GOPS 2024
shenzhen

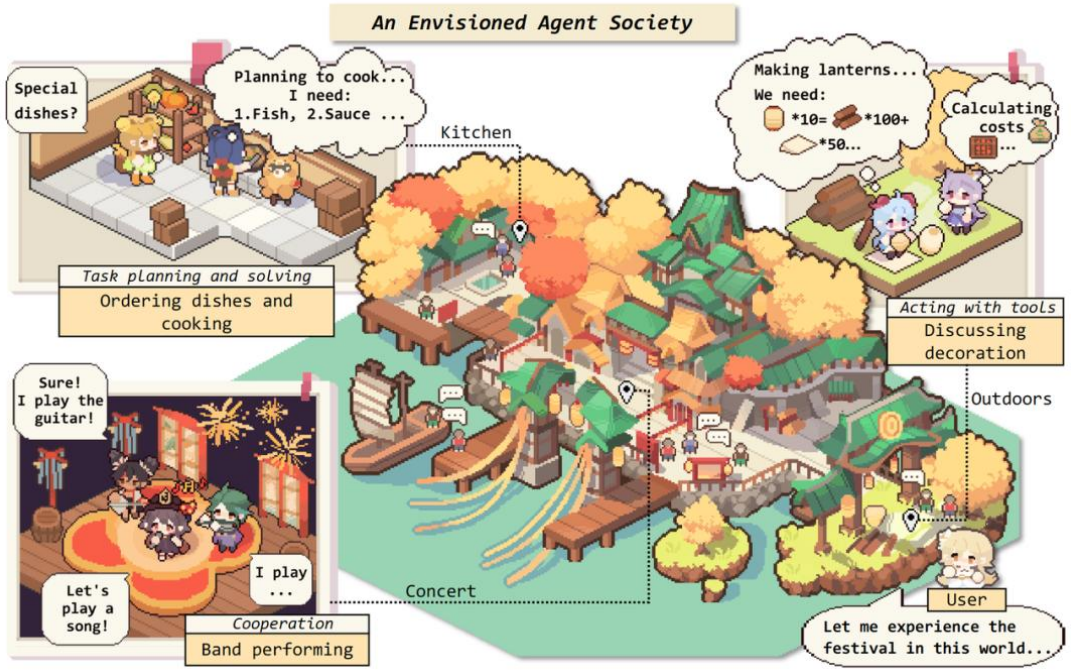
目录

content

PART 01

Agent的背景

大模型下的Agent

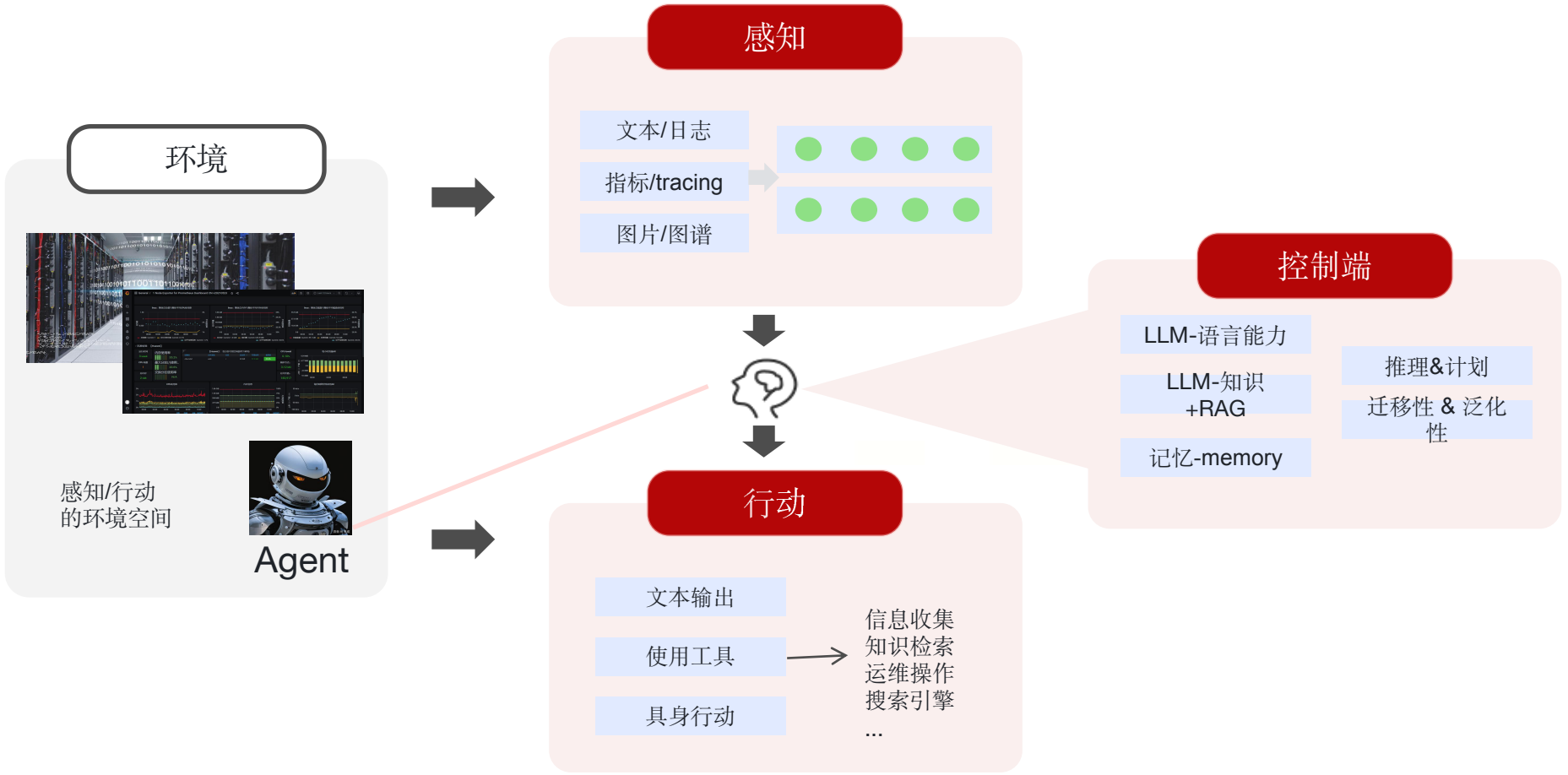


设想一个由智能代理构成的和谐社会，人类也可以参与其中。场景取材自《原神》中的海灯节。

LLM base Agent

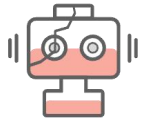
- LLM：通用人工智能-语料->互联网-NLP->多模态
- Agent = LLM+Planning+Feedback+Tool use
- 在LLM语境下，Agent可以理解为某种能自主理解、规划决策、执行复杂任务的智能体。
- Agent并非ChatGPT升级版，它不仅告诉你“如何做”，更会帮你去做。如果CoPilot是副驾驶，那么Agent就是主驾驶。

Agent的一个框架



1. 帮助用户从日常任务、重复劳动中解脱出来，减轻人类的工作压力，提高解决任务的效率；
2. 不再需要用户提出显式的低级指令，就可以完全自主的分析、规划、解决问题；
