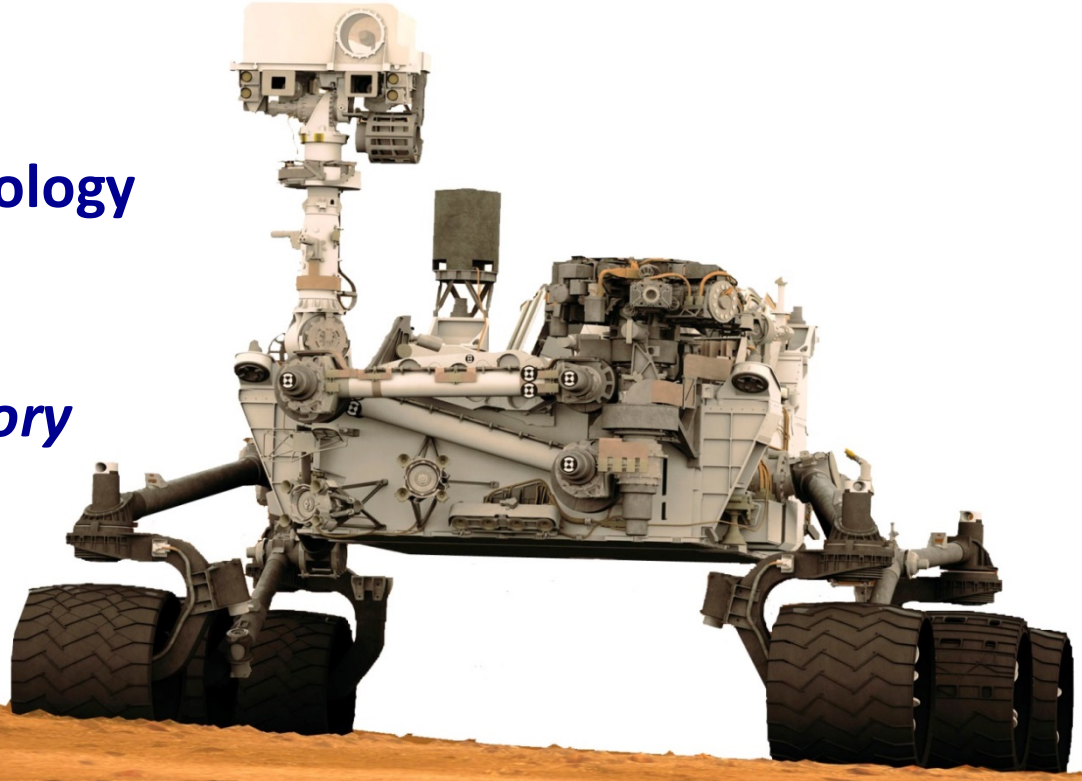
Jet Propulsion Laboratory
California Institute of Technology

Validation of Autonomous Space Systems

ISR Systems and Technology Workshop

MIT Lincoln Laboratory

June 8, 2016



Dr. Richard Doyle, Prog. Mgr.
Information and Data Science
NASA Jet Propulsion Laboratory
California Institute of Technology

with contributions from Dr. Steve Chien, Ms. Ann Devereaux, Dr. Tara Estlin, Dr. Gerard Holzmann, Dr. Michel Ingham, Dr. Terry Huntsberger, Dr. Andrew Johnson, Dr. Rajeev Joshi, and Mr. Raphael Some

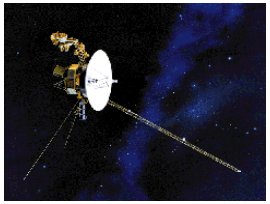
© 2016 California Institute of Technology.
Government sponsorship acknowledged.
UNCLASSIFIED

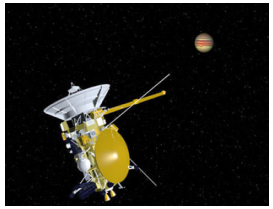
Jet Propulsion Laboratory
California Institute of Technology

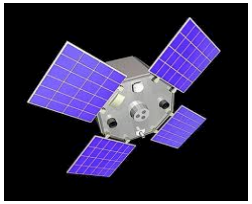
JPL's Work for NASA and Other Government Agencies

Numerous Spacecraft and Instruments across the Solar System and Beyond

Jet Propulsion Laboratory
California Institute of Technology


Two Voyagers (1977)

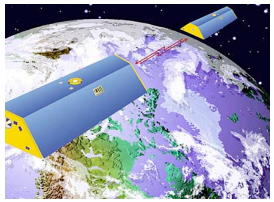

Cassini (1997)

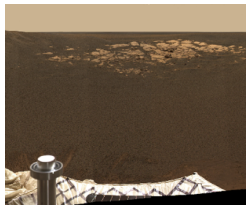

ACRIMSAT (1999)

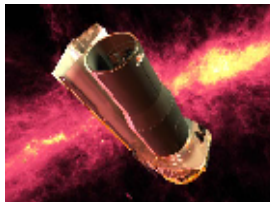
QuickSCAT (1999)

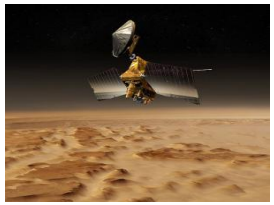
Mars Odyssey (2001)

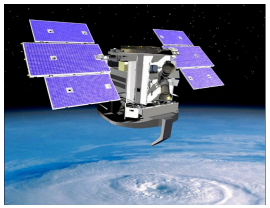
Jason 2 (2008)


GRACE (2002)

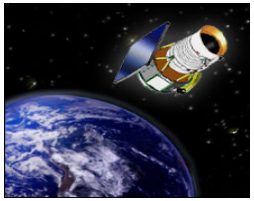

Opportunity (2003)

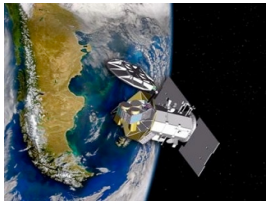

Spitzer (2003)

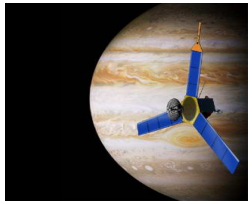

Mars Reconnaissance Orbiter (2005)

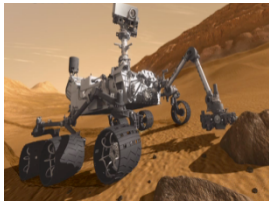

CloudSat (2006)

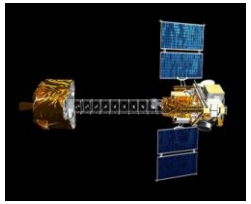
Dawn (2007)


Wide-field Infrared Survey Explorer (WISE) (2009)


Aquarius (2011)

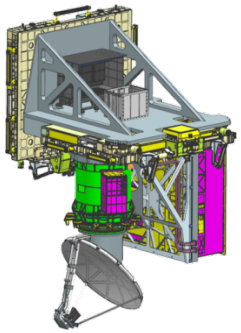

Juno (2011)

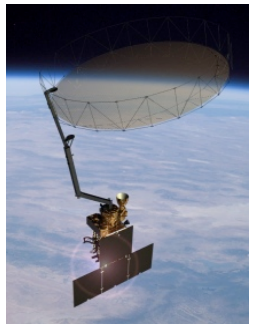

Curiosity (2011)


Nuclear Spectroscopic Telescope Array (NuSTAR) (2012)

Carbon Cycle: OCO-2 (2014)

