市禀赋、数字化基础、城市治理需求、财政能力等因素，科学设计本地 AI CITY 建设方案，避免重复建设、架构碎片化、建设目标脱离实际等问题，确保各地 AI CITY 建设路径可落地、运营可持续。

（五）评价导向

对地方政府，AI CITY 建设应注重能力集约化和应用实效性。以下评价导向供参考。

1、基础能力评价导向

（1）统筹集约

一是强化顶层统筹规划。坚持全市“一张蓝图”统筹建设，统一建设标准、统一底座体系，严控各部门、各区县各自为政、分散新增算力机房、AI 使能平台。

二是坚持存量提质利旧。优先盘活现有政务云、数据中心、感知设备及信息化系统，对零散老旧设施进行智能化升级改造，实现新旧设施融合复用、提质增效。

三是推行云服务集约赋能。转变自建自维模式，通过购买智算云服务等方式，按需弹性调配满足城市治理、民生服务、产业发展需求的算力规模。

（2）先进适用

一是打造特色垂直模型。不盲目追求通用大模型参数规模，结合本地产业特色与治理痛点，训练轻量化、高精度、高适配的行业垂直模型，打造城市 AI 建设辨识度与行业竞争优势。

二是精准适配智能体需求。针对高频重复、规则清晰、可自动处置的标

标准化业务场景，规模化部署智能体实现效能提升。对低频次、强人工决策、赋能效益低的场景，不盲目堆砌 AI 技术，杜绝形式化建设与资源冗余浪费。

(3) 智能原生

一是沉淀本地知识资产。持续扩展城市多维数据资源体量，为 AI 模型训练、智能决策提供充足数据支撑。结合城市治理需求和产业特色，针对性搭建高精度、可迭代、专业化的高质量数据集与行业专属语料库，系统化沉淀本地化城市知识资产。

二是落实全域 AI 原生设计。将 AI Ready 作为新建、改造项目前置标准，在智慧社区、智能工厂、城市基建等项目规划阶段，原生嵌入感知采集、智能分析、协同处置能力，搭建全域互联、全域智能的城市 AI 原生底座。

(4) 安全可靠

一是健全全周期安全管控体系。将安全审核贯穿 AI 需求梳理、模型训练、开发测试、部署运行、迭代下线全流程，严格把控训练数据合规性、算法安全性，防范数据泄露、算法漏洞、后门风险。

二是强化动态监测风险处置。落实 AI 应用上线前合规审查与安全检测，建立常态化运行监测、风险预警、溯源整改机制，实时管控 AI 系统运行、数据流转、智能体执行行为，实现安全风险早发现、可追溯、闭环处置。

三是筑牢整体安全合规底座。严格落实网络安全、数据安全、个人信息保护等法律法规及等保要求，构建纵深防御的全域安全架构，有效防范模型滥用、算法歧视、数据泄露等风险，全面保障城市 AI 基础设施、数据资源、智能应用安全可控。

2、应用实效评价导向

(1) 经济带动

考察人工智能直接带来的成本降低或收益提升效果，反映该场景应用人工智能产生的经济效益。可用场景上线后成本/收益类业务指标改善情况衡量，如：产值提升、不良品率下降幅度、人工成本节约等。

(2) 效率提升

考察该场景在时间方面的优化程度，体现人工智能提升速度或效率的赋能效果，反映该场景下治理高效化或服务便捷化程度。可用场景上线后时效类业务指标改善情况衡量，如：事项办结时效、排队时长、生产周期等。

(3) 均等普惠

考察该场景惠及的用户范围及规模，体现人工智能促进资源均衡配置的赋能效果，反映该场景下服务覆盖范围拓展、城乡差距缩小、惠及更多用户等普惠情况。可用落地应用范围衡量，如：用户占比、覆盖面积占比等。

(4) 业务渗透

考察人工智能功能覆盖该场景业务全生命周期各环节的比例，反映该场景下人工智能技术与业务的融合深度。

(5) 体验优化

考察人工智能优化服务类场景的实际效果，反映该场景下企业和群众办理业务的获得感与满意度情况。可用场景上线后评价类业务指标改善情况衡量，如：用户满意度改善、投诉办结率提升等。

(6) 预警预测

考察人工智能优化治理类场景的实际效果，反映该场景下对演变、波动、风险的分析、判别、预测、主动预警能力。可用场景上线后预测准确率水平及应用前后准确率提升情况衡量。

表 7 AI CITY 评价导向

评价维度	评价指标
基础能力	统筹集约 先进适用 智能原生 安全可靠
应用实效	经济带动 效率提升 均等普惠 业务渗透 体验优化 预警预测

第五章 华为落地实现

AI CITY 不是纸上蓝图, 华为已联合多个城市在城市超级智能体、治理大模型、安全治理、具身智能到智能政务等方面进行探索尝试。

（一）克拉玛依城市超级智能体

1、案例概述

克拉玛依具备扎实的政务数字化建设基础，2012 年建成政务云后续持续推进智慧城市、AI CITY 整体架构迭代建设。以国务院印发的《关于深入实施“人工智能+”行动的意见》为政策导向，结合本地印发的《克拉玛依市推进“人工智能+”行动工作方案（2026—2028 年）》，项目在算力底座、业务信息化系统、政策机制层面，均已具备开展城市级智能体建设的现实条件。

在城市治理实际运行过程中，传统城市大脑的应用局限性逐步显现。传统平台重点聚焦数据汇聚、态势感知和可视化展示，能够识别城市运行问题，但缺少完整的业务执行闭环，普遍存在“看得见问题，解决不了问题”的现实矛盾。各委办局业务系统相互独立，数据孤岛、部门墙问题较为突出，低保救助等跨部门民生业务高度依赖人工流转协调。同时行业内“重建设、轻运营”现象普遍，难以形成从问题发现到处置办结的价值闭环，基层工作人员承担大量重复性事务，群众办理跨部门业务流程繁琐，政务服务与城市治理效能仍存在提升空间。

针对上述治理痛点，克拉玛依联合华为共同打造城市超级智能体，将其作为 AI CITY 的核心引擎。该项目并非单一软件产品，而是一套多模态、跨平台的城市级 AI 认知操作系统与智能生态体系。项目创新采用“总-业务-委办局”三级多智能体治理架构，引入 A2A 智能体通信机制与混合式 AI 技术路线，优先选取业务需求高的社保民生领域作为试点场景，系统性应对顶层设计、数据底座、技术协同、场景落地、人机共治五大现实挑战，推动城市治理由被动响应向主动预警、从事后处置向事前干预转型。

2、建设架构

（1）总体谋划：“总-业务-委办局”三级多智能体治理架构

项目搭建“总控层-业务域层-执行层”三级多智能体体系，落实“1+N”全局统筹、专业协同的建设模式。

总控层：城市超级中枢，即 1+N 架构中的“1”，作为城市 AI 统一调度中

枢，搭载单智能体执行引擎、多智能体协同引擎两大编排引擎，承担多模态意图识别、复杂任务拆解、智能体调度分发、全链路审计追踪、执行结果校验反馈等核心职能，统筹调度全市域全部智能体资源。

业务域层：四大业务领域智能体集群（业务级 Agent）。一是城市治理领域 Agent 集群，包括城管执法 Agent、环境治理 Agent、交通管控 Agent、网格管理 Agent；二是民生服务领域 Agent 集群，包括政务服务 Agent、医疗保障 Agent、社区服务 Agent、教育服务 Agent，支撑低收入人群精准帮扶、社保业务办理、AI 社工数字人等场景落地；三是应急响应领域 Agent 集群，包括应急调度 Agent、舆情处置 Agent、防汛防火 Agent、安全管控 Agent；四是产品服务（产业经济）领域 Agent 集群，包括企业服务 Agent、经济运行 Agent、招商服务 Agent、园区管理 Agent。

