

上证 50ETF 期权 风控智能体

金融 AI 智能体行业场景落地方案

· option-vol-risk-agent V2

方案方向：金融 AI 智能体行业场景落地

方案载体：期权波动率风控工作台

文档版本：V1.0

编制日期：2026 年 10 月 11 日

目 录

1. 方案概述.....	4
2. 业务背景与场景痛点.....	4
2.1 业务大背景.....	4
2.2 为什么单合约持仓不够用.....	4
2.3 痛点汇总.....	5
3. 核心方案与智能体架构.....	6
3.1 四层架构.....	6
4. 技术选型与关键公式.....	7
4.1 定价模型：为什么选 Black-Scholes	7
4.2 隐含波动率反解：从价格倒推波动率.....	7
4.3 希腊字母：风险敞口的度量衡.....	8
Delta (δ)：标的价格敏感度	8
Gamma (Γ)：Delta 的变化速度	8
Vega (v)：波动率敏感度	8
Theta (Θ)：时间衰减.....	8
4.4 SSVI 波动率曲面拟合	8
Raw SVI（单期限切片）	8
SSVI（跨期限曲面）与套利检验	9
4.5 风险规则与分位门槛.....	9

4.6 检索增强知识库..... 9

4.7 模型调用与输出校验..... 10

5. 功能详解..... 11

5.1 行情数据..... 11

5.2 市场监测..... 11

5.3 持仓风控..... 12

5.4 压力测试..... 12

5.5 情景设置与归因..... 13

5.6 风险预警..... 13

6. 商业可行性论证..... 14

6.1 目标客户..... 14

6.2 为什么买单与如何收费..... 14

7. 场景适配度分析..... 14

8. 落地路径与结语..... 14

1. 方案概述

本方案面向金融 AI 智能体行业场景落地方向，以上证 50ETF 期权日终风控智能体为载体，提出并实现了一套可运行、可审计、可交付的 AI 智能体落地方案。系统覆盖期权行情数据构建、市场波动率监测、持仓压力测试与风险预警核查四个业务环节，在真实历史数据（2015 年 2 月 10 日至 2026 年 3 月 26 日，共 2,701 个交易日、306,480 条合约日记录）上完成了端到端验证。

方案的核心主张是：金融场景的 AI 智能体落地，不在于让大模型替代风控判断，而在于让大模型成为可审计风控流程中的解释与编排组件。数值与风险等级完全由本地规则引擎计算，模型只在证据齐备后进场解释，输出经过引用校验且不能修改任何数值与等级。

2. 业务背景与场景痛点

2.1 业务大背景

2026 年 9 月 10 日《期货公司监督管理办法》修订通过，2027 年 1 月 1 日起实行，做市与衍生品业务回归母公司。这一政策变化将显著增加期货公司风控条线的工作量。期权的价格只被三个东西推动：标的价格、时间、隐含波动率。标的价格和时间决定了风控需要对衍生品进行独立的估值建模——算出的数要和业务部门的估值偏差不超过 5%。隐含波动率则有一套完整的监测体系，主流模型是 Heston 和 SVI，本项目采用后者。

2.2 为什么单合约持仓不够用

期权持仓的风险至少有三个来源：标的价格方向（Delta）、波动率整体水平（Vega）、以及波动率曲面的形状变化（偏度、曲率）。前两个传统持仓表能覆盖，但第三个不行。举例子：持有大量虚值看跌和少量虚值看涨，从单合约看净 Vega 接近零，看起来波动率风险已对冲；但实际是在做空偏度——一旦市场恐慌，虚值看跌的隐含波动率飙升幅度远超虚值看涨，组合瞬间爆亏，单合约持仓表对此毫无预警。

