Iterative Risk Driven Design Approach for CEV Avionics

Smart Buyer Team Study Results

Project Management Challenge 2008

Daytona Beach, Florida

February 26 - 27, 2008

Michael Bay
Chief Engineer, BEI
NESC Avionics Technical Discipline Team

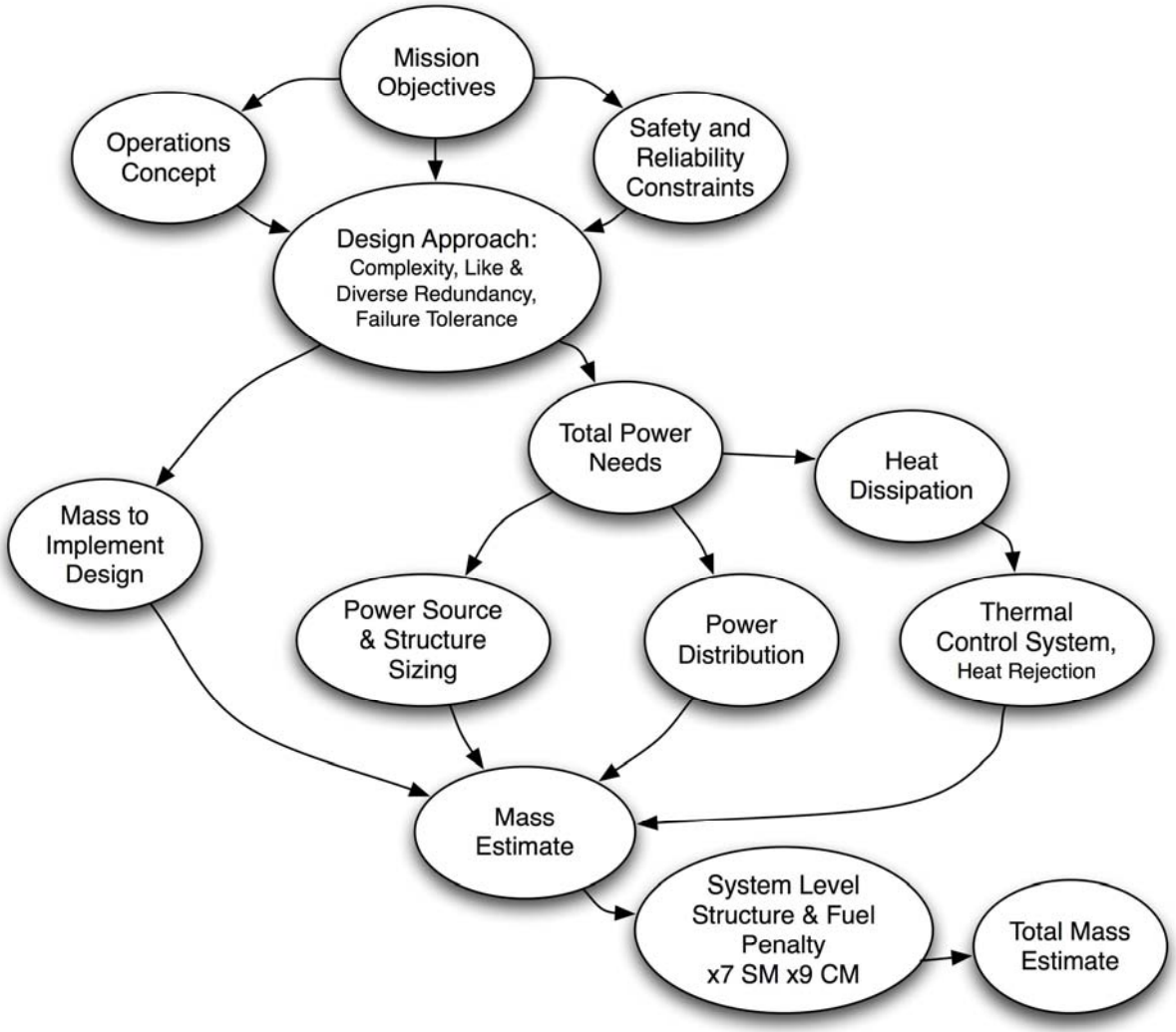
michael.bay@bayengineering.org
410-804-5111

Task Objective

- An agency-wide team lead by the NESC participated in a study chartered to assess driving requirements and consider alternative designs for the CEV.
- One of the tasks involved a study of the Avionics configuration for the CEV with the express purpose of identifying reliability and mass drivers and how the avionics configuration effects vehicle mass.
- Started with Design Analysis Cycle 1 and the requirements.
  - NESC team needed to decompose the minimum set of functions necessary to safely perform the mission
  - Linked mission objectives captured in the requirements (CARD) to functions and then link the functions to the block diagram implementation
- Tenet was “Safe” and “Simple”

