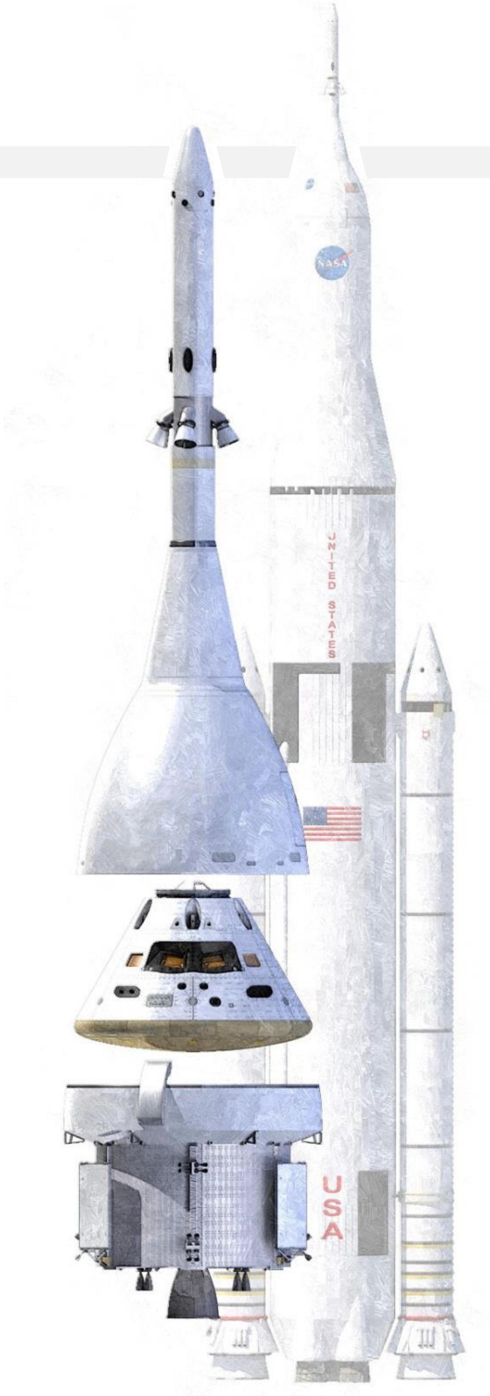


Reality Systems Engineering

PM&SE Briefing
Tim Otterson
September 21, 2016

Introduction

Reality (Political) Systems Engineering

- **Merging the rules and principles of systems engineering into the program realities of cost, schedule, and international partnerships**

- **A summary of the challenges planning and executing the Orion Critical Design Review (CDR) and the approaches employed to adapt systems engineering processes to program realities**

Plans are nothing; planning is everything.
Dwight D. Eisenhower

Outline

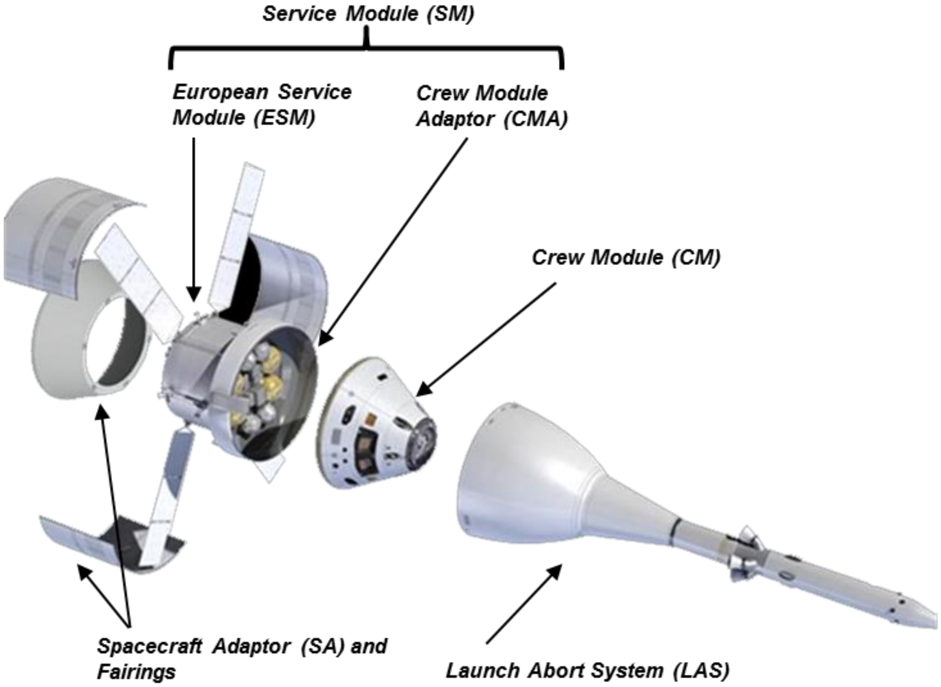
- **Background**

- **Program Realities**
  - Prolonged Design and Manufacturing Schedule Driven by Flat Budget
  - Asynchronous Development with International Partner
  - Incremental and Agile Development

- **Final Thoughts**

Orion Functional Description

Orion Top Level Functions & Configuration
- The Orion Spacecraft will serve as the primary crew vehicle for NASA Exploration Systems Development (ESD) missions in Low Earth Orbit (LEO) and Beyond Earth Orbit (BEO). The vehicle will be capable of conducting regular in-space operations in conjunction with payloads delivered by the Space Launch System (SLS) Launch Vehicle for all missions.



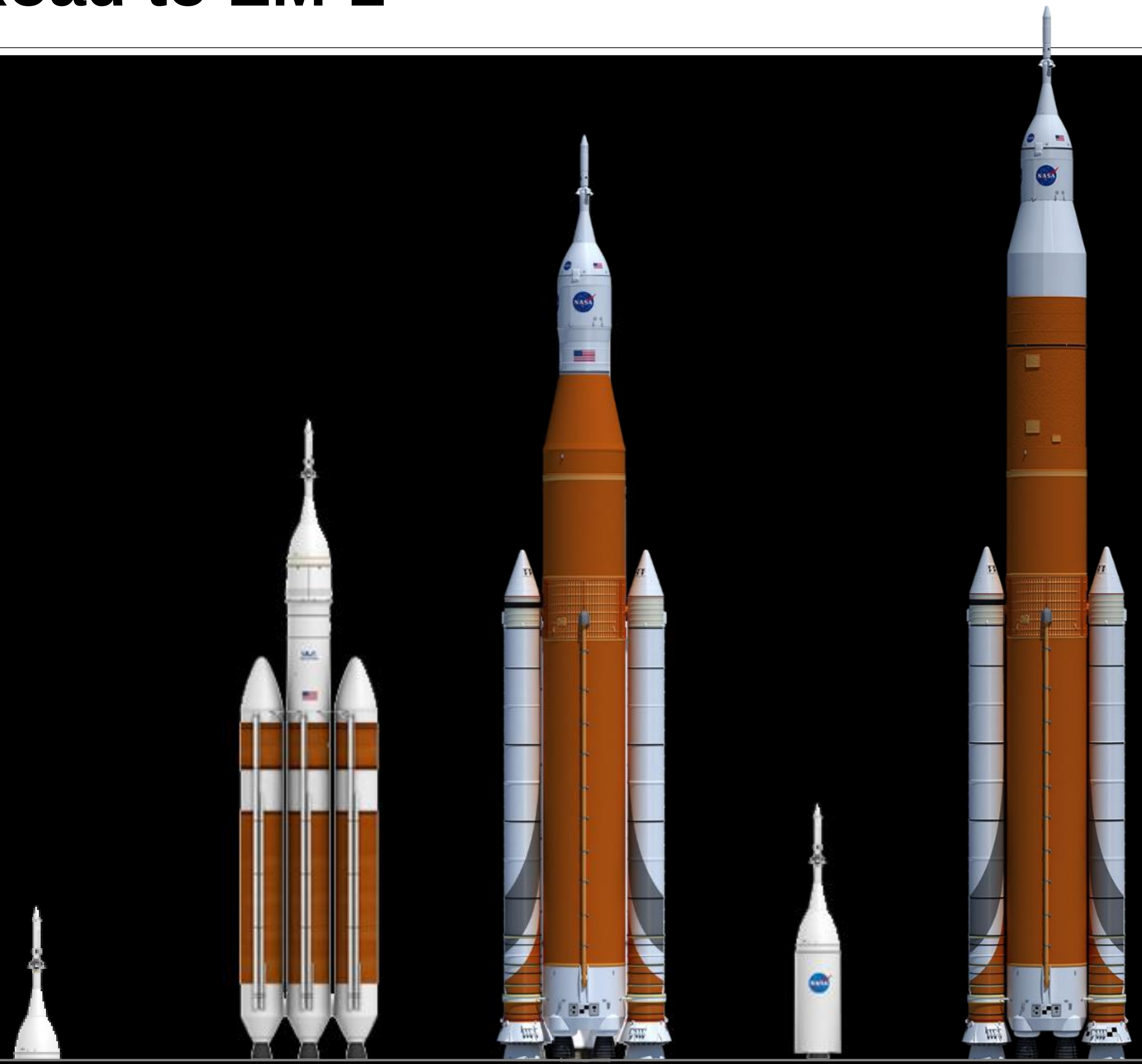
Crew Module (CM) Functions
The CM provides a habitable pressurized volume to support crewmembers and cargo during all elements of a given mission - from Launch Operations to Earth Entry, Descent, Landing, and Recovery.

