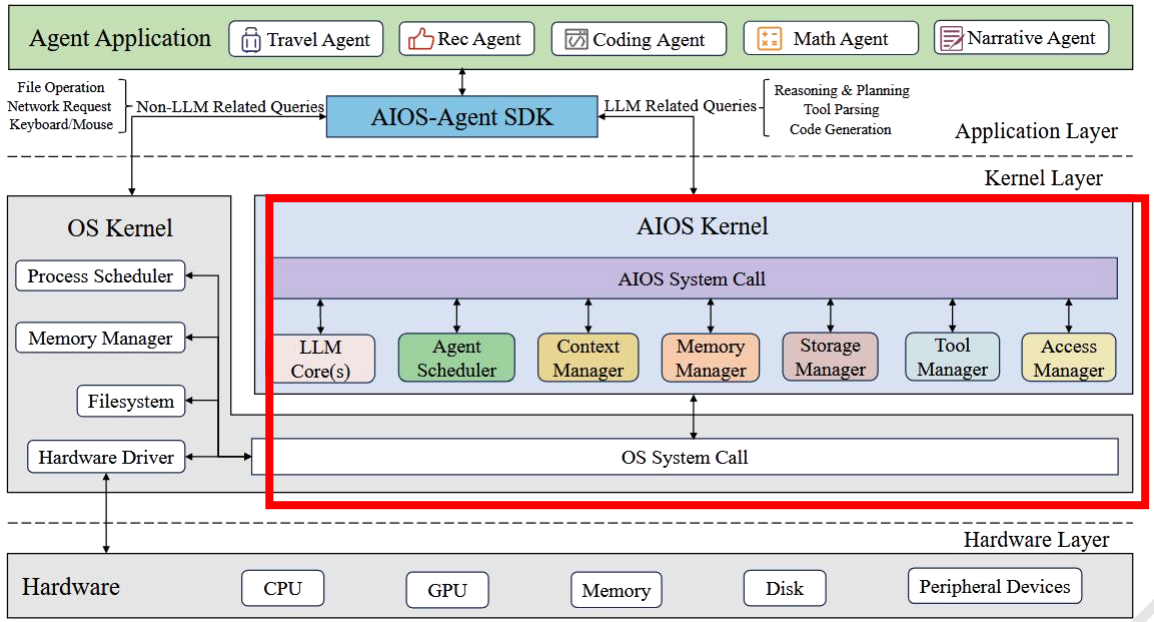
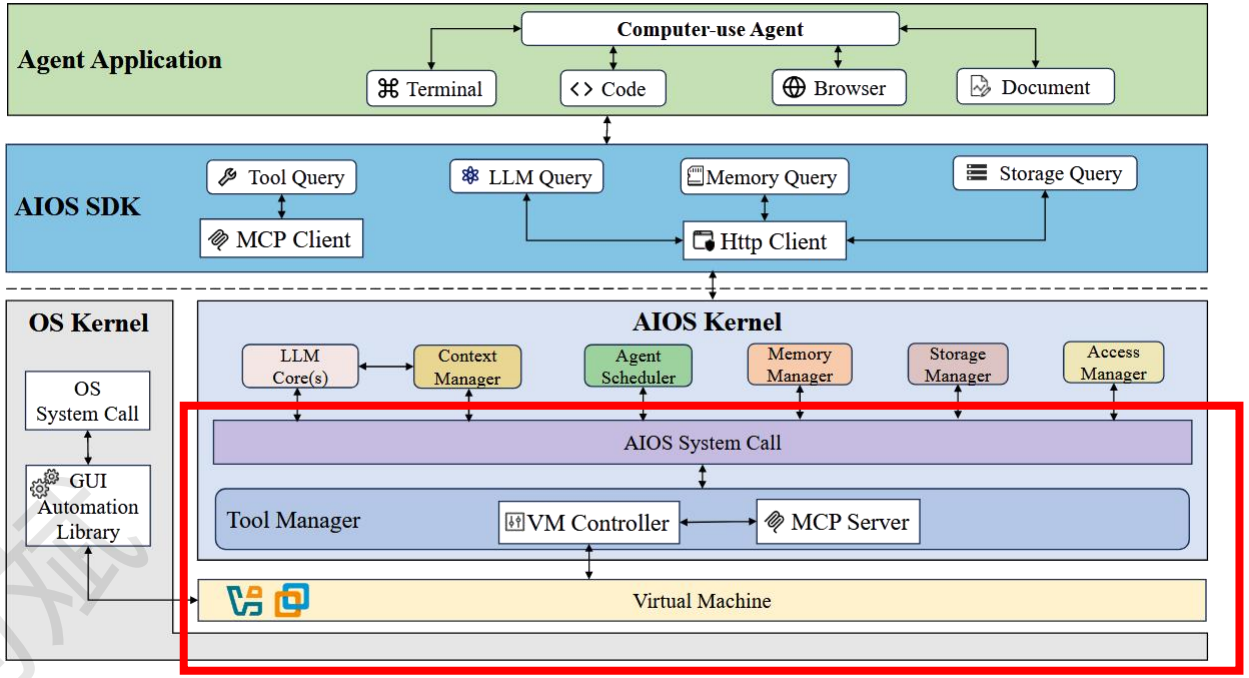


【来自AIOS: LLM Agent Operating System】



【来自LiteCUA】

AIOS call -> OS call

AI kernel -> OS kernel

AIOS call ->(tool manager) -> OS call

【在一个统一的GUI/环境上】

其中，【楷体】中内容为我的个人解读，不一定准确见谅。

FROM 马斌 2025.7.17

MCP 协议：Agent的语义理解 <-> 计算机可执行的操作命令

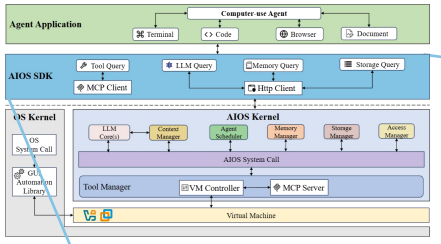
点击GUI图标 GUI控制信号

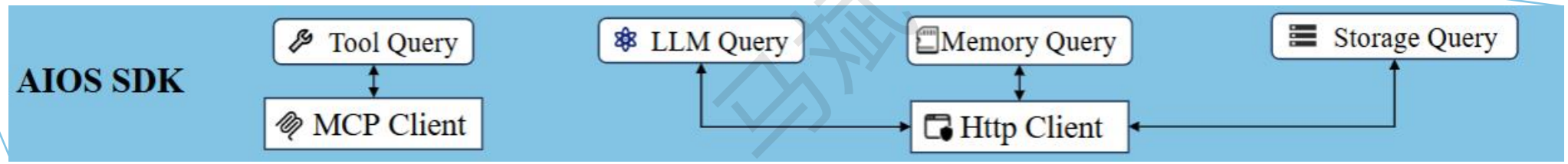
【计算机无法理解】

HTTP 协议：Agent命令 <-> 计算机系统中基础资源

请求LLM生成推理结果 LLM、内存、存储

【计算机可以理解】





【抽象的操作，计算机不理解，要专门的MPC去转义】

Tool Query

点击Chrome图标

click(100,100)

MCP Client

通过VM Controller在沙盒环境中执行

“写一封邮件”

LLM Query

打开邮件客户端

Memory Query 上一步操作是否成功

Storage Query 读取本地文件、保存生成文档

Http Client

“AIOS call”

再交给传统OS，去完成具体任务

“OS call”

【以上三种请求本身属于传统的数据层面查询或调用，无需语义映射计算机就可以理解。所以直接沿用Http协议就行】