SAND2016-4993C

Formal Verification of High-Consequence Controls

Sandia National Laboratories
Rob Armstrong, Geoff Hulette, Jackson Mayo, Karla Morris
Livermore, California 94551

Problem

Nuclear weapons digital controls and critical systems need assurance for safety and security beyond current commercial/academic tools

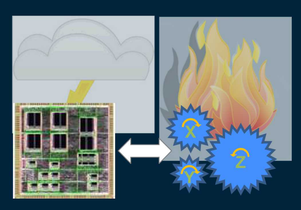
Safety requirements are *always/never* properties:

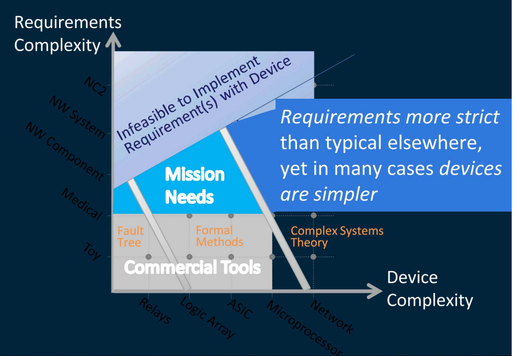
Testing ensures function, cannot ensure the absence of failure

Formal methods can ensure the absence of failure

Mission need exceeds even the usual formal tools

Ensure fail-safe in accident and extreme environments:





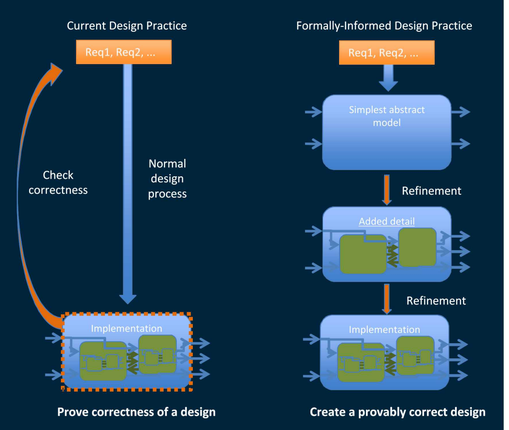
Approach

Formally informed design via abstraction refinement

Abstract model: easy to identify high-level requirements

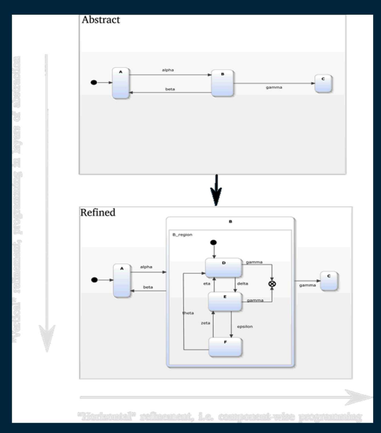
Refined model: closer to what is implementable in silicon

Abstraction/refinement formal methodology ensures safety and security (always/never) requirements from abstract idea through implementation



Domain-specific language based on statecharts: SNLcharts

- Similar to but more systematic than Event-B/iUML-B
- States are refined to encapsulate new states recursively
- Safety properties are formally preserved through refinement by "proof obligations" that must be discharged to complete the design



A variant of this methodology is used to design-in fail-safe modes for high-consequence digital controls

- View extreme environments as either an abstraction or a refinement

Results

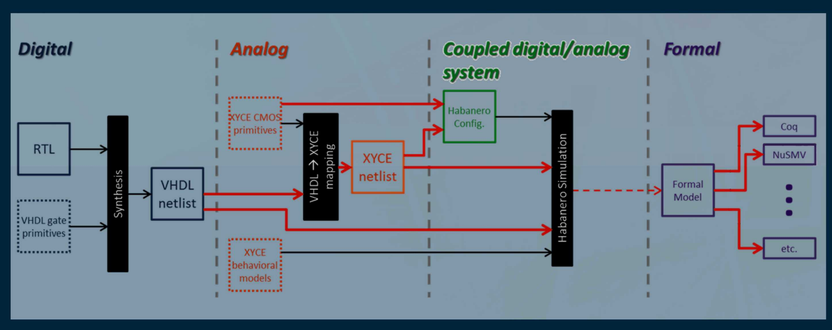
Formal Tool: Developed theory and statechart-like language similar to design methods in common use

Scalability: Tractable formal verification of safety and security even for complex designs

Fail Safe: Design methodology extends to out-of-nominal extreme environments that are otherwise difficult to guarantee for safety and security

Detail: Advancing formal analysis workflows for out-of-nominal electrical behavior of digital devices

- Mixed-signal simulation can reveal the digital imprint of a physical insult (e.g., radiation) on a circuit
- By including these digital upsets in a formal model, can then quantify effect on safety properties



Significance

Addressing needs for high-consequence digital control systems, where conventional design techniques are insufficient

- Provide *evidence* that "always/never" safety and security requirements are actually met by the controls
- Prevent these critical controls from being susceptible to all of the cyber-attacks, subversions, and abuses that conventional digital systems are heir to

This research is creating practical theories, tools, and methodology to ensure that safety and security requirements are met in high-consequence controls

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

SAND 2010-xxxP