



Perspectives on Dependable Computing for Solar System Exploration

Leon Alkalai
Center for Advanced Avionics
Jet Propulsion Laboratory
California Institute of Technology

2002 Pacific Rim International Symposium on Dependable Computing
(PRDC2002)
December 16-18, 2002
Tskuba International Congress Center, Japan



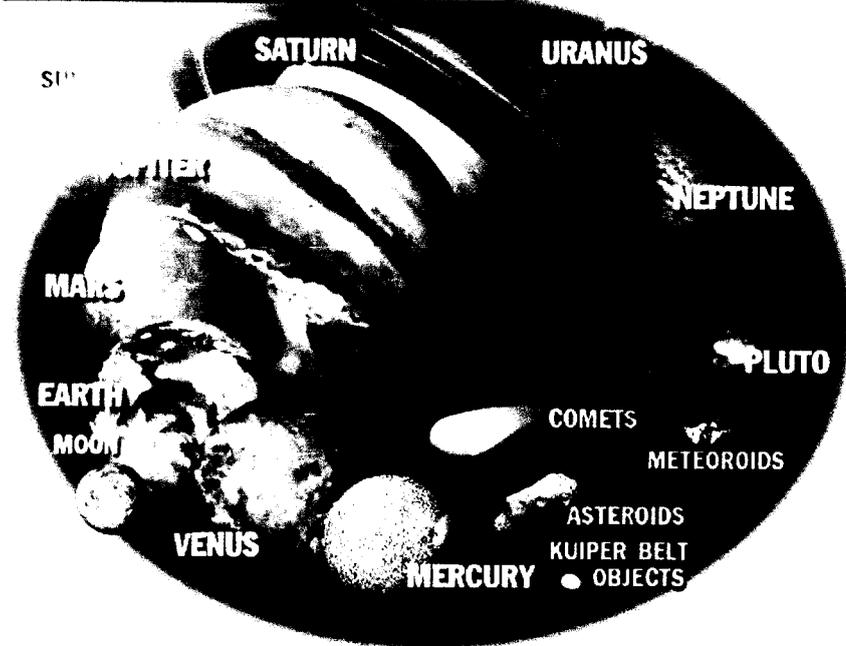
Space Science Themes



Astronomical Search for Origins



THE BODIES IN OUR SOLAR SYSTEM



Sun Earth Connection

CAMPAIGN 3 NASA

Understand the Geospace Environment

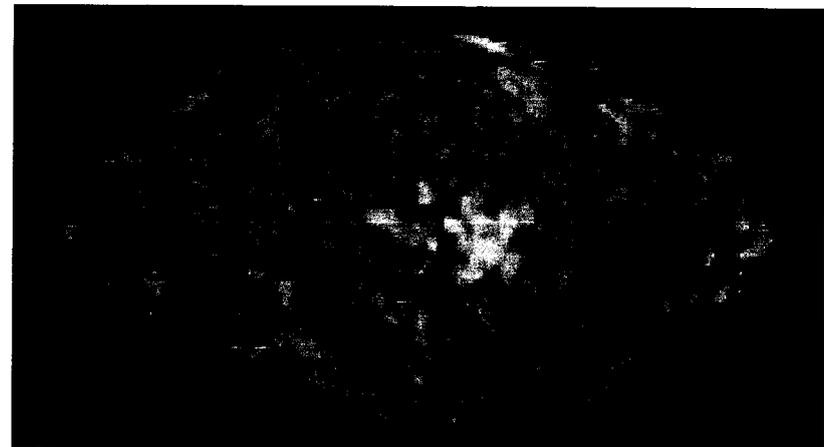
Geospace Dynamics

Regional Dynamics

Coupling and Boundary Process

MMS GEC MagCon ITM Waves Inner MagCon Tropical ITM DBC GSRI 64

Structure and Evolution of the Universe



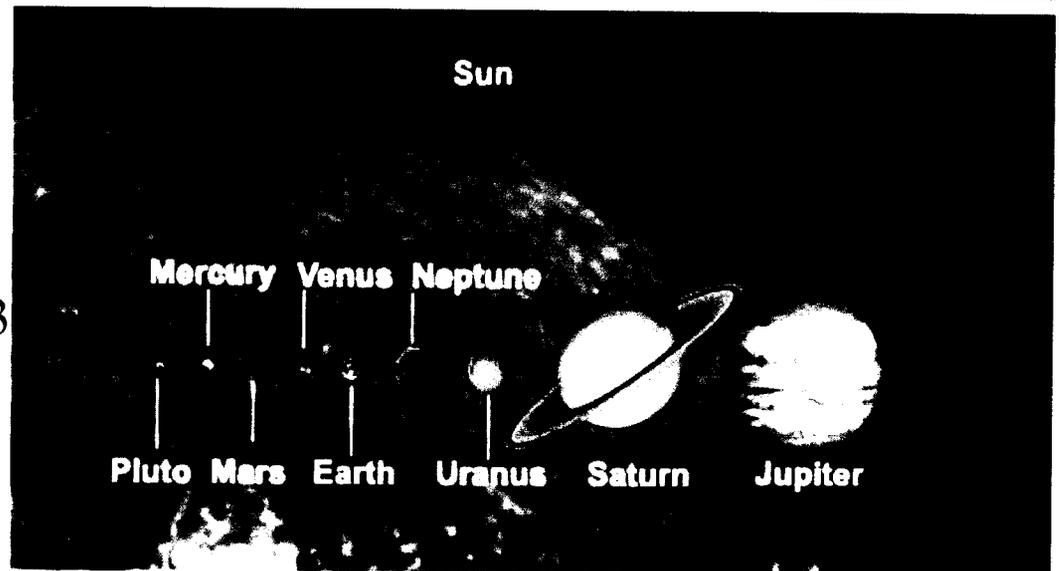


Exploring our Solar System

Current Missions

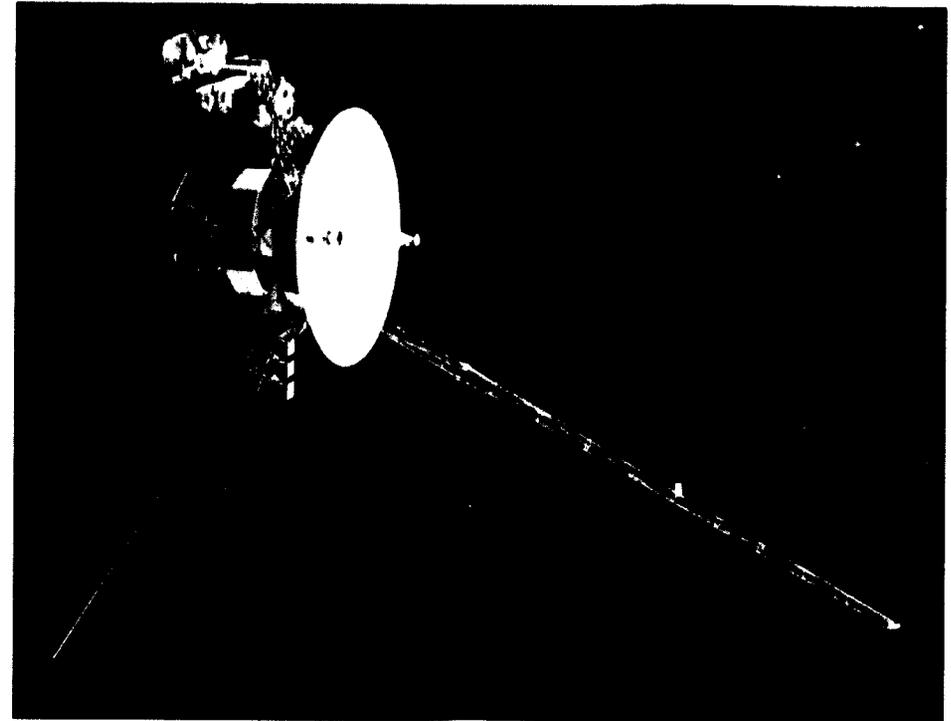
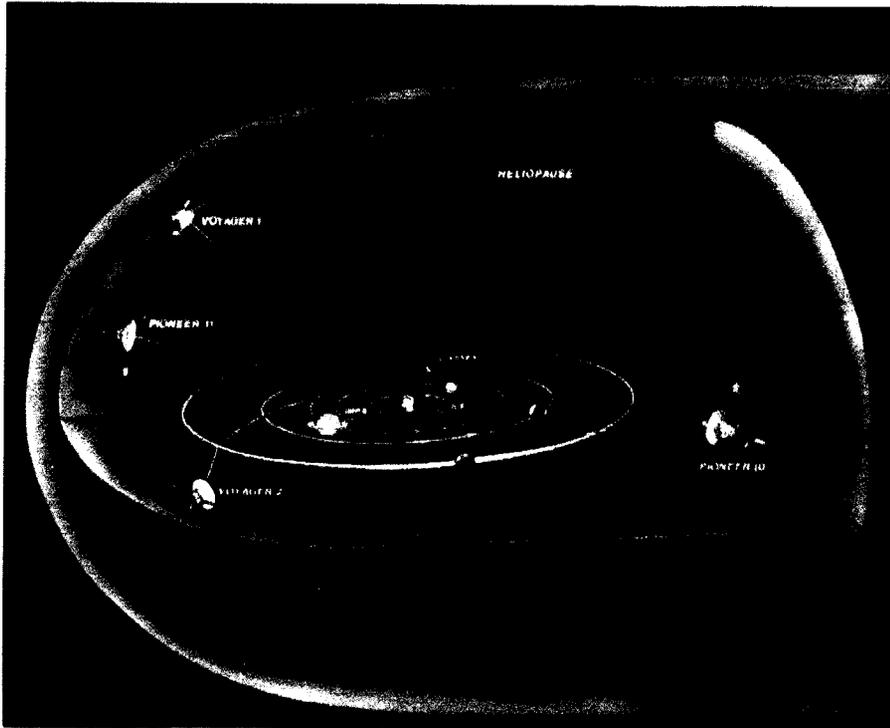


- Voyagers 1 & 2: 1977
- Galileo: 1989
- Ulysses: 90
- Cassini: 97
- Stardust: 99
- Genesis: 2001
- Mars Exploration:
 - Mars Pathfinder: 96
 - Mars Global Surveyor: 96
 - Mars Odyssey: 2001
 - Mars Exploration Rovers: 2003
 - Future Mars Missions





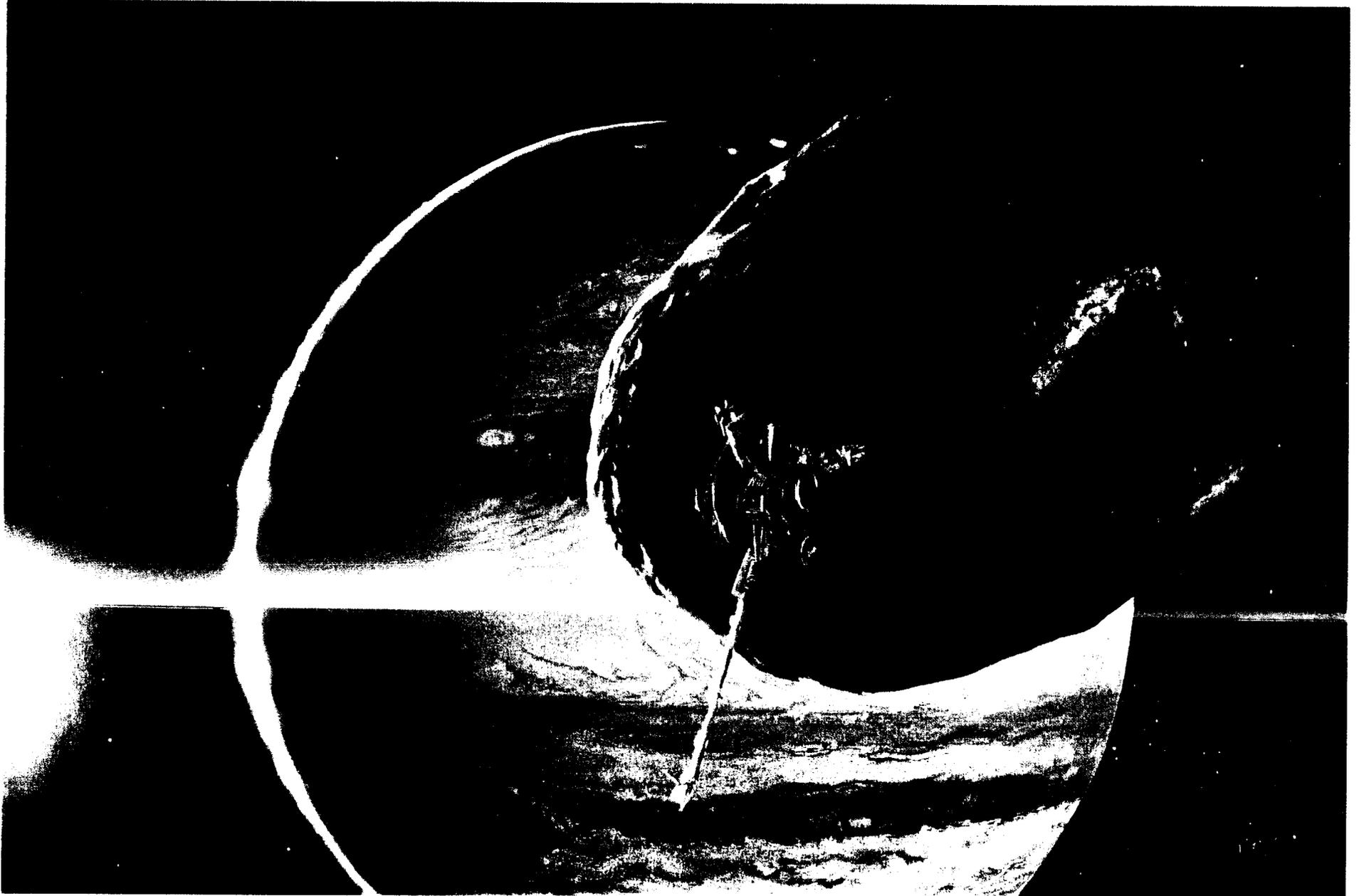
Voyagers 1 & 2: 1977 - Present



- Designed to tour Outer Planets: 1977 – 1989. Primary goal achieved.
- 25 years of continuous operation – now renamed Voyager Interstellar Mission
- Can operate until 2020 based on available power and attitude control propulsion
- With some loss of subsystem redundancy, operates with full science payload
- Spacecraft has extensive autonomous fault-detection and protection capabilities covering multitude of possible failures. Designed using radiation hard parts and extensive shielding.



