System Engineering of Autonomous Space Vehicles

Michael D. Watson, Ph.D., NASA MSFC
System Engineering Management Office

Stephen B. Johnson, Ph.D., Dependable System Technologies, LLC, and
University of Colorado, Colorado Springs

Luis Trevino, Ph.D., ISHM and Automation Branch, Jacobs Technology

Outline

- System Engineering of Autonomous Systems
- Spacecraft Systems Overview
- Spacecraft System State Variables
- Autonomy Stack
- Candidate Autonomous Algorithms for Spacecraft Systems
- Autonomous Algorithm Integration
- Summary

System Engineering of Autonomous Systems

- System Engineering seeks to obtain Elegant Systems which function
  - Effectively in their intended application and environment
  - Most efficiently as compared to options fitting the system context
  - Robustly in application and operation
  - Avoiding Unintended Consequences

System Engineering of Autonomous Systems

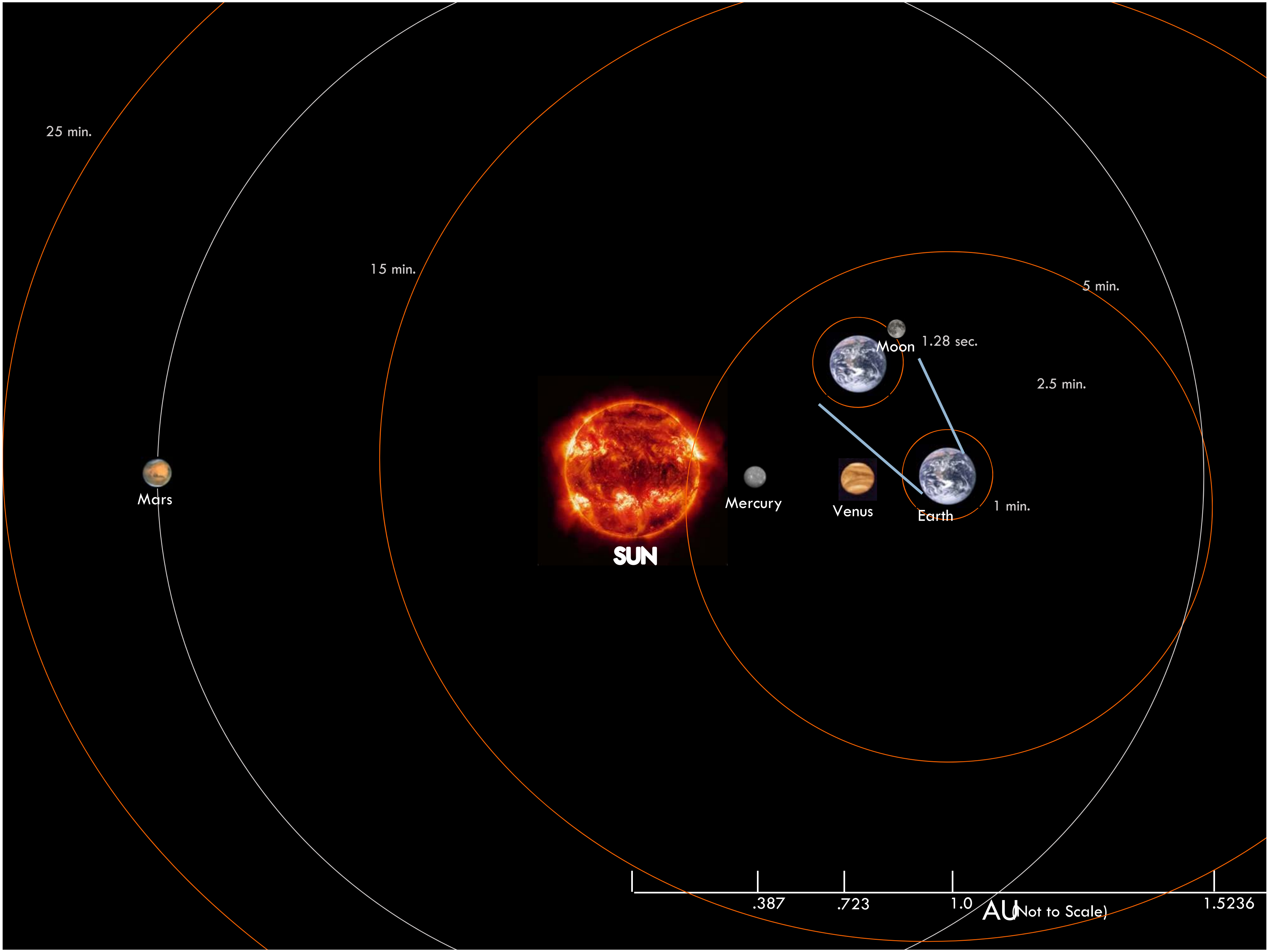
- Elegant System Engineering requires
  - Understanding the Mission Context
    - System Applications
    - System Environments (operational, test, abort, etc.)
  - Understanding the Physics of the System
    - System Interactions with themselves and with their environments are governed by their physics
    - Information Theory provides linkages between physical state representations and actual physical states
  - Managing the organizational influences on system design and the system context influences on the organization
  - Understanding Policy and Law Constraints
    - National Space Policy
    - International Space Treaties and agreements
      - Space Debris, Contamination, Property

