Microsoft Agent Framework (MAF)

Course Table of Contents (3-Day)

Module 1 - Introduction to Generative AI and AI Agents

- Evolution of Artificial Intelligence
- Generative AI Overview
- What are Large Language Models (LLMs)?
- Prompt Engineering Basics
- Tokens, Context Window and Temperature
- Understanding Hallucinations
- Limitations of LLMs
- Why AI Agents?
- AI Agents vs Traditional Applications
- Agent Lifecycle
- Real-world AI Agent Use Cases
- Popular Agent Frameworks
- Microsoft AI Ecosystem
- Introduction to Microsoft Agent Framework (MAF)

Lab

- Install Python
- Install Visual Studio Code
- Configure Environment
- Install MAF SDK
- Create First AI Agent

Module 2 - Agent Architecture

- Core Components of MAF
- Agent Class
- Models
- Messages
- Instructions
- Sessions
- Runtime
- Execution Flow
- Agent Lifecycle
- Hosting Options
- Project Structure

Lab

- Build First Echo Agent
- Build Chat Agent

Module 3 - Working with Models

- Connecting to Azure OpenAI
- Connecting to OpenAI
- Model Selection
- GPT-4.1
- GPT-4o
- GPT-4.1-mini
- Streaming Responses
- Error Handling

Lab

- Connect Agent to Azure OpenAI
- Streaming Chat Responses

Module 4 - Function Calling and Tools

- What are Tools?
- Tool Calling
- Function Calling

- Tool Discovery
- Tool Registration
- Parameter Binding
- Runtime Context
- Tool Approval
- Error Handling

Built-in Tools

- Web Search
- Code Interpreter
- File Search
- Computer Use
- Image Generation

Lab

- Calculator Tool
- Weather Tool
- Email Tool
- Database Lookup Tool

Module 5 - MCP (Model Context Protocol)

- Introduction to MCP
- MCP Architecture
- MCP Client
- MCP Server
- Connecting External Services
- Security Considerations

Lab

- Build MCP Server
- Connect MAF Agent to MCP

Module 6 - Memory and Context

- Stateless vs Stateful Agents
- Conversation History
- Session Management
- Memory Types
- Short-Term Memory
- Long-Term Memory
- Context Providers
- History Providers
- Session Persistence
- Truncation Strategies

Lab

- Persistent Chatbot
- Conversation Memory

Module 7 - Multi-Agent Systems

- Why Multiple Agents?
- Agent-to-Agent Communication
- Agent Routing
- Agent Handoff
- Orchestration
- Sequential Workflows
- Parallel Workflows

Lab

- Research Agent
- Planner Agent
- Executor Agent

Module 8 - Human-in-the-Loop

- Approval Workflows
- User Confirmation
- Interruptions
- Checkpoints

- Resume Execution
- Escalation Patterns

Lab

- Expense Approval Agent
- Leave Approval Agent

Module 9 - Enterprise Integration

- Calling REST APIs
- Database Integration
- SQL Server
- Azure Storage
- Microsoft Graph
- Outlook Integration
- Teams Integration

Lab

- CRM Lookup Agent
- Ticket Creation Agent

Module 10 - Security

- Authentication
- Authorization
- Secrets Management
- API Keys
- Azure Key Vault
- RBAC
- Secure Prompting
- Preventing Prompt Injection

Module 11 - Observability and Debugging

- Logging
- Tracing
- Diagnostics
- Monitoring
- Performance Tuning
- Error Handling
- Cost Optimization

Lab

- Enable Tracing
- Debug Agent Execution

Module 12 - Deployment

- Local Deployment
- Docker Deployment
- Azure App Service
- Azure Container Apps
- Azure Functions
- CI/CD Pipeline
- Configuration Management

Lab

- Deploy Agent to Azure

Module 13 - Capstone Project

Students build a complete enterprise AI solution.

Example Project:

- Customer Support Agent
- HR Assistant
- Banking Assistant
- IT Helpdesk Agent
- Knowledge Base Assistant

Project Features:

- Azure OpenAI
- Multiple Tools
- Memory
- MCP
- REST API Integration
- Human Approval
- Deployment to Azure

Hands-on Labs

The course should include around **18–20 labs**, for example:

1. First AI Agent
2. Chat Agent
3. Tool Calling
4. Weather Tool
5. Calculator Tool
6. Database Tool
7. REST API Tool
8. MCP Integration
9. Persistent Memory
10. Multi-turn Chat
11. Multi-Agent Workflow
12. Human Approval
13. Microsoft Graph Integration
14. Azure OpenAI Integration
15. Logging and Tracing
16. Docker Deployment
17. Azure Deployment
18. Final Capstone Project

Estimated Schedule

- **Day 1:** Modules 1–4 (Foundations, Architecture, Models, Tools)
- **Day 2:** Modules 5–8 (MCP, Memory, Multi-Agent Systems, Human-in-the-Loop)
- **Day 3:** Modules 9–13 (Enterprise Integration, Security, Observability, Deployment, Capstone)

This expanded syllabus is suitable for corporate training and gives learners practical experience beyond the original 6.4-hour self-paced material, aligning well with enterprise AI agent development using Microsoft Agent Framework.