Systems Engineering
Basic Principles Applied

Michael Bay

Bay Engineering Innovations, Inc
301-286-9759
michael.bay@bayengineering.org

Who Said This, and When?

“I believe that the fundamental difficulty is that we have all become so entranced with technique that we think entirely in terms of procedures, systems, milestone charts, PERT diagrams, reliability systems, configuration management, maintainability groups and the other minor paper tools of the "systems engineer" and manager.

We have forgotten that someone must be in control and must exercise personal management, knowledge and understanding to create a system. As a result, we have developments that follow all of the rules, but fail.”

“We have lost sight of the fact that engineering is an art, not a technique; a technique is a tool.”

“We must bring the sense of art and excitement back into engineering. Talent, competence, and enthusiasm are qualities of people who can use tools; the lack of these characteristics usually results in people who cannot even be helped by techniques and tools. We can all do better.”

Exploring Space is Exciting, Challenging But Unforgiving

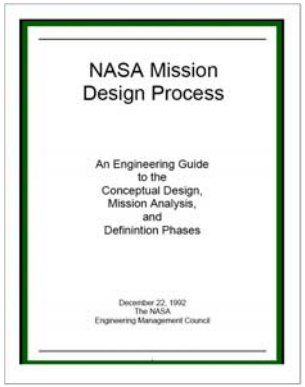
System Engineering Skills

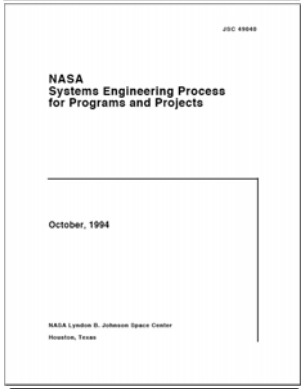
- System Engineers Can't Learn Everything They Need to Know Directly by Doing. Careers are too Short with No Need to Repeat the Mistakes of the Past
- High Value Resources are Available
- A Crucial Skill of a Systems Engineer Involves Knowing and Using Resources
  - A Systems Engineer can not possibly know everything, but through communications can facilitate a team that collectively addresses everything
  - and, There is No Cook Book!
  - Systems Engineers must understand and know how to apply basic principles and best practices grounded in past mission successes
- Resources for the Systems Engineer :
  - #1 = People, others who have done the job
  - Solutions to similar problems and challenges
  - Proven processes, lessons learned and affirmed, best practices, products and standards that have been developed over the years
    - Processes, best practices, and guidelines enable the successes of the past to be applied to the present
  - Library, articles, papers, textbooks, online resources

Recent Background

- 1989 to 1995: Effort to document successful NASA Systems Engineering Processes before those with the knowledge retire
  1. “The NASA Mission Design Process” EMC 1992
  2. “NASA Systems Engineering Process for Programs and Projects”, JSC-49040 prepared as companion to SE Handbook1994
  3. “NASA Systems Engineering Handbook” SP6105 1995
- Middle to Late 1990s: “Faster Better Cheaper”
  - NPG 7120.5A superceded NHB 7120.5 In 1998

    (No Phased Lifecycle, No mission risk classification)
  - “The NASA Mission Design Process”, JSC 49040 “NASA Systems Engineering Process for Programs and Projects”, and SP6105 “NASA Systems Engineering Handbook” all declared “out of print”
- Early 2000s: Efforts to return to some of the basic principles and processes inadvertently discarded as part of “Faster Better Cheaper”
  - 2004 NPR 8705.4 Risk Classification for NASA Payloads approved
  - 2005 NPR 7120.5C Update reinstates the Phased Lifecycle
  - 200? Return to Printing SP6105 NASA Systems Engineering Handbook





QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

NASA Systems Engineering Handbook SP6105

- An excellent resource for the proven processes, techniques, and methodologies grounded in 40+ years of successful NASA Space Systems Engineering

  "This handbook represents some of the best thinking from across NASA. Many experts influenced its outcome, and consideration was given to each idea and criticism. It truly represents a NASA-wide product and one which furnishes a good overview of NASA systems engineering."p.ix

  "This handbook was written to bring the fundamental concepts and techniques of systems engineering to NASA personnel in a way that recognizes the nature of NASA systems and the NASA environment." p.xi

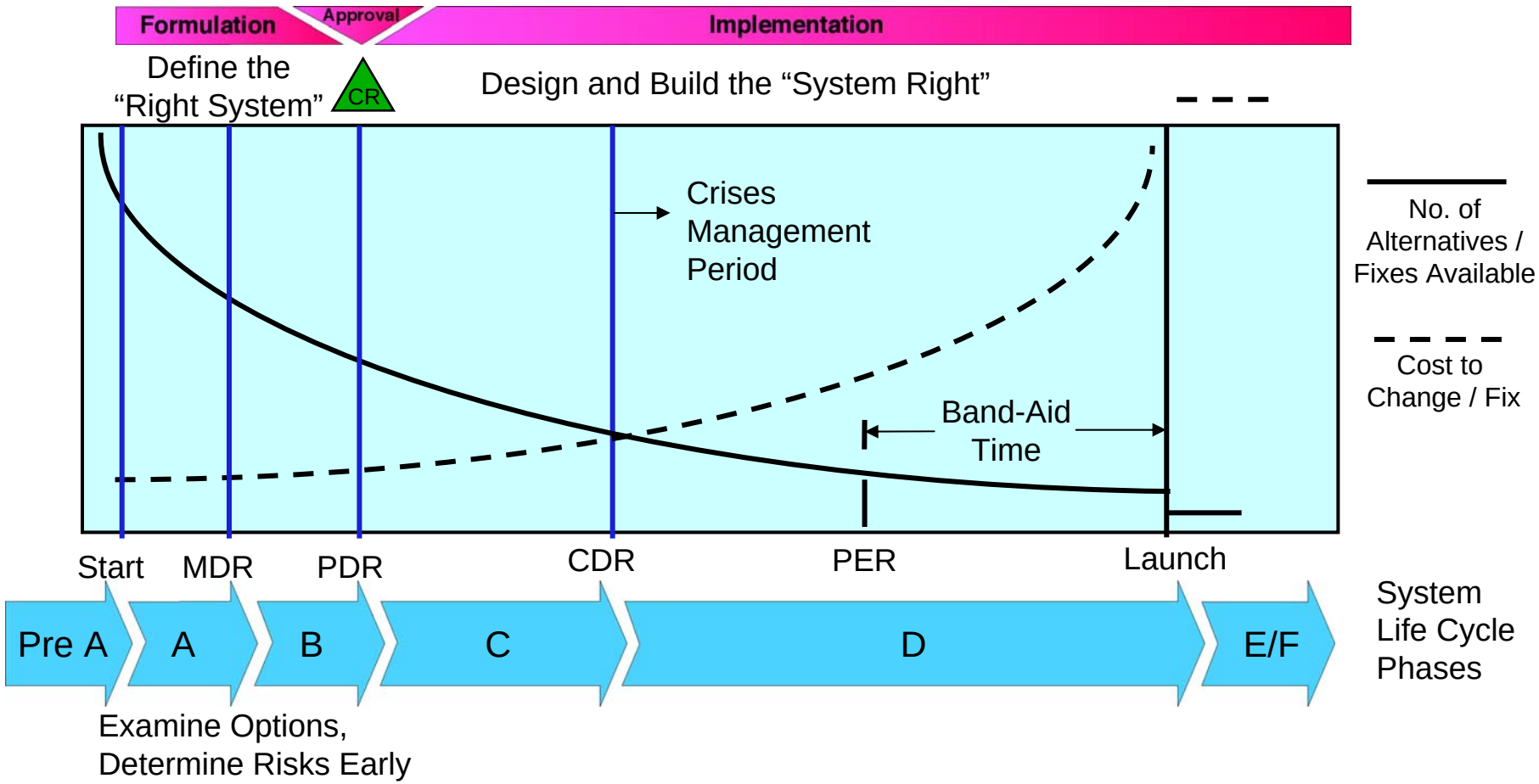
  "The main purposes of the NASA Systems Engineering Handbook are to provide:

