Representing Design Tradeoffs in Safety-Critical Systems

Jennifer Morris, Philip Kooman
[jenmorris, koopman]@cmu.edu
ECE Department, Carnegie Mellon University
ICSE WADS 2005
May 17, 2005

Carnegie Mellon

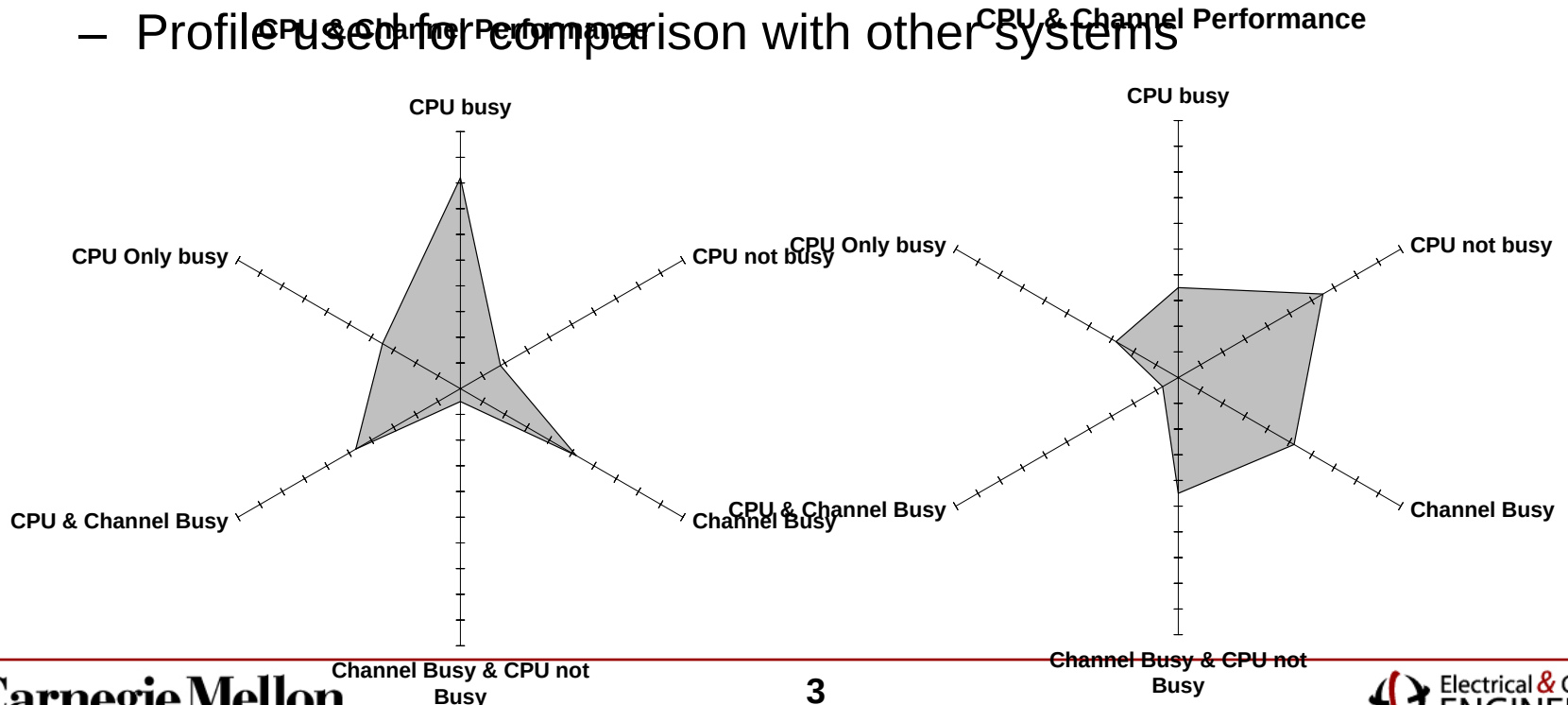
Electrical & Computer ENGINEERING

Motivation

- Increased reliance on software in safety-critical systems
- Effective strategies in place for some application domains
  - Aviation:
    - Fail-operational with triple modular redundancy
  - Rail:
    - Fail-stop with two-of-two systems
    - Fail-operational with dual two-of-two systems
- Can we apply these techniques to new application domains and achieve the same results?
- Which techniques should we choose?
  - For example, should we build x-by-wire cars like fly-by-wire planes?