Challenge - Control Mass

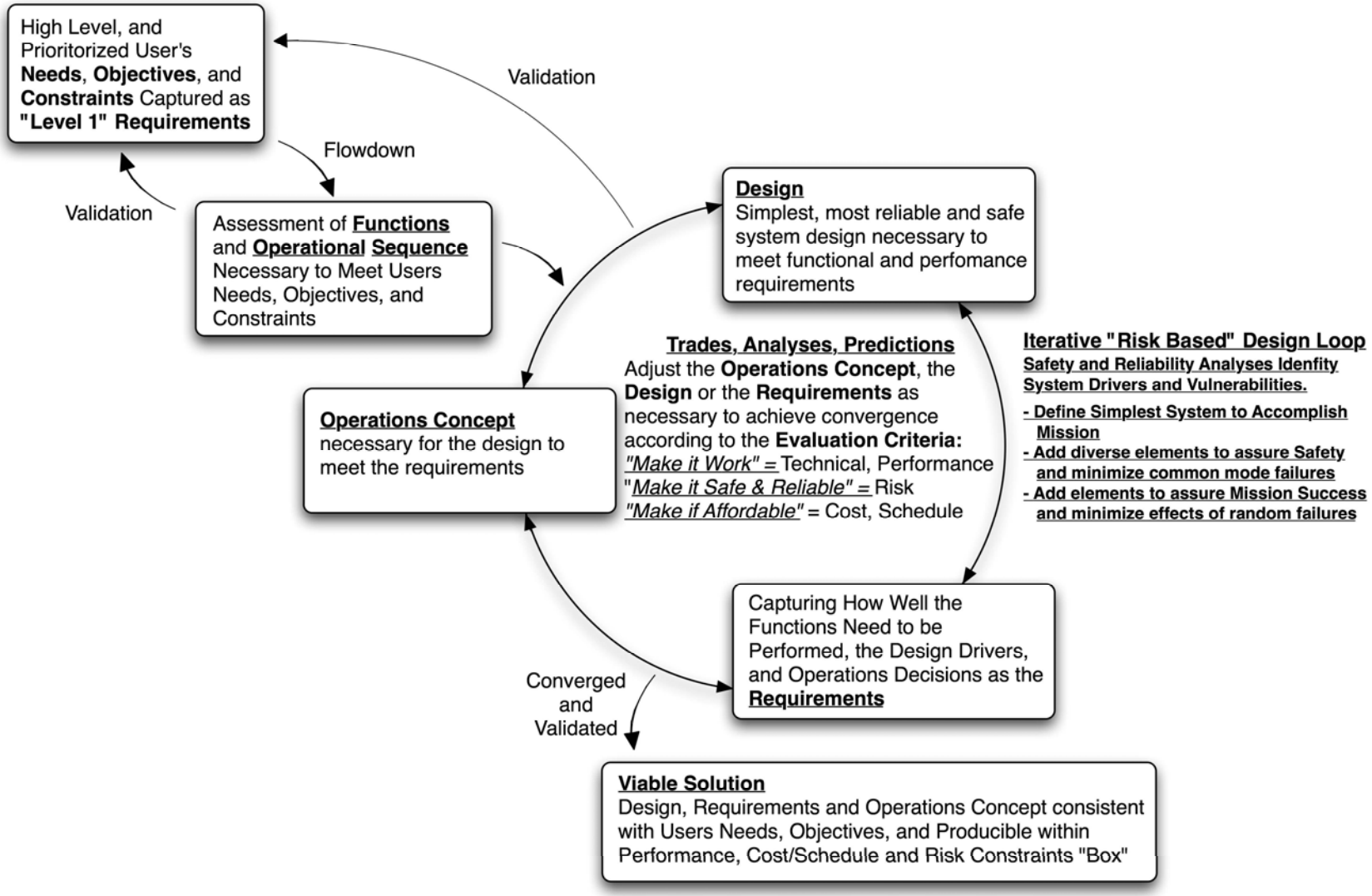
- **Power has a multiplicative effect on mass**
- **The configuration and complexity of electrical elements determines power needs**
- **There is significant "overhead" for every watt**
- **Allocation of scarce resources must consider the importance of the function they are supporting**



Prescriptions and Rules

- There is no a priori prescription for the design of a safe human rated system.
- No single process or single rule such as two failure tolerance will by itself assure safety and mission success.
- Hazards exist in context of a design and a unique operational sequence and which must be explored for each mission
- When considering safety as the absence of uncontrolled hazards, we realize that we can not write enough rules and requirements to preclude hazards and prevent latent defects.
  - We can not prove this "negative", i.e. that all hazards are controlled, or that there are no latent defects.
- Success is grounded in providing sufficient capabilities for “safe crew return” should system elements fail.
  - Teams seek a predictable design and then explore system weaknesses, risks, hazards, etc, in context of the specific operational sequence along with the natural and induced environments.

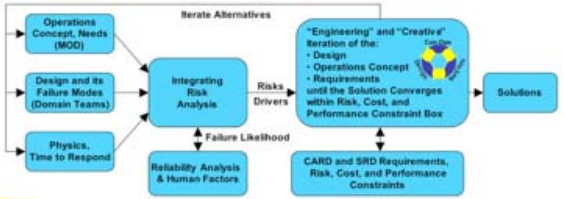
Overall Systems Engineering Approach



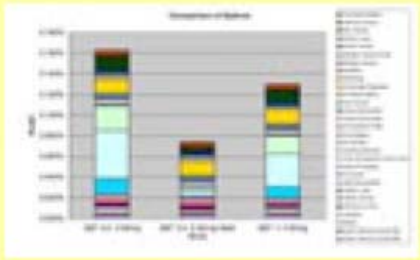
Broad Electrical Systems View Integrated with Safety and Mission Success Risk Assessments

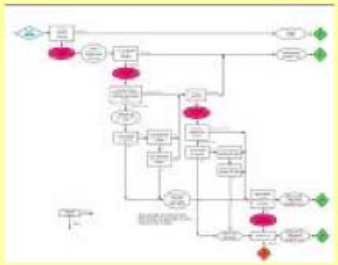
Integrated Electrical System
- "System View" of entire electronics
- Efficient and Upgradeable Avionics Interfaces
- Appropriate Selection of Redundancy
- Flexible Telemetry and Onboard Monitoring
- Efficient Power Distribution System

Continuous Cyclic Evaluation
- System Architecture Reliability trade
- Requirement vs. Operation Concept trade
- Electrical Design implementation trade

