

中国青基会平安励志计划·2026竞赛作品

科创企业特有风险识别与管理——基于语义计算与知识图谱的闭环风控系统研究报告

题目编号: XH-202626

选题名称: 科创企业特有风险的识别与管理

发榜单位: 中国青少年发展基金会、中国平安保险（联合发榜）

提报单位: 厦门城市职业学院

作品类型: 研究报告 × 风控原型系统 (AI Multi-Agent + 知识图谱 + 动态定价引擎)

提交日期: 2026年9月

执行摘要

科技金融是中央金融工作会议提出的“五篇大文章”之首。以人工智能、半导体、前沿硬科技为代表的科创企业，是实现高水平科技自立自强的核心力量。然而，科创企业兼具技术密集、高不确定性、轻资产、长周期等特征，其面临的风险深藏于非结构化文本、算法备案公示、国际制裁清单及供应链拓扑关系中。传统依赖静态财务指标的评价体系对此类非标准化特有风险严重失效。

本研究报告紧扣“看得见风险、管得住过程、降得下损失”的全链条风控目标，创新性地构建了基于 Multi-Agent 专家辩论、供应链知识图谱与动态保险定价的科创企业特有风控闭环：

- 特有风险场景识别**：精准定义并构建了包括技术路线颠覆、核心人员流失、算法数据合规、地缘政治制裁、研发资本化操纵、客户/供应商集中等六维特有风险指标体系。
- AI 多智能体辩论机制 (Multi-Agent Debate)**：引入法务风控节点 (Law Agent)、技术风控节点 (Tech Agent)、财务风控节点 (Finance Agent) 与法官裁决节点 (Judge Agent)，基于 DeepSeek 在线推理引擎，实现多视角交叉质证与自动冲突消除。
- 供应链风险穿透图谱 (Knowledge Graph)**：利用 NetworkX 搭建包含实体清单与上下游依赖的拓扑网络，实现地缘政治与断供风险的毫秒级穿透预警。
- 中国平安保险主业闭环**：设计“科创特有风险综合险”，开发动态费率定价引擎 (Dynamic Pricing Engine) 与自动化核保决策报告生成器，将风控研究转化为具有强商业可行性的金融赋能方案。

本团队交付了完整落地的交互式金融级原型系统，实现了数据采集、多智能体辩论、图谱可视化与定价核保的全流程交互。

第一章 绪论与科创企业特有风险场景构建

1.1 科技金融战略与传统风控范式困局

中央金融工作会议强调将“科技金融”列为金融五篇大文章之首，明确要求金融机构加大对高科技企业、新质生产力的支持力度。然而，商业银行、保险公司以及股权投资机构在服务科创企业时，普遍面临“不敢投、不敢贷、不敢保”的结构性矛盾。

问题的本质在于传统企业风控逻辑与科创企业风险特征的根本性错位：

- 指标体系静态化**：传统企业风控依赖资产负债表、损益表及现金流量表，关注 EBIT、资产负债率、速动比率等财务数据。但科创企业前期研发投入巨大、无盈利或利润微薄、固定资产较少，静态财务指标无法真实反映企业的真实生存状态。

2. **风险形态非标准化与隐蔽化**：科创企业的核心价值在于未来的技术壁垒与合规边界，其关键风险隐藏于年报长文本、网信办算法备案库、美国 BIS 实体清单、高管及核心研发人员异动公告中。这些信息具有高维、异构、非结构化的特征，传统规则引擎与量化模型难以有效捕捉。