  1) useful information to system engineers and project managers,
  2) a generic description of NASA systems engineering which can be supported by center-specific documents,
  3) a common language and perspective of the systems engineering process, and
  4) a reference work which is consistent with NMI 7120.4/NHB 7120.5." p.ix

SP6105 Core Chapters p.xi

- systems engineering's intellectual process,
  "2 Fundamentals of Systems Engineering"
  - Definitions, Successive Refinement, Trade Studies, Cost Effectiveness
- the NASA project life cycle,
  "3 Project Cycle for Major NASA Systems"
  - Systems Engineering Process Along the Life Cycle
- "4 Management Issues in Systems Engineering,"
  - Managing the Systems Engineering Process
  - Describing the Management Approach in the Systems Engineering Management Plan
  - Risk Management
  - Reviews Audits and Control Gates
  - Status Reporting and Assessment
  - Systems Engineering Process Assessment - How good is the Systems Engineering
- "5 Systems Analysis and Modeling Issues" ,
  - Trade Studies and Modeling
  - Cost Effectiveness Measures
- "6 Integrating Engineering Specialties Into the Systems Engineering Process"

Early Phases of the Life Cycle Have High Payoff



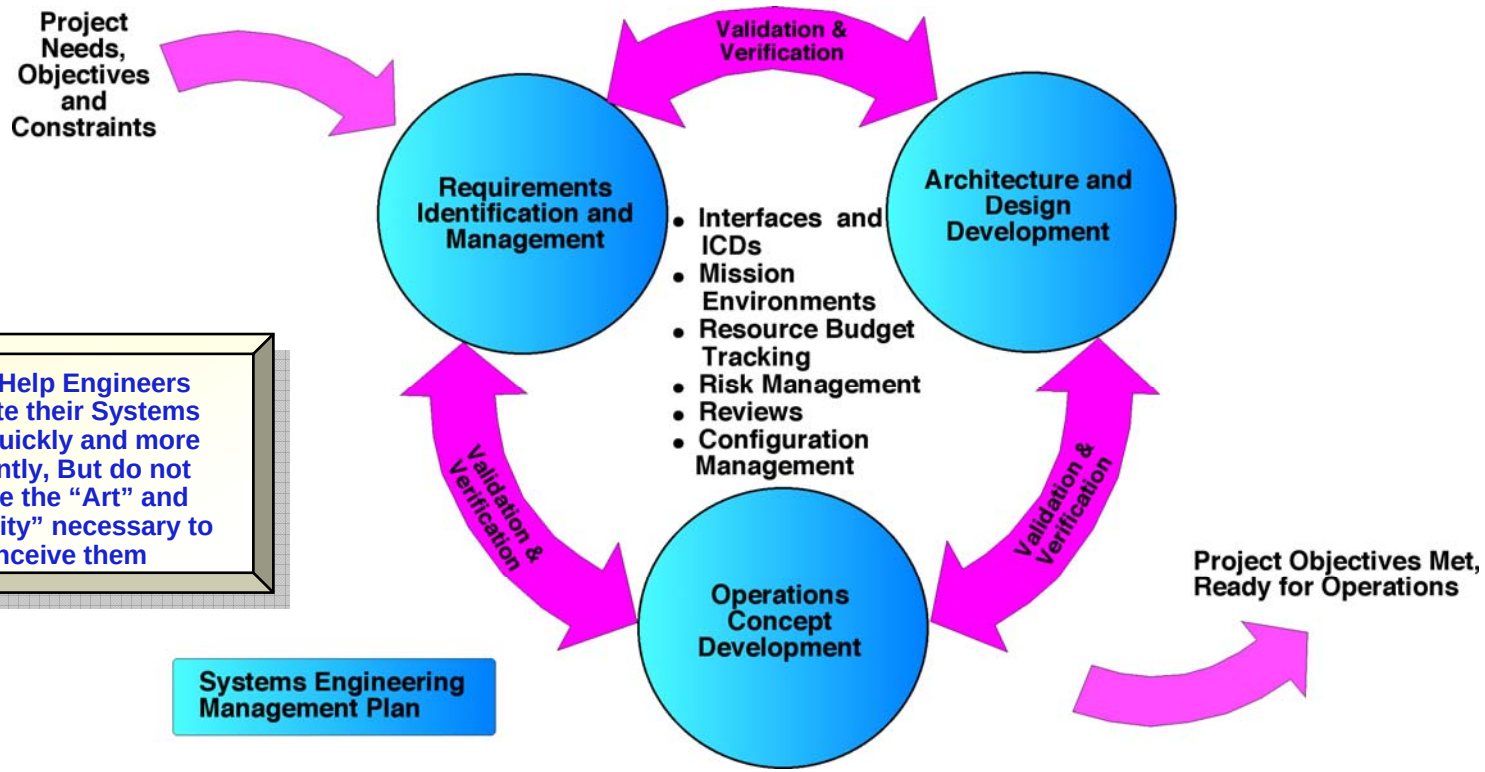
- **Life Cycle Phases define the activities and milestone review gates for proper <u>sequencing</u> and <u>pacing</u> of work**
- **Risk Management seeks to identify what could be done early to minimize chances of problems**

Iterative Nature of Systems Engineering

"The realization of a system over its life cycle results from a succession of decisions among alternative courses of action. If the alternatives are precisely enough defined and thoroughly enough understood to be well differentiated in the cost-effectiveness space, then the system manager can make choices among them with confidence." SP6105 2.5 p.7

- Section 2.5 Describes the Iterative Systems Engineering Processes
- Section 5.1 Describes the Trade Study Process

Iterative Interrelationship of Key Systems Engineering Functions



Tools Help Engineers Evaluate their Systems more quickly and more efficiently, But do not replace the "Art" and "Creativity" necessary to conceive them

"The objective of systems engineering is to see to it that the system is designed, built, and operated so that it accomplishes its purpose in the most cost-effective way possible, considering performance, cost, schedule and risk."

