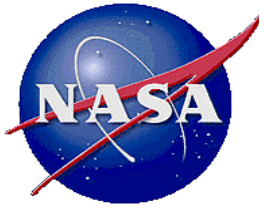
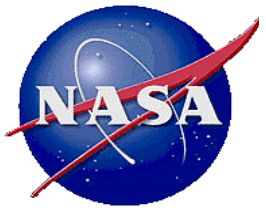


COMPUTING SUBSYSTEMS
(Safety and Reliability Challenges)

July 18, 2007

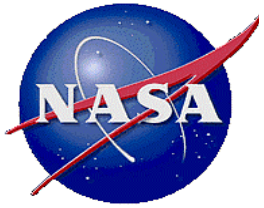
Homayoon Dezfuli, Ph.D.
Manager, System Safety
Office of Safety and Mission Assurance
NASA Headquarters

Role of Computing Subsystems



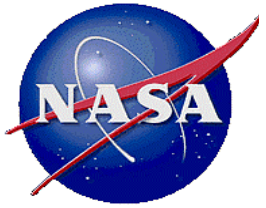
- **Perform safety-critical and mission-critical functions**
  - **Power management**
  - **Telemetry**
  - **Data and information handling**
  - **Communication**
  - **Hardware automation and control**
- **Have contributed to several spacecraft accidents**
  - **Software data specification errors**
  - **Software design specification errors**

What is NASA Doing?



- Improving system engineering (SE) processes to better handle hardware/software, software/human and software/software interfaces and design trade studies
- Improving software assurance processes
- Exploring the applicability of risk assessment techniques to risk-inform the SE and software assurance processes

Challenges for Risk-informing Software Safety



- **Need: Ability to predict (or bound) with a given level of confidence the likelihood of mission failure due to latent software defects to support**
  - **Risk management decisions (e.g., designing SW testing regimes for risk significant configurations)**
  - **Risk acceptability decisions (e.g., showing that a probabilistic safety criterion is being met)**
- **Based on results to-date, it appears that a combination of techniques is needed to satisfy this need**

Exploratory Ideas

- **Risk management decisions**
  - **Application of scenario-based accident modeling techniques to identify system-critical configurations, flight mode changes, and flight transients**
  - **Risk-informed testing regimes**
- **Risk acceptability decisions**
  - **Assignment of initial reliability levels (ranges) based on attributes such as design complexity, and SW quality V&V process considerations (risk classification of software elements)**
  - **Adjustment of reliability levels based on V&V and risk-informed test process findings (updating of initial reliability levels)**
- **Continue focused research**
  - **Beneficial to work with NRC**