

AI 赋能资产配置（十二）

DeepSeek 资产配置进阶实践的 20 个核心问答

核心观点

本报告针对 DeepSeek 在大盘择时、行业轮动、识别财务瑕疵等应用中涉及到的项目细节、技术原理以及方法对比与优化进行了详细的回答：本文系统梳理了 AI 技术在策略优化、风险识别与决策闭环中的关键作用，通过动态学习机制与智能决策框架的构建，AI 能将历史规律挖掘与实时信号解析相结合，形成具备自我进化能力的智能投研体系。

AI 通过非线性建模技术重构动态赋权机制，显著提升市场适应性。不同于经典风险平价模型的静态风险分配逻辑，AI 融合 XGBoost 特征筛选与深度学习的协同优势，创新性地引入信息系数平方加权、波动率敏感窗口等技术，实现了自适应半衰期调整机制等功能。这种动态赋权体系能够捕捉因子间的协同效应，在宏观因子与市场情绪的耦合分析中展现独特价值，有效应对市场突变场景。

AI 能将大盘择时与行业轮动相结合，提升策略解释力与前瞻性。多因子择时输出的大盘风险暴露系数作为行业轮动的“顶层约束”，同时行业轮动结果反哺择时因子，例如，让三标尺中的指标与多因子择时中的宏观因子形成交叉验证，考虑大盘对行业影响的同时，修正宏观数据滞后问题。

在财务风险识别领域，AI 的优势在于开创性地融合多维度分析框架。通过结构化财务指标与非结构化文本情感语调的协同分析，构建数值异常检测、文本语义解析、交易行为分析的三维风控体系。相比 Benford 定律等传统数值检测方法，AI 在识别隐蔽性造假方面展现独特优势，能够捕捉管理层文本中的语义矛盾与异常修饰。其进化路径指向领域预训练与动态特征库的融合，通过持续学习新型造假模式增强模型鲁棒性。

AI+RAG+Agent 体系通过决策闭环架构实现策略的自主进化。该体系以生成式 AI 为智能中枢，整合实时数据管道、动态知识检索与自动化风控模块，突破传统回测框架的静态局限。RAG 技术实现分钟级市场信息更新与噪声过滤，Agent 预设的多层级防御机制（包括波动率自适应调整、冗余策略池等）显著提升黑天鹅事件应对能力。这种架构创新使系统具备“感知-决策-验证-优化”的完整能力链，推动策略迭代周期从月度级压缩至实时级。

通过“AI 推理+人工兜底”混合模式，使 AI 技术框架业务落地具备双保险。RAG 与 Agent 技术强化了风险控制，极大程度避免了虚构关联，并能自动检测到逻辑矛盾。此外，通过纳入新的行业专家知识优化特征逻辑、当市场出现系统性风险或数据源异常时加入人工操作，能进一步提升稳健性。整体上，Agent 的恢复机制以自动化实时响应为基础，通过动态数据融合与模型迭代实现自愈能力，而人工干预则聚焦于极端场景与复杂语义的深度纠偏。

风险提示：AI 幻象风险；数据异化风险；监管规则适配风险；人机协同失效风险；策略同质化共振风险。

策略研究·策略专题

证券分析师：陈凯畅 021-60375429
chenkaichang@guosen.com.cn
S0980523090002

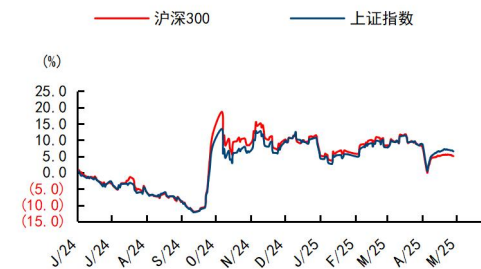
证券分析师：王开 021-60933132
wangkai8@guosen.com.cn
S0980521030001

证券分析师：董德志 021-60933158
dongdz@guosen.com.cn
S0980513100001

基础数据

中小板/月涨跌幅(%)	6202.33/-6.70
创业板/月涨跌幅(%)	1948.03/-8.47
AH 股价差指数	134.03
A 股总/流通市值(万亿元)	109.84/99.00

市场走势



资料来源：Wind、国信证券经济研究所整理

相关研究报告

《主题投资月度观察(2025年第4期)-科技前沿加速迭代，政策红利密集释放》——2025-04-29

《资金跟踪与市场结构周观察(第六十三期)-股市资金面“紧平衡”》——2025-04-29

《中观高频景气图谱(2025.4)——可选消费景气提振》——2025-04-29

《估值周观察(4月第4期)-全球权益市场回暖，估值温和扩张》——2025-04-27

《资金跟踪与市场结构周观察(第六十二期)-交投分化延续》——2025-04-22

内容目录

模型训练与权重优化	4
实战部署与系统架构	7
AI+RAG+Agent 体系与风险控制	9
方法对比与改进	11
风险提示	14

图表目录

图1: Boosting 集成学习方法示意	4
图2: 多因子择时、“三标尺”行业轮动相结合	8
图3: RAG 生成式 AI 应用架构	11
图4: DeepSeek 动态赋权与经典模型对比	12