期权隐含波动率曲面与风险观察

——从曲面形态、偏斜走势、期限结构到异常分级的多维风险监测——

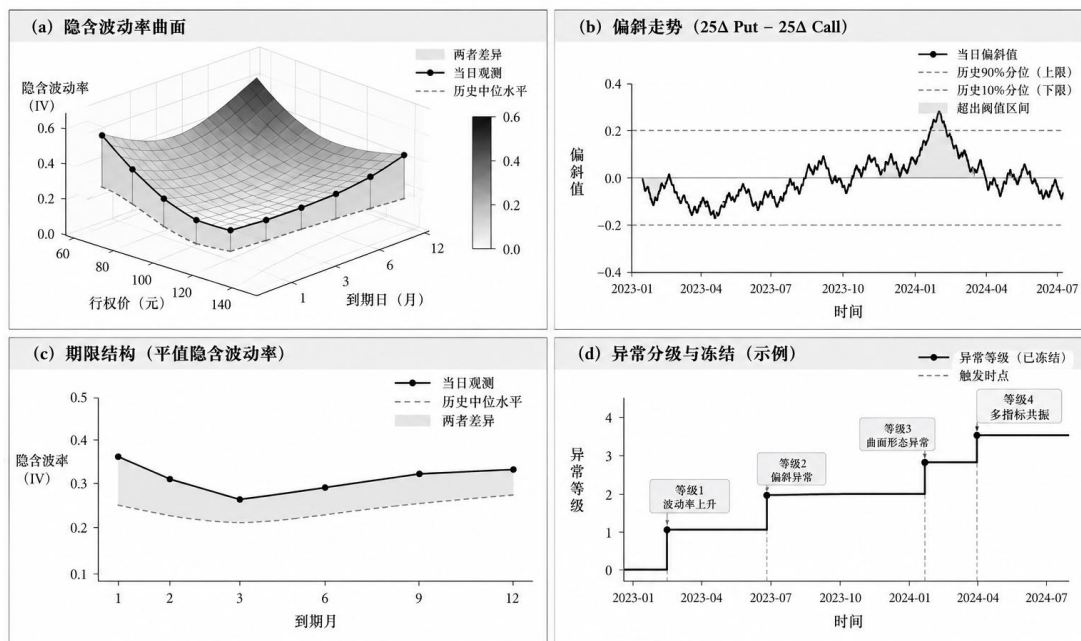


图1 波动率曲面三重风险：偏度、期限结构、曲率

2.3 痛点汇总

痛点	具体表现	本系统对应能力
口径黑箱	供应商 IV 不可复算，监管问询无法举证	独立 BS 定价+IV 反解，可下钻至源文件行号
异常靠盘感	偏斜/期限异常无系统化门槛	研究分位规则+事件冻结
损失定位粗	只给总盈亏，不知该动哪条腿	按到期月/合约腿归因
留痕散落	核查在即时通讯里，举证困难	五阶段状态机+审计链
模型不可控	大模型直接给结论合规不可接受	输出校验+引用白名单

3. 核心方案与智能体架构

3.1 四层架构

系统自下而上分为四层：数据层负责五类原始表的显式导入与独立反解；计算层完成定价、希腊字母与规则风险扫描；智能体层包括五阶段调查编排、八个只读核查工具与检索增强知识库；应用层为本地网页工作台加 AI 对话面板。

