ESMD Risk Management Workshop
Systems Engineering & Integration Risks

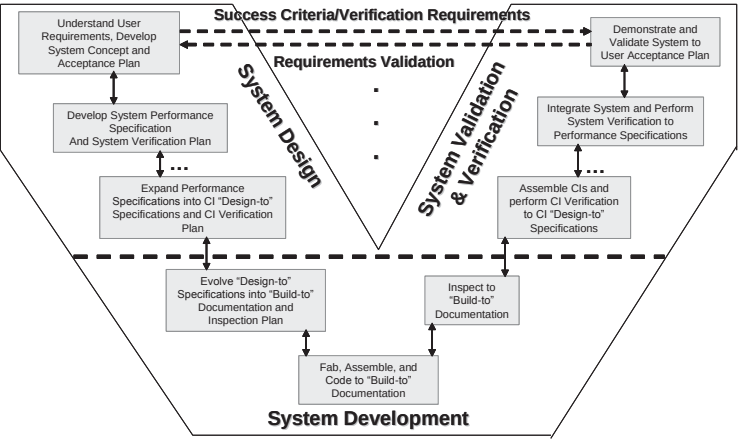
L. Dale Thomas, Ph.D., P.E.

October 12, 2005

Overview

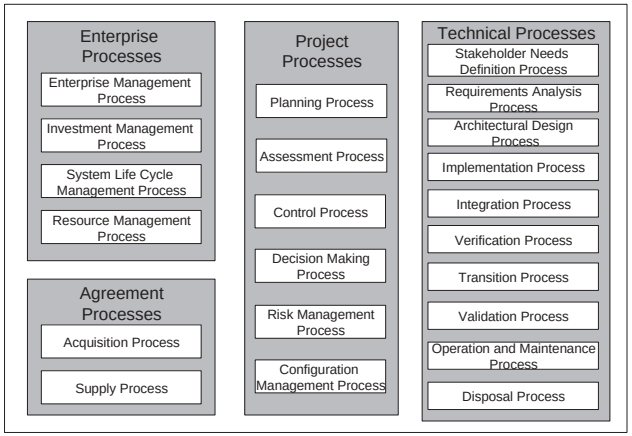
- The Systems Engineering Process
- Risks Identified During SE&I RFP Development
  - A Couple of Relevant Historical Anecdotes
- Selected SE&I Process Deficiencies & Their Consequences
- Remarks

Systems Engineering Process Models



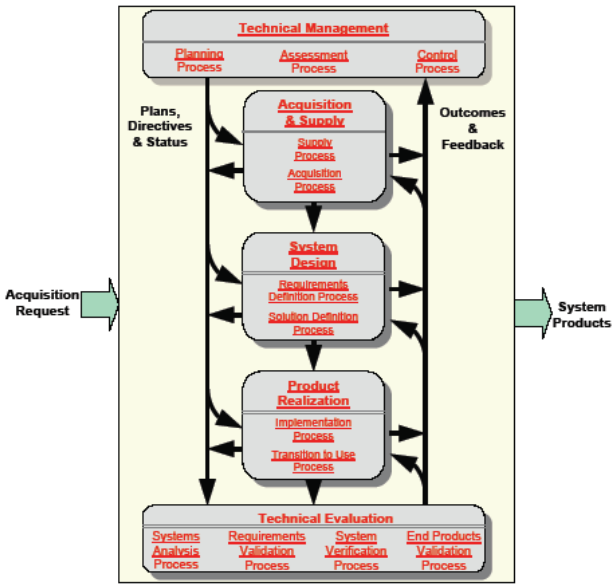
NASA SP-6105

Many models of the Systems Engineering process, and many definitions of systems engineering.

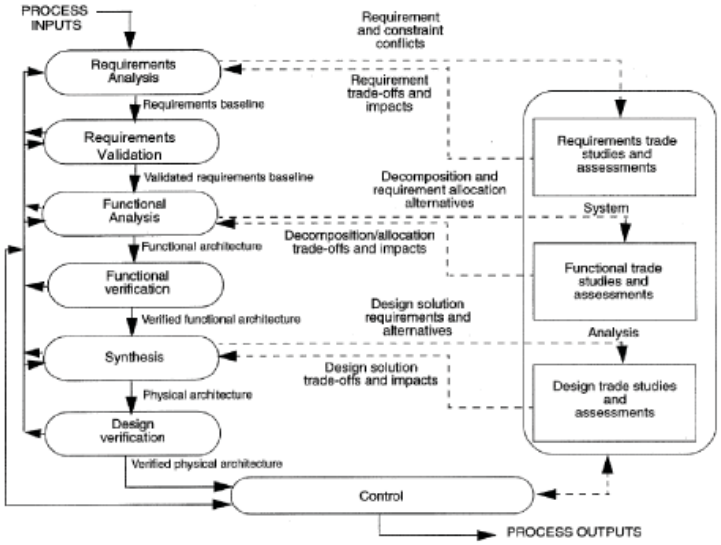


ISO/IEC 15288

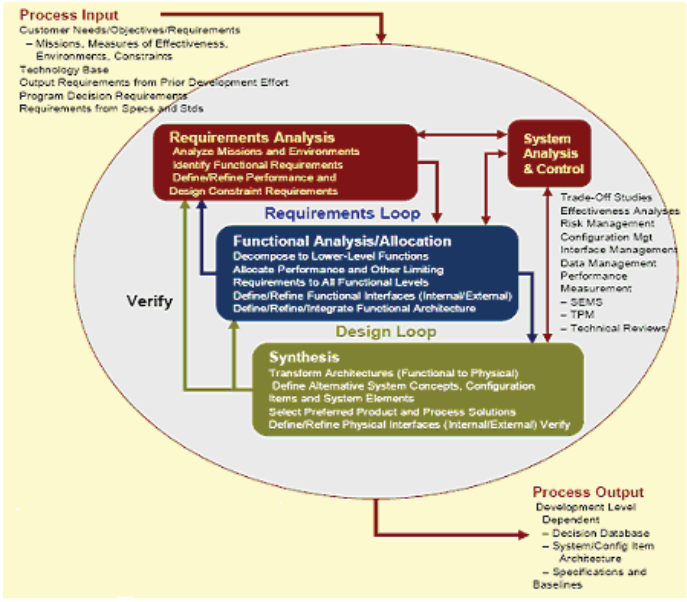
EIA-632



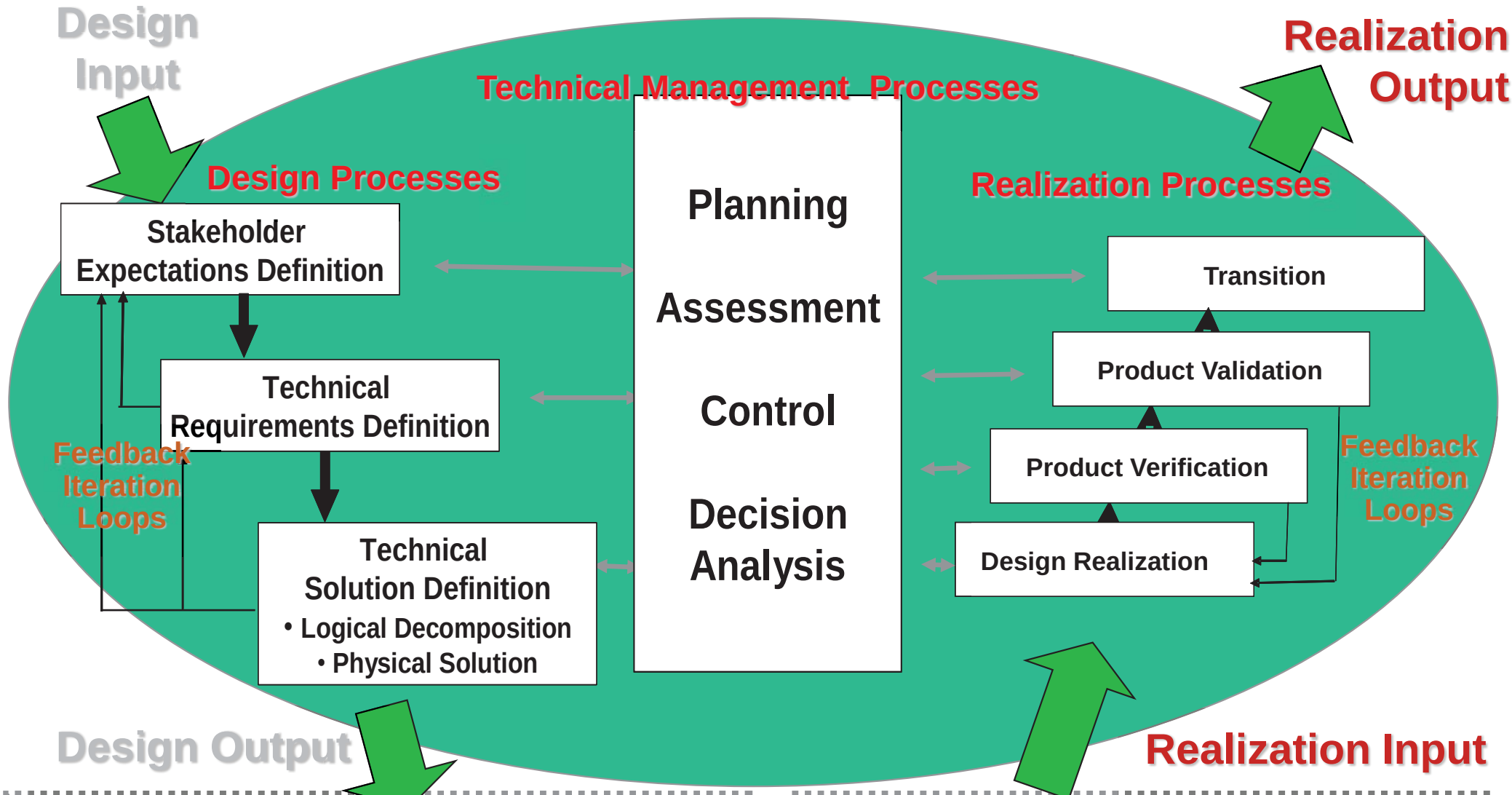
IEEE-1220



MIL STD 499C (draft)