NASA Systems Engineering Handbook SP6105 2.3

Key Systems Engineering Functions

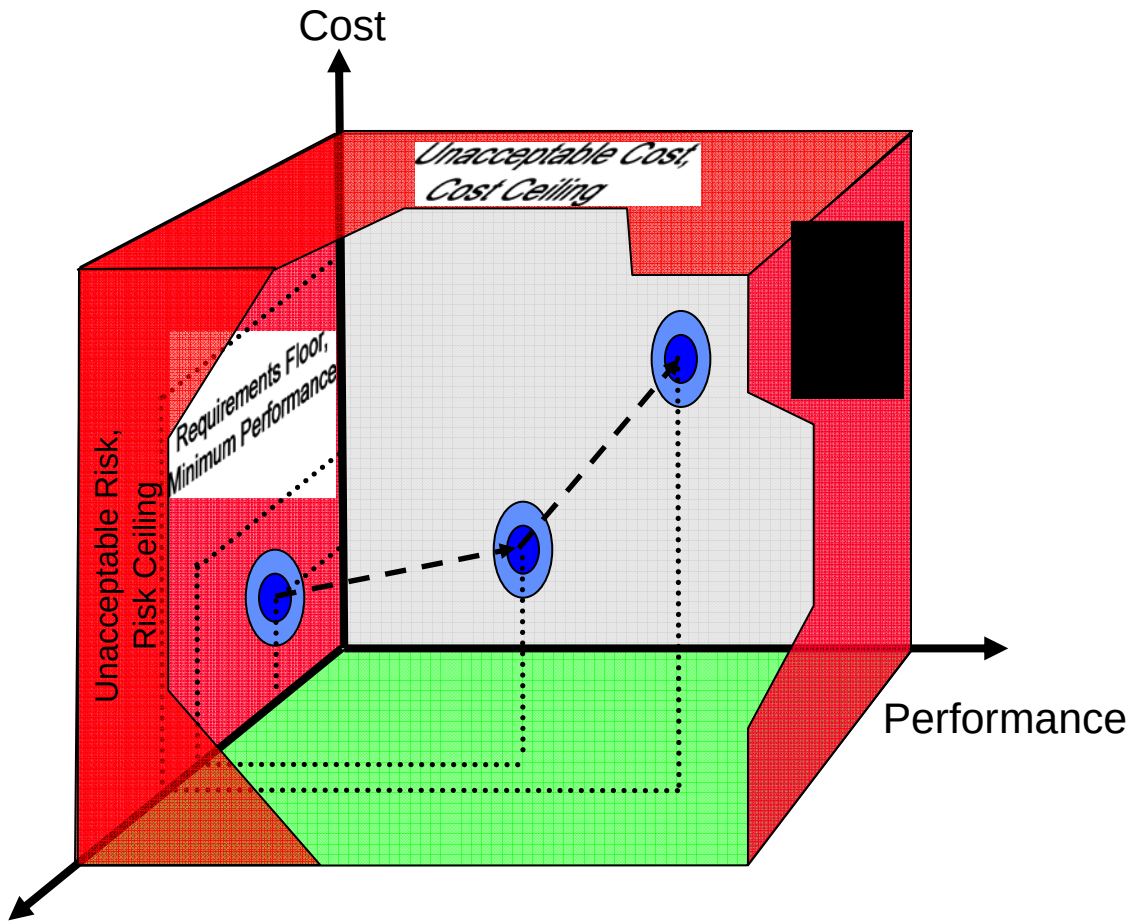
- Iterating Among The Three Key Functions Must Lead to a System With Consistent Design, Requirements and Operations Concept While Meeting Customer's Needs, Objectives, and Constraints which include Technical, Cost, Schedule and Risk
  - Requirements Identification and Management
    - Level 1 Requirements, Mission Success, Minimum Mission Success
      - Mostly Driven by Mission / Science
    - Top Down Hierarchy
      - Requirements Flow, Doc Tree, Product Breakdown Structure, WBS, Team Org
    - Identify, understand what is important, the drivers, so everyone knows their own role and who does everything else
  - Architecture and Design Development
    - What the End Item Looks Like:
      - Flight and Ground Elements, Hardware, Software, Operations Team
    - Critical Interfaces Among System Elements
    - Special accommodations for verification and test
      - Design for Testability
  - Operations Concept Development
    - How the End Item is Used to Meet the Requirements and Accomplish the Mission: Flight and Ground Elements, Hardware, Software, Operations Team
    - How the End Item can be verified and tested on the ground
      - Test Points, GSE impacts on Architecture and Design

Achieving Consistency of the Requirements, Design and Operations Concept

- Requirements, Architecture & Design, and Operations Concept need to be self consistent while meeting Customer Needs, Objectives and Constraints
  - If these are not consistent then the solution may not be the “Right System”, or may not have implemented the “System Right”
- Consistency is addressed repeatedly over the project life cycle
  - Phase A brings them into initial agreement - “Single Best System”
  - Phase B refines them and shows close agreement analytically - “Right System”
  - Phase C and D makes sure that they remain in agreement
- The “Validation” process assures consistency with Needs Objectives and Constraints, the “Right System” is chosen
  - Trade Studies
    - Select a single approach from a number of options
    - Establish Evaluation Criteria including Cost, Performance, Risk
  - Performance Predictions
    - Validate the candidate design meets customer needs and objectives based on operations concept
    - Operations concept includes the environments, orbit, sequence of operations
  - Decisions and Engineering Judgment
- The “Verification” process assures consistency with requirements, design and build the “System Right”

Evaluating Cost Effectiveness, Staying "In the Box"

Performance, Risk, Costs



- Safety
- Mission Success
- Development

- Start by defining "the box" for the mission
- Define a minimum performance system that meets cost and risk limits
  - Starting at what is technically possible and then scaling back to get "in the box" is much more difficult
- Leave margin to box limits to allow for the unexpected, risk mitigation, and growth
- Iterate system / trade / add additional capability where necessary
- Iterate requirements, design, and operations concept
- Resist Requirement "creep" and expansion
- Allow the "Is this the right requirement?" question