UNCLASSIFIED

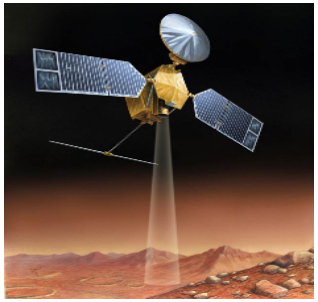

ISS – RapidSCAT (2014)


Soil Moisture: SMAP (2015)

A continuous robotic presence in orbit and on the surface of Mars

Jet Propulsion Laboratory
California Institute of Technology

2001 Mars Odyssey

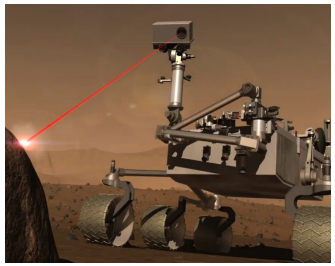


Mars Reconnaissance Orbiter

Mars Express (ESA)

Opportunity's tracks
Meridiani Planum

Opportunity



Curiosity

"Do not go where the path may lead, go instead where there is no path and leave a trail"

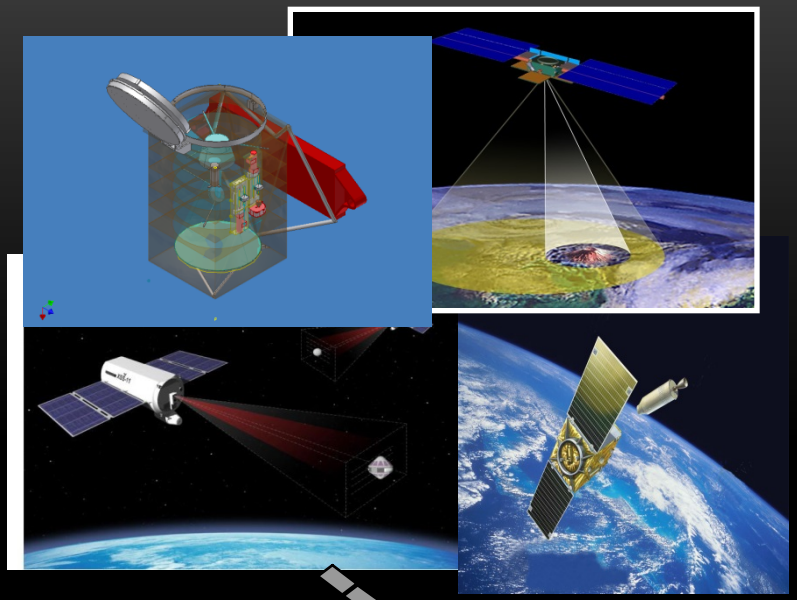
--- Ralph Waldo Emerson

National Space Technology Applications Summary

Solving problems of national security and national significance

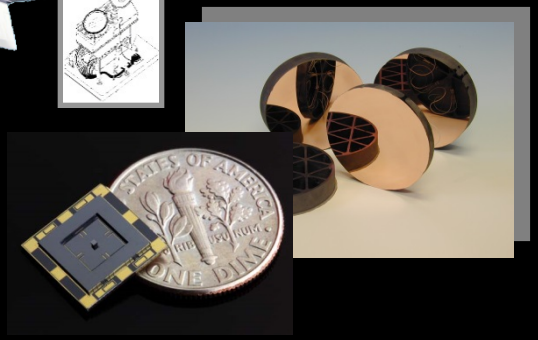
Tech. Demos

Gravity, magnetics, vibration, large lightweight optics, large structures, Micro & nano devices and dual band radars



Technology Development

Leader in S/C and UAV instrument applications, lasercom, radar, HSI, first responder



Sponsor needs and hard problems

Strong Tech base and exploiter of electro magnetic spectrum using unconventional and revolutionary means to provide persistent collection, analysis & applications

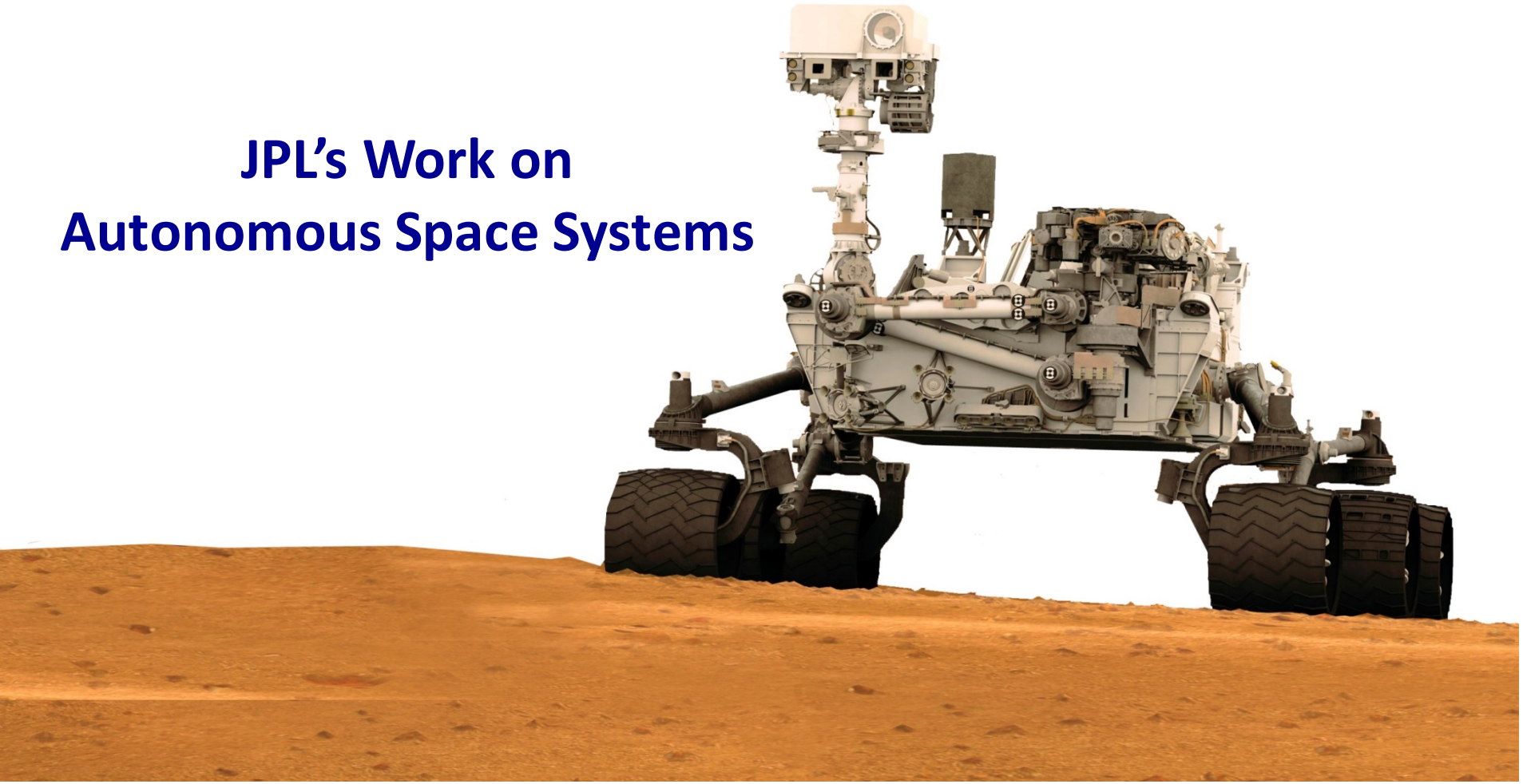
Strategic Relationships

Recognized experts by all major aerospace and USG sponsors
With responsive, agile business and technology support