Galileo: 1989 - Present





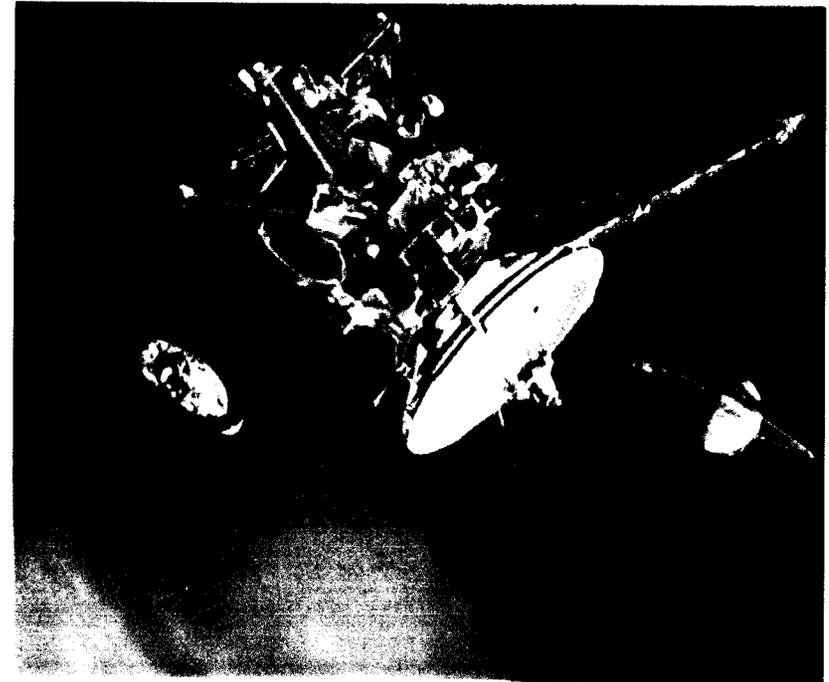
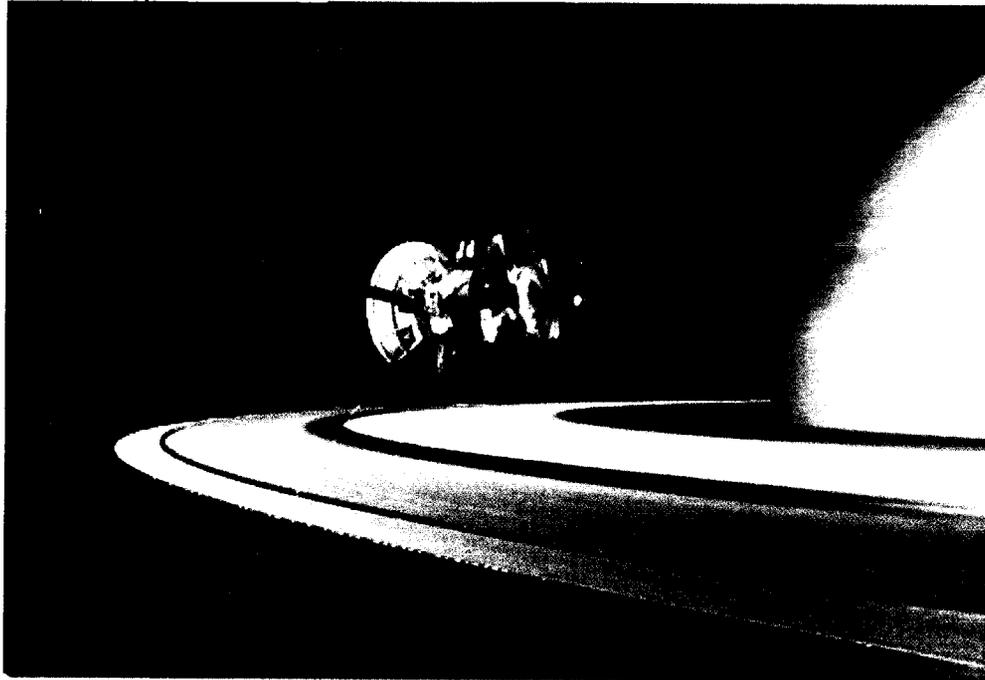
Galileo



- The spacecraft is now fully recovered from yesterday's anomaly in which the onboard fault protection routines detected a despun bus reset about 28 minutes before the closest approach to Io. Because this could be a potentially harmful event, the spacecraft put itself into a safe mode and canceled the science sequence. The flight team worked throughout the day and evening to re-establish nominal spacecraft operations and to acquire the final track of recorded data. Unfortunately, three tracks of data all planned for recording within hours of closest approach to Io were lost because of the spacecraft problem. At this time we think the problem resulted from the radiation environment near Jupiter.
- NASA's Galileo spacecraft is out of safing mode and has resumed normal flight operations, including playback of pictures and other science data gathered during the January 31 Europa flyby. Four hours after that flyby, Galileo entered safing mode--a built-in protection mode designed to turn off all non-essential spacecraft activities-- while the spacecraft was performing a sun acquisition turn. The turn was halted when onboard fault protection software determined that the turn was lasting longer than it should have. Normal operations of the spacecraft were restored Wednesday, February 10, and the playback of science data resumed Thursday morning, February 11. All observations made by Galileo's instruments during the close approach to Europa on January 31 were successfully stored and are being transmitted to Earth. After Galileo entered safing mode, scientists were unable to make planned distant observations of Europa, Io and Jupiter.
- Only four hours before the flyby, while Galileo was being bombarded by strong radiation near Io, its onboard computers reset and placed the spacecraft into standby mode. Onboard fault protection software told the spacecraft cameras and science instruments to stop taking data and enter a safe state until further instructions were received from the ground.



Cassini: 1997 - Present

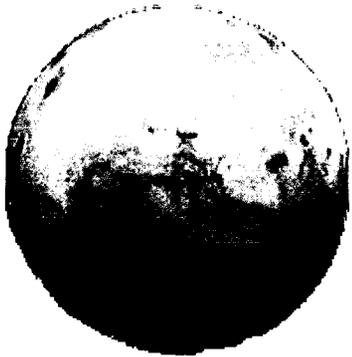


- First common subsystem Engineering Flight Computer (IBM)
- First use of Solid State Recorder technology in deep-space
- Extensive use of Application Specific Integrated Circuits (ASIC)
- Extensive use of RH technology and shielding
- Each subsystem has dual redundancy and cross-strapping. No single point of failure.





Mars Exploration Program



Mars Pathfinder – 1996

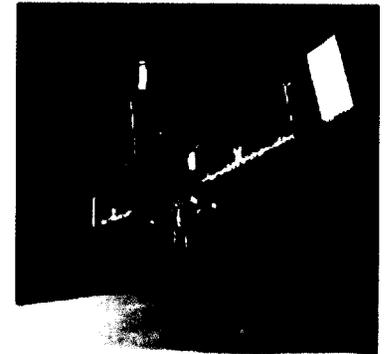


Mars Global Surveyor – 1996

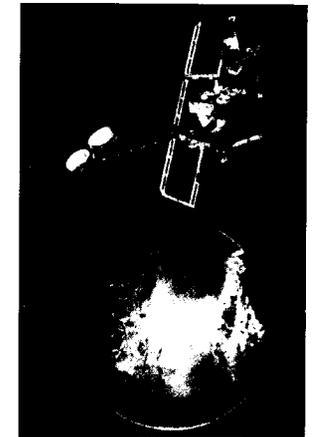
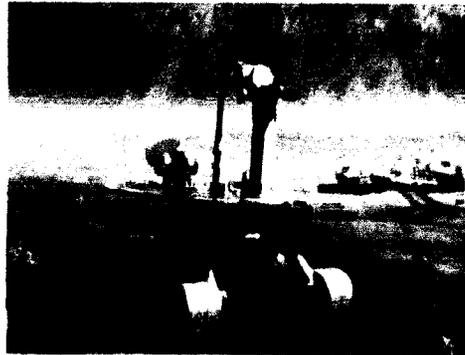
New Global Mars Topography from MOLA



Mars 2001 Odyssey



2003 Twin Mars Exploration Rovers





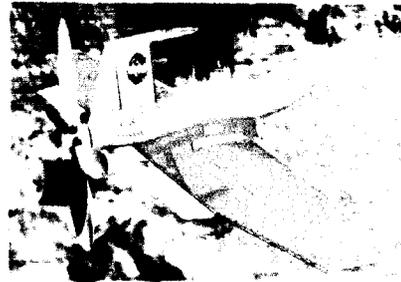
Future Mars Exploration Missions



2005 Mars Reconnaissance Orbiter



2007 Mars Scouts (4)



2009 Mars Science Laboratory



Future Mars Sample Return





NASA's Vision

- To improve life here
- To extend life to there
- To find life beyond

NASA's Mission

- To understand and protect our home planet
 - To explore the universe and search for life
 - To inspire the next generation of explorers
- ...as only NASA can

5 Strategic
Enterprises

Space
Science



Earth
Science



Biological
& Physical
Research



HEDS



Aerospace
Technology





Future Possible Europa Exploration



- Tremendous scientific opportunity
 - radar sounder, mapping
- Extreme Radiation Environment
- Extensive Shielding of electronics
- Extreme mass constraints
- Technology Freeze: 00-02
- Launch 04-06 time frame
- Technology Program:
 - X2000/CISM
- Follow-on missions:
 - Europa Lander
 - Europa penetrator/submarine



Future In-Situ Exploration



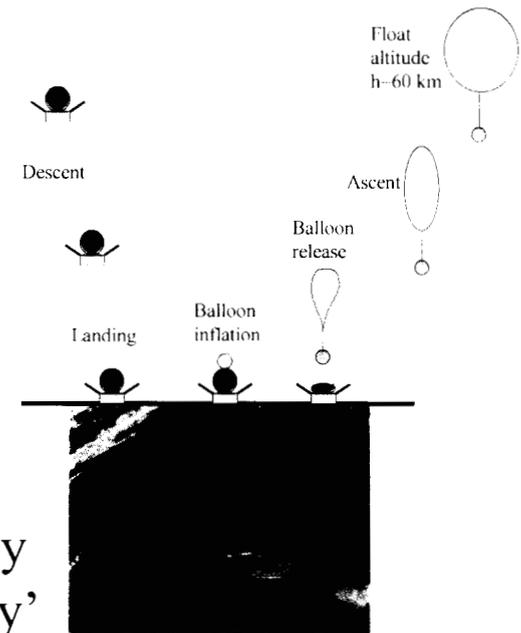
In Situ Exploration: EDI



Advanced Mobility: Titan Aerobot



Venus surface exploration and sample return



The future of solar system exploration is going to increasingly involve aspects of 'in-situ' exploration, advanced 'mobility' and 'sample capture and return'.

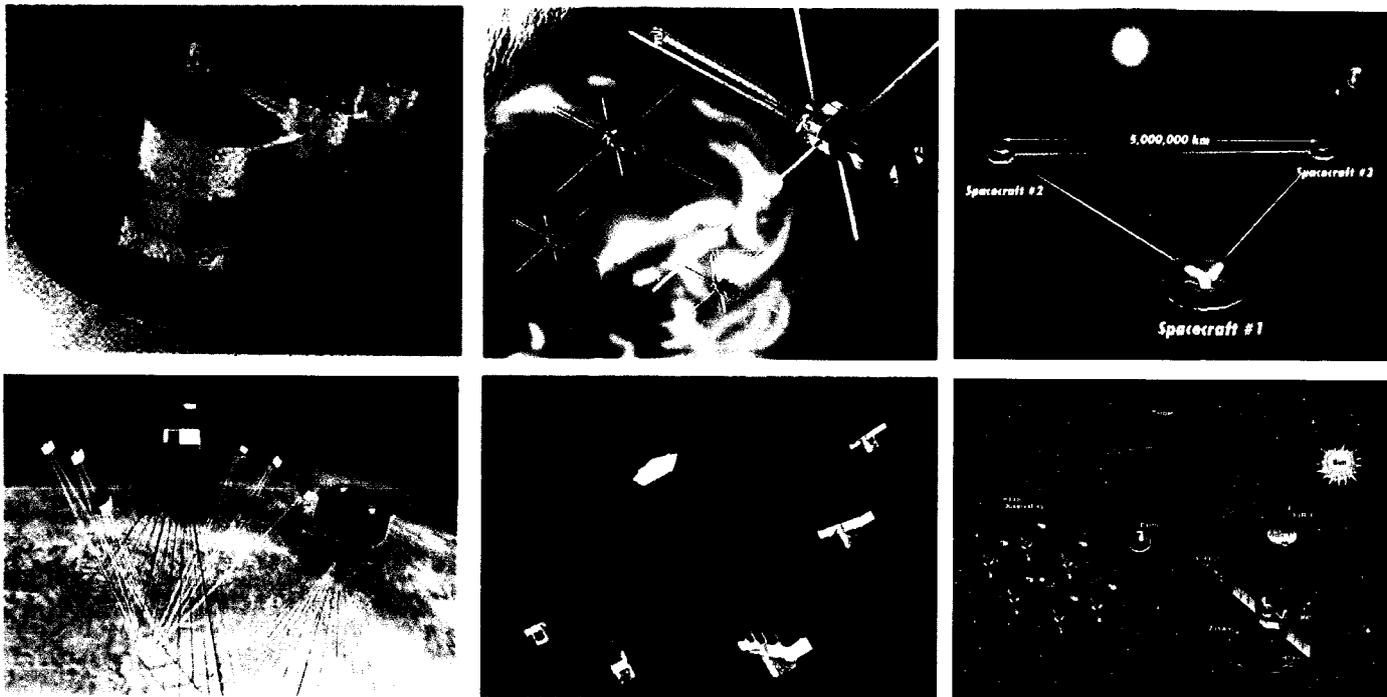
This in turn stresses the need for advanced systems miniaturization, on-board autonomous operations, and survivability in extreme environmental conditions.



Formation Flying – Distributed Science



A Set of Distributed Spacecraft Flying in Precision Formation to Enable Separated Aperture Interferometry Missions Achieving Unprecedented Astrometric and Imaging performance.



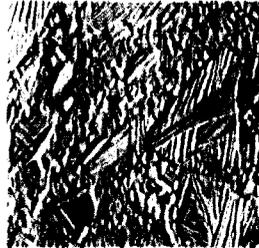


Survivable Systems for Extreme Environments

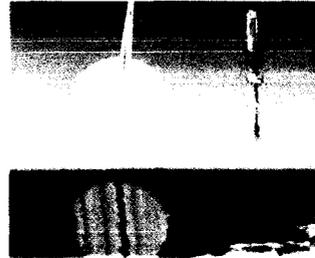
Venus surface exploration and sample return



Europa surface and subsurface



Titan *in situ*



Comet nucleus sample return



Mission	Low Temp.	High Temp.	High Radiation Levels	High Pressure	Other Environmental Conditions
Venus Surface Exploration and Sample Return		460C		90 Barr	Sulphuric acid clouds at 50 km 97% CO ₂ at the surface
Giant Planets Deep Probes	-160 C @ 0.1 Barr	380C	~ 100 Krad Equatorial	100 Barr	Methane, Ammonia clouds, extreme temperatures, and radiation for the equatorial
Comets/Asteroid Sample Return	-140 C		Probe		Dupe
Titan In-Situ	- 180 C			1.5 – 2.0 Barr	2-10% Methane Clouds Solid/liquid surface
Europa Pathfinder Lander	-160 C		5 MRad		½ dosage during mission ‘pump-down’ and ½ during prime mission



Neptune and Triton

/JPL/Publications/2002/PRDC-2002/alkalai.ppt

Exploration of Extreme Environments requires a comprehensive look at advanced thermal management techniques, high and low temperature electronics, radiation hard electronics, and advanced qualification methods.



Giant Planet Deep Probes
L. Alkalai, PRDC 2002, Japan

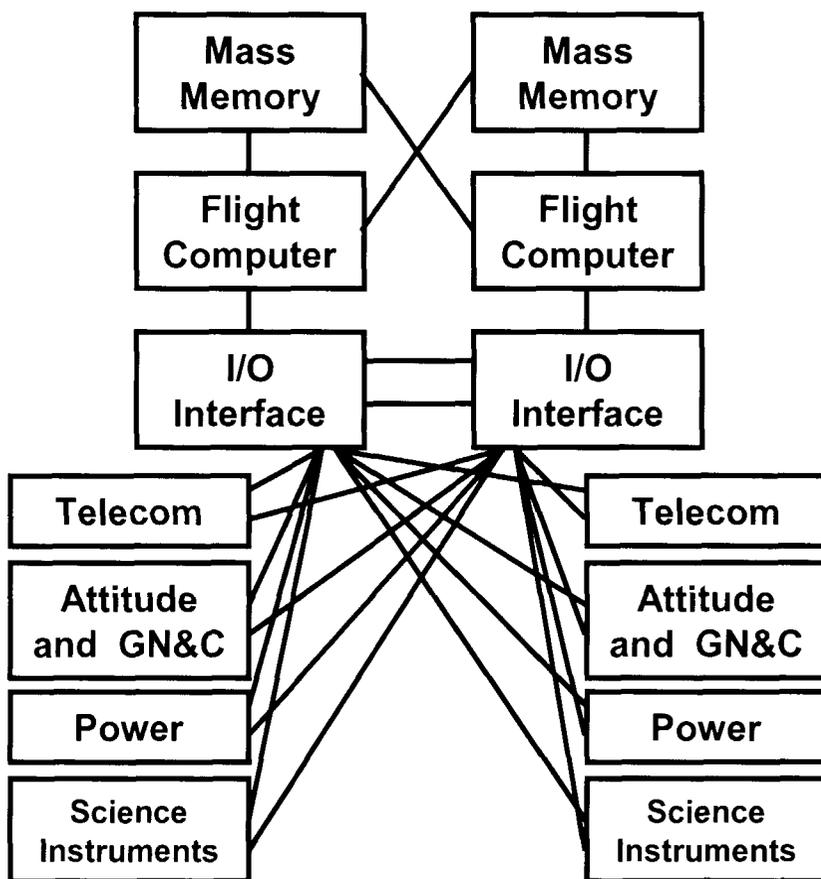


Dependable Computing in Previous Deep Space Missions

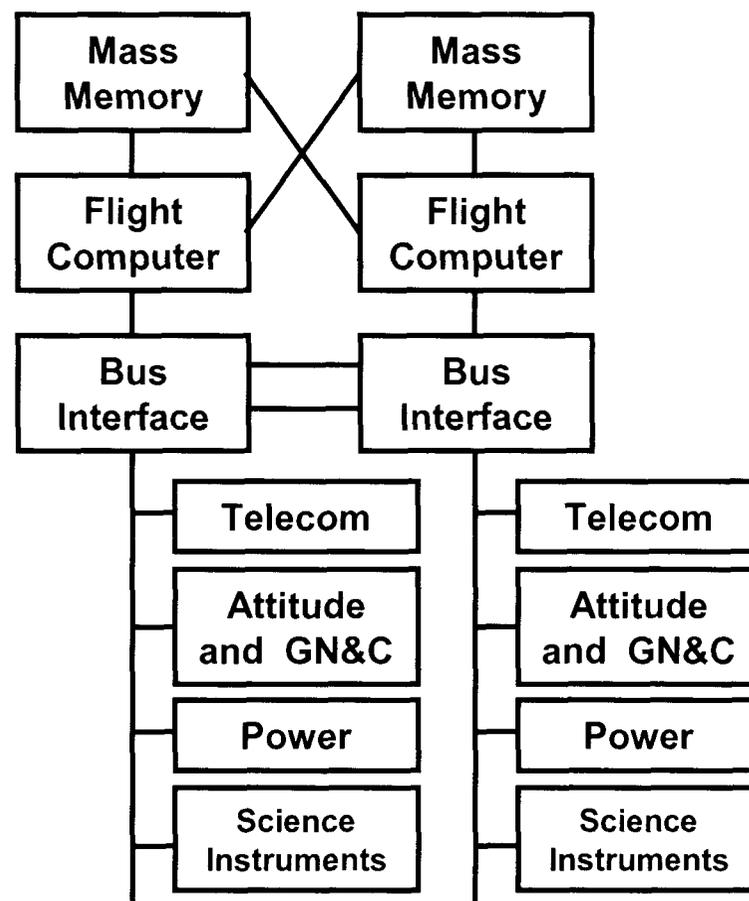


- Typical Dual-String Designs for Spacecraft

Point-to-Point Architecture



Bus-Based Architecture





Dependable Computing in New Generation of Deep Space Mission



- Characteristics of New Generation of Deep Space Missions:
 - Many missions focus on autonomous landers, rovers, sample return, etc.
 - Missions requirements are much more demanding:
 - Precision autonomous navigation, including Aero-Braking and Aero-Capture
 - Precision landing
 - Entry, Descent and Landing Hazard avoidance
 - Much higher processing requirements
 - Distributed processing
 - Much higher interface bandwidth requirements
 - Autonomous operation
 - High speed fault detection and recovery
 - The systems are physically smaller with higher functional density
 - Shrinking mission operation budget means smaller mission operations team
 - Must rely on on-board autonomous fault tolerance



