InfoQ 极客传媒

AI Scientist中的上下文动态优化与自我演进

演讲人：王则远

灵犀量子（北京）医疗科技有限公司

AiCon

全球人工智能开发与应用大会

AiCon
全球人工智能开发与应用大会

目录

极客邦科技 2026 年会议规划

促进软件开发及相关领域知识与创新的传播

参会咨询

查看会议

4月 · 北京 · 1200人

QCon 全球软件开发大会

会议时间：4月16-18日

- Agentic Engineering
- AgentOps
- 下一代模型架构与推理优化
- AI 原生基础设施
- 知识工程实践
- AI 安全

6月 · 上海 · 1000人

AiCon 全球人工智能开发与应用大会

会议时间：6月26-27日

- AI Infra 系统工程
- 多 Agent 协作与实践
- 多模态融合
- 模型训练与推理创新
- 数据平台与特征服务

8月 · 深圳 · 1000人

AiCon 全球人工智能开发与应用大会

会议时间：8月21-22日

- Agentic AI
- 轻量化与高效推理
- 多模态应用
- AI + IoT 场景实践
- AI 工业化落地

10月 · 上海 · 1200人

QCon 全球软件开发大会

会议时间：10月22-24日

- AI Agent
- Vibe Coding
- 智能可观测
- 推理基建
- 模型攻防
- AI x 创造力

12月 · 北京 · 1000人

AiCon 全球人工智能开发与应用大会

会议时间：12月18-19日

- 大模型架构创新
- 多模态 AI 产业融合
- 具身智能
- AI for Science
- 大模型安全

InfoQ 极客传媒

01 医学 AI Scientist 的机遇与研究缺口

医学“AI for Science”的崛起


THE LANCET

This journal Journals Publish Clinical Global health Multimedia Events About

PERSPECTIVES | Digital medicine · Volume 405, Issue 10472, P20, January 04, 2025 Download Full Issue

A clinical certification pathway for generalist medical AI systems

Pranav Rajpurkar [a] · Eric J Topol [b]

Affiliations & Notes Article Info

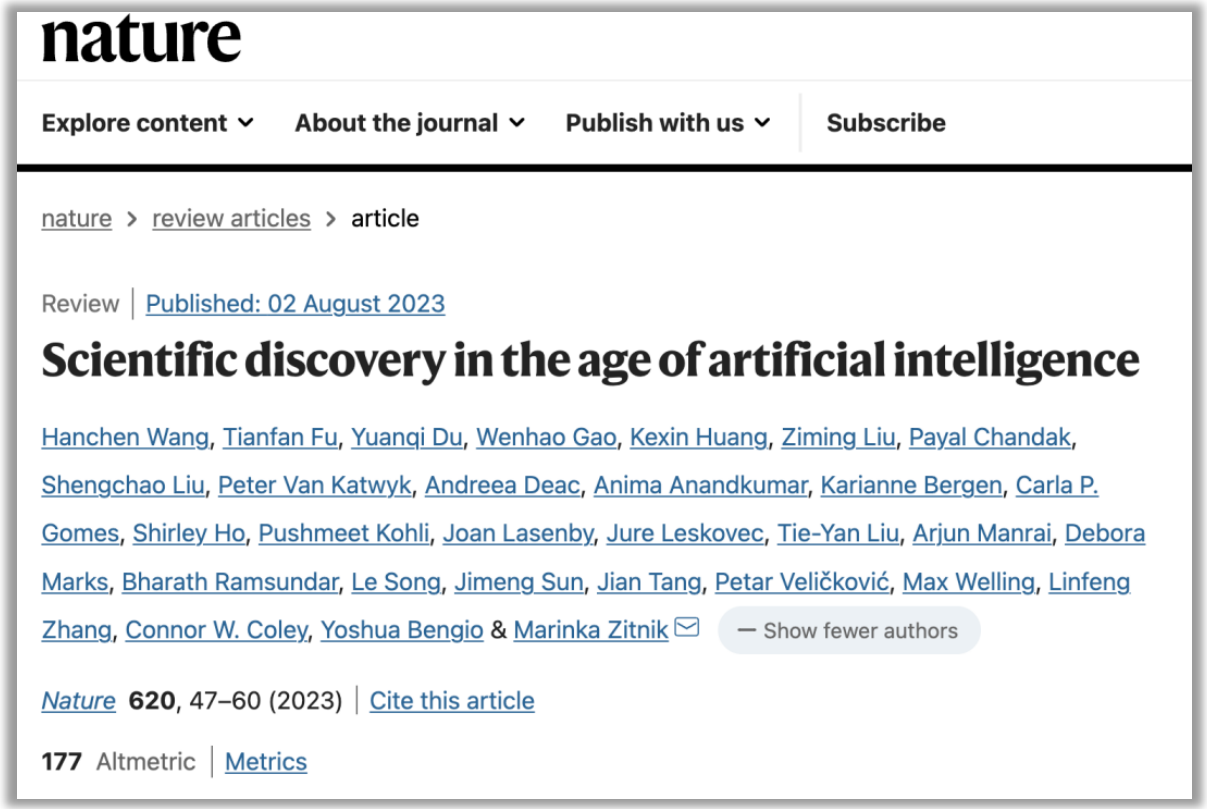
2025年1月，美国医学院院士Eric J Topol在LANCET发文阐述通用型人工智能系统的临床认证新路径，包括三步：

1、基础阶段：AI系统需展示对基础医学知识的理解，类似医学生完成基础科学教育。

2、专科任务执行：AI需将知识应用于实际医疗任务，如病史收集、健康教育和初步评估，同时接受严格的性能监控。

3、有条件自主与全面认证：随着能力展示，AI将逐步获得更大自主权，但最终仍需人类监督，并定期审查其输出以确保持续遵守医疗标准。

医学“AI Scientist”的出现



nature

Explore content ⌄ About the journal ⌄ Publish with us ⌄ Subscribe

nature › review articles › article

Review | Published: 02 August 2023

Scientific discovery in the age of artificial intelligence

Hanchen Wang, Tianfan Fu, Yuanqi Du, Wenhao Gao, Kexin Huang, Ziming Liu, Payal Chandak, Shengchao Liu, Peter Van Katwyk, Andreea Deac, Anima Anandkumar, Karianne Bergen, Carla P. Gomes, Shirley Ho, Pushmeet Kohli, Joan Lasenby, Jure Leskovec, Tie-Yan Liu, Arjun Manrai, Debora Marks, Bharath Ramsundar, Le Song, Jimeng Sun, Jian Tang, Petar Veličković, Max Welling, Linfeng Zhang, Connor W. Coley, Yoshua Bengio & Marinka Zitnik — Show fewer authors

Nature **620**, 47–60 (2023) | Cite this article

177 Altmetric | Metrics

人工智能（AI）越来越多地应用于科学学科， 用于整合大量数据集，改进测量，指导实验，探索与数据兼容的理论空间，并提供与科学工作流程集成的可操作且可靠的模型，用于自主发现。

传统的科学方法为“观察–理论–假设–实验–数据–分析–结论”，现今 AI 正越来越多地融入科学发现中，以加速研究，帮助科学家生成假设，设计实验，收集和解释大型数据集，并获得仅使用传统科学方法可能无法获得的见解。

研究动机与挑战

虽然 LLM 拥有广泛预训练知识，但医学/生物医药知识快速进化、领域专业、动态更新，共享知识库难以覆盖全部。

知识局限性

传统 LLM 的推理/chain-of-thought规划，在科研任务中面临超长依赖链、高不确定性、动态环境时，容易出现规划失效

规划脆弱性

即便有工具调用，也存在语义鸿沟（semantic gap）、参数误用、副作用风险，以及关键决策节点上缺乏可信度估计。

执行不可靠性

三大挑战引出的核心问题：如何构建一个能够从自身经验中学习 (self-improve)、实现能力持续进化 (self-evolve) 的专用智能体 (Specialized Agent)?

