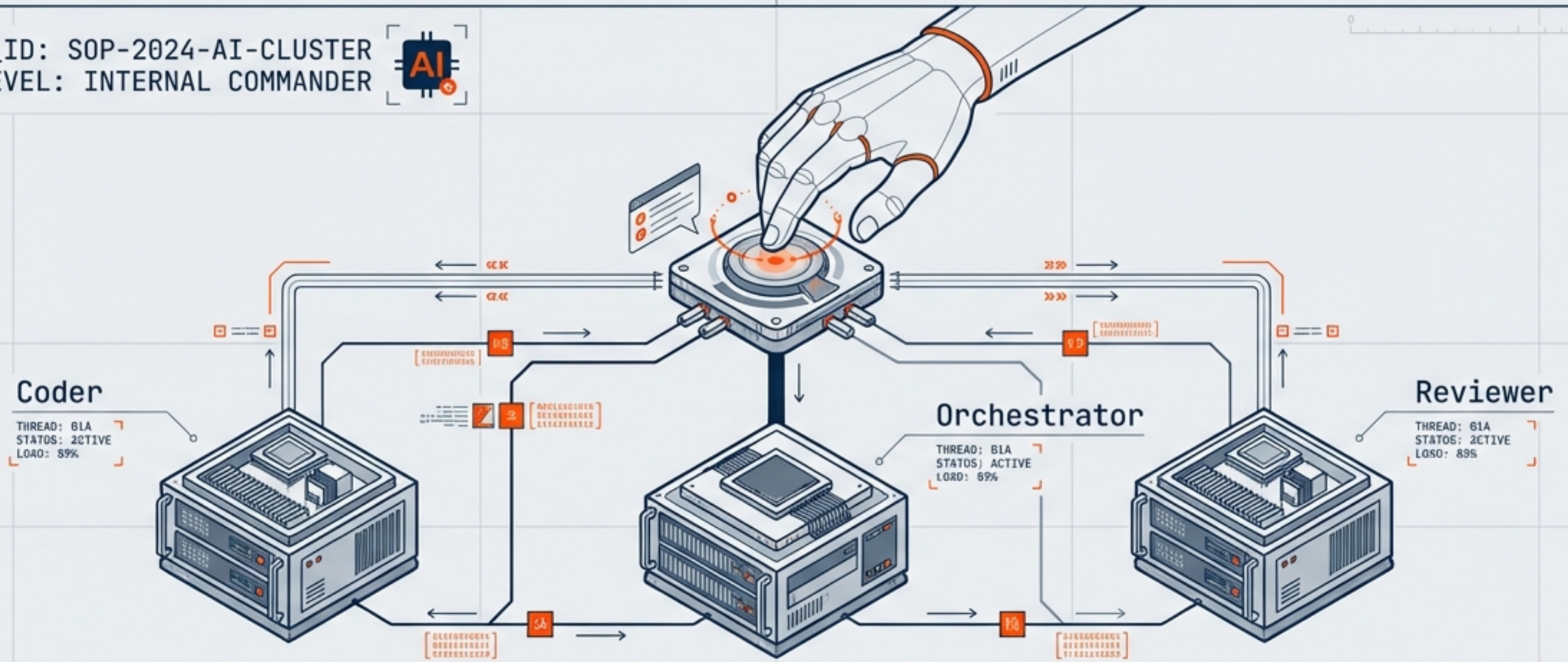
DOCUMENT_ID: SOP-2024-AI-CLUSTER
ACCESS_LEVEL: INTERNAL COMMANDER



数字员工集群运作全书

Digital Employee R&D Cluster: Operations Manual

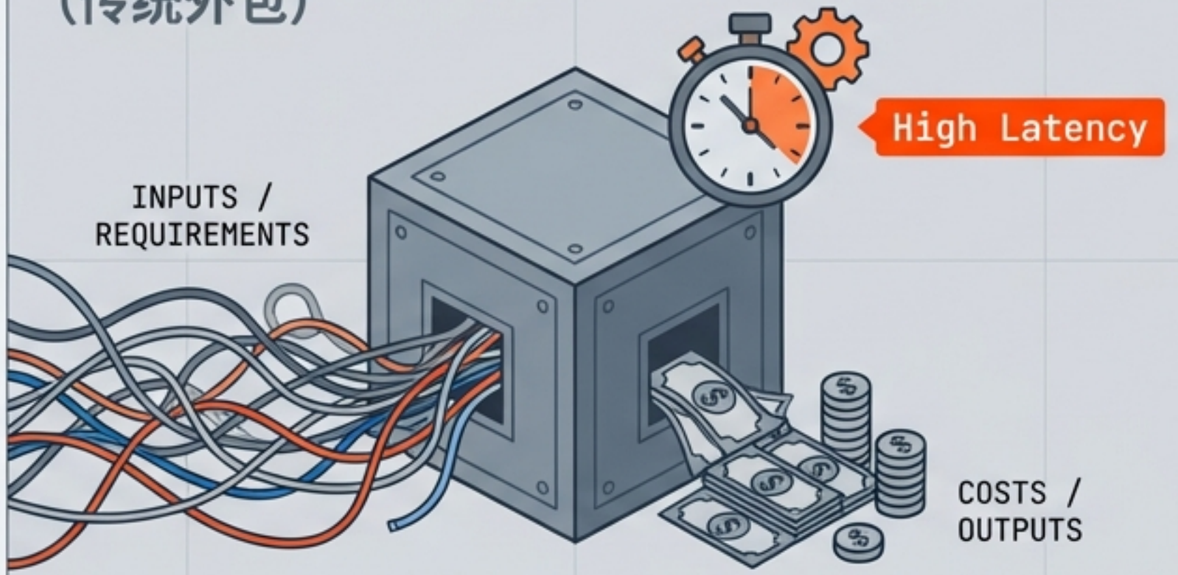
A Standard Operating Procedure for Managing Silicon-Based R&D Teams

