



# Achieving Control & Interoperability through Unified Model-based Systems and Software Engineering

Robert Rasmussen, Michel Ingham, and Daniel Dvorak  
Jet Propulsion Laboratory  
California Institute of Technology

AIAA Infotech@Aerospace Conference  
Arlington, Virginia  
September 27, 2005



# Outline

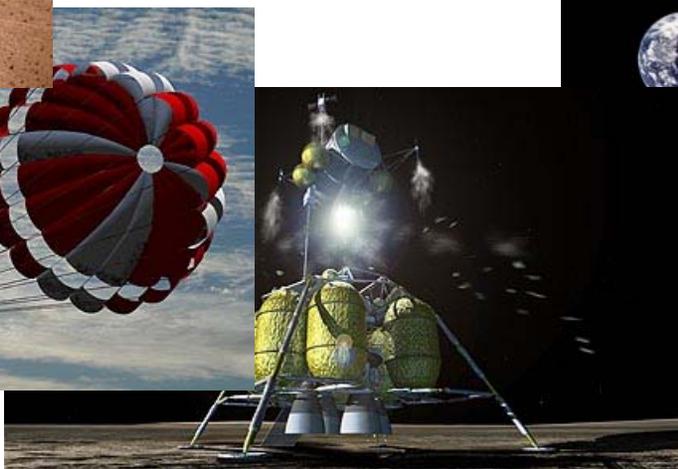
- ESMD's Challenge: Control & Interoperation of Complex Systems
- Fleshing out the Problem:
  - The Control Challenge
  - The Interoperation Challenge
- A Framework for Solutions
- Instantiating the Framework
  - The State Analysis systems engineering methodology
  - The Mission Data System software architecture
- Next Steps



# NASA's Exploration Systems Mission Directorate



Results of the Exploration Systems Architecture Study are out...