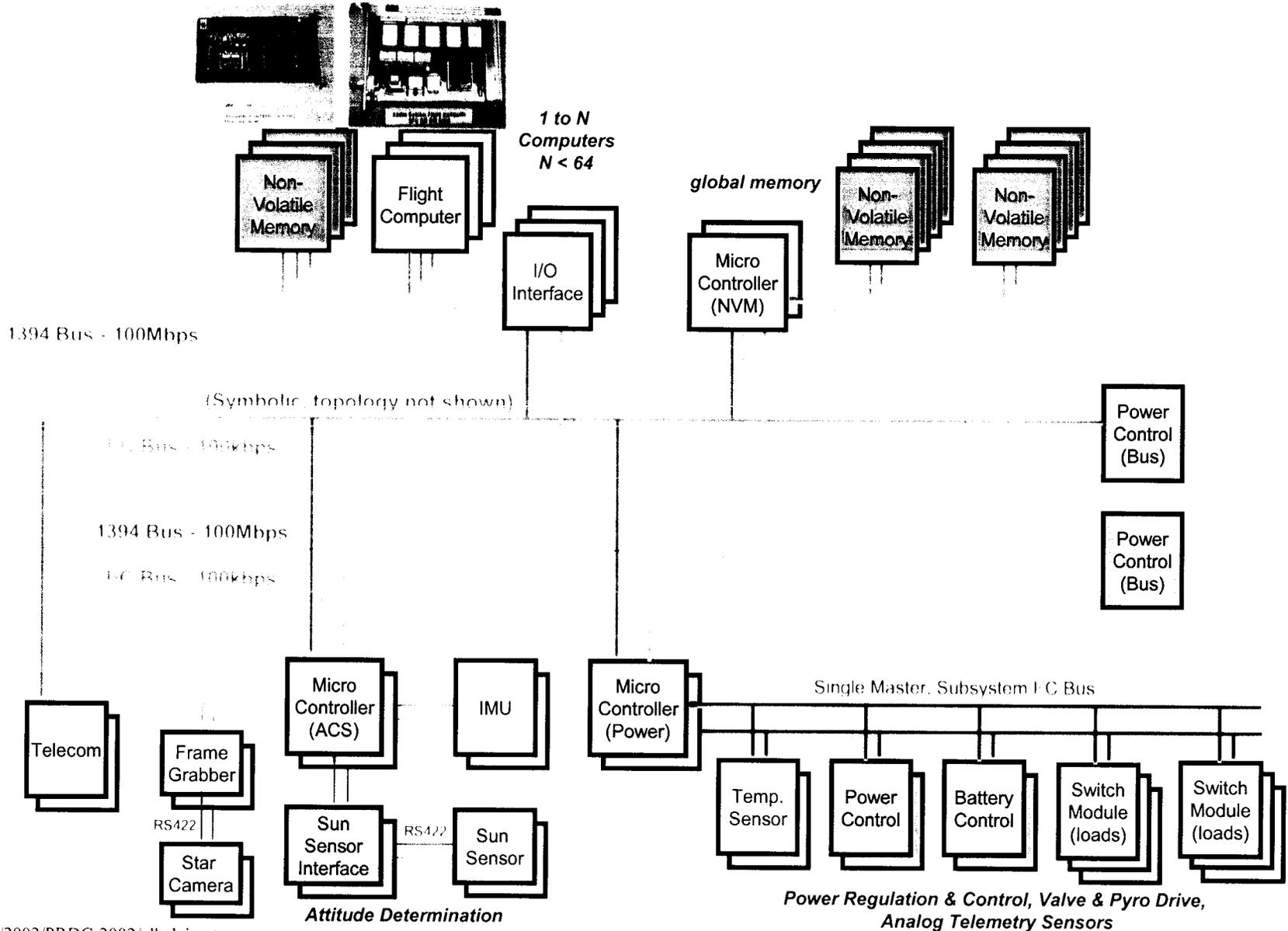
High-Performance Fault-Tolerant Bus Architecture Research at JPL



- Requirements for Distributed Processing, High Interface Bandwidth, and High Speed Fault Recovery Necessitate the Development of a High Speed Fault Tolerant Bus Architecture
- Commercial-Off-The-Shelf (COTS) Bus Standards Are Highly Desirable Because of Cost, Availability, and Performance Benefits.
- Two COTS Bus Standards Were Selected for the initial X2000 design:
 - the IEEE 1394 and I2C
- However, These COTS Buses Are Not Designed for the Highly Reliable Applications Such As Deep Space Missions. Therefore, the Focus of the Research is How to Achieve Highly Reliable Avionics Bus Architecture Using COTS Bus Standards

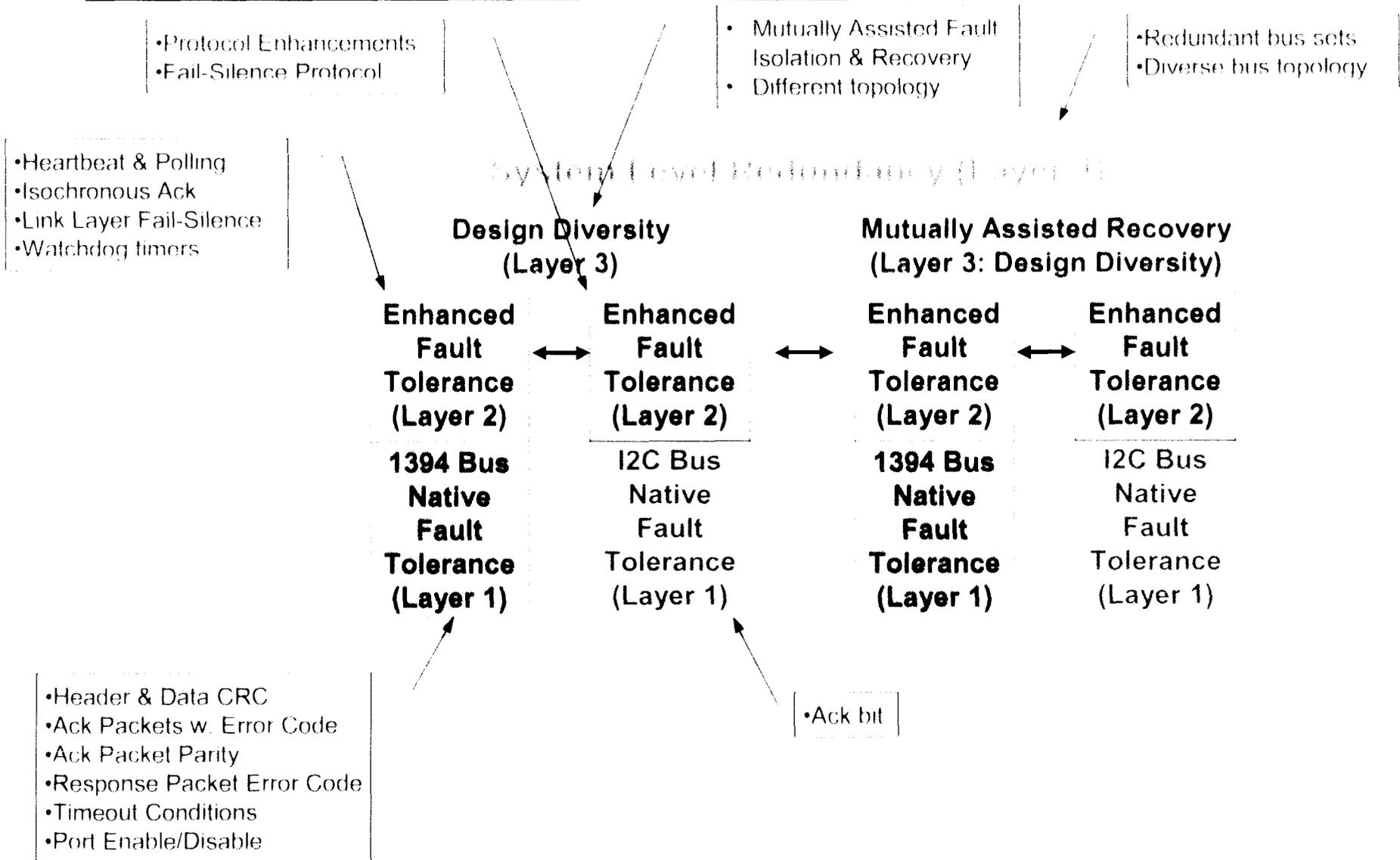


Baseline X2000 COTS Bus Architecture



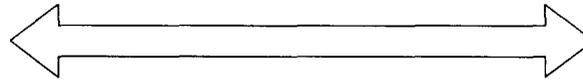


Multi-Layer Fault Tolerance Methodology for COTS-Based Bus Architecture





Design



Analysis

System Level Redundancy (Layer 4)

Design Diversity (Layer 3)

Design Diversity (Layer 3)

Enhanced Fault Tolerance (Layer 2)

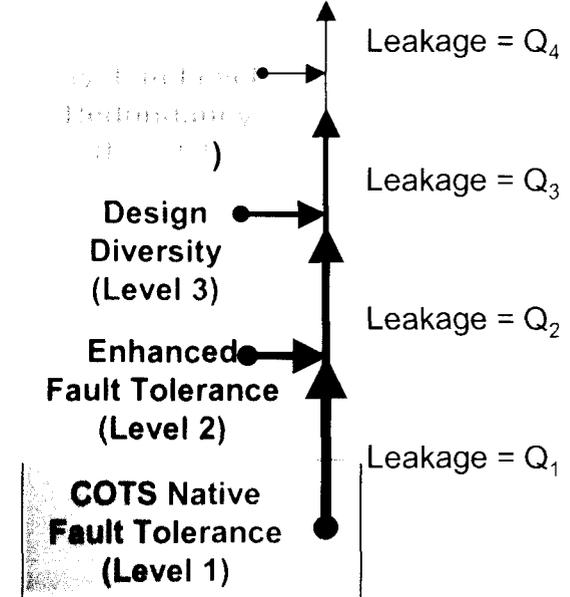
COTS # 1 Native Fault Tolerance (Layer 1)

COTS # 2 Native Fault Tolerance (Layer 1)

COTS # 1 Native Fault Tolerance (Layer 1)

COTS # 2 Native Fault Tolerance (Layer 1)

Fault propagation path



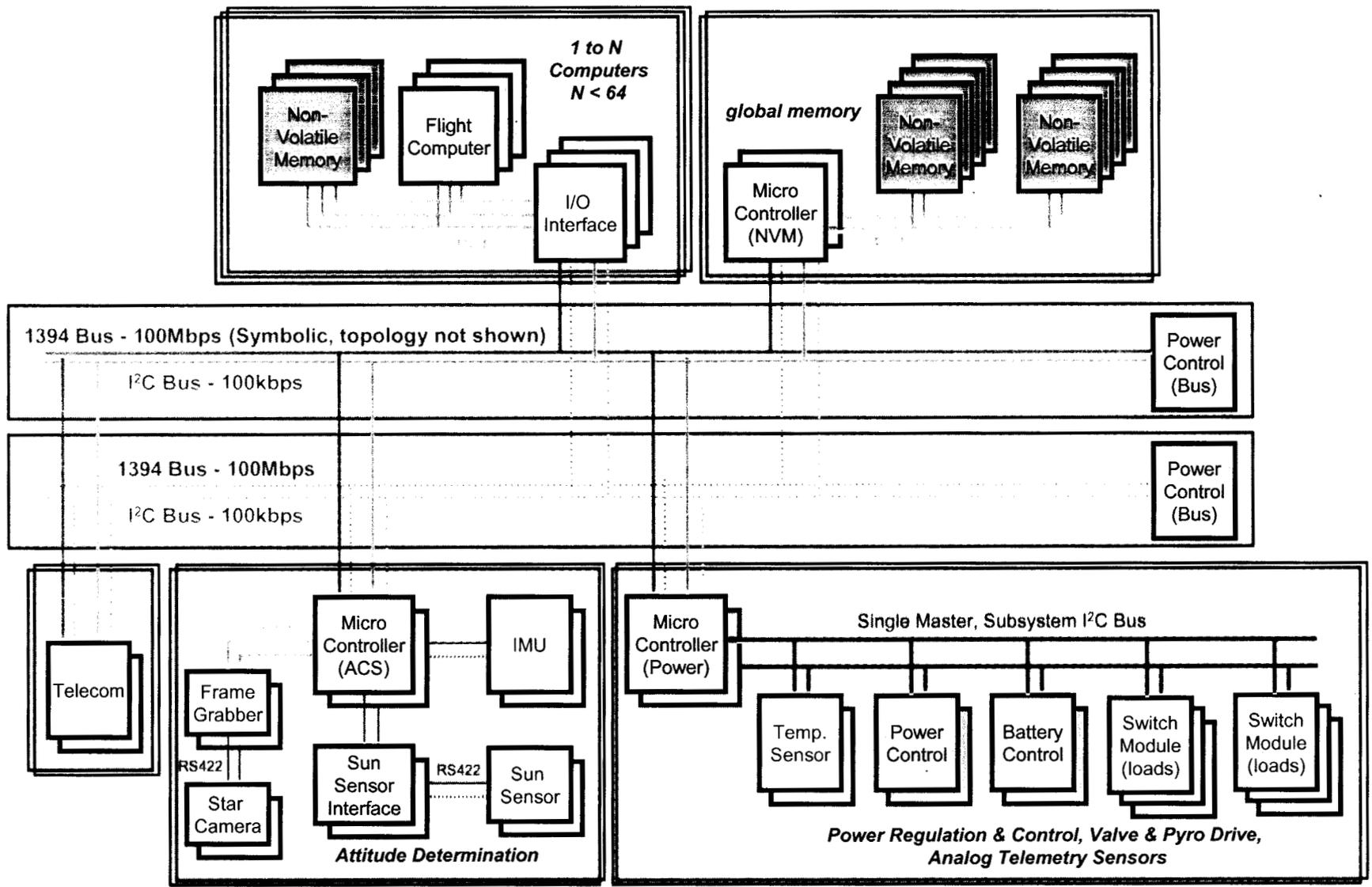
Fault Propagation Model of Multi-Layer Design

L. Alkalai, A. T. Tai, "Long-Life Deep-Space Applications," *Computer, IEEE*, Vol. 31, No. 4, IEEE Computer Society, April 1998, pp. 37-38.