VERSION: 1.0 V1 | OBJECTIVE: Defining the Management Lifecycle for Agentic Workforces | STATUS: ACTIVE

战略转移：从“外包黑盒”到“全透明管控”

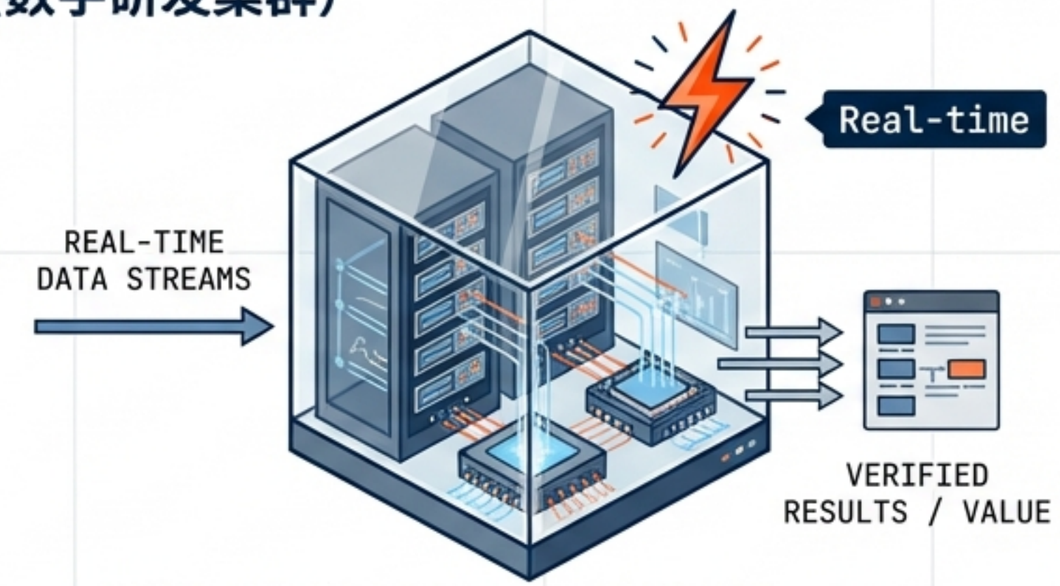
核心目标：可落地性（Actionability） — Define SOP for In-house Staff.