执行层：委办局专属 Agent，为各市直业务部门部署专属智能体，直接对接部门原有业务系统。各部门原始敏感业务数据保留在部门本地域内，仅对外输出脱敏统计指标，兼顾业务协同与数据安全管控。

(2) 整体架构：AI 城市数智底座

架构自底向上共计 6 大部分，包括云基础设施、一体化数据资源服务平台、智能体和模型相关服务、N 个应用、统一入口、运行保障体系。

最底层为**云基础设施**（政务云、互联网、政务外网），为 AI 城市提供统一云网资源支撑。

一体化数据资源服务平台包含四大平台，汇聚政务、社会、互联网企业等多源数据源，输出高质量语料集、知识库、数据仓库等数据资产。

智能体和模型相关服务包括通用智能体服务、智能体开发平台、模型部署开发平台。

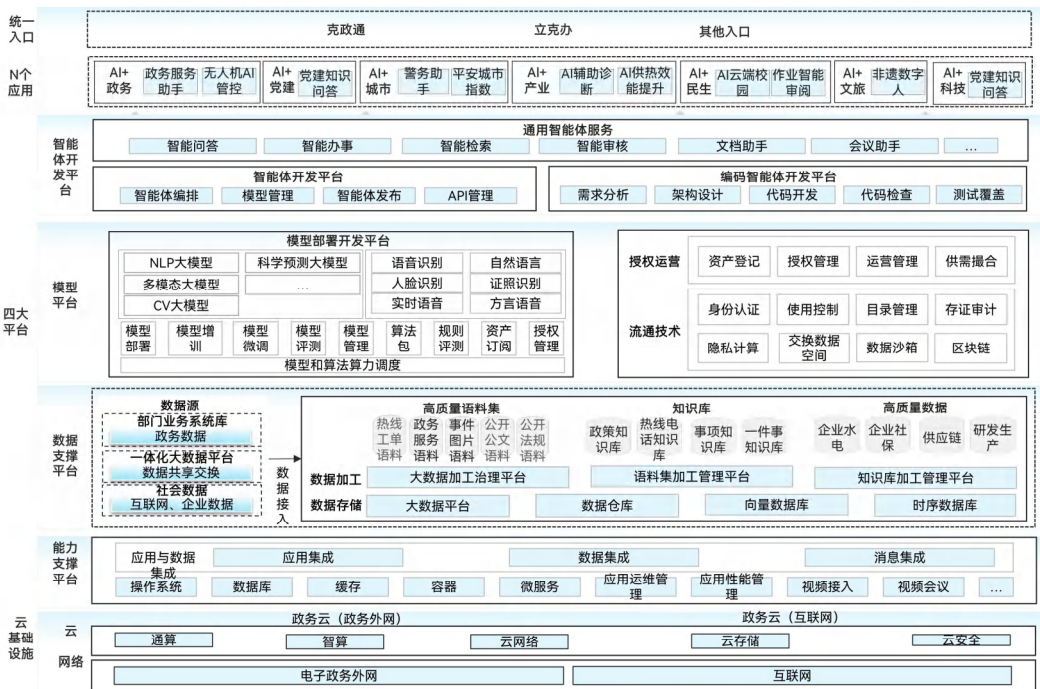


图 34 克拉玛依 AI 城市数智底座整体架构

(3) 运营体系：三层二支撑架构

三层核心体系包含应用层、中枢层、设施层。应用层承载政务、民生、产业各类智能体业务应用。中枢层为城市超级智能体的核心，部署双引擎与全套多智能体技术子系统，完成智能体调度与业务编排。设施层涵盖算力底座、城市数据湖、政务云基础设施、物联网感知终端。

两大支撑体系分别为安全保障体系、运营运维体系。安全保障体系构建一体化全生命周期安全防护，实现统一身份鉴权、全链路审计、敏感数据拦截、故障自动回滚。运营运维体系建立长效运营保障机制，围绕智能体迭代、数据资产运营、中枢能力升级、基础设施运维开展持续运营，保障系统可持续迭代演进。

(4) 关键子系统：支撑多智能体完整业务闭环运行

项目部署七大技术子系统，共同支撑多智能体完整业务闭环运行。注册与发现子系统负责智能体注册、能力目录管理，解决“谁能干什么”。通信与消息子系统（A2A）基于 AgentCard 智能体卡片、JSON-RPC2.0 消息协议，实现异构智能体自动发现、交互协同。管理与执行子系统完成 Agent 任务编

排执行，包含事件循环控制器、会话状态持久化、工具模型注册、意图路由、多种编排模式。协调与编排子系统开展复杂问题规划、约束校验、方案可行性评估。知识管理与共享子系统依托知识管理引擎，完成多源知识整合、检索、转化，避免信息孤岛。监控、诊断与自愈子系统实现运行指标监控、故障检测识别、故障自动恢复。安全子系统完成统一身份鉴权、注册校验、调用权限管控、运行时策略注入、敏感数据拦截、全链路审计、故障自动回滚。

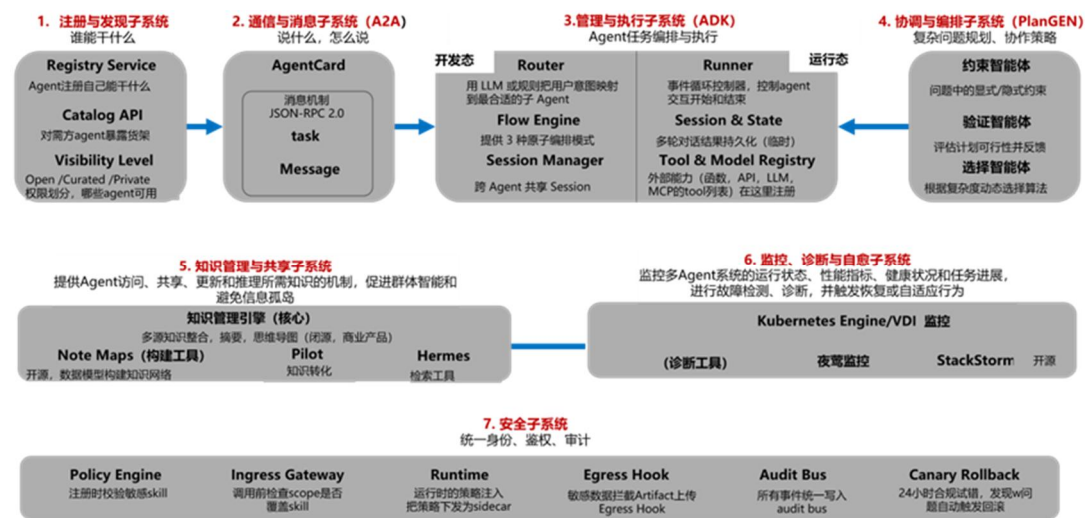


图 35 克拉玛依市城市多智能体协同关键技术实现

依托整套技术体系，项目形成六大核心能力。一是全栈感知交互能力，融合摄像头、传感器、无人机多类感知源，支持文本、语音、图像多模态交互。二是认知-决策-规划-编排能力，解析复杂业务意图，自动拆解跨部门复杂任务。三是 A2A 多智能体协同能力，支持不同厂商、不同业务域智能体自主协商协同。四是仿真-训练-部署闭环迭代能力，依托仿真生成极端场景样本，业务运行数据持续反哺模型优化。五是全链路数据治理底座能力，通过贴源层、标准层、融合层、共享层分层架构，结合隐私计算技术实现数据可信流通。六是全栈安全运营能力，覆盖数据、模型、应用、运营全生命周期安全管控。

