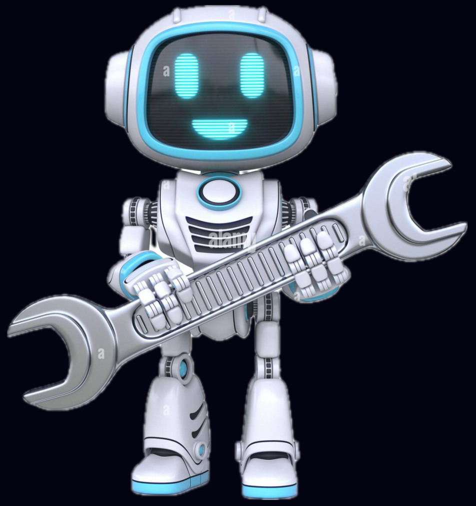
MCP in Practice

What is MCP?

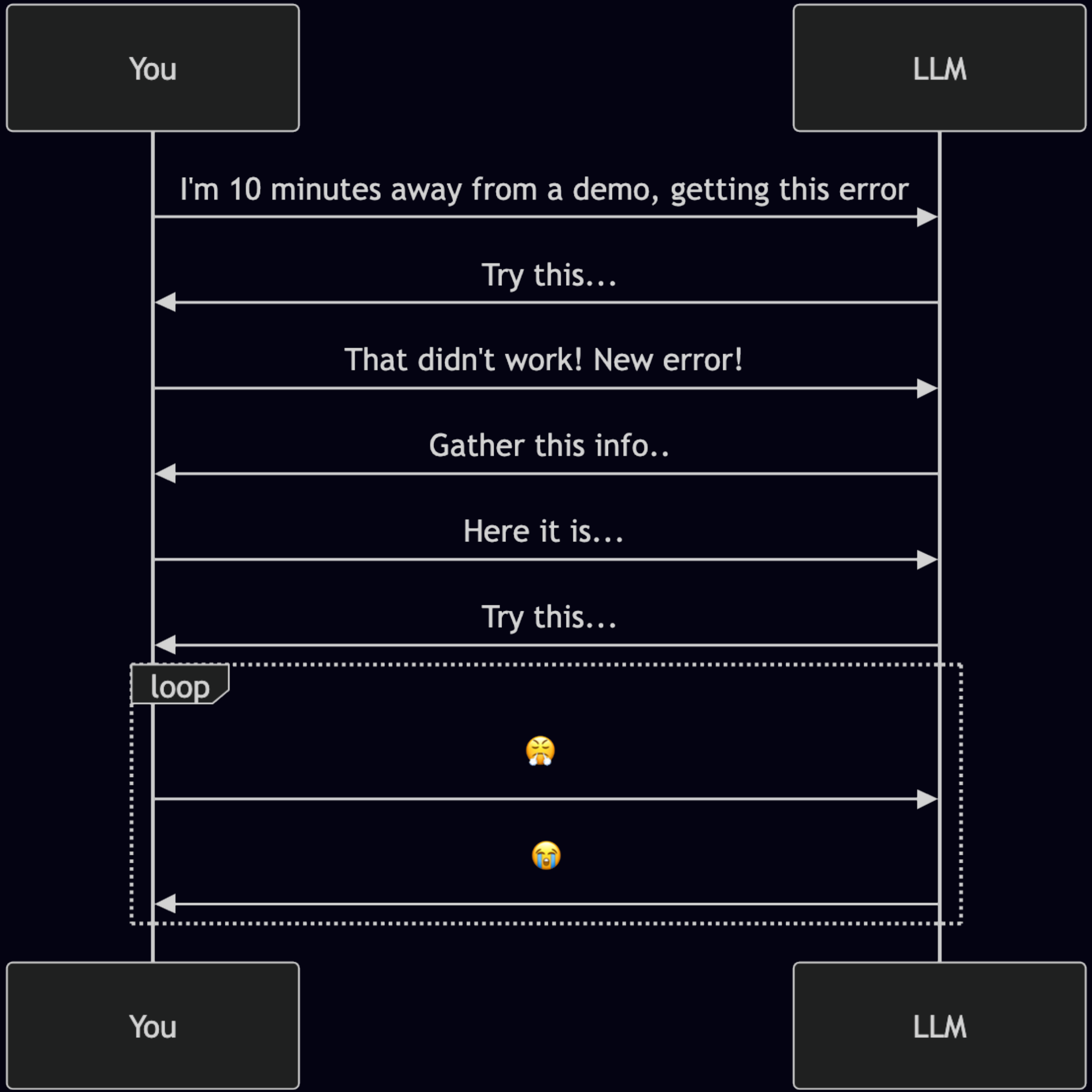
- Open Standard
- Created by Anthropic (Creators of Claude) in 2024
- Allows LLMs to connect to data and systems
- Enables agentic workflows