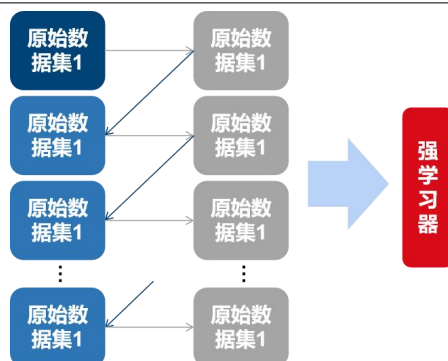
模型训练与权重优化

问题 1：报告中提到用 XGBoost 确定初始权重，能否简述基于 XGBoost 的“权重优化模型的路径”具体是如何操作的？

基于 XGBoost 的权重优化模型路径主要用于从历史数据中挖掘各因子对市场趋势的影响规律，并将其转化为初始权重基准。该过程首先通过 XGBoost 对历史股债市场数据（如宏观经济指标、资金流向等）进行特征重要性分析，量化各因子对“股债强弱走势”的解释能力，筛选出具有长期稳定性的高价值因子；然后将这些因子重要性结果作为训练样本输入 DeepSeek 模型，使其学习因子与市场状态的关联模式；最后结合当前市场环境，AI 基于历史规律生成初始权重框架，再通过动态赋权机制进行实时调整。这种方法的优势在于既保留了传统模型的逻辑可解释性，又能通过 AI 动态适应市场变化，同时避免了直接训练大模型带来的复杂性和资源消耗。

整个流程体现了“历史规律挖掘-规律映射学习-实时预测应用”的技术路径，通过 XGBoost 的先验分析为 AI 模型提供可靠的初始基准，再结合 DeepSeek 的推理能力实现权重的动态优化，在保证模型稳定性的同时提升对市场变化的适应能力。这种分阶段的设计既考虑了历史经验的传承，又充分发挥了 AI 在实时决策中的优势。

图1: Boosting 集成学习方法示意



资料来源：Wind，国信证券经济研究所整理

问题 2：DeepSeek 训练所用的数据样本量（时间跨度，如 3 年/5 年/更长）大概是多少？多大的训练样本或特定的训练方式可能导致过度拟合？是否有相关经验？

关于数据样本量的问题，本项目训练 DeepSeek 所使用的数据样本从 2015 年 9 月开始，数据频率为月度。首先是分析师底稿数据从该时间开始较为完备，这保证了样本数据的一致性和可用性；其次，近 10 年的跨度基本覆盖了完整的宏观经济周期，使数据具有较强的代表性，有助于模型充分学习宏观经济在不同时期的变化规律和特征。

关于过拟合问题，本项目中过拟合相对可控。一方面，从数据维度来看，本项目仅涵盖五大宏观框架及其核心指标，特征数量有限，远低于常见动辄 50+ 变量的高维模型，降低了过拟合风险；另一方面，生成式大模型并非依赖传统意义上的数据拟合，而是通过推理机制进行逻辑演绎与模式归纳，模拟人类认知过程，从

历史中主动挖掘潜在因果关系与结构特征，因此不必过度担心过拟合问题。

总体而言，相比传统机器学习模型，大模型推断结果附带清晰的逻辑链条，用户既可基于信任应用，也可在怀疑中验证筛选，这在一定程度上缓解了“黑箱问题”，提升了决策过程的透明度和灵活性。在当下的 AI 语境中，或许更应关注 AI 幻觉问题，而非过拟合问题。

问题 3：从宏观信号到组合构建中，短周期模型得出的“打分指示”如何转化为具体的战术配置权重（股债比例调整）？

将短周期模型的“打分指示”转化为战术配置权重，核心是通过风险资产暴露系数实现动态股债比例调整。综合打分区间（-1 至 1）被划分为若干风险等级，例如得分小于或等于 -0.5 时，定义为极端风险环境，此时股票仓位压缩至 20% 以下，债券及现金类资产占比提升至 80% 以上，以规避市场剧烈波动。当得分处于 -0.5 至 0 区间时，策略进入防御状态，股票仓位控制在 30%-50%，并配置高等级信用债对冲潜在风险；得分大于 0 时启动进攻型配置，其中 0 至 0.5 对应 50%-70% 股票仓位，0.5 以上则进一步提升至 70%-90%，债券部分仅保留利率债作为安全边际。

转化过程中需同步分析各维度因子（如宏观、资金、情绪）对当前打分的贡献度，形成“核心驱动因子矩阵”。例如，若宏观因子（如通胀领先指标）权重骤升，则针对性增加周期股配置比例；若情绪因子（如市场热度得分）超过阈值（如 0.8），则动态调高债券对冲比例以抑制过热风险。这种分层逻辑既保留了不同风险等级下的资产边界约束（如股票仓位上下限），也为宏观周期切换和投资者风险偏好变化提供了弹性调整空间。

问题 4：在动态赋权模型中，如何平衡因子有效性的实时调整与模型稳定性？例如，IC 值剧烈波动时，权重分配是否会产生过度频繁的调仓信号？

在动态赋权模型中，因子有效性的实时调整与模型稳定性的平衡主要通过以下技术机制实现：模型首先通过风险预算约束限制单一因子的影响力，例如设定单因子权重上限不超过 45%，避免单一因子的短期剧烈波动对整体策略产生过度干扰。同时，引入基于波动率的自适应窗口调整机制，动态控制观测周期长度——市场波动率升高时缩短窗口以增强对近期信号的敏感性，波动率降低时延长窗口以平滑噪声。这一设计通过弹性调节时间维度上的信号权重，兼顾了对市场变化的响应能力与长期稳定性。

在因子权重分配逻辑中，模型采用非线性加权公式对因子有效性（IC 值）进行处理，通过对 IC 值取平方强化高效因子的主导地位，同时天然抑制低效因子的短期波动影响。此外，模型通过固定调仓频率（如按周或月）对信号进行批量处理，避免高频噪声触发无效交易。例如，即使日内因子 IC 值剧烈波动，权重调整结果仅在预设周期结束时统一生效，从而降低过度交易风险。

