

GOAI 世界人工智能开源大赛

Antinet· 八官署

多 AI 知识库中间层

软件研发全流程协同 · Agent Infra 新智基座 · 方向三

作品简介

项目名称

Antinet· 八官署：多 AI 知识库中间层

问题与场景

研发团队在缺陷 / 需求 / 日志 / 反馈中识别根因并产出可验证修复方案；传统单 Agent 把聚合 / 定位 / 修复 / 验证混在一起，难审计、难降级、难复现。

核心解决方案

以「明朝内阁」治理体系映射为八官署多智能体框架；四色卡片结构化传递上下文；太史阁先读后写，实现知识复利。

创新点与差异化

① 可溯源四色卡片 ② AgentTeams 协同基点 ③ 15 热插拔 Skill ④ 记忆 + 共享状态 + 可观测 ⑤ 熔断降级不崩盘

开放 / 复用价值

Apache 2.0 开源；能力可迁移至企业 AI 编码合规审计、跨工具创意生产、智能客服知识自演化、个性化学习教育陪练。

当前进展

八署串连通跑，verify_production.py PASS；已接入真实本地 NPU（Genie qwen2.5vl3b）；Agent Identity / Skill 体系 / AgentTeams 映射文档齐备。

目录

1 场景与价值

3 多 Agent 协同设计

5 工程落地、运行验证与安全可审计

7 落地计划与进展

2 方案总览

4 Skills 工具体系

6 开源开放计划

8 Demo 视频

对应评分维度

场景价值与行业可复制性

25%

第一章

场景与价值

场景与价值

目标用户、核心痛点、方向三实例化与行业可复制性

目标用户：开发者与研发团队，需从 Issue / 日志 / 用户反馈中快速定位根因并产出可验证修复。

真实痛点：信息分散、根因定位靠经验、修复方案难审计、复盘知识随人走、单 Agent 把多阶段任务混在一起。

方向三实例化：缺陷 / 需求聚合 → 代码根因定位 → 修复生成与执行 → 测试 / 发布确认 → 上线复盘与知识沉淀。

行业可复制：四色卡片作为通用知识格式，同样适用于金融风控、客服复盘、运维复盘、材料研发。

差异化定位：不是单 Agent Demo ，而是让多个 AI 围绕同一份结构化知识协同的「知识库中间层」。

企业 AI 编码合规审计

Secrets 出域防控、改动审计

跨工具创意生产管线

素材 / 版本 / 决策集中管理

智能客服知识自演化

从静态文档到带溯源自活体

个性化学习教育陪练

错点追踪与可解释学习路径

对应评分维度

端到端方案与关键技术选型

—

第二章

方案总览

方案总览

端到端架构与主流程

用户 / 客户入口	缺陷、需求、告警、日志、反馈
指挥使 · 编排层	意图识别、任务拆解、异常熔断
锦衣卫 · 安检层	合规扫描、防假全文、密钥检测
密卷房 · 解析层	多格式解析与 OCR 三级 fallback
通政司 · 事实层	事实抽取 → 蓝卡
监察院 · 审计层	逻辑审查、Gap → 绿卡
丞相府 · 策略层	构效假说与行动建议 → 红卡
军机处 · 执行层	核验、产物落盘、报告生成
太史阁 · 记忆层	长期记忆、检索、知识回流、provenance

职责隔离：8 个具名 Agent 各司其职，每个环节可独立验证、独立降级。

四色卡片：蓝事实 / 绿解释 / 黄风险 / 红行动，作为多 AI 间唯一结构化上下文介质。

记忆总线：太史阁「先读库再干活、后写库做沉淀」，每次任务都在复用与增值知识。

设计基点：以 AgentTeams 角色模型为协同基点，后续迁移只需协议适配。

对应评分维度

多 Agent 协同与自主闭环能力

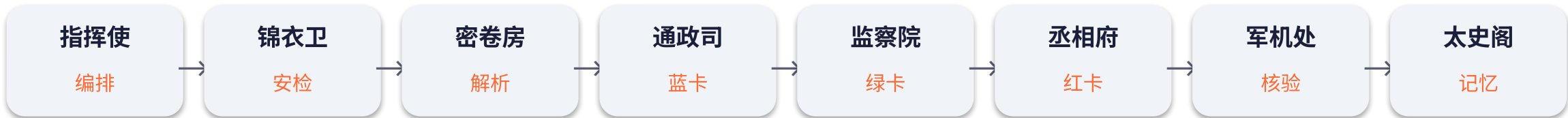
25%

第三章

多 Agent 协同设计

多 Agent 协同设计

Agent 分工、任务拆解、上下文传递、异常处理与安全边界



角色编排：8 个具名 Agent，身份、能力边界与协同关系见《Agent Identity 清单》（附录 A）。

任务拆解：指挥使状态机将用户主题拆为检索 / 解析 / 抽取 / 审查 / 假说 / 核验 / 回流子任务。

上下文传递：四色卡片 cite 链实现传递；每署只接收上游卡片，不读原始噪声。

异常与冲突：任一官署失败即触发指挥使熔断与规则引擎降级，大模型掉线 / 解析失败不崩盘。

安全边界：锦衣卫是唯一出域审批方；高风险动作（发布 / 合并）由指挥使状态机执行审批 / 回滚 / 审计。

对应评分维度

Skill 工程体系与生态复用

25%

第四章

Skill 工程体系

Skill 工程体系

15 个真实可运行 Skill 与完整规格

抽取类

four_color_cards
markdown_converter
local_audio_processor

知识类

knowledge_graph
book_skill
view_manager

展示类

infographic
html_report
report_automation
ppt_structure_draft
chart_recommendation