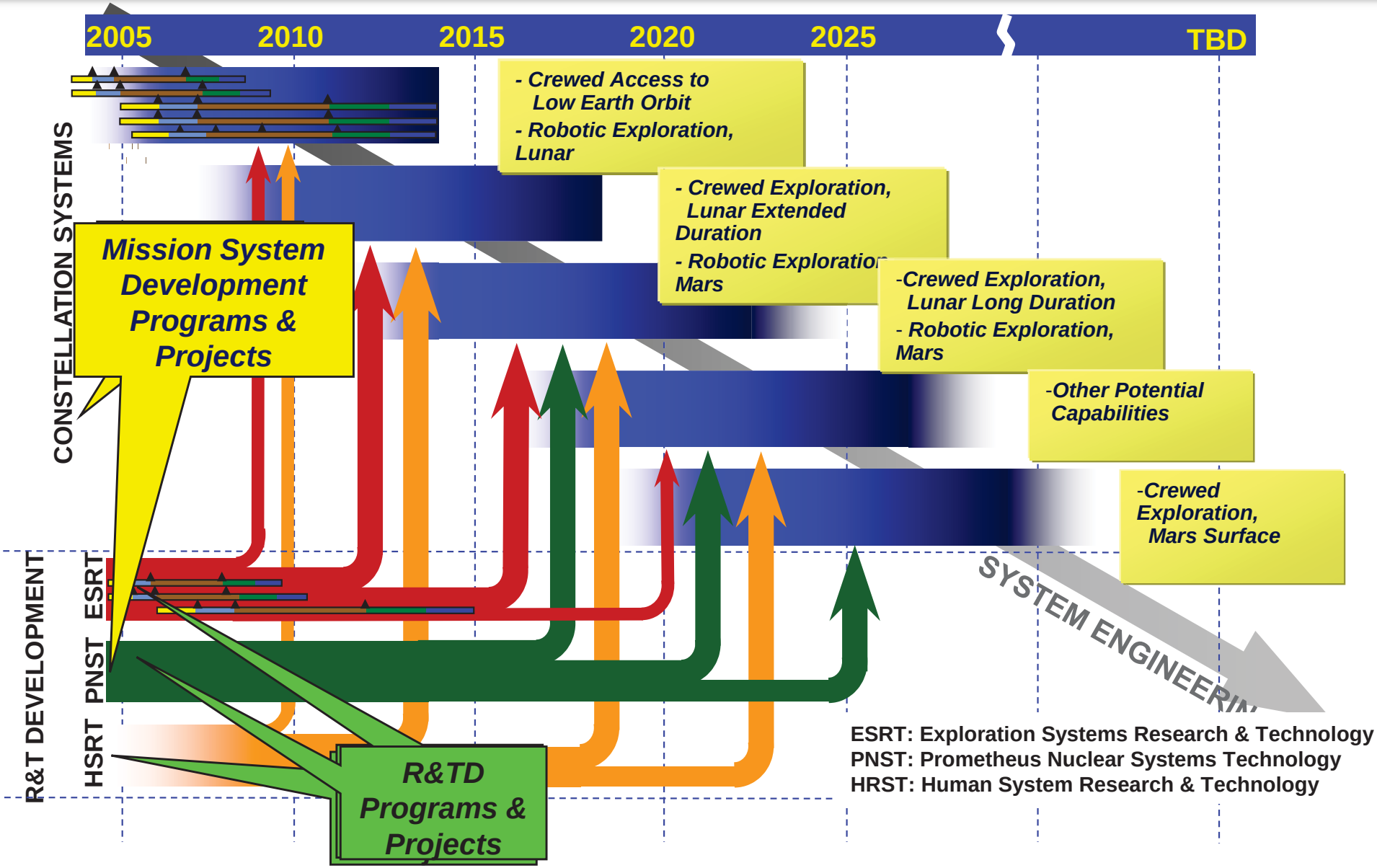
The NASA Systems Engineering Process



Design Processes applied to each product down and across product structure

Realization Processes applied to each product up and across product structure

The Pre-ESAS Exploration Architecture

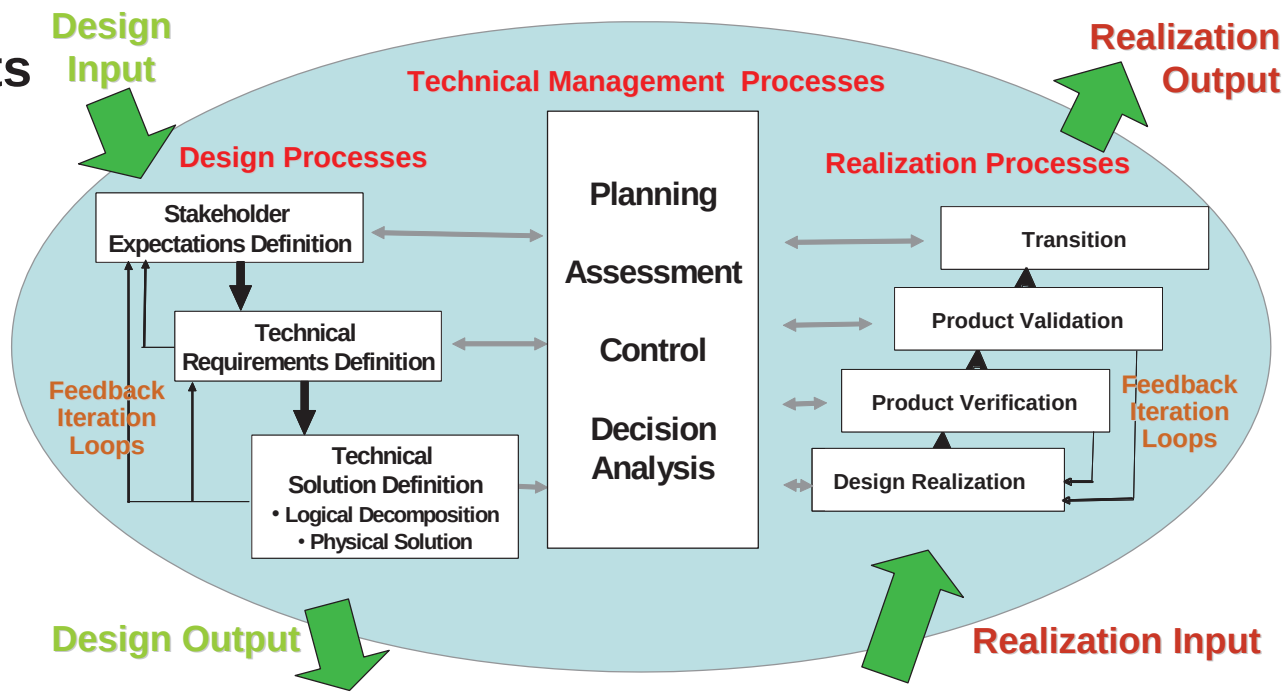


Architecture driven by evolution of enabling technologies.

Scope of SE&I RFP

Under previous ESMD AA, it had been planned to contract the Constellation Systems Engineering & Integration. This strategy has since been abandoned.