# ESMD's Challenge: Control & Interoperation of Complex Systems



- Capability
- Safety
- Operability
- Affordability



# ESMD's Challenge: Control & Interoperation of Complex Systems



- Capability
- Safety
- Operability
- Affordability

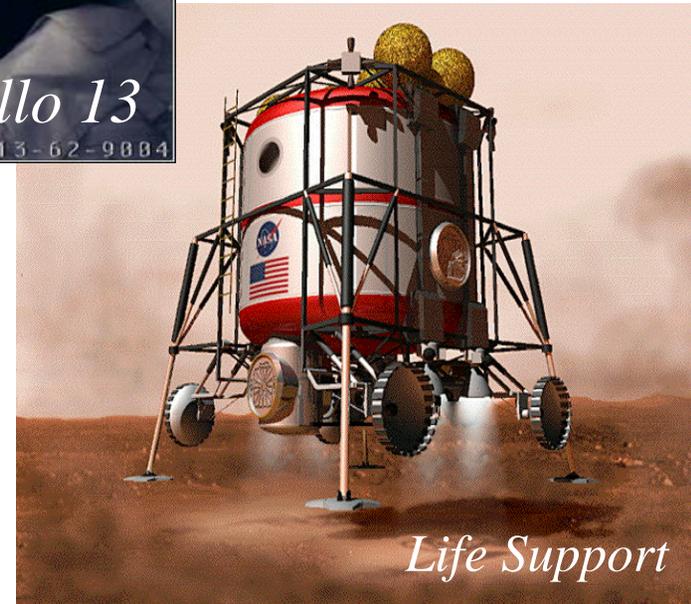




# ESMD's Challenge: Control & Interoperation of Complex Systems



- Capability
- Safety
- Operability
- Affordability

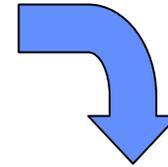




# ESMD's Challenge: Control & Interoperation of Complex Systems



- Capability
- Safety
- Operability
- Affordability





# ESMD's Challenge: Control & Interoperation of Complex Systems

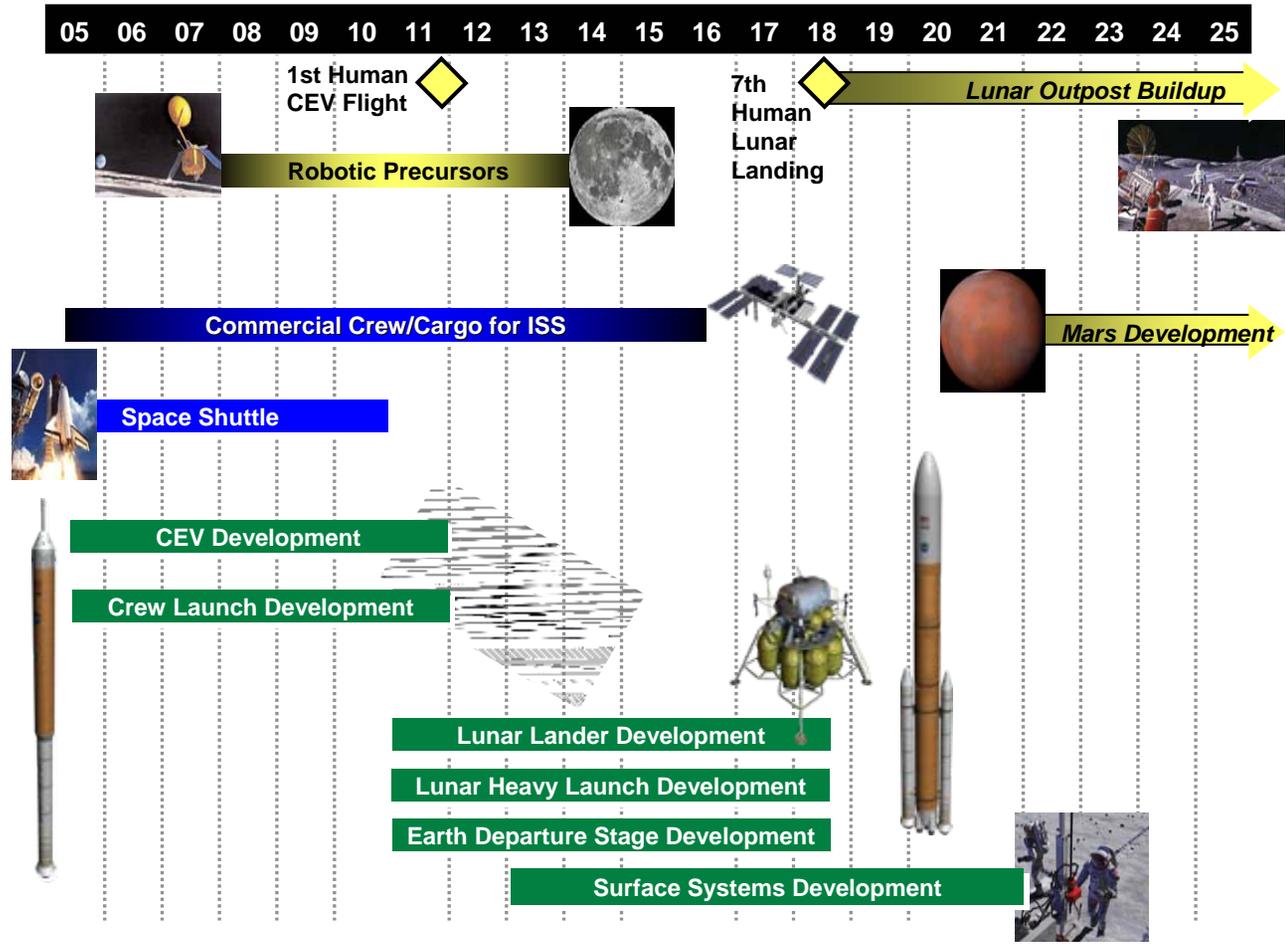


● Capability

● Safety

● Operability

● Affordability

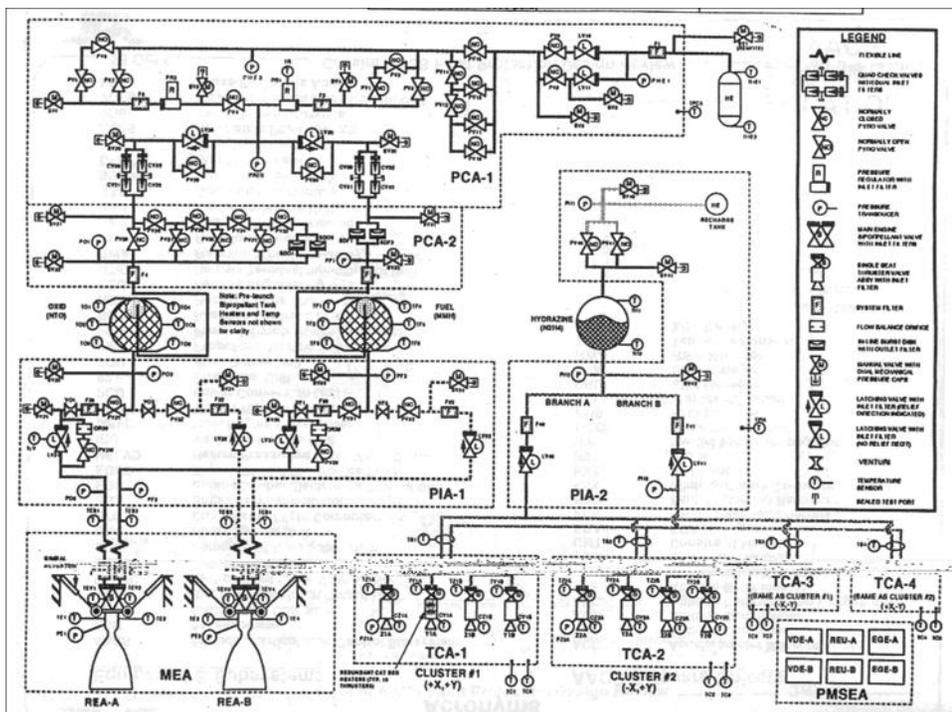




# The Control Challenge

- Managing large collection of components that are tightly coupled
  - Through shared resources, environmental interactions, design compromises or errors, degradation and failure modes
  - Habitual methods are already strained
  - New exploration systems will push the envelope

## Cassini Propulsion System

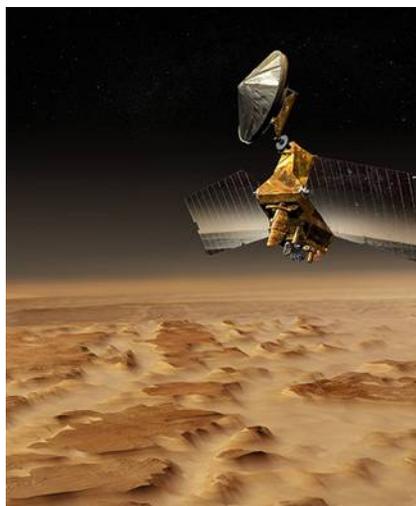


## Mars Polar Lander

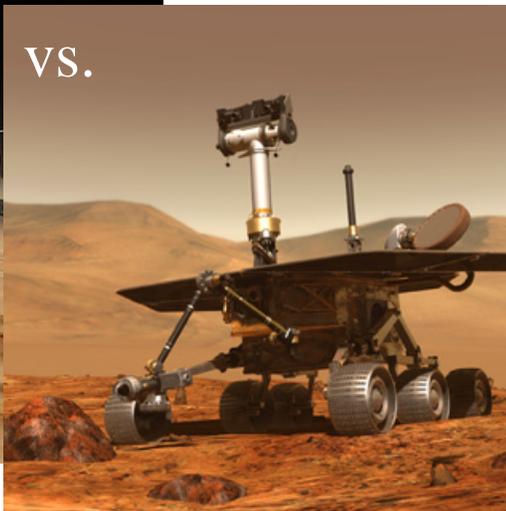


# The Control Challenge

- Managing large collection of components that are tightly coupled
  - Through shared resources, environmental interactions, design compromises or errors, degradation and failure modes
  - Habitual methods are already strained
  - New exploration systems will push the envelope
- Enabling operation in uncertain or remote environments
  - Interrupted communications, light time delays
  - Robots will be pressed to accelerate activities in support of human operations
  - To date, serious excursions into this operational model have been avoided



VS.