S. Chau, L. Alkalai, and A. T. Tai, "The Analysis of Multi-Level Fault-Tolerance Methodology for Applying COTS in Mission-Critical Systems," in Proceedings of the *IEEE Workshop on Application-Specific Software Engineering and Technology (ASSET'2000)*, Dallas, TX, March 2000.



X2000 Fault Containment Regions

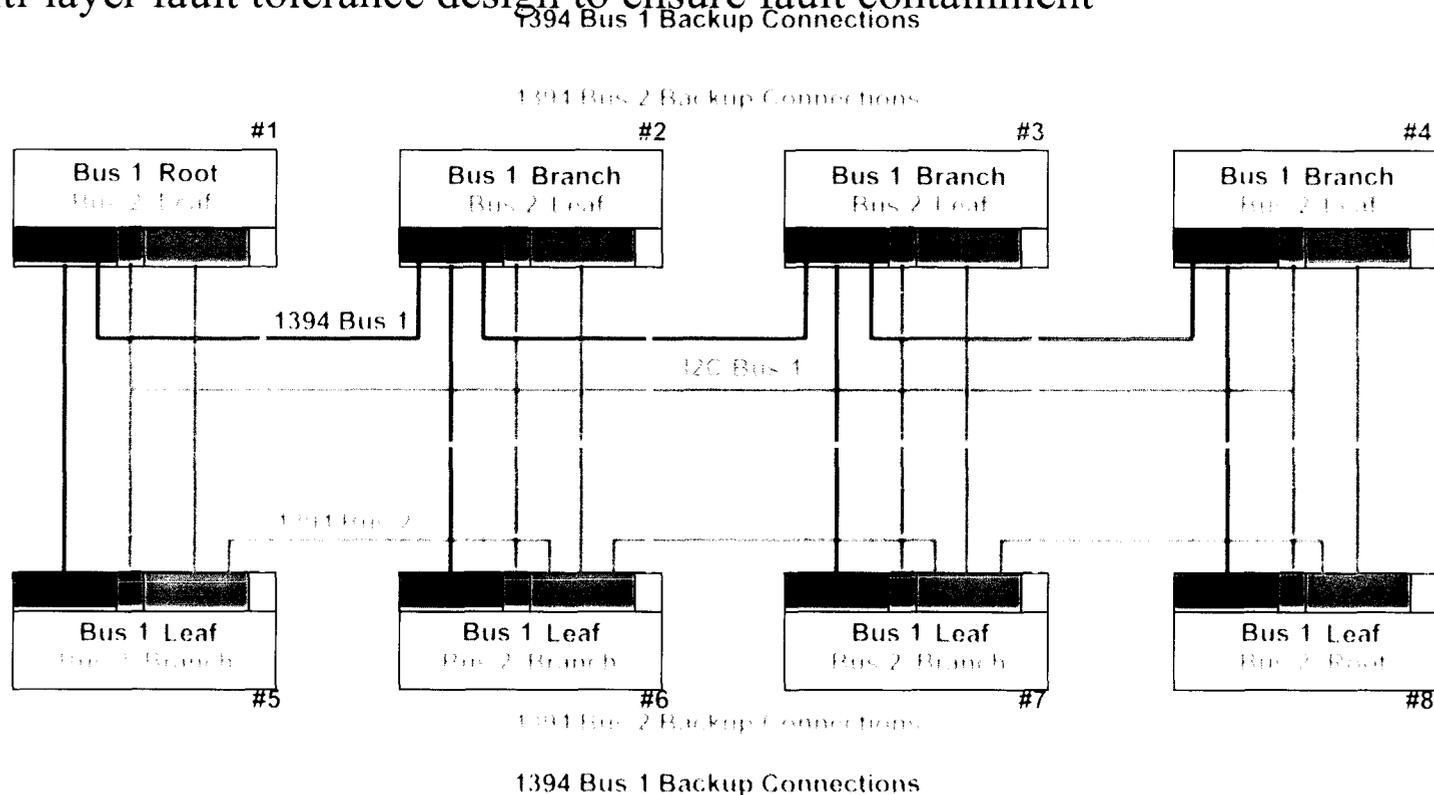




A Highly Reliable Distributed Network Architecture for Future Missions



- Support distributed computing
- Rich set of redundant interconnections
- Multi-layer fault tolerance design to ensure fault containment



L. Alkalai, S. Chau, A. Tai, J.B. Burt, "The Design of a Fault-Tolerant COTS-Based Bus Architecture," *Proceedings of 1999 Pacific Rim International Symposium On Dependable Computing (Prdc'99)*, Hong Kong, China December 16-17, 1999. Also, *IEEE Trans. Reliability*, Vol. 48, December 1999, pp. 351-359.

A. Tai, S. Chau, L. Alkalai, "COTS-Based Fault Tolerance in Deep Space: Qualitative and Quantitative Analyses of A Bus Network Architecture" will appear in proceedings of *HASE 99: Fourth IEEE International Symposium on High Assurance System Engineering*, Washington DC Metropolitan Area, November 17-19, 1999.



Realization of Multi-Level Fault Protection Methodology

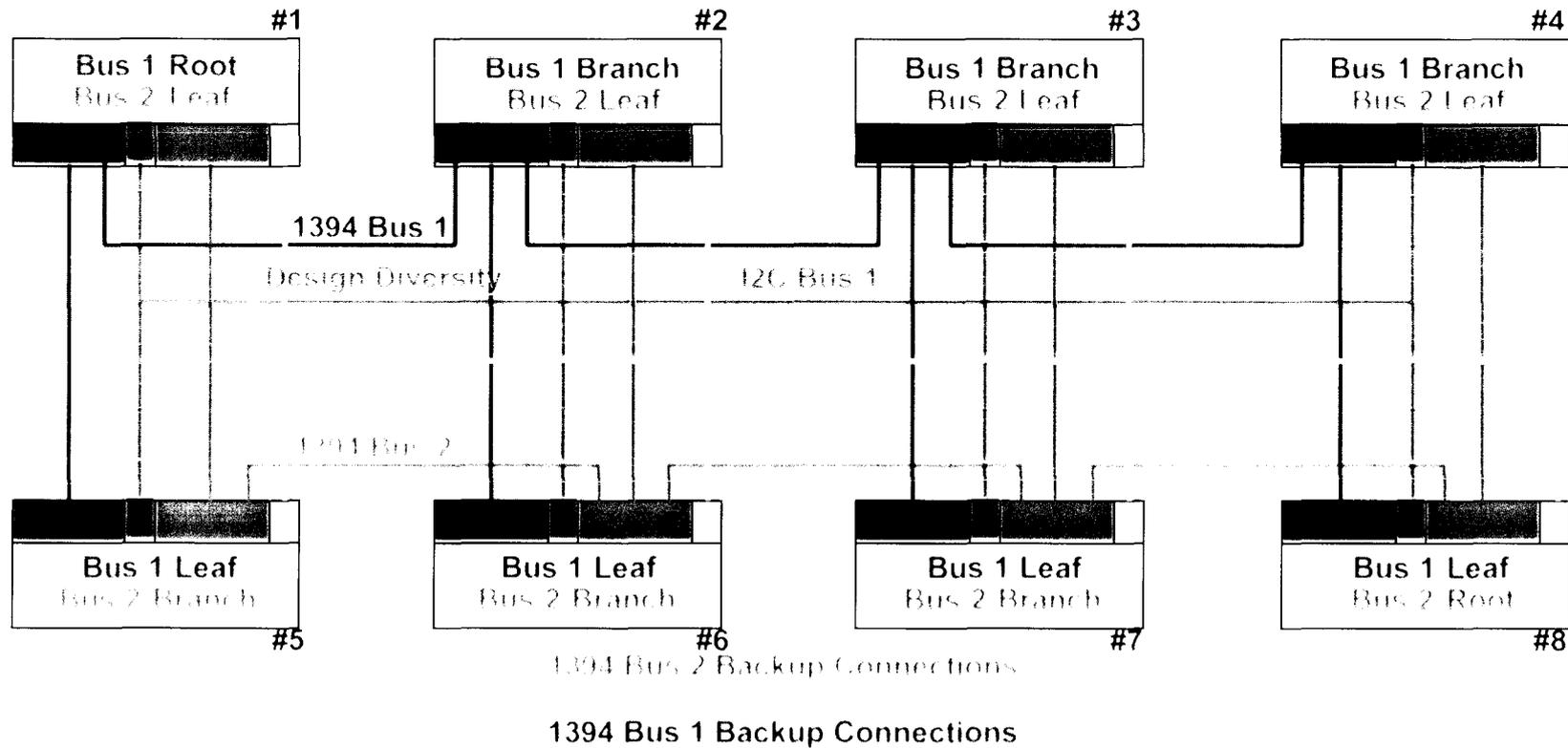


Cable IEEE 1394 has a tree topology

Enhanced Fault Tolerance
(An Example)

