Design Process

18-849b Dependable Embedded Systems

Kanaka Juvva

04/06/99

Required Reading: On Hierarchical Design of Computer Systems for Critical Applications, Peter Gabriel Neumann

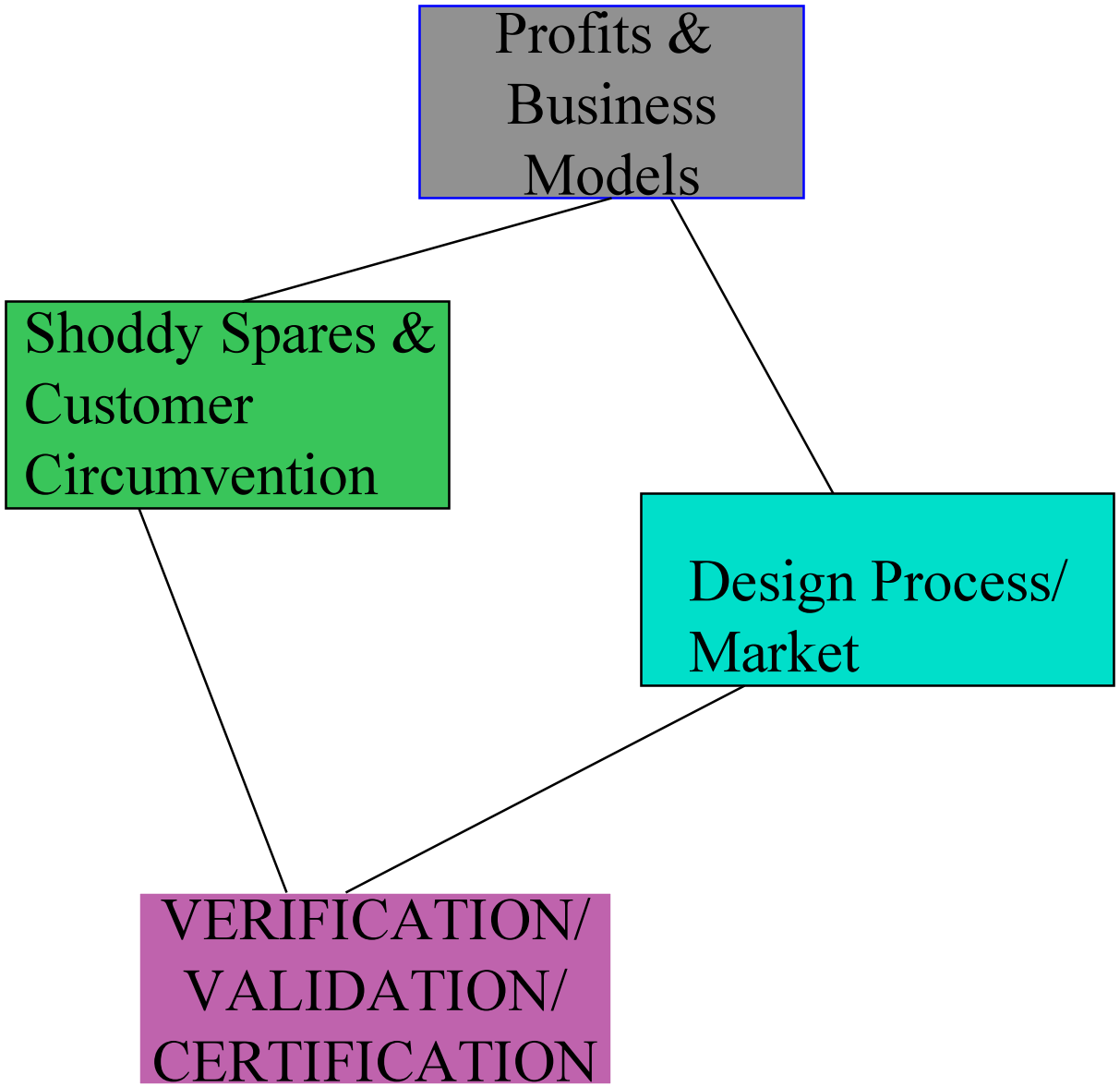
Books: Real-Time Systems Design Principles for Distributed Embedded Applications, Herman Kopetz

Carnegie Mellon

Overview: Design Process

- **Introduction**
- **Key concepts**
  - Computer design
  - System-level design
  - Life-cycle support
  - Business model support
- **Tools / techniques / metrics**
  - CAD Tools
  - Hardware/Software Codesign
- **Relationship to other topics**
  - Verification / Validation / Certification
  - Profits & Business Models
- **Conclusions & future work**

YOU ARE HERE MAP



Design Process

- **Embedded System design is about the system and not about the computer**
- **~3 billion embedded CPUs are sold each year**
- **Embedded systems are diversified**
  - eg. Signal Processing, Mission Critical Control System
- **Embedded computer design is different from desktop computer design**
  - Life-cycle and business driven factors are important rather than just throughput
  - Cost may matter more than speed
- **Perhaps there is no single design method which spans all types of embedded systems**