UNCLASSIFIED

Jet Propulsion Laboratory
California Institute of Technology

JPL's Work on Autonomous Space Systems



UNCLASSIFIED

Dust devils on Mars - MER

Jet Propulsion Laboratory
California Institute of Technology

Dust devils are scientific phenomena of a transient nature that occur on Mars

- They are challenging to reliably capture in images due to their dynamic nature
- Scientists accepted for decades that such phenomena could not be studied in real-time

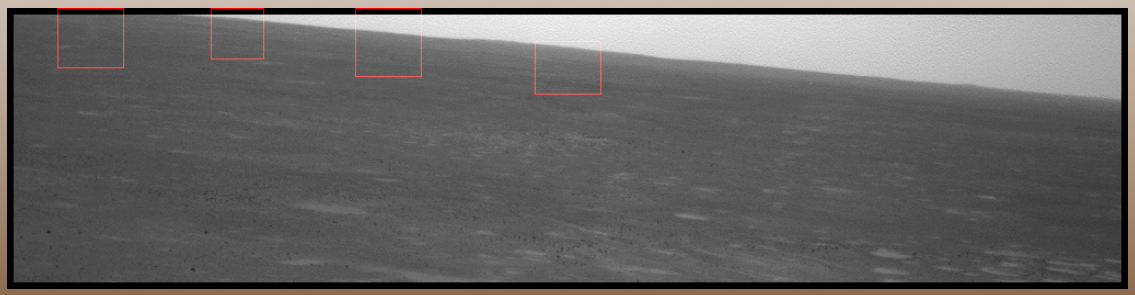
Spirit Sol 543
(July 13, 2005)

New onboard Mars rover capability (as of 2006)

- Collect images more frequently, analyze onboard to detect events, and only downlink images containing events of interest

Benefit

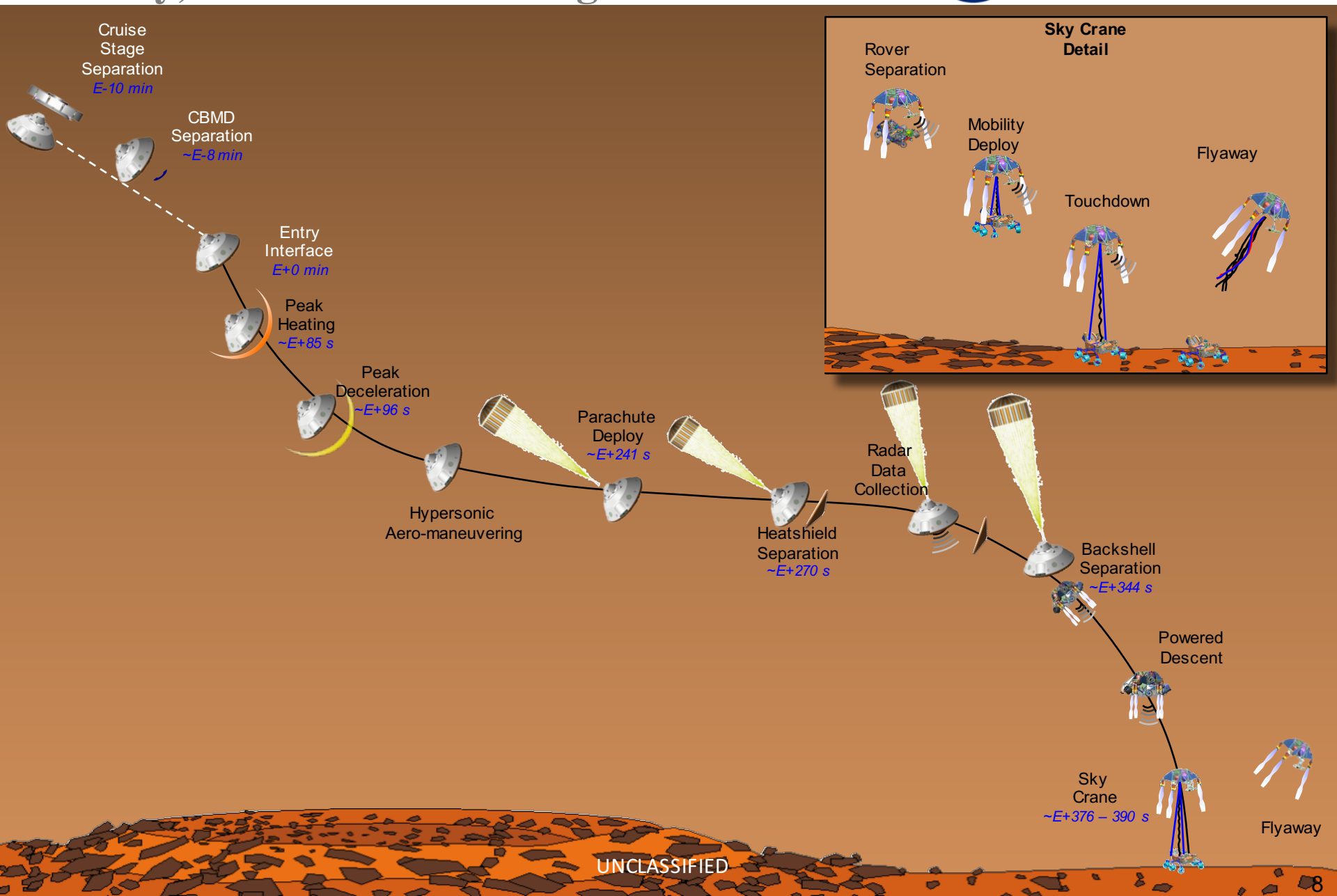
- < 100% accuracy can dramatically increase science event data returned to Earth
- *First notification includes a complete data product*



Credit: T. Estlin. B. Bornestein, A. Castano, J. Biesiadecki, L. Neakrase, P. Whelley, R. Greeley, M. Lemmon, R. Castano, S. Chien and MER project team