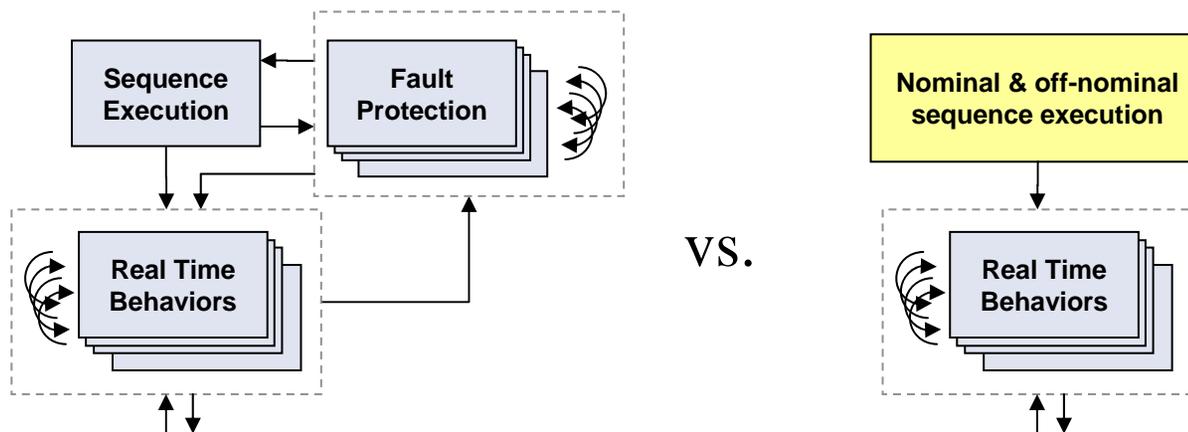
VS.





# The Control Challenge

- Managing large collection of components that are tightly coupled
  - Through shared resources, environmental interactions, design compromises or errors, degradation and failure modes
  - Habitual methods are already strained
  - New exploration systems will push the envelope
- Enabling operation in uncertain or remote environments
  - Interrupted communications, light time delays
  - Robots will be pressed to accelerate activities in support of human operations
  - To date, serious excursions into this operational model have been avoided
- Responding appropriately to anomalies
  - Integrated fault management
  - Automated or human-in-the-loop





# The Control Challenge

- Managing large collection of components that are tightly coupled
  - Through shared resources, environmental interactions, design compromises or errors, degradation and failure modes
  - Habitual methods are already strained
  - New exploration systems will push the envelope
- Enabling operation in uncertain or remote environments
  - Interrupted communications, light time delays
  - Robots will be pressed to accelerate activities in support of human operations
  - To date, serious excursions into this operational model have been avoided
- Responding appropriately to anomalies
  - Integrated fault management
  - Automated or human-in-the-loop
- Realizing affordable operations costs
  - Harness automation
  - Design for operability



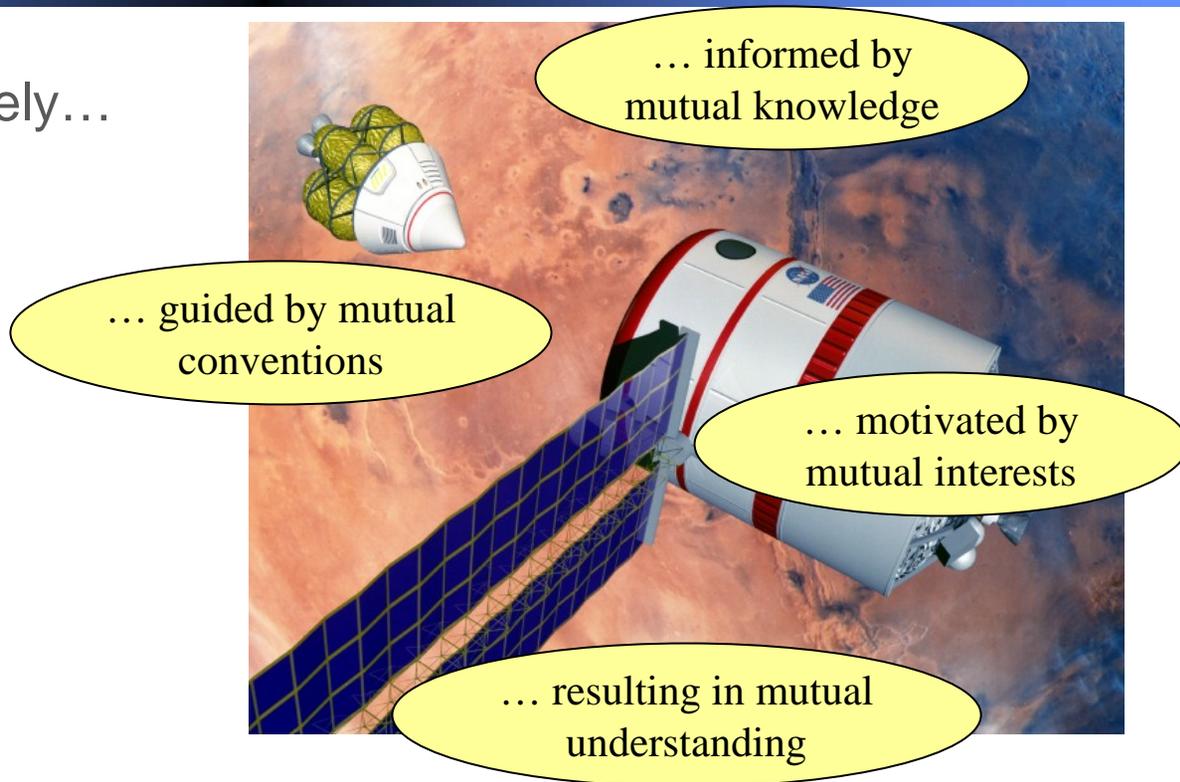
# The Control Challenge

- Managing large collection of components that are tightly coupled
  - Through shared resources, environmental interactions, design compromises or errors, degradation and failure modes
  - Habitual methods are already strained
  - New exploration systems will push the envelope
- Enabling operation in uncertain or remote environments
  - Interrupted communications, light time delays
  - Robots will be pressed to accelerate activities in support of human operations
  - To date, serious excursions into this operational model have been avoided
- Responding appropriately to anomalies
  - Integrated fault management
  - Automated or human-in-the-loop
- Realizing affordable operations costs
  - Harness automation
  - Design for operability
- Assuring system correctness and reliability
  - Close gap between systems and software engineering
  - V&V



# The Interoperation Challenge

- Communicating effectively...



