

1 DAY / LIVE INSTRUCTOR-LED, VIRTUAL OR ONSITE

AI Implementation

From Opportunity to Architecture

Turn AI pressure into a practical implementation plan.

Your organization is being asked to move faster with AI. The difficult part is deciding where it belongs, what it should be allowed to do, and how to tell whether it is good enough for real work. An impressive demo cannot answer those questions on its own.

This one-day course gives technical leaders and practitioners a practical framework for making those decisions. Follow a realistic enterprise application as it gains knowledge, tools, evaluation, and controls. See how architectural choices change quality, risk, latency, and cost, and where conventional software should remain in charge.

Through demonstrations, guided activities, and discussion, build the judgment to challenge proposals, compare approaches, and scope a credible pilot.

In this course, you will learn how to

- Identify worthwhile AI opportunities and recognize when conventional software is the better choice.
- Compare model, hosting, and routing options against quality, privacy, latency, and cost.
- Choose patterns for enterprise knowledge, tools, agents, and MCP integration.
- Define validation, evaluation, permissions, and approval around model behavior.
- Recognize security and reliability gaps before exposing a system to real users.
- Outline a bounded pilot with success criteria, ownership, and evidence for the next decision.

AUDIENCE + COURSE AGENDA

Make the time count.

Who should attend

Software and solution architects, engineering managers, technical leads, software engineers, platform and DevOps professionals, technical consultants, and product leaders involved in AI implementation decisions.

Learning experience

Architecture-focused demonstrations, guided exercises, and discussion in OpsPilot with synthetic data. The focus is understanding implementation choices; the two-day continuation develops the patterns in code.

Course agenda

Topics covered
Intro and classroom orientation
AI has changed the engineering decision
Choose the right opportunity and architecture
Give AI enterprise knowledge
Move from answers to controlled actions
Can you trust it? Evaluate the system
Security, production reality, and pilot planning

Topic order, pacing, and time spent on each subject vary with the group’s experience, questions, and learning needs. Topics are not assigned to fixed times or days. Plan to attend the full course.

DETAILED COURSE OUTLINE

What you will explore.

Part 1: Intro: connect the course to your work

Start with the implementation decisions your organization faces. Get oriented to OpsPilot, the classroom flight simulator, and learn what to observe when an AI system succeeds, fails, or needs human help.

- Course goals, participant context, and the learning path
- A realistic application with synthetic data
- Observe quality, cost, latency, and allowed actions

Part 2: AI has changed the engineering decision

Understand what a model adds to an application and what surrounding software must still control. Explore why a convincing answer can be wrong, and why a successful demo leaves important engineering questions unanswered.

- Code, AI, or hybrid: deterministic and probabilistic behavior
- Models, tokens, context, memory, and hallucination
- Escalation, confidence, approval, and observable failure

Part 3: Choose the right opportunity and architecture

Turn a painful business workflow into a bounded AI pilot. Compare model and hosting choices against the work you actually need done, including the full cost of routing, retries, and review.

- Automation versus augmentation; pilot scope and ownership
- Frontier, smaller, local, hosted, and privately deployed models
- Model selection, workflow cost, routing, and escalation

Part 4: Give AI enterprise knowledge

Learn how an application supplies current, authorized evidence to a model. Understand the mechanics of retrieval and the checks needed before presenting an answer as grounded in company information.

- Embeddings, semantic search, chunking, and retrieval-augmented generation (RAG)
- Documents versus authoritative APIs; RAG versus fine-tuning
- Access boundaries, prompt versions, citations, and evidence checks

DETAILED COURSE OUTLINE / CONTINUED

Connect learning to practice.

Part 5: Move from answers to controlled actions

Follow a proposed action through the application: structured output, validation, permission checks, approval, and execution. Compare fixed workflows with agent loops and decide when a direct API or Model Context Protocol (MCP) integration fits.

- Tool schemas, permissions, and approval for the exact action
- Retries, idempotency, partial failure, and durable progress
- Agent autonomy, stop conditions, direct APIs, and MCP

Part 6: Can you trust it? Evaluate the system

Define what acceptable behavior looks like and test it against independently checked examples. Learn why average quality scores can hide unacceptable failures and why an AI reviewer needs evaluation too.

- Deterministic validation, evaluation datasets, and quality rubrics
- Offline tests, runtime checks, AI review, and human escalation
- Check the answer and the actual outcome; state evaluation limits

Part 7: Security and production reality

Examine what happens when inputs are hostile, dependencies fail, or costs grow. Bring the architecture together into a practical pilot plan with explicit controls, evidence, and remaining readiness gaps.

- Prompt injection, data leakage, least privilege, and tool abuse
- Observability, versioning, regression evaluation, and graceful degradation
- Production-readiness review and a concrete first-pilot plan

What you take back to work

A shared vocabulary for AI implementation, a framework for architectural decisions, and a concrete starting point for your first pilot.

Continue with Applied AI Engineering to implement the patterns in code, or book the combined three-day AI Engineering Boot Camp.

Plan private training for your team

Discuss audience fit, delivery dates, and learning goals at www.attainable.tech/contact.html.