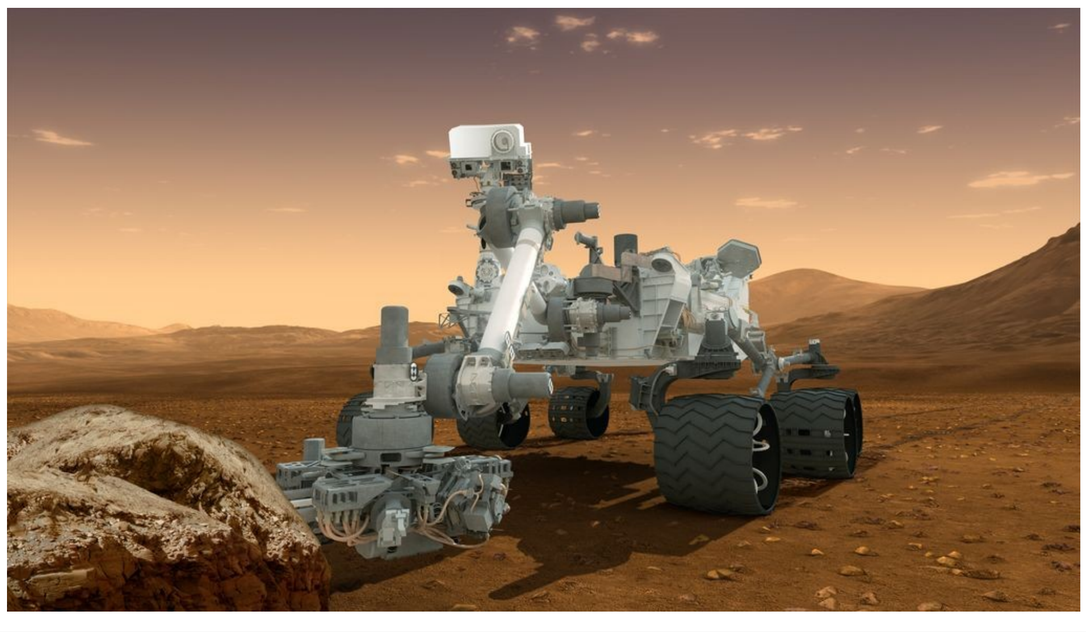
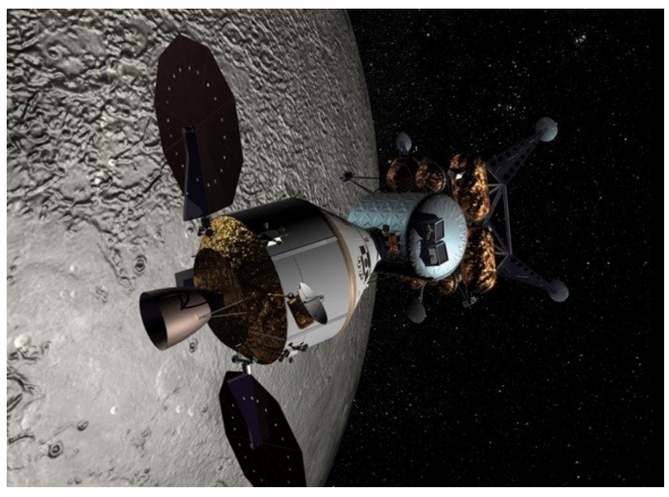
Comparison of IV&V of Uncrewed Projects and Crewed Projects



	Uncrewed	Crewed
Challenges	Many of these challenges apply to **all** projects (uncrewed and crewed) to varying degrees • Need to **prioritize areas on which to concentrate IV&V effort** o IV&V Resource constraints create a potential that not all safety and mission critical software would be analyzed. o Traditionally IV&V effort on uncrewed projects is focused on spacecraft software, with science package/instrumentation software analyzed only if time permits. • **IV&V efforts can be out-of-sync with Development Project schedule** o IV&V often becomes involved later in the software development lifecycle. § This either creates a bow-wave effect, with the analysts continually playing catch-up, or § Reduced analysis of the early products, which can cause errors to be overlooked. o Need to begin analysis when project starts in architecture phase o Occurs less often now than on past projects o The IV&V effort on OSIRIS-REx is an example of when IV&V would like to begin • IV&V impacted by **Development Project schedule replanning and availability of artifacts** o Changes in the funding baseline disrupt project schedules and artifact development. o These changes ripple on down to IV&V. o Historically, IV&V often doesn't receive project documentation until it has been approved for release. However, this varies by project. • Generally **more Software Re-Use** on uncrewed projects o On most uncrewed missions, there is more reuse of spacecraft software while instruments/science package software tends to be new. IV&V tends to concentrate on the spacecraft software (see above). o Heritage specifications, test procedures, scripts, etc. may not be sufficiently updated to represent new project's software. o Late and/or extensive changes may occur to a new project's artifacts. • Need to **obtain and retain people with the right skills** necessary for the analysis o All analysts have a basic set of IV&V skills, but familiarity with the particular spacecraft functions increase the immediate productivity of the team. o Knowledge of the design methodology and tools minimizes the ramp-up time needed before performing meaningful analysis.	• Crewed projects **need to prevent loss of crew** (LOC) even if loss of mission (LOM) occurs o Use of aborts to prevent LOC results in greater complexity, more scenarios o Uncrewed missions may have greater flexibility and time to reconfigure/recover/upload new software load once the spacecraft is in safe mode – less consumables to worry about if there is no crew who must be kept alive • Generally a **large amount of safety and mission critical software** on crewed projects o Increases likelihood that IV&V Resource (funding) constraints will create potential that IV&V cannot analyze all safety and mission critical software. o Shuttle IV&V initially looked at both safety- and mission-critical software (with >40 FTE), but cut back to just safety-critical software as budgets were reduced • Crewed projects often **design for greater redundancy** (2- or 3-fault tolerant), resulting in: o Greater complexity o More scenarios (and more complex ones) o More interfaces (usually) o More integration challenges • Crewed projects often involve **multiple launches/missions of continually evolving vehicles/systems**, with block upgrades made to flying ("operational") program o Multiple launches leads to evolution of vehicle systems and software over time (not "one-and-done") § Need better documentation to enable maintenance and evolution/upgrades o More change activity (engineering changes and anomaly fixes as well as block upgrades) over time § Hard to plan IV&V resources other than generic level of effort because specifics are not known until just before work