Open Problems in the formal verification of SPIDER

Lee Pike

Formal Methods Group,
NASA Langley Research Center (NASA LaRC)

Department of Computer Science,
Indiana University, Bloomington

28 April, 2004

Outline

- NASA LaRC Formal Methods Group
- SPIDER Project
- Preliminary Dissertation Ideas

NASA LaRC Formal Methods Group

NASA LaRC Formal Methods Group

- 9 Civil Servants
- 3 National Institute of Aerospace Researchers

NASA LaRC FM Group: Current Research

- Formal methods for embedded systems
- Theorem-prover Databases
- Model checking
- PVS extensions/improvements
- Accident investigation
- Formal analysis of air traffic management
- Standards development for software/hardware development
- Other applications of formal methods

NASA LaRC FM Group: Goals

- Technology Transfer
  - Industry
  - Academic Institutions
  - Government

- Basic Research
- Developing Industry/Government Standards
- Education
- Promoting Formal Methods

The SPIDER Project

SPIDER

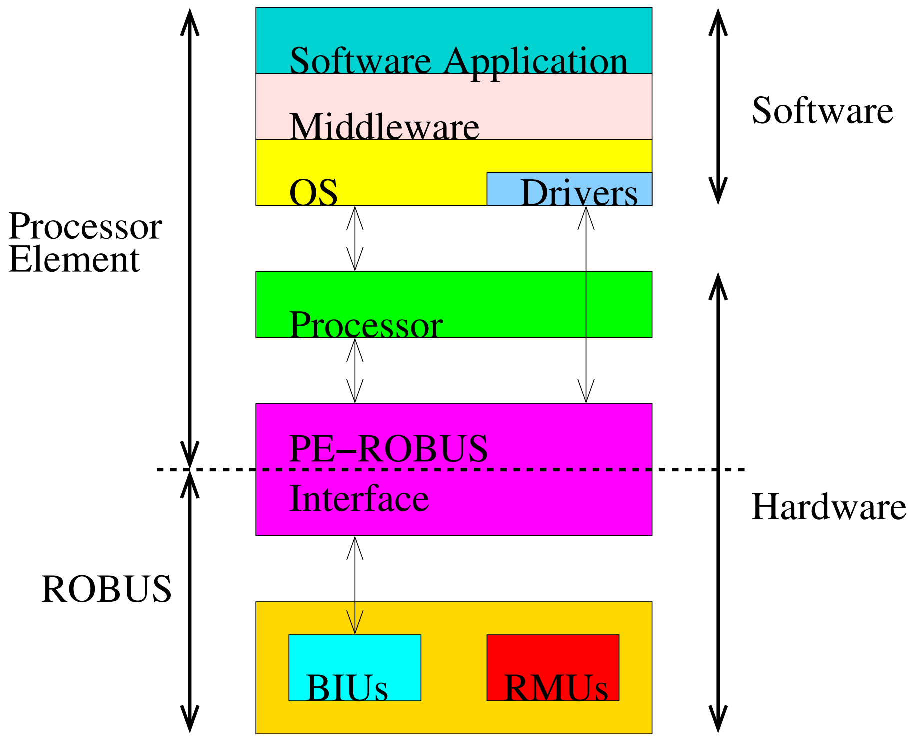
“Time turns the improbable into the inevitable”

—*Unkown*

SPIDER: What?

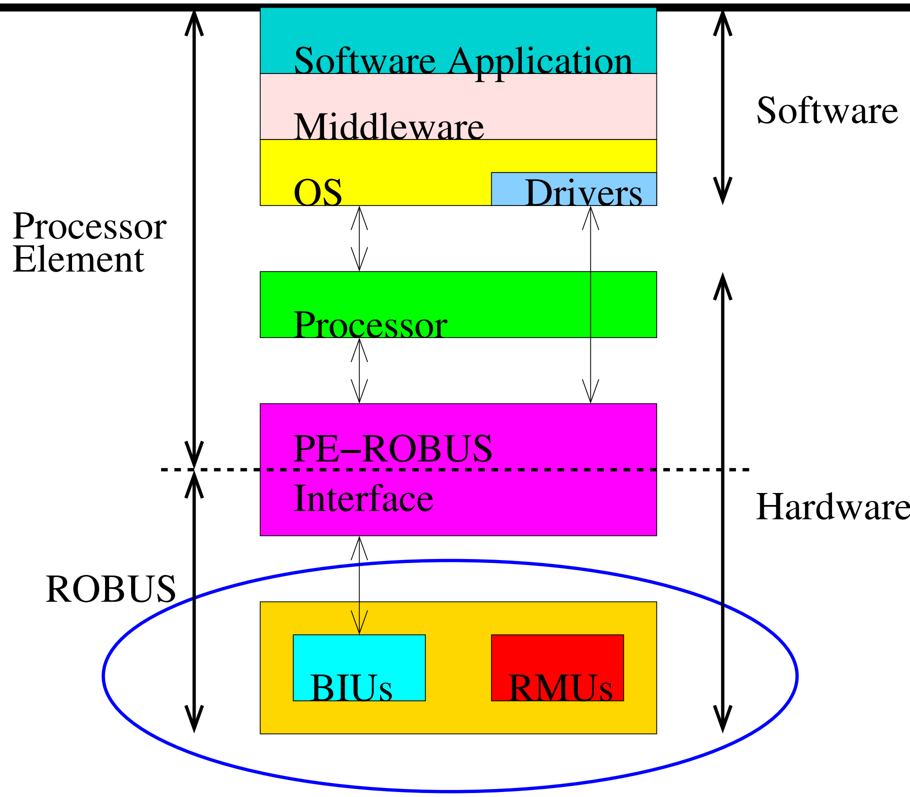
- Synchronized Processor-Independent Design for Electromagnetic Resilience (SPIDER)
- A synchronized, reconfigurable, fault-tolerant communications bus, the Reliable Optical BUS (ROBUS)