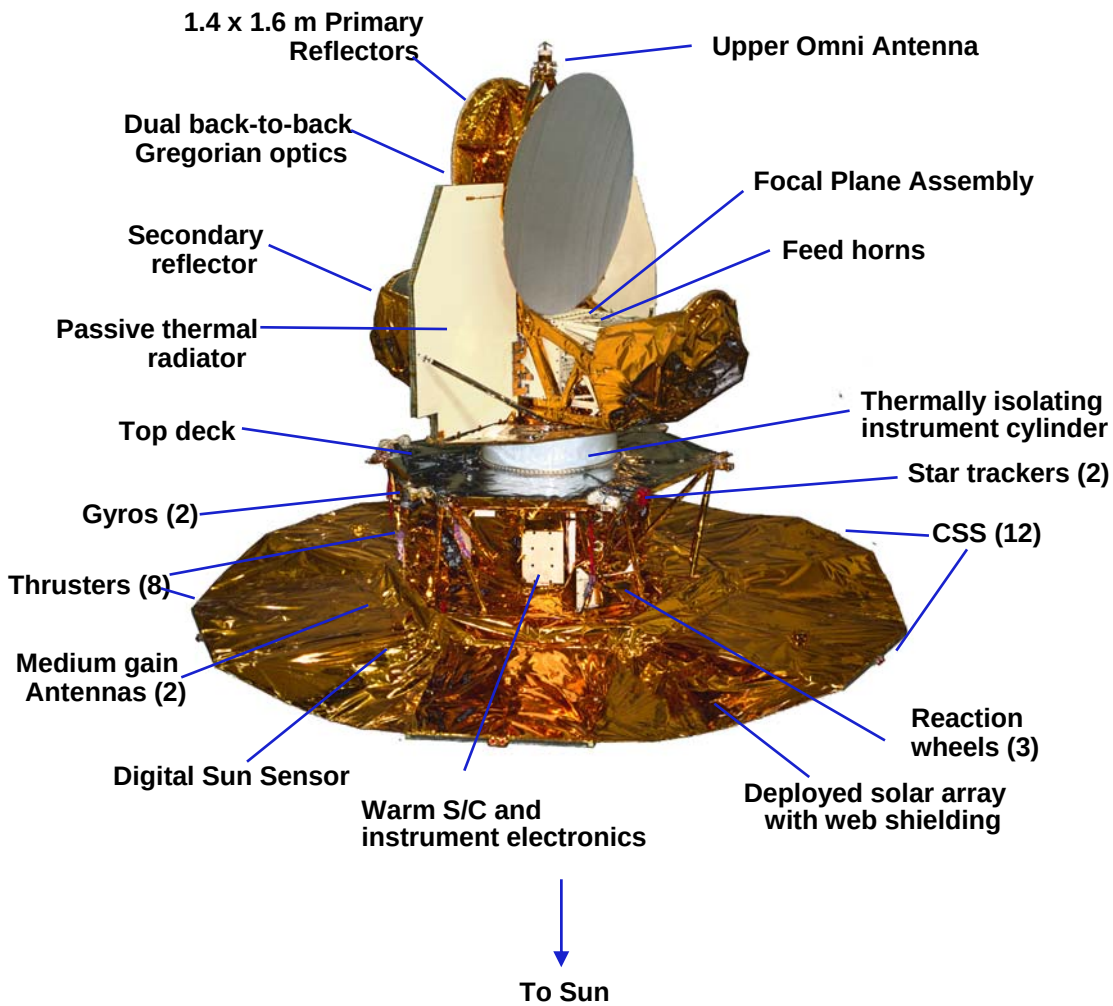
MAP Observatory, An Example

Microwave Anisotropy Probe

- Map the Cosmic Microwave Background Radiation
- Follow on to COBE with 50 times the resolution
- Medium Size Explorer, MIDEX
- Operate at L2, Store and forward data every day
- 3 Axis, Scan Sky at 1 revolution every 2 minutes
- 835 Kg, 3.6 meters tall, 5.1 across
- 400 Watt load, 72 Kg Fuel
- Launched 6/29/2001, successfully collected “MAP” of the early universe

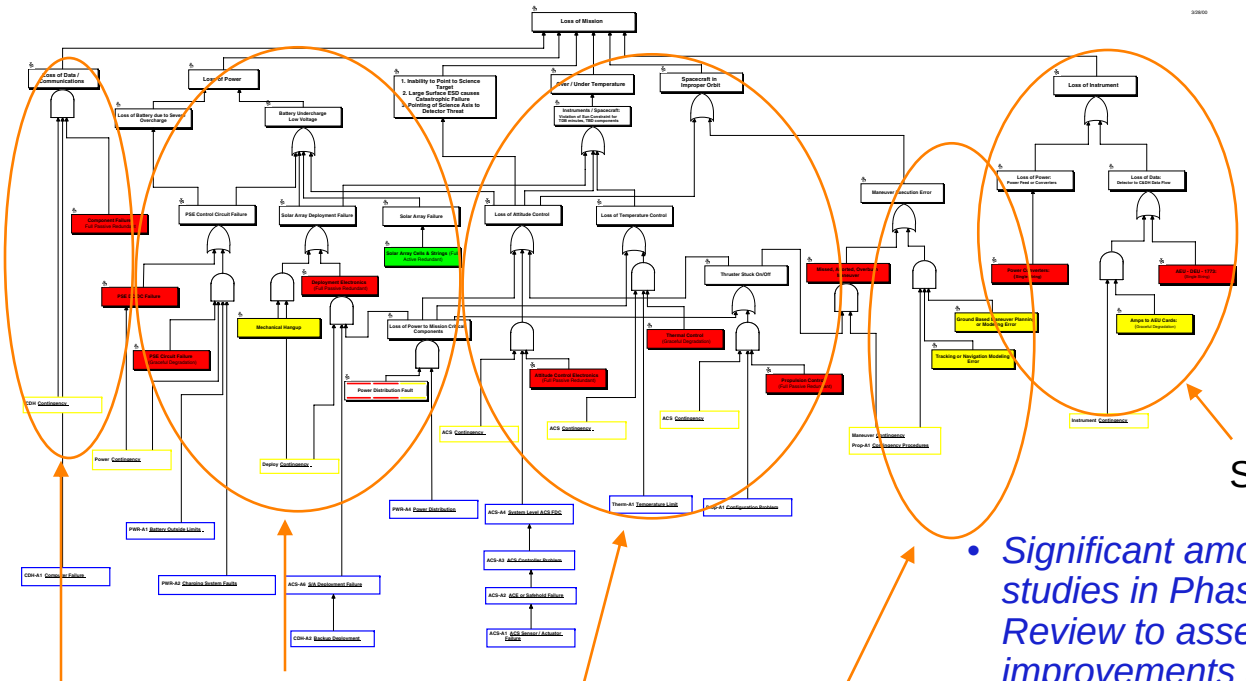
Systems Engineering Challenge

- Team Felt the Single String System Contained Too Much Mission Risk
- Identified Candidate System Reliability Improvements Along With Performance and Cost Impacts
- Team Adopted High Value Reliability Improvements During Phase B



Fault Logic Diagram /

Initial Mission Fault Tree (Phase A&B), Too Many SPFs



Science

Power & Deployment

Orbit, Attitude Control and Propulsion

Mission Operations

Communications

- *Significant amount of "red" boxes prompted trade studies in Phase B prior to the Confirmation Review to assess potential mission success improvements and risk reduction*
- *Critically Questioned whether we had the "Right System", given the acceptable risk, mission objectives, and cost constraints*

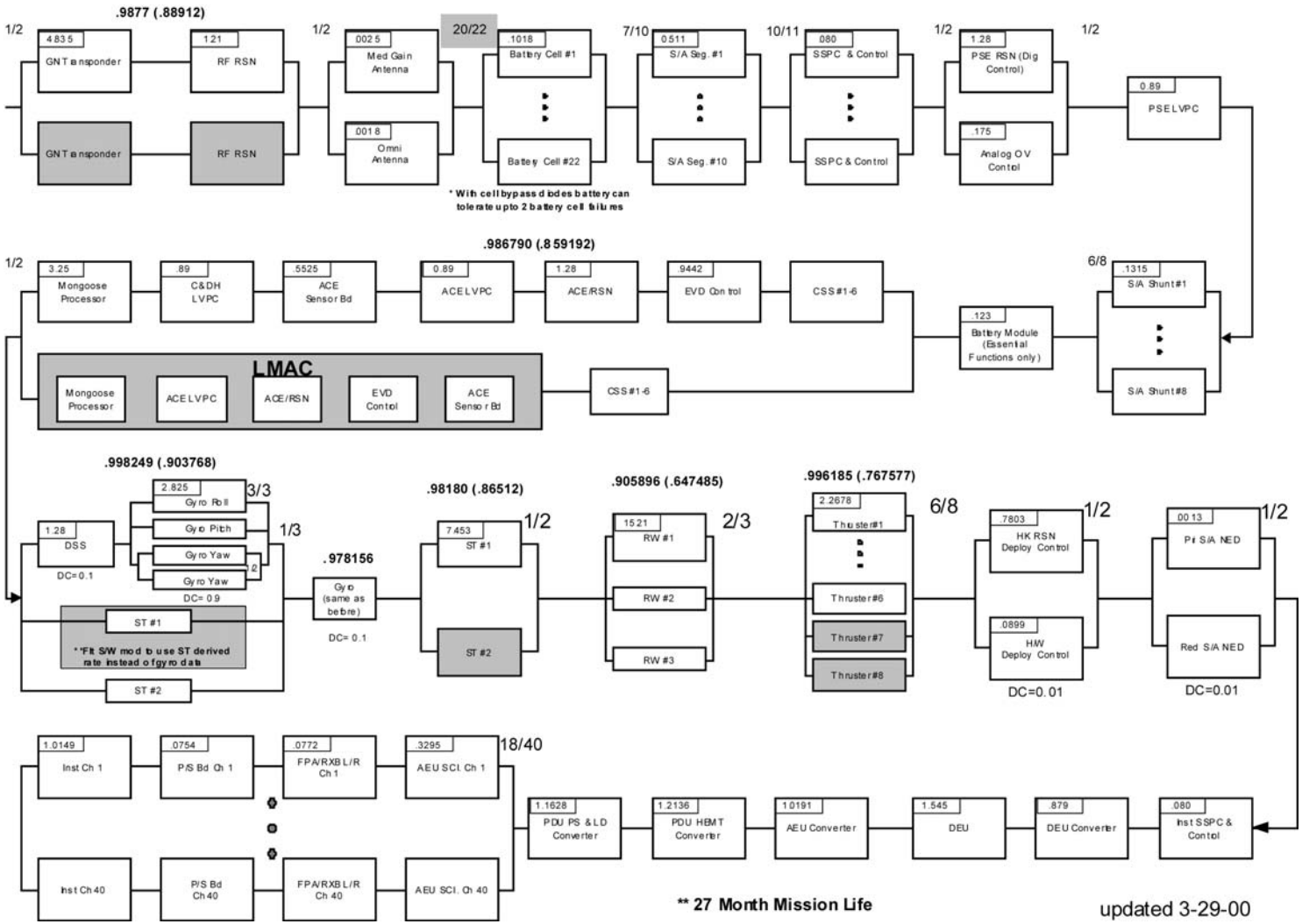
- Graphically Shows System Elements Susceptible to Single Point Failures (Red), Graceful Degradation (Yellow), or are Redundant (Green).
- Provides cross check of the Fault Tree (Top Down) to the FMEA (Bottoms Up)
- Used to identify Contingency Procedures and Onboard Fault Protection Algorithms that are necessary to implement Graceful Degradation and switch in Redundancy

