
AI ASSISTED SOFTWARE DEVELOPMENT FRAMEWORK (“AASD Framework”)

ALDA AASD Framework

Accelerating Development. Ensuring Quality.

Protecting Your Data.

ENTERPRISE READY

Highlights

01

The AI Revolution in Development

Why we built AA-SDF and how
it transforms software delivery

02

AA-SDF in Action

How our framework enforces
quality at every step

03

Security & Compliance

Enterprise-grade data
protection with flexible LLM
models

04

Our AI Ecosystem

Strategic partnerships and
proprietary AI tools

01

THE AI REVOLUTION

Why we built AA-SDF and how it transforms the way we deliver software

AI Is Reshaping Software Development — We're Following the Change

- 1. AI-assisted development is now a competitive necessity**

Not an optional perk. Teams that don't adopt AI will fall behind in speed and quality.

- 2. Since Q4 2025, AA-SDF is our company-wide standard**

After 18+ years of serving clients in USA and China, we've formalized our AI approach into a rigorous framework.

- 3. Move at AI speed without sacrificing quality**

Our framework delivers comprehensive features while maintaining production-grade quality.

- 4. Four layers of quality enforcement**

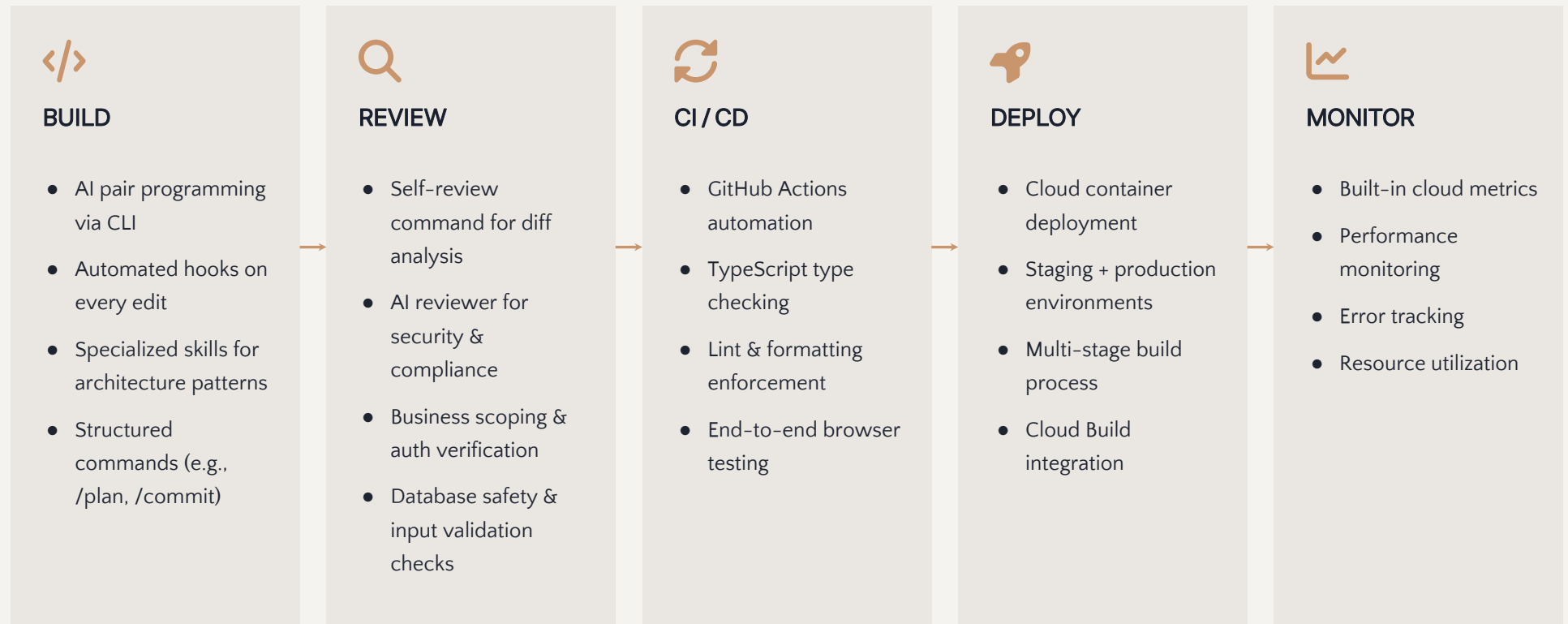
Real-time hooks, local validation, CI gates, and AI review — ensure nothing slips through.

- 5. AI accelerates execution — our expertise ensures outcomes**

Every architectural decision, implementation plan, and final code delivery is led and rigorously reviewed by seasoned engineers with deep domain knowledge.

