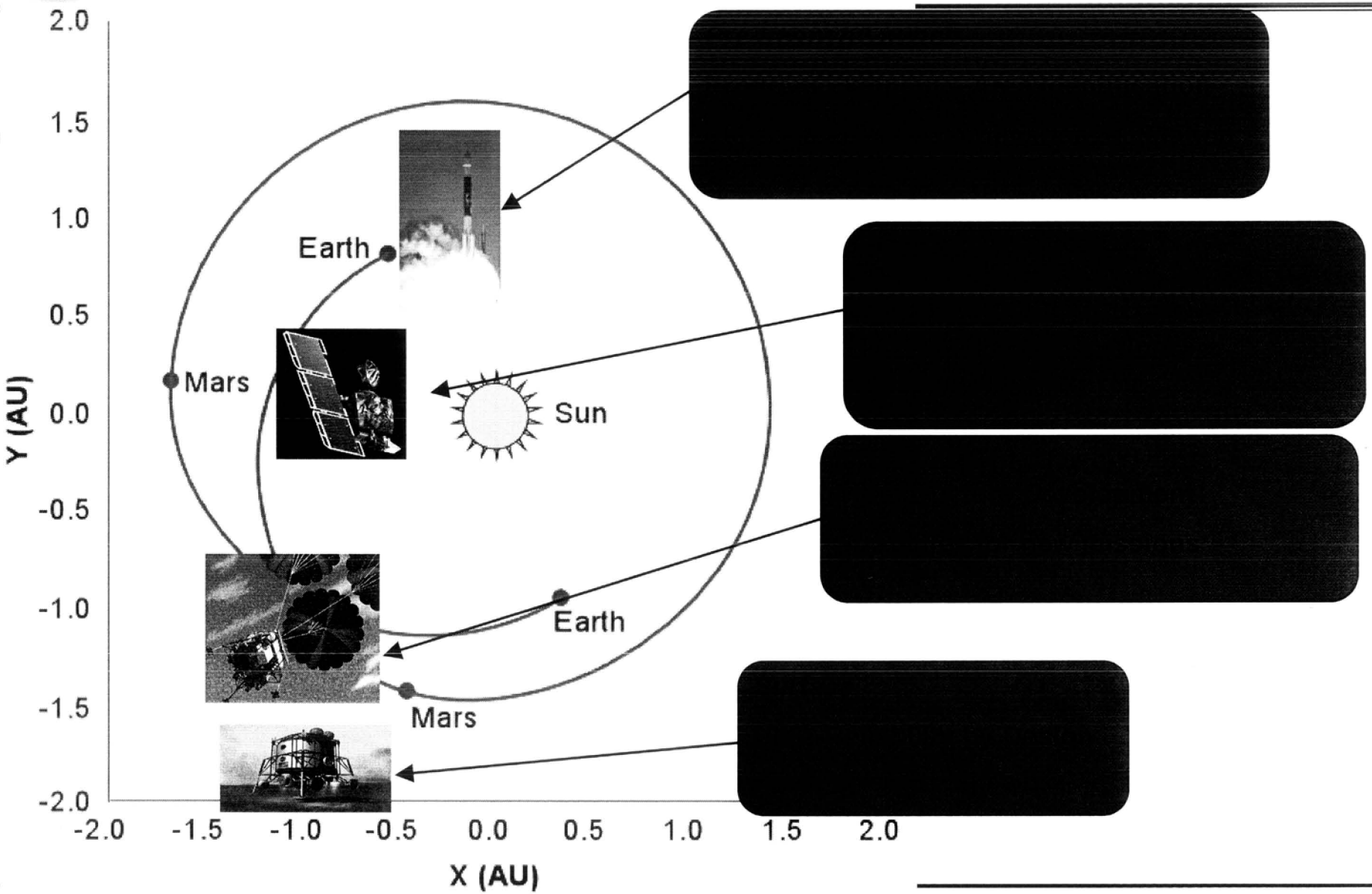
Ultra Reliability

Phil Napala – NASA Headquarters Code Q Sponsor

Charles Barnes – Assurance Technology Program Office Program Manager

Andrew Shapiro – Program Element Manager

Ultra Reliability Phases



Outline

- Objectives
- Approach
- Ultra Reliability Areas
- Plan Overview
- Work Flows
- Customers
- Summary

Global Objective

- The objective is to achieve NASA-wide reliability of one order of magnitude better than today

- Definitions
  - Ultra-reliability
    - Given a specific time frame – reliability one order of magnitude more than current standard
  - Long Life
    - Missions with a design lifetime of 20 years or more

Approach

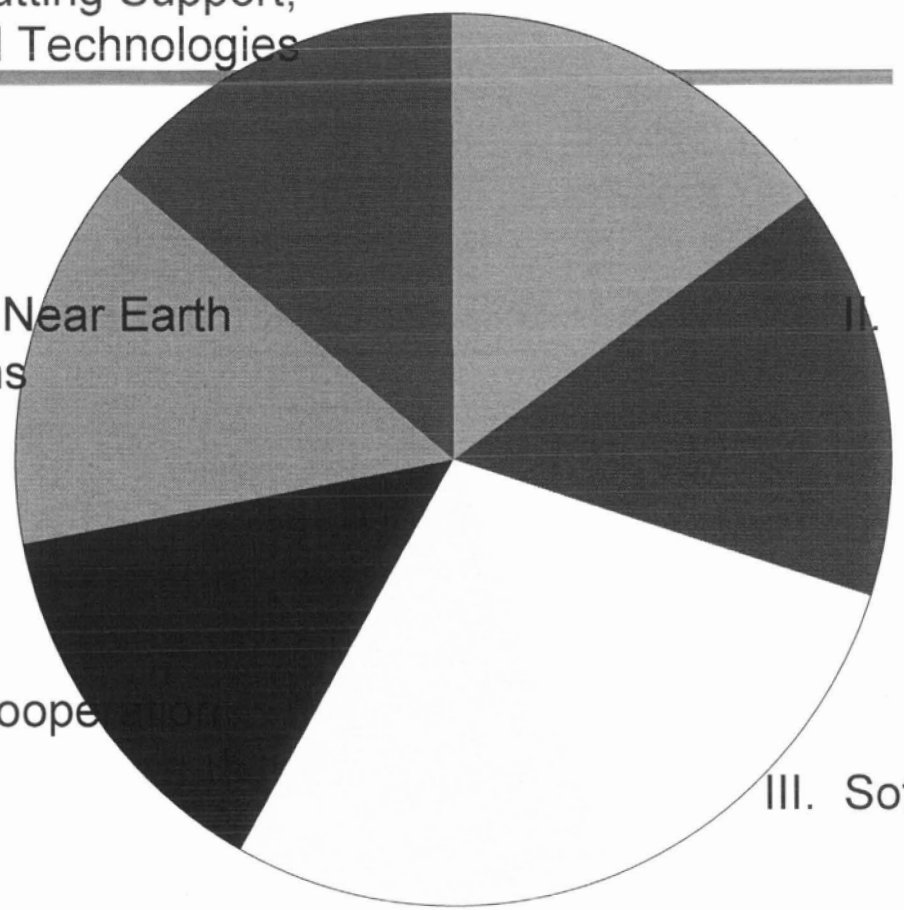
The approach for this program involves five steps:

1. Divide NASA systems into seven areas;
2. Establish areas champions and representatives from each NASA center;
3. Develop a reliability issue list for each area using a team of NASA experts in each area with the sector champion facilitating the effort;
4. Develop mitigation strategies for each of the areas' issues lists and ranking their importance by holding a workshop or with a working group of area experts from government (NASA and non-NASA), universities and industry;
5. Develop a set of tasks for each area in order of importance for improving the reliability of NASA systems.

