Relations Between Resilience and Validation

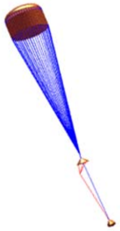
Richard J. Doyle
Solar System Exploration Technology Program
Jet Propulsion Laboratory
California Institute of Technology

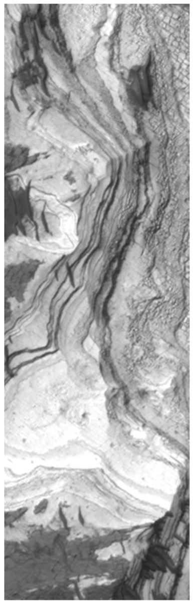
Keck Institute for Space Studies
Workshop on Resilience Space Systems

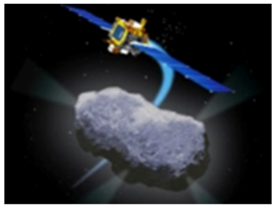
August 1, 2012

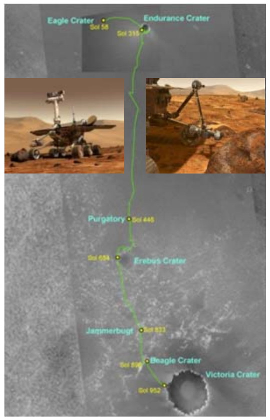
Validation: NASA Needs and Challenges

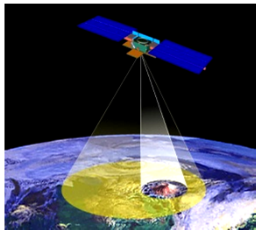
- **Autonomy** is indicated as a system capability when operating in uncertain, inadequately modeled environments
- The inherent **uncertainty** hobbles the ability to conceive and execute a comprehensive test program prior to launch
- NASA continues to advance **exploration** into remote environments which are increasingly dynamic and poorly characterized at arrival time

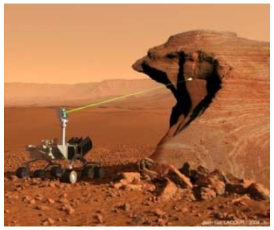






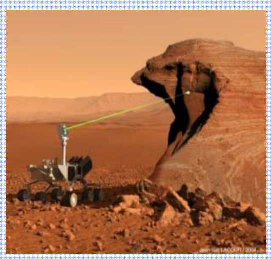






Validation of Autonomous Space Systems

CURRENT APPROACH



NASA Space Systems are validated today

- *By testing in high-fidelity testbeds*
- *Via simulations using physics-based models of the system and environment*
- *Using Monte-Carlo and other sampling techniques*

OPEN QUESTIONS

Validation Methodologies:

Can future autonomous systems validation be addressed by extensions to existing approaches or are new validation concepts needed?

System Behavior Envelopes:

Is it possible to define boundary conditions for permissible system behavior, independent of operating context, which

1. guarantees that system safety is preserved?
2. mission plans can be validated against at acceptable computational cost?
3. allows behavior flexible enough to accomplish mission objectives?

Lifecycle View:

What is the role of model-based design, engineering and reasoning techniques in support of autonomous systems validation? Is a full-lifecycle approach (i.e., into operations) required?

State Space Complexity:

What are efficient search techniques that can provide reliable, if probabilistic, validations of proposed mission plans or sequences?

Flight Computing:

What flight computational support is needed to validate mission plans that are generated onboard and informed by operating conditions in the environment?

IMPACT

Future NASA Missions and Scenarios Enabled:

- *Pinpoint and Safe Landing*
- *Proximity Operations at Primitive Bodies*
- *Fast Surface Mobility*
- *Surface Science During Traverse*
- *Agile (Time- and Knowledge-Limited) Science Operations*

Techniques and methodologies to validate that the system will "do the right thing" when autonomy is required in dynamic and uncertain operating environments

Resilience: Perspectives on Validation

- **From Fault Protection**
  - *Hard Core*: Preserve core mission functionality no matter what
  - *Fault Diagnosis*: Define faults to be departures from nominal behavior rather than through an enumerated list
  - *Behavior Envelopes*: Same insight, a range of permissible system behaviors, defined independent of operating context
- **From Software Verification**
  - *Lifecycle View*: Most powerful to specify behaviors formally, design out bugs (faults) early
  - *Equivalence Classes*: Not all state distinctions are useful
  - *Smart Testing*: Techniques for efficient sampling, most meaningful tests
- **From Automated Planning**
  - *Intent*: Goal-based planning techniques provide formal guarantees that intent is preserved in automatically generated plans
  - *Modeling*: Modeling the effects of actions on system and environment
  - *Projection*: What-if? state prediction to verify that a proposed plan does not violate safety conditions