

Challenges and Opportunities of Performing IV&V on an En- Route Science Mission

Presented by:
Jeremy Fienhold, MSIS

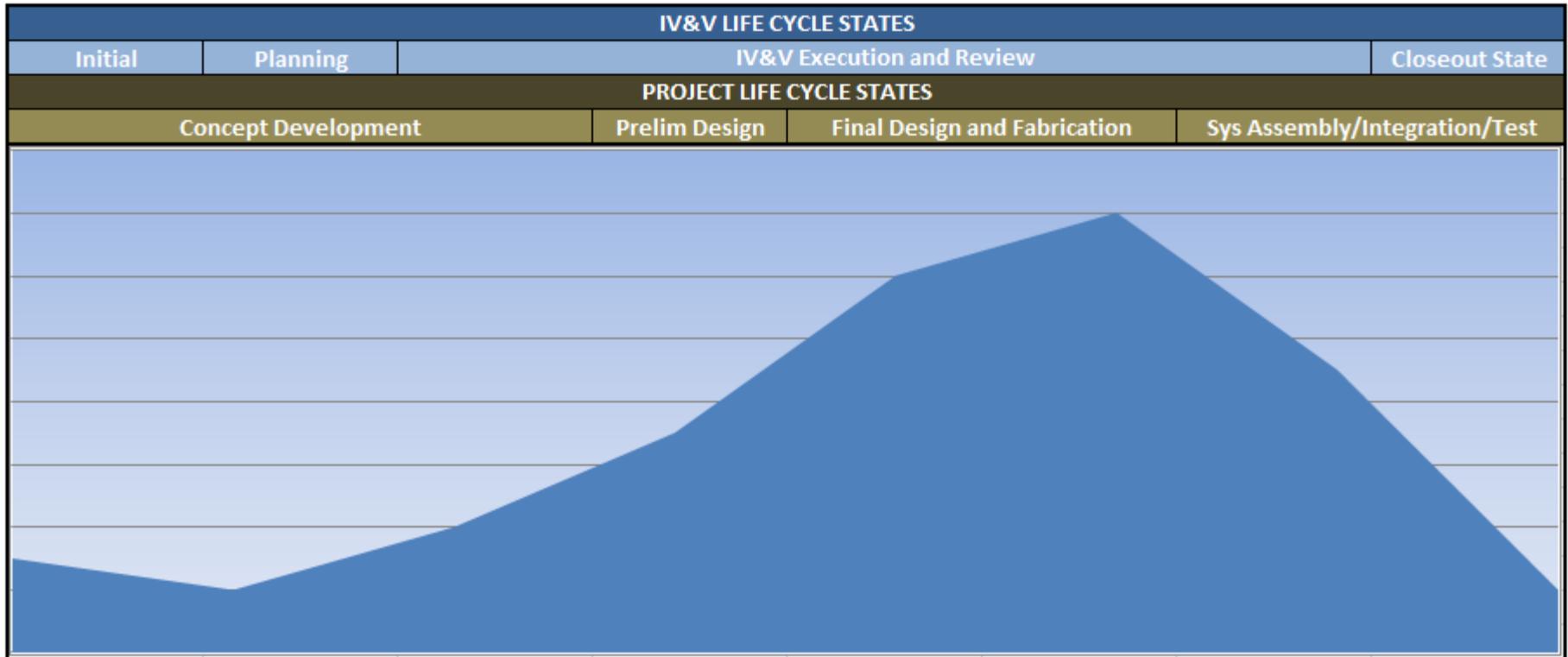
NASA IV&V Workshop
Morgantown, WV
Sept. 2012