1394 Bus 1 Backup Connections

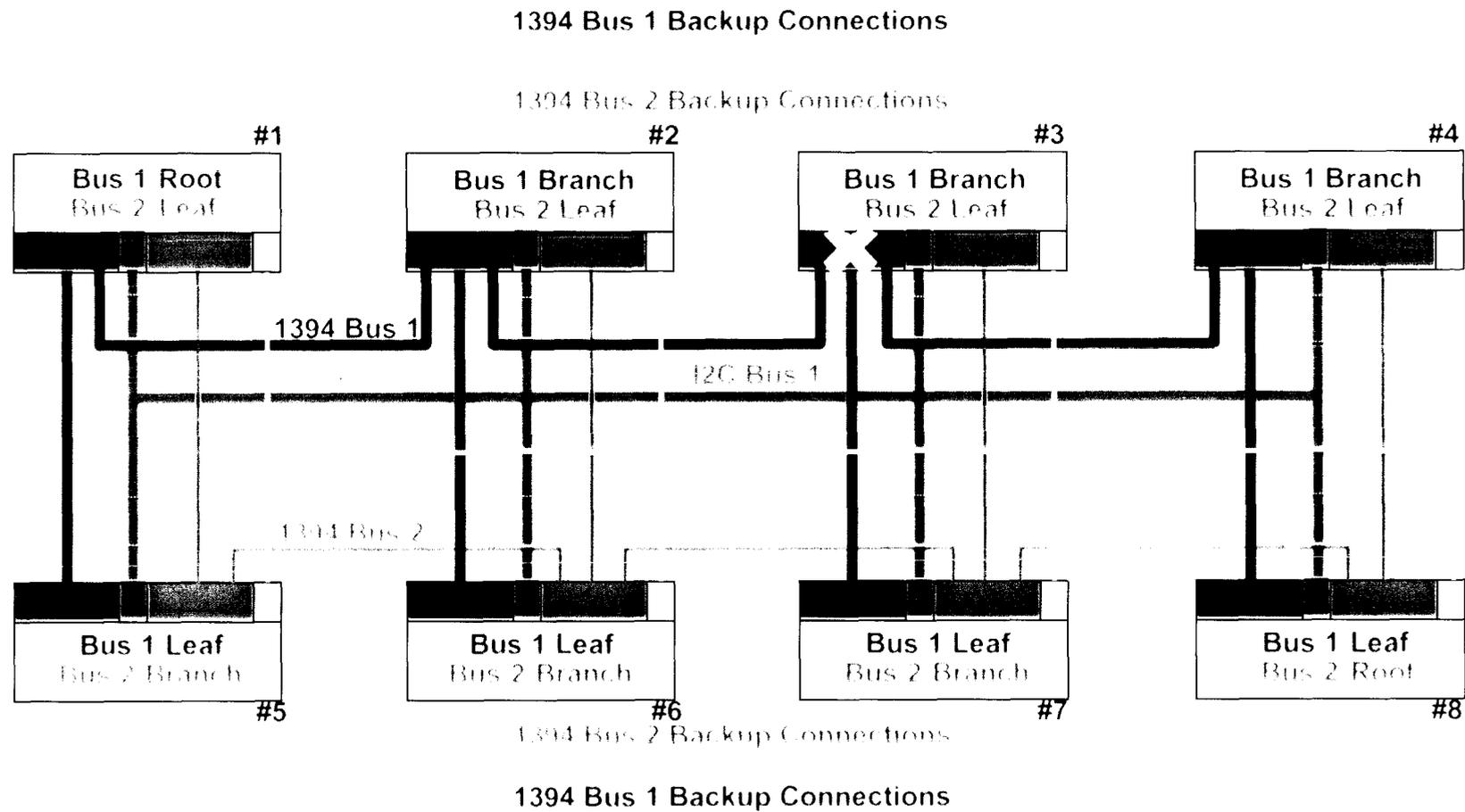
1394 Bus 2 Backup Connections



System Level Redundancy with Diverse Topology

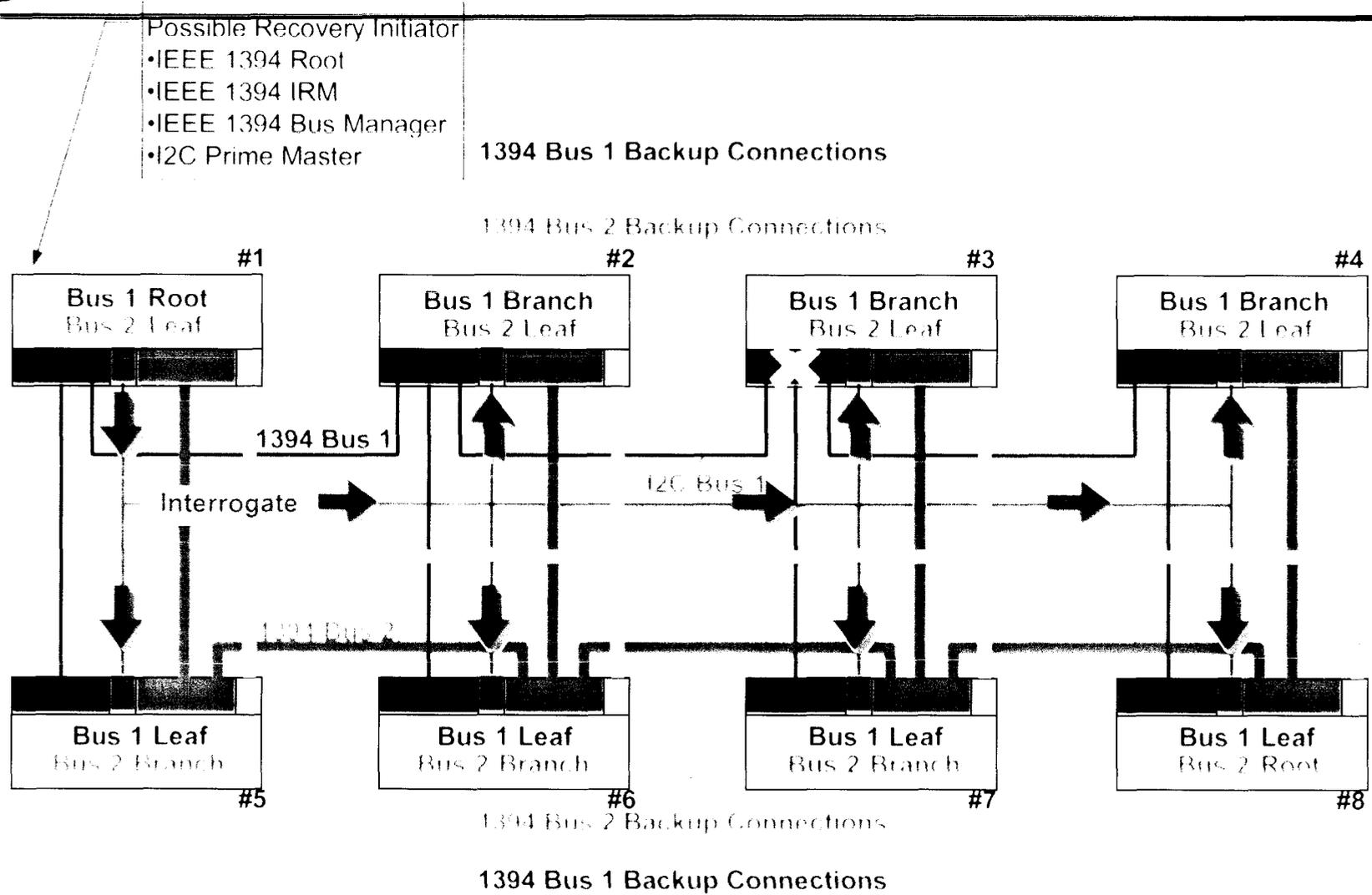


X2000 Fault Protection Strategy



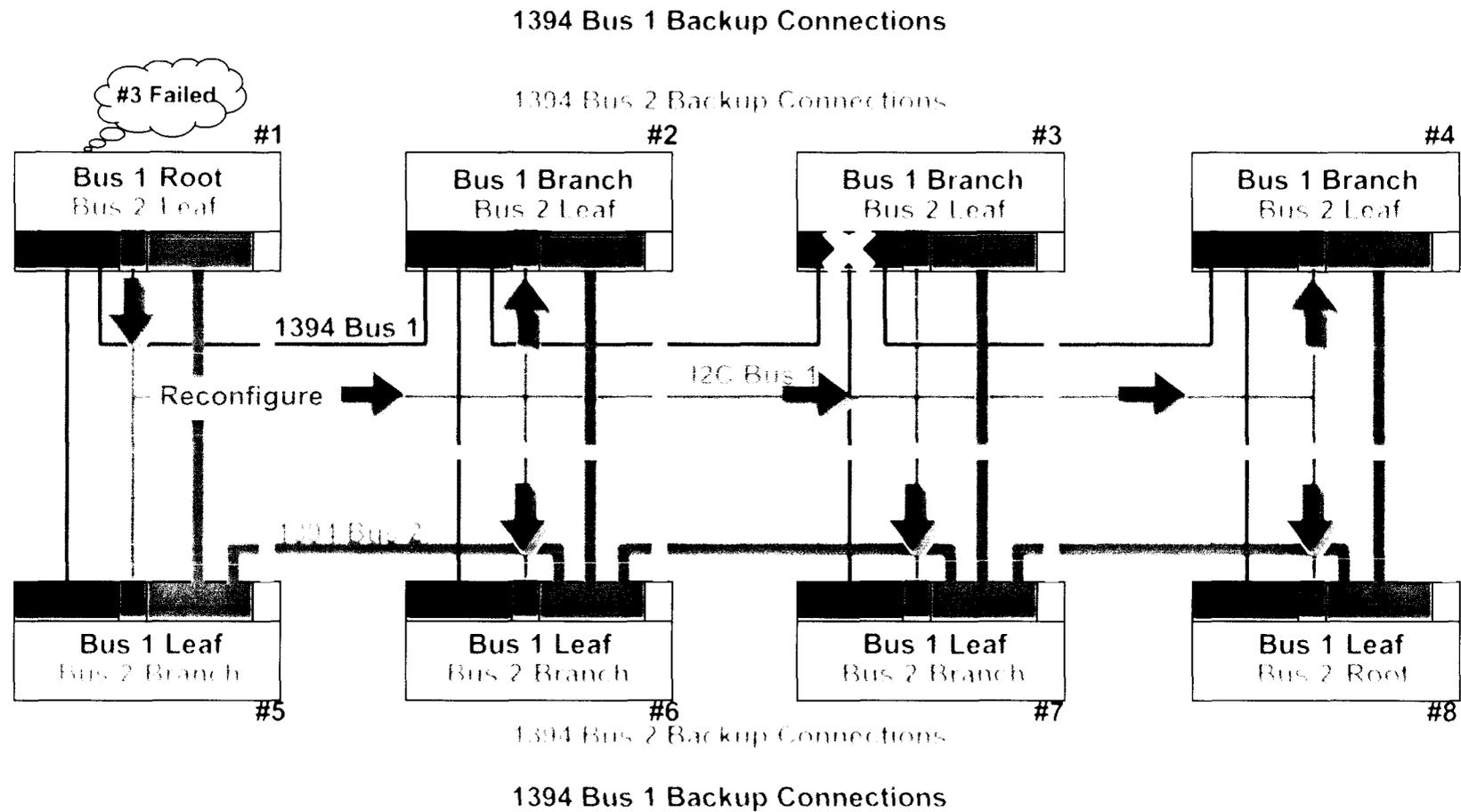


X2000 Fault Protection Strategy



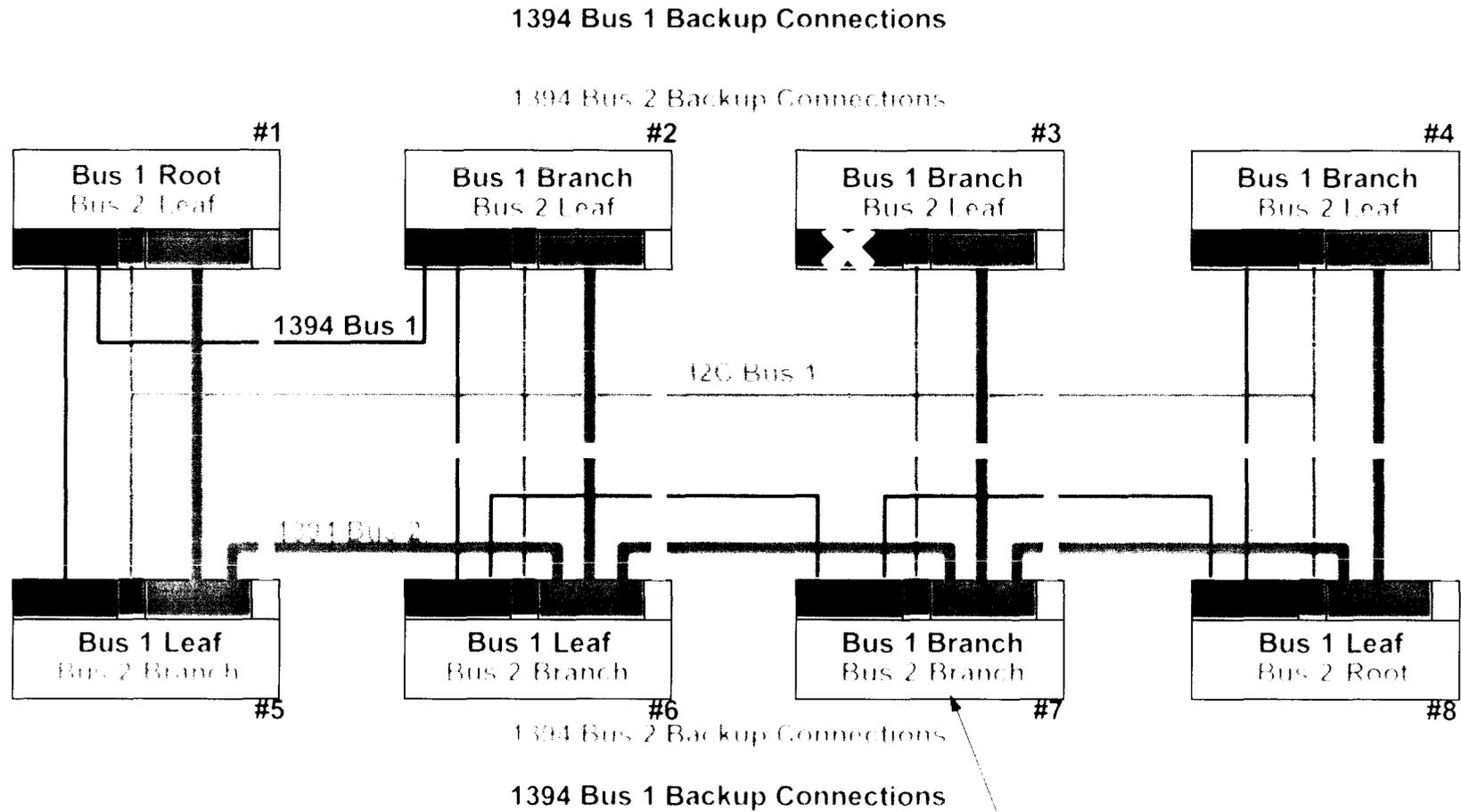


X2000 Fault Protection Strategy





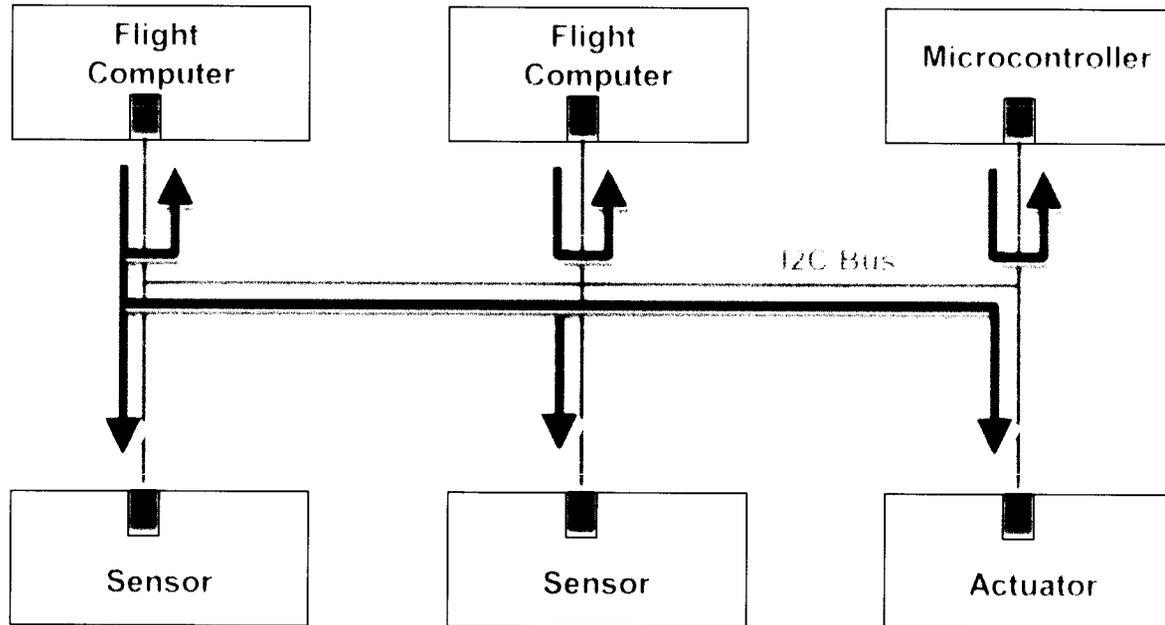
X2000 Fault Protection Strategy



Next fault recovery needs repair before bus switching if this node fails

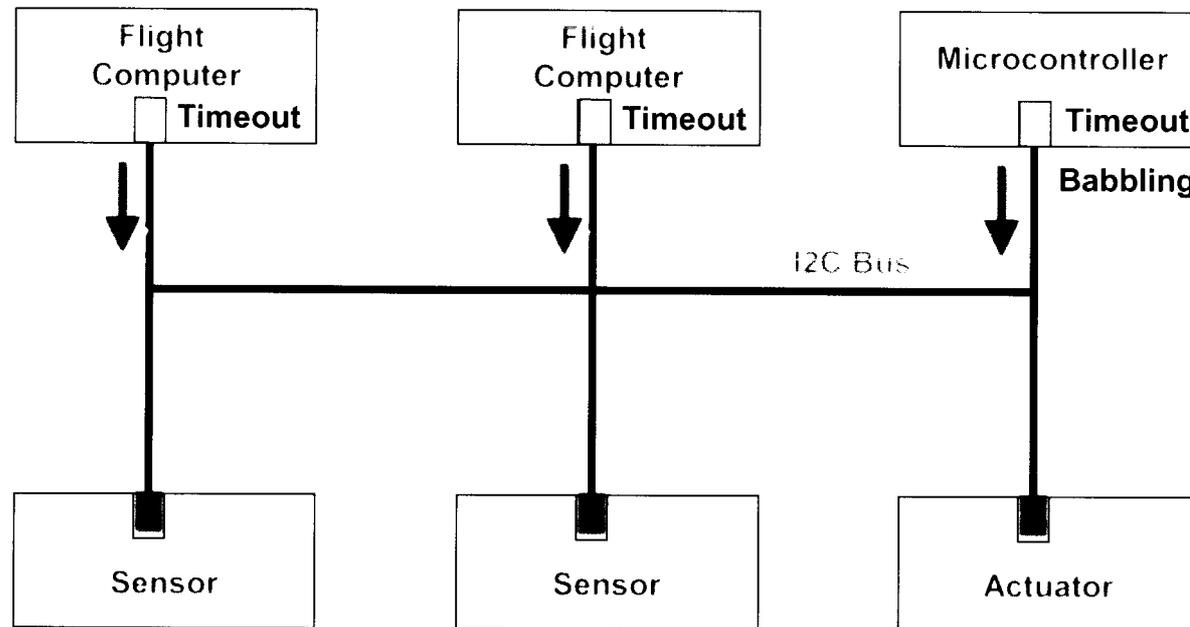


FC Bus Fault Protection: Fail Silence



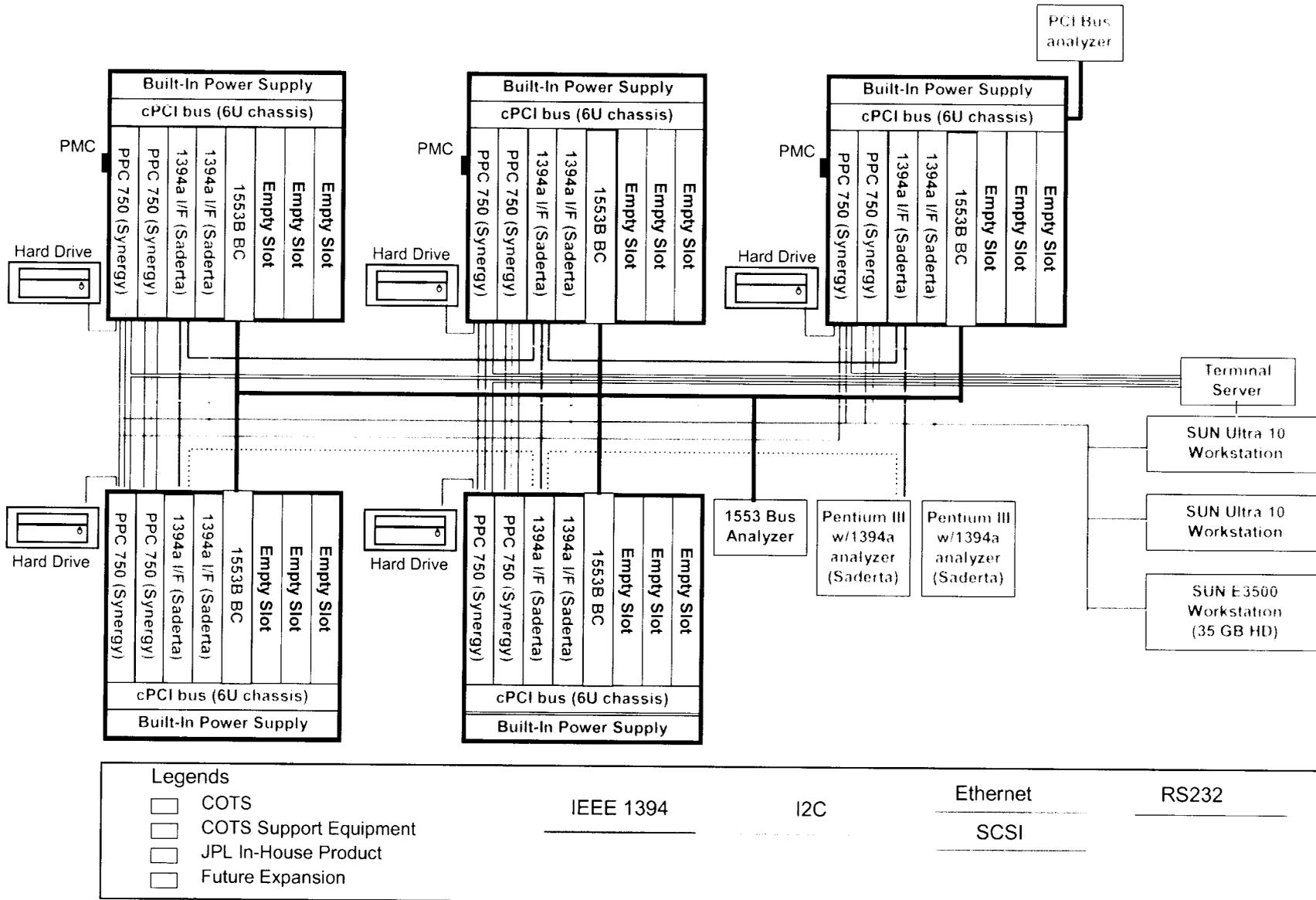


I²C Bus Fault Protection: Fail Silence





Architecture Testbed Configuration





Example of Fault Injection in IEEE 1394 Bus



Fault Injected in the Gap Count Register in the IEEE 1394 Bus
University of Illinois, Urbana Champaign