3、应用成效

(1) 社会效益

项目落地后民生服务获得感显著提升。AI 社工数字人“小克”实现 7×24

小时在线服务，全市布设 125 台终端，覆盖全部街道社区；超过 96%的政务服务事项可“网上办、掌上办、指尖办、自助办”，让“数据多跑路、群众少跑腿”的服务理念得到充分体现。在低收入人群精准帮扶场景，救助资格审核由传统人工数天压缩至分钟级，落地“政策找人”免申即享模式；急难救助紧急通道可实现 24 小时内资金发放，全流程日志留存，满足政务合规审计要求。平台面向老年人、残障群体提供适老化服务以及网格员上门帮办代办，有效弥合数字鸿沟。

城市治理范式实现升级，推动治理模式从事后处置、被动响应转向事前预警、主动干预，建成完整“感知-分析-决策-执行-评估”治理闭环。改变传统城市大脑“只发现、不处置”的局限，依托多智能体协同自动推动跨部门问题处置，减少部门之间大量人工协调流转工作，城市综合运营效率预计提升 30%以上。

项目斩获第九届数字中国创新大赛数字城市铂金奖，“1+N”模块化架构、A2A 多智能体协同技术方案具备较强可复制性，为国内资源型城市数智转型提供实践范本，部分民生业务场景已向新疆其他地州复制推广。

(2) 经济效益

算力建设模式实现转型，由完全依赖外包厂商定制建设，转变为政府搭建普惠算力底座，赋能本地企业开展 AI 创新应用，有效降低本地企业 AI 开发算力成本。项目将基层工作人员从咨询、材料核验等重复性工作中释放，使其可以投入入户走访、特殊群体关怀等高价值工作。同时带动本地智能体相关产业生态培育，孵化智能原生企业集群，探索 OPC 一人经济新模式，培育地方新质生产力。

(3) 技术生态

项目在政务真实生产环境完成 A2A 智能体通信、AgentCard 卡片规范、双引擎多智能体编排等前沿技术的落地验证；采用开放兼容架构，规避厂商锁定风险；混合式 AI 模式兼顾大模型通用能力与政务敏感数据本地安全。沉淀“仿真-训练-部署-反馈”闭环的工程化落地方法论，为国内城市级智能体项目建设提供可参考的实践案例。

（二）武汉超大城市治理智能体

1、案例概述

武汉作为素有“九省通衢”之称的国家中心城市，承载人口超过 1300 万。面对超大城市治理中数据共享效率有待提升、多级联动存在阻碍、应用智能化水平有限等共性难题，武汉联合华为推进数智武汉超大规模城市 AI City 建设，发布了超大城市运行管理智能体，构建了横向到边、纵向到底的全市城运体系。基于城市智能体，通过三层体系、四级应用的一网统管业务架构，构筑城市运行“一网统管”全域感知、智能联接、数智融合的先进技术架构，围绕“高效处置一件事”实现全市“可感、可视、可管、可控”，实现市区“一体联动”城运体系，打造了超大城市治理和城市智能体实践案例。

2、建设架构

（1）总体谋划：构建“王”字型城市运行体系

城运中心是推进“一网统管”的具象载体，作为城市运行“驾驶舱”，保障市领导“战时”在城运大厅开展跨部门综合指挥调度；作为“参谋部”，通过大数据监测分析，辅助领导科学决策；作为“中控台”，通过城运平台“四大中枢”，赋能线上线下高效处置一件事；作为“展示窗”，通过迭代升级一批、谋划建设一批实战管用的应用场景，充分展示武汉智慧城市的建设成果。

按照武汉城运中心建设工作方案，规划构建“王”字型城市运行体系，“三横”是市区街三级城运中心，“一竖”是纵向贯通的数据流、业务流、指令流。市级城运中心抓总体、强赋能，聚焦重大多跨事件精准调度；区级城运中心重联接、强实战，聚焦各类事件高效处置；街道级城运中心抓处置、强联动，聚焦群众急难愁盼问题快速响应。

武汉城运中心围绕“感知、预警、处置”的要求，建成市、区、街一体化综合调度平台，采用开放的平台架构，使能应用快速构建，融合音频、视频、网络等多种通信方式，在跨年夜、雨雪冰冻、春节、归元敬香、汉马、清明祭扫等重要节日、重大活动期间开展综合调度保障。从感知到 AI 全栈技术自主可控，同时场景与技术相互促进敏捷创新。建成城运综合调度大厅，接入

14 个市直部门专业指挥系统，实现多兵种协同作战；通过市、区、街一体化综合调度平台“一键直连”一线处置人员，通过事件枢纽做到指令“一键直达”。

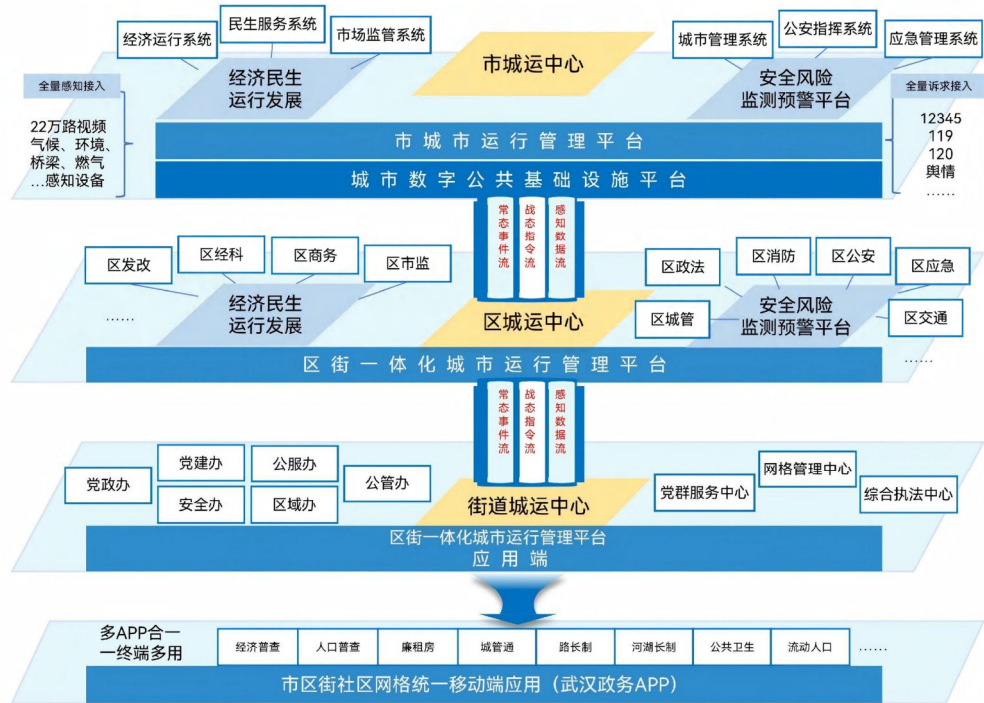


图 36 武汉城运中心“王”字型平台体系建设

(2) 智感中心：全域感知、实时发现、及时预警

智感中心通过大模型+小模型协同实现城市事件的泛化发现和精准识别，基于多模态大模型，对全域视频定时巡检，盘活武汉市数十万路摄像头，对城市事件和部件进行视频检索，包括城市治理、城市安全、交通管理等城市事件，通过搜索事件名称，视频抽帧事件画面，调取摄像头实时画面可以感知事件现状；通过小模型，利用机器替代人工 7*24 小时主动发现城市中的各类事件，及时上报预警。

在视觉感知上，汇聚了全市 22.7 万路摄像头、297 架无人机；在听觉感知上，聚合了 12345、119、120、舆情等 10 类事件来源 2825 余万件；在触觉感知上，汇聚了桥梁、水务、环境等各类感知设备，全市 200 个积水点监测点位、38 个空气监测点位，39 个水源水质监测点位，822 座桥梁监测点位、545 个瓶装燃气监测点位感知全覆盖。在智能预警方面，通过 25 种 AI 算法对 20000 路视频进行实时分析，通过语义分析对城市事件进行智能预警，

