Agentic Control Framework

Abhilash Chadhar

Agenda

- What is Agentic Control Framework (ACF)?

- Problems with LLMs – How ACF solves it?

- MCP (Model Context Protocol) & ACF architecture

- Why Context Engineering? - Reverse Engineering Claude Code

- Demo – ACF in verification workflow

- How ACF impacted my work

- How I use my spare time

- Future work

What is Agentic Control Framework (ACF)?

ACF: The Comprhensive Context Engineering Solution for LLMs

- Connects with humans via tables & graphics.
- Connects & provides tools to LLMS via MCP

Bridging the Gap Between AI & Human Understanding

A powerful orchestration layer that adds deterministic context packaging , priority scheduling, human intervention, and MCP tool bridges to ship reliable LLM work.

Problems with LLMs — How ACF solves it?

Hallucinations – Makes up responses

Limited Context

Memory & Statefulness

Transparency – we don't know what the LLM is doing

Lack of tools

Lack of tool/agent Orchestration

Context Engineering

Plan & Test-driven Workflow, Grounding

Task scoped retrieval

Persistent Memory

Human-in-the-loop controls (UI / reroute)

OS automation: terminal, browser, AppleScript

ML-driven priority scheduling

Structured outputs

Why Context Engineering?
Reverse Engineering Claude Code

- Heavy use of Prompt and Context Engineering
- Provide context in every query
- Plan with TodoWrite tool
- A single LLM query contains..

- System prompt
- User prompt
- Assistant response
- tool_call
- tool_result
- Assistant response → (repeat)
- Final answer

```
113
114
115   – NEVER assume that a given library is available, even if it is well known. Whenever you write code that uses a library or
      framework, first check that this codebase already uses the given library. For example, you might look at neighboring files, or
      check the package.json (or cargo.tenl, and so on depending on the language).
116   When you create a new component, first look at existing components to see how they're written; then consider framework choice,
      naming conventions, typing, and other conventions.
117   When you edit a piece of code, first look at the code's surrounding context (especially its imports) to understand the code's
      choice of frameworks and libraries. Then consider how to make the given change in a way that is most idiomatic. –Always follow
      security best practices. Never introduce code that exposes or logs secrets and keys. Never commit secrets or keys to the repository.
118
119   * Code style
120   💡
121   – IMPORTANT: DO NOT ADD ANY*** COMMENTS unless asked
122
123   * Task Management
124
125   You have access to the Todowrite tools to help you manage and plan tasks. Use these tools VERY frequently to ensure that you are
      tracking your tasks and giving the user visibility into your progress.
126   These tools are also EXTREMELY helpful for planning tasks, and for breaking down larger complex tasks into smaller steps. If you do
      not use this tool when planning, you may forget to do important tasks and that is unacceptable.
127   It is critical that you mark todos as completed as soon as you are done with a task. Do not batch up multiple tasks before marking
      them as completed.
128   Exarples:
129   <example>
130   user: Run the build and fix any type errors
131   assistant: I'm going to use the TodoWrite tool to write the following items to the todo list:
132   – Run the build
133   –Fix any type errors
134
135   I'm now going to run the build using Bash.
136
137   Looks like I found 10 type errors. I'm going to use the Tocowrite tool to write 10 items to the todo list.
138
139   marking the first todo as in progress
140
141   Let me start working on the first iten...
142
143   The first item has been fixed, let me mark the first todo as completed, and move on to the second item...
144   </example>
145   In the above example, the assistant completes all the tasks, including the 18 error fixes and running the build and fixing all
      errors.
```