Autonomy in Context: What and Why?

- Spacecraft and Surface System Autonomy is the enabling capability for Human Exploration beyond Lunar Sortie Missions
  - Autonomy is necessary for complex system operations
  - Timely response to unplanned or unscheduled events
- Propulsion, Structure, Thermal Conditioning, ECLSS, Electrical Power, Avionics, RCS, Communication are all understood sufficiently to allow engineered solutions to be reliably produced
  - Challenges do exist in terms of Space Environmental Effects, efficiency, compact size
    - Radiation Hardened computer processors needed
  - Physics and demonstrated solutions are available from which to engineer a vehicle
- Operations are sufficiently understood for terrestrial based execution, not on-board execution
  - Manual operations provide a rich knowledge base of planning and execution processes
  - Manual operations have a generic template (derived from Apollo/Saturn) applied uniquely to each spacecraft
  - Terrestrial based manual operations will not support operations beyond 5 light minutes from Earth
- Autonomous Operations are essential to Human Exploration of the Solar System

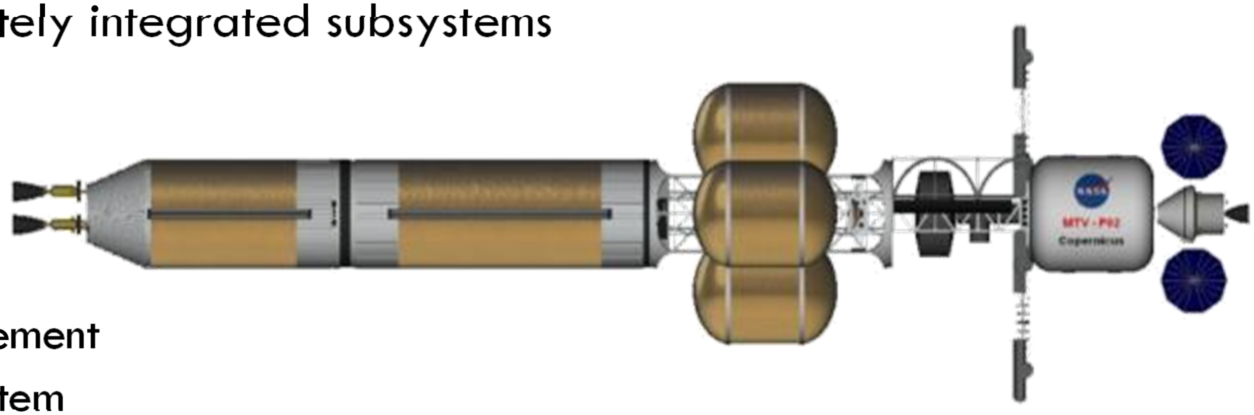
Operations Concept Drivers

- Small Crew Size (4-6)
  - 1 crew member per shift available for vehicle operations
  - Limited systems experts
- Complex Systems
  - Nuclear Power and Propulsion Systems
  - Life Support and Environmental Protection
  - USN Attack Submarines are similar complexity systems but have 134 crew members
  - ~525 high level functions to manage an interplanetary crewed spacecraft.
- Abort Scenarios
  - Unambiguous determination
  - Extremely low latency
  - Fully autonomous/automated (crew incapacitated conditions)
  - Vehicle reconfiguration necessary
- Long Communication Latency/Blockages
  - 15 minutes one way, 30 minutes round trip to Mars
    - Ground based intelligence not responsive to maintain crew safety
  - 1 hour blockage by Moon each Lunar orbit
- Harsh Environment
  - Solar flare radiation
  - Meteorites


25 min.
15 min.
5 min.
Moon
1.28 sec.
2.5 min.
Mars
SUN
Mercury
Venus
Earth
1 min.
.387
.723
1.0
AU
(Not to Scale)
1.5236

Spacecraft Systems Overview

- Beyond Earth Orbit (BEO) crew transport vehicle are comprised of several unique and intricately integrated subsystems
  - Propulsion
  - Structure
  - Electrical Power
  - Avionics
  - Thermal Management
  - Flight control system
  - Communication and Tracking
  - Vehicle Management (Guidance, Navigation and Control (GN&C) and Mission and Fault Management (M&FM))
  - Environmental Control and Life Support Systems (ECLSS)

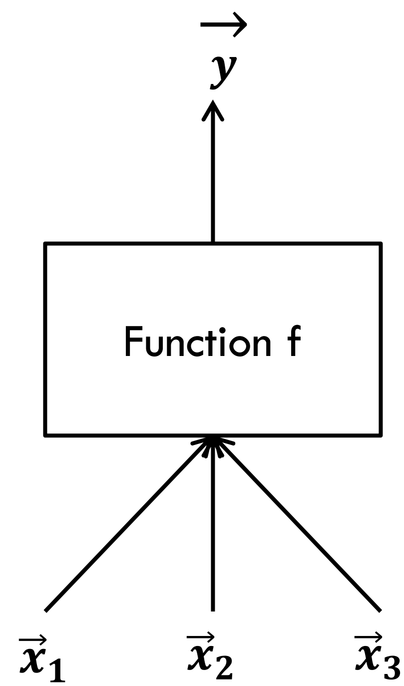


- Each of these subsystems are driven by unique physics and information theory relationships
- Control Theory governs the control of each subsystem both independently and at the vehicle level