TRADITIONAL OUTSOURCING
（传统外包）



- Opaque Processes（过程不透明）
- Billing by Headcount（按人头付费）
- IP & Security Risks（知识产权风险）

DIGITAL R&D CLUSTER
（数字研发集群）

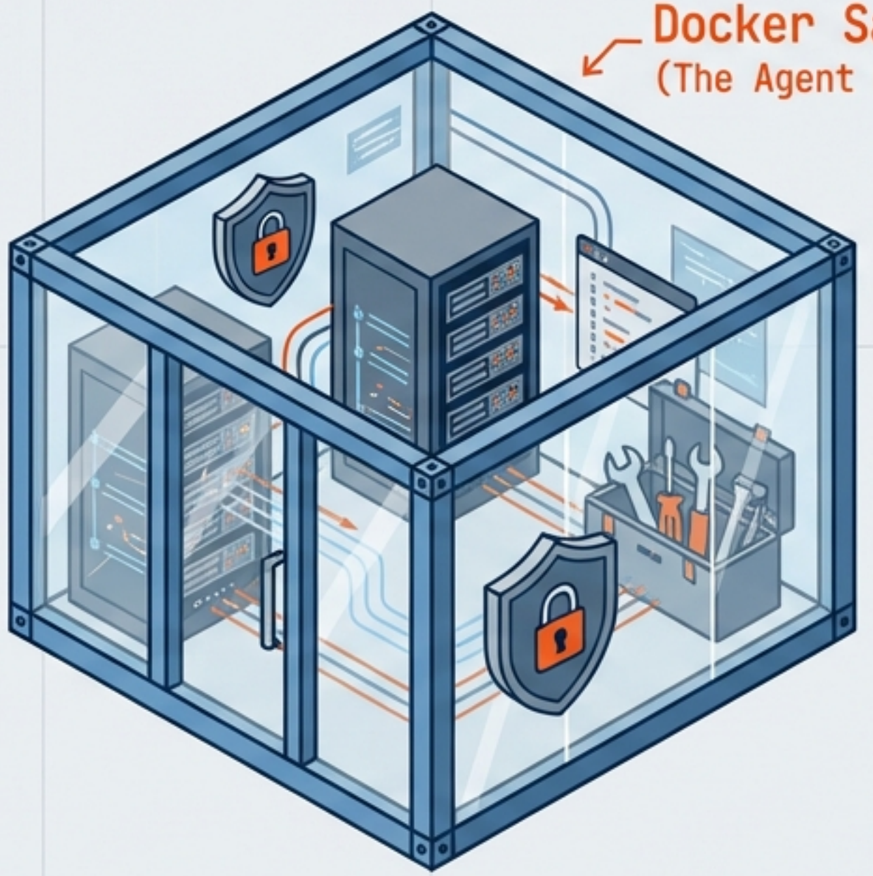


- 100% Auditability（全链路审计）
- Billing by Compute/Token（按算力付费）
- Zero-Trust Security（零信任架构）

ROLE REDEFINITION: From Coder (Writing Lines) → Commander (Managing Silicon Life)

入职配置 I：数字环境隔离

Onboarding I: Digital Environment Isolation



Standard Toolchain（标准工具链）

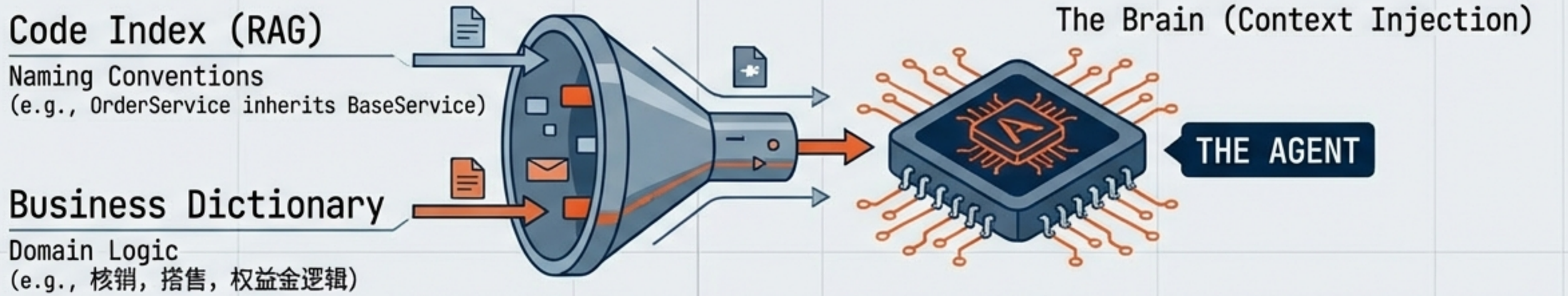
- ✓ Parity with Human Dev Environment
- ✓ Pre-installed Compilers & Libs

