More on this in the lecture on AI Agent

Project architectural requirements (A)

Agentic AI architecture

- LLM-driven agents that interact with each other
- Use tools to complete tasks
- Best for multi-step tasks
- MCP is an open protocol that lets LLM apps securely connect to tools, data, and services via standardized MCP servers.
- MCP server exposes tools/files/prompts; client (IDE/app/agent) calls them.

A1 – MODULAR STRUCTURE

Security of Agentic AI application

- Adopt a security mechanism
- MCP servers can access tools and resources
- Adopt a mechanism for access control
- Specify access permissions in advance

A2 – SECURITY PROTECTION

Checklist for a good project (B): touch these 4 points

Project structure and roadmap: modular and incremental

E.g., local app that does X **but also**

- A nice GUI for the app
- A GUI extension with a more advance library
- Can connect with similar apps over the internet
- Has an optional algorithm that speeds up certain computations
- Connect to an external module to send SMSs
- Optional database for large data storage

B1 – MODULAR STRUCTURE

In which tasks can AI support you beyond coding?

- Breaking down the project into tasks
- Defining the interfaces/APIs
- Software design
- Debugging
- Testing
- Performance optimization
- Learning new languages/libraries, etc

B2 – AI BEYOND CODING

Checklist for a good project (B): touch these 4 points

Overall aim for a project that you would not be able to compete without AI

- Libraries that you don't know
- (part of the project in) languages that you don't know
- Tasks/optimizations/functionalities that you would find very challenging

B3 – PUSH AI TO THE LIMIT

It is OK if part of the project fails and/or you cannot compete all the project

Optional: include some AI for coding (optional) functionality in the project

- A code editor that helps you developing code
- A learning platform for coding
- Automated generation of configuration scripts
- Self-improving code in the project
- …

B4 – (OPTIONAL) META LEVEL

Project description submission

Group work, individual grade

2 pages, A4 format, 12 points, Times font

Structure:

- Group composition
- High-level idea for how to address A1
- No need to address A! in the project description
- Explain how you expect to address points B1 to B4