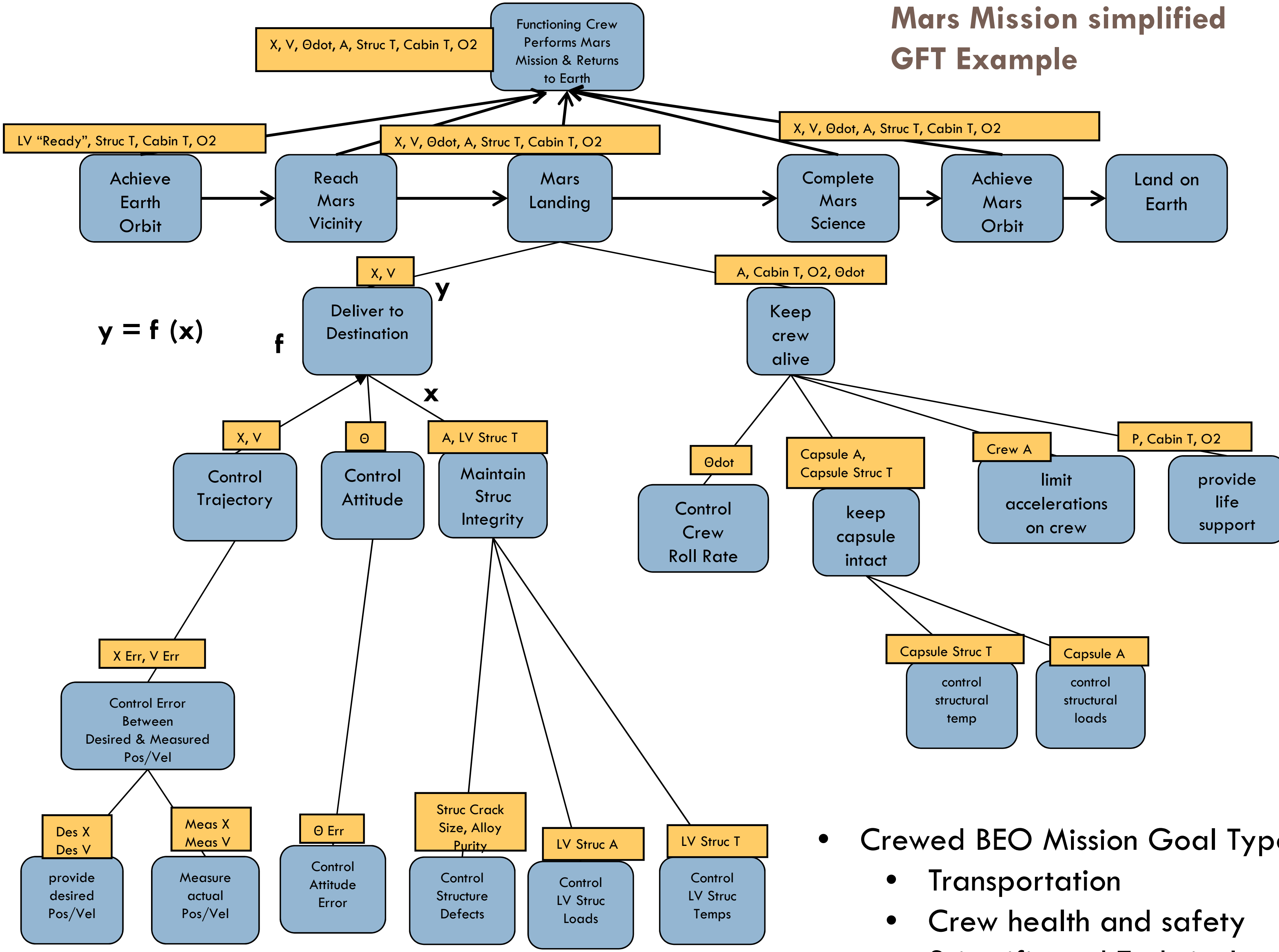
State Variable Methodology

- Goal/Function Tree
  - State Variable to define System Performance
    - State variables are defined as inputs and outputs to functions: y=f(x)
      - x = inputs to the functions f
      - f transforms the inputs into the outputs y
    - Goals = Requirements => define intended range of the output state variables y
    - Failure = state (value) of output state variable y is out of intended range
    - State variables enforce strong connection of the functional decomposition to the system's physical laws and causation
    - The state variables are the connection between function and design—exist in both function and design representations
  - Allows system to be analyzed in each mission phase and goals which can have different ranges and values for each state variable
    - Allowed leak rates vary inversely with time from Earth Return date

$$R_l \leq \vec{y} \leq R_h \rightarrow G$$



Mars Mission simplified GFT Example



- Crewed BEO Mission Goal Types
  - Transportation
  - Crew health and safety
  - Scientific and Technical

Transportation Goals

- Position, Velocity, Acceleration
- Earth Departure, Mars Departure
  - Propulsion System
  - Flight Control System
- Interplanetary Coast
  - Propulsion System
  - Flight Control System
- Planetary Orbital Insertion
  - Propulsive
  - Aero Braking
- Surface Descent
  - Propulsive
  - Aero Surfaces
- Planetary Mobility
  - Drive force
  - Control System

Crew Health and Safety Goals

- Provides link between human health and System Performance
  - Biological
  - Psychological
- Biological State Variables are linked directly with System State Variables
  - Biological
    - Heart rate
    - Respiration rate
    - Food intake
    - Water intake
    - Solid and Liquid waste production rate
  - Spacecraft Systems
    - Breathable air (oxygen concentration, carbon dioxide concentration, atmospheric pressure)
      - Oxygen can be stored as LOX and converted to gas as needed
    - Drinkable water (mass)
    - Consumable food (mass)
    - Solid and Liquid waste processing/disposal (mass)
    - Vehicle acceleration rates (linear and rotational accelerations)
    - Crew Cabin/Suit temperature (temperature and humidity)
    - Activity (work and exercise) and sleep times (hours or minutes / crew day)
    - Communication System (family communications (email, video, audio), entertainment, etc.)
- Ranges vary with mission phases