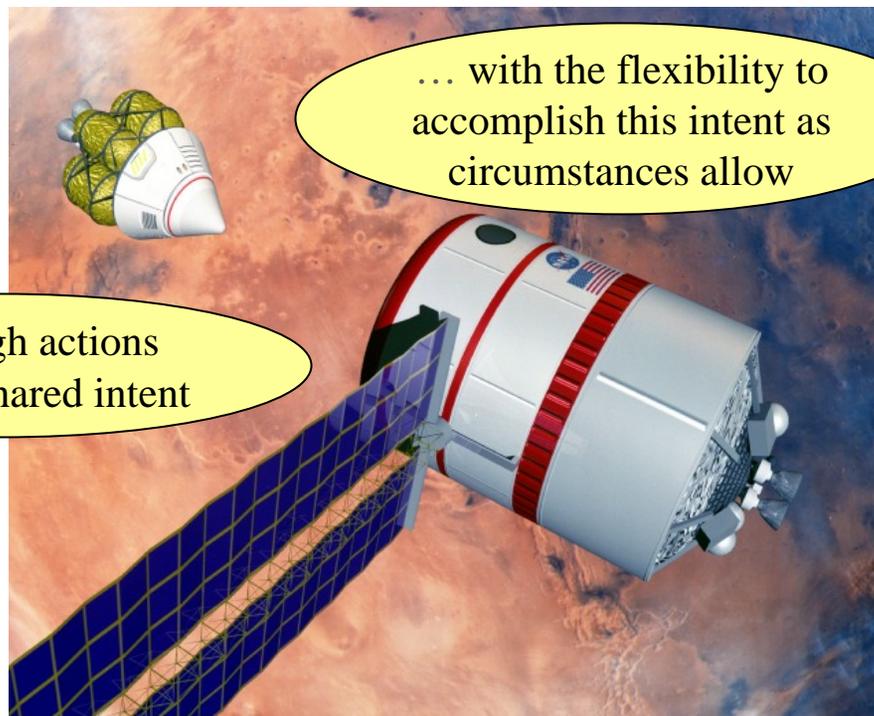


# The Interoperation Challenge

- Communicating effectively
- Collaborating with confidence...

... through actions  
based on shared intent

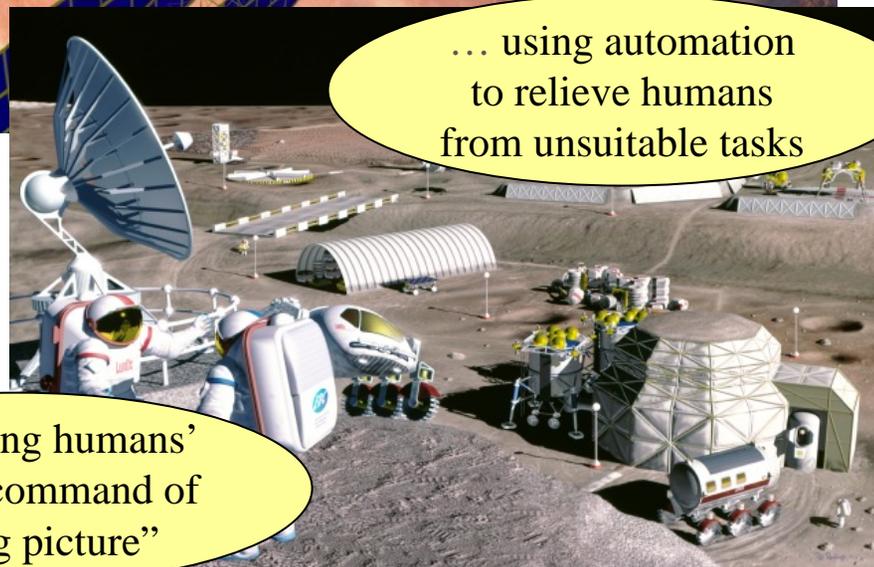
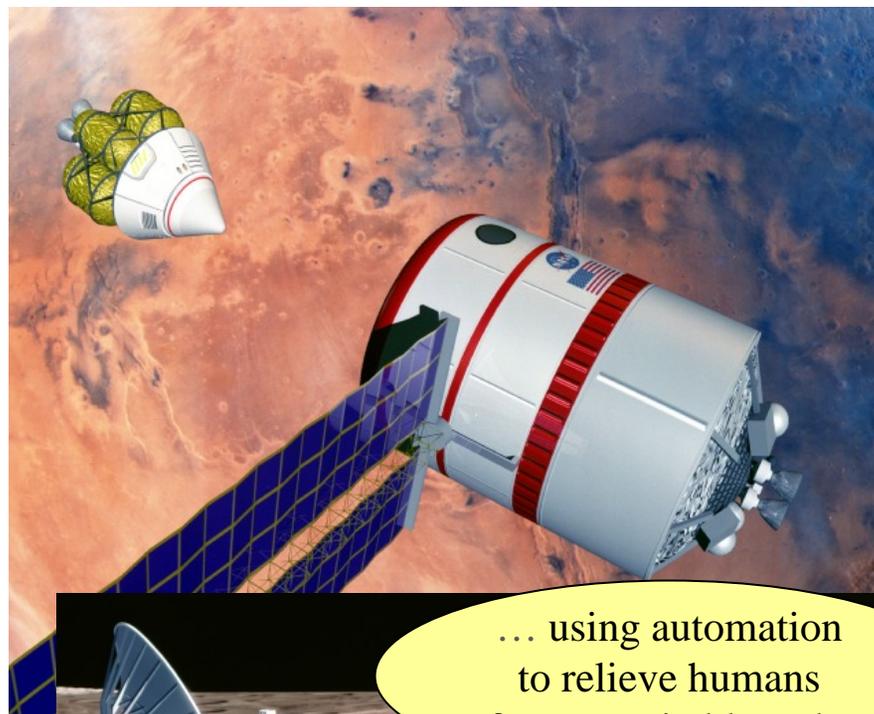
... with the flexibility to  
accomplish this intent as  
circumstances allow





# The Interoperation Challenge

- Communicating effectively
- Collaborating with confidence
- Coordinating humans and robots...



