



*Empirical. 675 tool calls aggregated across 5 LLM(s) (DeepSeek-V3 + Qwen2.5-72B-Instruct + Qwen3.5-35B-A3B + MiniMax-M2.5 + GLM-4-32B-0414) producing tool calls in response to adversarial prompts across 6 attack categories. Each call is fed to every protocol's host-side validator (the real dcp.bridge.Bridge for DCP; jsonschema for MCP / IoT-MCP / OpenAPI). Corpus in tools/gen\_llm\_corpus.py + llm\_corpus.json; aggregation in tools/bench\_hallucination\_empirical.py.*