Perspectives on Transportation Cyber-Physical Systems

Paul S. Miner

Safety-Critical Avionics Systems Branch

NASA Langley Research Center

18 November 2008

Relevant NASA Programs

- ## Aeronautics Research
  - ### Airspace Systems Program
    - http://www.aeronautics.nasa.gov/programs_asp.htm
    - http://www.jpdo.gov/
  - ### Aviation Safety Program
    - http://www.aeronautics.nasa.gov/programs_avsafe.htm

- ## Space Exploration
  - ### Constellation Program
    - http://www.nasa.gov/mission_pages/constellation/main/

Common Technical Challenges

- Mix of both infrastructure and vehicle-specific challenges

- Complex systems of systems
  - Multiple organizations and vendors involved in development and operation
    - Partners in some aspects are competitors in others
  - (Sub-)System decompositions potentially different from existing experience base

- Changing roles and responsibilities for both humans and automation

- System Evolution
  - Need to maintain assurance as systems evolve over multiple decades

Essence of Engineering Complex Systems

"As Eads, Flad, and Pfeifer knew, the essence of sound engineering lay in clearly stating the assumptions upon which calculations are based so that they may be checked at all times for lapses in logic and other errors. It is thus imperative that engineering premises be set down clearly, and that the calculations that follow be systematically and unambiguously presented, so that they may be checked by another engineer with perhaps a different perspective on the problem."

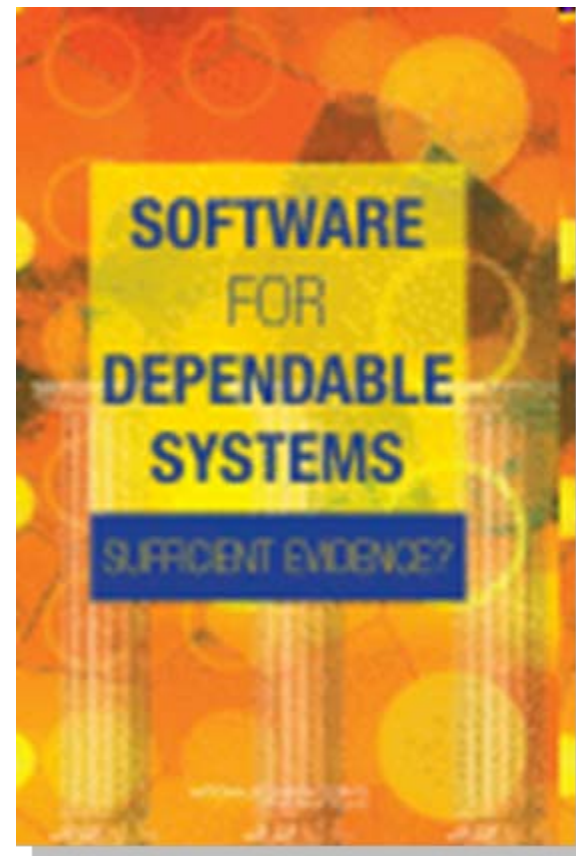*Henry Petroski, "Engineers of Dreams", p. 44, Alfred A. Knopf, New York, 1995.*

Sufficient Evidence?

What are the

- explicit claims,

- evidence, and

- expertise

required for safe deployment of transportation cyber-physical systems?

Challenges going forward

- Focus on explicit claims and evidence provides a basis for bridging gaps between different disciplines
  - It is a necessary step
- There is a need for an effective means to preserve/update dependability claims as complex systems evolve over multiple decades
- Need to provide capability to continually improve the systems, claims and evidence
  - As knowledge improves, we must reflect this in our engineering practices