同时利用 AI 大模型建设提升研判分析能力，日均分析约 3 万件。



图 37 智感中心多种感知能力

智感中心有力支撑了城市治理智能化转变。一是从人工巡查到视频采集，通过智能视频抓取技术，实现对占道经营等城市管理问题的自动巡查，对违规行为进行识别，并自动报警推送。二是从被动管理到主动参与。传统人工模式下，出现各种社会治理事件或城市管理事件，如出店经营屡禁不止，违规停车防不胜防等等，采用智能监控分析技术将街域范围内的人、物、机制等系列资源统一起来，通过社区、物业、商家、居民、执法力量共治。三是从事后处理到实时处理。基于视频网络的建设，实现了对市政、环卫、停车等城市管理行业，以及重点社区的全覆盖，不仅能支持拍摄监控点位范围内的生物特征、车牌等信息，还应能实时掌握车辆违停、渣土车违规运输，还应能随时录像存储。四是从单一视角到统领全局。通过武汉市城市管理、社会治理等多个委办局的视频监控点位的共享和联网互通，避免重复建设的同时可以实现跨委办局的能力共享。

(3) 分析中心：辅助决策、监督考核、行政问效

武汉市整合交通、人口、环境、防汛排涝、营商环境、城市安全等 20 个领域，十大类 53 小类共 1450 项体征指标，并汇聚 141 亿条数据。构建包括人员、车辆、城市部件、城市事件和风险源的武汉城市治理一本账，以及城市全要素清单、主体清单和权责清单，通过建立城市治理台账摸清家底。比

如武汉市通过人员信息关联就业、社保数据，可精准定位失业群体并推送帮扶政策；车辆台账与交通卡口数据联动，能快速排查套牌车、报废车；城市部件台账标注每盏路灯、每段管网的位置与状态，故障报修后可直接调度最近维护团队。

全要素清单明确治理对象的数量、属性与关联关系，让资源调配更高效。比如将窨井盖与地下管线纳入同一清单管理，暴雨前可通过清单快速定位易积水点的井盖位置，提前组织加固；主体清单与权责清单则厘清部门职责边界，在违建事件中，系统依据清单自动匹配城管、规划部门的协同流程，避免推诿导致的处置延误。根据对工单的智能打标签结果，生成预警模型，包括热点主体、突发热点、群体高发、持续热点、潜在热点、重复投诉、敏感诉求、消极话题和消极潜在。通过模型对工单的智能分析判断，极大地提高了事件工单的流转效率。

武汉城运平台提供0代码报告生成工具，结合大模型智能打标签能力，可以秒级生成城运中心工作报告，涵盖城管、水务、应急等多领域知识以及多种图形模板，通过配置的方式支撑日报、专报、周报的一键生成，以雨情为例，报告包含综合统计、热点话题等多类专项，助力工单高效闭环。

(4) 协调中心：业务枢纽、闭环赋能、部门处置

通过构建横向到边、纵向到底的协调中心，实现武汉各级城运中心多跨协同、高效运转。纵向市级城运中心作为总体平台，整合全市数据资源与指挥权限，通过标准化接口与区、街镇、社区四级平台实时联动。横向打破部门“信息孤岛”，建立跨领域协同机制。例如当发生极端天气时，市级城运中心自动触发应急响应，同步调度气象、交通、水务、应急等部门数据，气象局提供降雨预测，交通局调配公交临时绕行线路，水务局监控河道水位，应急管理局协调抢险物资，各部门数据在同一平台实时共享，避免重复沟通。通过纵横结合的方式，实现城市事件的全闭环。

(6) AI 智能体：意图驱动的 AI 超级应用

武汉城运中心已经开展建设城市治理和城市安全领域智能体超级应用，城市治理超级应用实现一句话生成预警、一句话分析视频、一句话指挥调度；城市安全超级应用实现火灾速报、内涝速报和安全态势专报。相较于 AI 点状赋能，通过 Agentic AI、意图理解简化菜单式交互。通过智能任务规划，自主调用、执行城市治理、城市安全的各类业务系统、工具平台能力。



图 40 AI 智能体应用

3、建设运营模式

(1) “三级联动”的组织架构创新

建立“市级统筹、区级主战、街道（社区）落地”的三级城运体系；通过《武汉市城市运行管理条例》明确三级权责，将数字化平台使用纳入干部考核，解决了“多头管理、推诿扯皮”的痛点。

(2) “平急结合”的指挥机制创新

日常状态下，采用“部门专业处置+城运平台监督”模式，各职能部门通过平台共享数据，城运中心负责跟踪督办；应急状态下，启动“城运中心统一指挥+部门垂直调度”模式，临时赋予城运中心跨部门指挥权，可直接调动公安、消防、水务等资源，事后回归常态权责。

4、应用成效

(1) 有力支撑城市精细化治理

通过城运平台集成全市 22.7 万路高清视频、297 架无人机感知能力，实时接入十大类事件来源，能全面掌握全市气象、交通运行、保供、重要区域大客流等情况，实时监测城市运行态势。

(2) 有效降低城市运行成本

城市运行管理平台精准预测节假日拥堵趋势，交通拥堵指数降低 15%。AI 每日分析近千座桥梁动态、燃气管道监测等问题，累计发现超过 10 万条事件，燃气安全事故率下降 60%。

(3) 显著提升市民满意度

武汉 12345 政务服务热线等平台优化效果显著，单工单处理时长从 10 分钟缩短至 0.5 分钟，市民政务服务满意度提升至 98%。

(4) 高效保障城市重大活动

在跨年夜、融雪防冻、春运保障、汉马赛事、清明祭扫等重要节日和重大活动中，为市领导指挥调度决策提供了数智支撑，确保了活动的顺利进行和城市的平稳运行。

（三）上海国地中心具身智能实训场

1、案例概述

当前，人形机器人在高端制造、城市服务、应急救援等领域加快场景落地，应用边界不断拓展，规模化产业落地需求日益凸显，但行业仍面临高质量数据可靠传输与持久存储难、数据治理复杂、数据产权界定不清，以及真实场景采集成本高、仿真验证效率不足、模型训练算力需求大、具身能力缺少统一评测等挑战。

作为工信部与上海市政府联合授牌的人形机器人行业国家级创新中心，国地中心肩负“1+N”训练场布局和数据基座建设的战略使命，坚持以真实场景为牵引，围绕人形机器人具身智能迭代升级，以数据全生命周期治理为关键抓手，按照分层递进的建设路径，打通仿真训练与实景应用双向闭环，推动人形机器人从单点试验、实验室原型向常态化、规模化产业化落地升级。国地中心联合华为及华为云，依托 CloudRobo 具身智能平台的仿真与评测能力、云上昇腾算力以及具身模型联合创新能力，构建覆盖数据采集治理、仿真生成、模型训练、能力评测和场景验证的具身智能实训体系。

2、建设架构

构建贯通训练场与真实场景、连接线下数据底座与云上智能算力的具身智能实训架构。线下基于华为 OceanStor Pacific 分布式存储承载机器人多模态数据，通过基模采训中台完成数据汇聚与治理；云上依托昇腾算力支撑具身模型训练与迭代，并通过 CloudRobo 提供场景仿真、模型评测和能力验证，最终由场景应用中台将模型能力部署至真实产业场景，形成“数据采集—仿真生成—模型训练—综合评测—场景应用—运行回传”的持续迭代闭环。

（1）基础底座层

以华为 OceanStor Pacific 分布式存储为核心，打造统一的机器人训练场存储底座，建成 6PB 专属资源池，提供海量存储、高并发吞吐、统一调度管理能力，为上层数据处理和模型训练提供支撑。配套全栈轻量云解决方案，对 AI 服务器、存储、网络、虚拟化、容器等各类资源实现统一纳管。同时按