Ultra Reliability Areas

- The particular Ultra Reliability Areas identified for the purposes of this task were based on the results of the Ultra Reliability workshop held in May of 2002
- Parsing of NASA components for Ultra Reliability is difficult
- No single parsing satisfies all work objectives
- The specific area parsing may be altered as the project progresses

Ultra Reliability Components



ECS

Engineering for Complex Systems

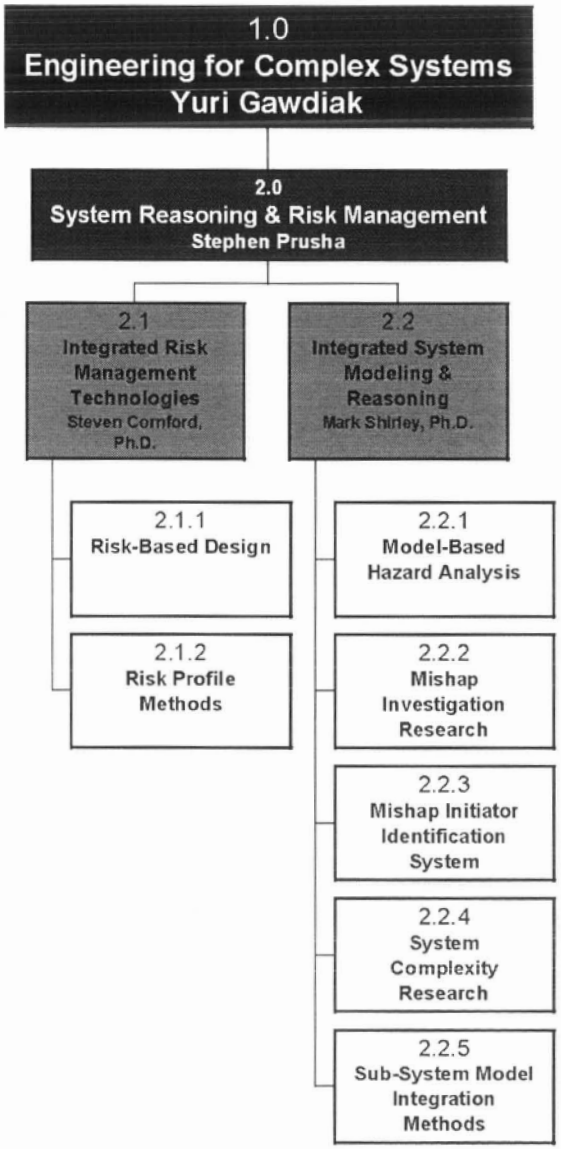
I. Engineering for Complex Systems

- Engineering for Complex Systems involves a large number of ongoing projects
- A relevant example related to the Ultra Reliability program is System Reasoning & Risk Management (SRRM)

SRRM Summary

- SRRM focuses on research and development of tools and technology to *better understand, characterize, and manage* mission and system risk.
- Addresses key risk areas identified by formulation studies
  - Design, requirements, risk/hazard analysis, anomaly resolution
  - Technology maturity/readiness
- Emphasis on formulation-phase design
  - High leverage
  - Largely unaddressed by current risk management methods
- Project structure
  - Two product classes
    - Risk Tool Suite for Advanced Design
    - Investigation Methods & Tools
  - Core research areas supporting these products
    - Model-Based Hazard Analysis
    - Complexity Research
    - Risk Characterization and Visualization
    - Risk-Based Design and Optimization

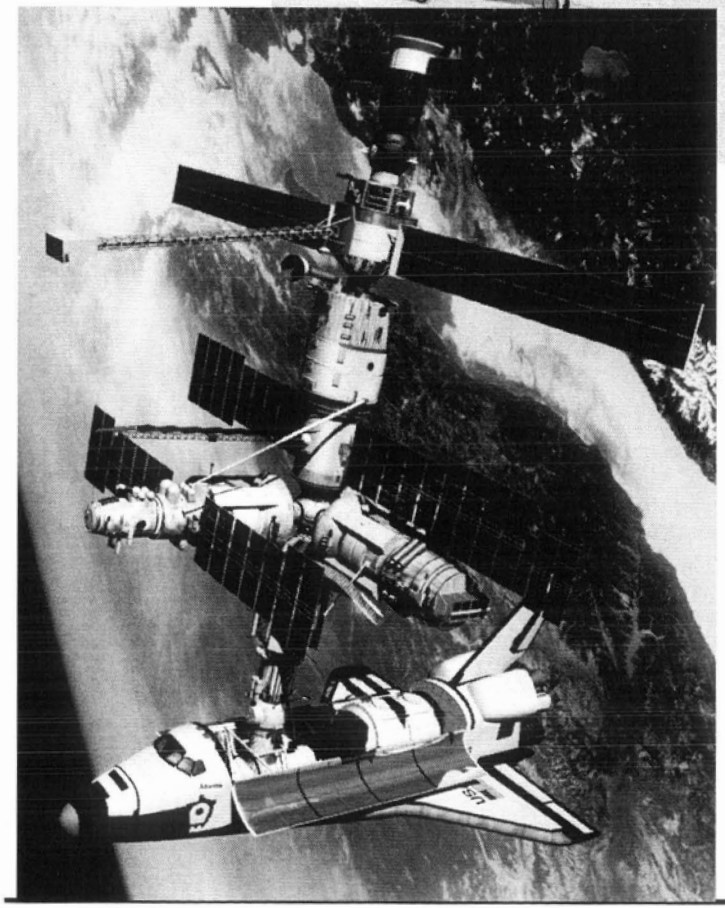
System Reasoning & Risk Management
Work Breakdown Structure

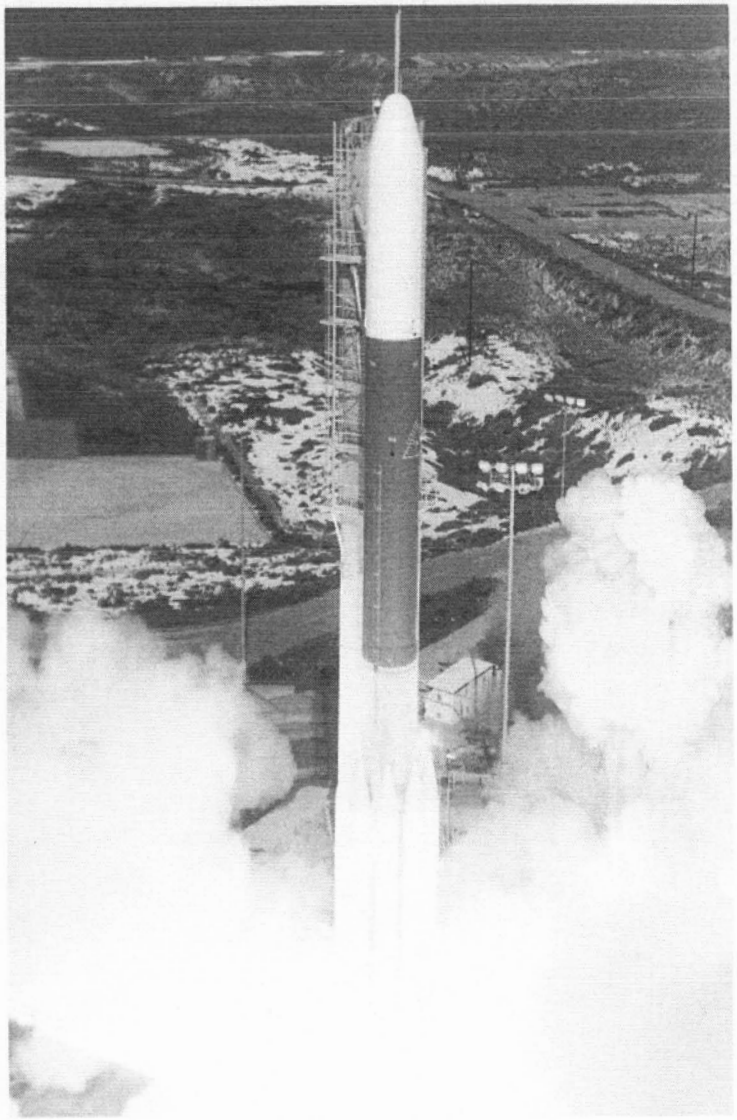


- **Integrated Risk Management Technologies** - develop integrating frameworks and architectures to apply traditional risk models, SRRM-developed models, and other technologies to improve risk assessment. This includes developing methods and tools to integrate both qualitative and quantitative information/knowledge in a normative risk management decision-making process, as well as demonstration and validation of these technologies. Initial efforts will focus on the early conceptual and formulation phase design processes.

- **Integrated System Modeling & Reasoning** - develop and mature tools that use models of system structure, behavior and function to identify hazards and assess risk. This includes understanding how system mishaps occur, with particular emphasis on the role of system complexity as a contributing factor, and on analyzing complex designs using model-based methods for identifying potential system accidents, including system-wide interactions that are more likely to be missed by subsystem design teams.