ESMD Requirements



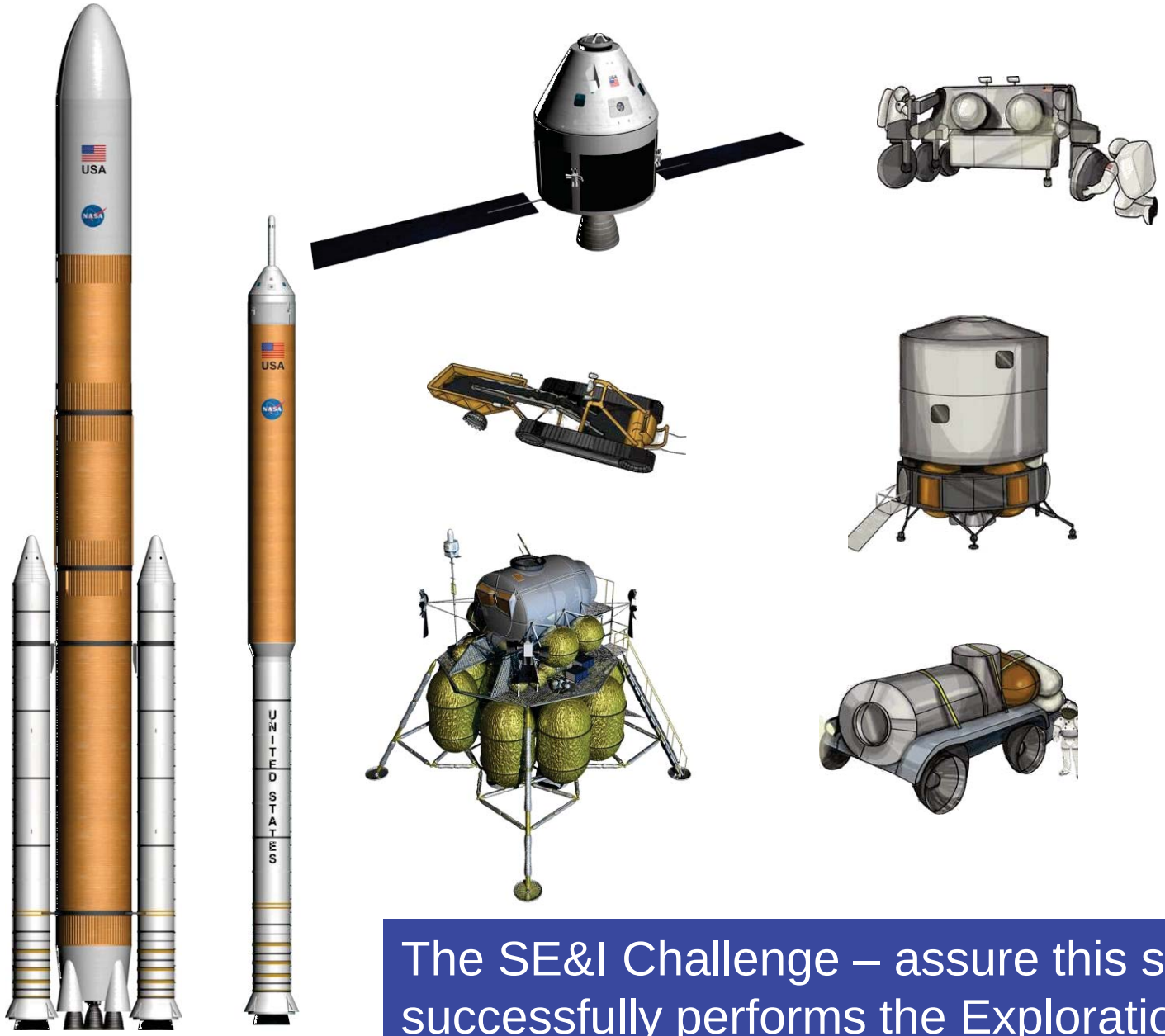
Mission Configurations

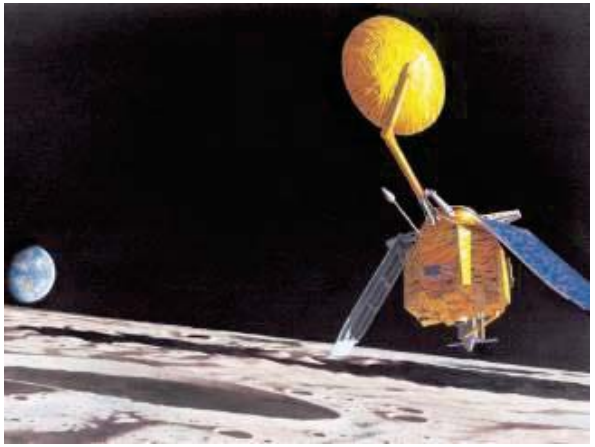
Constellation Element Requirements

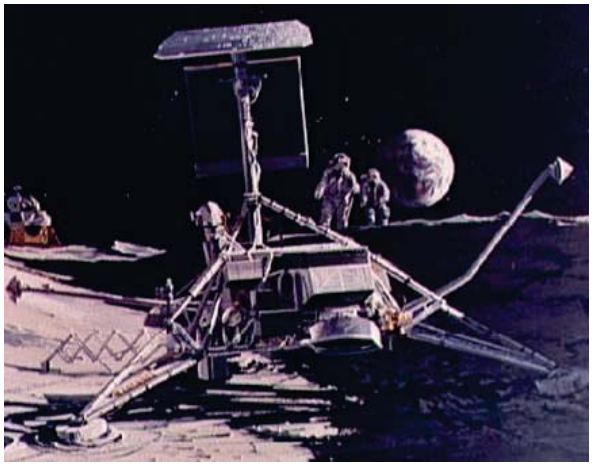
Constellation Elements

The SE&I Task was (1) definition of the overall architecture & definition of the elements in concert with technology development & maturity, and (2) integration of the elements to form mission systems.

Elements of the Exploration Architecture
(as defined by the ESAS)







The SE&I Challenge – assure this set of elements successfully performs the Exploration Missions.

SE&I RFP Risks

- Reviewed risks identified during SE&I RFP development
- Of 14 major risks, 7 largely mitigated; the following, in my view, remain:
  - Human Rating Requirements
  - Technical Standards
  - Long Term Interoperability
  - Modeling & Simulation Standards
  - Integration Complexity
  - Requirements Changes beyond Phase A
  - Technology Maturity
- All these risks will manifest themselves as changes to the technical baseline & associated contracts with associated cost & schedule impacts.

SE&I RFP Risks (con't)

- Human Rating Requirements
  - Was a source of considerable requirements uncertainty for the Space Launch Initiative and Orbital Space Plane Program, simply because NASA has never developed a Human-Rated space flight system under it's guidance.

- Technical Standards
  - Different Centers within NASA will levy different technical standards on different contracts for elements of the Exploration Architecture that must be integrated.

SE&I RFP Risks (con't)

- Long Term Interoperability
  - Selected inter-generational elements of the architecture must be interoperable. For example, the Lunar Lander must be interoperable with the CEV, which will drive requirements in the block upgrade of the CEV, which will still be required to be interoperable with the Crew Launch Vehicle.

- Modeling & Simulation Standards
  - Need Exploration-wide model verification, validation, & accreditation guidance such that models & simulations developed by different organizations can be integrated. Need this soon so that it can be levied on contracts at their inception.

SE&I RFP Risks (con't)

- Integration Complexity
  - "Another important design rule, which we have not discussed as often as we should, reads: Minimize functional interfaces between complex pieces of hardware. In this way, two organizations can work on their own hardware relatively independently. Examples in Apollo include the interfaces between the spacecraft and launch vehicle and between the command module and the lunar module. **Only some 100 wires link the Saturn launch vehicle and the Apollo spacecraft, and most of these have to do with the emergency detection system.** The reason that this number could not be even smaller is twofold: Redundant circuits are employed, and the electrical power always comes from the module or stage where a function is to be performed. For example, the closing of relays in the launch vehicle could, in an automatic abort mode, fire the spacecraft escape motor. But the electrical power to do this, by design, originates in the spacecraft batteries. The main point is that a single man can fully understand this interface and can cope with all the effects of a change on either side of the interface. If there had been 10 times as many wires, it probably would have taken a hundred (or a thousand?) times as many people to handle the interface."

    - Low, George M., "What Made Apollo a Success?" *Astronautics and Aeronautics* 8 (3), March 1970, pp. 36-45.

SE&I RFP Risks (con't)

- Requirements Changes beyond Phase A
  - During the NASA Jet Propulsion Laboratory's development of the Mariner 3 and 4 interplanetary spacecraft in the mid 1960's, project managers kept statistics on design changes and observed "that the majority of the projects' 1,174 design changes occurred at subsystem interfaces and in subsystems that contained state-of-the-art equipment."
    - Ref: Johnson, Stephen B. *The Secret of Apollo: Systems Management in American and European Space Programs*, The Johns Hopkins University Press, Baltimore, 2002, p. 107-108.

SE&I RFP Risks (con't)

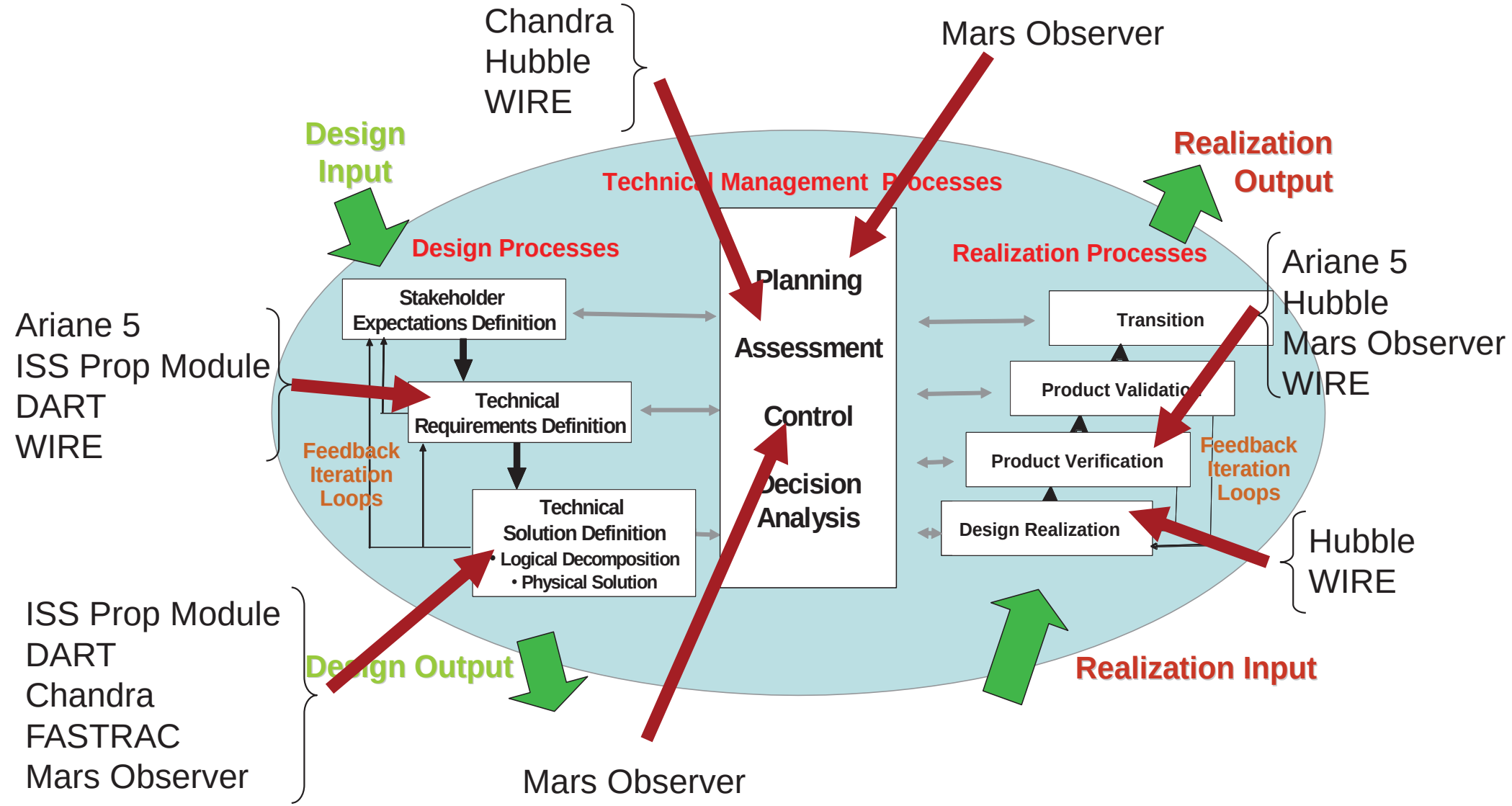
- Technology Maturity
  - Technology maturity morphs to "use of heritage hardware", which introduces it's own risks (*more to come on this one later*).

- Note: New developments are risky, but so is the use of heritage systems. In our business, there are no free lunches!