Spacecraft Adapter (SA) Functions
- Provide structural connection to the launch vehicle from ground operations through orbital injection
- Provide protection for SM components from atmospheric loads and heating during first stage flight

Launch Abort System (LAS) Functions
The LAS provides an abort capability to safely transport the CM away from the launch vehicle stack in the event of an emergency on the launch pad or during ascent.

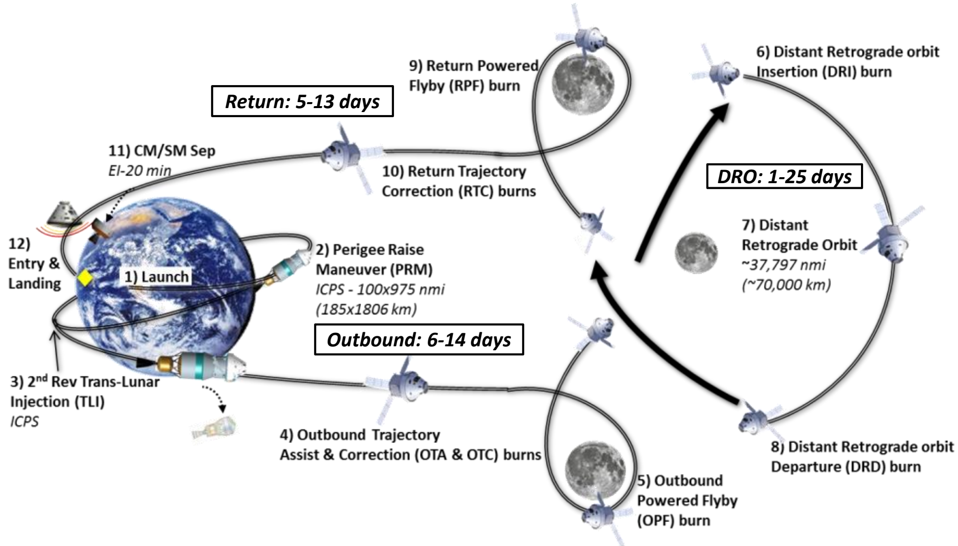
Service Module (SM) Functions
The SM, comprised of the two subcomponents the Crew Module Adapter (CMA) and the European Service Module (ESM), provides services to the CM in the form of propulsion, consumables storage, heat rejection and power generation.

Orion Road to EM-2



- [x] May 2010 PA-1
- [x] Dec. 2014 EFT-1
- [ ] EM-1
- [ ] AA2
- [ ] EM-2

Design Reference Missions: EM-1 & EM-2

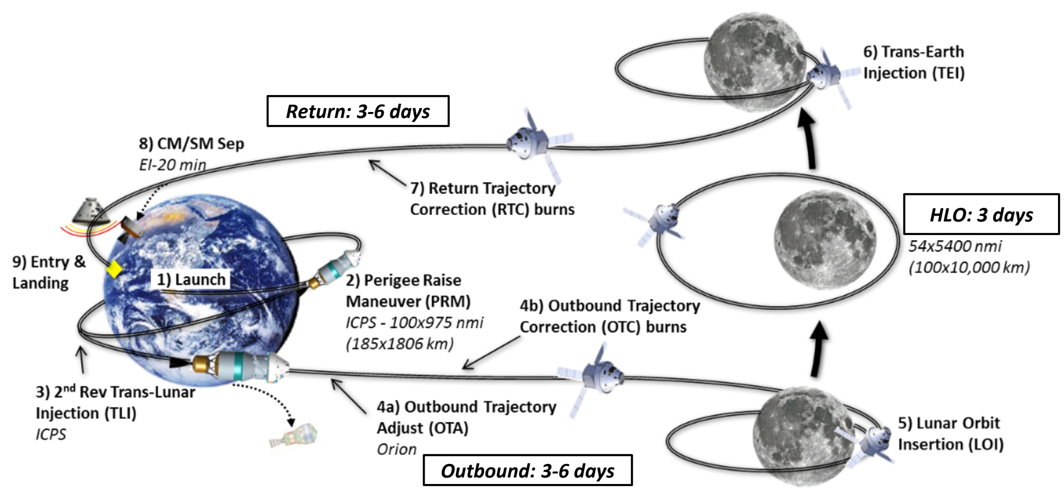


EM-1: Uncrewed Distant Retrograde Orbit (DRO)

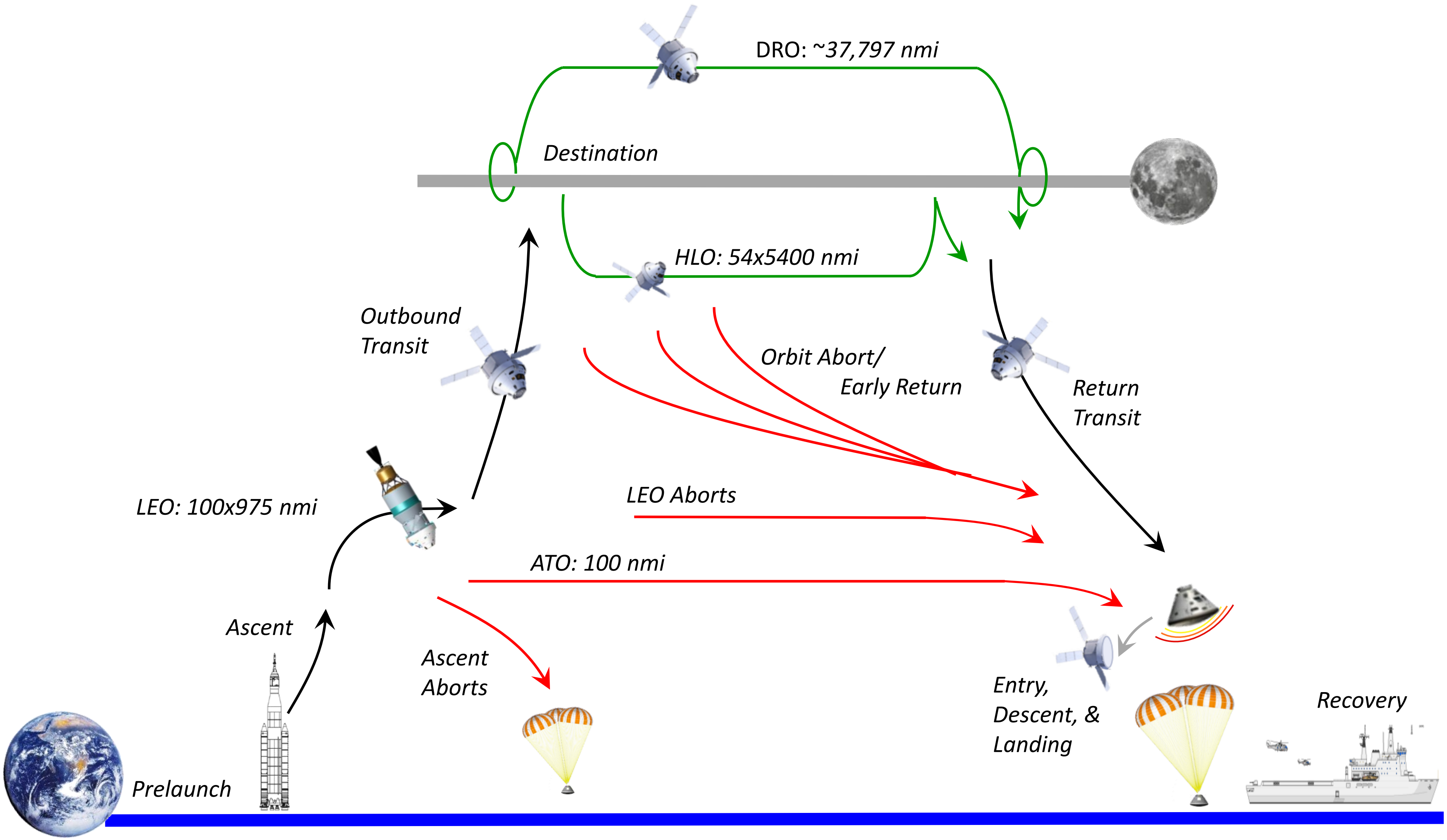
- Total Mission Duration: 21-43 days
- Orion: Fully functional core systems and capabilities for uncrewed missions, and Development Flight Instrumentation system
- SLS: 5 segment SRBs, 4 RS-24D, Interim Cryogenic Propulsion Stage