II. Hardware

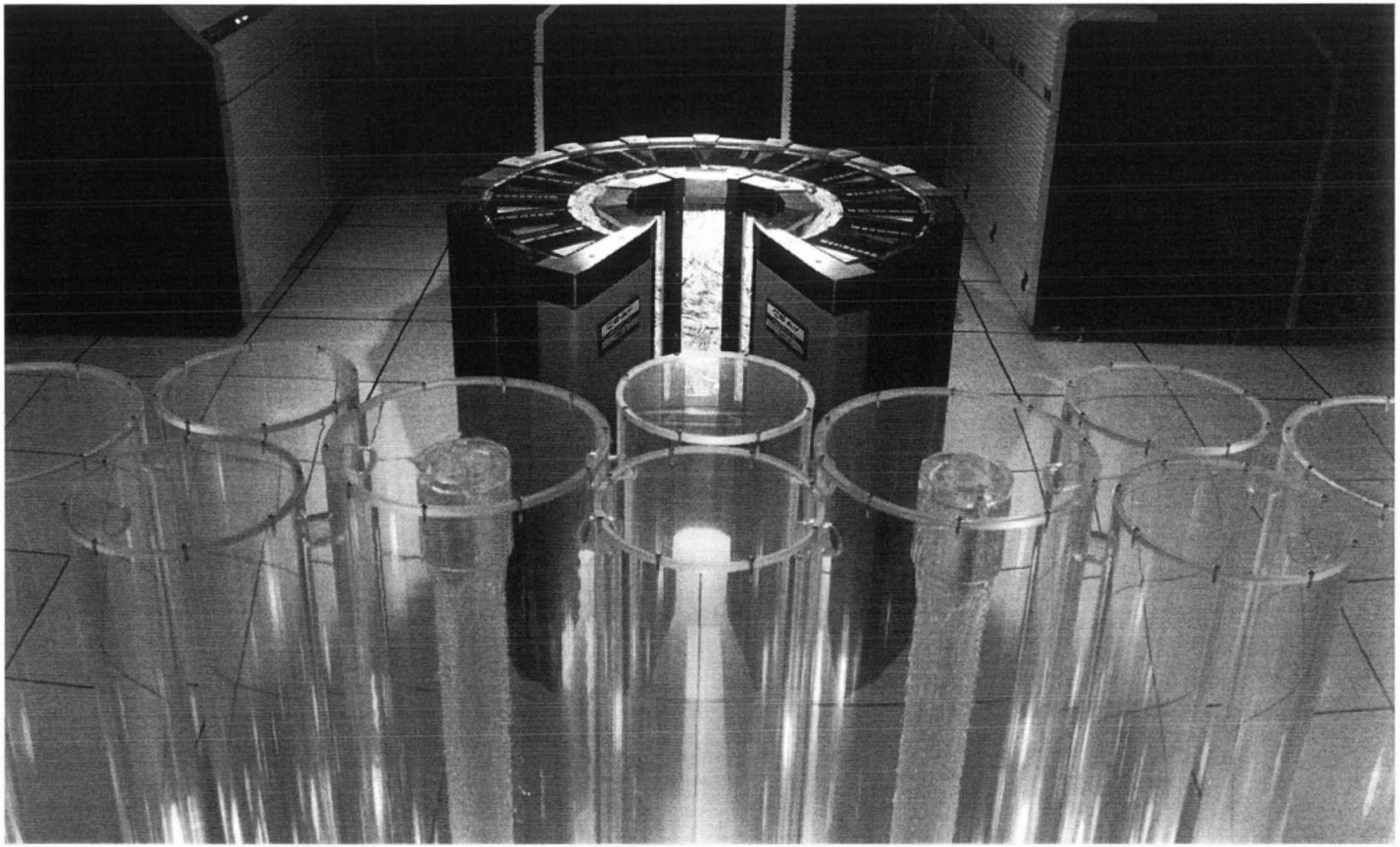




II. Hardware

- Hardware involves a variety of large systems (and subsystems) including (but not limited to):
  - Aircraft
  - Aerospace Vehicles
  - Launch Vehicles
  - Manned Spacecraft

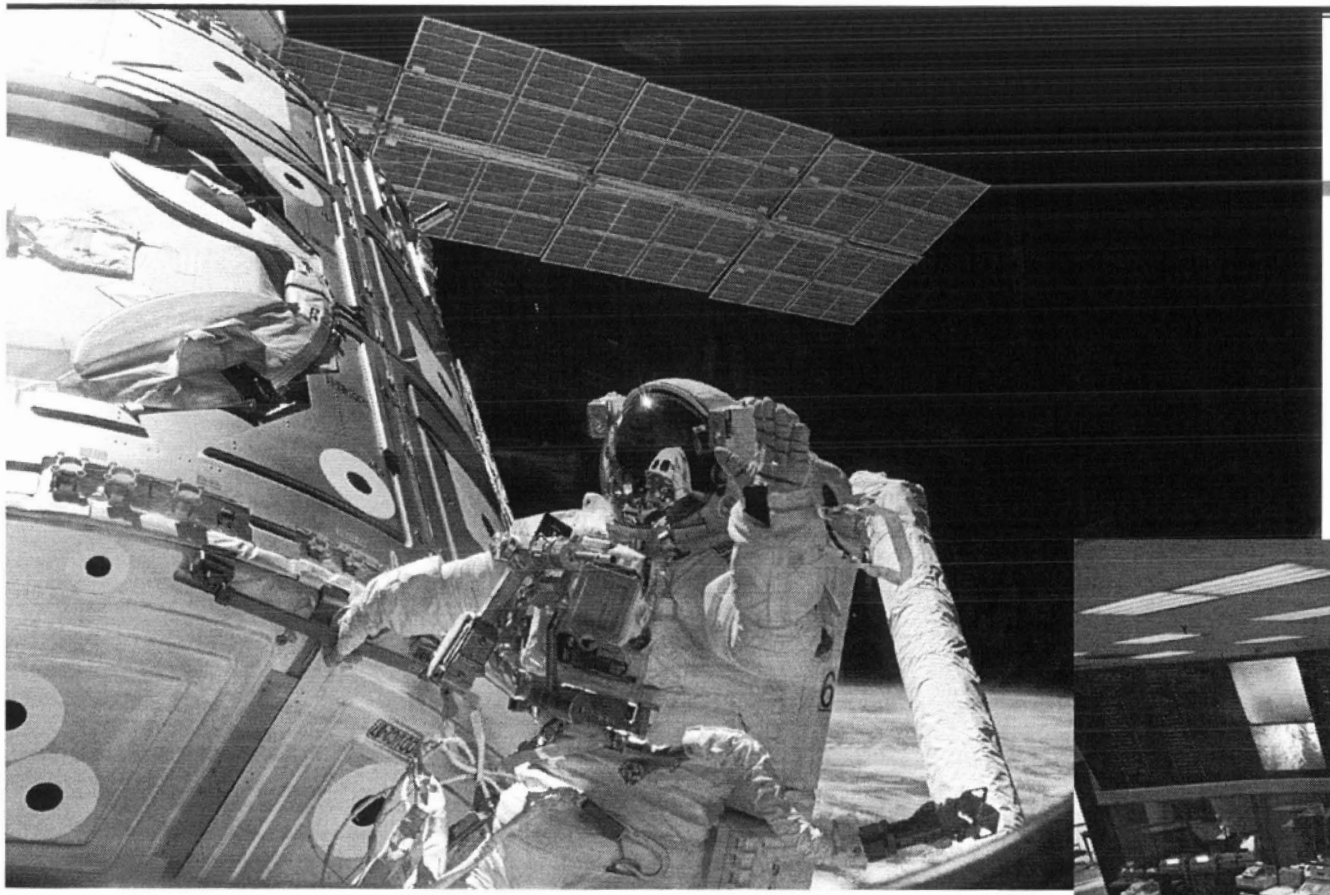
III. Software

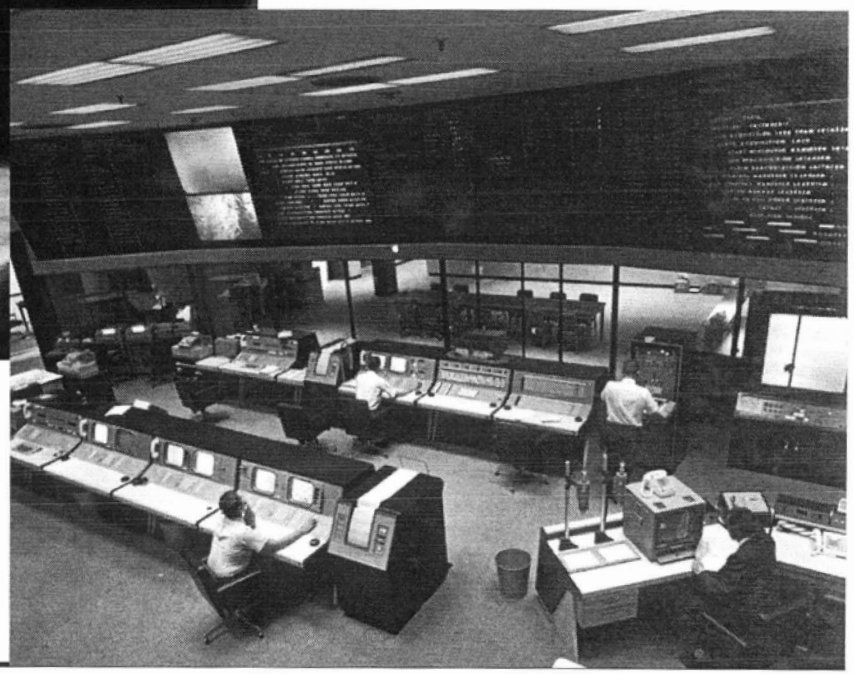


III. Software

- Software now comprises a significant fraction of the functionality and expense of spacecraft and support systems
- Reliability of software is difficult to define as well as difficult to determine
- A significant effort is required to understand this issue