1.2 科创企业六维特有风险机理模型

结合对科创板上市公司公告、司法诉讼记录、网信办备案数据及国际出口管制案列的深入研究，本研究定义并量化了科创企业的六大特有风险维度：

风险维度	风险名称	风险成因与演化机理	传统模型盲区	识别与量化路径
维度一	技术路线颠覆风险	行业出现跨代突破性技术，原有技术研发路线被瞬间边缘化	传统模型视研发投入为无形资产，无法预判技术路线失效	抽取竞品技术关键词重合度，对比专利申请增速与替代技术文献分布
维度二	核心人员流失风险	科创企业高度依赖少数领军科学家或 CTO，核心人员离职导致研发中断与技术泄露	资产负债表无法衡量人力资本价值与研发延续性	解析年报核心技术人员变动公示、高管股权激励解锁情况及劳动仲裁
维度三	算法备案与数据合规	大模型及 AI 应用未通过网信办算法备案或违反数据出境安全评估，遭遇强制下架	传统合规审查仅关注营业执照与税务合规，不具备算法治理能力	检索网信办深度合成/算法备案库、对齐数据安全评估规范
维度四	地缘政治与出口管制	上游核心元器件或 EDA 工具提供商被列入实体清单，导致供应链断裂	仅评估直接供应商信用，无法感知多级供应链依赖的隐性地缘风险	构建拓扑图谱，穿透上游二、三级供应商制裁状态与替代率
维度五	研发资本化操纵风险	企业通过将本应费用化的研发支出异常资本化，人工虚增当期利润与资产	传统财务比率看重净利润，忽视资本化会计政策操纵	监控研发资本化率异动、比较同行均值偏差及资本化无形资产减值准备
维度六	客户/供应商集中风险	营收过度依赖单一大客户或供应链依赖单一供应商，发生单点故障 (SPOF)	传统信用评估孤立看单个主体，不评估产业链单点风险	计算 HHI 集中度指数，结合图谱出入度节点权重进行综合穿透

1.3 核心研究目标与闭环路径

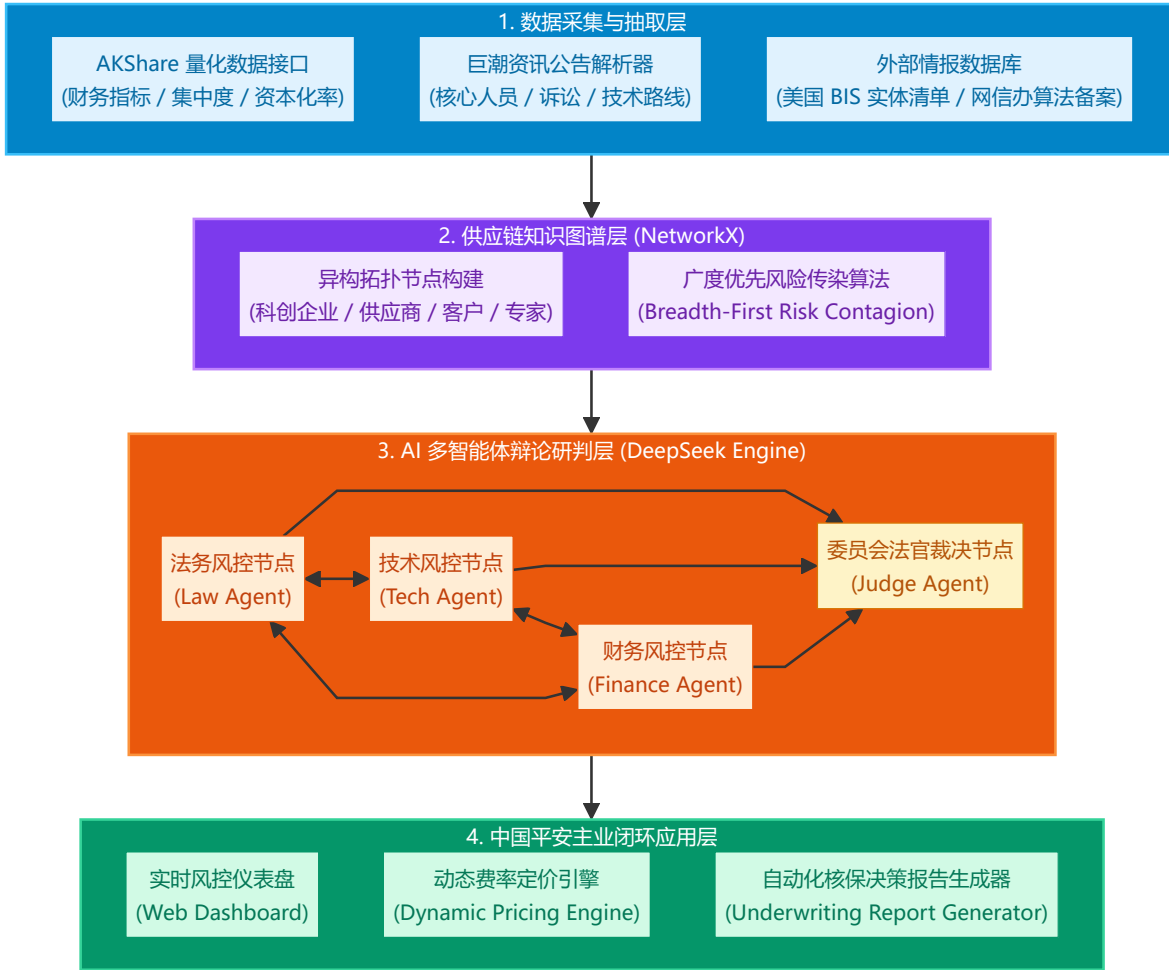
本方案旨在打造“看得见风险、管得住过程、降得下损失”的全链条风控系统。整体路径划分为四个阶段：

