Theme: Composition of System Properties

John Rushby

Computer Science Laboratory
SRI International
Menlo Park CA USA

System Properties

- Properties like safety, security, real-time guarantees
- These are properties of the whole system
  - e.g., no single component makes an airplane safe
  - Though a single component can easily make it unsafe

  i.e., these are emergent properties
- That's why the FAA certifies only airplanes and engines
  - Components certified only as part of an airplane or engine
  - Because you need to examine them in their context of interaction

  i.e., certify only closed systems
- But this is becoming ruinously expensive, even infeasible
- The interest now is in open systems

Composition of System Properties

- New goal is assurance of system properties when systems are built by composition
  - Take a "safe" system and modify it
  - Join two "safe" systems together
- Seems like an oxymoron
  - System properties
  - But system built from parts
  - Whole system is not examined

Composing System Properties

- Limit unintended interaction
  - Strong protection properties of OS, network etc.
  - And strongly assured

  Powell, Suri, Muller, Iyer, Kopetz, Heiser, Aoki, Nakajima
- Ensure intended interaction
  - Previously, put system together, then analyze
  - Now, analyze as pieces are added, or at runtime

  Tokoro, Takai Yokote, Kuramitsu, Ishikawa, Nakazawa
- cf. "Just-in-time Certification" (ICECCS 2007), "Runtime Certification" (RV08), "Formalism in Safety Cases" (SSS10)
- Current NASA projects in IVHM:

  Monitor properties from Assurance Case

  http://www.csl.sri.com/~rushby/abstracts/csl-09-02
- Service Oriented Architecture, Proof Carrying Code, MILS

Challenges: Medical Device Plug'n'Play

- IV blood pressure sensor and bed height correction
- Heart-lung machine and imaging
- Anaesthesia and laser throat surgery

Future systems will take more responsibility for preservation and construction of system properties