must begin § Need resources with the right skills - Cross-training - Critical skills maintenance activities § Block upgrades create more integration challenges • Crewed projects usually involve **long-duration development, with sustaining engineering occurring post-first-launch**; uncrewed projects experience similar challenges, but longer durations make the project more susceptible to them o Greater likelihood of Development Project schedule uncertainties and replanning that impact IV&V schedule and resources, resulting in IV&V Project re-planning § Result from variety of reasons including changes in funding baseline, technical issues, catastrophic events (LOC, LOM, near misses), etc. that disrupt Development Project schedules and artifact development. o Need to maintain IV&V critical skills and knowledge for 20+ years via cross-training and critical skills maintenance activities o Need better documentation to enable maintenance and evolution/upgrades o Greater need to feed lessons learned and root cause analysis into continuous improvement of systems o Increased likelihood of loss of access to or availability of critical IV&V analysis tools § Need alternative or backup for one-of-a-kind tools or testbeds, leading to increased cost or acceptance of risk of downtime in event of failure or loss § Commercial tools generally more accessible/available, but subject to different challenges for which longer duration increases the likelihood - Vendor abandons tool or goes out of business, e.g., MATRIX-X vendor on ISS - Vendor makes undesirable changes to tool driven by larger market, resulting in impacts to IV&V usage - Need to upgrade commercial tools when IV&V PC operating systems upgraded (e.g., Windows XP to Windows 7)
Best Features of IV&V's Approach	• Projects tend to be smaller, therefore, o Get to work on more domains o Shorter development time, however mission duration still can be long, e.g., New Horizon, Dawn, JUNO o Easier to coordinate between Development Project team and IV&V team • Unencumbered by Human rated requirements • Usually little or no post-launch real-time support • Variety of science mission technology, e.g., ion propulsion for DAWN, plutonium power for New Horizon, SpaceWire instrument interface for JPSS • Flight software often has more innovative approaches such as VML (JPL), used on JUNO, GRAIL, MAVEN and others • Autonomous operation requirements due to data latency for deep space missions o Self-reconfigured as needed to react to unplanned events o Self-correcting health management, FDIR (Fault Management) o Safe Mode without panic troubleshooting • IV&V sense of ownership/Involvement on uncrewed missions • Develop and maintain understanding of mission operations and environment	• Retention of critical skills leads to increased confidence in IV&V process o Develop and maintain understanding of operational environment and crew use of the system o Significant domain knowledge (onboard/ground systems/software) and project history • Maintain solid working relationship with development team and project team in general o Strong sense of IV&V ownership; passion for project and project success o Post-launch, real-time mission support; leverage use of IV&V critical skills for the good of the project • Root cause analysis and Corrective/Preventive Action Analysis Processes lead to continuous process improvement by learning from mistakes and process escapes • Quick response to critical issues; Risk assessment in timely manner in order for issues to be properly dispositioned • Dedicated tool development organization affords IV&V analysts with the ability to be able to make specific tool request to aid in timely/more productive completion of analysis

Comparison of IV&V of MPCV EFT-1 and MPCV EM-1 and Beyond

	MPCV EFT-1	MPCV EM-1 & Beyond
