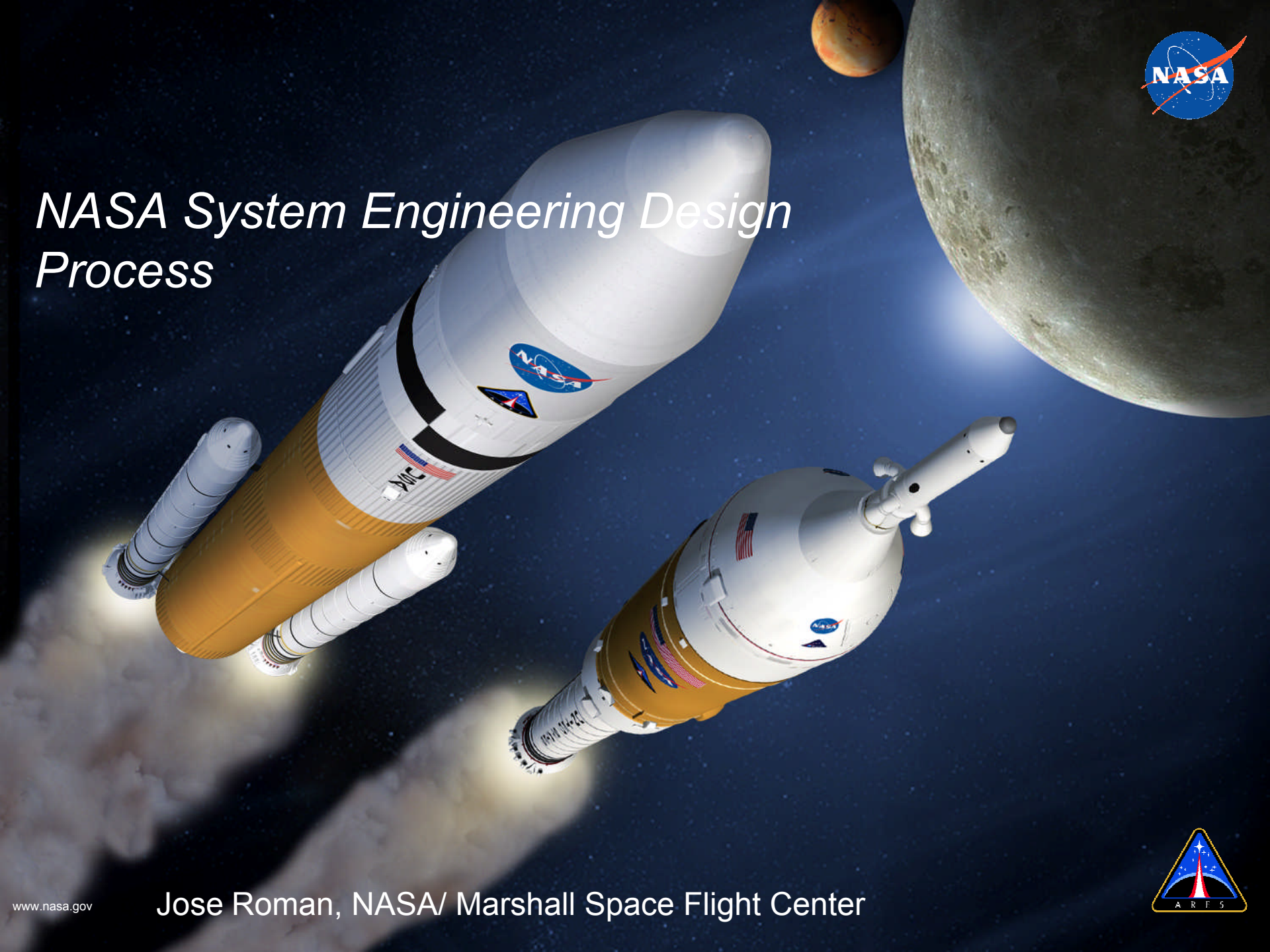


NASA System Engineering Design Process

Jose Roman, NASA/ Marshall Space Flight Center

What is System Engineering

- **Systems engineering is a methodical, disciplined approach for the design, realization, technical management, operations, and retirement of a system.**
- **A "system" is a construct or collection of different elements that together produce results not obtainable by the elements alone.**
- **The elements, or parts, can include people, hard- ware, software, facilities, policies, and documents; that is, all things required to produce system-level results.**
- **The results include system-level qualities, properties, characteristics, functions, behavior, and performance. The value added by the system as a whole, beyond that contributed independently by the parts, is primarily created by the relationship among the parts; that is,**
  - how they are interconnected.1 It is a way of looking at the "big picture" when making technical decisions.
  - It is a way of achieving stakeholder functional, physical, and operational performance requirements in the intended use environment over the planned life of the systems.
- **In other words, systems engineering is a logical way of thinking**

