Managing Space System Faults: Coalescing NASA's Views

Presented at the IEEE Aerospace Conference, Big Sky Montana

Brian K. Muirhead
Lorraine Fesq
NASA/ Jet Propulsion Lab

March 5, 2012

Jet Propulsion Laboratory, California Institute of Technology.
Copyright 2011 California Institute of Technology. Government sponsorship acknowledged.

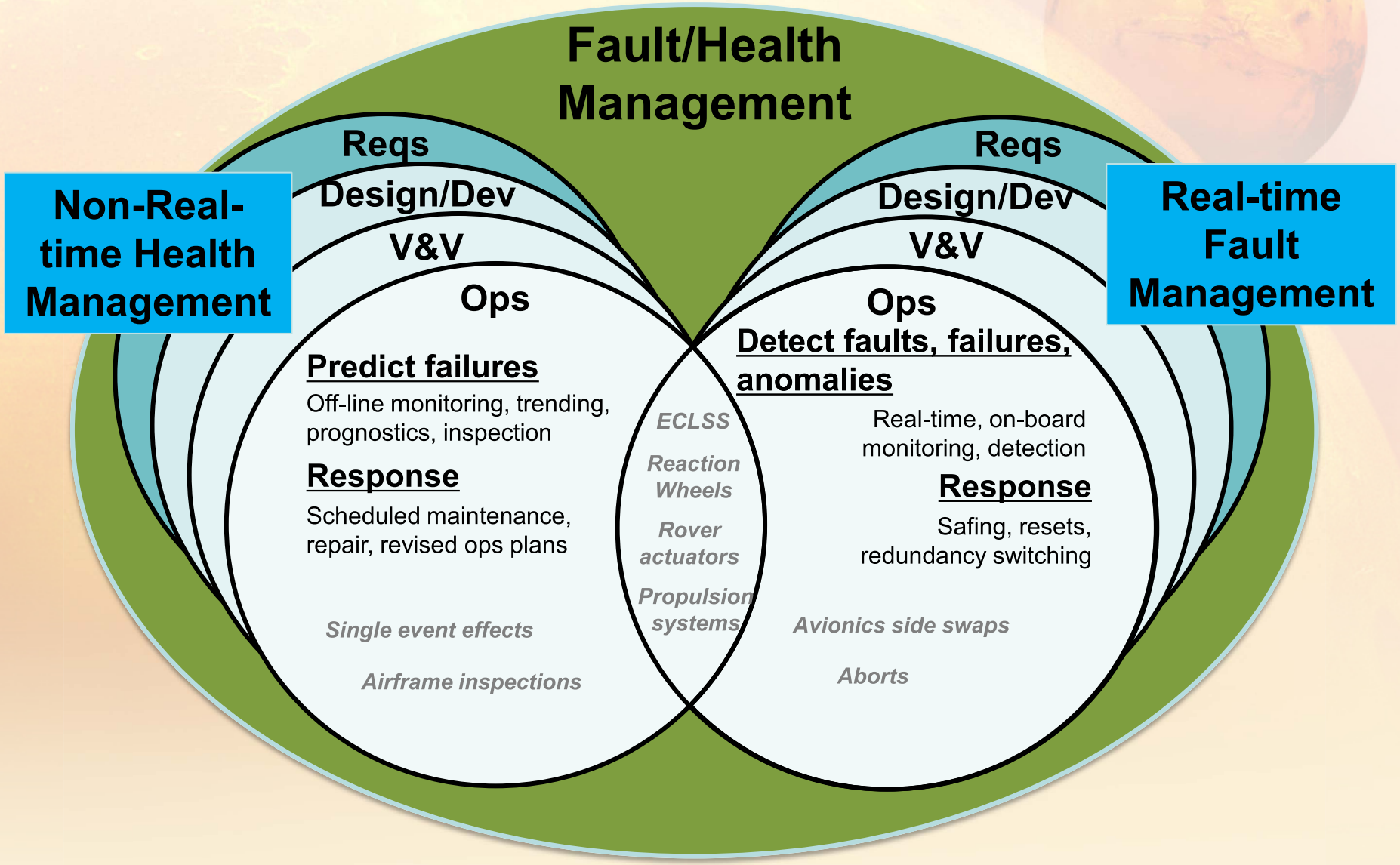
Agenda

- Introduction
- A NASA view of Health Management (HM) and Fault Management (FM)
- Robotic missions
- Shuttle and International Space Station (ISS)
- Changes in human rating requirements
- Humans beyond low Earth orbit: Constellation
- Ultimate challenge: Human exploration of Mars
- Conclusions