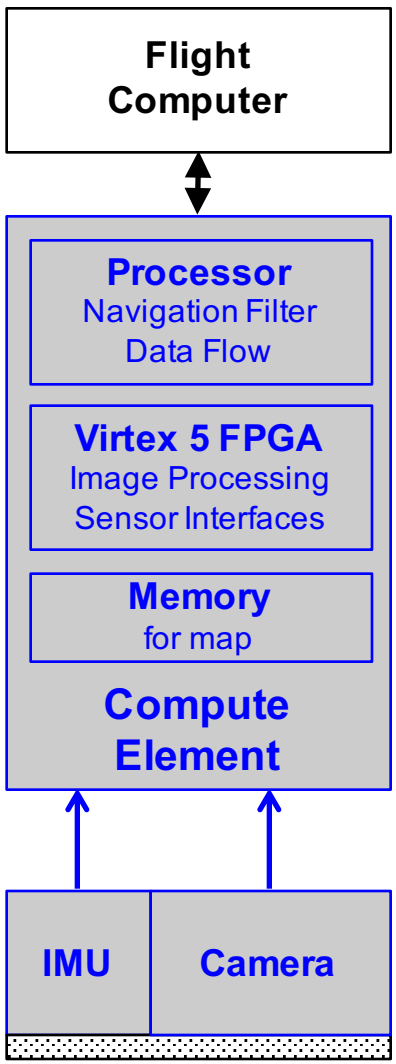
Entry, Descent and Landing - MSL

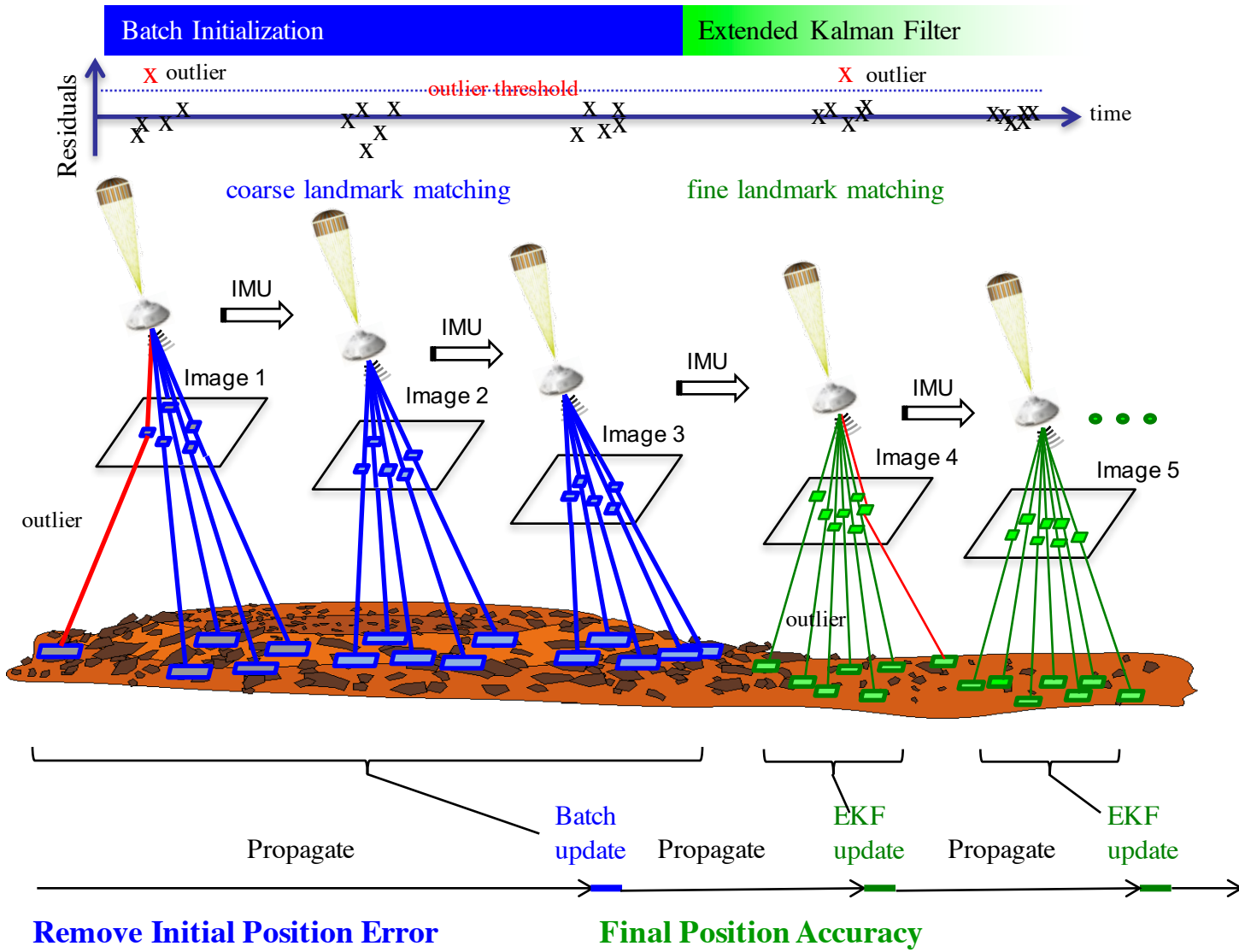
Jet Propulsion Laboratory
California Institute of Technology



Lander Vision System – Mars 2020

Jet Propulsion Laboratory
California Institute of Technology





Credit: A. Johnson

LVS Field Test Movie

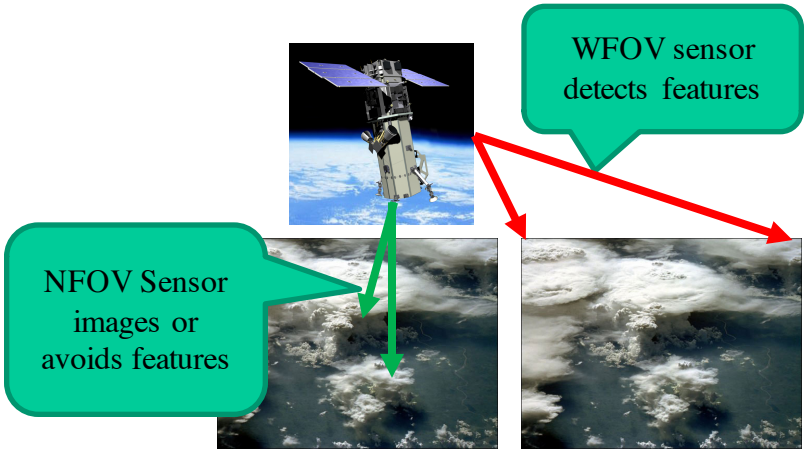
Jet Propulsion Laboratory
California Institute of Technology

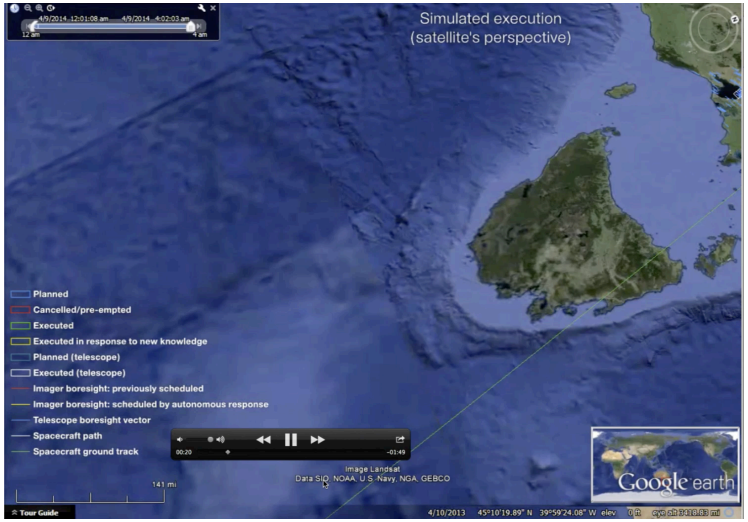
Credit: A. Johnson

Autonomous direction of narrow field of view (NFOV)

Jet Propulsion Laboratory
California Institute of Technology

- Autonomous onboard analysis of data from wide FOV (WFOV) forward looking sensor used to re-direct nadir looking NFOV sensor
- Significant improvement in utilization of NFOV instrument:
  - Can avoid bad data such as clouds (e.g. OCO-3 redirection) or
  - Track science features such as cloud fronts, ocean color fronts,
  - Can search for spectral signatures, dwell on high value targets such as volcanic features
- Applicable in situations where narrow FOV sensor is agile enough for within overflight re-tasking: agile spacecraft, fast steering mirror, electronically steered sensor, gimbaled airborne, or re-fly flight-line
- Prototype demonstrated in flight software for spectral search with agile spacecraft in low Earth Orbit (10's seconds closed loop)