IV. Human Actions

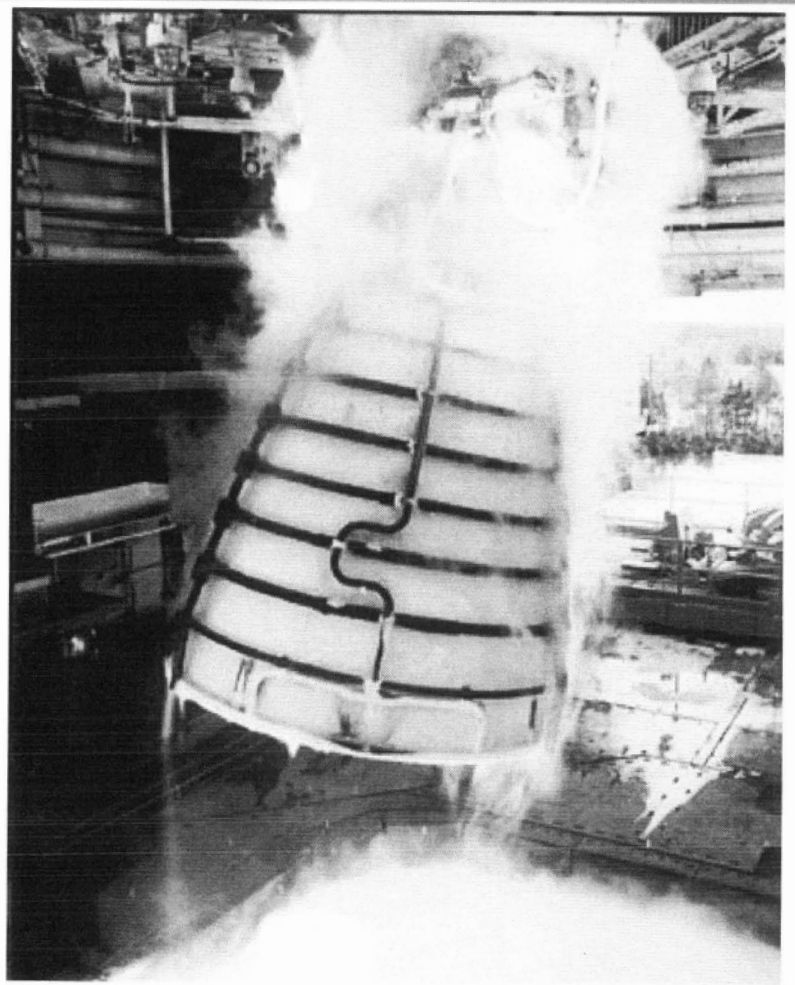


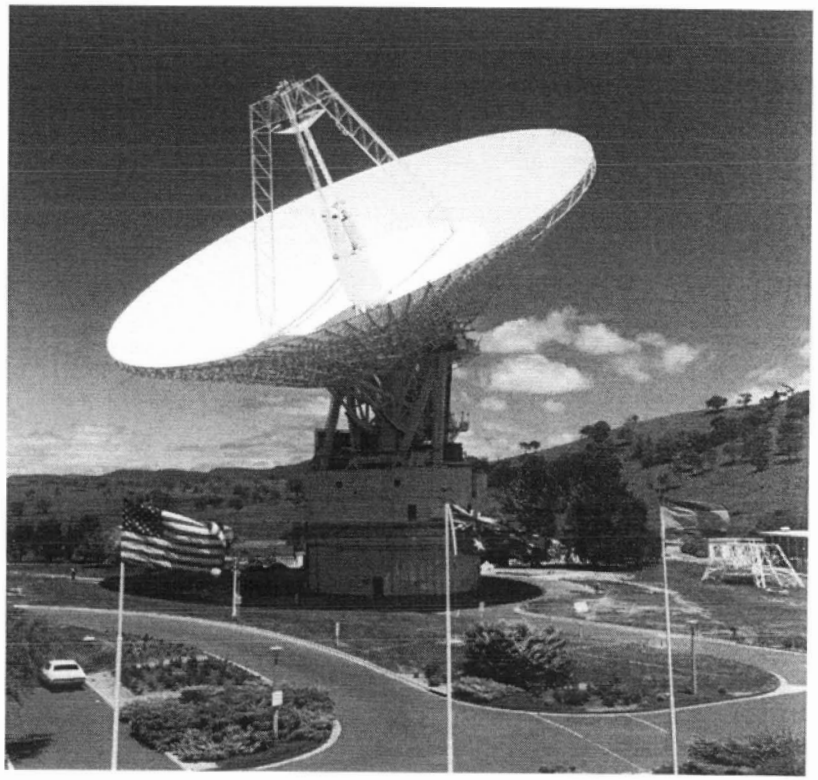


IV. Human Actions

- The actions of humans both in space and on the ground as they interact with various systems (most of them complex) are important factors in the reliability of systems
- Ultra Reliability methods must account for the interactions of humans with the systems under consideration

V. Infrastructure

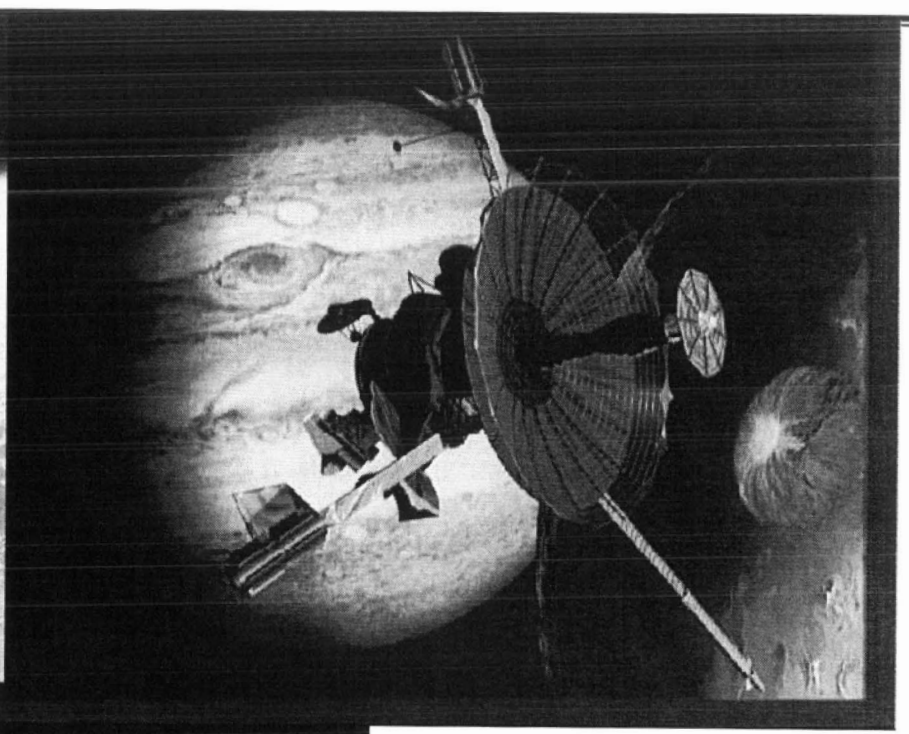


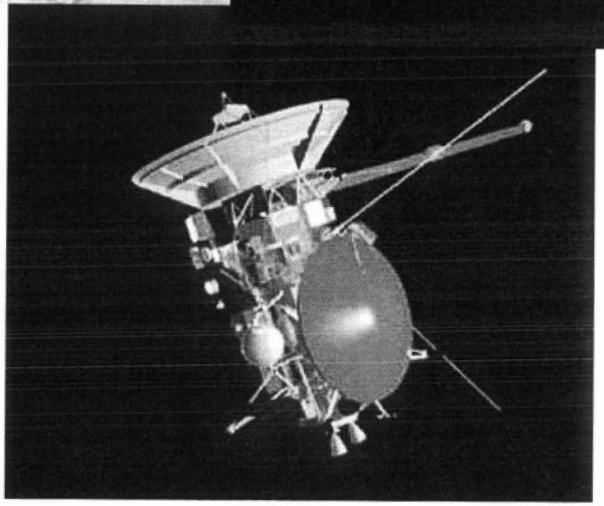


V. Infrastructure

- Results of the 2002 Ultra Reliability workshop indicated a need for infrastructure support and intercenter cooperation in all areas in order to make significant progress
- A considerable test capability exists across NASA centers which is often underused
- One of the aims of the Ultra Reliability program is to foster cooperation and make use of this outstanding capability

VI. Earth Orbiting and Long Life





VI. Earth Orbiting and Long Life

- The long-life missions aspect of Ultra Reliability has been pursued by Dr. Henry Garrett
- The next few slides are a part of this work
  - ***Space Systems Failure Analysis***
    Suzanne Thompson
  - ***Assessment of In-flight Anomalies of Long Life Outer Planet Missions***
    Alan R. Hoffman, Nelson W. Green, Henry B. Garrett

Space Systems Failure Analysis

Reliability and Risks of Space Systems Failures

- Objectives:
  - An overview of a space systems failure analysis, complete with documentation and evaluation of spacecraft launch vehicle and satellite failures, is the subject of this research.
  - The database of space systems failures is reviewed and a comprehensive catalog of world space launch failures from 1928 through 2003 and satellite failures from 1959 through 2003 is compiled from a number of open sources.
  - The focus of this research consists of satellite and launch vehicle success and failures rates, with emphases on the main causes of those failures.
- Approach:
  - Classify the reliability of space system failures over time.
  - Study the impact of space system failures on space mission cost effectiveness.
  - Examine the implications for reliability enhancement for future space systems.
- Purpose:
  - The intent of this analysis is to identify the critical causes and processes involved in space-related failures and recommend ways to mitigate space system mission failures in the future.

