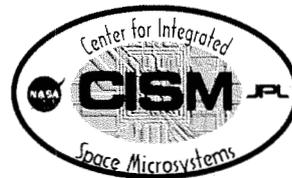




Advanced Avionics Systems for Dependable Computing in Future Space Exploration

Leon Alkalai, Savio Chau, Ann Tai

Center for Integrated Space Microsystems
Jet Propulsion Laboratory
California Institute of Technology



GOMAC – 2002
March 12th, 2002

leon@cism.jpl.nasa.gov

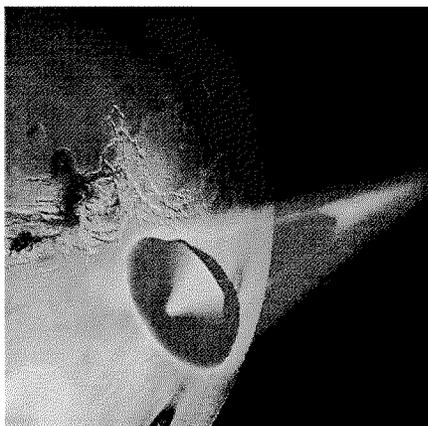
URL: <http://cism.jpl.nasa.gov>

Tel. 818 354-5988

Fax. 818 393 5013



Potential Customers: Mars 09 Smart Lander/Rover Mission



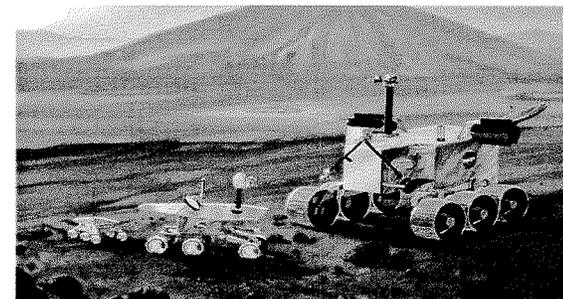
GUIDED ENTRY

Approach

- Strong, multi-disciplinary team
 - NASA centers
 - Industry
 - Universities
- Early pre-project with extensive technology program

Conduct Significant Science*

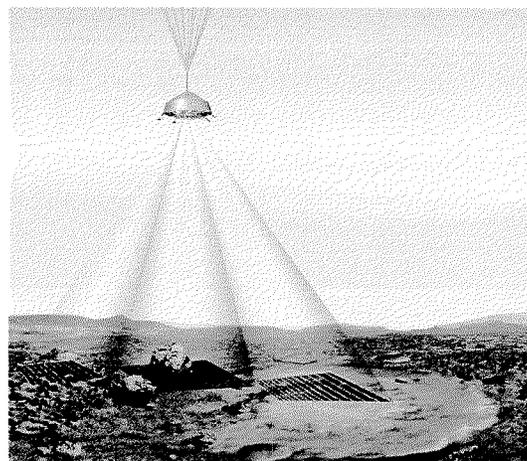
- Sub-surface drilling
- In-situ soil/rock analysis
- Atmospheric measurements



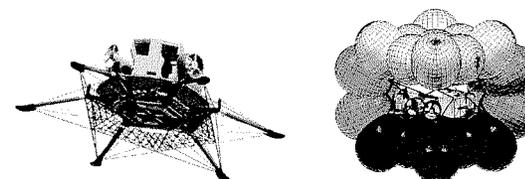
SURFACE MOBILITY

Demonstrate Next-Generation Lander/Rover Capabilities

- Global access
 - latitude range
 - surface elevation
 - rugged terrain
- Accurate/safe landing
- “Go-to” mobility
- Extended mission operations



HAZARD DETECTION/AVOIDANCE



ROBUST TOUCHDOWN SYSTEM

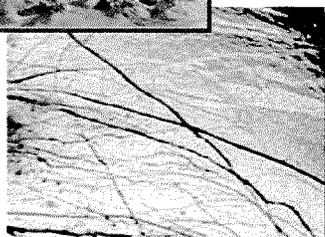
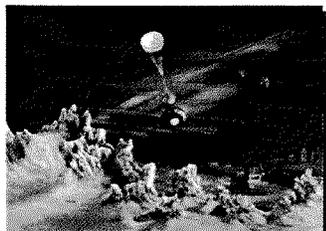
*No “strawman” payload yet defined, examples of possible experiments listed



Potential Customers: Solar System Exploration (circa 2008)



Cassini/Huygens

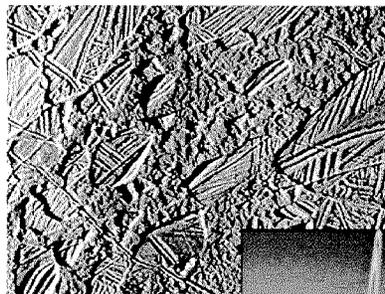


Galileo-
Europa

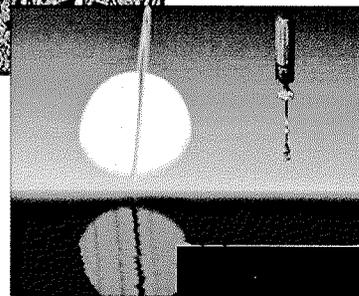
Exploring Organic Rich Environments:

- Extreme Radiation Environments
- Extreme Temperature Environments
- Long Duration missions
- Long latency of communications
 - highly autonomous operations
 - miniaturization of systems
 - design for high survivability, fault-tolerance, and high availability

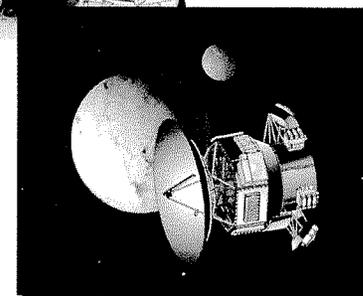
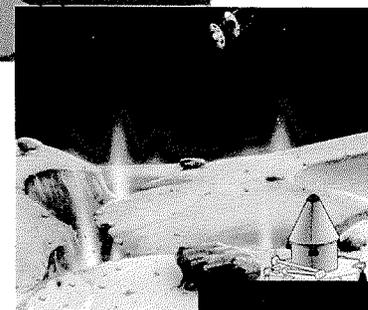
Europa Orbiter/Lander



Titan Explorer



Comet Nucleus
Sample Return



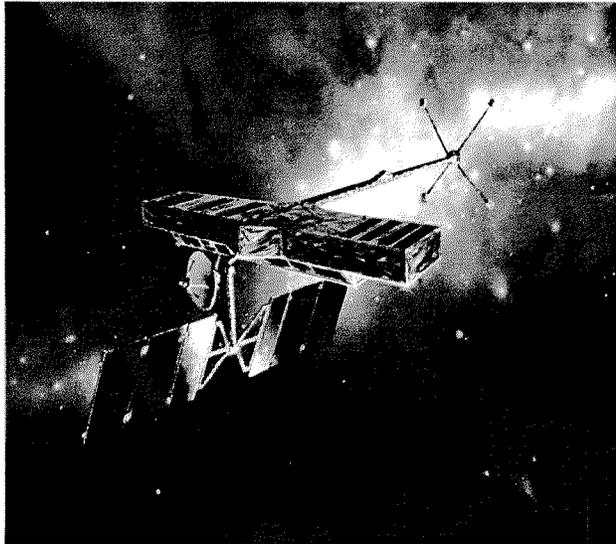
Pluto/Kuiper Express



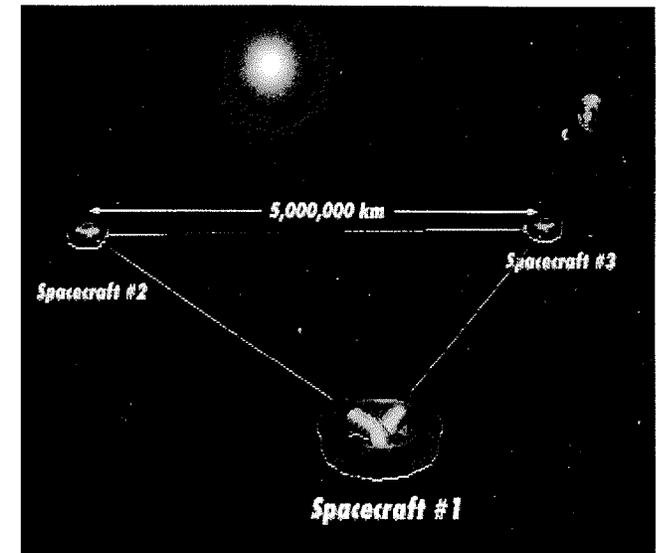
Potential Customers: Astrophysics (2009)



Space Interferometry Mission (SIM)



Laser Interferometry Space Antenna (LISA)



Space based Interferometry

- High precision metrology
- Pico-meter laser interferometry
 - Highly miniaturized electronics
 - High performance computing
 - Micro-Newton Thrusters
 - Disturbance reduction control
 - High Performance inertial sensors

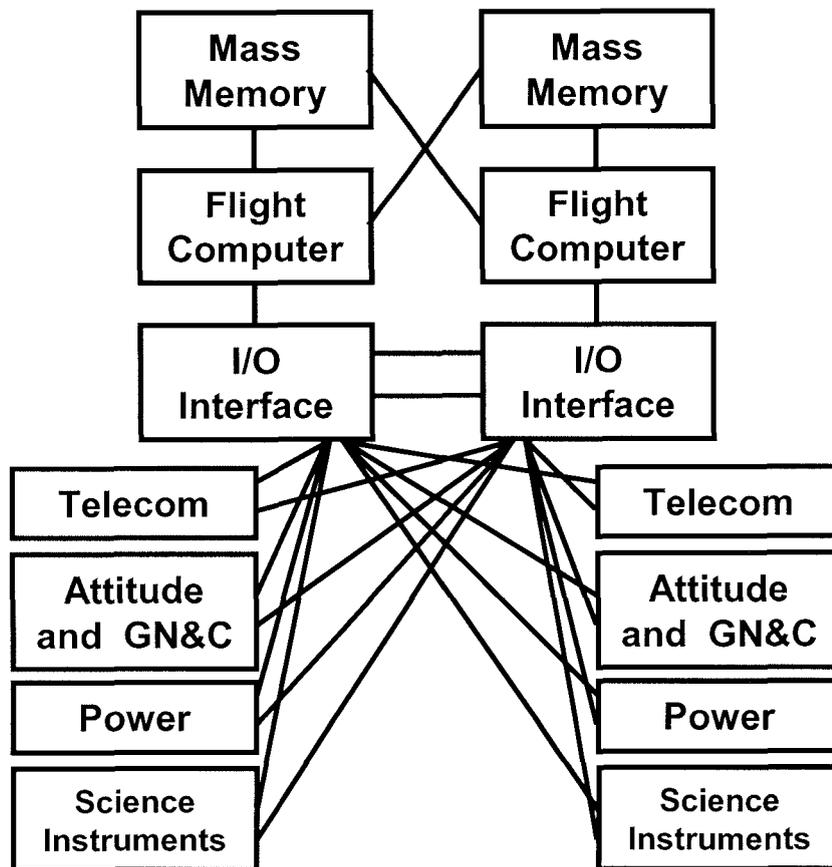


Dependable Computing in Previous Deep Space Missions

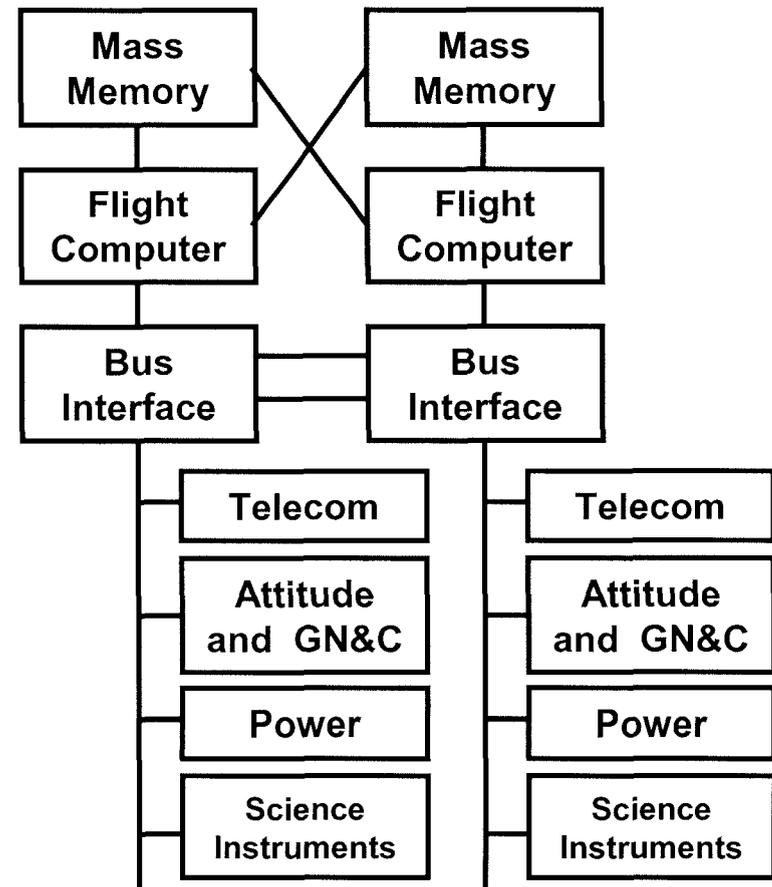


- Typical Dual-String Designs for Spacecraft

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



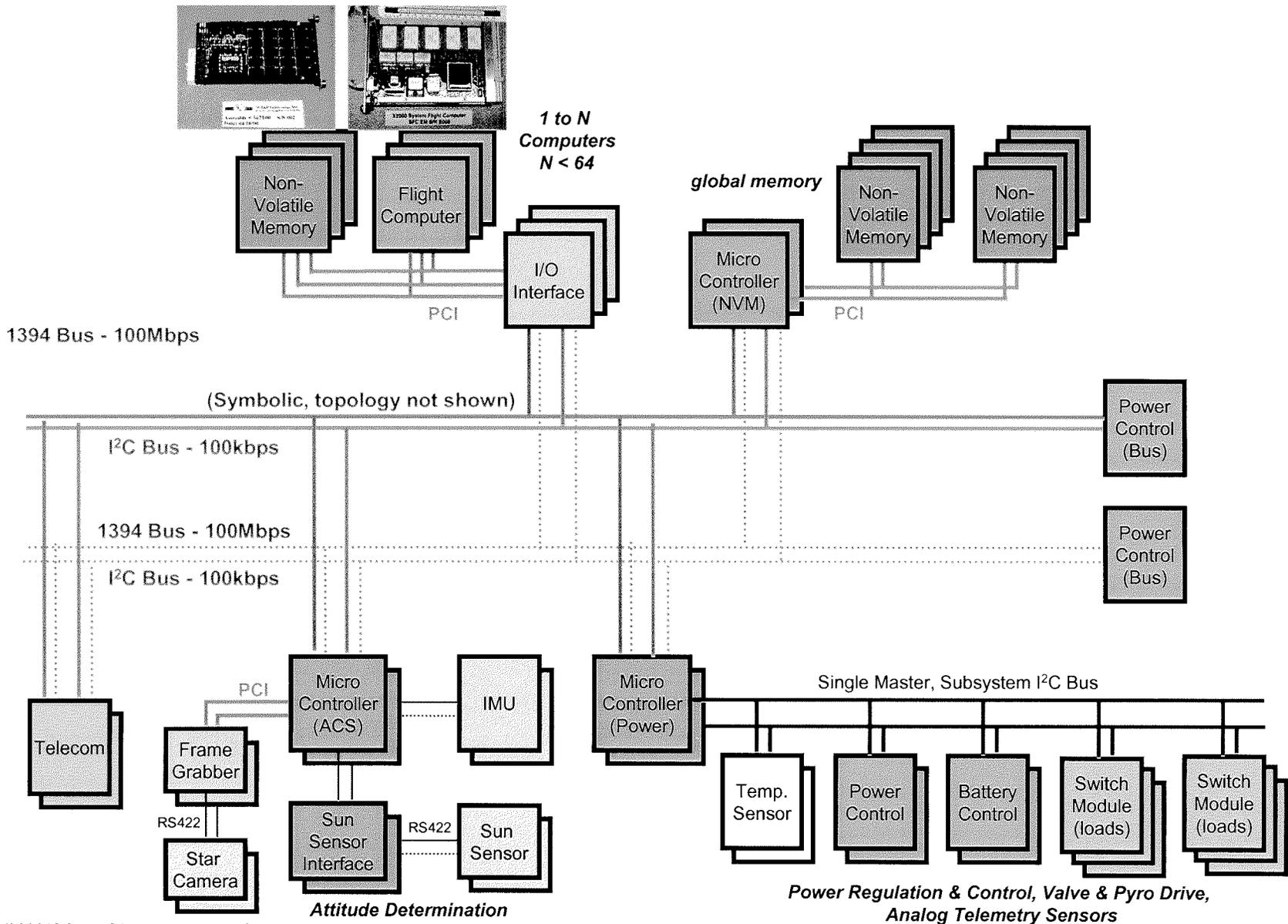
High-Performance Fault-Tolerant Bus Architecture Research at JPL



- 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

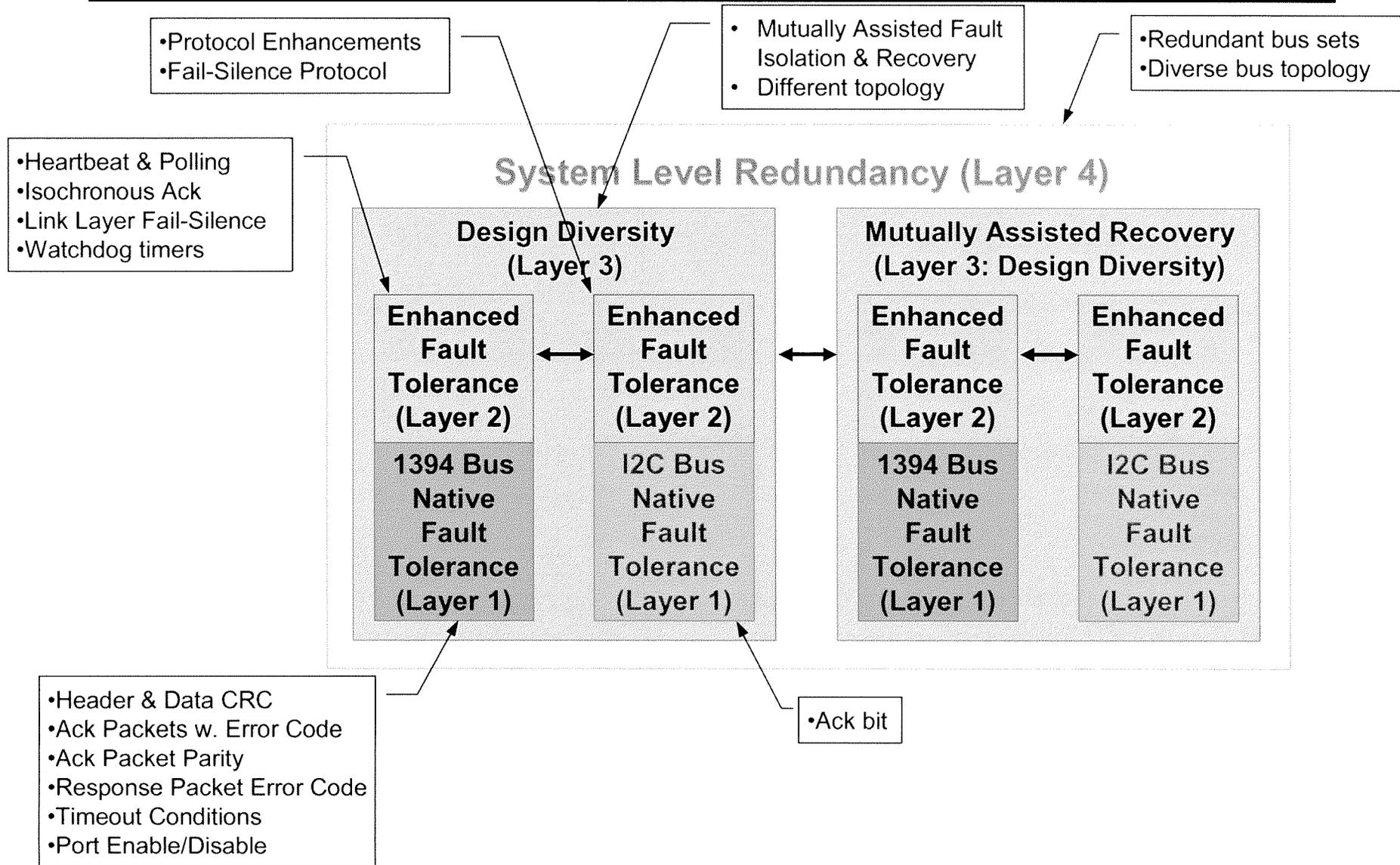


Baseline X2000 COTS Bus Architecture





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

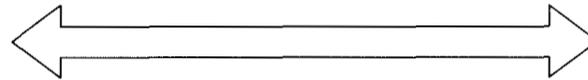




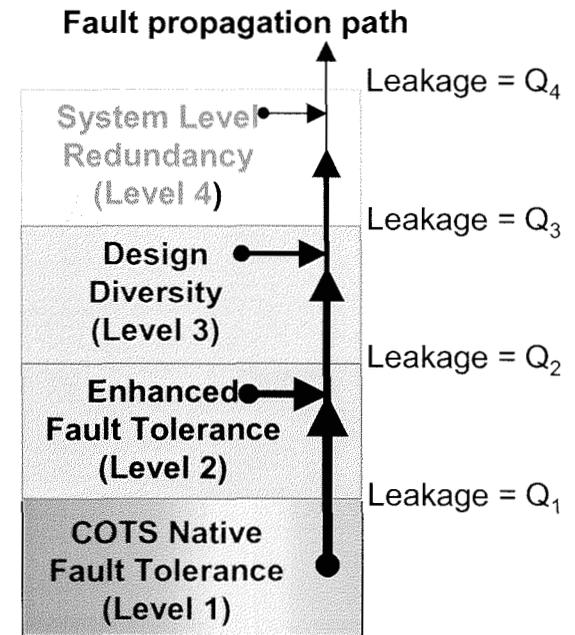
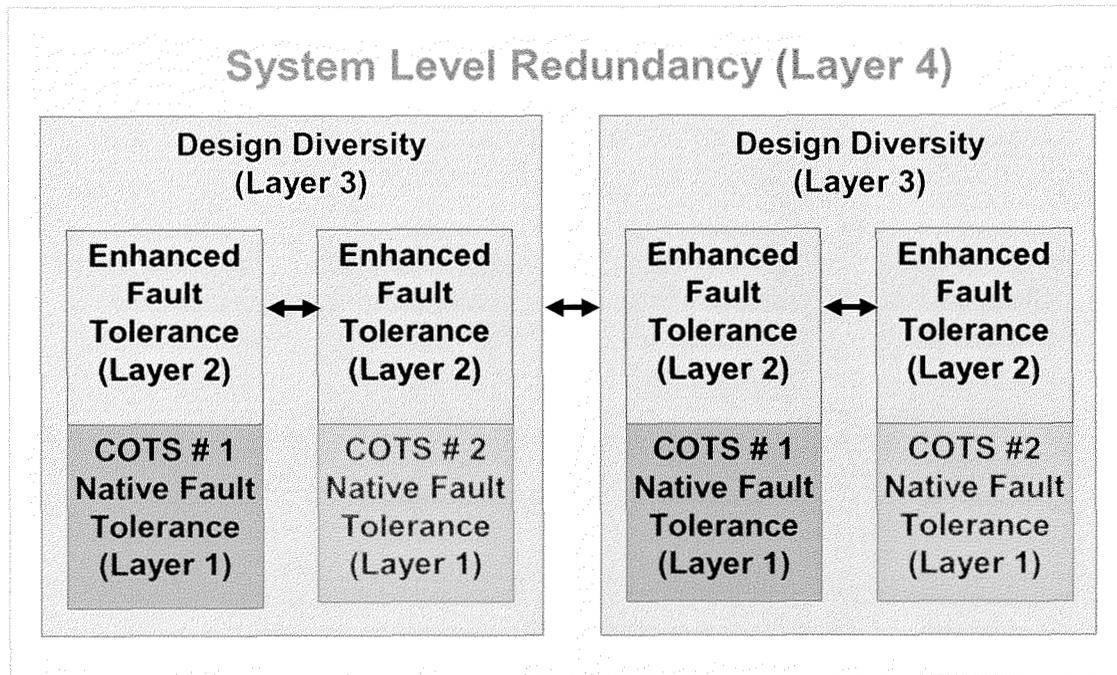
A Framework for the Design of Highly Survivable Avionics Systems using COTS