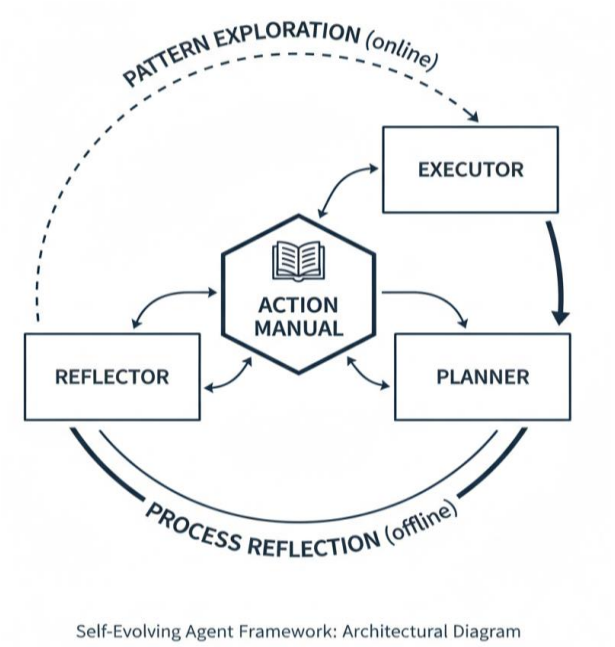
02

核心框架实现

核心框架概述

基于动态上下文 (Dynamic Context) 的自主进化机制

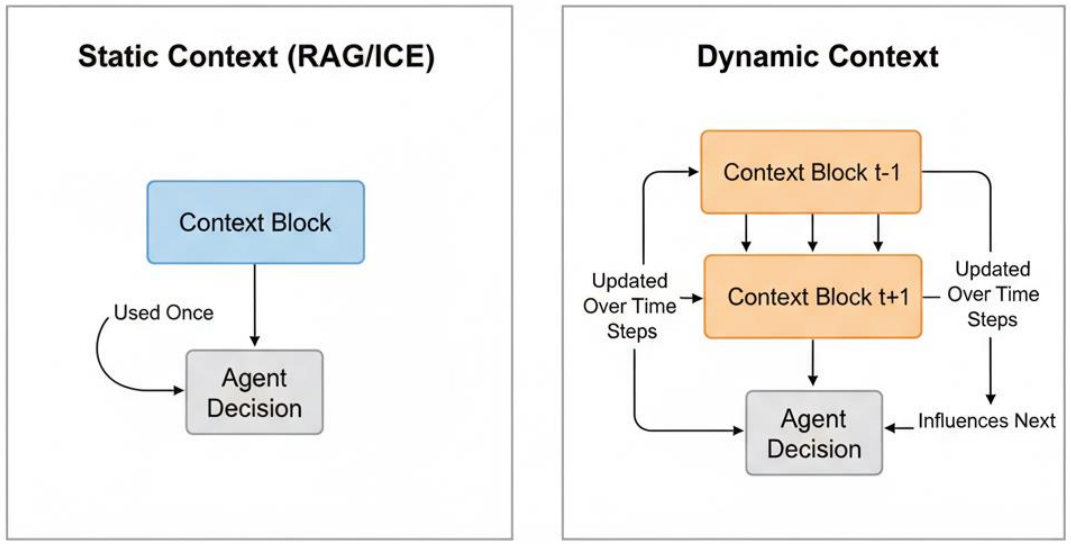
与传统的一次性上下文 (如 RAG, ICE) 不同，它会随着任务进程持续演化



Self-Evolving Agent Framework: Architectural Diagram

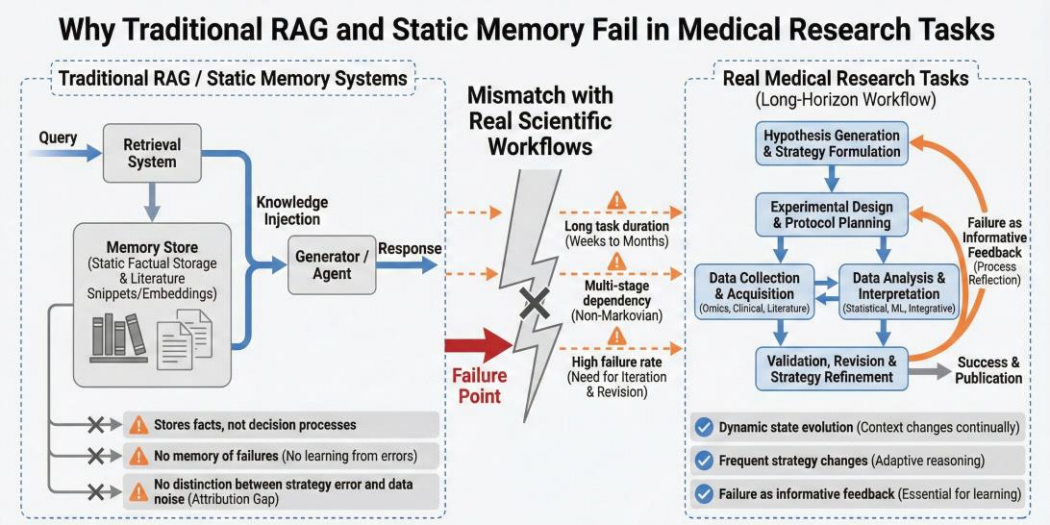
- 中心组件是“行动手册 (Action Manual)”—— 一套元认知 (meta-cognitive) 策略集合 (不是静态知识库 /记忆库)，用于指导智能体在不同情境下如何决策与行动。
- 通过“模式探索 — 过程反思 (Pattern Exploration & Process Reflection, PE-PR)”的双循环机制，实现 闭环学习 (Closed-Loop Learning)：
  - 模式探索 (Pattern Exploration)：在线 (on-line) 过程中识别高价值行动模式 (Action Patterns)，并尝试泛化。
  - 过程反思 (Process Reflection)：任务结束后 (off-line) 对执行轨迹 (Execution Trace) 进行因果归因 (causal attribution)，尤其针对失败或次优路径，生成修正策略 (remediation strategies)。
- 最终，PE-PR 输出被整合入 Action Manual，实现能力随时间、任务经验不断演化 (self-evolve)。

理论基础



- 传统方法（如 RAG，ICE）属于“一次性上下文注入（one-shot context injection)”，适用于短期任务/较窄领域，但难以应对科研任务中的时序依赖与情境变化。
- 科研任务（尤其医学 /生物医药）通常是高度专业化 + 长周期 + 多步骤 + 高不确定性，要求智能体 能够在任务执行过程中不断适应、调整、学习 (in-task learning/online learning)。
- 因此，需要一种动态上下文机制 (Dynamic Context Mechanism)，允许上下文随着任务进程实时更新，并对智能体决策产生持续影响。
- 这种设计可以有效提高智能体对复杂、长周期任务的适应性和泛化能力。

为什么传统 RAG / Memory 在医学科研任务中失效?



1）医学科研任务的真实特征

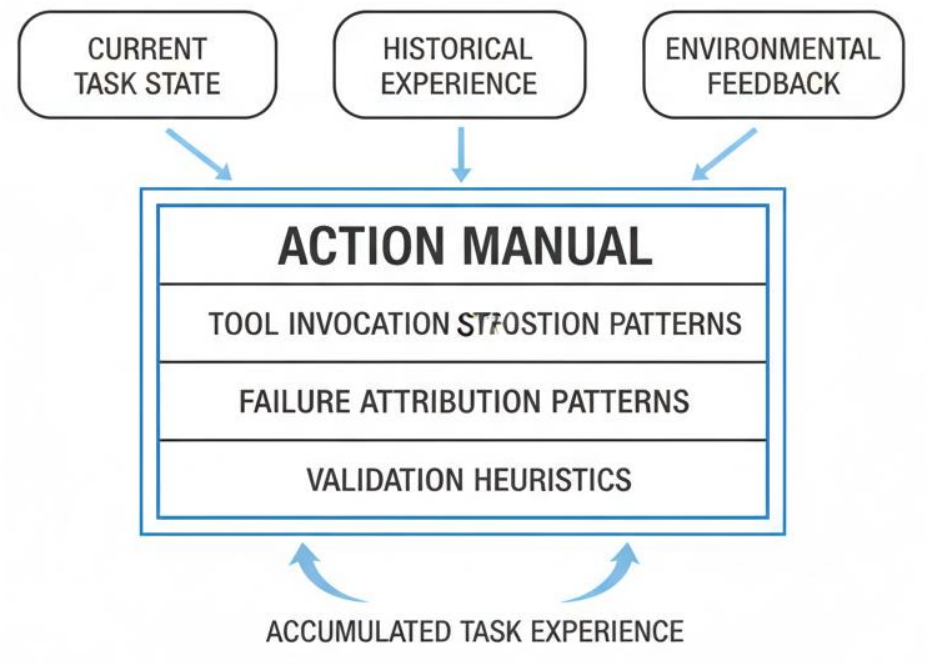
- 长周期、多阶段任务链：医学科研往往涉及假设提出 → 实验设计 → 数据收集 → 模型调整 → 验证修正等多个阶段，各阶段相互影响，任务跨度往往是数小时到数天甚至更长。
- 高失败率本身就是信息：在科研里，失败不是异常，是决策有效性的重要反馈信号，能提供因果归因线索。
- 任务动态性强：中间结果会不断改变策略方向，相比短任务，执行状态在任务间持续变化。

2）传统 RAG / Memory 的三个根本局限

- 只存“知识”，不存“决策路径”：RAG 和静态记忆只注入事实或文献，不记录“为什么这么做”。
- 失败经验不可复用：系统不会积累“失败是怎么来的、以后如何避免”，导致每次见到类似问题都要重新推理。
- 无法区分“策略错 versus 数据噪声”：单纯的知识检索无法回答是策略决策导致失败还是数据本身噪声干扰。

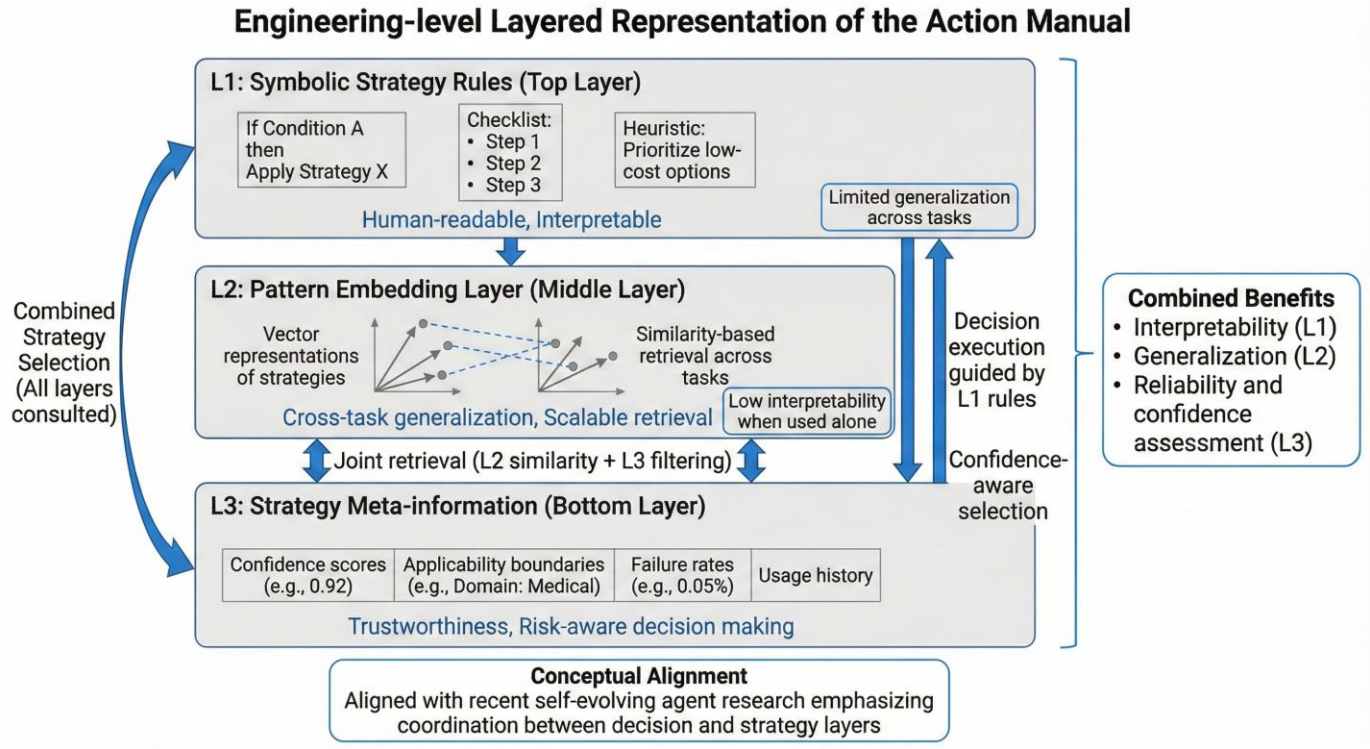
“行动手册 (Action Manual)”的定义与组成

定义：一个结构化、动态演化的策略知识库 (meta-knowledge repository)，编码“如何成功执行任务”的元知识 (meta-knowledge)，包括但不限于：工具调用序列、问题分解策略、失败归因模式、验证启发式规则等。



