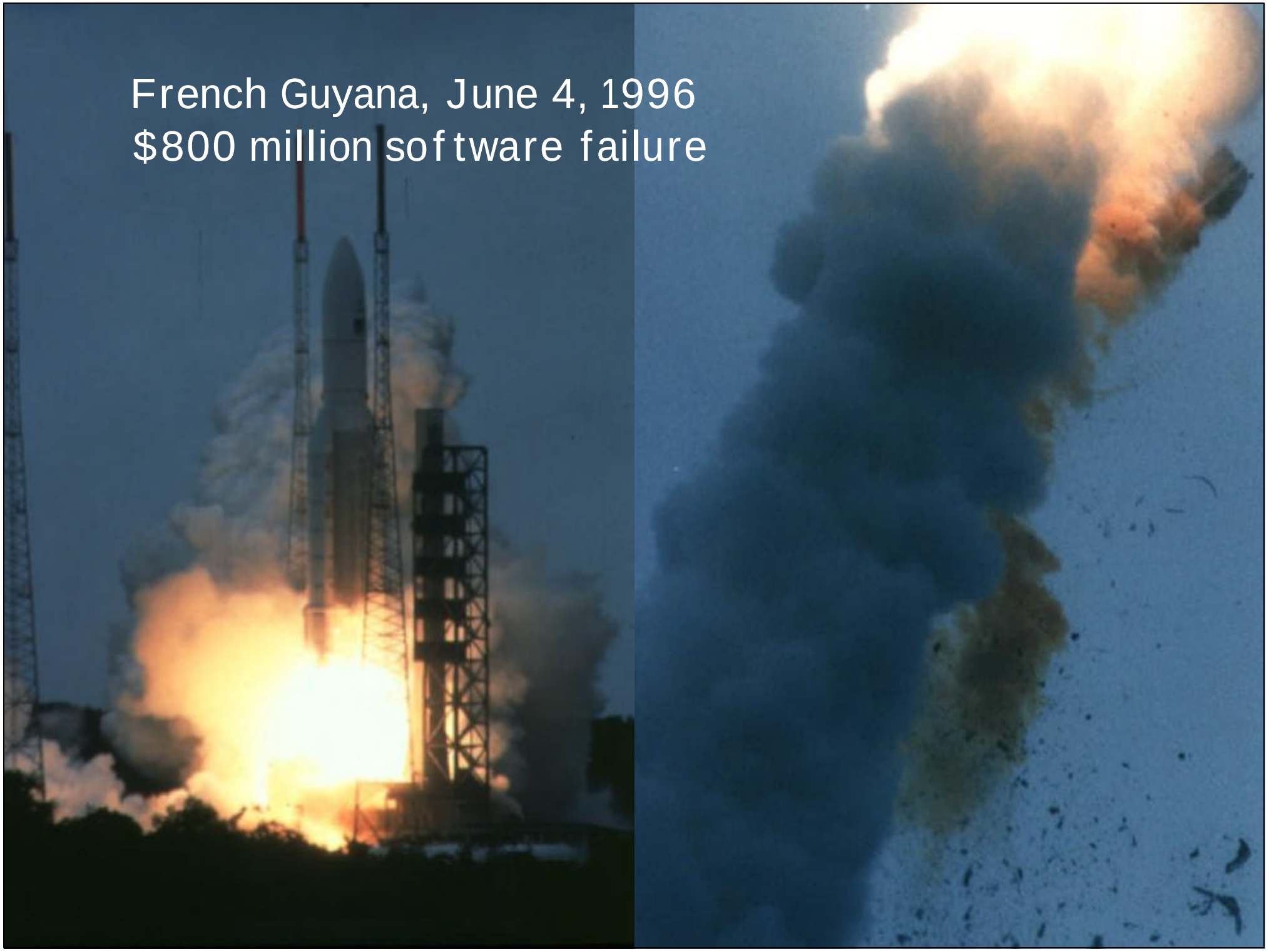
Theory in Practice: Formal Methods for Software & Hardware