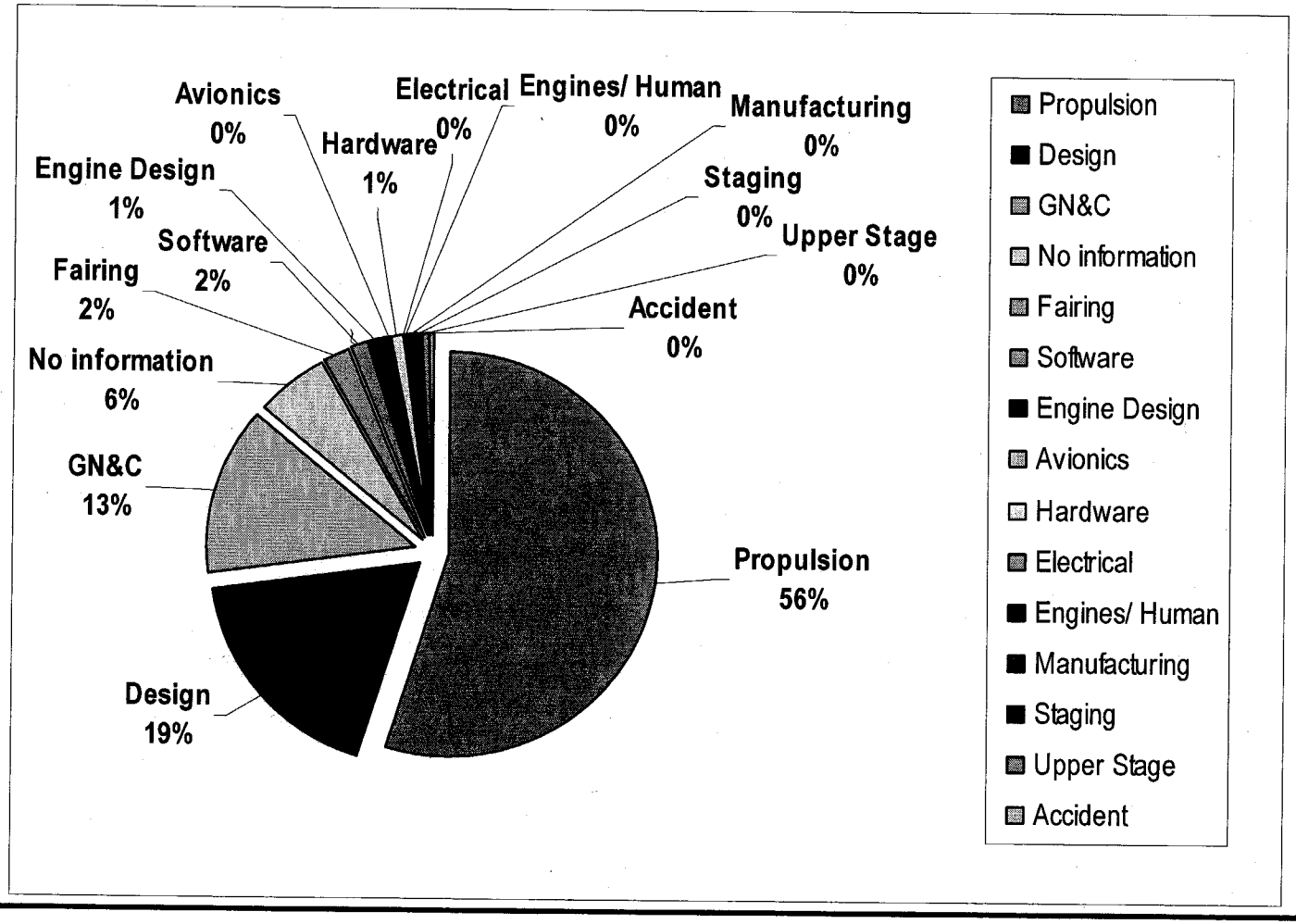
Failure Sample: Launch Vehicles

Space Systems Failure Analysis

Launch Vehicle	Satellite Payload	Description	Primary cause	Country	Organization	Date (mm/dd/yy)
A3	not known	The rocket impacted and exploded 300 m	Engine cutoff	Germany	Von Braun	12/04/37
A3	not known	The rocket crashed a short distance from	Engine cutoff early	Germany	Von Braun	12/06/37
A3	not known	The rocket impacted into the Baltic Sea and	No parachute deployment Engine	Germany	Von Braun	12/08/37
A3(Final launch of A3)	not known	Missile lost in Baltic Sea	No parachute deployment Engine	Germany	Von Braun	12/11/37
Ariane-1(V02)	Firewheel/CAT/OSCA	The 1st stage of the Ariane-1(V02)vehicle	combustion instability a	Europe	Europian Space Agency(ESA)	5/3/1980
Ariane-1(V05)	Marecs-B/Sirio-2	The 3rd stage engine of the Ariane-1 (V05)	The most probable cause of failure for the	Europe	ESA	9/9/1982
Ariane-3 (V15)	BCS-3/Spacenet-3	The 3rd stage of the A	The Failure Inquiry Bo	Europe	ESA	9/12/1985
Ariane-2 (V18)	Intelsat VA	The 3rd stage of the A	All evidence indicates t	Europe	ESA	5/30/1986
Ariane-44L (V36)	Superbird-B/BS-2X	The Ariane-44L (V36) exploded	The thrust loss of the v	Europe	ESA	2/22/1990
Ariane-44LP (V63)	Eutelsat 2F5/Turksat 1	The 3rd stage of the A	Shutdown of the 3rd-st	Europe	ESA	1/24/1994
Ariane-42P (V70)	PAS-3	The 3rd stage of the A	The 3rd stage produce	Europe	ESA	12/1/1994
Ariane-5 (V88)	4 Clusters	The Ariane-5 (V88) ve	The failure was attribut	Europe	ESA	6/4/1996
Ariane 5	Amsat P3D	premature shutdown	Roll torque from engine caused	Europe	ESA	10/20/1998
Ariane 5	BSAT2b,Artemis	Loss of partial thrust from 3 rd stage	Due to a combustion instability	Europe	ESA	7/12/2001