SE&I Risk Mitigation

- Plan the ***Exploration*** SE&I task
  - Develop a comprehensive & coherent Systems Engineering Management Plan (SEMP)
  - Include sub-tier activities such as CEV and CLV, including Contractor efforts, within scope
    - Ensure adequate resources to perform SE&I
- Execute the full systems engineering process
  - Ensure SE&I process during early program phases/prior to development contract award
  - Periodically monitor compliance to SEMP
    - Best practice from USN Fleet Ballistic Missile Program (ref. John Schafer, Chief Engineer)
- But it's not as easy as it looks.
  - Pressure to short-cut or even omit steps.
  - Especially when a Contractor proposes good rationale & expected efficiencies.
  - Especially when you're using heritage hardware or software!
- ***So what are the consequences of SE process shortcuts?***

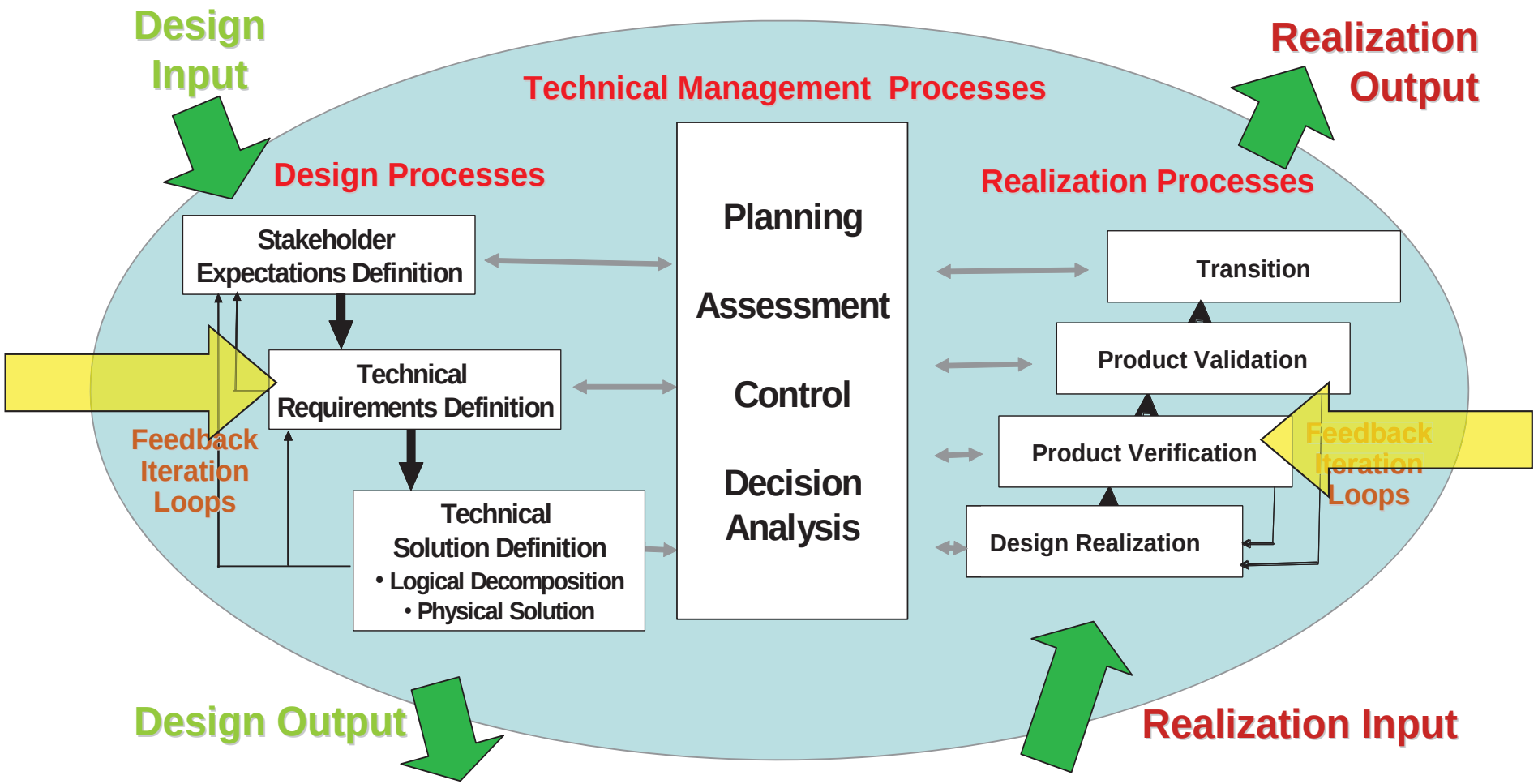
Selected Systems Engineering Process Deficiencies



Ariane 5 Flight 501 Failure

MSFC/Dale Thomas

Incomplete Technical Requirements Definition and Product Verification

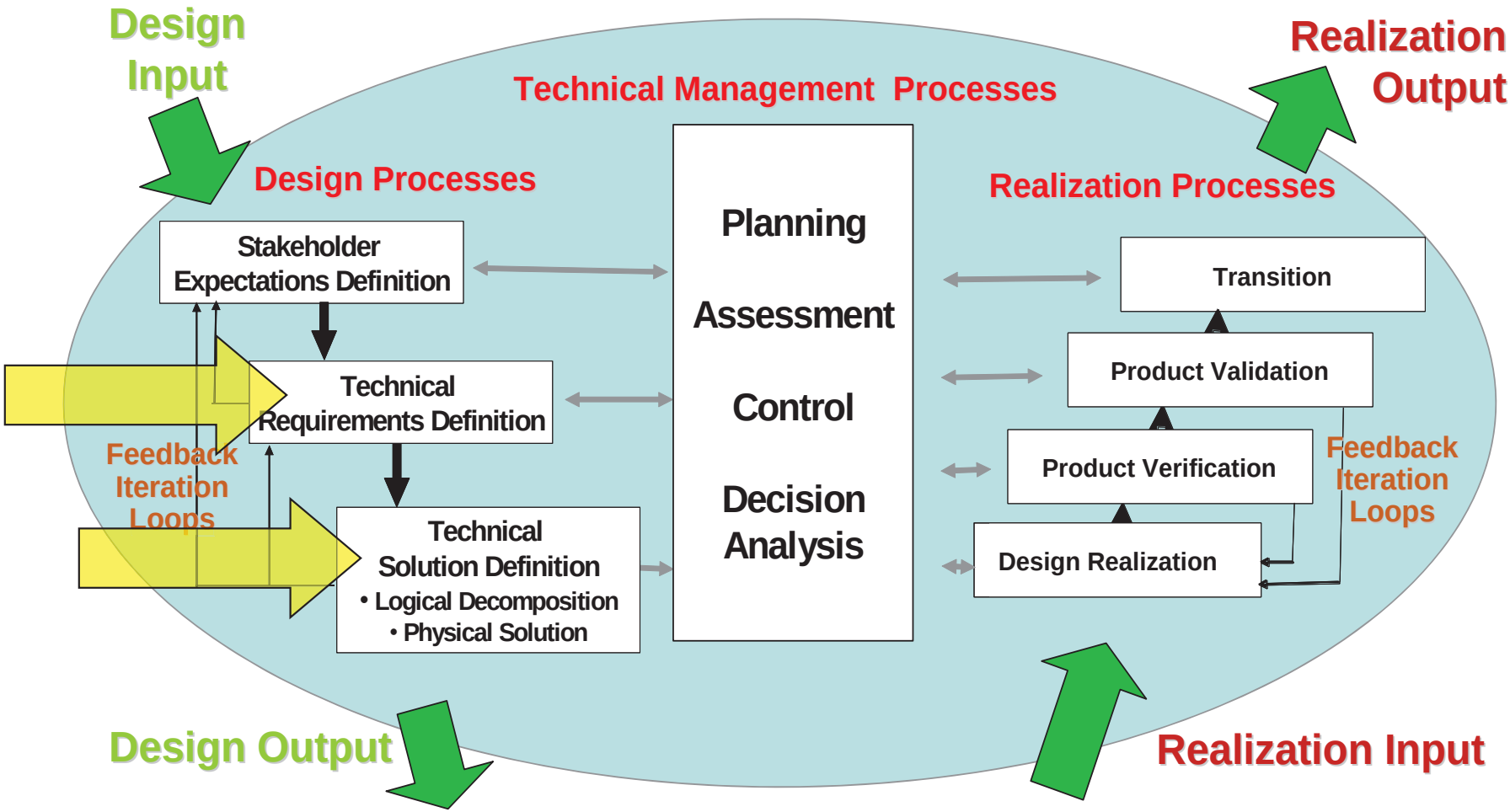


Ariane 5 Flight 501 Failure

- Issue: Reuse of the Inertial Reference System (SRI) from the Ariane 4.
  - Software functionality in general was maintained for commonality reasons, based on the view that it was not wise to make changes in software which worked well on Ariane 4.
  - A special feature of the SRI on previous versions of Ariane, but not needed on Ariane 5, was the primary cause of the error.
- Impact: Erroneous operation of the SRI and On-Board Computer led to flight failure at 40 seconds into the flight.
- SE&I Deficiencies:
  - The SRI Systems Specification did not include operational restrictions for the chosen implementation. Such a declaration, which should be mandatory for every mission-critical device, would have served to identify any non-compliance with the trajectory of Ariane 5.
  - Closed-loop simulations conducted as a part of system functional testing did not include the SRIs.
- Reference: Flight 501 Failure Report by the Inquiry Board, Prof. J.L. Lions (chair).

