Governed MCP Command Broker

Deciding at the tool boundary

A team can write “open a draft” in every agent’s instructions and still end up reviewing an attempted publication. The last practical point to enforce the distinction is the tool that can cause the effect.

Bind the operation to its destination

Start with the worker identity, assignment, target and proposed operation. A private draft and a public pull request use different audiences. A commit in a worktree and a direct update to a protected branch have different consequences. The broker needs enough structured information to judge the effect being requested.

The suite design brings proxy and tool routes through a common authority path. A decision authorizes a bounded attempt. The executor’s result and an observation of the repository tell the reviewer whether the attempt took effect.

Repeat the recorded commit exercise

Use an ordinary fixture repository and a worker whose grant covers inspection. Have it request a commit through the governed broker. The recorded ARF run kept the repository at one commit after refusal and recorded the denied request. Then an explicit grant permitted the same tool. The changed permission explains the new verdict without attributing it to a change in the model.

When repeating the exercise, keep the initial revision, the policy revision and the resulting repository state. Have the reviewer identify all three before reading the agent’s summary. This puts a concrete check on a statement as casual as “I only edited the worktree.”

Give a denial a defined ending

In a governed tool route, policy evaluates the agent's requested operation and the broker controls whether the executor may call that tool. A local note or other follow-up needs its own authorized operation. The scripted Decision Press release scenario sends a denied direct push to a local handoff note and sealed record; other denials stop that run. In a review, compare the policy decision, executor attempt and target observation, and include the operator's response when the policy asks for one.

Tracing a commit back from the repository

Record	Owner	What it establishes
Commit proposal	Requesting worker	The operation and target the agent wanted.
Grant or refusal	Decision returned to the broker	Whether that attempt was permitted.
Repository state	Target observation	Whether the revision actually changed.
Follow-up scope	Workflow owner	Which work may happen after a denial.

Sources and evidence

Refusal at the tool boundary · Implementation record · Try a release in the Decision Press