Science and Technology Goals

- Information Return
  - Communication systems
    - Transmission rates
      - radiated power
      - signal strength
      - beam width
- Sample Return
  - Containment System (mass, pressure, leakage rate)
  - Samples (mass)

Autonomy Stack

- Autonomy must operate consistent with the physical control laws of the vehicle systems
- Multiple subsystems exist within the vehicle
  - Management algorithms must match subsystem physical control laws
- Vehicle level integration is a unique set of relationships dependent on the subsystem types chosen
  - Type of Propulsion
  - Type of Flight Control System(s)
  - Type of ECLSS
  - Type of Electrical Power Generation
  - Etc.

Autonomy Stack

- Vehicle Autonomy has 5 distinct functions
  - Control
  - Monitoring (sensing)
  - Performance Determination
  - Diagnostics
  - Prognostics

FDIR

ISHM

Control System

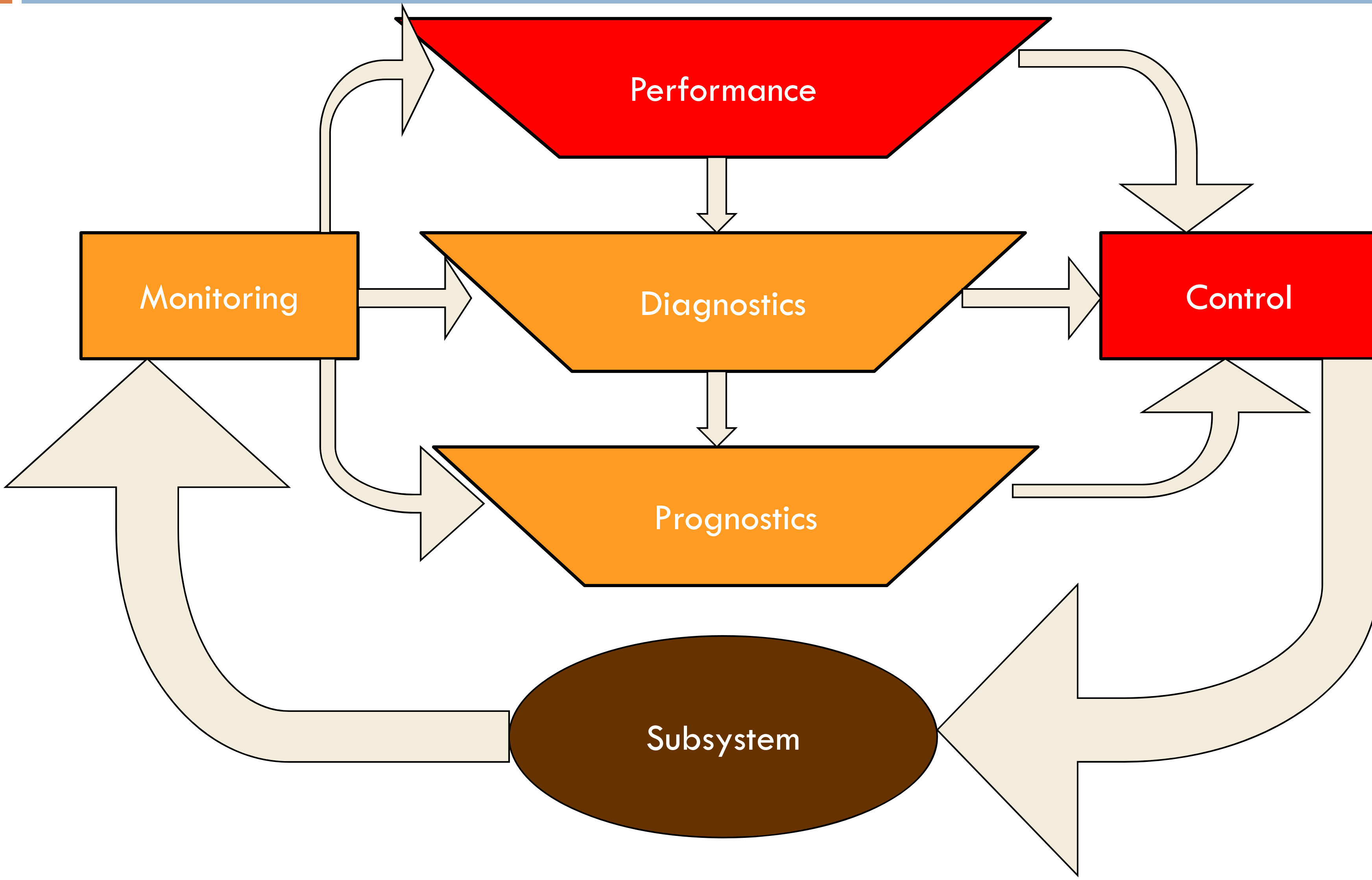
- Subsystems Autonomy has the same 5 distinct functions
  - Control
  - Monitoring (sensing)
  - Performance Determination
  - Diagnostics
  - Prognostics

