



Rover Autonomy System Validation

MSL Focused Technology Task

Lorraine Fesq

5/8/03



Problem Statement

- Are current V&V practices sufficient to ensure safe Rover operations?
What is cost/payoff of additional V&V?
- What, if any, additional V&V needs are introduced by increasing the Rover's autonomous surface capabilities (implies increase in software complexity?)?
 - FSW capable of traversing multiple sols in response to 1 uplink session
 - FSW capable of reliably/safely traversing terrain not yet seen from surface level by ground operators
 - FSW shall approach target and place instrument with no further uplink
- MSL has base-lined the Mission Data System (MDS) architecture for flight and ground.
 - How do we characterize the applicability of conventional and emerging Verification and Validation (V&V) methods to MDS?
 - How does MDS enable better V&V methods?



Objectives

Mitigate risk of using software-based surface operations capabilities

- Establish and demonstrate V&V techniques that validate baseline capabilities and enable deployment of enhanced capabilities
- Architect and demonstrate in-flight protection system that bounds rover system behavior to within acceptable, safe region



Definition of Verification and Validation

Verification: Asks “Are we building the product *right*?”
Determines degree to which the work products of a given phase conform to specifications, e.g., “is this a correct implementation of the design?”

Validation: Asks “Are we building the *right* product?”
Evaluates system at end of development to determine compliance with *requirements* and to ensure system performs to customer’s expectations.



V&V of Autonomy: Challenges

Less Autonomous

- Short time cycle (sec..hour)
- Human deals with unexpected
- Open-loop, easy to test
- Tractable state space, testing is appropriate

More Autonomous

- Long time cycle (day..year)
- Machine deals with unexpected
- Closed-loop, hard to test
- Huge state space, testing is insufficient



Overview of Current Approaches

Currently, the following techniques are used to verify/ validate aerospace systems and ensure safe operations

- Informal methods
 - Reviews, code walkthroughs
 - Processes: configuration management, change control board, problem report tracking
- Testing
 - Simulator-based
 - Testbeds
 - Flight hardware
- Reactive on-board Fault Protection
 - Detects off-nominal conditions
 - Transitions vehicle to “safe” configuration
- Special design for mission-critical activities





Proposed Technical Approach

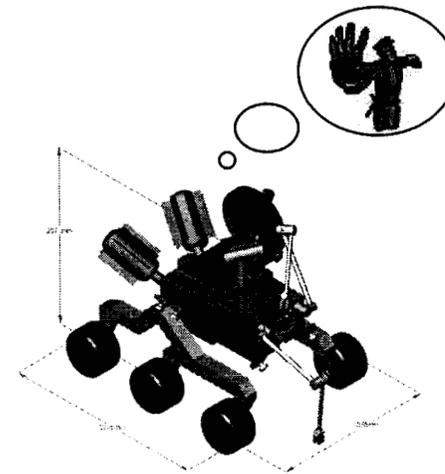
- Add Formal Methods to toolbox
 - Apply mathematical/symbolic manipulation techniques to prove putative properties of software artifacts
 - Runtime monitoring evaluates running code
 - Static analysis detects errors w/o executing code
 - Model checking verifies finite state concurrent systems
 - Pro: early detection, exhaustive check of all paths, proof of correctness
 - Con: cost to develop models, formal specs
- Automate processes: auto-code generation, automated testing
- Create Pro-active Protection System
 - Anticipates unsafe behavior
 - Prohibits entry into unsafe behavior region

```
p = x - 0.75;
y = sqrt (p);
}

/* unreachable or dead code
void wff () {
  int x = random_int();
  int y = random_int();
  if (x > y) {
    x = x + y;
    if (x < 0) {
```

color-coded reporting:

Green	always correct
Red	always incorrect
Orange	may be incorrect
Gray	never executed