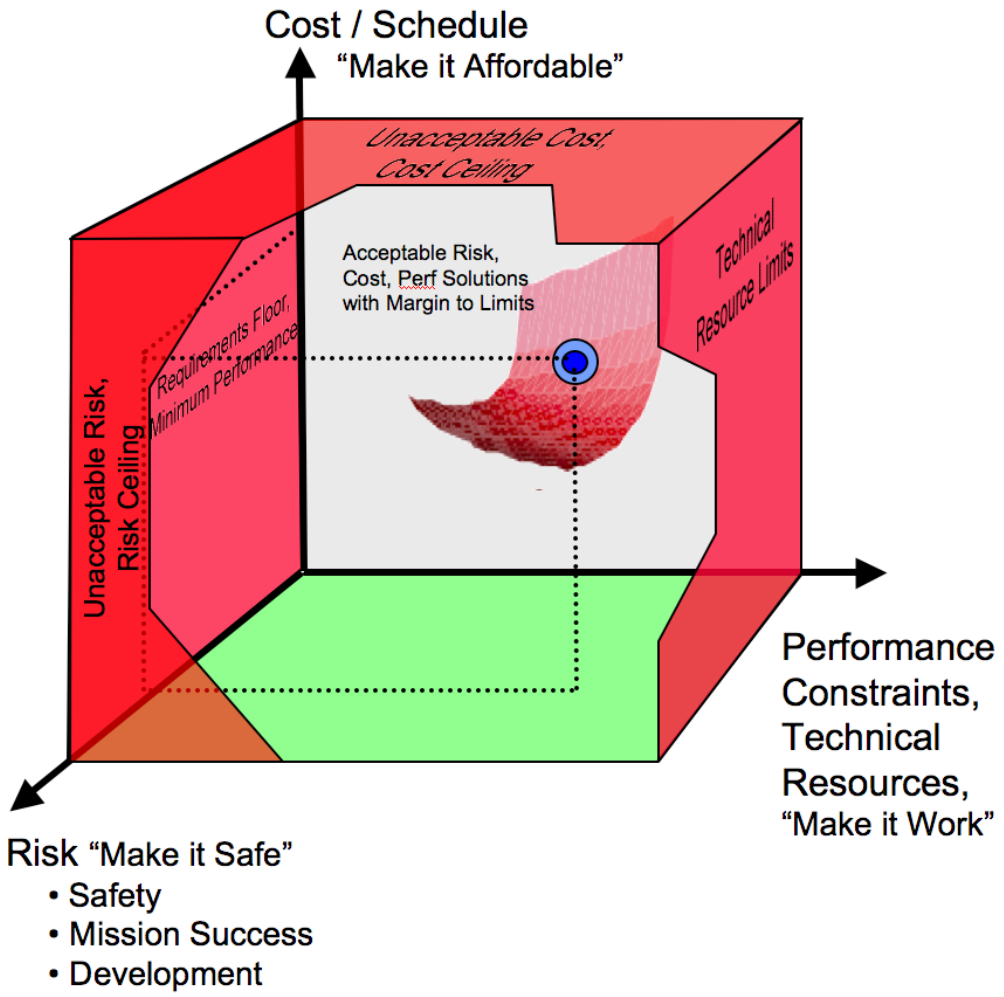


Integrated Reliability Analysis
- Event Sequence Diagrams
- Mission Ops & Off-Nominal Evaluation
- Fault Detection & Response Time
- Alternative Architecture Evaluation





Evaluating Effectiveness, Staying "In the Box"
Performance, Risk, Costs



- **Start by defining "the box" boundaries**
- **Define a minimum system that attempts to meet risk, performance and cost**
  - **Starting with 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 to address risk drivers**
- **Iterate design, operations concept, and requirements**
  - **Allow the "Is this the right requirement?" question**
- **Resist requirements "creep" and expansion**
- **Add complexity only where necessary for Safety and Mission Success**

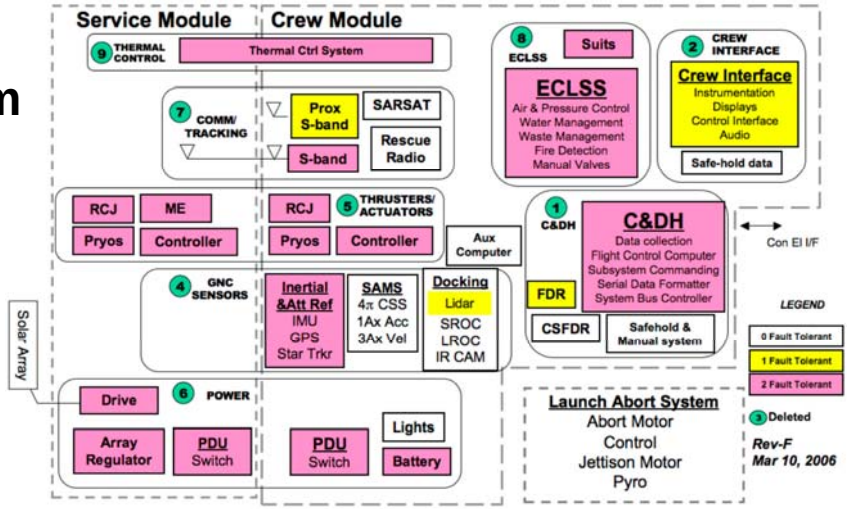
Managing Complexity

- Spaceflight is a highly integrated activity that operates on the boundaries of technological abilities and requires the sequential success of a large number of active subsystems all of which are operating close to their limits.
- Complexity can impede the designer's understanding of how system elements couple and interact with each other and with natural and induced environments
  - Interaction of the system with various planned and unplanned operational scenarios
  - Interaction with nominal and off nominal environmental extremes
  - As systems become more complex they become less predictable, hence their safety and reliability becomes less certain
- Manage Complexity to Achieve Safety and Reliability
  - Complexity should be limited to what is needed to accomplish the mission objective
  - Designers need to consider the ultimate effects of complexity on system safety and reliability
- Managing and Integrating Pieces into a Cohesive Whole
  - Common method for managing large and complex systems is to divide the whole into smaller, simpler "manageable" pieces
  - Challenge becomes the process of reintegrating the pieces into a cohesive system while avoiding adverse couplings and interactions that may affect safety and reliability

- **Complexity is often the Antithesis of Safety and Reliability**
  - Keep Mission Objectives as simple and clear as possible. Allows solid validation basis for subsequent design activities
  - Restrain the proliferation of requirements until their "consequence" and "cost" are known

Identifying Critical Functions

- **Identify functions necessary to assure crew safety and functions necessary for mission success**
- **Understand how system level fault tolerance drives individual Avionics functions**
- **Allocate high level functions to subsystem areas consistent with risk strategy**
- **Iterate placement of functions within subsystem areas as necessary to improve safety and reduce risk**
- **Assignment of critical functions to a product and responsible person / team**