Design



Analysis



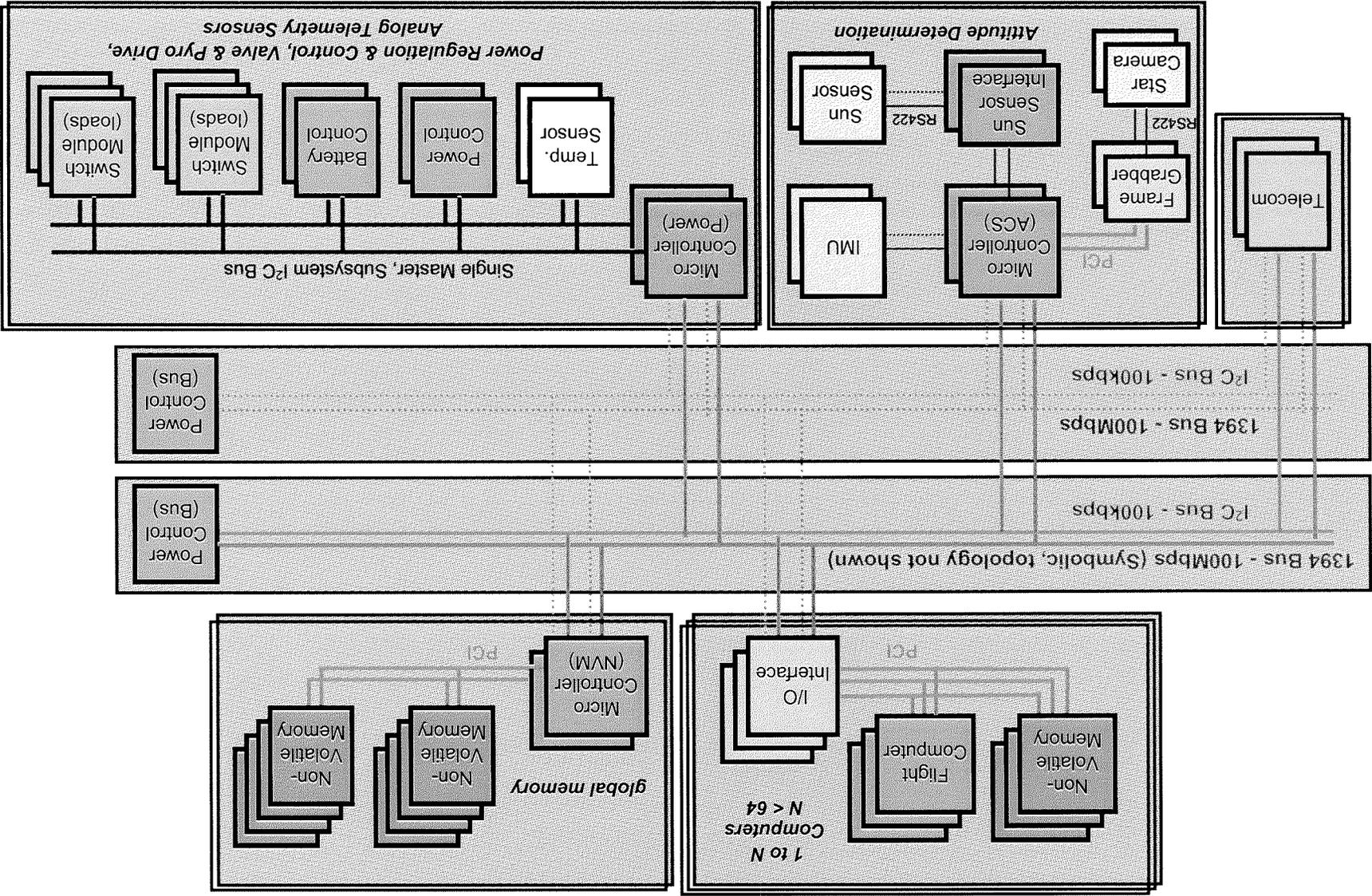
Fault Propagation Model of Multi-Layer Design

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

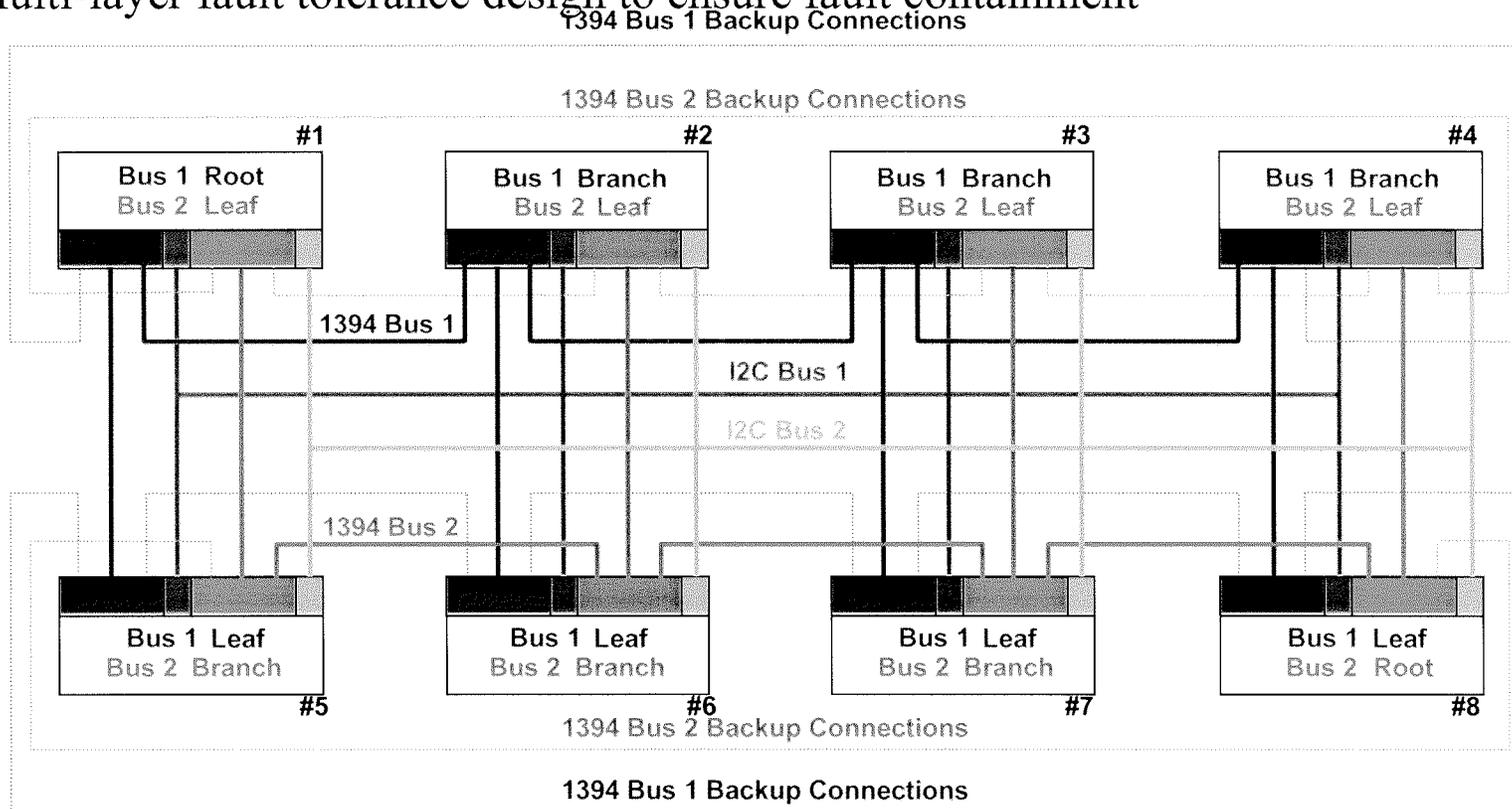




A Highly Reliable Distributed Network Architecture for Future Missions



- 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

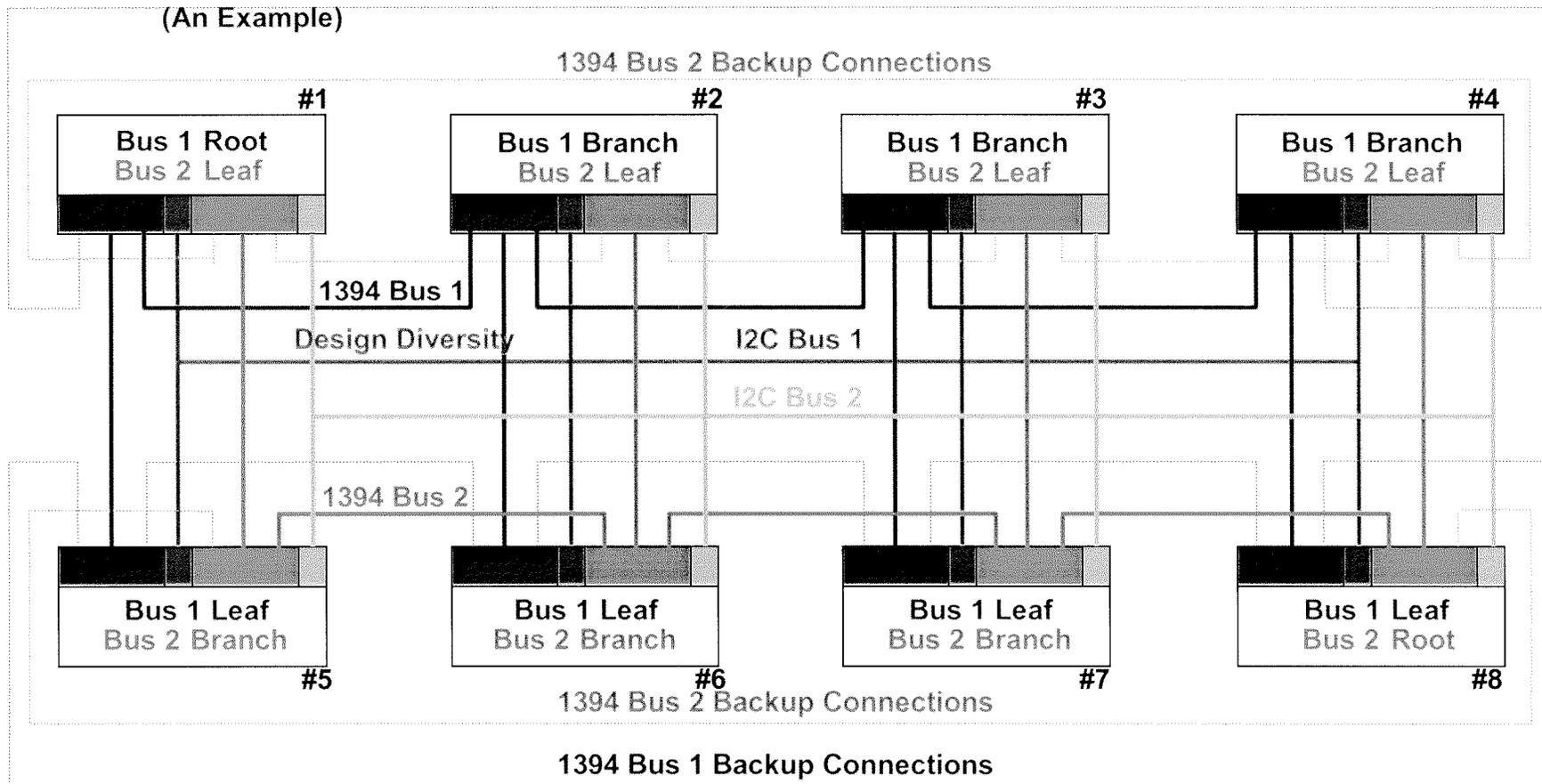


Cable IEEE 1394 has a tree topology

Enhanced Fault Tolerance
(An Example)