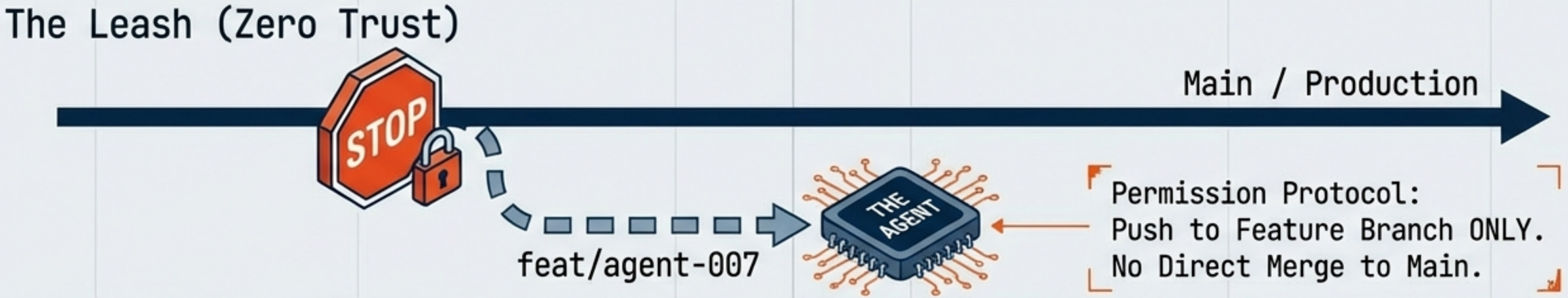
Environment Specs（环境规格）

- ✓ Base Image: Corporate_Std_v4.2
- ✓ Dependency: Frozen/Locked Versions
- ✓ Linter Rules: Strict Mode Enabled

入职配置 II：上下文注入与权限管控

Onboarding II: Context Injection & Access Control





核心SOP：Agentic研发循环五步法

Core SOP: The 5-Step Agentic R&D Loop

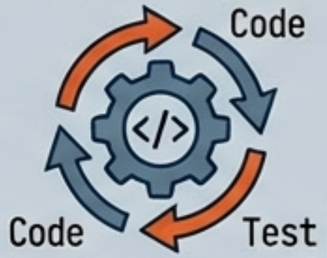
1 Step 1: Task Triage (任务指派)

Human Defines -> Orchestrator Splits

2 Step 2: Spec & Plan (方案设计)

Agent Proposes -> Human Approves

3 Step 3: Coding & Self-Fix (编码与自愈)



The Loop: Code <-> Test

4 Step 4: Agent Review (自动审计)

360-degree Scan

5 Step 5: Final Sign-off (最终签收)

One-Click Merge

Human Commander Zones (人类指挥区)

Agent Execution Zones (代理执行区)

步骤 1：任务指派（Task Triage）

ROLE: In-house Architect & Orchestrator Agent

Jira/GitLab issue ticket

Implement User Login Logic

#Agent-Task

INPUT:
Current User Schema (JSON)

