SAFETY AND SECURITY THROUGH INTEGRATED ASSURANCE

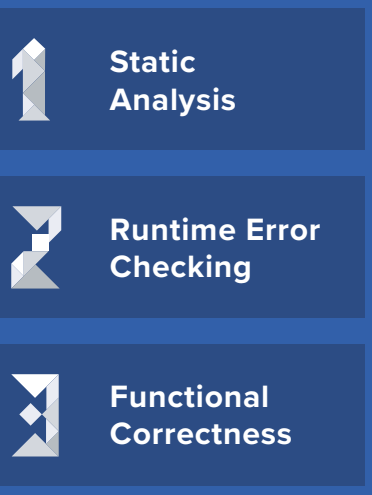
Program Overview

Modern systems rely on software, but software is often fragile and prone to vulnerabilities. Advanced software assurance tools are capable of detecting weaknesses. On their own, assurance tools are difficult to use and understand. Tangram Flex's engineering team identified the best assurance tools for integrating cyber resiliency in to our customer's software development environment, making complex software assurance tools accessible.

Technical Approach

Tangram determined three types of software assurance needs for our customer: static analysis, runtime error checking, and functional correctness.

Combining assurance tools helped our customer's engineers understand their code. Tangram integrated assurance tools into reusable workflows within the customer's continuous integration (CI) environment. The workflows are simple to use and provide our customer's engineers with readable assurance results. Engineers were able to quickly identify and act on critical safety and security risks.



Cyber Resilient Code with Tangram Pro™

Tangram Flex uses a component-based approach to assurance. Embedded and cyber-physical systems are broken down into smaller pieces so assurance tools can be applied in three ways:

to components themselves

to code that connects components

to systems where components integrate

Tangram Pro™ helps engineering teams generate cyber secure software to connect components together. Tangram Pro™'s automatic workflows include advanced assurance tools. Full spectrum analysis at each step of development provides engineers with clear, usable assurance evidence.