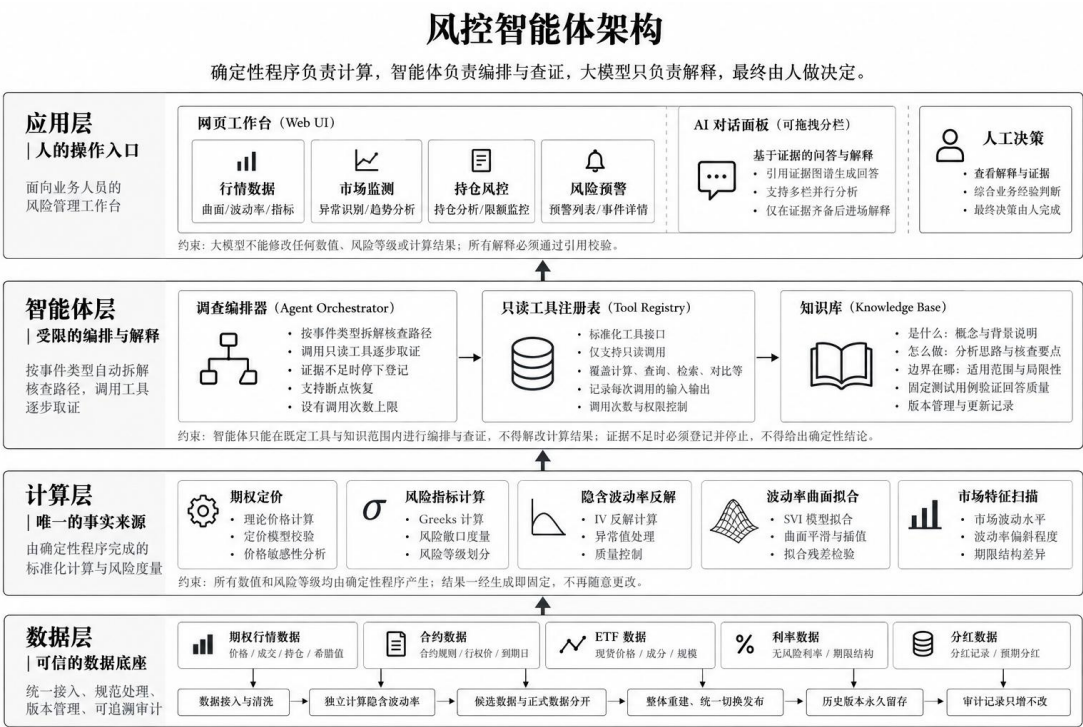


图 2 智能体四层架构

4. 技术选型与关键公式

4.1 定价模型：为什么选 Black-Scholes

期权定价模型的选择取决于三个因素：欧式/美式、是否有解析解、参数是否可解释。上证 50ETF 期权是欧式的，而 Black-Scholes 模型对欧式期权有精确的闭式解——这意味着定价速度极快，且每个中间量都有明确的金融含义。对于含路径依赖的结构（如雪球），则用 CRR 二叉树逐步回推。

$$C = S \cdot N(d_1) - K \cdot e^{-rT} \cdot N(d_2)$$

认购期权价格 = 标的现价 $\times N(d_1)$ - 行权价 $\times$ 折现因子 $\times N(d_2)$

$$d_{1,2} = \frac{\ln(S/K) + (r \pm \sigma^2/2)T}{\sigma\sqrt{T}}$$

$d_{1,2}$ 由标的价格、行权价、利率、波动率和到期时间共同决定

其中 S 是标的现价（经分红调整）， K 是行权价， r 是无风险利率（连续复利）， σ 是年化波动率， T 是到期时间（ACT/365 天计数）。分红以现值扣除法处理： $S_{adj} = S - PV(\text{分红})$ 。

技术说明 选型理由：Heston 模型虽更贴近现实，但需求解偏微分方程或特征函数逆变换，参数校准困难。对于日终盘后场景，BS 的精度已足够，速度和可解释性优势更大。

4.2 隐含波动率反解：从价格倒推波动率

业务方给出期权价格，如何反推市场对未来波动的预期？这就是隐含波动率反解问题：给定 C_{mkt} ，找 σ 使得 $BS(\sigma) = C_{mkt}$ 。

$$\sigma_{n+1} = \sigma_n - \frac{C(\sigma_n) - C_{mkt}}{v(\sigma_n)}$$

牛顿迭代法（本项目实际采用更稳定的 Brentq 方法）

本项目采用 `scipy.optimize.brentq`（Brent 方法）而非牛顿法。原因：牛顿法需要计算 Vega 作为导数，当期权深度虚值或临近到期时 Vega 趋零，迭代发散；Brent 方法是区间收缩法，不需要导数，只要给一个包含根的区间就能保证收敛。精度参数：最大迭代 100 次、根容差 10^{-12} 、价格核对容差 10^{-6} 。