White Box - Failure Propagation
Red Colored Box - Single Point Failures
Yellow Colored Box - Graceful Failures
Green Colored Box - Redundancy Failures
Yellow Outline Box - Ground Contingency Procedure
Blue Outline Box - Onboard FDC
Red Outline Box - Critical Software

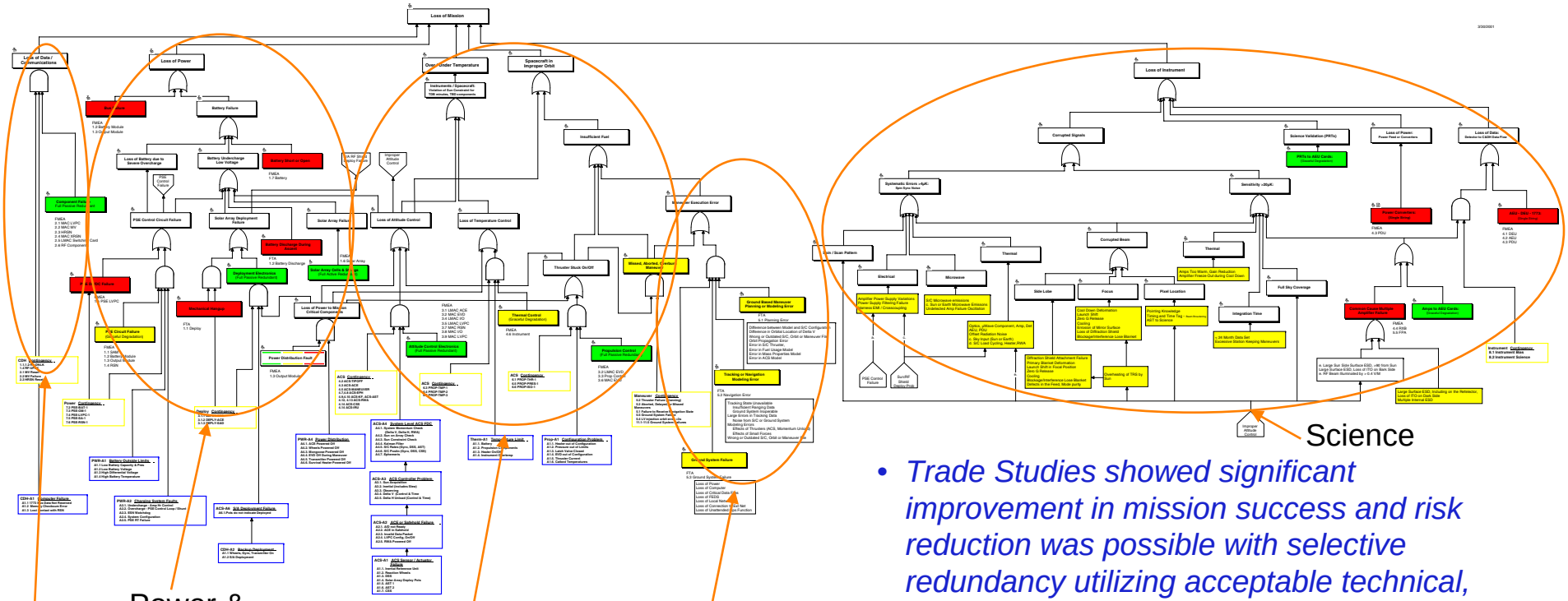
Reliability Analysis

Supported notion that system contained too many “Weak Links”

- Dark Grey boxes identify analysis driven reliability improvements



Fault Logic Diagram /
Final Mission Fault Tree Example (Phase C/D/E Final Flight)



- *Trade Studies showed significant improvement in mission success and risk reduction was possible with selective redundancy utilizing acceptable technical, cost and schedule resources*
- *Significantly less "Red" boxes, More Green and Yellow*
- *Much Better Understanding of Instrument*

- Graphically Shows System Elements Susceptible to Single Point Failures (Red), Graceful Degradation (Yellow), or are Redundant (Green).
- Provides cross check of the Fault Tree (Top Down) to the FMEA (Bottoms Up)
- Used to identify Contingency Procedures and Onboard Fault Protection Algorithms that are necessary to implement Graceful Degradation and switch in Redundancy

White Box - Failure Propagation
Red Colored Box - Single Point Failures
Yellow Colored Box - Graceful Failures
Green Colored Box - Redundancy Failures
Yellow Outline Box - Ground Contingency Procedure
Blue Outline Box - Onboard FDC
Red Outline Box - Critical Software

MAP Reliability Improvement Results

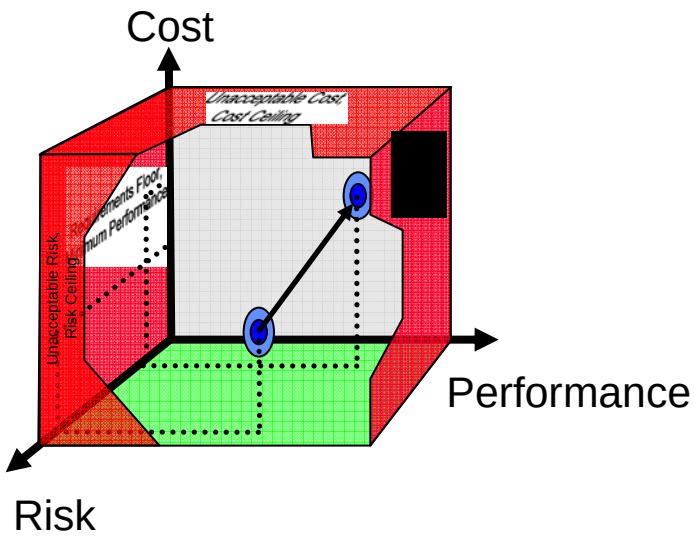
- MAP Initially a Single String Design
- Reliability Analysis Showed a Significant Improvement was Possible to strengthen the “weakest links” to mission success:
  - Flight Software to provide a 2 of three Reaction Wheel Control Mode
  - Add 2 more thrusters to the 6 in order to provide functional backups
  - Redundant Transponder, Star Tracker, ACE and C&DH Electronics
  - Add Minimal Backup Electronics for Critical Deploy & Housekeeping Functions
  - Flight Software to allow Star Tracker to backup Gyros
- Reduce launch risk by eliminating mission specific “offload” of solid propellant from 3rd stage. Add 4th solid motor to launch vehicle 1st stage to increase mass to orbit
- Project Reserves (Mass, Power, Cost and Schedule) were applied for the above improvements
- Improvements considered but not implemented due to existing robustness, process controls, and graceful degradation inherent in system along with large required expenditure of technical, cost and schedule resources:
  - Redundant Instrument Electronics
  - Redundant Power System Electronics
- Based on Reliability analysis, System as Launched was significantly more reliable than initial Single String System

