CAICT 中国信通院

AiAB 人工智能关键技术和应用评测 工业和信息化部重点实验室

集智 蓝皮报告

人工智能研发运营体系（MLOps）实践指南（2023 年）

中国信息通信研究院云计算与大数据研究所

人工智能关键技术和应用评测工业和信息化部重点实验室

2023年3月

版权声明

前　言

随着国家新型基础设施建设发展战略（2020）、国家“十四五规划和2035年远景目标纲要”等系列政策的出台，人工智能（AI）发展迎来新一轮红利，科技革命和产业升级处于进行时。近年来，AI工程化的研究热度持续提升，其目的是帮助组织在数智化转型过程中，更高效、大规模地利用AI创造业务价值。人工智能研发运营体系（MLOps）作为AI工程化重要组成部分，其核心思想是解决AI生产过程中团队协作难、管理乱、交付周期长等问题，最终实现高质量、高效率、可持续的AI生产过程。

MLOps的发展呈现出逐渐成熟的态势，近几年国内外MLOps落地应用正持续快速推进，特别是在IT、银行、电信等行业取得明显效果。与此同时，MLOps行业应用成熟度不足，使得组织在制度规范的建立、流程的打通、工具链的建设等诸多环节面临困难。因此本指南旨在成为组织落地MLOps并赋能业务的“口袋书”，围绕机器学习全生命周期，为模型的持续构建、持续交付、持续运营等过程提供参考，推进组织的MLOps落地进程，提高组织AI生产质效。

本指南由中国信通院云计算与大数据研究所、人工智能关键技术和应用评测工业和信息化部重点实验室联合发布。本指南站在组织如何布局和落地MLOps的视角，以模型的高质量、可持续交付作为核心逻辑，系统性梳理MLOps概念内涵、发展过程、落地挑战等现状，并基于MLOps的理论研究和实践案例分析组织如何构建MLOps框架体系和关键能力，最后总结和展望其发展趋势。

由于AI产业的快速变革，MLOps落地应用持续深入，工具市场不断迭代，我们对MLOps的认识还有待继续深化，本指南可能仍存在不足之处，欢迎大家批评指正。

目　录

图 目 录

表 目 录

一、MLOps 概述

MLOps 是通过构建和运行机器学习流水线（Pipeline），统一机器学习（ML）项目研发（Dev）和运营（Ops）过程的一种方法，目的是为了提高 AI 模型生产质效，推动 AI 从满足基本需求的“能用”变为满足高效率、高性能的“好用”。本章首先阐述组织在 AI 大规模生产过程中凸显的管理问题，然后梳理 MLOps 概念和意义，并分析落地 MLOps 所遵循的原则。

（一）AI 生产过程管理问题凸显

Gartner 调查发现，只有 53%的项目能够从 AI 原型转化为生产[1]。AI 生产转化率低的主要原因在于模型全链路生命周期管理存在问题，包括跨团队协作难度大、过程和资产管理欠缺、生产和交付周期长等。

第一，跨团队协作难度大。机器学习项目生命周期中涉及业务、数据、算法、研发、运维等多团队，团队间缺乏相同的技术和业务背景知识作为协作基础，从而带来沟通屏障。同时每个团队的协作工具不尽相同，从数据和算法转化为推理服务的整个过程漫长而复杂，从而增大协作难度。

第二，过程和资产管理欠缺。模型生产过程无标准化管理，导致 AI 资产的价值无法有效发挥。原因在于以下几方面：一是生产过程冗长难管理，AI 模型生产过程涉及的环境、流程复杂，各部门习惯于小作坊的生产模式，重复造轮子现象普遍；二是 AI 资产无集中共享机制，组织内数据、特征、模型等碎片化 AI 资产无法共享使用，优秀实践经验难以沉淀。

[1] Gartner,《Top Strategic Technology Trends for 2021》.

第三，生产和交付周期长。机器学习模型生产和交付是一个漫长、复杂又易出错的过程，且耗费的时间成本较高。据 Algorithmia 报告显示，38％的企业花费超过 50％的时间在模型部署上[2]。这一现象的主要原因有三：一是模型文件的生产需要经过不断重复的实验和评估；二是模型服务需要通过编写服务代码和配置参数，并达到业务需求后，方可部署上线；三是业务效果的保证需通过在线模型开展服务验证和结果对比。

（二）MLOps 概念与意义

MLOps 通过连接模型构建团队、业务团队及运维团队，为机器学习模型全生命周期建设标准化、自动化、可持续改进的过程管理体系，使组织规模化、高质量、高效率、可持续地生产机器学习模型。MLOps 能有效缓解 AI 生产过程的各种管理问题，提升 AI 生产的转化效率。

来源：中国信息通信研究院

图 1 MLOps 示意图

MLOps 理念源于面向软件工程的管理方法论 DevOps，起初希望可以参考传统软件生产过程的管理方法，以应对提质增效的挑战。然而 DevOps 并不完全适用，因为机器学习项目是以数据、算法、代码、

[2] Gartner,《Gartner Top 10 Data and Analytics Trends for 2021》.

模型为核心的**动态模式**，整个过程充满探索性、实验性和不确定性。若要迎合动态模式的需求，需要一种融合了机器学习特性的 DevOps 方法或体系，MLOps 应运而生。MLOps **意义和价值**主要体现在以下几方面。

第一，建立团队协作机制。通过在组织级明确各流程中各角色（例如业务人员、数据工程师、数据科学家、运维工程师等）和职责，并以流水线的方式连接各团队成员的工作，使团队协作机制得以建立，打破沟通屏障，让不同角色各司其职（例如，使数据科学家不用再沦陷于处理繁琐的模型更新和维护等工作），降低团队间整体合作成本。

第二，实现敏捷交付过程。通过自动化流水线等方式实现敏捷交付，从而提高模型交付效率，加快模型迭代速度，提高模型效果，提供更丰富、更优质的产品体验。

第三，构建全链路反馈闭环。通过贯通需求、开发、交付、部署、运营多环节的全链路，嵌入合规、监管、道德、安全等要求，形成完整的全链路流水线。同时，持续改进和简化原有运营和治理流程，高效率、低风险地实现持续集成、部署、训练和监控，形成有效的反馈闭环。

第四，统一管理 AI **资产。**机器学习项目中数据、算法、特征和模型等资产是一个有机整体，通过对 AI 资产的高效统一管理，并加以风险防控和安全管理等手段，实现有效治理。

（三）MLOps 实施原则

作为 AI 基础设施之一，MLOps 促进各团队高效协作，提升业务价值产出。一般来说，实施 MLOps 需要遵循的原则包括自动化、持续性、版本化、可监控、可测试、可追溯、可复现、可协作等。

来源：中国信息通信研究院

图 2 MLOps 实施原则

自动化包括模型自动化构建、自动化集成、自动化测试、自动化部署等，减少人工操作，提高操作准确性，是 MLOps 的核心。

持续性包括持续集成（CI）、持续部署（CD）、持续训练（CT）、持续监控（CM），是 MLOps 实现全流程闭环的基础。

版本化包括数据、模型和代码等 AI 资产的版本控制能力，是达到可复现、可追溯的基础，是保证资产可在组织各层面共享使用的基本能力之一。

可监控包括模型、模型服务及模型生产过程等维度的健康状态监控能力，以发现数据漂移和概念漂移，识别问题和改进方向，是维护高质量模型服务的基础。

可测试从模型评估、集成测试、系统测试、业务测试、生产验证等过程维度，保障模型的功能、性能和可信能力（安全性、保密性、可解释性、公平性等）满足需求，是保证模型交付质量的重要手段。

可追溯通过“效果→模型→实验→数据”全流程追溯过程的实现，提供模型实验及数据的血缘回溯能力，是根因分析的基础，是事后审计的手段，也是过程可信的体现。

可复现通过端到端记录模型构建过程相关数据、算法、参数等元数据信息，支持重现实验过程并获得高度相似的结果，是数据科学家开展模型工程的重要支撑。

可协作确保不同团队角色在数据、代码和模型上进行协作，是全流程可持续闭环实施的协作基础，是提高团队整体效率的保障。

二、MLOps 发展现状与挑战

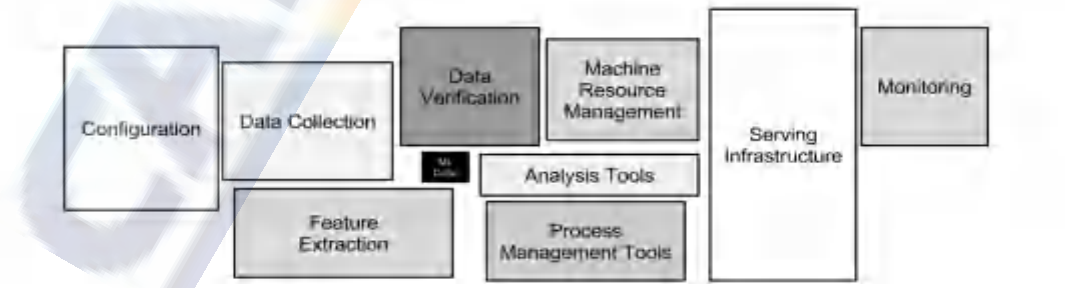
MLOps 在国内外得到了广泛应用，并在多个行业取得了实质性效果。本章首先阶段性梳理 MLOps 发展历程，然后从落地应用和工具市场等角度分析当前发展现状，最后总结了 MLOps 落地面临的挑战。

（一）MLOps 发展过程

1.发展历程

2015 年至今，从业界意识到机器学习项目技术债给 AI 生产上线带来的潜在巨大影响伊始，MLOps 前后经历了斟酌发酵、概念明确、落地应用三大阶段。

斟酌发酵阶段（2015 年至 2017 年前后）。2015 年 Google 在 Conference and Workshop on Neural Information Processing Systems（NIPS）上发布的论文《Hidden Technical Debt in Machine Learning Systems》首次提出机器学习项目技术债问题，一方面，机器学习项目具有传统软件工程的代码运维问题，这部分问题占比较小；另一方面，机器学习项目本身存在数据依赖关系不稳定、配置易出错、实验不可重现等问题，为模型的持续运维和迭代带来大量隐患。这篇论文标志着机器学习高效落地问题被明确提出和正视，也催生了产业界形成系统化的方法论和规范化的管理流程，解决技术债问题的强烈需求。

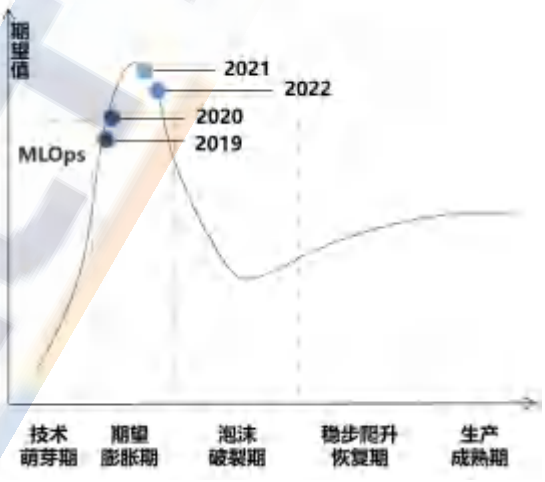


来源：《Hidden Technical Debt in Machine Learning Systems》

图 3 机器学习技术债示意图

概念明确阶段（2018 年至 2019 年前后）。2018 年业内人士逐渐开始密集讨论大规模生产中机器学习生命周期集成化管理的重要性，MLOps 这一概念被提出并逐步接受。2019 年《Continuous Delivery for Machine Learning》[3]提出的 CD4ML 理念，阐述了机器学习项目如何开展持续交付(CD)，并提出端到端的交付流程。CD4ML 将传统软件工程中的持续交付方法论扩展到机器学习中，使跨团队成员可基于数据、代码和模型，实现机器学习项目小步快跑、安全持续的增量式迭代。

落地应用阶段（2020 年至今）。2020 年以来，产业焦点集中于 AI 大规模快速落地，布局 MLOps 平台或工具的需求日益迫切，推动组织数智化转型成为产业界追逐的目标。2021 年，Gartner 将包括 MLOps 在内的 XOps 列为 2021 年十大数据和分析技术趋势之一[4]。此外，从 2019 年到 2022 年，Gartner 连续 4 年将 MLOps 纳入数据科学与机器学习技术成熟度曲线[5]。2021 年，中国信息通信研究院牵头开展 MLOps 系列标准编制，以引导产业有序发展，形成行业自律规范。



来源：Gartner

[3] Continuous Delivery for Machine Learning，https://martinfowler.com/articles/cd4ml.html.
[4] Gartner,《Gartner Top 10 Data andAnalytics Trends, 2021》.
[5] Gartner, 《Hype Cycle for Data Science and Machine Learning》（2019,2020,2021,2022）.