EM-2: Crewed High Lunar Orbit (HLO)

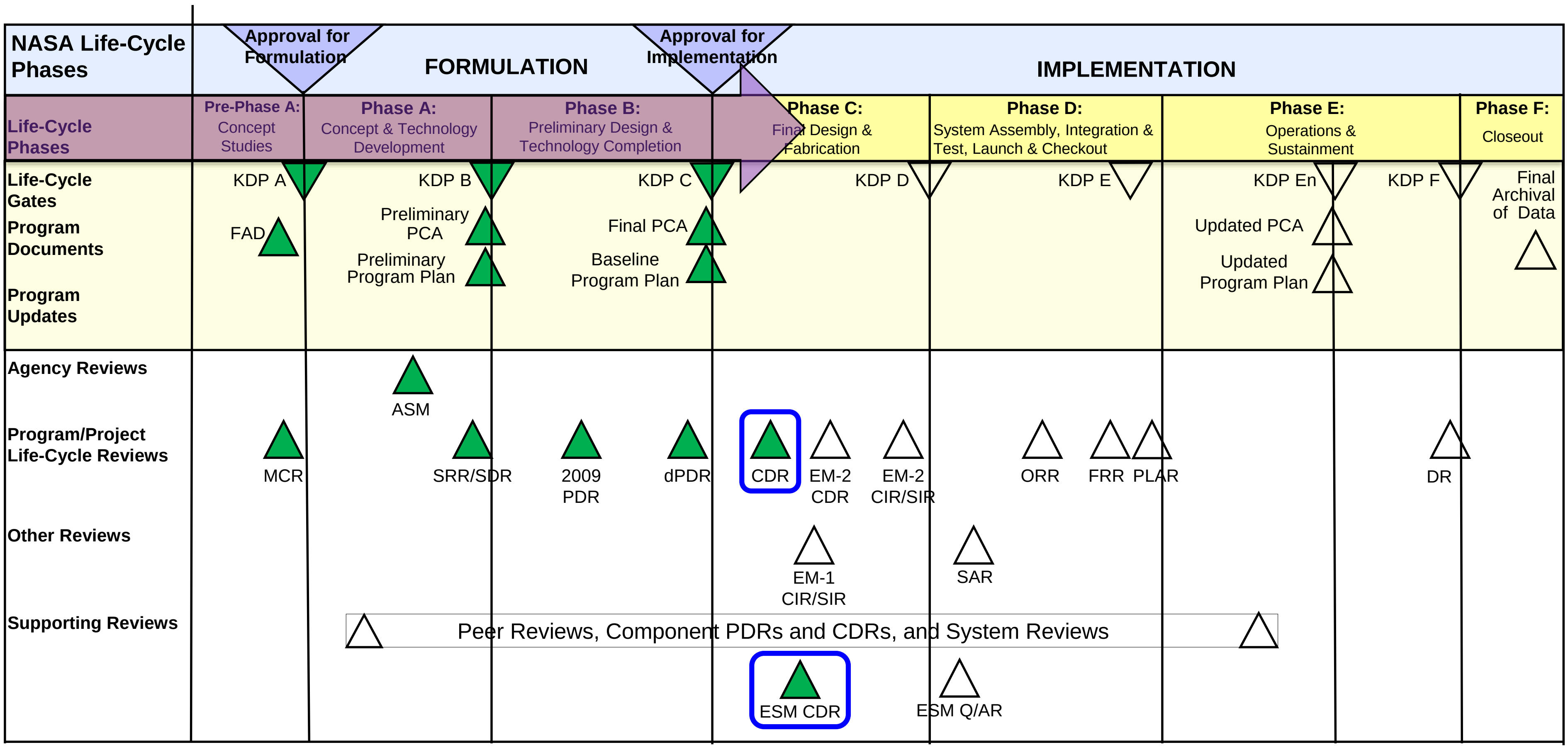
- Total Mission Duration: 9-13 days
- Orion: Added capabilities for crewed missions include full ascent abort, flight crew equipment, and life support system
- SLS: 5 segment SRBs, 4 RS-24D, Exploration Upper Stage
- Other mission profiles are under review for the actual mission



Consolidated Mission Diagram



Orion MPCV Life Cycle Progression



Maintained Compliance with NPR 7120.5E and NPR 7123.1B

CDR Scope

- **CDR addressed the integrated spacecraft at a system and subsystem level**
  - Component level CDRs were conducted and scheduled based on component procurement needs
- **CDR included common aspects of the EM-1 and EM-2 designs, and unique EM-1 subsystems such as DFI**
  - Covers applicable extensible performance requirements such as 4 crew, 21 day capability; and demonstrates a design evolution path to deferred requirements such as EVA and RPODU
- **EM-2 unique systems addressed at EM-2 CDR**
- **CDR will address ESM aspects affecting the interfaces and the integrated spacecraft and subsystems**
  - ESM design details addressed at the ESM CDR
- **CDR will address FSW detailed requirement flow-down, overall design and interface definition, development plans, and test plans**
  - FSW DDRs performed with each incremental software build will cover the detailed FSW modeling, code production, and test results

Summary of EM-2 Unique Content
ECLSS • Air Revitalization • Fire Detection and Suppression • Full CM Pressure Control • Waste Management • Liquid Cooling Garment
Crew Systems/Flight Crew Equipment • Suits • Food System • Stowage System
Cabin Lights, Power Utility Panels
Displays and Controls
Full EM-2 Flight Software • Crew / Piloting Support • Backup Flight Software
Communications and Tracking • Emergency Comm • Recovery Comm • Audio System
Active Launch Abort System

CDR Objectives and Success Criteria

Objectives

Demonstrate that the maturity of the design is appropriate to support proceeding with full-scale fabrication, assembly, integration and test

Determine that the technical effort is on track to complete the system development while meeting performance requirements within the identified cost and schedule constraints.