1394 Bus 1 Backup Connections

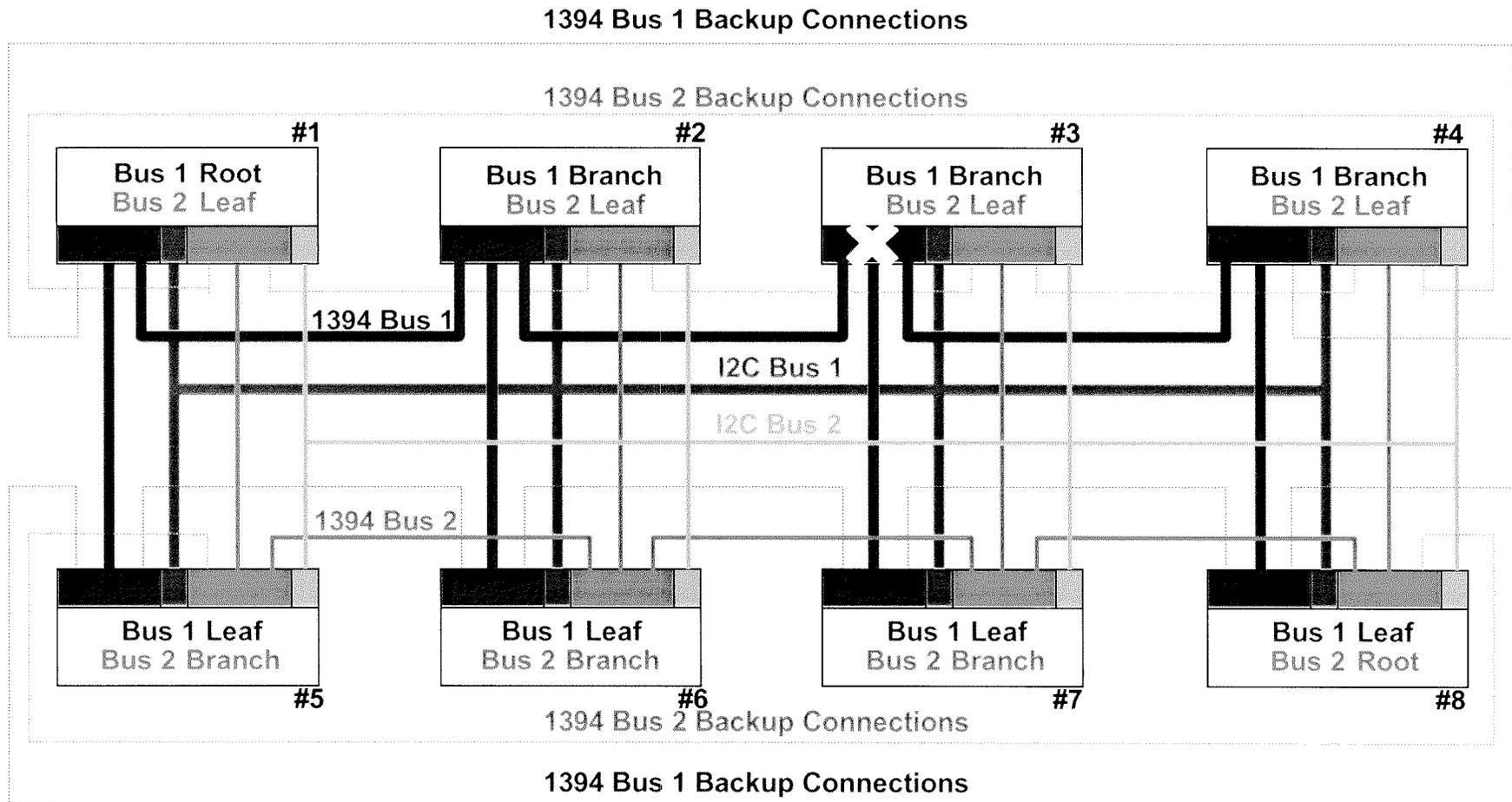
1394 Bus 2 Backup Connections



System Level Redundancy with Diverse Topology



X2000 Fault Protection Strategy





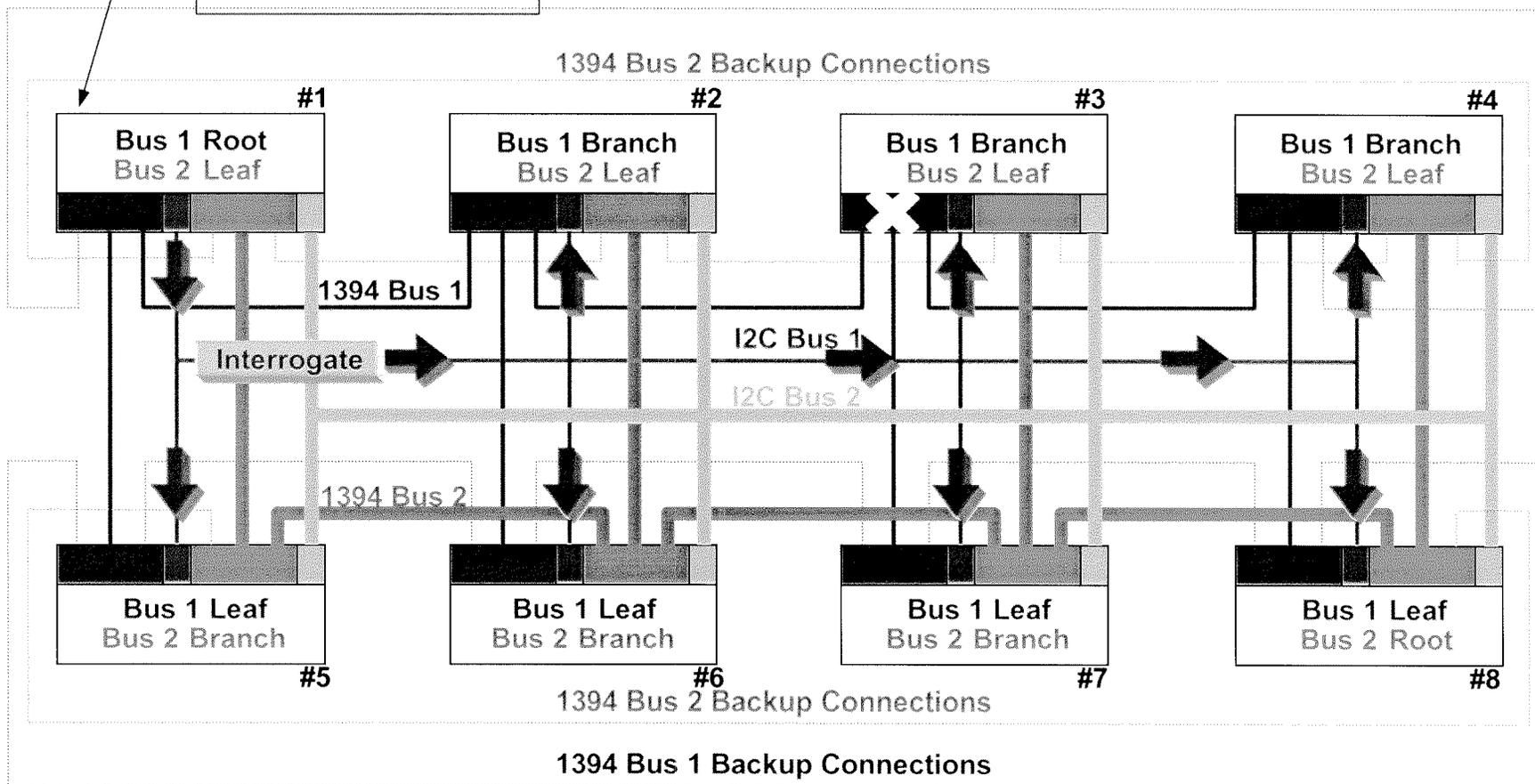
X2000 Fault Protection Strategy

Possible Recovery Initiator

- IEEE 1394 Root
- IEEE 1394 IRM
- IEEE 1394 Bus Manager
- I2C Prime Master

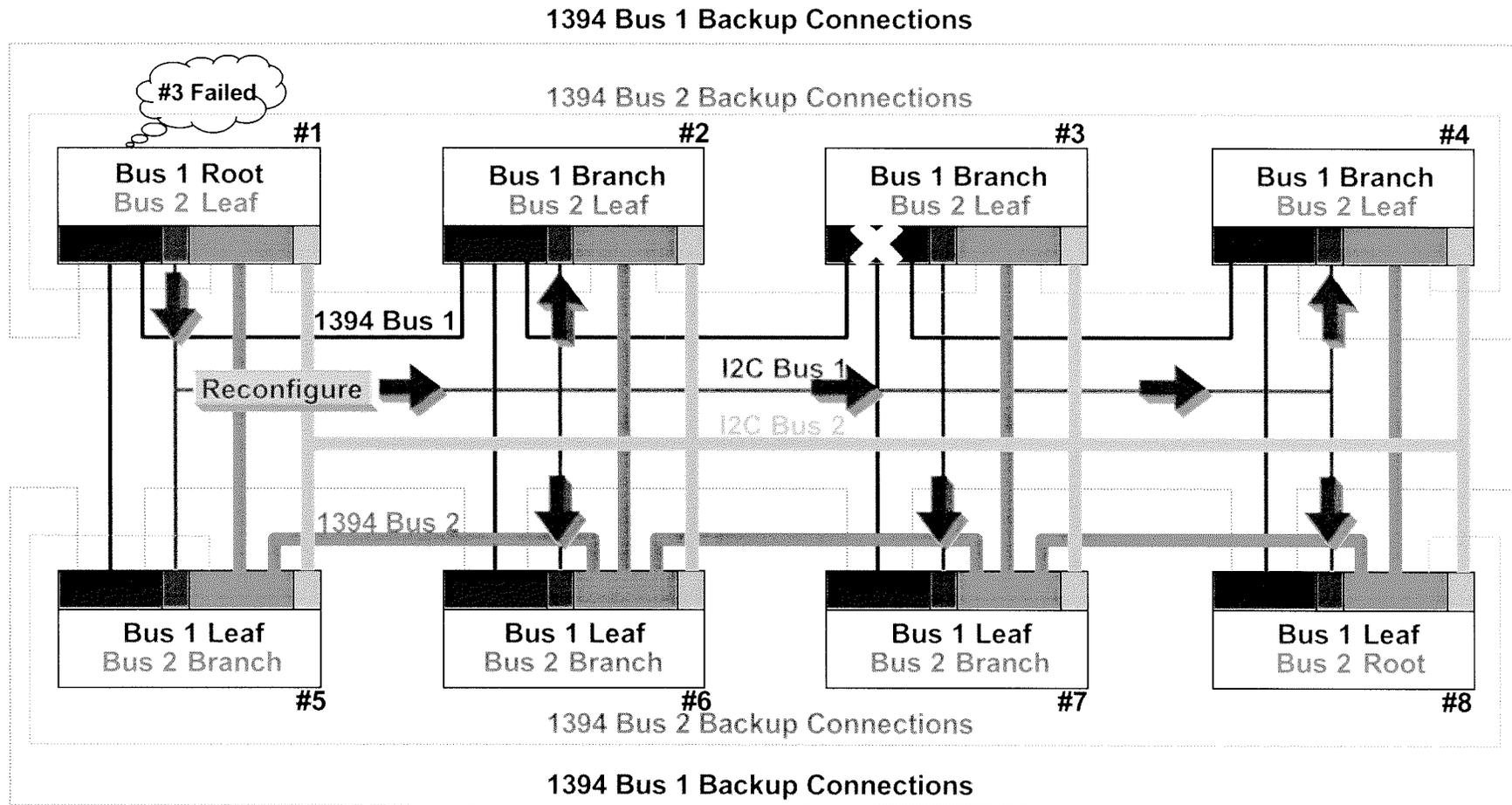
1394 Bus 1 Backup Connections

1394 Bus 2 Backup Connections



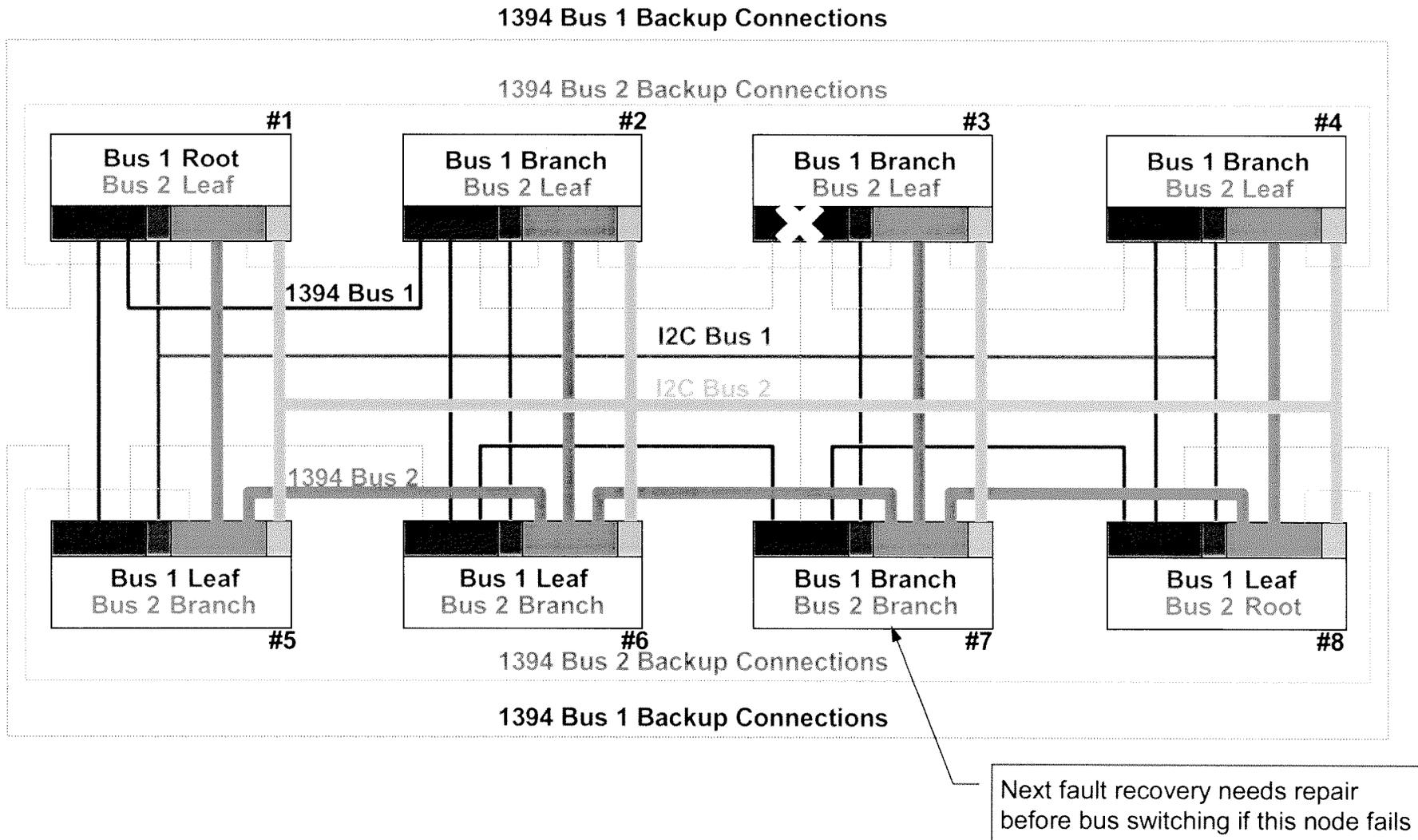


X2000 Fault Protection Strategy



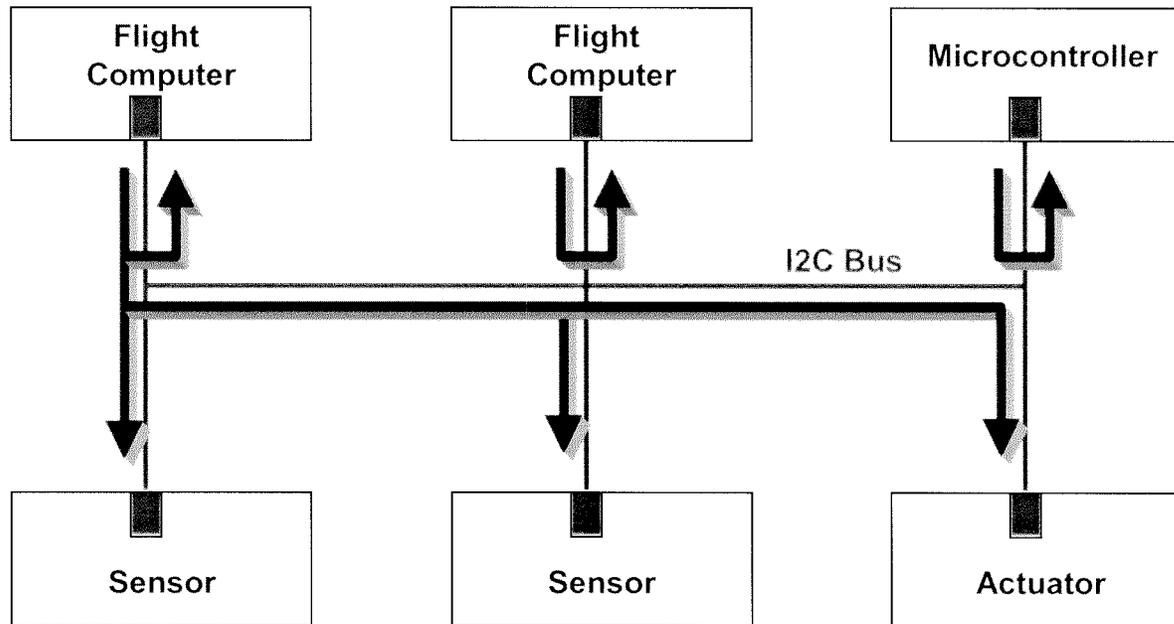


X2000 Fault Protection Strategy



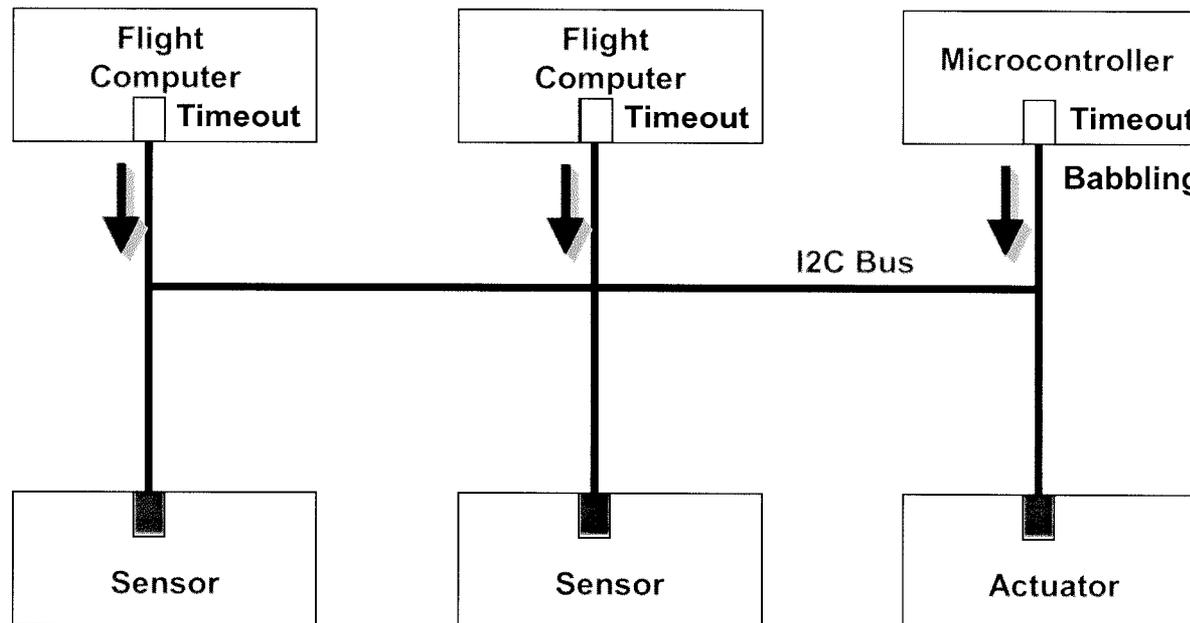


I²C Bus Fault Protection: Fail Silence



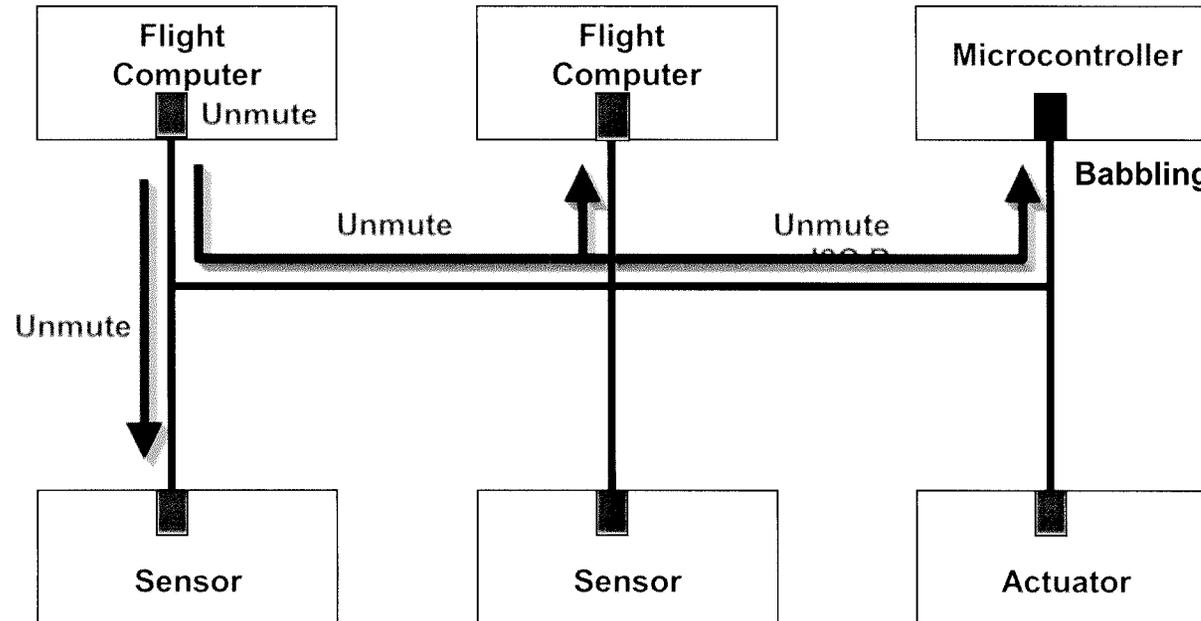


I²C Bus Fault Protection: Fail Silence



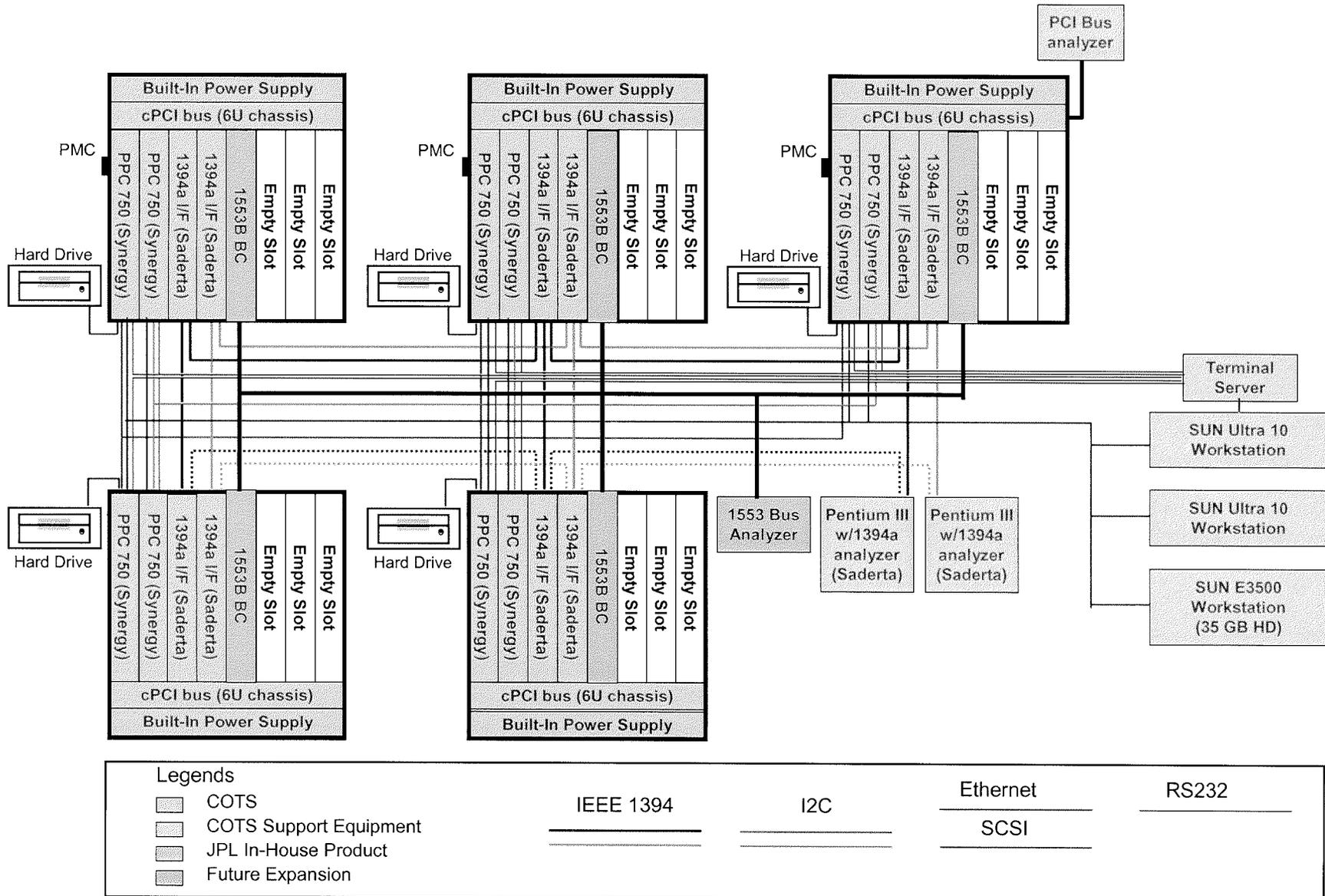


I²C Bus Fault Protection: Fail Silence





Architecture Testbed Configuration



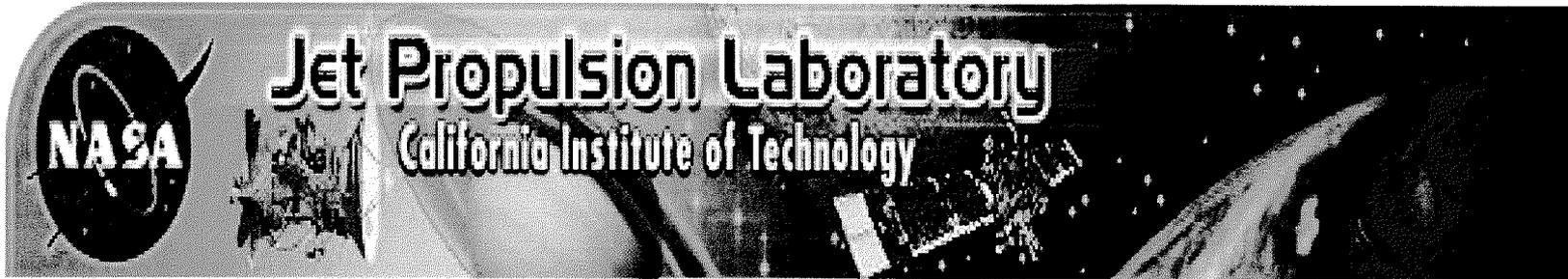


Example of Fault Injection in IEEE 1394 Bus



Fault Injected in the Gap Count Register in the IEEE 1394 Bus

(A)



Before Fault Injection

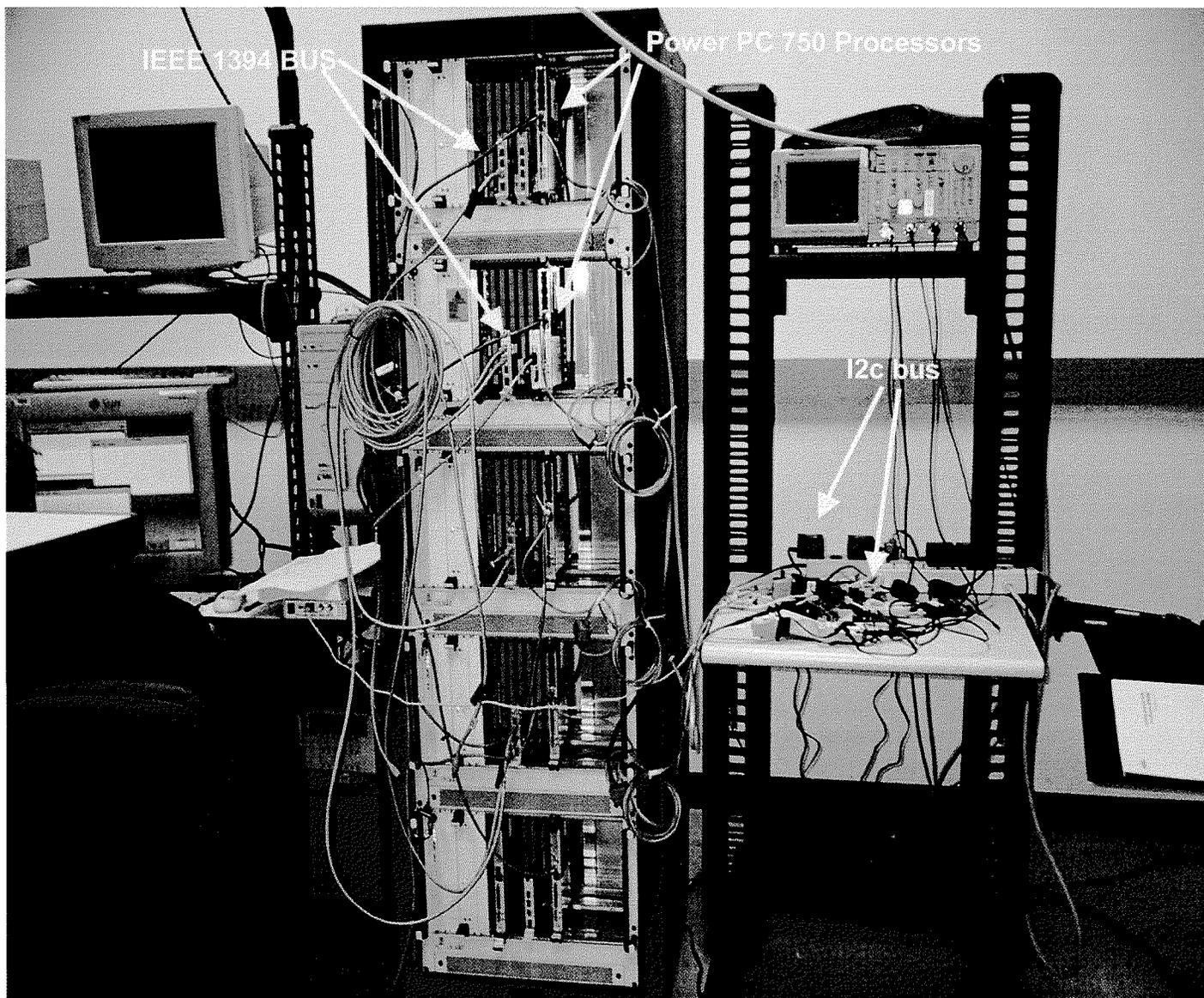
(B)



After Fault Injection



Distributed Flight Computer Testbed





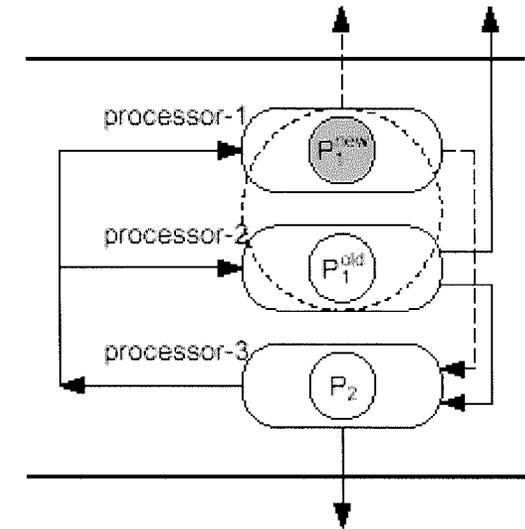
Guarded Software Upgrade



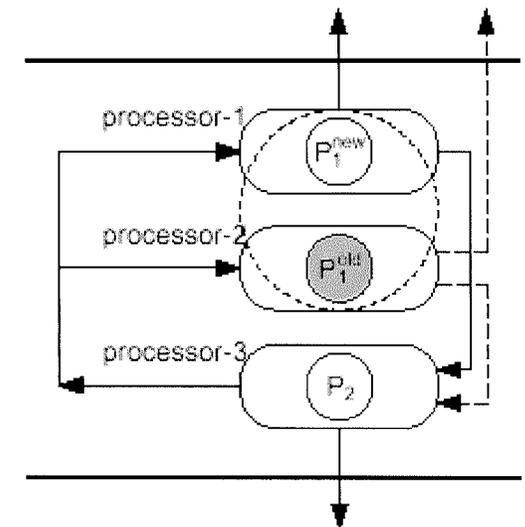
- **Motivation:**
 - Flight software for long life deep space missions have to be upgraded periodically to correct design bugs or due to change of mission phases
 - Unprotected software upgrades have previously caused severe and costly damage to space missions and critical applications
- **Objectives:**
 - 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.

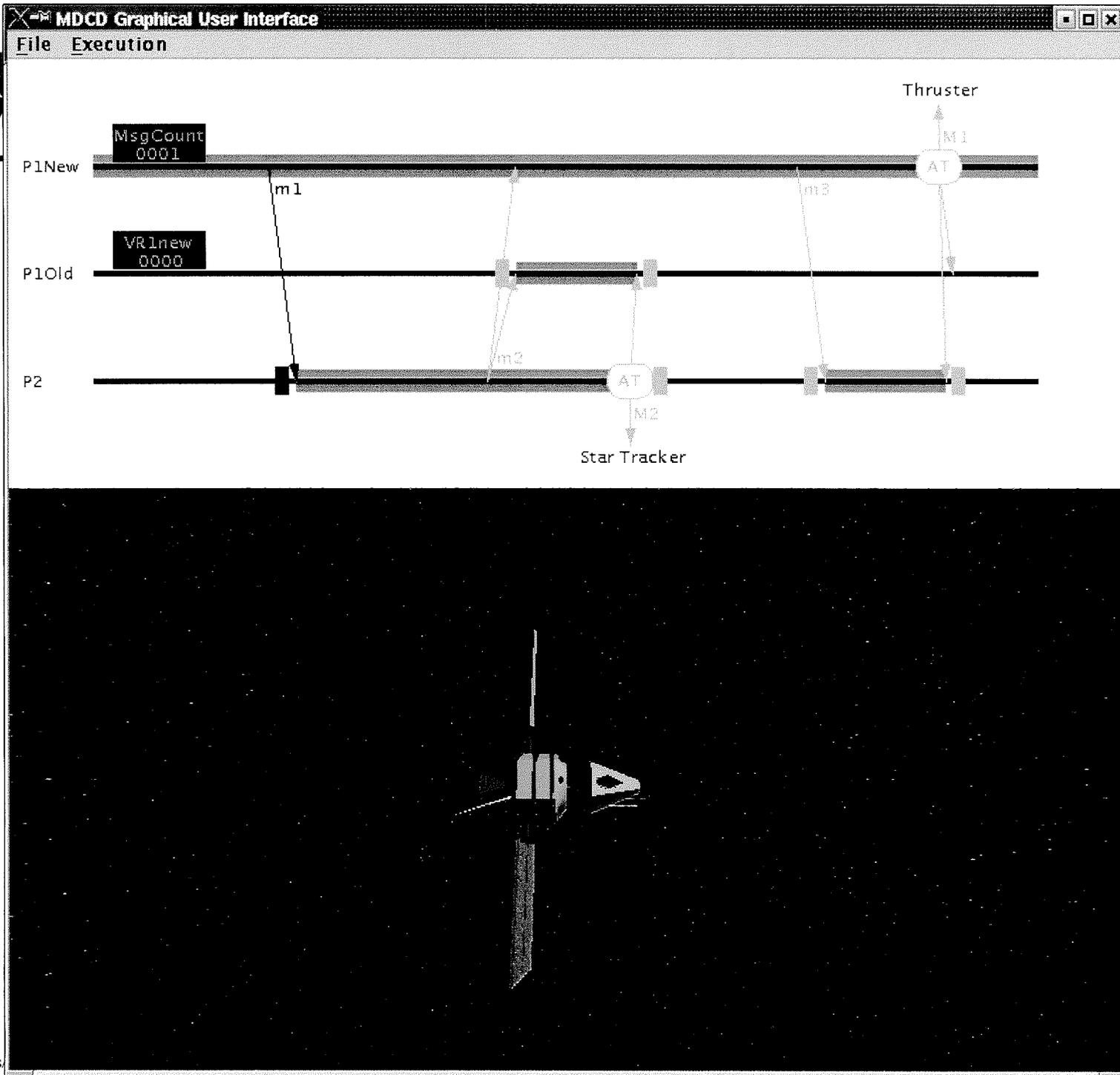
A. T. Tai, K. S. Tso, L. Alkalai, S. Chau, and W. H. Sanders, "On the effectiveness of a message-driven confidence-driven protocol for guarded software upgrading," in Proceedings of the *4th IEEE International Computer Performance and Dependability Symposium (IPDS 2000)*, Schaumburg, IL, March 2000.