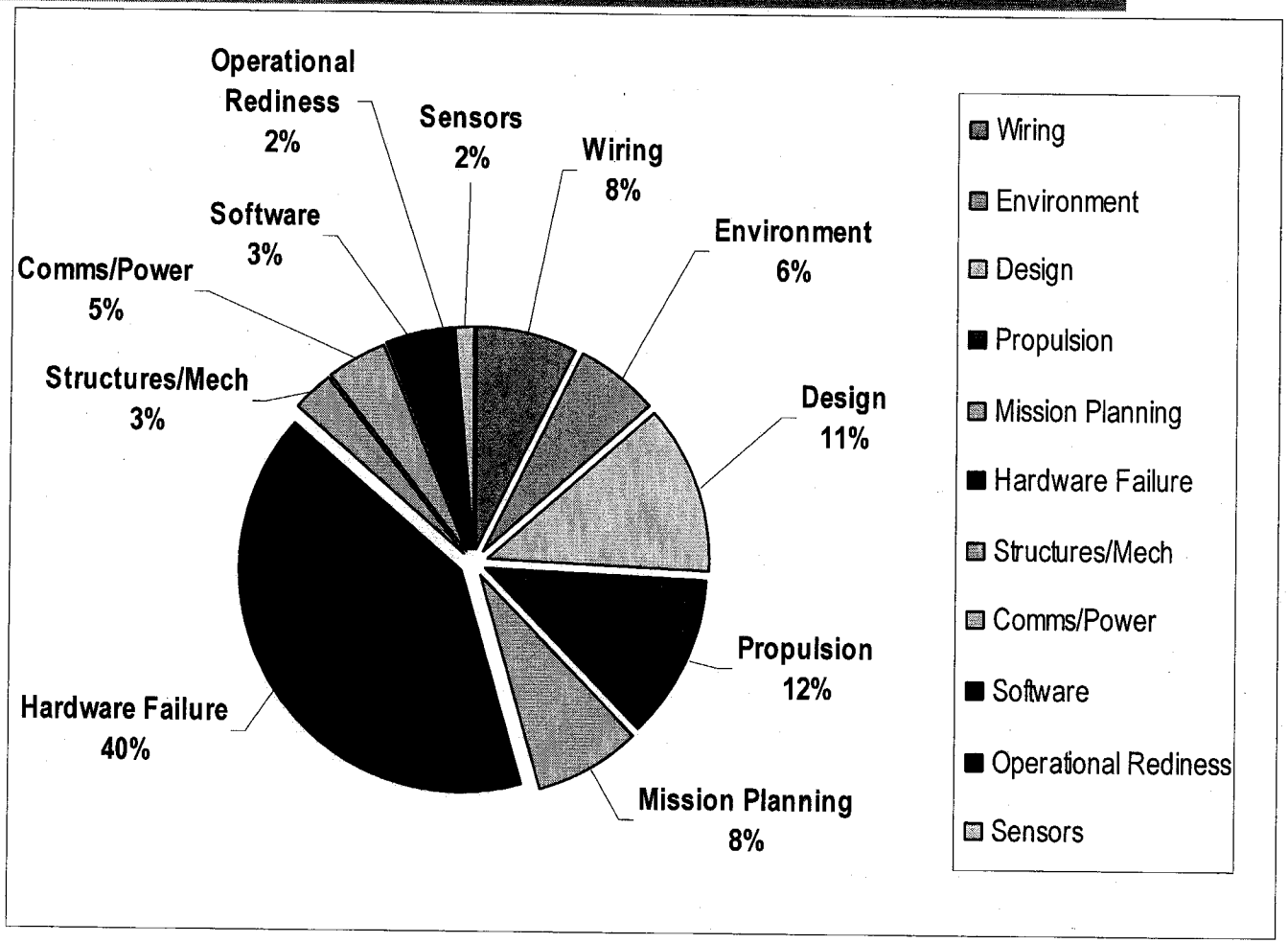
Space Systems Failure Analysis

Launch Vehicle Failure Classification



Space Systems Failure Analysis

Satellite Failure Classification



Space Systems Failure Analysis

Space Systems Reliability Enhancement

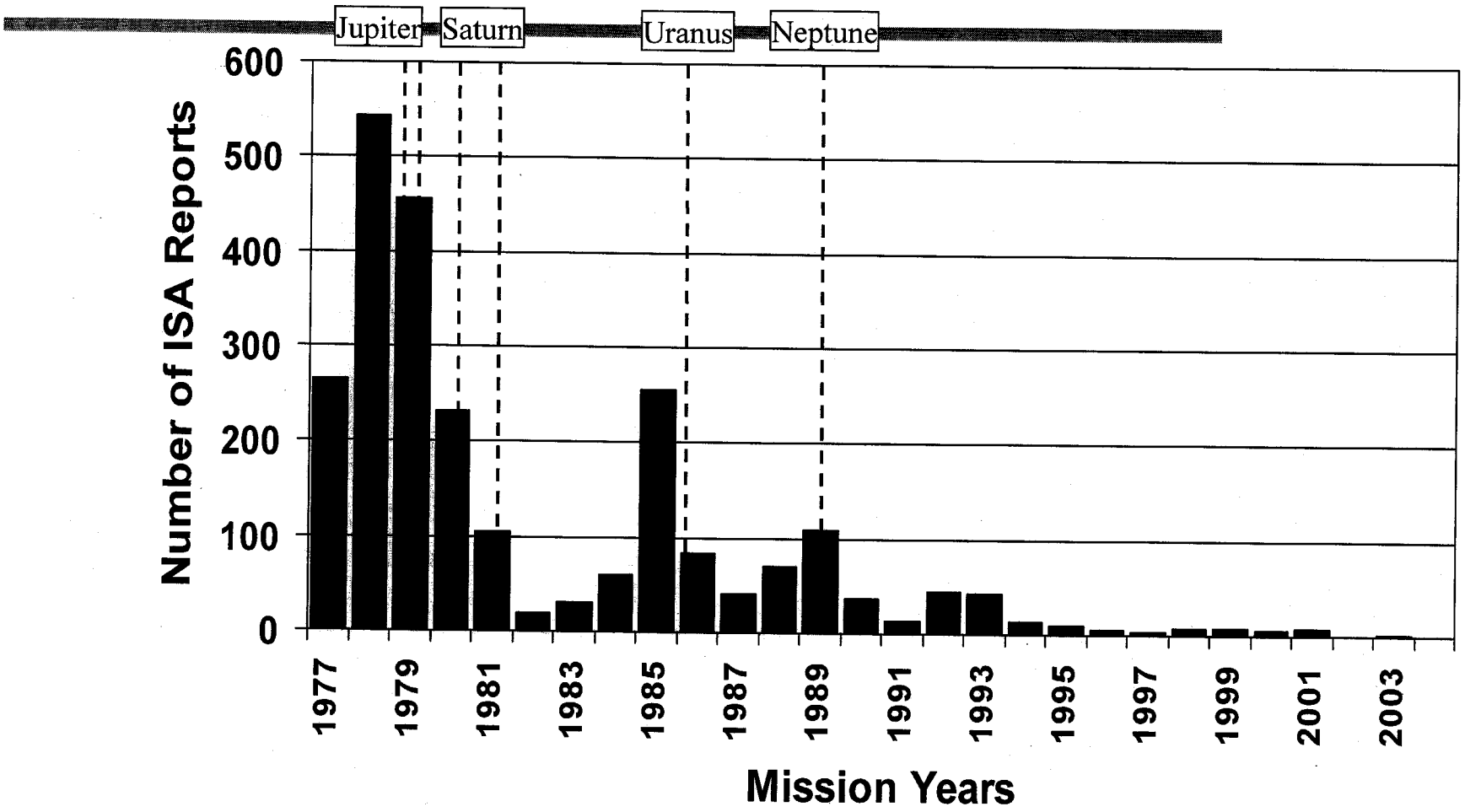
- Constant awareness of space systems by attending spacecraft technical meetings, symposiums and workshops.
- Create a comprehensive review of lessons learned to avoid recurrence of space system failures.
- Limit space launch operations within the envelope of design environment and flight experience.
- Those that manufacturers space systems should make public failures experienced to preclude future mishaps.
- The developmental stages of design should increase their test effectiveness.
- Future space missions should have a plan for potential failures.

Study Objectives

- Analyze in-flight anomaly reports for outer planet spacecraft to gain a better understanding of the technology and management approaches needed to build machines than can fly to the edge of the solar system and into interstellar space.
- Determine if redundancy was utilized, the type utilized (block vs functional). and which phase of the flight it was applied
- Determine the relationship between the number of anomalies and the occurrence of major flight events
- Identify long life mission planning and management issues that must be addressed for future missions

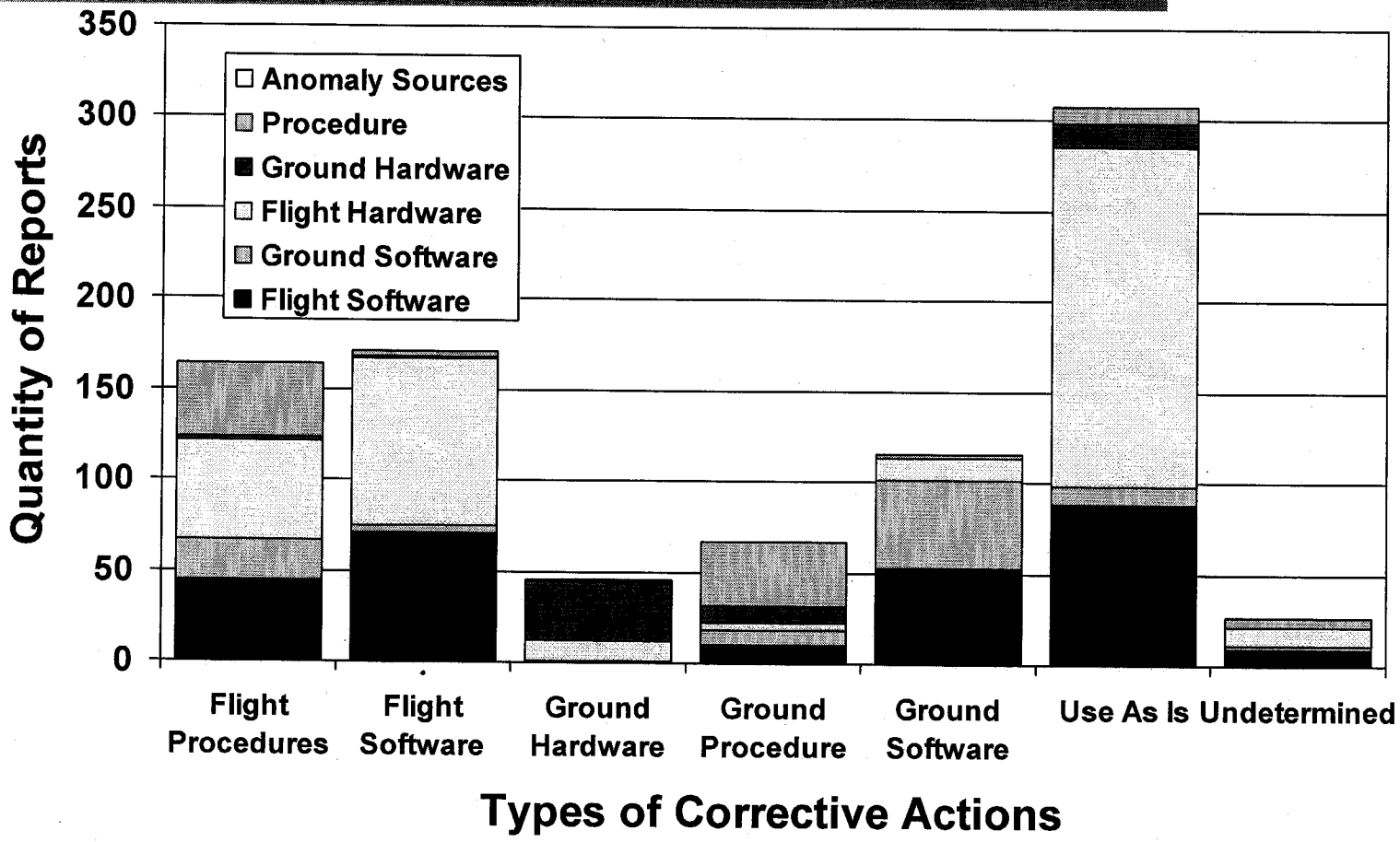
Assessment of In-flight Anomalies of Long Life Outer Planet Missions

