

# System Engineering Challenges of Mars Science Laboratory's Entry, Descent and Landing

...Or, "7 Years of Terror"



Ann Devereaux

MSL Flight Systems and Fault Protection Lead

MSL EDL Deputy Lead

Mars 2020 Flight Systems Engineering Lead



Copyright 2013 California Institute of Technology. Government sponsorship  
acknowledged. ( URS239980)



# 台科學家駕駛 好奇號發



### 好奇號 登陸火星

■ 今年11/26日 發射升空

■ 飛行8個多月， 飛越地球、 離火星10分鐘， 距離與太空船 分離， 開始定期向 火星。

【本報專訊】原台電總機 美國太空總署(NASA) 火星探測器「好奇號」(Curiosity) 將由美國 8年重慶， 歷經8個多月、5.7萬公 里的飛行旅程， 將於在臺灣時間昨 天(7日)晚上10時30分發射升空， 為 人類火星探測邁出一步。

在地球操作能發射好奇號的團隊， 包括台灣科學界正、副首腦。

美國36年探 測火星， 探測器 材料、利用7架「火 箭車」與以往6架「火 車」不同， 這次發射 出 的探測器將與發 射 器 人 類 火 星 探 測 邁 出 一 步。

### 認清火星

資料來源：綜合電 大 小 直徑0.792公里(地球1/756公里)

1英寸多長 1米比地球多40分鐘 重 力 僅 地 球 的 38% 人 在 地 球 上 重 68 公 斤， 在 火 星 上 重 26 公 斤

大氣 95.3%二氧化碳、2.7%氮氣、 1.6%氬氣、0.1%氫氣

地 球 每 年 降 雨 約 1000 公 厘， 火 星 每 年 降 雨 約 0.0389 公 厘

濕度 攝氏25度至零下15度

水分 僅40年前前河河和海洋

地 球 每 年 降 雨 約 1000 公 厘， 火 星 每 年 降 雨 約 0.0389 公 厘

## WETTER

23°

Heute ist es am Morgen noch recht frisch. Nachmittags wird es sehr sonnig.

# NEU Vorarlberger Tag

DIENSTAG, 7. AUGUST 2012



## Die Geheimnisse des Mars

Nach der spektakulären Landung des Mars-Rovers Curiosity: Rätsel unserer Nachbarwelt

### POLITIK

#### Syrien: Regime zerfällt

Neben Diplomaten und Militärs hat sich nun auch der Premier abgesetzt. S. 6/7

### VORARLBERG

#### Angeklagt

Bis zu zwei Jahre Haft wegen fremdenfeindlicher Internet-Postings. S. 14/15

## EXKLUSIVNĚ V LN: Jak si dělili kořist

# Půlka Rathovi nestačila, chtěl přidat milion

# LIDOVÉ NOVINY

NEZÁVISLÝ DENÍK ZALOŽENÝ 1893

SEKCE 7. SRPNA 2012 CENA 16 Kč

# Volte nás, dostanete slevu

Lidovci lákají na levnější telefonování • Nabízejí slevu 60 % na mobil a 15 % na elektřinu a topení

### MILOŠ ZEMEK

**Billboard lidovců**

**Společné ústředí**

- **Společné ústředí**, lákají na billboardních plátech v okolí Prahy
- **U občanů šetrně a topení** mají slevu 15 procent, v mnoha městech telefonuje 60 procent
- **Ne věříme pak milionářům a krádežnickým pátrákům na slevu** typičtí

Příběh zájezdu do firmy, která dodává elektřinu přímo v bytě lidem v Praze. Ustřížte červeno, nezaplatíte a za topení v obcích domcích.

Našli strany s tím, že lidovci přispívají slevě. Je to...



### Sedm minut strachu a pak...

Američtí vědci z NASA našli první v neprobádaných předčasných mrazech v historii astronomie. Na Mars se po dlouhém čekání úspěšně vytvořila podzimní laborator. Když byla v příštích několika minutách astronomie a pak bezpečně přistála, sleva byla 1600 ústředí. Článek na str. 2

# Pustil Knapkovou závodit, ale jistý si nebyl

Lidovci Nutry Pavla Knapky, byla by šlo o to, že by se mohl stát... Knapka v příštích několika... Mladý muž... ZPRÁVY V LN V LONDÝNĚ... Lidové noviny... Číslo 163



# But – it wasn't easy

- Five very different operational domains
  - Laboratory setting, launch pad, deep space cruise, Mars atmospheric, Mars surface
- Largest Mars rover mission yet
  - 3365 Kg (dry) launch configuration
  - 900 kg Rover
  - Sheds  $\frac{3}{4}$  of mass (= functionality??) on its way to surface
- Complex guided entry and soft touchdown scheme for landing
  - ~ 7 minutes from atmospheric entry to touchdown
  - ~14 minute one-way light time at approach to planet
  - Direct-to-earth communication lost before touchdown
  - **High levels of autonomy and fault tolerance a must!**

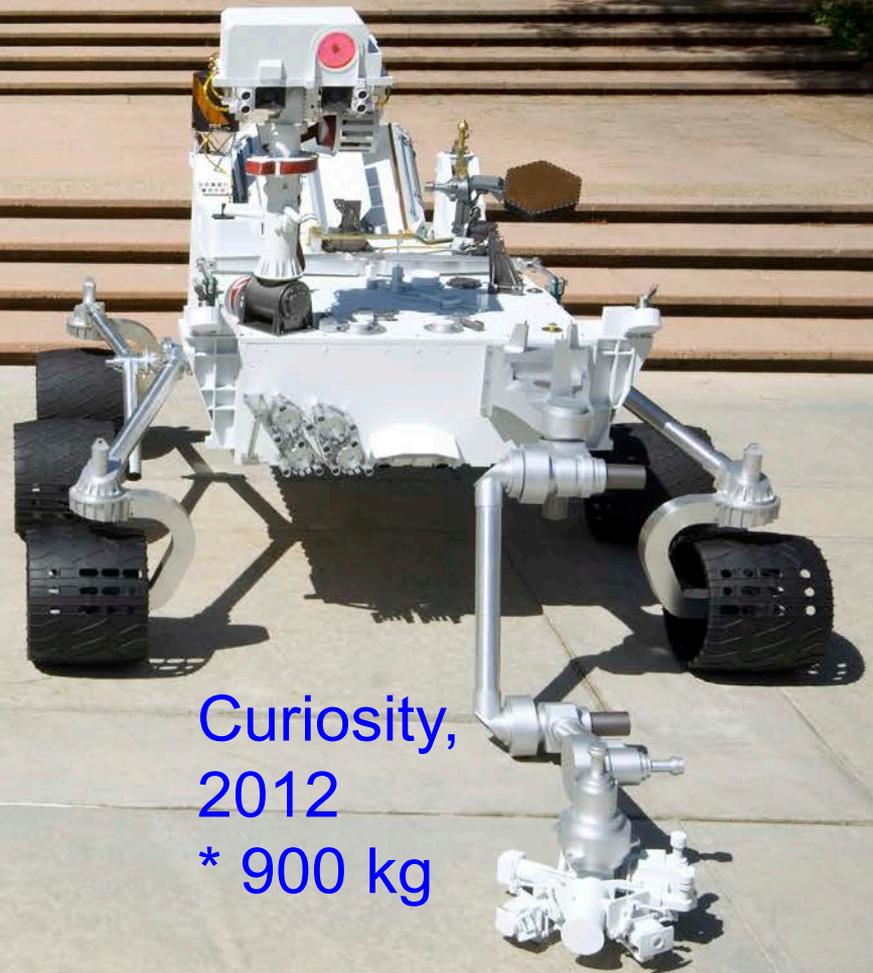
# Family Tree – “Heritage”