FDIR

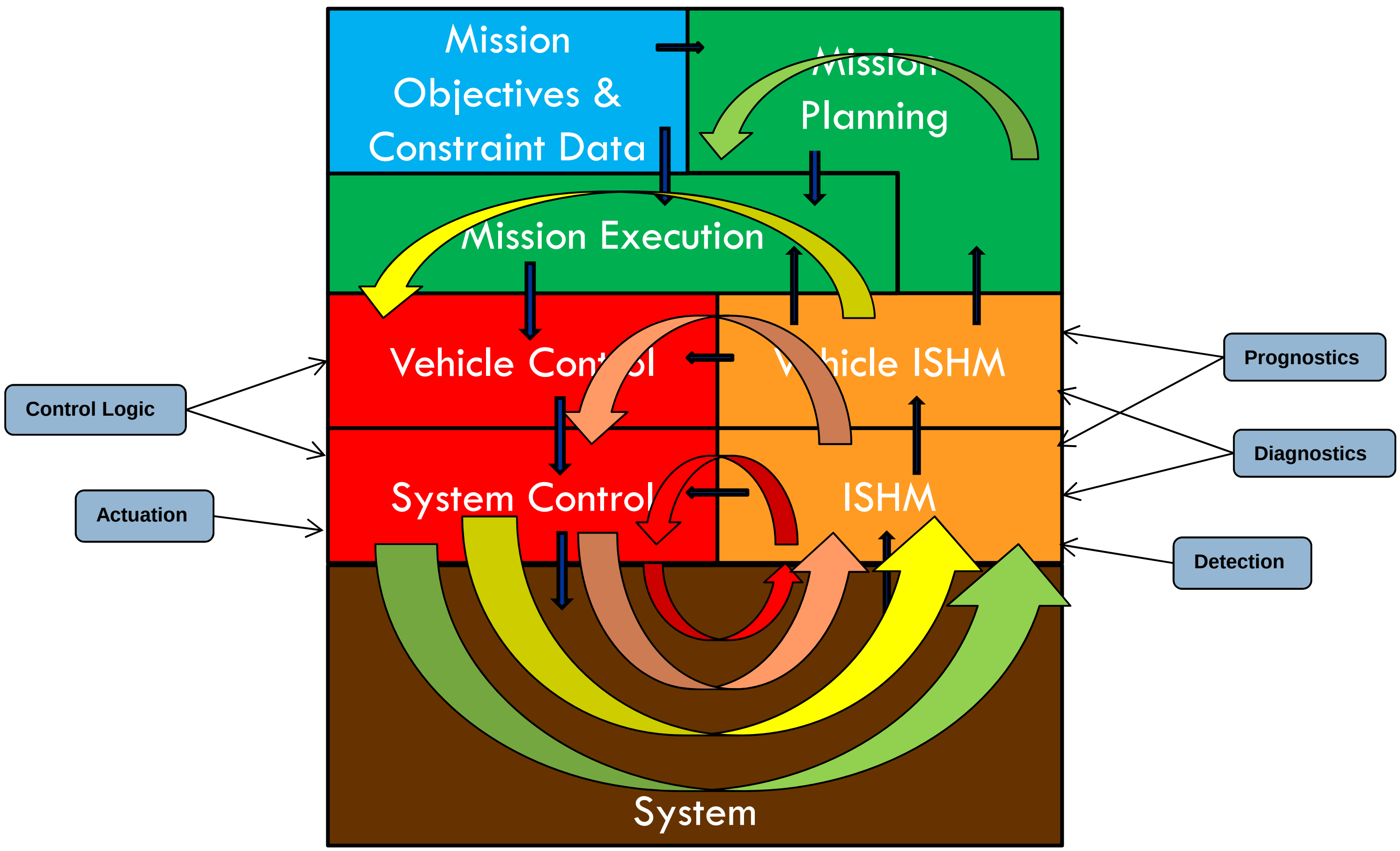
ISHM

Control System

Subsystem Management Functions for System Control



Autonomy System Stack



Candidate Autonomous Algorithms for Spacecraft Systems

- Several classes of Autonomous Algorithms
  - Expert Systems
  - Neural Networks
  - Bayesian Belief Networks
  - Model Based Reasoning
  - Fuzzy Logic
- Demonstrated in marine, space, industrial, and aviation applications
- Verification and Validation (V&V) approaches will need to be defined for these algorithms, both individually and as an integrated set
  - Formal V&V Methods (e.g., model checkers) need to be properly applied
  - Non-deterministic V&V methods need definition

Candidate Autonomous Algorithms for Spacecraft Systems

- Expert Systems
  - Expert rules establish decision structure
  - Knowledge base contains rules and relationships
  - Serves well as a central authority where rules/relationships are clearly established
  - Can be processing intensive with high data storage requirements depending on rules and rule relationship complexities
  - Well suited for:
    - Mission Planning, Crew and Mission Constraint Management
    - Subsystems with clear cut physical equations and well understood interrelationships

Candidate Autonomous Algorithms for Spacecraft Systems

- Neural Networks
  - Gradient Descent Methods
    - Deterministic due to the underlying mathematics
    - Ideal for nonlinear and interpolative applications/situation
  - Static Networks
    - Learning during training operations only
    - Quality of application based on quality of training cases
  - Dynamic Networks