Life Cycle

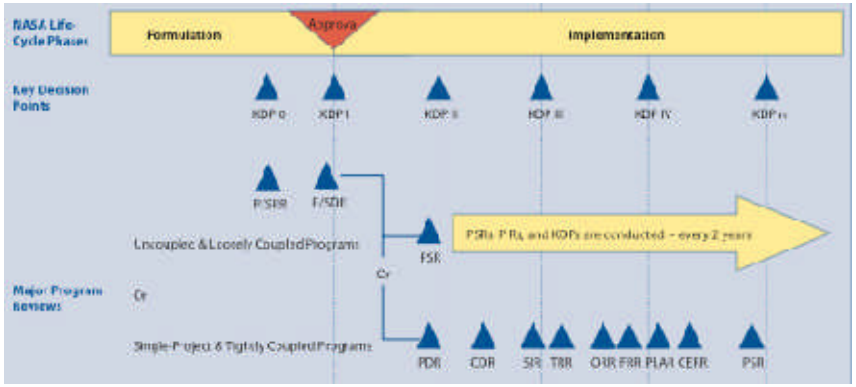


Figure 3.0-1 NASA program life cycle

CDR Critical Design Review
CERR Critical Event Readiness Review
DR Decommissioning Review
FRR Flight Readiness Review
KDP Key Decision Point
MCR Mission Concept Review
MDR Mission Definition Review
ORR Operational Readiness Review
PDR Preliminary Design Review
PFAR Post-Flight Assessment Review
PIR Program Implementation Review
PLAR Post-Launch Assessment Review
TRR Production Readiness Review
P/SDR Program/System Definition Review
P/SRR Program/System Requirements Review
PSR Program Status Review
SAT System Acceptance Review
SDR System Definition Review
SIR System Integration Review
SRR System Requirements Review
TRR Test Readiness Review

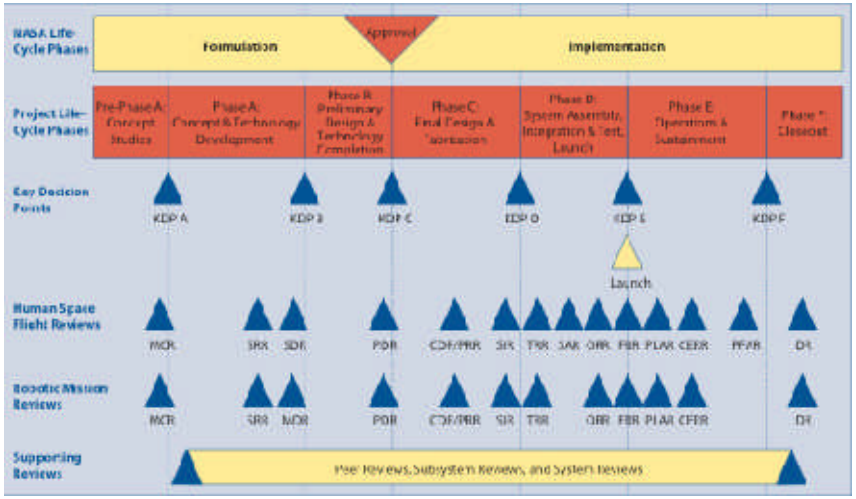


Figure 3.0-2 NASA project life cycle

One of the fundamental concepts used within NASA for the management of major systems is the program/project life cycle

- Decomposing the project life cycle into phases organizes the entire process into more manageable pieces.
- Each phase terminate with a Key decision point (KDP).
- KDP are supported by major reviews, (SDR, PDR, etc)

Project Phases

In the effort to seek out more cost-effective designs, trade studies should precede—rather than follow—system design decisions. Major products to this point include an accepted functional baseline for the system and its major end items. The effort also produces various engineering and management plans to prepare for managing the project's downstream processes, such as verification and operations, and for implementing engineering specialty programs.

3.5 Project Phase B: Preliminary Design and Technology Completion

During Phase B, activities are performed to establish an initial project baseline, which (according to NPR 7120.5 and NPR 7123.1) includes "a formal flow down of the project-level performance requirements to a complete set of system and subsystem design specifications for both flight and ground elements" and "corresponding preliminary designs." The technical requirements should be sufficiently detailed to establish firm schedule and cost estimates for the project. It also should be noted, especially for AO-driven projects, that Phase B is where the top-level requirements and the requirements flowed down to the next level are finalized and placed under configuration control. While the requirements should be baselined in Phase A, there are just enough changes resulting from the trade studies and analyses in late Phase A and early Phase B that changes are inevitable. However, by mid-Phase B, the top-level requirements should be finalized.