ISS Propulsion Module

Incomplete Technical Requirements Definition and Technical Solution Definition



ISS Propulsion Module

- Issue: Reliance on heritage Space Shuttle propulsion system components with little/no initial oversight.
  - Since ISS Propulsion Module was to be an ISS element, ISS on-orbit hardware life requirements levied on the Propulsion Module systems.
  - Shuttle hardware did not meet ISS requirements (Certified for 30 days on orbit; requirement 12 years).
- Impact: Contributed to significant technical and programmatic baseline impacts, leading to cancellation of the Project.
- SE&I Deficiency:
  - Contractor design team assumed that heritage Shuttle flight hardware met NASA requirements for ISS.
  - Government oversight identified the issue in the Systems Requirements Review.
- Reference: Steve Richards, Project Manager & Dr. Fred Bickley, ISS PM Chief Engineer

DART Spacecraft Major Components

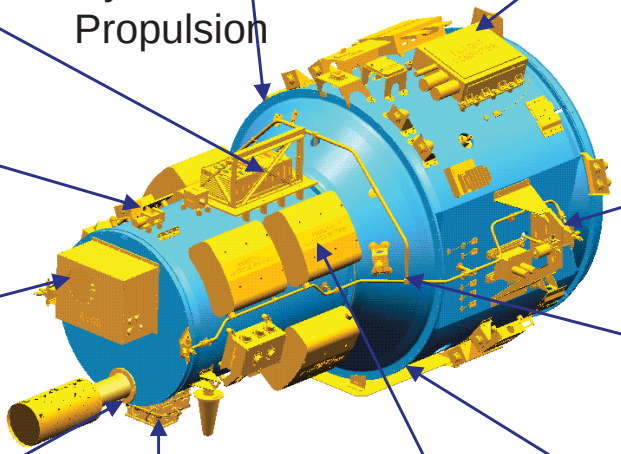
Hydrazine Propulsion

Flight Computer

Modular Avionics

Video Imager

RCS Thrusters



AVGS

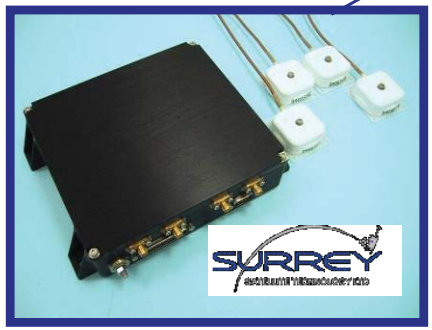
Structure

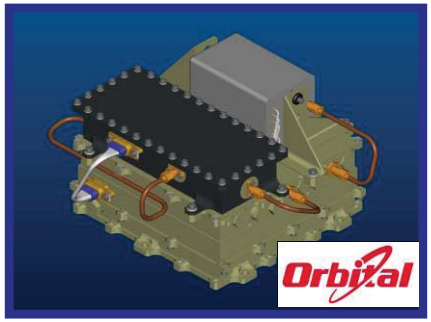
GPS Rx

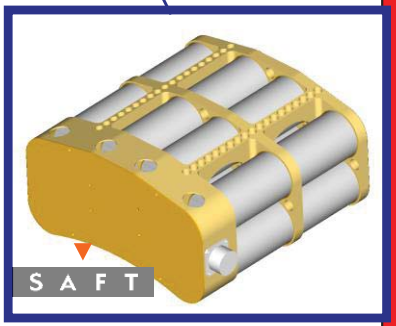
UHF Rx

Li Ion Batteries

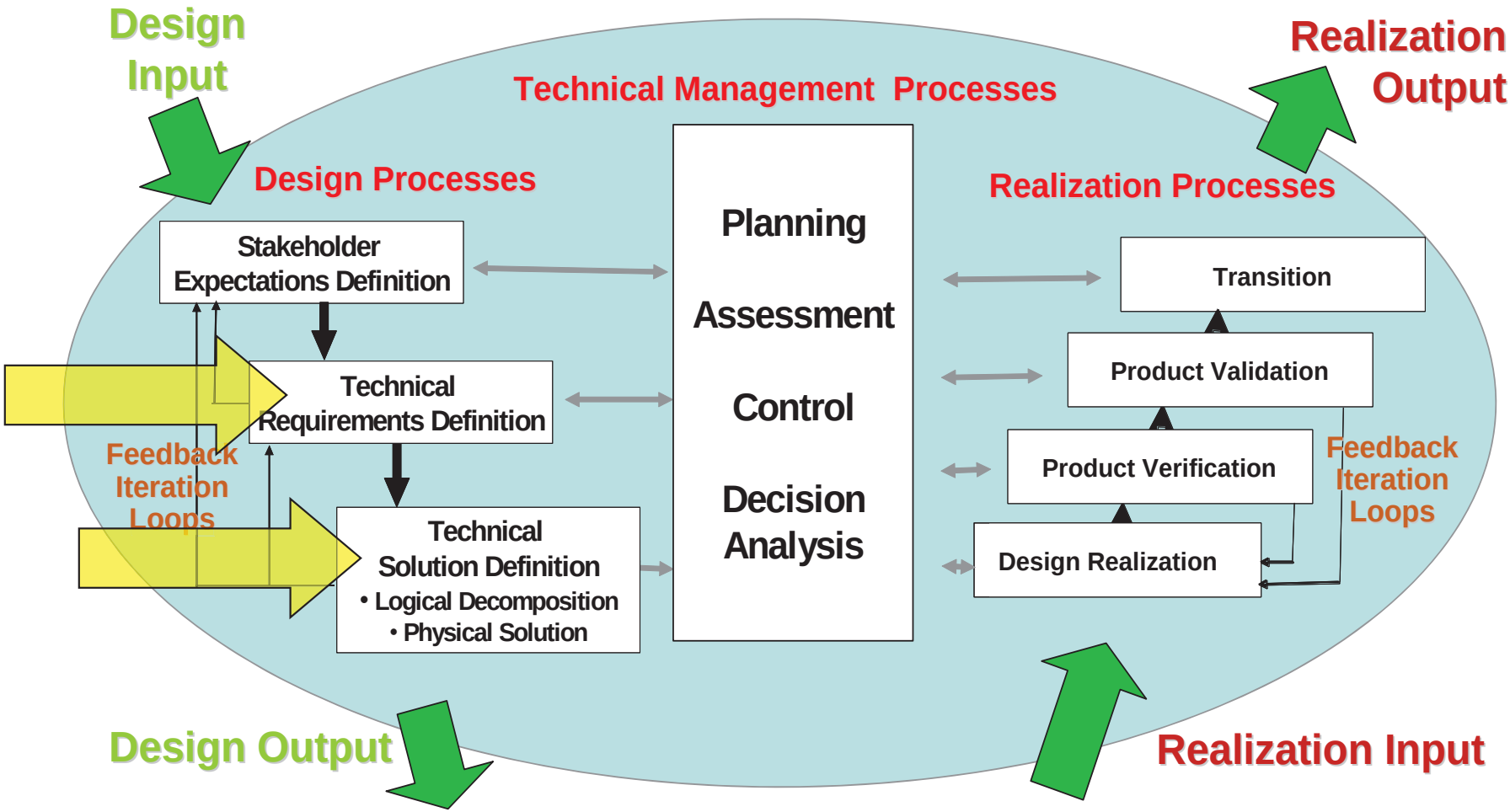
IMU







Incomplete Technical Requirements Definition and Technical Solution Definition



DART (Demonstration of Autonomous Rendezvous Technology) - launched 2005

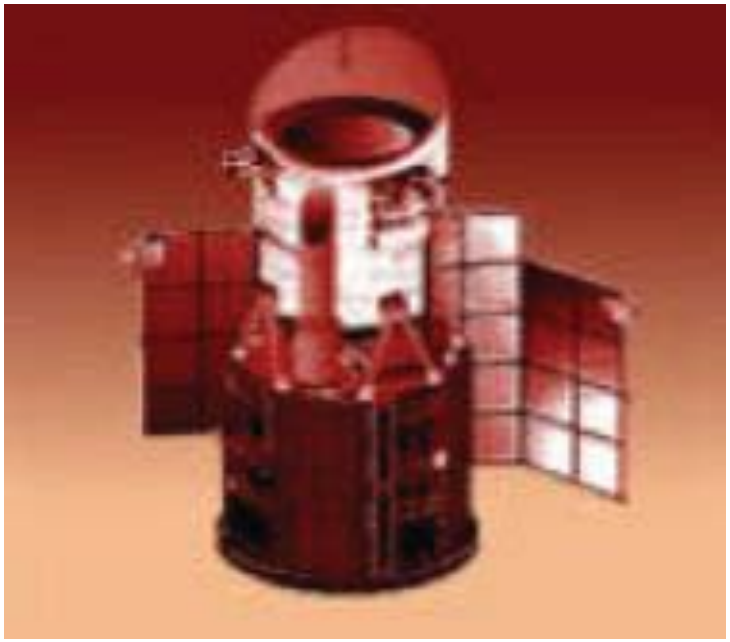
- Issue: The DART program made extensive use of heritage and off-the-shelf components. Some avionics components had not been qualified for DART's operating environment or were not space rated.

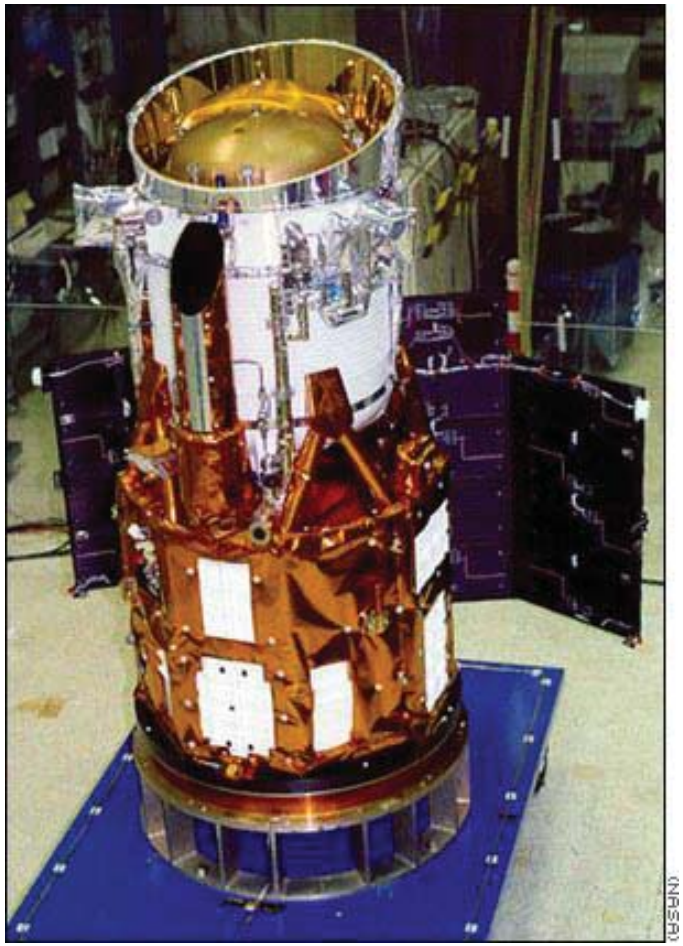
- Impact: Resulted in major disassembly of the spacecraft to test these components, which added 6 months of schedule slip and a significant cost.