Tom Henzinger


French Guyana, June 4, 1996
$800 million software failure

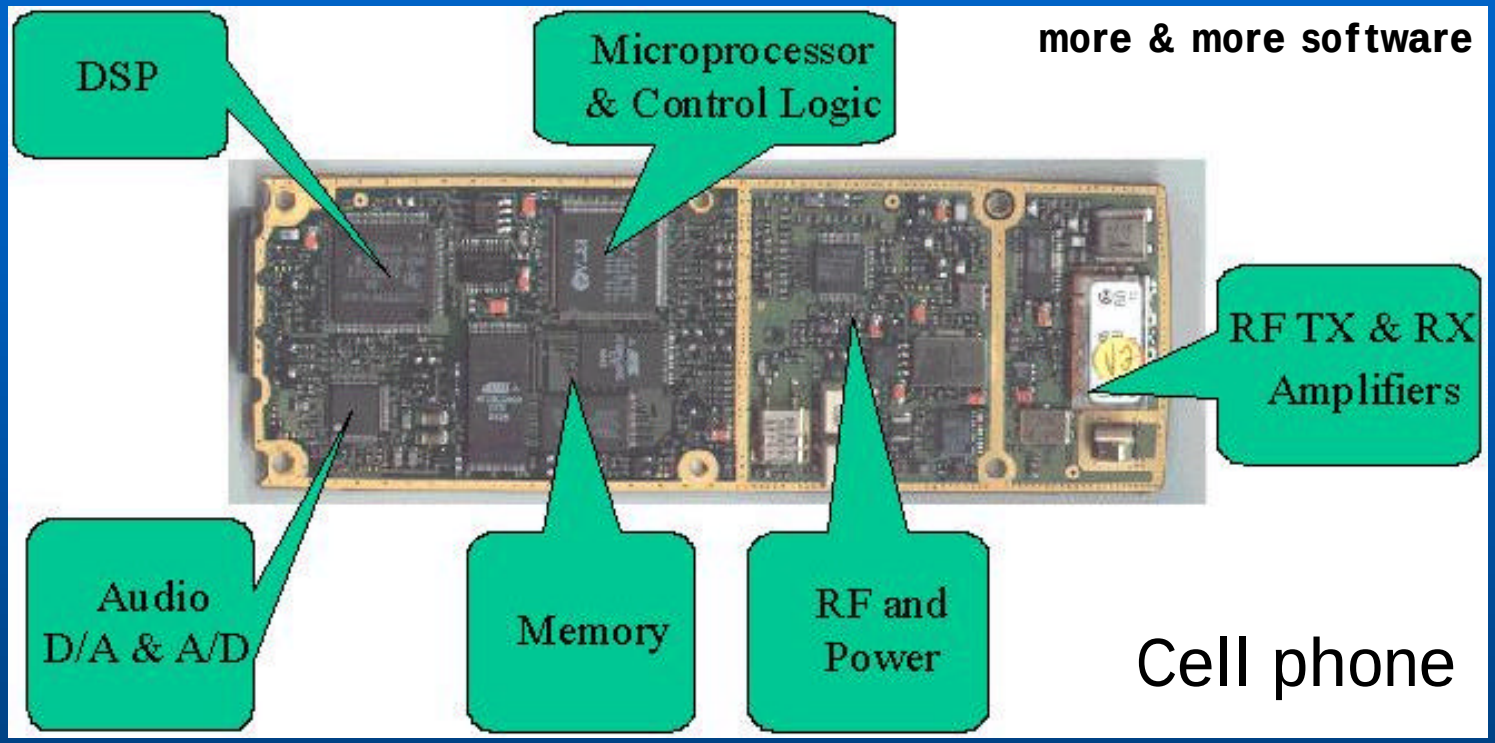

Mars, July 4, 1997
Lost contact due to real-time priority inversion bug

$4 billion development effort

> 50% system integration & validation cost


400 horses
100 microprocessors
M NH 2519

EMBEDDED SYSTEMS



- **REACTIVE:** digital system interacting with environment

  CONCURRENT, often **DISTRIBUTED**

- **HYBRID:** environment is analog (the physical world)