OUTPUT:
JWT Token & User Object

DoD:
Unit Tests Passed, 200ms Latency

Orchestrator Agent

DB Schema

API Endpoint

Auth Logic

步骤 2：方案设计与对齐（Spec & Plan）

Replacing Meetings with Async Documentation

The Artifact

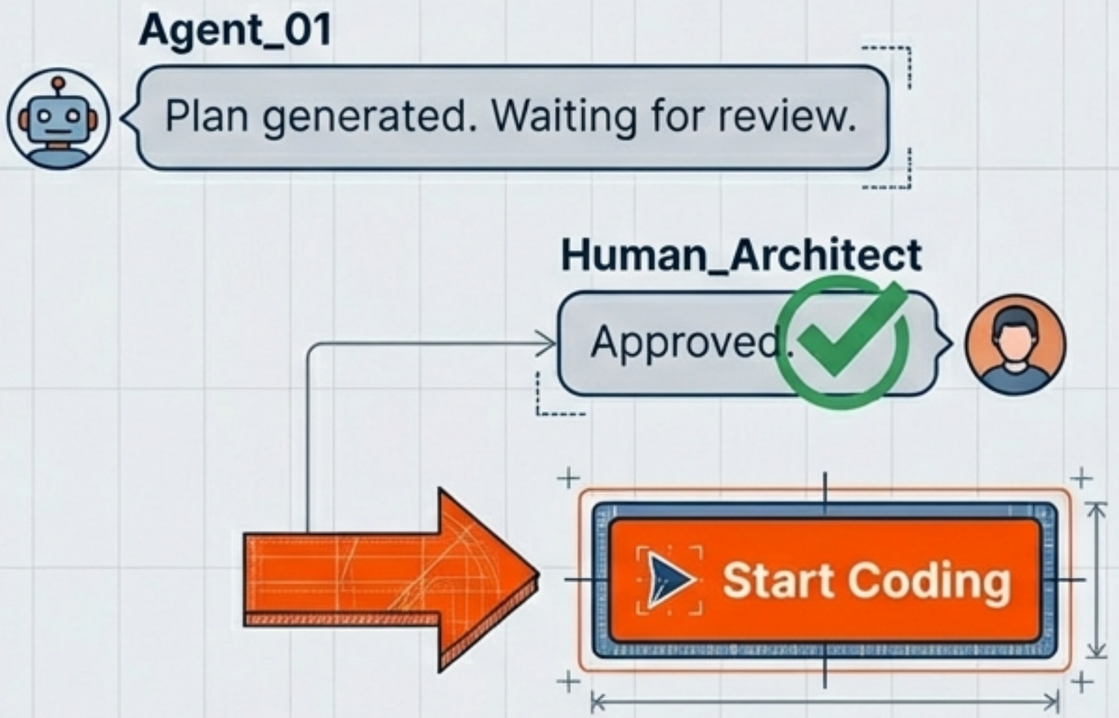
Implementation_Plan.md

```
## Affected Files
- src/auth/login.ts
- src/api/user.ts

## Interface Changes
- POST /api/v1/login
- Response: { token: string,
user: User }

## Logic Flow
1. Validate input credentials
2. Query DB for user
3. Verify password hash
4. Generate JWT
5. Return response
```