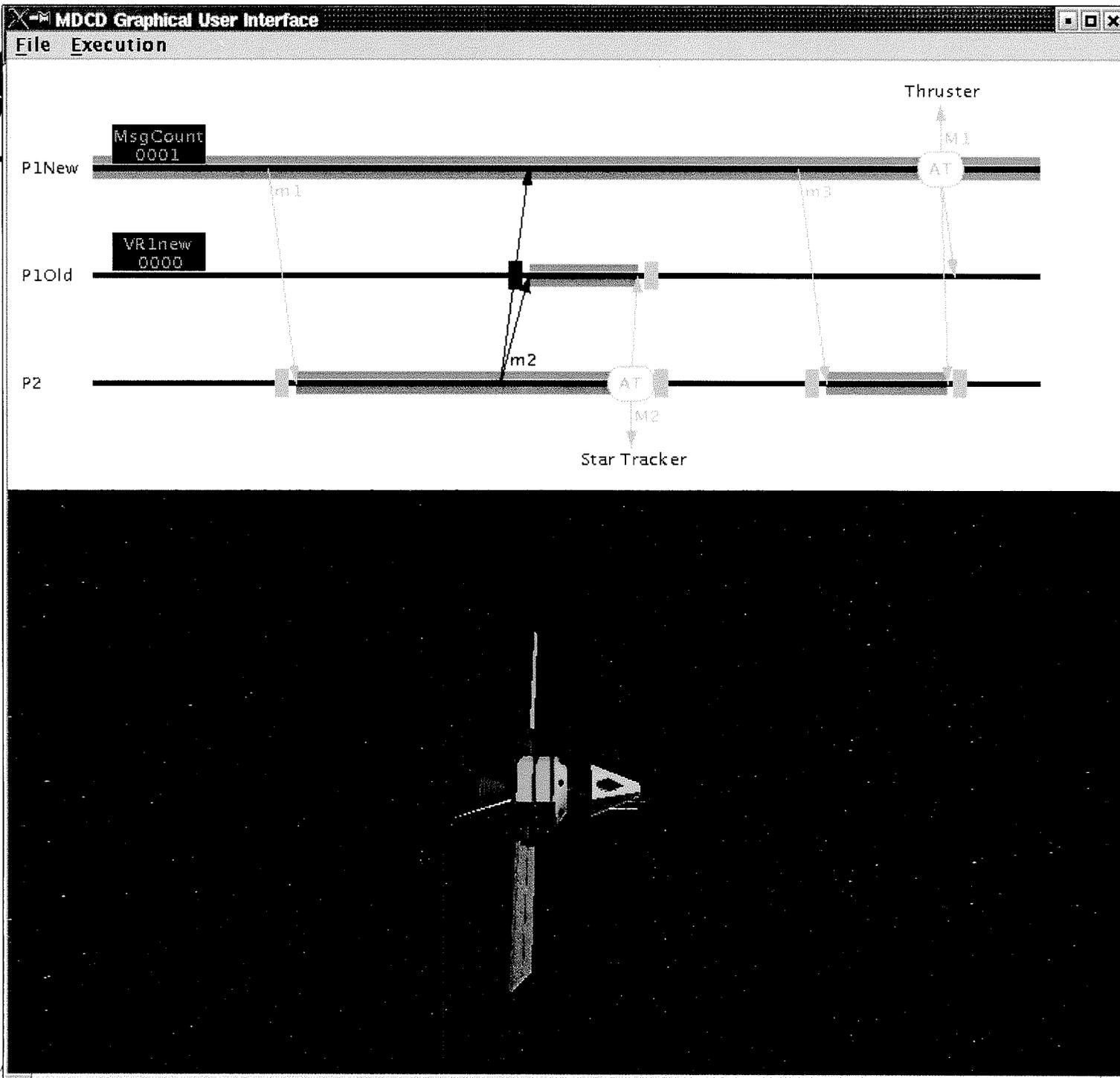


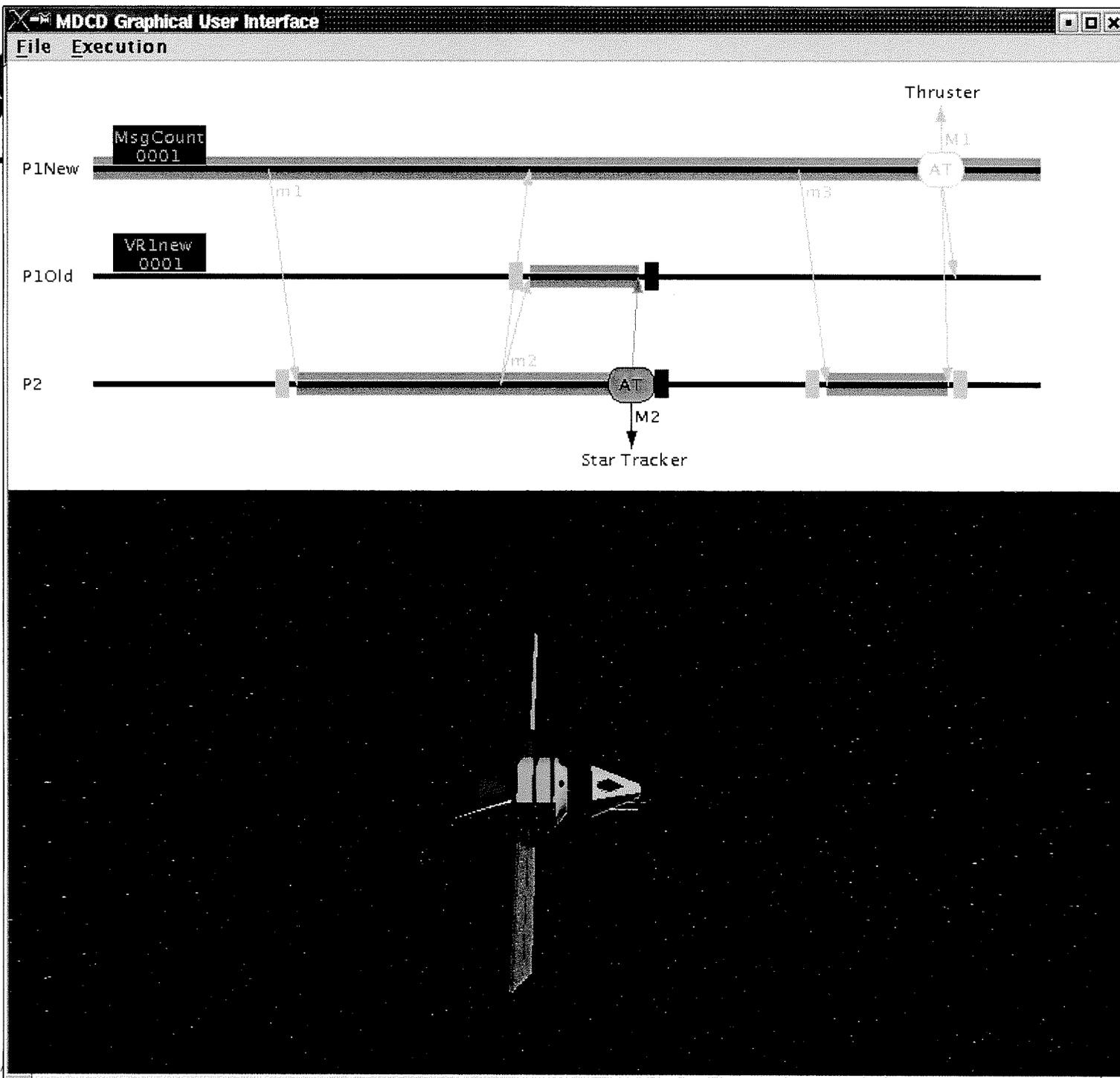
(a) Onboard Validation Stage

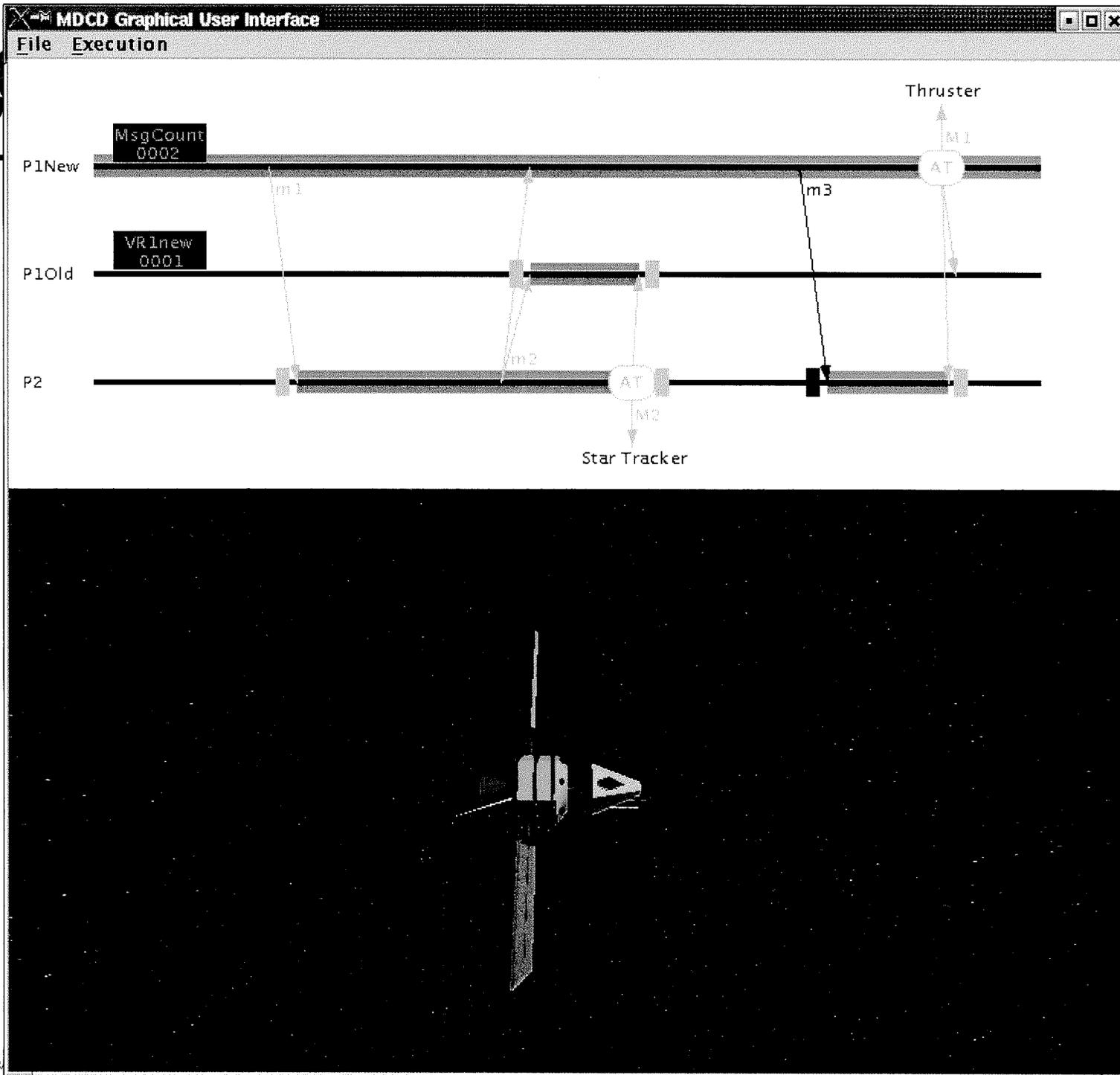


(b) Guarded Operation Stage









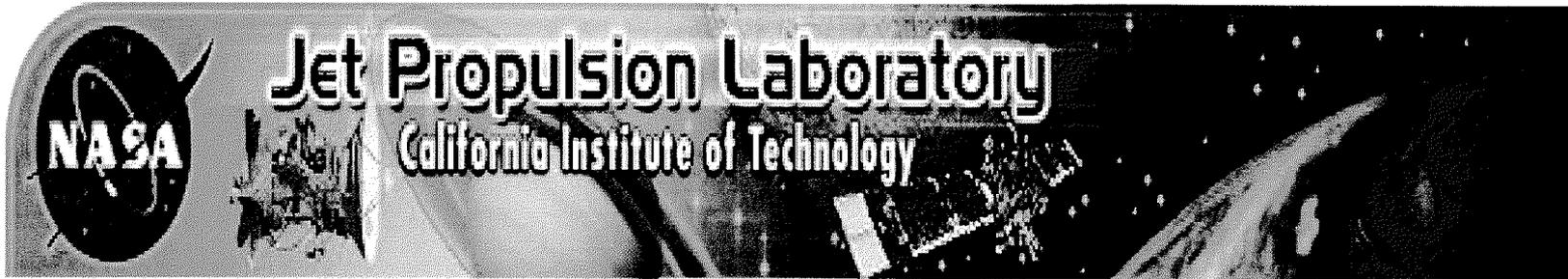


Example of Fault Injection in IEEE 1394 Bus



Fault Injected in the Gap Count Register in the IEEE 1394 Bus

(A)



Before Fault Injection

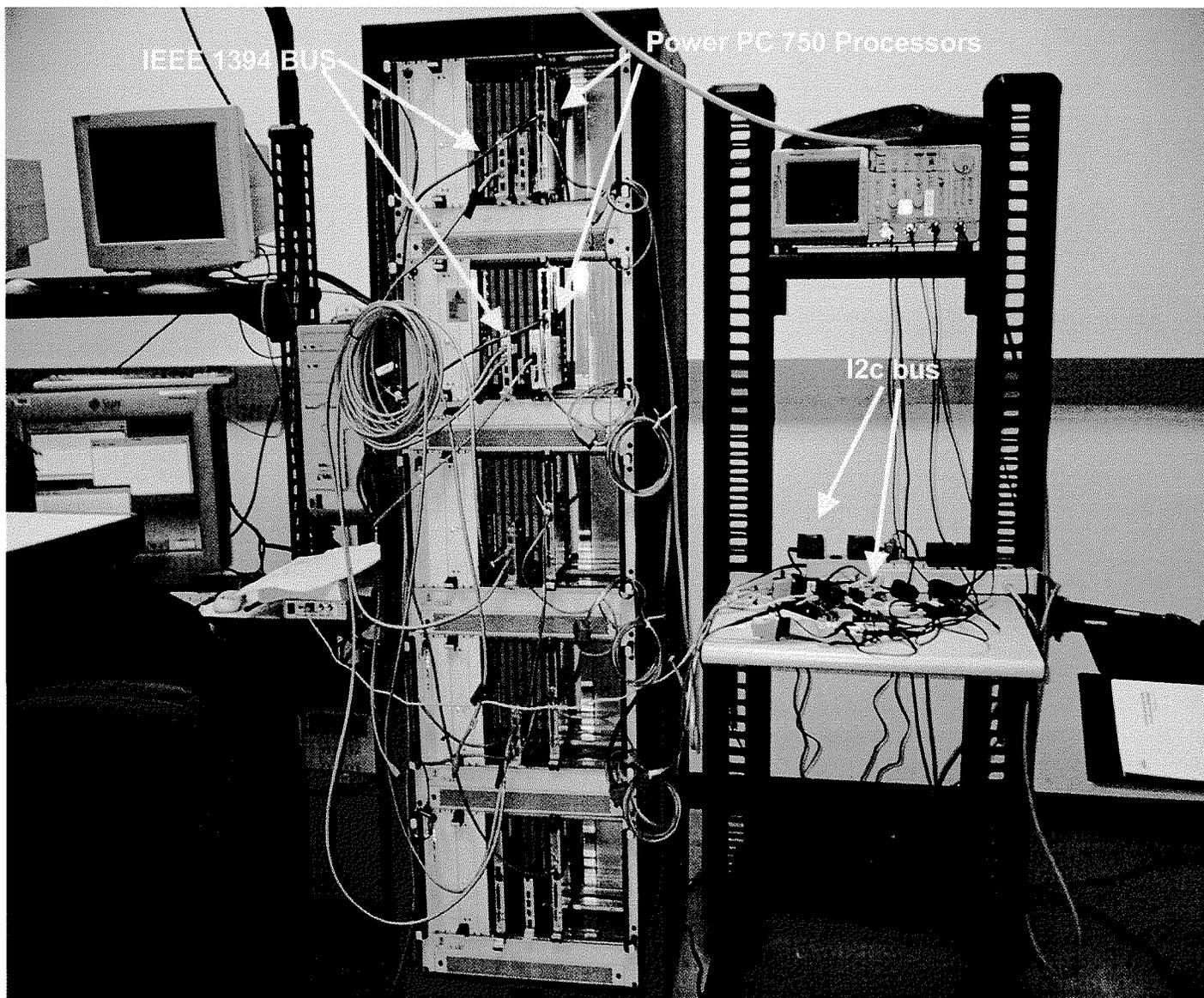
(B)

