GRAMMATECH

REAFFIRM

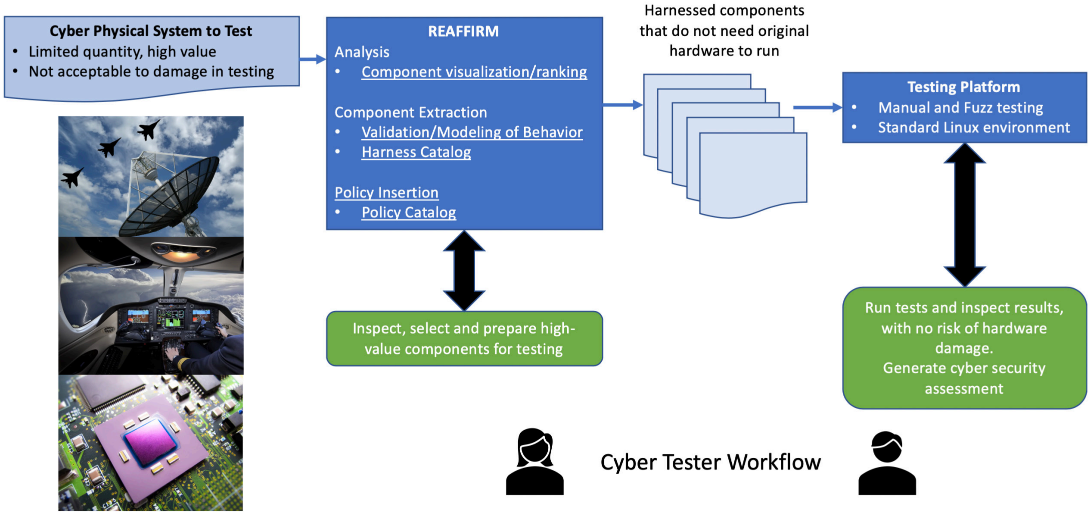
Reverse Engineer, Analyze, and Fix Firmware

Reverse Engineering
Software Composition Analysis
Static Application Security Testing
Dynamic Application Security Testing
Proof of Vulnerability

Design
Development
✓ **Pre-Deployment**
✓ **Deployment**
✓ **Sustainment**

Problem	Avionics and embedded weapon systems are cyber-physical systems with high security and safety requirements. Cyber security assessments and testing are complicated by limited knowledge about the firmware, and by the expense and risk of damage when working with real hardware.
Market Need	Facilitate cyber security assessments and testing of embedded systems by enabling better understanding of firmware components and supporting virtualized testing.
Approach	Extract security-relevant *components* from firmware, *present and rank* them for the analyst, *identify and isolate* the hardware-coupled portions, and *virtualize* these for testing. Support *reproducibility* and *gradual automation* of workflows.
Applications	Understanding, testing and patching of embedded devices for the military (weapons controls, navigation systems), critical infrastructure (industrial-control systems) and everyday applications (automotive controls, medical devices).

The REAFFIRM Workflow:



Cyber Physical System to Test
- Limited quantity, high value
- Not acceptable to damage in testing

REAFFIRM

Analysis
- Component visualization/ranking

Component Extraction
- Validation/Modeling of Behavior
- Harness Catalog

Policy Insertion
- Policy Catalog

Inspect, select and prepare high-value components for testing

Harnessed components that do not need original hardware to run

Testing Platform
- Manual and Fuzz testing
- Standard Linux environment

Run tests and inspect results, with no risk of hardware damage.
Generate cyber security assessment

Cyber Tester Workflow

REAFFIRM Innovations	State of the Art
Automated tooling for reverse-engineering, architecture recovery, and component visualization	Ad-hoc collections of tools to perform discrete reverse engineering tasks limit an analyst's efficiency and ability to evaluate cyber threats.
Component extraction and harnessing to allow virtualized testing without hardware	No support for component extraction. Only low-risk, end-to-end tests are conducted to avoid hardware damage.
Workflow captures analysis process and supports gradual automation of manual tasks, with both human- and machine-readable artifacts	Informal workflows with no principled support for gradual automation. Lack of reproducibility, duplicated work.

Current Status

- TRL 6 – in transition to multiple organizations
- Supports ia32, ARM 32-bit/Thumb, PowerPC 32-bit
- MIPS support in progress

Use Cases

- Cyber vulnerability research
- Virtualization of Cyber Physical Systems
- Micro-patching firmware

GRAMMATECH

FOR MORE INFORMATION
www.grammatech.com

EMAIL research@grammatech.com

© GrammaTech, Inc. All rights reserved.
GrammaTech Inc. Proprietary Information.