Pathfinder,  
1997  
\* 25 kg



Spirit &  
Opportunity,  
2004  
\* 175 kg



Curiosity,  
2012  
\* 900 kg



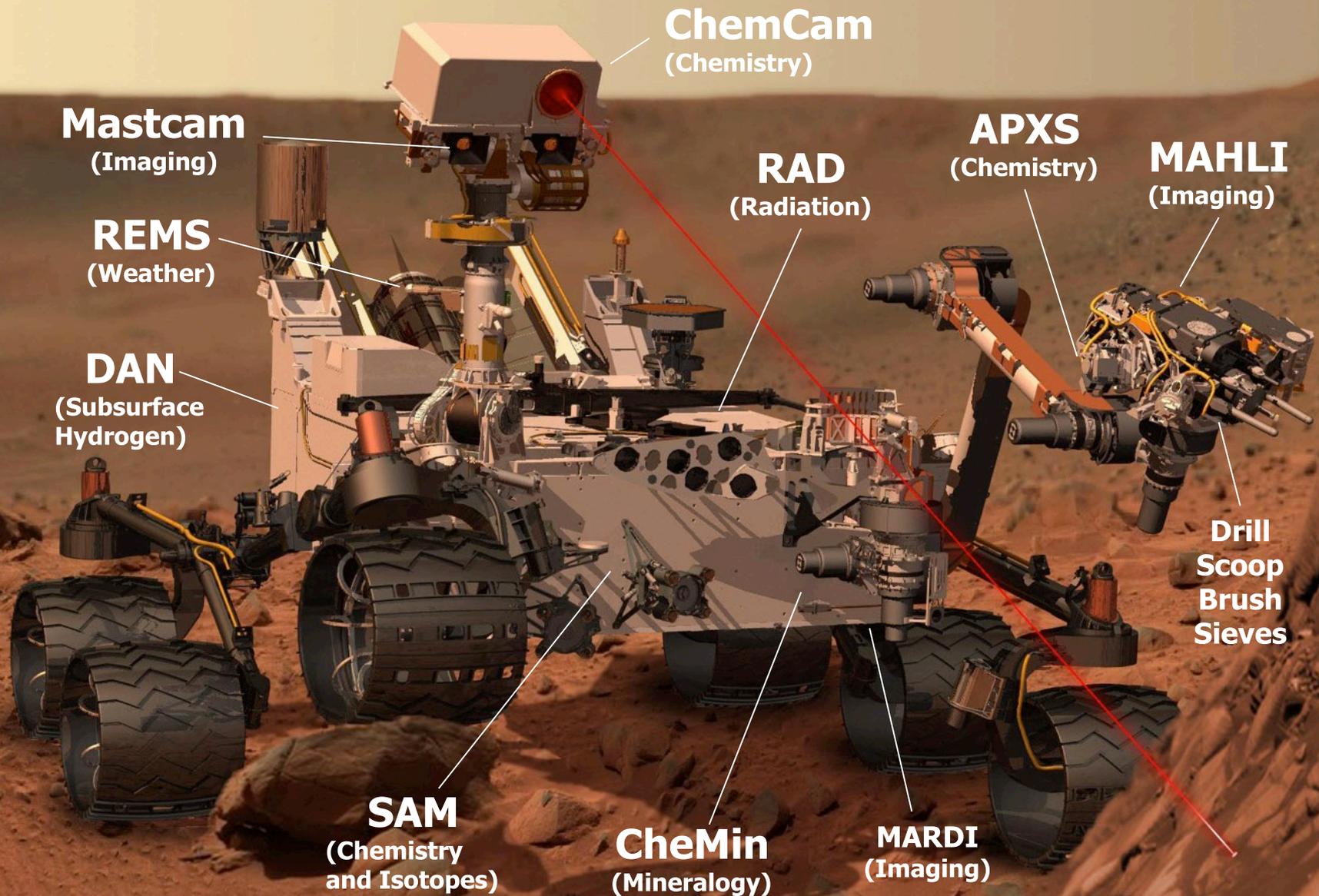
Curiosity,  
2012

Mini Cooper,  
2011

# Agenda

- Overview of MSL Mission
- MSL Avionics Architecture & Fault Protection
- Entry, Descent and Landing Design
- Looking forward to Mars 2020!

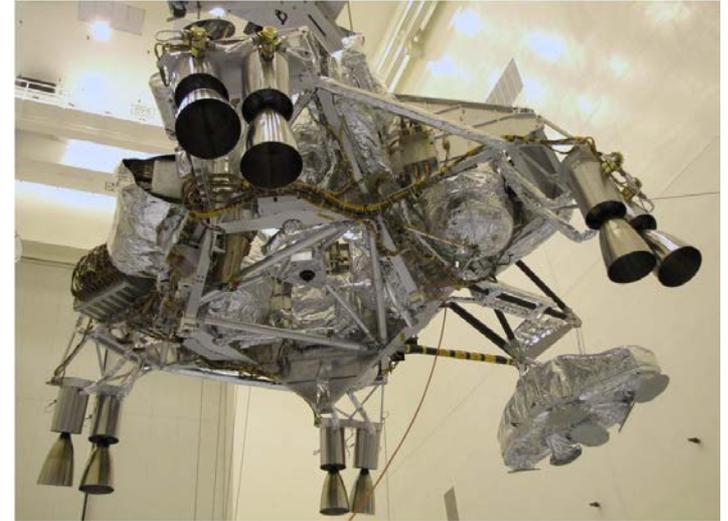
# Mars Science Laboratory



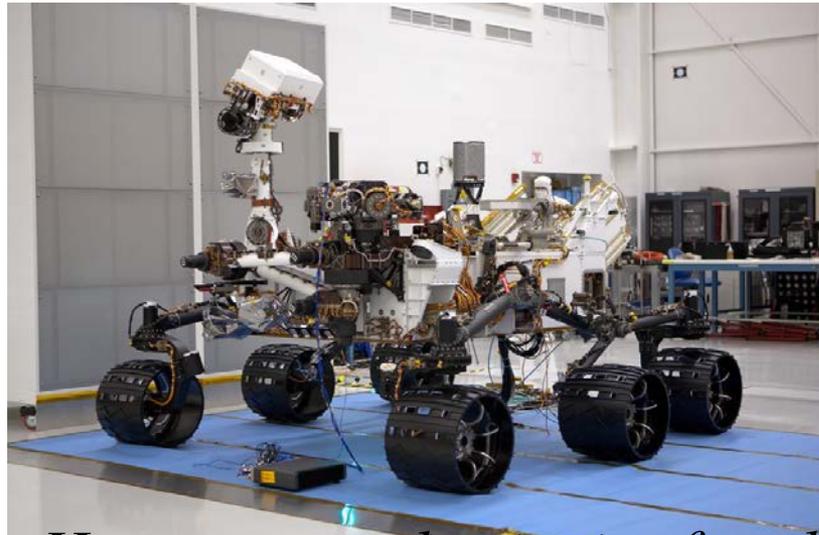
# MSL Mission Phases



*Cruise Stage:  
Rover &  
Descent  
stage  
encapsulated,  
with Cruise  
stage flying*

