

AI-Assisted Development

Using AI-Assisted Development to Provide Contextual, Event- Driven Integration Across the Enterprise

A ManTech White Paper

Using AI-Assisted Development to Provide Contextual, Event-Driven Integration Across the Enterprise

Introduction

Code-generating artificial intelligence (AI) is a category of tools that automates the development and maintenance of software called machine programming. Training models and data are run against billions of lines of source code from publicly available sources such as GitHub repositories and, in the case of ManTech's Enterprise Smart Assistant (MESA), an unsupervised learning technique in machine learning (ML) that uses neural networks as generative models to automatically learn the natural features of the source code. This source code analysis allows the code-generating AI to parse natural language and generate code in response, translate code to natural language, and provide code suggestion and review during debugging in up to a dozen different programming languages, to name just a few use cases.

This White Paper presents ManTech's MESA platform that enhances the software development life cycle (SDLC) using an extensible architecture that enables pluggable tools and features. MESA provides both out-of-the-box and custom integrations along with sophisticated capabilities.

Problem Statement

The use of AI/ML to accelerate the SDLC is transforming enterprises and requiring a shift in the skillsets needed to deploy and manage large, complex environments. A number of industry and academic initiatives (OpenAI's Codex, CMU's PolyCoder, and DeepMind's AlphaCode) and commercial offerings (GitHub Copilot and Amazon CodeGuru) are enabling AI-assisted code explanations, review, and generation. These projects and tools can be confusing to customers and lead them to question the value of AI-assisted development for their organization and the overall reliability of a self-learning model.

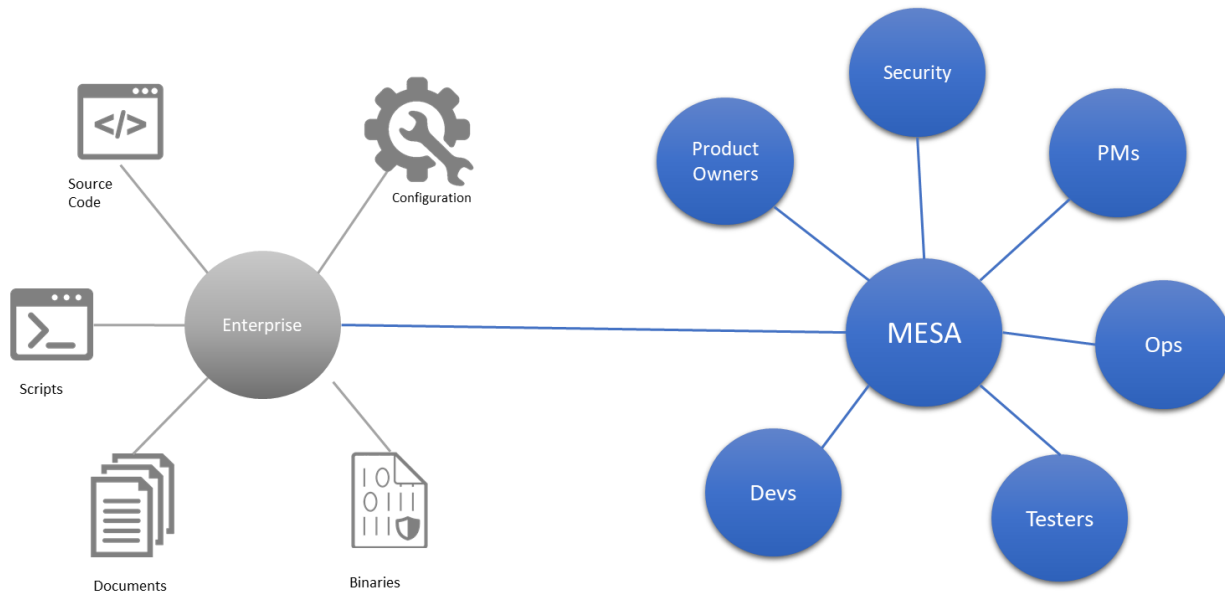
Additionally, integrating new services, especially AI/ML-enabled solutions, can be complex. It's not uncommon for large enterprise organizations to have dozens or even hundreds of pipelines to manage. MESA decouples system engineering and software development life cycle events from the CI/CD pipeline and makes them accessible through a subscriber model.

ManTech's AI-Assisted Development Platform

ManTech's Enterprise Smart Assistant (MESA) is our new platform that uses AI to translate code into natural language for conceptualizing, understanding, and securing the software development process. MESA frees organizations from pipeline management and empowers expert teams to build enterprise capabilities with less reliance on DevOps engineers or developers.