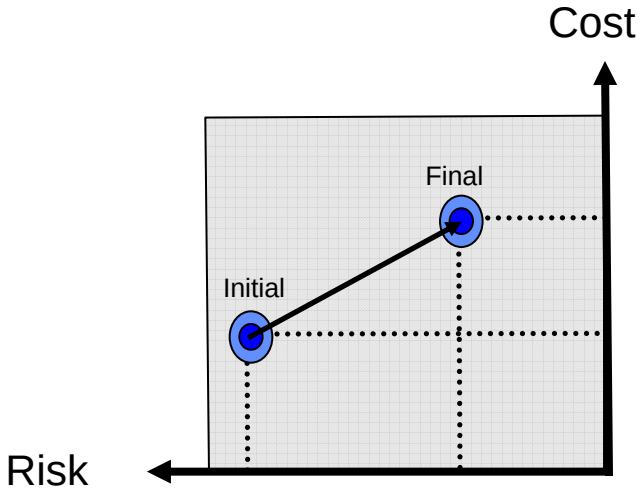
MAP Reliability Improvement Results

	Reliability Improvement	Location	Performance	Future Descope (Mass, Pwr)	System Reliability Improvement	Mass	Power	Cost	Schedule	Comments
1	Flight Software to allow 2 out of 3 Wheels	Mongoose ACS Software	Minimum Science, Reduced Control & Acquisition	N/A	70%	0	0	Med	Low	S/W change can be delayed until failure
2	2 More Thrusters, Flight Software to allow Thruster Backup	Same bracket as Radials	Minimum Science, Additional Fuel Usage	No	30%	1.2	4 Watts Heater	Low	Low	
3	2nd Transponder & XRSN	XRSN in MAC, Xpndr beside existing on bottom deck	100%	Yes	11%	6.5	6 Watts, 0 Heater	Med	Low	
4	2nd Star Tracker	Under Top Deck near PSE	100%	Yes	13%	7	8-12 Watts	Med	Low	
5	"Little MAC" - 2nd Mongoose, LVPC & Minimal ACE RSN, 2nd set of 6 CSS Eyes	Beside MAC on same panel	Minimal Function, Minimum Science	Yes	14%	6.5	0 Watts	Med	Low	
6	Flight S/W to allow Star Tracker to backup Gyros	Mongoose ACS Software	No Backup for Acquisition, 100% Mission	N/A	9%	0	0	Low	Low	
	Subtotal				249%*	21.2	22 Watts			
	Reliability improvement of selected options				249%*					
7	2nd AEU & PDU 20/20 Configuration, DEU Single String	Bottom Deck, PDU Under Top Deck w/4th Wheel	Loss of 1/2 of Instrument	No	7%	10.3	8.5 Watts	Med	High	3 mos for windings, No Actels
8	4th Wheel	Bottom Deck equally spaced, or on Bottom Deck TBD	100%	Yes	13% 4th wheel w/ S/W; 83% 4th wheel inc S/W (2 of4); 57% w/o S/W(3 of 4)	17	10-15 Watts Heater	Med	Med	Large Mechanical System Impact
9	PSE Linear Regulators and Assurance Output Modules Remain On	2nd side of existing boards	100%	No	2%	0.2	0 watts	Med	Med	Long Lead Parts
10	DEU with 20/20 split		Loss of 1/2 of Instrument	No	11%			High	High	Parts Availability, Actels
	Subtotal				108% or 78% *	27.5	23			
	Reliability improvement potential of all options				326% *					
	* The percentage improvement is <u>not</u> a summation of the individual option improvement percentages.									

MAP Lessons Affirmed

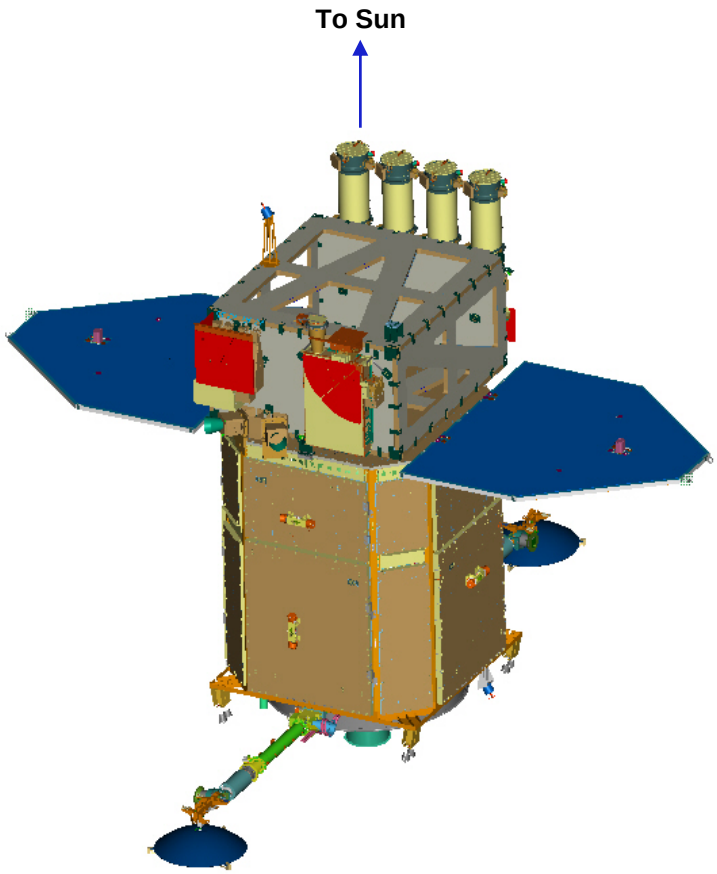
- Reliability Analysis when applied early in the lifecycle provides a useful technique for evaluating mission robustness
- When applied early in the life cycle, alternate design options can improve Reliability and Reduce Risk
- With margin to Cost, Performance and Risk Constraints, Project Teams can Iterate the System Design