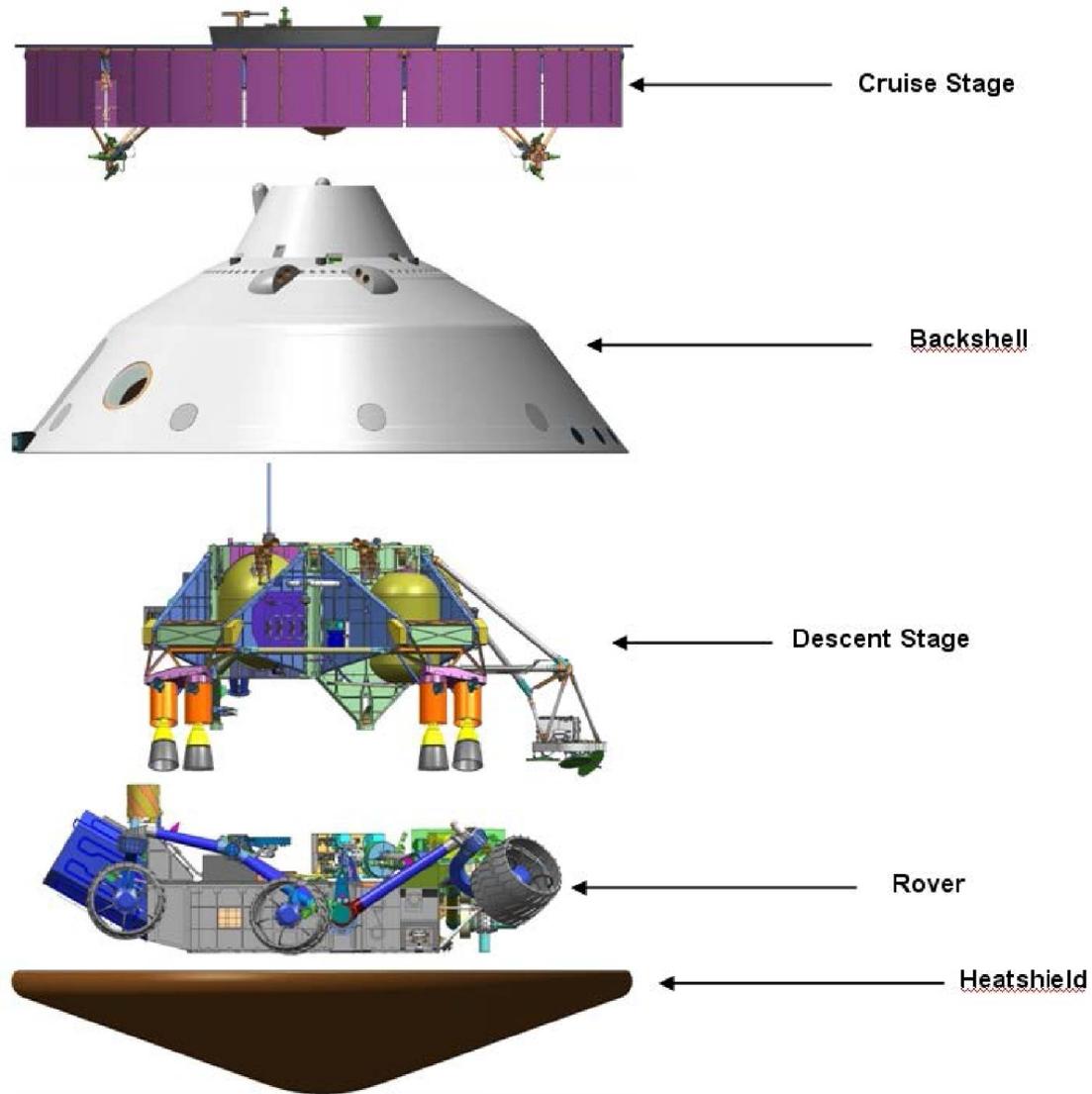


*Descent Stage:  
Lowers Rover to  
surface and then  
flies away*

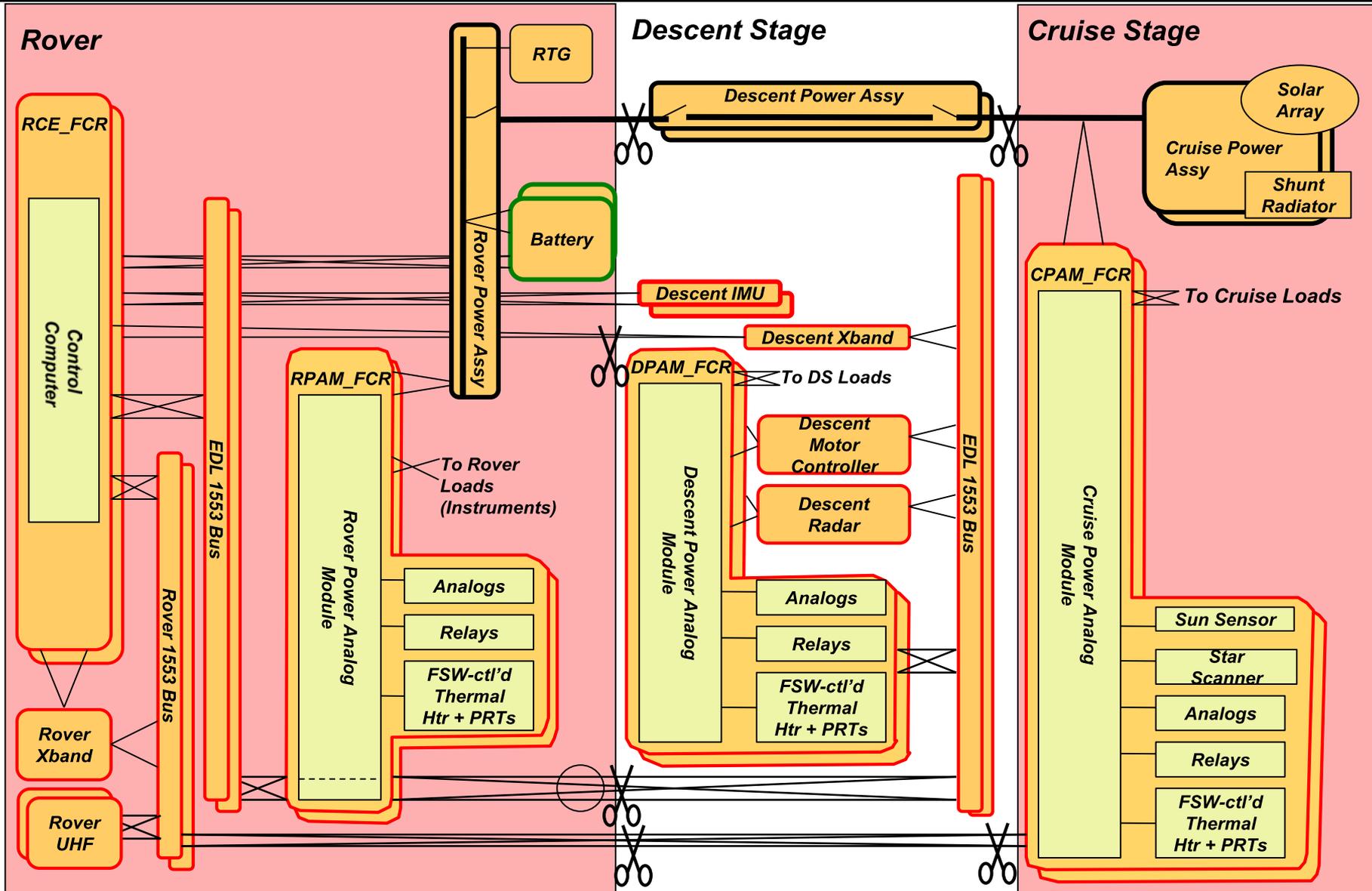


*Rover: Houses control avionics for all stages*

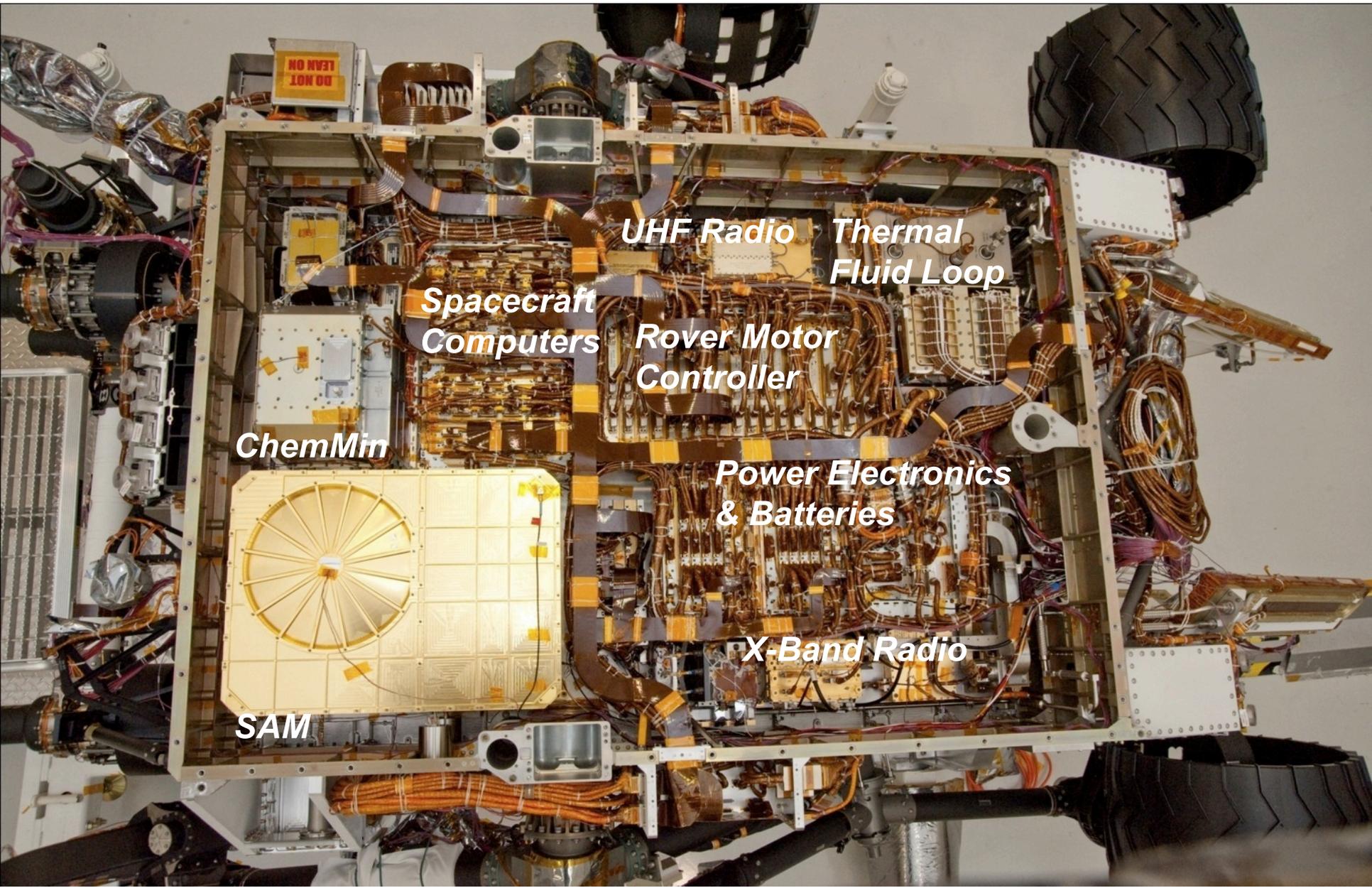
# Stacked Configuration



# Avionics Architecture – Fault Containment Regions



# Rover Electronics Bay



DO NOT  
LEAN ON

UHF Radio

Thermal  
Fluid Loop

Spacecraft  
Computers

Rover Motor  
Controller

ChemMin

Power Electronics  
& Batteries

X-Band Radio

SAM

# Generic Fault Protection Toolbox

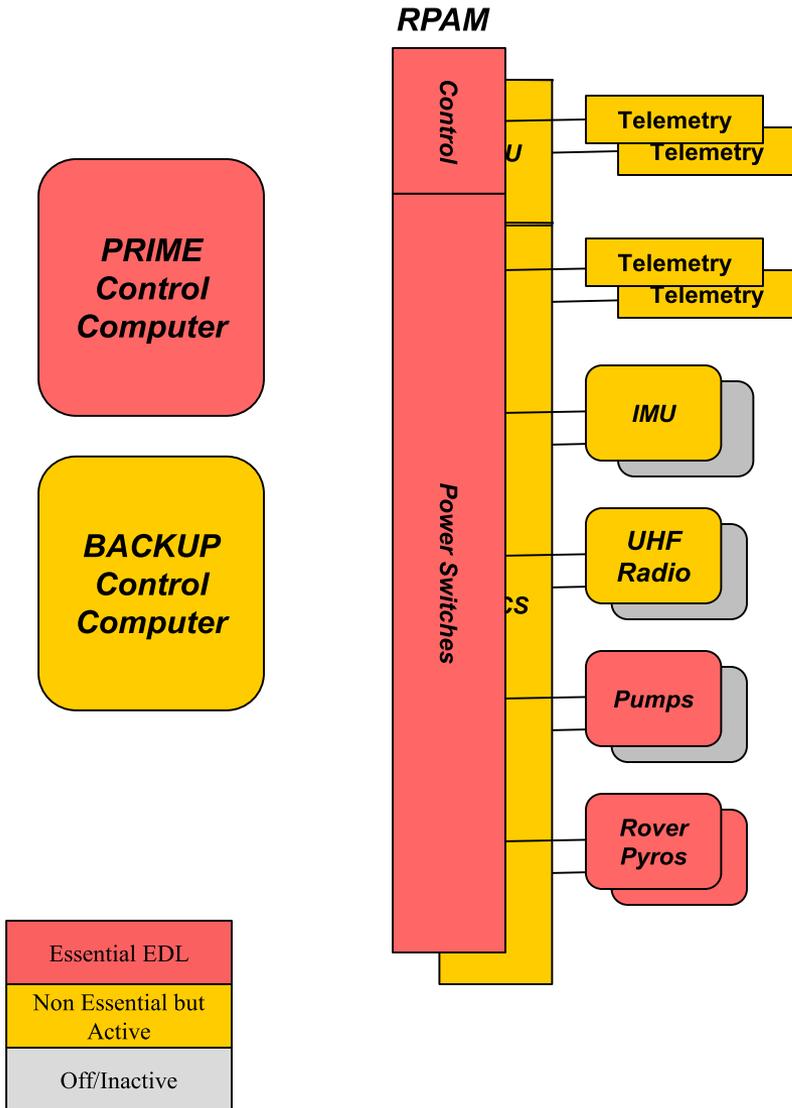
- Responses always start with
  - Stop autonomous behaviors (auto navigation or EDL)
  - Put vehicle in “safe” configuration
- Then optional, in order of escalation
  - Swapping device (suspect clients)
  - Swapping PAMs (suspect interface providers)
  - Swapping control computers (suspect master)
- Always finish
  - Reset monitors – “clean slate” for new problem or for trying something different for a persistent problem

# Evolution of Redundancy

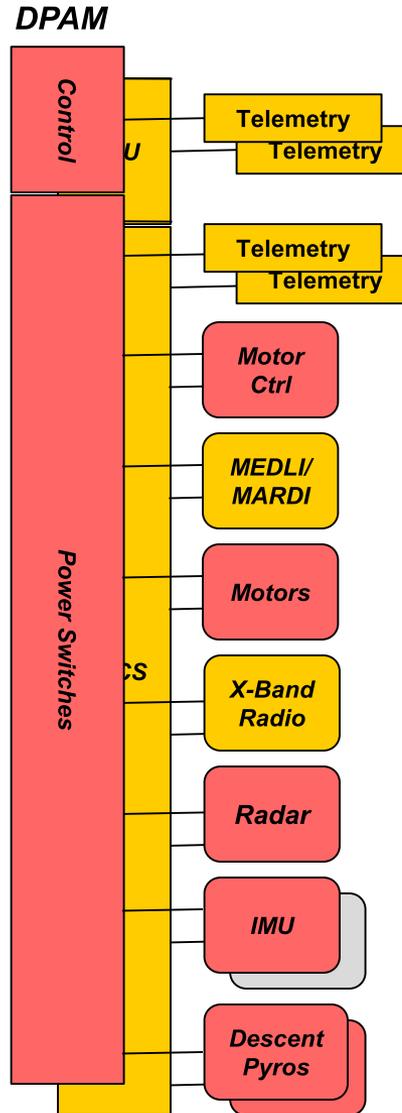
- 1. (Circa 2005) Single string
  - Modeled on MER rovers
- 2. (Circa 2006) Dual string w hot backup PAMs, maybe RCE “hot swap” for EDL
  - Computers were designed with internal cross-strapping so one computer could determine the state of the other, and act accordingly
  - PAMs were designed with internal cross-strapping between redundant pairs, and complementary sense/control logic for graceful degradation of capability
- 2. (Circa 2008) Dual string w hot backup PAMs, no RCE hot swap
  - Complexity of having mirrored computer states was deemed not worth risk
- 3. (Pre-Launch slip Circa 2009 – “MSL 2.0”)
  - CRUISE AND SURFACE: Dual string PAMs/RCEs operated as single string
    - As implementation matured, it became clear (wrongly, in retrospect) that there would not be enough test hardware to have dual-string testbeds. In the spirit of “Fly Like You Test”, spacecraft was re-architected to run single string, with cold redundant pairs
    - Difficulties arose due to the already designed-in cross-strapping of pairs, and re-designing of fault protection to be based around swaps (“big hammer” approach)
  - EDL: Partial dual-PAMs and “Second Chance” RCE
    - Level of comfort with baseline system reached threshold beyond which more testing did not lower risk (there be dragons..)