- “行动手册”特点：
  - 动态演化：随经验 & 任务积累不断更新，而不是静态知识。
  - 可检索/可解释：不仅仅是黑箱记忆，而是结构化规则/策略集合，以便审查、调试与理解。
  - 情境感知 (Context-aware)：策略能够根据当前任务状态、历史经验、环境反馈做出调整。
- “行动手册”并非传统意义上的数据库/记忆库，而是智能体决策时参考的元认知上下文 (meta-cognitive context)。

Action Manual 的工程化分层表示



Action Manual 三层结构

L1：策略规则层（Symbolic）– 可解释性

– if–then 规则 / 检查表 / 经验启发

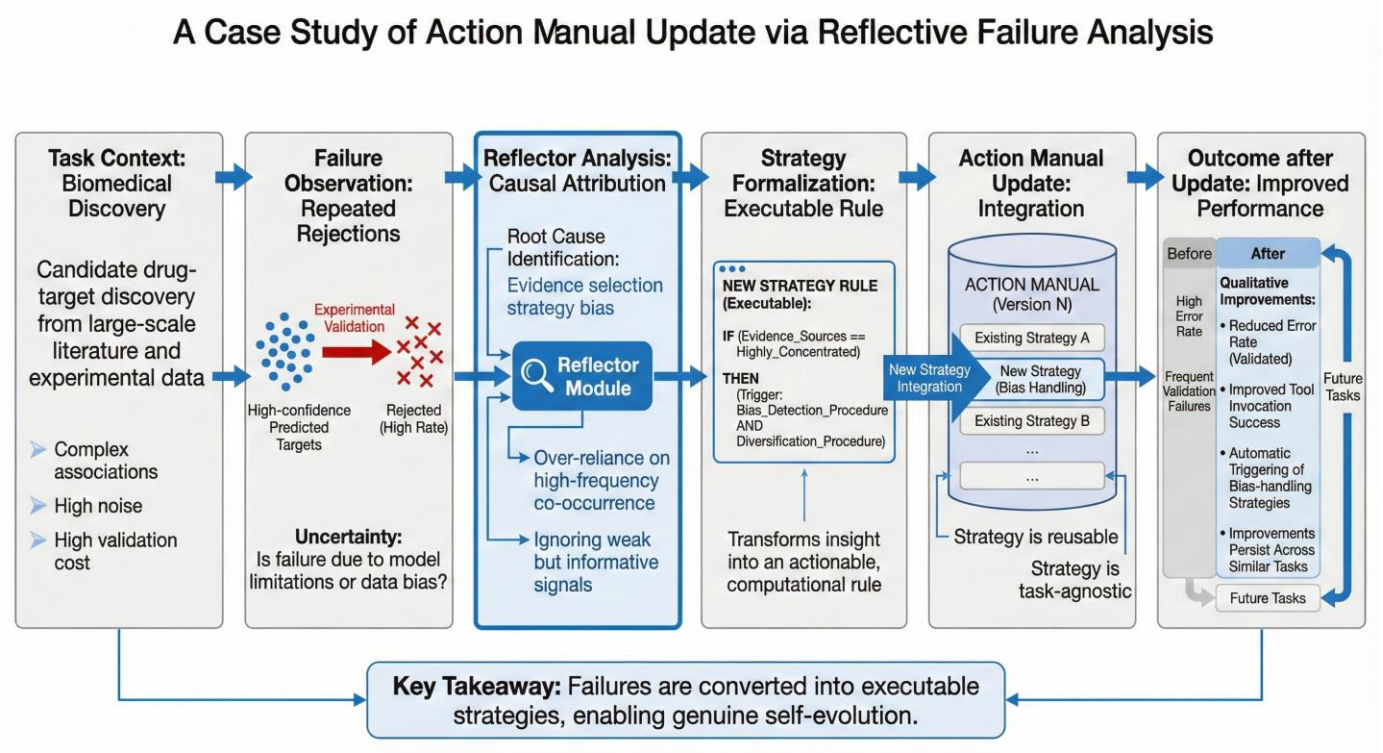
L2：模式向量层（Embedding）– 泛化能力

– 任务间相似性检索 / 索引

L3：策略元信息层（Meta）– 可信度评估

– 置信度、适用边界、失败率

Action Manual 案例



1) 任务背景

- 目标：在大规模文献 + 实验数据中识别潜在候选靶点
- 主要难点：关联模式复杂、噪声干扰高、验证成本高

2) 失败现象

- 多轮自动推断过程中高置信度候选靶点反复被实验否定
- 原因难定位：是模型能力问题还是样本偏置?

3) Reflector 的归因结论

问题不在基础模型，而在“证据选择策略”：偏好高频共现文献，忽略弱信号，导致误判与错误决策路径

4) 写入 Action Manual 的新策略

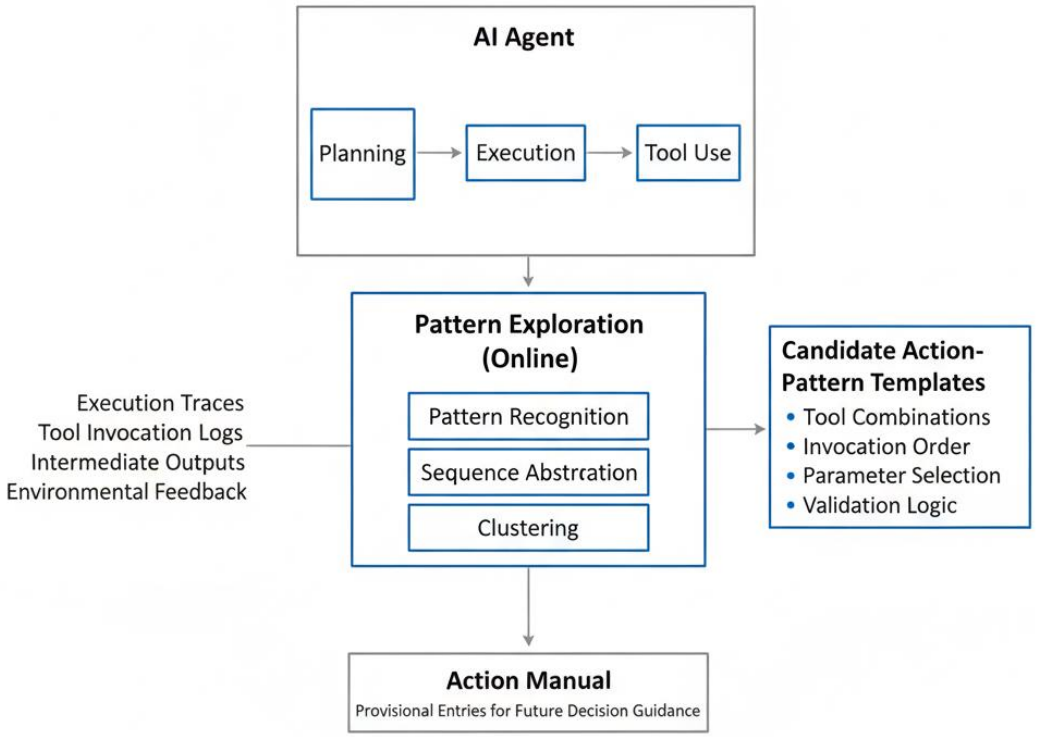
“当证据来源高度集中在少数几个数据源时，必须触发偏倚检测流程。”