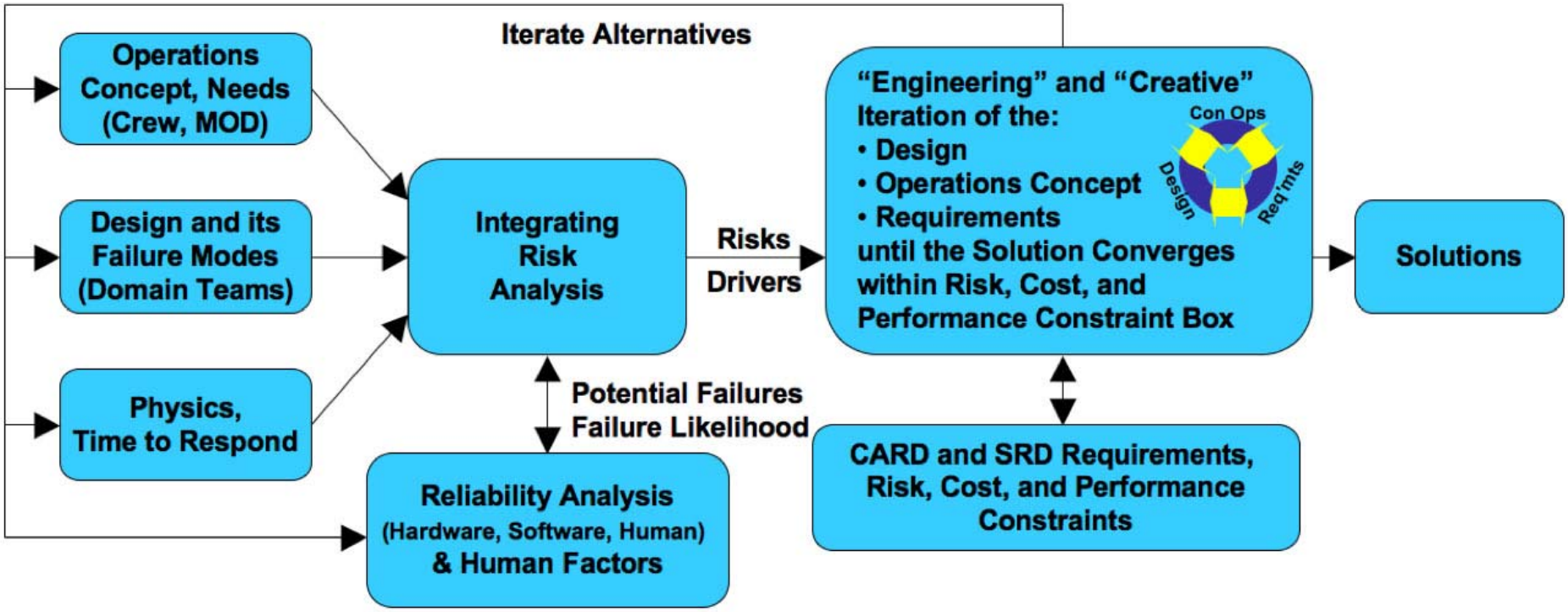
Safety Critical Functions are shown in Red, Mission Critical in Yellow, and noncritical in White

Design Iterations Based on Risk

- The approach started with the simplest design to "make it work" meaning accomplish the mission objectives with inherent safety[1]
- Add diverse and lower performance strings to ensure safe return of the crew, "make it safe"[1]
- Add additional strings necessary to "make it reliable"[1] meeting mission objectives
- Assure the system is "affordable" from both technical resource and programmatic perspectives
- An "Integrating Risk Analysis" was used to assess the operational scenario, the design of the system along with its failure modes, and the physics of the situation to identify the risk drivers
  - Safety and reliability analyses were used to estimate the relative advantage of one configuration over another.
- Alternate designs, operations concepts, or requirements were investigated when the system did not meet constraints or high level driving requirements.
- These steps can't be done in isolation and need to be assessed together. However there is a Hierarchical ordering
  - While Safety is paramount,
  - Safety is moot if the system doesn't perform its function
  - Affordability is moot if the system is not safe

[1] "Build up" approach provides rationale for each string of failure tolerance

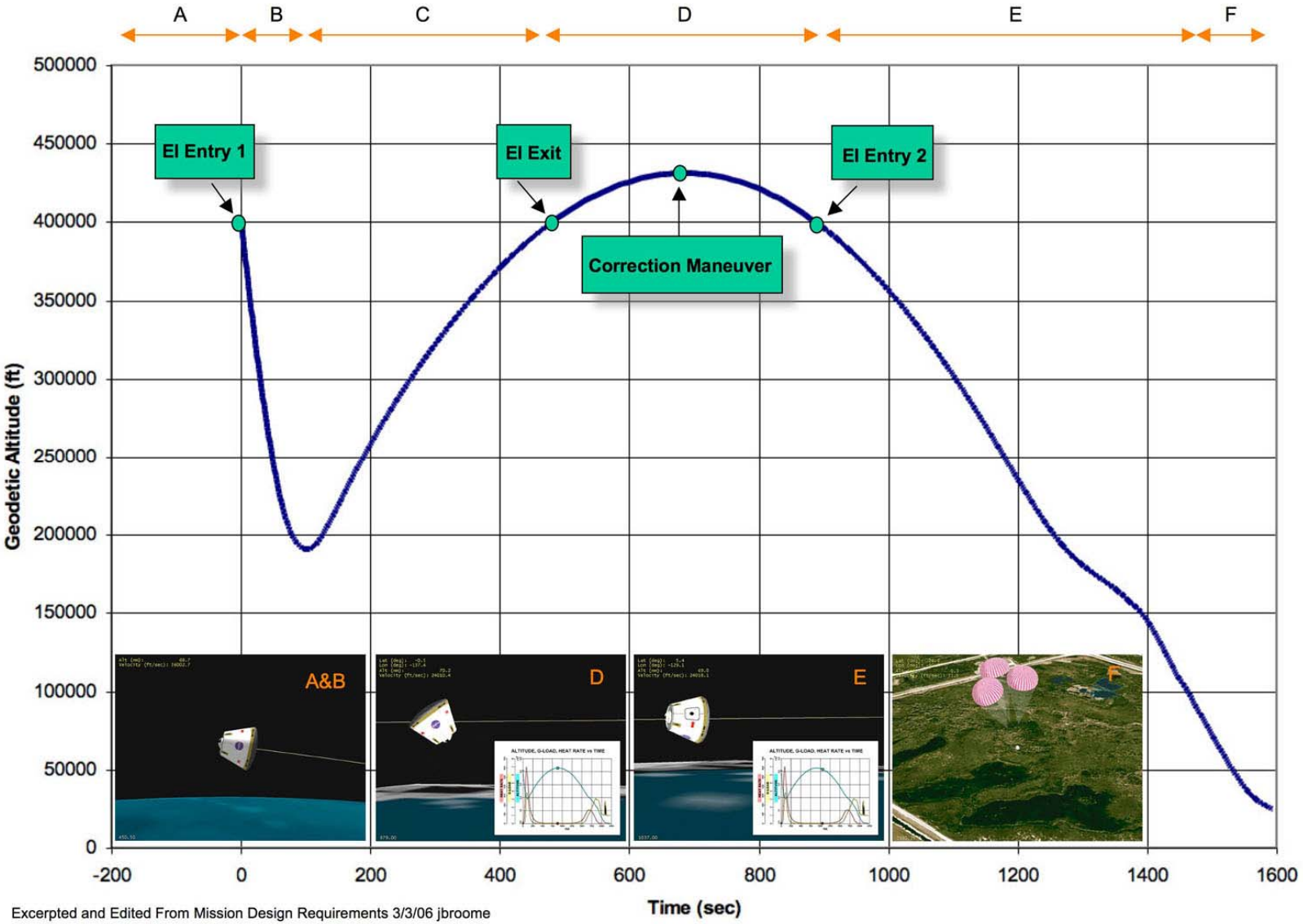
Integrating Risk Analysis Flow Chart



- **The team used Event Sequence Diagrams to evaluate the operations concept, the failure modes inherent in the design, and the physics / time required to respond, along with reliability modeling to identify the drivers for the avionics architecture**
- **Team iterated the total System Design, Operations Concept, and Requirements to meet project Performance, Cost, and Risk Constraints**
- **Mission Phases Configurations / Solutions Studied:**