MCP (Model Context Protocol) & ACF architecture

Open standard to plug AIs into tools/data — like "USB for AI"
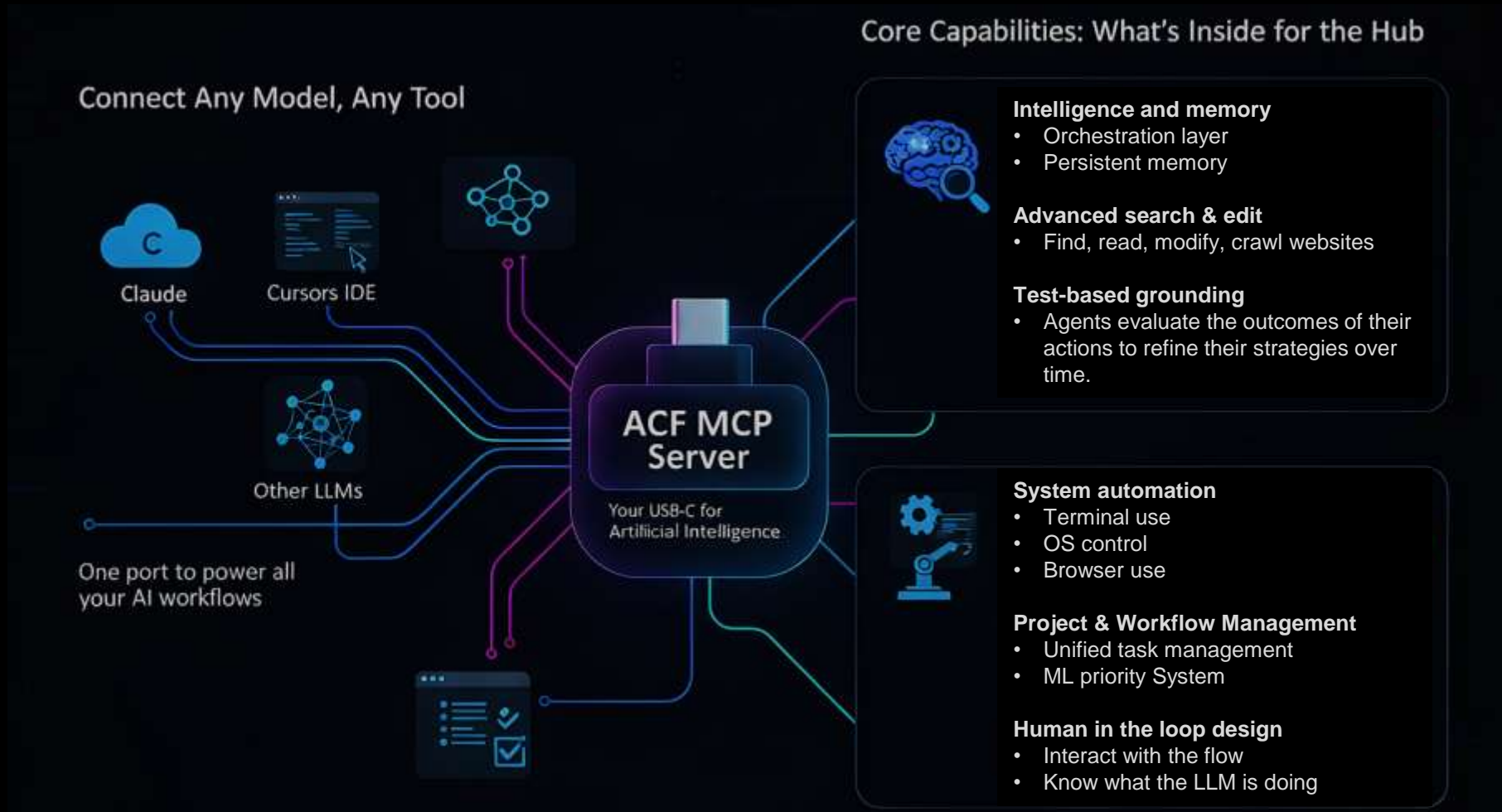
DEMO: ACF MCP server with Claude Desktop

Create a new workspace for cvaó riscv processor design and verification.
Add all the following detailed tasks and subtasks and execute them.
Clone the repo, setup the tools and then run a simple test. Once it passes run a complex test and display the results with coverage in an HTML and open it in safari
Log all errors when you get them and save the report.
Get the most recent bug from GitHub, reproduce it and resolve it.

Research

Opus 4.1

How ACF impacted my work

Deliver in unfamiliar domains

Faster spec lookup & cross-checks

Build faster, review deeper

High-quality AI still comes at a premium.

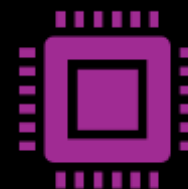Easy to chase 'Jarvis', stay outcome-focused and scoped.