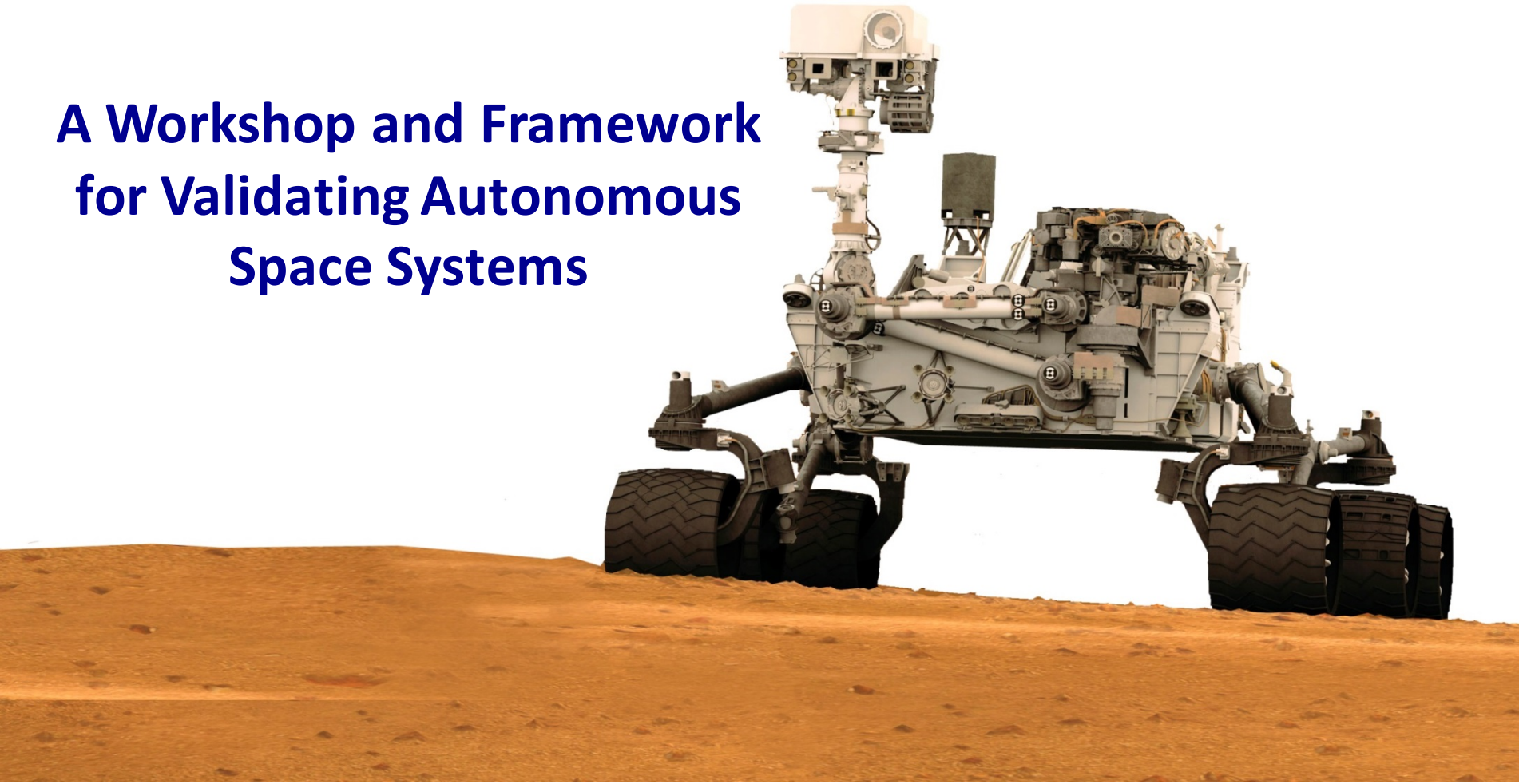


Visualization from agile spacecraft flight software prototype.

Credit: S. Chien

Jet Propulsion Laboratory
California Institute of Technology

A Workshop and Framework for Validating Autonomous Space Systems

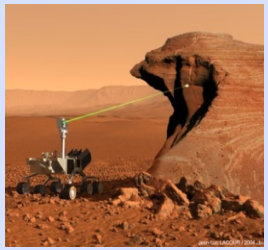


UNCLASSIFIED

Validation of autonomous space systems

Jet Propulsion Laboratory
California Institute of Technology

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?

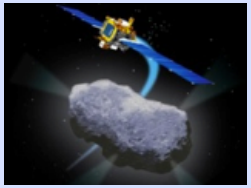
Flight Computing:

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 Potentially Enabled:

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



Techniques and methodologies to validate that the system will "do the right thing" when autonomy is required