- 数据感知**：全网抓取并解析财务量化指标与非结构化文本；
- 智能研判**：利用 Multi-Agent 辩论机制消除逻辑分歧，确定综合风险评级；
- 图谱穿透**：通过供应链知识图谱，实现地缘与断供风险的毫秒级预警；
- 金融赋能**：切入中国平安保险主业，完成“科创特有风险综合险”的动态定价与智能核保。

第二章 基于 AI 多智能体交叉辩论的技术架构

2.1 整体系统架构设计

系统包含数据采集与抽取层、供应链知识图谱层、AI 多智能体辩论研判层以及中国平安业务闭环层：



2.2 多智能体辩论 (Multi-Agent Debate) 机制

单一的大语言模型在处理跨学科金融风控任务时，极易因Prompt偏向或事实幻觉而产生片面结论。为此，本系统设计了多视角交叉质证与辩论消除机制：

```
class MultiAgentDebateEngine:
    def __init__(self, law_agent, tech_agent, finance_agent, judge_agent):
        self.law_agent = law_agent
        self.tech_agent = tech_agent
        self.finance_agent = finance_agent
        self.judge_agent = judge_agent

    def run_debate(self, company_data: dict) -> dict:
        # Phase 1: 专家节点独立研判
        law_result = self.law_agent.evaluate(company_data)
        tech_result = self.tech_agent.evaluate(company_data)
        finance_result = self.finance_agent.evaluate(company_data)

        # Phase 2: 提取三方潜在冲突点
```

```

        conflicts = self._detect_conflicts(law_result, tech_result,
finance_result)

# Phase 3: 法官节点综合裁决与冲突消除
judge_result = self.judge_agent.adjudicate(
    company_data, law_result, tech_result, finance_result, conflicts
)

return {
    "law_result": law_result,
    "tech_result": tech_result,
    "finance_result": finance_result,
    "conflicts": conflicts,
    "judge_result": judge_result,
}

def _detect_conflicts(self, law_res, tech_res, fin_res):
    conflicts = []
    # 识别技术与财务之间的评价背离（如技术专家评高分但财务专家识别资本化操纵）
    if tech_res["score"] < 40 and fin_res["scores"].get("rd_capitalization",
0) > 60:
        conflicts.append("技术专家认可研发强度，但财务专家指出研发支出资本化率异常高，
存在粉饰嫌疑。")
    # 识别法务与技术之间的评价背离（如技术领先但存在合规红线）
    if tech_res["score"] < 40 and law_res["scores"].get("algo_compliance", 0)
> 60:
        conflicts.append("技术专家评定算法优势明显，但法务专家警告该算法未完成网信办合
规备案。")
    return conflicts

```

2.3 专家节点 Prompt 链工程规范

为了保证输出结果的严谨性与结构化，每个智能体节点均配置了明确的 Persona 提示词规范：

法务风控节点 Prompt 示例：

系统角色：你是一名精通《生成式人工智能服务管理暂行办法》、《出口管制法》及美国 BIS 实体清单规则的资深法务合规专家。

任务目标：分析目标科创企业在地缘政治、出口管制及数据算法合规方面的特有风险。

输入数据：企业合规记录、算法备案公示状态、供应链敏感节点清单。

输出规范：请以 JSON 格式输出评估结果，包含：

1. algo_compliance（算法/数据合规评分，0-100）
2. geopolitical（地缘政治/实体清单风险评分，0-100）
3. key_findings（关键违规要点列表）