技术说明 Brent 方法结合了二分法的稳定性和逆二次插值的速度，是 scipy 推荐的标准求根方法。它保证在给定区间内一定收敛，而牛顿法可能跳到区间外。

4.3 希腊字母：风险敞口的度量衡

Delta (δ)：标的价格敏感度

$$\Delta = \partial C / \partial S = N(d_1)$$

标的每涨 1 元，认购期权价值变动 $N(d_1)$ 元

净 Delta 6,215.8 意味着标的每涨 1 元组合价值变动约 6,216 元——极其看涨的持仓结构。

Gamma (Γ)：Delta 的变化速度

$$\Gamma = \partial^2 C / \partial S^2 = \phi(d_1) / (S \cdot \sigma \cdot \sqrt{T})$$

标的价格变动 1 元，Delta 变动多少

净 Gamma 968,558.7 说明 Delta 极不稳定，通常是持有大量临近到期的平值期权。

Vega (v)：波动率敏感度

$$v = S \cdot \phi(d_1) \cdot \sqrt{T}$$

波动率每升 1 个百分点，期权价值变动 v 元

净 Vega 68.3 元说明波动率上升对组合有利。

Theta (Θ)：时间衰减

$$\Theta = -S \cdot \phi(d_1) \cdot \sigma / (2\sqrt{T}) - r \cdot K \cdot e^{-rT} \cdot N(d_2)$$

每过一天，期权价值因时间流逝而变动多少

净 Theta -15.5 元说明每天流失 15.5 元时间价值——期权买方的典型特征。

4.4 SSVI 波动率曲面拟合

单个期权只有一个 IV，但同一标的、同一天到期的期权有几十个不同行权价——这些 IV 在三维空间中构成一张曲面。曲面的形状变化才是波动率风险的核心。

Raw SVI (单期限切片)

$$w(k) = a + b \cdot [\rho \cdot (k - m) + \sqrt{((k - m)^2 + \sigma^2)}]$$

总方差 w 是对数行权价 k 的函数

其中 $k = \ln(K/F)$ 是对数行权价， a 是总方差最小值， b 控制倾斜程度， ρ 决定偏度方向， m 是拐点位置， σ 控制平滑度。五个参数含义清晰，业务人员可以直接理解和沟通。

SSVI（跨期限曲面）与套利检验

SSVI 在 Raw SVI 基础上让参数随期限变化，拼成完整曲面。系统实施三类约束校验：参数域要求（ $b \geq 0$ 、 $|\rho| < 1$ 、 $\sigma > 0$ ）、蝶式套利检验、垂直价差检验。不通过的曲面被拒绝使用。

技术说明 为什么不用局部波动率模型（Dupire）或 Heston 直接拟合？SVI 参数少（5 个 vs Dupire 需要整条密度曲线）、计算快（闭式公式 vs 偏微分方程），且 Gatheral-Jacquier(2014)证明了 SSVI 在特定条件下无静态套利。

4.5 风险规则与分位门槛

系统对三项市场指标（IV 水平、偏斜、期限差）各设置研究分位门槛。分位的含义是：当前值在历史分布中处于什么位置。

$$Q_p = \inf\{x : F_n(x) \geq p\}$$

样本分位数：最小值 x 使得至少 p 比例的历史观测不超过 x

门槛条件：至少 60 个有效观测才开始计算；窗口最多 252 个交易日。不足 60 个观测时预警列为数据待查而非强行判定。分位取线性插值法，取 5% 和 95% 作为异常上下界。单日触发不算预警，需连续 2 个以上有效日持续异常才合并为事件。

4.6 检索增强知识库

AI 助手基于确定性检索的知识库（20 个知识源、43 条回归用例）而非模型自由生成。检索采用词项重叠打分：标题命中×3 分、小节×2 分、精确短语+4 分，配合中文 2/3/4 字 n -gram 切分和 21 组同义词映射。同一问题永远命中同一条知识，结果可复现、可审计。

技术说明 为什么不用向量数据库？向量化检索语义理解更强，但结果不可复现（同一问题可能因嵌入模型版本不同而命中不同内容）。对于风控场景，可复现性和零外部依赖比语义灵活性更重要。