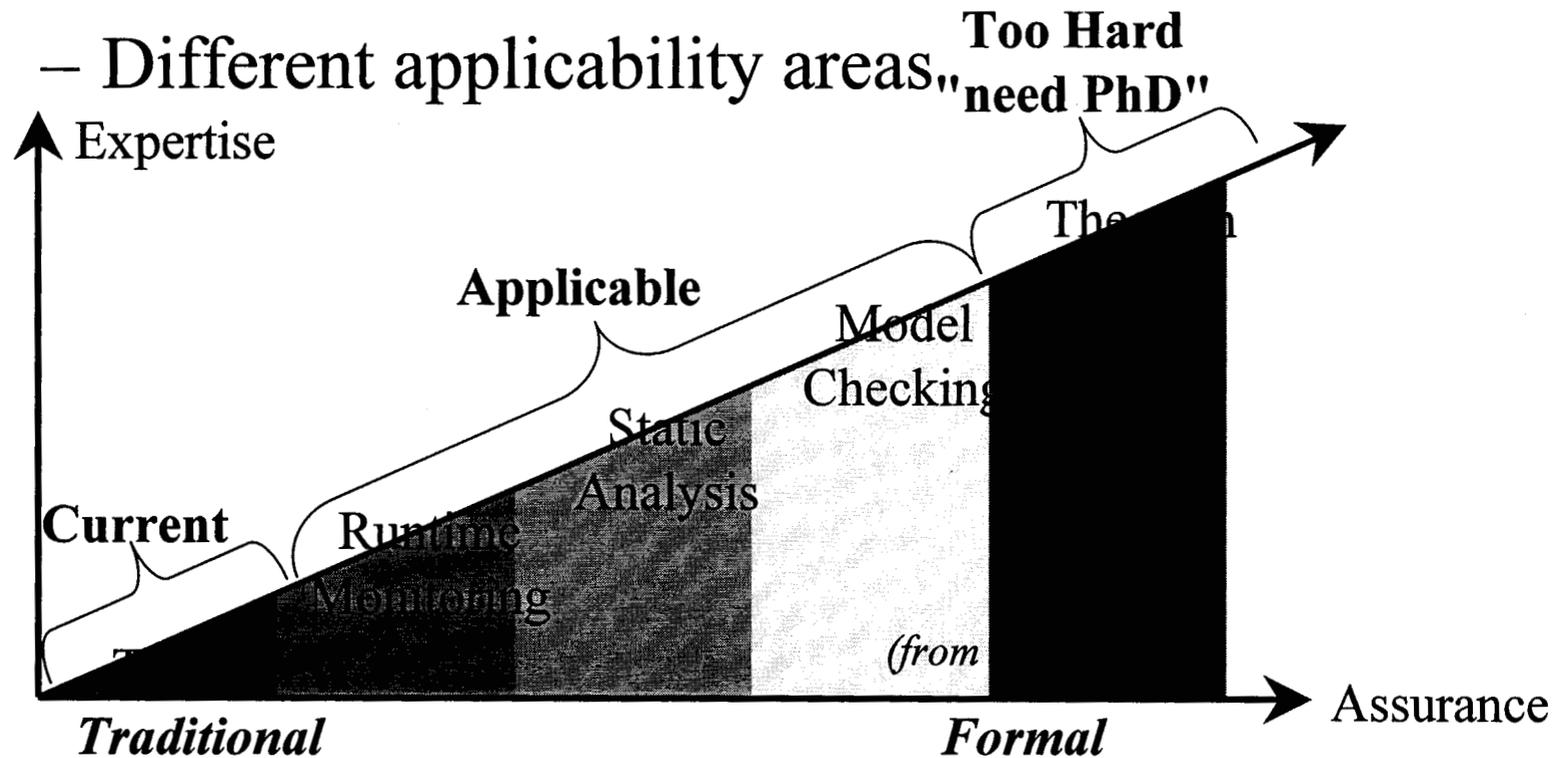




Formal Methods

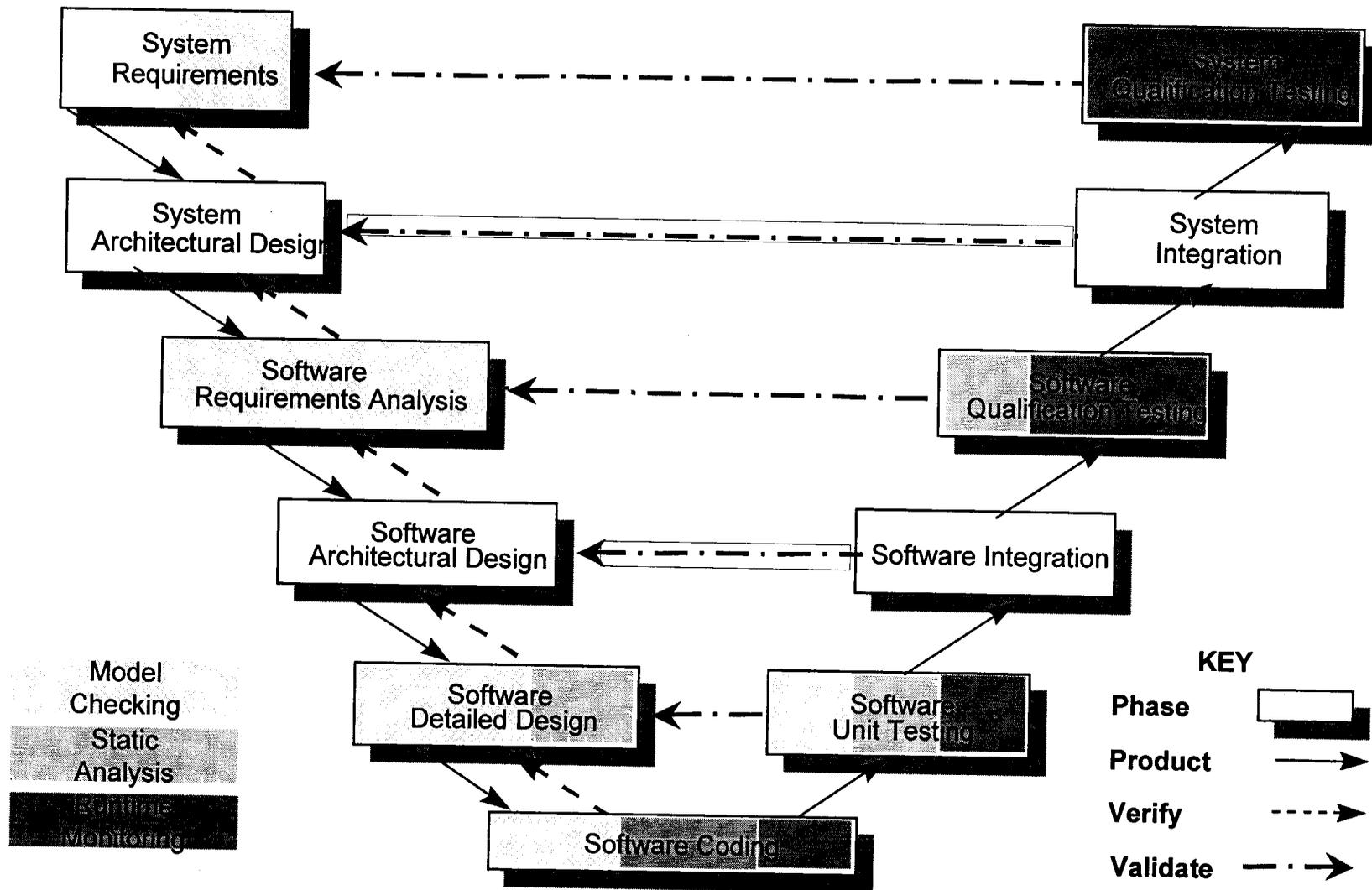


- Different "formal" methods
 - Different strengths
 - Different applicability areas



