



Introduction to Designing with AI Agents

Frantz Lohier, PhD – Sr AI and robotics strategist
Amazon AWS – WWSO organization



- Introduction and definitions, types of agents
- Agents and autonomy
- Architecture components
- Multi-agent architectures
- Popular agent frameworks

Agent ▶ AI/LLM Agent ▶ Agentic Workflow ▶ Agentic System

What is an Agent?

Any system that can:

- Perceive its environment
- Make decisions
- Take actions

Example: Thermostat

- Senses temperature (perception)
- Compares to threshold (decision)
- Turns heating on/off (action)

Graph representation:

>> Single node with I/O

Key point:

Agency doesn't imply complexity

What is an AI Agent?

An agent that uses AI/ML for one of its core function (e.g., ML pipeline)

Example:

- Robotics systems w/ computer vision
- Recommendation systems
- Game-playing AI

Graph representation:

>> Static graph (ML nodes)

Key point:

Not necessarily language based

What is an LLM Agent?

AI agent that uses LLM as core reasoning engine:

- Combines language model with tools/skills
- Takes natural language input
- Produces actions/outputs

Example: GitHub Copilot

- Perceives: Code context, comments
- Decides: What code to suggest
- Acts: Generates code completion
- Uses LLM for reasoning about code

Graph representation: central LLM node statically connected to:

- Input edges (context, prompts)
- Tool edges (APIs, functions)
- Output edges (actions, responses)

Key point:

There must be autonomous decision-making loop (LLM + Tools ≠ agent)

What is an Agentic Workflow?

Predetermined sequence of LLM operations:

- Fixed routing/branching logic
- No autonomous planning
- Tools/APIs called in defined order

Example: Support Ticket Classifier

- Input: Customer ticket
- LLM classifies severity
- Routes to correct department
- Reports classification reason

All steps pre-defined

Graph representation:

- Contains static feedback loops (cycles)
- Not all cycle graphs are agentic
- State flows between iterations

Key point:

Cycles enable learning and adaptation, but need purpose

What is an Agentic System?

Ecosystem of autonomous agents with emergent behaviors:

- Dynamic multi-agent collaboration
- Self-organizing capabilities
- No predetermined interaction patterns

Example: Team project assistant

- Agents choose their collaboration:
 - Research & Writing agent might pair up
 - Editor might work alone or with Writer
 - New agent roles can emerge
- Not a fixed workflow (Research→Writing→Editor)

Graph representation:

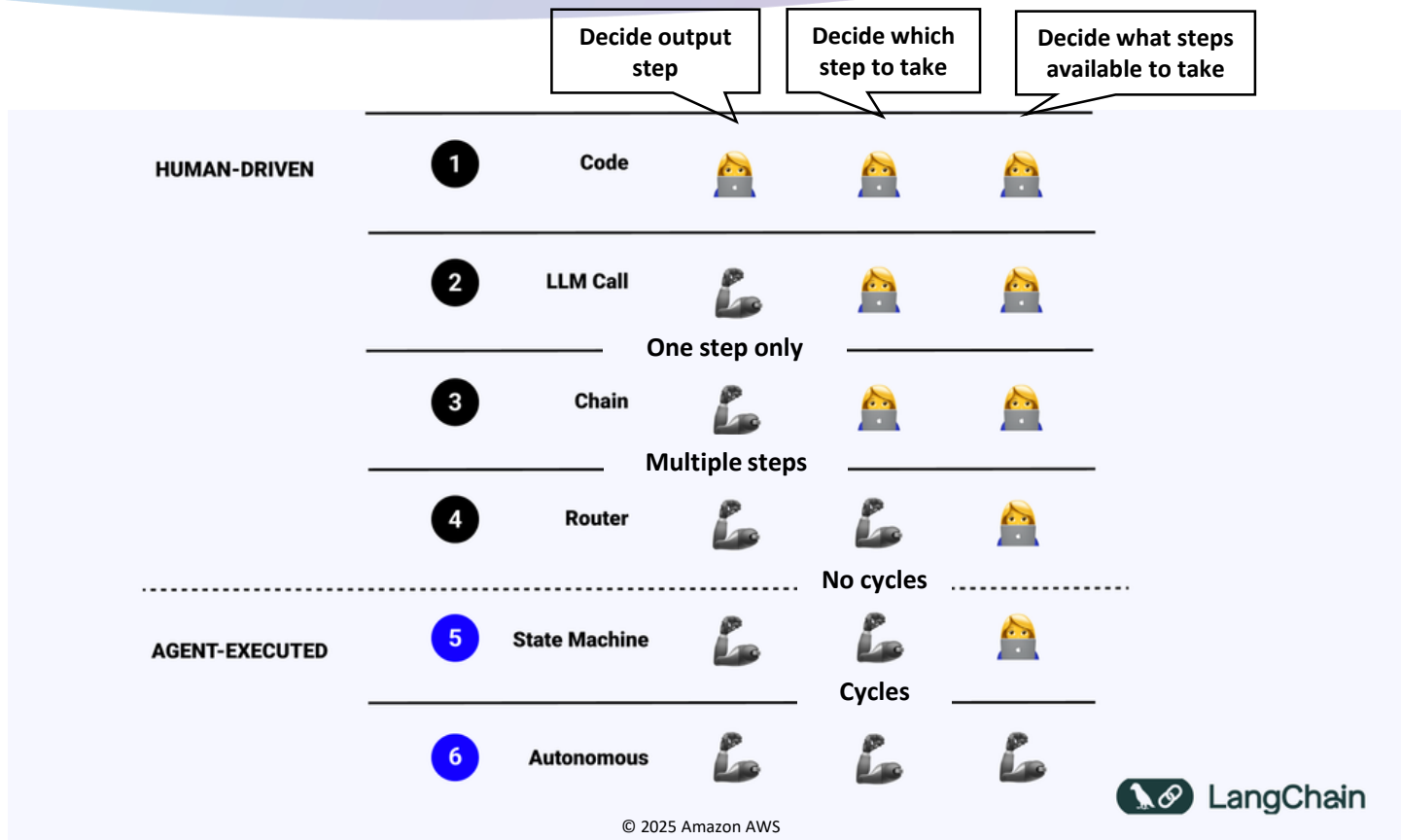
- Dynamic connections between agents
- Relationship can form/change
- More like social network than assembly line

Key point:

Differs from multi-agent workflows where interaction patterns are fixed

Agency and Autonomy

Agency vs Autonomy: Levels in LLM Application



Agent Architecture Components

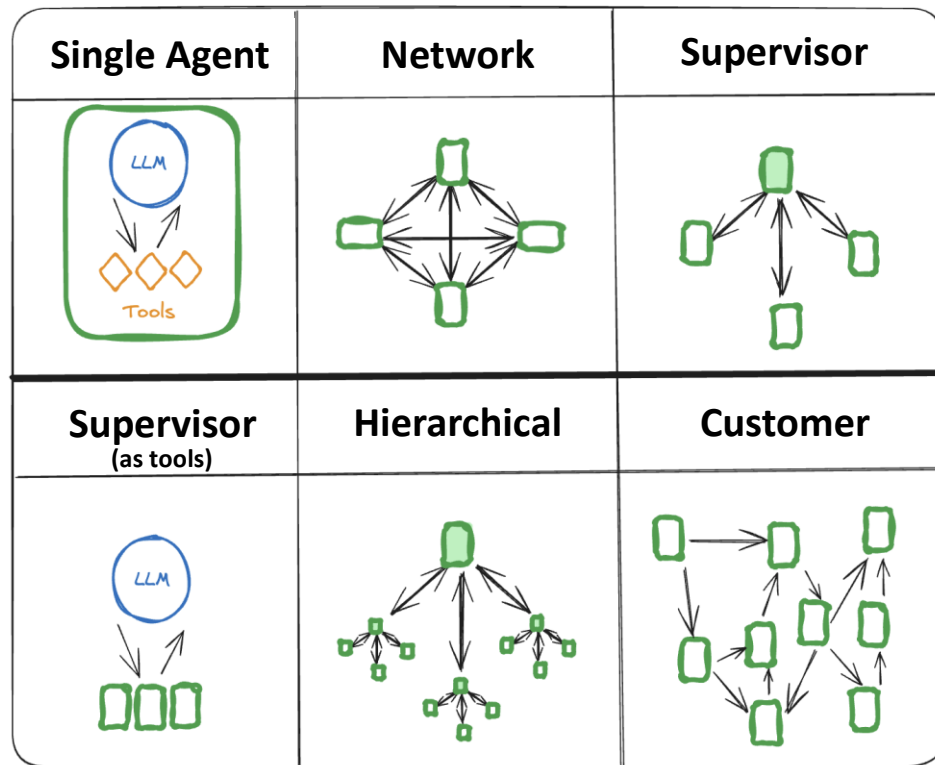
Multi-agent Architectures

What is it?