Software development and systems engineering (SE) is a fast-moving and dynamic industry. With MESA, teams can apply the latest changes in ML, security, and infrastructure automation while ensuring compliance with development standards and policies. MESA decouples SE and SDLC events from the continuous integration/continuous delivery (CI/CD) pipeline and makes them available through a subscriber model.





Understand and Empower

MESA provides greater visibility and insight into code changes. The MESA Explainer plugin combines the best of third-party AI tools and customer algorithms to provide code suggestions and reviews, increasing code quality and enabling code convergence to best practices and standards, and explains, in plain English, what is happening when code changes are made by developers. This enables project managers, customers, product owners, and testers to streamline the decision process for feature deployments and code changes, assess the relevance of certain requirements, and auto-generate release notes—with less reliance on developers. That said, developers, too, can benefit from this capability during source merges when MESA more efficiently provides insight into their colleagues' actions.

Secure

The “Shift Left” strategy of testing early in the development process, while important, is no longer enough to ensure a secure SDLC. Consider a well-known, severe vulnerability incident, Log4Shell. Using traditional methods to validate that development teams remediated this vulnerability would require inserting scans into pipelines to verify that the library version was corrected or redacted. Typically, a security team would work with a DevOps team to identify the pipelines to change, make the required changes, and implement scan report collection procedures. This process is expensive and time-consuming with no guarantee of total coverage across projects.

With its event-driven approach, MESA provides the security team with the autonomy to independently check and validate code and configuration changes at the level of changes, thereby avoiding pipeline changes and allowing the team to target their efforts on the deltas and/or perform bulk code base scans. As new security requirements arise, the scans can be plugged into MESA to integrate with security information and event management (SIEM) and monitoring tools.

Innovate

By removing the dependencies on pipeline modifications, development team sprint schedules, and DevOps engineering expertise, MESA frees experts to spend more time developing new



applications and capabilities. Individuals and small teams can experiment with enterprise tools without impacting the production cycle or using the cycles of DevOps engineers.

Personas and Scenarios

- **Developer**

Using the git-pull model, developers often perform code merges and reviews. However, developers—especially those in large teams—may be unfamiliar with the code, complicating these quality assurance processes and impacting productivity.

MESA presents information about code changes to assist developers in this decision-making process. One of the strengths of MESA is that the OpenAI engine allows the operator to explain code in different contexts, such as for a developer versus a project manager, resulting in explanations tailored to the reader's perceived level of expertise.

- **Information Security Officer**

Information security officers (ISOs) need to ensure that required security checks are added to the software development life cycle. A common scenario would have the ISO direct a DevOps engineer what to scan for and how to format reports, then integrate the data with SIEM tools and wait for the next sprint plan to implement and transmit the scan results. However, this is a suboptimal and error-prone approach due to the swiftness with which modern threats surface. In addition, development teams may not implement the organization's security policy across all of their projects and pipelines.

Using MESA's event-driven security, any committed artifact that the ISO deems necessary is detected and scanned. As vulnerabilities such as the Log4j hack are reported, the ISO's security team can connect their SIEM tools, dashboards, and log aggregators to MESA to search and alert on found vulnerabilities. This approach puts the ISO's security team in control and enables them to achieve compliance with configuration and code standards in their ecosystem.

- **System Administrator**

System administrators are responsible for the successful operation of a wide variety of systems and software, and often rely on configurations provided by a development team. However, some software development decisions could affect system performance and increase operating costs; for example, creating Kubernetes manifests without memory or processor constraints could result in runaway pods that overconsume resources.

MESA has a Kubernetes Configuration Scanner component that can monitor Kubernetes file check-ins and scan for policy violations without impacting the development team or requiring fluency in programming languages like JSON and YAML or in Kubernetes cluster management.

- **Project Manager**

Project managers commonly rely on developers to explain changes in code baselines, but these explanations are often excessively detailed and fail to provide context for the changes.