Success Criteria

CDR Success Criteria complies with NPR 7123.1B and Lockheed Martin Command Media with exception of tailored Software Criteria

Software success criteria was tailored to align with the model-based, incremental development approach of the Orion flight software

Subsystem Success Criteria defined and applied to all SSDRs

No	Success Criteria*	7123.1B Mapping
1	Requirements and Plans	10, 11
2	Verification, Validation, and Test	5, 6
3	Design, Analysis, and Manufacturability	1, 4, 12, 13, 14, 16
4	Technical Interfaces	2
5	Software	17 *(tailored)*
6	Technical Margins	7
7	Safety and Mission Assurance	9
8	Assembly and Integration	6
9	Ground, Mission & Recovery Operations	6, 15
10	Cost and Schedule	3, 7
11	Risk	8

**Full description in Backup*

Performing Vertical and Horizontal Evaluation

- Avionics, Power, and Wiring
- Guidance, Navigation, and Control
- Struct (Int, CM, SM, LAS), TPS, Mech
- CM and SM Propulsion
- ECLS / PTC
- Pyrotechnics
- Landing and Recovery
- Launch Abort System

Vertical Evaluation of Subsystems

Subsystem Design Reviews (SSDRs)

- **Focus to Review / Evaluate:**
  - Design against functional and performance specs
  - Design adequacy and maturity
  - Correct design options have been selected
  - Open issues and adequacy of forward plans
  - Integration of subsystems with the rest of the vehicle
  - Test and verification approach
  - Risks and risk management strategies
  - Subsystem readiness to proceed to fabrication, assembly, integration, and test
- **Identify and disposition subsystem level RFAs**

Horizontal Cross-System Evaluation

- Vehicle Configuration & Architecture
- Test & Verification and Assembly & Integration
- Cross Program Integration
- Human System Integration
- Integ Vehicle and Mission Performance
- Management Review Team

SSDR out-briefs, self-assessment results presented to Management Review Team

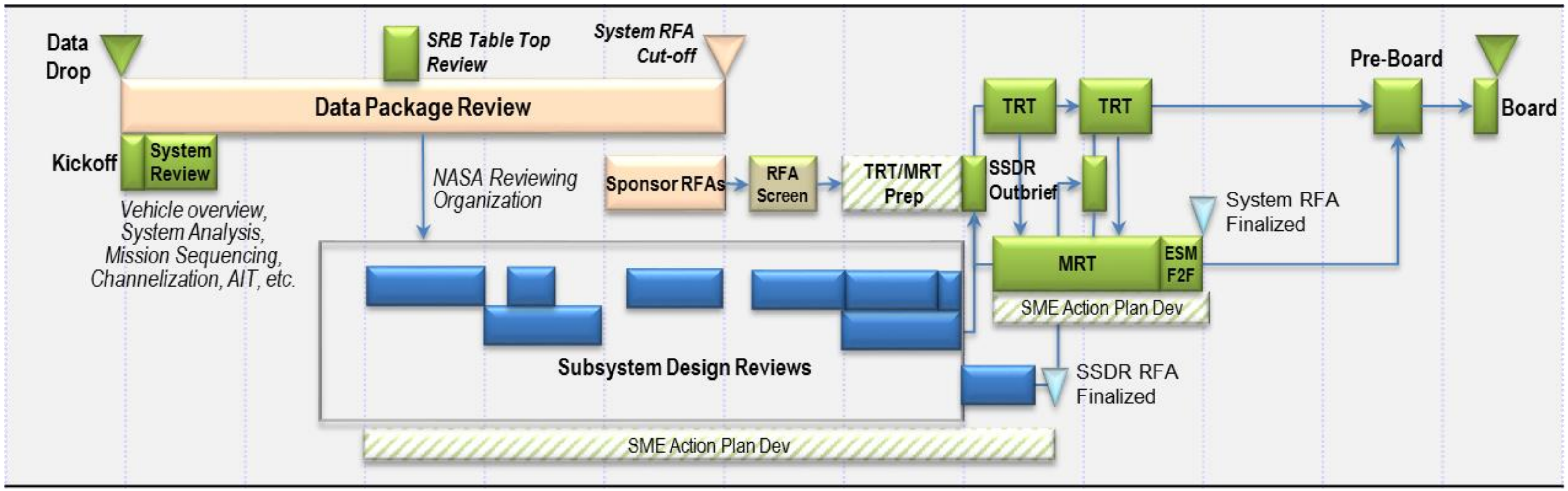
Targeted Review Teams (TRTs)

- Perform a cross-system evaluation of the design organized by system-level integration challenges
- Identify and disposition associated RFAs
- Provide recommendation to proceed to Pre-Board

Management Review Team (MRT)

- Disposition RFAs for overarching programmatic items against success criteria not covered by the Targeted Review Teams (Ex: S&MA, Rqmts)
- Conducts ESM F2F with ESA/Airbus
- Serves as ad hoc Pre-Board during the course of Targeted Reviews to adjudicate issues elevated from the Targeted Review Teams or SSDRs
- Provide recommendation to proceed to Pre-Board

CDR Schedule and Process Flow



- **Process provides for system, subsystem, and cross-system evaluation of the design**
  - **Data Drop:** System and subsystem products released for review
  - **Kick-off:** Review objectives, criteria, process, and product orientation
  - **System Review:** Provides system level overviews of performance analysis, vehicle design overview, test and verification, and assembly and integration
  - **Subsystem Design Reviews (SSDRs):** Vertical evaluation & discussion of issues at the subsystem level
  - **Targeted Review Teams (TRTs):** Horizontal evaluation of key cross system threads

Reality:

Prolonged Design and Manufacturing Schedule Driven by Flat Budget

Reality: Prolonged Design and Manufacturing Schedule Driven by Flat Budget

- **Budget challenges are not new and will be a reality for the foreseeable future**
- **The challenge of a flat budget is that it stretches out the design and manufacturing timeframe adding integration complexities**
  - Results in “leading” and “lagging” subsystem designs driven by the procurement, fabrication, and assembly and integration schedules
- **From NASA Office of Inspector General (OIG), NASA’s Management of the Orion Multi-Purpose Crew Vehicle Program (Report No. IG-16-029):**

“…the Orion Program’s budget profile through at least 2018 has been nearly flat with an annual rate between 5 and 10 percent of total design, development, test, and evaluation costs”

“GAO guidance shows a bell-shaped curve as the optimal funding profile for research, development, testing, and evaluation because more resources are needed as development progresses and programmatic risks are identified and remediated”