Voyager Incident Surprise Anomaly Quantities by Year



Assessment of In-flight Anomalies of Long Life Outer Planet Missions

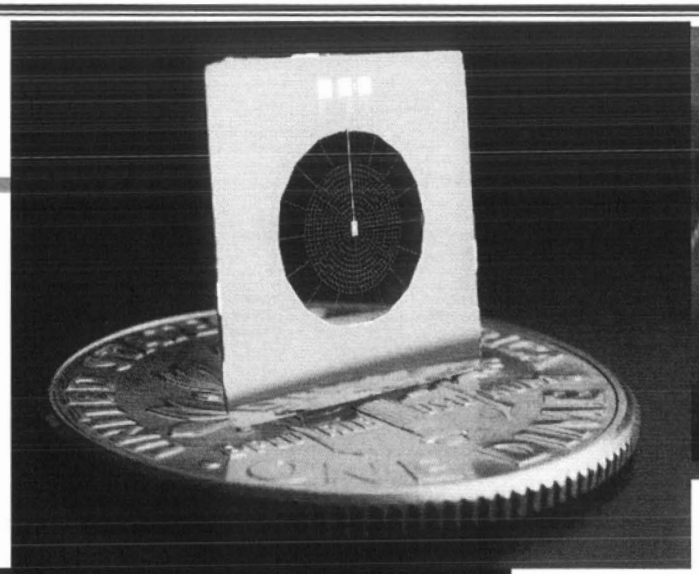
Galileo Types of Corrective Actions with Anomaly Sources

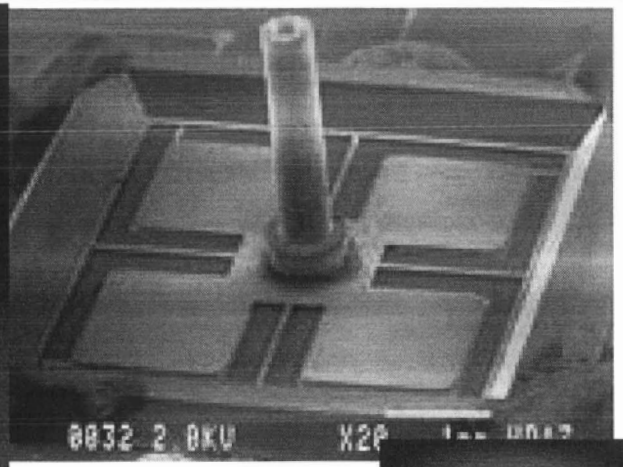


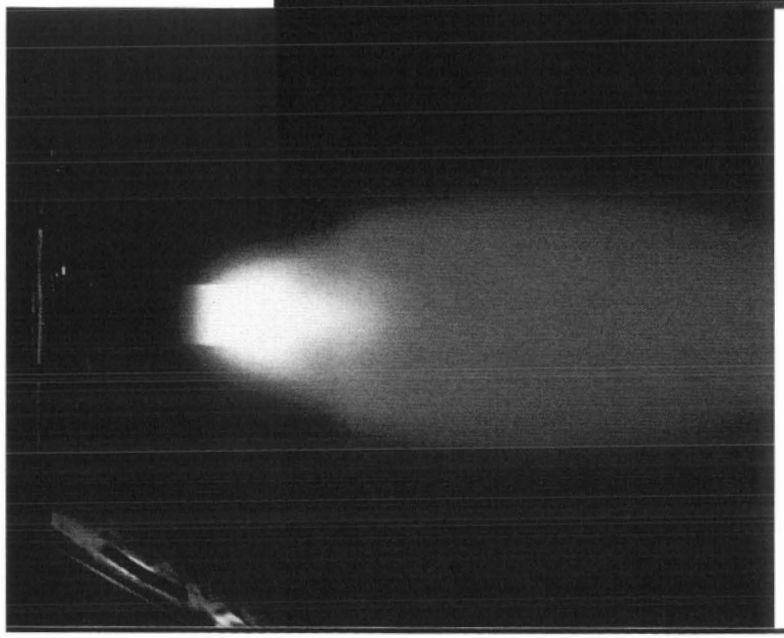
Summary

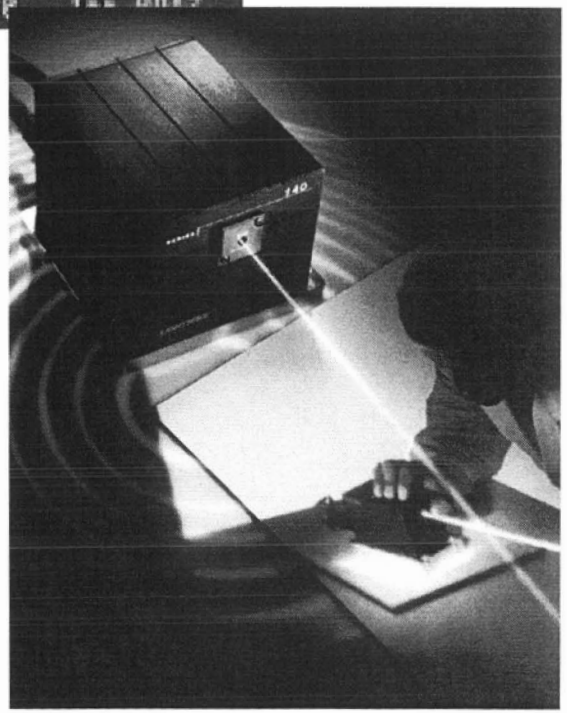
- Anomaly reports analyzed for three deep space spacecraft with an accumulated flying time of sixty six years
- Redundancy has been used on all of these missions at different phases of the flight
- Number of anomalies increased as major flight events occurred
- Long life missions planning to include:
  - Skill retention for progressively obsolete spacecraft
  - Knowledge management for systems and instrument control