模型还通过多因子协同验证增强稳定性。当某一因子出现异常波动时，系统自动检验其他关联因子的信号一致性，若多数因子指向相反方向，则延迟异常因子的权重调整。这种交叉验证机制与交易成本模型结合，进一步过滤低置信度信号，确保调仓指令的收益能够覆盖潜在摩擦成本。所有设计均围绕“规则框架内的动态优化”展开，既保留了传统模型的逻辑可解释性，又通过 AI 的实时学习能力适应市场状态变化，最终在测试周期内实现风险收益比的显著提升。

问题 5：财务造假样本的行业分布不均是否导致模型对低风险行业的误判？是否需要引入行业分层采样优化训练集？

财务造假样本的行业分布不均（如通讯服务行业占比 19.4% 而金融、公用事业不

足 8.5%) 可能导致模型对低风险行业的误判风险。这种不均衡会使模型过度学习高发行业的特征模式, 例如通讯服务行业常见的“虚构收入”或“重大遗漏”等造假手段, 而对低风险行业(如金融业的表外资产隐匿、公用事业的周期性利润波动)的特征捕捉不足。具体表现为两类问题: 一是模型可能将低风险行业的正常经营波动(如公用事业因基建周期导致的毛利率下滑)误判为异常信号; 二是对低风险行业的特有造假模式(如金融业的合规性措辞修饰)缺乏敏感性, 导致漏检。

项目中已通过行业属性处理部分缓解这一问题, 具体方法是将万得一级行业分类作为控制变量, 并采用**独热编码**(One-Hot Encoding)对行业属性进行特征化。这一设计旨在强制模型区分不同行业的运营特征与语言风格, 例如金融行业的“资本充足率”表述与公用事业的“基建投资周期”描述在文本和财务指标上存在显著差异。通过独热编码的行业标签, 模型能够学习行业间的基线差异, 避免将行业特性(如公用事业的低利润率)误读为异常信号。例如, 某公用事业公司的低毛利率若处于行业正常区间, 即使绝对值低于全市场平均水平, 模型也会结合行业标签判定其为合理波动。

然而, 这种行业属性处理的局限性在于其依赖行业分类的完整性与样本的代表性。若某些行业(如金融)的造假样本量过少, 独热编码引入的稀疏特征可能无法充分表征其风险模式。对此, 项目中进一步采用行业分位数校准和代价敏感学习进行补充——情感语调分数按行业内相对排名标准化(而非全市场统一阈值), 并通过加权损失函数提高少数类样本(如金融行业造假案例)的训练权重。例如, 某金融企业的情感分数若处于同行业后 10% 分位, 即使其绝对值高于其他行业, 仍会被标记为异常。

为进一步优化模型对行业分布不均的鲁棒性, 可引入行业分层采样与迁移学习的组合策略。分层采样要求从每个万得一级行业中按比例抽取等量的正负样本(如强制金融行业抽取与通讯服务行业等量的造假案例), 以均衡化训练集分布。同时, 对样本稀缺行业(如公用事业), 通过迁移学习复用相似行业(如能源)的语料特征, 结合行业独热编码的差异化标签进行领域适配。

实际应用中, 行业属性处理与分层采样的协同需解决两大挑战: 一是行业分类的粒度问题, 例如万得一级分类中的“金融”涵盖银行、保险、券商等差异化子领域, 需进一步细分以提高模型对细分风险的捕捉能力; 二是动态更新机制, 例如新兴行业(如金融科技)出现时, 需快速构建基础语料库并校准行业基准。总体而言, 现有方法(行业独热编码、分位数校准)可以与优化方向(分层采样、迁移学习)共同构成多层防御体系。

问题 6: 在行业轮动策略中, 如何通过交互指令让 AI 解释“三标尺”权重分配逻辑(如景气度>趋势>拥挤度)? 能否要求输出阈值调整的数学依据?

在行业轮动策略中, 通过交互指令让 AI 解释“三标尺”权重分配逻辑的功能, 基于 DeepSeek 的语义解析能力结合项目中的技术框架设计实现。项目中, DeepSeek 通过动态分位数机制、自适应核密度估计、多头潜在注意力(MLA)、交互特征工程等技术优化传统模型的局限性。

DeepSeek 的动态分位数机制通过滚动窗口(如过去 36 个月数据)和衰减系数(如 0.95)赋予近期数据更高权重, 突破了传统模型使用固定分位数阈值的局限, 减轻了市场环境变化时策略失效的问题。自适应核密度估计会根据数据密度动态调整带宽, 例如在换手率突增的区域使用较小带宽, 在平稳区域使用较大带宽, 以更敏感地识别交易过热或市场突变。多头潜在注意力(MLA)技术通过并行分析多个因子间的关系, 动态分配权重, 例如当趋势与拥挤度反向运动时, MLA 会自动

降低拥挤度的权重，优先保留景气度与趋势的协同效应。当景气度与趋势共振时，交互特征的贡献度显著提高，而景气度维持高位但趋势转弱，AI 会降低该组合特征的优先级，提示需谨慎配置。

用户可通过自然语言指令获取 AI 的数值结果与可视化输出。例如，输入“输出当前动态分位数阈值”，AI 会返回经过滚动窗口和衰减系数调整后的具体数值（如景气度阈值从历史均值 6.5% 升至 7.2%）。输入“展示 MLA 注意力权重热力图”，AI 会生成图表，标注不同市场状态下的因子权重差异（如牛市中趋势权重占比 50%，震荡期拥挤度权重提升至 50%）。这些输出使策略决策过程透明化，用户可直观理解 AI 的调整逻辑，并根据实时数据优化配置。