5) 更新后的效果

相似任务上错误率显著下降；工具调用成功率提升

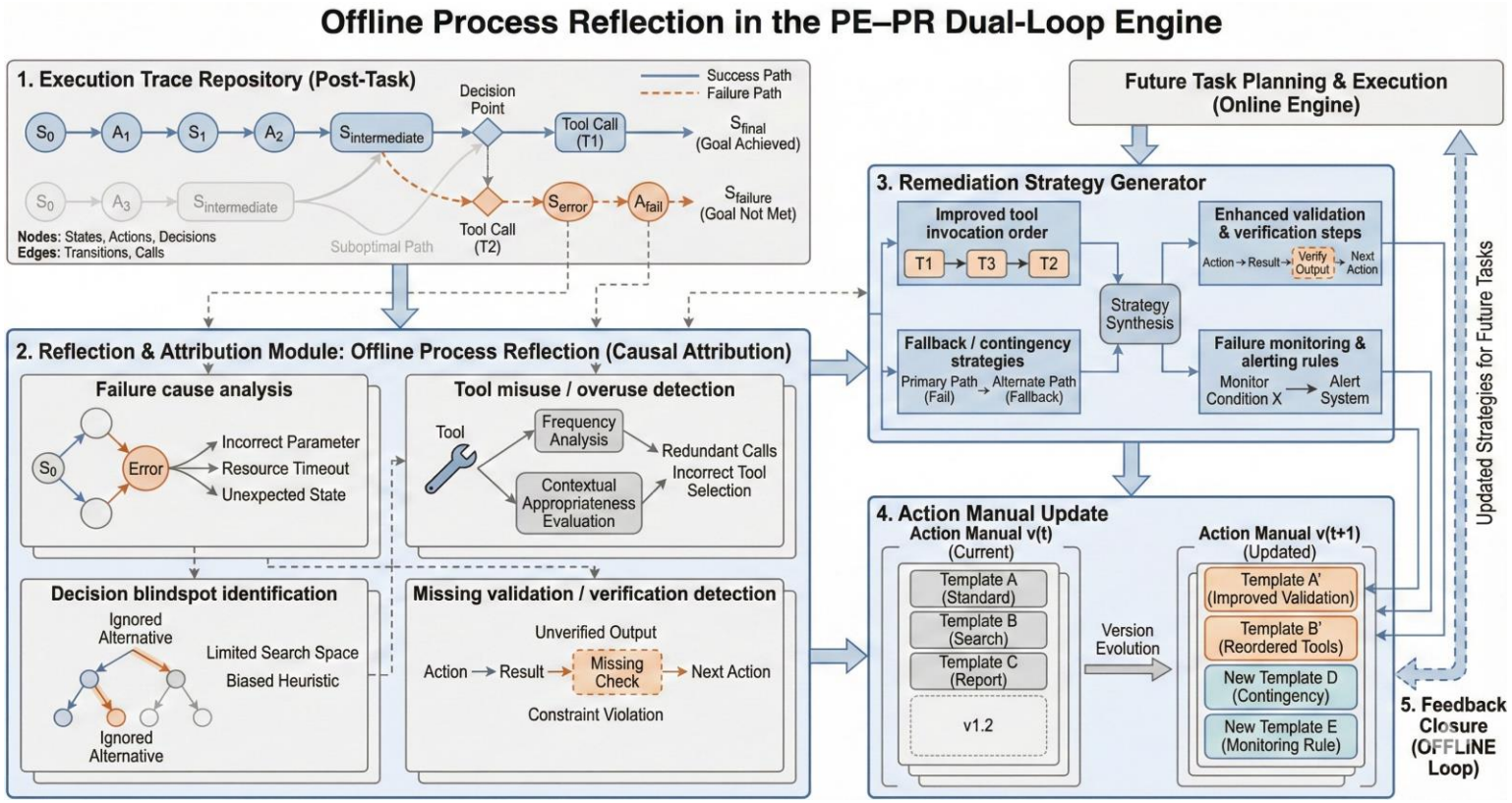
再遇类似偏倚情境能自动触发策略调整

PE-PR 双循环引擎机制（模式探索）



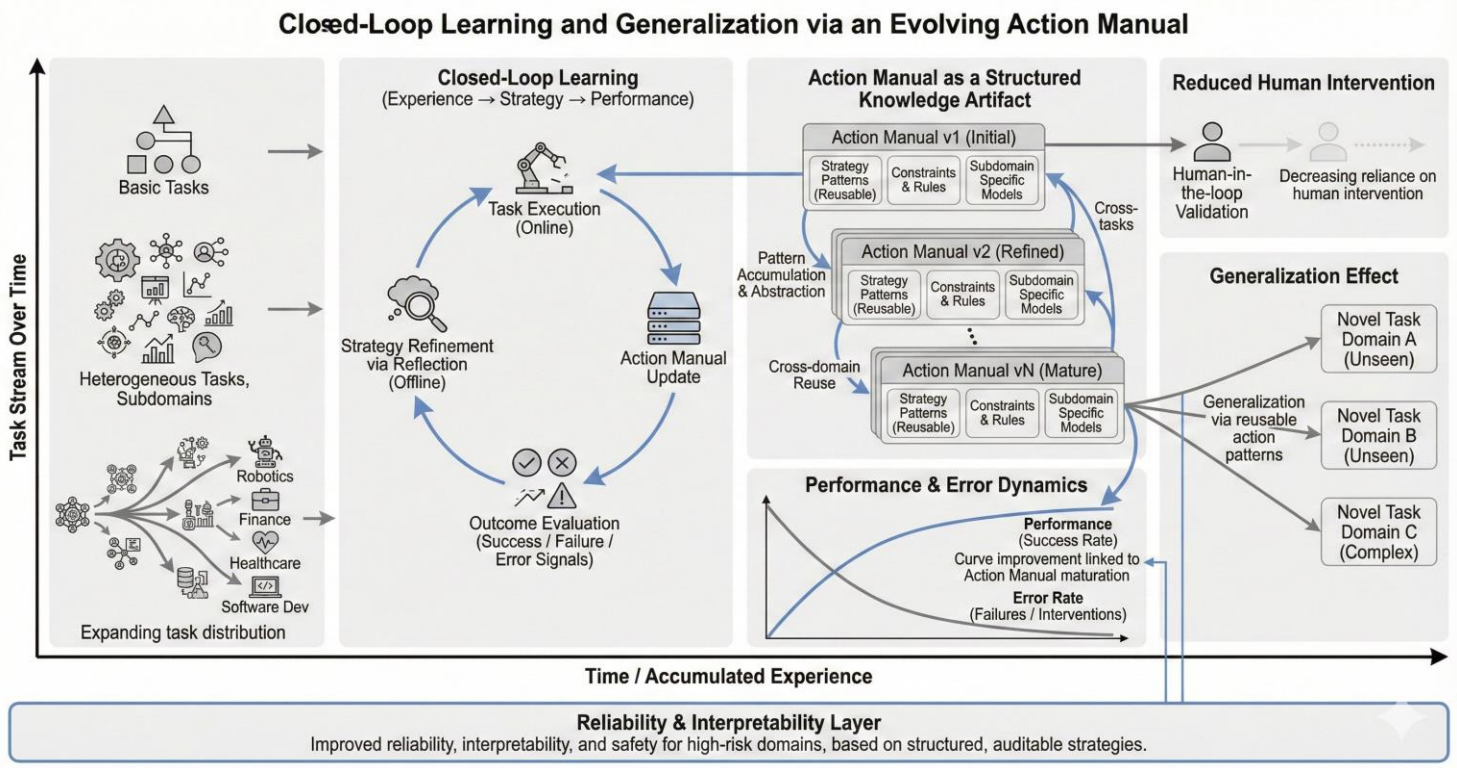
- 在线机制（on-line）：当智能体执行任务（planning + execution + tool use）时，系统监控执行过程、工具调用日志、环境反馈、中间结果等。
- 通过算法（例如pattern recognition、sequence mining、clustering等）自动识别其中反复出现、表现良好的“高价值行动模式 (action patterns)”。
- 将这些模式提炼、泛化，形成 candidate 策略（action-pattern templates），可能包括“某类任务 — 推荐工具组合 + 调用顺序 + 参数选择 + 验证方式”。
- 这些 candidates 会被暂存到“行动手册（Action Manual）”中（或者待审批 /筛选）— 为未来任务提供参考。

PE–PR 双循环引擎机制（过程反思）



- 离线机制 (off–line)：当任务 (或一批任务) 完成后，对整个执行轨迹、中间结果、成功/失败 / 次优路径进行因果归因，尤其针对失败或表现不佳的路径。
- 反思目标包括：识别失败原因、发现误用 / 滥用工具, 识别决策盲点, 以及策略中遗漏的验证 /校验步骤。
- 根据反思结果，生成可操作的修正策略，例如：更好的工具调用顺序、更严格的验证机制、备用方案、失败监控 /告警机制等。
- 将这些修正策略整合回“行动手册 (Action Manual)”中，优化现有策略集合。

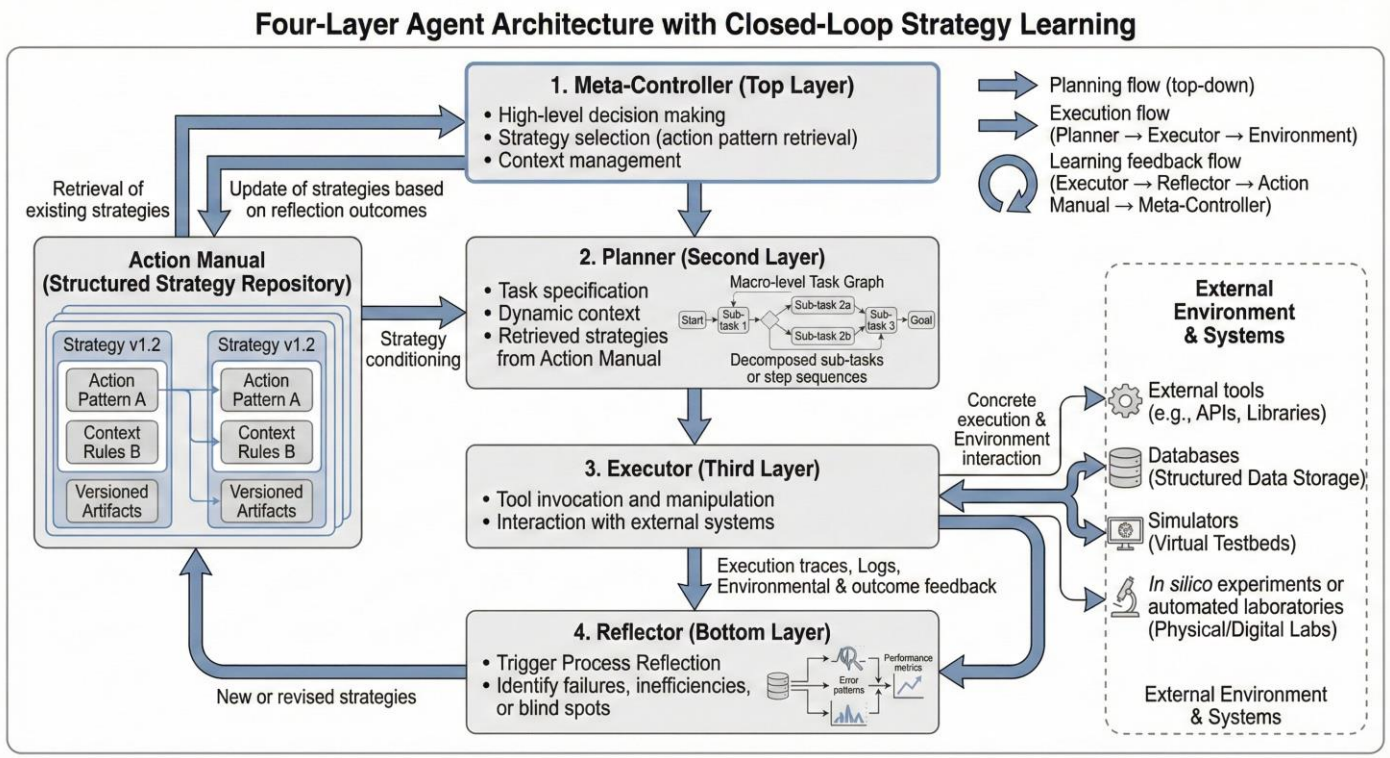
闭环学习的意义



- 持续自我改进：随着任务数量和多样性增多，智能体不断积累经验，将成功/失败的教训转化为策略，提升未来表现。
- 增强泛化能力：Action Manual 中积累的模式 / 策略，并不局限于单个任务，可跨任务、跨子领域 (subdomains) 复用/适配。
- 降低对人为干预（Human in the Loop）的依赖：初期可能需要人工审查 candidate 策略；但长期目标是使系统能自动选择/验证 /优化策略。
- 提高可靠性&可解释性：与黑箱模型不同，“行动手册 + 策略集合”是结构化和可审查的，为高风险领域（如医学）的信任、安全、合规提供基础。