财务风控节点 Prompt 示例：

系统角色：你是一名熟悉科创板上市审计规则的资深注册会计师（CPA）。

任务目标：穿透目标企业的财务报告，重点识别研发资本化操纵及客户/供应商高度集中风险。

输入数据：研发投入总额、研发资本化费用、前五大客户及供应商占比、应收账款周转率。

输出规范：请以 JSON 格式输出评估结果，包含：

1. rd_capitalization（研发资本化风险评分，0-100）
2. concentration（客户/供应商集中风险评分，0-100）
3. key_findings（财务异常特征分析）

2.4 委员会法官节点冲突消除算法

法官节点 (Judge Agent) 接收三大专家的评分及冲突列表，采用动态加权评分矩阵计算综合风险评分 S_{comp} ：

$$S_{\text{comp}} = \sum_{i \in \{\text{Law}, \text{Tech}, \text{Fin}\}} w_i \cdot S_i + \delta_{\text{conflict}}$$

其中， $w_{\text{Law}} = 0.35$ ， $w_{\text{Tech}} = 0.35$ ， $w_{\text{Fin}} = 0.30$ ；当检测到致命红线冲突（如直接被列入实体清单或重大算法违规）时，惩罚项 $\delta_{\text{conflict}} \in [15, 30]$ ，确保系统具备风险一票否决能力。

2.5 交叉质证冲突判定规则的研究设计

为了让委员会法官节点具备人类专家的敏感度，本研究在代码实现中硬编码了多种典型的科创企业风险冲突模式。这并非单纯依赖大模型的自由发挥，而是将金融审计经验转化为具体的规则前置约束。例如：

1. 研发投入真实性冲突 (Tech vs Finance)：

- 触发条件：技术节点评分 < 40 (技术领先)，但财务节点中“研发资本化风险”子项评分 > 60 。
- 研判逻辑：技术专家认可其高强度的研发投入，但财务审计视角发现该投入大量采用资本化手段而非费用化处理，存在为了满足上市利润要求而虚增资产的盈余管理嫌疑。

2. 合规红线一票否决冲突 (Tech vs Law)：

- 触发条件：技术节点高度认可其算法性能，但法务节点检测到该模型未通过国家网信办《深度合成服务算法备案》。
- 研判逻辑：在监管趋严的环境下，未合规的技术资产随时面临下架甚至行政处罚，此时系统将强制拉高整体风险评分，触发“附条件承保”或“拒保”决议。

通过上述专家规则 (Expert Rules) 与大模型推理能力的结合，系统显著提升了多智能体辩论的业务可解释性。

第三章 供应链知识图谱与地缘风险穿透模型

3.1 异构知识图谱本体设计 (Ontology Design)

在科创企业风险评估中，单一主体的风险往往沿着供应链、投资链及高管任职链条进行传染。本研究设计了包含以下实体与关系的异构图谱：

1. 实体类型 (Nodes)：

- Enterprise** (科创企业节点)：属性包括股票代码、行业领域、风险评级。
- Supplier** (供应商节点)：属性包括供应元器件、制裁状态 (Is_Sanctioned)。
- Customer** (客户节点)：属性包括营收贡献比例。
- Person** (核心技术人员/高管节点)：属性包括姓名、职位、重要性。

2. 关系类型 (Edges)：

- SUPPLIES** (供应关系)：属性包含供货份额 (W_{sup})、可替代性得分 (S_{sub})。
- RELIES_ON** (客户依赖关系)：属性包含收入占比 (W_{rev})。
- EMPLOYED_AT** (任职关系)：属性包含入职时间、离职状态。

