Software Testing in DevSecOps for DoD

Delivering High-Quality, Reliable Embedded Systems

The Department of Defense's (DoD) own war analysis reports that current force plans would leave the United States' military unable to deter and defeat adversary aggressions if steps to maintain and arguably regain a technological edge were not pursued. Profound and unsettling consequences exist for the U.S., its allies, and the world if the DoD doesn't achieve its modernization strategy. Modernizing will provide the U.S. military with the ability to deter coercion, aggression, and even war.

Modernized strategic warfighting concepts, like Joint All-Domain Command and Control (JADC2), connect many systems with the goal of making the battlespace interoperable, expandable, cybersecure, safe, and reliable in all aspects of operational topology.

DoD's modernization strategy requires the delivery of high-quality software systems that are interoperable, expandable, and sustainable. It includes the formalization of DevSecOps, leveraging test automation to curb consequences of system errors, and compliance and conformance to proven standards that ensure safe and secure mission-critical requirements.

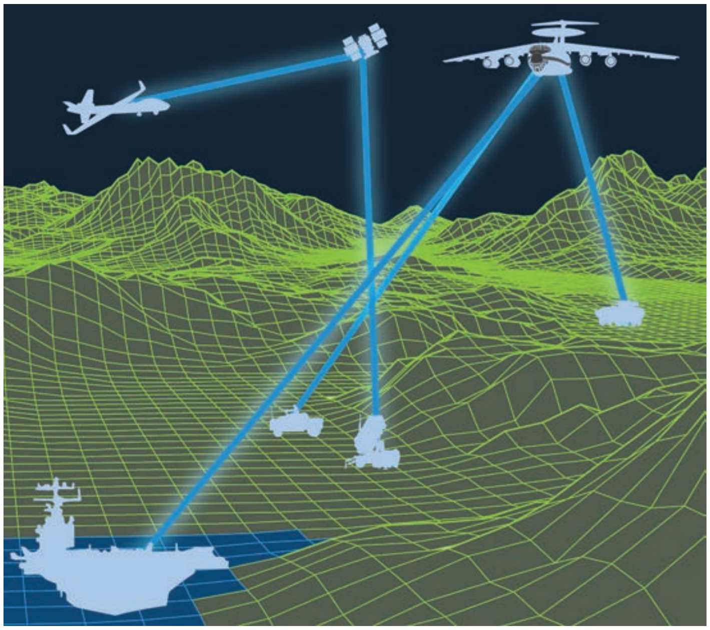
Modernize Into DevSecOps

The formalization of DevSecOps in DoD is part of the modernization strategy that enables innovation and faster deployment times to keep pace with the growing demands of the modern battlefield without sacrificing quality and security. Protecting mission-critical software applications is a priority that starts with building in software quality and security right from the start.

Consequences of System Errors

Preventing errors in these modern warfare systems before going into production is critical. If they aren't caught early in the software development life cycle (SDLC), the consequences are dire and include:

- Serious warfighter mistakes
- Production delays
- Cost overruns



Leverage Test Automation

Automated testing solutions help modern warfighters by ensuring that the software they use in all missions is secure, safe, and performs under high levels of stress. Testing early—prior to production—helps to ensure fewer threat vectors, mistakes, and problems during your workflow. It also leads to easier fixes, shortens deployment times, and lowers project costs.

By automating static analysis, unit, integration, system, and regression testing, your team can reduce the labor, complexity, and burden of manual testing. Artificial intelligence (AI) helps developers prioritize and address the static coding violations with highest risk and impact to software quality. AI also eases static analysis adoption.

Contact Us

Talk to an expert to learn how your team can continuously deliver high-quality, reliable embedded software systems.

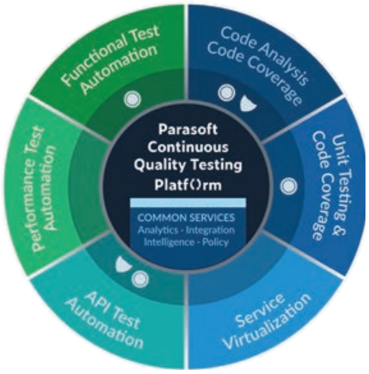
Make Testing Continuous

Continuous testing provides an automated, unobtrusive way to get immediate feedback on the risks associated with a software release candidate. Testing during the initial development cycles is 25 to 30 times less expensive than testing just prior to production. A software bug that needs five development hours at $200 per hour to fix costs $1,000 when caught early versus $30,000 when caught late in the SDLC.

Ensure Standards Compliance & Conformance

The software embedded within connected warfare systems has real-time, safety, cybersecurity, and mission-critical requirements. Automating source code analysis, unit testing, and code coverage makes it easier and faster to achieve compliance for standards like:

- MISRA C and C++
- DO-178C Level A-D for airborne and military systems
- FACE$^{\text{TM}}$ conformant software for airborne systems
- DO-326A for cybersecurity


Functional Test Automation
Code Analysis Code Coverage
Unit Testing & Code Coverage
Service Virtualization
API Test Automation
Performance Test Automation
Parasoft Continuous Quality Testing Platf()rm
COMMON SERVICES
Analytics · Integration
Intelligence · Policy

Parasoft's Continuous Quality Testing & Functional Safety Compliance Solutions

Deliver software that's safe, secure, and reliable. Parasoft's continuous quality testing and functional safety compliance solutions unify and automate static code analysis, unit testing, integration, and system testing. Run stress, endurance, and spike testing to ensure that connected systems can handle the load. Teams can create rich, multi-profile test scenarios to scale performance testing and accelerate load and performance testing by reusing API tests for nonfunctional scenarios.

CAPABILITIES

Coding Standards

Employ static analysis within the CI/CD DevOps workflow to conform to industry coding requirements more easily, such as JSF, DISA, CERT, CWE, OWASP, MISRA, AUTOSAR C++ 14, and custom coding standards.

Security

Find security vulnerabilities and bugs early using static analysis coding standards (SEI CERT C/C++, CWE, OWASP).

Code & Test Coverage

Ensure 100% code covered through statement, branch, and MC/DC methods satisfy compliance requirements to DO-178C. For Level A, automate assembly or object code verification.

Dynamic Analysis Security Testing (DAST)

Find security threats during runtime as required by DO-326A with unit, integration, and system security testing. Perform API, fuzz, penetration testing, and service virtualization to find threats that expose sensitive data embedded in APIs and prevent API attacks.

Verification & Validation

Seamlessly integrate software verification and validation into C and C++ development to increase code quality, ensure security and safety, and expedite compliance to DoD standards.

Containers

Ensure containerized solutions meet DoD security standards and best practices with Parasoft's static application security testing (SAST) tool, which has been containerized and pre-approved for use by DoD and other key federal agencies. It's available for download from the Iron Bank repository.

Parasoft SAST in Iron Bank

With recent attacks targeting the software supply chain, Parasoft realizes the importance of hardening and securing the toolchain to mitigate software integrity issues. Notably, Lockheed Martin, in addition to the F-35 Joint Program Office (JPO), has formalized the Parasoft SAST solution as part of its software testing process for quality and security.