3. 在解放用户的双手以后，尝试解放大脑：在前沿科学领域充分发挥潜能，完成创新性的、探索性的工作。

常见的Agent分类

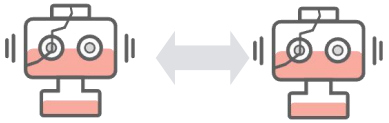


单Agent

任务导向

创新导向

生命周期导向



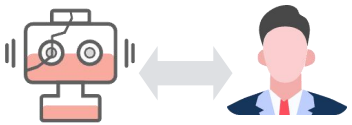
多Agent

有序合作型互动

无序合作型互动

对抗型互动

混合型



人机交互

人工指导

平等合作

生成式LLM->单Agent->多Agent

- 自治的任务Agent->反思/拆解/规划+自动工具执行->Agent
- 思考的快与慢：sys1 sys2->复杂任务->Agent
- 人类简史：穴居人vs智人-> 量变引质变，多样性，社会性->Multi-Agent
- 记忆脑：工作记忆、笔记: 短/长memory；做梦->FT

常见的Agent的类型，分为单Agent，多Agent，和人机交互。其中单/多Agent类型是完全自治

Agent的通用框架

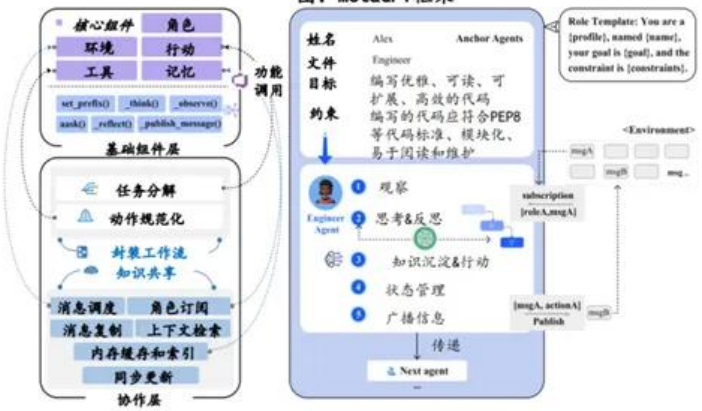
- AutoGPT
- BabyAGI
- Langfuse
- HuggingGPT
- XAgent：“双循环”结合；