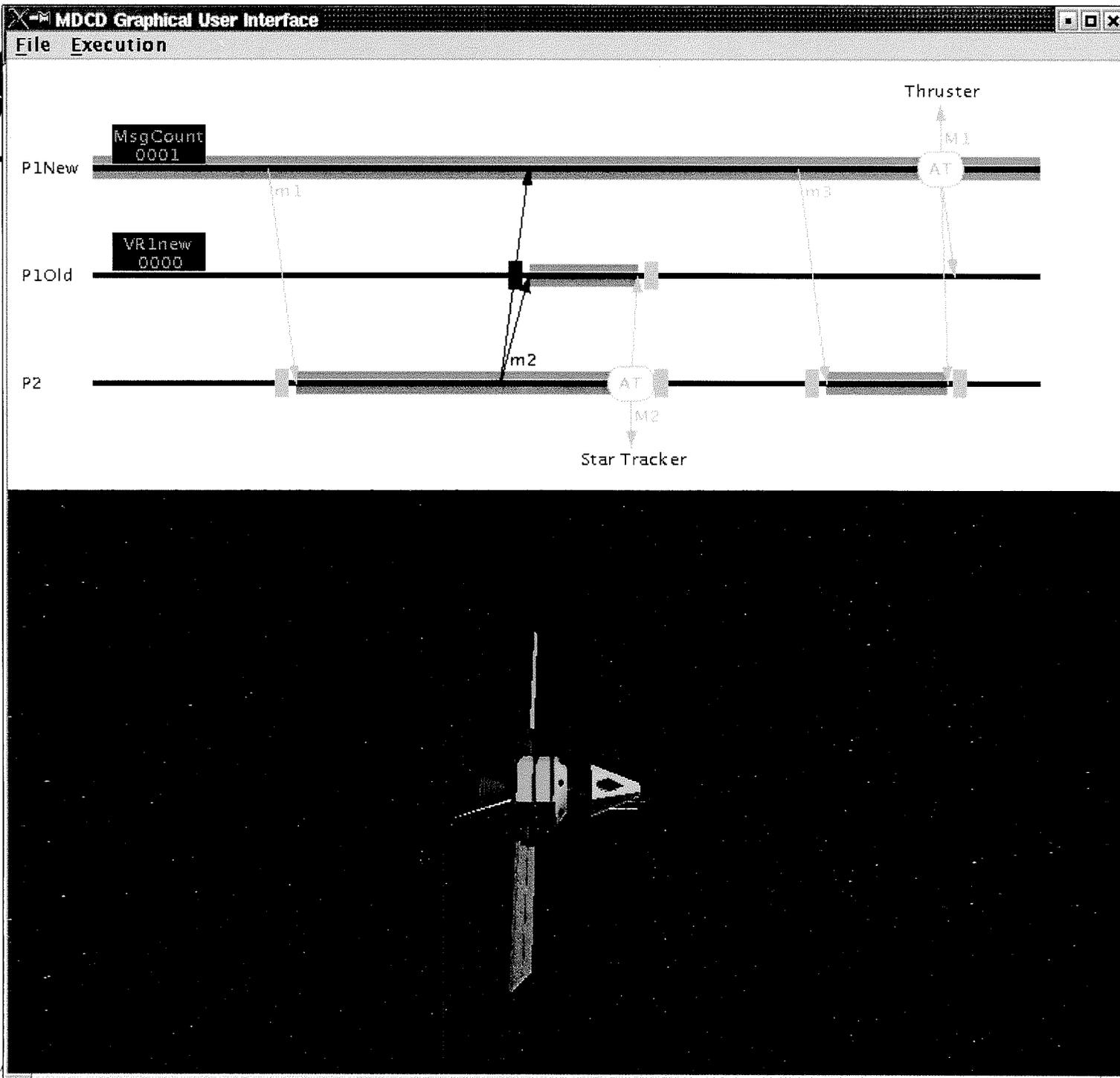


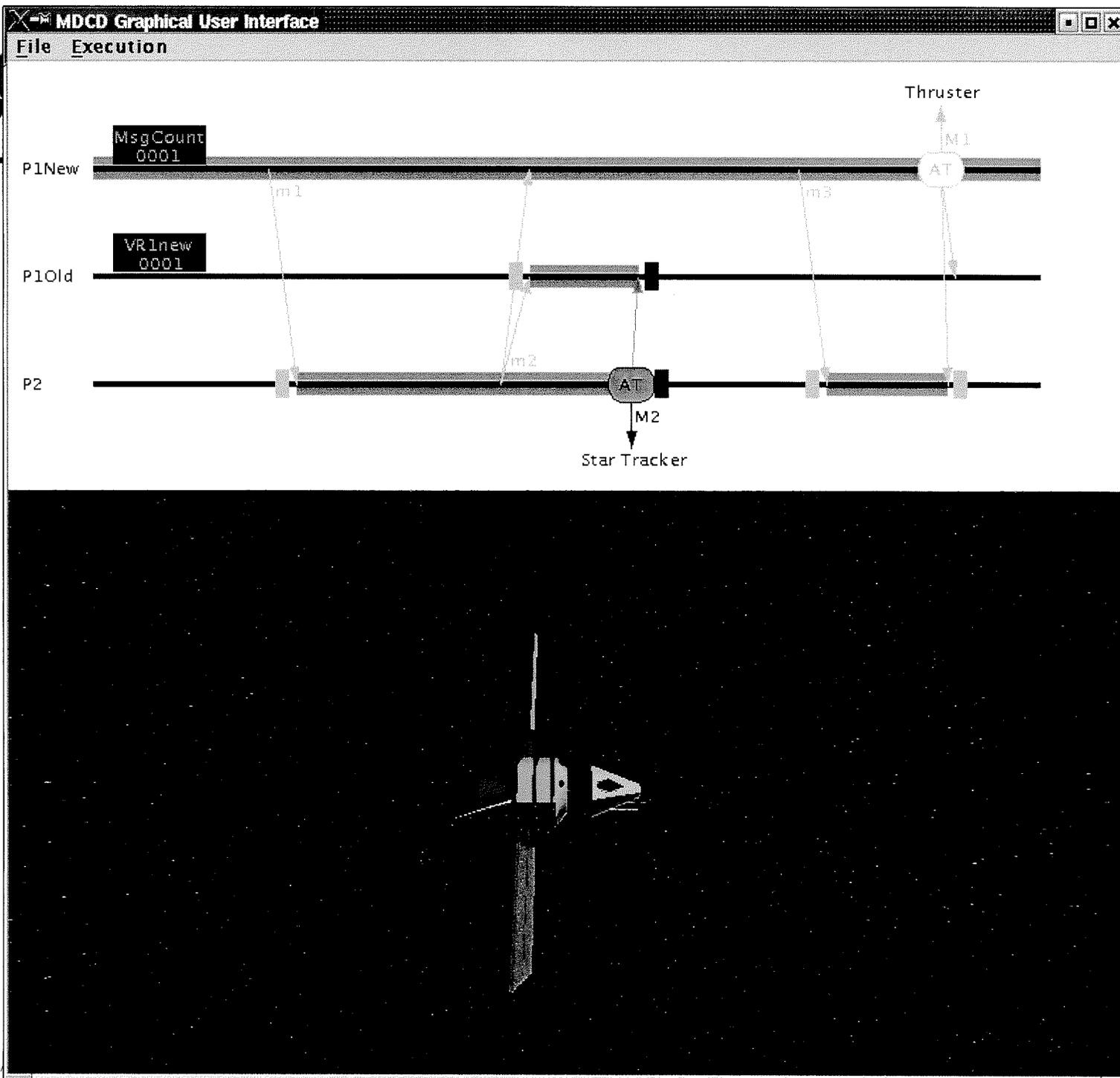
After Fault Injection

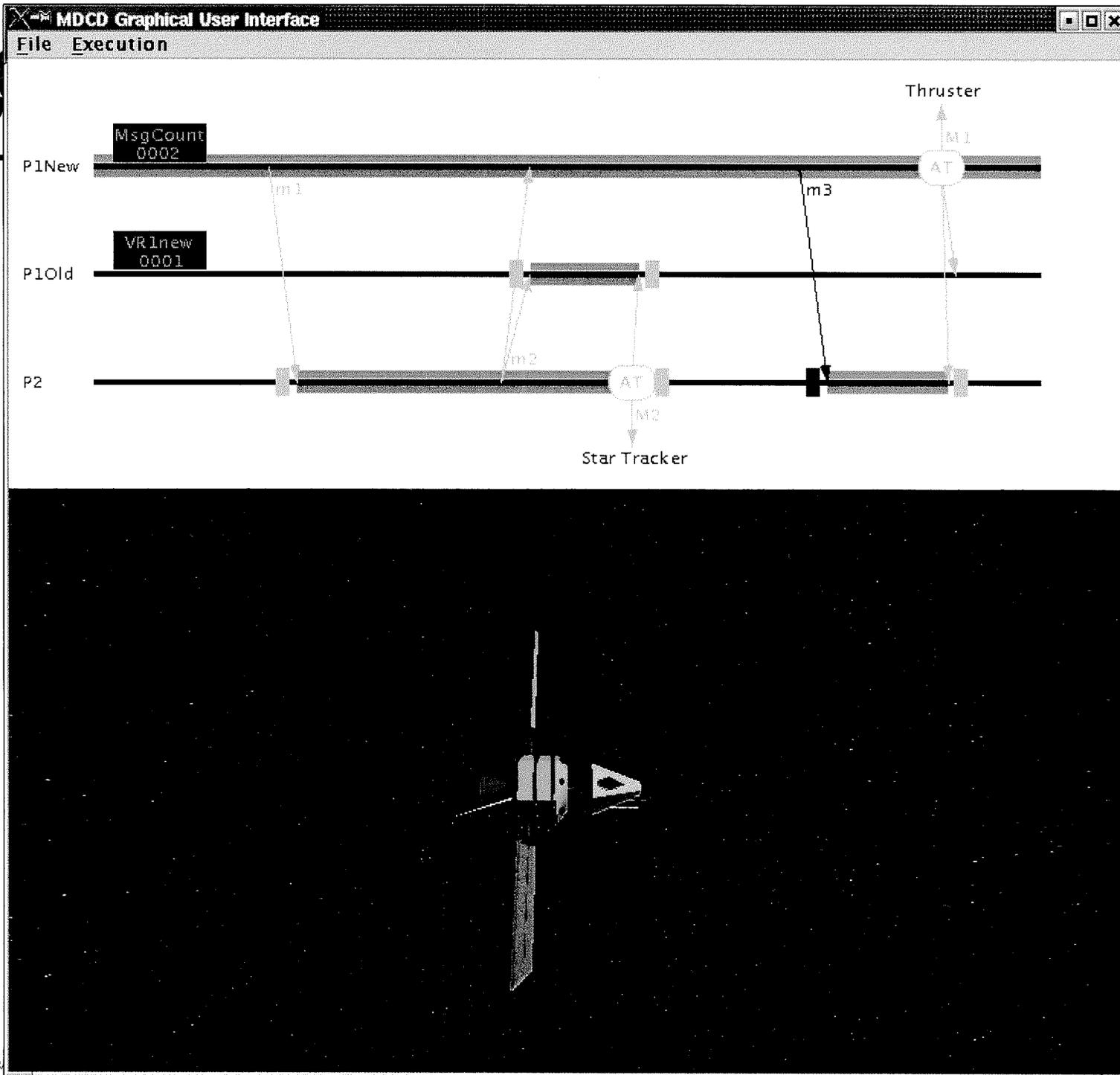


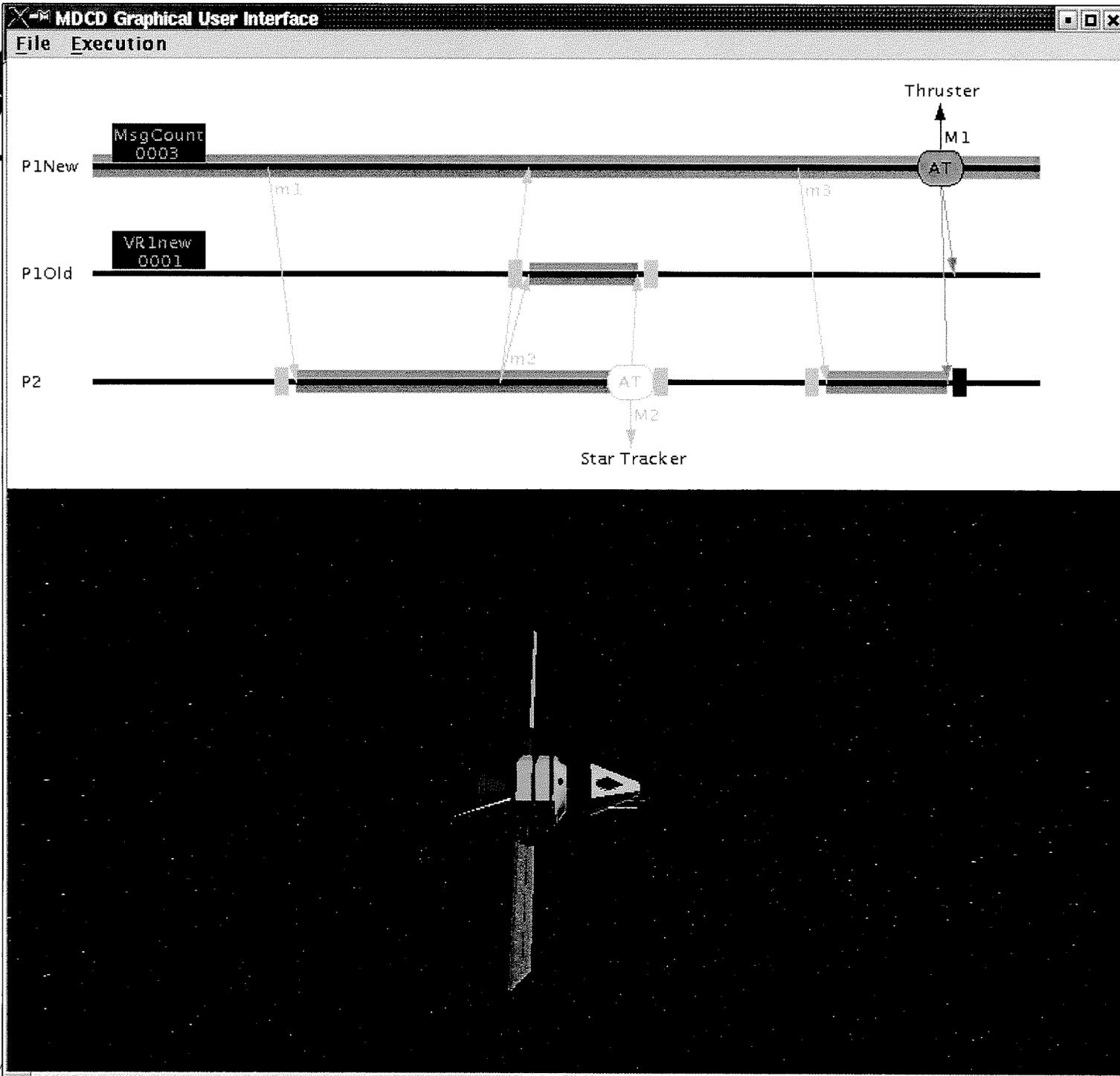
Distributed Flight Computer Testbed

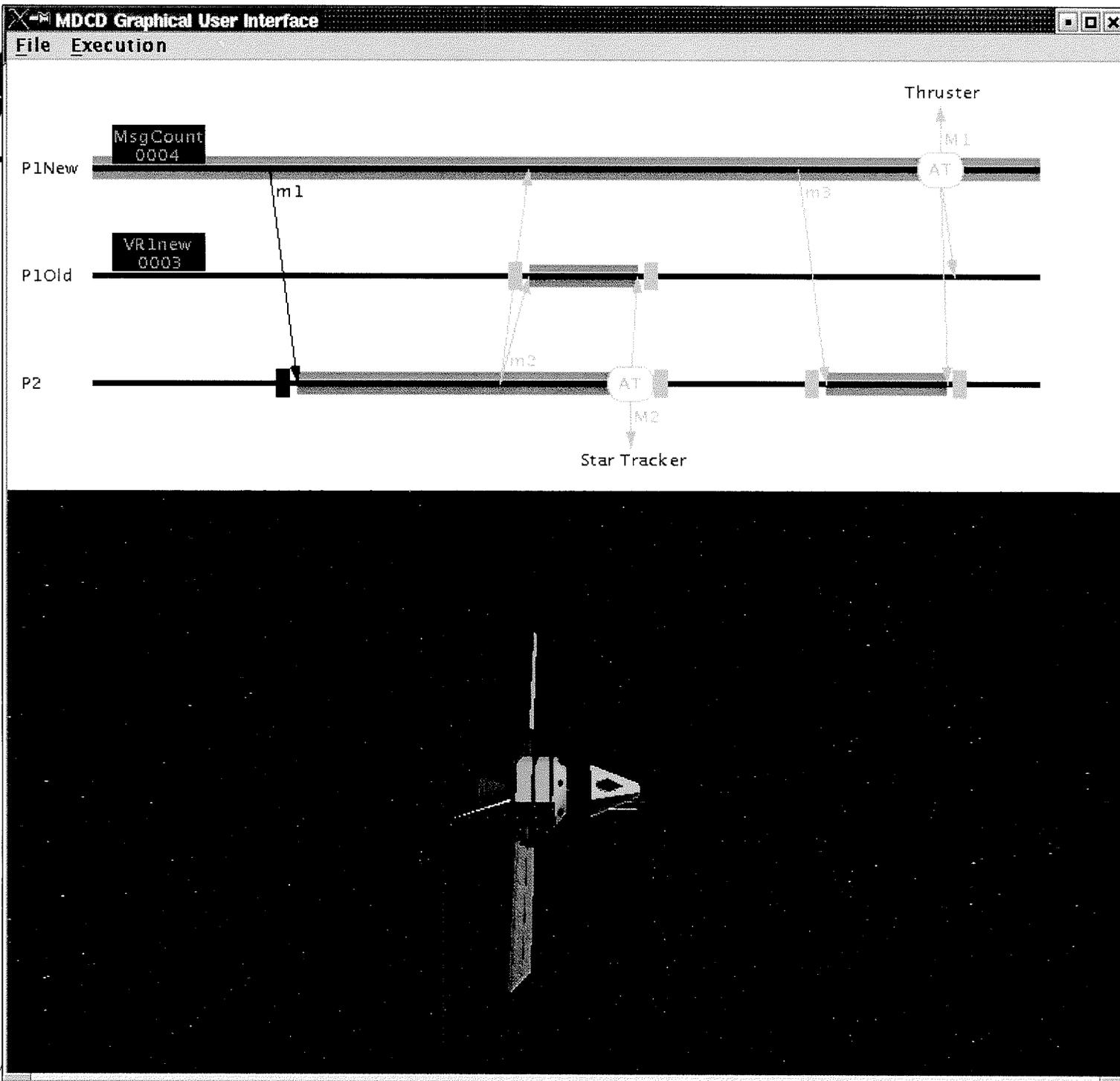


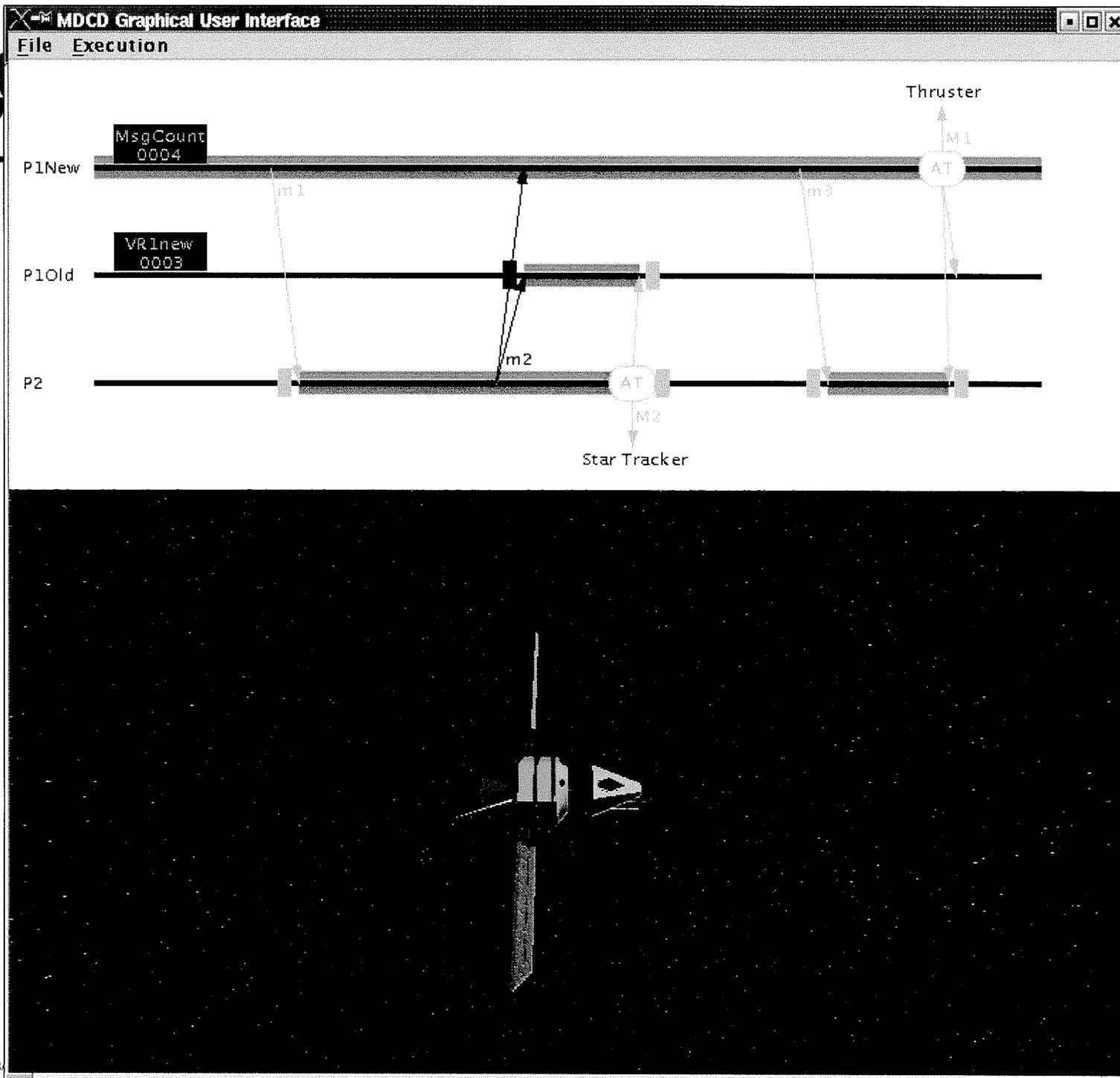