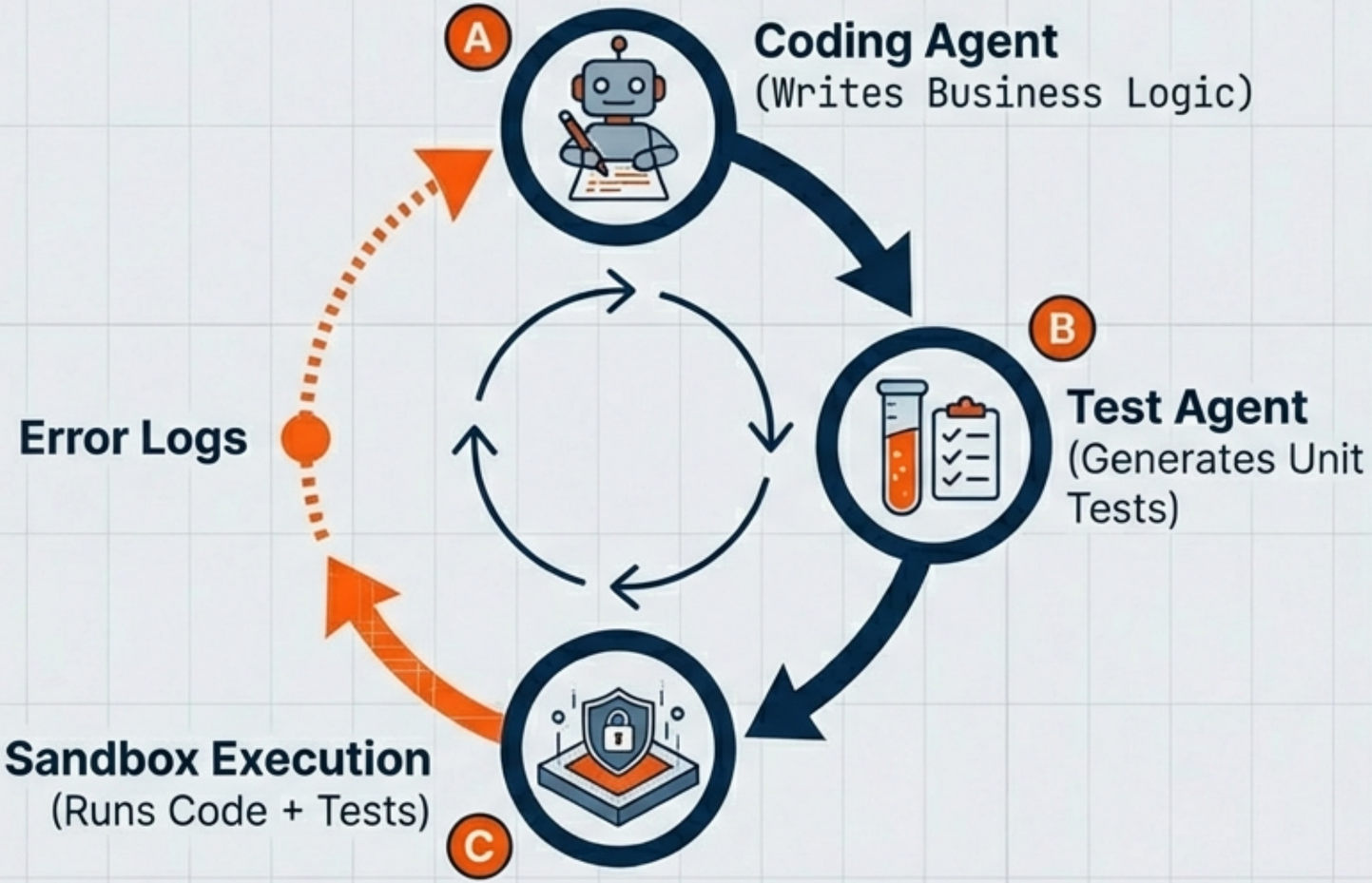
The Gatekeeper



Objective: Ensure architectural alignment before token consumption.

步骤 3：自动编码与自检（Coding & Self-Fix）

The Autonomous Production Loop



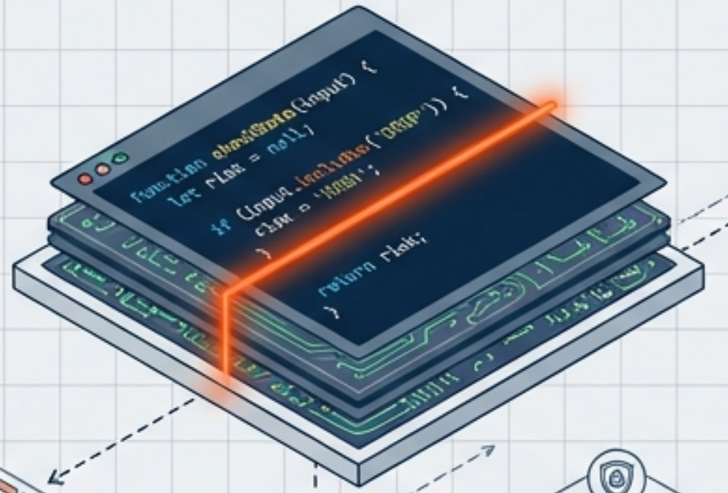
THE 3-STRIKE RULE

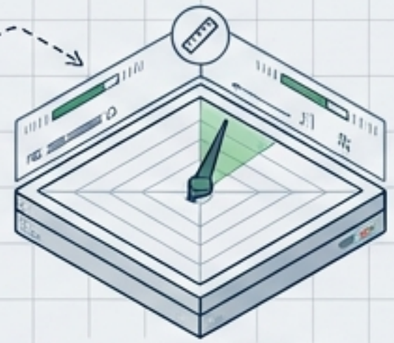
Max 3 Self-Repair Loops allowed.

If Fail Count > 3
THEN
⚠ Trigger "Human-Intervention-Needed".

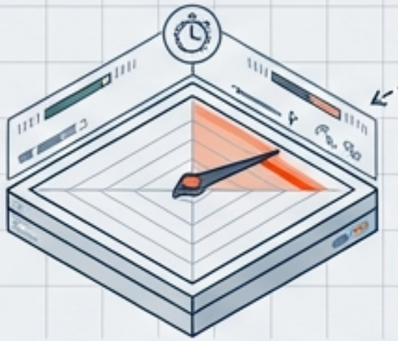
步骤 4：自动代码审计 (Agent Review)

ROLE: Review Agent

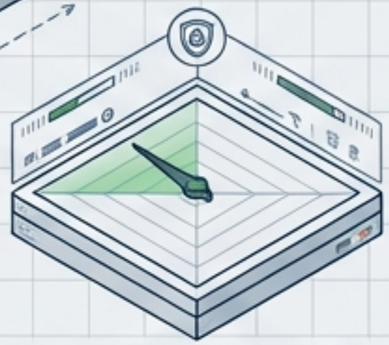




Norms (规范违例)
Check Naming & Style Specs.



Performance (性能影响)
Check Complexity & Latency.



Security (安全风险)
Check SonarQube & Injection Flaws.