  REAL-TIME, often **MOBILE**

SCIENCE

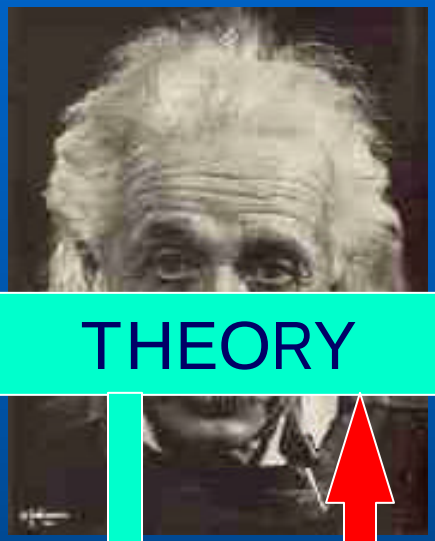
Natural Systems

ENGINEERING

Artificial Systems

PURE

Abstract Systems

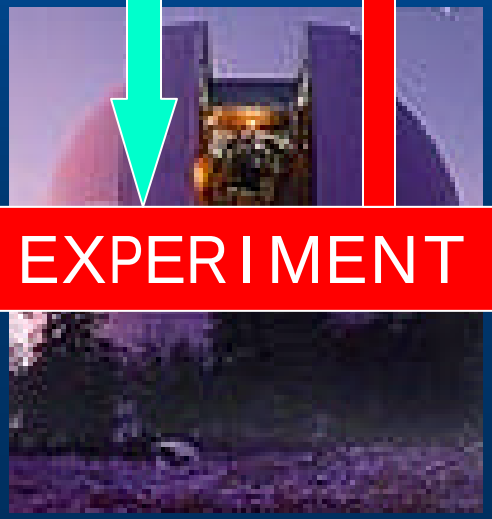


THEORY

Veri/Falsi fication

APPLIED

Concrete Systems



EXPERIMENT

DESIGN

SCIENCE

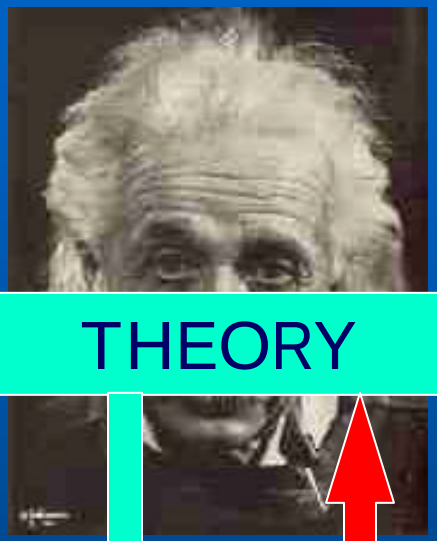
Natural Systems

ENGINEERING

Artificial Systems

PURE

Abstract Systems



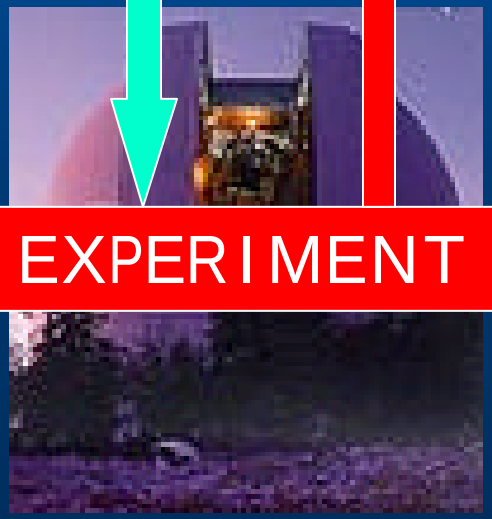
THEORY

ANALYSIS

Veri/Falsi fication

APPLIED

Concrete Systems



EXPERIMENT

DESIGN

DESIGN VERI/FALSIFICATION

- by simulation
- by test

Poor coverage
High recovery cost