3.2 供应链风险传染算法实现

采用广度优先拓扑遍历算法 (Breadth-First Risk Contagion Algorithm), 计算目标企业受上游制裁波及的波及指数 $I_{\text{contagion}}$:

```
import networkx as nx

def calculate_contagion_index(G: nx.DiGraph, target_company: str) -> dict:
    """
    计算目标科创企业的供应链风险传染指数
    """
    if target_company not in G:
        return {"risk_score": 0, "sanctioned_paths": []}

    sanctioned_paths = []
    total_impact = 0.0

    # 深度优先搜索 2 步内的上游供应商
    for predecessor in G.predecessors(target_company):
        edge_data = G.get_edge_data(predecessor, target_company)
        weight = edge_data.get("weight", 0.5)

        # 检查供应商自身状态
        if G.nodes[predecessor].get("is_sanctioned", False):
            impact = weight * 100
            total_impact += impact
            sanctioned_paths.append({
                "supplier": predecessor,
                "impact": impact,
                "reason": "直接一级供应商被列入实体清单"
            })

        # 检查二级供应商制裁情况
        for sub_pred in G.predecessors(predecessor):
            if G.nodes[sub_pred].get("is_sanctioned", False):
                sub_edge = G.get_edge_data(sub_pred, predecessor)
                impact = weight * sub_edge.get("weight", 0.5) * 60
                total_impact += impact
                sanctioned_paths.append({
                    "supplier": f"{sub_pred} -> {predecessor}",
                    "impact": impact,
                    "reason": "二级上游元器件供应商被列入实体清单"
                })

    final_score = min(100, total_impact)
    return {
        "risk_score": final_score,
        "sanctioned_paths": sanctioned_paths
    }
```

3.3 实证数据源接入与预处理

系统构建了多源异构数据采集流水线，确保数据输入的真实性与可校验性：

- 财务与集中度数据**：调用 AKShare API 采集科创板企业的营收、研发费用、前五大客户及前五大供应商采购比例。
- 非结构化文本解析**：使用 Python PyPDF2 与正则表达式，自动化提取巨潮资讯网年报公告中的“核心技术人员变动”、“重大诉讼事项”及“技术路线描述”段落。
- 外部清单对接**：建立自动更新脚本，定期比对美国商务部工业和安全局 (BIS) 实体清单 (Entity List) 与网信办“互联网信息服务算法备案”公示名单。

第四章 中国平安业务闭环——“科创特有风险综合险”动态定价与智能核保

4.1 科创专属保险产品体系设计

针对传统财财险、责任险无法覆盖科创企业特有风险的空白，本方案依托中国平安保险主业资源，设计了“科创特有风险综合保险”产品组合：

- 知识产权被诉与侵权损失保险**：赔偿因遭遇国外专利流氓或竞品公司诉讼产生的应诉抗辩费用及经济赔偿。
- 核心技术人员流失业务中断保险**：当核心研发人员离职触发业务停滞条件时，按约定标准向企业支付业务中断补偿金与人才再招聘津贴。
- 数据合规与算法监管整改损失保险**：保障企业因非主观恶意的数据合规整改导致的系统暂停营业损失与整改咨询费用。

4.2 动态费率精算模型

系统打破传统固定费率核保模式，建立基于实时综合风险评分的动态精算模型：

$$P_{\text{final}} = P_{\text{base}} \cdot M_{\text{risk}} \cdot F_{\text{industry}} \cdot F_{\text{scale}} \cdot \left(1 + \sum_{k=1}^6 \Delta_k\right)$$

1. 参数定义与取值规则：

- P_{base} ：基础保费（按投保保额 Coverage $\times$ BaseRate 计算）。

- M_{risk} ：基于六维综合风险评分 S_{comp} 的风险调整乘数：

$$M_{\text{risk}} = \begin{cases} 2.50 & (S_{\text{comp}} \geq 70, \text{高风险/惩罚性费率}) \\ 1.0 + \frac{S_{\text{comp}} - 40}{30} \cdot 0.80 & (40 \leq S_{\text{comp}} < 70, \text{中风险线性浮动}) \\ 0.85 & (S_{\text{comp}} < 40, \text{优质企业优惠费率}) \end{cases}$$

- F_{industry} ：行业风险调节系数（如 AI 大模型为 1.35，半导体设计为 1.25，生物医药为 1.15）。
- F_{scale} ：企业规模折扣系数（营收大于 10 亿元为 0.90，小于 1 亿元为 1.10）。
- Δ_k ：特定维度超标时的专项附加惩罚费率（例如当发现研发资本化率超过 40% 时，附加 $\Delta_{\text{cap}} = 0.20$ ）。