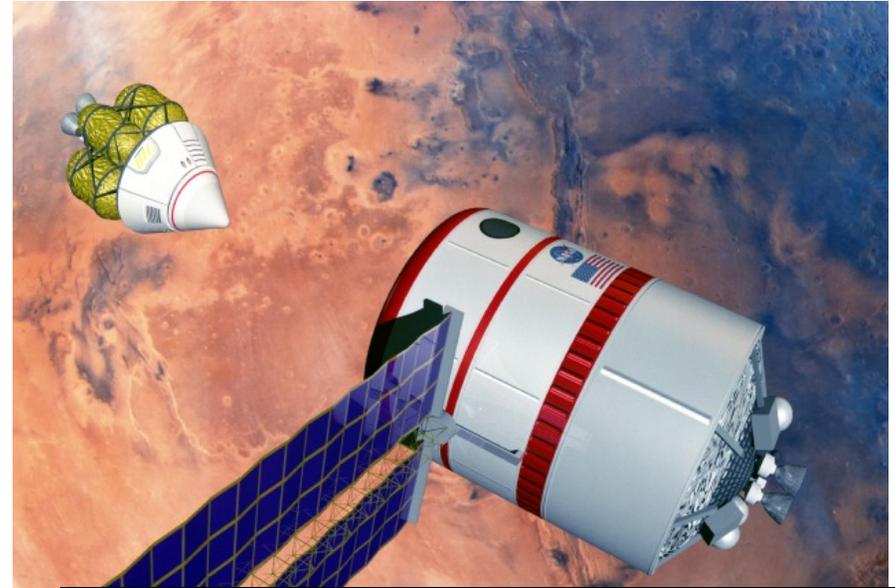
... using automation  
to relieve humans  
from unsuitable tasks

... honoring humans'  
superior command of  
the "big picture"



# The Interoperation Challenge

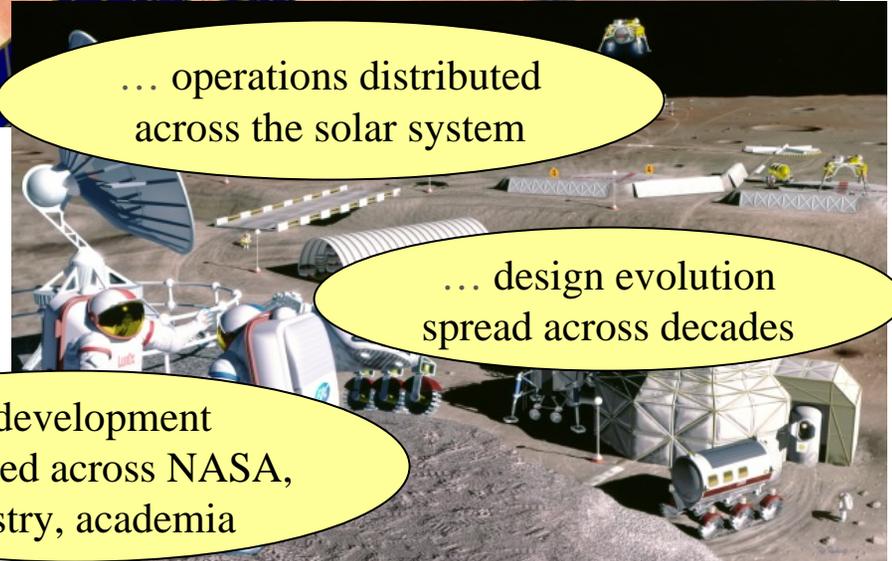
- Communicating effectively
- Collaborating with confidence
- Coordinating humans and robots
- Managing a large, distributed engineering effort...