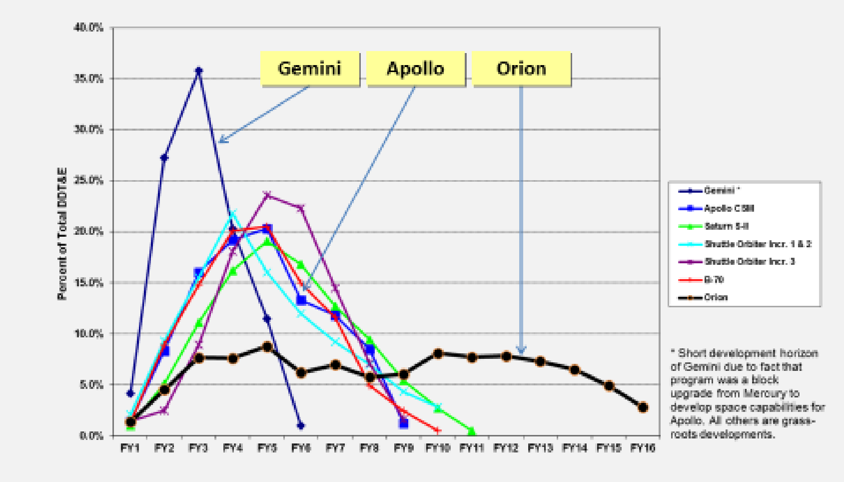


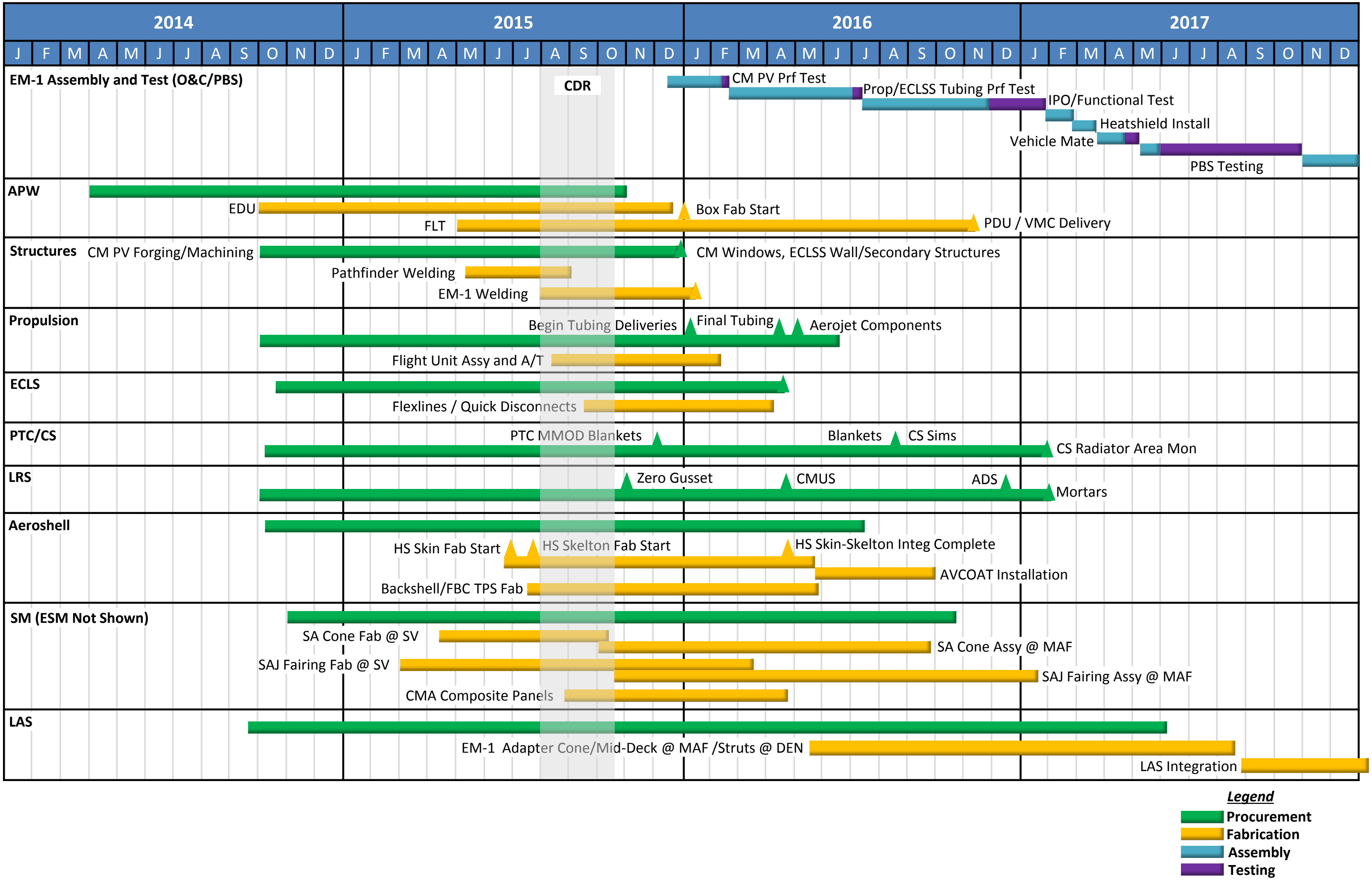
Figure compares Orion Program funding to funding for Gemini, Apollo, and other development programs.

Addressing A Prolonged Design Timeframe

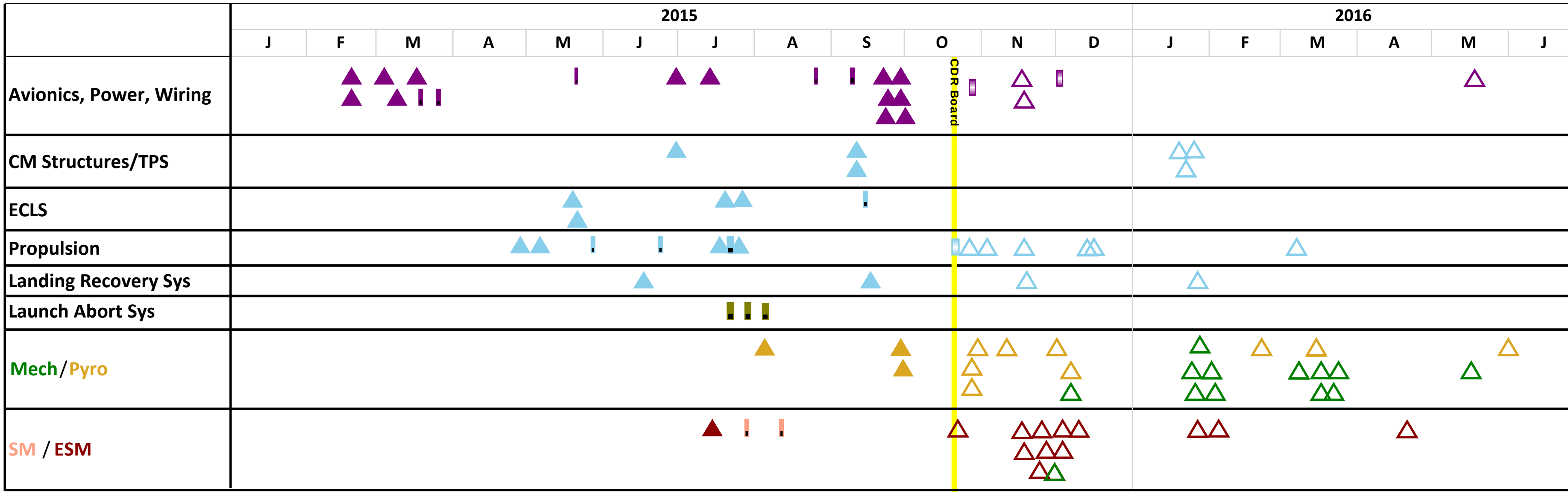
- **Assess the design integration risk to "leading" and "lagging" subsystem or component designs**
  - Maturity of the interface design
  - Maturity of the environments for "leading" designs
  - Integrated subsystem and system performance margins
  - Maturity of "lagging" subsystem or component development
    - Development testing
    - Engineering release schedule
    - Design heritage, technology readiness
    - Degree by which design is coupled to other aspects of the vehicle

- **Establish the needed integration activities and milestones**
  - Incremental design integration
  - Conduct reviews preceding and following the life cycle reviews
    - Lock-down designs and interfaces for "leading" designs
    - Assess subsystem or system level impacts for "lagging" designs
    - Ensure system-level stakeholders engagement

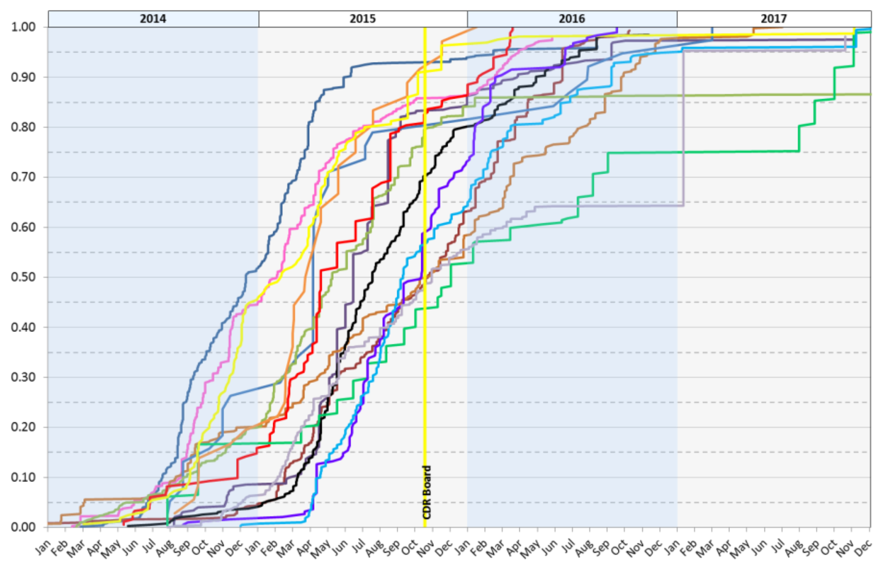
Hardware Procurement and Fabrication Schedule



Component and Engineering Release Schedules



EM-1 Component CDR Schedule



EM-1 Drawing Release Schedule

“Leading” Subsystem: Structures

- **Crew Module structure design and fabrication was a leading design for the EM-1 build**

- **Interim design reviews implemented to enable release of long lead procurements to support build milestones**

Hardware Review

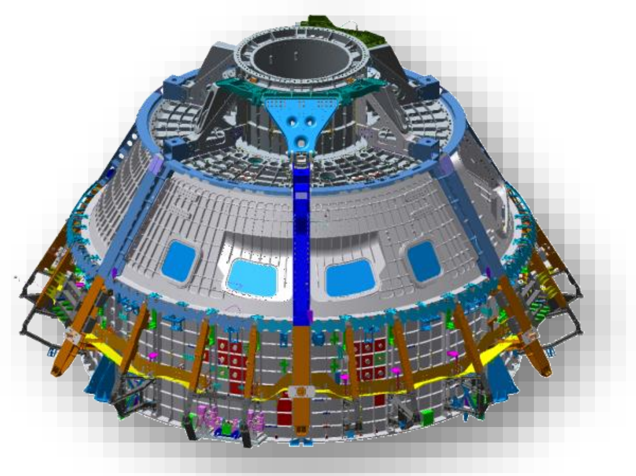
- Interfaces
- Loads and Environments
- Manufacturability
- Materials and Processes
- Test Overview