需调用华为云昇腾算力，承载具身模型训练、调优和推理验证任务，实现本地数据底座与云上智能算力协同。

(2) 平台能力层

建设基模采训中台，部署多源异构采集终端和一体化数据治理平台，建立行业数据标准规范，实现真实作业数据、遥操作数据和仿真数据的全域汇聚与统一治理。引入华为云 CloudRobo 具身智能平台，开展机器人任务场景构建、并行仿真、模型评测与能力验证，通过仿真数据补充真实数据，并在进入真实场景前对模型能力进行验证。同时，按需提供数据工程、模型工程和智能体开发能力，支撑具身模型持续开发与迭代。

(3) 技术创新层

构建“五模四台一集”的“5+4+1”具身智能技术体系，以真实场景需求为牵引，从应用价值和技术可行性评估切入。国地中心与华为云围绕具身模型开展联合共创，基于行业场景数据和云上昇腾算力，推进模型训练、调优及场景适配，并通过 CloudRobo 完成仿真测试与综合评测，贯通“场景评估—任务定义—数据采集—数据治理—数据集沉淀—模型训练—仿真评测—场景部署—运行回传—迭代优化”全流程。

(4) 场景生态层

以基模采训中台为核心枢纽汇聚全域训练数据，通过场景应用中台向应急救援、能源电力等真实产业场景输出模型与机器人能力。真实场景产生的运行数据、任务结果和失败案例持续回流，经数据治理后用于模型再训练，并通过 CloudRobo 开展仿真复现和回归评测，形成“仿真验证—实景应用—数据回流—模型优化”的持续增益循环。

3、核心能力

数据高效存储管控能力：采用华为 OceanStor Pacific 分布式存储，打造三大核心能力。一是高并发吞吐能力，可支撑大规模数据集高速加载与实时数据注入，缩短模型迭代的数据准备时间；二是海量弹性扩展能力，可安全、长期存储机器人作业原始视频、点云等历史数据，满足算法回溯、重复训练、

合规留存等需求；三是集约化管理能力，通过统一管理视图实现数据按场景分层存储、集中调度，解决传统数据散乱存储、管理无序的问题。通过高吞吐数据供给和云上云下协同，为昇腾算力上的具身模型训练与迭代提供稳定的数据支撑。

全链路数据流转能力：打通数据湖的多协议互通，支持 S3、NFS、HDFS、POSIX 等多种协议并发访问，可自适应处理大小 I/O 混合负载，实现数据导入、脱敏、上传全流程一体化。同时，具备冷热数据自动分级、全局智能调度能力，支持数据跨训练场按需流动、云上云下灵活调度，推动数据管理从传统“静态存储”升级为“动态智能流转”。支持真实采集数据、仿真生成数据及模型训练数据在训练场、CloudRobo 和云上昇腾算力之间按需流转，支撑数据治理、模型训练、仿真评测和结果回流。

闭环式具身智能迭代能力：依托“5+4+1”具身智能技术体系，通过五类模型协同、四大平台贯通和白虎 2.0 数据集持续沉淀，国地中心与华为云联合推进具身模型研发与场景适配。基于云上昇腾算力完成模型训练、调优和推理验证，利用 CloudRobo 开展仿真测试、能力评测与回归验证，构建“以场景为牵引、以数据为基础、以模型为核心、以评测为门禁、以应用反馈为驱动”的闭环技术体系。

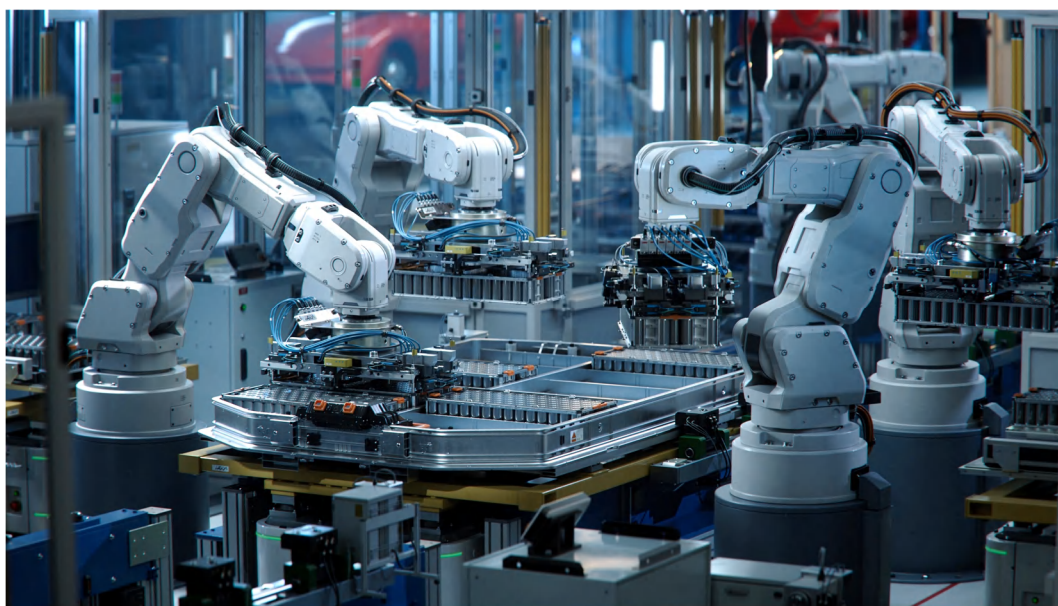
4、应用成效

(1) 产业生态

成功打通训练场到真实产业场景的业务闭环，国地中心已与上海市消防救援局、国网上海电力等六方主体达成合作，落地应急救援、能源电力等六大核心应用赛道，推动人形机器人投入真实产业环境常态化作业，实现了技术成果从研发、训练到落地应用的完整转化。基于统一的数据底座、云上昇腾算力和 CloudRobo 仿真评测能力，为生态伙伴提供从数据准备、模型训练到场景验证的公共技术支撑，降低具身智能技术进入行业场景的验证门槛。上海市人形机器人中试服务平台在浦东全面投运，形成年产 2000 台整机的规模化制造产能，有效推动人形机器人产业从单点试点走向规模化落地。

(2) 技术成效

通过标准化数据治理体系和闭环迭代机制,打通机器人数据采集、治理、训练、评测、应用及回流的全生命周期链路,提升数据利用效率和模型迭代效率。国地中心联合华为云建设具身智能实训场样板点,以 OceanStor Pacific 承载海量多模态数据,以云上昇腾算力支撑具身模型训练与调优,通过 CloudRobo 开展场景仿真、模型评测和能力验证,并围绕具身模型开展联合共创,形成“真实数据沉淀—仿真数据补充—模型训练—综合评测—场景应用—运行数据回流”的完整数据与模型飞轮,为后续“1+N”训练场建设和多行业场景复制提供可复用的技术路径。



（四）无锡 AI CITY 具身智能与产业焕新

1、案例概述

在数据和模型融合迭代的浪潮下，人工智能正由虚拟世界加速驶向实体经济的深水区，成为重塑城市产业竞争力的关键引擎。

作为长三角先进制造业的重要基地，无锡拥有门类齐全的工业体系与海量真实的产业场景。然而，在传统工业迈向智改数转的过程中，如何跨越技术落地的“最后一公里”，让大模型真正走进车间、赋能中小企业，成为摆在眼前的现实课题。

为破解传统产线换线周期长、改造成本高、严重依赖熟练工等痛点，无锡数据集团联合华为云，以 CloudRobo 具身智能模型平台为技术底座，结合无锡本土丰富的工业场景与需求，构建起以工业场景为核心、多技术融合叠加的具身智能服务体系和场景化解决方案。它如同制造名城的“小脑”，联动多种机器人本体形成“双手”，实时感知生产一线的细微变化，为产业集群焕新、柔性智造升级提供坚实支撑。