... operations distributed  
across the solar system

... design evolution  
spread across decades

... development  
distributed across NASA,  
industry, academia



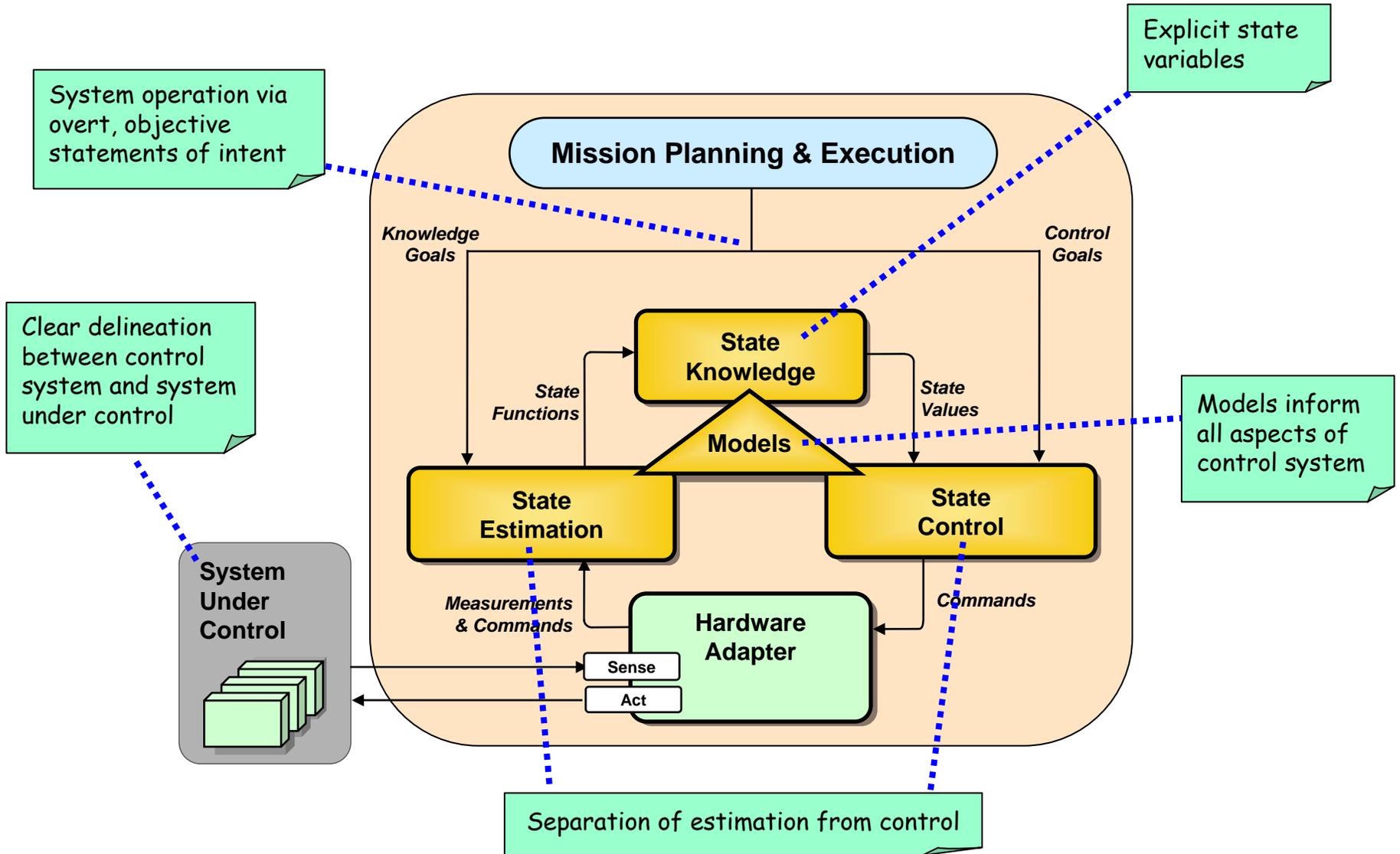


# A Framework for Solutions

- No single solution to all of these challenges
- Objective: devise a unifying framework and approach to guide the effort
- Essential elements:
  - State- and model-based control architecture
  - Unified systems and software engineering
  - Design for integration, reuse and evolution
  - Processes to assure quality and timely deliveries
- JPL's Mission Data System provides an instance of such a framework...

