Multi-Disciplinary Tradeoffs

18-849b Dependable Embedded Systems

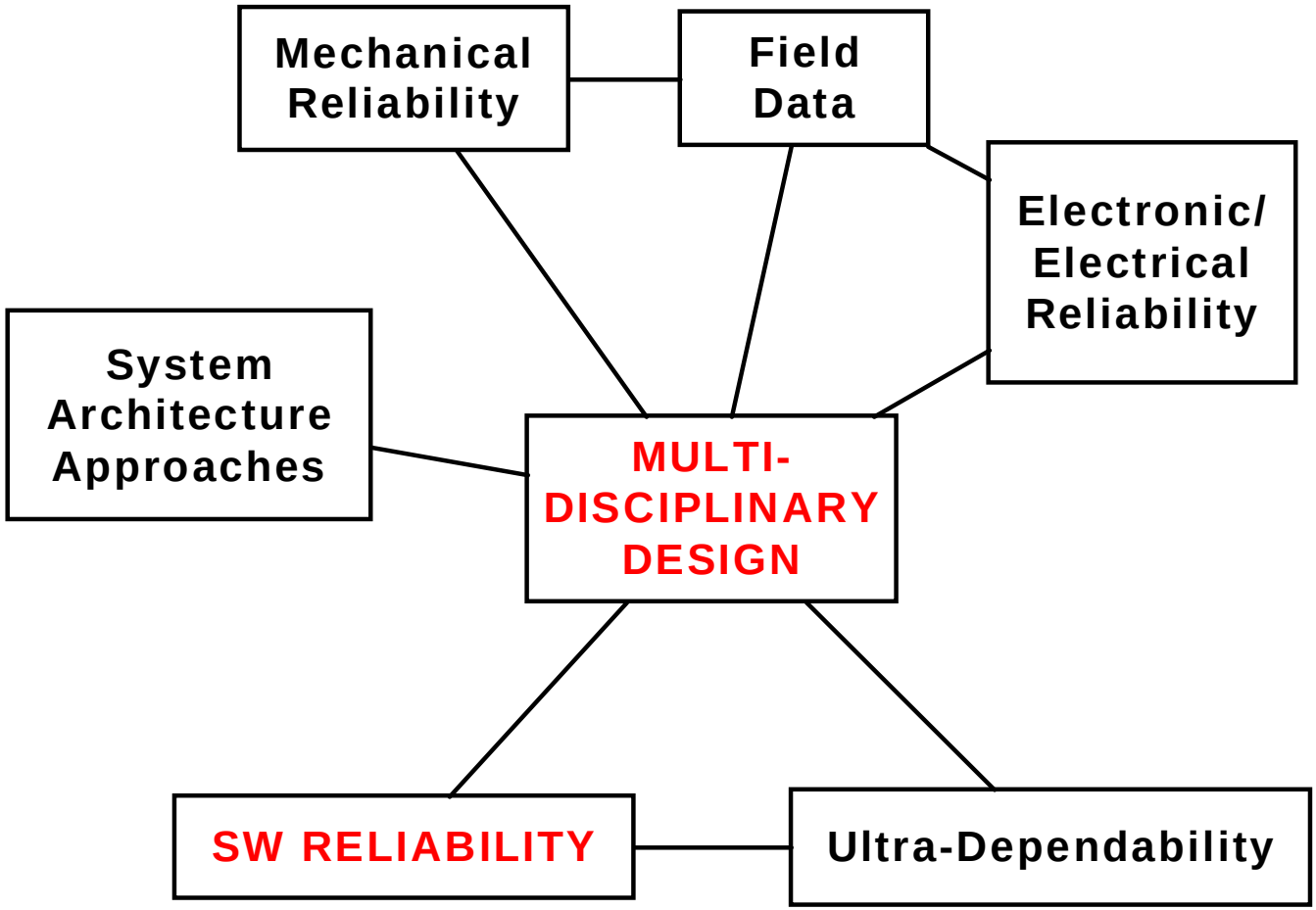
Phil Koopman

3/30/99

Required Reading: *Critical System Properties: Analysis and Taxonomy*, **Rushby**

Carnegie Mellon

You Are Here:


Mechanical Reliability
Field Data
Electronic/ Electrical Reliability
System Architecture Approaches
MULTI-DISCIPLINARY DESIGN
SW RELIABILITY
Ultra-Dependability