SPIDER: What?

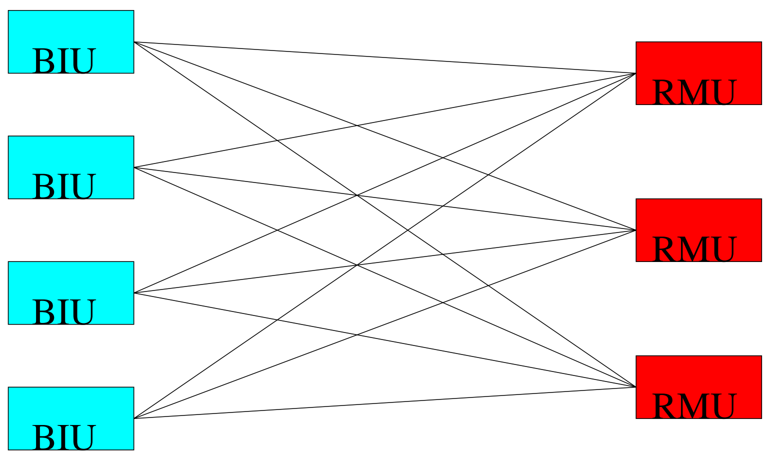


Software Application
Middleware
OS
Drivers
Software
Processor Element
Processor
PE–ROBUS Interface
Hardware
ROBUS
BIUs
RMUs

SPIDER: What?


Software Application
Middleware
OS
Drivers
Software
Processor
Element
Processor
PE–ROBUS
Interface
Hardware
ROBUS
BIUs
RMUs

SPIDER: What?



The ROBUS

Lee Pike
lee.s.pike@nasa.gov

SPIDER: Who?

- Formal methods:
  - Paul Miner (lead)
  - Jeffrey Maddalon
  - Alfons Geser (NIA)
  - Radu Siminiceanu (NIA)
  - Lee Pike

- Engineering:
  - Mahyar Malekpour
  - Wilfredo Torres-Pomales

- Industry Partners:
  - Derivation Systems, Inc.

SPIDER: Who?

- We are a small group:
  - Approx. 2 FTE formal methods
  - Approx. 1.5 FTE engineering

- (TTTech has over 110 FTE employees)

What Distinguishes SPIDER?

- Formal methods integrated into system design.

- A generous maximum fault assumption.

- Sophisticated fault-tolerant protocols.
  - Interactive Consistency
  - Distributed Diagnosis
  - Clock Synchronization
  - Reintegration
  - Start-up/Restart
  - Schedule update

SPIDER: Project Goals

- Develop an ultra-reliable communications bus for use in safety-critical applications such as
  - Federated commercial avionics
  - Space-exploration vehicles
  - Unmanned aerial vehicle communications (UAVs)

- Provide a case-study for FMs in systems development.
  - For FAA guidelines in hardware design assurance.
  - For demonstrating the feasibility & utility for other x-by-wire safety-critical systems.

- Basic research in formal methods, fault-tolerance, distributed systems, and intrusion-tolerance.

SPIDER: Project Goals

- Design a fault-tolerant system for extreme environments:
  - Probability of bus failure $\leq 10^{-10}$ for a 10 hour mission.
  - High malicious fault-arrival rates acceptable.
  - Long mission times/repair intervals feasible.

- Make formal methods understandable to non-experts.
  - Engineers, architects, etc.
  - Certification authorities

lee.s.pike@nasa.gov

SPIDER: Open Problems in FM

Many formal methods, no formal integration

- Theorem proving (PVS)

- Model checking (SMART, etc.)

- Hardware Synthesis (DRS, VHDL)

lee.s.pike@nasa.gov

SPIDER: Open Problems in FM

- Different specifications of the protocols.
  - PVS: Specs compose processes and the environment.
  - SMART/DRS/VHDL: Specs are of individual processes (and all but SMART do not model the environment).

- What good are our formal specs if our engineers and certification authorities cannot decipher them?

lee.s.pike@nasa.gov

Specification Differences

- A process-level behavioral specification:
  - Is how we think about distributed algorithms & protocols (?).
  - Can be decomposed from the environment.
  - Is the initial specification from which an implementation of a single process can be derived.

- A system-level behavioral specification:
  - Allows for simple & transparent proof methods, especially in a theorem-prover.
  - Is the natural model for reasoning about global environmental assumptions.