Stress/Sizing Review

- Load Conditions
- Analysis Approach/Tools
- Preliminary Analysis Results

Mass Checkpoint Review

- Final assessment of mass prior to engineering release

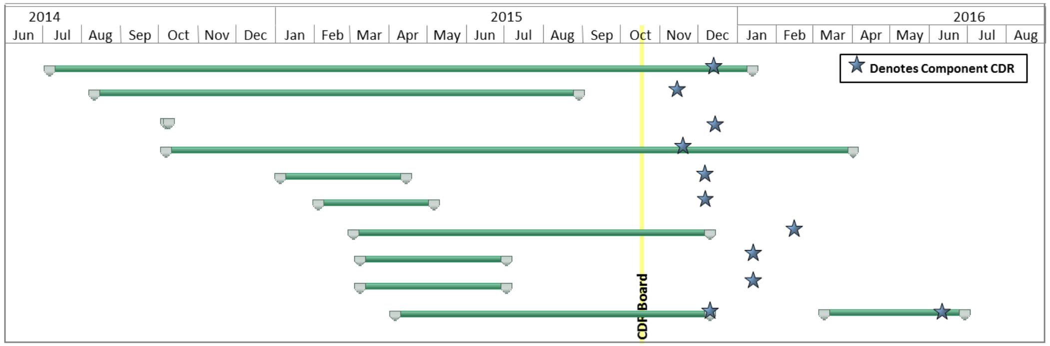


Crew Cabin Structure

“Lagging” Subsystem: Mechanisms and Aeroshell

- **Lagging designs driven primarily to manufacturing needs and budget constraints**

- **Controls put in place to ensure that design integration was addressed and to limit risk at CDR**
  - Interfaces
  - Mass
  - Completion of Development tests
  - TPS Preliminary Sizing
  - Vet incremental analyses (defined by System Stress)



Mechanism Development Test and Component CDR schedules

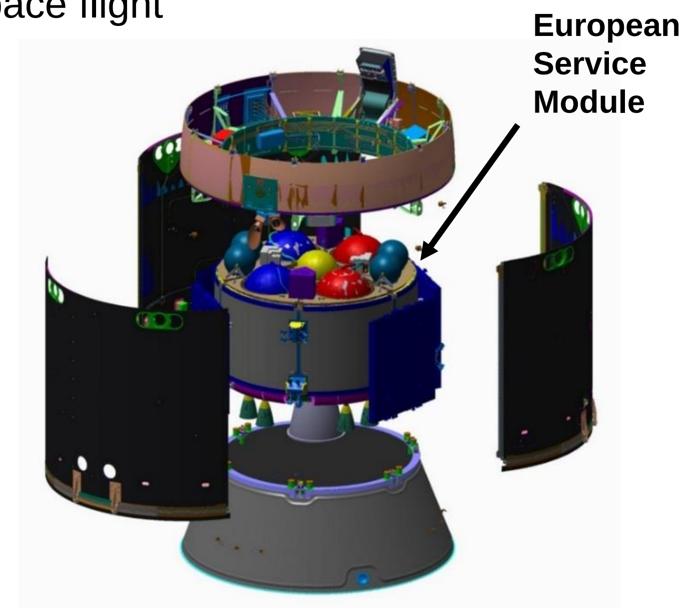
- **Established a Close-Out ERB following the lagging component design reviews**
  - Updated technical baseline
  - Address design integration issues

Reality:

Asynchronous Development with International Partner

European Service Module (ESM)

- **ESM is an integral part of several subsystems**
- **ESM development schedule trails the rest of the Program**
- **ESM supports the following capabilities**
  - In-space translational delta-V capability to transfer the vehicle Provide orbital maintenance and attitude control
  - High altitude ascent abort propulsion after LAS jettison
  - Consumables to support in-space habitable environment while attached to the CM (Water, O2, and N2 storage)
  - Power generation and storage required for in-space flight
  - Primary thermal control while mated with CM
- **ESM interfaces**
  - Structural
  - Consumable storage
  - Thermal control
  - Electrical
  - Software (CMA) – Controllers (ESM)
  - GNC (CM) – Propulsion (ESM)



Addressing Asynchronous Development with an International Partner

- **Define design content to meet subsystem and system development schedule**
  - Data product maturity expectations and delivery schedule
  - Importance of mapping to bilateral agreements
  - Greater importance of effective bilateral design team coordination

- **Be adaptable to schedule changes**
  - To the extent possible de-couple development interdependencies and schedules

- **Establish clear re-integration activities and milestones to manage risk when design content is immature**
  - Leverage existing International Partner reviews
  - Conduct reviews preceding and following the life cycle reviews
    - Lock-down designs and interfaces for “leading” designs
    - Assess subsystem or system level impacts for “lagging” designs
    - Ensure system-level stakeholders engagement

ESM Data Products for System Review

Project Planning
ESM AIT Plan
ESM Verification Plan
ESM Schedule Report
ESM Certification Plans
ESM EMC Control Plan
ESM Instrumentation Plan
ESM Contamination Control Plan
ESM Production Transportation Plan
Natural Environments Assessment Plan
ESM Structural Verification Plan

Specifications and Documents
ESM Specification Tree
ESM Drawing Tree
ESM Product Tree
Functional Design Definition Files
ESM Software System Specification

Performance
ESM Budget Report (Mass, Prop)
ESM Budget Report (Power)
Mission Data Base Report
Interface Control Document
ESM Mechanical Env Support Spec
ESM Ext Thermal Env Support Spec
ESM Equip. Env Test Support Spec
ESM Ionizing Radiation Env Support Spec

Architecture and Design Definition
ESM Arch & Design Definition Report
ESM Design Register (Schematics)
ESM CAD Model

Safety
ESM Safety Hazard Reports for Flight Phase
ESM Ground Safety Hazard Analysis
ESM Probabilistic Risk Assessment

Reliability and Maintainability
MPCV-ESM Production Transportation Plan
ESM Failure Modes Effects Analysis & Critical Items List (FMEA/CIL)

Analysis Data
System Design Data Book
MDPS Design and Analysis Report
Thermal Mathematical Models
THMM Description Report
FEM
Prop Performance Model Description
Prop S/S Performance Analysis
Sun Sensor Design Report
MPCV FM1 KSC Ground Operations Plan
ESM-Mission Operational Data
Channelization Data

ESM Content Expectations for CDR

- **All System Level products incorporate ESM Content**
  - Examples: CAD, MEL, PEL, etc.

- **The SSDRs will address interface and integration aspects of the ESM subsystem design**
  - Overview of the ESM subsystem design including a summary of open design trades, issues, and requirement non-compliances that impact or represent a risk to the integrated system, subsystem or interfaces
  - Details of the subsystem hardware and software interface designs
  - Results of integrated subsystem performance and mission analysis including subsystem level technical margins and technical performance measures
  - Integrated subsystem test and verification, and assembly and integration plans
  - Integrated subsystem operations concepts
  - Integrated subsystem safety and reliability analysis, and risks

- **Review of the ESM provided subsystem hardware design occurred at the ESM component and subsystem CDRs**