Historical IV&V Lifecycle of a Science Mission

- Ramping of effort IV&V uses in a general project life cycle

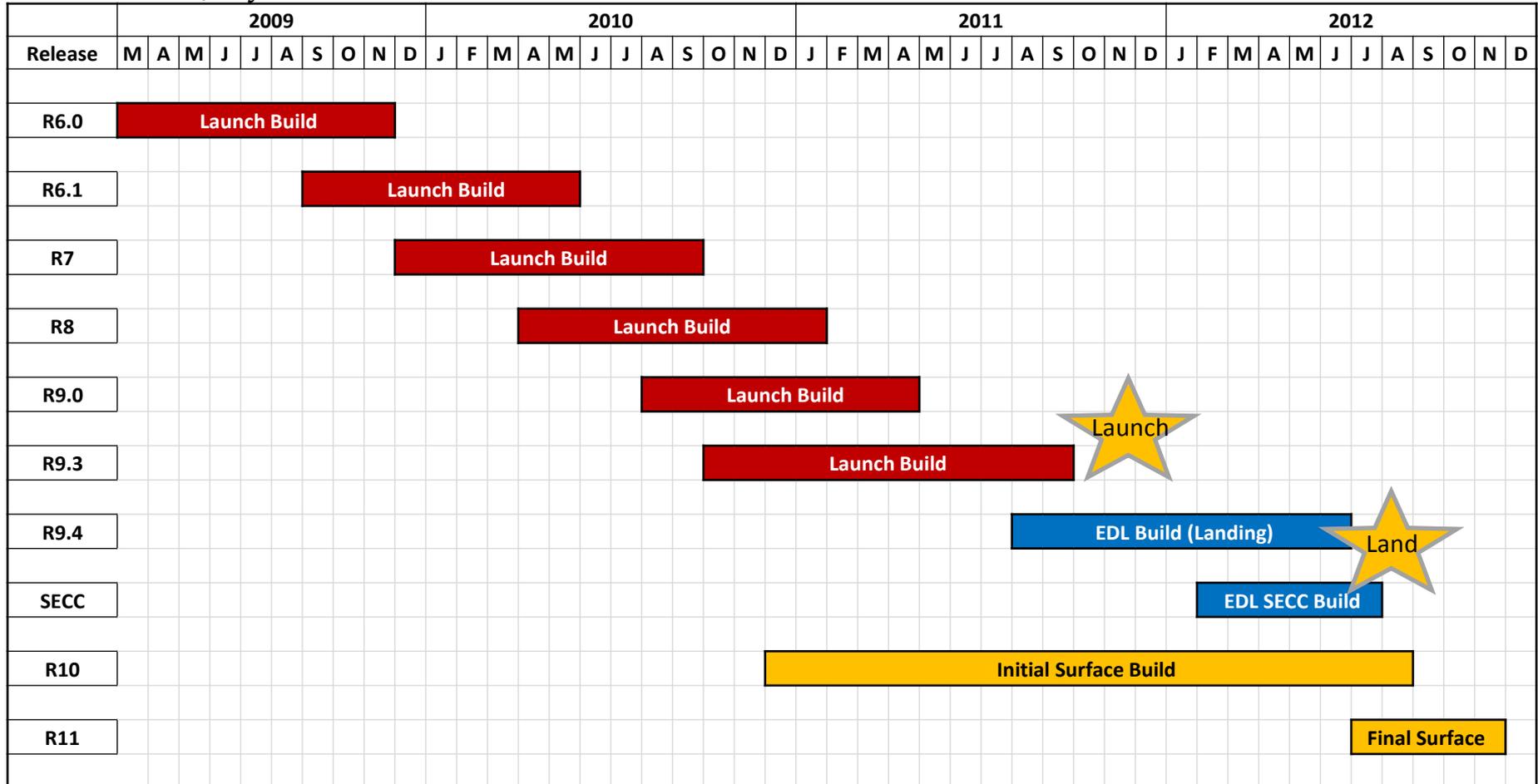


Many times, this is a very iterative process



What The Plan Evolved To

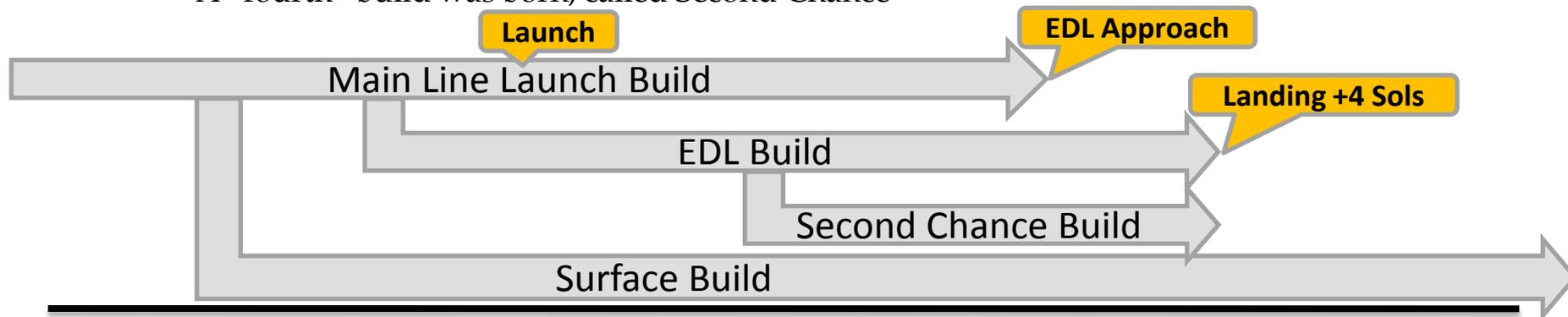
- As of July 2012





Project Side Driving Forces

- As Launch approached in late 2010, the Project decided that instead of forcing all the FSW development to be complete by launch:
 - They could test all hardware and hardware interfaces prior to launch
 - Split FSW Builds into 2 parallel builds: Launch/EDL and Surface, with Surface build development planned for after launch.
 - They could utilize the on-Earth test beds, both simulated and engineering models, to test new FSW development
- Again, as Launch approached in early 2011, for the same reason as above:
 - Split the Launch/EDL build into a Launch and an EDL build, with planned EDL build development after launch.
 - Most of EDL is simulated performance anyway, so testing after launch was not a concern.
- In early 2012, with the extra development time that was bought, the Project decided to utilize the second string, RCE, to provide a backup computer for EDL
 - A “fourth” build was born, called Second Chance





What The Plan Meant to IV&V

- Parallel/Tiered efforts of all stages of analysis: design, implementation, testing
For different builds within each parallel line
 - Launch Build
