AI SDLC Fundamentals

Build the mental model for AI-assisted software development

20	2	10-15
SESSIONS	WEEKS	TOTAL HOURS

Program Overview

A lecture-only fundamentals program establishing the mental model for LLMs, context engineering, agentic workflows, tool calling, and security.

Format

20 independent micro-courses, each 20-30 minutes. Designed for flexibility - take them at your own pace.

Suggested Pace

2 sessions per day over 10 business days. Complete the full program in just 2 weeks.

No Code Required

Pure lecture format - no development environment needed. Labs and applied work come in later phases.

Assessment

End-of-module test with critical safety pass/fail gates. Certification upon completion.

Who This Is For

Target Audience

- ✓ Software engineers looking to understand AI-assisted development
- ✓ Platform engineers building AI tooling and infrastructure
- ✓ Technical professionals preparing for hands-on labs
- ✓ Team leads evaluating AI coding tools for their teams
- ✓ Anyone who will use CLI agents, API calls, or tool-based workflows

What You'll Learn

By completing this program, you will be able to:

- ✓ Explain what an LLM does at inference time and what it cannot do (no in-session learning, no durable memory)
- ✓ Understand training vs inference and why "crystallized intelligence" matters for how you use models
- ✓ Master context windows and how context assembly affects quality and safety
- ✓ Distinguish chatbot UI vs raw API usage vs agentic harnesses (IDE, CLI, cloud agent)
- ✓ Explain agentic workflows (plan-act-observe-reflect) and where they break in practice
- ✓ Understand tool calling, MCP, and when each approach is justified

- ✓ Apply safe judgment on tool permissioning and least privilege principles
- ✓ Recognize and mitigate prompt injection attacks

1 Foundation & Environment

Orientation and enterprise constraints

Course 01

Course Orientation

What "agentic coding" means, the 3-layer stack mental model (model, harness, workflow), and what success looks like.

20-30 min Lecture

Course 02

Tooling & Constraints

Enterprise reality: approved models, data classification, security reviews, and the "off-network coaching" model.

20-30 min Lecture

2 LLM Core Concepts

How language models actually work

Course 03

LLMs & Tokens

Next-token prediction, tokens as units (not words), and failure modes from token framing: hallucination, overconfidence, format drift.

20-30 min Lecture + Demo

Course 04

Transformer Mental Model

Embeddings, attention, and output distribution at a high level. Why transformers handle dependencies somewhat but still fail in long contexts.

20-30 min Lecture + Diagrams

Course 05

Training vs Inference

"Crystallized intelligence" - capabilities frozen at training time. What fine-tuning changes (behavior) vs what it doesn't (core limits).

20-30 min Lecture

Course 06

Context Window & Memory

Context window mechanics: truncation, recency bias, "lost instructions." Why context engineering is a real skill.

20-30 min Lecture + Demo

3 Prompting & Context Engineering

The craft of communicating with models

Course 07

Prompting Fundamentals

Prompt anatomy: role, constraints, examples, acceptance criteria, output contract. Prompt hygiene and testable outputs.

20-30 min Lecture + Examples

Course 08

Chatbot vs Raw Model Call

What chatbot UIs hide: system messages, safety wrappers, memory. The roles/messages mental model and why API-level thinking matters.

20-30 min Lecture + Diagrams

Course 09

Prompt Contracts & Output Schemas

Why contracts matter for grading, automation, and safety. Structured outputs: sections, key-value, JSON schema.

20-30 min Lecture + Examples

Course 10

Context Engineering Workshop

"Working set" construction: what to include, ordering, compression. Avoiding context poisoning and managing your context budget.

20-30 min Workshop

4 Agents & Harnesses

From chatbots to autonomous workflows

Course 11

Agents vs Workflows

Agent definition: LLM + tools + loop + objectives. The agentic loop (plan-act-observe-reflect) and where agents fail.

20-30 min Lecture + Diagrams

Course 12

Harness Taxonomy

Chatbot vs IDE assistant vs CLI agent vs cloud agent. Comparing tool surface, permissions, and auditability.

20-30 min Lecture + Comparison

Course 13

Agentic Coding Method

The operational workflow: plan, diff, test, narrate. Why workflow design matters more than any single tool.

20-30 min Lecture + Templates

Course 14

Model Mixing & Selection

Why mixing models works (no durable memory). When to use "bigger thinking" vs "smaller fast" models. Trade-offs: cost, latency, safety.

20-30 min Lecture + Decision Tree

5 Tool Calling & Integration

Extending model capabilities safely

Course 15

Tool Calling

Structured function invocation via the harness. Why tool calling expands capability and why it introduces risk.

20-30 min Lecture + Examples

Course 16

MCP vs API Calls

Direct API calls vs Model Context Protocol. When MCP is justified vs when it adds unnecessary complexity.

20-30 min Lecture + Comparison

6 Security & Safety

Critical knowledge for safe deployment

Course 17

Securing Tool Calls

Least privilege: allowlists, scopes, approval gates. Auditability: logs, transcripts, accountability.

20-30 min Lecture + Examples

Course 18

Prompt Injection

What injection is, common patterns (documents, web pages, repo text), and mitigations: isolation, hierarchy, gating, validation.

20-30 min Lecture + Examples

Course 19

Security Scenarios Lab

Analyze real scenarios: pick safe permissions, identify injection attempts, choose mitigations. Reinforce critical safety principles.

20-30 min Interactive Lab

Course 20

Integrated Capstone

End-to-end walkthrough: API calls, harness behavior, tool calling, injection attempt, mitigations. Final recap and Q&A.

20-30 min Demo + Q&A

Certification & Assessment

Complete the program with our end-of-module assessment

End-of-Module Test

- 10 questions (12-15 minutes)
- 6 comprehension questions
- 4 scenario judgment questions
- Pass threshold: 80% overall (8/10)

Critical Safety Gates

- Prompt injection recognition
- Least-privilege tool permissioning
- Untrusted input handling
- Hard fail if any missed

Upon Completion

- Certificate of completion
- Ready for Labs & Applied phases
- Foundation for advanced courses
- Feedback questionnaire (5-7 min)