图 4 Gartner 数据科学和机器学习技术成熟曲线

2.发展现状

MLOps 产品提供方和应用方不同程度地受益于 MLOps 体系的蓬勃发展。随着工具市场和行业应用的发展不断推进，新工具不断涌现，在 IT、金融、电信等行业得到了广泛应用和落地。根据情报和市场研究平台 MarketsandMarkets 2022 年研究报告显示，MLOps 市场规模将从 2022 年的 11 亿美元增长到 2027 年的 59 亿美元[6]。

（1）资本市场持续火爆，MLOps 工具不断创新

近年来，MLOps 相关工具链已成为 AI 投融资领域的明星赛道，涌现了诸多以 MLOps 工具为主打产品的初创公司。例如，聚焦于深度学习可视化工具的 Weights & Biases 获得 2 亿美元融资，且平台估值达 10 亿美元；聚焦于提供机器学习平台的 Tecton 获得 1.6 亿美元融资；聚焦于机器学习模型多硬件适配部署的 OctoML 获得 1.33 亿美元融资，且平台估值达 8.5 亿美元。

在资本市场的驱动下，MLOps 工具持续创新。据不完全统计，目前全球约有 300 多款工具，大致可分为两类：一类是 MLOps **端到端工具平台**，为机器学习项目全生命周期提供支持。端到端工具平台包括国外的 Amazon SageMaker、Microsoft Azure、Google Cloud Platform、DataRobot、Algorithmia、Kubeflow、MLflow 等，国内的百度智能云企业 AI 开发平台、阿里云机器学习平台 PAI、华为终端云 MLOps 平台、腾讯太极机器学习平台、九章云极 DataCanvas APS 机器学习平台等；另一类是 MLOps **专项工具**，对特定步骤提供更为集中的支持，主要包括数据处理、模型构建、运营监控三大类。专项工具包括国外

[6]https://www.marketsandmarkets.com/Market-Reports/mlops-market-248805643.html?gclid=EAIaIQobChMItqHNwYaw_AIVBilMCh1sqwwbEAAYASAAEgKnBPD_BwE.

Cloudera 提供的数据共享工具，DVC 和 DAGsHub 提供的数据和模型版本管理工具，Neptune.ai 提供的元数据管理工具等，国内的星环科技提供的运营监控工具，第四范式提供的特征实时处理工具，云测数据提供的标注工具等。

来源：中国信息通信研究院

图 5 MLOps 工具分类一览

（2）MLOps 行业应用稳步推进，落地实践成果颇丰

第一，国外 MLOps 落地广泛、效果显著。其主要应用于组织内部的服务运营、产品或服务开发、营销、风险预测及供应链管理等场景，应用行业涉及 IT、金融、电子商务、制造、化工和医疗行业等。

IT 行业：应用 MLOps 后，美国某 IT 公司将开发和部署新 AI 服务的时间缩短到原来的 1/12 到 1/6，运营成本降低 50%；德国某 IT 公司，通过自动化编排和实验跟踪，以相同的工作量运行 10 倍的实验数量；以色列某 IT 公司实验复现时间减少 50%；某美国出行科技公司三年内机器学习产品数量从零扩展到数百个。

金融行业：应用 MLOps 后，新加坡某保险公司推理结果的生成时间从几天缩短至不到 1 小时；欧洲某大型保险公司节省了大量维护

和调查时间，可实时跟踪和比较模型性能，并自动检测以前需要数月才能检测到的漂移；美国某支付公司可实时部署和运行其反欺诈预测模型，并实时分析新数据以适应新威胁。

电子商务：应用 MLOps 后，荷兰某酒店预定网站通过打通机器学习模型生产流程，提高了生产规模，具备应用 150 个面向用户的机器学习模型的能力，逐步推进 AI 规模化落地。

制造业：应用 MLOps 后，土耳其某水泥制造公司通过提升模型生产效率和质量，大大提升了 AI 赋能业务的能力，使得替代燃料的使用量增加 7 倍，减少 2%的二氧化碳排放总量，成本降低 3900 万美元。

化工行业：应用 MLOps 后，美国某化工企业将模型部署周期从原来的 12 个月缩减至 30 到 90 天。

医疗行业：应用 MLOps 后，美国某医疗企业通过快速构建和测试模型，为业务提供精准决策，使得每年从患者日支付的护士工时中节省 200 万美元，通过减少患者住院时间每年可节省 1000 万美元[7]。

第二，国内 MLOps 处于规划和建设前期，落地探索成效初显。IDC2022 年预测，到 2024 年 60%的中国企业将通过 MLOps 来运作其机器学习工作流[8]。近 3 年来，国内各行业开始探索契合自身特点的 MLOps 落地解决方案。在数智化转型热潮中，IT、金融和电信等数字化程度较高的行业处于相对领先地位，其他行业进展稍缓。

IT 行业：凭借在数据方面拥有的先天优势，IT 行业最早开始构建 MLOps 并驱动其业务智能化水平的提升。如百度、华为、阿里、京东等，关注机器学习项目全生命周期的优化和改进，并在原有 AI

[7] https://research.aimultiple.com/mlops-case-study/#introducing-mlops-to-your-business.
[8] IDC, 《IDC FutureScape: 全球人工智能（AI）及自动化市场 2022 预测——中国启示》.

中台或云服务平台上逐步扩展 MLOps 过程管理功能，实践效果明显。百度通过应用 MLOps 使得开发周期缩短 54%，测试周期缩短 67%，所投入的人天数缩减 57%[9]。

金融行业：鉴于对风险的敏锐嗅觉，金融行业在使用 MLOps 驱动业务增长的同时，对模型风险的关注与日俱增。如工行、农行、浦发银行、中原银行、中信证券等，细分上千个应用场景，重点聚焦于模型生产、模型管理、模型安全、模型风险等方面，借助 MLOps 实现模型全流程管控。中原银行通过应用 MLOps 将模型上线周期从周缩短至天，将模型部署时间从小时级缩短至秒级[9]。

电信行业：由于用户数量巨大，模型上线后的运营监控成为电信行业关注的重点之一。如联通、移动等，对模型运营监控的关注度较高，以保证模型的稳定性。某电信运营商应用 MLOps 建立模型运营监控体系，实现模型持续训练，节省人力 300 人天/年，成本降低 80%[9]。

（二）MLOps 落地挑战

近年来，我国 MLOps 逐步在多行业中得到布局应用。将 MLOps 引入模型开发阶段的实践较为成熟，而 MLOps 引入到模型交付和模型运营阶段的落地处于逐步规划建设中。在这个渐进式过程中，MLOps 落地面临着诸多挑战。

一是组织落地驱动力不足。对于大多数组织而言，MLOps 落地驱动力不足。首先体现在 MLOps 建设成本较高，但短期内价值无法立即显现，导致必要性分析难度增大；其次是 MLOps 技术栈不清晰，且部分组织对已有 AI 能力和规模不确定，无法明确 MLOps 建设的目标成熟度，导致制定技术方案的难度加大；最后是业内缺乏成熟的

[9] 数据来源：中国信息通信研究院行业调研访谈.

MLOps 实践指南作为指导，缺乏标杆组织和案例作为参考，导致诸多组织落地 MLOps 时“摸着石头过河”，进程缓慢。

二是支撑工具选型难、集成难。虽然 MLOps 工具市场目前处于蓬勃发展阶段，为应用方提供了许多选择，但随之带来的问题也比较明显。一方面，由于工具种类繁多，功能复杂，解决某一环节问题的工具往往有许多个，缺乏统一的能力标准；另一方面，尽管 MLOps 开源工具占多数，但如何将多个工具有效集成和打通，整合全生命周期各项关键能力，很大程度依赖于组织和人员的技术能力。这两个原因导致组织落地 MLOps 时，面临解决方案难决策、平台难选取、工具链难集成等难题，导致难以实现 MLOps 的快速落地。

三是模型治理和可信道阻且长。机器学习模型的治理错综复杂，体现在两个方面：一方面，同一模型在不同业务场景面临的风险程度和所需更新频次不同，不同类别模型所需的生产过程和风险等级亦不同；另一方面，模型面临的事前、事中和事后风险包括生产过程不可追溯、线上模型效果下降、模型存在偏见、推理结果不可解释、无法审计等，导致 AI 可信落地难。

四是环境间的交互难以平衡。企业内部的 MLOps 实践过程需要有效管理开发环境、测试环境、准生产环境、生产环境等之间的关系，外部需要有效打通与 DevOps、DataOps、FeatureOps 的连接，同时又要保证流程的简洁和安全。环境间的交互障碍，导致 MLOps 的自动化进程受限。

三、MLOps 框架体系

机器学习项目生命周期伴随着 AI 的发展早已形成，而 MLOps 的出现驱动产业界对机器学习项目生命周期进行了完整梳理。本章由信通院和行业专家结合机器学习和 MLOps 相关理论研究和产业实践，围绕机器学习项目的全生命周期，对业界现有的 MLOps 框架体系做出总结归纳。

（一）机器学习项目生命周期

机器学习项目以需求、数据、代码、算法为输入，以模型、模型服务为输出，其生命周期主要包括定义问题、数据收集、数据处理、模型训练、模型评估、模型部署等过程。

来源：中国信息通信研究院

图 6 机器学习项目生命周期示意图

MLOps 围绕持续集成、持续部署、持续监控和持续训练，构建和维护机器学习流水线，并通过流水线的衔接形成全生命周期闭环体系。基于 MLOps 框架的机器学习项目生命周期通常包括需求设计、开发、交付和运营四个阶段，细分为需求管理、数据工程、模型开发、模型交付、模型运营等过程。

需求管理：根据商业目标与业务需求，开展可行性分析，编制技术需求和技术方案。

数据工程：将源数据处理成可用数据，并存储至合适位置便于流转。

模型开发：在实验环境中，对模型进行训练、参数调优、评估与选择等过程，得到最优模型。

模型交付：将模型与配置、代码和脚本等进行封装，生成可交付物，并部署至目标环境。

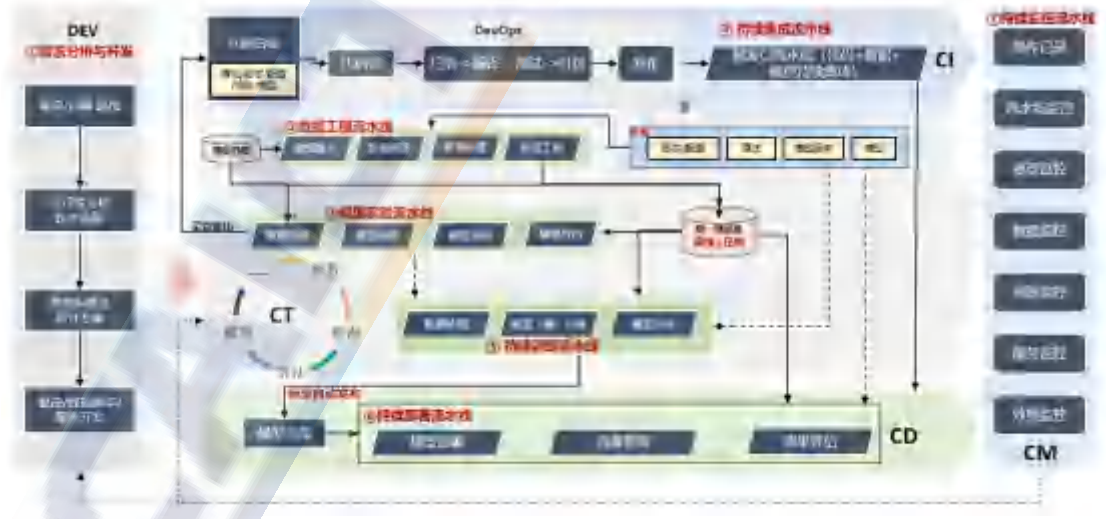
模型运营：在生产环境中为上线的模型服务提供监控和运营维护能力。

来源：中国信息通信研究院

图 7 基于 MLOps 框架的机器学习项目生命周期示意图

（二）MLOps 流程架构

典型的 MLOps 流程架构包含需求分析与开发、数据工程流水线、模型实验工程流水线、持续集成流水线、模型训练流水线、模型服务流水线、持续监控流水线七个部分。



来源：中国信息通信研究院

图 8 MLOps 流程架构示意图

1.需求分析与开发

需求分析与开发是指对业务方的需求进行分析和设计，对规则、代码、脚本等进行开发。目的是解决机器学习项目中需求管理流程混乱、不同角色对于需求的理解不一致及风险不可控等问题，从源头提升项目质量，降低需求变更带来的影响。

主要输入：业务需求。

主要步骤：

1)将业务需求转为技术问题，确定使用机器学习模型解决潜在业务问题的可行性及必要性，评估模型潜在的风险。

2)设计机器学习项目架构，确定要使用的技术。

3)梳理项目过程需要的数据，以及数据处理过程和规则（例如，数据采集和标注规则，数据转换、清洗、特征选择和特征生成规则等），这些规则会根据后续的反馈持续迭代更新。

4)开发对应的算法、训练代码、数据脚本、模型服务代码等。

5)基于算法和脚本，触发数据工程和模型实验流程，得到最佳特征数据与模型参数等。

主要输出：项目计划，设计文档，用于数据工程、特征工程、模型训练及模型服务的代码与配置。

2.数据工程流水线

数据工程流水线是指以流水线方式，对数据进行接入、处理、存储、分析等工程化处理。目的是解决数据来源繁杂、数据及特征难以共享、数据管理不统一等问题，为模型开发及模型服务提供干净可用的数据原料。

主要输入：原始数据、数据处理和特征工程的代码与配置。

主要步骤：

1) 接入并提取原始数据，包括流数据、静态批处理数据或云存储数据。

2) 对原始数据进行初步分析探索，挖掘并分析数据内部结构、分布等规律，检查数据质量。

3) 数据处理从数据清洗与转换开始，以预定义的转换规则作为输入，处理数据异常、缺失、冗余等问题，生成可用格式的数据作为输出。

4) 最大限度地从原始数据或处理后的数据中提取、变换为新的或更高级的特征，预定义的特征工程规则作为输入，将生成的特征作为输出，并存储至特征库。

主要输出：处理后的数据、特征。

3.模型实验流水线

模型实验流水线是指以流水线方式，采用数据、算法和参数进行训练的实验过程。目的是解决过程难以回溯、实验难以复现、错误难以追查、参数难以配置和选择等问题，提高模型生产质量，并为持续训练提供基础。