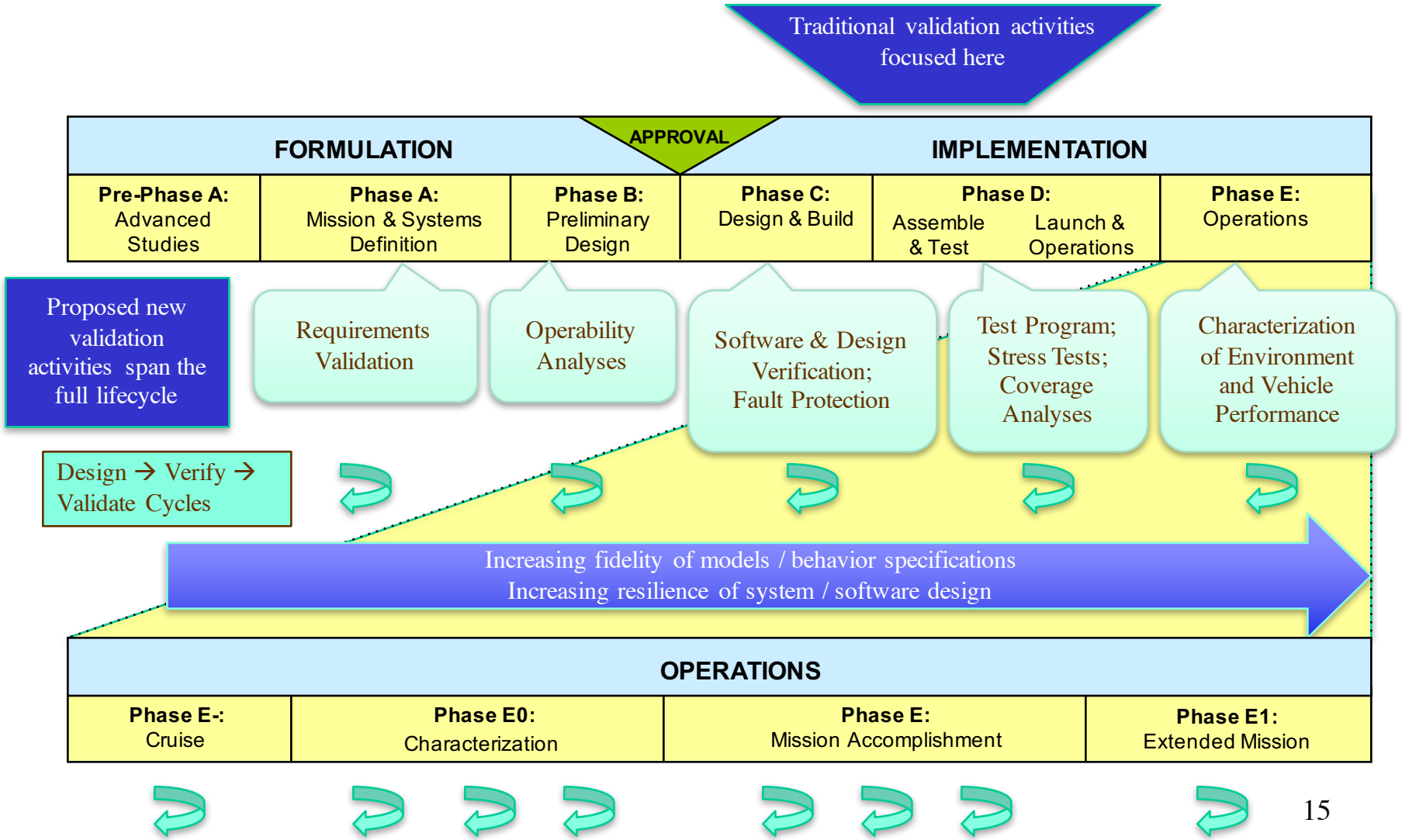
Technical tall poles

Jet Propulsion Laboratory
California Institute of Technology

- **Computational complexity of autonomous systems**
  - Equivalence classes to manage state space explosion – Not all state distinctions are useful
  - Search heuristics – Anchor near a known solution (adaptation); distance metrics to assess proximity to failure conditions
  - Behavior envelopes – Which behaviors are always safe? Guarantees that the trajectory from one safe state to another is also safe.
- **Going beyond fault protection**
  - Improved situational awareness
  - Systems that can assess risk factors during operations, understand their own behaviors, and know when to ask for help
- **Multi-agent systems and emergent behavior**
  - Separated functional modules trade design ease for run-time complexity (potential for subtle, unanticipated interactions)
  - MSL utilized control dominance protocols and well-defined interactions and information exchange
- **The human element of validation, the role of trust**
  - Beliefs about a system, decision to (provisionally) delegate authority to a system
  - Recovery of trust after a failure
  - Systems that know what they don't know
- **Validation as continuous, incremental operationalization**
  - All systems evolve
  - Flexibility to evolve taken up not just in operations concept, but in software upgrades, perhaps even design or requirements changes
  - Not unique to autonomous systems or characterization challenges – extended missions
  - Ongoing validation, punctuated by design → verify → validation cycles

Lifecycle view of validation activities

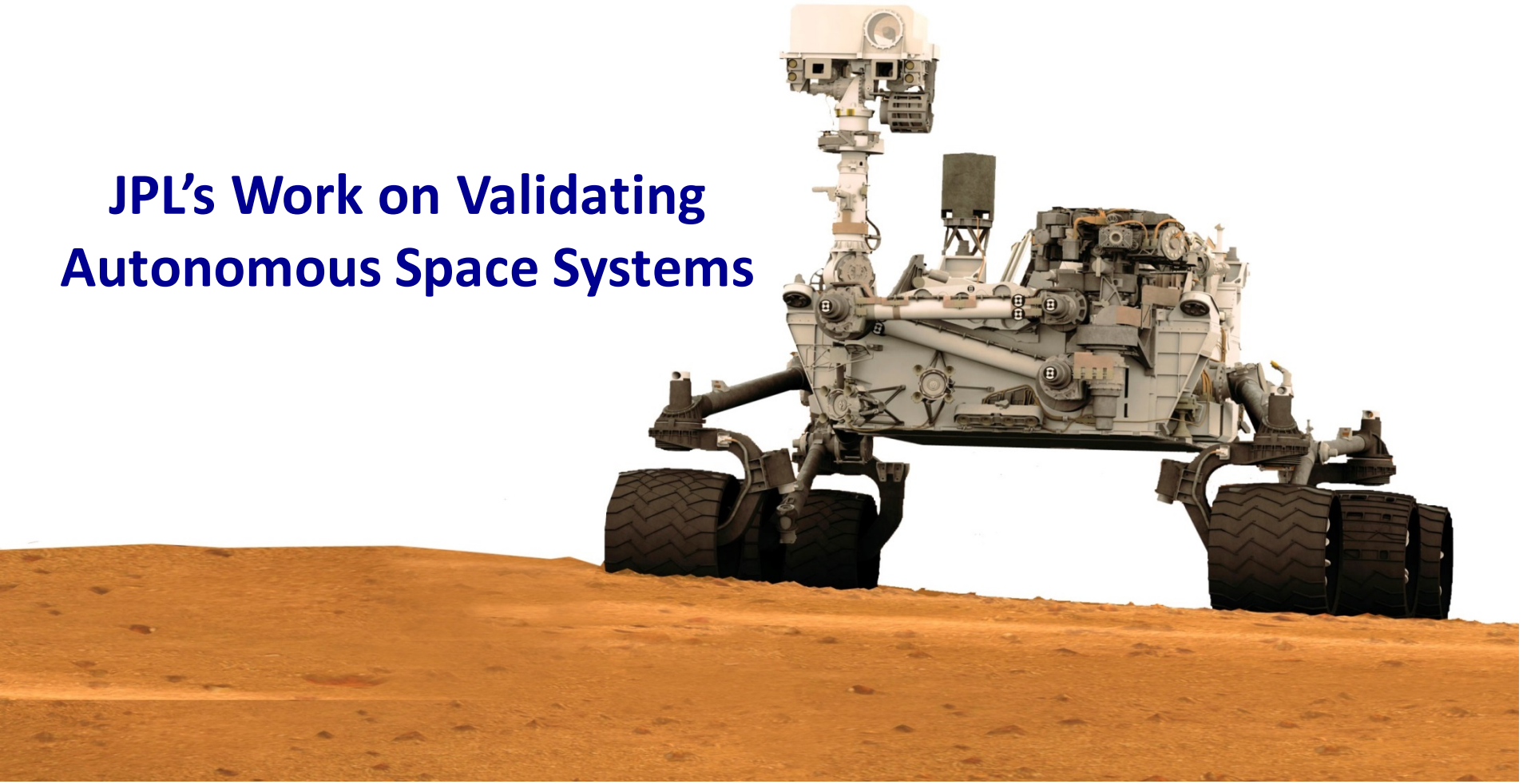
Jet Propulsion Laboratory
California Institute of Technology