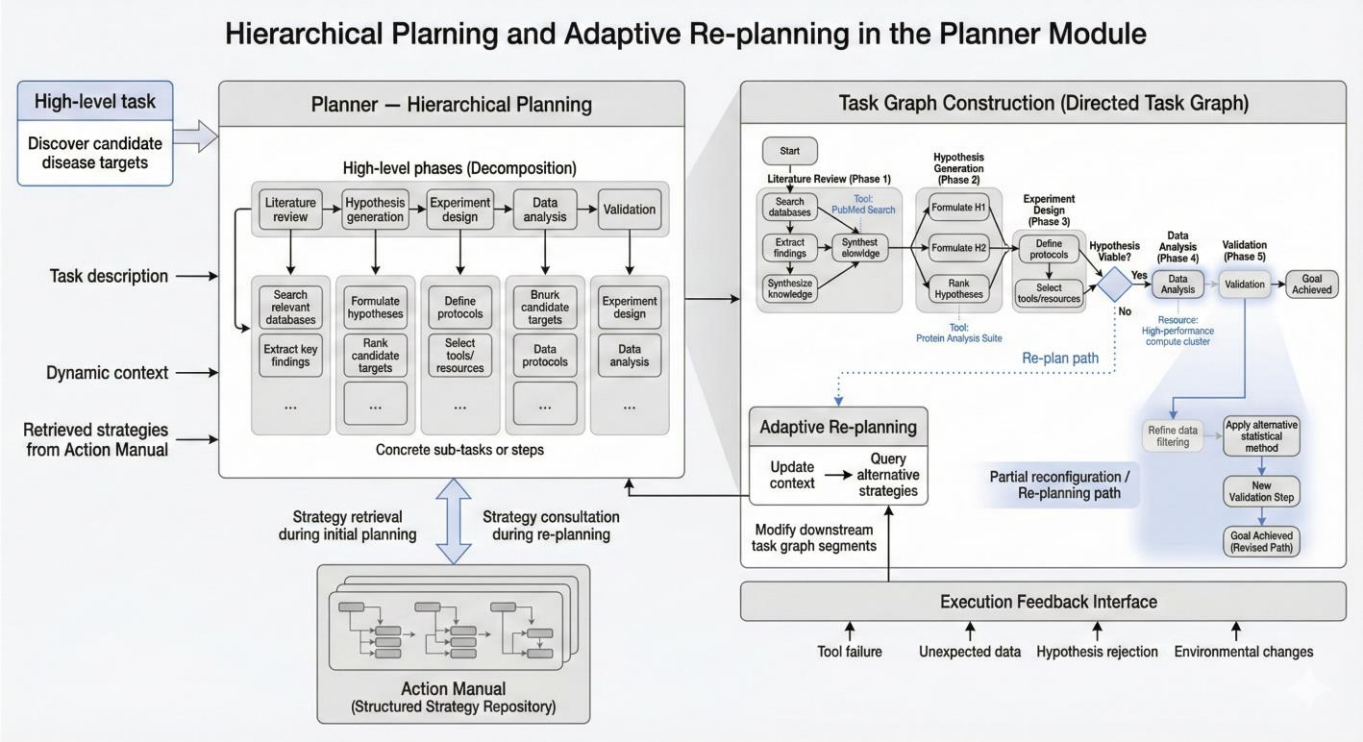
03 关键过程算法实现

系统架构总体设计 — 四层智能体模型



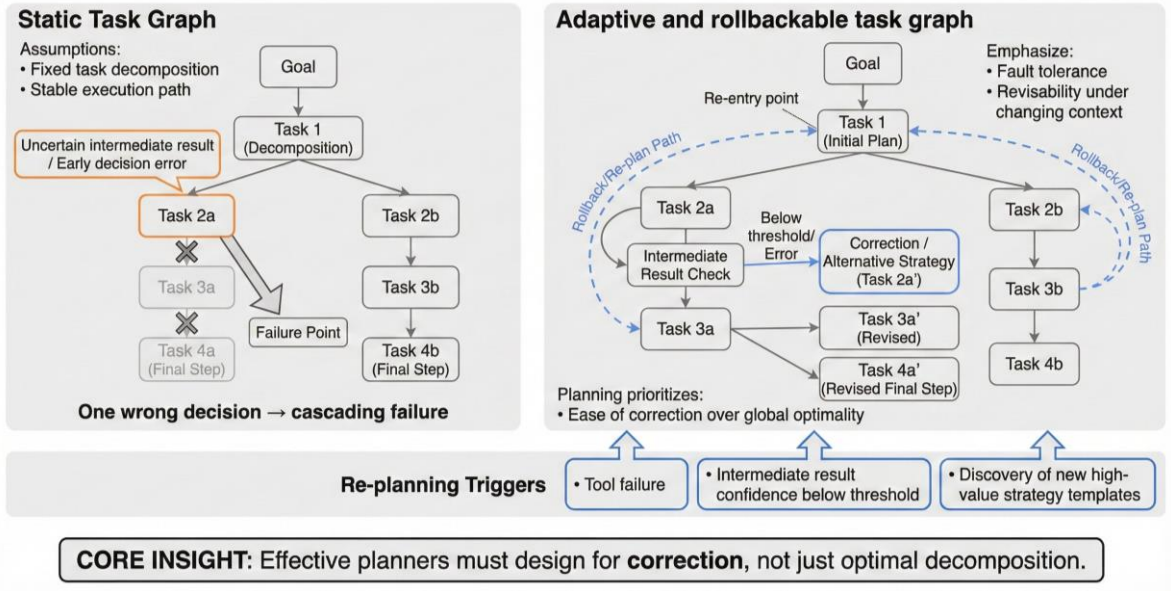
- 元控制器（Meta–Controller）— 负责高层决策、策略选择（调用何种子策略/action pattern）、背景 context 管理（包括 Action Manual 的检索/更新）。
- 规划器（Planner）— 基于任务描述 + 当前上下文生成宏观任务图（Task Graph），并负责分解成子任务/步骤。
- 执行器（Executor）— 执行器负责具体工具调用/操作（tool invocation/manipulation），包括与外部工具、数据库、模拟器、实验平台（in silico 或自动化实验室）的交互。
- 反思器（Reflector）— 负责根据执行结果、执行轨迹（execution trace）与反馈（environmental/ outcome feedback）启动反思机制，并将学到的新策略注入 Action Manual。

Planner 模块 — 分层规划 + 自适应重规划



- 分层规划（Hierarchical Planning）：Planner 利用 Action Manual 里的策略 + 当前上下文（动态）将高层任务（如“发现疾病候选靶点”）分解为若干子任务（文献调研 → 假设生成 → 实验设计 → 数据分析 → 假设验证）。
- 融合Task Graph + 子任务/步骤，清晰表示任务依赖、资源/工具使用、任务顺序、条件/分支（branching）等信息。
- 自适应重规划（Adaptive Re-planning）：在执行过程中（或执行失败 / 中断 /环境变化时），当环境反馈或中间结果偏离预期时（例如工具失败、数据不符合预期、假设被否定等），Planner 根据最新上下文（包括反馈 + 报告）+ Action Manual 的建议，重新规划后续步骤 /路径。

Planner 的第一个大坑：静态 Task Graph



有效的 Planner 不只是生成任务拆解，还要设计“可修正控制机制”。

1）初版设计

- 使用树状 / 有向无环图（DAG）表示任务分解
- 假设分解后的路径是稳定的

2）实际问题

- 中间结果可信度不确定：中间预测 / 推断往往不可靠，可能导致整条路径不稳
- 一步错 → 后续全错：如果 early decision 是错的，会导致“所有后续执行”的无效