当前，依托 CloudRobo 平台，该体系汇聚多维工业数据与前沿具身算法，重点聚焦扁线电机柔性插装、柔性焊接、精密螺丝锁付等细分场景，推动具身智能技术在中小企业产线中初步实现规模化落地与应用。

在此基础上，相关场景化应用融合多模态感知与高精度力觉控制，有效破解扁铜线易变形、端部空间狭小等工业精细操作难题，动态规划插装轨迹，使换型时间从数小时缩短至分钟级，显著降低次品率。

2、解决方案

（1）平台架构

基于 CloudRobo 具身智能平台，系统构建了“数据-模型-产线”闭环的自回归与自进化应用转化架构，覆盖从实验室研发到工业级交付的全生命周期。

底层感知与数据采集层：依托工业现场高精度视觉与力觉传感器，实时捕捉多维工业数据（如扁铜线微小形变与状态），构建多模态数据回流通道的。

中枢模型与闭环训练层：

1) 实验室预训练 (90%成功率)：采用仿真环境与离线/历史数据，通过强化学习 (RL) 与 Sim2Real 预测，完成具身智能大模型的基础算法训练与预测验证。

2) 上线小量培训 (95%-99%成功率)：利用基于低成本离线训练与人机共控微调 (安全策略监控+降本策略)，实现产线快速对接与试运行。

3) 正常产线运行 (99.999%成功率)：模型下发至现场执行套件，实现高精度的实时自主规划与柔顺控制。

4) Corner Case 修复与自进化：针对运行中的异常数据进行分析提取、针对性强化训练与验证评估，驱动模型常态化持续迭代。

顶层应用层：聚焦扁线电机柔性插装、柔性焊接及精密螺丝锁付等高难度工业场景，打通智能落地“最后一公里”。



(2) 技术先进性

全流程“自回归+自进化”数据闭环：通过“数据采集→模型微调→现场运行→异常数据回流→增量训练”的完整自回归机制，实现任务成功率从实验室90%到工业级99.999%的阶梯式跃升。

大模型驱动的多模态柔顺感知与自主规划: 融合高精度视觉与触觉感知, 使机器人具备动态形变感知与无损插入能力; 依托云端具身智能大模型, 实现动态轨迹规划与多根扁线同步插装, 有效解决传统固定轨迹算法“看不准、插不进”的痛点。基于 CloudRobo 平台, 面向具体工业场景完成多模态数据的采集、清洗、标注与增强, 构建高质量场景数据集。随后开展具身模型训练、微调与仿真验证, 形成从数据到模型再到仿真的闭环, 为真实产线落地提供支撑。

低成本 Sim2Real 迁移与人机共控安全机制: 通过虚拟仿真与强化学习预训练, 配合线上小样本微调与人机共控安全策略, 大幅降低新产线部署与改造成本, 避免中小企业对高资历熟练工的过度依赖。

3、应用成效

提质增效与高良品率: 通过“视觉+力控”多模态感知与动态柔顺控制, 解决传统自动化设备在扁铜线微小形变下“看不准、插不进”的行业难题。将复杂狭窄铁芯槽的多线同步无损嵌入成功率从实验室阶段提升至工业级 99.999%, 大幅降低工件损耗, 保证产线高良品率与稳定节拍。

极简部署与降低改造成本: 依托“Sim2Real 虚拟仿真预训练+人机共控小样本微调”的技术路径, 实现新产线快速对接与上线调试。部署周期与二次改造成本相比传统方案显著下降, 极大降低了对高资历熟练工的依赖, 实现从“依赖经验”到“算法赋能”的转变。

自我演进与长效运营: 基于“数据采集→异常回流→增量训练→模型下发”的自回归数据闭环机制, 系统具备对工业 Corner Case (边缘异常场景) 的自主修复与持续进化能力, 保障产线在面对多样化变型需求时仍能保持长期高效的柔性生产。

4、生态扩展

(1) 工业千行百业的多元延伸

扁线电机柔性插装的成功实践了具身模型的强泛化能力与跨场景迁移能力, 并加速向更多高复杂度工业细分场景拓展:

柔性焊接：针对复杂焊缝与非标工件，依托多模态感知实时捕捉焊接过程中的热变形，实现智能轨迹自动生成与自适应动态纠偏，大幅提升焊缝质量与加工稳定性。

精密螺丝锁付：动态适应不同孔位布局与狭窄空间，结合高精度力矩反馈与柔顺控制，实现全方位防扣线、防滑丝与漏锁检测，保障高可靠性装配。

(2) 具身数据服务与生态普惠

在深化落地解决方案的同时，进一步开辟了“面向模型公司的具身数据服务（采治训推一体）”第二增长曲线，推动产业生态与中小企业数字化转型：

数据生态与商业化高速扩张：已对接超 15 万小时的具身数据需求，完成签订超 4 万小时、总金额超过 1400 万元的高质量数据服务订单；同时，“数据合伙人计划”已吸纳 20 家行业成员单位，构建起可持续进化的高质数据生态。

赋能中小企业“数转智改”：通过提供即插即用、轻量化且高性价比的具身智能软硬件方案与数据普惠服务，降低智能化升级门槛，切实破解中小企业“不会转、不敢转”的痛点。

（五）深圳龙岗“龙小二”AI 原生城市治理智能体

1、案例概述

深圳市龙岗区依托“All in AI”战略，依托华为云、鲲鹏、昇腾等 ICT 基础设施，持续打造各类智能体应用场景，目前已经陆续上线了八个“龙搭子”人工智能产品矩阵。以“龙”为姓，覆盖工业、教育、医疗、治理、低空、居住、文旅、企服八大场景，将抽象的 AI 技术转化为市民熟悉的“城市伙伴”。分别是：**龙医生**：健康搭子，健康守护龙“马”精神。**龙老师**：学习搭子，学子的 AI 私教。**龙导游**：旅游搭子，AI 辅助沉浸趣游“导”此一游。**龙管家**：居家搭子，市民的数字家园智护相伴。**龙小二**：治理搭子，城市运行智能守护。**龙飞手**：巡飞搭子，空中“慧眼”全时值守。**龙师傅**：产业搭子，AI 赋能智造同行。**龙 i 企**：企业服务搭子，企业和员工的 24 小时“智能合伙人”。“龙小二”AI 原生城市智能体是其中典型的场景之一。

2、建设架构

“龙小二”依托于华为昇腾的强大算力和云天励飞、谛视万象等多家厂商的智能体、CV 大小模型等相关技术底座以及多类场景算法能力，构建了具备“自感知、自思考、自执行、自进化”能力的 AI 原生城市治理智能体。

龙岗区汇聚了全区摄像头、无人机、物联感知、12345 等各类数据，多源融合，形成龙岗区城市治理的高质量知识库，“龙小二”持续进行学习，最终构建起“自感知、自思考、自执行、自学习”的“四自”城市治理新范式。龙小二从底层架构出发，以 AI 原生理念重新定义城市治理系统，让 AI 能力如同操作系统般贯穿感知、认知、决策、执行的全链路。这让城市治理的核心主体，第一次从“人”变成了“人机共生”的智能体。

3、核心能力

“龙小二”通过“自感知、自思考、自执行、自进化”能力，既能应对日常城市治理的普通事件，也能应对大规模重大应急场景的全流程主动防控与执行。

重大应急场景举例：汛期防控

2026 年 7 月下旬，台风“红霞”逼近广东深圳时，“龙飞手”调动 40 余架无人机进行沿河道、低洼边坡、山林全域开展前置排查。领导一句话下发巡检任务，“龙小二”智能体自主调取画面，快速甄别，几分钟内锁定多处营业点位，线索直达各街道工作群，基层工作人员第一时间上门劝导群众避险。同时“龙小二”还精准识别树木倒伏、道路积水等隐患，同步归集群众防汛求助工单，一键分流至街道处置。“龙小二”已经成为工作群中不可或缺的网格员、分拨员、督办员等等多种角色。