Introduction

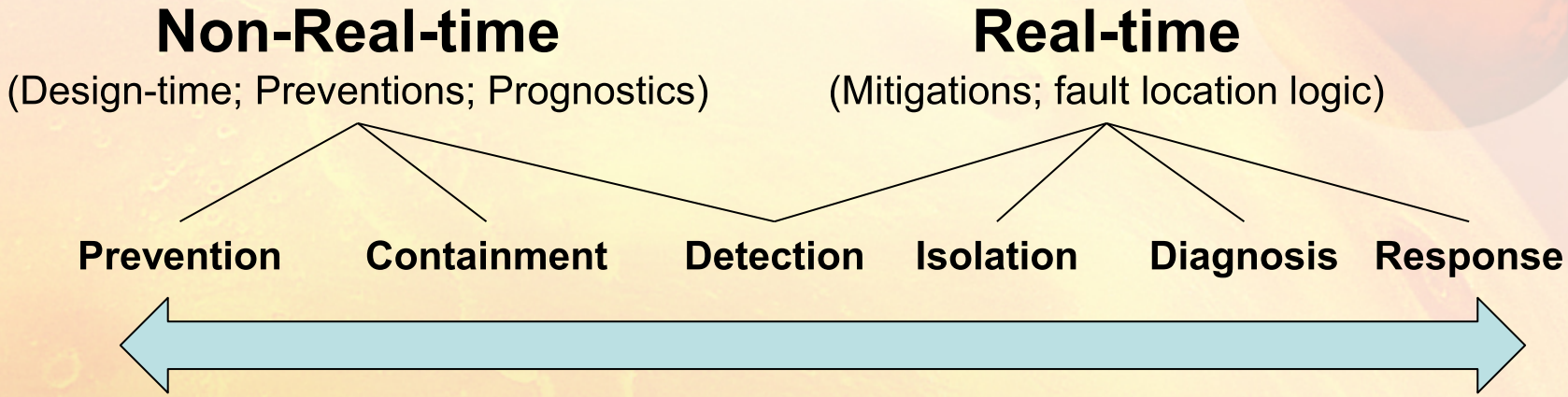
- This talk explores differences and relationships between health management and fault management as it applies to NASA robotic and human missions
- The current practice and future challenges are discussed with application to both robotic and human exploration of Mars
- The need for high reliability systems, particularly avionics and software, will be discussed