AA-SDF: A Complete Framework for AI-Assisted Development

Covering the entire lifecycle from idea to production



AA-SDF: Defining and Verifying Delivery

How AI reshapes product manager, project manager, and QA roles



Product Manager

Value Architect

- Build runnable code prototypes
- Signal-driven roadmaps
- Cross-functional pairing with devs
- Natural-language data queries



Project Manager

Delivery Orchestrator

- AI-generated sprint plans
- Real-time risk forecasting
- Auto-synced action items across tools
- Velocity-predictive backlogs
- Live health dashboards



QA

Quality Sentinel

- Natural-language test generation
- Self-healing test suites
- Closed-loop quality immunity
- AI-predictive defect targeting
- Pixel-level AI visual testing

Common thread: All three roles shift from document-and-handoff to runnable-artifact-and-continuous-feedback. Human judgment moves up the stack to strategy, ethics, and creative direction; AI handles execution, maintenance, and pattern recognition.

02

AA-SDF IN ACTION

How our framework enforces quality at every step of development

Four Layers of Defense — From First Edit to Production

By the time code reaches merge, it has been validated 4 times

01 REAL-TIME HOOKS

Auto-lint on every edit · Core logic change alerts · Branch protection · Typecheck reminders

02 LOCAL VALIDATION

Self-review checks scoping, auth, compliance · Submit runs typecheck + lint + smoke tests + AI review

03 CI GATES

TypeScript type check · Lint enforcement · End-to-end browser tests — all blocking merge

04 AI REVIEW

AI reviewer agent reviews complete diff for logic bugs, security issues, and compliance

KEY INSIGHT

"By the time code reaches merge, it has already been auto-linted on every edit, self-reviewed for security, tested locally, and AI-reviewed."

4x

Validation layers

0

Direct main branch edits

100%

Core business logic edits flagged

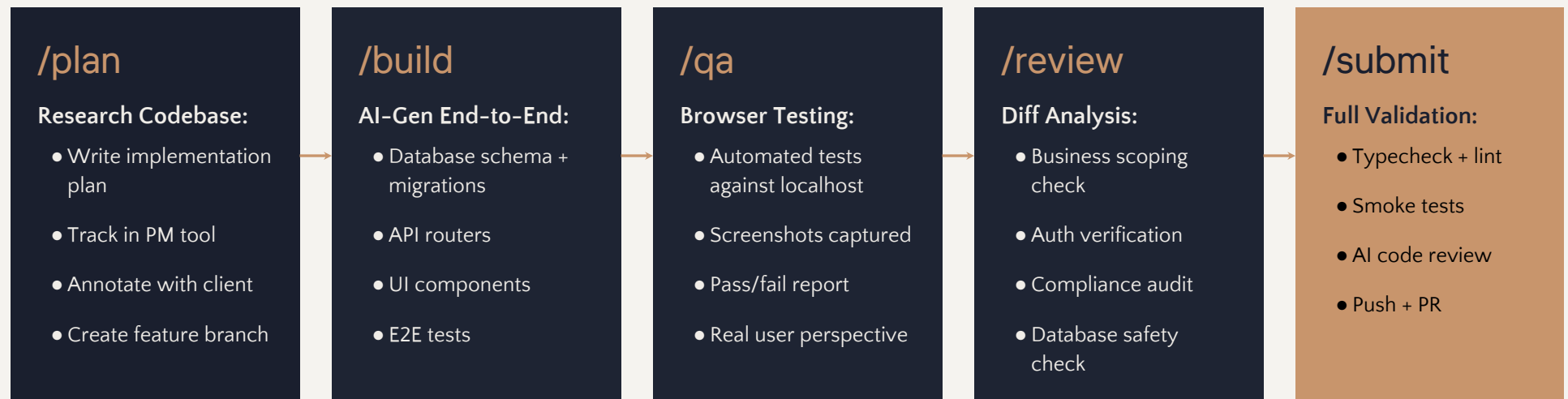
3

Blocking CI gates

CI is the **third** line of defense — not the first. Most issues are caught before code ever reaches the repository.

Structured AI Workflow — Plan, Build, Validate, Submit

Every feature follows the same rigorous pipeline



RISK CATEGORIZATION

● LOW

New UI page, form field, content change — builder decides

● MEDIUM

New data models, sensitive data features, integrations — quick check

● HIGH

Auth changes, billing logic, bulk operations — design review

Rule of thumb: If a feature touches more than 2–3 files or involves data model / authorization changes, start with a plan. The 10-minute annotation cycle prevents hours of rework.

Intelligent Hooks — Automated Guardrails on Every Edit

Hooks ALWAYS execute — unlike instructions which can be deprioritized

PRE-TOOL USE (CAN BLOCK)



Branch Protection

Blocks any file edits on main or prod branches. Forces feature branch workflow. Exit code 2 = deny.

WHY HOOKS MATTER

Unlike instructions in configuration files (which AI can deprioritize), **hooks always execute**. They are enforced at the system level.

This means:

- No developer can accidentally edit production branches
- Every code change is automatically formatted
- Core business logic changes trigger mandatory review alerts
- Type safety is never forgotten

POST-TOOL USE (ADVISORY)



Auto Format & Lint

Runs on every code file edit. Zero-config formatting and linting.



Core Logic Alert

Flags edits to core business logic files (e.g., auth, billing, data models). Triggers mandatory review before commit.