VII. Cross-Cutting Technologies









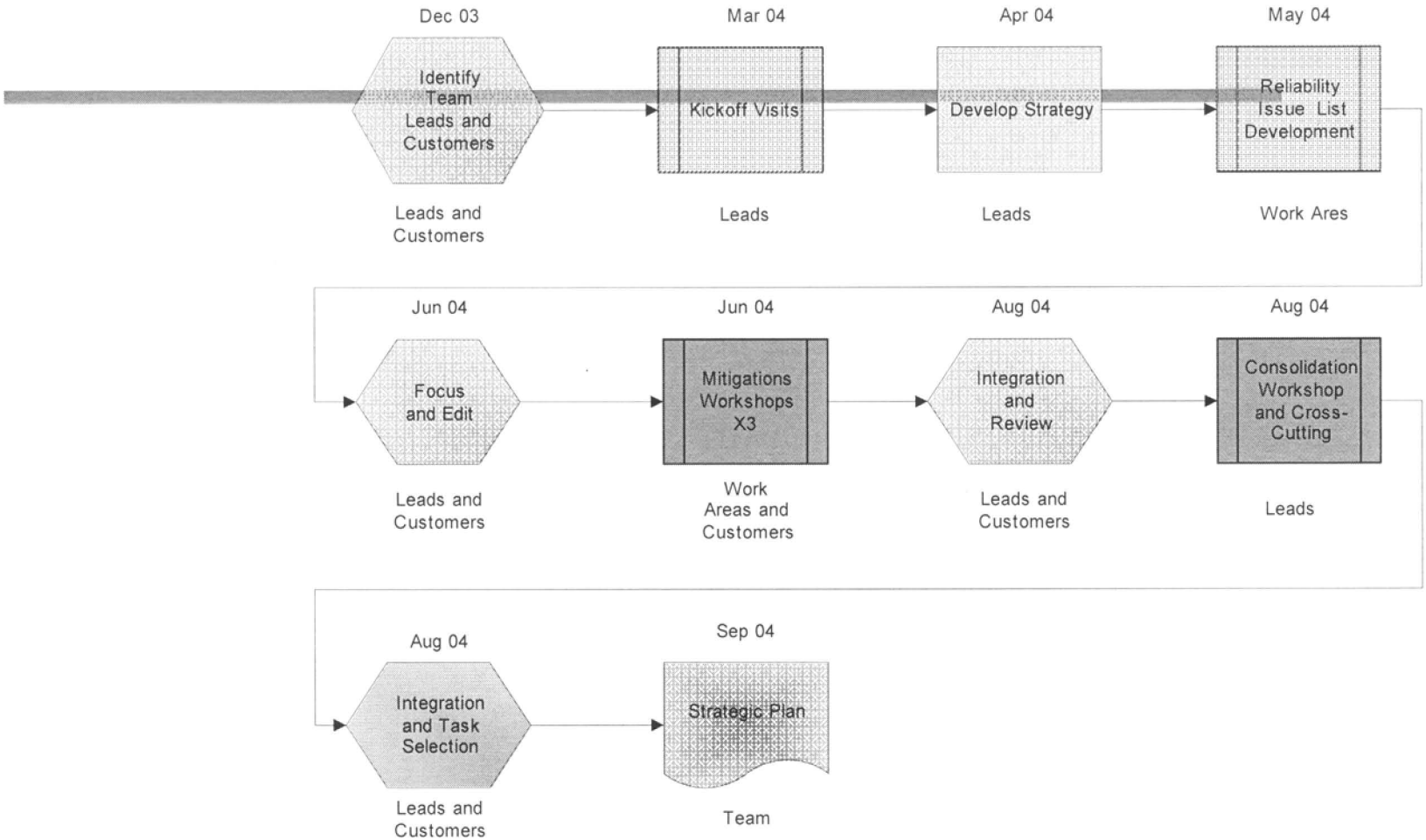
VII. Cross-Cutting Technologies

- Certain technologies appear to be relevant across a large number of systems and mission profiles, for example:
  - Validation and Verification
  - Electronics
  - Optical Systems
  - Instruments
  - Data Processing
  - Communications
  - Reliability and Risk Assessments and Models
  - Materials
  - Power Systems

Ultra Reliability Plan Overview

		Products
First Year (FY04)	1. Planning a. *Area Identification* b. *Reliability issue Identification* c. *Mitigation and Task Identification*	Key reliability issue identification Reliability assessment Mitigation approaches and techniques
(FY05~08)	2. Execution of reliability assessment /improvement tasks a. *Initial Task Start* b. *Re-Evaluation* c. *New Initial Tasks* d. *Re-Evaluation*	Execution plan for NASA-wide strategy for Ultra Reliability
(~FY09)	3. Infrastructure Development	Necessary to accomplish 10X improvement
(~FY10)	4. Strategies for New Missions	Ultra Reliability by Design (increased by 10X)

Ultra Reliability Work Flow



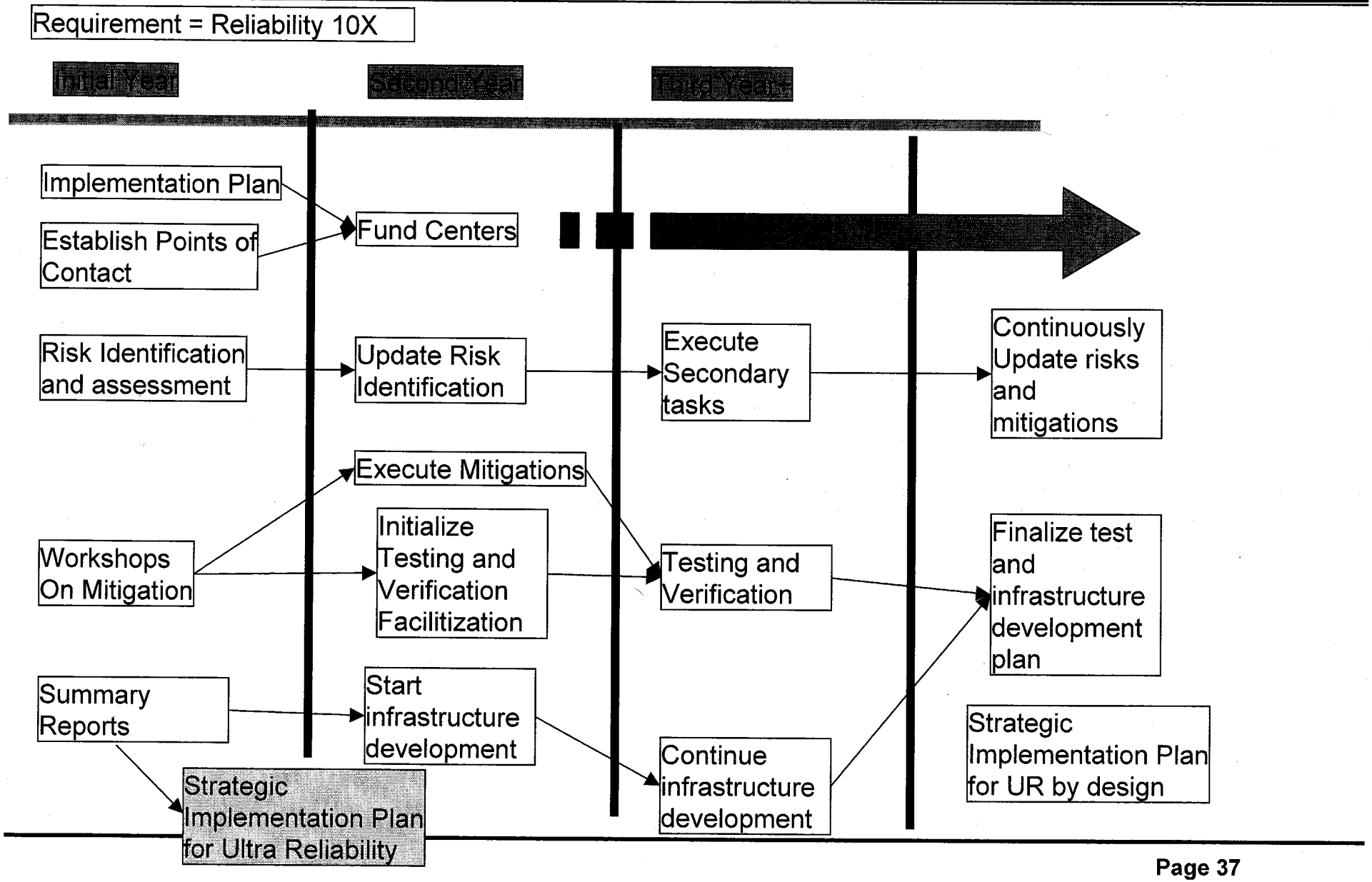
Customers

- For this project the world is divided into work areas and customers
- Customers are resident in both the mission codes and the performing centers
- The following page is meant to be representative and is not necessarily comprehensive

Customers

		Categories
■ Technology	• JSC • KSC • MSFC	Manned Space Missions
■ EO	• GSFC • JPL	Earth Orbiting Missions
■ Aero	• GRC • LaRC • DFRC	Aeronautical and Aerospace Vehicles
■ Science	• JPL • GSFC	Planetary and Deep Space Mission
■ Launch Vehicles	• MSFC • SSC	Booster

Ultra Reliability – Implementation Strategy



ONE NASA

- This program needs to be NASA-wide:
  - to address different ultra-reliability needs in different NASA Enterprises
  - to leverage the wide variety of expertise across all of NASA
  - to get buy-in and make this a successful program
  - to develop a NASA - wide infrastructure (paramount)
  - to leverage overlapping issues
    - to take advantage of related on-going NASA tasks
- There is a lead center for each major area, but many centers should participate and be funded in each area
- Metric for leveraging of internal Code Q research
- The development of reliability assessment is a key for success
  - Intelligent consistent use of existing NASA methods and an opportunity to develop novel ways of assessing reliability

Summary

- A pathway for a strategic plan for increasing the reliability of NASA missions one order of magnitude has been defined
- A short term plan has been defined
- We are ready to go!
  - Area leaders have be identified
  - Customer representatives are being identified
  - Reliability issue lists are being developed in each area
  - Reliability workshops have been scheduled