Model-Based Embedded Software Development

HCES 2003 Kickoff Presentation

Paul L. Jones, U.S. FDA
Center for Devices and Radiological Health

Presentation based on HCES 2002 Focus Group presentation:

Rajeev Alur (Penn)
Bob Cook (Georgia Southern)
Paul Jones (FDA)
Daniel Kroening (CMU)
Luqi (NPS)
Frank Sledge (NCO)
Scott Smolka (Stony Brook)
Steve Van Albert (WRAIR)

Purpose of This Talk

- Recap last year's workshop (from the perspective of one of the focus groups).
- Kickoff 2nd day of this year's workshop:
  - *develop roadmap for future HCES research*
- Provide FDA (/CDRH/OST) perspective on embedded software development.

Vision for the Future

- Embedded Software Development as a true *engineering* discipline.
- How: Model-based design, analysis, and implementation.
- Formal specification and verification seamlessly integrated into process.
- Model: EDA -- $4bn/yr industry.

Tool Set of the Future

- Requirements
  - Capture and analysis tool
  - Environment (user model etc.)
- Modeling
- Simulation with user interaction, prototyping
- Verification
- Code Generation
- Testing including automatic test generation
- Evolution and Documentation

Tool Set Characteristics

- Traceability
- Formal semantics
- Certifiability (by law or by competition)
- High-confidence accountability
- Usability
- Measurability

Technology Assessment

- Medical device industry process same as fifty years ago.
- Software development technology has kept pace in terms of functionality but not in terms of *ilities*: reliability, security, performance, power, mem. footprint, etc.
- Hardware has separable requirements; EDA an engineering discipline.

Technology Transfer

- Standardization process needed.
- Product Flow:
  - academic (proof of feasibility)
  - open source
  - private sector adds value to productize

Why Fund At All?

- If we don’t fund it, many more people will be injured or die.
- Huge number of embedded applications and huge financial implications.
- Every year, 98% of 5.7bn new processors deployed in embedded applications. Embedded in quality of life.

FDA Interest in HCES

Current devices

- many of today's devices contain ES
  - choclear implants, eximer lasers, infusion pumps, etc

Future devices

- biomedical, MEMS, telemedicine, home use

FDA Software Reviews

Present review process

- Quality system process oriented
  - Rely on Regulations
  - Rely on Standards
- Review life cycle artifacts
  - Emphasis on risk mgmt & effectiveness

High Confidence is not an inherent property of this process!!

FDA Software Reviews

Future reviews

- Software will be certified by mfr to “some” property(s);
  e.g. correctness, usage reliability
- Proactive review by FDA before mfr invests in an unapproveable design

Generalized Infusion Pump Project

Research areas :

NOTE – this is not CARA

- Capturing requirements
  (from diverse domain experts)
- Open system development
- Certifications methods for a regulatory environment

*** Can publish results