4.7 模型调用与输出校验

引用校验 回答中引用的证据编号必须在服务器白名单内。

数值校验 模型新增的数值（非服务器提供的）会被拒绝。

等级校验 模型不能修改风险等级（优先复核/观察/数据待查三级由规则引擎决定）。

声明校验 不能夹带正式放行、交易指令等违规表述。

任何一项不通过，系统保留本地计算依据并显示失败状态——宁可没有解释，也不给错误的解释。

5. 功能详解

5.1 行情数据

五类原始表逐项上传，字段核验、口径确认后从结算价独立反解 IV，拟合 SSVI 曲面。候选与正式分离，经交接包与六阶段管线验收后切换。

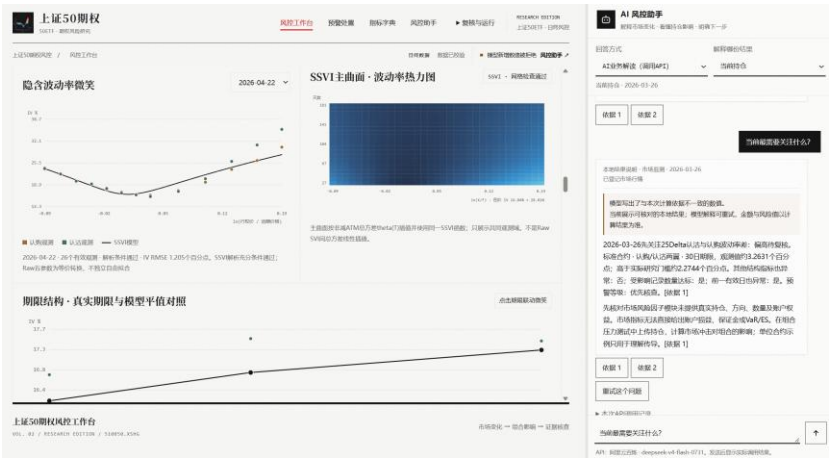


图 3 行情数据模块

5.2 市场监测

三因子监控、今日市场解读白话摘要、走势回放、微笑/期限/热力图配解读说明、AI 报告生成。



图 4 市场监测模块

5.3 持仓风控

上传工作簿后八项 KPI 一屏呈现，欧式 BS/CRR 双模型。

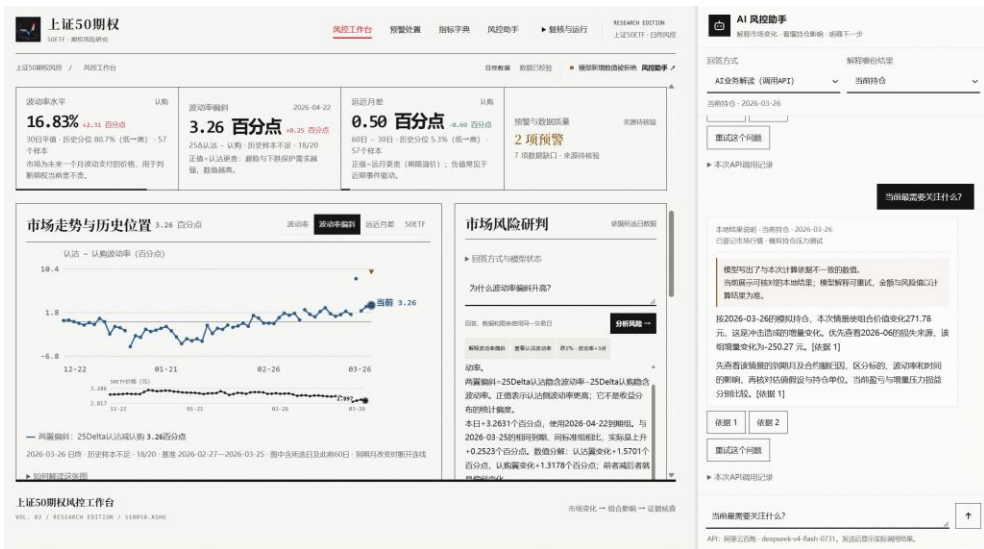


图 5 持仓风控模块

5.4 压力测试

标的×波动率情景矩阵，损失归因到到期月/合约腿，反向压测。

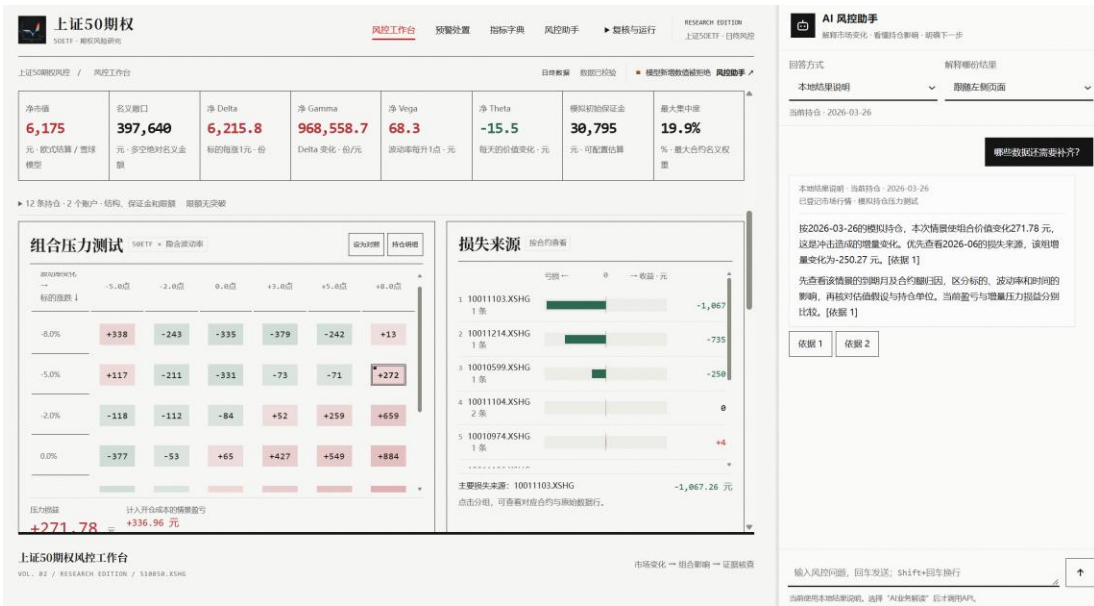


图 6 压力测试模块

5.5 情景设置与归因

预设+自定义风险因子，五种归因维度，历史情景回放与 VaR/ES 参考。



图 7 情景设置与损失来源归因

5.6 风险预警