DESIGN VERI/FALSIFICATION

- by simulation
- by test

Poor coverage
High recovery cost

- by proof
- by algorithm

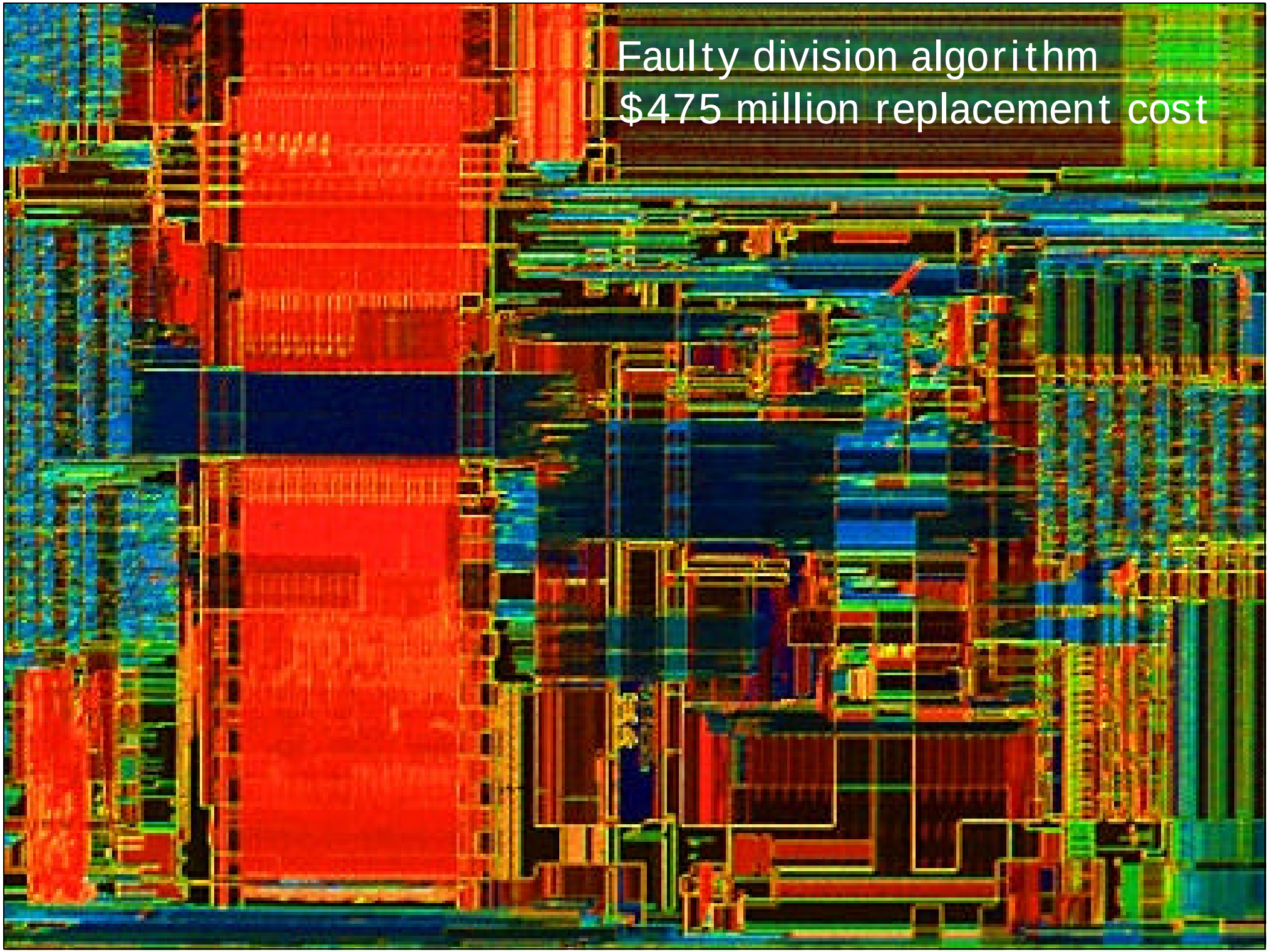
DESIGN VERI/FALSIFICATION

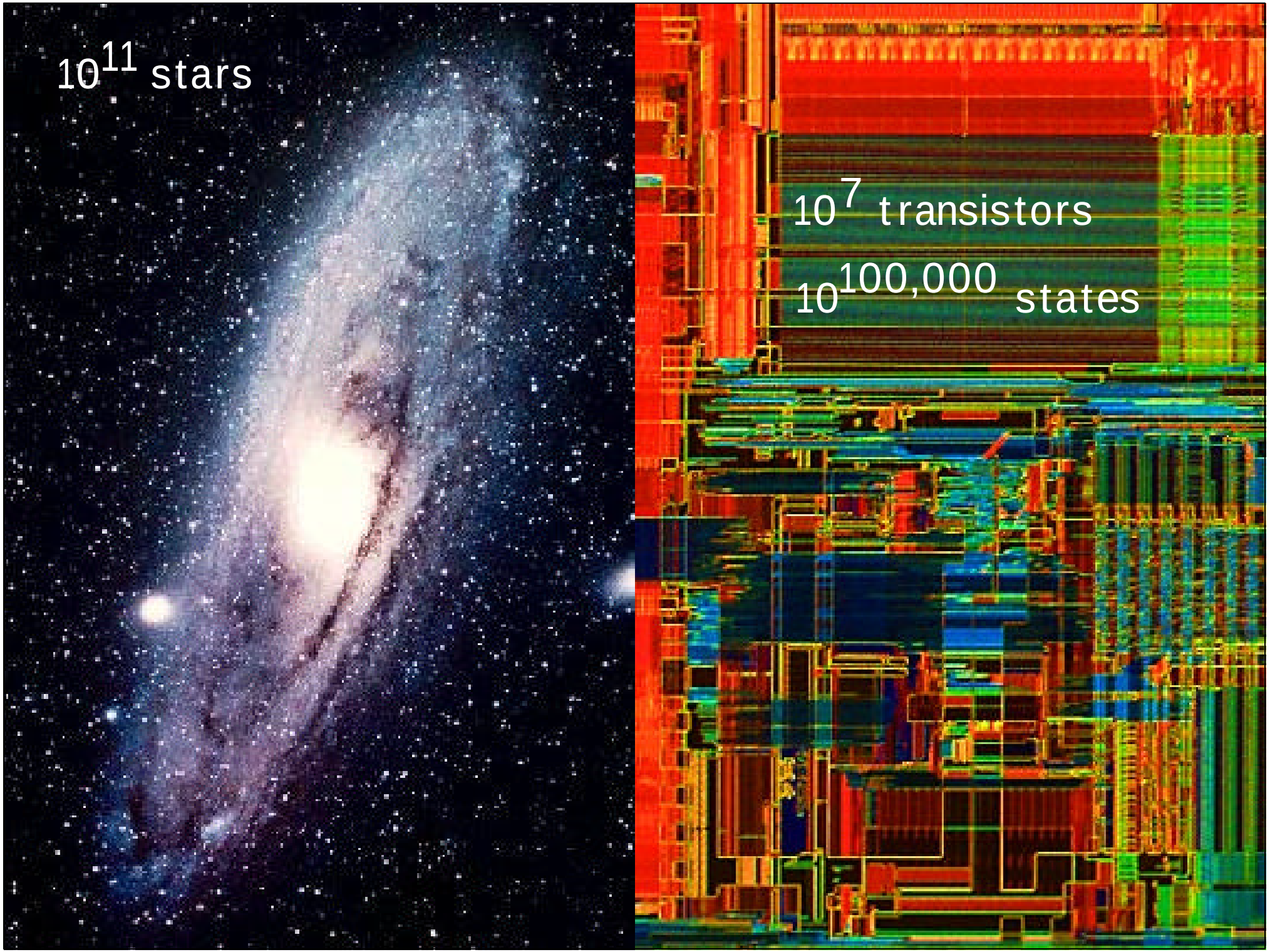
- by simulation
- by test

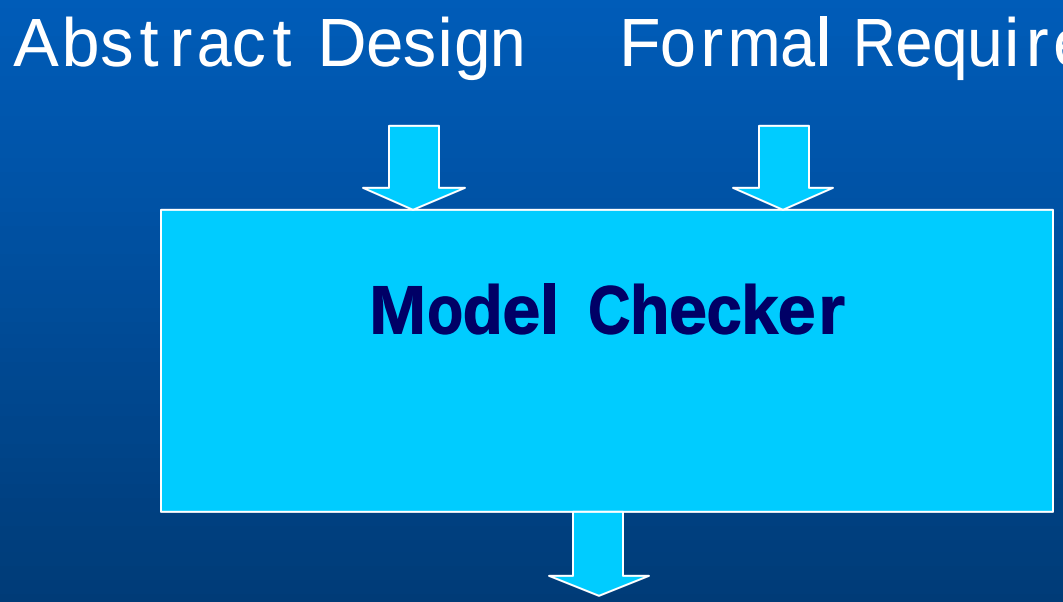
Poor coverage
High recovery cost

- by proof
- by algorithm

"Model Checking"


Faulty division algorithm
$475 million replacement cost

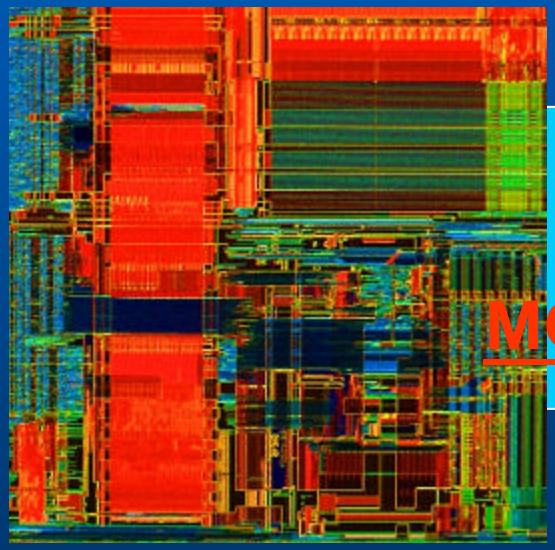

10^{11} stars
10^{7} transistors
$10^{100,000}$ states



- **Design parameters** for which requirements hold
- **Error trace** if requirement is violated