- SE&I Deficiency:
  - Early reliance on heritage hardware was not reviewed by engineering.
  - Therefore, proper time and funding was not allowed for re-qualification, verification, and validation of heritage hardware.

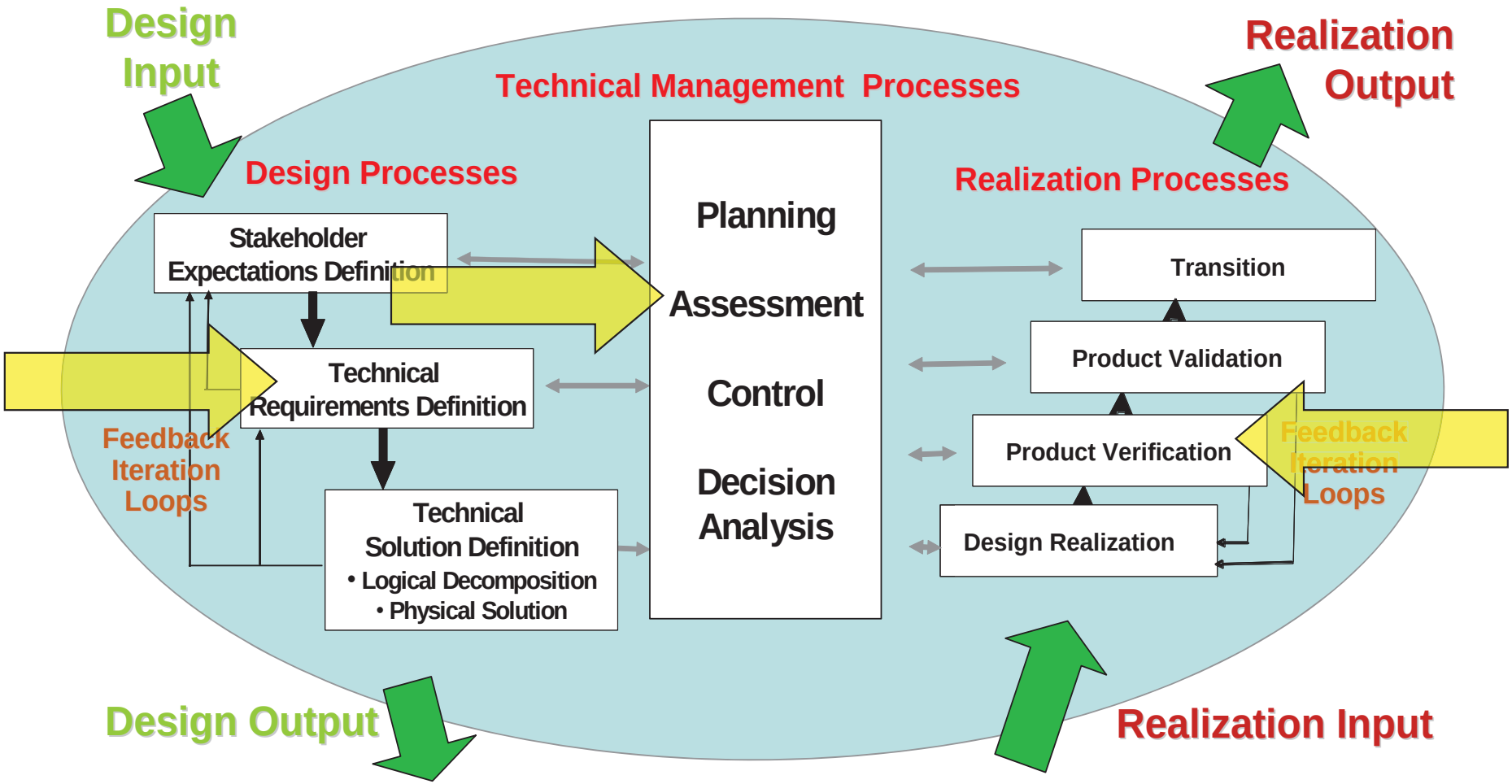
- Reference: Chris Calfee, Vehicle Systems Manager for DART

Wide-Field Infrared Explorer (WIRE) mission





Incomplete Technical Requirements Definition, Inadequate Assessment, and Insufficient Product Verification



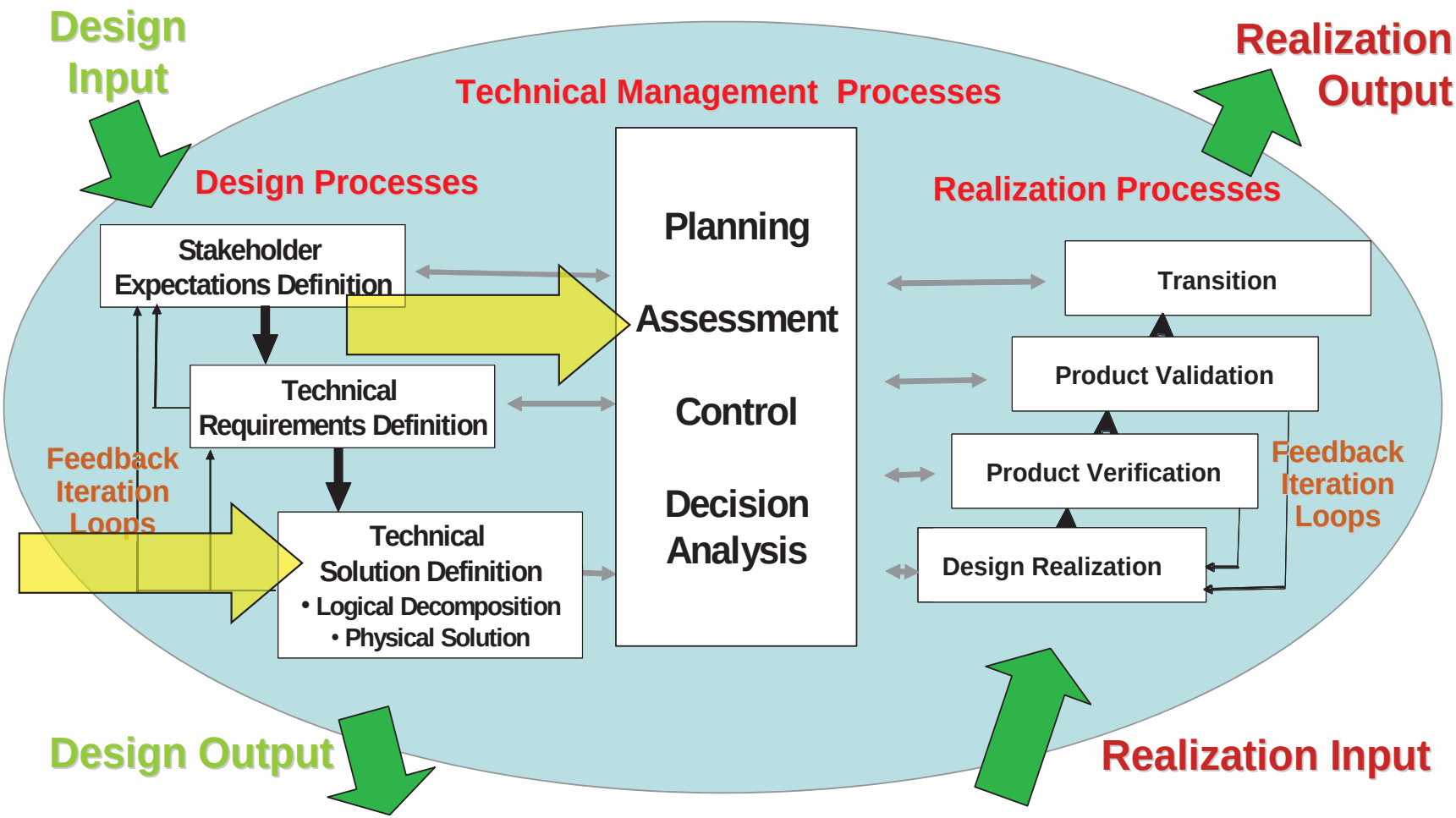
Wide-Field Infrared Explorer (WIRE) mission

- Issue: Investigation board found two potential opportunities to catch a fatal design error in the pyro electronics: Design review process and during test program.
- Impact: Loss of scientific mission (was recovered and was used for a number of asteroseismology investigations)
- SE&I Deficiency:
  - Mission development requirements were delegated through three layers of organizations; lack of detailed design review of key components
  - Inability to perform end-to-end testing; poor fidelity of pyro test box
  - Anomaly during testing was not recognized as a potential design flaw
- Reference: WIRE Case Study by James S. Barrowman