At NASA, "Health Management" consists of Non-Real-time and Real-time

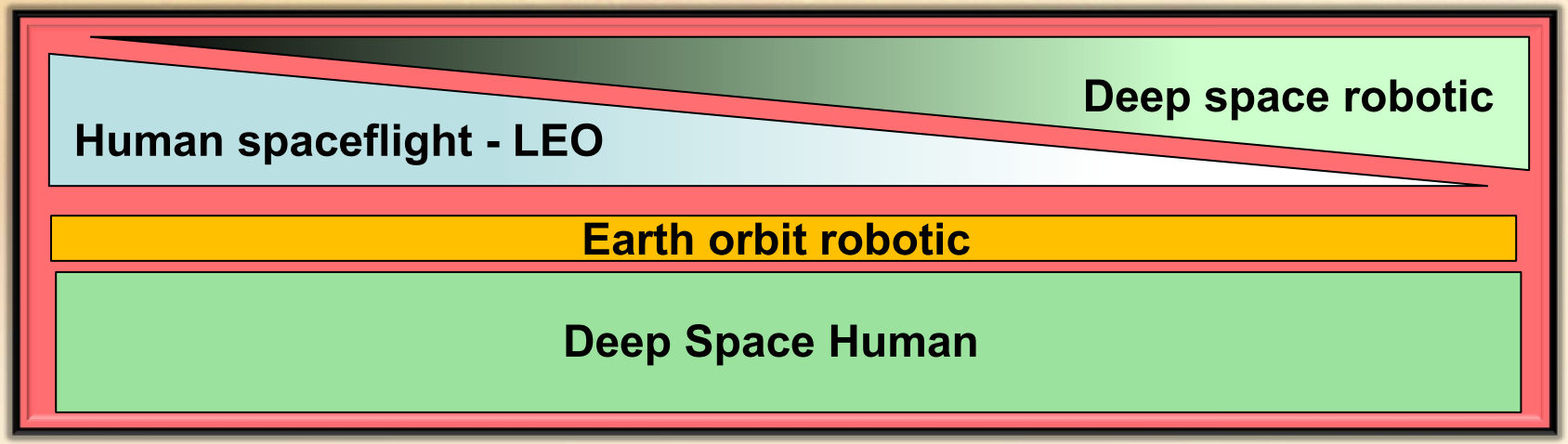


Spectrum of Health/Fault Management

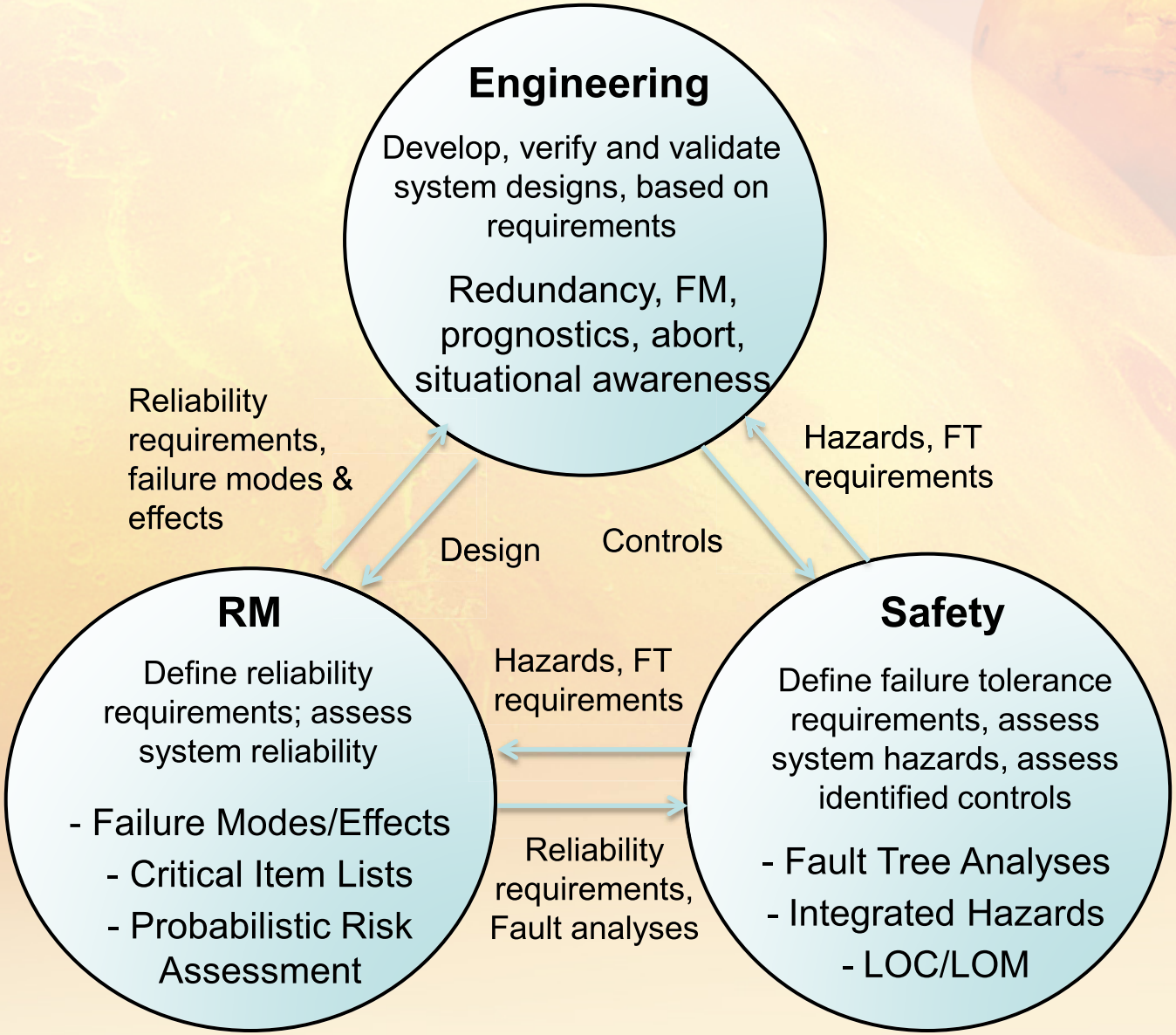
- A spectrum of issues/options affect HM/FM scope and implementation