MCP gives tools to AI



Why MCP?

Without MCP



You

LLM

I'm 10 minutes away from a demo, getting this error

Try this...

That didn't work! New error!

Gather this info..

Here it is...

Try this...

loop

😤

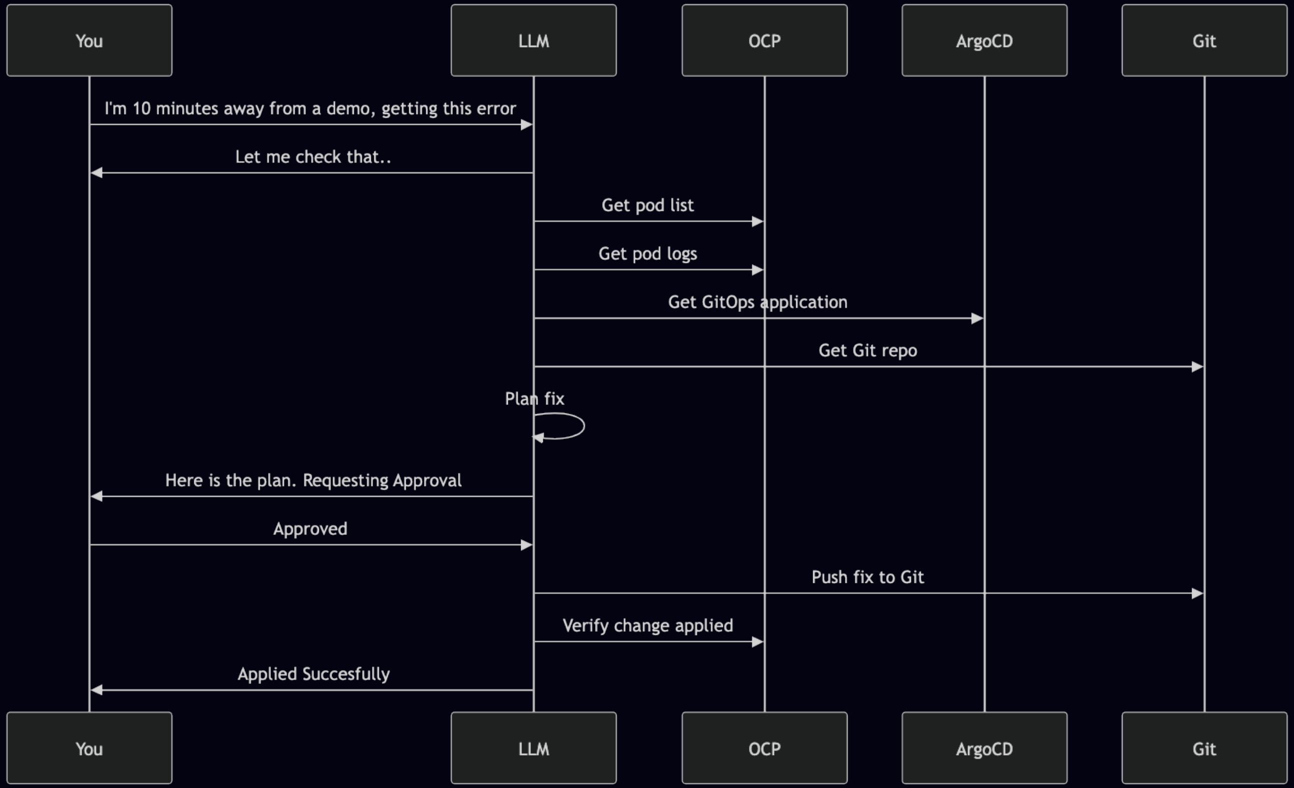
😭

You

LLM

Why MCP?