Description	• Uncrewed demonstration/test flight • Not required to meet any NASA Human-Rating requirements • Short duration mission (two orbits, few hours) • Very limited Environmental Control and Life Support System (ECLSS) • Limited communications • Stored electrical power only • Guidance and Navigation o Looser landing accuracy o Direct entry o No Dissimilar Backup flight control system o No ascent abort coverage	• Uncrewed but fully human rated test flight (EM-1), eventually crewed flights (EM-2 and beyond) • Required to meet all NASA Human-Rating requirements • Longer duration mission (6-to 8-day lunar flyby for EM-1, longer durations for EM-2 and beyond) • Full ECLSS • Full communications suite • Stored and generated electrical power • Guidance and Navigation o Tighter landing accuracy o Direct entry o Dissimilar Backup flight control system o Full ascent abort coverage
Challenges	• **IV&V for Orion MPCV started post PDR** o IV&V coverage was not available as MPCV program completed requirements development milestones o IV&V is working diligently to provide real-time value o IV&V needs to ask clearly for needed information and/or documentation • EFT-1 has **Integrated Modular Architecture (IMA)/partitioned architecture** o New to NASA, previously unflown on spacecraft o Increased configuration management complexity o Potential to increase system fault tolerance § Partitioned software contains faults, impact of faults are usually limited to the partition § Need to analyze how partitions can fail and protection against such failures o The definition of architecture is different o Architecture imposes CPU burdens greater than monolithic systems with similar functional requirements • MPCV **code will be mostly auto-generated** o Code is hard to read, requiring analysis to be done at a higher level of abstraction o Code can be inefficient o Few analysts on IV&V team have worked with this methodology o Rhapsody tool for design/code is also new for IV&V and NASA human-rated missions • **V&V results of COTS and legacy code in flight software are not available** due to proprietary issues o Significant amount of legacy code for MPCV o COTS and legacy code will not be subjected to comprehensive program V&V o Legacy and COTS code was developed using different standards such as DO-178B rather than NASA-specific processes with associated artifacts • **Innovative development approach** o EFT-1 a "prototype" demonstration flight o Software Requirements Report (SRR) versus Software Requirements Specification (SRS). SRR "rolls-up" several SRS requirements to a high-level single requirement. Verification is performed on the higher level requirements. o Methodology uses non-traditional techniques § Most significant is the auto-generation of flight software § Reviews for auto-generated code is optional § Auto-generated code is run through the unit test tool, LDRA, to ensure adherence to coding standards via static analysis § Architecture, SRS, Design documents are generated from models	All the crewed project top challenges apply plus the following MPCV EM-1 specific challenges: • **Greater autonomy/onboard software-controlled capability** than any previous human-rated spacecraft o Will operate farther from Earth longer than any previous human-rated mission (in both distance and duration) § Crew and spacecraft must be able to solve problems without physical help or, for Mars and asteroid missions, timely communications with the ground (due to transmission time) • **Greater range of operational environment** for various MPCV missions (EM-1 and beyond) compared to prior crewed projects o Expect that operational environment will likely change from flight to flight, unlike Shuttle, ISS, Apollo where the operational environment from flight to flight was essentially unchanged • **Formal verification of SRS requirements** that were informally verified for EFT-1 • **Use of prototype