问题 7：情感语调因子在未训练行业（如科创板）中是否有效？如何验证其泛化能力？

情感语调因子在科创板等未训练板块或行业中的有效性需结合其设计原理与跨行业验证方法综合判断。理论上，该因子聚焦于财报文本中的情绪矛盾、模糊表述等通用风险信号，这些特征不依赖于特定行业的财务结构或业务模式。例如，科创板企业若存在财务瑕疵，其财报可能通过异常情感倾向（如过度乐观修饰技术成果、矛盾叙述研发进展与现金流压力）暴露风险，即使其业务涉及高研发投入或技术术语密集，这类信号仍可能被情感因子捕捉。

验证泛化能力时，需设计针对性测试。首先，可独立抽取新行业或板块的公司历史财报数据，构建该行业或板块的正常样本情感分数基准，对比问题公司（如已被监管处罚的企业）的情感分数是否显著偏离行业分布。其次，采用模型迁移方法，将原模型直接应用于未训练数据，观察其情感分数与财务健康指标（如审计意见类型、现金流异常波动）的关联性。若结果显示情感因子能有效区分风险样本，或与已知造假特征呈现负相关，则支持其跨行业适用性。此外，引入人工专家对未训练文本进行情感标注，与模型结果对比一致性，可进一步验证可靠性。实际应用中，需警惕未训练行业财报中技术术语可能导致的误判，可通过优化文本预处理规则或引入行业特定语义校准，提升模型在未训练行业中的稳健性。

实战部署与系统架构

问题 1：技术环境使用哪些编程语言、AI 框架与回测平台？

在技术环境方面，项目主要依托 Python 语言完成全流程开发。Python 作为金融量化与 AI 融合的首选编程语言，承担了数据清洗、模型构建、AI 对话接口调用、可视化绘图以及回测数据准备等核心任务。其开源生态与丰富的第三方库（如 NumPy、Pandas、Matplotlib）为灵活实现复杂逻辑提供了基础，同时兼顾了代码可扩展性与团队协作效率。

AI 框架层面，项目未涉及大模型的训练或微调，而是通过调用外部生成式 AI 服务（DeepSeek-V3）完成推理任务。项目的技术实现聚焦于通过提示工程（Prompt Engineering）引导生成式 AI 完成动态决策。系统通过设计结构化的对话指令，将历史宏观数据与经济周期理论转化为模型可理解的语义输入，驱动其推理过程。模型基于实时输入的标准化因子特征（如景气度、趋势等指标），生成适应市场状态的最优权重分配方案。这一路径的核心在于优化对话指令的逻辑层次、提升数据与知识的融合效率，并建立模型输出与金融决策规则的可解释性关联，而非对大模型本身进行参数训练或结构调整。

回测平台方面，由于项目处于验证宏观周期权重预测可行性的初期阶段，采用了

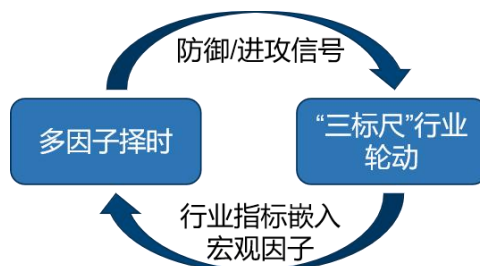
自主研发的回测框架。该框架实现了基础收益计算与风险指标（如夏普比率、最大回撤）的评估，但尚未集成专业量化平台（如 Backtrader、Zipline）的交易信号生成、动态仓位管理、交易成本模拟等高级功能。

问题 2：项目从试验到实盘耗时多久，是否有灰度机制（如分阶段资金投入）？组合构建中，如何使多因子择时、“三标尺”行业轮动相结合？

该项目目前定位于研究导向的初步探索阶段，其核心目标在于验证基于宏观框架的资产配置方法论的有效性。项目底层逻辑依托卖方分析师构建的宏观研究体系，主要聚焦于策略模型的学术验证与框架优化，尚未进入实际资金运作环节。由于仍处于理论验证期，暂未涉及实盘交易所需的资金管理系统、风控模块等基础设施搭建，也未制定灰度机制相关流程（即通过小规模资金、限定标的试运行逐步扩大应用的过渡方案）。当前研究重心在于回溯测试的严谨性验证、模型对市场状态切换的适应性分析以及动态参数调整机制的可解释性构建，为后续可能的实战化转型积累方法论基础。

多因子择时输出的大盘风险暴露系数作为行业轮动的“顶层约束”。例如：当多因子择时模型输出空仓信号时，使行业轮动模型进入“防御模式”，股票仓位整体缩减，行业仓位更加分散，且增强模型对于低贝塔行业的偏好；当多因子择时模型输出强进攻信号时，开放高弹性行业配置权限，允许单一行业超配。同时行业轮动结果反哺择时因子。如将三标尺中的拥挤度指标嵌入多因子的“情绪维度”，作为市场过热预警的补充信号、三标尺中景气度指标与多因子的“宏观因子”形成交叉验证，修正宏观数据滞后问题。

图2：多因子择时、“三标尺”行业轮动相结合



资料来源：Wind，国信证券经济研究所整理

问题 3：如何整合多维数据（如宏观指标、行业景气高频数据、社交媒体情绪）优化资产配置模型的输入？不同频率数据（日频行情、月频宏观）如何对齐？

多维数据的整合依赖于 DeepSeek 的全链路赋能框架。在宏观层面，模型整合了 GDP、CPI、利率政策等传统指标，并通过动态知识更新技术（RAG）注入实时数据（如行业景气指数），以捕捉经济周期转向信号。中观层面，卫星图像、专利数据等另类信息被转化为结构化指标（如技术图谱、供应链关系网络），用于实时监控行业竞争格局变化。微观层面，模型融合了门店客流统计、社交媒体情绪等非结构化数据，通过多模态数据对齐机制（如归一化、Z-Score 标准化）与传统财务指标结合。