Entry
Launch
Uncrewed Lunar Loiter
Critical Maneuver

Example: Skip Entry Profile Split into “Phases”



Excerpted and Edited From Mission Design Requirements 3/3/06 jbroome

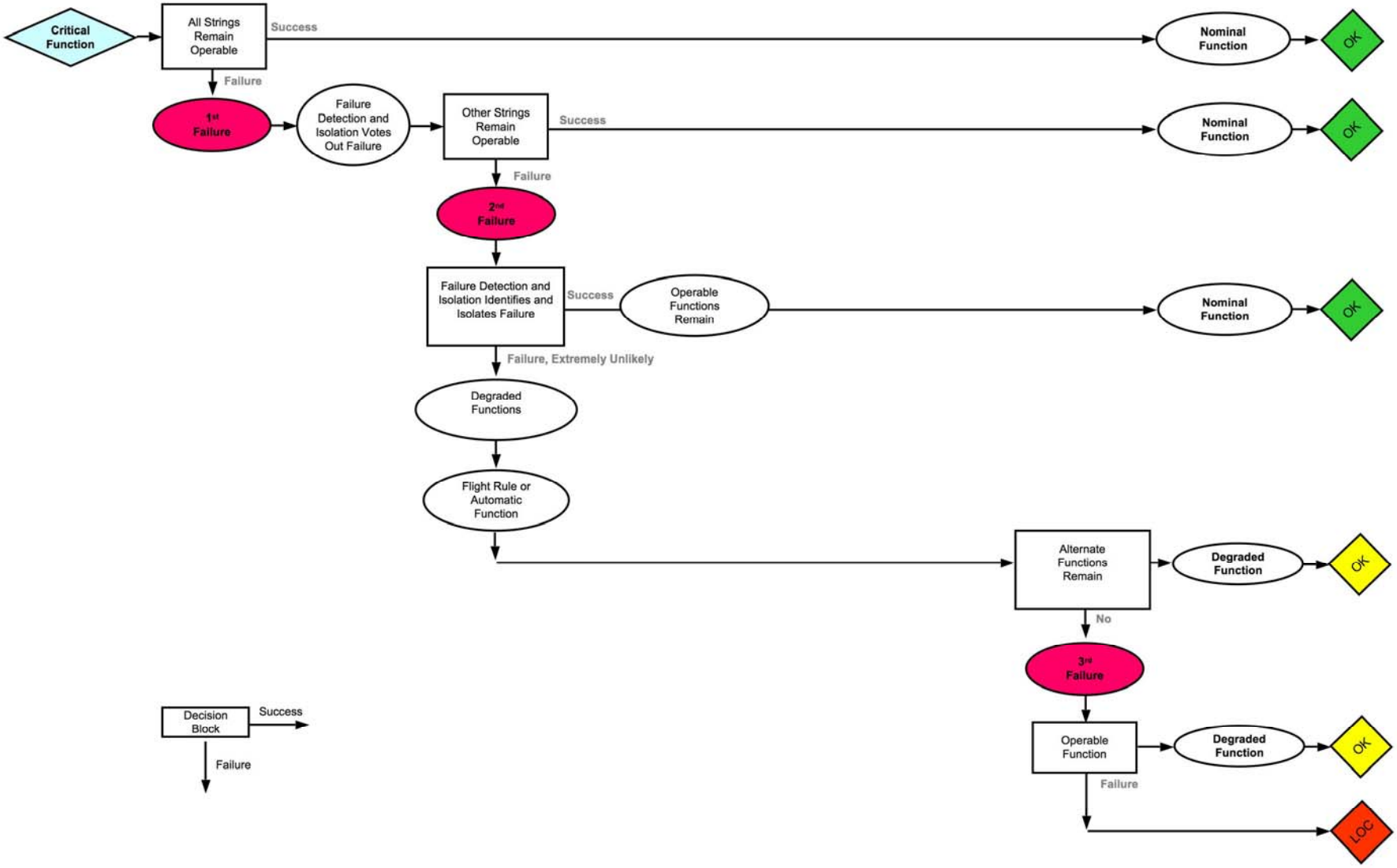
Entry Phases Assessment of Backup Modes

- **Transitions to Backup Modes during Entry Phases**
  - **Ability to transition from Guided Entry to Manual and Ballistic Backup Modes**
  - **Consequence of entering Manual and Ballistic Modes**

