

石卓灵

☎ 13208105936 ✉ jorlin1101@outlook.com

◎ AI应用工程师 | Agent 开发 ⇄ github.com/jorlin1101-cyber



教育背景

电子科技大学	电子信息 (硕士)	2022.09 - 2025.06
西南石油大学	电子信息科学与技术 (本科)	2017.09 - 2021.06
• 科研成果及奖项: EI期刊第一作者论文1篇; 发明专利申请1项 (第二发明人, 导师第一); 优秀研究生及研究生学业二等奖学金; 全国大学生数模省一等奖、MCM H奖 (队长)		

专业技能

- **LLM 与 Agent 应用:** LLM API 集成、Prompt 设计与评测、LangGraph、Agent Runtime Harness、多 Agent 编排、Prompt/Skill 演进、结构化输出
- **RAG 与检索增强:** RAG、BGE-M3、BM25、RRF、Grounded Generation、引用校验
- **后端与数据工程:** Python、FastAPI、Pydantic、PostgreSQL、SQLite、Redis Streams、Docker、n8n
- **工程质量与可观测性:** pytest、Ruff、mypy、Prometheus、OpenTelemetry
- **编程与语言能力:** C/C++、MATLAB/Simulink、英语 CET-6、日语 JLPT N2

项目经历

SecurePR Agent | 多Agent PR审查与安全修复系统 2026.05 - 2026.07

项目介绍: 面向 PR 风险发现与安全修复场景, 构建**可恢复 Agent Runtime Harness 与多 Agent 协作系统**, 覆盖代码风险识别、证据复核、受限修复、编译测试、Draft PR 交付及评测驱动演进。

技术亮点:

- **可恢复 Runtime Harness:** 针对长流程 Agent 的中断、调用失败及预算失控问题, 统一管理**任务状态、Token/时间预算、自动重试、持久化 Checkpoint、断点续跑与 Run Trace**; 接入 OpenTelemetry 和 Prometheus, 实现执行链路**可观测、可中断、可恢复**。
- **多 Agent 审查与安全修复:** 构建 Lead → Specialists 并行审查 → Critic 独立复核 → Lead 汇总决策的协作链路; 结合仓库检索、静态扫描、AST 与测试证据确认风险, 由受限 Fixer 生成补丁, Verifier 通过**编译与测试门禁**后创建 Draft PR。
- **评测驱动的 Prompt/Skill 演进:** 将误报、漏报、坏修复及运行异常沉淀为失败案例, 自动生成候选 Prompt 与 SKILL.md; 通过 **Validation 提升 + 隐藏 Holdout 非退化双门禁**决定版本激活, 并支持**候选去重、版本审计与一键回滚**。
- **上下文压缩与分层记忆:** 在 Token 预算内优先保留高风险证据、历史 Observation 与 Critic 反馈, 构建 Working、Episodic、Semantic **三层记忆**, 支持按租户和仓库隔离检索及任务归档。
- **可复现离线评测:** 构建 **100 条合成受控 PR Diff**, 包含 40 条风险样本和 60 条干净样本, 并按文件路径、行号区间与 CWE 类型进行一对一匹配; 固定评测口径下, 候选方案 **F1 从 81.9% 提升至 91.3% (+9.4 个百分点)**, 高风险召回率从 **84.2% 提升至 94.7% (+10.5 个百分点)**, 干净 PR 准确率达到 **91.7%**。

AI销售线索决策与CRM路由原型 2026.04 - 2026.05

项目介绍: 面向销售线索、评分与客户跟进场景, 建从数据清洗 → 结构化事实提取 → 确定性评分 → RAG 辅助建议 → CRM 五路路由的端到端服务, 兼顾决策可解释性、生成可靠性与工程交付质量。

技术亮点:

- **数据契约与决策边界:** 以FastAPI/Pydantic构建**强类型链路**; LLM仅提取**结构化事实**, PolicyV1**确定性输出评分、意向与 Reason Code**, 支持解释和回放。
- **RAG全链路检索评测:** 按H2切分47个Chunk, 以BGE-M3向量化并融合Dense+BM25+RRF; 在18条人工标注查询上, **Hit@1=18/18, Hit@3=18/18, MRR@3=1.000, nDCG@3=0.8331**。
- **Grounded生成与安全降级:** RAG前冻结决策, 基于Top-3白名单证据生成建议; **拦截注入、未知引用与结构异常**, 降级至模板或人工复核。
- **工作流与质量保障:** 以n8n实现五路路由并Docker交付; 离线CI禁外网Socket, 验收**577项测试通过、覆盖率95%**, Ruff/Mypy通过。

工作经历

北京润科通用有限公司 仿真建模工程师 2025.07 - 2026.01

- **需求拆解与模型交付:** 从客户协议和需求文件中提取、分类、编号需求并建立追踪关系; 独立使用Simulink搭建**国标充电协议模型**和**报文收发原型**, 完成平台接入、演示评审与测试。
- **跨语言接口集成:** 针对C++平台调用Python模型的需求, 开发C++/Python调用链, 处理调用入口、参数与数据类型转换、返回值及异常映射, 并集成至公司平台成功运行。
- **模型实现与性能验证:** 根据客户协议要求, 完成Simulink、C/C++、S-Function、M函数及Stateflow等模型的搭建与产品平台集成, 使各模型能够在公司软件产品中稳定运行, 并通过测试验证仿真周期小于400 μs; 同时搭建**反射内存数据接口**, 编写Bash脚本及调试、验收文档, 支持项目交付。