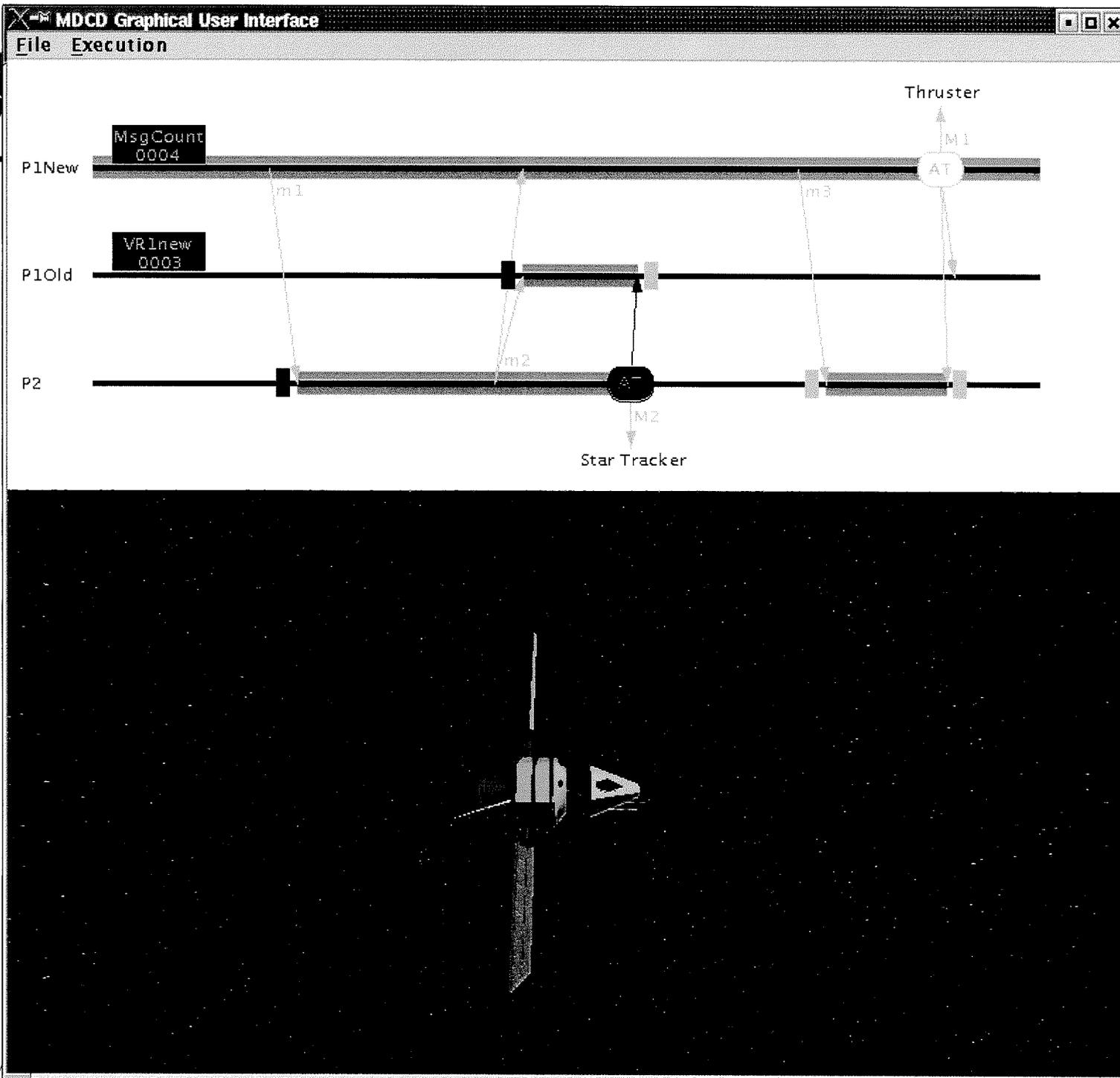


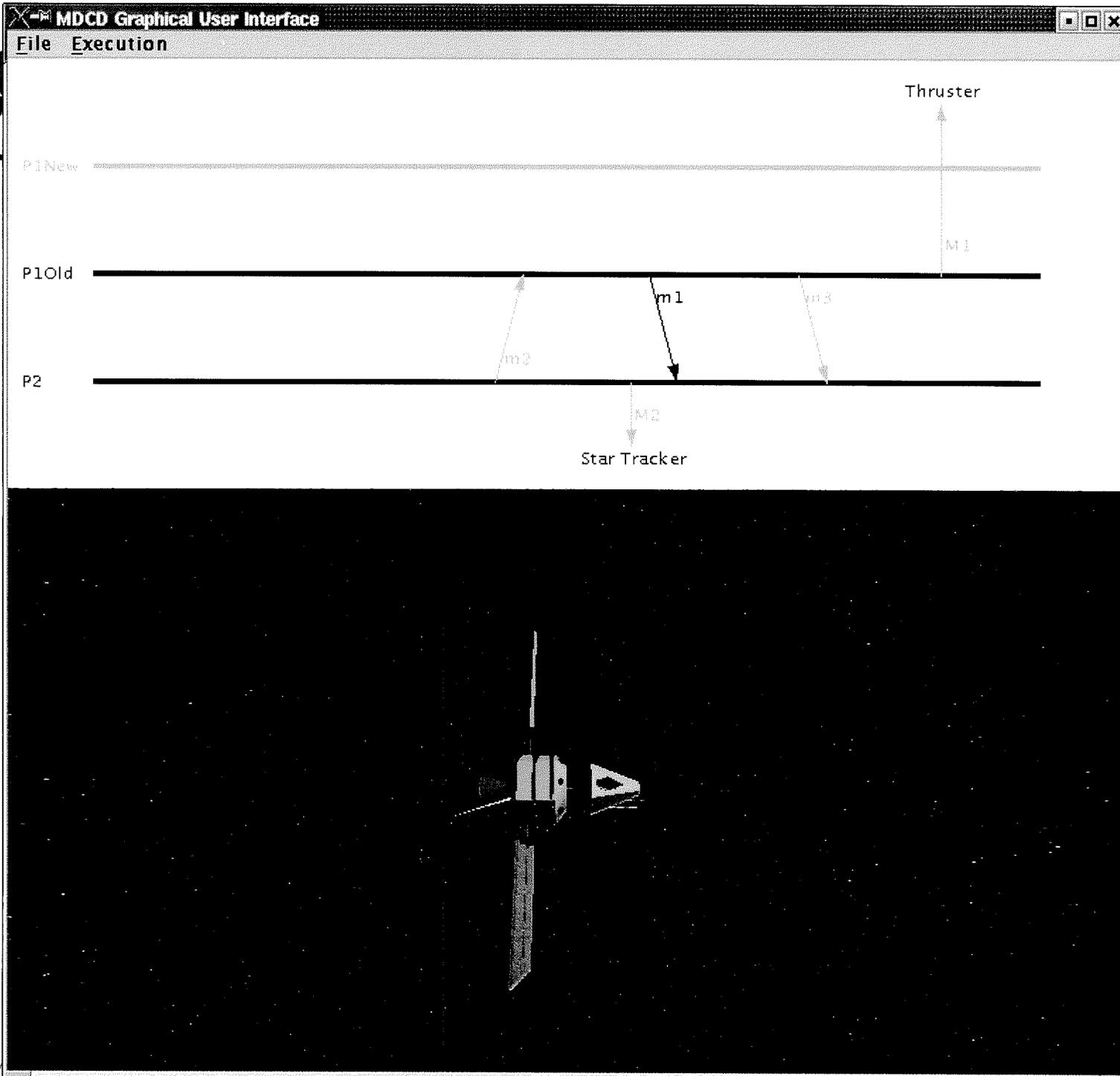


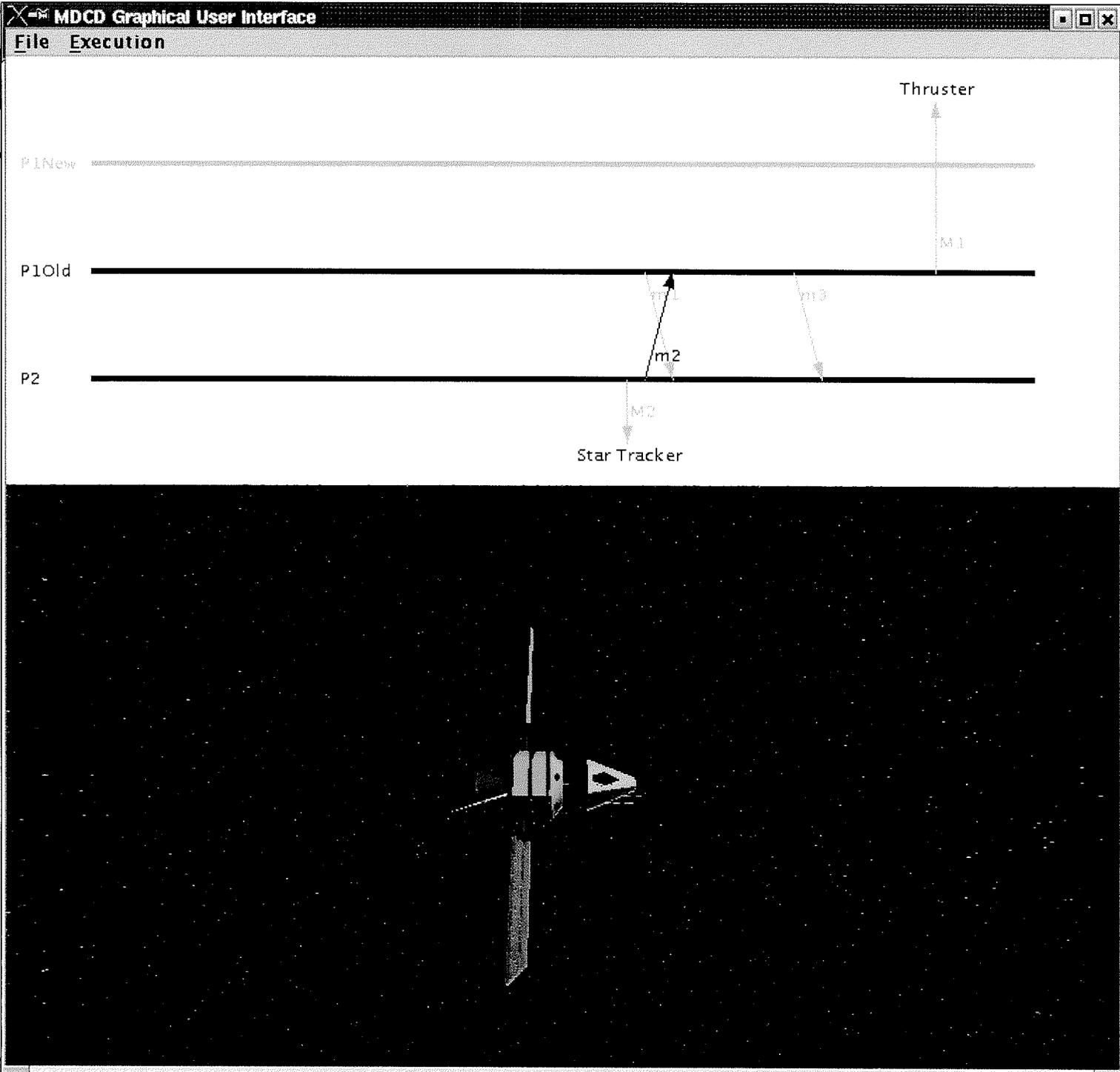


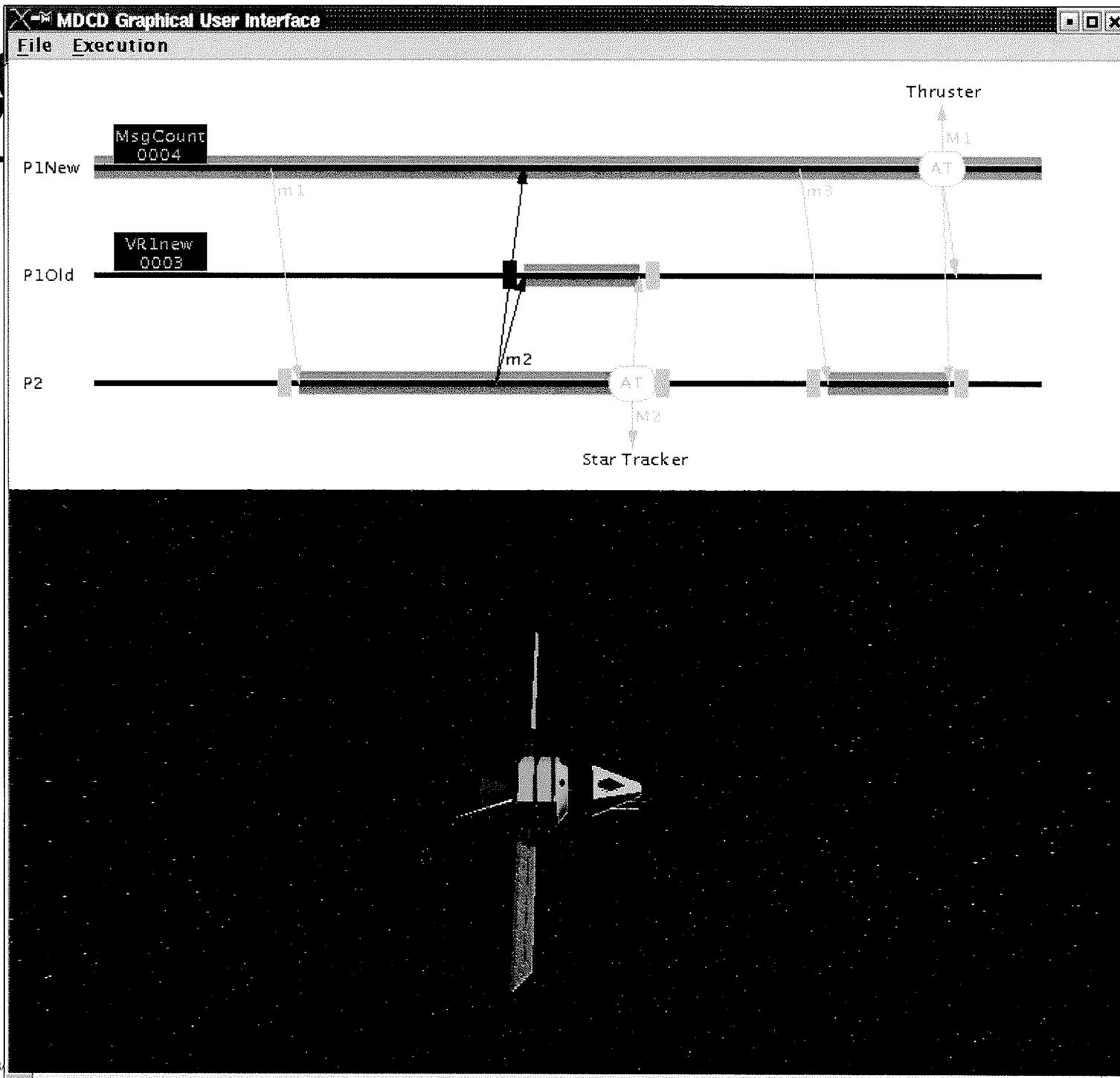


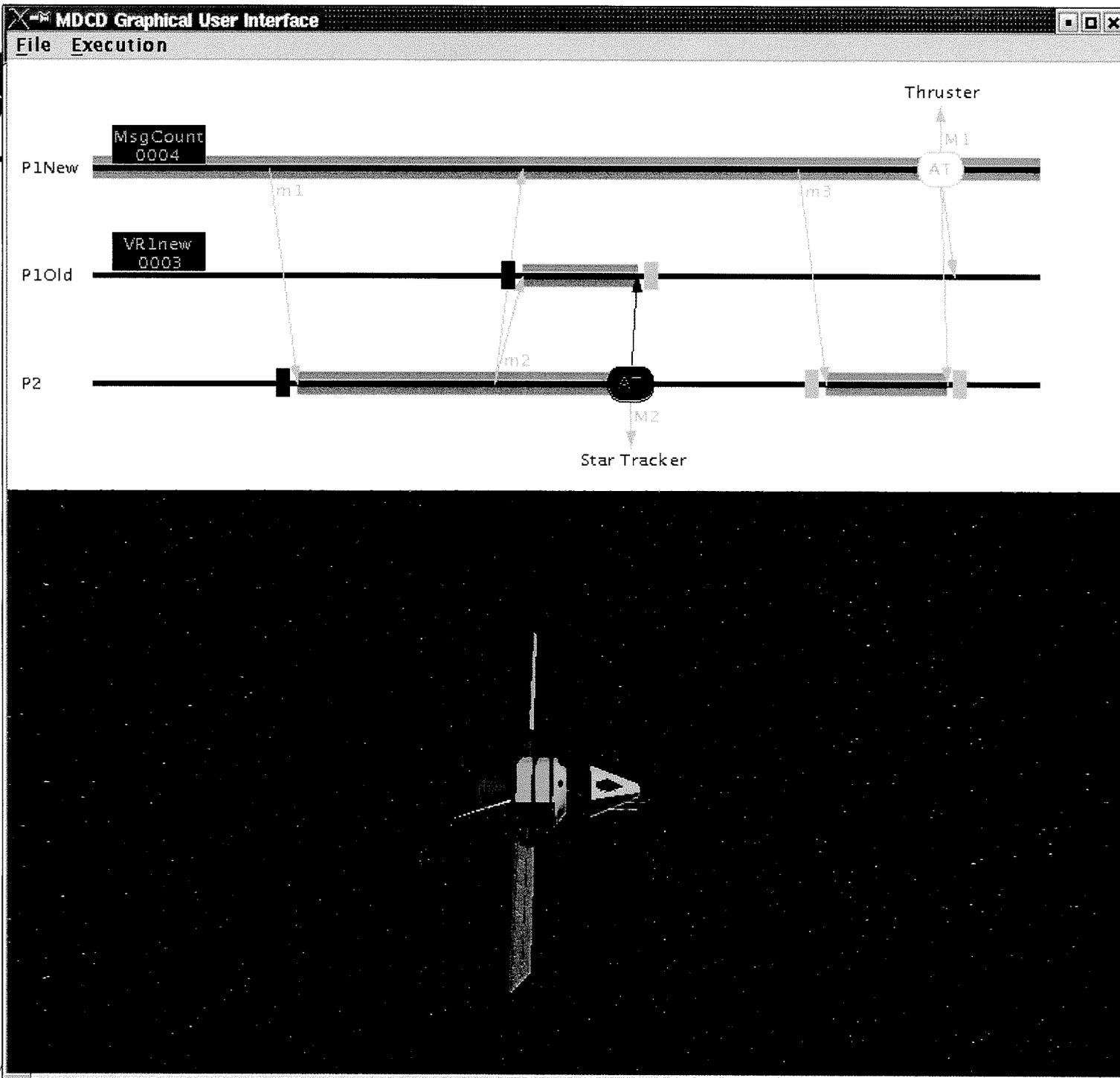


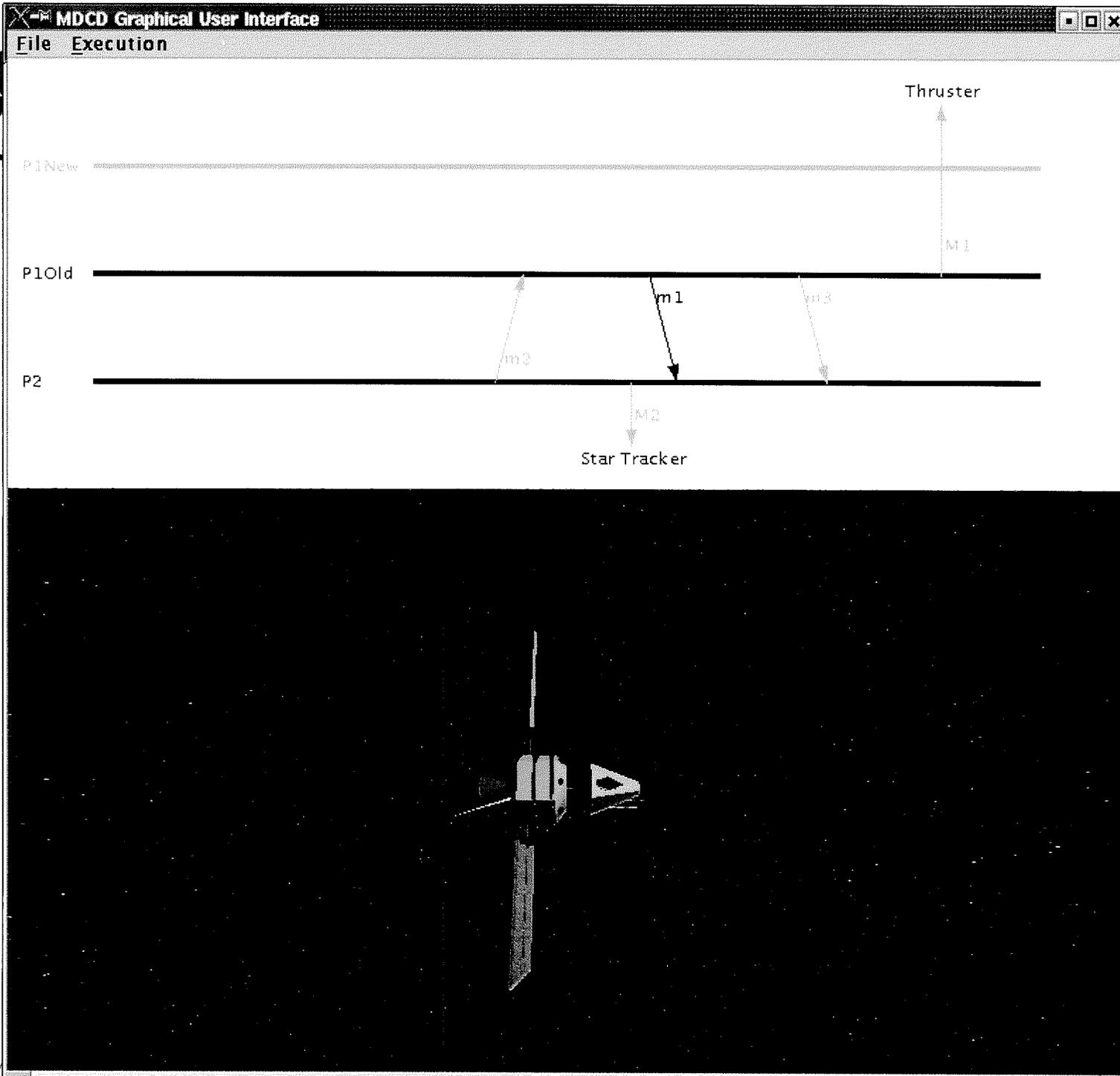


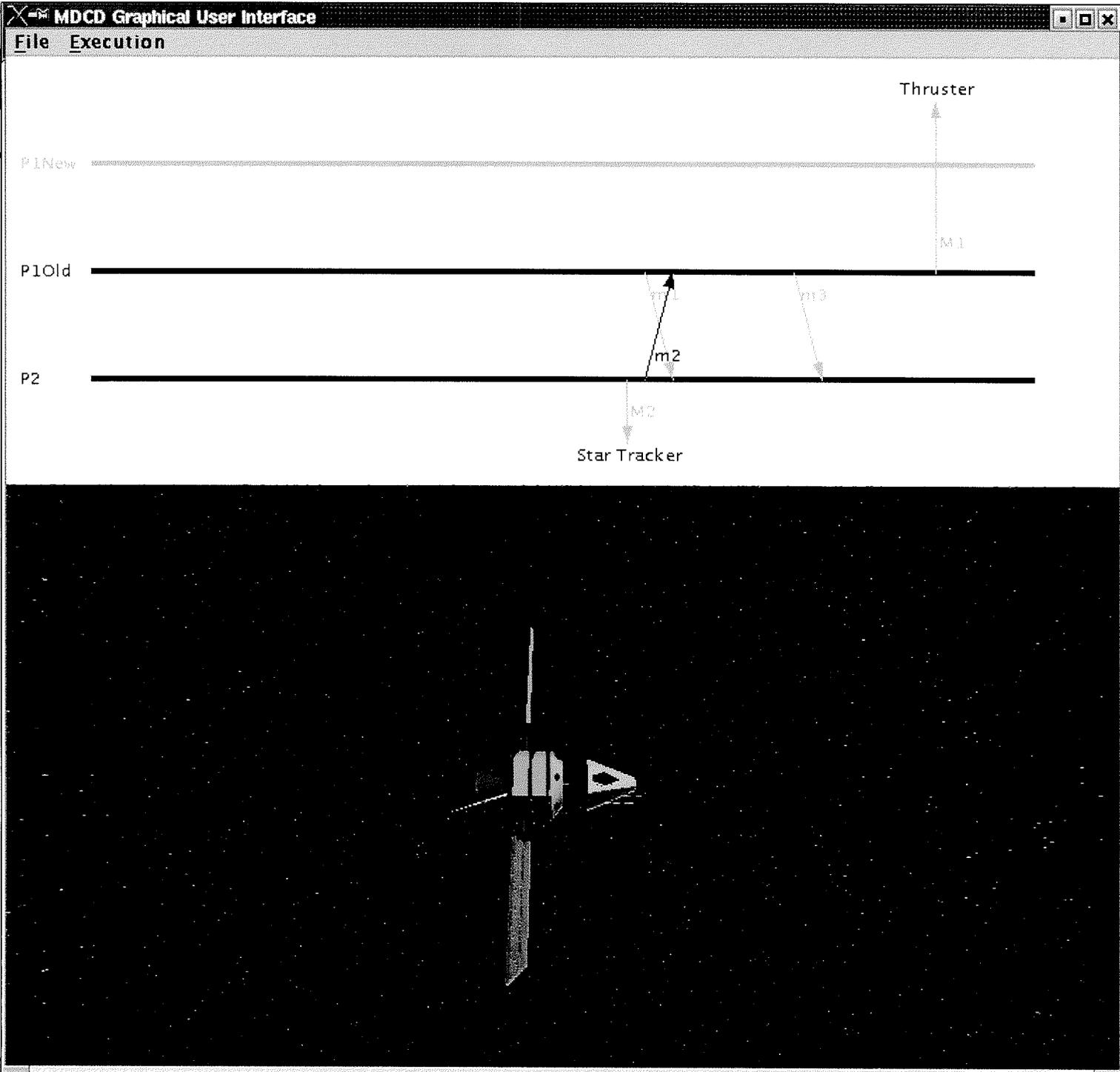