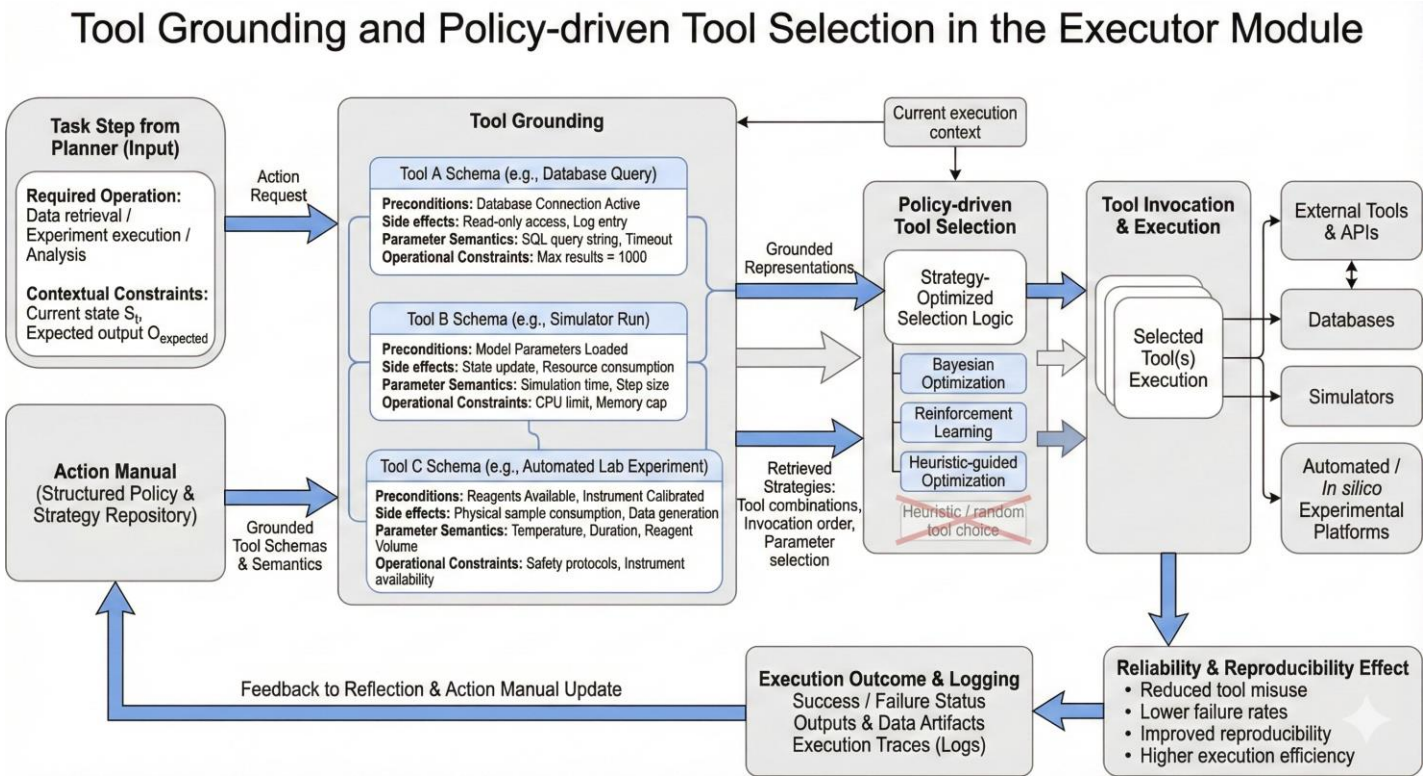
3）改进方案

- 可回滚子图（rollbackable subgraph）：相当于“容错路径”，允许在上下文变化后回滚到合适节点
- 规划不再追求最优，而是“易修正”：保证路径即使偏离也易于修正

4）重规划触发条件示例

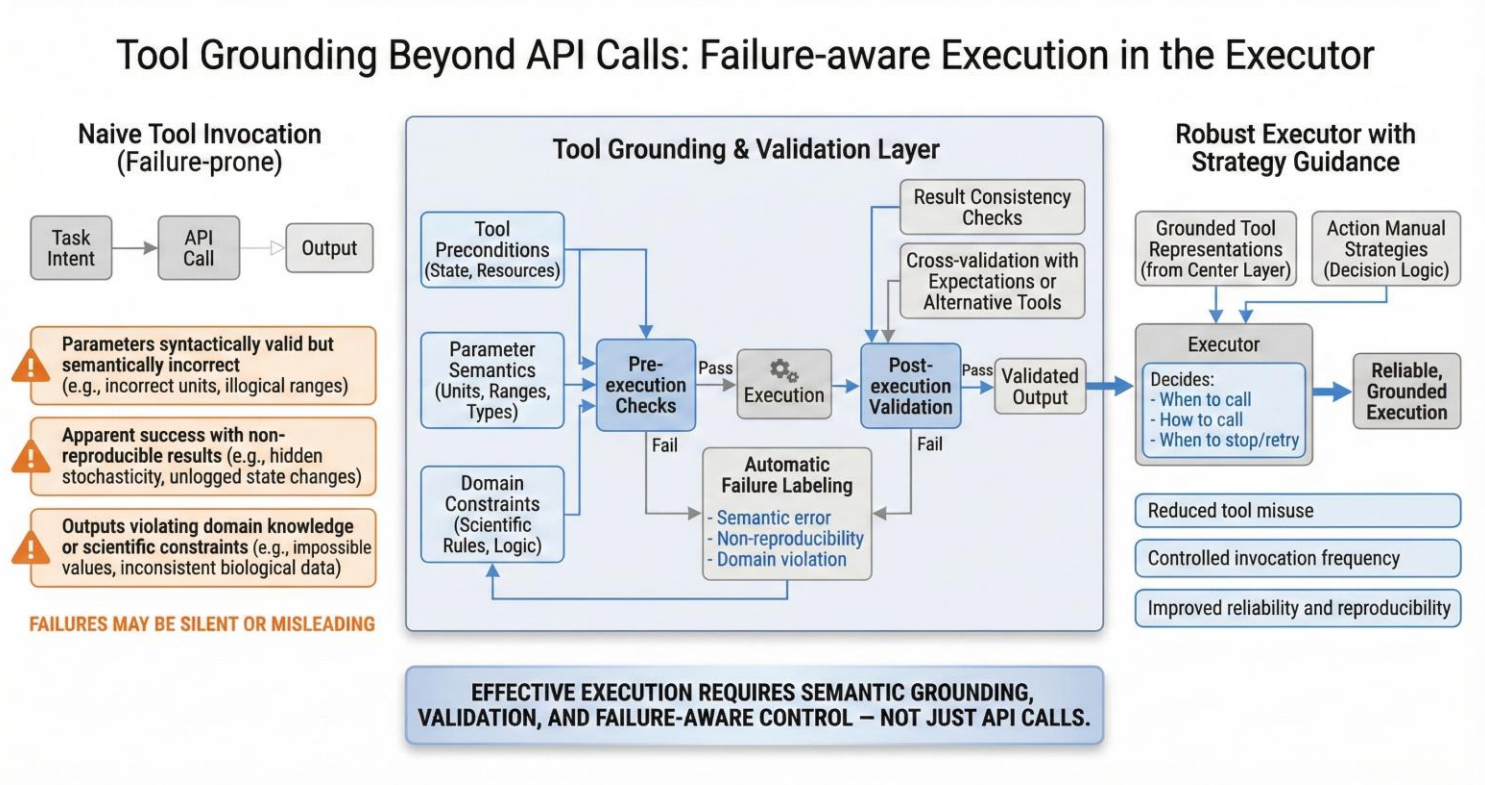
- 任何工具失败
- 中间结果偏离预期阈值（confidence threshold）
- 发现新的高价值策略模板

Executor 模块 — Tool Grounding与策略驱动工具选择



- Tool Grounding：不仅仅是简单 API 调用，而是让智能体理解工具的先决条件（preconditions）、副作用（side-effects）、参数语义（parameter semantics）—— 相当于让 LLM“理解工具真实行为与限制”。
- 策略驱动（Policy-driven）工具选择：使用 Action Manual 中记录的策略 /工具组合 + 调用顺序 + 参数选择。可以结合贝叶斯优化（Bayesian Optimization）、强化学习（Reinforcement Learning）或 heuristic selection，替代传统启发式（heuristic）/随机（random）选择。
- 这种设计可以减少因工具误用或误调用引起的大规模失败/不可重复性（non-reproducibility），并提高工具调用效率 &可靠性。