Graphical Tools for Comparing Application Domains

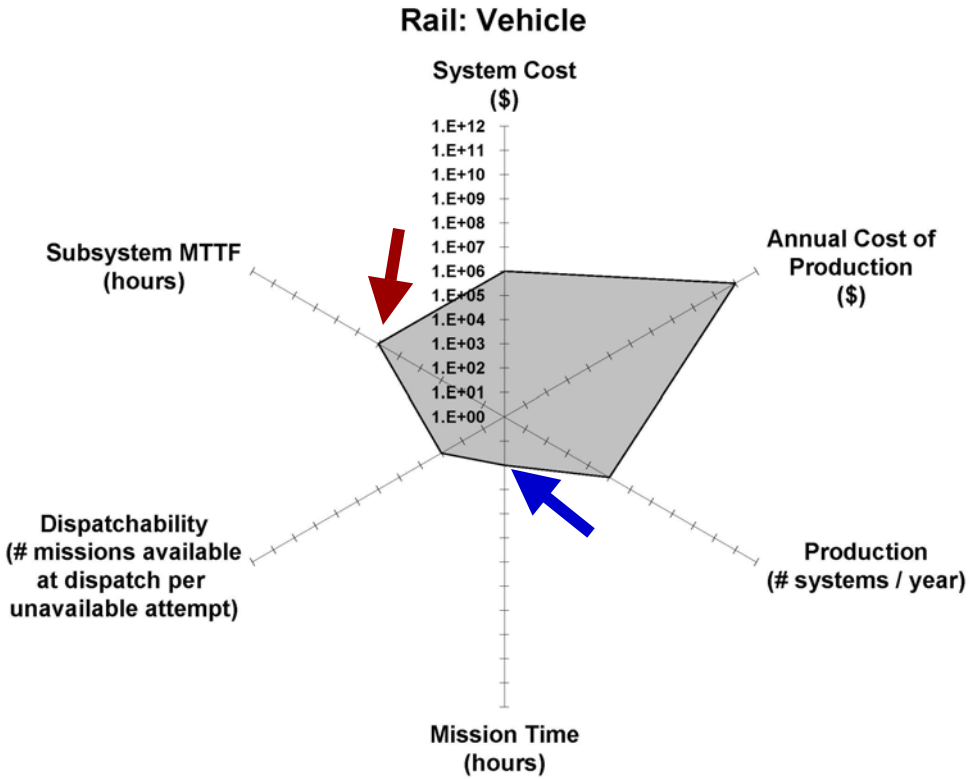
- Kiviat graphs [Kolence & Kiviat '73, Esponda and R. Rojas '92]
  - "Spider Plot"
  - Used to compare software performance
  - Various system metrics plotted on multiple axes
  - Profile used for comparison with other systems