不同频率数据的对齐通过多种方法实现。日频行情数据（如技术指标 DMI）直接保留原始频率，而月频宏观数据（如 PMI）通过线性插值或前向填充扩展为日频序列，与行情数据保持时间对齐。例如，当月度 PMI 发布后，当月所有交易日沿用该值直至新数据更新。高频数据（如 30 分钟行情）则通过滚动窗口计算均值或波动率，降频至与宏观数据匹配的周期。对于政策类数据（如利率调整），采用

事件驱动对齐，以事件发生日为锚点，后续交易日沿用该值直至新事件触发更新。

问题 4：当前模型基于历史舞弊模式（如虚构利润）训练，若企业采用新型造假手段（如虚增无形资产），模型如何动态识别？是否需要持续更新舞弊特征库？

当前模型在应对新型造假手段（如虚增无形资产）时，需依赖其多维度特征的综合分析能力。项目中，模型通过结构化财务指标（如偿债能力、现金流分析）与非结构化文本情感语调因子的协同作用，能够捕捉异常信号。例如，虚增无形资产可能导致“无形资产占总资产比例异常升高”或“研发支出与无形资产增长不匹配”，这类异常可能触发财务指标预警；同时，文本情感分析可识别管理层在描述技术成果时的矛盾表述（如过度强调“行业领先”但缺乏具体商业化数据），这类模糊修饰可能暴露造假意图。此外，模型中的非线性算法（如 MLP、LightGBM）能够挖掘财务指标与文本信号间的隐含关联，即使新型造假未在历史数据中出现，仍可能通过特征组合异常被间接识别。

然而，模型的动态识别能力存在局限。若造假手段高度依赖新型会计规则漏洞（如通过复杂交易虚增无形资产估值），仅依赖现有特征库可能失效。因此，需持续更新舞弊特征库以覆盖新风险维度，纳入新的行业专家知识优化特征逻辑，形成“财务指标+文本语义+外部数据”的动态融合体系。

AI+RAG+Agent 体系与风险控制

问题 1：项目体系目前是主要用于回测验证，还是已支持模拟盘/实盘的自动执行和动态调仓？Agent 体系在应对突发市场事件（如黑天鹅）时的鲁棒性是如何通过机制加强的？

当前金融投研的 Agent 体系仍处于理论设计与分块功能验证阶段，其核心价值在于构建“数据驱动决策、规则约束风险、反馈优化策略”的智能投研框架。尽管目前尚未实现实盘执行，但其通过动态规则引擎、实时数据处理、策略进化机制等设计，为应对黑天鹅事件提供了理论上的鲁棒性保障。未来需解决的关键挑战包括：1) 实时交易接口的稳定性：确保 Agent 与券商/交易所系统的低延迟对接；2) 合规性与透明度：满足金融监管对策略可解释性的要求；3) 算力与成本优化：在实时监控和交易场景中平衡计算资源与模型性能。

在应对突发市场事件（如黑天鹅）时，Agent 机制的鲁棒性设计主要体现在四个方面：1) 动态规则引擎与实时风险阻断：预设最大回撤阈值、行业拥挤度分位数等硬性指标，当市场波动突破阈值时，自动执行阶梯式减仓或行业轮换。其次持续监测因子信息系数和胜率，实时监测因子失效信号，自动降低其权重并检索替代指标。2) 多模态数据接入与动态处理：除实时整合宏观经济指标、资金流数据等，嵌入特有的事件驱动推理模块，通过 RAG 模块检索外部知识库，将政策文件、行业研报等非结构化数据转化为量化的风险信号。3) 历史情景回溯与强化学习提升策略适应性：定期调用回测模块，验证当前参数在历史黑天鹅事件下的表现，以此触发参数自动修正。其次，当连续两个月出现“因子失效误判”（如误判通胀因子上行导致仓位过高），Agent 自动触发“规则库升级”，引入波动率调整后的 IC 阈值（如 $IC > 0.2$ 且波动率 $< 15\%$ 才赋予高权重），降低参数漂移风险。4) 模块化架构预设冗余策略池：预设多套备选策略（如趋势跟踪、均值回归），当主策略失效时，自动切换至次优策略。

问题 2：在大盘择时与行业轮动中，Agent 具体如何运作以实现风险控制并自动化执行策略验证全流程？

在大盘择时与行业轮动研究中，Agent 可作为智能执行中枢，通过“数据接入-规则驱动-动态决策-反馈优化”闭环实现全流程自动化运作。首先，Agent 借助 RAG 实时检索宏观数据（如高频通胀指标）、资金流（北向资金动向）、市场情绪（舆情指数）等多源信息，经标准化处理后，传输至模型层预设的多因子择时与三标尺行业轮动模型。在大盘择时中，Agent 依据 IC 衰减加权公式动态分配多维因子权重，结合波动率自适应调整观察窗口（如牛市用 60 日短窗口、震荡市用 240 日长窗口），生成实时仓位建议；若触发最大回撤阈值（如 12%）或因因子失效预警（IC 连续三期 < 0.1 ），则自动执行阶梯式减仓或因因子替换（如用美债收益率斜率替代中美利差）。在行业轮动中，Agent 通过动态分位数机制（赋予近期数据更高权重）筛选行业，利用多头注意力机制平衡景气度、趋势、拥挤度的交互影响，例如当动量与拥挤度背离时自动降低拥挤度权重。此外，Agent 定期调用回测模块验证策略有效性，结合 RAG 获取的外部知识（如碳中和政策对电力设备的影响）更新规则库，形成“数据驱动决策、规则约束风险、反馈优化策略”的智能闭环，显著提升策略适应性与风险控制能力。