主要输入：原始数据、特征、模型实验所需代码与配置。

主要步骤：

1) 利用特征库的能力，结合原始数据，开展数据分析，得到模型实验所需数据集。

2) 触发多轮模型训练，不断调整和选择性能最优算法和超参数。

3) 对不同模型参数进行交叉测试和验证，一旦性能指标达到预期，迭代训练将会停止。模型训练和模型评估任务可根据条件重复触发。

4) 导出模型并提交至仓库，包括训练算法、数据脚本、服务代码、模型等。

主要输出：最佳算法、数据脚本、模型服务代码与配置、模型文件、实验指标。

4.持续集成流水线

持续集成流水线是指以流水线方式，对模型和代码进行持续构建与集成的过程。目的是解决模型及代码构建、集成测试、安全扫描等过程繁琐、易出错、集成效率低下等问题，并以流水线的自动化提高交付质量。

主要输入：最佳算法、数据脚本、模型服务代码与配置、模型文件。

主要步骤：

1) 将代码、模型、配置等要素进行构建打包和集成测试，生产出可交付的部署包（例如镜像文件、JAR 包等）。

2) 将构建、测试、扫描等过程进行集成，以生成持续集成流水线。

3) 对集成过程出现的问题进行反馈和处理，提高集成成功率。

主要输出：部署包。

5.持续部署流水线

持续部署流水线是指以流水线方式，将模型服务部署至目标环境并开展相应评估的过程。目的是解决部署周期长、部署配置易出错、部署进程启动晚、流量接入配置复杂、模型运行状态不稳定等问题，做好模型为业务系统提供推理服务的充分准备。

主要输入：部署包、特征、服务工作流配置（例如更新策略或 AB 实验策略等）。

主要步骤：

1) 将模型服务部署至目标环境，并通过更新策略将新版本模型服务进行持续部署。

2) 对已部署模型服务配置相应流量管理策略，使其按照策略有序接入流量并开展验证和评估工作。

3) 根据已分配流量在模型上的运行结果，评估模型效果优劣，驱动模型优化。

主要输出：模型服务、评估报告。

6.持续训练流水线

持续训练流水线是指以流水线方式，依据相关条件的触发持续对模型进行训练的过程。目的是解决数据漂移、模型服务不符合预期等业务问题，以及重新训练复杂耗时等效率问题，提高模型自生产能力。

主要输入：流水线配置（包括节点、触发条件、参数等）、旧数据、新数据、特征。

主要步骤：

1) 从特征库自动提取版本化特征。

2) 自动化开展数据准备和验证，并拆分数据集。

3) 根据模型实验阶段已选择的算法和超参数，对新数据进行自动训练。

4) 执行自动化的模型评估、超参数迭代。

5) 训练后的模型被导出并保存至模型仓库。

6) 根据需要触发模型测试及持续部署流水线。

主要输出：新模型。

7.持续监控流水线

持续监控流水线是指以流水线方式，贯穿 MLOps 端到端生命周期，持续对过程和结果开展监控，同时在特定场景特定条件下触发模型重新训练的过程。目的是解决模型效果下降的问题，通过监控发现问题并持续改进，提高过程流转效率，确保模型服务质量。

主要输入：各类指标数据。

主要步骤：

1) 收集各类指标值，并进行记录和保存。

2) 根据既定规则开展数据分析。

3) 根据分析结果生成报告，必要时为触发器提供数据。

主要输出：分析结果、触发值。

（三）MLOps 相关角色

尽管机器学习模型的构建主要由数据科学家完成，但要最终为业务系统提供推理服务却需要多角色合作。组织应围绕 MLOps 流程的持续运转，明确角色与分工，可提高多角色间的协作效率，从而提升整体生产效率和质量。下图展示了 MLOps 相关角色分工示意图，但由于 MLOps 领域的飞速发展，将来可能出现的新角色暂未列出。同时，在许多组织中，各角色可能是专职或兼任，具体如何安排应视组织结构和业务场景等情况而定。

来源：中国信息通信研究院

图 9 MLOps 相关角色分工示意图

典型 MLOps 相关角色分工包含业务人员、项目经理、机器学习架构师、数据工程师、数据科学家、软件工程师、测试工程师和运

维工程师等。表 1 展示了在实际的机器学习项目全生命周期中，业务人员、数据科学家等各类角色所关注的不同重点及具体的工作职责。

表 1 MLOps 相关角色职责要求

角色	关注点	工作职责
业务人员	业务需求	1.识别和收集产品的新需求、缺陷和改进方向； 2.提出明确的需求目标，在交付阶段进行需求验收。
项目经理	项目全生命周期过程	1.带领团队进行业务需求的可行性分析； 2.制定项目计划，统筹把控和管理项目全流程的进度、成本、质量、风险、资源等； 3.推动项目持续优化改进，复盘问题并协调制定改进措施。
机器学习架构师	组织级机器学习体系架构	1.统筹设计硬件、底层技术、开发平台到上层应用的架构； 2.规划设计 MLOps 流程架构，保障机器学习项目生产过程的一致性，从而确保生产质量的可控； 3.管理和维护各条机器学习流水线，确保流水线的可扩展和灵活性。
数据工程师	数据	开展数据探索性分析，并对数据进行清洗、筛选、加工等处理，同时构建特征工程（可与数据科学家共同构建），完成数据准备工作。
数据科学家(建模专家)	机器学习模型	1.将业务需求转化为技术需求； 2.跟进数据准备过程，确保数据的高质量； 3.模型开发过程中，选择性能最佳的算法和超参数，开展模型构建、模型训练、模型评估和模型选择，输出精准、高效的模型； 4.模型交付、运营监控过程中，配合问题定位和决策。有的组织在模型构建阶段，亦开展模型优化和压缩等工作。
软件工程师	模型工程化	1.将数据科学家提供的模型转化为模型服务，开发服务代码，便于模型服务与业务系统无缝协作； 2.对模型进行优化或压缩、集成和部署模型服务。

角色	关注点	工作职责
测试工程师	模型测试	开展模型效果验证、模型服务的功能与非功能测试。
运维工程师	模型交付与运营维护	开展模型服务的上线部署和运营监控工作，保障模型生产运行的可靠性和高可用。

来源：中国信息通信研究院

值得关注的是，近年来行业开始出现 MLOps 工程师角色，职责主要包括 MLOps 平台部署与维护、流水线构建与管理、模型优化、度量改进等。MLOps 工程师在 Linkedln 新兴职业排行榜中高居榜首，五年内增长了 9.8 倍[10]。国内绝大部分组织中的 MLOps 工程师职责由数据科学家、软件工程师或运维工程师兼任，相信随着 MLOps 的普及与发展，MLOps 工程师将成为专职岗位。

实践案例：中原银行的模型风险分析师

中原银行在风险合规要求较高的场景中，设置模型风险分析师的角色，对数据科学家开发的模型进行验证评估，确保模型设计方案、开发过程满足既定的业务诉求，并满足监管、合规等相关政策要求。

1. 模型需求设计，结合统计方法与专家经验，验证模型原理和方法的合理性、模型的可用场景和局限性，清晰理解模型的特征、影响及参数估计情况，确保满足业务需求。

2. 建模过程验证，检查建模过程的合理性，包括需求管理、数据工程、模型开发等过程的准确性、合规性、可控性。

3. 模型效果验证，将模型输出结果与真实结果进行比较，检验概率、模型参数的区分能力、准确性、稳定性等，确保模型稳定可靠。

[10] 《如何成为 MLOps 工程师》，MLOps 工程实践.

四、MLOps 关键能力与技术实践

当前，MLOps 概念逐渐明晰，应用落地持续开展。组织在落地时，以总体流程架构为主线，以计划解决的问题为目标，对关键能力各个击破，逐步形成 MLOps 落地效应。

为顺利构建和实施 MLOps 流水线，组织需提前做好关键能力的建设予以支撑。本章围绕 MLOps 过程管理、制品管理和基础保障三个维度，以业界共识为基础，提出了 12 个关键能力，并对工程实践过程中应考虑的核心要点展开分析，同时提供优秀实践案例以供参考，梳理了部分 MLOps 工具链清单（见附表）。

来源：中国信息通信研究院

图 10 MLOps 关键能力示意图

（一）数据处理

数据处理是将源数据加工处理成模型开发所需数据，为模型开发及最终决策提供高质量数据。数据处理是 MLOps 生命周期的上游环节，是模型训练的基础，高质量的数据有助于生成更优质的模型。

核心要点：

● 对接入的源数据进行数据清洗、数据转换、数据增强等处理，以减少数据异常、缺失、冗余等问题，提高数据质量。源数据通常包

括结构化数据和非结构化数据（例如文本、图像、音频等），结构化数据的处理包括去重、处理无效值和缺失值等。文本数据的处理包括降低字频、添加生僻字等；图像数据的处理包括旋转、翻转、裁切等；视频数据的处理包括抽帧等；音频数据的处理包括降噪等。

● 当使用了文本、图像等非结构化数据时，需对处理好的数据进行标注。例如，文本类标注包括文字检测框、文字内容识别等；图像类标注包括目标检测框、语义分割块、关键点等；点云类标注包括目标检测框、语义分割块等；视频类标注包括目标识别框、语义分割块、关键点等；音频类标注包括语音、语调、音素等。

● 支持大批量数据的接入和处理，具备一定自动化数据处理能力。

实践案例 1：广东移动的数据处理

广东移动的数智化运维平台在数据工程过程中，为了应对复杂、海量、多样化的运维数据的搜集、处理、标注带来的挑战，进行了如下改造：

1. 多类型数据处理能力：针对异构多数据源、多格式类型的数据，应用分类方法识别数据类型，对多种类型数据通过聚合运算、零值处理、缺失值填充等方式进行处理，并根据场景需要实时加载数据。

2. 海量数据传输保护：在整个数据处理过程中，为确保海量数据传输的完整性和效率，在数据工程全流程，包括数据采集、数据传输、数据处理、数据接收、数据存储等过程均设置了保护机制。一是应用多区、多宿主机上多 HUB(集线器)仓库处理中心，保证传输正常。二是设立流量限制和过载保护机制，如避免流量突增、设立表空间监控阈值等，保证处理集群的稳定性。

来源：广东移动

图 11 广东移动的数据处理能力示意图

实践案例 2：格物钛的数据处理

格物钛通过数据平台为数据工程团队提供以数据为中心的高效、便捷、安全的管理能力，并提供数据核心管理模块:

1. 将数据工程中原本分散的原始数据、语义数据、元数据统一进行管理、高效读写、处理与检索。

2. 提供便捷的版本管理能力，保证数据与模型的迭代可追溯、可复现。

3. 提供在线可交互的可视化能力，使得所见即所得。

4. 提供细颗粒度的权限管控与访问记录能力，保证数据的使用安全与数据血缘追踪能力。

5. 自定义的自动化工作流，让数据工程人员可以快速搭建不同的数据处理管道，如数据清洗、数据降采样、数据预标注、模型训练等，加速数据的流动与处理效率。

6. 提供丰富的开发者工具让数据与代码、系统轻松完成集成。

来源：格物钛

图 12 格物钛的数据处理能力示意图

实践案例 3：云测数据的数据处理

云测数据标注平台结合数据在环和模型迭代在环新方式，将数据采集、处理、标注、训练、模型输出等进行持续迭代集成，支持图像、点云、视频、文本、语音等数据的加工处理，帮助企业快速获得高质量训练数据。

1. 通过数据标注平台，一是引入模型输出预识别结果，进一步降低人力成本；二是在迭代后期，人员只处理关键高价值数据并对 AI 辅助标注结果进行审核验证，大幅降低算法研发人员投入成本，减少模型训练时间。

2. 通过数据管理系统，在数据安全、大容量数据处理、数据挖掘、数据增强等方面，大幅提升数据使用效率，通过数据分级检索和数据资产管理能力，提升团队协作效率，持续挖掘数据价值。

3. 基于标准化 API 接口，实现与企业数据底座无缝对接，加速企业 MLOps 数据处理速度，实现业务数据处理和训练一体化。

来源：云测数据

图 13 云测数据的数据处理能力架构图

（二）模型训练

模型训练是基于数据集和算法进行训练，包括算法选择、超参数优化、模型评估和选择等主要环节，最终输出已训练模型。模型训练的建模方式主要包括 Notebook 自定义开发编码方式、低代码拖拽建模方式、AutoML 自动机器学习建模方式等。模型训练是 MLOps 的

核心步骤，训练过程的效率提升和训练结果的质量提升，对 MLOps 整体质效的保障起着至关重要的作用。

核心要点：

● 快速找到模型的最佳算法及对应超参数。超参数选择的方法通常包括手动搜索和自动搜索（例如，网格搜索、随机搜索、贝叶斯优化、遗传算法等）。

● 通过评估指标，对模型进行批量评估，并可视化和比较模型性能，选定最优模型。

● 合理地最大化地使用训练资源。从工程化角度，组织希望同一时间并行执行多组模型训练，从成本角度，组织又希望有限的算力资源可以被高效利用，因此有效平衡资源的利用非常重要。

● 支持多种 AI 框架开展模型训练。

● 支持模型的可解释（例如采用特征重要性等方式）。

实践案例 1：华为终端云的模型训练

1.大模型的高效训练：华为终端云 MLOps 平台通过自研 PS 训练框架，结合华为自研算力硬件，提供近线增量训练能力，打通离线全量训练-近线增量训练-在线推理全流程，支撑推荐 500G+大模型的高效训练与上线。

2.资源的合理调度：训练任务资源调度存在明显波峰波谷和多种资源(V100、A100、NVLink 等)诉求等现象，同时为满足训练 SLA 和优先级诉求，华为终端云从以下三方面增强调度能力:

1) 支持调度优先级与资源可预期排队能力，构建基线+超分的资源配额分配，满足高优先级任务 SLA。

2) 支持可视化任务调度日历图，辅助算法科学家合理设置任务调度时间，削峰填谷，提高整体资源占用率。

3) 支持跨资源池混合调用与资源弹性伸缩，满足算法工程师对资源的突发诉求。

实践案例 2：百度的模型训练

百度智能云企业 AI 开发平台提供 Notebook 建模、可视化建模、作业建模、自动化建模、产线建模等多种建模方式，支持主流机器学习和深度学习开发框架，并能通过 Docker 镜像的形式来支持其他框架和第三方软件库。平台内置 ERNIE 等全面领先的 NLP 模型，以及各领域各方向的高精度预训练模型，并支持对大模型进行训练加速。该平台帮助不同建模水平的人员提升建模效率，助力企业构建统一的 AI 基础设施。

来源：百度

图 14 百度的模型训练架构图

（三）构建集成

构建集成是将代码、模型、配置等要素进行构建打包和集成测试，生产出可交付物（交付物的形态例如有部署包、镜像等）的过程，涵盖模型构建（模型训练过程）和模型服务构建。构建集成是将模型转换为服务的关键环节，真正意义上实现从数据到服务的跨越。通过持

续集成的标准化、自动化流程，大幅缩短交付周期，减少人工实施和返工成本。

核心要点：

● 对构建过程进行规划、设计和执行，包括构建的类型、触发方式、执行周期等内容。

● 将构建与测试等环节进行衔接，形成持续集成流水线，通常包括模型构建、代码打包、集成测试、静态扫描等，某些情况下还包括模型转换与模型优化。

● 当数据、代码、模型、配置等发生变更时，可快速触发持续集成流水线。

● 对集成过程中出现的问题具备自动化反馈和管理机制（例如，对解决时长进行管理），以及一定的问题修复能力，为高频率集成提供基础。

实践案例 1：马上消费的构建集成

在 MLOps 平台中，持续构建与集成需要解决不同角色（数据工程师、机器学习算法工程师、工程开发人员、模型运营人员等）的平滑协作、不同阶段（开发、构建、部署等）的自动化运行。马上消费的智马平台为了应对持续构建与集成的需求，支持以下持续化能力：

1. 新特性、新算法更新时触发自动持续构建集成，完成构建、集成、测试等完整的流程并发布新的 ML pipeline。

2. 更新数据、模型衰减时触发新的 ML pipeline 运行，完成持续训练和部署。

3. 按计划触发新的 ML pipeline 运行。

4. 按配置触发 ML pipeline 的不同阶段运行。

来源：马上消费

图 15 马上消费的构建集成流程图

实践案例 2：腾讯的构建集成

腾讯的太极机器学习平台（Tai Ji Machine Learning Platform）为腾讯广告场景打造了一站式平台，贯穿特征管理、样本生产、模型训练、模型服务等主要环节，提供全流程广告模型开发功能和协作空间 workspace 能力，围绕构建与集成将各个环节自动化，提高生产效率。主要包括以下能力：

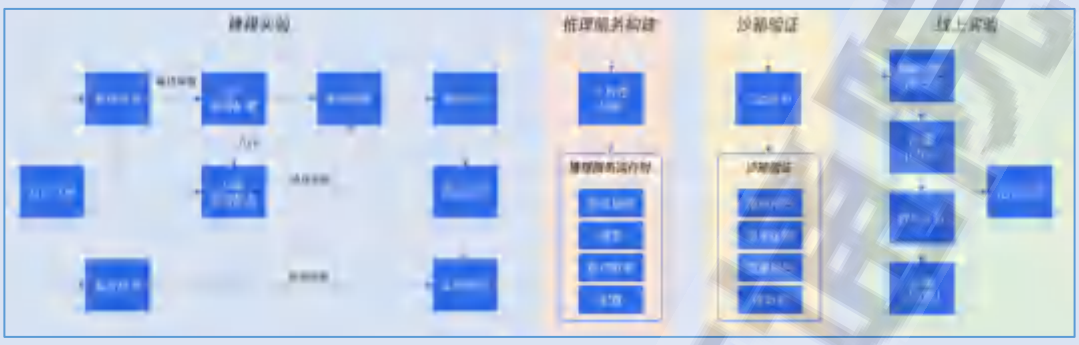
1. 持续实验：算法工程师可通过 fork 能力将线上基线模型及其参数配置等“复制”后进行持续实验，通过特征选择、模型结构优化和超参优化等实验探索效果更好的模型。

2. 持续训练：模型上线后不断有实时样本生成，通过持续训练将实时样本输入到模型中不断迭代训练，这样避免模型上线后的效果衰减。

3. 模型构建：模型经过离线评估后，通过集成腾讯智研 CI/CD 系统的 Pipeline 能力，先进行模型一致性校验，然后将模型训练拓扑结构、模型及推理运行时自动构建为算法包制品，用于模型在线部署。

4. 沙箱验证：沙箱环境是一个预发布环境，通过引流一部分线上真实流量验证算法相关指标。沙箱验证不通过将会拦截模型线上实验和部署流程，沙箱验证通过后可经主动触发和批量调度将模型发布到生成环境进行流量实验和放量。

5. 在线实验：模型上线后需要在经过 AB 实验逐步进行小流量实验、放量实验和固化实验，通过线上对算法和业务指标的评估，逐步完成线上模型的更新替换。



来源：腾讯

图 16 腾讯的 MLOps 平台示意图

（四）模型服务

模型服务是通过配置和管理所依赖的参数，形成模型服务部署至目标环境，以 API 接口等方式为业务系统所调用，输出预测结果，并根据用户需求灵活分配计算资源。模型服务通常包括实时服务和批量服务两种方式。模型服务是实现模型在线全生命周期托管，简化业务系统集成模型的过程。通常在大多数情况下，模型以独立服务的方式与业务系统解耦。

核心要点：

● 支持服务的可视化创建和编排，对服务启动过程进行监控，服务启动后支持在线缩扩容、服务停止、流量分配、服务限流、负载均衡等能力。

● 使用参数配置构建在线、离线或流式推理服务镜像。

● 集成常见 AI 框架，例如，Tensorflow、Pytorch、Marian、Mxnet、Sklearn 等。

● 通过配置和触发更新策略，实现模型服务的自动化部署。更新策略通常包括灰度更新、滚动更新、蓝绿更新等。

● 根据应用场景的需求，支持低延迟、近实时(在线)预测服务，或高吞吐量批处理(离线)预测服务。

● 集成 A/B 测试能力，支持自定义实验、流量、指标、报表等，提供效果监控，为业务系统决策提供支撑。

● 对模型服务进行版本化管理和权限控制。

实践案例 1：浦发银行的模型服务

浦发银行深度学习平台 MLP 实现对人工智能模型从训练、测试、部署、运行、迭代的全生命周期的研发管理，引入多种机器学习、深度学习先进算法和模型，实现模型开发与模型投产无缝衔接。主要模块包含:

1. 模型选择：内置多种经优调后的预训练模型，可查看模型整体评估情况（包括指标曲线和混淆矩阵等），全面对比分析各项指标。

2. 模型调试：内置多种模型优化技术用于优化模型推理性能，支持云边端各类硬件的部署要求，可配置模型在线测试和批量测试能力。

3. 服务编排：通过服务组件编排，对一系列原子能力进行组合，并支持多维度管理和调度编排服务。

4. AB 实验：支持在控制变量的情况下完成模型效果比对，依据请求分发的流量策略进行 AB 测试的指标展示。

5. 发布上线：支持在线预测服务、离线预测服务，满足服务发布过程中的在线调试、异步批量预测、模型转换、压缩和加密等处理需求；支持通过血缘关系追踪模型和数据，根据已有关系快速更新模型；灵活支持各种预测服务的数据回流方式。

6. 指标监控：自动监控模型运行状态，并在检测出现问题时发送邮件警告；依据模型监控的整体情况，触发模型自动重训；支持对模型效果偏移的实时监控，保障业务应用效果。

来源：浦发银行

图 17 浦发银行模型服务示意图

实践案例 2：建行的模型服务

中国建设银行的“天权·人工智能平台”模型服务化模块可使模型更快、更合规地应用于生产，其包括模型管理、模型封装、模型部署、模型监控等功能，模型服务化提供两种解决方案：

1. 低代码解决方案，平台为用户提供丰富的推理服务器，支持对符合推理服务器规范的模型包进行快速部署。

2. CI/CD 解决方案，平台为用户提供一系列 CI/CD 和编排工具，支持推理组件的构建和推理图的编排，具备模型组件化编排和部署能力。

1) 封装空间，提供云端的开发环境，支持多种技术栈，集成在线编辑器。

2) 封装实验，提供丰富的封装案例，支持在线运行封装案例，以便熟悉封装框架。

3) 封装流水线，提供多种类型的封装流水线模板，可用于快速构建不同类别的推理组件，具备持续集成能力。封装流水线种类包括基础镜像封装流水线、组件镜像封装流水线等。

4) 镜像仓库：对基础镜像和组件镜像进行统一管理。基础镜像包括官方基

础镜像和自定义基础镜像，组件镜像包括模型镜像、转换器镜像、路由器镜像、合并器镜像等。

5) 设计器：可用于在线编排推理组件，实现不同的推理逻辑，满足不同场景的推理需求。组件化的编排方式，提升了不同场景下组件的复用能力。

6) 推理图：提供推理图的统一管理能力，支持推理图的版本化管理。

来源：建信金科

图 18 建行模型服务架构图

实践案例 3：中移在线中心的部署发布

中国移动在线营销服务中心负责中国移动全国 10 亿客户线上营销服务的统筹运营，其内部 Polaris MLOps 平台的模型部署方案遵循流动、反馈、实验等 3 大原则。流动原则缩短了开发运维交付周期。反馈原则为建设安全可靠的工作体系提供保障。实验原则使组织的改进和创新成为日常工作的一部分。使用 Polaris MLOps 后，算法类服务发布频率由数月一次提升为每月数十次，发布周期大幅降低。

1. 代码、模型部署准备

1）已经通过评审的代码推送到 Git 仓库。始终确保代码和基础设施处于可部署状态，所有合并到主干的代码都可以安全地部署到生产环境。在源头保障代码质量。

2）模型通过评估加密后，推送至基于 DVC 二次开发的模型仓库。为保证 SLA，不推荐同时发布新版本代码、模型。

2. 执行 CI/CD 流水线

该过程以容器云平台为基础设施，动态完成镜像构建，镜像构建完成后实时销毁构建环境。整套持续集成、持续交付流程以开源工具或自主研发工具为主，以公共组件面向全在线中心提供服务。

1）CI/CD 流水线在执行前应首先完成配置并通过测试验证。

2）执行 CI 流水线，流水线将同时从模型仓库和 Git 仓库中分别拉取模型、代码，通过镜像构建工具完成代码编译、模型加载、镜像构建。

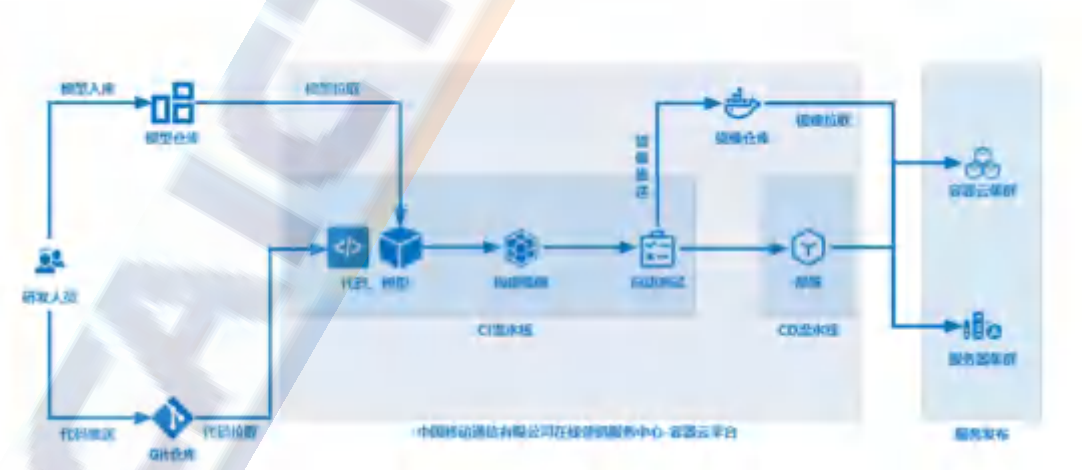
3)通过自动化测试的镜像将被推送至镜像仓库或直接触发 CD 流水线执行完成模型部署。自动触发 CD 流水线功能可选择开启或关闭，开启时会自动触发 CD 流水线执行，关闭时镜像将被直接推送至镜像仓库。

3. 服务发布

1）平台默认提供蓝绿发布、滚动发布两种发布方式。可以通过 CD 流水线完成服务发布，发布方式可根据实际情况进行选择。

2）服务发布过程出现异常时，可以通过平台轻松实现服务回滚。服务将从镜像仓库获取指定版本镜像，并从平台获取相应配置。

3）自动化测试触发 CD 流水线选项被关闭时，手动选择执行蓝绿发布或滚动发布。



来源：中移在线营销服务中心

图 19 中移在线中心 Polaris MLOps 平台模型部署流程

实践案例 4：星环科技的部署发布

星环科技的模型部署发布流程如下：

1) 将模型开发平台训练生成的模型文件，上架并注册至模型仓库。

2) 创建服务推理图，基于业务场景构建（一个或多个）模型的推理逻辑，选择模型运行时环境，并装载指定模型及其部署版本。

3) 将推理逻辑整体部署为模型服务，包括两类应用类型。一是将模型部署发布为实时应用服务，配置模型所需资源、部署策略等信息，最终生成实时响应的模型服务 API 接口；二是将模型部署为批处理作业，配置模型所需资源、数据来源、结果输出、调度方式等信息，最终生成模型批量预测任务。

