

AI AGENT PRODUCT FACTORY: ARCHITECTURE BLUEPRINT

10 Core Layers & 40+ Production Modules Specification

GitHub: <https://github.com/sh15aa/agentreusable> • Python 3.12+ • Enterprise Grade

10 Architectural Layers Overview

Layer 1: Identity & Config	AgentIdentity, AgentConfig, AgentManifest, Environment policies, status tracking.
Layer 2: LLM Gateway & Economics	Multi-provider routing by task complexity, streaming, cost economics, pricing models, fallback cascades.
Layer 3: Multi-Tier Memory	Working memory scratchpad, conversation compaction, semantic vector search, episodic experience learning, hybrid RAG (BM25+Dense).
Layer 4: Sandboxed Tools & Builtins	Central ToolRegistry, WebSearchTool, BrowserTool (SSRF-hardened), PythonSandboxTool (AST-hardened), FileProcessingTool.
Layer 5: Orchestration & Workflows	PlanningEngine dynamic decomposition, WorkflowEngine parallel DAG execution, SupervisorAgent multi-agent messaging.
Layer 6: Human-in-the-Loop	HumanApprovalQueue for high/critical risk tool actions with pause/resume state persistence.
Layer 7: Validation & Verification	StructuredOutputEngine Pydantic parsing with auto-repair, SelfVerificationEngine fact verification, CitationEngine source provenance.
Layer 8: Security & Governance	RBAC permissions, MemoryGovernance PII redaction (email/phone/SSN), SecretStore zero-leak isolation, SSRF network validation.
Layer 9: Evaluation & Benchmarks	GoldenDataset evaluation test cases, LLMAsJudge 1-5 rubric scoring, RegressionRunner automated benchmarks.
Layer 10: Observability & APIs	Tracer distributed spans, AuditLogger tamper-evident log, AgentAnalytics metrics, FastAPI production SSE server.

Factory CLI Commands

```
# List available agent templates
uv run python -m cli.main list-templates

# Run an agent template directly
uv run python -m cli.main run research "Investigate latest developments in autonomous AI"

# Run automated regression benchmarks
uv run python -m cli.main eval research
```

Master Assembler: AgentFactory

```
from agent_factory.factory import AgentFactory
from templates.research_agent import create_research_agent

factory = AgentFactory()
agent = create_research_agent(factory)
result = await agent.run("Investigate new breakthroughs")
```