- Different ways to organize AI agents to solve complex problems
- Like organizational design, but for AI teams
- Break down complex systems when:
 - Agent has too many tools to manage effectively
 - Context becomes too complex for single agent
 - Need multiple areas of specialization

Key point:

Architecture choice shapes how AI teams work together



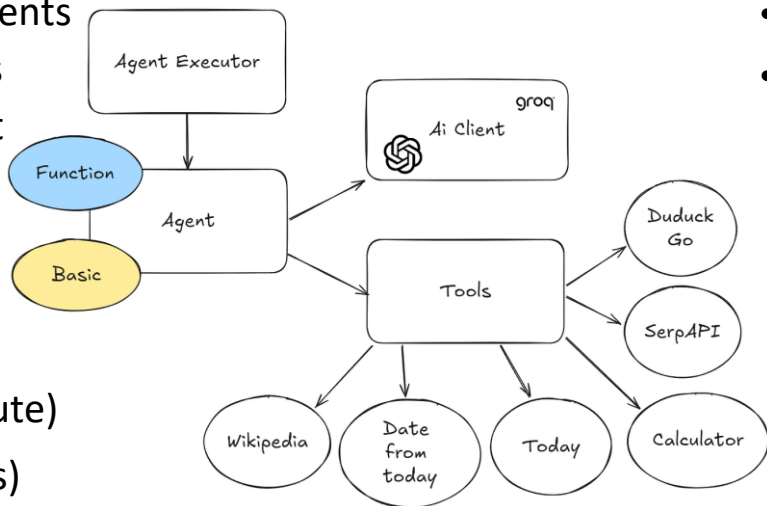
Tools & Tool Use

What is it?

- External capabilities for agents
- APIs, functions, or services
- Way to affect environment

Types of Tools:

- Information retrieval
- Action tools (write, compute)
- System tools (file, API calls)
- Analysis tools (math, code)



Example:

- Basic calculator function
- Advanced HPC cluster tools:
 - Job submission
 - Resource monitoring
 - Data transfer
 - Results analysis

Key point:

Tools let agents interrogate and affect real systems

Overview of Frameworks for Developing with Agents

Overview of Frameworks for Developing with Agents

What is a framework?

- Development toolkit and patterns
- Pre-build components and abstractions
- Best practices and guardrails

Why use one?

- Avoid reinventing the wheel
- Standard patterns for common needs
- Community and ecosystem support

When to build custom:

- Unique architectural needs
- Specific performance requirements
- Full control needed

Key point:

**Frameworks speed development,
but know when to go custom**



LangGraph

Conclusion and Q&A

Key Remarks and Take-aways

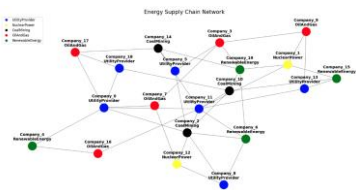
- Agentic AI is currently hyper-hyped with confusion on terms and scope
- The technology is progressing very fast*. Paired with techniques like RAG, agentic systems are very powerful decision-making tools for dynamic data analysis
- Companies are building libraries of ready-to-use agentic systems; similar to AI frontier models, there will be “blue-print” agentic systems models for targeted industries and use-cases
- **Cloud-computing and datacenters** will be instrumental in scaling up the compute and data storage demand

**The AI agent public database is listing 67 agentic systems by 2025: <https://aiagentindex.mit.edu/>*



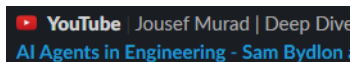
Towards effective genAI multi-agent collaboration: Design and evaluation for enterprise applications:

<https://www.amazon.science/publications/towards-effective-genai-multi-agent-collaboration-design-and-evaluation-for-enterprise-applications>



Energy market simulation example:

<https://aws.amazon.com/blogs/hpc/simulating-complex-systems-with-llm-driven-agents-leveraging-aws-parallelcluster-for-scalable-ai-experiments/>



Engineering with AI Agents:

https://www.youtube.com/watch?v=FosQ9_zRtHE