Chandra X-ray Observatory GSE

MSFC/Dale Thomas

Incomplete Technical Solution Definition and Inadequate Assessment

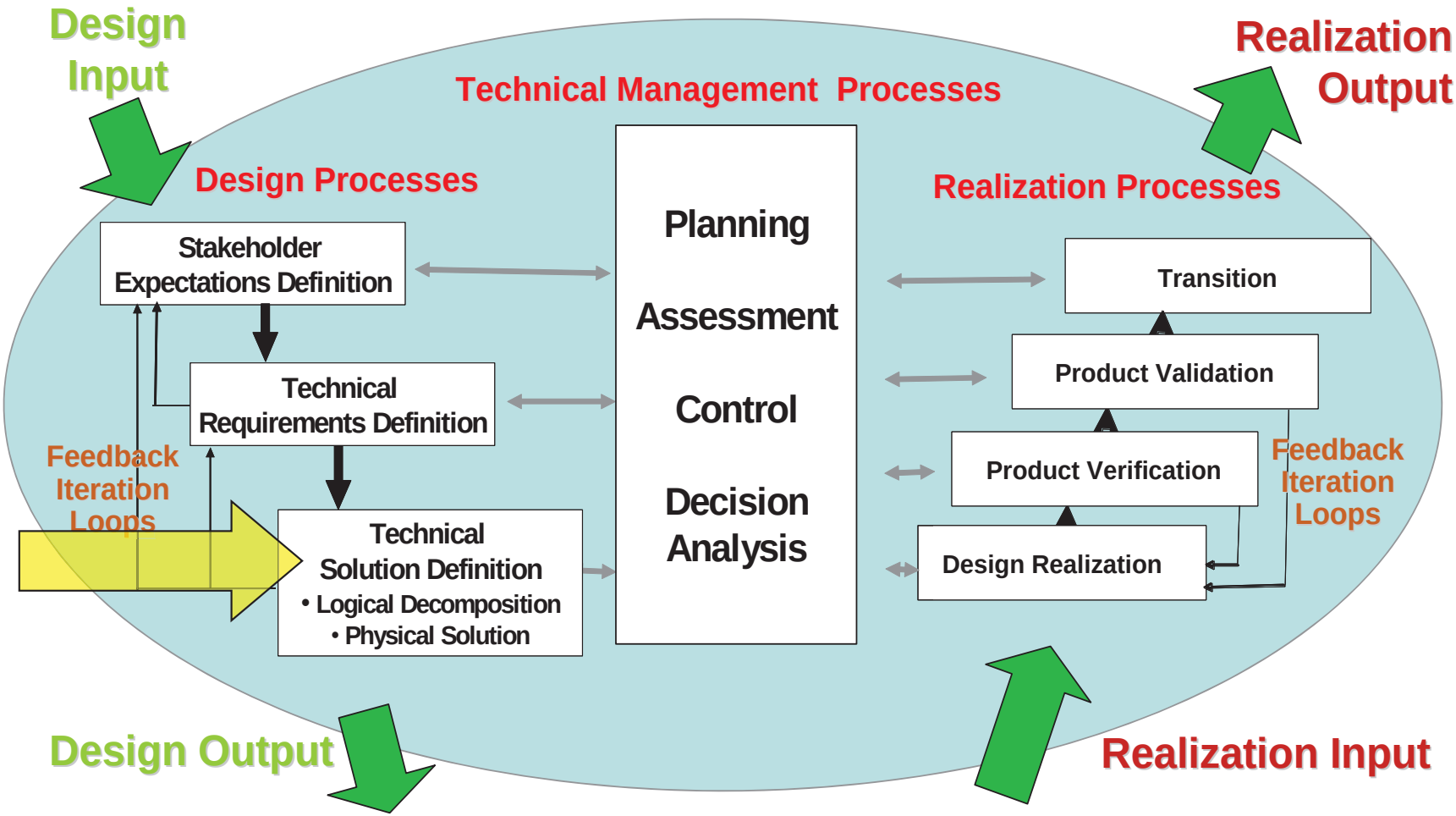


Chandra X-ray Observatory

- Issue: Early testing (9/97) revealed major underestimation of integration effort to support a August 1998 launch. Use of prime's existing GSE was the primary issue.
- Impact: Prime added FTE's and MSFC provided FTE's at prime's location to support 24/7 integration schedule for the July 1999 launch date.
- SE&I Deficiency
  - Inadequate Program requirements vs. GSE capabilities assessment
    - GSE had inadequate oversight/visibility early in program (existing GSE was part of an ongoing classified program)
    - GSE was provided by separate branch from program (Prime's program lacked penetration)
    - Older GSE technology lacked automation capabilities and inadequate off-line equipment to support debugging activities.
- Reference: Fred Wojtalik, Program Manager

FASTRAC Engine Seal Failure

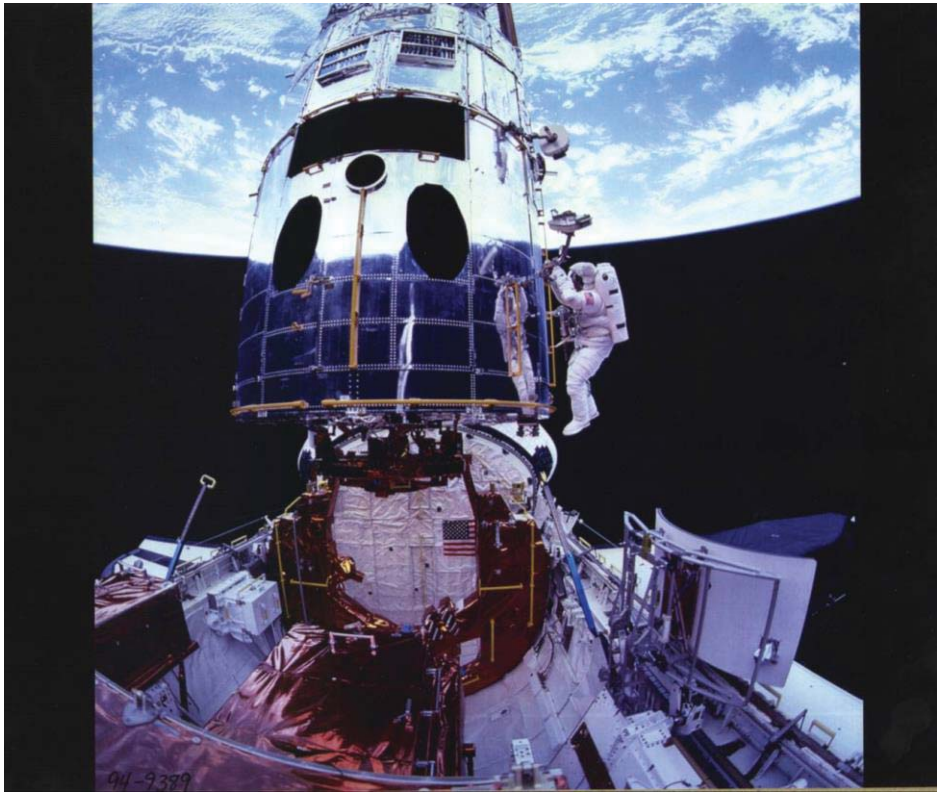
Incomplete Technical Solution Definition



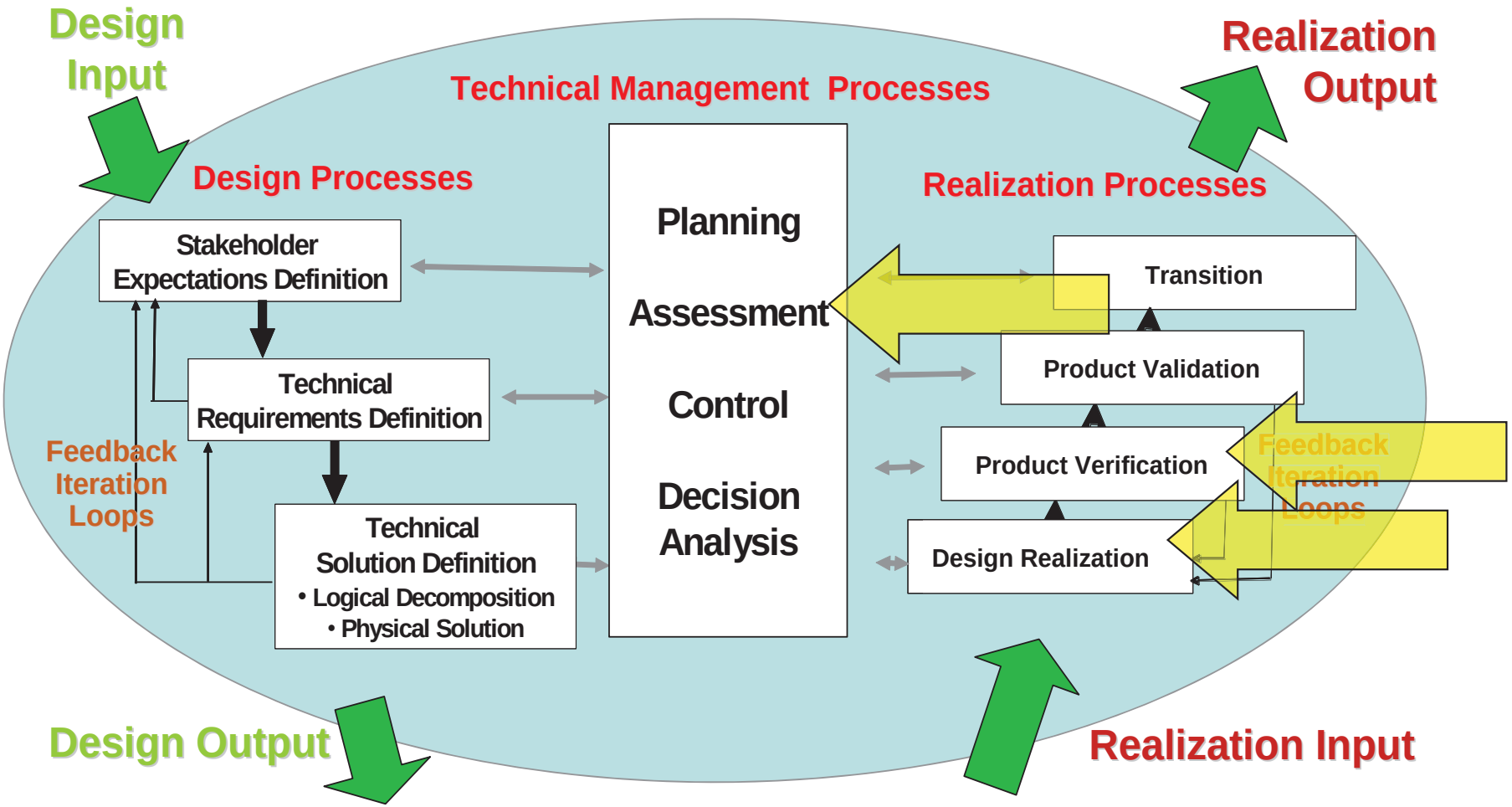
FASTRAC Engine Project

- Issue: Selection of Operational Cryogenic LOX Valve for use with RP-1 Fuel.
  - Cursory assessment erroneously deemed RP-1 environment less severe than LOX.
- Impact: Resulted in minor test stand fire, loss of approximately one month hot fire schedule, emergency, real time valve test, evaluation and redesign; co-location of government “tiger team” personnel onsite at contractor facility with 7 day/week, extended shift operation team during test and evaluation, valve redesign cost.
- SE&I Deficiency:
  - No Detailed analysis of valve design in new application
  - Valve operation in new environment was not thoroughly investigated; Material property (i.e. modulus of elasticity) change with temperature was overlooked, resulting in excess deflections during valve transient operation and failure of valve to close properly on command.
- Reference: George Young - Chief Engineer; Tim Ezell – Tiger Team Member