三级分级预警队列，35 条证据引用可逐条点开，五阶段核查状态机与人工复核。



图 8 预警处置与证据链核查

6. 商业可行性论证

6.1 目标客户

分层	付费主体	核心诉求
核心层	期货公司风险管理子公司、券商衍生品部	统一口径压测、雪球估值、损失归因
扩展层	期货公司风控部、托管机构	日终监控留痕、监管举证、新人上手
机会层	私募与量化机构	独立口径复核、偏斜与期限信号

6.2 为什么买单与如何收费

合规价值：审计链只增不改。效率价值：AI 助手即时回答并附引用。风险价值：系统化门槛减少漏报。自主可控：从零重建不锁供应商。收费：软件授权/私有化部署/数据与知识服务/场景定制。

7. 场景适配度分析

判据	表现	含义
证据密集	每条预警绑定观测值/门槛/源行/证据编号	有料可用
流程可拆解	核查路径按事件家族分支	编排有骨架
判断有规则边界	数值与等级由冻结规则计算	模型约束在安全区
出错代价高	风控误判直接影响处置	必须可审计
高频日常	日终监控每日运行	提效可累积
长尾解释需求	大量口径与流程追问	知识库价值放大

8. 落地路径与结语

阶段	周期	内容	验收标志
试点验证	1-3 月	核心客户从零重建	数据独立运行
产品化	3-6 月	多品种扩展、部署包装	私有化部署脚本

阶段	周期	内容	验收标志
规模推广	6-12 月	MCP 接口、订阅服务	首批客户续约

金融 AI 智能体的落地难点不在模型能力，而在业务边界、证据链与人机职责的工程化。本方案把口径自主、规则判定、工具编排、知识落地与受约束解释整合为一个已验证的闭环：系统算数，工具查证，模型解释，人工决定。