UNCLASSIFIED

Jet Propulsion Laboratory
California Institute of Technology

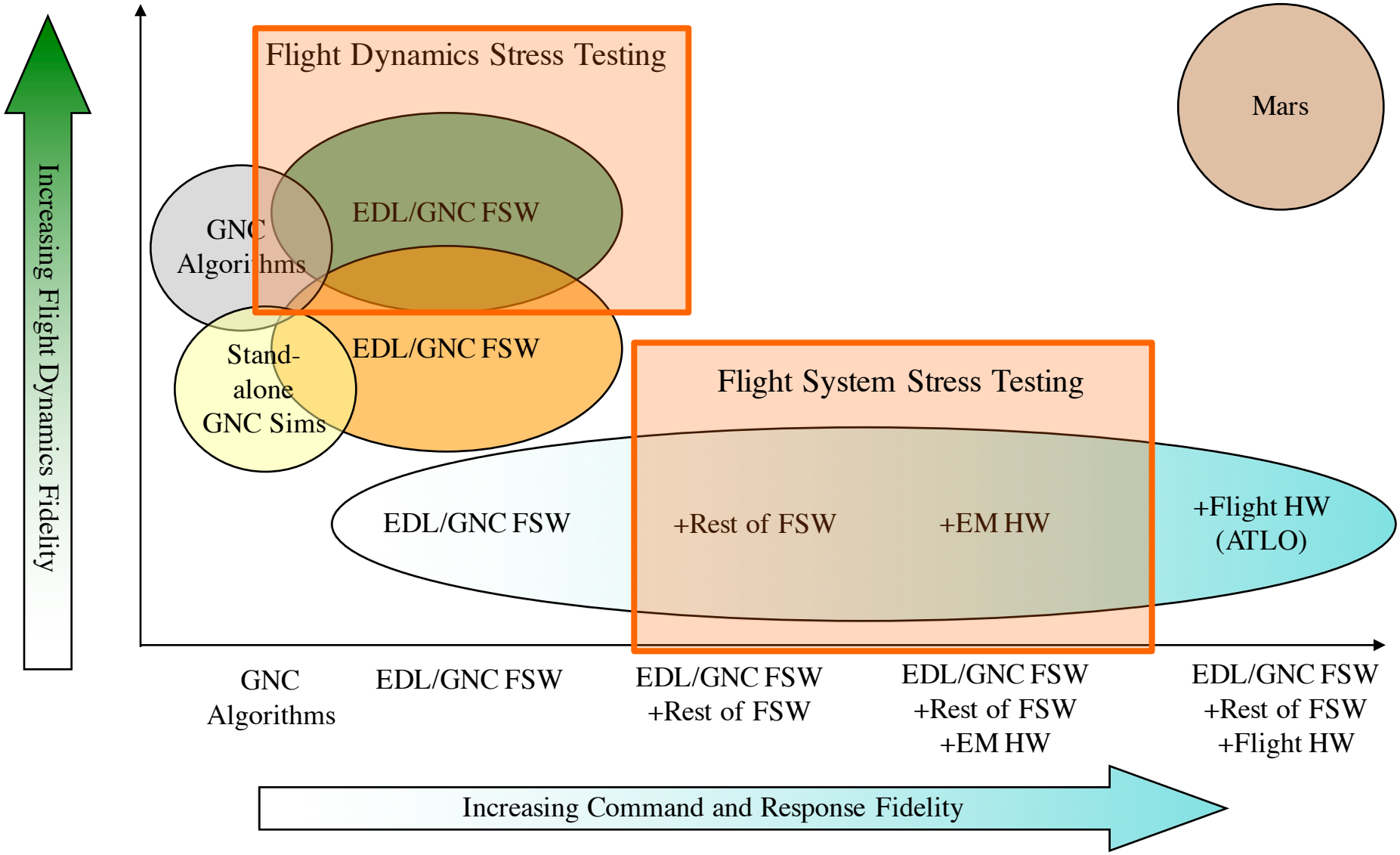
JPL's Work on Validating Autonomous Space Systems



UNCLASSIFIED

Mars Science Laboratory – V&V map

Jet Propulsion Laboratory
California Institute of Technology



Credit: A. Devereaux

Mars Science Laboratory – EDL design

Jet Propulsion Laboratory
California Institute of Technology

- Exquisite *pas de deux* between EDL Timeline actor and GNC Mode Commander actor
- EDL Timeline module
  - Executes sequences of timed events - "Anchors" – set at absolute times (relative to other Anchors) or by GNC triggers (e.g., achieving threshold velocities)
- GNC Mode Commander
  - Focused on flight dynamics modes – entry guidance, flight on parachute, powered flight, landing

UNCLASSIFIED

Credit: A. Devereaux

Focus on design phase

Jet Propulsion Laboratory
California Institute of Technology

Spot: A computer language specifically targeted at testability, verifiability and validation of complex software systems

The problem with software: *uncontrolled state space and complexity*

Why Spot is different: *Spot manages and constrains state space*

- *In Spot we discretely identify state* parameters and place them in well defined structures, noting constraints such as valid ranges and important state combinations or sequences
- *In Spot, we retain only those distinctions in state space* that are meaningful relative to mission objectives – not all state distinctions are useful
- *In Spot we tightly control* the configuration and use of memory and inter-module communication that can cause state space expansion, logic errors and other programming hazards

Benefit:

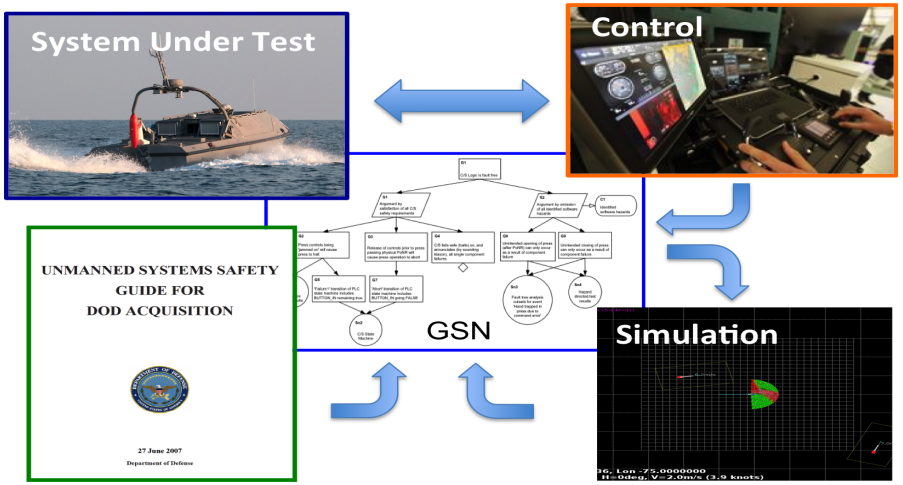
- A run time monitoring system can check system state for correctness, and an external tester such as Spin can automatically generate and apply millions of test vectors, generate models and perform analysis to verify correct operation.

Credit: R. Some

Focus on test phase

Jet Propulsion Laboratory
California Institute of Technology

Formal Model for Autonomy Assurance Case Development and Efficient Testing

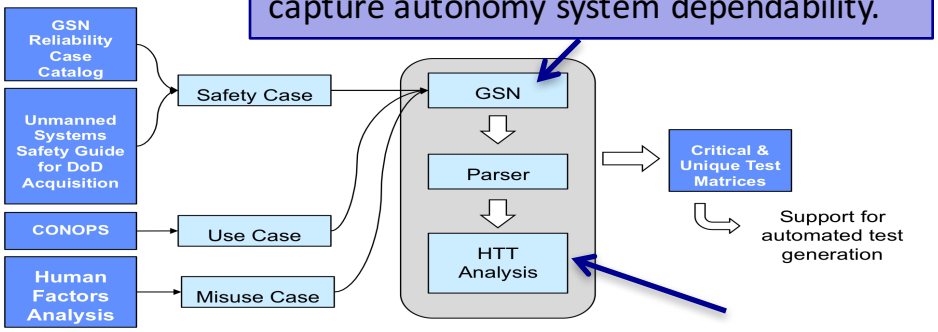


Payoff to DoD: Captures DoD autonomy safety requirements, CONOPS, and use cases all <u>within a single framework</u> for efficient V&V testing, as well as addressing regression analysis needed for future upgrades and revisions

Challenge: The large number of potential test cases needed to provide assurance guarantees for adaptive autonomous systems precludes exhaustive testing

Approach:

Goal Structuring Notation (GSN) used to capture autonomy system dependability.