Hubble Space Telescope Spherical Aberration



Flawed Design Realization, Incomplete Product Verification, & Inadequate Assessment



Hubble Space Telescope Spherical Aberration

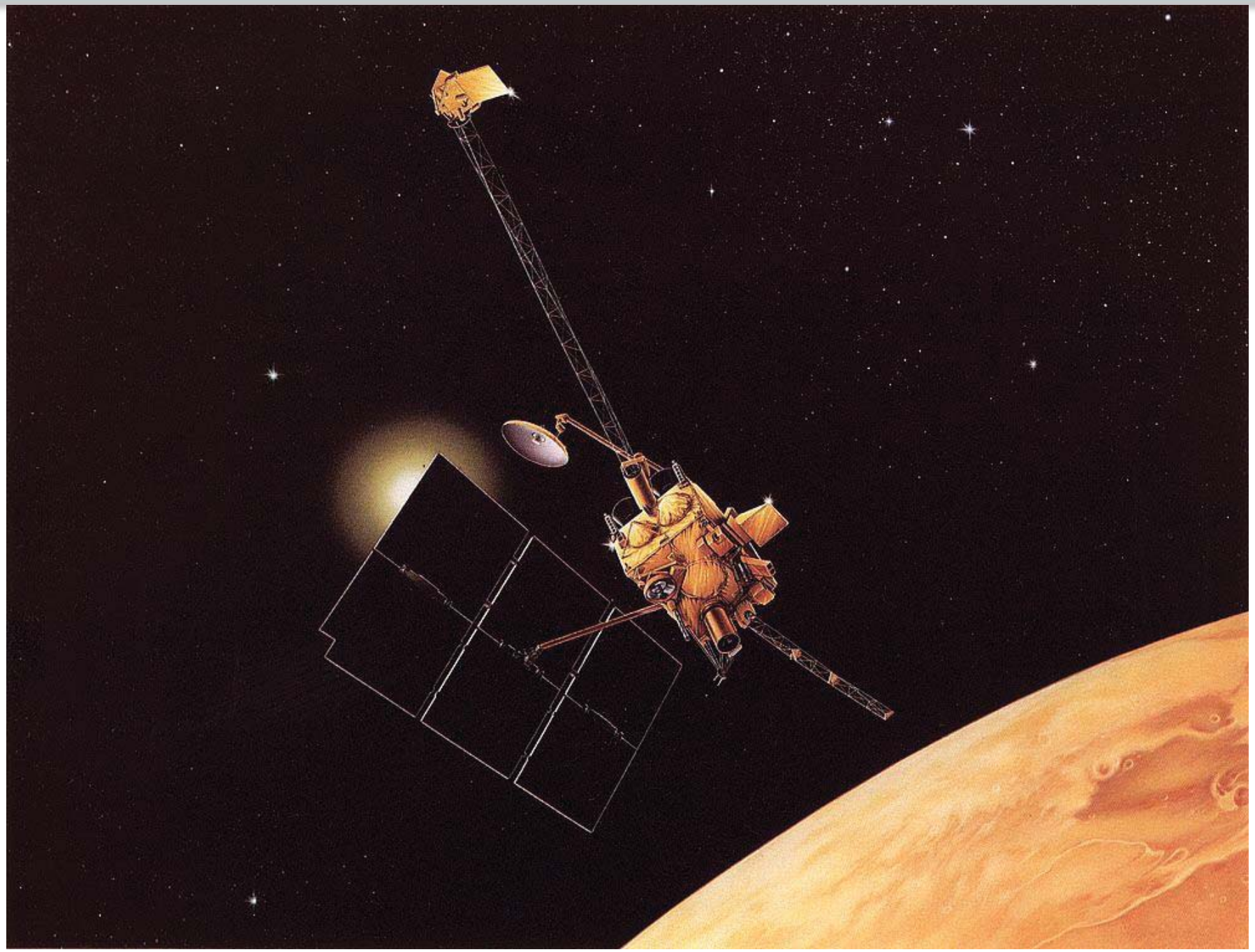
- Issue: Primary mirror improperly ground, resulting in a spherical aberration that rendered the wide field camera useless.

- Impact: COSTAR (the Corrective Optics Space Telescope Axial Replacement) was developed to counter the effects of the flawed shape of the mirror.
  - COSTAR was a telephone booth-sized instrument which placed 5 pairs of corrective mirrors, some as small as a nickel coin, in front of the Faint Object Camera, the Faint Object Spectrograph and the Goddard High Resolution Spectrograph.
  - Installed on the first HST Servicing Mission

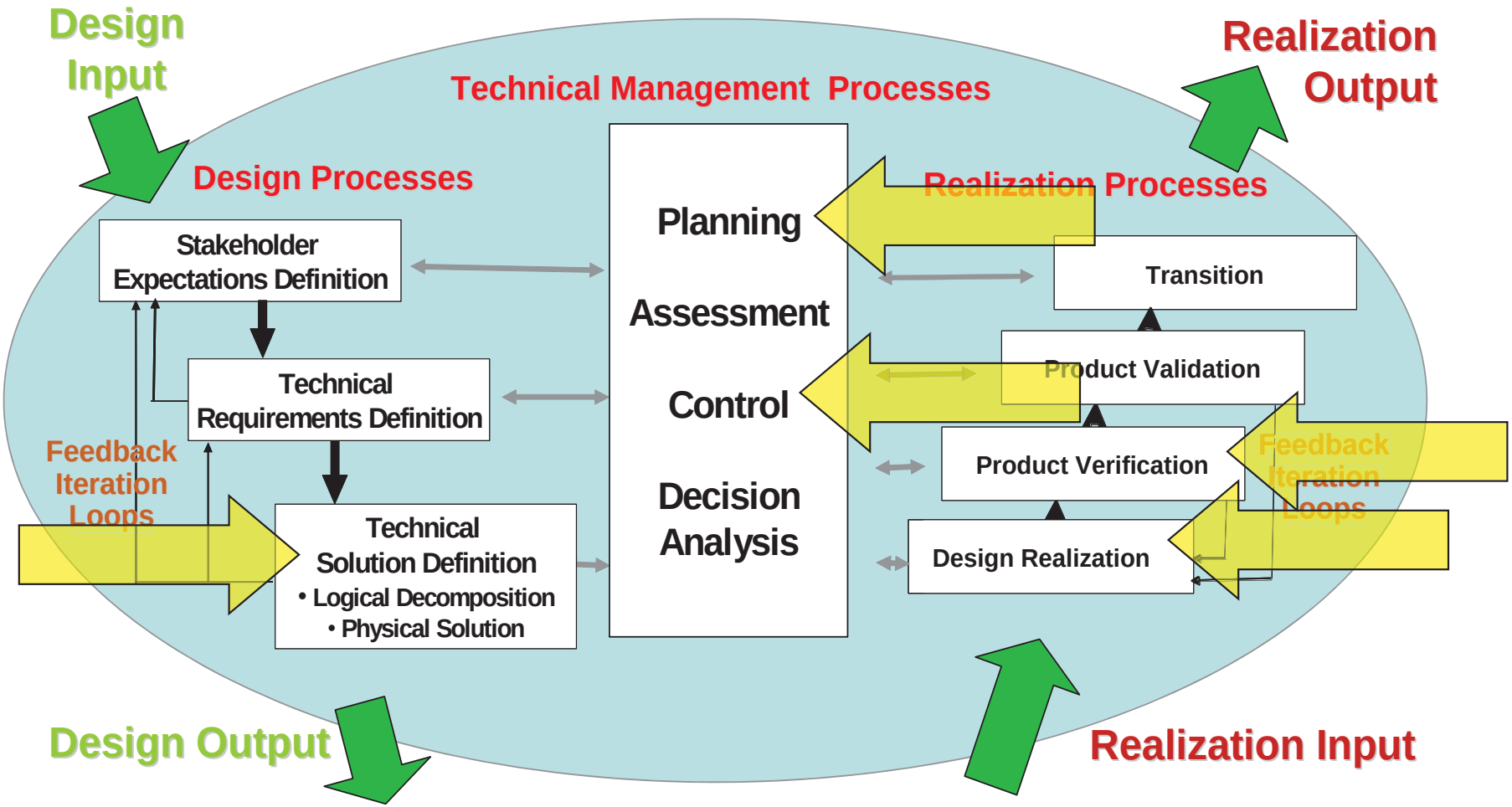
- SE&I Deficiency:
  - The reflective null corrector (RNC) used as an optical template to shape the mirror was flawed, resulting in an improperly shaped primary mirror.
  - Data from other devices used in mirror alignment & calibration indicated problems with the RNC, but these results were discounted as being flawed themselves.
  - End-to-end test of the Optical Telescope Assembly was not performed due to expense.

- Reference: HST Optical Systems Failure Report

Mars Observer



Inadequate Planning & Control, Flawed Technical Solution Definition & Design Realization and Incomplete Product Verification



Mars Observer

- Issue: Design and component heritage qualification that was inappropriate for the mission.

- Impact: Contact with Mars Observer was lost three days before scheduled orbit insertion, for unknown reasons.

- SE&I Deficiency:
  - failure to qualify the traveling wave tube amplifiers for pyro firing shock;
  - design of the propulsion system;
  - use of a fault-management software package that was not fully understood,
  - The Board also noted that “the discipline and documentation culture associated with, and appropriate for, commercial production-line spacecraft is basically incompatible with the discipline and documentation required for a one-of-a-kind spacecraft designed for a complex mission. Mars Observer was not a production-line spacecraft.”

- Reference: Mars Observer Mission Failure Investigation Board Report

Remarks

- There are very real consequences for short-cutting the Systems Engineering process.
- Prime contracts are often negotiated on the basis of assumptions that pre-suppose the outcome or even omit selected steps of the systems engineering process.
- Reuse of exiting technology or heritage hardware/software can tempt one to omit steps in the front end of the systems engineering process.
- When system testing is scaled back, technical assessment must be scaled up proportionately.