来源：星环科技

图 20 星环科技 MLOps 流程图

（五）运营监控

运营监控是对模型生产过程和线上运营情况进行持续监控，便于及时发现和排查问题，保障模型的效果稳定和可靠，辅助运营决策。运营监控通常分为模型监控和运维监控。

1. 模型监控包括，一是数据监控，对数据及特征进行监控，识别数据漂移情况，保障数据的及时、准确和完整性等；二是模型性能监控，对模型的性能指标（准确率、召回率等）进行评估，保障模型结

果的可信；三是模型效果监控，根据模型服务的推理结果，监控业务指标，保障业务目标的达成。

2. 运维监控包括，一是基础设施监控，对主机或容器的健康状况、资源（CPU、GPU 等）使用率、I/O 占用率等进行监控，保障运行环境的稳定；二是服务监控，对模型服务性能（服务数量、访问量、时延、并发等）、异常调用等进行监控，保障模型服务的可靠性；三是过程监控，对各任务或流水线的运行情况（执行结果、SLA 等）进行监控，保障模型生产过程的稳定和可靠。

运营监控是在环境变化的情况下，及时发现模型问题，以决策在线更新或重新训练模型，从而提供更稳健和更优质的推理服务，并可持续改进 MLOps 过程质效。

核心要点：

● 通过监控的自动化实时能力，实现持续监控和运营的目标。

● 支持历史监控数据或事件的记录，保证监控过程的可追溯能力。

● 建立健全的预警、分析和处置机制，包括全自动化的预警能力，部分自动化或智能化的分析和处置能力。

● 与持续训练流水线高效衔接，在实时性要求较高等场景下，运营监控应为持续训练提供强有力的支持，实现模型重训和在线更新。

实践案例 1：中国联通软件研究院的运营监控

1. 模型生产监控，从数据质量监控、特征稳定度监控、模型稳定度监控、多维度监控等方面监控模型生产质量，是模型有效赋能的基础。

数据层面：进行数据质量监控和特征稳定度监控，包括及时性、空值率、波动率、特征稳定度等。

模型层面：监控模型推理结果的分布稳定度，以及模型在时间维度和省分维度。

2. 模型成效闭环运营分析，从多维度、多指标实现模型赋能成效的运营分析。

● 营销漏斗分析：剖析营销策略，客观评价模型成效，以成效引导模型赋能提升。

● 时间维度分析：时间维度监控模型是否持续保持稳定且高质量的赋能成效，成效出现下滑时借助漏斗分析，甄别模型问题。

● 省分维度分析：剖析同一模型在不同省分的表现差异，借助漏斗分析定位策略问题，沉淀标杆案例。

● 多指标监控：监控触达量、办理量、办理率、触达办理率、topN 触达办理率等核心指标，分析运营问题，为模型优化提供建议。

来源：联通软件研究院

图 21 联通软件研究院模型成效闭环运营分析示意图

实践案例 2：中原银行的运营监控

中原银行的运营监控主要包括以下五大维度：

1.基础平台：CPU、GPU、内存、网络等维度的监控和预警。

2.开发工具：机器学习平台、智能决策平台、知识图谱等平台自身的运维监控。

3.数据基础服务与治理平台：

● 通用性数据：针对统一特征加工，全链路实现模型数据的监控，该部分通过特征特征加工平台实现(规划中)。

● 定制性数据：通过数据加工平台（数栈、数据前置），监控加工过程中出现的逻辑等问题进行监控。例如，逻辑加工成功与否(数栈)、数据加工过程(天

梯)等。

4.模型维度监控:

- 统计模型：性能(GINI、KS、AUC、LIFT)、稳定性(评分分布、PSI)等。
- 规则模型：触发率等。
- 变量评估：性能(IV)、稳定性(PSI)等。

5.业务维度监控:

- 准入漏斗：申请量、通过量(通过率)、提款客户数(提款率)等。
- 运营情况：累计授信金额、余额、违约余额、不良余额等。
- 业务指标：贷中(预警率)、贷后(入催率、出催率等)。

（六）模型重训

模型重训是在机器学习项目的动态环境中，通过模型重训开展持续迭代，生成新模型替换旧模型，以维持模型性能。模型重训通常包括离线重训和在线（生产环境）重训两种。模型重训是为了减少由于数据漂移和内容漂移带来的风险，并为数据科学家提供模型持续优化的快速渠道，以降低训练成本，提升模型新鲜度。

核心要点：

● 模型重训包括两个前提，一是明确了监控指标和触发条件，二是具有配置好的模型训练流水线。

● 通过持续监控流水线的输出（例如，当监控指标低于阈值时，输出触发请求），或人工方式，触发模型重训任务的执行。

● 对于安全性要求较高的某些场景，或者当对模型需要进行较大变更时，可以选择离线重训。对于实时性要求较高的某些场景，可以选择在线重训。

● 部署发布时，应考虑模型训练流水线的更新。例如，有的组织在部署发布模型服务时，将模型训练所需配置一并发布，以供持续训练流水线获取最新配置，便于重新训练的开展。

实践案例：蚂蚁的模型重训

蚂蚁在构建持续训练能力时，首先解决三个问题何时应重新训练模型、应使用哪些数据重训、应该重新训练什么。

来源：蚂蚁

图 22 蚂蚁的持续训练能力示意图

通过构建持续训练链路和自动化训练能力，当告警中心监测到模型性能出现衰退或数据漂移等情况后，通知博弈中心，并依据在博弈中心配置的迭代模板进行模型自迭代流程。一般迭代模板主要分为以下四大类:

1.模型重训，包括 AutoRefit 和 AutoRetrain。

1）AutoRefit 即模型自动迭代能力，是由监控中心持续对线上模型性能进行监控，当相关指标低于阈值时，触发训练中心的训练任务进行持续训练。训练中心收到监控中心发出的迭代请求后，从案件中心中获取最新样本集，依据 AuotML 的自动模型选择和自动参数寻优能力自动训练出最新模型。最新模型推送到测评中心，由测评中心对模型进行性能、鲁棒性、公平性、机密性等全方位的测评，达到准出条件后，产出测评报告，并推送到发布中心。在发布中心通过一键部署、AB 测试和自动发布能力将模型发布到线上，由此完成一次完整的模型迭代过程。

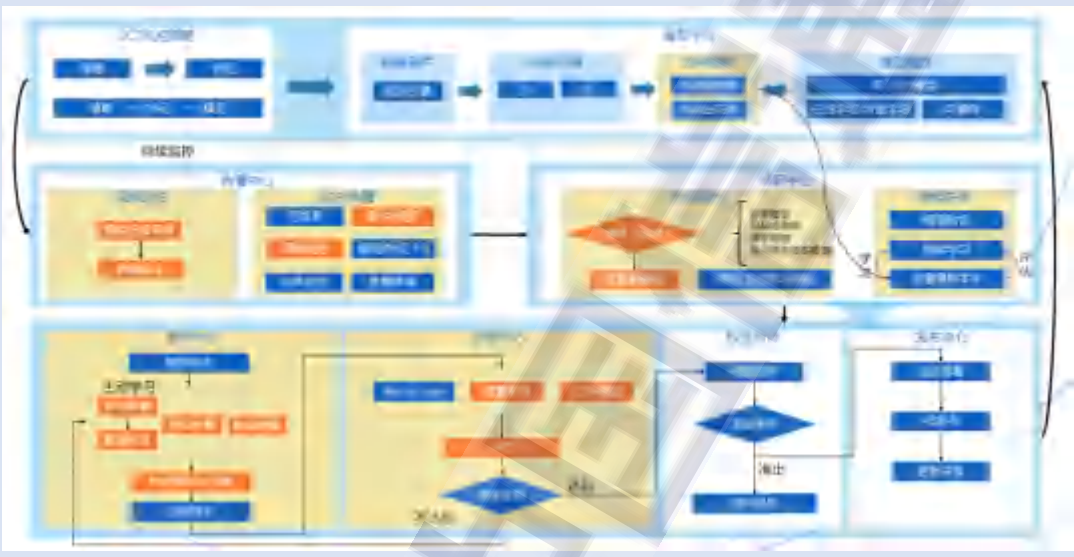
2）AutoRetrain 即模型自动生产能力，在 AutoRefit 效果甚微时自动触发。相较 AutoRefit，增加了自动特征工程能力,包括 AutoML 中的自动特征工程、自动模型选择和参数寻优（深度学习中是神经网络结构搜索 NAS）等全部

能力，也实现了端到端的机器学习自动化全过程，打通了从研发到生产的全链路。

2.增量学习，主要解决知识遗忘的问题。

3.持续标注与主动学习，主要解决在没有标注的场景下模型监控与迭代问题。

4.SOTA+HPO，主要解决将最新模型快速在业务场景落地的问题。



来源：蚂蚁

图 23 蚂蚁的持续训练流程图

（七）实验管理

实验管理是对实验过程和信息进行有序、有效的管理，管理内容包括环境、特征、参数、指标、模型信息等，并支持实验配置记录与版本控制、可视化管理、实验结果对比等能力，保证实验的可重复性，并提供可视化管理界面，支持实验结果对比，提升模型探索效率。实验管理是为了跟踪实验过程和变化，快速实现结果比对和过程重现，提升模型探索效率，提高可追溯能力。

核心要点：

● 收集并记录实验所需信息，包括实验结果、各环节执行结果、执行配置（数据、代码、参数等）。

● 基于可追溯和可复现的要求，可跟踪并查看实验信息。

● 开展实验版本管理，并对实验过程及结果进行对比。

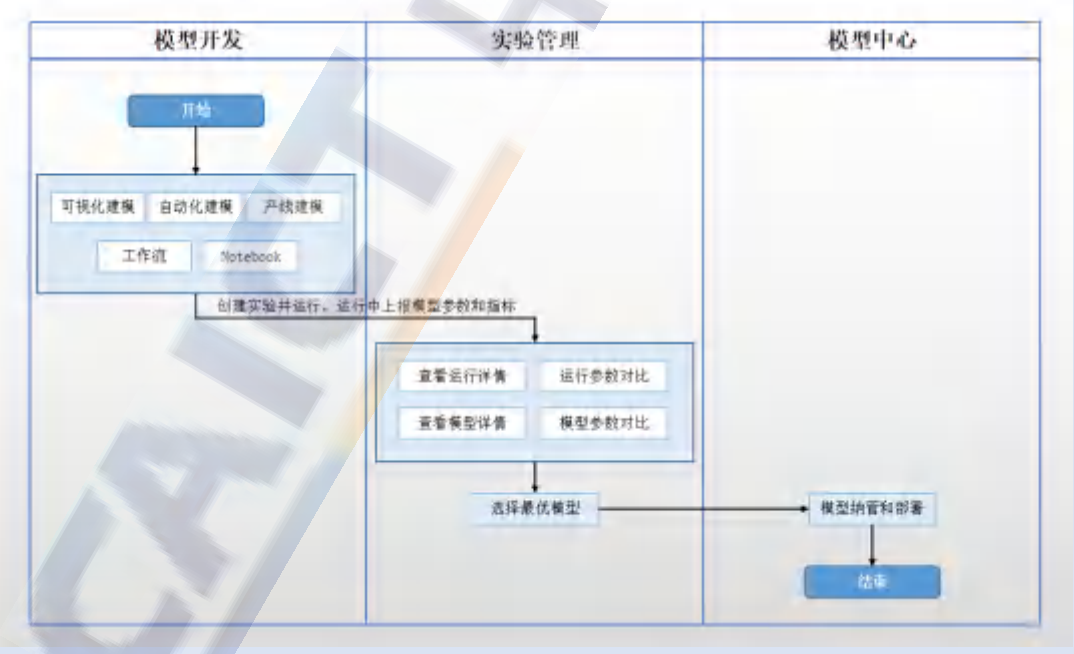
● 选择合适的实验跟踪方法，例如采用实验管理工具，或搭建定制的实验管理平台等方式，开展自动化跟踪。