- Mission characteristics determine emphasis and level of automation

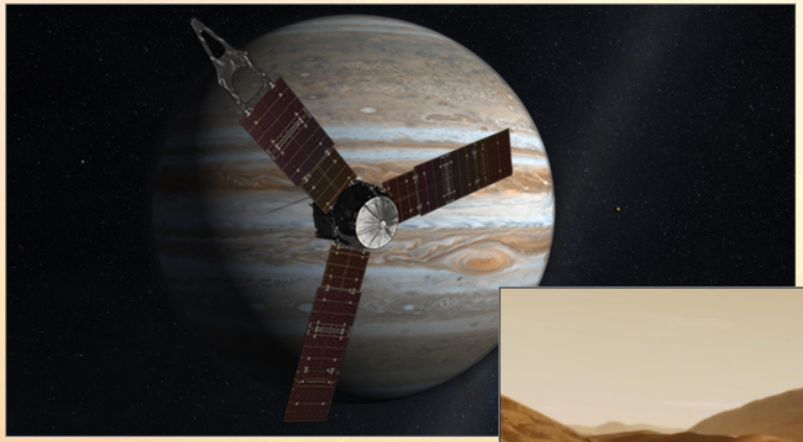


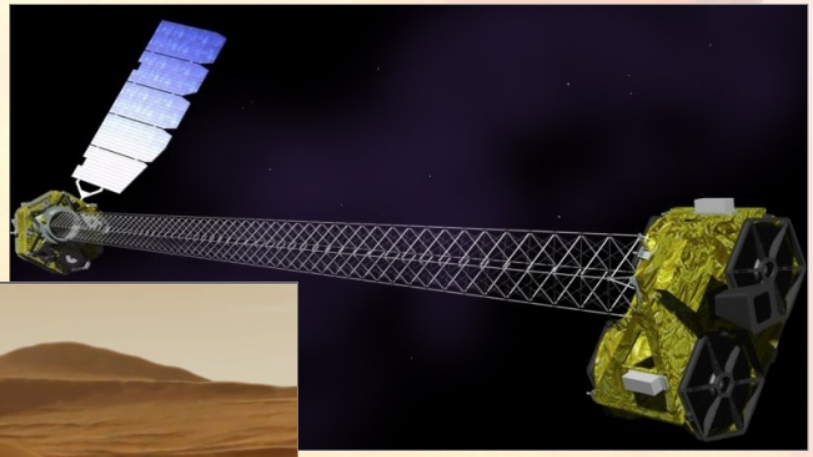
HM/FM is an engineering discipline with interfaces to Reliability/Maintainability (RM) and Safety