Executor 的真实挑战：Tool Grounding ≠ API 调用



1) 三种工具失败形态

- 参数合法但语义错误：结果看似成功，但语义上与任务目标不符
- 工具成功但结果不可复现：一次成功 ≠ 始终有效
- 工具成功但违背领域常识

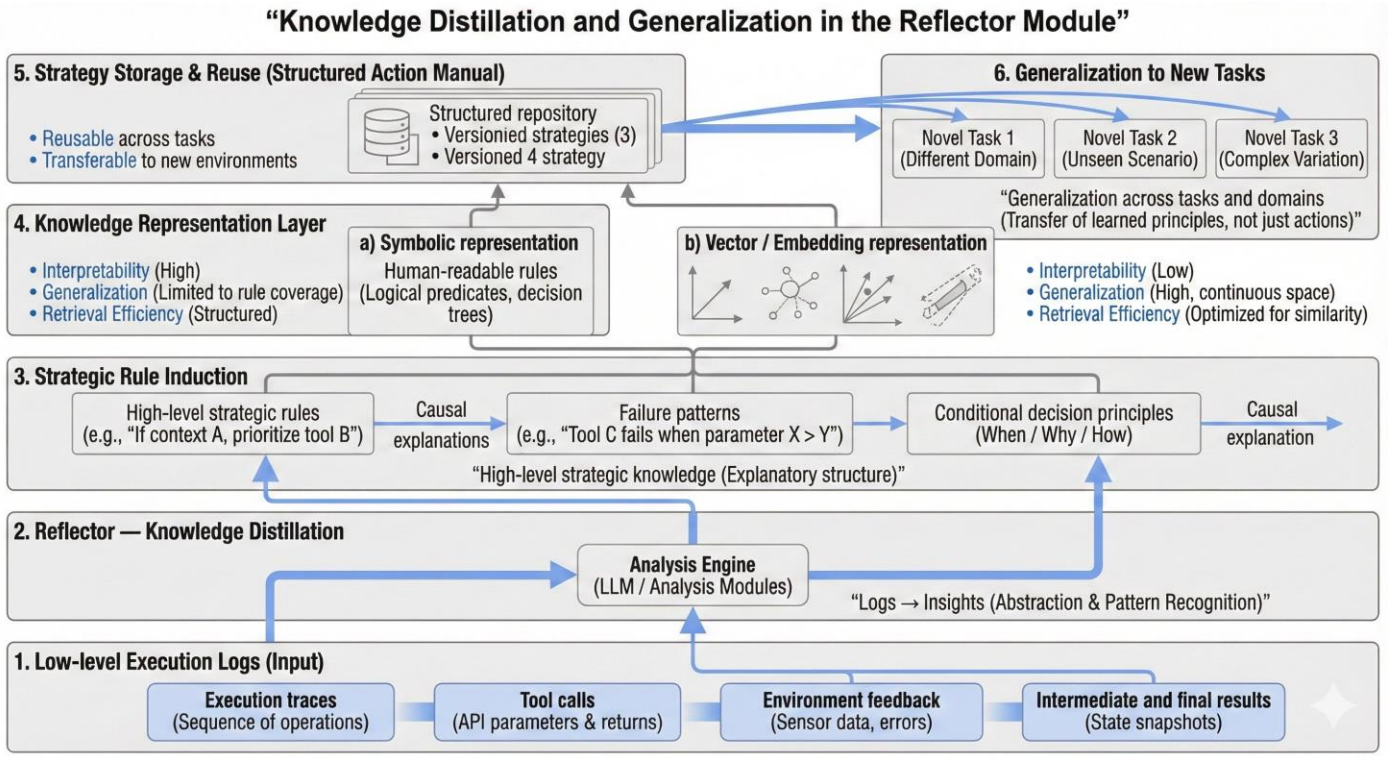
2) Executor 的应对策略

- 工具先决条件检查：执行前验证参数逻辑有效性
- 结果一致性验证：多次交叉验证输出与预期是否一致
- 失败类型自动标注：不同失败路径用不同标签指导后续处理

3) Action Manual 如何减少工具滥用

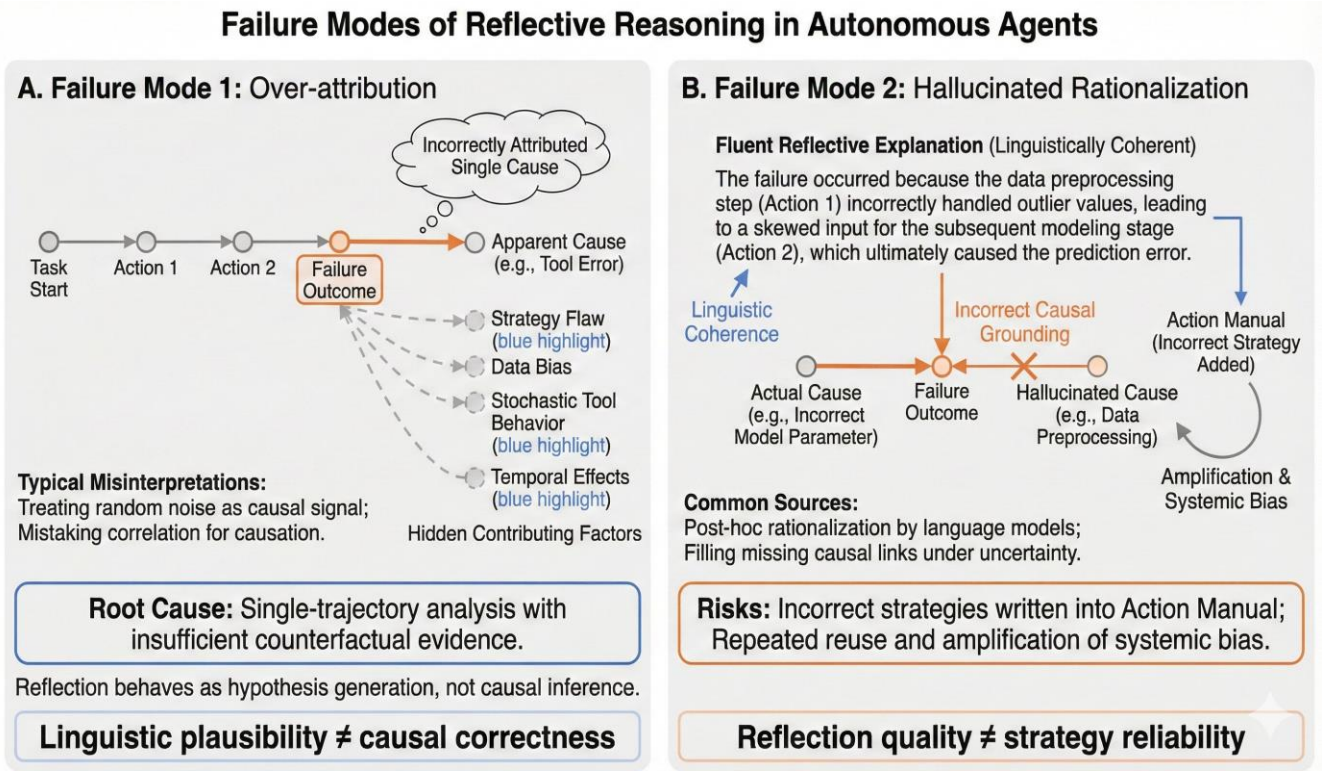
- 指导何时调用工具、如何调用，并防止过度调用

Reflector 模块 — 知识蒸馏与泛化



- 从日志到洞察（logs → insights）：Reflector 将低阶的执行日志（low-level logs / trace + tool calls + environment feedback + results）输入到大模型 /分析模块，由其抽象为高阶策略规则（high-level strategic rules）。
- 知识表示与存储：探讨将这些策略规则以符号化（symbolic）或向量化（embedding / vector）形式存储，以平衡可解释性（interpretability）、泛化能力（generalization）与检索 /执行效率（retrieval / runtime efficiency）。
- 这样可以让智能体不仅"记住"以前做过什么，还"理解"为何这样做（why / when / how），并在新任务 / 环境下泛化（generalize）使用。

Reflector 的第一个问题：反思一开始是“不可信的”



1）过度归因（Over-attribution）

- 现象：Reflector 倾向于把一次失败归因为某一个“看似合理”的单一因素；实际上失败往往来自 多因素耦合（策略 × 数据 × 工具 × 时序）
- 典型误判模式：将随机噪声当作因果因素；将结果相关性误判为因果关系
- 本质原因：单次任务轨迹（single trajectory）样本量极小；缺乏跨任务对照，无法进行稳健因果推断

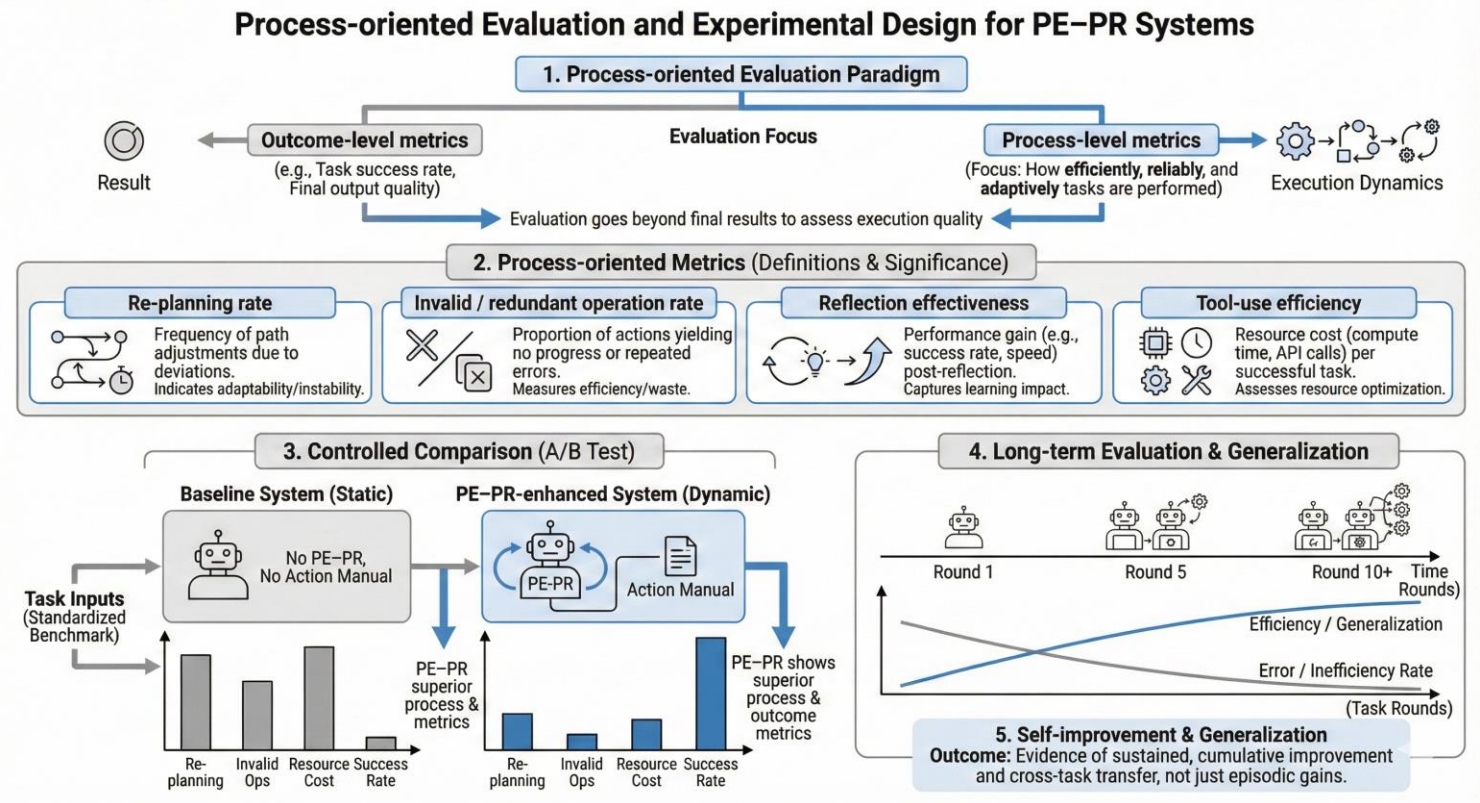
在这一阶段，“反思”更像是假设生成器，而不是可靠的因果解释器

2）编造“合理原因”（Hallucinated Rationalization）

- 现象：反思输出在语言上高度自洽、逻辑通顺；但与真实失败原因不一致
- 常见来源：LLM 的 post-hoc rationalization 倾向；在信息不充分时“补全因果链”
- 风险：错误策略一旦写入 Action Manual，会被反复调用；形成“系统性偏差放大”