Overview: Multi-Disciplinary Tradeoffs

- **Introduction**
  - Appropriate combination of disciplines required to achieve goals
- **Key concepts**
  - Concurrent design/design-for-X
  - Hardware/Software Codesign
  - Using the right technology for the job
  - Inherent multi-disciplinary tensions (*e.g.*, safety vs. reliability)
- **Tools / techniques / metrics**
  - Mostly CAD tools in the mechanical engineering domain
- **Conclusions & future work**
  - Many opportunities; difficult area

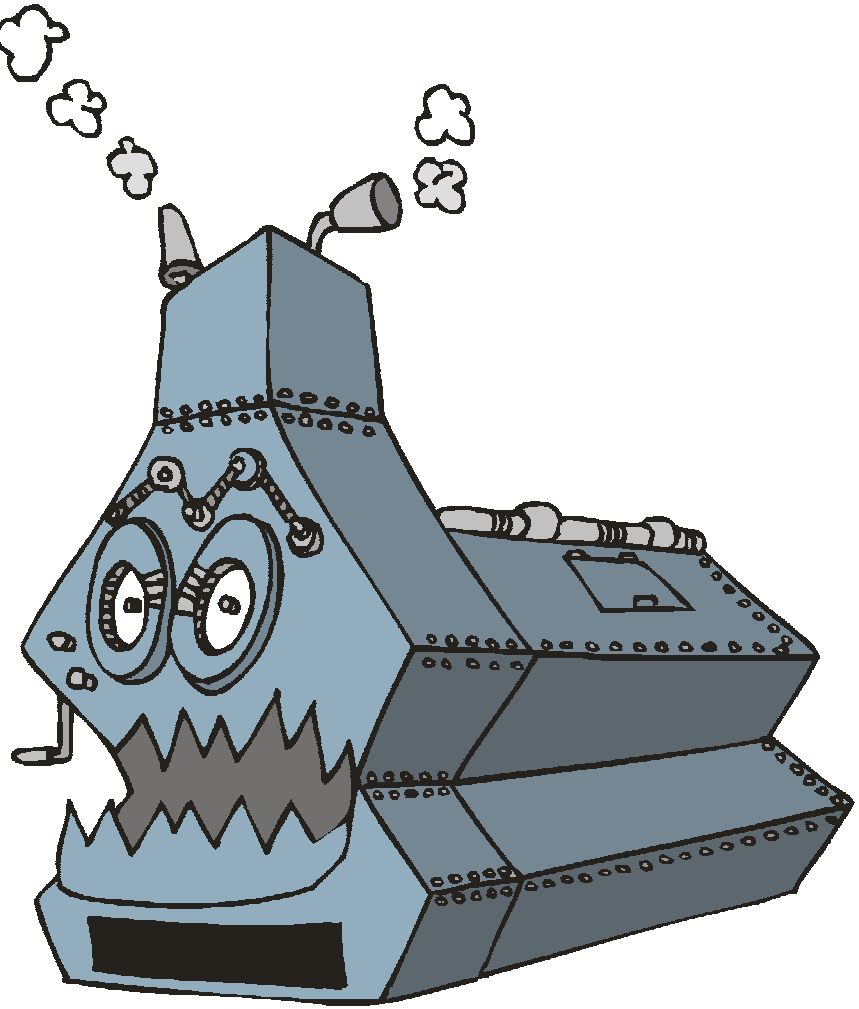
Concurrent Design / Design-For-X

- **Design-For-X for multi-objective satisfaction**
  - Design for: Assembly, Recycling, Reliability, Service,...
  - Typically CAD tool evaluation rather than synthesis
  - Primarily a mechanical engineering approach
    - Some circuit board CAD tools beginning to do this

- **Concurrent design/ cross-functional teams**
  - Put all the different engineers in one room
  - Do life-cycle phase planning concurrently instead of consecutively