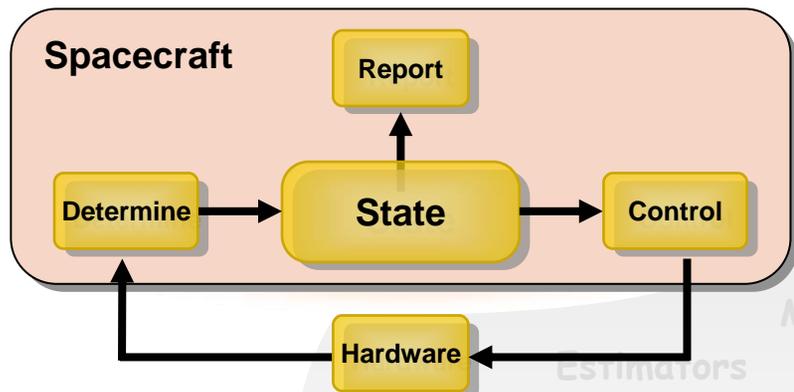


# Principled Architecture



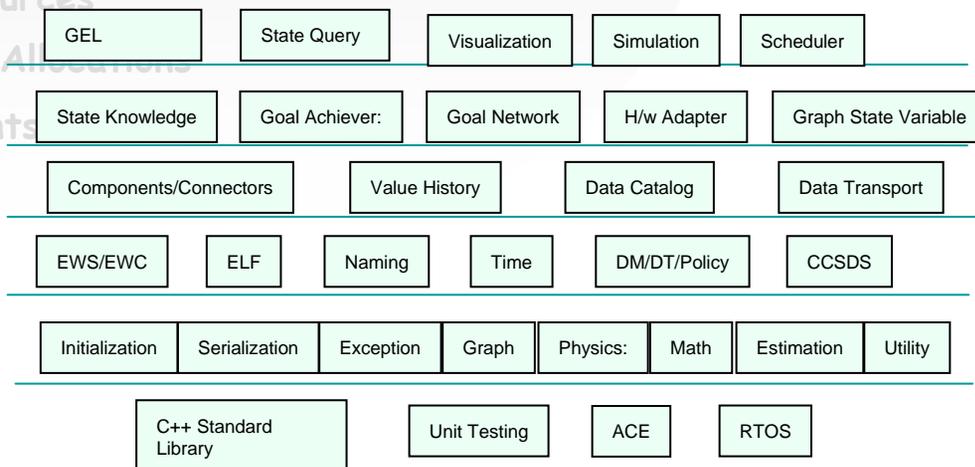


# Bridging the Gap between Systems & Software Engineering



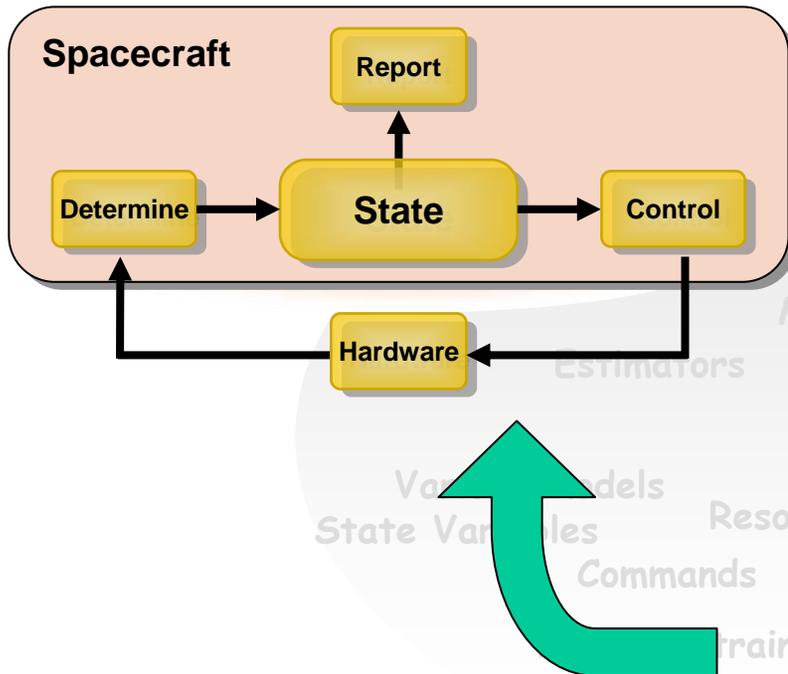
**State Analysis:  
Model-based Requirements  
Map Directly to Software**

**Common Vocabulary  
Reduces Errors of Translation**

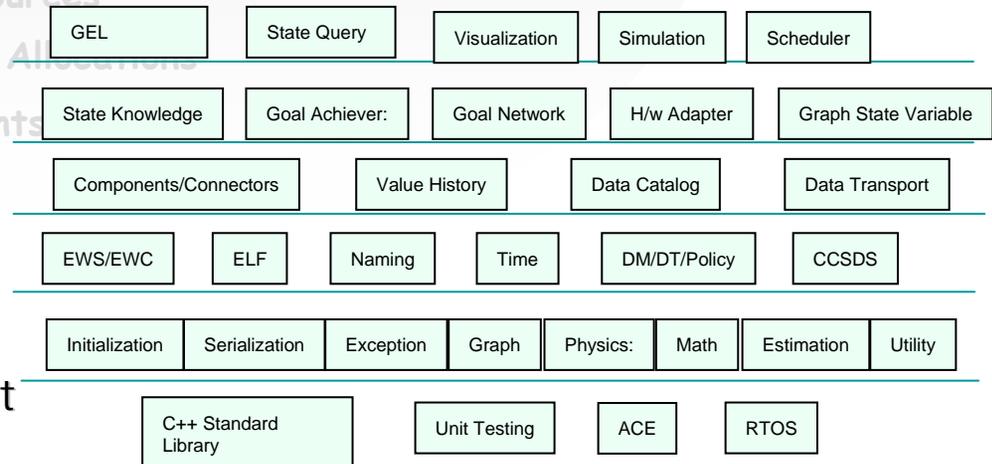




# Bridging the Gap between Systems & Software Engineering



Embedded control systems developed as adaptations of reusable framework software



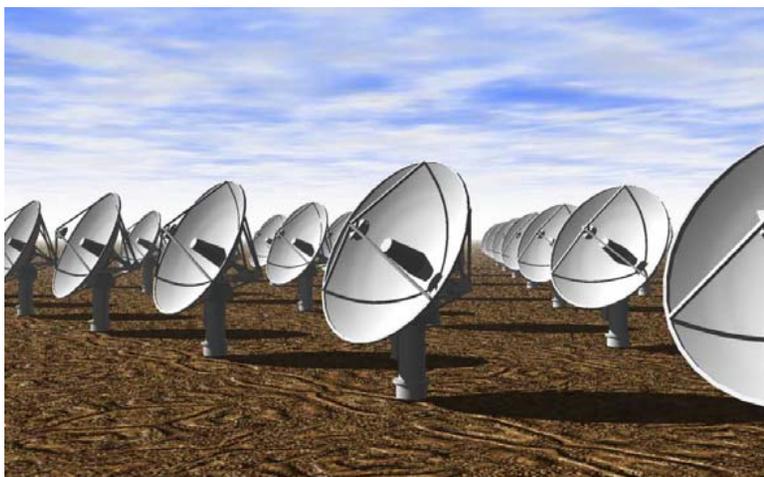
Supports rigorous software engineering practices

- Iterative incremental development
- Performance & process metrics
- Workflow & CM tools for full lifecycle
- Straightforward costing