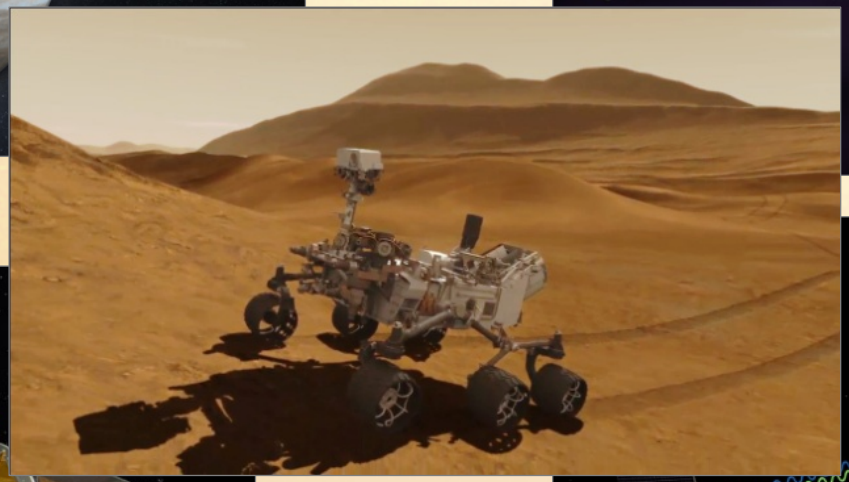


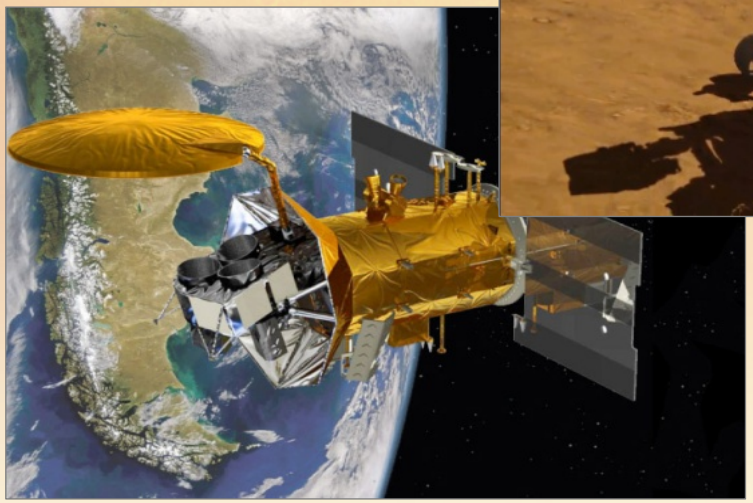
Robotic Missions

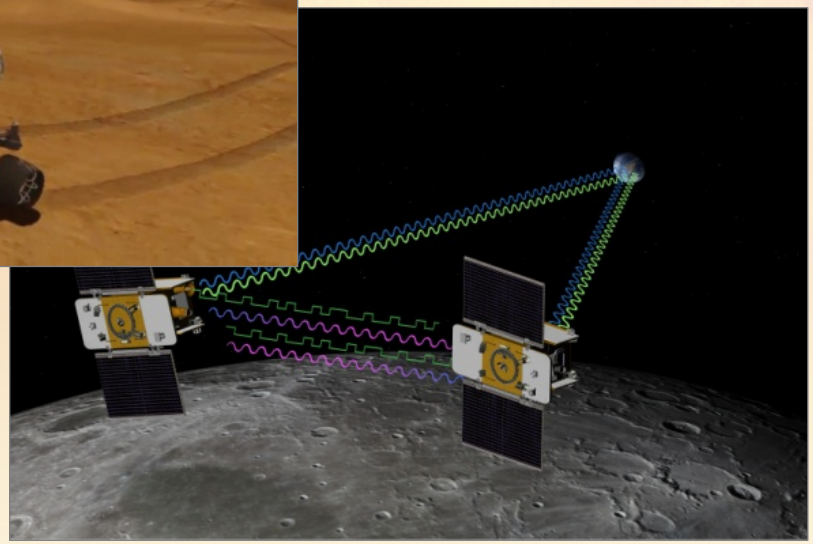
- HM is primarily FM with some monitoring/trending of limited life elements