 - EDL Build (Second Chance FSW included)
 - Surface Build



- How do you keep analysis and change impact synched across different development lines?
- How do you perform issue resolution across different development lines, with different deadlines?
- How do you respond/what can IV&V provide to in-flight issues while still analyzing developmental FSW builds?



IV&V Focus

- IV&V focused on four (4) critical behaviors of the nominal FSW:
 - Fault Protection (FP)
 - Entry, Descent, and Landing (EDL) including Launch, Cruise, & Approach (LCA) associated with pre-EDL and Cross Cutting (CC)
 - Autonomous Navigation (AutoNav)
 - Sampling Acquisition / Sample Handling and Processing (SA/SPaH)

PBRA Results (IV&V scope)	Associated MSL Phase/Domain	Associated IV&V coverage (est)	Comments
EDL	LCA	75%	IV&V PBRA defined EDL to include pre-EDL through touchdown and be stable (power, communicate with earth, ability to upload, etc)
	EDL	97%	
	Cross-Cutting	100%	
	Fault Protection	100%	
SA/SPaH	Surface Sampling	65%	Includes SA/SPaH delivery to instruments but not instruments themselves (SAM, CheMin) Surface general content includes coordinated behavior mgr, actuators and MC, HGA, Comm
	CC, FP	100%	
	Surface General	50%	
Autonomous Surface Operations	Surface General	100%	Mobility considered part of surface general. ASO is a superset of other mobility options (e.g. commanded)
	Surface Remote Science	35%	