2. 动态定价计算逻辑实现代码：

```
def calculate_dynamic_pricing(company_data: dict, risk_result: dict,
product_config: dict) -> dict:
    comprehensive_score = risk_result["comprehensive_score"]
    base_premium = product_config["base_premium"]

    # 1. 风险乘数计算
    if comprehensive_score >= 70:
        risk_multiplier = 2.50
        is_insurable = False # 建议拒保
    elif comprehensive_score >= 40:
        risk_multiplier = 1.0 + ((comprehensive_score - 40) / 30.0) * 0.80
        is_insurable = True
    else:
        risk_multiplier = 0.85
        is_insurable = True

    # 2. 行业系数
    sector = company_data.get("sector", "")
    industry_factors = {"人工智能": 1.35, "半导体": 1.25, "生物医药": 1.15, "高端制造": 1.05}
    industry_factor = industry_factors.get(sector, 1.0)

    # 3. 最终保费与保额调整
    final_premium = base_premium * risk_multiplier * industry_factor
    deductible_rate = 0.05 if comprehensive_score < 40 else (0.10 if comprehensive_score < 70 else 0.20)

    return {
        "product_name": product_config["name"],
        "is_insurable": is_insurable,
        "base_premium": base_premium,
        "final_premium": round(final_premium, 2),
        "risk_multiplier": round(risk_multiplier, 3),
        "industry_factor": industry_factor,
        "deductible_rate": deductible_rate,
        "underwriting_decision": "同意承保" if is_insurable else "拒绝承保"
    }
```

4.3 自动化核保决策报告生成引擎

系统集成了 Markdown 核保决策报告生成器，自动整合公司基本面、六维风险评分、多智能体辩论研判过程及动态定价结论：

```
=====
==
                                中国平安保险 · 科创企业核保决策报告
=====
==
报告编号：RPT-20260913-688256                                生成时间：2026-09-13 10:30:00
被保险企业：寒武纪科技股份有限公司                        股票代码：688256
所属行业：半导体及芯片设计                                评估结论：【附条件承保】
```


一、六维风险综合评估

综合风险评分：**68分**（中高风险）

- 技术路线颠覆风险：**45分**（中）
- 核心人员流失风险：**35分**（低）
- 算法与数据合规风险：**75分**（高）
- 地缘政治与出口管制：**82分**（极高）
- 研发资本化操纵风险：**40分**（中）
- 客户/供应商集中度：**65分**（中高）

二、多智能体交叉验证审计意见

[法务专家 (Law Agent)]:

上游 EDA 软件供应商 Synopsys 存在潜在出口管制风险；算法备案公示信息符合规范。

[财务专家 (Finance Agent)]:

前两大客户占总营收 **82%**，存在严重单点依赖风险；研发费用资本化率 **15%**，处于合理区间。

[委员会裁决 (Judge Agent)]:

企业总体具备较高技术壁垒，但上游供应链受制裁波及风险显著，且客户集中度偏高。

三、核保决策与特约条件

1. 承保方案：同意承保“科创特有风险综合险”

2. 基础保费：¥100,000 --> 动态调整后保费：¥168,750（风险乘数：1.35）

3. 免赔率：10%

4. 特约特别约定：

- 投保企业须在 **90** 天内提供上游 EDA 工具的备用国产化替代预案；
- 排他条款：因主动违反出口管制法规导致的设备断供不在理赔范围内。

第五章 原型系统实现与应用展示

5.1 系统开发环境与技术栈配置

本作品交付了可直接运行的完整金融级 Web 系统原型。开发环境与核心组件如下：

- **前端与交互框架**：金融级 Web 交互框架 (支持多页面路由与全局 State 同步)
- **矢量与图谱可视化**：Plotly 5.18+ / PyVis 0.3+ (网络拓扑渲染)