Future work

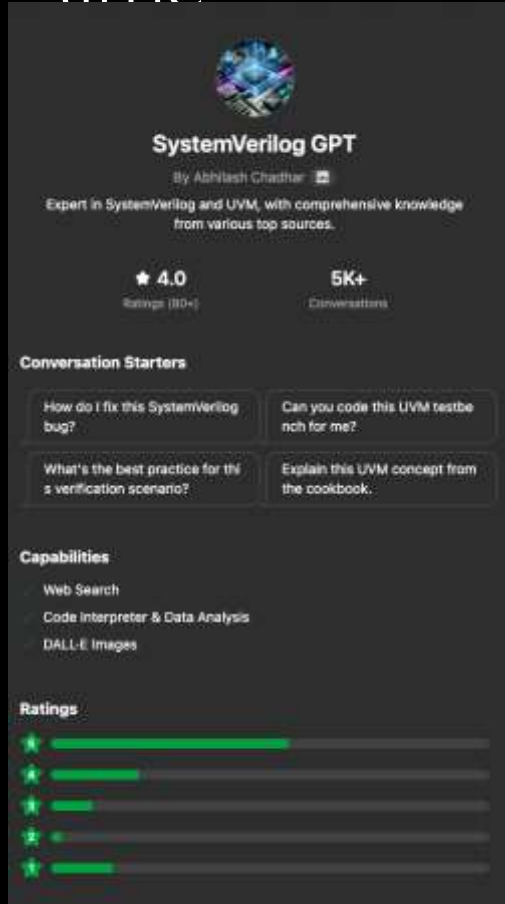A complete AI operating system.

Better RAG strategies.

Improved AI driven debug tools.
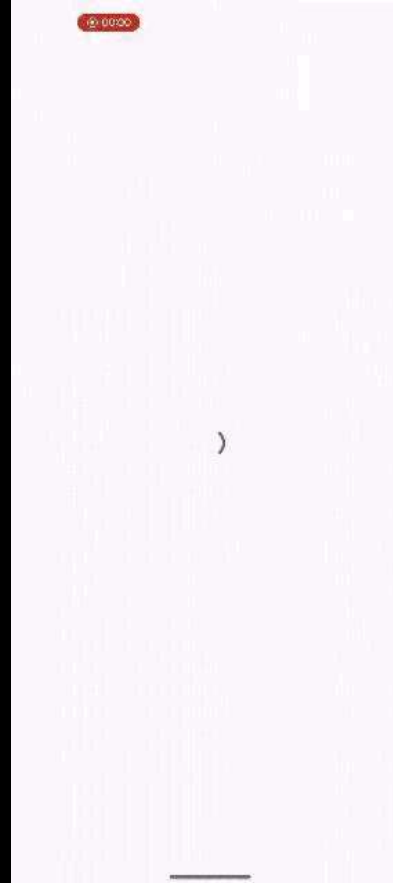
Specialized agents for Chip development.

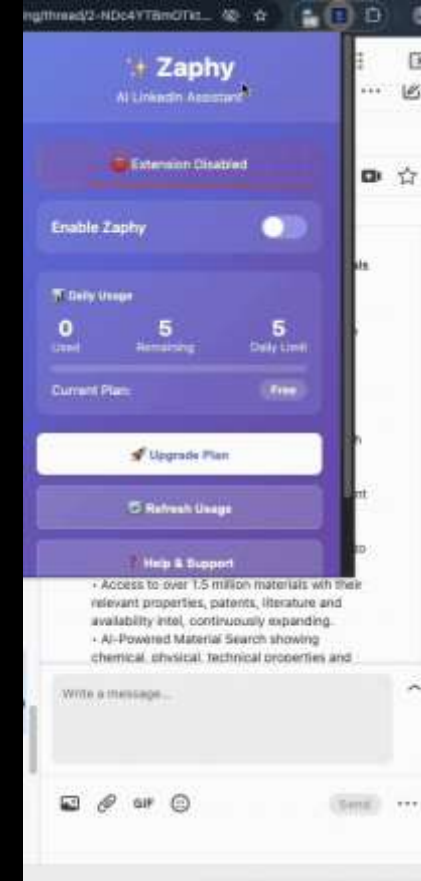# What I do with AI in my spare time

SV Agent
Launched Aug 2024

BevyBeats
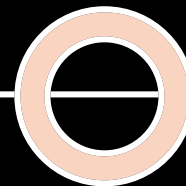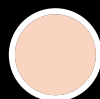Spotify with AI music generation

Yuj
Personalized workout creator

Zaphy
LinkedIn Ai message responder

PyRISCVDV, AI therapist, Websites, MCP servers and many more ..

Thanks

Questions?

More : https://futureatoms.com

GitHub: https://github.com/FutureAtoms

Contact: abhilash@futureatoms.com