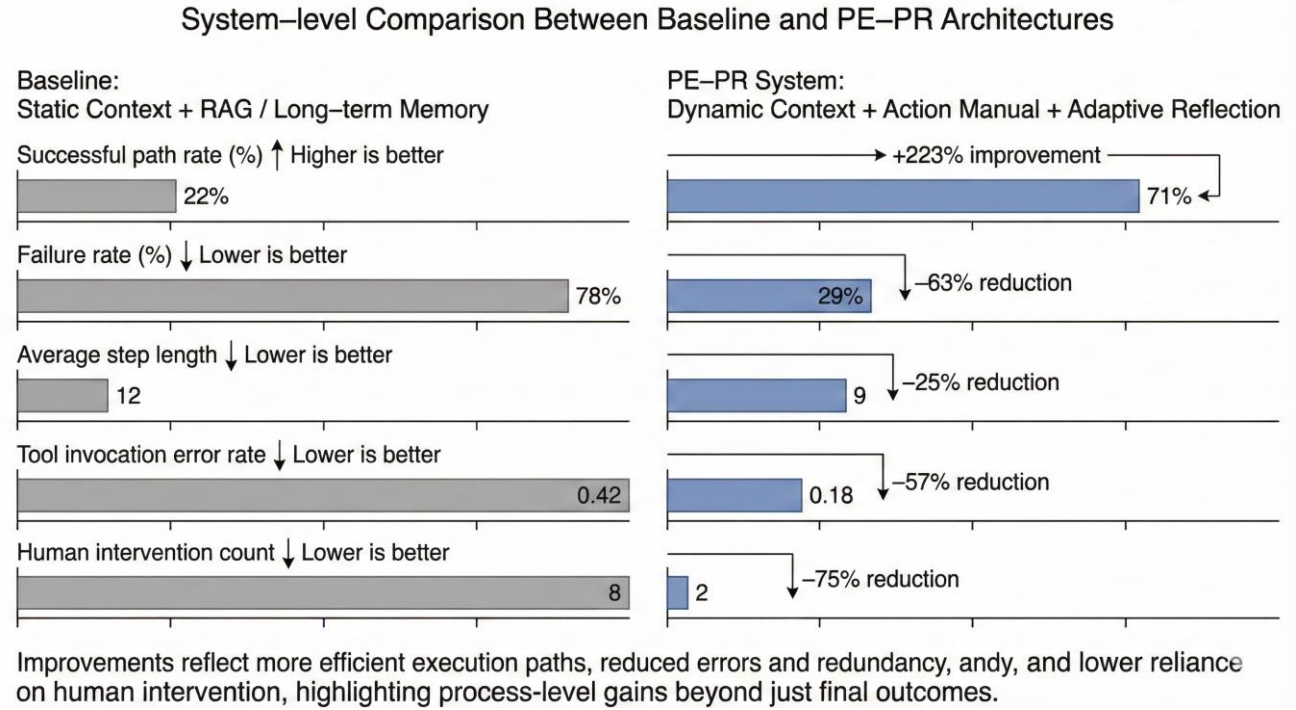
04 实验、评估与挑战

评估与实验设计 — 如何衡量与验证



- 评估范式（Evaluation Paradigm）：不仅关注最终结果，还强调过程导向（process-oriented）的指标（metrics），包括：
  - 规划修正率
  - 无效/冗余操作率
  - 反思（reflection）有效性：即反思后策略是否能改善后续任务表现
  - 工具调用/资源利用效率
- 对比实验（A/B Test）：对比传统静态上下文系统（baseline）和引入 PE-PR + Action Manual 的系统，观察两者在上述指标上的差异。
- 长期考察（Long-term evaluation）：通过多轮任务、多样任务（不同疾病 /研究方向 /数据类型），考察智能体是否真正“自我进化（self-improve）”/能力泛化。

Before / After PE–PR（1w+ Test Cases）



对比系统定义

Baseline：静态上下文 + RAG / 长记忆

PE–PR 系统：动态上下文 + Action Manual + 自适应反思循环

关键对比指标

指标	Baseline	PE–PR System
成功路径率	22%	71%
失败率	78%	29%
平均步骤长度	12	9
工具调用错误率	0.42	0.18
人工介入次数	8	2

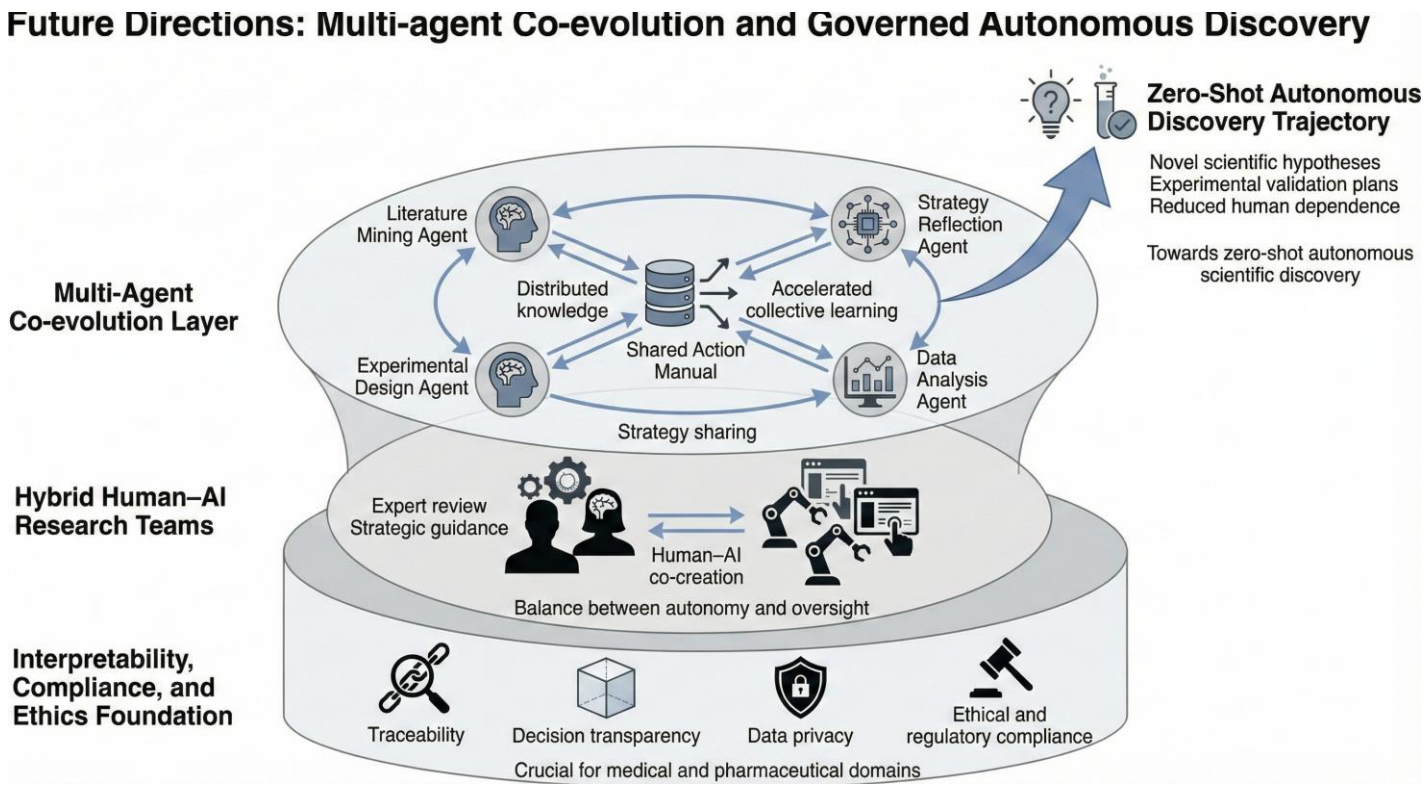
当前挑战与潜在风险


1
稳定性—可塑性困境
系统需要不断学习新策略 (plasticity)，但又不能轻易遗忘 /破坏之前已验证的旧策略 (stability)，如何平衡二者是关键挑战。
2
计算开销 vs 性能
反思 (Reflection) 模块 + 模式挖掘 (Pattern Exploration) 会带来额外计算开销/延迟 (latency)，可能影响响应速度/实时性。
3
人机协同的设计问题
在高风险 /高不确定性领域 (如医学)，完全自动化可能不安全。如何设计可信、有效的人工机制 (human-in-the-loop) 是必须解决的问题。
4
数据 /工具异构性
不同任务可能依赖不同类型的数据 (omics，clinical，literature)、工具 (模拟器、数据库、实验平台)，如何统一 &兼容仍是挑战。

05

挑战、展望与未来方向

评估与实验设计 — 如何衡量与验证



- 多智能体协同进化（Multi–Agent Co–evolution）：构建共享Action Manual 的AI Scientist 群体，不同 agent 擅长不同子任务（文献调研、实验设计、数据分析、策略反思等），实现分布式知识/策略共享，加速collective learning。
- 迈向零样本自主发现（Zero–Shot Autonomous Discovery）：当 Action Manual 达到足够复杂性和完备性后，有可能实现智能体在无（或极少）人类干预 /领域知识输入下，自主生成全新、有价值的科学假设，并推动实验 /模拟验证。
- 混合人机协作（Hybrid Human–AI Research Teams）：设计人工干预 /审查机制 、人机知识协同，在保证可靠性、合规性、安全性的前提下发挥最大效率。
- 可解释性、合规性与伦理框架：特别是在医学 /药物领域，需要考虑可追踪性（traceability）、策略/决策透明性（transparency）、数据 /隐私 /伦理合规（compliance, privacy, ethics）等。

极客邦科技 2026 年会议规划

促进软件开发及相关领域知识与创新的传播

参会咨询

查看会议

4月 · 北京 · 1200人

QCon 全球软件开发大会

会议时间：4月16-18日

- Agentic Engineering
- AgentOps
- 下一代模型架构与推理优化
- AI 原生基础设施
- 知识工程实践
- AI 安全

6月 · 上海 · 1000人

AiCon 全球人工智能开发与应用大会

会议时间：6月26-27日

- AI Infra 系统工程
- 多 Agent 协作与实践
- 多模态融合
- 模型训练与推理创新
- 数据平台与特征服务

8月 · 深圳 · 1000人

AiCon 全球人工智能开发与应用大会

会议时间：8月21-22日

- Agentic AI
- 轻量化与高效推理
- 多模态应用
- AI + IoT 场景实践
- AI 工业化落地

10月 · 上海 · 1200人

QCon 全球软件开发大会

会议时间：10月22-24日

- AI Agent
- Vibe Coding
- 智能可观测
- 推理基建
- 模型攻防
- AI x 创造力

12月 · 北京 · 1000人

AiCon 全球人工智能开发与应用大会

会议时间：12月18-19日

- 大模型架构创新
- 多模态 AI 产业融合
- 具身智能
- AI for Science
- 大模型安全

InfoQ 极客传媒

InfoQ 极客传媒

THANKS

探索 AI 应用边界

Explore the limits of AI applications

AiCon

全球人工智能开发与应用大会