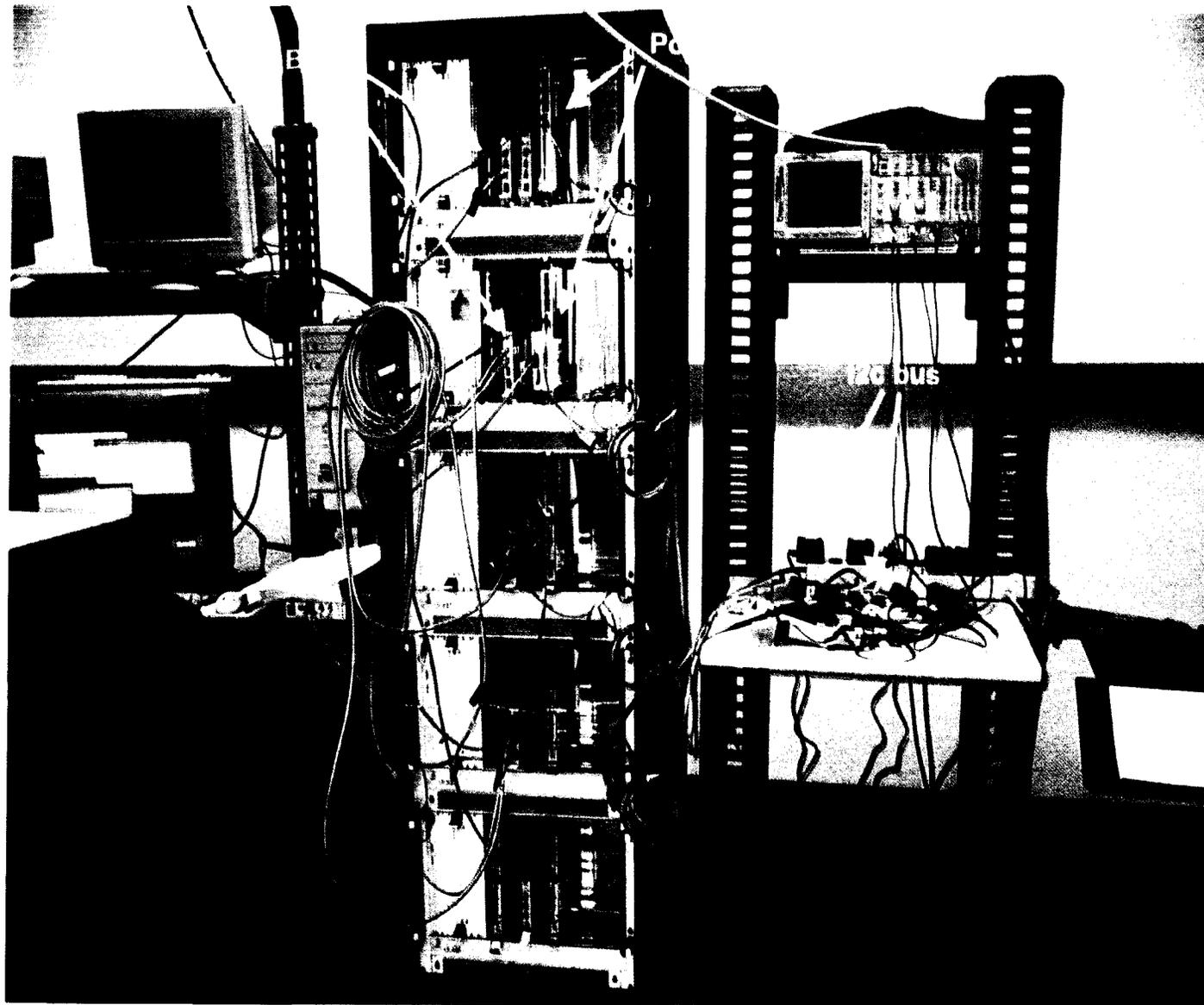
Before Fault Injection



After Fault Injection



Distributed Flight Computer Testbed





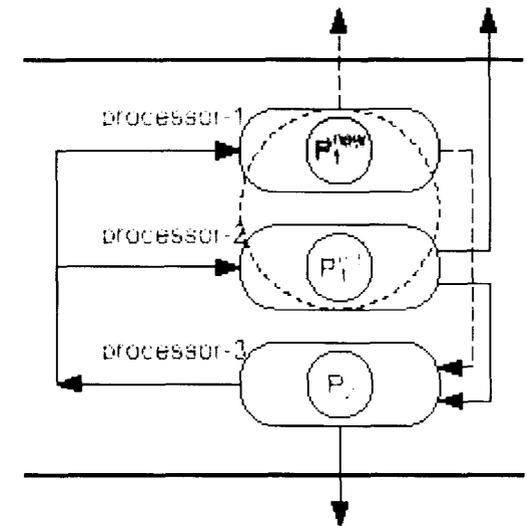
Guarded Software Upgrade



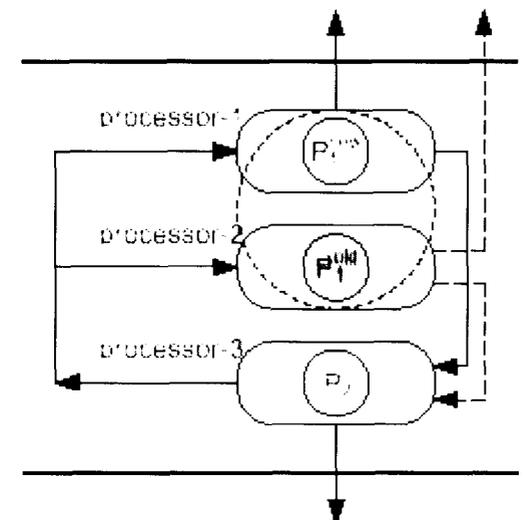
- **Motivation:**
 - Flight software for long life deep space missions have to be upgraded periodically to correct design bugs or due to change of mission phases
 - Unprotected software upgrades have previously caused severe and costly damage to space missions and critical applications
- **Objectives:**
 - Update flight software without System Reboot
 - Fall back to previous version of the software if failures occur during the upgrade
- **Approach:**
 - Use the old version of the software to “guard” the new version during the transition
 - Turn over the control to the new software only when the right level of confidence is reached

A. Tai, K. S. Tso, L. Alkalai, S. N. Chau, and W. H. Sanders, "On low-cost error containment and recovery methods for guarded software upgrading," in Proceedings of the *20th International Conference on Distributed Computing Systems (ICDCS 2000)*, Taipei, Taiwan, April 2000, pp. 548-555.

A. T. Tai, K. S. Tso, L. Alkalai, S. Chau, and W. H. Sanders, "On the effectiveness of a message-driven confidence-driven protocol for guarded software upgrading," in Proceedings of the *4th IEEE International Computer Performance and Dependability Symposium (IPDS 2000)*, Schaumburg, IL, March 2000.



