High Dependability Computing Program

Michael Evangelist  
Director of Research  
Carnegie Mellon University-West  
Moffett Field, California
Improve Dependability, Reduce Risk

• Focus of the panel
  – “technologically enabled advanced risk-management framework for NASA that provides end-to-end capabilities”

• Dependable technology, techniques, and engineering practice important element for risk reduction
Goal of This Presentation

- Overview HDCP research approach and concepts
- Status report on activities
- Transferring the ideas
HDCP Research Model

research idea → instantiation → testbeds

credible version → into practice

NASA activities increase left to right, top to bottom
HDCP Technical Goals

- Investigate NASA dependability issues
- Develop technologies, techniques, and processes for dependable computing
- Create testbeds for empirical validation and develop dependability measures
- Support model-based technology transition
HDCP Testbeds

Special testbed project: Golden Gate (Sun/JPL/HDCP implementation of MDS using Real Time Specification for Java)

MDS = Mission Data System
CTAS = Center-TRACON Automation System
MERBoard = Mars Exploration Rover Board

primary testbed research
other testbed research
Overview of HDCP Research

- Define MDS more precisely
- “Self-healing” algorithms
- USCRover testbed
- Tool to ensure MDS conformance
- New approach to defect seeding
- Investigation of RTSJ as real-time language (Rocky 7 testbed)

LONGER-TERM GENERAL PROJECTS
- Dependability through new approaches to testing
- Analytic assurance of safe concurrency for Java programs
- Dependability attributes and models
- Re-architecture of MERBoard interface for usability
- Prototype of TSAFE, component that checks conformance to flight plans
Overview of Shorter-Term Projects

- Verification & validation for MSL
  
  Helping MSL develop a dependable V&V process based on our experience with the SEL at Goddard

- “Dependability cases” for MDS
  
  Systematize arguments to establish the dependability characteristics of a system

- Systems administration assistant
  
  Automated assistance to improve dependability when astronauts function as systems administrators

- MDS return-on-investment analysis
  
  Applying the COCOMO model to investigate value of MDS architectural approach
FY 2003 Testbed Activities

- Complete Rocky 7 deployment
- GG testbed experiments
- Apply Java analysis tools

- Complete USCRover testbed
- MDS testbed experiments
- Tool to assist MDS compliance
- Apply “self-healing” algorithms

**GENERAL PROJECTS**

- Implementation of new testing approaches
- Validation studies for dependability model

- In-depth study of architectural approach to usability
- Apply usability ideas to new testbed

- Expand TSAFE to help design future air-traffic management system
FY 2003 Supporting Activities

- Verification & validation for MSL
  
  Complete the V&V plan for MSL and help supervise the implementation

- “Dependability cases” for MDS
  
  Complete enough cases to investigate the value of systematizing arguments for dependability characteristics

- MDS return-on-investment analysis
  
  Finish application of classical COCOMO model to investigate value of MDS architectural approach
Research into Practice

- First 18 months devoted to understanding NASA problems, creating technology, setting up testbeds, and designing initial experiments
- Second 18 months will see significant experimentation and iteration of research
- Final 18-month period devoted to new testbeds and model-based technology transition
TGIR Theme

• Keys to success in 21st Century
  – implementing policies through strengthened partnerships
  – innovation in research practices
  – leadership in technology
TGIR Theme

• Keys to success in 21st Century
  – implementing policies through strengthened partnerships
    – NASA partnerships growing stronger with CMU, MIT, the Universities of Maryland, Southern California, and Washington, and Sun Microsystems (among others)
  – innovation in research practices
    – four-step process requiring iterative testbed evaluation a new approach for software research
  – leadership in technology
    – models and measures for assessing dependability level, significant application of the new Real Time Specification for Java, technology to support lightweight formal methods, usability approach to architecture, new techniques for defect seeding, ...