# EDL-Centric Look at Redundancy

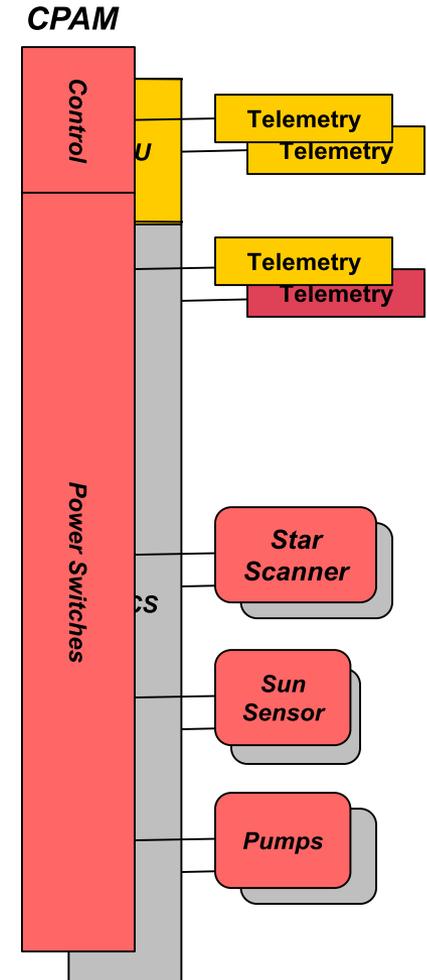
Rover



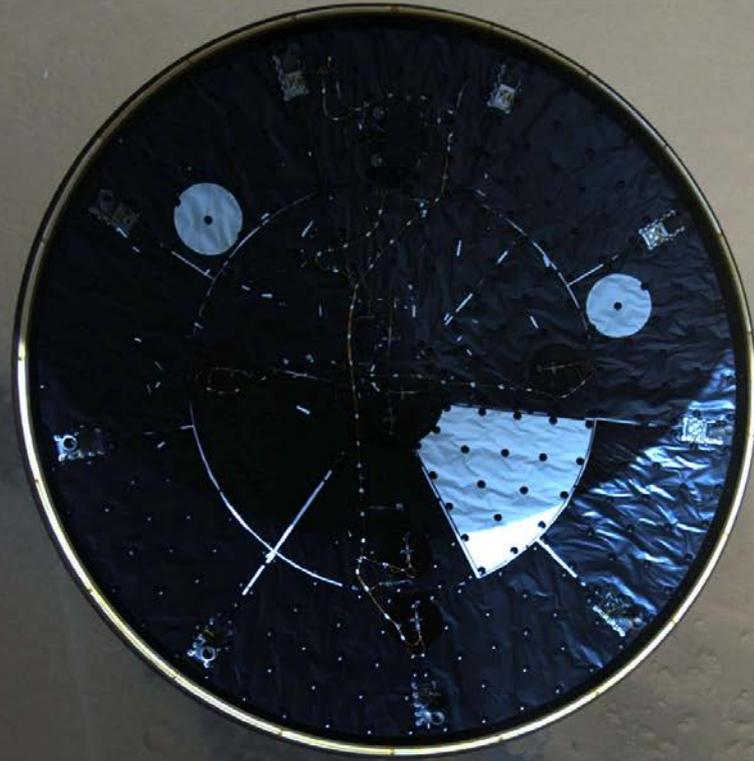
Descent Stage



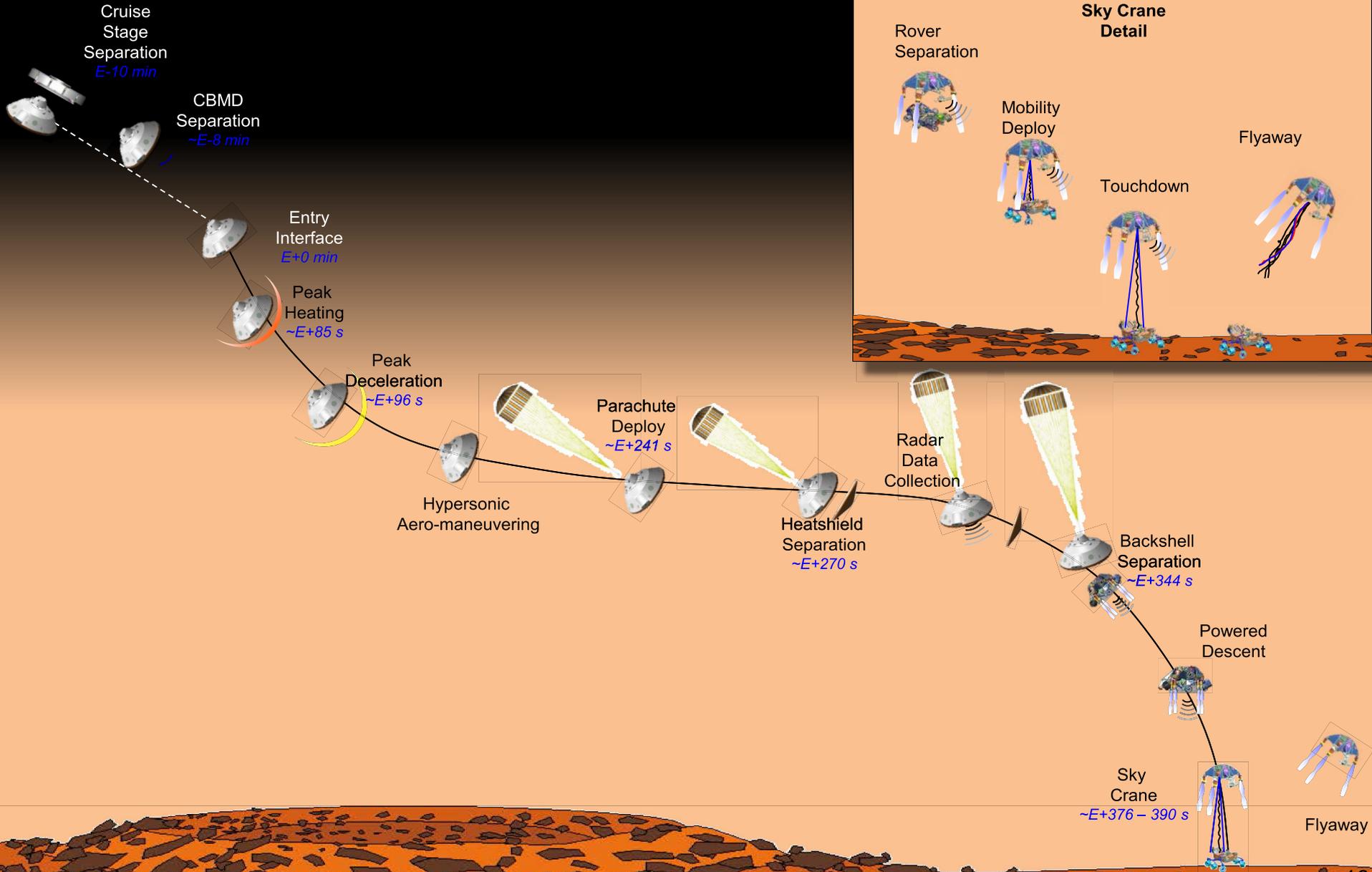
Cruise Stage



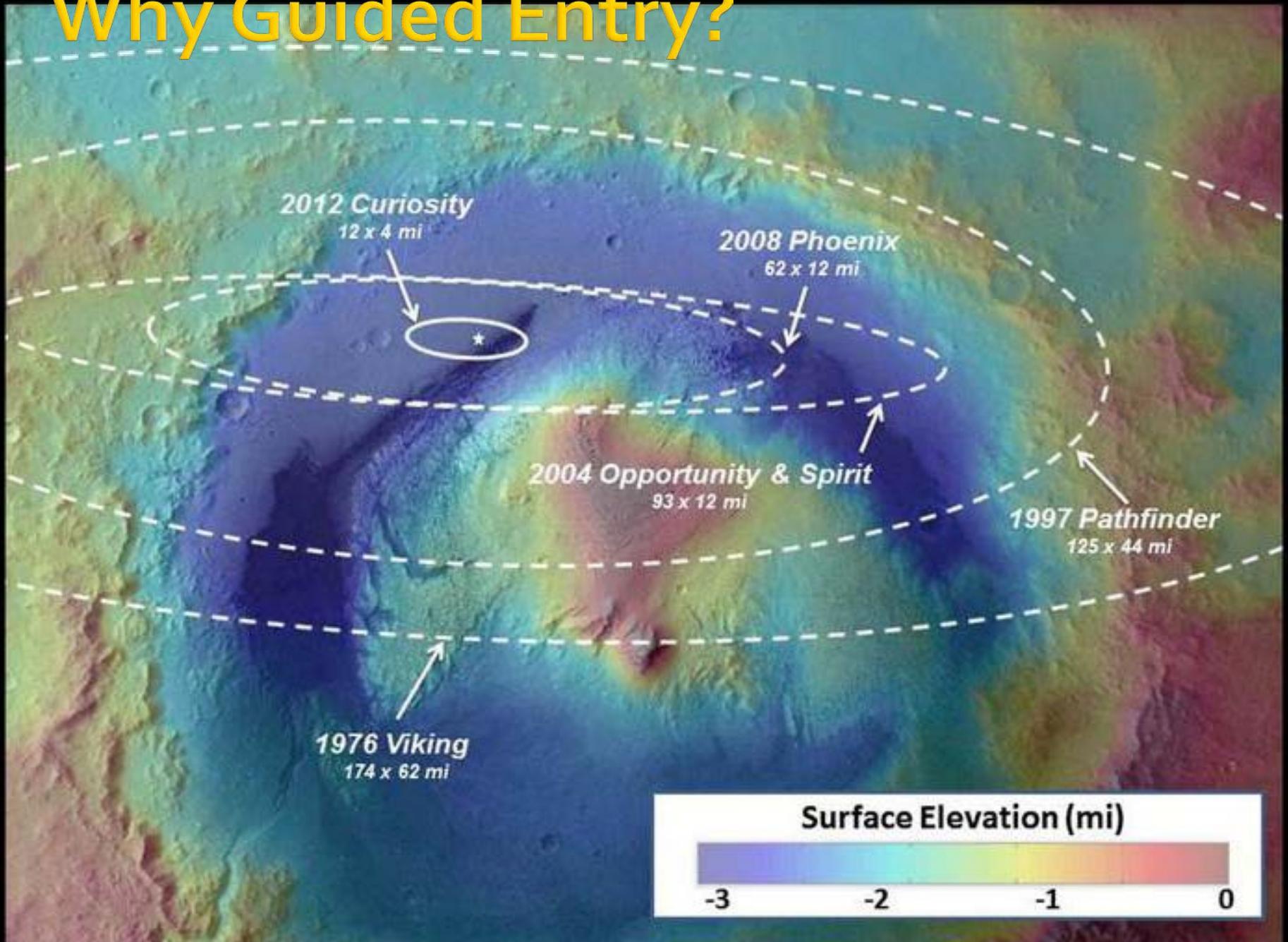
# MARDI Camera – Do No Harm?



# Entry, Descent and Landing Overview



# Why Guided Entry?



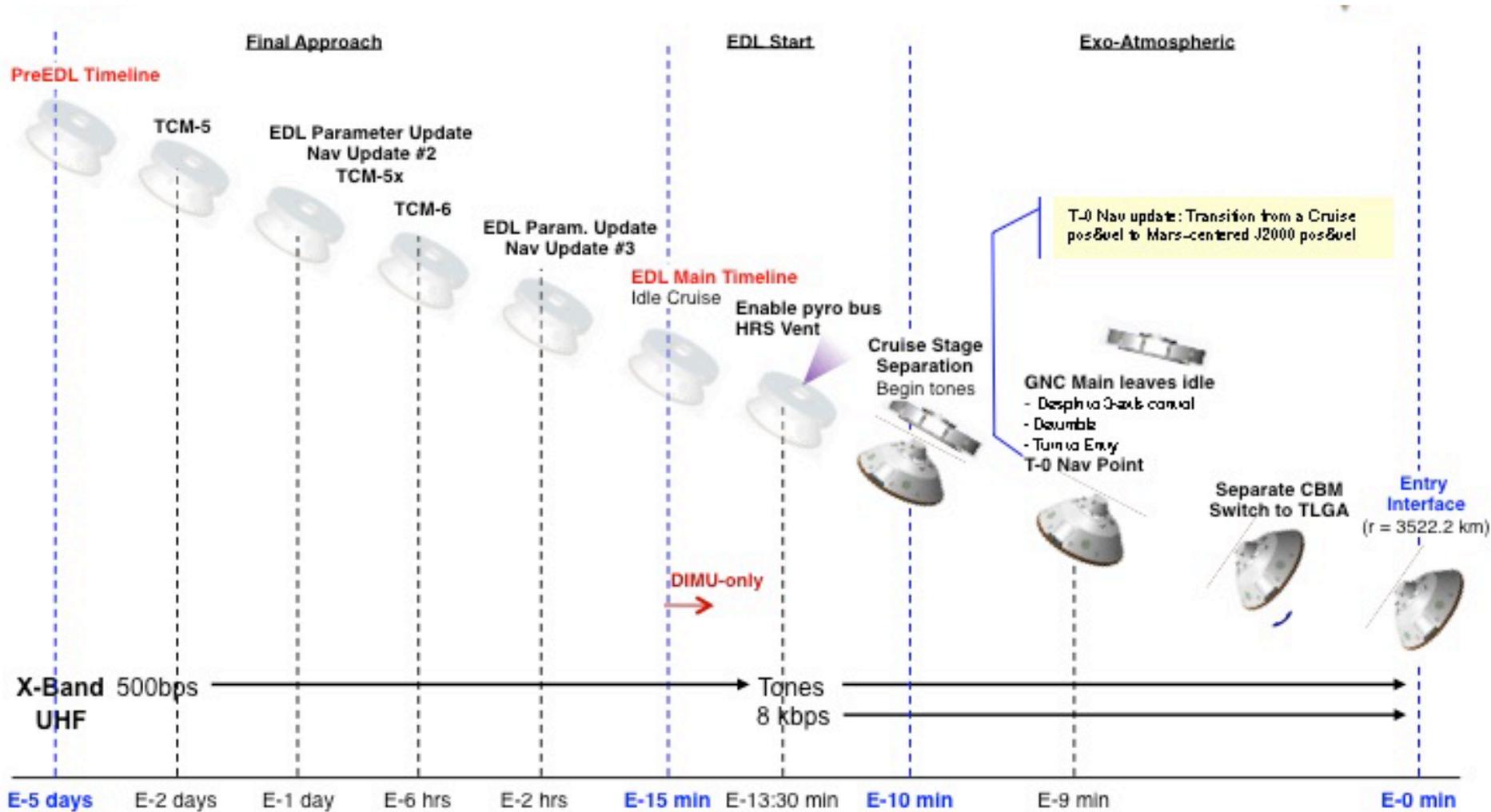
# MSL EDL Control Design

Exquisite pas de deux between two autonomous players: an EDL Timeline actor and Guidance Mode Commander (MC) actor

- EDL Timeline module
  - Executes sequences of timed events - “Anchors” – set at absolute times (relative to other Anchors) or by MC triggers (e.g., achieving threshold velocities)
- Guidance Mode Commander
  - Uses sensor data to call flight dynamics modes – entry guidance, flight on parachute, powered flight, landing

Did NOT want to introduce a third – Fault Protection!