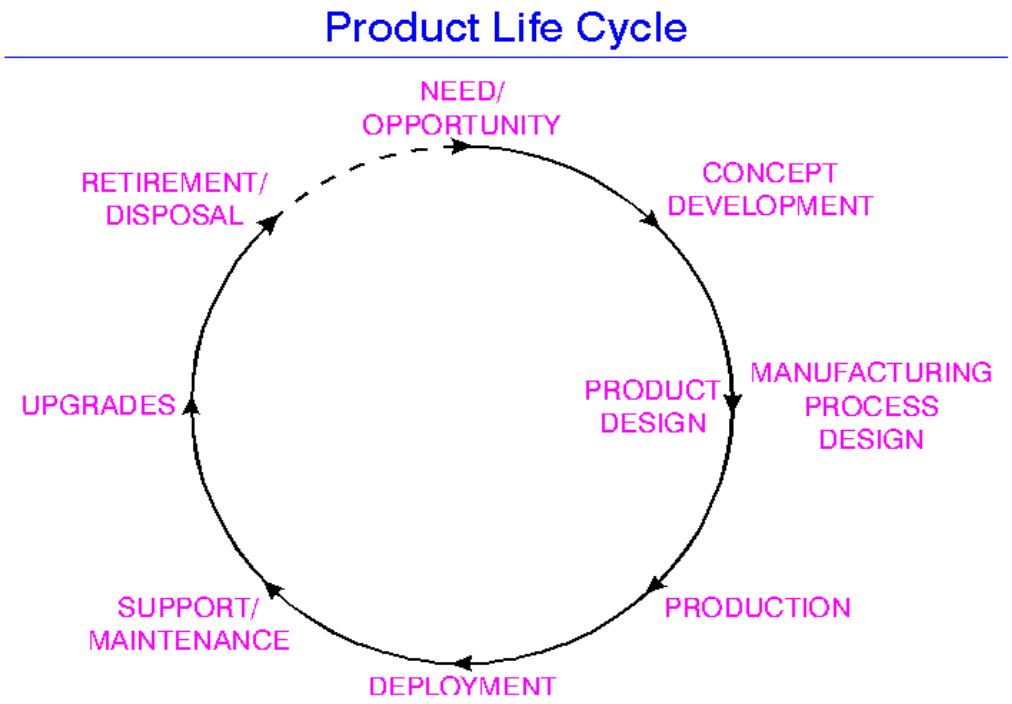
Computer Design Requirements

- **Real time/reactive operations**
  - Worst case performance often limits design
  - Accurate performance prediction before system is built
- **Small size, low weight**
  - Embedded computers are embedded in something
  - Weight may be critical
- **Low power, limited cooling**
- **Safe and reliable**
  - Realistic reliability predictions with commercial component
  - Low-cost reliability -- without brute force redundancy
- **Moderate to extreme cost sensitivity**
  - Variable "cushion factor" to handle different requirements for cost vs. product robustness with same component database

System Level Design

- **End-product utility is the goal**
  - Products sold on the basis of price & features
  - Feature-list wars
  - Fad technologies (e.g., fuzzy logic rice cookers)
  - Seldom which CPU is in the system
- **System safety & reliability**
  - Mission-critical systems use redundancy
  - The software problem -- software can invite complexity; complexity invites problems
- **Power management**
  - Power is often limited due to heat or power storage capacity

Life-Cycle Issues



- **Long product life/low cost can emphasize life-cycle issues**
- **Life-cycle optimization should include trading design costs vs. other costs**
  - Cost of CAD tools
  - Cost of manpower
  - Cost of prototyping

Tools / Techniques

- **CAD Tools**
  - Used in almost all phases of life-cycle
- **Hardware/Software Codesign**
  - Merges computer design and system design phases
  - Research stage and slowly catching up

Relationship To Other Topic Areas

- **Verification/Validation/Certification**
  - An important phase of life-cycle
  - Any design change may require safety recertification or regression testing
  - Major changes may require other certification for EMI or reliability
- **Business Models**
  - Design vs. fabrication cost
  - Cycle time (time to market)
  - Product families
  - Database & component library maintenance

Conclusions & Future Work

- **Embedded System design involves many issues**
- **Turnaround time / time to market**
- **Design qualification/certification**
- **Life-cycle support & configuration management**
- **FPGA in future**
- **Standard components (HW&SW) as building blocks**
  - composition instead of synthesis

On Hierarchical Design of Computer Systems for Critical Applications

- **"One design approach of particular interest here involves the structuring of a critical system into design layers such that flaws in, or misuse of, the higher-level layers cannot contaminate the lower layers"**
- **Hierarchical decomposition for downward-only dependencies**
  - Security
  - Privacy
  - Fault-tolerance
- **Levels of Hierarchy**
  - Most-critical functions
  - Somewhat-critical
  - Noncritical