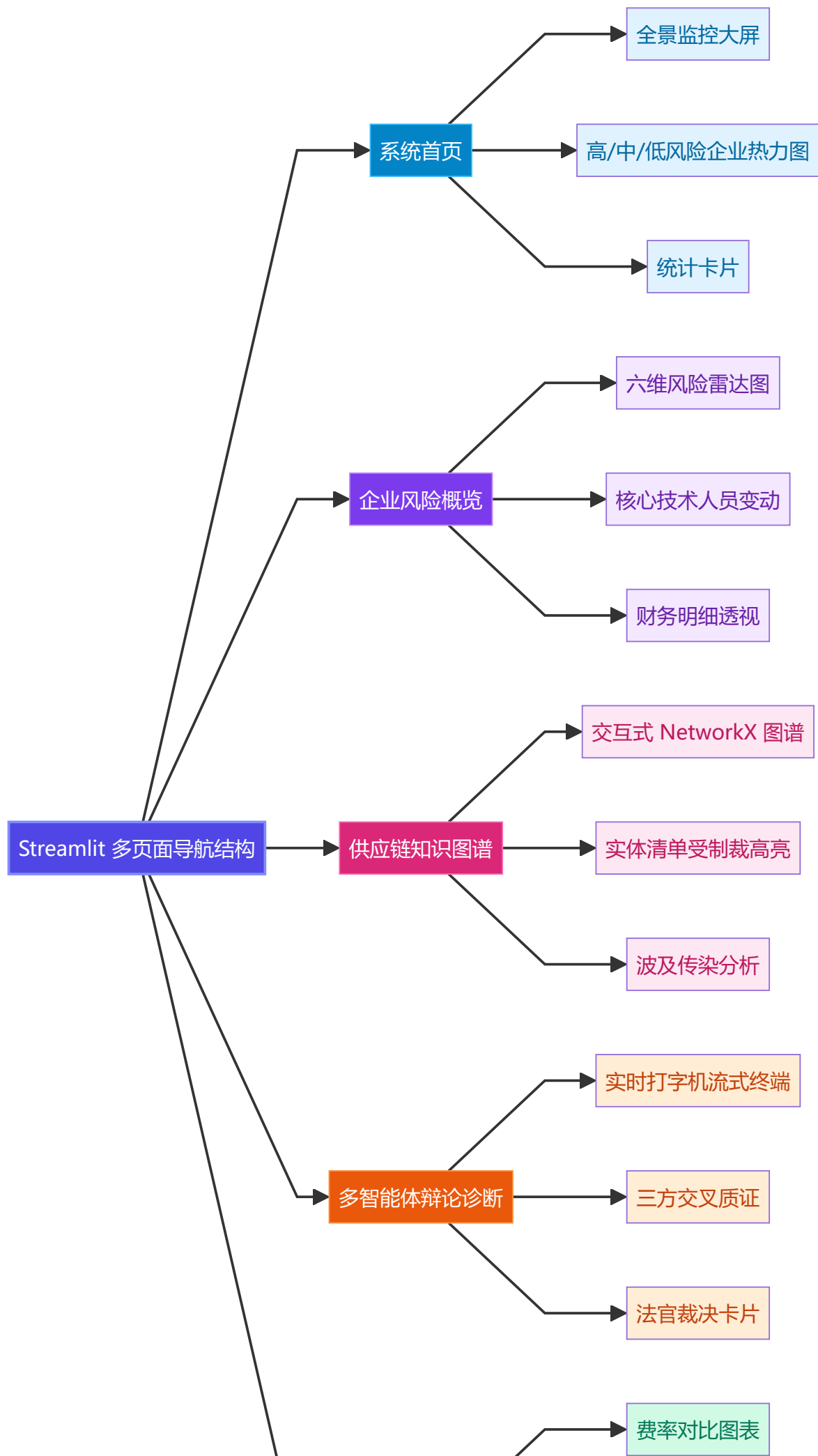
4.2 系统模块架构与导航结构

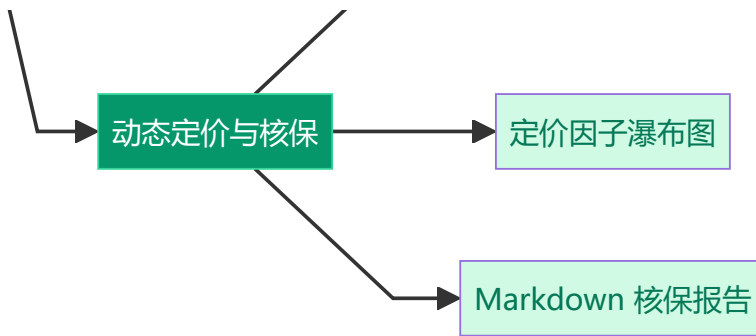
金融级 Web 多页面导航结构

- **大模型推理引擎**：DeepSeek API (deepseek-chat 引擎)
- **知识图谱与计算库**：NetworkX 3.0+、Pandas 2.0+、NumPy
- **数据可视化库**：Plotly Express & Graph Objects (暗黑金融科技主题)