Reactive Systems, e.g. Cache Coherence Protocols

Abstract Design Formal Requirements



Model Checker

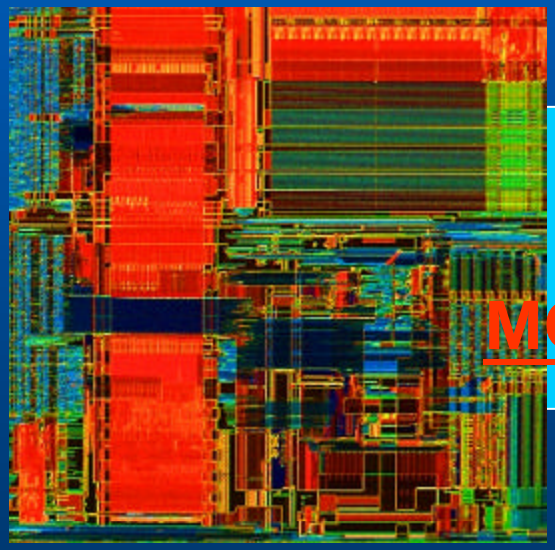
MOCHA

- **Design parameters** for which requirements hold
- **Error trace** if requirement is violated

Reactive Systems, e.g. Cache Coherence Protocols

Hybrid Systems, e.g. Aircraft Landing Gear Control
Automotive Fuel Injection
Air Traffic Control

Abstract Design Formal Requirements



Model Checker

MOCHA **HyTech**

- **Design parameters** for which requirements hold
- **Error trace** if requirement is violated

INTERDISCIPLINARY

CS Theory (Algorithms & Complexity)

Programming Languages (Models & Semantics)

CAD (Design & Validation)

Control Theory (Hybrid Systems)

CURRENT PROJECTS

Verification theory:

- Infinite-state model checking
- Probabilistic model checking
- Game-theoretic methods in model checking

Design Methodology:

- Hierarchical component-based design
- Time-triggered programming (Giotto)

Applications:

- Software (joint NSF ITR project with Aiken and Necula)
- Embedded Control Systems (joint DARPA project with Lee and Sastry)
- Real-time Networks (joint MURI project with Zakhor)
- Hardware (Giga-Scale Research Center)

www.eecs.berkeley.edu/~tah