● 实验异常的原因定位，支持部分自动化或智能化定位和分析能力。

实践案例 1：百度的实验管理

百度智能云企业 AI 开发平台提供实验管理能力，支持用户查看实验和训练任务的详细信息，跟踪每个训练任务的运行状态、指标和日志，提升模型开发质量。

通过实验管理，一是用户可对比同建模或跨建模方式下的实验效果；二是以实验对比找到关键影响因素，方便复现和调优；三是实现全平台建模方式的全过程记录。



来源：百度

图 24 百度的实验管理流程图

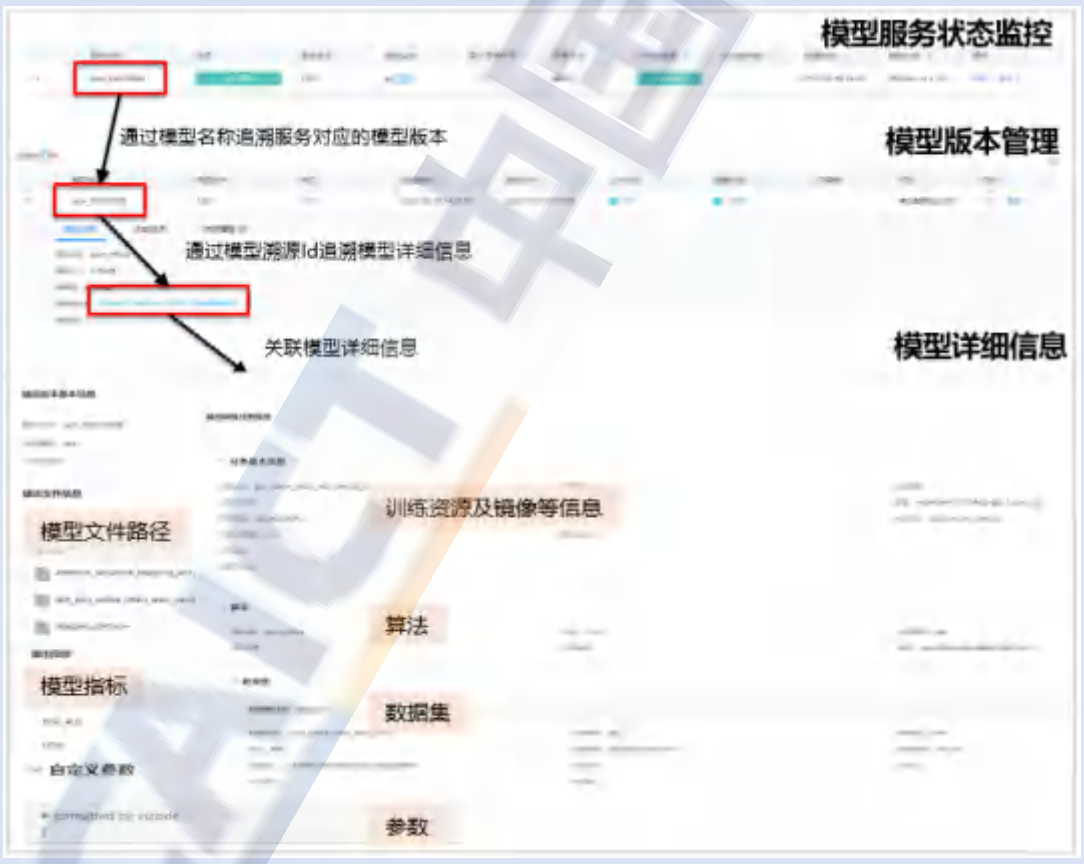
实践案例 2：华为终端云的实验管理

华为终端云 MLOps 平台在实验管理方面的基本能力如下：

1. 支持以模型/任务为起点，结合实验配置版本管理（特征配置、算法配置、任务/参数配置）与实验过程记录留存能力，可视化追溯模型实验全过程，支持模型可复现。

2. 支持配置模型评估指标在多组实验间的快速对比能力，帮助开发者快速筛选出最佳实验。

3. 支持 AutoML、Jupyter 等工具，辅助开发者快速完成数据探索与超参优化过程。



来源：华为终端云

图 25 华为终端云的实验管理界面

（八）流水线管理

流水线管理是通过提供机器学习任务的编排能力和容错能力，允许设置任务的依赖关系和调度配置，并对失败的任务生成报告和告警，从而为自动化高效执行任务提供基础。流水线管理使数据科学家等团队成员从繁琐的手动机器学习工作流程中解放出来，以便拥有更多时间研究和优化模型。

核心要点：

● 以模型为中心构建流水线，并通过数据处理、特征工程和模型训练等任务的周期性依赖关系进行关联。

● 支持灵活的任务执行策略（例如，使用周期性、定时、消息等方式触发流水线），同时根据上下游依赖就绪情况持续运转流水线。

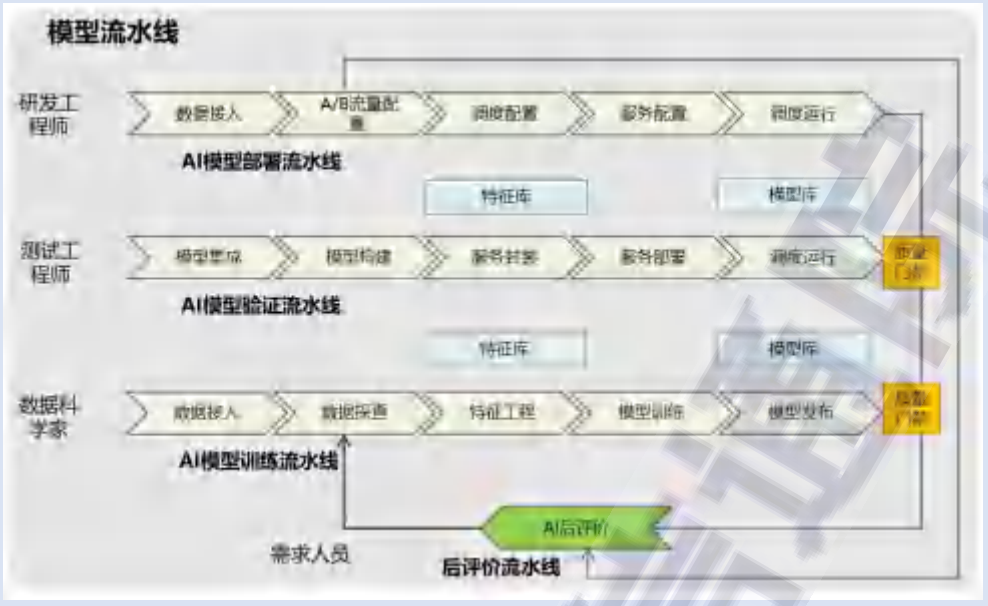
● 支持可视化编排能力、串行及并行逻辑控制能力，和版本控制能力。

● 将任务节点与推理组件沉淀为原子能力，支持流水线复用。

实践案例 1：中国农业银行的流水线管理

中国农业银行构建标准的 AI 模型训练、验证、部署、后评价等流水线，规范各阶段工作，促进数据科学家、测试工程师、研发工程师等不同角色的人员协同，提质增效。

流水线具备可视化编排、版本管理、便捷复用、易于追溯等特点，流水线之间能够顺畅、自动衔接。面向用户提供流水线服务，可满足自动化运行、实验可复现、可重复使用、并发执行、环境解耦等要求。模型流水线依赖数据流水线提供规范数据，也具备并拓展了 DevOps 流水线的相关能力适配 AI 模型的构建、集成、测试和部署等。后评价流水线主要用于判断、反馈并驱动 AI 模型的持续训练。

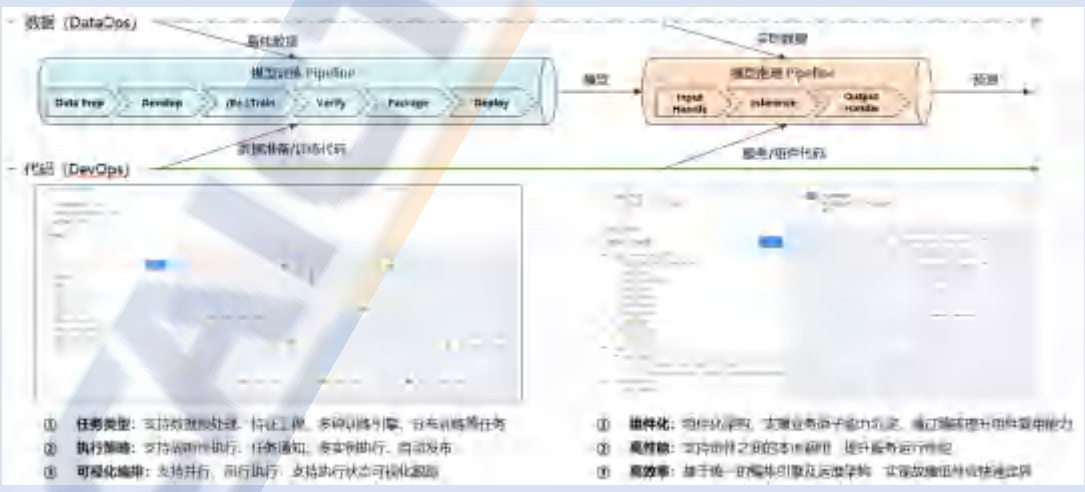


来源：农行

图 26 农行的流水线管理示意图

实践案例 2：华为终端云的流水线管理

华为终端云 MLOps 平台，支持以模型为中心的任务 Pipeline，同时结合 DataOps 数据管理与 DevOps 代码包开发部署能力，实现数据流转、代码部署、训练、推理的全流程编排和自动化实施，具备灵活的执行策略、可视化编排、组件复用等关键能力。



来源：华为终端云

图 27 华为终端云的流水线编排可视化能力示意图

（九）特征管理

特征管理是通过建立一个集中式存储区（如特征平台），对特征全生命周期进行标准化处理和管理（如生产、存储与消费等），提升特征工程效率。特征存储区别于传统数据管理方式，它需要同时考虑离线特征和在线特征的存储，一是为实验提供非实时的特征数据，二是为在线推理服务提供高吞吐、低延迟的服务。特征管理是为了将特征在组织内部统一管理和共享，并通过离线在线特征的统一，提高模型训练和推理服务效果的一致性。

核心要点：

● 对特征的基本元数据、数据来源、计算逻辑、特征版本等进行统一管理。

● 对特征进行分组及多版本的集中存储，保证特征获取时的性能与稳定。

● 通过特征重要性分析、相关性分析等过程，选择特征。

● 根据场景需求，保证离线特征和在线特征处理逻辑及结果的一致性。（例如原始特征在线获取和特征在线转换等）。

● 对特征生产、特征存储、样本生成等代码开展算子化、配置化开发。

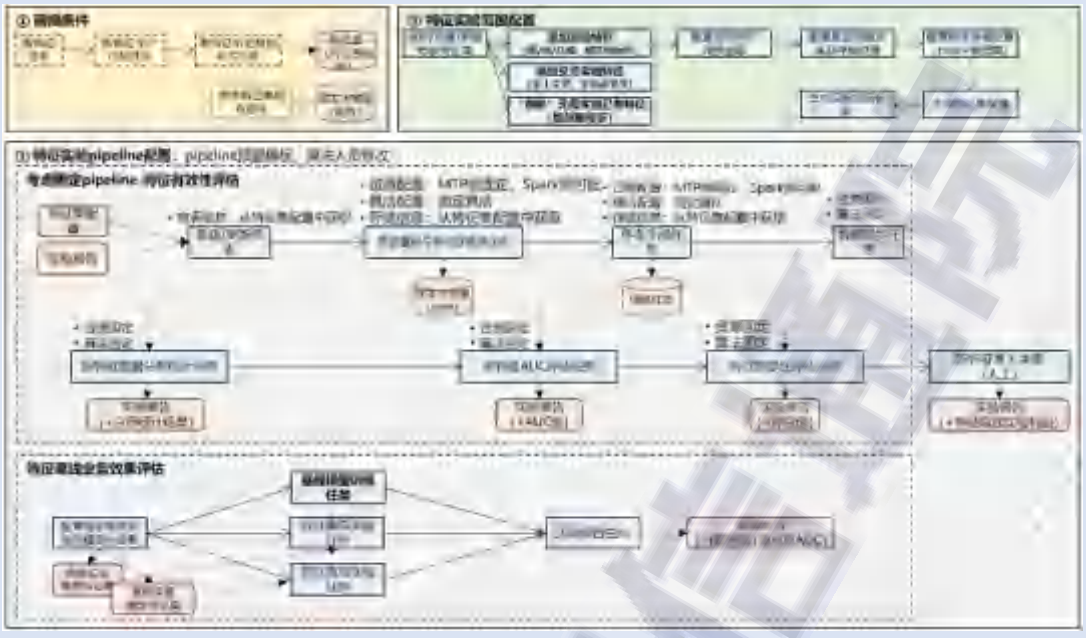
实践案例 1：华为终端云的特征管理

华为终端云在落地特征工程时，面临高效特征实验与特征服务性能方面的挑战时，采取以下措施：

实现高效特征实验能力。一是，持快速的实验配置与实验管道定义能力；二是，支持实验管道+实验配置的编译执行，支持自动执行与人工确认节点；三是，实验管道支持可视化节点编排与模板能力。

保障特征在线服务性能。通过特征在线服务，支持 API 方式的特征实时获取与转换能力。在面对推荐场景下的高频特征获取和实时特征生产场景，通过

高性能的存储中间件来解决特征获取性能问题。



来源：华为终端云

图 28 华为终端云的特征实验流程图

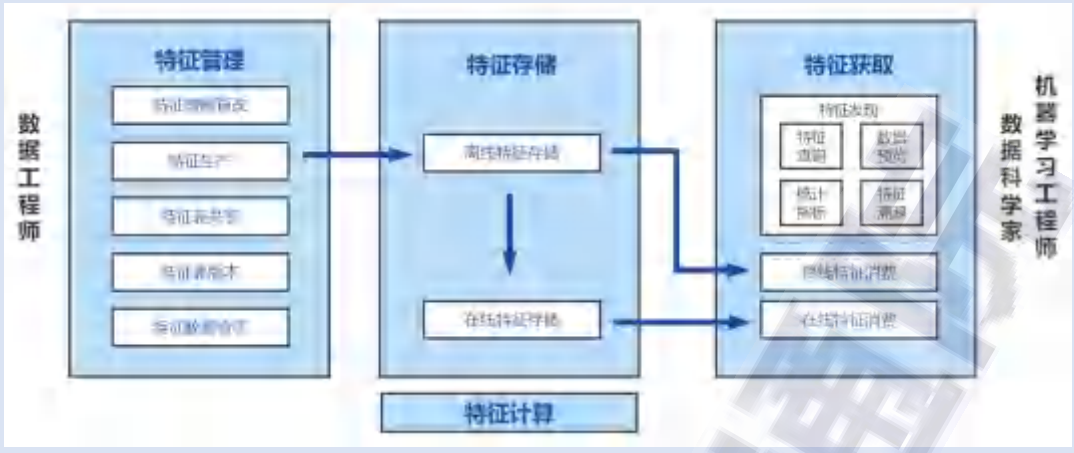
实践案例 2：浦发银行的特征工程

浦发银行深度学习平台 MLP 提供特征工程能力，用于保证特征数据一致性和实现特征数据质量的全链路自动化监控。

1. 特征工程的自动化能力：自动进行特征构建、提取、选择等任务，支持特征血缘和下游影响分析能力，可配置特征计算逻辑，对特征数据进行比对设置和版本化管理。

2. 构建离在线一体特征库：解耦特征生产和特征消费环节，降低数据端到端的依赖；支持不同团队间的特征共享和复用，以及特征溯源和追踪；同时支持离线特征高吞吐使用场景和在线特征低延迟使用场景。