Actually, the Phase B baseline consists of a collection of evolving baselines covering technical and business aspects of the project: system (and subsystem) requirements and specifications, designs, verification and operations plans, and so on in the technical portion of the baseline, and schedules, cost projections, and management plans in the business portion. Establishment of baselines implies the implementation of configuration management procedures. (See Section 6.5.)

In Phase B, the effort shifts to establishing a functionally complete preliminary design solution (i.e., a functional baseline) that meets mission goals and objectives. Trade studies continue. Interfaces among the

Phase B: Preliminary Design and Technology Completion

Purpose

To define the project in enough detail to establish an initial baseline capable of meeting mission needs

Typical Activities and Their Products

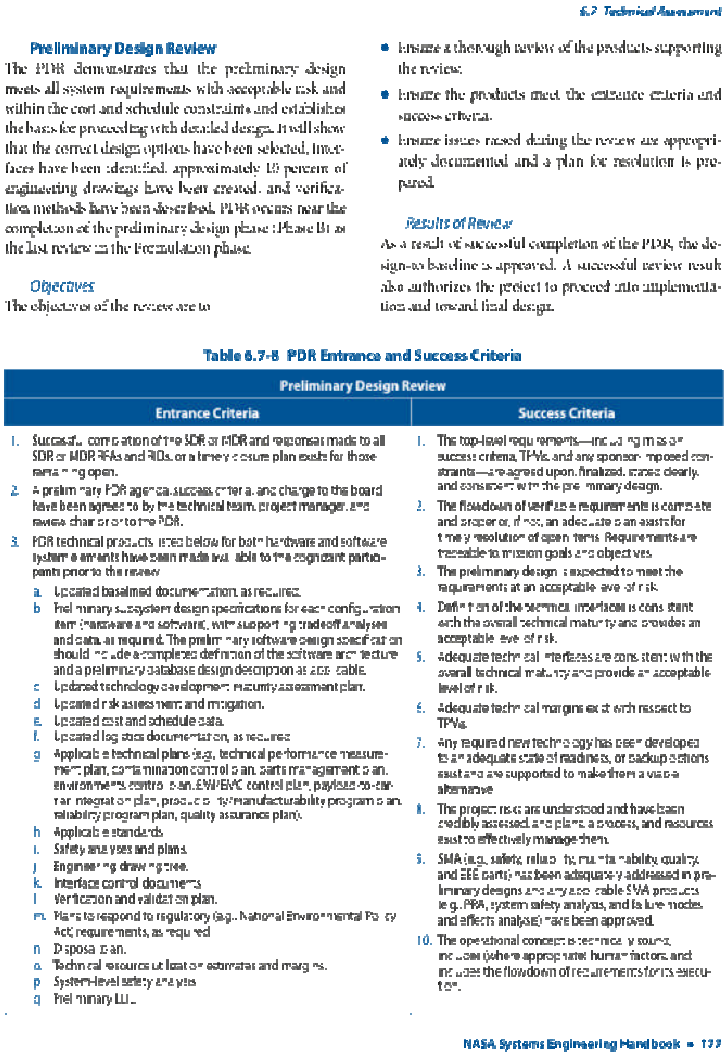
- Baseline the project plan
- Review and update documents developed and baselined in Phase A
- Develop science/exploration operations plan based on matured ConOps
- Update engineering specialty plans (e.g., contamination control plan, electromagnetic interference/electromagnetic compatibility control plan, reliability plan, quality control plan, parts management plan)
- Update technology maturation planning
- Report technology development results
- Update risk management plan
- Update cost and schedule data
- Finalize and approve top-level requirements and flowdown to the next level of requirements
- Establish and baseline design-to specifications (hardware and software) and drawings, verification and validation plans, and interface documents at lower levels
- Perform and archive trade studies' results
- Perform design analyses and report results
- Conduct engineering development tests and report results
- Select a baseline design solution
- Baseline a preliminary design report
- Define internal and external interface design solutions (e.g., interface control documents)
- Define system operations as well as PI/contract proposal management, review, and access and contingency planning
- Develop appropriate level safety data package
- Develop preliminary orbital debris assessment
- Perform required Phase B technical activities from NPR 7120.5
- Satisfy Phase B reviews' entrance/success criteria from NPR 7123.1

Reviews

- PDR
- Safety review

- Project is divided into two major life cycle phases
  - Formulation
  - Implementation
- Each major phases are divided into project life cycle phases
  - Pre-Phase A
  - Phase A-E
  - Each phase has a purpose and a goal to achieve at the end of cycle
  - At the end of each phase a major review is performed to determined the completion of the phase

Major reviews



6.7 Technical Assessment

Preliminary Design Review

The PDR demonstrates that the preliminary design meets all system requirements with acceptable risk and within the cost and schedule constraints and establishes the basis for proceeding with detailed design. It will show that the correct design options have been selected, interfaces have been identified, approximately 10 percent of engineering drawings have been created, and verification methods have been described. PDR occurs near the completion of the preliminary design phase. Phase B is the last review in the Formulation phase.