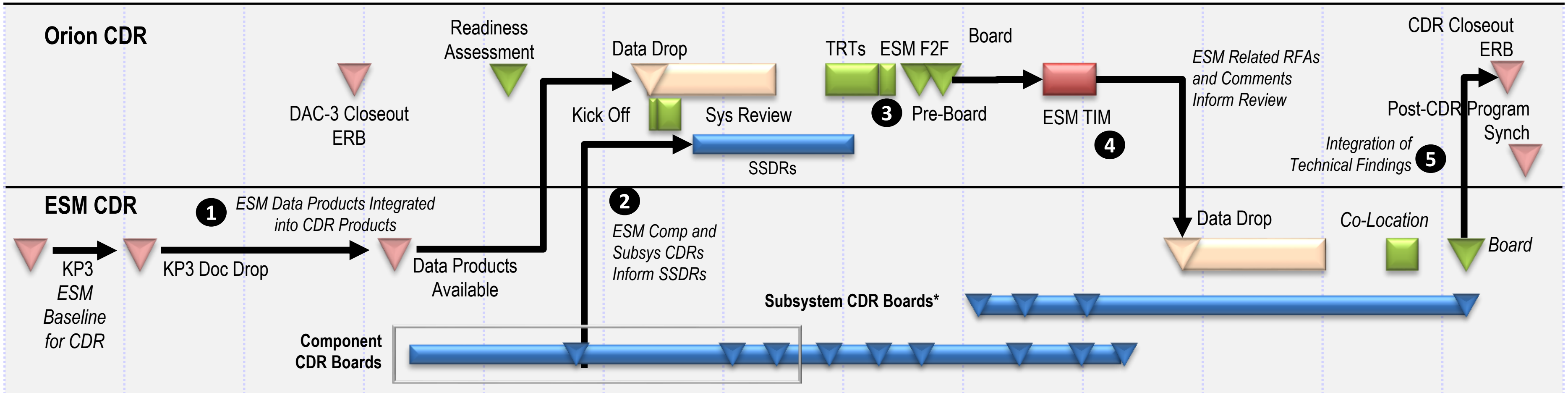
Re-Integration Activities and Milestones

- **Post CDR re-integration milestones and objectives were added to the Program to address areas that did not meet CDR maturity**
  - Results from Component CDRs occurring after CDR Board, such as Aeroshell, Mech and Pyro
  - Results from ESM CDR planned to occur after CDR Board
  - Pre-declared RFAs and significant CDR findings

- **Established CDR Closeout ERBs**
  - Present, discuss, and address technical integration issues resulting from the ESM CDR and component CDRs completed post System CDR
  - Establish updated technical baseline based on the conclusion of the ESM CDR and component CDRs completed post System CDR
  - Attendance to include stakeholders and CDR Pre-Board members

- **Established a Post-CDR Program Synch meeting**
  - Address critical actions from the CDR Closeout ERBs
  - Status results of post-ESM CDR re-integration analyses, design and verification activities
  - Assess closure progress of high criticality RFA's and Board actions (including ESM CDR RIDs)
  - Attendance to include stakeholders and CDR Board Members

ESM CDR Integration Schedule



Integration activities and milestones established to mitigate impacts of the Orion CDR preceding the ESM CDR

1. ESM content incorporated into the system level products
2. ESM content affecting the subsystem interfaces and the integrated subsystem are addressed at the SSDRs
3. ESM F2F established to gain ESA/Airbus agreement on ESM related RFA closure plans, and inform ESA/Airbus on ESM CDR relevant comments
4. ESM TIM will discuss ESA/Airbus ability to capture the relevant ESM CDR comments in the ESM CDR data products
5. ESM CDR technical findings and any necessary technical baseline changes will be addressed at the CDR Closeout ERB. Results of the CDR Closeout ERB, status of any required re-integration activities, and a status of high criticality RFAs will be reported out at the Post-CDR Program Synch.

Reality:

Incremental and Agile Development

Flight Software Approach to CDR

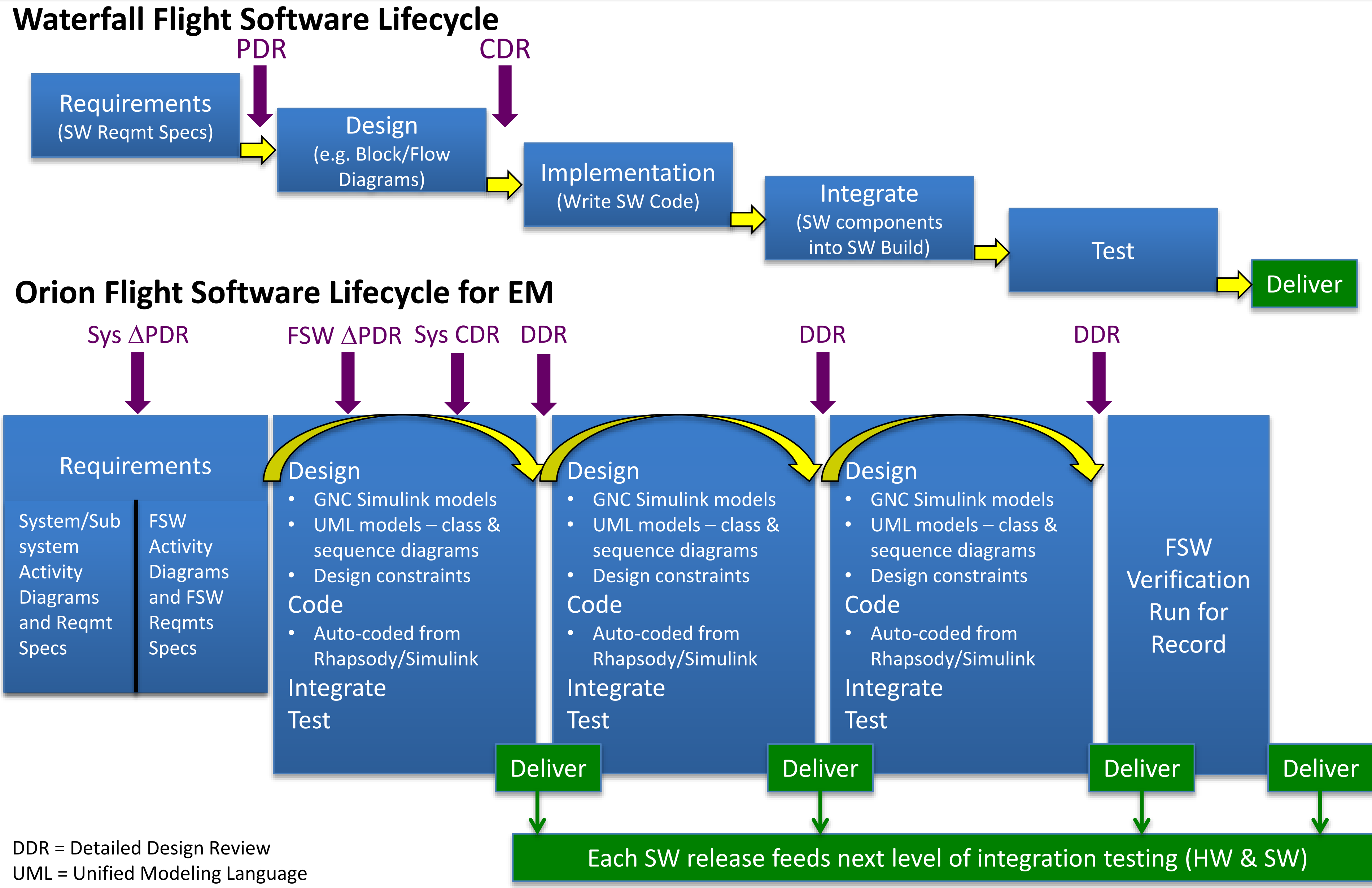
- **Traditionally, both hardware and software present their detailed designs at CDR as well as the required integrating elements**
  - System requirements, system design, performance, and command and data definition were presented at CDR

- **Program adopted both a model-based and an “Agile” (iterative) approach for software development, the detailed software design will not be complete by CDR**
  - Detailed design is developed in an incremental fashion rather than all at once
  - Model-based design is matured for each release and implementation (or code) flows directly from those models
    - Lessens the dependency on a “Software CDR” to ensure we have correct detailed design prior to coding and coding is a much smaller portion of the overall effort

- **Incremental detailed design for FSW is presented through a series of Detailed Design Reviews (DDRs) that occur at the end of each major software release (every 6 months) but after System CDR**
  - Software will review the new features implemented during the previous release (every 6 months)
  - Covers content that was either not presented at CDR or which has matured since then
  - Primary audience is software team, however, System participation is required to review products that have matured and to ensure software implementation meets the needs of the system

- **Tailoring of the standard CDR approach for FSW was reviewed with OCE and S&MA**

