SỔ TAY TÁC TỬ AI & QUẢN TRỊ NGỮ CẢNH

AI Agents & Context Engineering Handbook

> **Tóm tắt tài liệu:** Sổ tay tổng hợp kiến thức toàn diện về Tác tử AI (AI Agents), cơ chế Gọi hàm (Function Calling), Kỹ thuật Quản trị Ngữ cảnh (Context Engineering) và Kiến trúc Tác tử Chuyên sâu (Deep Agents). Được biên soạn dựa trên bộ tài liệu chính thức từ Prompt Engineering Guide.

Thông tin	Chi tiết
Chủ đề	AI Agents, Context Engineering, Function Calling, Multi-Agent Systems
Tác giả / Nguồn	Prompt Engineering Guide (promptingguide.ai)
Ngôn ngữ	Tiếng Việt (Thuật ngữ chuyên ngành giữ nguyên tiếng Anh)
Định dạng Font	Times / Serif (Noto Serif - Hỗ trợ chuẩn Unicode Tiếng Việt cho MacOS)

LỜI NÓI ĐẦU

Sự phát triển của các Mô hình Ngôn ngữ Lớn (LLM - Large Language Models) đã mở ra một kỷ nguyên mới trong trí tuệ nhân tạo. Tuy nhiên, việc dừng lại ở các phản hồi văn bản đơn thuần không đủ để giải quyết các bài toán phức tạp trong thực tế. Sự dịch chuyển từ các mô hình tạo sinh tĩnh sang các **Tác tử AI tự chủ (AI Agents)** đang định hình lại cách chúng ta xây dựng phần mềm thông minh.

Cuốn sách này được thiết kế như một tài liệu hướng dẫn chuẩn mực, giúp các nhà phát triển, kĩ sư dữ liệu và chuyên gia AI hiểu rõ bản chất, kiến trúc cốt lõi và phương pháp tối ưu hóa Tác tử AI thông qua **Kỹ thuật Quản trị Ngữ cảnh (Context Engineering)**.

CHƯƠNG 1: TỔNG QUAN VỀ TÁC TỬ AI (INTRODUCTION TO AI AGENTS)

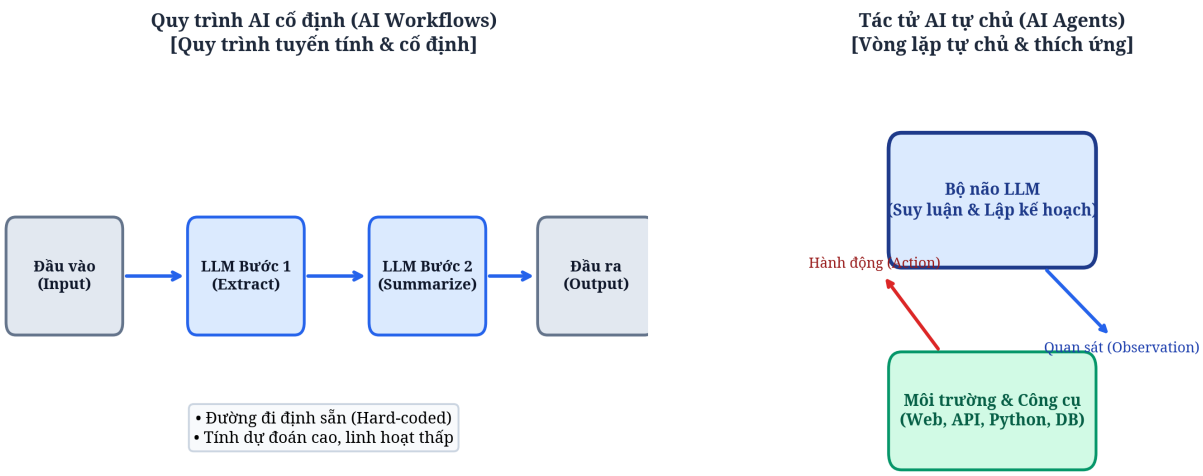
1.1 Định nghĩa Tác tử AI (AI Agent là gì?)

Tác tử AI (AI Agent) là một hệ thống tự chủ được vận hành bởi Mô hình Ngôn ngữ Lớn (LLM Core), có khả năng tự nhận thức môi trường, lập kế hoạch suy luận, đưa ra quyết định linh hoạt và tương tác với các công cụ bên ngoài (External Tools) để hoàn thành các mục tiêu phức tạp mà không cần sự can thiệp liên tục của con người.