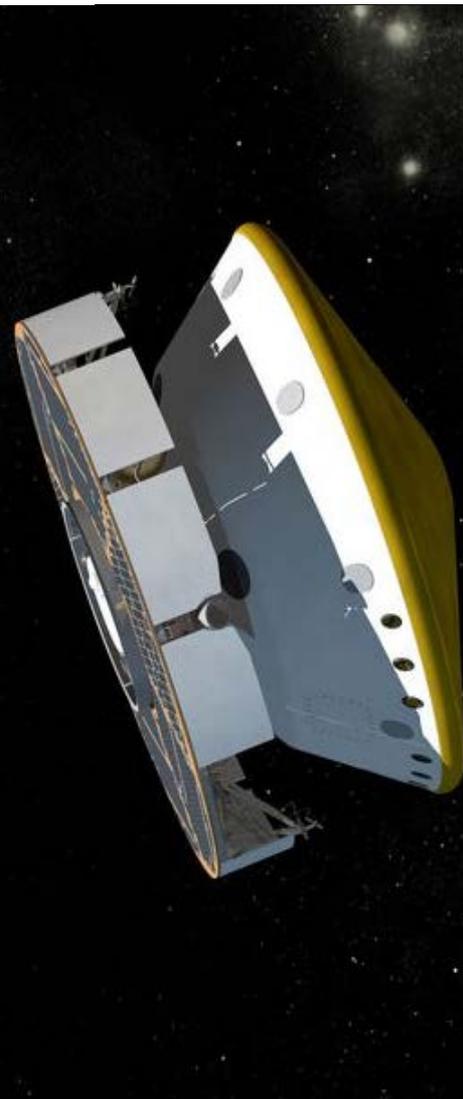
Keeping Synched – Before Launch



- Before the Surface Build split out
 - Some requirements and design were available and IV&V had started analysis. Once the decision was made, all surface analysis was deferred until launch and EDL analysis was complete.
- Before the EDL Build split out
 - Most of the MSL design and implementation analysis had already been completed prior to the split, due to the criticality of EDL to the mission.
 - Test analysis was still in work and continued as did change impact of continued development
- Before Launch
 - Launch and Cruise critical sub-systems and functions needed to be identified and all in-scope requirements, designs and current issues needed to be focused on to ensure that Launch build critical components were “go” for launch
 - EDL build development continued along with IV&V analysis



Keeping Synched – After Launch



After Launch, prior to 2012

- Post-launch on-flight reset forced continued IV&V analysis on Launch build
- EDL build development continued along with IV&V analysis
- Surface build development continued and IV&V had to catch up with remaining Surface analysis

After Launch, in 2012

- Launch build was finally finished
- Second Chance build was introduced and a portion of the IV&V team was set in motion to analyze a “new” build
- IV&V EDL build analysis was wrapping up with issue resolution and change impact ongoing
- IV&V Surface build analysis was continuing

Pre-Landing

- EDL, Second Chance and early surface operation critical sub-systems and functions needed to be identified and all in-scope requirements, designs and current issues needed to be focused on to ensure that Landing build critical components were “go” for landing. Not that it was turning around!
- IV&V Surface build analysis continued with test analysis, change impact and implementation analysis
- Surface Build 11 was split from early surface operations build, Build 10, and development continues post-landing



Resolving Issues Issue

- As noted prior, multiple project milestones presented different focal points for project readiness reviews.
 - Approaching Launch, it became obvious that our current configuration in MKS Integrity (ORBIT) was not going to provide the flexibility needed for MSL. To match the project we needed three distinct “projects” in ORBIT
 - Launch specific issues
 - EDL specific issues
 - Surface specific issues
 - Since the EDL and Surface builds splintered off of the Launch build at a point in time, it was necessary to evaluate whether a TIM was needed in multiple categories.
 - Even with the same TIM in different “projects,” a proposed fix may only resolve for one of the development lines. Which is the correct way to track these particular concerns
 - The different “project” created a very useful way to keep the TIMs in different bins as we approached both the Launch and Landing readiness reviews
 - Made it easy on the project to view their burn down needs in a simple manner without needing IV&V to translate issue summaries
-



In-Flight Anomalies and IV&V Response

- Day of Year (DOY) 333, 2011 - The prime MSL computer performed a “warm” reset 3 days after launch and put the spacecraft in safe mode
 - As luck would have it, because the MSL IV&V team was still working on EDL and Surface analysis, all the knowledge was still there to offer assistance
 - Obviously, the project jumped quickly to action and when IV&V offered, they quickly jumped at the offer of assistance
 - IV&V analysts had just recently looked at about a handful of pre-Launch “red-flag” PFRs where during testing, resets had occurred, but with no repeatability or obvious cause.
 - Considering the magnitude of test runs that were performed compared against the miniscule number of resets that occurred, the project had accepted the risk for launch
 - IV&V concluded that all of the PFRs we looked at, would have most likely been memory corruption induced
 - Once IV&V received the data related to the reset, we were able to conclude that this reset was similar in nature to a couple of the PFRs that were analyzed.
 - The cause ended up being a memory management configuration of the compute element
 - IV&V was able to rule out FSW as the cause of the reset, in fact, the fault protection portion of the FSW handled the error the way that it was designed
-



Lessons Learned and Possibilities for the Future

- BE FLEXIBLE!!!
 - Even when you think you know the plan, it's already changed
 - When the project plan changes, IV&V must re-prioritize to stay in synch
- Cross-analysis provided IV&V analysts the tools to be prepared to move at a moments notice to another task
- Having the right tools set up the right way, simplifies the evidence needed for evaluating different project gateway readiness
- Having the flexibility to draw in the past analyst experience during in-flight operational anomalies is a valuable tool to the mission



QUESTIONS
&
THANK YOU!