问题 3：Agent 在触发风控操作（如暂停调仓）后，如何重新评估市场状态并恢复交易？是否依赖人工干预？

在触发风控操作（如暂停调仓）后，Agent 通过自动化流程与人工干预结合的方式重新评估市场状态并恢复交易。首先，Agent 会借助 RAG（检索增强生成）技术实时抓取最新市场数据（如流动性指标、波动率、行业拥挤度等），动态更新风险因子计算模型。例如，若因流动性枯竭触发暂停，Agent 将持续监测订单簿深度、买卖价差等高频数据，待流动性恢复至预设安全阈值（如买卖价差回归历史均值 1.5 倍以内）后，自动启动参数修正流程。这一阶段可能调用时变 Kalman 滤波或自适应核密度估计技术，重新校准波动率预测衰减系数或资产相关性矩阵，并通过轻量级回测验证调整后策略的历史稳健性，最终在多维度信号（风险指标达标、因子贡献度平衡、市场情绪修复）协同满足时解除风控限制。

人工干预主要作为自动化逻辑的补充与兜底机制。当市场出现系统性风险或数据源异常时，预设规则可能无法覆盖复杂场景，需分析师介入调整阈值或直接锁定仓位。此外，即便项目中显示出有效性，但情感语调因子仍可能引发模型误判。对于明显的误判，需要人工修正语义逻辑或补充定性研判。整体上，Agent 的恢复机制以自动化实时响应为核心，通过动态数据融合与模型迭代实现自愈能力，而人工干预则聚焦于极端场景与复杂语义的深度纠偏。

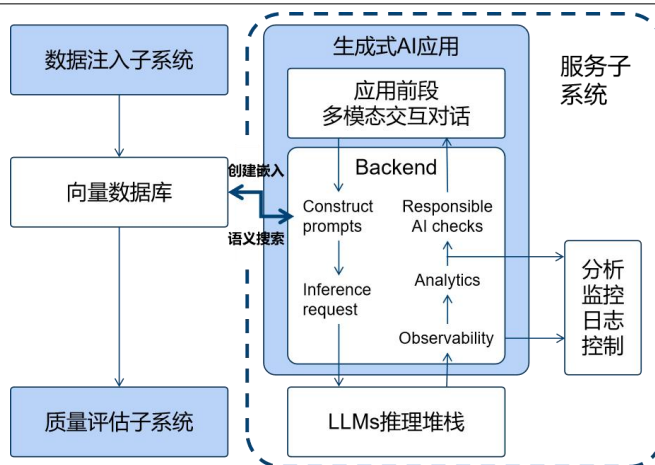
问题 4：Agent 调用 RAG 时，如何通过 Prompt 过滤噪声数据（如政策文件冗余内容）？RAG 如何实时更新行业数据？

在 Agent 调用 RAG（检索增强生成）时，通过 Prompt 设计过滤噪声数据的核心逻辑是结合语义约束与结构化指令。例如，针对政策文件中的冗余内容，系统会在 Prompt 中嵌入关键词提取规则与上下文范围限制。具体而言，可设计如“请仅提取与‘新能源补贴’‘碳关税’相关的条款，并忽略法律条文中的程序性描述”的指令，引导 RAG 优先检索与当前策略目标强相关的段落。同时，RAG 内部通过元数据过滤（如文档类型标签、发布时间范围）和语义相似度阈值（如仅保留与“行业轮动”“景气度预测”相关性高于 0.8 的内容）实现噪声剔除。这一过程类似于图书馆员根据书目分类和摘要关键词筛选资料，而非逐字扫描全文。

RAG 实时更新行业数据的实现路径依赖于动态数据管道的构建。首先，系统通过 API 接口与多源数据库（如万得、彭博、行业监管平台）直连，按预设频率（如分钟级）抓取最新指标（如行业换手率、大宗商品价格）。其次，RAG 采用流式处理引擎（如 Apache Kafka）对原始数据进行清洗与对齐，例如将不同频率的日

频财报数据与实时交易信号统一为标准化时序格式。最后，更新后的数据被注入增量索引模块，通过向量化嵌入（如 BERT 编码）与现有知识库融合，确保模型检索时优先返回最新信息。例如，当某行业突发政策利好时，RAG 可在 10 分钟内完成政策文本解析、行业指数关联性分析，并将结果同步至策略决策链路。这一机制在项目中体现为“动态知识更新”功能，直接解决了传统模型因数据滞后导致的策略失效问题。

图3: RAG 生成式 AI 应用架构



资料来源：Wind, 国信证券经济研究所整理

问题 5：“幻觉”风险在资产配置场景中的典型表现是什么？如何通过技术手段抑制此类风险？

在资产配置场景中，“幻觉”风险主要表现为 AI 模型生成缺乏数据支持的结论。例如，AI 可能虚构不存在的历史经济指标关联性（如错误地将某行业股价波动与无关的宏观指标强关联），或误判市场拐点（如基于噪声数据错误预测衰退周期结束）。“AI 推理不稳健性”正是此类风险的直接体现——模型可能因训练数据偏差或高频噪声干扰，输出看似合理但缺乏逻辑验证或推理依据的配置建议。

项目中提到的 RAG（检索增强生成）与 Agent 技术强化了风险控制。RAG 通过动态接入权威经济数据库，限制 AI 仅基于已验证知识生成结论，避免虚构关联。例如，若 AI 试图引用未经验证的“新型领先指标”，可以令 RAG 强制替换为标准化宏观数据（如 PMI、失业率）。Agent 方面则可以通过预设行为规则（如最大回撤阈值、单因子暴露上限）实时监控策略风险敞口，并在检测到逻辑矛盾时（如“高景气度行业配置权重为负”）自动回滚至安全参数。