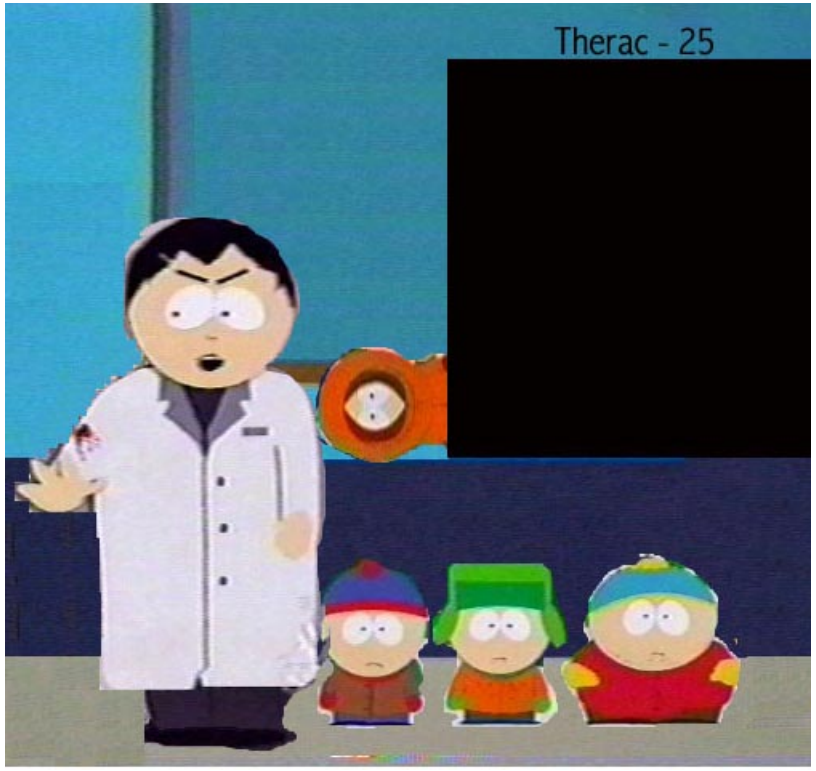
Hardware/Software Codesign

- **CAD/synthesis approach to HW/SW tradeoffs**
  - Start off with system description
  - Perform HW/SW partitioning
  - Optimize speed/cost/power/etc.
- **At this point only a niche approach**
  - Does not deal with analog portions of systems
  - Requires synthesizable description
    - Most won't take C source code for the software input
  - We'll see how it scales in the future



Use The Right Technology For The Job

- **Some technologies invite unnecessary complexity**
  - Be careful of using software for safety interlocks
    - Therac 25
    - Future elevators?
  - Put *necessary* complexity in software for dependability
    - Tune-up-free engines



- **Pick the right role for people**
  - Too stressful invites errors
  - Too boring invites “drop-out”
  - People are good at novelty; machines are good at repetition

Inter-Disciplinary Design Tensions

- **Not always possible to maximize in every dimension**
  - There are some inherently antagonistic properties
- **Safety vs. Reliability**
  - A system that never operates might be perfectly “safe”
  - A system that operates in unsafe situations is “reliable”
- **Security vs. Utility**
  - A system that lets nobody log in may be perfectly “secure”
- **Performance vs. Real-Time**
  - Real-time jitter increases with statistical performance improvement techniques (*e.g.* cache memory)

Tools / Techniques

- **CAD Tools for inter-disciplinary design**
  - Design-for-X tools in mechanical engineering
  - Circuit board evaluation tools (thermal / RFI / manufacturability)
  - Hardware/software codesign

- **Management & Process techniques**
  - Concurrent/multi-disciplinary design teams

Relationship To Other Topic Areas

- **Tradeoffs of mechanical/electronic/etc. reliability**
- **Architecture approach**
  - Should enable multiple technology solutions to critical properties
  - If restrictive, can force poor tradeoffs
- **Software reliability**
  - Sometimes non-software approach relieves SW reliability pressure
- **Ultra-dependability**
  - Ultra-dependable systems require clever tradeoffs among, and probably use of multiple approaches to dependability

Conclusions & Future Work

- **Important to keep a broad perspective**
  - Hammers only work on some screws
  - Use all the tools in your technological toolbelt

- **Efforts to work in this area are more mature on mechanical side than computer side**
  - Design-for-X efforts are in practice
  - HW/SW codesign is limited in scope and still a research topic

- **Global optimality is a worthy quest**
  - It is also a long, hard road

PAPER: Critical System Properties

- **Contrast of different system properties**
  - Dependability
  - Safety
  - Security
  - Real-time

- **You can’t always get what you want**
  - Specifically, discusses inter-disciplinary tensions