TypeScript Alert

Reminds to run typecheck when server/API files change.



Schema Change Alert

Reminds to regenerate client when database schema changes.

Specialized AI Agents — Expert Reviewers for Every Task

Each agent has specific tools and dedicated workflow



Senior Code Reviewer

AI REVIEW AGENT

- Business scoping verification
- Authorization & role checks
- Compliance & data protection audit
- Database safety & input validation
- Severity levels: Critical / Warning / Note



Test Generator

TEST AUTOMATION ENGINEER

- Creates automated browser tests from plans
- Executes in real-time with browser tools
- Generates robust, reliable test code
- Follows best practices from execution logs
- Single test per file, descriptive naming



Test Healer

TEST DEBUGGING EXPERT

- Systematically debugs failing tests
- Examines error details & page snapshots
- Root cause analysis for selectors, timing
- Fixes and verifies iteratively
- Marks flaky tests as skip when needed



Test Planner

QA STRATEGIST

- Explores application interface thoroughly
- Maps primary user journeys & critical paths
- Happy paths, edge cases, error handling
- Detailed step-by-step test scenarios
- Independent, order-agnostic scenarios

03

SECURITY & COMPLIANCE

Enterprise-grade data protection with flexible LLM cooperation models

Flexible LLM Cooperation — Your Data Security, Your Choice

You control the LLM. We control the quality.

A Your Enterprise Plan

Use your existing LLM Enterprise Plan for maximum data security. No code leaves your environment. Full audit trails and compliance with your IT policies.

B We Subscribe on Your Behalf

We subscribe to your preferred LLM's Enterprise Plan. Costs added to contract. Ensures compliance with your data governance requirements.

C Hybrid Model Approach

You use your preferred LLM for research and solution design. We implement and validate using our Enterprise Plan (e.g., Kimi) — fully integrated into AA-SDF with the same quality guarantees.

SECURITY TRADE-OFFS BY COOPERATION MODEL



Security Setup Effort

- A AA-SDF build-in security tooling; just plug into your existing plan and policies. (L)
- B We build and manage one clean environment plus the contractual wrapper. (M)
- C Same AA-SDF security baseline, but two environments to integrate and a boundary to manage. (H)



Your Involvement

- A Grant access and run internal approvals. (H)
- B Review vendor and contract terms. (M)
- C Govern research LLM inputs and approve dual flow. (M-H)



Risk to You

- A Data stays under your contract. (L)
- B Covered by our contract; vendor managed by us. (L-M)
- C Raise compliance and audit concerns where strict industry requirements apply. (M)

Compliance & Data Protection — Built Into Every Line of Code

Automatic safeguards for regulated industries (e.g., healthcare, education)

EXAMPLE: SENSITIVE DATA MODELS

Taking a healthcare project as an example — all auto audit-logged:

Patient Records	Assessments
Treatment Plans	Treatment Sessions
Prescriptions	Health Data
Billing Records	Personal Logs
Protected by role-based access + audit logging	

ROLE-BASED ACCESS CONTROL

Every query **MUST** include tenant isolation filtering — no exceptions.

Specific roles and access patterns are customized per project and client requirements.

SECURITY CHECKLIST

- ✔ **Tenant Isolation**
Every query enforces tenant filtering; complete data isolation per client.
- ✔ **Role-Based Access Control**
Sensitive data models protected by project-specific roles and access patterns.
- ✔ **Audit Logging & Alerts**
All sensitive data access auto-logged; compliance alerts trigger on file edits.
- ✔ **Data Handling Safeguards**
No sensitive data in logs, errors, or test fixtures; soft delete prevents access to archived records.
- ✔ **Input Validation**
Strict validation enforced on all API endpoints.

04

OUR AI ECOSYSTEM

Strategic partnerships and proprietary tools that extend our AI capabilities

AI Partners & Proprietary Tools — Beyond Development

From development to operations to end-user tools — AI at every layer

PARTNERSHIP



Autoptic.ai

AI-Powered DevOps Automation

We partner with **Autopic** for AI-driven DevOps workflows, demonstrating our commitment to embracing AI across the **entire software lifecycle** — not just coding.

This partnership enables:

- Automated operational workflows
- AI-enhanced deployment pipelines
- Continuous optimization of infrastructure

More Info: <https://www.autoptic.ai/>

PROPRIETARY TOOL



DigiAI USA

AI Agent Platform for Enterprises

Our proprietary platform lets enterprises **build and launch AI agents in minutes** — no coding required.

Compatible with all major LLMs:

- OpenAI GPT • Anthropic Claude
- Google Gemini • Meta Llama • AWS Bedrock

Perfect for enterprises without development teams who need custom automation and AI integration.

More Info: <https://www.digaiusa.com/>

LET'S BUILD THE FUTURE

Together

Your data security is non-negotiable. Your project success is our mission.

We continuously monitor industry best practices to refine our framework and maximize value for every client.

10+

Years Experience

20+

Clients in USA & China

50+

Projects Delivered