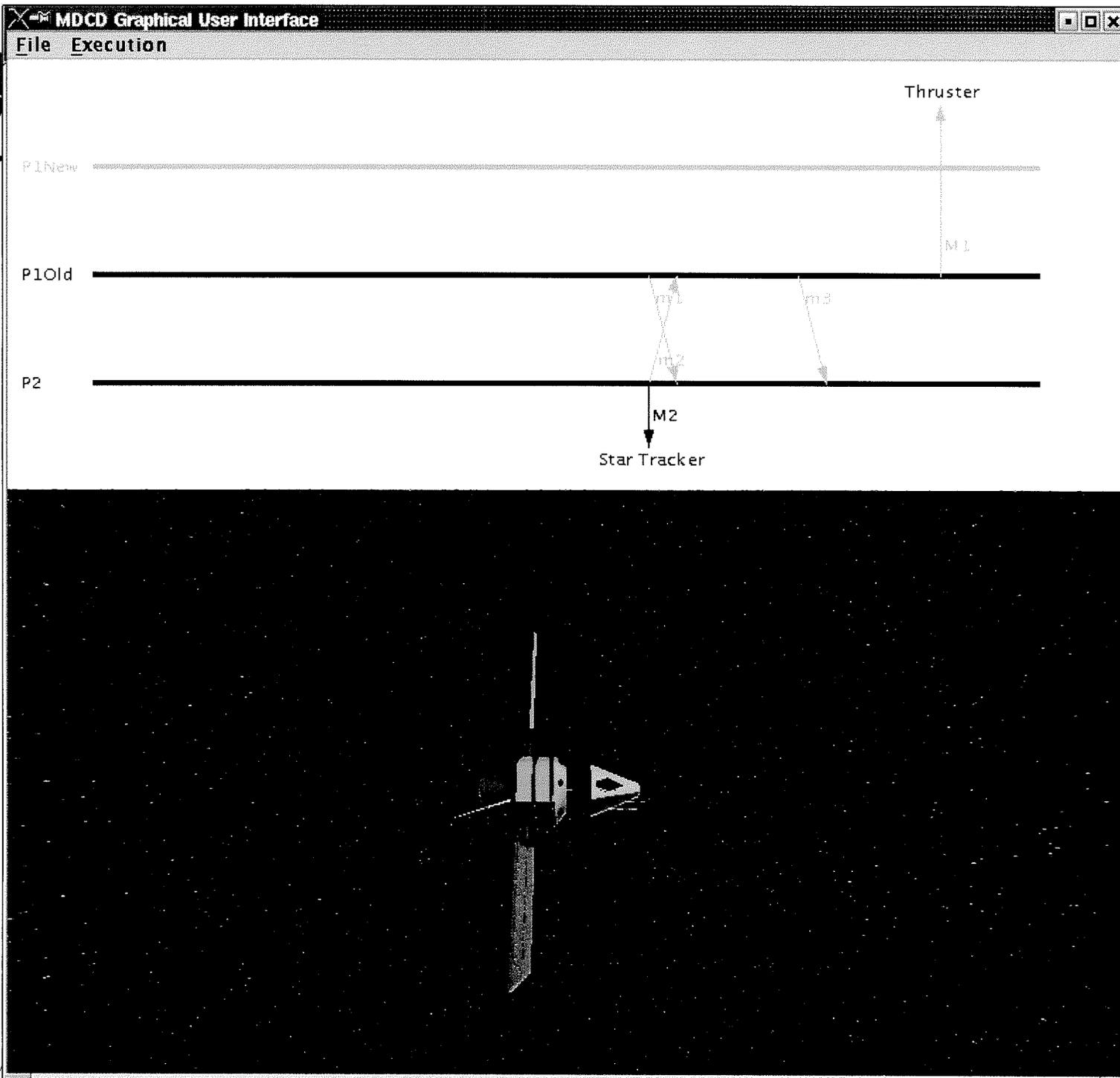


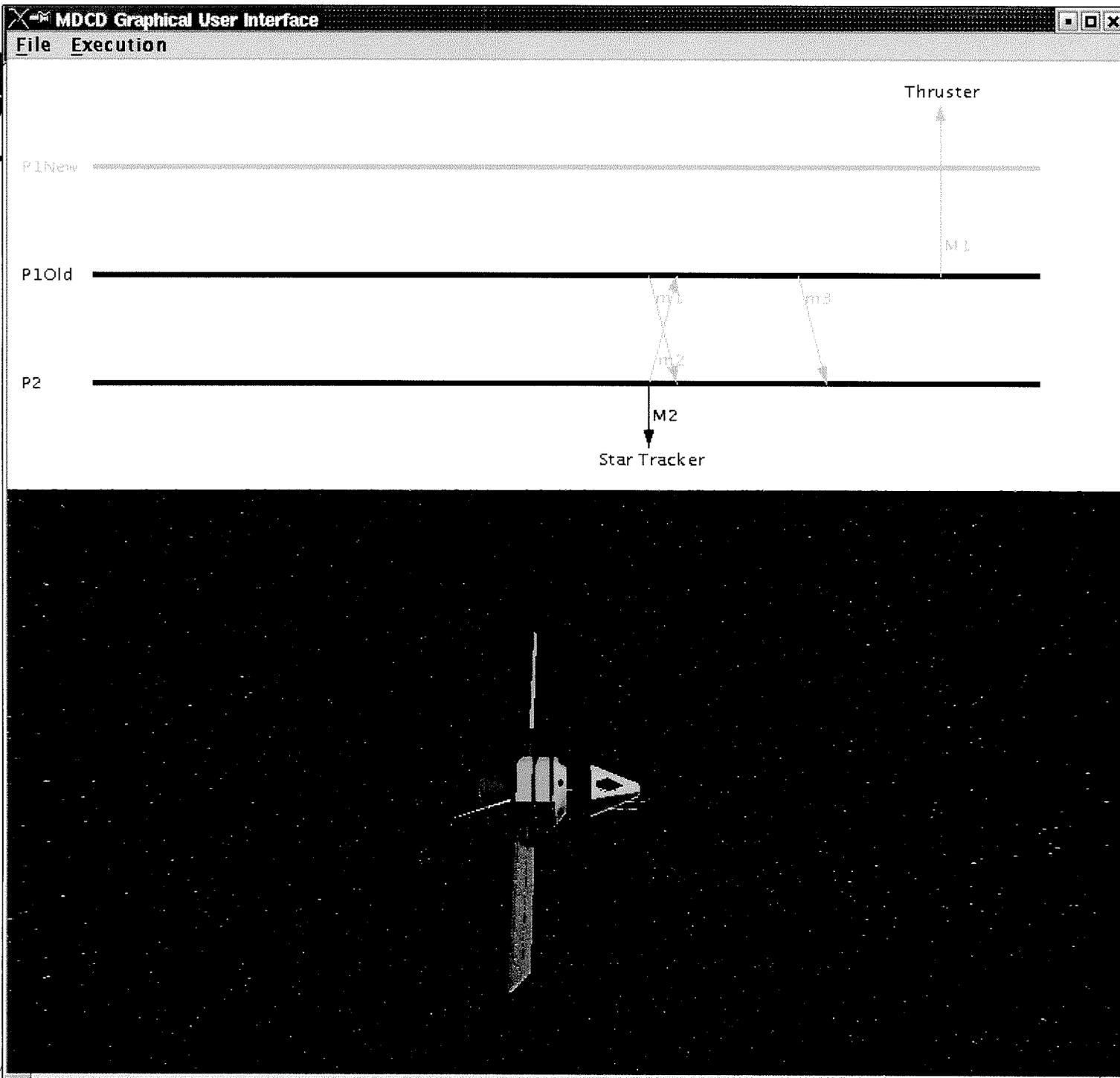


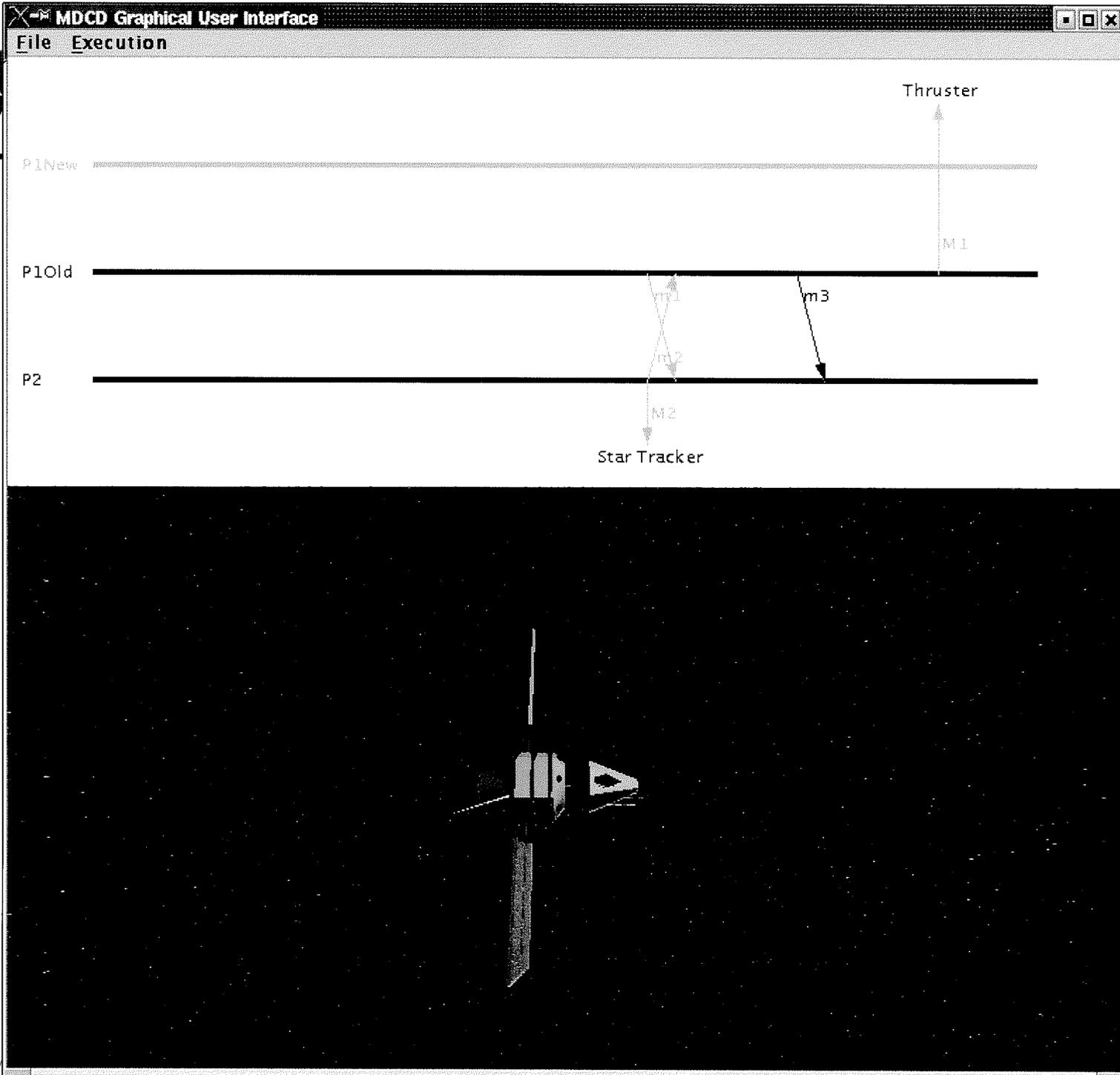


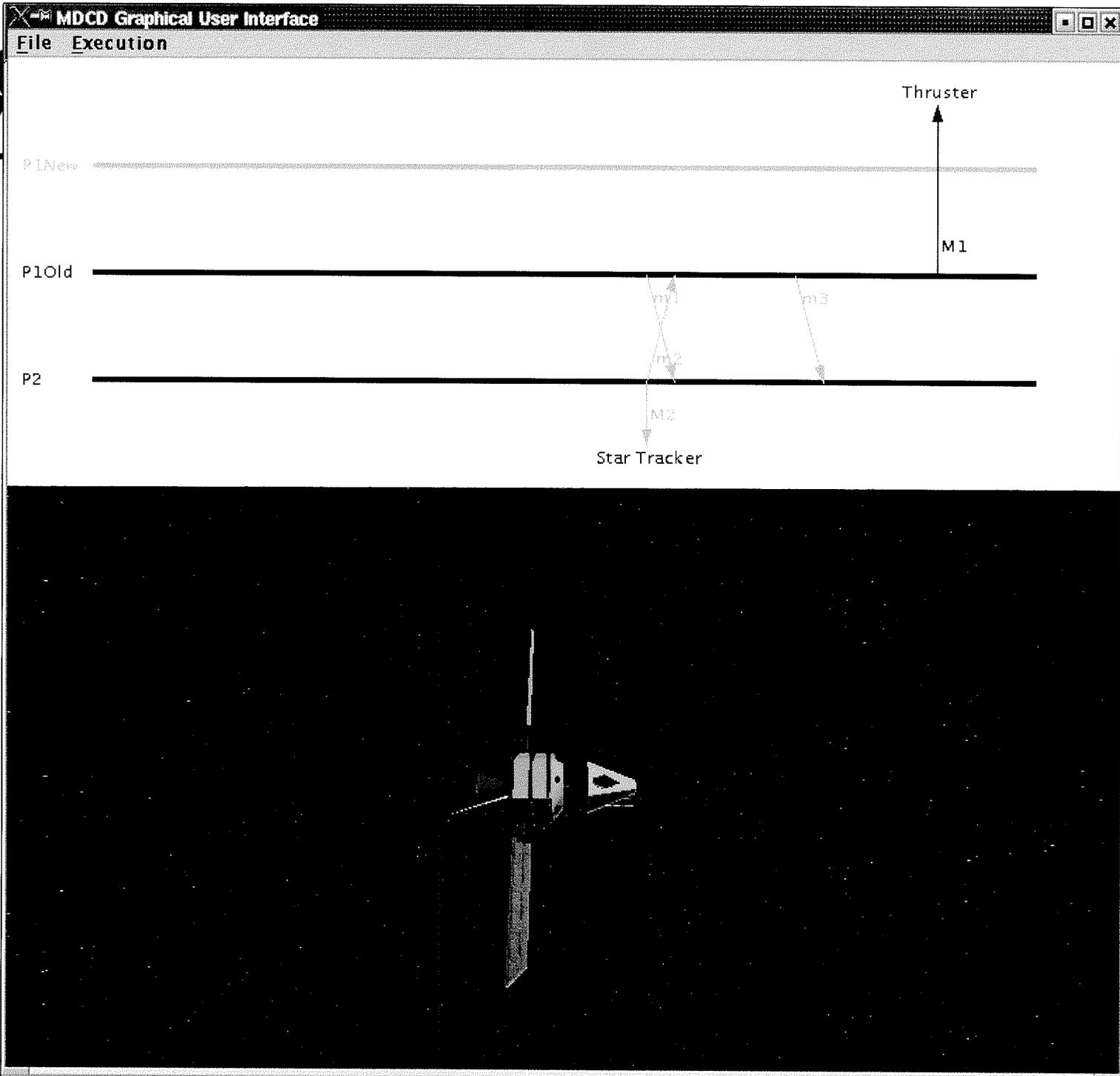


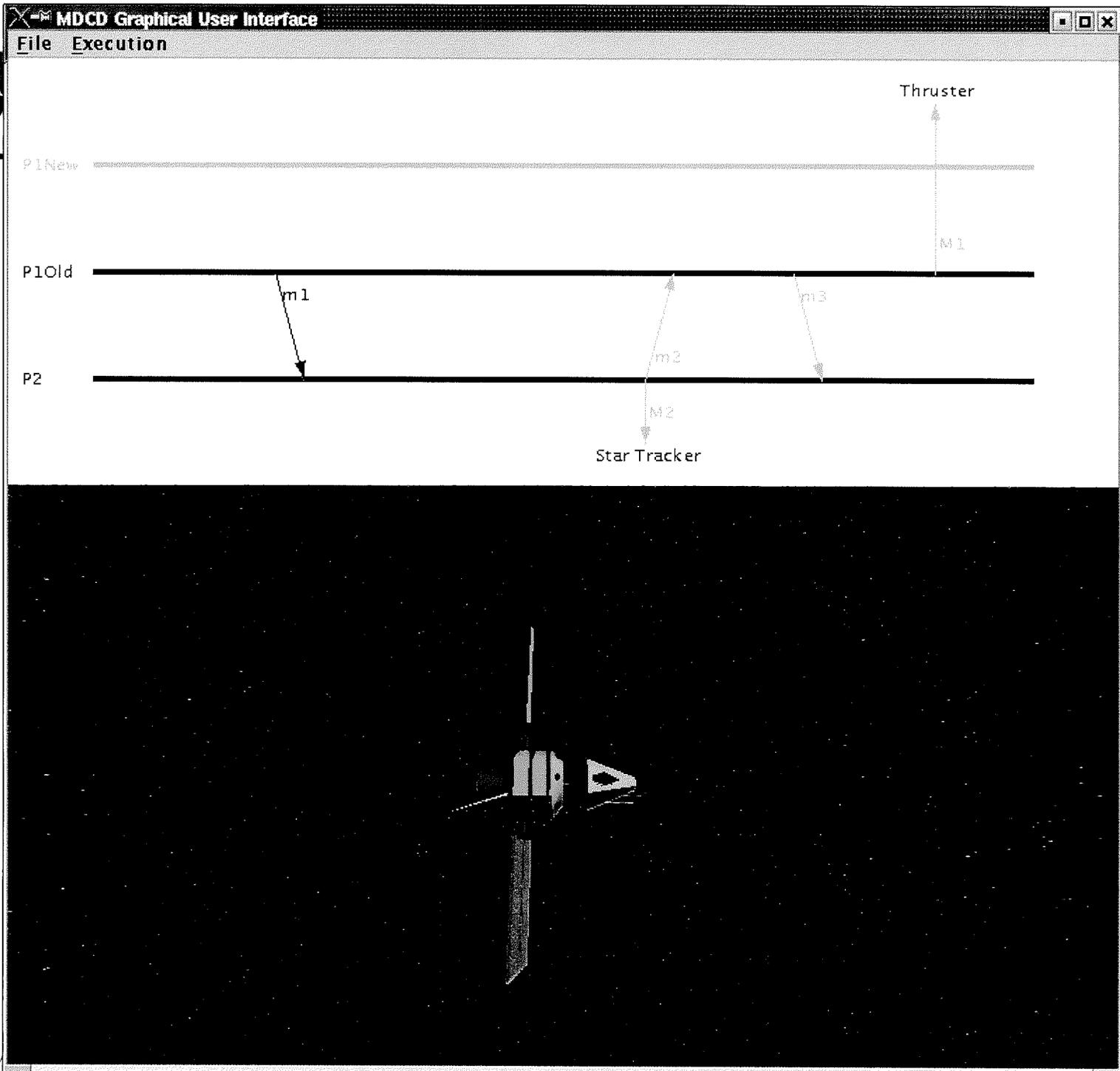


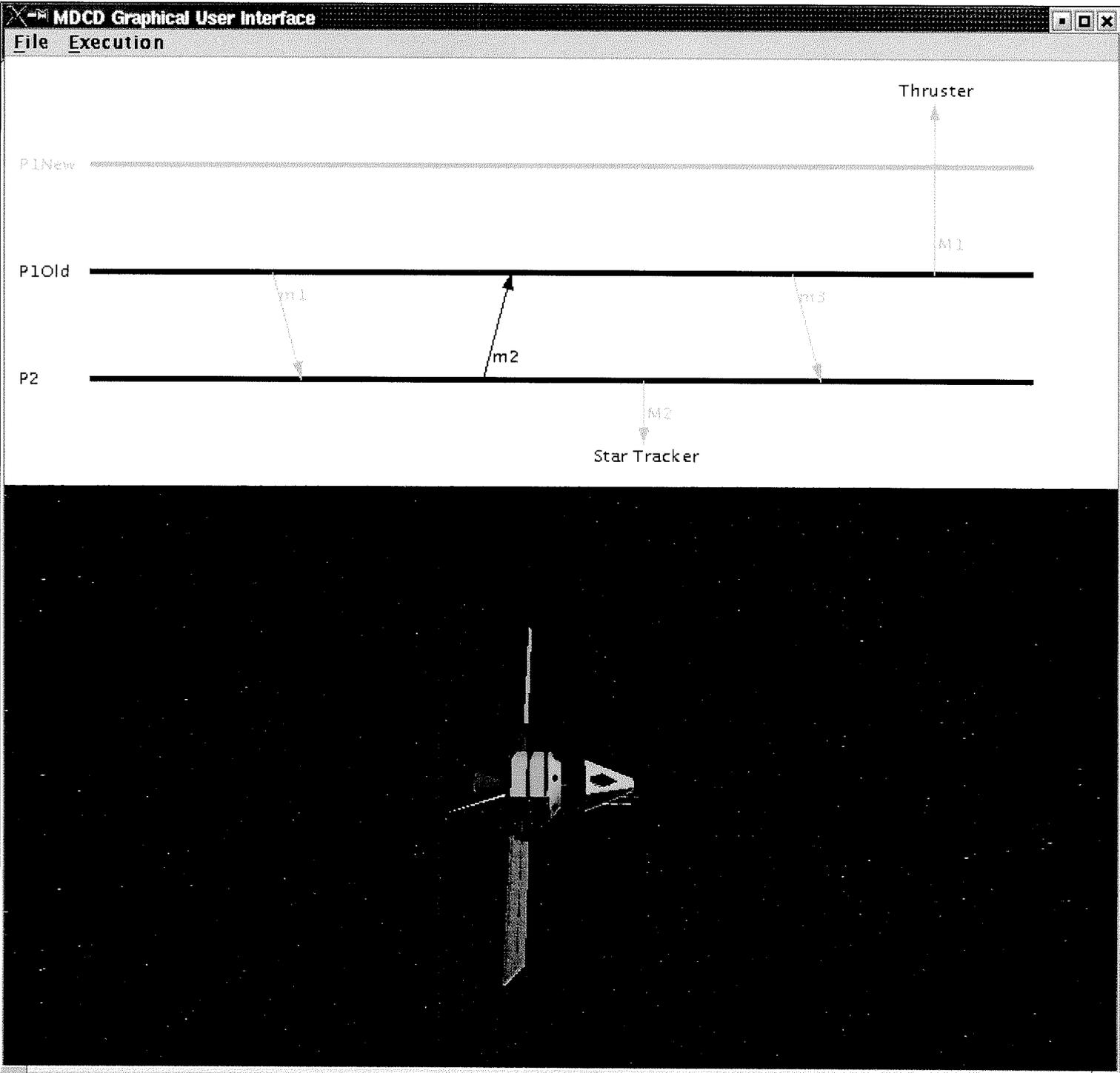


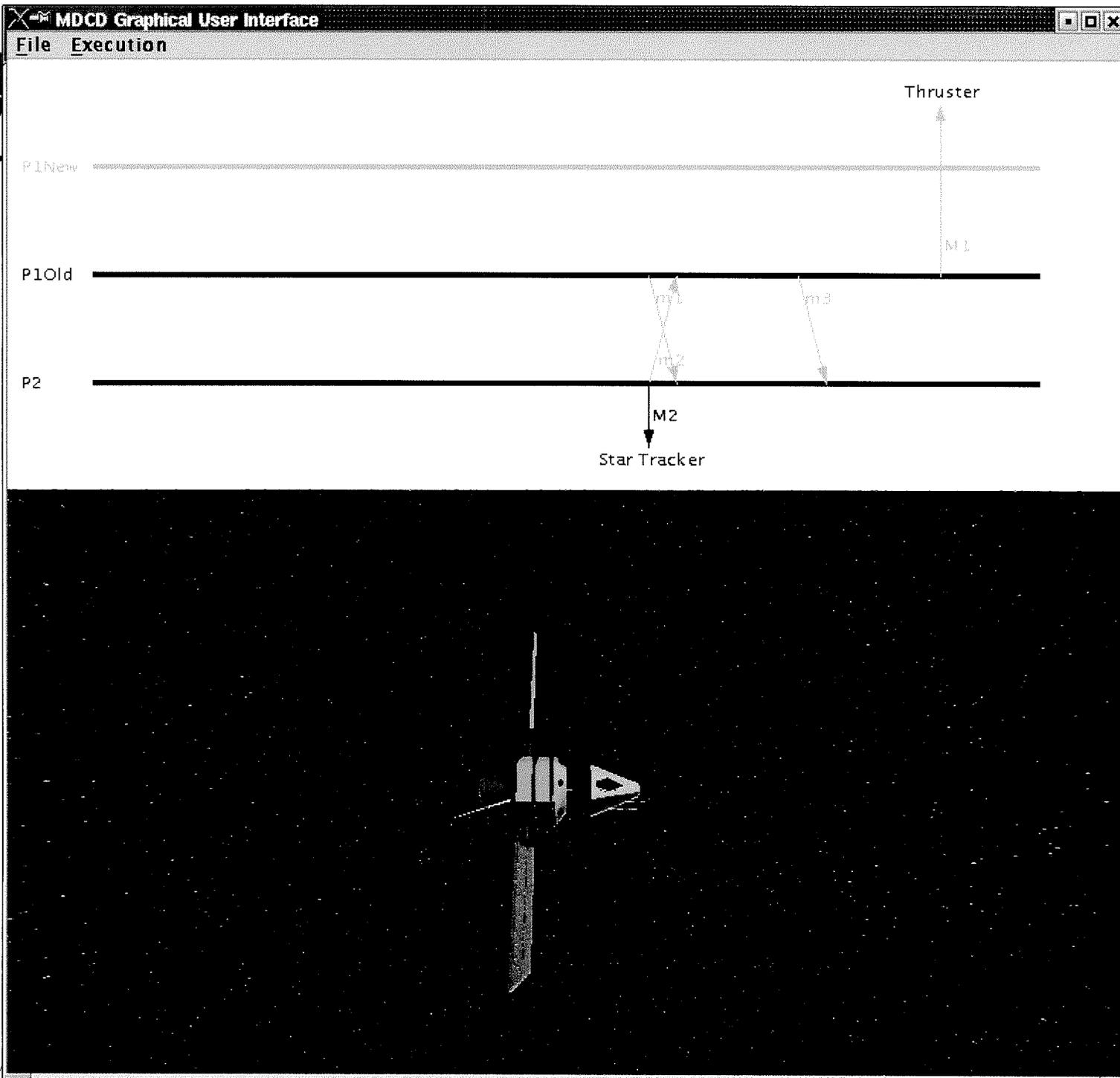


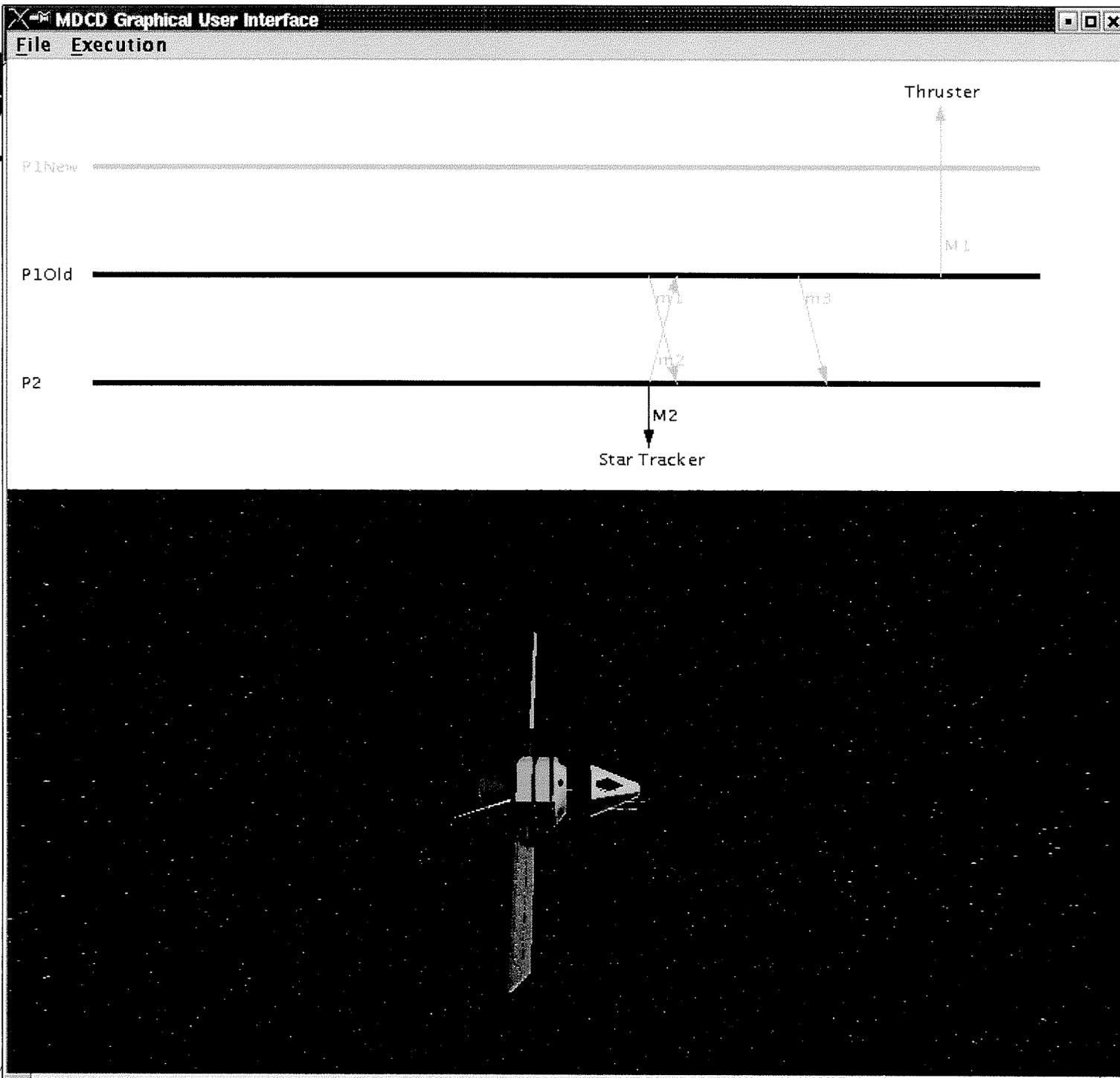