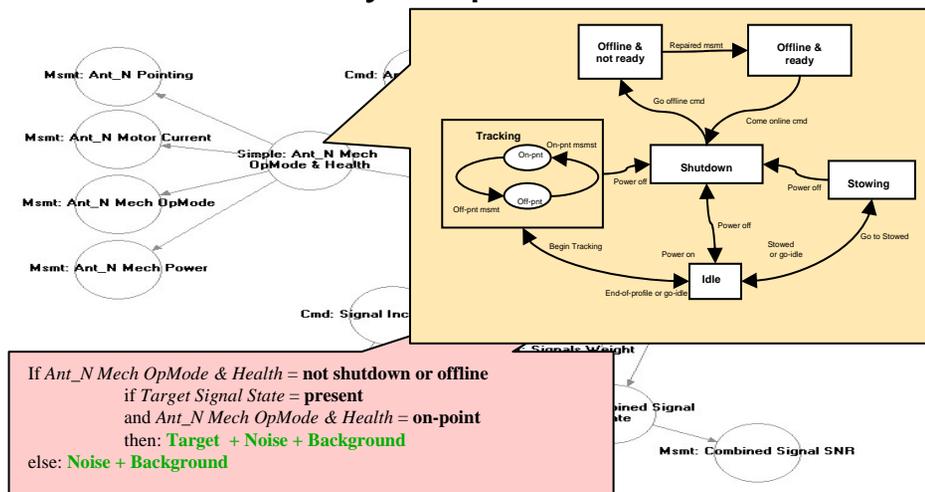


# Overview of State Analysis

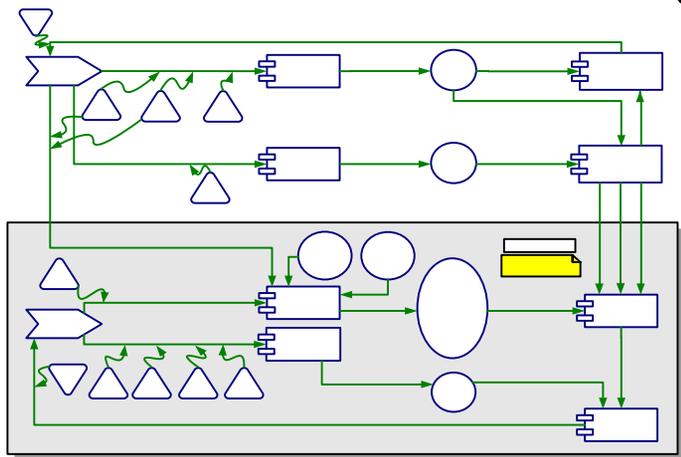
## 1. System to be controlled



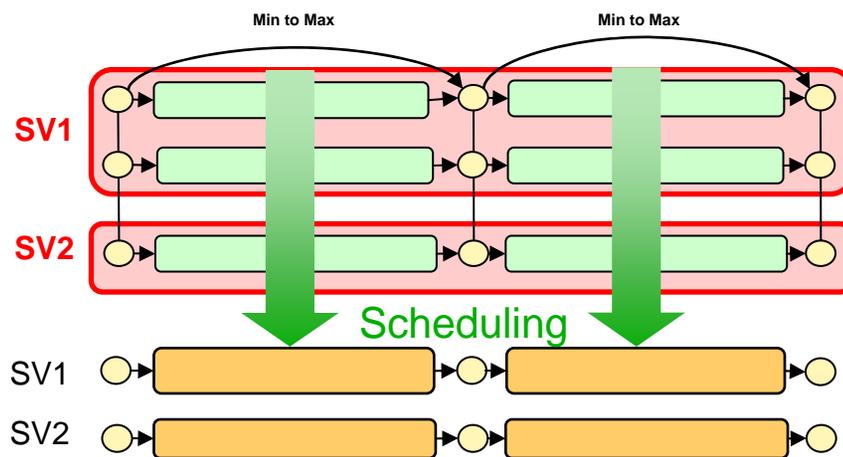
## 2. State Analysis produces model



## 3. Model informs software design



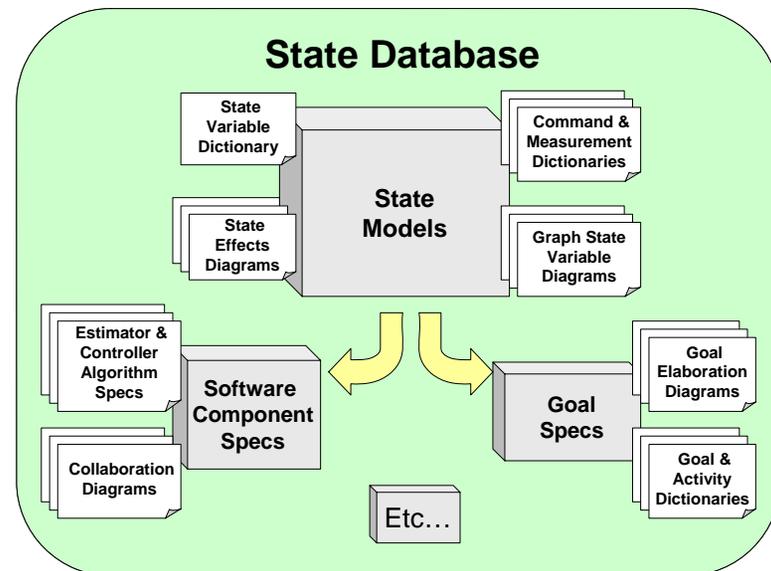
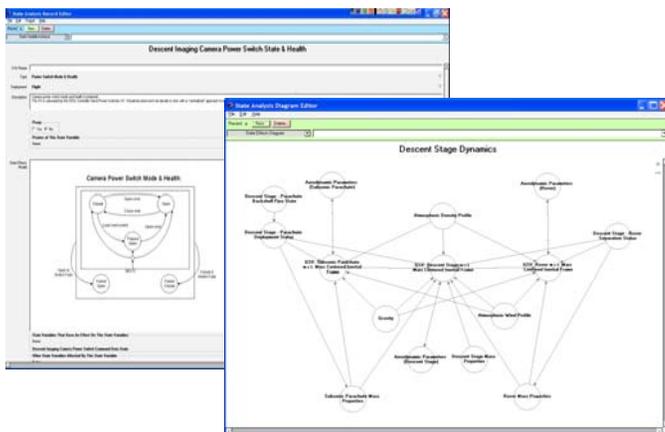
## 4. Model informs operations





# MDS Adaptations & Tools

- Under development at JPL since 1998
- Prototypes:
  - Rocky 7 & 8 rover testbeds
  - Mars powered descent
  - Deep Space Network Array
- Tools:
  - State database and client
  - Report generation
  - Software analysis and code generation
  - Cost model





# Proposed Approach

- Use this type of framework as a springboard for development of the architecture needed for ESMD
- Establish interoperability standards group, define standard across systems [FY'06]
- Field prototypes of ESMD-relevant systems for demonstration and evaluation (Analog Mission Testbeds) [FY'06-'11]
- Produce formal specification from interoperability standard [FY'08]
- Bring candidate technologies conforming to standard to the point of full deployment readiness [FY'12; sooner if CEV must be compliant]
- Parallel effort among NASA, industry, academia
- Interim realignment exercises across participants
- Accommodate appropriate legacy systems
- Show that both flight and ground can be addressed effectively
- Demonstrate full life-cycle development, and significant re-use



BACKUP SLIDE



# Platform for Technology Infusion

- Hazard avoidance algorithm
  - Gestalt (used on MER)
- GN&C Extended Kalman Filter framework
  - Specialized for MSL EDL
- Deliberative planning and reactive execution
  - CASPER algorithms (used on EO1)
- Software architecture techniques
  - CMU Studio Project
- RT Java Implementation
  - Golden Gate Project (SUN/CMU/JPL)
- Platform for Integrated System Health Management and Model-based execution technologies
  - MIT Titan mode estimation & reconfiguration