Report Card

Review_Report.pdf

STATUS: PASSED

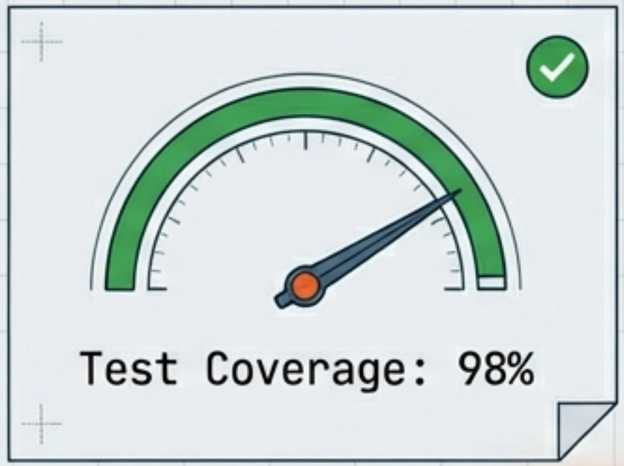
Summary:
Code meets performance & security benchmarks.
No major violations.

STATUS: WARNING

Summary:
Minor style issues detected. Latency within acceptable limits. Injection risks cleared.

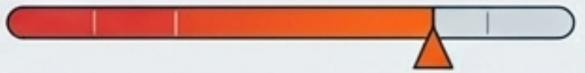
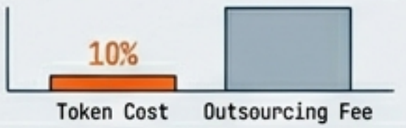
步骤 5：最终签收（Final Sign-off）

The Commander's Control



- **Workflow:** Human does NOT read every line.
- **Action:** Review Reports -> One-Click Merge.
- **Benefit:** High-level control, zero syntax fatigue.

绩效考核表（KPI Dashboard）

Category（类别）	Metric（指标）	Definition（定义 / 描述）	Warning Line / Target（预警线 / 目标值）
Effectiveness（产出效能）	Agent-FPR (First Pass Resolution) 	Percentage of issues resolved by Agent on the first attempt without human intervention.	⚠ < 60% (Optimize Prompt) 
Resilience（自愈能力）	Self-Fix Rate 	Rate at which the Agent autonomously corrects errors or failures during execution.	⚠ < 80% (Check Context) 
Efficiency（人力节省）	Human-Touch Ratio 	Average time spent by humans on tasks initially handled by Agent.	🎯 < 15 mins/task 
Cost（成本优化）	Token-vs-PSP 	Cost comparison between Agent token usage and traditional PSP (Professional Services Provider) fees.	🎯 < 10% of Outsourcing Fee 

风险管控与回滚预案（Risk Control & Continuity）

Systematic Risk Mitigation & Fail-Safe Protocol

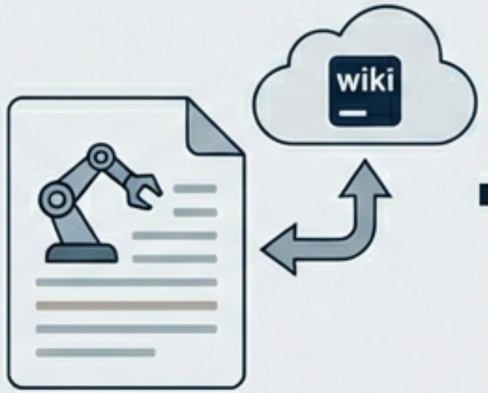
Anti-Hallucination

Tool: Check-Dependency

Imono: JetBrains Mono: Mandatory validation for non-standard libraries.

Safety Line

Anti-Silo



Tool: Doc Agent

Imono: JetBrains Mono: Weekly Logic Summaries auto-pushed to Team Wiki.

Disaster Recovery

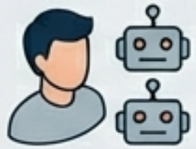
Action: Prompt-Rollback

Imono: JetBrains Mono: Instant Human Takeover of affected modules.

