

Model Context Protocol for Scientific Software: Building AI Interfaces That Actually Work

Monday, 7 September 2026 13:45 (15 minutes)

Large language models are rapidly becoming useful assistants for software development, analysis, and documentation. In practice, however, the limiting factor is rarely the model itself. The hard part is giving the model reliable, secure access to the tools, data, and domain knowledge that scientists already use.

This talk introduces the Model Context Protocol (MCP) from the perspective of scientific software developers. Rather than focusing on prompt engineering or custom foundation models, we'll examine how MCP servers expose existing Python libraries, databases, workflow systems, and experiment services to AI assistants through well-defined interfaces.

Using examples from high-energy physics (e.g. dataset databases, analysis metadata, and workflow services) we will discuss practical patterns for building MCP servers, handling authentication without exposing user credentials, and designing interfaces that remain useful across different LLM providers and experiments.

You will hopefully have a concrete understanding of when an MCP server is appropriate, how to build one around an existing Python project, and why interoperable tool interfaces are likely to matter more than model-specific integrations.

Primary author: STARK, Giordon Holtsberg (University of Chicago)

Presenter: STARK, Giordon Holtsberg (University of Chicago)

Session Classification: Talks