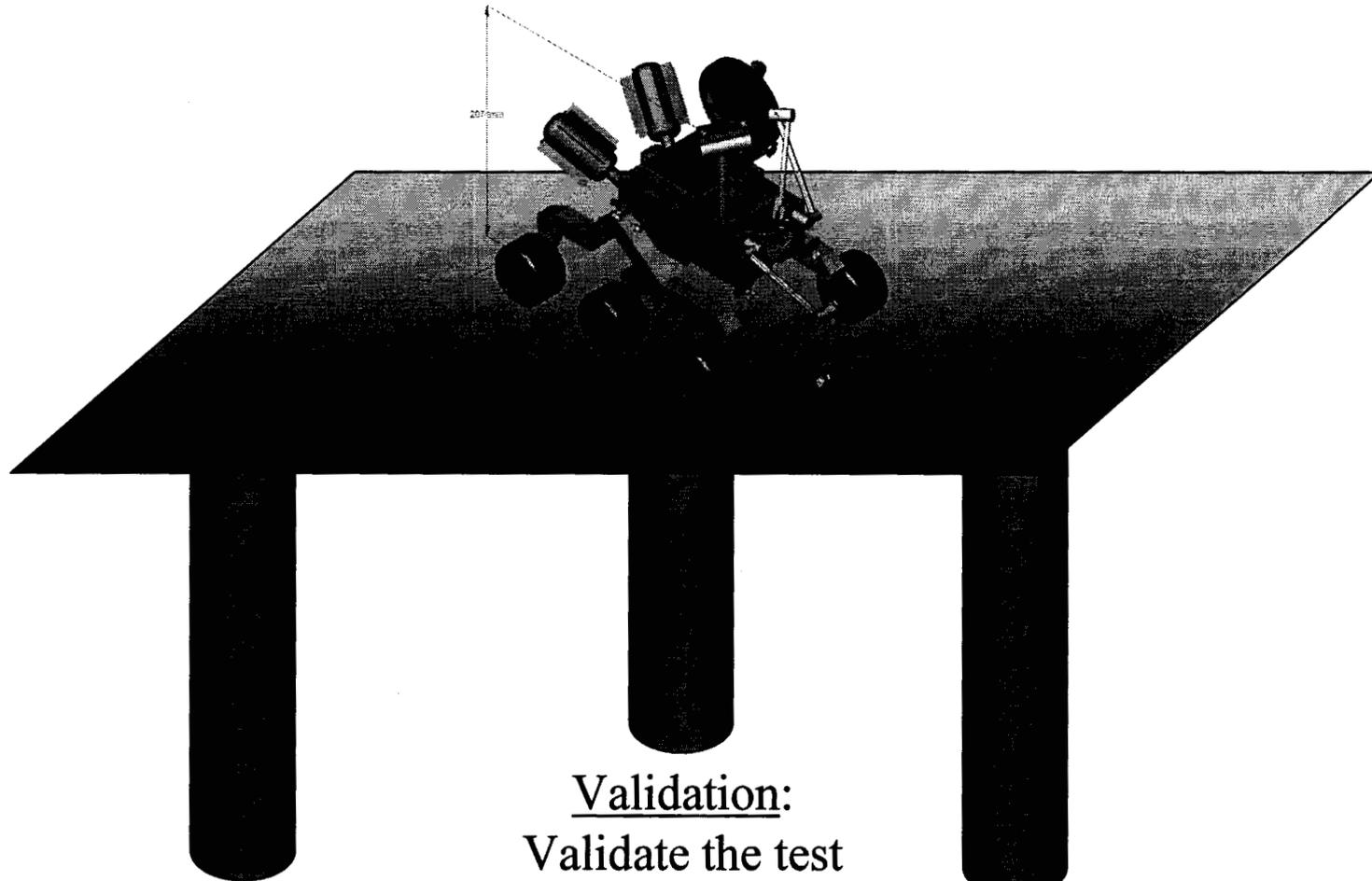


Formal Methods in the Software Lifecycle





The Three Pillars of Autonomy V&V



Verification:
Prove the
software
is correct

Validation:
Validate the test
Environment, then
validate the system
Within the
environment

Protection:
Provide and
verify a
safety net



Plan of Attack

- Benchmark current JPL V&V practices
- Survey V&V techniques and processes available outside of JPL
- Identify system and software errors to be expunged, and cross-reference appropriate V&V technique/process
- Analyze V&V needs of MSL Rover system and align with available V&V techniques
- Identify gaps where existing techniques are insufficient/lacking
- Engage broader community of researchers to seek out promising technologies to fill gaps, and promote collaboration and maturation of technologies
- Establish requirements for, design and demonstrate pro-active fault protection system to bound rover behavior



Milestones and Schedule

- FY03
 - Complete V&V techniques surveys
 - Perform gap analysis
 - Hold workshop to engage broader community and identify promising V&V technologies
- FY04
 - Select and fund development of promising V&V technologies to mature to TRL5/6
 - Design and prototype pro-active fault protection system to monitor and bound rover behaviors
- FY05
 - Infuse, demonstrate and assess comprehensive V&V techniques and processes in concert with 9/05 software demonstration
 - Demonstrate strawman pro-active fault protection system integrated with 9-05 software demonstration