图 42 “龙小二”城市治理智能体

目前，“龙小二”与“龙飞手”正在探索实现全自动联动、协同作战，是未来重点建设方向。搭建“龙小二”“龙飞手”空地协同治理体系，借助智能算力减轻基层人员压力，能推动城市治理从被动抢险转向提前预判、全域智能防控。

日常城市治理举例：占道经营提醒

依托全域视频智能感知体系，龙小二日均解析图片 250 万张、感知城市运行数据近 20 万条，自动识别占道经营、路面破损、井盖缺失、河道积水、工地违规、后厨隐患等各类城市问题，实现高频治理问题“机器自动看、智能主动判”。同时搭建分层政务知识库与长短中三期记忆架构，能够自主拆解复杂任务、研判风险趋势、规划处置方案，联动四足机器狗、无人机等智能终

端完成现场劝导、隐患处置、数据回传，实现“发现-研判-调度-处置-复盘”全链路无人干预闭环。

以占道经营提醒为例，“龙小二”发现占道经营，自主生成任务工单下发任务给机器狗，自主规划路径，机器狗自行前往事发地、喊话提醒，最后时间处理完毕反馈结果、智能体识别事件闭环、关闭事件、机器狗返回。整个流程中，“龙小二”+机器狗全流程自主处置，无需人工介入。



图 43 “龙小二”+机器狗占道经营提醒场景

4、应用成效

“龙小二”是龙岗区打造的 AI 原生城市治理智能体,具备自感知、自思考、自执行、自进化能力，推动城市治理从人海巡查向算力治理转型。系统整合视频监控、民生诉求等多源数据，部署多类算法，覆盖应急防汛、市容管理等场景。在暴雨红色预警实战中，自动启动汛期模式，高频扫描全区易涝点、河道、树木倒伏风险点位，短时间内分析数十万张监控图像，发出上千次精准预警，预警准确率较高，隐患信息直达一线处置人员，完成人力无法完成的提前巡查任务。

“龙小二”联动机器狗、“龙飞手”低空无人机平台形成空地协同处置闭环，自动派单分流工单，实现隐患前置发现、闭环处置。有效减少人工盯守压力，推动治理由事后处置转向事前预防，释放基层人力聚焦群众服务，为超大城市基层治理数字化、智能化探索出新范式。

（六）深圳市气象大模型

1、案例概述

深圳地处华南沿海，属亚热带海洋性气候，是台风、暴雨、雷暴、强对流等灾害性天气的高发区。在全球气候变化背景下，极端天气气候事件频发、强度增强，深圳面临的气象灾害风险日趋复杂严峻。作为粤港澳大湾区的核心引擎和人口高度密集的超大型城市，深圳气象防灾减灾工作呈现出以下显著高敏感性、高复杂性、高时效要求、高分辨率需求的特点。华为云联合深圳市气象局打造的首个人工智能区域预报模型“智霖”1.0 于 2024 年投入使用。“智霖”区域模型以华为云盘古气象大模型为基础，融合区域高质量气象数据集，可快速得到未来 5 天深圳及周边地区空间分辨率为 3 公里，包含气温、降雨、风速等气象要素的预报。区域预报模型已在多次冷空气过程的气温预报和龙舟水的暴雨预报中为预报员提供可靠参考，并在台风“摩羯”等路径预报工作中表现优异，预测结果更稳定、更精准。深圳市气象局提出“三步走”战略需求，对应三期建设目标：

一期（智霖大模型 1.0）：夯实底座，实现 AI 预报从“0 到 1”的突破。建设高质量再分析数据集（5 年以上、3km 分辨率），完成全球 AI 预报模型的本地化微调和区域预报模型开发，实现未来 5 天、3km 分辨率、1 小时时间步长的业务化预报能力，预报准确性较传统高分辨率数值模式提升 5%，25 分钟内完成预报推理，系统故障率低于 1%。

二期（智霖大模型 2.0）：拓展能力，构建集合预报体系。在确定性预报基础上，构建不少于 30 个成员的集合预报系统，实现从“单一结果”向“概率预报”的跨越，每日运行频次由 2 次提升至 4 次，推理速度大幅优化（单成员两卡并行 5 日预报 10 分钟内完成），预报准确性较欧洲中心高分辨率数值模式提升 5%。

三期（智霖大模型 3.0）：追求卓越，实现核心技术突破。针对极端天气预报这一世界性难题，在确定性预报精度（ETS 评分较欧洲中心提升 10%）、台风强度预报（3 天误差降低 10%）、生成式 AI 与物理约束融合、集合预报系统升级（7 天预报、30 成员、1km 分辨率）、系统稳定性（无故障时间 99%

以上）等方面实现全面突破。

2、建设架构

为支撑上述高复杂度 AI 气象模型的训练与业务化运行，需构建坚实的数据与算力底座。整体架构遵循“利旧改造与新建结合”的原则，打造集数据汇聚、算力调度、模型管理于一体的智能底座。新建深圳 3km/1km 高质量再分析资料数据集（≥5 年），在原有基础上打造实时雷达、卫星、探空、地面等多源观测数据，改造海量多元数据同化与预处理管道，新建高性能 GPU 集群，配套高速并行文件存储和低延迟网络，以满足大模型训练和推理的算力需求，打造 AI 算力资源池。

数据支撑层为模型提供“燃料”。一期建设的 5 年、3km 分辨率再分析资料集是核心，结合实时观测数据，形成训练与推理的数据闭环。模型训练与微调层是技术核心。一期基于华为盘古气象模型进行迁移学习与本地微调；二期开发区域预报模型；三期引入物理约束与生成式 AI，提升区域降水事件的预报性能与探测概率。模型推理层支撑业务化运行。包含确定性预报、集合预报（30+成员）、专项模型（台风强度）以及后处理模块（如偏差订正、降尺度、生成式 AI 的集合成员生成）。业务服务层将模型能力封装为标准 API，供前端预警发布平台、决策支持等业务系统调用。支持高并发、低延迟的实时推理请求。应用场景层最终服务于深圳气象防灾减灾的各类具体场景。



图 44 深圳市气象大模型架构图

3、核心能力

依托华为 ModelArts 平台：新建“智霖”系列模型（1.0/2.0/3.0），包括全球模型的本地化微调、区域预报模型的开发、集合预报系统、物理约束生成式模型等核心算法功能。

海量数据处理能力：支持 TB 级气象多源数据的清洗、同化、融合与高效读取，满足高频次模型训练与推理需求。

高性能并行计算能力：具备强大的多卡 GPU 并行推理能力，确保单集合成员在两卡并行下 5 日预报耗时<10 分钟，30 个成员 5 日集合预报及后处理总耗时<60 分钟。

高可用与自动化调度能力：系统具备故障自动隔离与恢复能力，保障无故障运行时间达 99%以上，支持推理任务的自动化编排与全链路监控。



图 45 深圳市气象大模型能力示意图

4、应用成效

通过三期建设，深圳“智霖”项目显著提升深圳作为超大城市应对气候变化和极端天气的“韧性”，为建设更高水平的平安深圳提供坚实的气象保障，助力实现“监测精密、预报精准、服务精细”的目标。

预报能力实现代际跃升。确定性预报对华南区域降雨的 ETS 评分全面超

越欧洲中心高分辨率模式，三期提升 10%；台风强度预报误差降低 10%；实现 1km、1 小时的“城市级”精细网格预报，能够精准刻画局地强对流、城市热岛等微尺度天气过程；建成 30+成员的集合预报系统，提供更可靠的概率预报产品，为决策者提供“风险地图”而非单一“结果”。

防灾减灾效能显著提升。对极端暴雨、台风等灾害性天气的预警信号发布提前量有望提升 30%以上。5 日预报在 25 分钟内（三期 60 分钟完成 30 成员集合）完成，支撑高频次、滚动式更新，为水务调度、交通管制、人员转移等应急决策赢得宝贵时间。通过更精准的预报和更及时的预警，有效减少因气象灾害造成的直接经济损失。