    - Learning during real time operation
    - Validation and predictability
  - Implementation
    - Hardware (fast)
    - Software
    - Complexity can be difficult to verify and may require specialized chips (e.g., ASIC)
  - Ideal for
    - Control of highly nonlinear subsystems
      - Propulsion, Flight Control System transients
    - Interpolation
      - Good where there is limited knowledge of complex physical interactions
      - Real time adaptation in the event of spacecraft subsystem reconfiguration (failure response)

Candidate Autonomous Algorithms for Spacecraft Systems

- Bayesian Belief Networks
  - Applies Bayes Rule to Determine System State
    - Prior States
    - Current Belief probability
  - Best employed as an information source for other subsystem or vehicle autonomous algorithms
    - Helps clarify/validate uncertainty
    - Aids inference and reasoning (e.g., augments Expert Systems)
  - Well Suited for:
    - Performance Determination
      - Vehicle
      - Subsystem

Candidate Autonomous Algorithms for Spacecraft Systems

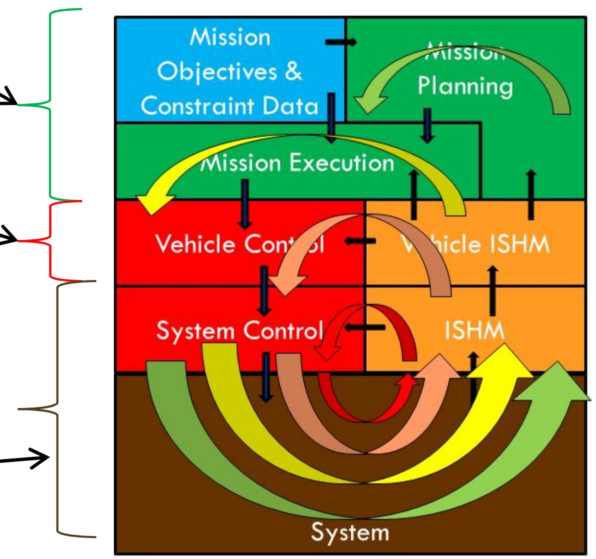
- Model Based Reasoning
  - Models based on extensive domain knowledge
    - Can leverage design models
    - Uncertainty based on fidelity of model implemented
  - Software architecture must address
    - Efficient Programming Language
    - Operating System capable of dealing with
      - Conflict resolution
      - Efficient processing
      - Embedded systems for mission critical applications (i.e., software health management)
  - Well Suited for:
    - Vehicle and Subsystem Diagnostics
    - GN&C (Kalman Filter)