# EDL Timeline – Approach to Entry

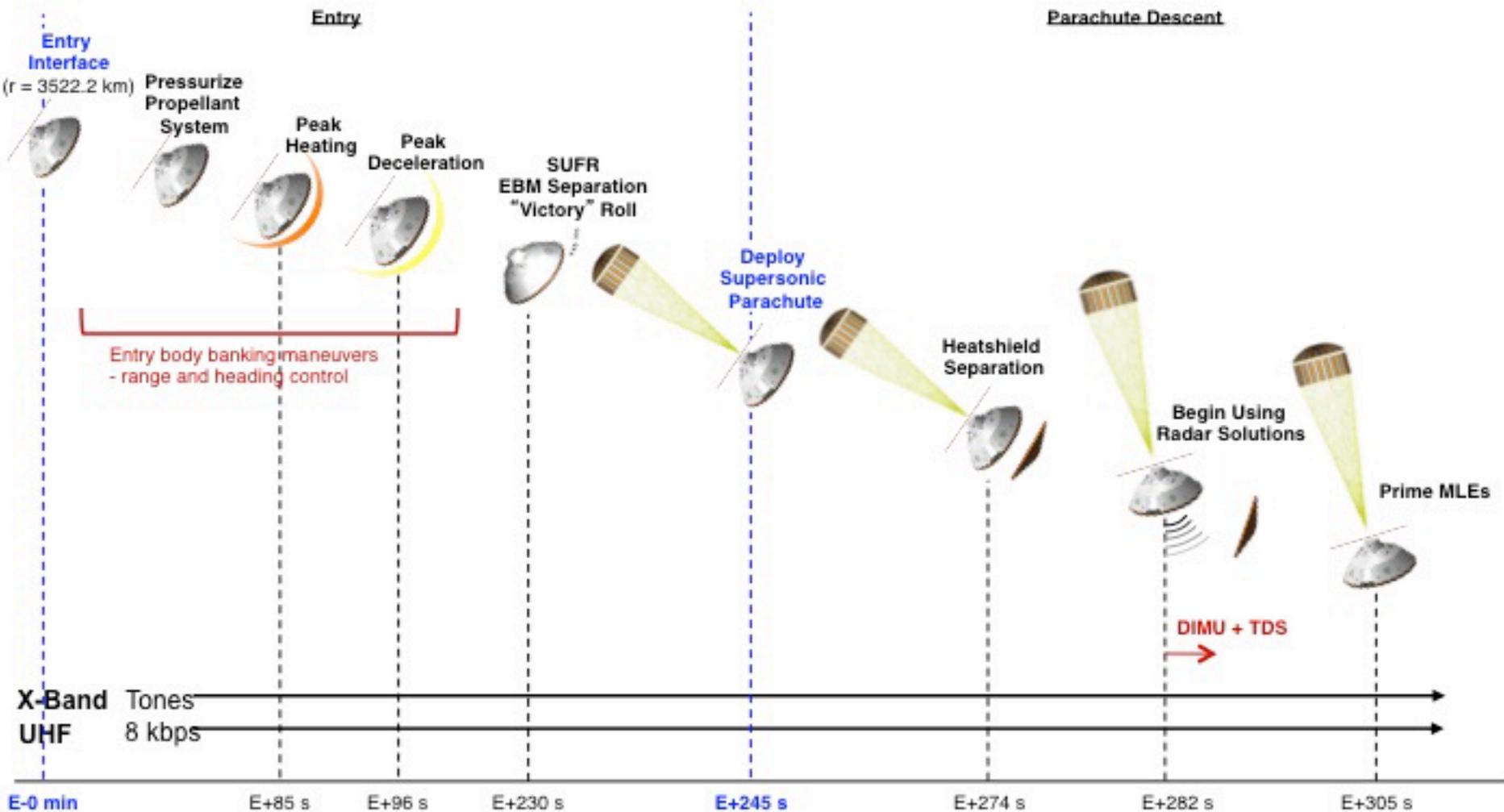


All FP enabled (single fault tolerant ops)

SFP responses disabled (zero fault tolerant)

Backup computer "Second Chance" enabled

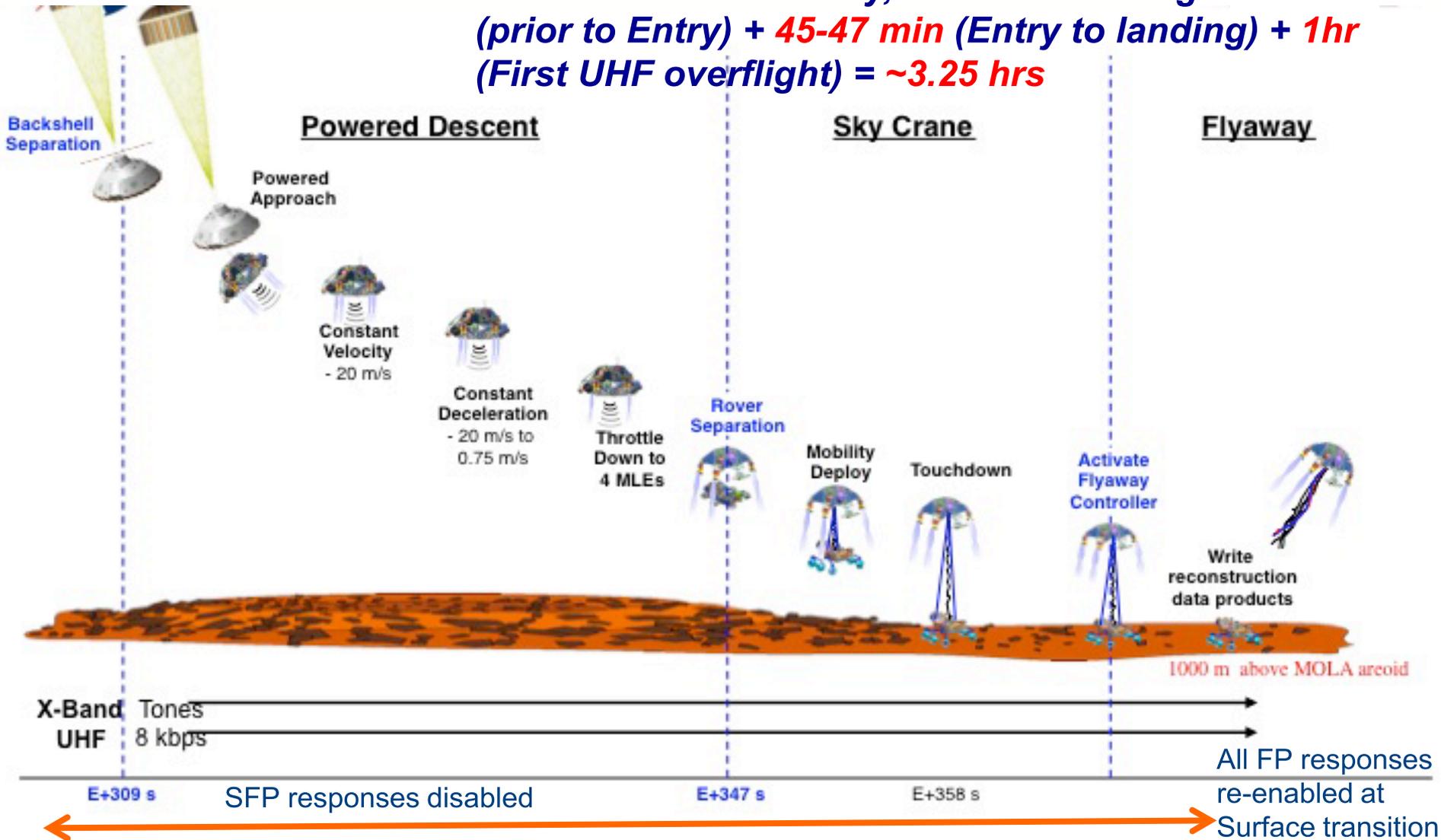
# EDL Timeline – Parachute Deploy



← SFP responses disabled (zero fault tolerant) →  
Local Monitors still trip/run

# EDL Timeline – Landing

*Total FS Full Autonomy, No Commanding = ~ 1.5hr (prior to Entry) + 45-47 min (Entry to landing) + 1hr (First UHF overflight) = ~3.25 hrs*



# How to tell testing is comprehensive?

Consider the ways we can look at the system

- Defined success criteria for landing
  - Pyro timing, computer messaging, dynamics envelopes; criteria all plugged into analysis tools to give green, yellow or red light to each test run
- Address and test Known Knowns
  - Specific Verification Items (pyro functionality, etc) defining proper modes of the Flight System
  - EDL Functional Certifications, defining how the functional components of the system need to behave correctly for overall success
- Address and test Known Unknowns
  - Monte Carlo runs, varying atmospheric/flight parameters to bound system performance
  - Fault protection testing, applying known faults to system to verify recovery
- Address and test Unknown Unknowns
  - Stress testing, throwing faulted situations at system without defining specific faults that may have caused them (e.g., muting all telemetry)

# Verification/Validation Approach

- MSL's core autonomous systems (e.g. entry descent and landing, fault protection, sleep/wake) assumes that the DESIGN is correct and that any off-nominal event is due to environmental effects or hardware failure.
  - Defects, however few, undermine this assumption.
- Primary pathway to eliminate design defects is through systematic testing.
  - One testbed to test cruise and EDL
  - Another testbed to test the rover
  - Software simulations capability
- There is not enough time to test all of the permutations and combinations.