3. 特征数据自动化监控：通过 KS、AUC、PSI、排序性等指标开展特征实时监控；依据每个变量在训练时的分箱与上线后的分箱差异，判断特征分布是否发生了偏移，并实现自动预警；特征故障恢复：通过报警机制、自动定位和提醒处理机制提高特征故障恢复能力；支持定期监控报告（周、月、季度）反馈机制。



来源：浦发银行

图 29 浦发银行的特征工程流程图

（十）模型管理

模型管理是通过标准化的模型接口，将大量的自训练模型和第三方模型进行统一集中管理。管理对象主要包括模型和模型服务。模型管理贯穿模型从上线到下线的全过程，有助于对模型资产进行统一盘点和管理，全面了解模型运行状态，便于模型共享使用，同时为模型风险管理、模型审计和模型可解释打下基础。

核心要点：

● 对模型进行注册和纳管。

● 对模型资产进行管理，包括对模型文件、模型使用文档、模型评估指标与报告、模型服务的统一纳管。例如，增删改查、分类、权限管理、模型卡片等。

● 对模型进行版本控制(包括基础信息、运行环境、输入输出等)，支持更新查看、多维度比对、版本提交、版本回滚等能力。

实践案例 1：河南移动的模型管理

河南移动融智工场通过算法中台对算法模型进行统一管控，包括模型接入、视图、分类、泛型、适配、共享复用等，提供算法模型的生命周期管理、版本管理、模型分享以及统一部署能力。

1.模型接入管理：对开发型、内置型、三方型的算法模型进行管理，通过标准化的模型接入接口，将训练完成的模型纳入算法中台。

2.模型视图管理：对接入算法模型的版本信息、脚本信息、和环境信息进行查询、修改，可实现对算法模理的清理、统一发布部署等。

3.模型分类管理：对接入的算法模型进行聚类，提炼算法模型共性部分，为用户提供更加精准贴合需求的算法模型。目前算法中心沉淀了包括指标异常检测、指标预测、日志模式识别、日志异常检测、根因分析与推荐、告警降噪、多指标维度分析七大类场景的算法模型。

4.模型泛型管理：将纳入管理的算法模型拆解重组装，形成和业务结合紧密的泛型，为后续服务化打下基础。提供算法模型及泛型的版本管理，支持对算法模型、算法泛型的效果和性能的评估、管理，支持多类算法、多类泛型的对比评估分析，可实现对算法模型、泛型进行标注说明。

5.模型适配：根据多样化的业务需求进行算法模型、泛型推荐，使得模型更加适配实际场景的业务需求。

6.模型共享复用：遵循 TMF Open API 标准提供规范的 RestAPI，将算法模型以服务化方式对外开放，实现模型能力的高复用、高敏捷、快速迭代。

来源：河南移动

图 30 河南移动的模型管理示意图

实践案例 2：百度的模型管理

百度智能云企业 AI 开发平台通过模型中心的建设对模型进行集中纳管，包括模型导入、管理、评估、加速、加密、共享，支持构建和调试部署包，支持将模型快速部署至各类运行环境。

1. 模型纳管：可管理本平台训练得到的模型，也可导入第三方模型并进行统一管理。其中本平台训练模型可来源于零代码建模的图像、文本、语音、视频、结构化、场景建模模型，也可来源于全功能开发的 Notebook 建模、可视化建模、自动化建模及智能产线建模。第三方导入模型支持从本地上传或从存储选择，支持以模型文件或镜像形式导入。其中，模型文件支持 TensorFlow、PaddlePaddle、PyTorch、Sklearn、XGBoost、ONNX、PMML 等主流框架。

2. 多版本模型管理：可存储单个模型的多版本信息，包括版本号、模型来源、模型状态、模型类型、模型框架、网络结构/算法类型等，便于对多版本模型进行比较，以决定需采用的具体模型。

3. 部署包管理：可管理面向部署的模型镜像或 SDK 文件，以提升部署效率。支持基于模型文件、模型镜像或 Helm Chart 来构建部署包。

4. 模型评估：支持在云端和边缘环境下对多个模型的效果和性能进行全面评估。

5. 模型加速：可在降低少量模型推理准确性的情况下大幅压缩模型复杂度，提升模型性能，增加同等计算资源下预测推理服务的吞吐量。

6. 模型部署：支持模型云部署（发布为预测服务）和边缘部署（下发至边缘设备）。

7. 模型加密：导出模型时支持对压缩文件进行加密。

8. 模型共享：可将模型分享至当前项目所在组织或全平台。

来源：百度

图 31 百度的模型管理流程图

实践案例 3：九章云极 DataCanvas 的模型管理

九章云极 DataCanvas APS 机器学习平台，支持对机器学习模型、深度学习模型和预训练模型等进行分组和集中管理，并实现不同模型的统一评估和比对，从而识别冠军模型，以确保最佳模型性能。在某商业银行 ModelOps 平台建设过程中，应用 DataCanvas APS 构建了涵盖标准建模、过程管控、敏捷部署、灵活迭代、持续监控到退役下线的全生命周期模型管理闭环体系，打造适用于该商业银行的完整模型生态。通过模型管理模块注册纳管了平台自训练及第三方生产的近百个 AI 模型，按照业务场景细分为智能营销、智慧风控、运营支撑、审计合规、智能运维、创新应用等进行集中分类管理。通过对企业的 AI 模型资产的梳理分类、模型状态及版本的精细化管理，缩短了近 30%的模型迭代周期。

来源：九章云极

图 32 九章云极 DataCanvas 模型管理功能示意图

（十一）仓库管理

仓库管理是建立多个仓库存储和管理不同的 AI 资产，包含元数据仓库、特征仓库、模型仓库、代码仓库、参数仓库等，以提供资产的版本化存档、访问、复用、追溯等能力。仓库管理实现了对各类资产的有序管理，是 AI 资产治理的基础。

核心要点：

● 版本管理：仓库管理承担重要信息存档的功能，需要支持版本控制及权限管理能力，以实现版本对比和追溯能力，并提高协作效率。

● 任务复现：所存档的信息支持在新的任务中共享和复用。例如，元数据和特征，可以在新的训练任务中被引用，从而实现相关任务的复现。

● 信息追溯：通过查询所存档信息被使用的情况，在操作时留痕，便于后续任务复现和项目复盘等阶段进行回溯。

● 持续更新：仓库管理的信息支持用户进行编辑和更新，确保信息准确和可用。

实践案例 1：中移研究院的元数据管理

中移研究院在落地 MLOps 过程中，通过 MongoDB 记录各任务元数据，并以日志方式将数据引入、特征工程、模型训练、模型服务等环节产生的元数据实时写入并存储。

● 数据引入：引入时间、引入数据行数、列数、特征名、特征类型、数据特征（分布、空值比例、0 值数等统计数据）等。

● 特征工程：数据行数、列数、特征名、特征类型、运行时间、运行时长、运行环境、函数、参数、特征工程模型位置、生成数据位置、生成数据行数、列数、衍生特征类型、衍生特征名称等。

● 模型训练：引入数据位置、算法名称、算法版本、算法参数、资源消耗、运行时间、运行时长、模型性能、模型位置等。

● 模型服务：数据行数、运行时长、运行结果、结果精度、结果位置等。

实践案例 2：中信证券的 MLOps 平台和模型仓库

中信证券数据智能平台（DIP）作为一站式数据科学平台，是集数据准备与探索、环境构建、特征工程、算法实现、模型构建、模型管理、模型发布、模型服务运维于一体的多租户机器学习平台，实现了模型全生命周期闭环开发管理，形成了工程化的模型生产与批量化的模型管理体系。

来源：中信证券

图 33 中信证券的机器学习生命周期示意图

1. 环境：通过 Docker 技术为数据处理、代码编程、模型服务提供可定制化的运行时环境。

2. 数据：DIP 提供了数据的全生命周期管理功能，覆盖了数据采集、数据探索、数据处理等过程，提供了大量数据分析工具，实现高效地数据探查与数据分析。

3. 算子：算子是算法的载体，DIP 不但预置了常见的算子，还允许自定义新算子，极大的扩展了 DIP 可用范围，提升算子的高可用性与复用性。

4. 探索空间：基于 web 的多语言集成开发环境，用户不但可以操作工作空间中的各类文件，而且可以通过 FAAS 来直接使用项目下的数据集、算子等对象，编程人员可以在探索空间高效的进行数据处理、模型开发与验证等工作。

5. 自动建模：DIP 中预置了对常见数据分析场景的处理模型，用户只需要提供数据即可完成模型的自动训练。

6. 工作流：用户可以根据实际场景组合数据集和算子来构建工作流，从而解决特定场景下的机器学习问题。

7. 模型仓库：提供批量化的模型管理服务，如模型文件校验、模型评估、可视化解释等，被管理的模型既可以是基于工作流或自动建模训练的模型，也可以是使用代码基于开源机器学习框架训练的模型

8. 模型服务：自动建模或工作流的训练得到模型，而服务则是模型的运行实例。

（十二）模型安全

模型安全是指保障机器学习模型的机密性、完整性和可用性。机密性是为防止模型架构、参数及训练数据、测试数据被泄露的风险；完整性是为防止攻击者通过操控训练数据或测试数据而引导模型输出特定结果的风险；可用性是保障合法用户能够访问模型的准确输出和特征等权限内的信息。模型安全为行业应用提供安全保障，是决定模型是否可用的基础。通过模型安全的管控，使模型在数据收集、模型训练和模型应用等阶段减少遭受攻击的风险。

核心要点：

● 加强模型本身安全性。从算法和模型两个维度，一是从源头提升算法设计逻辑的安全性（例如算法设计不应存在歧视偏见等），以及算法依赖库的安全性；二是防范模型被攻击（例如药饵攻击、闪避攻击、模仿攻击、逆向攻击、供应链攻击、后门攻击等）。

● 加强模型生产过程安全性。一是防范数据在传输、存储和使用过程中被窃取或泄露，并保证数据隐私性；二是防范算法和模型在传输、存储及使用过程中被窃取或泄露；三是保证模型生产过程相关步骤的安全性；四是保证数据准备过程、建模过程、部署上线过程的可追溯性。

● 加强模型可解释性。贯穿生产过程对模型开展解释工作，包括特征可解释、算法可解释、参数可解释、模型无关可解释等。

● 制定多方位的防御策略。例如，某一种针对对抗攻击的防御方案无法适用于所有类型的对抗攻击，因为在阻挡一种攻击时，可能给

攻击者留下一个新的漏洞。因此，模型安全的防御需要通过集成的方式，均衡考虑和融合多种防御方案。

实践案例 1：绿盟科技的模型安全

模型在生命周期中潜藏着各种安全风险，因此绿盟科技在数据收集阶段、模型训练阶段和模型预测阶段均采取对应的防御措施保护数据、模型的安全，如下图所示。

来源：绿盟科技

图 34 绿盟的模型安全防御策略示意图

在数据收集和模型训练阶段，数据窃取会破坏数据机密性，数据投毒通过篡改数据或添加恶意数据影响模型性能。后门攻击则通过植入触发器影响模型决策结果。相应的防御策略包括恶意样本识别、数据清洗、隐私保护方法（同态加密、差分隐私、安全多方计算）、数据正则化、后门检测与移除等。

在模型预测阶段，攻击者通过逃逸攻击误导模型的决策过程。相应的防御策略包括对模型输入或模型训练过程进行数据随机化、数据增强、对抗训练，通过防御蒸馏、梯度正则化来修改模型结构等。此外，攻击者也可以通过逆向工程、模型窃取、模型反演等方式推断出训练数据分布、训练集的属性信息或模型参数、模型架构等隐私。因此，模型持有者通常采用隐私保护方法、区块链技术等防御策略提升模型的安全性。

实践案例 2：蚂蚁的模型安全

蚂蚁提供安全的 MLOps 生产链路，构建了从模型研发到发布、线上推理、监控可迭代的全生命周期。其核心点在于全链路自动化执行能力。在需求中心完成模型需求的对焦和立项；在案件样本中心完成样本口径确认、样本的生成和特征仿真，并依靠 AutoML 能力，自动完成特征生成、自动模型选择和自动训练；在蚁鉴测评中心，自动完成模型测评和模型压缩，产出模型评测报告；在发布中心对模型进行一键部署，发布到生产环境；在预测中心提供模型推理服务，并对在线模型进行实时预测；在监控中心持续对线上模型进行多维监控，当监控到模型性能衰退时，自动触发下一步的模型迭代流程。

来源：蚂蚁

图 35 蚂蚁的 AntSecMLOps 架构图

在蚂蚁大安全有两类核心业务场景，一是与交易、转账等直接和资金打交道的资金安全场景，二是与小程序、文本、图片、音视频打交道的内容安全场景。针对这两种不同的场景，算法工程师和数据科学家们应用 AI 研发各种反洗钱、反欺诈、反赌博等各种守护用户安全的策略和模型。同时，蚂蚁通过其蚁鉴的 AI 安全检测平台，对样本、策略、模型、业务进行测评。一是对样本的质量、多样本的分布相似度、样本独立性、样本多样性进行评估；二是对策略的效能（例如覆盖率、打扰率）、策略间覆盖的重合度和增益进行评估；三是对模型多个维度进行测评（例如模型本身性能、模型稳定性 PSI、线上推理时性能（QPS/RT）及可信相关测评；四是在离线仿真环境下，模拟线上真实环境观测