方法对比与改进

问题 1：DeepSeek 的动态赋权公式与经典风险平价模型（Risk Parity）的权重分配逻辑有何区别？

DeepSeek 的动态赋权公式与经典风险平价模型（Risk Parity）的核心差异在于风险视角与调整机制的灵活性。风险平价模型以均衡资产风险贡献为目标，通过历史波动率或相关性静态分配权重，例如债券与股票按波动率倒数比例配置。这种方法的局限性在于假设风险结构长期稳定，难以适应市场状态突变（如流动性危机或政策冲击）。而 DeepSeek 的动态赋权模型引入了时变风险预算与因子有效性衰减函数，因子权重随信息系数（IC）动态调整，并受波动率敏感系数约束。

项目中，模型通过自适应窗口捕捉市场半衰期变化，在牛市中缩短窗口以响应短期信号，在震荡市中延长窗口以过滤噪声。这种动态逻辑突破了风险平价模型对历史数据的静态依赖，更贴合实际市场中风险源的时变特性。

图4: DeepSeek 动态赋权与经典模型对比

对比维度	经典风险平价模型	DeepSeek动态赋权模型
逻辑核心	追求资产间风险贡献均衡，基于历史波动率与相关性静态分配权重，假设风险结构长期稳定	以因子有效性（IC值）为核心驱动，结合时变风险预算与市场状态敏感参数动态调整权重
局限	依赖静态历史数据，难以应对市场突变（如流动性危机、政策冲击），极端场景下风险分散失效	动态调整依赖高频数据质量，计算复杂度高，需辅助工具解释非线性决策逻辑
突破	无	引入市场半衰期概念与波动率敏感系数，通过IC平方加权强化高效因子，支持因子失效预警与替代
风险分散能力	稳定市场表现优异，极端场景下风险结构突变时分散效果崩溃（如2020年股债相关性反转）	动态捕捉风险源变化，极端市场回撤控制更优
收益捕捉效率	依赖长期均衡收益，对短期趋势响应滞后（如牛市初期仓位提升缓慢）	通过非线性加权与自适应窗口，强化高效因子作用，提升收益捕捉速度
回撤控制	尾部风险敏感度高，依赖历史波动率阈值	动态波动率阈值+硬性仓位约束，叠加多因子协同验证过滤噪声信号
计算复杂度	低复杂度，仅需协方差矩阵求逆运算，适合中小机构部署	高复杂度，实时计算信息系数（IC）、多因子协同验证及非线性优化，依赖高性能算力支持

资料来源：Wind, 国信证券经济研究所整理

问题 2：DeepSeek 的动态赋权模型与传统多因子框架相比，在资产配置中有何核心优势？

DeepSeek 动态赋权模型相较于传统多因子框架的核心优势体现在非线性关系建模与失效因子识别能力上。传统框架通常依赖线性加权（如等权或固定 IC 加权），无法处理因子间交互效应（如宏观因子与情绪因子的协同或冲突），且难以捕捉因子有效性的时变性（如技术指标在牛市中有效而在熊市中失效）。DeepSeek 通过多头潜在注意力（MLA）与交互特征工程，显式建模因子间的非线性关系，例如生成“景气度×趋势”的二阶特征，并通过注意力门控机制动态分配权重。此外，模型内置因子失效拐点检测功能，例如当因子 IC 值持续低于阈值时自动降低其权重，避免传统框架因因子钝化导致的策略漂移。项目中 2020-2024 年回测数据显示，动态赋权模型夏普比率较基准提升 46%，最大回撤压缩至 12%，验证了其对市场结构突变的适应能力。

问题 3：在财报情感分析中，DeepSeek R1 通过“情感语调分数”识别财务瑕疵，而传统方法（如 Benford 定律）依赖数值异常检测。这两种范式在误报率（False Positive）和隐蔽性造假识别能力上有何差异？

DeepSeek 通过情感语调分数识别财务瑕疵，其核心优势在于捕捉文本中的情绪矛盾、模糊表述等非结构化风险信号。这类信号可能更适用于识别隐蔽性造假（如管理层通过复杂叙事掩盖财务问题），因为即使数值数据被精心调整（如虚增利润），文本中的异常情感倾向（如过度乐观修饰或逻辑矛盾）仍可能暴露风险。然而，情感分析的误报率可能较高，尤其是在行业术语或常规风险提示较多的场景中（如科创板企业频繁提及技术不确定性），模型可能将中性表述误判为负面信号。相比之下，Benford 定律依赖数值分布异常检测（如首位数字偏离自然分

布），对传统造假手段（如虚构流水）敏感，但在面对隐蔽性造假（如利用会计准则漏洞虚增无形资产）时，若造假数据人为符合数值分布规律，其检测能力会显著下降。同时，Benford 定律的误报率受行业特性影响较大，例如零售业流水天然符合 Benford 分布，而金融衍生品交易数据可能偏离，导致误判。总体而言，情感分析长于捕捉文本隐含风险，但对语义噪声敏感；数值分析对传统造假有效，但对高隐蔽性手段存在盲区。

问题 4：基于 Zero-Shot 的财报文本分析在技术术语密集场景（如生物医药专利描述）中是否会失效？是否需要结合领域预训练提升专业性？

在技术术语密集场景中，基于 Zero-Shot 的财报文本分析可能部分失效。通用模型（如 DeepSeek R1）虽能捕捉文本情感倾向，但其对专业术语和行业特定表达的理解存在盲区。例如，生物医药财报中常见的“基因编辑技术临床转化率”“III 期临床试验”等术语，可能被模型误判为负面信号，尤其是当技术性风险提示（如“试验存在不确定性”）与财务风险无直接关联时，易导致误报率上升。