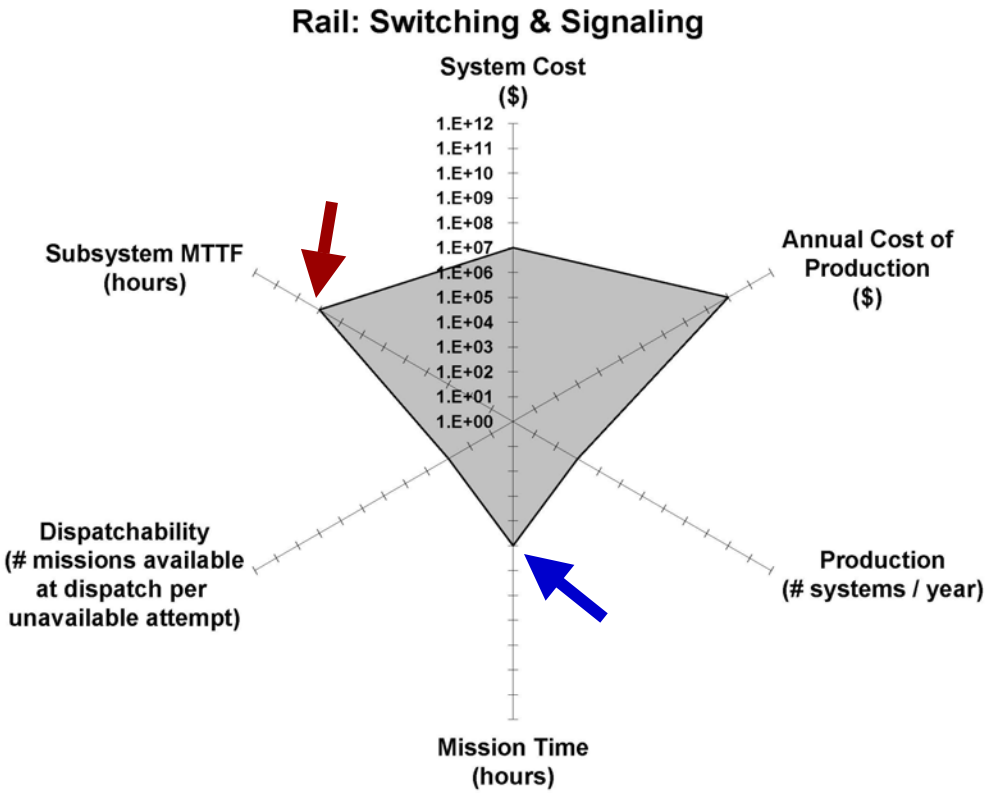


Rail Systems

	Switching & Signalling	Vehicle
System Cost ($)	**10^7** (BART upgrade $45 million)	**10^6** (BART car $2 million)
Production	**10^3**	**10^5**
~Market Size ($)	**10^{10}** (Tens of $ billions)	**10^{11}** (Hundreds of $ billions)
Mission Time (hours)	**10^5** (Tens of years)	**10^2** (Several days)
Dispatchability	**10^3** (~ .1-.2% failed at dispatch)	**10^3** (~ .1-.2% failed at dispatch)
MTTF (hours)	**10^9** (~100,000 years)	**10^6** (~100 years)
Fault-Tolerance Strategy	**Dual fail-stop 2-of-2 systems**	**Fail-stop 2-of-2 system**