Solar Dynamics Observatory

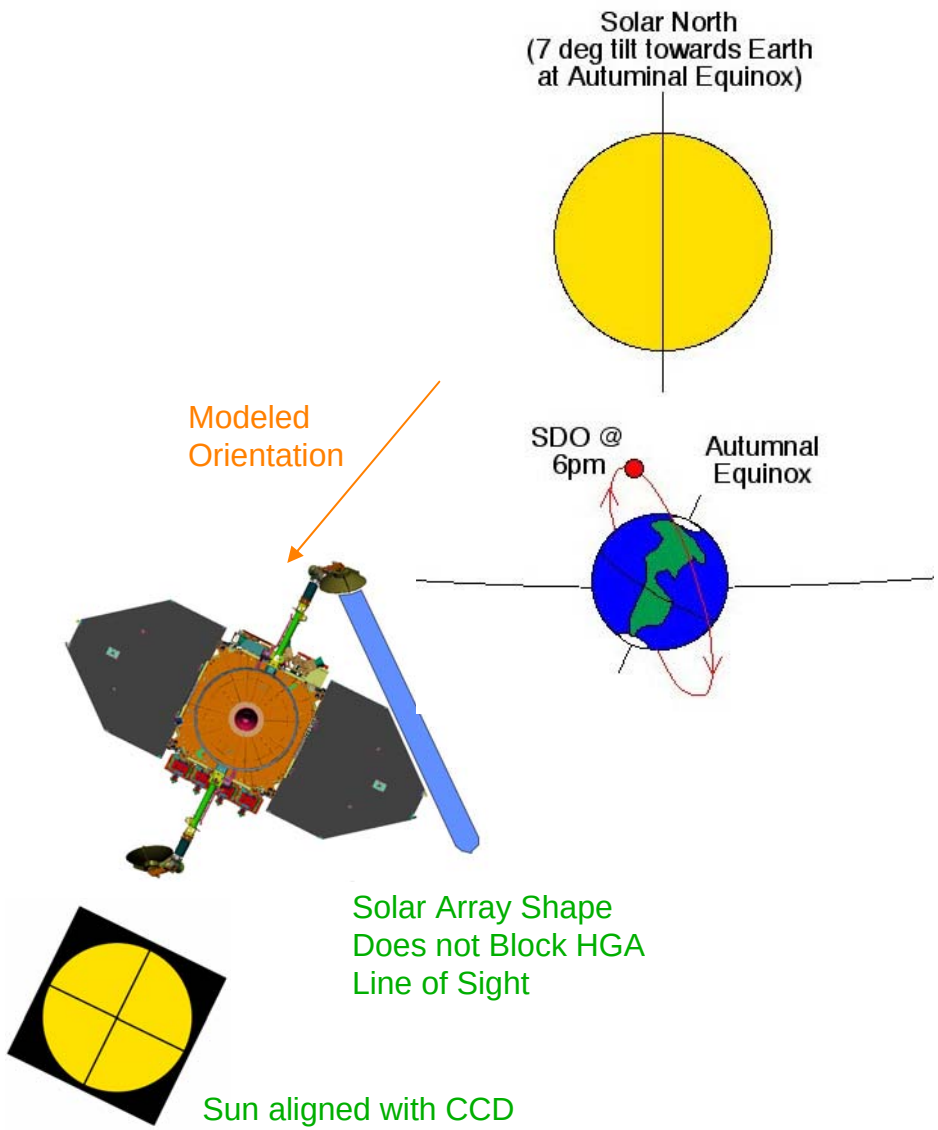
- SDO carries a suite of solar observation instruments to monitor and downlink continuous, real time science data of the sun and distributes it to Instrument analysis sites
- 6 high resolution 4Kx4K pixel cameras taking pictures every 4 seconds
- Geosynchronous orbit to allow continuous downlink line-of-sight to dedicated ground station for continuous downlink capability
- Ka-band Science downlink required to meet 150 Mbps science downlink data rate
- 5.25 year Mission Life
- Propellant provided for 10 year operational life, 5 year design life



Approximate characteristics:
- Mass: 3200 kg
- Width: 2.25 m
- Height: 5.25 m

Satellite High Gain Antenna Pointing

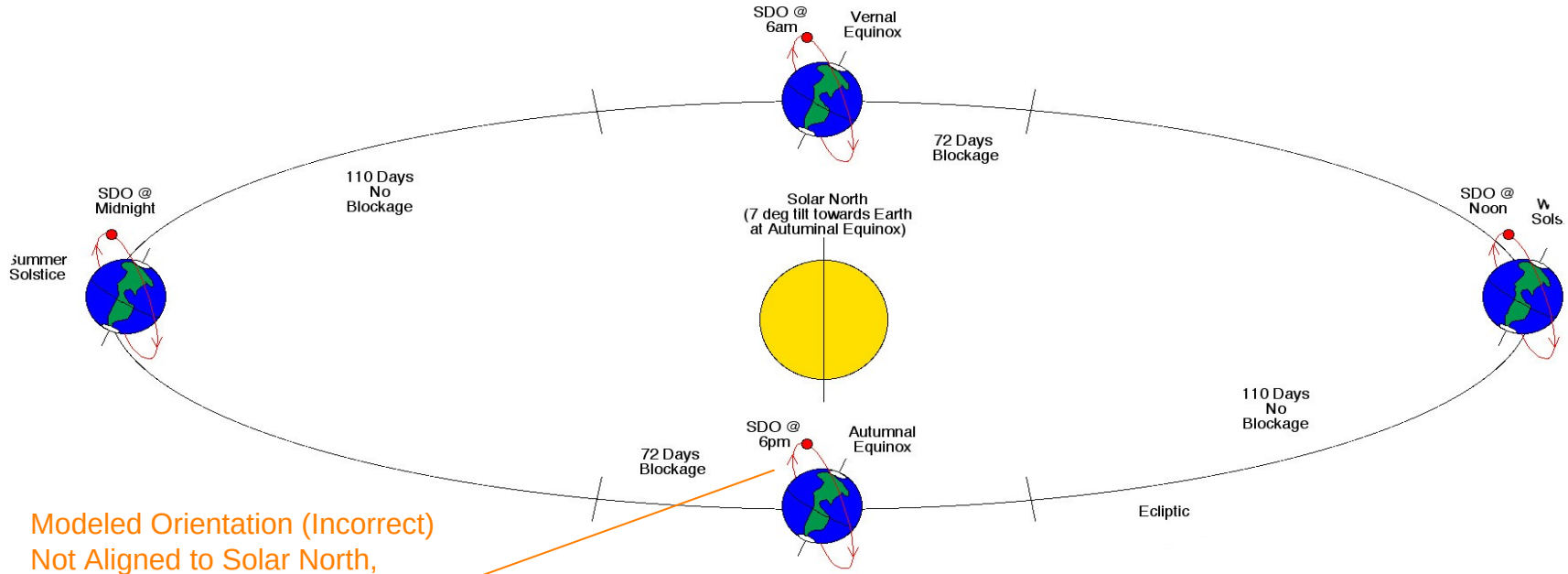
- Camera CCDs vertical axis required to be aligned with Sun's poles
- During S/C Phase A and B System Design a 3D modeling tool was used to identify where the Solar Arrays might block the HGA field of view
- Results of the modeling indicate that shaping the Solar Arrays like a "home plate" provides clearance for the High Gain Antenna Beams.



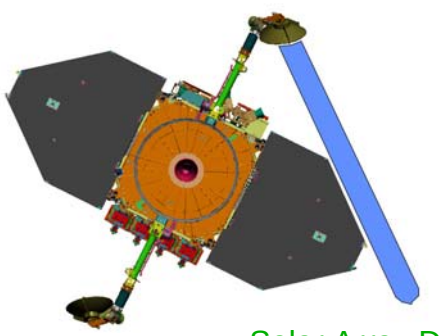
When You Least Expect it …

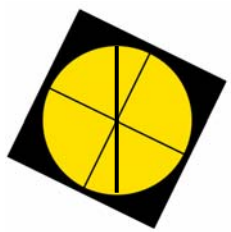
- 6 months after Project CDR,
  - All sub contracts have been in place
  - Flight Hardware fabrication and Flight Software Coding are underway
- Flight Software Testers see discrepancies in vectors describing Solar North
- HGA field of view and mechanical blockage analysis performed 2 years earlier with a 3D modeling tool aligned S/C Z-axis with the vector identified as “Solar Celestial North”
  - This variable was believed to correspond with the Sun’s north pole. It does not. It is parallel with Earth’s celestial North Pole
  - The result is the orientation of the CCD in the FOV studies is off by as much as 26 degrees about S/C roll (X-axis) during the equinoxes
- Correcting this error by realigning the S/C Z axis with Solar North results in the solar arrays and spacecraft interfering with each HGAS once a day
- As a result, preserving the original operations concept of using one HGAS for a period of six months, then switching to the other (or doing an 180 flip in the event of a HGAS failure) will result in up to two hours of lost science data each day during occultation season due to blockage of the required antenna beams

