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
Die Genehmigung ist das Ergebnis einer langen Diskussion und ein wichtiger Schritt für die Entwicklungen in Vorarlberg.

Nach der späten Ankunft des Mars-Rovers des Rätsels unseres Vertrauens, sind die Forscher nun bereit, die Landung zu beobachten und die Daten zu sammeln.
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 ¾ 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!
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

- Cruise Stage
- Backshell
- Descent Stage
- Rover
- Heatshield
Avionics Architecture – Fault Containment Regions

Rover
- Control Computer
- EDL_1553 Bus
- Rover Xband
- Rover UHF
- RCE_FCR

Descent Stage
- Descent Power Assy
- Descent IMU
- Descent Xband
- Descent Motor Controller
- Descent Radar
- OPAM_FCR

Cruise Stage
- Cruise Power Assay
- Shunt Radiator
- CPAM_FCR
- To Cruise Loads
- EDL_1553 Bus
- FSW-ctl’d Thermal Htr + PRTs
- Analogs
- Relays
- Sun Sensor
- Star Scanner
- Analogs
- Relays
- FSW-ctl’d Thermal Htr + PRTs
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

PRIME Control Computer

Backup Control Computer

RPAM

Control

Telemetry

Telemetry

IMU

UHF Radio

Pumps

Rover Pyros

Descent Stage

DPAM

Control

Telemetry

Telemetry

Telemetry

Telemetry

Motor Ctrl

MEDLI/MARDI

Motors

X-Band Radio

Radar

IMU

Descent Pyros

Cruise Stage

CPAM

Control

Telemetry

Telemetry

Telemetry

Telemetry

Star Scanner

Sun Sensor

Pumps

Essential EDL
Non Essential but Active
Off/Inactive
MARDI Camera – Do No Harm?
Entry, Descent and Landing Overview

- Cruise Stage Separation: 
  - E-10 min

- CBMD Separation: 
  - E-8 min

- Entry Interface: 
  - E+0 min

- Peak Heating: 
  - E+85 s

- Peak Deceleration: 
  - E+96 s

- Hypersonic Aero-maneuvering

- Parachute Deploy: 
  - E+241 s

- Heatshield Separation: 
  - E+270 s

- Radar Data Collection

- Backshell Separation: 
  - E+344 s

- Powered Descent

- Sky Crane: 
  - E+376 ~ E+390 s

- Flyaway
Why Guided Entry?

- 2012 Curiosity: 12 x 4 mi
- 2008 Phoenix: 62 x 12 mi
- 2004 Opportunity & Spirit: 93 x 12 mi
- 1997 Pathfinder: 125 x 44 mi
- 1976 Viking: 174 x 62 mi

Surface Elevation (mi):
-3 to 0
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

- **PreEDL Timeline**
  - TCM-5
  - EDL Parameter Update Nav Update #2 TCM-5x
  - TCM-6
  - EDL Param. Update Nav Update #3

- **Final Approach**
  - EDL Main Timeline
  - Idle Cruise
  - Enable pyro bus HRS Vent

- **EDL Start**
  - cruise stage separation
  - begin tones

- **Exo-Atmospheric**
  - GNC Main leaves idle
    - despins Quad conical
    - Dervees
    - Tuned Entry
  - T-0 Nav Point
  - Separate CBM Switch to TLGA
  - Entry Interface
    - \( r = 3522.2 \) km

- **X-Band UHF**
  - E-5 days E-2 days E-1 day E-6 hrs E-2 hrs E-15 min E-13:30 min E-10 min E-9 min E-0 min

- **Communication**
  - X-Band 500bps
  - UHF 8 kbps

- **Operational Changes**
  - All FP enabled (single fault tolerant ops)
  - SFP responses disabled (zero fault tolerant)
  - Backup computer “Second Chance” enabled

- **T-0 Nav update**
  - Transition from a Cruise post-Spel to Mars-centered J2000 post-Spel
EDL Timeline – Parachute Deploy

Entry Interface
(\(r = 3522.2\) km)

- Pressurize Propellant System
- Peak Heating
- Peak Deceleration
- SUFR EBM Separation “Victory” Roll

Parachute Descent

- Deploy Supersonic Parachute
- Heatshield Separation
- Begin Using Radar Solutions
- Prime MLEs

Entry body banking maneuvers - range and heading control

X-Band Tones
UHF 8 kbps

E-0 min E+85 s E+96 s E+230 s E+245 s E+274 s E+282 s E+305 s

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