1.2 Phân biệt Quy trình AI (AI Workflows) và Tác tử AI (AI Agents)

Sự khác biệt căn bản giữa Quy trình AI cố định và Tác tử AI tự chủ nằm ở **tính linh hoạt và khả năng ra quyết định (Decision-Making Autonomy)**:

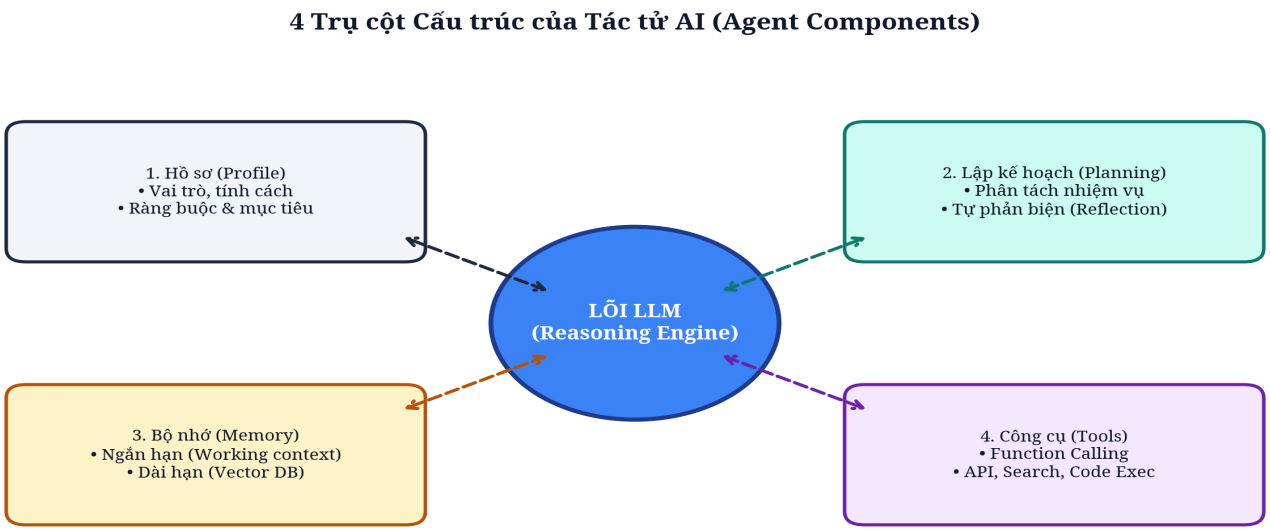
Tiêu chí so sánh	Quy trình AI (AI Workflows)	Tác tử AI (AI Agents)
Luồng thực thi (Execution Flow)	Cố định, định sẵn theo sơ đồ (Hard-coded / Deterministic)	Tự động điều chỉnh dựa trên phản hồi từ môi trường (Dynamic Loop)
Khả năng linh hoạt (Flexibility)	Thấp. Chỉ xử lý các bước được lập trình trước	Rất cao. Tự chọn công cụ và chiến lược xử lý
Khả năng tự sửa lỗi (Error Recovery)	Cần quy tắc xử lý lỗi ngoại lệ cố định (Fallback rules)	Tự phản biện (Self-Reflection) và thử lại bước khác
Trường hợp sử dụng (Use Cases)	Trích xuất dữ liệu, tóm tắt theo mẫu, định dạng văn bản	Nghiên cứu sâu, lập trình tự động, phân tích tài chính đa bước



Hình 1.1: Sơ đồ so sánh giữa Quy trình AI tuyến tính (AI Workflows) và Tác tử AI tự chủ (AI Agents).

CHƯƠNG 2: CÁC THÀNH PHẦN CỐT LÕI CỦA TÁC TỬ AI (AGENT COMPONENTS)

Một Tác tử AI hoàn chỉnh được cấu thành từ 4 trụ cột kiến trúc chính, xoay quanh Bộ não LLM (LLM Engine):



Hình 2.1: Kiến trúc 4 trụ cột cấu thành nên một Tác tử AI chuyên nghiệp.

Thành phần	Chức năng chính	Giải thích & Ví dụ cụ thể
1. Hồ sơ (Profile)	Định hình vai trò & ranh giới	Đóng vai trò như nhân dạng của Tác tử (ví dụ: 'Bạn là chuyên gia phân tích tài chính cao cấp'). Định hướng tông giọng và các rào cản an toàn (Guardrails).