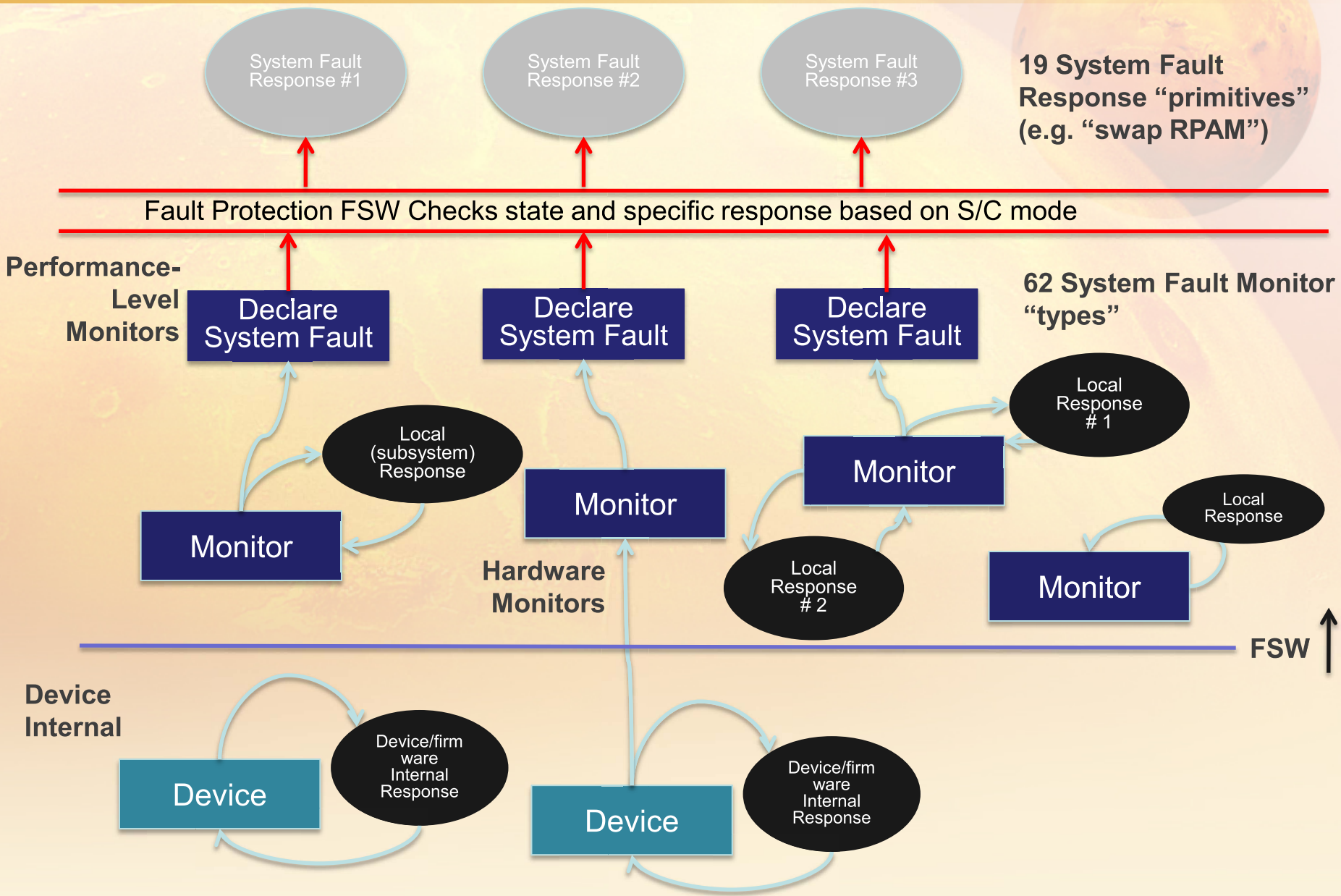




Robotic Mission Fault Management Features

- Every science mission's flight system requires a degree of FM autonomy
  - Earth orbiters feature early critical events, short communication latencies and frequent communication opportunities which allow most FM functions to be performed on Earth by human operators and advisory systems
  - Deep space missions, have unique critical events (orbit insertions, entry/descent/landing), long light-time delays, Deep Space Network (DSN) constraints, system resource constraints (e.g., battery state of charge) which preclude human operator intervention, and thus dictate extensive FM autonomy
  - All flight systems require FM that can contain the effects of failures and preserve functionality critical to keeping the system safe until operators can respond
- System complexity drives FM complexity including the following characteristics:
  - Structural complexity (e.g., the number of interconnected components)
  - Behavioral complexity (e.g., the variety of behaviors required)
  - Distributed complexity (e.g., the coordinated control of physically decoupled assets such as in formation flying and swarm missions)
  - Operational complexity (e.g., reliance on interactions between disparate systems and teams)

MSL On-Board Fault Protection Overview



Robotic Mission HM/FM Design Environment

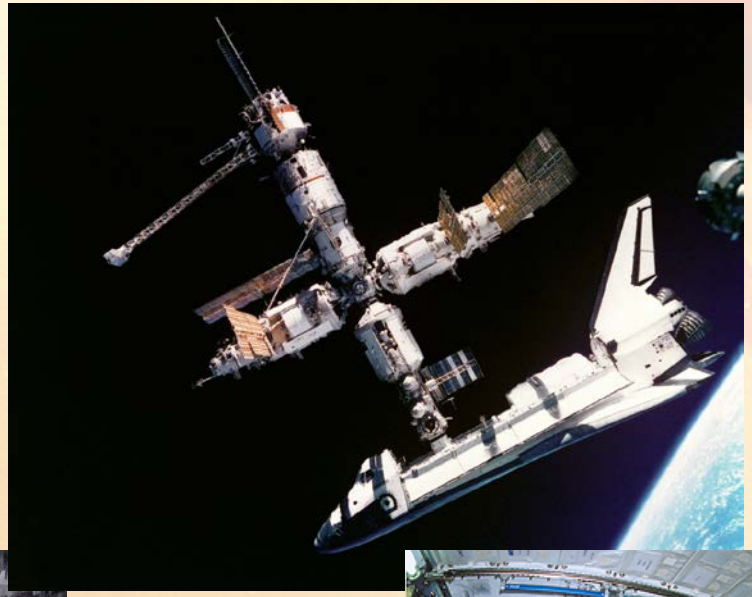
- **Limited hardware redundancy**
  - Development costs of space systems are strongly coupled to system mass. Given cost and mass constraints, science missions often employ functional and informational redundancies instead of hardware-identical redundancy.
  - Single string (no redundancy at all) is no longer uncommon (e.g. Mars Pathfinder, MERs, SMAP)
- **High reliability and long lifetime**
  - Overall reliability is driven by operational lifetimes of many years (e.g. Cassini nominal mission 11 years)
  - Design for harsh operating environments including launch dynamics, low pressure/vacuum, high radiation, and extreme temperature and fluctuations/cycles
  - Attaining the required reliability over a mission's lifetime is usually achieved by conservatism in component selection (e.g. heritage, high reliability parts), design margins (e.g. temperature) and extensive testing