3D Configuration and Modeling Challenge



Modeled Orientation (Incorrect)
Not Aligned to Solar North,
Aligned to Earth North

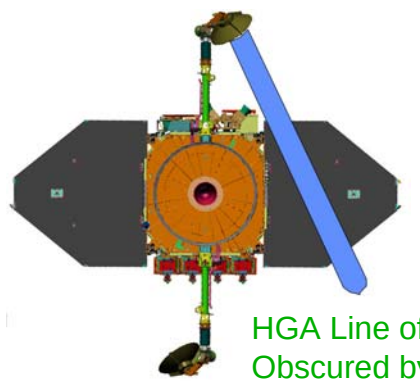


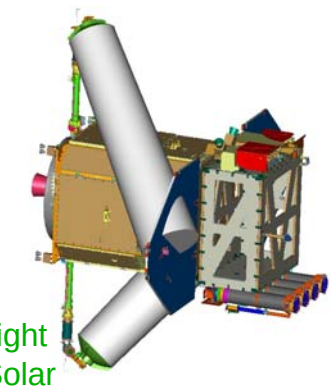


Sun's North Pole not aligned with CCD

Solar Array Does not Block HGA Line of Sight

Desired Solar North Orientation Results in Blockage





HGA Line of Sight Obscured by Solar Array With Properly Oriented S/C

HGA Blockage Alternates Considered

Scenarios		Performance	Ka-Band System Reliability Prediction	$ At Risk[1]	Operating time per year (Each Xmtr)	Transmitter Cycling (Cycles per year for Each Xmtr)	RF Switch Cycles (per yr for each RF Switch)	Cost
Baseline	Switch Transmitters and HGA every 6 months,	Does not meet Science Requirement	0.9975	0.31M	182	2	0	0
0	Do nothing Lose Science Data, Change Requirement	Does not meet Science Requirement	Like Baseline					0
1.1	Handover, Both Xmtr On, Hotter Temperature	Meets Req	0.9648	4.47M	255 24-hr days	2	0	Low
1.1a	Handover, Both Xmtr On, Cool Temperature	Meets Req	0.9820	2.3M	255 24-hr days	2	0	Low
1.2	Handover, Cycle Xmtr	Meets Req	0.9971	0.36M	182 24-hr days	145	0	Low
1.3	**Handover, One Xmtr On, Split Power to both HGA**	Meets Req, Utilize Link Margin	**0.9996**	**0.04M**	**365**	**0**	**0**	**Medium**
1.4	Handover, Throw RF Switch	Meets Req	0.9871	1.62M	365	145	145	Low
2	Fly with Discrete Roll Offsets, Change Operations Concept	Degradation, Meets Min Req	Like Baseline					Low
3	Change Orbit and Operations Concept	Additional Eclipses and Loss of Data	Like Baseline					Low
4	Change Design, Location of Array and HGA	Meets Req	Like Baseline					High

Selected

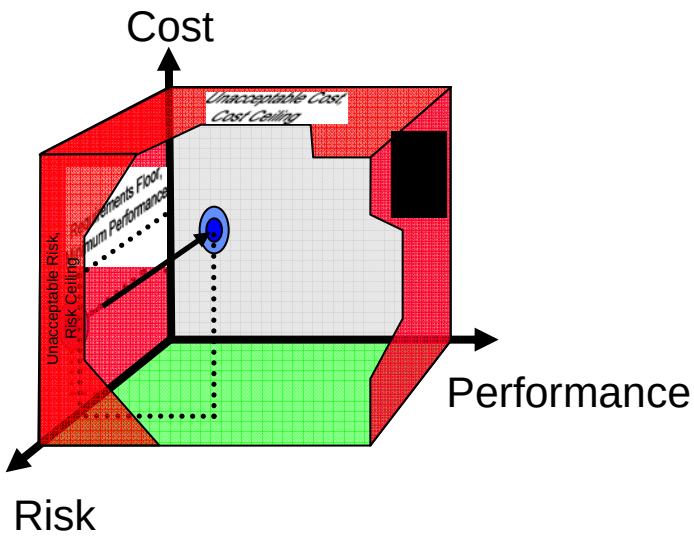
1. $ at Risk = $P_{failure}$ X Average Mission Value, (Average = Mission Value / 2)

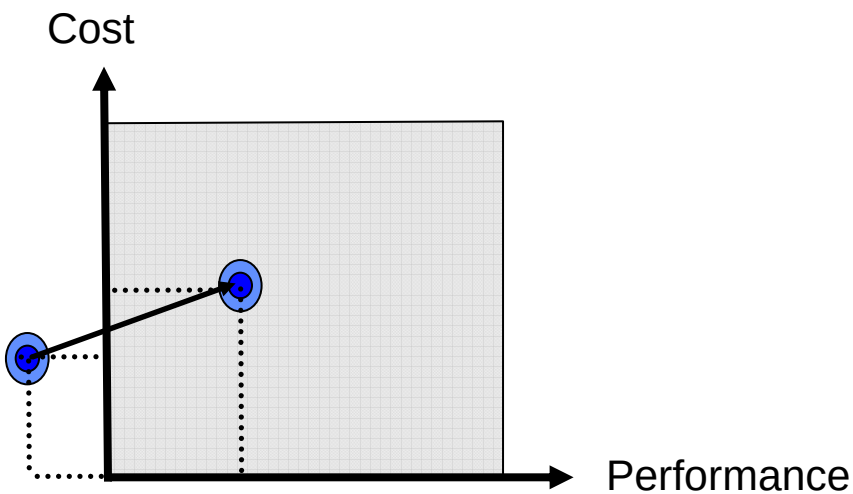
HGA Blockage Selected Solution

- Fly Spacecraft with CCD oriented as intended
- Utilize HGA Handovers to avoid blockage
- Change Some Requirements, Design and Operations Concept :
  - Requirements: Allow < 2min data loss during twice daily handovers
  - Design:
    - Remove RF switch and add a power splitter to route transmitter power to both HGAs
    - Select different polarizations for two HGAs
    - Flight Software to perform handover and unused antenna park
    - Ground system to receive and combine data from both polarizations
  - Operations Concept: Twice Daily Handovers
- Not the cheapest, but balanced the Requirements Importance and Risk versus Cost

SDO Lesson Affirmed

- Having the right modeling tool set up, assumptions, and variable initialization are critical to getting the right output
- When solving problems Requirements, Design, or Operations Concept alternatives should be considered as trade candidates
  - Requirements are not Inviolate, neither are the design and operations concept
  - Do not be afraid to ask, “Is this the Right Requirement”
- Having a clear understanding of project constraints (technical, cost, schedule, and risk) is critical to effective trade evaluation criteria
- Maintain and Utilize Margin to Maneuver inside the Box





As A Learning Organization

- Systems Engineers as a community need to act in a manner consistent with a Learning Organization if they do not desire to repeat mistakes of the past
- What does this mean:
  - Seek what was done in the past, how it was done, why it was done
  - Distill the best principles, proven processes and practices
    - NASA Systems Engineering Handbook SP6105
    - NASA Systems Engineering Process for Programs and Projects JSC49040
    - NASA Mission Design Process, EMC 1992
  - Apply the principles, processes and practices to the problem at hand
  - Be able to explain Why what you are doing, Why your solution is the right one
  - Honestly evaluate the goodness of your Systems Engineering

Iterative Systems Engineering Techniques Balance Performance, Cost, Schedule, and Risk