Embedded Software Verification Challenges and Solutions

Chao Wang, NEC Labs, Princeton

Shuvendu Lahiri, Microsoft Research, Redmond

Daniel Kroening, Oxford University

ICCAD Tutorial
November 11, 2008

The Speakers

Chao Wang

System Analysis & Verification

NEC Labs America

Shuvendu Lahiri

Software Reliability Group

Microsoft Research

Daniel Kroening

Computing Laboratory

Oxford University

Outline

- What programs?
- Program verification using verification condition generation
- Static Program Analysis
- Predicate Abstraction
- Bounded Model Checking (BMC)

What programs

- Embedded software
  - Avionics, device drivers, ….
- Written in C
  - Uses pointer arithmetic, bitwise operators, arrays, (some) lists
- Set of properties
  - Absence of runtime errors (null dereference, buffer overrun,…)
  - Type state properties (lock api usage)