(七) 武汉医保影像云

1、案例概述

2026 年 6 月 22 日，国家医保局发布了《“医保影像云”基础规范》，明确依托全国统一医保信息平台，实现医疗机构间影像检查数据跨省互通共享。目前，全国统一的医保信息平台累计归集的医保影像云索引数据已达到 4.3 亿条。作为国家医保局指定的医保影像云建设试点先行城市，武汉走出了一条融合顶层设计、技术底座与商业运营的创新之路。从“物理胶片”到“数字影像”，从“孤岛存储”到“云端”共享，武汉市医保局携手超大城市数智运营商武汉云，在华为云提供的云计算底座与高阶服务支持下，以“数智”之力撬动医保健康领域的深层次变革。

2、建设架构

为了支撑起全市乃至全省海量医疗影像的互联互通，武汉云在技术架构上进行了前瞻性的顶层设计，构建了“1+1+N”的整体技术架构。其中，第一个“1”是医保影像云平台，集成软件平台、可信空间、云平台、通算与智算等能力；第二个“1”是实体的共享服务中心基地，作为数据汇聚与运营指挥的中枢；“N”则代表面向医保局、医疗机构、参保人以及运营方的多个服务端。这一架构为海量影像数据的安全流转搭建了坚实的数字骨架。

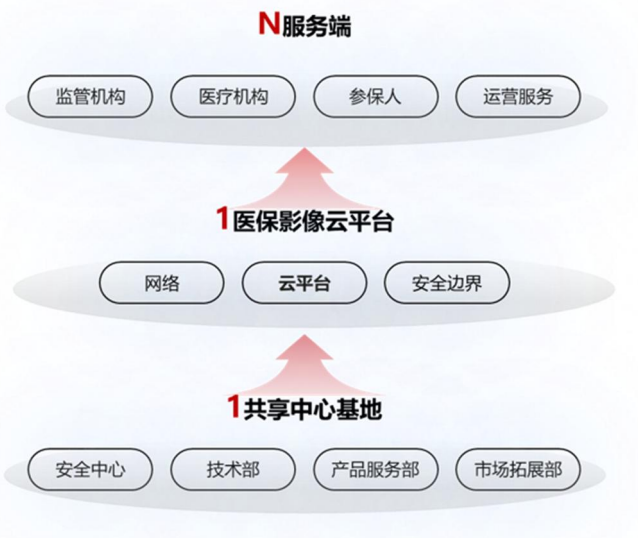


图 46 武汉医保影像云“1+1+N”整体技术架构

武汉云联合华为云，以华为云为技术底座，共同打造了“五统一”平台标准：统一数据标准、统一数据管理、统一安全出口、统一传输加密、统一自主创新体系。这套标准体系与国家医保局发布的《“医保影像云”基础规范》在数据采集、质量控制、安全管理等核心要求上高度同频，确保了武汉的试点实践从一开始就与国家顶层设计对齐，为后续实现全国范围内的“路路通”奠定了坚实基础。

平台从硬件、软件到操作系统与云平台，实现了统一自主创新体系，保障了国家医保数据的安全可控。而统一服务体系则确保无论是医生跨院调阅，还是患者手机端查看，都通过统一入口和标准接口实现，保证全省乃至未来全国范围内，影像调阅服务的体验一致与高度可用。

3、核心能力

为了实现对海量、异构数据的统一管理，平台将分散在各医院 PACS/HIS 系统中的影像数据，按照统一标准进行采集、建库与治理。通过部署在医院现场的前置机，实现数据的标准化上传，并在武汉云与华为云联合构建的云基础设施上构建了强大的影像数据能力平台。

考虑到医保数据的高度敏感性，安全是贯穿始终的生命线。平台通过构建端到端的传输加密保护与统一的安全出口管理，实现了高等级的安全防护。影像数据被智能地分为“热数据”与“冷数据”存储在新一代影像数据湖中，既确保了高并发场景下调阅的流畅性，又兼顾了数据全生命周期存储的经济性与安全性。与此同时，平台从硬件、软件到操作系统与云平台，实现了统一自主创新体系，保障了国家医保数据的安全可控。而统一服务体系则确保无论是医生跨院调阅，还是患者手机端查看，都通过统一入口和标准接口实现，保证全省乃至未来全国范围内，影像调阅服务的体验一致与高度可用。

4、应用成效

医保影像云的价值，远不止于“存起来”与“查得到”。在武汉的实践中，这一平台正在成为智慧监管与高效诊疗的双向引擎。2025 年 12 月，湖北正式成为全国首个全区域启动医保影像云跨省调阅的省份。在平台的设计蓝图与临床对接规划中，医保影像将无缝融入医生的日常诊疗流程。医生在开具检

查单时，只需嵌入院内信息系统，在获得患者授权后，即可一键调阅其在整个武汉市甚至省内其他医疗机构的历史检查报告与原始影像文件。这种嵌入式的设计最大的优势在于不干扰医生的既有工作习惯。系统在后台实现极速的影像传输与展示，辅助医生更迅速、全面地掌握患者历史病情，从而在源头上有效规避不必要的重复检查。

在监管维度，武汉市医保局与武汉云也在同步探索医保监管过程中的深度应用，推动医保治理从“被动应对”走向“主动智治”。系统通过大数据反欺诈与 AI 质控能力，能够自动识别疑似欺诈骗保行为。例如，通过“不同患者相同检查 DICOM 文件碰撞”的算法，平台可以精准定位虚假检查、重复收费等违规现象。这种基于数据驱动的“智防”手段，让医保基金的监管变得前所未有的精准、高效，为医保基金的安全筑起了一道坚实的数字屏障。从“人防”到“智治”，从“事后追责”到“事前预警”，武汉医保影像云正在重塑医保监管的底层逻辑。

结语



AI CITY 是 AI 原生的智慧城市，作为人工智能时代智慧城市发展新理念和新范式，绝非传统智慧城市简单叠加 AI 技术的迭代升级，而是下一代智慧城市底层逻辑的颠覆性变迁与发展模式的系统性升维。通过 AI 原生的高价值城市智能服务，让城市具备可感知、会思考、能行动、自迭代、高安全、易交互的系统性能力。

在大模型、智能体、云原生技术持续迭代的驱动下，城市发展正式从传统的数据驱动阶段，迈向知识驱动阶段，并加速向“城市超级智能体”跨越式演进，摆脱城市作为被动管控“物理容器”的传统定位，进化为具备全域感知、智能思考、自主行动、动态迭代与持续生长能力的“超级智能体”。

AI CITY 的建设发展始终坚守价值本位、摒弃形式主义，避免“为建而建、为智而智”的传统数字化建设误区，不局限于流程线上化、设备智能化的表层升级，而是以全维度价值创造为核心，让数字技术、智能算力、数据资源真正转化为可落地、可感知、可长效的发展效能，切实提升市民生活获得感、强化企业发展竞争力、优化城市治理掌控力、激活城市永续发展生命力。

立足人工智能发展浪潮，AI CITY 打造高质量、高价值智能服务，将重塑智慧城市建设的底层逻辑与发展范式，重新定义数智时代城市进化的全新未来，为建设创新、宜居、美丽、韧性、文明、智慧的现代化人民城市提供有力支撑！



商标声明

 HUAWEI, HUAWEI,  是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

版权所有 © 华为技术有限公司和国家信息中心共同所有。保留一切权利。
非经华为技术有限公司和国家信息中心共同书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

国家信息中心

地址：北京市西城区三里河路58号
联系电话：010-68557221
邮 编：100045
www.sic.gov.cn

华为技术有限公司

深圳龙岗区坂田华为基地
电话：+86 755 28780808
邮编：518129
www.huawei.com