Mars Science Laboratory FM by Phase

- Launch/Cruise/Approach (8.5 months)
  - Single fault tolerant and preserves the spacecraft in a power-thermal-comm-safe (& consumables) state for up to 2 weeks
  - Autonomous support for computer reset recovery provided for cruise operations
  - "Prime string" redundancy configuration to be used during EDL, which is "selected" in late cruise.
- EDL (EDL mode change ~20 days out, EDL event ~7 minutes)
  - EDL phase (starting several days prior to cruise stage separation) is single string and is NOT be single fault tolerant.
  - No autonomous support for computer reset recovery provided for EDL.
  - Computer reset recovery prior to start of entry managed by the Ops Team.
  - Effort to implement additional back-up capability is underway and is expected to be in place for EDL
- Surface (One Mars year, two Earth years)
  - Single fault tolerant and preserves the spacecraft in a power-thermal-comm-safe (& consumables) state indefinitely
  - Autonomous support for computer reset recovery provided for surface operations
  - After an on-board fault no support for autonomous resumption of normal sequence operations
  - Greatest current challenge is in the Sample Acquisition and Processing/Handling system

Shuttle and International Space Station (ISS)

- HM emphasis is on maintenance, inspection/repair, analysis of operational life, with limited instrumentation for health monitoring



New Human Rating Requirements

- In 2007 the core requirement for redundancy for human rating was changed. Up to that point the basic requirement for redundancy was for two failure tolerance against catastrophic events.
- New requirements were driven by the need to provide the safest possible vehicle(s) while recognizing that for systems designed to go beyond LEO, the impact of imposing a blind two failure tolerance requirement would significantly impact the limited technical resources of mass, volume, and power.
- Efforts involving engineering, safety and mission assurance, and the crew office resulted in the following new core requirement:

  The space system shall provide failure tolerance to catastrophic events, with the specific level of failure tolerance (1, 2 or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis.

Impact of New Human Rating Requirement

- The emphasis is on the overall system capabilities utilizing similar systems, dissimilar systems, cross-strapping, and/or functional interrelationships that "ensure minimally acceptable system performance despite failures."
- Redundancy does not, by itself, make a system safe, it is the responsibility of the engineering and safety teams to determine the safest possible system design given the mission requirements and constraints.
- The culture of human systems engineering believes in common mode failures (based on experience from Shuttle), more than the robotic community and therefore often try to implement dissimilar redundancy.
- It is also highly desirable that the space flight system performance degrades in a predictable fashion to allow sufficient time for failure detection and, when possible, system recovery even when experiencing multiple failures.

Fault Management Requirements

- The following are high level definitions and guidance for design of human-rated spacecraft. Finding the best allocation of FM functionality between automated (no human involvement), autonomous (no crew but ground engagement) and the crew is a major challenge.

  1) The space system shall provide the capability to detect and annunciate faults that affect critical systems, subsystems, and/or crew health. Rationale: A fault is defined as an undesired system state. A failure is an actual malfunction of a hardware item's intended function. It is necessary to alert the crew to faults (not just failures) that affect critical functions.

  2) The space system shall provide the capability to isolate and recover from faults that would result in a catastrophic event or an abort. Rationale: The intent is to provide isolation and recovery from faults where the system design (e.g. redundant strings or system isolation) enables the implementation of this capability.