为提升专业性，未来可结合领域预训练与混合监督学习。以生物医药领域为例，可以在领域内科学文献、专利文本及历史财报数据上对模型进行增量预训练，强化其对专业术语上下文和行业逻辑的理解。同时，通过 Prompt 工程嵌入领域规则，例如明确技术术语的中性化处理（如“临床试验阶段描述不直接关联现金流压力”），避免语义误判。此外，还可以引入少量专家标注数据（如标记专利价值与财务健康度的关联性），对模型进行微调，使其能够识别技术密集文本中的隐藏风险信号。理论上 Zero-Shot 扩展路径（如嵌入监管规则库）可进一步适配，从而在保持通用性的同时，增强对技术术语密集场景的适应能力。

风险提示

AI 幻象风险

生成式模型在缺乏充分数据锚点时可能虚构虚假关联逻辑，例如错误构建宏观指标与资产价格的因果关系，或生成缺乏实证支持的配置建议，导致决策依据失真。

数据异化风险

宏观指标统计口径调整、行业分类标准重构或财务数据披露规则变更，可能破坏模型特征体系的逻辑一致性，例如新经济行业划分模糊化导致景气度判定偏差，需依赖动态校准机制应对。

监管规则适配风险

AI 生成的决策逻辑链条存在“黑箱化”特征，与金融监管要求的透明度标准存在冲突，例如无法完整回溯权重调仓的微观决策依据，可能面临合规性审查压力。

人机协同失效风险

自动化决策与人工干预的权责边界模糊化，可能在市场剧烈波动时出现风控响应延迟或操作冲突，例如 Agent 的强制平仓指令与基金经理主观判断产生对立，需明确权限。

策略同质化共振风险

AI 模型广泛采用相似训练框架与因子库，可能导致市场参与者的策略趋同，加剧资产价格波动与流动性突变，引发系统性风险。

免责声明

分析师声明

作者保证报告所采用的数据均来自合规渠道；分析逻辑基于作者的职业理解，通过合理判断并得出结论，力求独立、客观、公正，结论不受任何第三方的授意或影响；作者在过去、现在或未来未就其研究报告所提供的具体建议或所表述的意见直接或间接收取任何报酬，特此声明。

国信证券投资评级

投资评级标准	类别	级别	说明
报告中投资建议所涉及的评级（如有）分为股票评级和行业评级（另有说明的除外）。评级标准为报告发布日后 6 到 12 个月内的相对市场表现，也即报告发布日后的 6 到 12 个月内公司股价（或行业指数）相对同期相关证券市场代表性指数的涨跌幅作为基准。A 股市场以沪深 300 指数（000300.SH）作为基准；新三板市场以三板成指（899001.CSI）为基准；香港市场以恒生指数（HSI.HI）作为基准；美国市场以标普 500 指数（SPX.GI）或纳斯达克指数（IXIC.GI）为基准。	股票 投资评级	优于大市	股价表现优于市场代表性指数 10%以上
		中性	股价表现介于市场代表性指数 $\pm 10\%$ 之间
		弱于大市	股价表现弱于市场代表性指数 10%以上
		无评级	股价与市场代表性指数相比无明确观点
	行业 投资评级	优于大市	行业指数表现优于市场代表性指数 10%以上
		中性	行业指数表现介于市场代表性指数 $\pm 10\%$ 之间
		弱于大市	行业指数表现弱于市场代表性指数 10%以上

重要声明

本报告由国信证券股份有限公司（已具备中国证监会许可的证券投资咨询业务资格）制作；报告版权归国信证券股份有限公司（以下简称“我公司”）所有。本报告仅供我公司客户使用，本公司不会因接收人收到本报告而视其为客户。未经书面许可，任何机构和个人不得以任何形式使用、复制或传播。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以我公司向客户发布的本报告完整版本为准。

本报告基于已公开的资料或信息撰写，但我公司不保证该资料及信息的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映我公司于本报告公开发布当日的判断，在不同时期，我公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。我公司不保证本报告所含信息及资料处于最新状态；我公司可能随时补充、更新和修订有关信息及资料，投资者应当自行关注相关更新和修订内容。我公司或关联机构可能会持有本报告中所提到的公司所发行的证券并进行交易，还可能为这些公司提供或争取提供投资银行、财务顾问或金融产品等相关服务。本公司的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中所意见或建议不一致的投资决策。

本报告仅供参考之用，不构成出售或购买证券或其他投资标的的要约或邀请。在任何情况下，本报告中的信息和意见均不构成对任何个人的投资建议。任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。投资者应结合自己的投资目标和财务状况自行判断是否采用本报告所载内容和信息并自行承担风险，我公司及雇员对投资者使用本报告及其内容而造成的一切后果不承担任何法律责任。

证券投资咨询业务的说明

本公司具备中国证监会核准的证券投资咨询业务资格。证券投资咨询，是指从事证券投资咨询业务的机构及其投资咨询人员以下列形式为证券投资人或者客户提供证券投资分析、预测或者建议等直接或者间接有偿咨询服务的活动：接受投资人或者客户委托，提供证券投资咨询服务；举办有关证券投资咨询的讲座、报告会、分析会等；在报刊上发表证券投资咨询的文章、评论、报告，以及通过电台、电视台等公众传播媒体提供证券投资咨询服务；通过电话、传真、电脑网络等电信设备系统，提供证券投资咨询服务；中国证监会认定的其他形式。

发布证券研究报告是证券投资咨询业务的一种基本形式，指证券公司、证券投资咨询机构对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向客户发布的行为。

国信证券经济研究所

深圳

深圳市福田区福华一路 125 号国信金融大厦 36 层

邮编：518046 总机：0755-82130833

上海

上海浦东民生路 1199 弄证大五道口广场 1 号楼 12 层

邮编：200135

北京

北京西城区金融大街兴盛街 6 号国信证券 9 层

邮编：100032