plan,dispatch,act

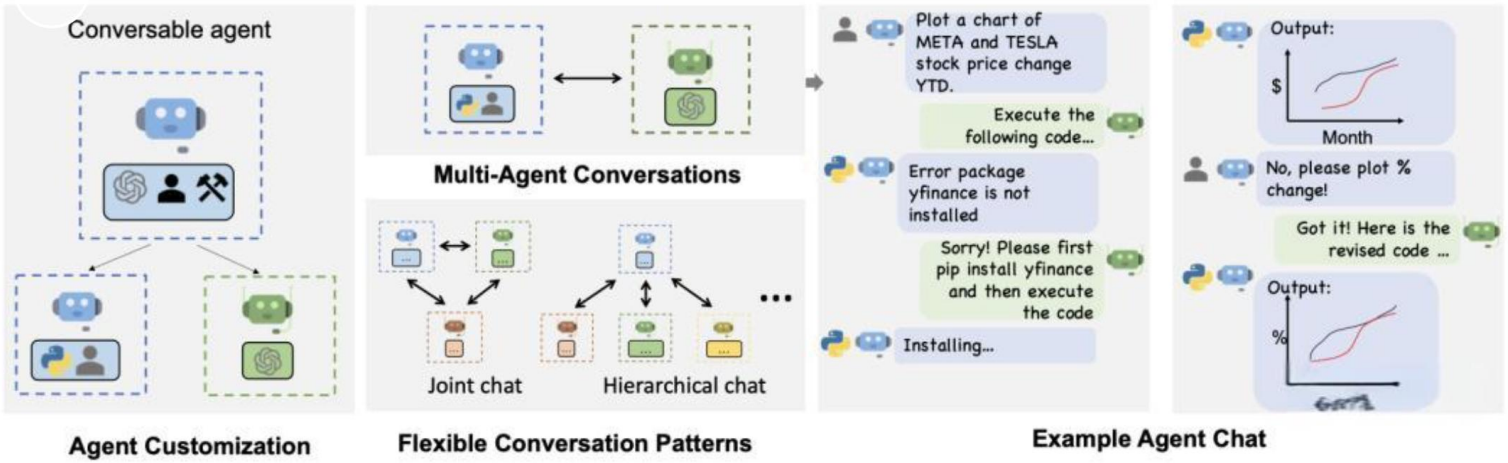
- AutoGen
- MetaGPT
- ChatDev
- ...