MVP 实验：Starbucks 营销配置接口

MVP Case: Starbucks Marketing Configuration Interface

Mission Parameters



Resources
1 Human Commander + 3 Agents

Time Limit
48 Hours

Scope
Marketing Activity Config Interface
（会员系统中的营销活动配置接口）

Success Metrics

Requirement Description → DONE

Code Generation → DONE

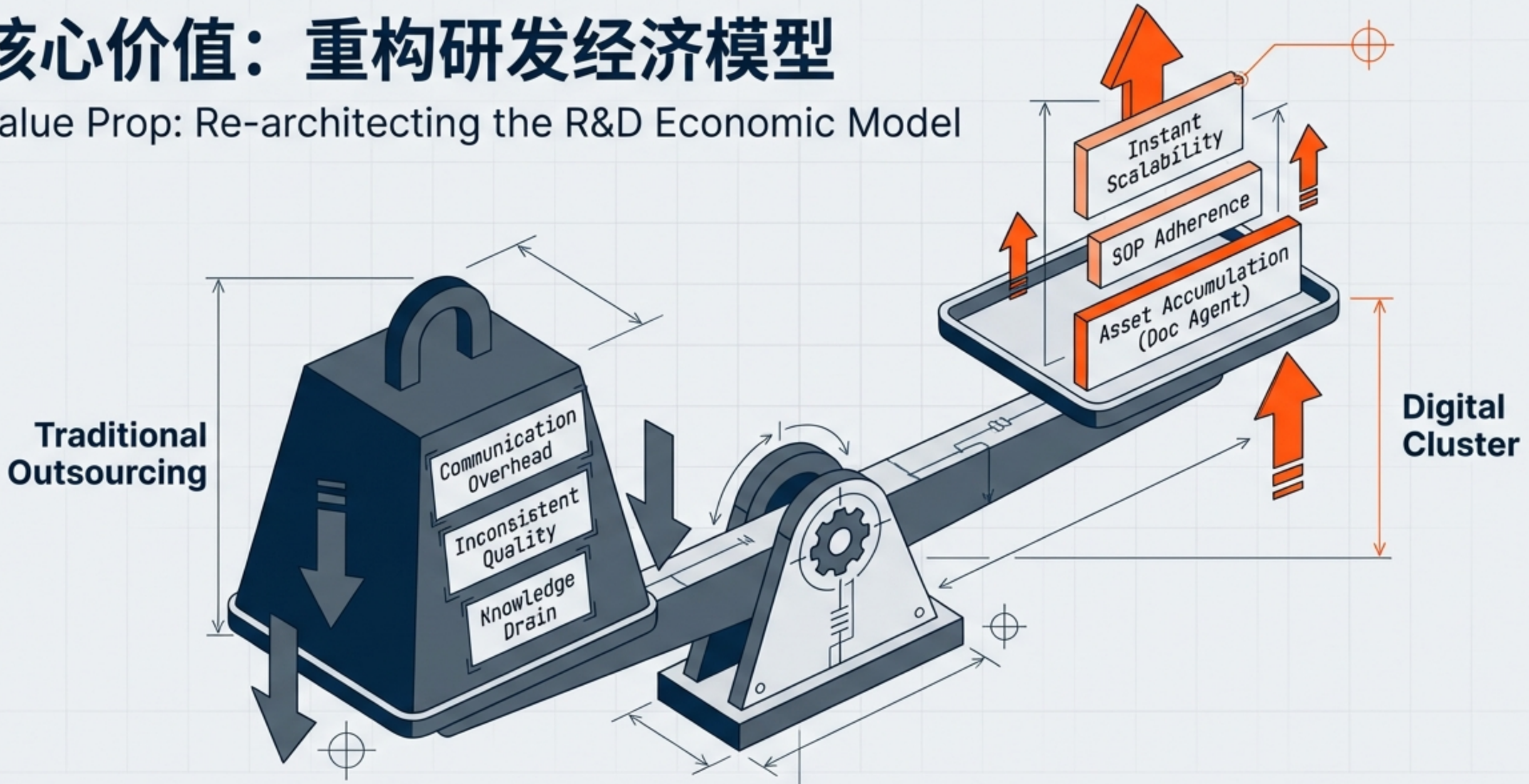
Unit Tests → DONE

Merge to Branch → DONE

Result: Zero alignment meetings. 100% Code Coverage.

核心价值：重构研发经济模型

Value Prop: Re-architecting the R&D Economic Model



Conclusion: Turning variable, external labor into fixed, programmable internal assets.

下一步行动计划

Next Steps: Phase 1 Execution

01 Initiate Review Agent: Safest entry point. Deploy on non-critical repos.

02 Setup GitLab CI/CD: Implement Agent Pipelines (Source: config_template_v1).

03 Prompt Engineering: Develop `Implementation_Plan.md` prompt templates.

“The goal is not just to write code faster, but to build a self-evolving R&D organism.