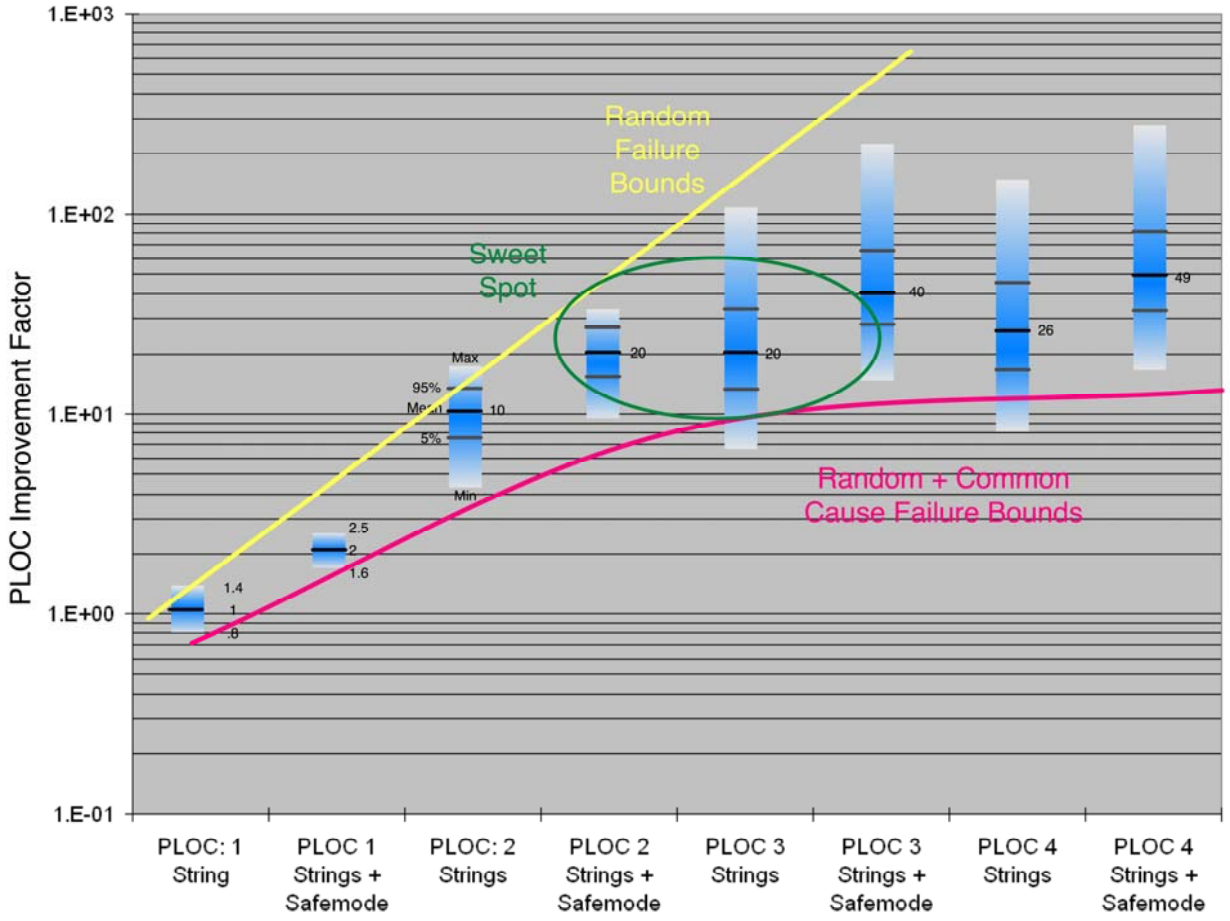
Entry Phase	Characteristic	Time to Isolate Failure	Landing Dispersion of Manual Mode	Consequence of "No Control" Ballistic Entry	Landing Dispersion of Ballistic Entry
A Entry Targeting	Set Entry Attitude, Rates, Nav State.	Minutes to set Entry 1 Attitude	Many 1000s nm	Survivable, High G loads (~ 12 g's), Need acceptable entry attitude	Many 1000s nm
B Entry 1	Major Range and Bearing Adjustment, Energy Management, Control Bank Angle	Seconds, Vehicle stable	Many 1000s nm	Survivable, High G loads. Becomes an entry to surface.	Many 1000s nm
C Skip Exit	Control Bank Angle, Lift Vector	Seconds, Vehicle stable	100s -1000s nm	High G Loads after 2nd entry, Need control to set up for Entry	1000s nm
D Exoatmospheric Coast and Adjust	Skip Dispersion Control, Maneuver Not Crew Critical, Medium Range and Bearing Adjustment, Set Attitude +/- 45 degrees and rate +/- 1 deg/sec to second entry	Minutes to set Entry 2 Attitude	0-100s nm	High G Loads, Need control to set up for Entry, Set Attitude +/- 45 degrees and rate +/- 1 deg/sec to second entry	100s -1000s nm
E Entry 2	Final Entry, analogous to "Direct Entry". Set Entry Attitude, Rates, Nav State.	Seconds, Vehicle stable	0-10s nm	Survivable, High G Loads (~9 g's)	100s -1000s nm
F Chute	Chute	No Issue	None, Not Applicable	None, Not Applicable	None, Not Applicable

Integrating Risk Analysis

Example Event Sequence Diagram



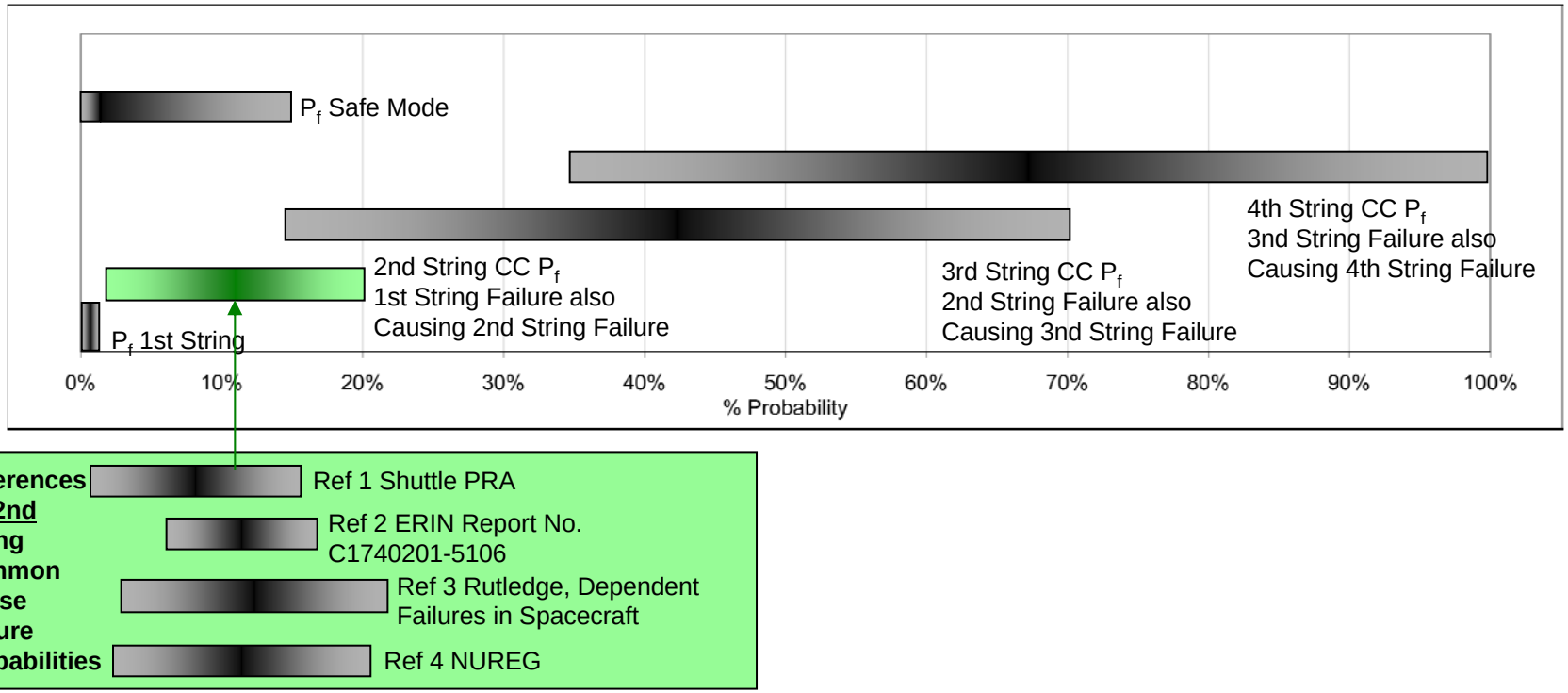
Consideration of “Generic” and other Common Cause Failure Modes