Test Case (2013-2015):

Technology Transfer Agreement (TTA) with NAVSEA PMS 406:

- On-water testing of JPL-developed integrated high resolution stereo sensing and autonomous control system CARACaS (Control Architecture for Robotic Agent Command and Sensing) on the UISS (Unmanned Influence Sweep System)
- Used high throughput test (HTT) 2-factor analysis derived from the TTA reqts table
- Test cases reduced from 124,416 to 23 *cutting the test time by almost* ***4 orders of magnitude***

High Throughput Testing (HTT) multi-factor used to generate efficient number of test cases.

UNCLASSIFIED

Credit: T. Huntsberger

Jet Propulsion Laboratory
California Institute of Technology

Scenario-Based Randomized Testing

Motivation

Traditional integrated testing focuses on scripted scenarios, each exercising a single system feature
Does not usually explore *interactions* among features that lead to unexpected behaviors
Manually writing individual tests to exercise multiple features is expensive

Approach

Test engineers write "scenario skeletons" in declarative form (easy to read and maintain)
Each scenario skeleton exercises a specific function or feature by specifying
- initial state assumptions, commands for exercising function, and properties to be checked
From such a description, a test engine automatically generates large numbers of test cases

Benefits

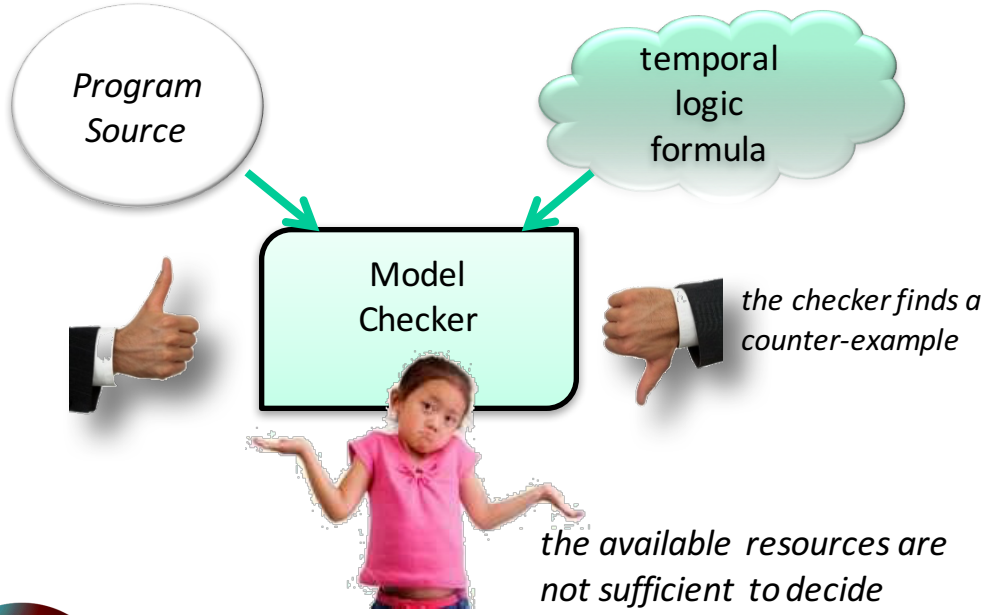
Randomization forces system into unexpected corners (not biased by human expectations)
A declarative notation makes it easier to write new tests quickly
Easy to parallelize

Credit: R. Joshi

Jet Propulsion Laboratory
California Institute of Technology

software model checking

- given a formula in linear temporal logic and a program, a model checker tries to find executions of the program that violate the formula



the Spin Model Checker, developed and maintained by JPL's Gerard Holzmann, is a popular explicit-state logic model checking tool.

It uses several strategies to deal with "state space explosion" problems.

Spin checked

LARS
NASA/JPL Laboratory for Reliable Software

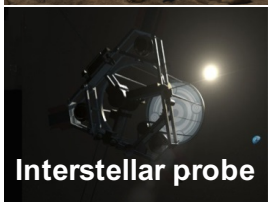
Credit: G. Holzmann

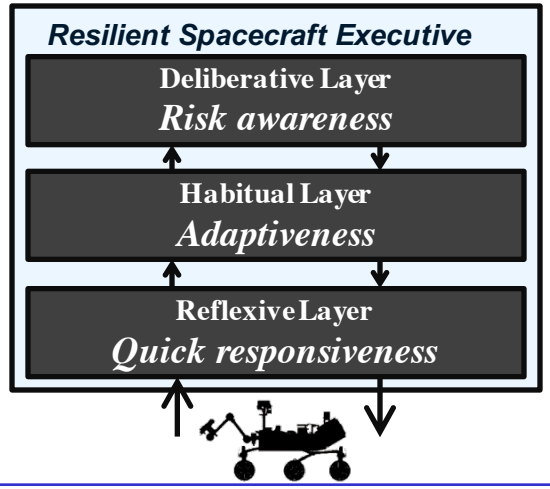
UNCLASSIFIED

Focus on operations phase

Jet Propulsion Laboratory
California Institute of Technology

Resilient Risk-Aware Autonomy for the Exploration of Uncertain and Extreme Environments





Objective: Develop a *Resilient Spacecraft Executive* to:

- adapt to component failures to allow graceful degradation
- accommodate environments, science observations, and spacecraft capabilities that are not fully known in advance
- make risk-aware decisions without waiting for slow ground-based reactions

Why this is important to NASA and JPL:

- Enables robotic explorations of harsh, remote, and inaccessible destinations
- Reduces operational risk and associated cost

FY15: Design and develop core algorithms of RSE; develop formal behavior models; validate algorithms through small-scale demo using simulation, rover testbed in Mars Yard, and AUV submarine.
FY16: Integrate algorithms and behavior models; deploy RSE on simulator/hardware for Venus lander and/or Mars rover scenarios.

JPL Team

Dr. Mitch Ingham
Dr. Hiro Ono
Dr. Tara Estlin
Dr. Leslie Tamppari
(JPL)

KISS-funded collaborators

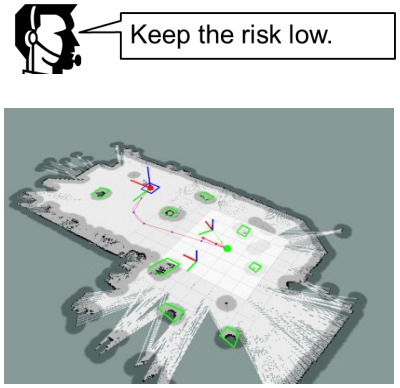
Prof. Richard Murray
(Caltech)

Prof. Brian Williams
(MIT)

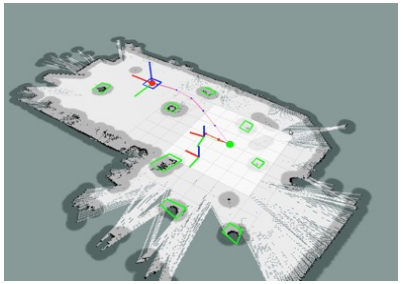
Dr. Richard Camilli
(Woods-Hole O.I.)

Overview of Approach and Early Results:

System adapts its behavior depending on acceptable level of risk



Low Risk



High Risk

UNCLASSIFIED

Risk-aware autonomy

Jet Propulsion Laboratory
California Institute of Technology

Major findings

Jet Propulsion Laboratory
California Institute of Technology

- For missions requiring characterization of a partly unknown environment, validation activities must continue into operations
- Formal modeling and analysis techniques in support of validation should be applied across the full lifecycle
- Current validation practices must be generalized to an ongoing process, punctuated by design → verify → validate cycles

Validation as continuous, incremental operationalization

NASA

CALIFORNIA INSTITUTE OF TECHNOLOGY

1891

JPL