requirements/design/code as base for human-rated system** – reuse or start over from scratch using full-up processes? – unclear at this time what the plan is • **Reduced integration oversight at the HEO-ESD level** requires inter-program initiative at the MPCV, SLS, GSDO, and other elements/programs level to work integration specifics ➔ risk of interface mismatches (not so much at ICD level, but behavior on the other side of the interface) • Affordability #1 driver – "adequate" safety ➔ increased risk acceptance; requires **mindset shift – have to adjust the "right" amount** – not too little (too restrictive, leading to conflict), not too much (unsafe) o How much is "safe enough"? • MPCV **code will be mostly auto-generated** o Code is hard to read, requiring analysis to be done at a higher level of abstraction o Code can be inefficient o Analysts on IV&V team will have gained experience working with this methodology on EFT-1 o Analysts on IV&V team will have gained experience working with Rhapsody tool for design/code on EFT-1, but tool will still be relatively new for NASA human-rated missions
Features of IV&V's Approach	• Validation of requirements will be at SRR level o No validation of SRS requirements • Validation of test cases will be to high-level requirements • Static code analysis tools will not be run on auto-generated code • Tracing of requirements to design and code will be done using Rhapsody tool and models • Will be modest change request analysis or regression testing • Develop and maintain solid working relationship with development team and project team in general o Strong sense of IV&V ownership; passion for project and project success o Ease of access to project documentation  	• IV&V Focus o Target safety-critical requirements o Subject to IV&V Portfolio-Based Risk Assessment (PBRA) and funding, mission-critical software will likely be out-of-scope for IV&V analysis o Likewise, a streamlined approach to verifying fault, redundancy, and interface management requirements will need to be established o Analysis of any necessary regression testing of EFT-1 ➔ EM-1 baseline software o Validation of lower level SRS requirements (instead of high level SRR validation performed with EFT-1) o Validation of test cases will be to lower level SRS requirements • Develop and maintain IV&V critical skills o IV&V analysts need an understanding of operational environments (especially as they change from mission to mission), fault management, redundancy management, interface management and crew use of the system o Significant domain knowledge (onboard/ground systems/software) and project history • Maintain solid working relationship with development team and project team in general o Strong sense of IV&V ownership; passion for project and project success o Ease of access to project documentation o IV&V participation in post-launch, real-time mission support; not only leverages use of IV&V critical skills for the good of the project but increases analyst knowledge of the project • Incorporate Root Cause Analysis and Corrective/Preventive Action Analysis Processes to provide continuous process improvement by learning from mistakes and process escapes. Similarly, integrate Continual Improvement Process to enhance what was done right but could have been done better • Provide analysis and risk assessment of critical issues in a timely manner in order to aid project with proper dispositioning • Utilize dedicated tool development organization (Software Assurance Tools - SWAT) to overcome analysis challenges



John Bradbury, Human Exploration & Operations IV&V Mission Lead, TASC john.w.bradbury@ivv.nasa.gov
James Dell, MPCV IV&V Analyst, SAIC james.d.dell@ivv.nasa.gov
David Frazier, MPCV IV&V Analyst, TASC david.e.frazier@ivv.nasa.gov
Valerie Stewart, MPCV IV&V Analyst, SAIC valerie.m.stewart@ivv.nasa.gov