(a) Onboard Validation Stage



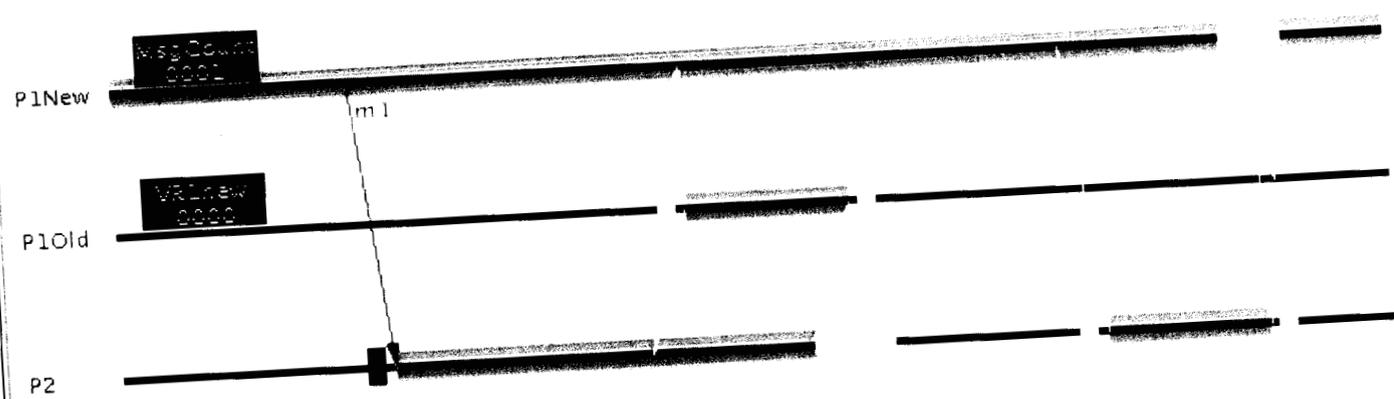
(b) Guarded Operation Stage



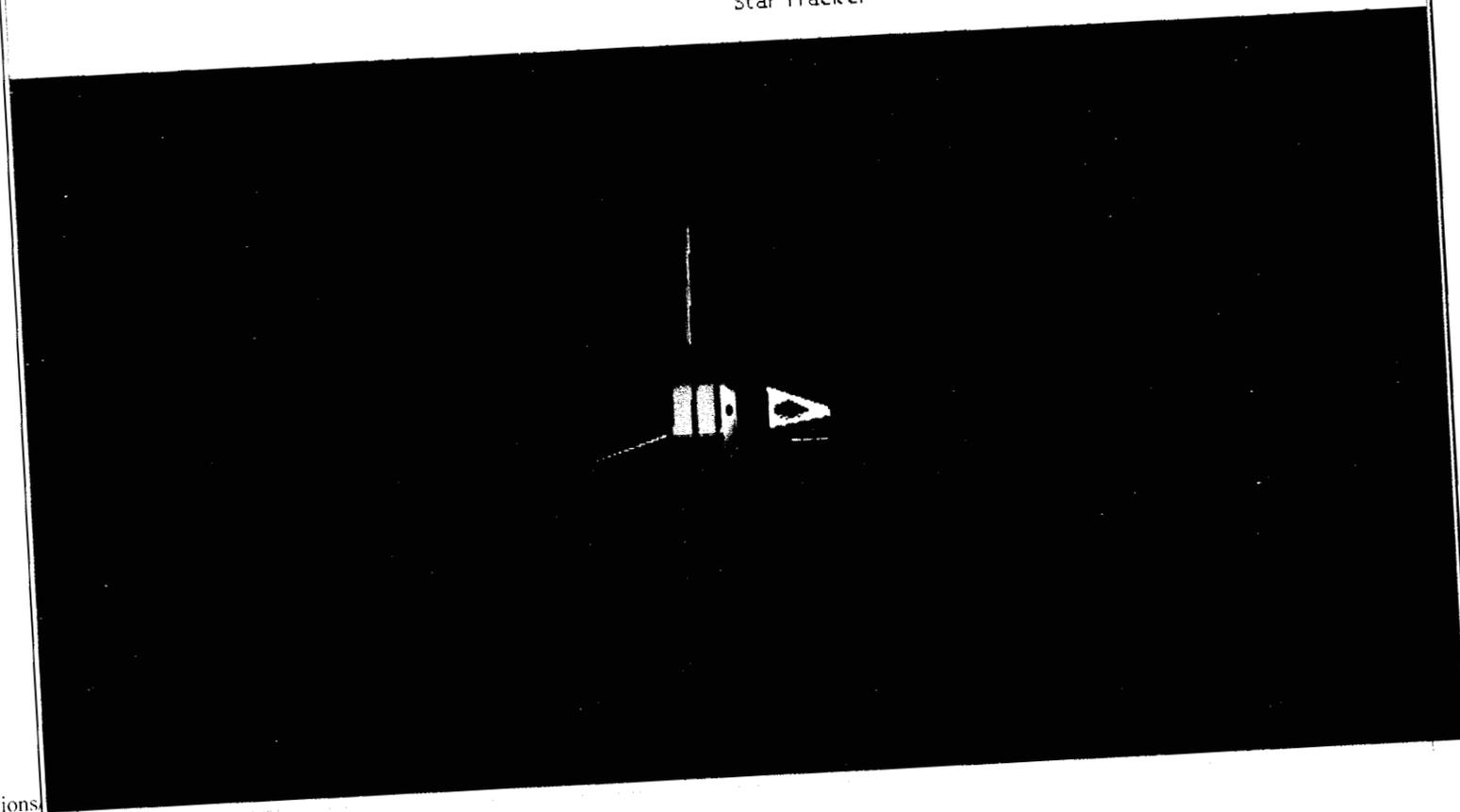
MDCD Graphical User Interface

File Execution

Thruster

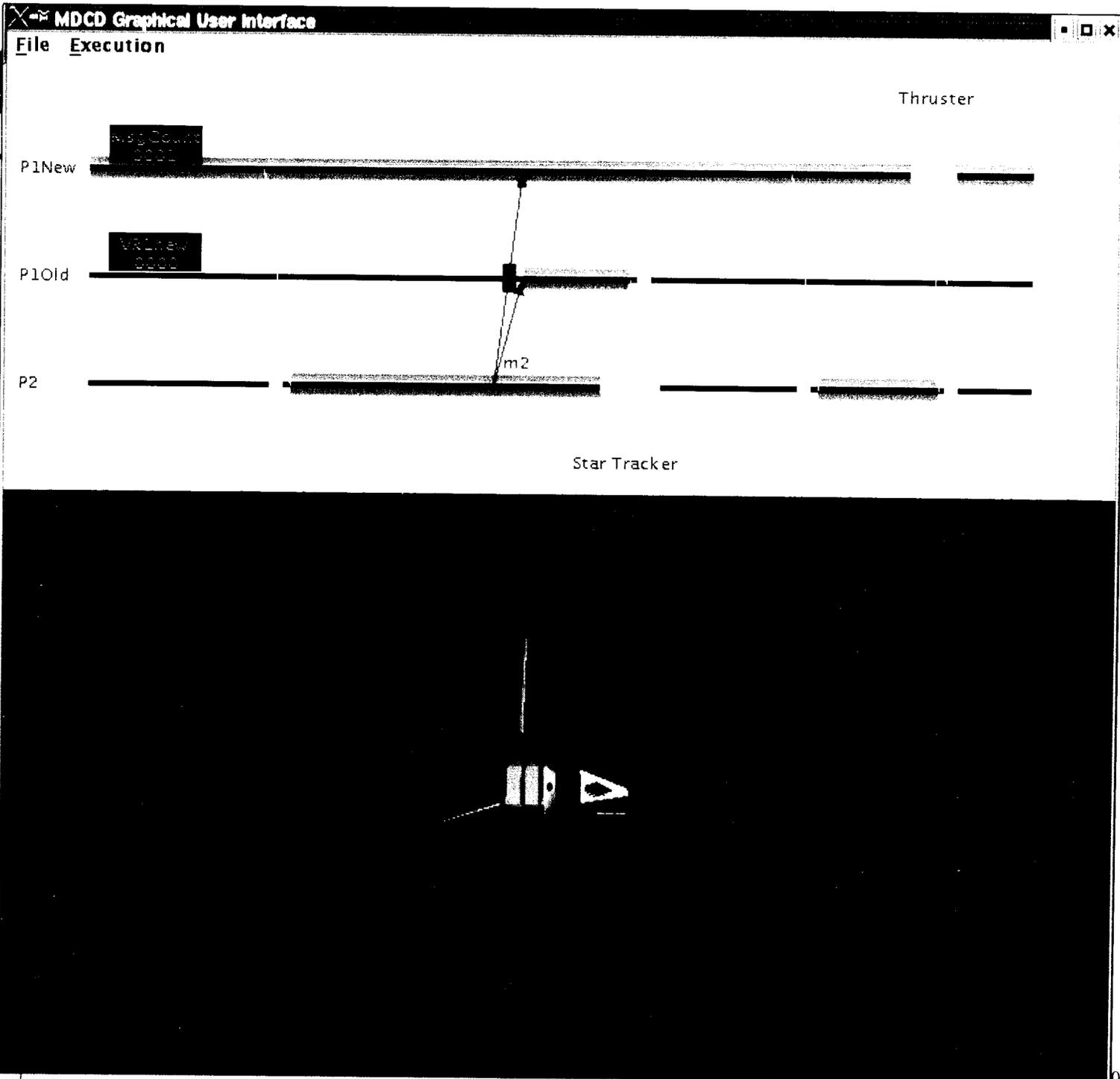


Star Tracker



JPL

002, Japan



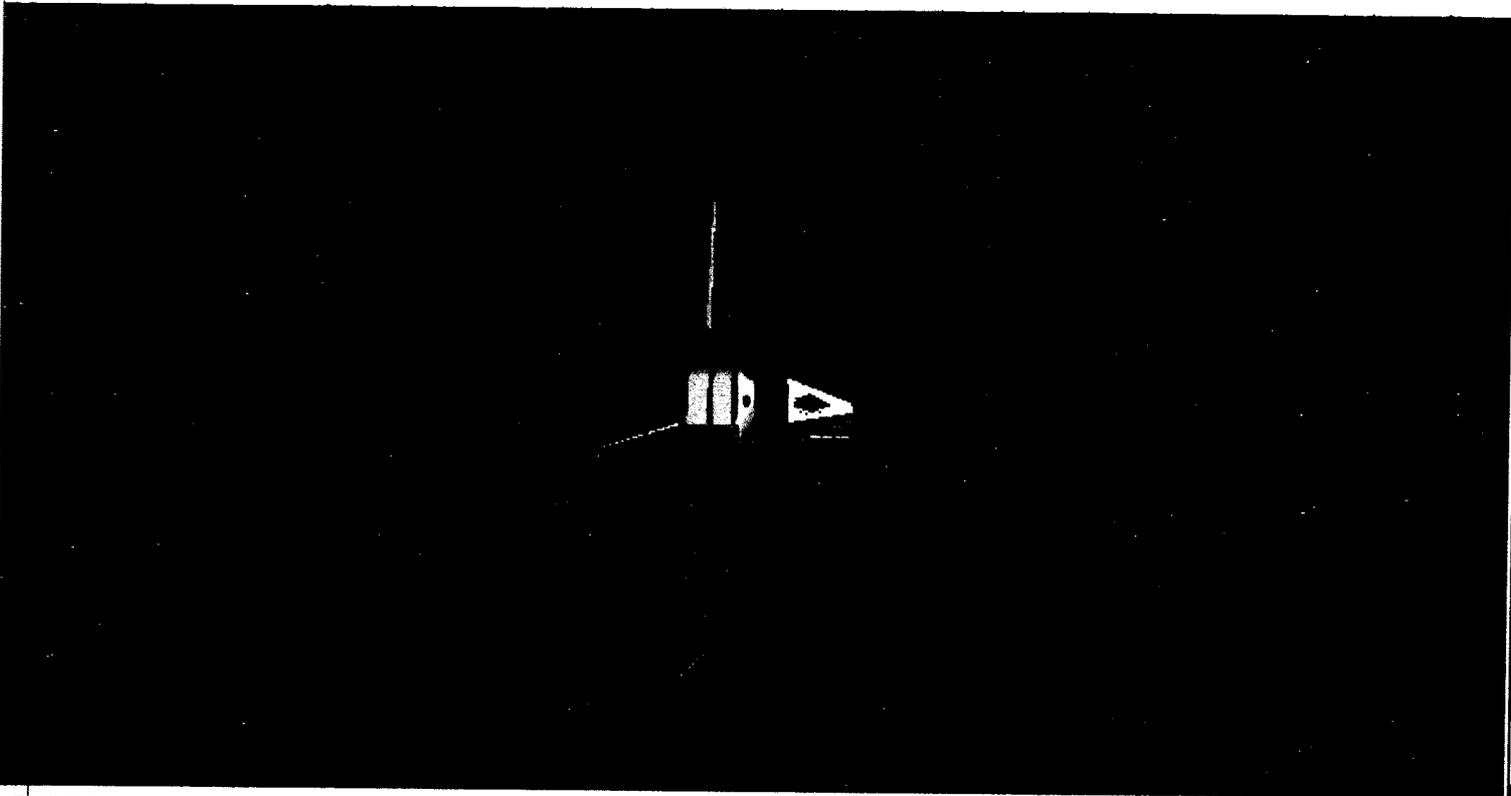
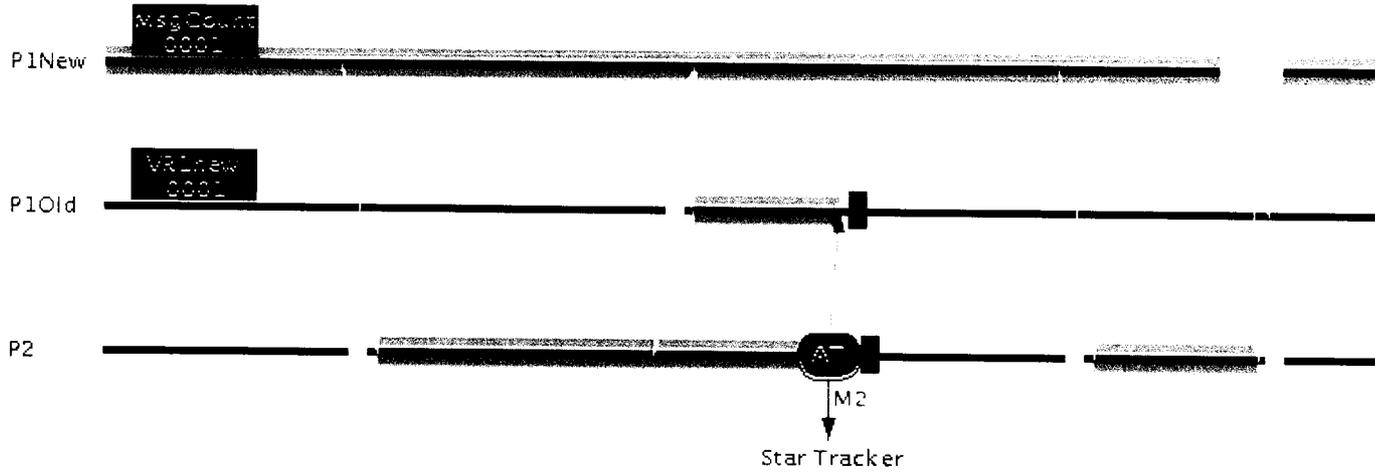
JPL