治理类

card_filter
markdown_formatter
invoice_skill

单个 Skill 规格：名称 / 用途 / 输入输出 / 调用条件 / 依赖工具 / 失败处理 / 安全边界 / 复用价值 / 与协同流程的关系。

复用与生命周期：统一 Skill 基类（name/description/category/parameters_schema/execute），支持热插拔、版本化、失败降级。

生态对接：核心抽象层与 github.com/anbeime/skill 公开技能商店接口对齐，迁移到新运行时只需协议适配。

赛道要求：Skill 是必选项；本方案 15 个真实 Skill 可独立部署，亦可被外部 Agent 复用。

对应评分维度

工程落地与安全可审计

20%

第五章

工程落地、运行验证与安全可审计

工程落地、运行验证与安全可审计

可运行性、运行证据、可观测与安全治理

可运行性

python scripts/run_survey.py 主链路跑通
verify_production.py 输出 consistency:PASS , 退出码 0
可接入 CI 幂等重跑

运行证据

verify_report.json : parsed_oa_ratio 7/10
provenance/knowledge.md 全链路回放
四色卡片样例可审计

可观测 / 检索

太史阁 = 记忆存储 + 共享状态管理
provenance 日志 = Trace / Log / Metrics
超额满足 2/4 项要求

安全治理

默认本地 NPU , 数据不出域
锦衣卫合规扫描 + 密钥检测
指挥使状态机审批 / 回滚

云产品选型边界：Nacos / Higress / PolarDB / RocketMQ / LoongSuite 均可等价替换，迁移成本已在映射文档中逐条论证。

对应评分维度

开放 / 开源贡献

5%

第六章

开放 / 开源计划

开放 / 开源计划

可复用成果、接口契约与开源协议

开源协议： Apache 2.0 ； 本方案 materials-agent/ 仓库结构公开。

可复用成果： 四色卡片开放格式、八署编排运行时、15 Skill 抽象层、provenance 日志格式。

接口契约： 等价外部工具集成契约（协议 / 鉴权 / Schema / 错误 / 审计 / 迁移成本），不使用 MCP 也给出等价方案。

文档与示例： Agent Identity 清单、AgentTeams 映射文档、Skill 工程体系说明、DEPENDENCIES.md 第三方依赖边界。

数据集： OpenAlex （CC0）合法复用；闭源 API 的接口与降级逻辑均开源。

Skill 生态： 核心 Skill 与 github.com/anbeime/skill 公开技能商店对齐，可被外部 Agent 直接复用。

开源目标

把「多 AI 可审计记忆总线」做成标准件，而不是绑定在某个封闭产品里。

对应评分维度

当前进展与整体可行性

—

第七章

落地计划与进展

落地计划与进展

当前进展、里程碑与风险控制



当前进展：八署 pipeline 可复现、verify PASS、真实本地 NPU 接入、Agent Identity / Skill / AgentTeams 映射文档齐备。

复赛目标：迁移八署至 AgentTeams 运行时，接入 Higress / Nacos / PolarDB，完成代码仓库 PR/ 测试 / 发布完整闭环。

风险控制：初赛阶段诚实披露降级现状（解析预存全文模拟 7/10、代码仓库工具链复赛落地），避免粉饰。

对应评分维度

团队能力与执行可行性

—

第八章

团队介绍

团队介绍

成员背景、分工与成果（请补充真实信息）

成员 1

负责人 / 架构

多 Agent 系统设计、八署编排、AgentTeams 映射

成员 2

算法 / Skill

四色卡片模型、Skill 抽象层、本地 NPU 接入

成员 3

工程 / 落地

可运行链路、验证脚本、provenance 与可观测

提示：请在此页替换为真实成员信息，包括学校 / 公司、岗位 / 专业、核心技能、过往项目 / 获奖经历及作品合集链接。

Demo 视频与提交信息

docs/track1/Antinet_GOAI_track1_demo.mp4 (45 秒, 1080p)

作品名: Antinet· 八官署 (软件研发全流程协同 · 多 AI 知识库中间层)

赛道: GOAI 赛道一 · Agent Infra 新智基座 · 方向三「软件研发全流程协同」

开源仓库: materials-agent/ (Apache 2.0) + github.com/anbeime/skill 公开技能商店

Demo 入口: `scripts/run_survey.py` 主链路 + `verify_production.py` CI 可复现