AI Sidecar Command Agent

Full Product Specification, Commercial Prospectus & Developer Brief

Version 2.0 – August 2025  
Author: RickPublic / ChatGPT

# 1. Executive Summary

The AI Sidecar Command Agent (AISA) is a lightweight local execution framework that extends the utility of AI tools such as ChatGPT by interpreting structured command blocks ([COMMAND]) and executing them securely within a sandboxed environment. It enables persistent AI workflows, traceability, and compliant human-AI collaboration in coding, writing, and publishing contexts.

# 2. Purpose and Context

AISA addresses the fundamental limitations of AI assistants—lack of persistent memory, local file access, and workflow continuity. This tool creates a local execution bridge, allowing AI to work alongside users in managing content, repos, and version-controlled tasks without cloud dependency.

# 3. Functional Requirements

• Parse [COMMAND] blocks from markdown or plaintext.  
• Execute file system and Git operations securely.  
• Track file lineage and maintain JSON logs.  
• Allow dry-run simulation and rollback.  
• Enforce sandboxed execution.  
• Manual override system for user control.  
  
Example [COMMAND] block:  
[COMMAND]  
create file summary.txt  
edit file report.md append 'Finalized'

# 4. Non-Functional Requirements

• Cross-platform (Linux/macOS/Windows)  
• Python 3.8+, minimal dependencies  
• No external internet access  
• Plugin architecture and GUI expandability  
• Permission-aware (run as safe local user)

# 5. System Architecture

Modular architecture includes:  
• Command Parser  
• Shell/Git Executor  
• Metadata Tracker (JSON)  
• Audit Logger  
• [Optional] Feedback Agent

[IMAGE: AISA\_Architecture\_v1.png]

# 6. Setup Instructions

• Install Git and Python 3.8+  
• Create /incoming, /staging, /archive, /registry  
• Run the parser on markdown files  
• Review logs/state after each run  
• Sample config:  
{  
 "sandbox": true,  
 "log": "./registry/logs.json"  
}

# 7. Build Strategy and Time Estimates

• CLI Parser & Sandbox Setup: 6–8 hrs  
• Git Command Wrapper: 5–7 hrs  
• Logging & Dry-run: 5–6 hrs  
• Metadata Tracker: 3–4 hrs  
• Manual Approval Interface: 4–5 hrs  
• GUI (Optional): 20–40 hrs

[IMAGE: AISA\_Timeline\_Phasing.png]

# 8. Developer Instructions

Developers must follow modular milestones:  
1. Parse [COMMAND] blocks in .md files.  
2. Execute file/Git actions securely.  
3. Maintain JSON state and logs.  
4. Implement rollback/dry-run system.  
5. Develop approval interface (manual Y/n).  
6. Keep testable modules, use docstrings.  
7. Submit work in small, validated commits.  
  
NOTE: Developer must sign NDA and IP assignment.

# 9. Commercial Viability

Target Users: AI creators, solo devs, content curators, civic coders  
Freemium Model: CLI (free), GUI/Pro Plugin (paid)  
Pricing: $200–500/user; $2k enterprise site licenses  
Use Case Scenarios: [IMAGE: AISA\_UseCases\_Summary.png]

# 10. Marketing Strategy

Launch via: Hacker News, Reddit (r/ChatGPT), Product Hunt  
SEO Tactics: 'Give ChatGPT Memory', 'AI Git Assistant'  
Demo Screencasts, Open Beta via Substack + Discord  
[IMAGE: Logo\_AISA\_Mock1.png]

# 11. UI Mockups

[IMAGE: Mockup\_CommandQueue\_UI.png]  
[IMAGE: Mockup\_FileLineage\_UI.png]  
[IMAGE: Mockup\_SessionReplay\_UI.png]

# 12. Financial Forecast

Open Source Adoption: Free CLI  
MVP Users: 200 x $200 = $40k  
Pro Add-ons: 50 x $500 = $25k  
Enterprise Licenses: 5 x $2,000 = $10k  
Phase 1 Total = $75k+  
[IMAGE: Chart\_Revenue\_Tiers.png]

# 13. Competitive Landscape

Compared to Notion AI, LangChain, and Copilot:  
• AISA offers structured, local execution with traceable AI commands.  
• No IDE dependency.  
• Zero-cloud reliance.  
• Simple setup.

# 14. Future Expansion

• GPT plugin integration  
• Voice/mobile command client  
• Publishing pipelines for Substack  
• Smart archive manager (based on AI use)  
[IMAGE: AISA\_FutureModules.png]

# 15. Call to Action

We’re looking for:  
• Python/Node developer  
• UI/UX designer  
• Early user testers  
Email: rick@groupbuild.org  
[QR or form link placeholder]