5.2 核心页面结构与功能列表

原型系统包含五个规范化的业务板块：





5.3 核心功能创新与金融可解释性设计

1. 沉浸式多智能体推演可视化 (Explainable AI 展现):

在金融风控领域，黑盒模型往往无法被合规部门接受。本系统在辩论诊断页面，实时拉取并展示三大风控专家与委员会法官的推理思维链 (Thinking Stream)。这种全过程透明可视化的设计，让核保人员不仅知其然，更能“知其所以然”，大幅提升了 AI 介入强监管金融业务的可解释性。

2. 图谱视角的风险穿透与高亮预警:

有别于传统风控系统孤立展示企业数据的做法，本原型在知识图谱模块实现了“风险沿供应链传染”的动态高亮。当系统检索到某二级供应商位列美国 BIS 实体清单时，会自动沿拓扑网络将风险路径标红，直观呈现地缘政治带来的断供波及效应，为保险精算提供直观的证据链。

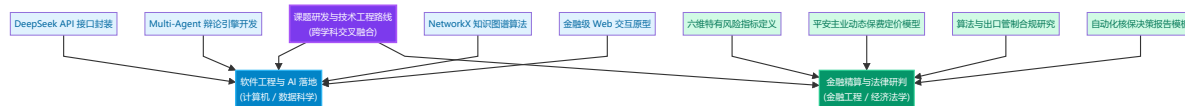
3. 规则引擎与大模型混合驱动的智能核保:

在最终定价与报告生成环节，系统摒弃了完全由 LLM 自由发挥的不可控模式，采用了“硬规则 + 柔性文本”的混合架构。综合评分硬性决定基础保费的上浮系数与免赔额（如 `score >= 70` 直接拒保或实施惩罚性费率），而大模型则负责基于这些硬结论，润色并生成带有“特约条款（如限期寻找国产化替代方案）”的标准 Markdown 核保报告。

第六章 课题研发与跨学科技术路线说明

6.1 课题研究技术路线架构

本项目研究与工程实现充分融合了计算机软件工程、大模型算法、金融精算与经济法学等多学科方法论，形成了清晰完整的研发技术路线：



6.2 跨学科研发成果

- AI 与软件工程实现:** 完成了后端 Python 数据流水线搭建、DeepSeek API 接口封装、Multi-Agent 辩论质询逻辑与 Prompt 链测试、NetworkX 异构知识图谱拓扑建图，以及金融级 Web 交互原型的全套工程开发。
- 金融精算与法律研究:** 深入研读科创板上市公司年报与 BIS 实体清单案例，构建六维特有风险量化指标体系，设计平安“科创特有风险综合险”产品条款，推导动态保费精算模型，并撰写标准化核保决策报告模板。

第七章 结论与未来展望

7.1 研究结论总结

本研究针对科创企业技术密集、高不确定性及非标准化特有风险突出的时代痛点，成功构建了“基于 AI 多智能体交叉辩论 × 供应链知识图谱”的新型风控范式，并打通了中国平安保险主业的动态定价与智能核保闭环：

- 精准定义了技术路线颠覆、核心人员流失、算法合规等六维特有风险指标，填补了传统静态财务风控的盲区。
- 引入多智能体交叉辩论与冲突消除机制，克服了单一大模型评估的视角片面性与事实幻觉。
- 建立供应链拓扑知识图谱，实现了地缘政治制裁风险的毫秒级穿透预警。
- 推出“科创特有风险综合险”及动态定价引擎，将学术研究转化为具备强可行性的金融产品原型。

7.2 场景扩展与应用前景

本研究成果具备极高的通用性与扩展潜力，可进一步辐射至多个相关金融场景：

- 商业银行“科技贷”质押审查**：帮助银行穿透评估科创企业的专利技术真实价值与供应链稳定性，降低坏账风险。
- 硬科技 VC/PE 智能尽职调查**：为股权投资机构提供自动化的技术路线颠覆性预警与高管履历穿透工具，提升尽调效率。
- 再保险与巨灾风险组合管理**：为再保险公司评估高科技产业链的系统性断供风险，优化风险组合配置。