With MCP...

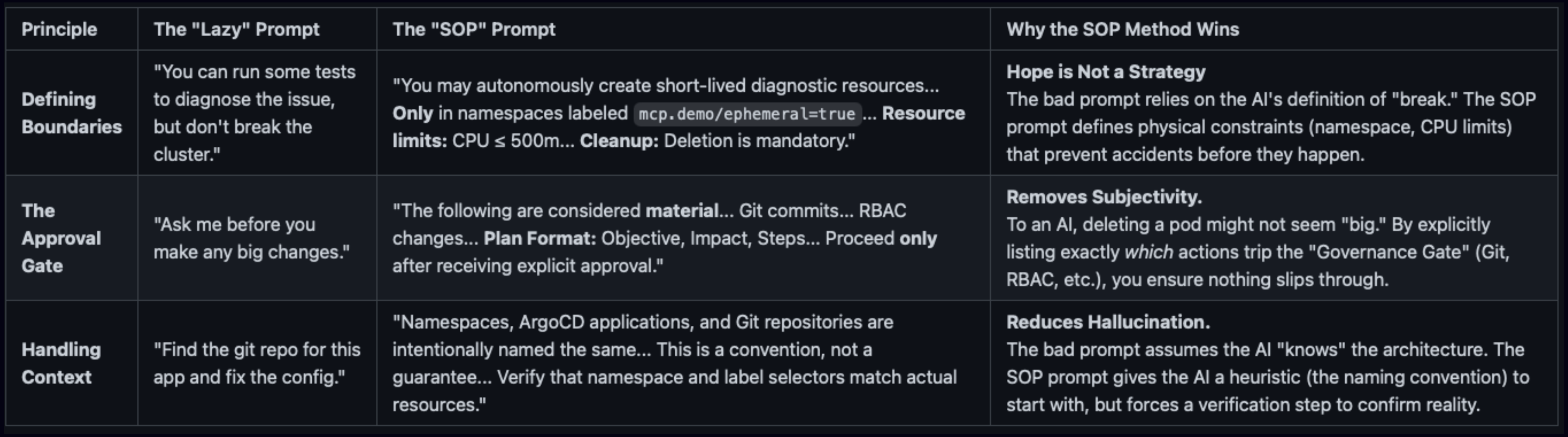


Tools for the demo

- `openshift-mcp-server` - Kubernetes/OpenShift API operations
- `gitea-mcp-server` - Git repository operations
- `argocd-mcp-server` - ArgoCD (aka Openshift GitOps) application management

Prompt Engineering

Intent vs. Instruction



Principle	The "Lazy" Prompt	The "SOP" Prompt	Why the SOP Method Wins
Defining Boundaries	"You can run some tests to diagnose the issue, but don't break the cluster."	"You may autonomously create short-lived diagnostic resources... **Only** in namespaces labeled `mcp.demo/ephemeral=true` ... **Resource limits:** CPU ≤ 500m... **Cleanup:** Deletion is mandatory."	**Hope is Not a Strategy** The bad prompt relies on the AI's definition of "break." The SOP prompt defines physical constraints (namespace, CPU limits) that prevent accidents before they happen.
The Approval Gate	"Ask me before you make any big changes."	"The following are considered **material**... Git commits... RBAC changes... **Plan Format:** Objective, Impact, Steps... Proceed **only** after receiving explicit approval."	**Removes Subjectivity.** To an AI, deleting a pod might not seem "big." By explicitly listing exactly *which* actions trip the "Governance Gate" (Git, RBAC, etc.), you ensure nothing slips through.
Handling Context	"Find the git repo for this app and fix the config."	"Namespaces, ArgoCD applications, and Git repositories are intentionally named the same... This is a convention, not a guarantee... Verify that namespace and label selectors match actual resources."	**Reduces Hallucination.** The bad prompt assumes the AI "knows" the architecture. The SOP prompt gives the AI a heuristic (the naming convention) to start with, but forces a verification step to confirm reality.

Ambiguity is the enemy of automation. If you don’t define ‘safe’… the AI will.

DEMO

Have fun exploring the world of MCP!

[finished]