Foundations of Hybrid and Embedded Software and Systems: Project Overview

Program Review
May 10th, 2004
Berkeley, CA

UC Berkeley: Chess
Vanderbilt University: ISIS
University of Memphis: MSI

Foundations of Hybrid and Embedded Software Systems

NSF-ITR Investigators

Ruzena Bajcsy, Ras Bodik, Bella Bollobas, Gautam Biswas, Tom Henzinger, Kenneth Frampton, Gabor Karsai, Kurt Keutzer, Edward Lee, George Necula, Alberto Sangiovanni Vincentelli, Shankar Sastry, Janos Sztipanovits, Pravin Varaiya.

ITR-Center Mission

- The goal of the ITR is to provide an environment for graduate research on the design issues necessary for supporting next-generation embedded software systems.
  - The research focus is on developing model-based and tool-supported design methodologies for real-time fault-tolerant software on heterogeneous distributed platforms.
- The Center maintains a close interaction between academic research and industrial experience.
  - A main objective is to facilitate the creation and transfer of modern, "new economy" software technology methods and tools to "old economy" market sectors in which embedded software plays an increasingly central role, such as aerospace, automotive, and consumer electronics.

Chess

Mission of Chess

To provide an environment for graduate research on the design issues necessary for supporting next-generation embedded software systems.

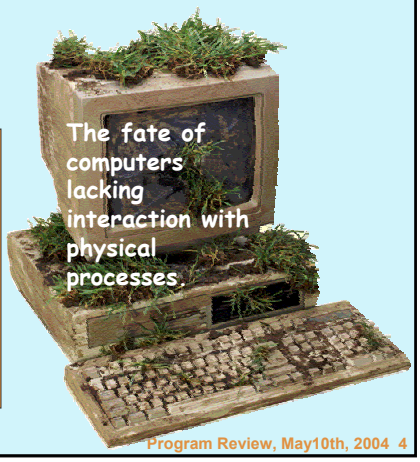
- Model-based design
- Tool-supported methodologies

For

- Real-time
- Fault-tolerant
- Robust
- Secure
- Heterogeneous
- Distributed

Software

We are on the line to create a "new systems science" that is at once computational and physical.



Chess

Embedded Software: Problem for Whom?

- *DoD (from avionics to micro-robots)*
  - *Essential source of superiority*
  - *Largest, most complex systems*
- *Automotive (drive-by-wire)*
  - *Key competitive element in the future*
  - *Increasing interest but low risk taking*
- *Consumer Electronics (from mobile phones to TVs)*
  - *Problem is generally simpler*
  - *US industry is strongly challenged*
- *Plant Automation Systems*
  - *Conservative solutions to date*
  - *Emerging importance of SCADA/DCS in Critical Infrastructure Protection*

chess

Key Properties of Hybrid & Embedded Software Systems

- **Computational systems**
  - **but not first-and-foremost a computer**
- **Integral with physical processes**
  - **sensors, actuators**
- **Reactive**
  - **at the speed of the environment**
- **Heterogeneous**
  - **hardware/software, mixed architectures**
- **Networked**
  - **adaptive software, shared data, resource discovery**
  - **Ubiquitous and pervasive computing devices**

chess

Project Approach

- Model-Based Design (the view from above)
  - principled frameworks for design
  - merging specification, modeling, and design
  - manipulable (mathematical) models
  - enabling analysis and verification
  - enabling effective synthesis of implementations
- Platform-Based Design (the view from below)
  - exposing key resource limitations
  - hiding inessential implementation details
- Tools
  - concrete realizations of design methods

Foundational Research

- The science of computation has systematically abstracted away the physical world. The science of physical systems has systematically ignored computational limitations. Embedded software systems, however, engage the physical world in a computational manner.
- We believe that it is time to construct an Integrated Systems Science (ISS) that is simultaneously computational and physical. Time, concurrency, robustness, continuums, and resource management must be remarried to computation.
- Mathematical foundation: **Hybrid Systems Theory: Modern Integrated Systems Science.**

… and Embedded Software Research

- Models and Tools:
  - Model-based design (platforms, interfaces, meta-models, virtual machines, abstract syntax and semantics, etc.)
  - Tool-supported design (simulation, verification, code generation, inter-operability, etc.)
- Applications:
  - Flight control systems
  - Automotive electronics
  - National experimental embedded software platform
- From resource-driven to requirements-driven embedded software development.