Objectives

The objectives of the review are to

- Ensure a thorough review of the products supporting the review.
- Ensure the products meet the entrance criteria and success criteria.
- Ensure issues raised during the review are appropriately documented and a plan for resolution is prepared.

Results of Review

As a result of successful completion of the PDR, the design-to baseline is approved. A successful review result also authorizes the project to proceed into implementation and toward final design.

Table 6.7-8 PDR Entrance and Success Criteria

Preliminary Design Review	
Entrance Criteria	**Success Criteria**
1. Successful completion of the SDR or MDR and responses made to all SDR or MDR RFAs and RIDs, or a timely closure plan exists for those remaining open. 2. A preliminary PDR agenda, success criteria, and charge to the board have been agreed to by the technical team, project manager, and review chair prior to the PDR. 3. PDR technical products listed below for both hardware and software system elements have been made available to the cognizant participants prior to the review: a. Updated baselined documentation, as required. b. Preliminary subsystem design specifications for each configuration item (hardware and software), with supporting trade-off analyses and data, as required. The preliminary software design specification should include a complete definition of the software architecture and a preliminary database design description as applicable. c. Updated technology development maturity assessment plan. d. Updated risk assessments and mitigations. e. Updated cost and schedule data. f. Updated logistics documentation, as required. g. Applicable technical plans (e.g., technical performance measurement plan, contamination control plan, parts management plan, environmental control plan, EMI/EMC control plan, payload-to-carrier integration plan, producibility/manufacturability program plan, reliability program plan, quality assurance plan). h. Applicable standards. i. Safety analyses and plans. j. Engineering drawing tree. k. Interface control documents. l. Verification and validation plan. m. Plans to respond to regulatory (e.g., National Environmental Policy Act) requirements, as required. n. Disposal plan. o. Technical resource utilization estimates and margins. p. System-level safety analysis. q. Preliminary LLIs.	1. The top-level requirements—including mission success criteria, TPMs, and any sponsor-imposed constraints—are agreed upon, finalized, stated clearly, and consistent with the preliminary design. 2. The flowdown of verification requirements is complete and proper or, if not, an adequate plan exists for timely resolution of open items. Requirements are traceable to mission goals and objectives. 3. The preliminary design is expected to meet the requirements at an acceptable level of risk. 4. Definition of the technical interfaces is consistent with the overall technical maturity and provides an acceptable level of risk. 5. Adequate technical interfaces are consistent with the overall technical maturity and provide an acceptable level of risk. 6. Adequate technical margins exist with respect to TPMs. 7. Any required new technology has been developed to an adequate state of readiness, or backup options exist and are supported to make them available when needed. 8. The project risks are understood and have been credibly assessed, and plans, a process, and resources exist to effectively manage them. 9. SMA (e.g., safety, reliability, maintainability, quality, and EEE parts) has been adequately addressed in preliminary designs and any applicable SMA products (e.g., PRA, system safety analysis, and failure modes and effects analysis) have been approved. 10. The operational concept is technically sound, including (where appropriate) human factors, and includes the flowdown of requirements for its execution.

- Each major review has a purpose and a goal
- An entry and exit criteria are defined before the review is performed to assess the acceptance of the review
- Typically this reviews are performed by the team/project presenting to a board
- The Board is the entity that determine the success of the review and approving the completion of the current life cycle phase and approving to move into the next phase
- The board is composed of experts, managers, etc.

Documents

- **NASA Space Flight Program and Project Management Requirements, NPR 7120.5D**
  - http://nodis.hq.nasa.gov/npg_img/N_PR_7120_005D_/N_PR_7120_005D_.pdf
- **NASA System Engineering Process and Requirements, NPR 7123.1A**
  - http://nodis3.gsfc.nasa.gov/npg_img/N_PR_7123_001A_/N_PR_7123_001A_.pdf
- **NASA System Engineering Handbook, SP-2007-6105,**
  - http://education.ksc.nasa.gov/esmdspacegrant/Documents/NASA%20SP-2007-6105%20Rev%201%20Final%2031Dec2007.pdf