# V&V Summary – Overlapping Approaches

- Flight Dynamics
  - Simulation: Multiple 100K Monte Carlo runs
- Flight System
  - Testbed/"Spacebed" test: ~ 800 Verification Items
- Stress testing
  - Testbed/Simulation test: ~300 Stress Test cases
- EDL Functional Certifications
  - Testing/Analysis: ~81 individual EFCs containing total ~900 elements of success tree
- "Second Chance" backup FSW testing
  - Testbed/Simulation test: ~300 Verification Items

# Stress Test Validation Regimes

- **Priority 1 –**
  - Faults the system has been specifically designed for and are expected to be survivable
  - Faults that are likely to reveal underlying dependencies
    - Even if they are “extreme” faults that may result in a crash landing
- **Priority 2 –**
  - Faults that may be survivable but have not been explicitly designed for
- **Priority 3 –**
  - Faults that are not expected to be revealing
  - Faults that are not expected to be survivable and we understand the failure mechanism

# What ended up being surprises?

- Actual EDL *much cleaner* than any test we'd done
  - Many tests compromised by faulty sim/support equipment or test operator error
  - Actual EDL environments were much more benign than simulated environments
  - Most feared problems were “boogiemen”: undefined noise causing resets, etc., which did not materialize
- Conclusions – real EDL did not stress our system and its fault handling, and by extension, our design and testing program cannot be fully vindicated

# What's Next? Mars 2020 Rover

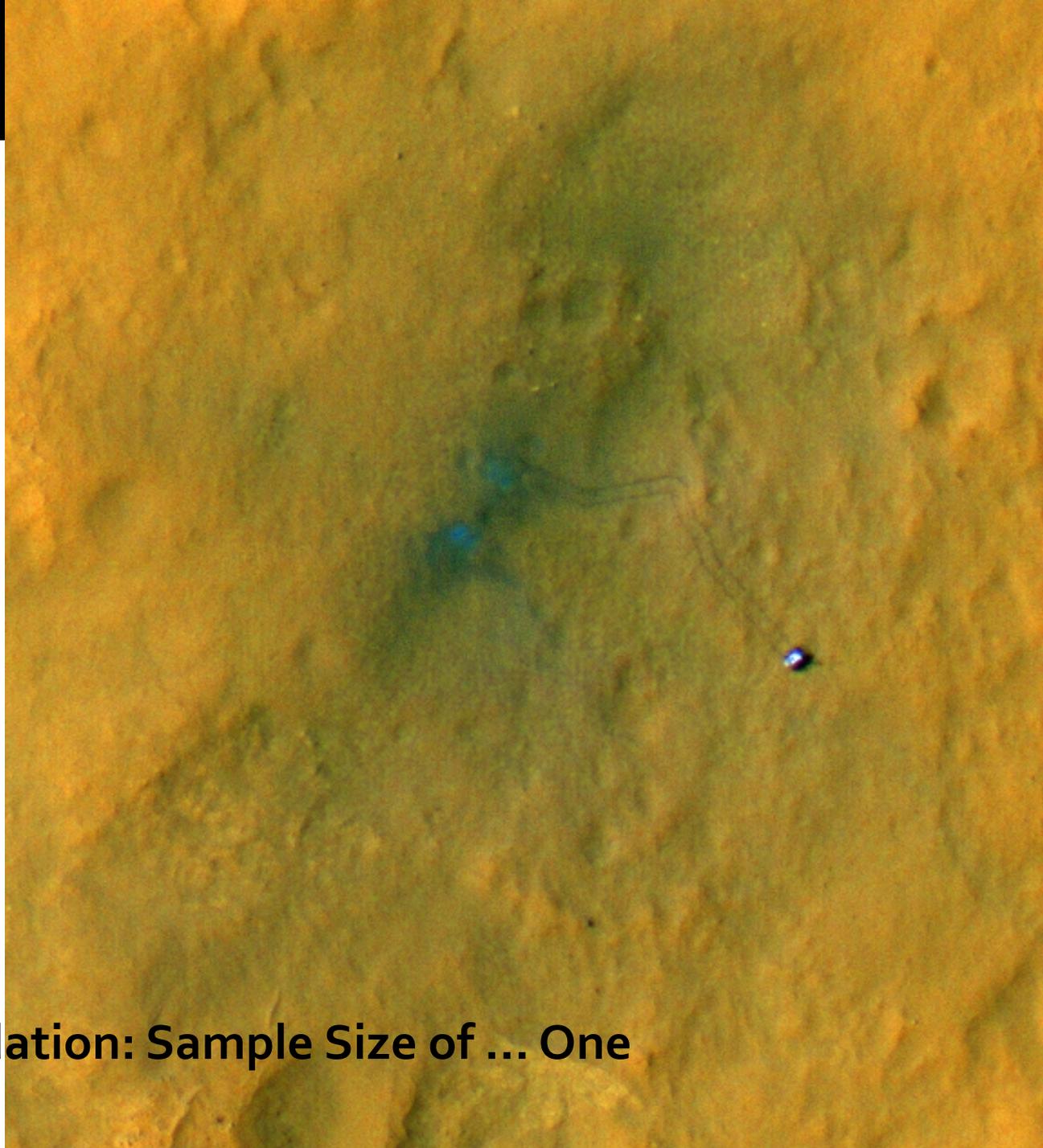
- Premise: Refly MSL
  - Baseline MSL build-to-print
  - New science & tech payloads (still being defined over FY'14)
  - CAN'T MAKE COST BOGIE UNLESS RETIRE RISK BY MAXIMIZING REFLY
- Launch in 2020
  - Vast amounts of HW/SW at post-CDR level
  - Instrument/Sampling System at traditional Phase A level
- System Engineering Organization
  - Need to staff commensurate with both post-CDR and Phase A tasks (and still 7 years from launch)
- Risk Areas
  - Heritage creep/blowback
  - New arm/caching system (cache must be forwards compatible with Mars Program sample return missions yet to be designed!)
  - Payload selection bloat/low TRL selections
  - Parts/personnel obsolescence

# SE Reflection: MSL Challenges

- Overall complexity (holy cow!)
  - Required large team, but then, drove myriad deep information silos
  - Hard to understand scope of work at any one time across project
    - Wide open trade space/concurrent engineering through lifecycle
  - SE not aligned with products; little continuity
- Project bathtub at launch slip (goodbye heritage)
  - Personnel continuity
  - Artifacts continuity
  - Fundamental project risk shift (example, disabling hot-backup redundancies)
- Requirements dilution (how much risk have we retired?)
  - Too many, too flat, too uneven, too outdated
  - Requirements flow-down not aligned with products/deliverers (corollary – functions not well-aligned with products)
  - Inconsistent flow-down of ICD and error-budget type requirements
- Rushed end-game (can't change Solar System geometry)
  - V&V red-giant star armageddon (fast bloat up, much V&V deferred til post launch)
  - SE products struggle to keep up with as-built (design descriptions, etc.)
  - Constant parameter/test configuration uncertainty

# Rover tracks

(photo taken by Mars  
Reconnaissance Orbiter)



MSL Platform Validation: Sample Size of ... One