策略、模型和策略+模型三者在业务上的表现。

来源：蚂蚁

图 36 蚂蚁的蚁鉴-AI 安全检测平台

五、MLOps 总结与展望

（一）总结

从数字化到智能化时代的跨越中，人工智能不断为行业深化赋能，成为了组织可持续发展的重要方向。而 MLOps 作为人工智能生产落地的重要推动力，为行业缔造更多商业价值。

MLOps 助力组织建立标准化管理体系，保障模型生产质量。为有效缓解 AI 生产过程的跨团队协作难度大、过程和资产管理欠缺、生产交付周期长等管理问题，MLOps 应时而生。MLOps 为机器学习模型全生命周期建设标准化、自动化、可持续改进的过程管理体系，使组织规模化、高质量、高效率、可持续地生产机器学习模型。

MLOps 技术发展逐步成熟，但组织落地挑战不一而足。从 2015 年至今，MLOps 前后经历了斟酌发酵、概念明确、落地应用等三大阶段。当前 MLOps 体系迅猛发展，带动着 MLOps 产品提供方和应用方的效能升级。一方面，资本市场持续火爆，MLOps 工具创新涌现；另一方面，MLOps 行业应用稳步推进，落地实践成果颇丰。组织将 MLOps 引入到机器学习项目全生命周期是一个渐进式过程，在发展过程中仍面临着诸多挑战，例如，组织落地驱动力不足，支撑工具选型难、集成难，模型治理和可信道阻且长，环境间的交互难以平衡等。

MLOps 框架体系趋向流程化，落地范式显露雏形。为填补国内 MLOps 实践指南的空白和弥补行业可用标杆案例的不足，中国信通院联合产业专家对现有的业界 MLOps 框架体系做出梳理和归纳，覆盖到包含典型 MLOps 流程架构和典型 MLOps 相关角色。典型的 MLOps 流程架构包含 7 大部分，需求分析与开发、数据工程流水线、模型实验工程流水线、持续集成流水线、模型训练流水线、模型服务流水线、持续监控流水线等；典型 MLOps 相关角色包含业务

人员、项目经理、机器学习架构师、数据工程师、数据科学家、软件工程师、测试工程师和运维工程师等。此外，本指南收录了 12 大典型关键能力的 27 个业界实践案例，给各行业的组织布局规划 MLOps 提供有益参考和指引。

（二）展望

MLOps 的高成熟度应用并不是一蹴而就的，实际生产的 MLOps 体系还处于较低的成熟度。我们需要重视这一阶段爆发的待解决问题，如离线在线特征相互隔离、AI 资产缺少沉淀、自动化水平受制约等。因此，资产管理、过程管理、运营模式、特征平台、工具平台、大模型及可信 AI 等各项能力的持续发展跃迁，正成为 MLOps 发展的新趋势。

MLOps 将在机器学习项目大规模高效率生产的基础上，不断迎接 AI 工程实践所带来的新挑战，推动 AI 资产安全有序管理，促进持续高效运营，保证模型及其生产过程更稳定、更可靠、更安全、更透明，充分发挥人工智能的经济价值和社会效益。

第一，构建健全的 AI 资产治理体系。对数据、代码、特征、模型、元数据等 AI 资产进行有效管理和沉淀，将为组织带来更多长远价值。随着 AI 模型越来越多，已有诸多组织开始或已经构建了良好的模型管理体系，对模型开展了集中统一的管理和共享，但对模型安全和风险，以及算法和元数据等 AI 资产的管理略显薄弱或缺失。因此，构建组织级健全的 AI 资产治理体系，将是 MLOps 持续改进方向之一，也是提高 MLOps 能力成熟度水平的重要体现。比如，事前制定 AI 资产全局和局部的安全管理体系，事中做好 AI 资产生产过程保障，并对 AI 资产开展可追溯管理和运行监控，事后强化审计机制。

第二，MLOps 自动化水平进一步提高。由于 MLOps 需多平台打通，与各资产仓库有效衔接，与各信息系统高效调度，当前诸多 MLOps 实践过程中的自动化水平还不够高。接下来，数据工程、模型实验、持续集成、持续部署、持续训练、持续监控等流水线的自动化水平，及流水线间的衔接效率，将得到进一步提升，从而实现高效率、可持续的机器学习项目全生命周期管理能力。

Analytics Insight 预测，AutoML 向 AutoMLOps 转变，将是 2023 年 MLOps 十大发展趋势之一[11]。未来，我们不仅需要模型构建过程的自动化，更需要全链路的自动化能力。

第三，构建可观测的高效模型运营体系。现阶段的 MLOps 模型运营主要是实现上线模型的监控，自动化发现问题并通知告警。未来将从三个方面持续优化运营模式，一是提高运营自动化水平，包括智能化分析能力、自动化处置能力等；二是提升运营的全面性，覆盖 MLOps 全生命周期的运营体系，可有效地持续改进 MLOps 运行过程；三是增加可观测能力，提高决策速度、决策质量及决策智能化水平。构建更加高效、更加全面、更加智能化、可观测性更强的模型运营体系，将是全面落地 MLOps 的重要部分。

第四，特征平台为高质量模型保驾护航。随着 FeatureOps 概念的深入和落地，特征平台将围绕离在线特征存储的互通和一致性、特征的高吞吐及低时延的调用、特征的自治化能力，持续挖掘和发挥特征的价值。特征平台作为特征管理的重要部分，将为模型训练、模型更新、在线推理提供更多支撑。

第五，MLOps 平台化能力持续提升。当前 MLOps 处于发展初期，工具繁杂，许多组织以解决问题为导向而选择工具，但又面临工具选

[11]https://www.analyticsinsight.net/top-10-mlops-trends-and-predictions-to-lookout-for-in-2023/.

型和集成难的问题。而随着模型越来越多、业务需求越来越复杂，MLOps 平台化需求将成为趋势，帮助组织更体系化、更便捷、更灵活、更快速地使用 MLOps 助力产业升级。

Gartner 预测，到 2026 年将有 80%的软件工程组织建立平台团队[11]。未来，组织将综合考虑 AI 项目的数量及需求、组织结构、战略规划、已有技术资产、成本，及当前 MLOps 成熟度水平等要素，选择端到端平台工具，或工具链+解决方案的方式，以平台化模式开展更大规模的落地。

第六，提升 MLOps 能力应对大模型带来的挑战。随着大模型等新技术的落地应用，MLOps 应持续优化其技术架构，从低代码或无代码化、算力资源的访问和优化等方面持续提升性能，以应对大规模数据和预训练模型带来的挑战。例如，在搜索、广告、推荐等互联网核心业务场景，正从简单的小模型过渡到数万亿参数的大模型，而适用于普通模型生产的 MLOps 可能无法满足今后需求，因此 MLOps 将基于流水线，在海量样本构建、模型增量与全量的训练和部署、模型推理、模型回滚、模型回溯等方面提升能力；在大型语言模型方面，LLMOps 将成为 MLOps 发展的重要分支[12]，为基础模型的下游微调和部署发布等过程高效赋能。

第七，可信 AI 助力组织可持续发展。落地 MLOps 的短期目标通常是提升模型迭代能力及效率，且在诸多组织中得以实现。而长期目标将在效率提升基础上，更多地关注模型安全与风险。通过保证模型的技术属性（准确、可信、鲁棒等）和社会属性（可解释、透明、隐私、安全、无偏见等），筑牢 AI 风险管理防线和安全防线，构建 AI 可信体系，为组织生产更加更负责任的 AI 项目，助力组织可持续发

[12] https://www.forbes.com/sites/robtoews/2022/12/20/10-ai-predictions-for-2023/?sh=51a9e1ddfab7.

展，将是未来持续探索之方向。

参考文献

1.Mark Treveil & the Dataiku Team, Introducing MLOps:How to Scale Machine Learning in the Enterprise.

2.Kreuzberger D, et al. Machine Learning Operations (MLOps): Overview, Definition, and Architecture[J]. 2022.

3.Sculley D, et al. Hidden Technical Debt in Machine Learning Systems[J]. Advances in neural information processing systems, 2015:2494-2502.

4.Google. MLOps: Continuous delivery and automation pipelines in machine learning.

5. Khalid Salama, et al. Practitioners guide to MLOps: A framework for continuous delivery and automation of machine learning.

6.李攀登. MLOps 实战:机器学习从开发到生产. 电子工业出版社, 2022.

7.彭河森，汪涵. 构建实时机器学习系统.机械工业出版社, 2017.

8.周志华：机器学习，清华大学出版社, 2016.

附表

附表 1 MLOps 工具链清单

关键能力	常用工具	
	国外	国内
数据处理	MapReduce、Labelme、CVAT、SQL、HDFS、Amazon Sagemaker、Alluxio、Spark、Pandas	百度 EasyData 智能数据服务平台、百度众测平台、华为云 ModelArts、华为云 DataArts、整数智能数据平台、云测数据标注平台、九章云极 DataCanvas APS 机器学习平台、新华三绿洲平台
模型训练	Amazon Sagemaker、Microsoft Azure、Google Cloud Platform、Databricks	百度智能云企业 AI 开发平台、华为云 ModelArts、九章云极 DataCanvas APS 机器学习平台、Colossal-AI
构建集成	Jenkins、CML(Continuous Machine Learning)、AWS CodePipeline and Step Functions、Azure DevOps	腾讯蓝鲸、阿里云效、九章云极 DataCanvas APS 机器学习平台、华为云 CodeArts
模型服务	模型服务配置：Kubernetes、Docker; 搭建 API 服务的程序框架：Flask、Kubeflow 的 KServing、TensorFlow Serving、Seldon.io 服务、BentoML; 批量推理：Apache Spark; 云服务工具：Microsoft Azure ML REST API、AWS SageMaker Endpoints、IBM Watson Studio 和 Google Vertex AI 推理引擎：TensorRT、TensorFlow Lite	百度智能云企业 AI 开发平台、华为云 ModelArts、九章云极 DataCanvas APS 机器学习平台 推理服务化：PaddlePaddle Serving、MindSpore Serving 推理引擎：MindSpore Lite（华为）、MNN（阿里）、TNN（腾讯）、MACE（小米）
运营监控	Microsoft Azure、Algorithmia、Evidently AI 和 Deepchecks（结构化数据）、Seldon Alibi（非结构化数据）、Grafana、Kubeflow、MLflow、Amazon SageMaker 模型监控器、Prometheus+Grafana	百度智能云企业 AI 开发平台、华为云 ModelArts、星环科技 Sophon MLOps
模型重训	Airflow、Prefect、Ploomber	华为云 ModelArts
实验管理	MLflow、Neptune AI、Microsoft Azure、Amazon Sagemaker、Weights and Biases、DagsHub	百度智能云企业 AI 开发平台、九章云极 DataCanvas APS 机器学习平台
特征管理	Google Feast、Featuretools、AWS Feature Store、Tecton.ai、Hopswork.ai	百度智能云企业 AI 开发平台、九章云极 DataCanvas APS 机器学习平台、第四范式 OpenMLDB

模型管理	Google Vertex AI、Microsoft Azure AI Builder、AWS SageMaker、Dataiku、MLflow	华为 ModelArts、百度智能云企业 AI 开发平台、九章云极 DataCanvas APS 机器学习平台、中国移动九天可视化建模平台
流水线管理	Airflow、MLflow、Kubeflow、TensorFlow、ZenML、TFX	百度智能云企业 AI 开发平台、华为云 ModelArts
代码仓库	GitLab、GitHub 和 Gitea	码云 Gitee、华为云 CodeArts
元数据管理	Kubeflow Pipelines、AWS SageMaker Pipelines、Azure ML 和 IBM Watson Studio、MLflow	百度智能云企业 AI 开发平台
数据版本管理	Dagshub、Databricks、DVC	百度智能云企业 AI 开发平台、九章云极 DataCanvas APS 机器学习平台
模型安全	Cleverhans、Advertorch、DeepRobust、Opacus	百度 AdvBox、上海交通大学 DAmageNet
端到端平台	Kubeflow、MLflow、Neuro 、Microsoft Azure、Google Cloud Platform、Amazon SageMaker、Valoha、Algorithmia、Neu.ro MLOps	百度智能云企业 AI 开发平台、华为终端云 MLOps 平台、华为 ModelArts、蚂蚁 AntSecMLOps、腾讯太极机器学习平台、九章云极 DataCanvas APS 机器学习平台、绿盟科技 SecXOps、中国移动九天可视化建模平台

注：表格所述工具清单，来自于部分企业的调研报告，后续将持续更新。

编制说明

本指南的撰写得到了 AI 领域多家企业与专家的支持和帮助，主要参与单位如下。

参编单位：中国信息通信研究院、华为终端有限公司、中国联合网络通信有限公司软件研究院、中国移动通信有限公司研究院、上海浦东发展银行股份有限公司、中国农业银行股份有限公司、建信金融科技有限责任公司、中原银行股份有限公司、中信证券股份有限公司、北京百度网讯科技有限公司、北京九章云极科技有限公司、思特沃克软件技术(北京）有限公司、新华三技术有限公司、中移动信息技术有限公司、中国移动通信集团广东有限公司、北京神州绿盟科技有限公司、中国移动通信有限公司在线营销服务中心、星环信息科技(上海）股份有限公司、格物钛（上海）智能科技有限公司、北京云测信息技术有限公司、蚂蚁科技集团股份有限公司、马上消费金融股份有限公司、腾讯科技（深圳）有限公司、北京华佑科技有限公司、中国移动通信集团河南有限公司、北京菱云科技有限公司、北京蔚时科技有限公司、云南白药集团医药电子商务有限公司、南京新一代人工智能研究院。

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62309514

传真：010-62304980

网址：www.caict.ac.cn