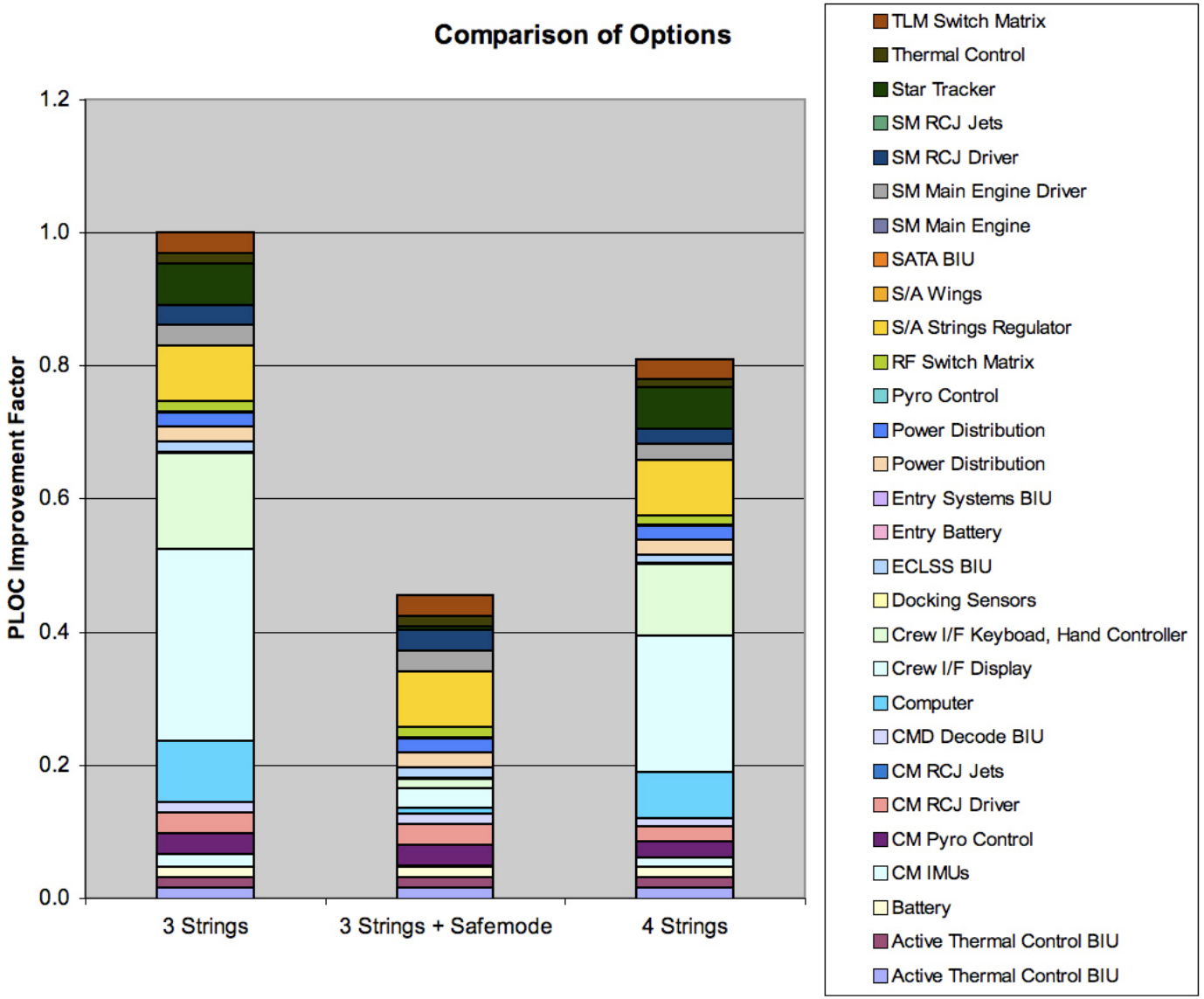
Limited reliability improvement above the sweet spot due to common cause failure effects

Considering Common Cause Failures

- **Common Cause Failure Probability for 2nd Failure is traceable to published data, see below**
- **Engineering judgment leads the team to prefer a diverse Safe Mode as opposed to a 4th copy of what has already suffered 2 failures**