FSW Lifecycle Comparison



DDR = Detailed Design Review
UML = Unified Modeling Language

SW Artifacts for CDR/DDRs

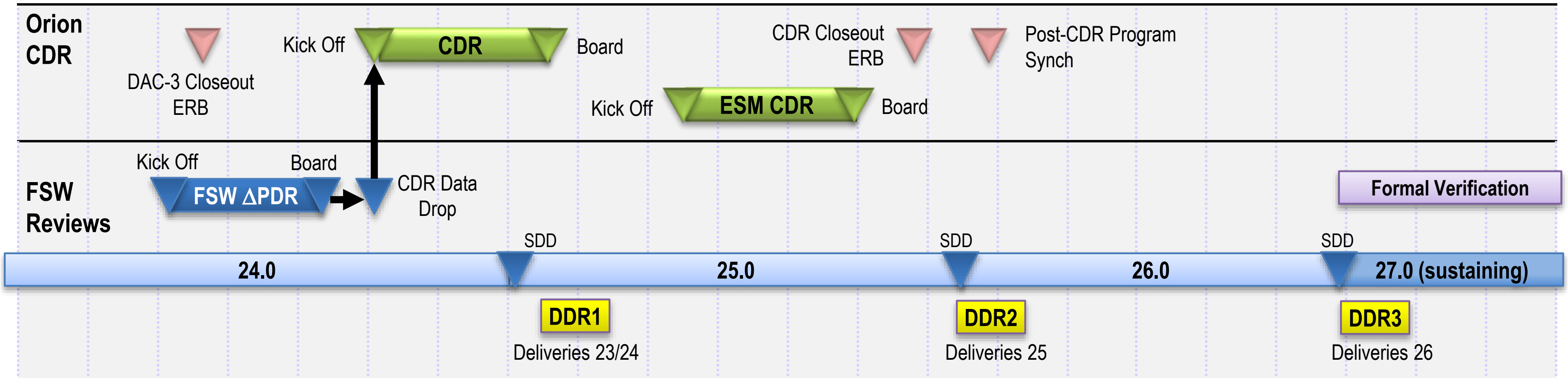
(from MPCV 72579 CDR Process Plan)

Section	Orion CDR	DDRs
General	All the criteria covered	
Plans	All the criteria covered except for execution level details of the test planning	Software test plans at the execution level including SW readiness for testing, detailed test procedures, and test training
Requirements	All the criteria covered	

Design	• Design process (methodology, standards)
	• Design solution (make/buy, reuse/heritage)
	• Final architecture definition
	• Software design
	    • Activity diagrams (enterprise, system, FSW levels) and internal block diagrams
	    • Description of functionality and operational modes
	    • Resource and utilization constraints
	    • Safety considerations addressed in the design
	    • Data storage concepts
	    • IT Security features identified
	• Interface Design – Preliminary
	• Data and Command Dictionary – Preliminary
	• Technical resource utilization estimates and margins updated
	• Detailed timing and storage allocation compiled
	• Failure detection and correction requirements and approach
		• Software Detail Design Products
		    • Class and Sequence Diagrams (UML)
		    • Interrupts and/or exception handling
		    • Detailed description of software operation and flows
		    • Identification of operational limits and constraints
		    • Algorithms sufficient to satisfy their requirements
		    • Data Storage Structure
		• Interface Design
		    • Bit-level definition of the data passed in an interface
		    • Input and output data and formats identified
		• Data and Command Dictionary
		• Failure Detection and Correction (FDC) design
		• Designs comprising the software completed, peer reviewed and placed under change control

Analysis	• Hazard analysis / Software Assurance Classification Report • Subsystem-level and preliminary operations safety analyses exist • Risk assessment and mitigation updated • Reliability analysis and assessments updated • Operational Concepts • Product build-to specs • Status of change requests	• Algorithm accuracy • Critical timing and sequence control • Undesired event handling • Operability • Failure Mode and effects analyses
Other	All the criteria covered	

FSW CDR Integration Schedule



- **System ΔPDR**
  - Functionality was allocated to individual processors using Activity Diagrams
  - Ensured physical processors and interfaces would “work” – properly sized
  - Ensured work scope (SLOC estimate) was validated at processor level
- **FSW ΔPDR**
  - Functionality allocated to CSCIs within processors using Activity Diagrams and SRS requirements
  - Ensured partitions, local memory and I/O buses, memory resources adequate
  - Reviewed the software architecture, requirements, and initial design for EM, including changes to EFT-1 design to support EM objectives
- **System CDR**
  - Leverages FSW CSCI requirements and performance predictions to show software will meet allocated functions given box, card, and bus designs
  - Uses FSW developers at SSDRs/TRTs to monitor for needs not captured in top-down requirements analysis process
- **FSW DDRs**
  - Instead of reviewing detailed design all at once, conduct detailed design reviews (DDRs) every 6 months following each FSW Delivery and ensure FSW implementation meets functional and performance requirements

EM software development underway prior to FSW ΔPDR to enable CPU analysis needed to show software will meet processor allocations for System CDR while software requirements were matured for the later software deliveries

Final Thoughts – Key Principles

- **Stakeholder coordination**
- **Communicate risk and gain Program and Tech Authority acceptance**
- **Fully understand the intent of the systems engineering requirements, but ask what is meaningful to the Program**
  - Tailor as needed but demonstrate how that intent is being met
  - Maintain traceability
- **Strong industry-to-government collaboration**
- **Continuously communicate The Plan**
- **Never become complacent with the current plan – it will change**
- **Principles apply to all phases, not just design**

Backup

Success Criteria (1 of 2)

1. **Requirements and Plans:**
   a) All program specifications are current and consistent with detailed design
   b) Component specifications are complete or sufficiently mature to support program procurement, fabrication, and assembly plans
   c) The program/project has demonstrated compliance with applicable NASA Exploration System, Program and implementing Center requirements, standards, processes, and procedures
   d) Full upward and downward requirement traceability is maintained.
   e) TBD and TBR items are clearly identified with acceptable plans and schedule for their timely disposition and closure.

2. **Verification, Validation, and Test:**
   a) The product verification and product validation requirements and plans are complete.
   b) The testing approach is comprehensive, test requirements defined, and the test plans are complete and sufficient to progress into the next phase.
   c) TLYF exceptions are identified; and risk/mitigation associated with each TLYF exception has been assessed

3. **Design, Analysis, and Manufacturability:**
   a) The detailed design is expected to meet the functional and performance requirements with adequate margins.
   b) Analysis of the system and subsystems has been completed, summarized, and demonstrates that system meets the functional, performance, and mission requirements with acceptable margins.
   c) Appropriate modeling and analytical results are available and have been considered in the design
   d) The product technical baseline is complete and adequate to proceed with fabrication, assembly, integration, and test.
   e) Engineering test units, life test units, and/or modeling and simulations have been developed and tested per plan.
   f) Material properties tests are completed along with analyses of loads, stress, fracture control, contamination generation, etc.
   g) EEE parts have been selected, and planned testing and delivery will support build schedules.
   h) Manufacturability has been adequately included in design.
   i) Any required new technology has been developed or the viable alternative has been selected to proceed with fabrication, assembly, integration, and test.

4. **Technical Interfaces:**
   a) External and internal interface control documents are sufficiently mature to proceed with fabrication, assembly, integration, and test, and plans are in place to manage any open items.

Success Criteria (2 of 2)

5. **Software:**
   a) Software components meet the exit criteria defined in NASA-HDBK-2203, NASA Software Engineering Handbook as modified by Appendix G.

6. **Technical Margins:**
   a) Adequate spacecraft technical margins (e.g. mass, power, memory) exist with respect to TPMs.

7. **Safety and Mission Assurance (S&MA):**
   a) Safety and mission assurance (e.g., safety, reliability, maintainability, and quality) have been adequately addressed in system and operational designs, and any applicable S&MA products (e.g., PRA, system safety analysis, and failure modes and effects analysis) meet requirements, are at the appropriate maturity level for this phase of the program's life cycle, and indicate that the program safety/reliability residual risks will be at an acceptable level.

8. **Assembly and Integration:**
   a) The planning for system assembly, integration, and launch site operations is sufficient to progress into the next phase.

9. **Operations:**
   a) The operational concept has matured, is supported by the vehicle design, is at a CDR level of detail, and has been considered in test planning.
   b) The planning for mission operations (launch through recovery operations) is sufficient to progress into the next phase.

10. **Cost and Schedule:**
    a) The program cost and schedule estimates are credible and within program constraints.
    b) Adequate programmatic margins resources and control processes exist to complete the development within budget, schedule, and known risks.

11. **Risk:**
    a) Risks to mission success are understood and credibly assessed, and plans and resources exist to effectively manage them.