Chess

Some Current Research Focus Areas

- Software architectures for actor-oriented design
- Interface theories for component-based design
- Virtual machines for embedded software
- Semantic models for time and concurrency
- Design transformation technology (code generation)
- Visual syntaxes for design
- Model checking hybrid systems
- Autonomous helicopters
- Automotive systems design

- Mobies
- SEC
- Fresco
- Ptolemy
- HyVisual
- Metropolis
- BEAR
- MESCAL

Chess

"Center" Organization

- Funding Sources
  - Large NSF ITR
  - Other federal (NSF, DARPA, MURI, etc.)
  - Industrial (Participating Member Companies): IT and applications (automotive, aerospace, consumer electronics)
- Outreach
  - Curriculum development
  - Community colleges (EECS 20)
  - SUPERB program
  - SIPHER program
- National Experimental Platform for Hybrid and Embedded Systems and Software NEPHEST
- Embedded Software Consortium for Hybrid and Embedded Systems (ESCHER)

NSF ITR Organization

- **PI:** Shankar Sastry
- **coPIs:** Tom Henzinger, Edward Lee, Alberto Sangiovanni-Vincentelli, Janos Sztipanovits
- **Participating Institutions:** UCB, Vanderbilt, Memphis State
- **Five Thrusts:**
  - Hybrid Systems Theory (Henzinger)
  - Model-Based Design (Sztipanovits)
  - Tool-Supported Architectures (Lee)
  - Applications: automotive (ASV), aerospace (Sastry)
  - Education and Outreach (Karsai, Lee, Varaiya)
- **Five year project: kick-off meeting November 14th , 2002. First Review May 8th, 2003, Second Review Dec 3rd, 2003.**
  - Weekly seminar series
  - Ptolemy workshop May 9th, 2003
  - NEST + CHESS Workshop May 9th, 2003

Thrust 1 Hybrid Systems

- **Deep Compositionality**
  - Assume Guarantee Reasoning for Hybrid Systems
  - Practical Hybrid System Modeling Language
  - Interface Theory for hybrid components
- **Robust Hybrid Systems**
  - Bundle Properties for hybrid systems
  - Topologies for hybrid systems
  - Stochastic hybrid systems
- **Computational hybrid systems**
  - Approximation techniques for H-J equations
  - Synthesis of safe and live controllers for hybrid systems
- **Phase Transitions**

Thrust II: Model Based Design

- **Composition of Domain Specific Modeling Languages**
  - Meta Modeling
  - Components to manipulate meta-models
  - Integration of meta-modeling with hybrid systems
- **Model Synthesis Using Design Patterns**
  - Pattern Based Modal Synthesis
  - Models of Computation
  - Design Constraints and Patterns for MMOC
- **Model Transformation**
  - Meta Generators
  - Scalable Models
  - Construction of Embeddable Generators

Thrust III:Advanced Tool Architectures

- Syntax and Synthesis
  - Semantic Composition
  - Visual Concrete Syntaxes
  - Modal Models
- Interface Theories
- Virtual Machine Architectures
- Components for Embedded Systems

Thrust IV: Applications

- Embedded Control Systems
  - Avionics
  - Veitronics
  - Wireless Embedded Systems
- Embedded Systems for National/Homeland Security
  - Air Traffic Control
  - UAVs/UGVs
- Networks of Distributed Sensors
- Hybrid Models in Structural Engineering
  - Active Noise Control
  - Vibration damping of complex structures

Thrust V: Education and Outreach

- **Curriculum Development for MSS**
  - Lower Division
  - Upper Division
  - Graduate Courses
- **Undergrad Course Insertion and Transfer**
  - Goals and ABET requirement
  - New courses for partner institutions (workshop held March 1st 2003)
  - Introduction of new courses (will be replacing control course at upper division level by embedded software course)
  - New elective courses
  - Expansion of SUPERB program (6 + 4 students in Summer 03)
- **Summer Internship Program in Embedded Software Research (SIPHER)**

Outreach Continued

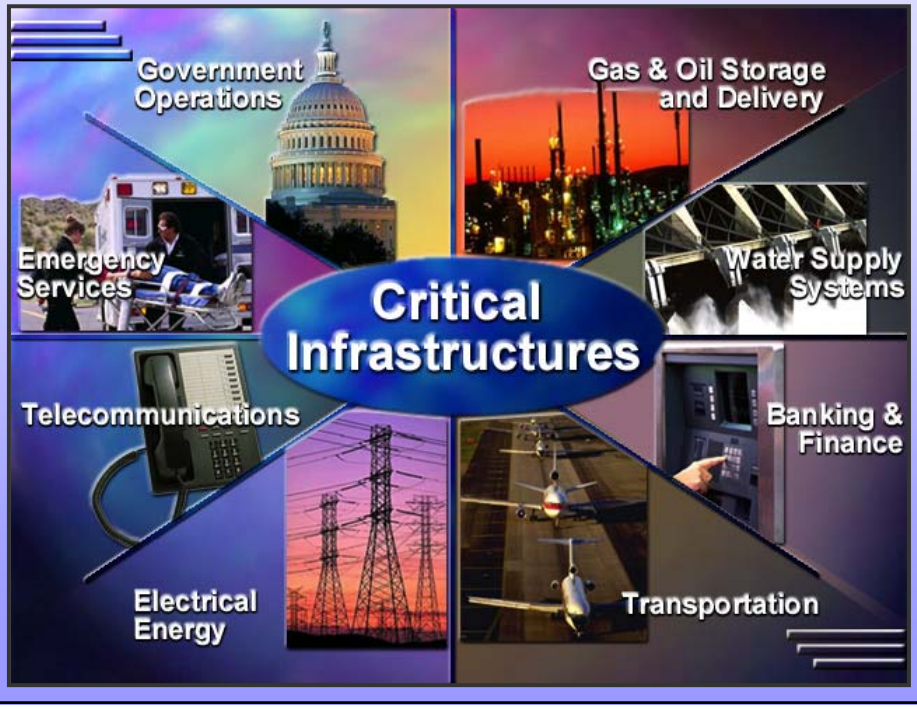
- **Interaction with EU-IST programs**
  - Columbus (with Cambridge, l'Aquila, Rome, Patras, INRIA)
  - Hybridge (with Cambridge, Patras, NLR, Eurocontrol, Brescia, KTH)
  - ARTISTE: Educational Initiatives (Grenoble, INRIA, ETH-Zurich)
- **Foundation of non-profit ESCHER**
  - Interaction with F-22/JSF designs
  - Secure Networked Embedded Systems