Candidate Autonomous Algorithms for Spacecraft Systems

- Fuzzy Logic
  - Classical Mathematical Set Theory
  - Requires deep knowledge of subsystem physical rules and interactions to properly train
  - Provides support to Reasoning Systems (e.g., Model Based Reasoning)
  - Well Suited for:
    - Flight Control Systems

Autonomous Algorithm Integration

- 3 Levels
  - Mission Execution and Planning
  - Vehicle Management
    - Subsystem Integration Based
    - Physics form basis of subsystem interactions
      - Form basis of normal or failed states
  - Subsystem Level
    - Physics based



Autonomous Algorithm Integration

- Subsystem Level Autonomy
  - Keys:
    - Understanding the physics of the system
    - Selecting an autonomous algorithm that can
      - effectively manage the system physics(take the necessary actions based on all interactions)
      - and responsively manage the system physics (take the necessary action in a timely manner)
  - System physics are driven by the internal system processes, interactions with other systems, and interactions with the environment, all of which must be managed by the algorithm
  - System-level algorithm matching involves knowledge of the system transfer functions which include external system and environment interactions
    - Control Theory is important in implementation.
      - The physics will define the poles and zeros of the control system and the relative proximity of the system response to these locations.
      - System Transfer Functions must be defined and matched with the characteristics of the autonomous algorithms

Autonomous Algorithm Integration

- Vehicle Level Autonomy
  - Keys:
    - Integration of the systems autonomous algorithms into a cohesive and response management system
    - Algorithms taking proper responses to planned and unplanned conditions
      - Managing the subsystem physics effects on the vehicle are essential
    - Manage interactions between systems
      - Vehicle must manage cooperative vs. competitive subsystem responses such that subsystems do not counter each other's actions leaving the vehicle in a failed state

Autonomous Algorithm Integration

- Mission Execution and Planning
  - Keys:
    - Mission Execution
      - Manages the total execution of the all mission aspects from a vehicle stand point
        - Proper knowledge of the current vehicle states
        - Progress toward specific mission objectives
      - Mitigates subsystem interaction effects through adjustment to system control parameters in response to specific physical events.
    - Mission Planning
      - Based on
        - Proper knowledge of the current vehicle states
        - Progress toward specific mission objectives
      - Conducts Re-planning (with crew approval) to ensure future vehicle states will stay within mission objectives and constraints
      - Three Levels
        - Strategic: Earth-based controls will also be involved
        - Tactical: Crew input and approval
        - Emergency: Automated to prevent loss of mission, crew, or compromise of crew safety

Summary

- Human exploration outside of the Earth planetary system (beyond Earth orbit) requires autonomous operation of the vehicle
  - Communication Latencies
  - Crew size Limits
  - Vehicle Complexity
- A fully autonomous vehicle of this complexity will require multiple autonomous algorithms working cooperatively within a set of mission objectives and system constraints
  - The understanding of the physics of the systems, system interactions, and environmental interactions is essential to the system engineering of this complex system
  - The Goal-Function Tree methodology provides a system engineering approach to define the vehicle state variables and their interactions.
- Algorithms at the vehicle level will need to handle future projected states to enable safe mission execution and planning.
- Verification and validation approaches will need to be defined for these algorithms, both individually and as an integrated set
  - V&V will also need to borrow from Formal Methods (e.g., model checkers)
- Applications looking at autonomous system cooperation will be essential to the development of human rated spacecraft operated away from the Earth planetary system