

Advanced Tool Integration for Embedded Systems Assurance (HASTEN)

Rajeev Alur (UPenn)
Carl A. Gunter (UPenn)
Sampath Kannan (UPenn)
Insup Lee (PI, UPenn)
Oleg Sokolsky (UPenn)

Robert P. Cook (GSU)
Elsa Gunter (NJIT)
Kang G. Shin (UMich)

Personnel

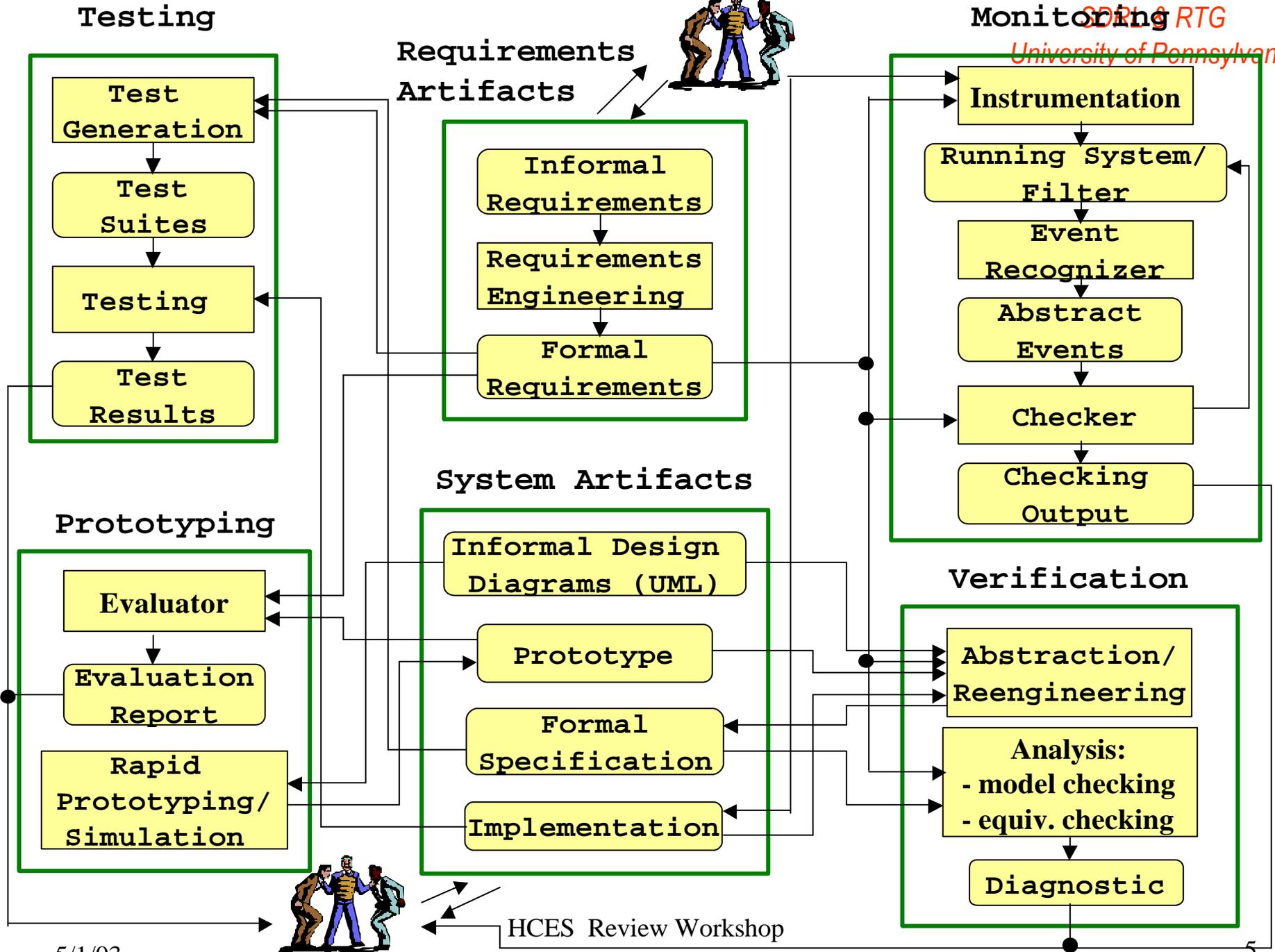
- PI's: Rajeev Alur, Robert P. Cook, Carl Gunter, Elsa Gunter, Sampath Kannan , Insup Lee, Kang G. Shin, Oleg Sokolsky
- Graduate students: , Alwyn Goodloe, Yerang Hur, Michael McDougall, Wonhong Nam, Usa Sammapun, Zonghua Gu, Sharath Kodase, Yi Meng
- Tech Staff: David Arney
- Postdoctoral fellows: Tugkan Batu, Hyung-Seok Hong, Madhu Parthasarathy, Li Tan

Embedded Systems

- Difficulties
 - Increasing complexity
 - Decentralized
 - Safety critical
 - Resource constrained
- Properties of embedded systems
 - Adherence to safety-critical properties
 - Meeting timing constraints
 - Satisfaction of resource constraints
 - Supporting fault tolerance
 - Domain specific requirements
- Development of reliable and robust embedded software

Goals of the HASTEN Project

- High Assurance Systems Tools and ENvironments (HASTEN)
- Develop techniques and tools for “end-to-end” software engineering of embedded systems
 - Requirements capture
 - Specification, analysis, simulation
 - Implementation generation and validation: code generation, testing
 - Deployed system monitoring, checking, and steering
- Integrated use of tools
 - Vertical integration (reuse models)
 - Horizontal integration (layered modeling and analysis)
- Case studies
 - automotive controllers, mobile robots, medical devices, real-time Java, embedded Linux



Poster Session

- Translating informal requirements to formal models: two case studies, Dave Arney, UPenn
- The Linux Kernel Verification Project (LV), Bob Cook, Georgia Southern University
- OpEm: Open APIs for Embedded Systems, Alwyn Goodloe, UPenn
- Requirements Management System, Elsa L. Gunter, NJIT
- End-to-end design and analysis of embedded real-time systems, Zonghua Gu and Kang G. Shin, University of Michigan
- Specification-based test generation for hybrid systems using CHARON, Hyoung-Seok Hong, UPenn
- Counter-example guided predicate abstraction of hybrid systems, Franjo Ivancic, UPenn
- Model-based code generation for hybrid systems, Jesung Kim, UPenn
- BDD-based and SAT-based approaches to solving games, P. Madhusudan and Wonhong Nam, UPenn
- Run-time Monitoring, Checking, and Steering, Usa Sammapun, UPenn
- Property-based test generation, Li Tan, UPenn

Talks

- Sampath Kannan, Mining for Patterns and Anomalies in Data Streams (25 mins)
- Kang Shin, End-to-end design of embedded real-time systems (20 mins)
- Elsa Gunter, Challenges of LTL Specification of CARA (20 mins)
- Insup Lee, Test Generation from Specifications (15 mins)