Emerging Research Area: Embedded Systems for Homeland Security

Technology needs were classified into areas:

- Information Assurance and Survivability
- Security with Privacy
- Secure Network Embedded Systems (SENSE)
- Validated Hybrid Systems models for interdependencies of infrastructures
- Public Private Partnerships for Technology Transition

chess



Secure SCADA and beyond

We think that there is a great deal to be done in terms of operationalizing secure versions of SCADA (Supervisory Control And Data Acquisition) and DCS (Digital Control Systems) for the infrastructures considered, especially power, natural gas, chemical and process control, etc. However, the sense was that this infrastructure was going to be gradually replaced by networked embedded devices (possibly wireless) as computing and communication devices become more ubiquitous and prevalent. Thus, the major research recommendations were for an area that we named Secure Networked Embedded Systems (SENSE).

SCADA of the Future

- Current SCADA
  - Closed systems, limited coordination, unprotected cyber-infrastructure
  - Local, limited adaptation (parametric), manual control
  - Static, centralized structure
- Future requirements
  - Decentralized, secure open systems (peer-to-peer, mutable hierarchies of operation)
  - Direct support for coordinated control, authority restriction
  - Trusted, automated reconfiguration
    - Isolate drop-outs, limit cascading failure, manage regions under attack
    - Enable re-entry upon recovery to normal operation
    - Coordinate degraded, recovery modes
  - Diagnosis, mitigation of combined physical, cyber attack
  - Advanced SCADA for productivity, market stability, manageability

Secure Network Embedded Systems

Embedded Software prevalent in all critical infrastructures. Critical to high confidence embedded software are open source techniques for

- Automated Design, Verification and Validation
  - Verified design in a formal, mathematical sense
  - Validated design in an engineering sense
  - Certifiable design to allow for regulatory and certification input
- High Confidence Systems
  - Narrow waisted middleware
    - Trusted abstractions, limited interfaces
    - Algorithms and protocols for secure, distributed coordination and control
  - Security and composable operating systems
  - Tamper Proof Software
- Generative Programming
- Intelligent Microsystems: infrastructure of the future with security codesign with hardware and software.

Layers of Secure Network Embedded Systems

- Physical Layer
  - Attacks: jamming, tampering
  - Defenses: spread spectrum, priority messages, lower duty cycle, region mapping, mode change, tamper proofing, hiding.
- Link Layer
  - Attacks: collision, exhaustion, unfairness
  - Defenses: error correcting code, rate limitation, small frames

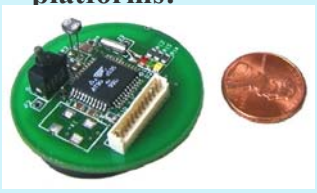
Layers of Secure Network Embedded Systems

- Network and Routing Layer
  - Attacks: neglect and greed, homing, misdirection, black holes
  - Defenses: redundancy, probing, encryption, egress filtering, authorization, monitoring, authorization, monitoring, redundancy
- Transport Layer
  - Attacks: flooding, desynchronization
  - Defenses: client puzzles, authentication
- Embedded System/Application Layer
  - Attacks: insider misuse, unprotected operations, resource overload attacks, distributed service disruption
  - Defenses: authority management (operator authentication, role-based control authorization), secure resource management, secure application distribution services

chess

Foundations: Smart Dust and Motes

Berkeley experimental platforms:



- Atmel ATMEGA103
  - 4 Mhz 8-bit CPU
  - 128KB Instruction Memory
  - 4KB RAM
- 4 Mbit flash (AT45DB041B)
  - SPI interface, 1-4 uj/bit r/w
- RFM TR1000 radio
  - 50 kb/s
  - Sense and control of signal strength
- Network programmable in place
- Multihop routing, multicast
- Sub-microsecond RF node-to-node synchronization
- Provides unique serial ID's
- Sensor board: acoustic and magnetic sensors

chess

Modeling: Research Needs

- New Modeling and Simulation Tools for Hybrid Systems. CIP systems involve multiple models of computation (discrete, continuous, logical, differential equations) and many hierarchical levels and granularities. Simulators for such systems need to be made numerically robust and probabilistically accurate.
- Tools for the assessment of level of risk. Risk assessment for determination of deployment of fixed budget to most critical areas.
- Development of simulation test-beds for red-teaming exercises, interdependency evaluation, response preparation and assessment.