  3) The crewed space system shall provide the capability for the crew to manually override higher level software control / automation (such as configuration change and mode change) when the transition to manual control of the system will not cause a catastrophic event.

Mars Design Reference Architecture 5.0
Low-Earth Orbit Operations Challenges

- Maintenance of vehicles in low-Earth orbit (LEO) for extended durations (300-390 days) to accommodate launch campaign
  - 7+ Earth-to-Orbit launches per mission
- Long-term system maintenance (micro-meteoroid / orbital debris and cryogenic fluid management)
- Automated Rendezvous and Docking (AR&D) of large elements in LEO to minimize in-space assembly by crew
- Failure-tolerant launch/docking sequence to achieve <10% Loss of Mission
- Common thread: highly dependable avionics and software

Mars Design Reference Architecture 5.0 Autonomous Operations Challenges

- Advanced autonomous capabilities are required due to long communications latency, lack of routine resupply
  - Identification of system failure modes
  - Model Based Reasoning techniques
  - Software verification and validation
  - Fault detection and reconfiguration
  - Trends identification and predictions
  - Lowest level component repair

Conclusions

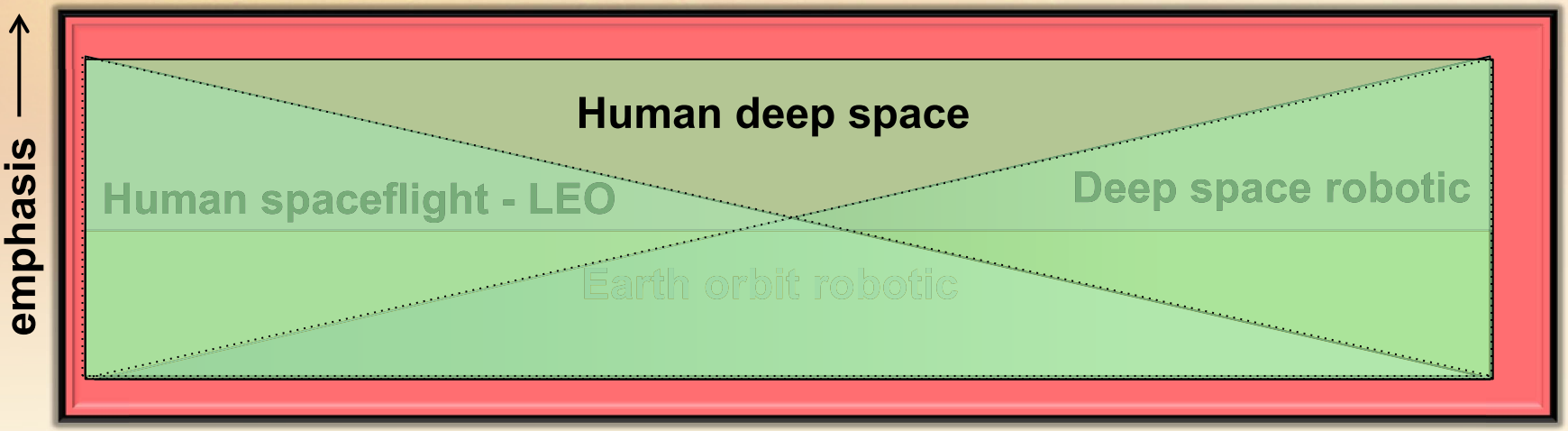
- HM/FM is an important part of human and robotic spaceflight and is particularly critical for long duration spaceflight, especially with humans beyond low earth orbit
- System architects, stakeholders and designers need to become more aware of and conversant in the issues, design options, V&V and operations of HM/FM throughout the program/project lifecycle
  - Need to incorporate HM/FM based on needs, cost and risk
  - Balance/optimize automation vs human-in-the-loop (in space and on the ground)
  - Develop and deliver highly dependable avionics and software across all systems
- There is potential for collaboration and mutual benefit across the aerospace industry through working together in HM/FM but we need to understand much better, from our respective points of view and mission contexts, this discipline, its drivers, benefits and limitations

Spectrum of System Health Management

- A spectrum of issues/options affect SHM scope and implementation

Non-Real-time
(Design-time; Preventions; Prognostics)

Real-time
(Mitigations; fault location logic)

Prevention **Containment** **Detection** **Isolation** **Diagnosis** **Response**

- Mission characteristics determine emphasis and level of automation