MDCD Graphical User Interface

File Execution

Thruster





MDCD Graphical User Interface

File Execution

Thruster

P1New

P1Old

P2

Star Tracker





MDCD Graphical User Interface

File Execution

Thruster M1

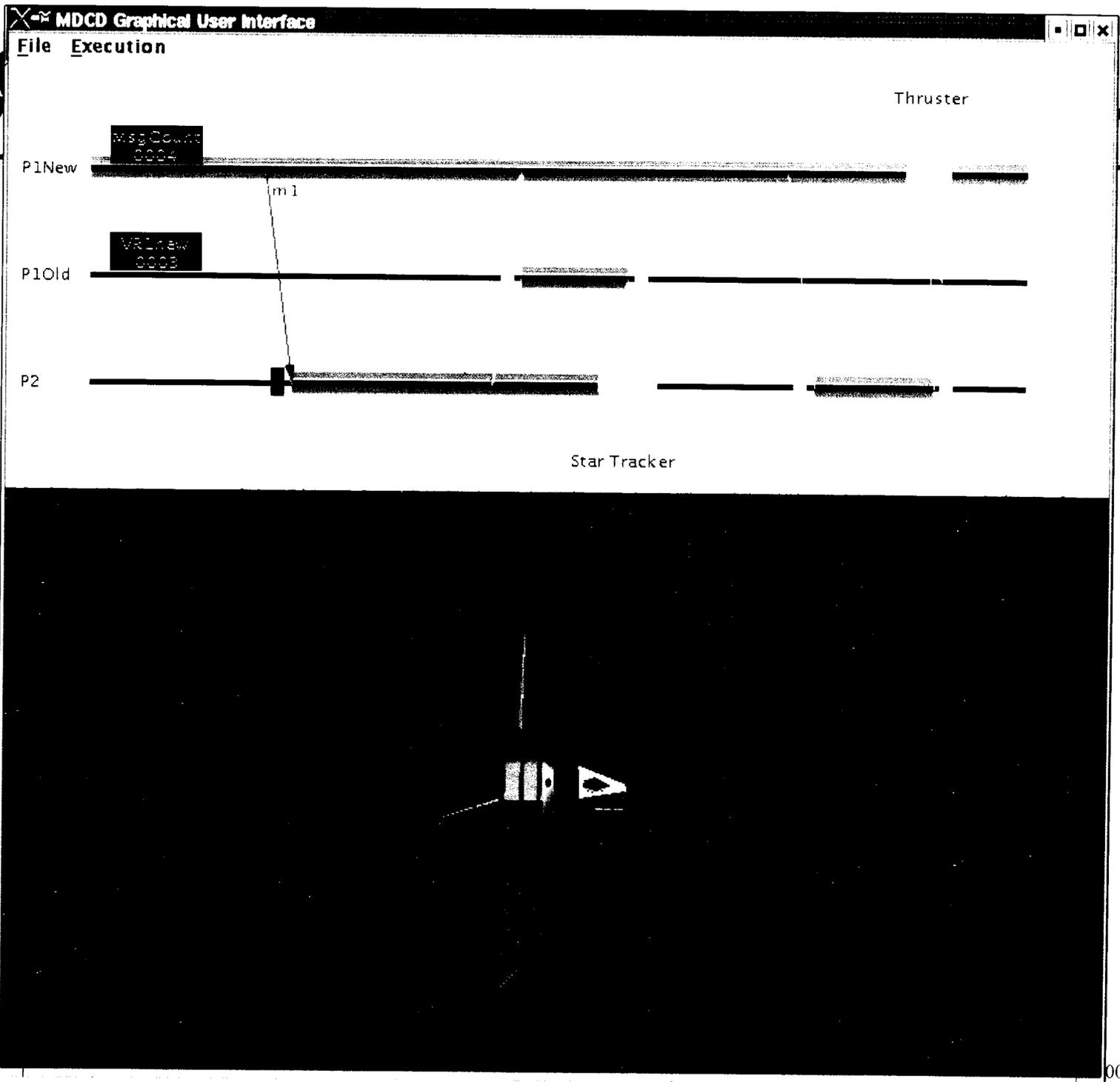
P1New

P1Old

P2

Star Tracker





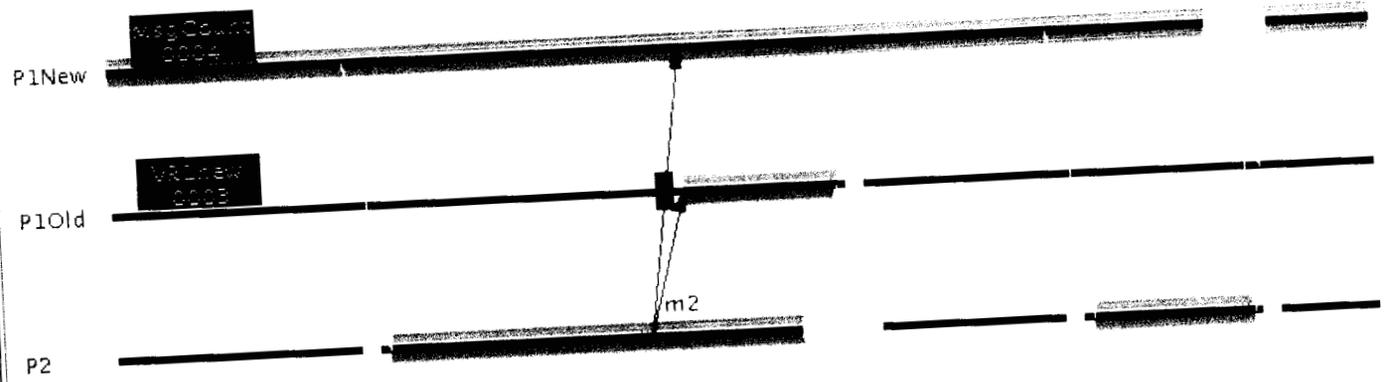
JPL



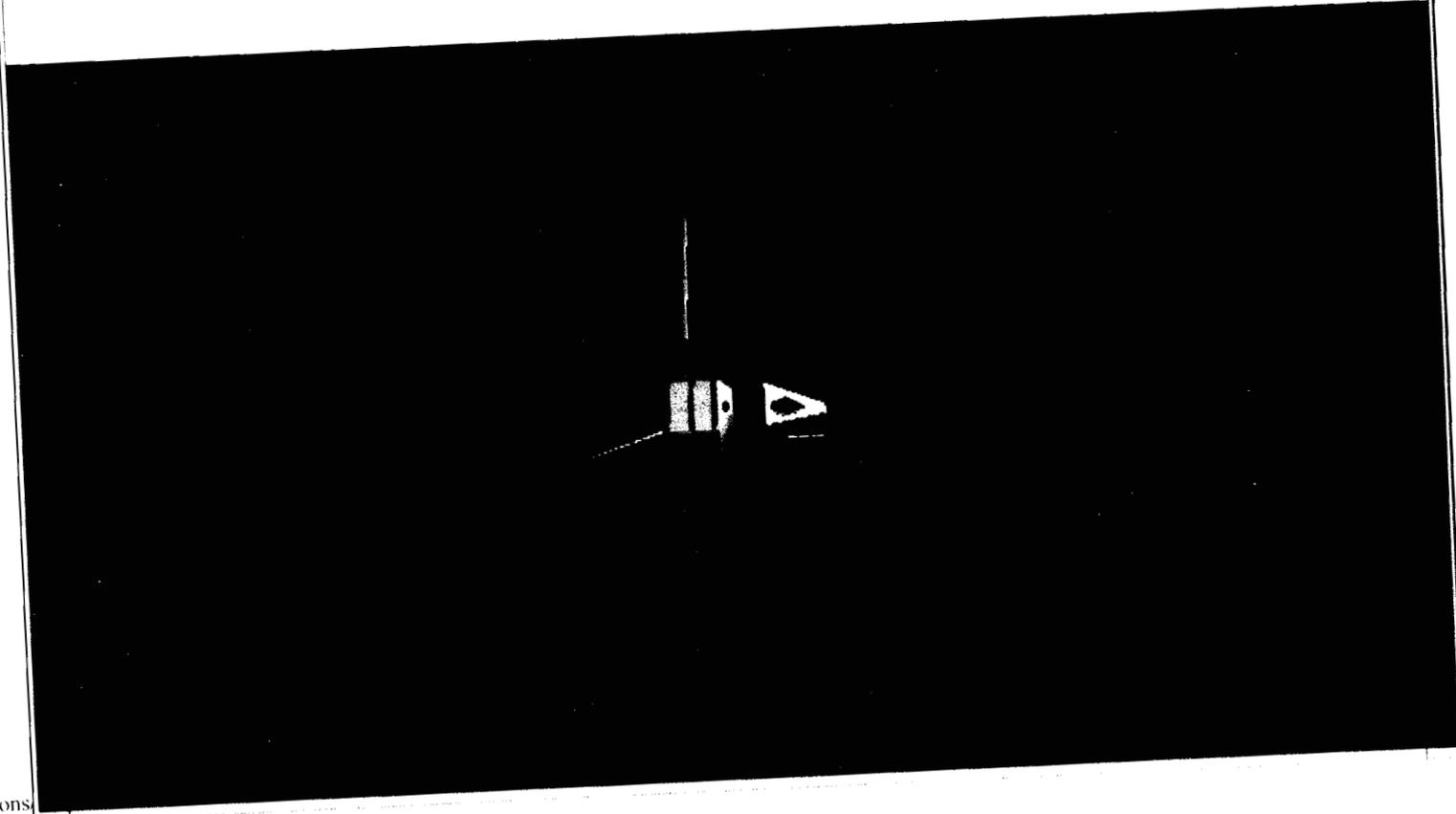
MDCD Graphical User Interface

File Execution

Thruster



Star Tracker



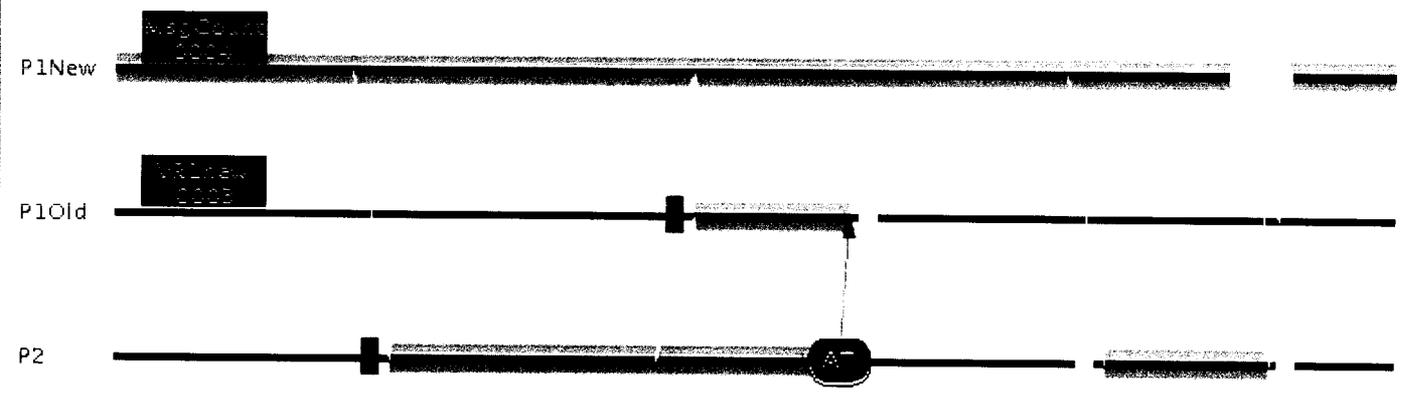
JPL



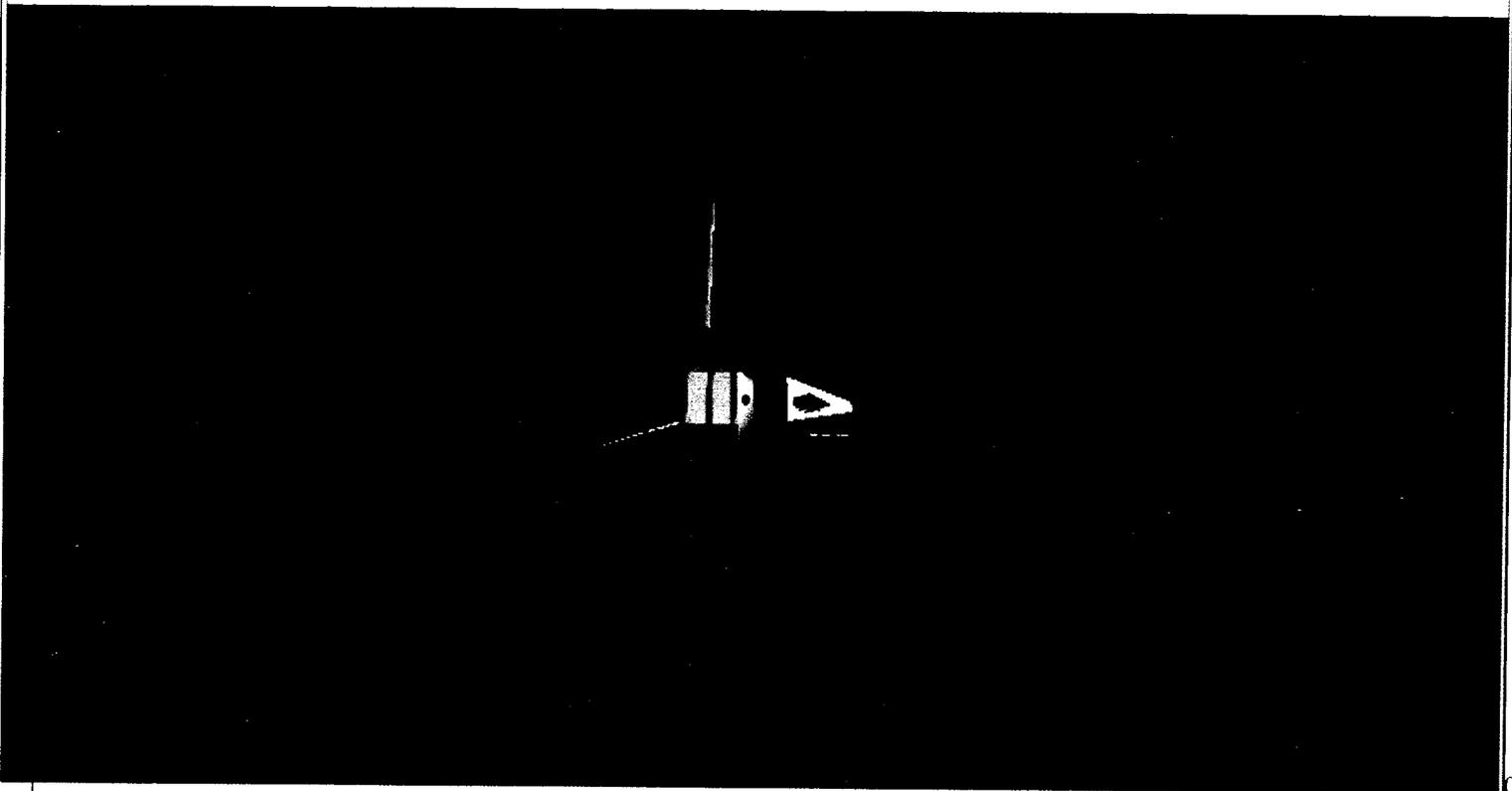
MDCD Graphical User Interface

File Execution

Thruster



Star Tracker





MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

m1

Star Tracker

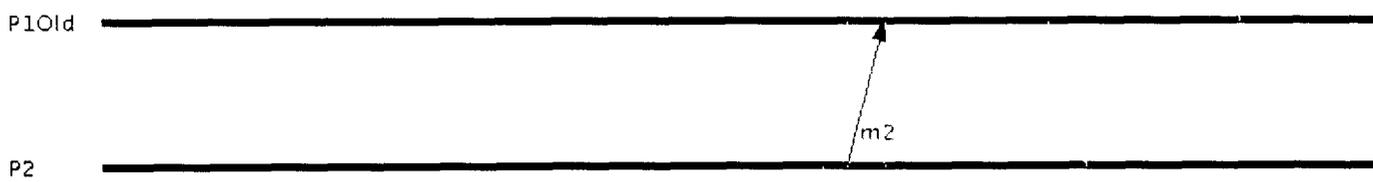




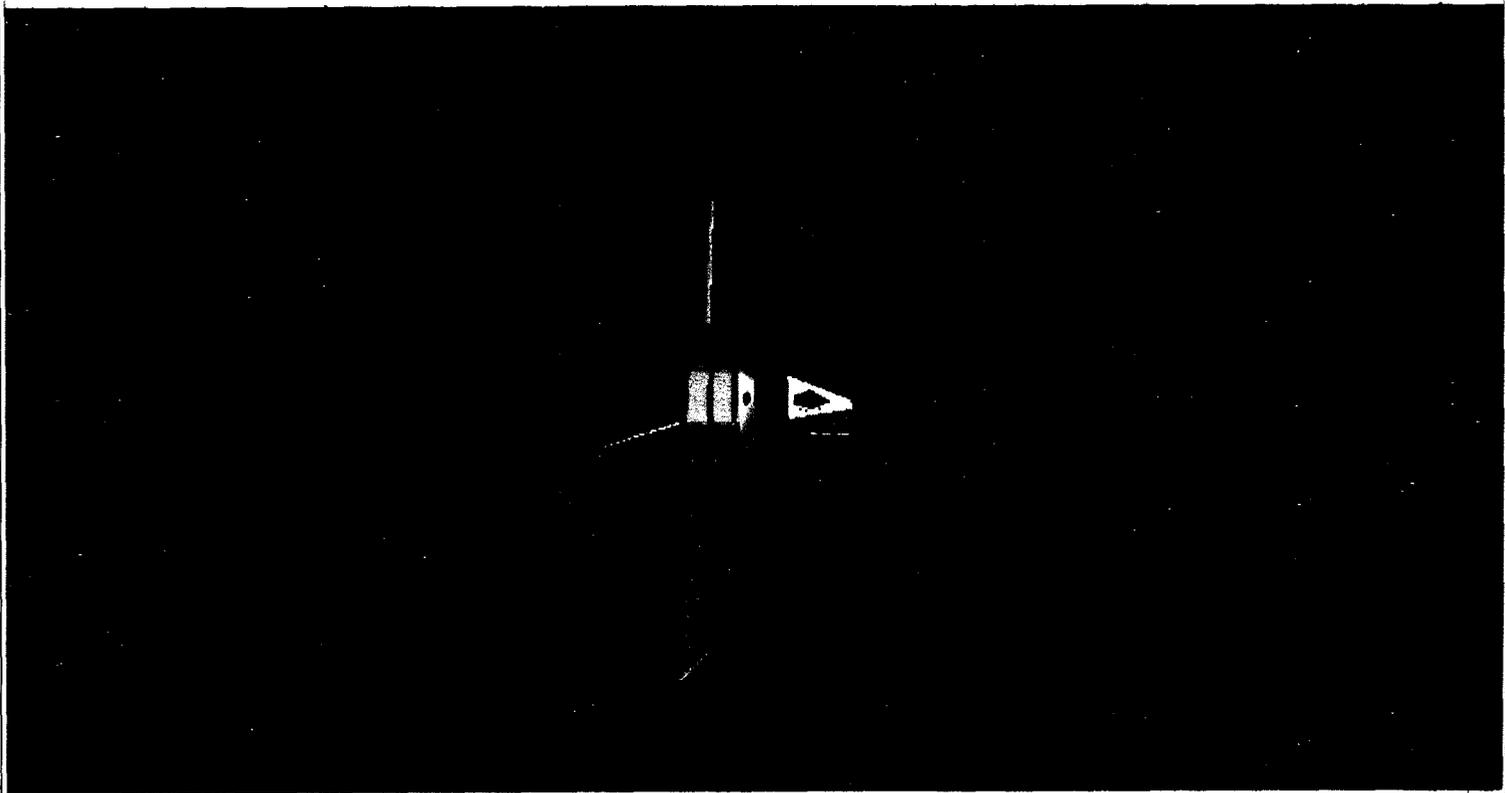
MDCD Graphical User Interface

File Execution

Thruster



Star Tracker



JPL



MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

M2

Star Tracker





MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

m3

Star Tracker





MDCD Graphical User Interface

File Execution

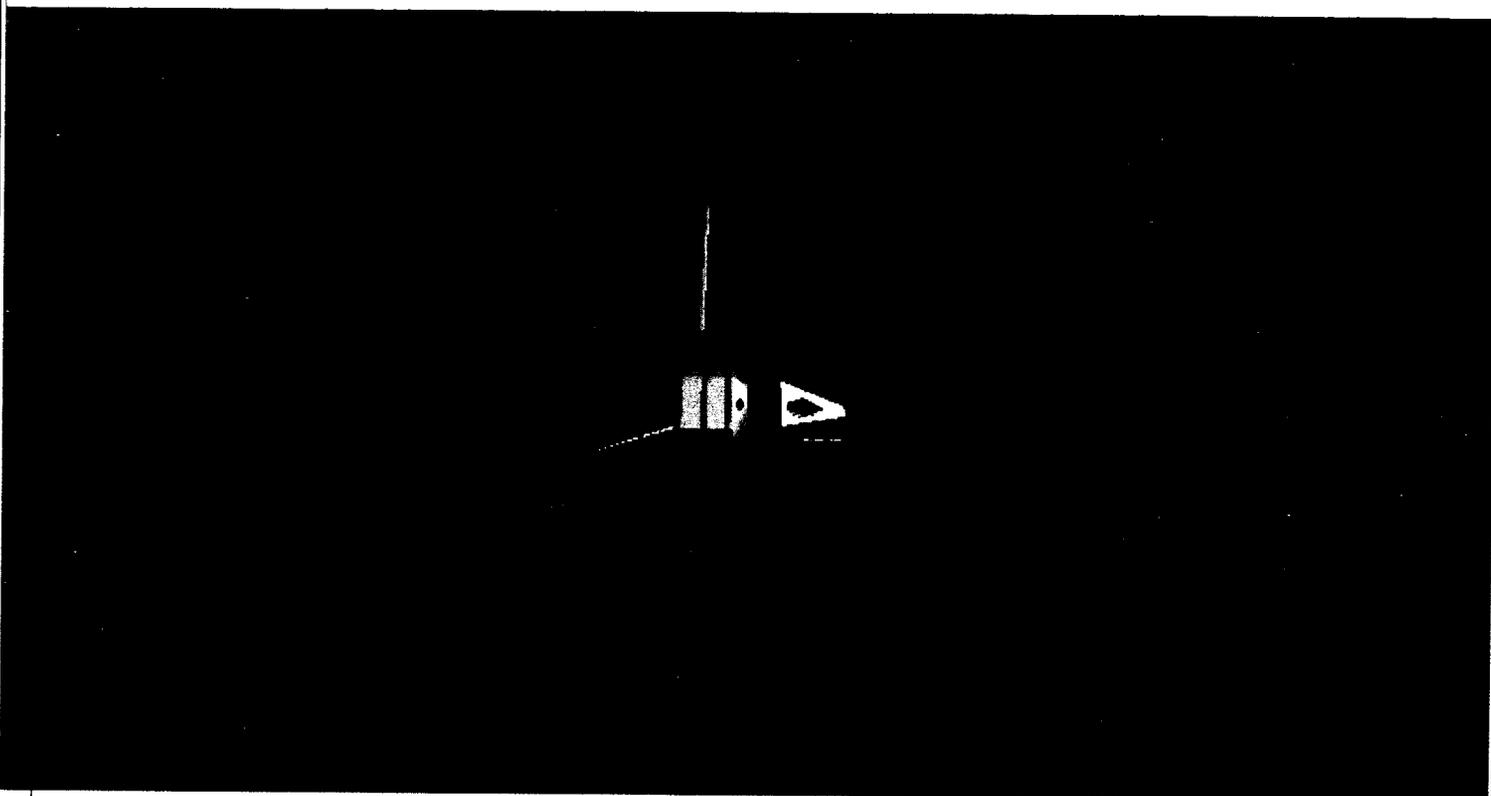
Thruster

M1

P1Old

P2

Star Tracker



JPL



MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

m1

Star Tracker





MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

m2

Star Tracker





MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

M2

Star Tracker





MDCD Graphical User Interface

File Execution

Thruster

P1Old

P2

m3

Star Tracker

JPL



MDCD Graphical User Interface

File Execution

Thruster

M 1

P1Old

P2

Star Tracker

JPL



- Characteristics of Future Deep Space Missions:
 - Future Space Exploration Missions are ambitious:
 - Precision navigation control for spacecraft aerobraking and aerocapture
 - Precision entry-descent-landing with hazard avoidance
 - Highly autonomous operations
 - Long-duration missions in extreme environments
 - Miniaturized systems for sample returns, ascent vehicles, mobile units, etc.
 - Distributed surface science - network science - constellations of spacecraft
 - Formation flying (e.g., interferometry missions)
 - These missions require a new look at high performance dependable computing
 - Distributed processing among multiple spacecraft, and within a spacecraft
 - High performance computing and power efficient computing that supports long-life, high availability of systems
 - Autonomous, on-board fault-detection, isolation and repair
 - Fault adaptation
 - A framework for using COTS for the design of future, highly reliable systems



References

- “COTS-Based Fault Tolerance in Deep Space: Qualitative and Quantitative Analyses of a Bus Network Architecture,” in *Proceedings of the 4th IEEE International Symposium on High Assurance Systems Engineering*, Washington D.C., Nov 1999
- “Design of a fault-tolerant COTS-based bus architecture, ” *IEEE Trans. Reliability*, vol. 48, pp. 351-359, Dec. 1999
- “The design of a fault-tolerant COTS-based bus architecture,” *Pacific Rim International Symposium on Dependable Computing*, Hong Kong, China, Dec. 1999
- "The Implementation of a COTS Based Fault Tolerant Avionics Bus Architecture", in the *Proceedings of the Aerospace 2000 Conference*, Big Sky, Montana, Mar. 2000
- "COTS-based fault tolerance in deep space: A case study on IEEE 1394 application," *International Journal of Reliability, Quality and Safety Engineering*, vol. 9, June 2002.
- “A design-diversity based fault-tolerant COTS avionics bus network,” in *Proceedings of the Pacific Rim International Symposium of Dependable Computing (PRDC 2001)*, Seoul, Korea, Dec. 2001.

Note: Some of these references can be found in <http://www.ia-tech.com/obm/>



References

- "On the effectiveness of a message-driven confidence-driven protocol for guarded software upgrading," *Performance Evaluation*, vol. 44, pp. 211-236, Apr. 2001.
- "Low-cost error containment and recovery for onboard guarded software upgrading and beyond," *IEEE Trans. Computers*, vol. 51, Feb. 2002.
- "Low-cost flexible software fault tolerance for distributed computing," in *Proceedings of the 12th International Symposium on Software Reliability Engineering (ISSRE 2001)*, Hong Kong, China, pp.148-157, Nov. 2001.
- "Synergistic coordination between software and hardware fault tolerance techniques," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2001)*, Goteborg, Sweden, July 2001.
- "Onboard guarded software upgrading: Motivation and framework," in *Proceedings of the IEEE Aerospace Conference*, Big Sky, MT, Mar. 2001.
- "On low-cost error containment and recovery methods for guarded software upgrading," in *Proceedings of the 20th International Conference on Distributed Computing Systems (ICDCS 2000)*, Taipei, Taiwan, Apr. 2000.
- "On the effectiveness of a message-driven confidence-driven protocol for guarded software upgrading," in *Proceedings of the 4th IEEE International Computer Performance and Dependability Symposium (IPDS 2000)*, Schaumburg, IL, Mar. 2000