图：MetaGPT的智能体以SOP形式合作

图：MetaGPT框架



资料来源：深度赋智，东吴证券研究所



比传统AIOps的优势

1. 流程：使用Agent的planning的能力，实现分析/执行等任务的自动化执行。

2. 整合：工具和数据的整合，可以利用反思和工具调用，实现传统工具的调用，不同类型数据自动分析。

3. 知识：利用LLM和RAG的方式，充分利用公域和私域的知识，能更好的优化运维相关的分析和操作场景

4. 交互：从web页面的交互方式，向“对话”的交互方式转变，降低交互复杂度。

5. 编程：通过编程能力，可以实现故障自愈，性能优化等场景。

带给AIOps的新的机遇

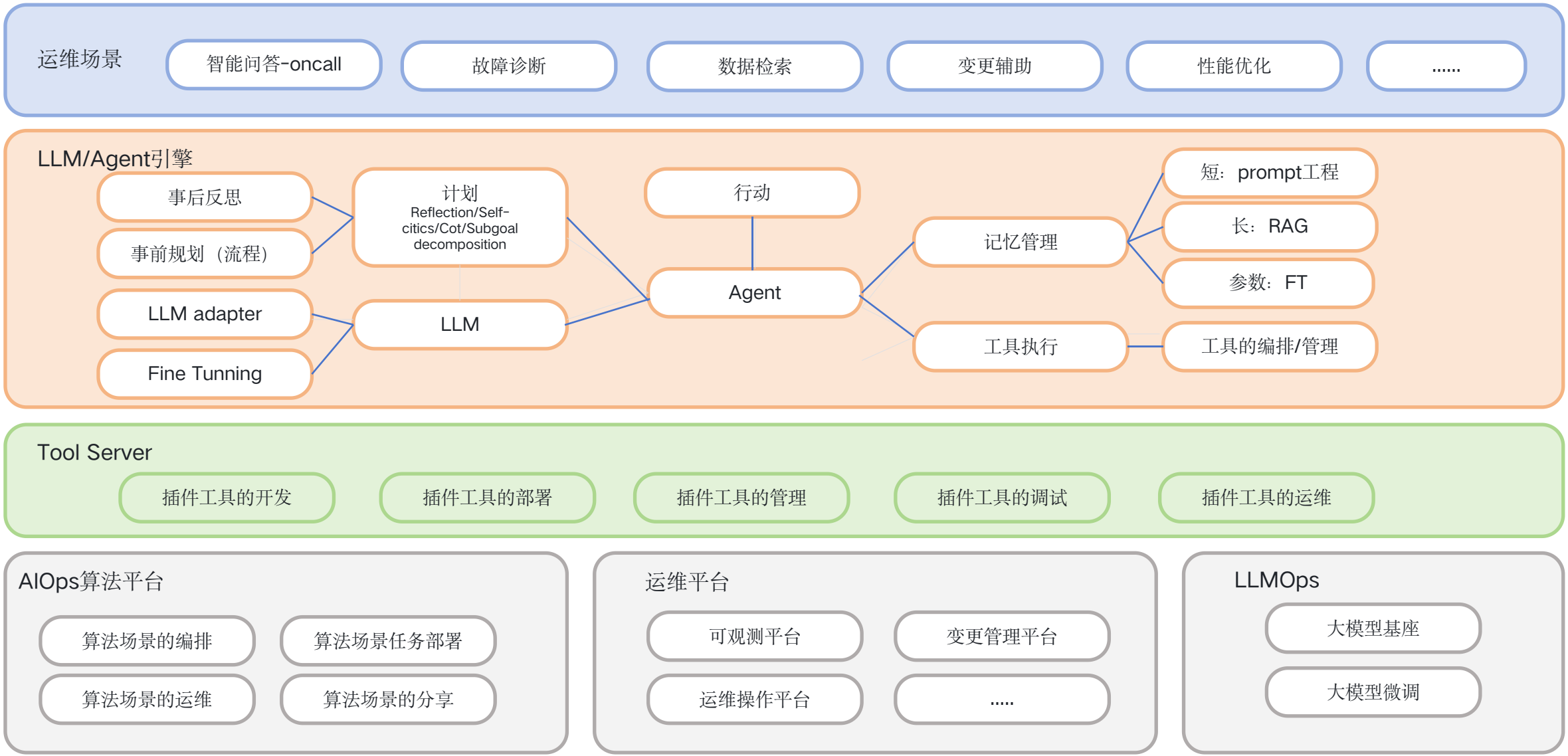
	过去	现在
异常检测	依赖定制分析，难于利用多模态的数据	利用Transformer架构，使用多模态数据 MetricFM　LogFM　.....
故障诊断	依赖专家经验，人工调试观察，固定流程	大模型自动诊断Agent FT/RAG　工具的使用　单/多Agent
故障修复	依赖人工处理，自动化程度低	大模型自动修复-自治，计划/反思 FT/RAG　工具的使用　单/多Agent coding　自治规划
告警收敛	依赖规则，自适应度低	利用大模型的语义相似+KG进行收敛 多模态　规划/反思
ChatOps	依赖编排，智能程度不高	利用大模型实现辅助+自治 意图/计划　工具的使用

GOPS 2024
shenzhen

PART 02

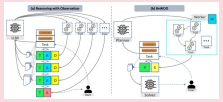
AI Agent的建设实践

LLM Agent基础架构



LLM Agent的常用范式/方法

反思（Reflection）



LLM 检查自己的工作，以提出改进方法。
通过反思提升单次回答的效果。与CoT相似

工具使用（Tool Use）

LLM 拥有网络搜索、代码执行或任何其他功能来帮助其收集信息、采取行动或处理数据。可使用ReAct和function call的方式

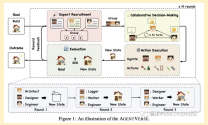
规划计划（Planning）

LLM 提出并执行一个多步骤计划来实现目标。可以先规划后执行，也可以逐步反思和任务拆解来规划任务。

记忆管理（RAG/prompt）

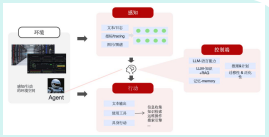
LLM通过检索等方式补充知识，方式回答的幻觉，更新最新的知识。prompt给予短期的记忆，给予指令。

多智能体协作（Multi-Agent）



多个 AI 智能体一起工作，分配任务并讨论和辩论想法，以提出比单个智能体更好的解决方案。

环境互动/人工介入



通过感知和工具的使用，实现对于环境感知和互动，并通过工具的学习，实现工具库。
通过人工介入实现半自治。

基于可编排的平台，使用常用的范式和工具，根据具体的运维场景进行定制化的编排。
协作方式：对话+工具+反思->角色+协作方式+规划/流程+具身
创新性：知识要补充+更新，生成式的模型的Temperature要合理，prompt要引导
自学习：要格式化总结知识和问答
突破token限制：attention重构，RAG+compress，大模型重构