An Architecture Supporting Formal and Compositional Binary Analysis

A traditional microprocessor provides binary compatibility, optimizing compilers, and driver support.

But reasoning is difficult due to complexity in modeling...
- global machine state
- mutability
- large numbers of instructions and features
- arbitrary control flow
- unenforced call conventions
- implicit instruction semantics

Certification costs for highest assurance software (EAL6+) exceeds $10,000 per line of code.

The functional abstraction still allows for real applications.

We formally prove that:
- The core ICD functions are correct
- All system components respect data integrity of key values
- The system will always meet real-time deadlines

The platform can be built in real hardware.

Our prototype runs on a Xilinx Artix-7 FPGA, with resources comparable to ordinary embedded CPUs.

Joseph McMahan
Michael Christensen
Lawton Nichols
Jared Roesch
Sung-Yee Guo
Ben Hardekopf
Timothy Sherwood

*University of Washington, Seattle

University of California, Santa Barbara

COMPUTER SCIENCE
UC SANTA BARBARA
Computing, Environmental