Comparison of Failure Contributors

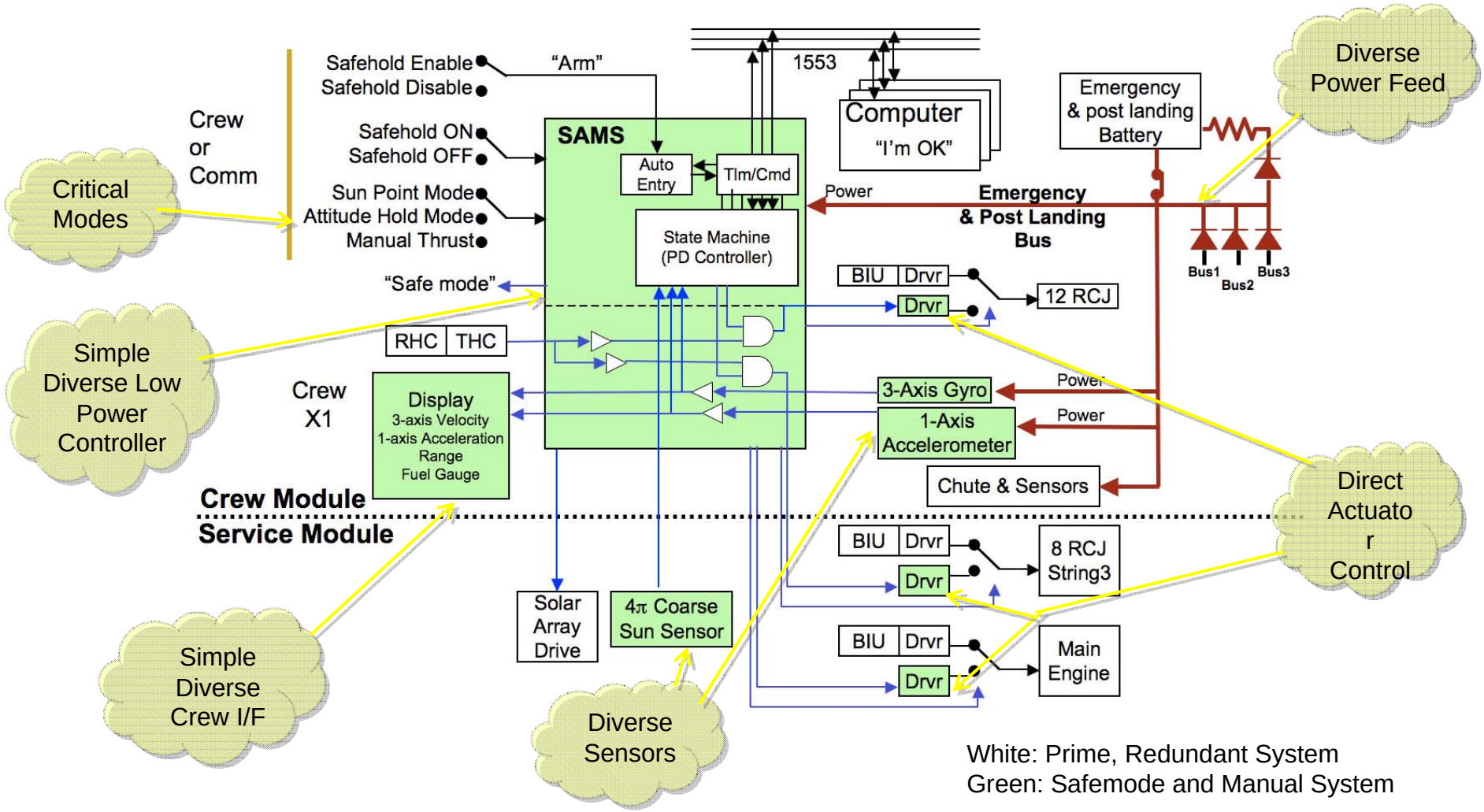


- **4th String "compresses" likelihood of all failure sources but is limited by a common cause factor**
- **A dissimilar Safemode dramatically reduces likelihood of system failure because of a minimal common cause factor**

System Risk Drives the Design Solution

- **Entry Drives:**
  - **3 Strings (2 necessary, 3rd to vote failures) Plus Manual Safe Mode**
  - **CM Jet Fault Tolerance / Redundancy**
- **Un-crewed Lunar Loiter Drives:**
  - **3 Strings (2 necessary, 3rd to vote failures) Plus Sun Pointing and Attitude Hold Safe Mode**
- **Other On Orbit Modes Benefit from Safe Mode**
  - **Independent, Simple, Low Power, Sun Safe Attitude provides functional retreat and safe haven from Major Prime Avionics System Anomalies**
  - **Capability for Manual Attitude and Maneuver Control, low power mode using a minimal system similar to "Apollo 13"**

Application of Dissimilar or Diverse Systems



White: Prime, Redundant System
Green: Safemode and Manual System

Simple Dissimilar System
Safehold And Manual System

- **Simple robust system with two basic functions**
  - Safehold Mode – Enables stable & safe attitude, power positive state including ground communications during Uncrewed Lunar Loiter. Provides time for system diagnostics and recovery from failures(s).
  - Manual Control – Direct crew control of the Reaction Control Jets & Main Engine with simple display feedback.
- **Features**
  - Simple to ensure predictability, hence safer and more reliable
  - Minimal functionality, but sufficient for safe crew return
  - Robustness by proven technology, low parts count & thorough engineering test & analysis
  - Low power, low mass & minimal software
  - State machine or micro-controller based
  - Dissimilar design from Prime Computer and Network
- **What the Dissimilar Safemode is not:**
  - A Back-up Flight System (BFS), It is not full performance
  - A general purpose reprogrammable flight computer

Conclusion

- There are no a priori prescriptions taken by themselves that ensures a safe design
- Designers must use risk drivers to control the complexity obscuring hazards and unintentional interactions / coupling of system elements
- Build up Approach provides rationale for system design decisions based on top down risk assessments
  - Affirmative rationale for the system design, its complexity, and the existence of each system element
  - Rationale for resources Mass and Power, cost
  - Build up approach lessens the likelihood of having to lop off pieces of a design to get back “in the box.”
- Generic or Common Cause Failures must be Considered
- Severe mass constraints require the wise utilization of scare mass resources to protect safety and mission success.
- Merging of technical expertise and experience of the human spaceflight, robotic and research centers was effective in identifying alternate concepts that reduce complexity, power and mass.

Abstract: Iterative Risk Driven Design Approach for CEV Avionics, Smart Buyer Team Study Results

An agency-wide team lead by the NESC participated in a study chartered to assess driving requirements and consider alternative designs for the CEV. One of the tasks involved a study of the Avionics configuration for the CEV with the express purpose of identifying reliability and mass drivers and how the avionics configuration effects vehicle mass.

Safety and reliability analysis results provided an important input to the systems engineering approach used to evaluate the overall design. The primary design tenet was “Safe and Simple”. An integrated "electrical systems" team was assembled that included representatives and input from any vehicle subsystem that contained electrical components. The team also included members from mission design, mission operations, software and integrated vehicle health monitoring groups.

The mission timeline, vehicle configuration, and the concept of operations were used to determine the fault tolerance drivers based on the simplest set of functions necessary to accomplish mission objectives. The team started with the simplest possible design (single string in this case) necessary to accomplish the functions. With an understanding of the risk drivers, the team iterated the design and operations concepts to improve failure tolerance, redundancy and reliability based on risk. Safety and reliability analyses were used to estimate the relative advantage of one configuration over another. The approach was to "make it work" first using the simplest design with inherent safety, add diverse and maybe lower performance systems to "make it safe", add additional strings necessary to "make it reliable", and then assure the system is "affordable". Alternate designs, operations concepts, or requirements were investigated when the system did not meet constraints or high level driving requirements. This "build up" approach provided definitive rationale for every box, every watt and every pound of mass contributed by the avionics. In the end decision makers utilized the results of the study to select an optimum configuration based on risk along with knowledge of the necessary power and mass resources.