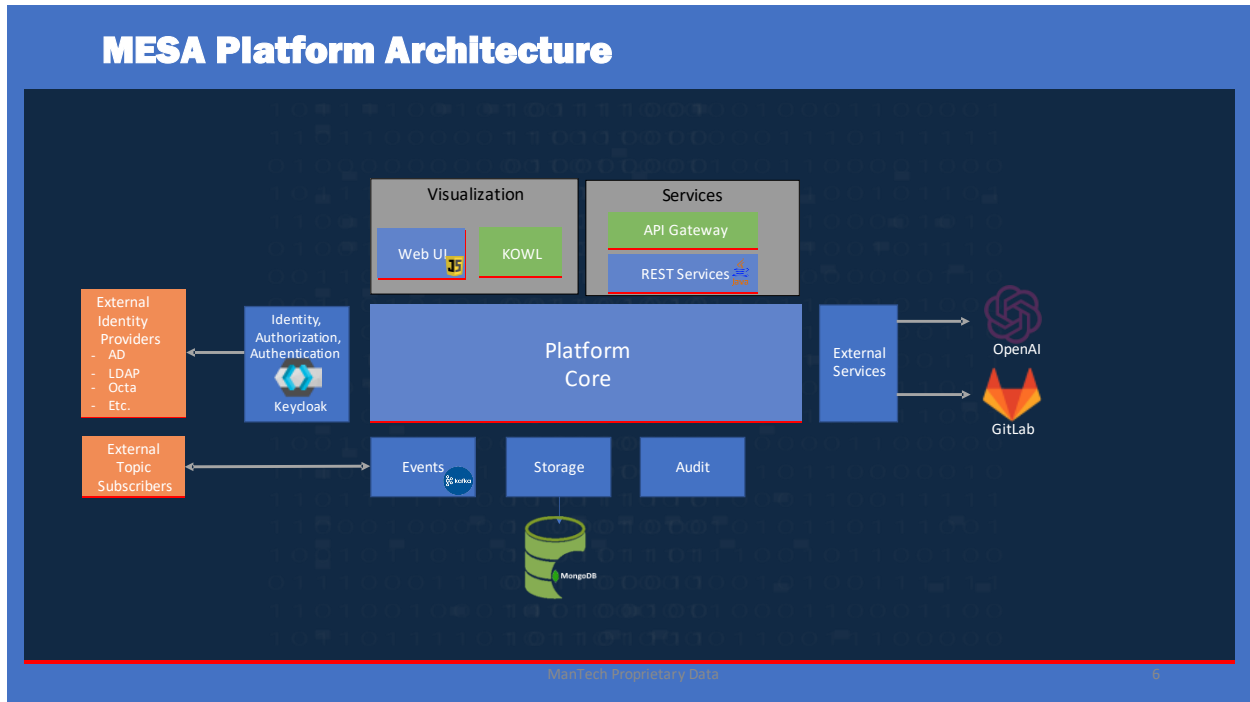
Using AI/ML-driven code explanations, MESA provides simple and concise information that only targets specific changes in a software release, test coverage, or requirements traceability, allowing project managers to independently make informed decisions.



Out-of-the-box Components

The MESA platform supports integration through a representational state transfer (REST) service application programming interface (API) and Kafka topics for asynchronous event communication. MESA's internal components include an authentication and authorization module built on Keycloak, MongoDB for persistent storage, and a user interface for end-user and administrative interaction.

ManTech has extensive experience supporting customer environments across every security classification domain and in hybrid, multi-cloud enclaves. MESA can be integrated into a complex enterprise or as a brand-new implementation, based on the infrastructure and existing tools.



The real power of MESA is its ability to tap into external products. The number of enterprise tools seems boundless and organizations have their preferred products. MESA is architected to work with a wide variety of tools, particularly those that are common or de facto standards. MESA does the heavy lifting by providing a suite of integrations out of the box.

MESA's set of integrated tools provides the following capabilities:

- Code explainer
- Container scanner
- Git-repo interface
- Jira integration
- Kubernetes YAML scanning
- Search and analytics on SDLC events
- Visual data routing, transformation, and system mediation

Benefits

MESA delivers the following key benefits:

- Decouples pipelines from external activities on artifacts, allowing for faster adoption of capabilities and innovations.
- Is tool independent: organizations can use their favorite tools.
- Can be implemented with no disruption of existing workflows, reducing operational risks.
- Allows third parties to integrate with SDLC events—external teams can work autonomously without impacting the development teams.
- Targets just the changes, rather than bulk scanning the repository, reducing alert fatigue and allowing prioritization of events.
- Uses event-based integration that is highly decoupled, which supports multi-cloud deployments and multi-modal messaging.

Conclusion

MESA's hyperparameters, topic visualizations, and SIEM integration logic are uniquely tailored for federal agencies. MESA leverages natural language interpretation using large-scale generative AI models with reasoning and comprehension capabilities and applies it to development code. This provides real-time insight into the software development life cycle and delivers the appropriate level of abstraction based on the operator's function and role. Existing capabilities, tools, and third-party plugins do not provide this level of enhanced functionality.

MESA will run models that capture semantic similarities in text during text and code searches that can be customized to answer specific questions, summarize large amounts of information, or generate original content such as proposal language or policy/procedure documentation.

MESA offers significant advantages for enhancing and securing systems engineering and SDLC environments. Beyond the use cases and related personas outlined in this white paper, MESA is highly customizable and, as transformative technologies such as AI/ML and cloud computing continue to advance, will accommodate innovation and increase the value proposition.

To learn how code-generating artificial intelligence can securely and efficiently improve insight into the software development life cycle in your enterprise environment, please reach us at:

ContactUs@mantech.com