Rail Systems

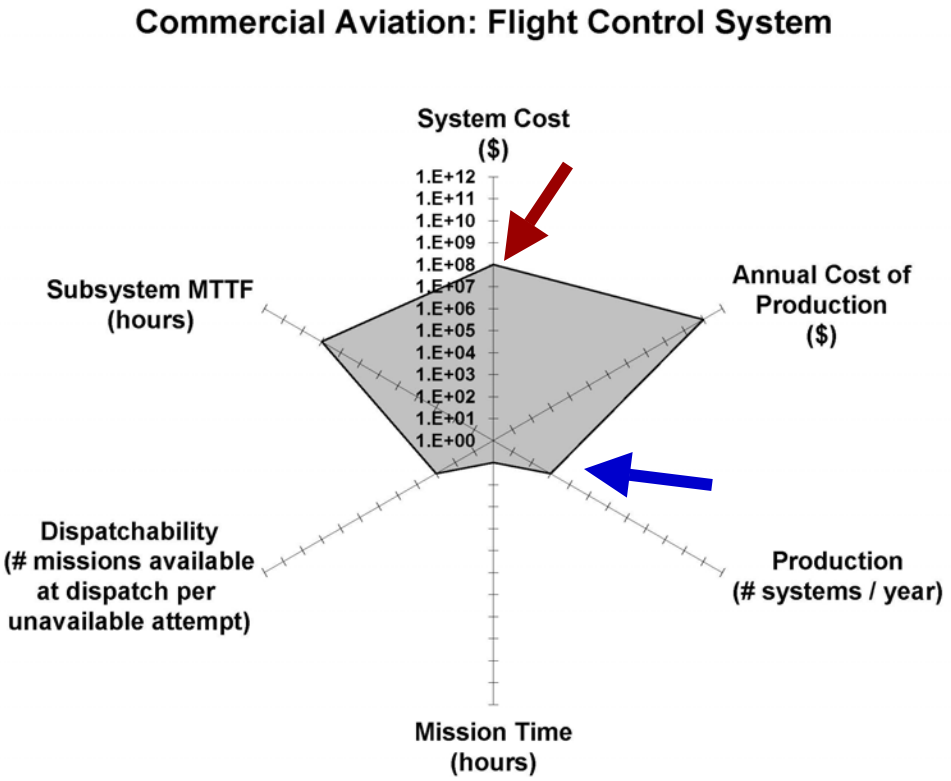


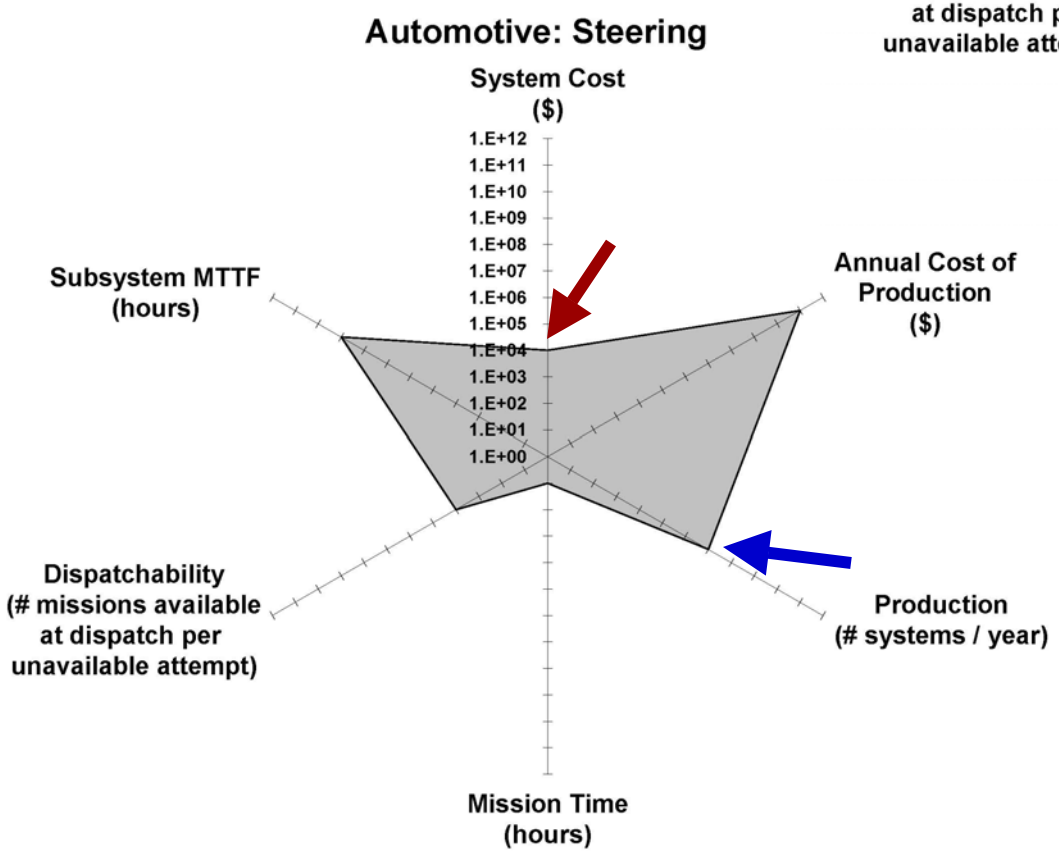


Aviation Flight Control & Automotive Steering

	Aviation Flight Control	Automotive Steering
System Cost ($)	**10^8** (Hundreds of $ millions)	**10^4** (Tens of $ thousands)
Production	**10^3**	**10^7**
~Market Size ($)	**10^{11}** (Hundreds of $ billions)	**10^{11}** (Hundreds of $ billions)
Mission Time (hours)	**10^1** (Several hours)	**10^1** (Several hours)
Dispatchability	**10^3** (~.1-.2% failed at dispatch)	**10^4** (~.01-.02% failed at dispatch)
MTTF (hours)	**10^9** (~100,000 years)	**10^9** (~100,000 years)
Fault-Tolerance Strategy	**Triple modular redundancy**	**Duplex modular redundancy (?)**

Aviation Flight Control & Automotive Steering





What do We Observe?

- Rail signaling & switching vs. vehicle
  - S & S have higher unit cost, but vehicles have higher annual cost
  - S & S have much higher MTTF & mission time
  - Might use similar software dependability strategies, different hardware strategies
- Aviation vs. automotive
  - Similar MTTF & mission time, annual cost
  - Automotive has higher dispatchability
  - Aviation has much higher unit cost
  - Aviation software dependability strategies might be more likely to work for automotive than hardware strategies

Summary and Future Work

- A particular dependability strategy that is successful in one application domain might not be appropriate for another
  - Many different requirements to consider
  - For example, cars have lower per-unit cost, but high volume might permit software, rather than hardware, techniques to be affordable
- A graphical representation of the various design tradeoffs might help system architects choose a strategy
  - Visualization aids help architects deal with complex tradeoffs
- Yet unanswered research questions:
  - Which system characteristics/requirements should be included?
  - Can we graph and compare specific, real-world applications?
  - How do we verify the usefulness of the graphs?

References

- **BART System Facts**. San Francisco Bay Area Rapid Transit District Website, http://www.bart.gov/about/history/systemFacts.asp, accessed February 28, 2005.
- M. Esponda and R. Rojas. **A graphical comparison of RISC processors**. *ACM SIGARCH Computer Architecture News,* 20(4):2–8, September 1992.
- K. W. Kolence and P. J. Kiviat. **Software unit profiles & Kiviat figures**. *ACM SIGMETRICS Performance Evaluation Review*, 2(3):2–12, September 1973.
- N. Leveson. **Safeware: System Safety and Computers**. Addison-Wesley Publishing Company, Reading, Massachusetts, 1995.
- **Air Travel Consumer Reports**. U.S. Department of Transportation Website, http://airconsumer.ost.dot.gov/reports/index.htm, accessed February 28, 2005.

Representing Design Tradeoffs in Safety-Critical Systems

Jennifer Morris, Philip Kooman
[jenmorris, koopman]@cmu.edu
ECE Department, Carnegie Mellon University
ICSE WADS 2005
May 17, 2005

Carnegie Mellon

Electrical & Computer ENGINEERING

Automotive Steering & Throttle/Braking