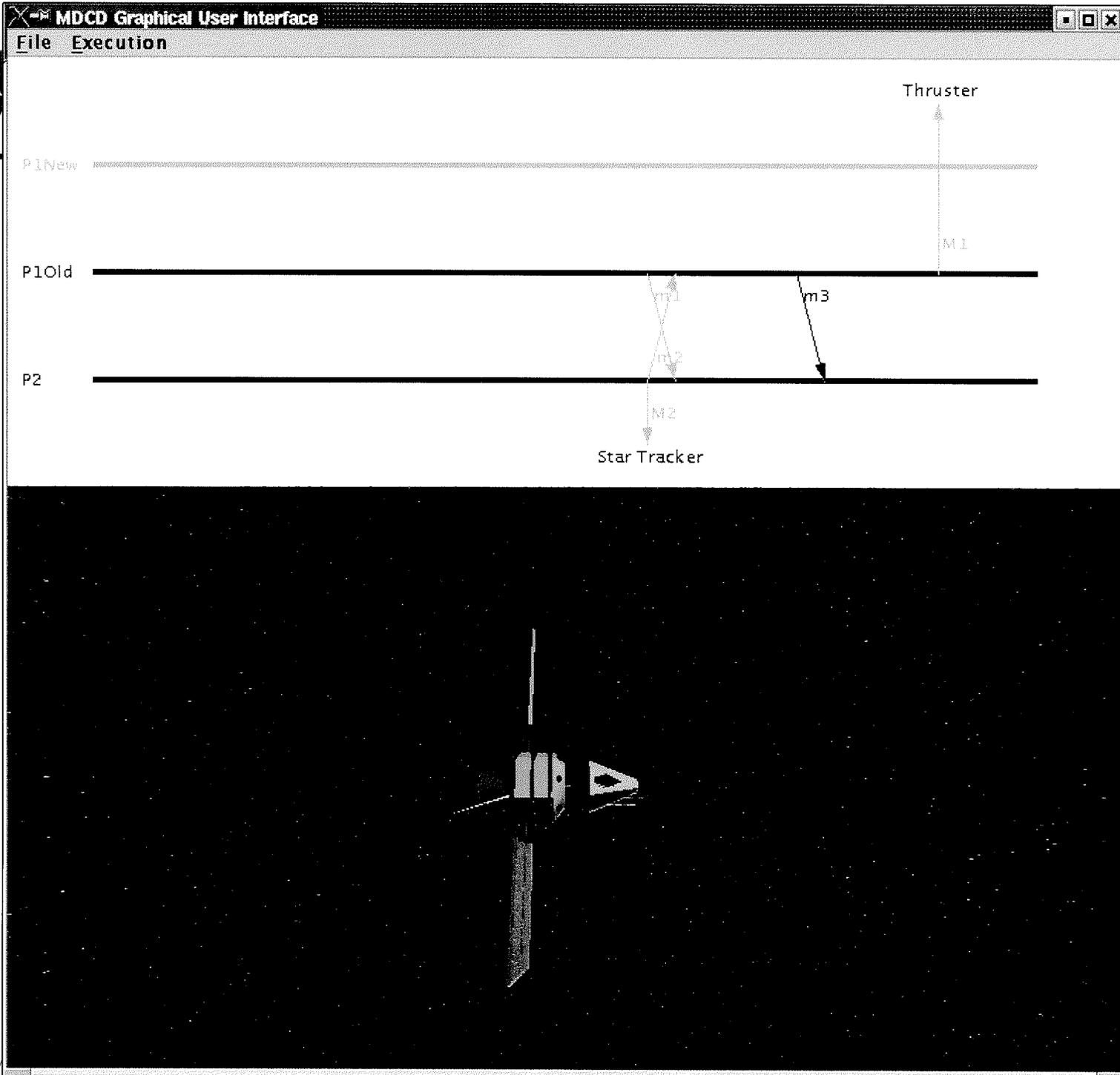


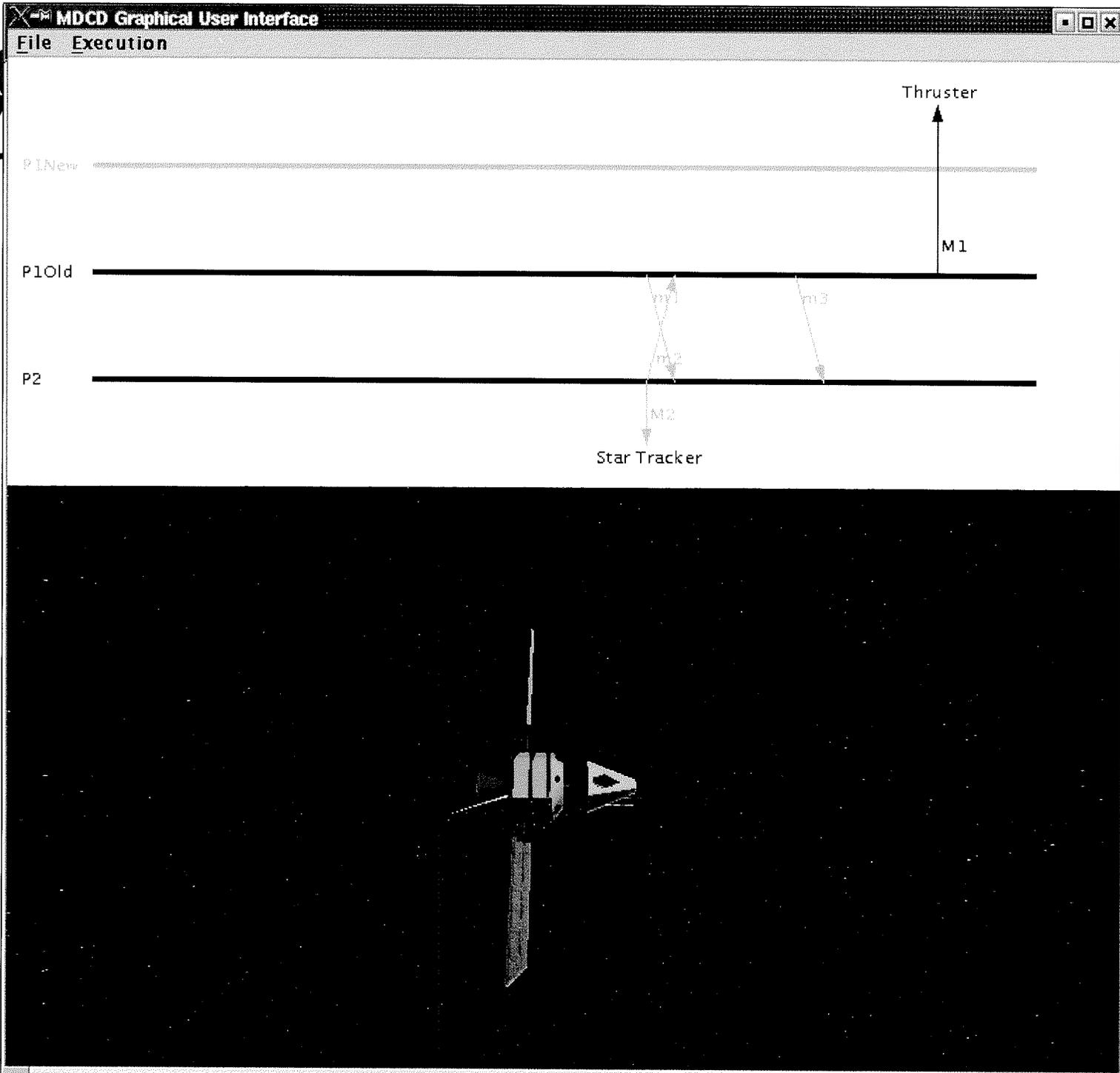


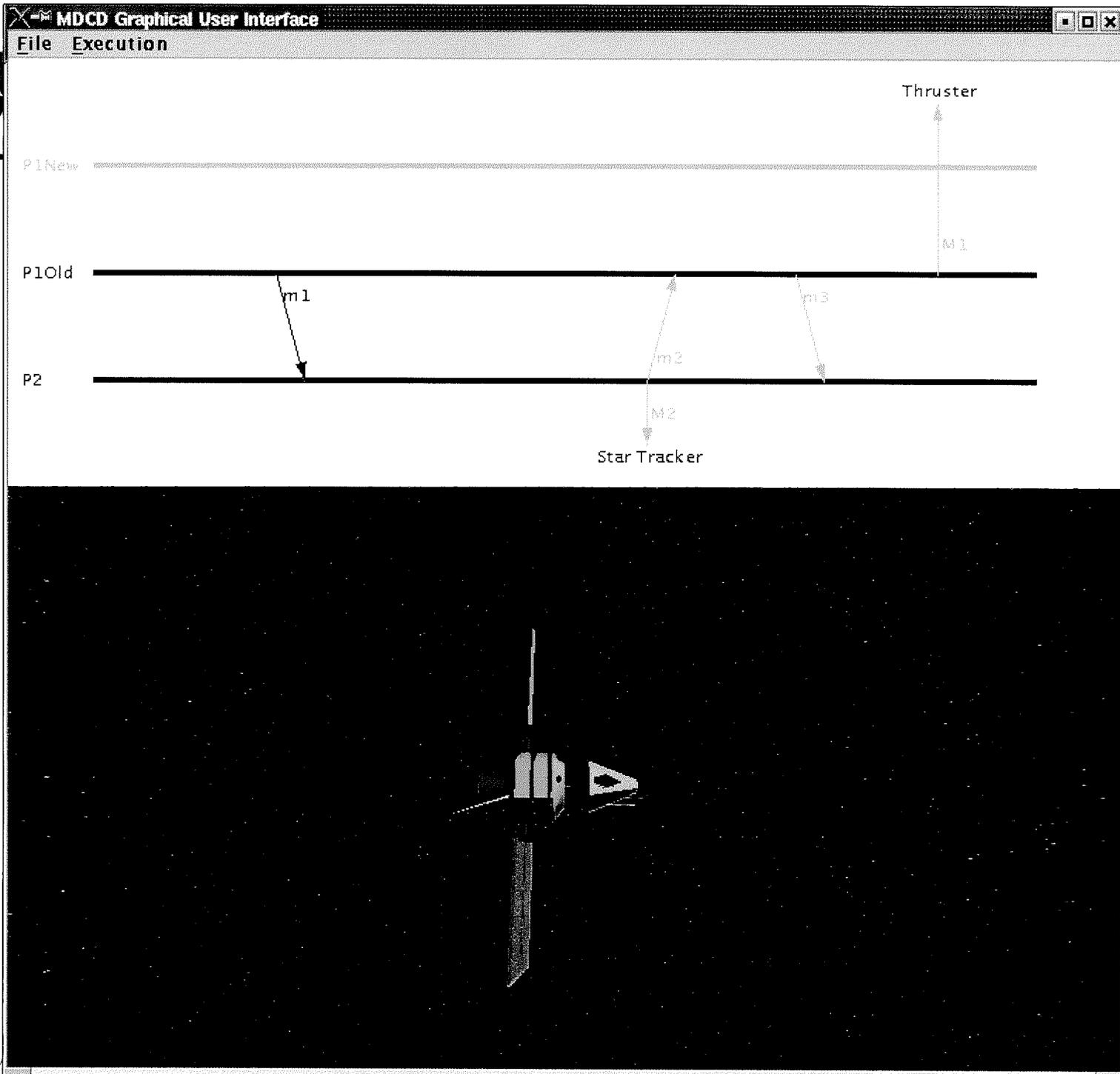


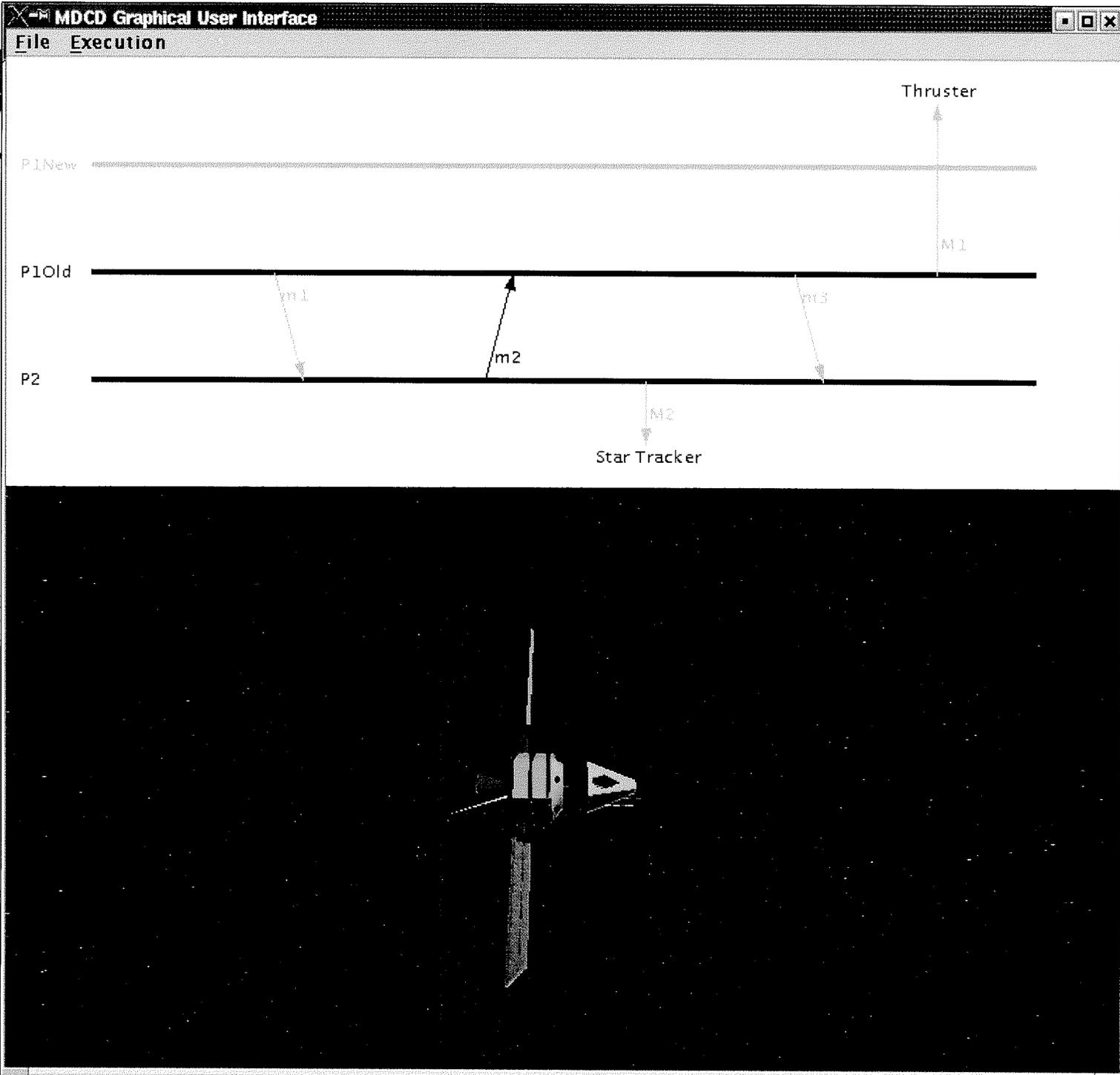


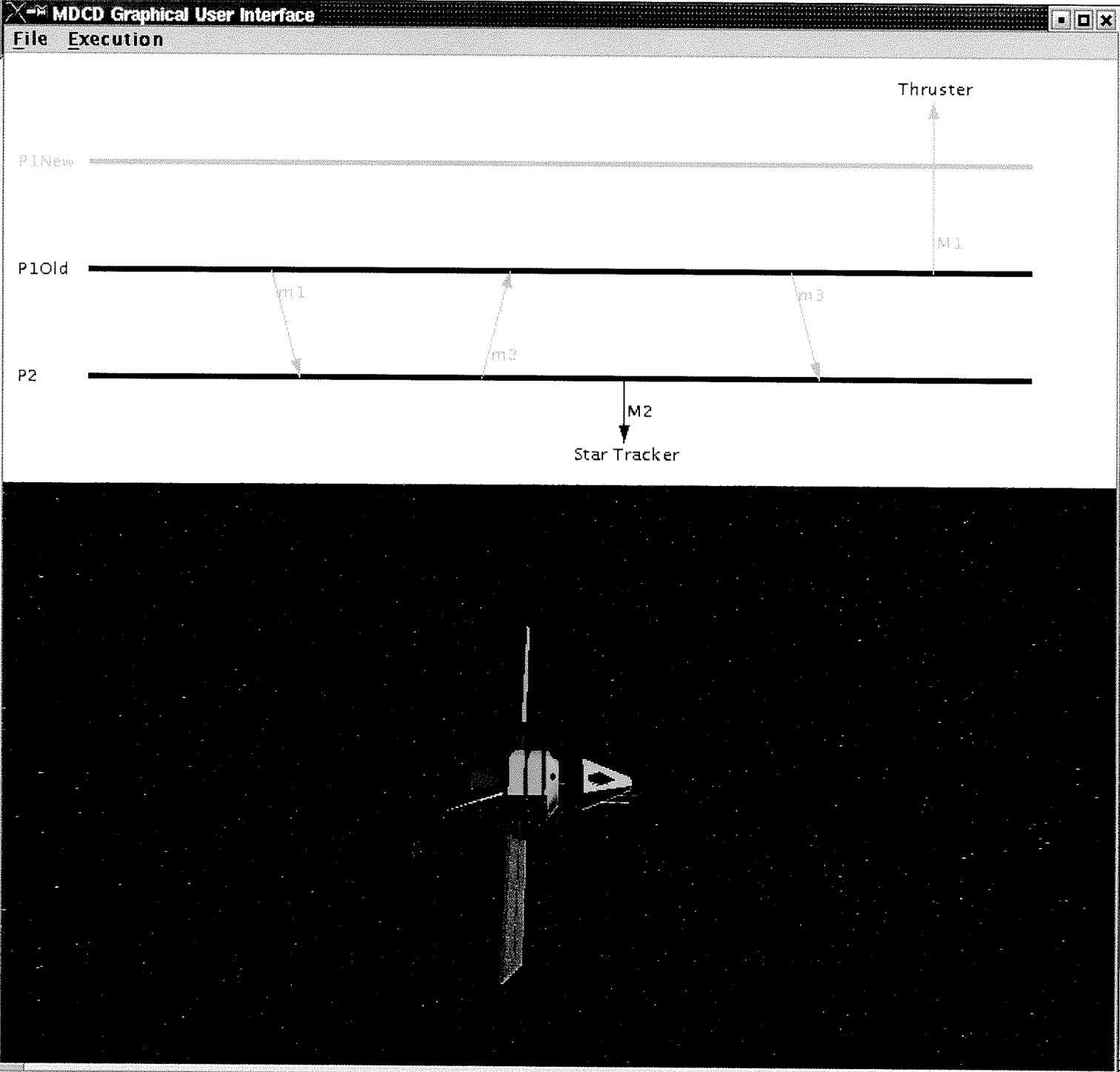


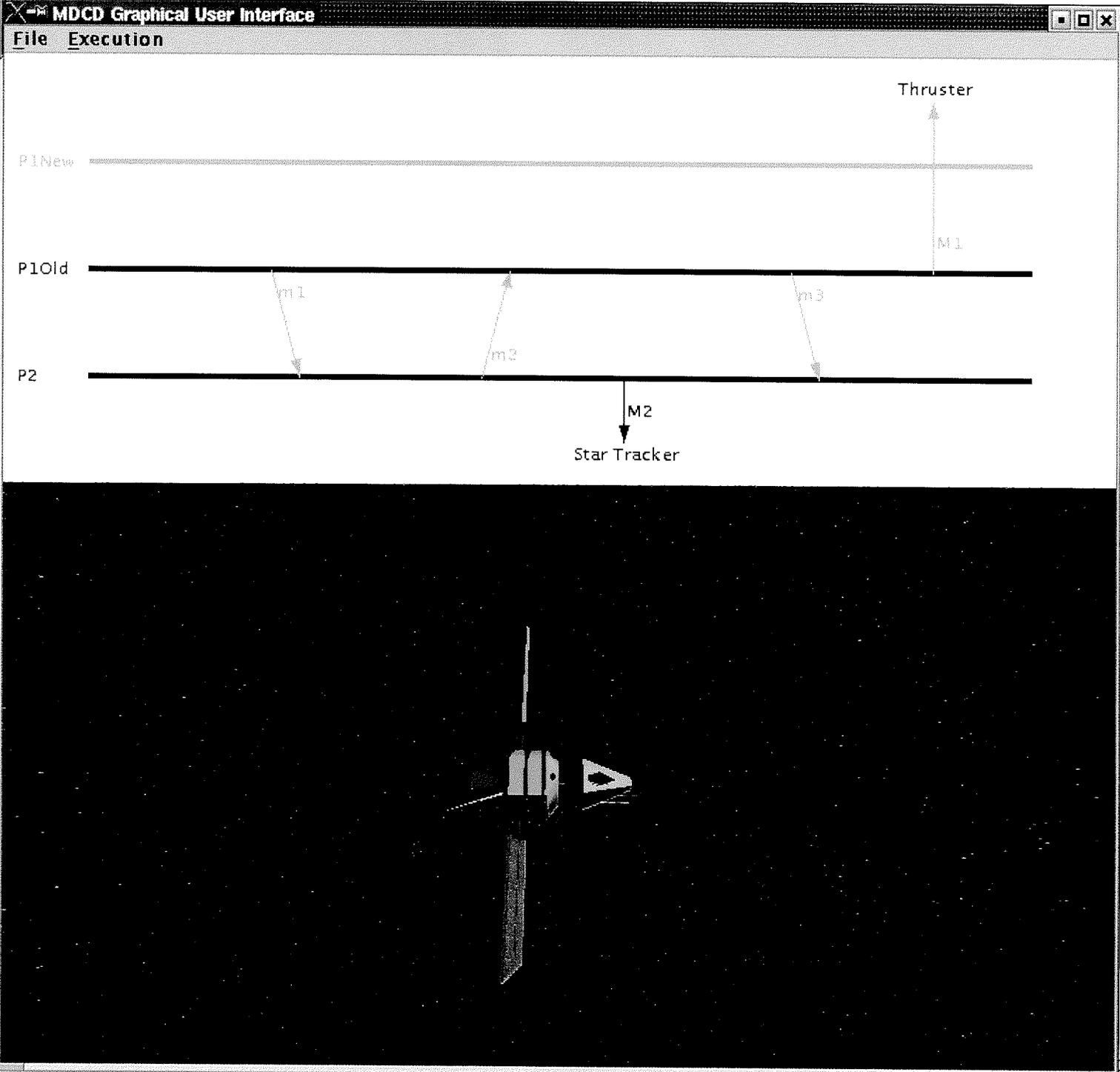


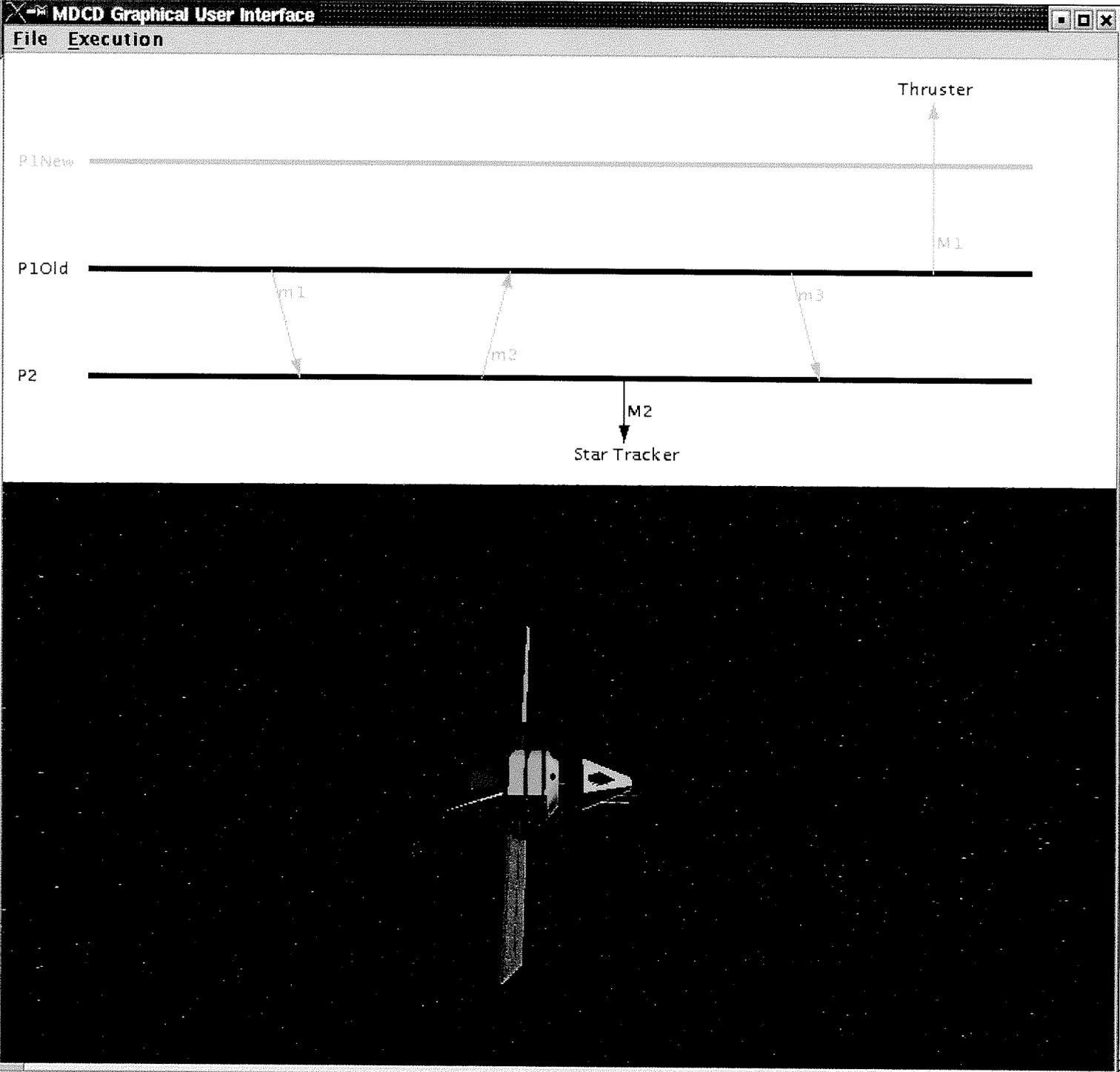


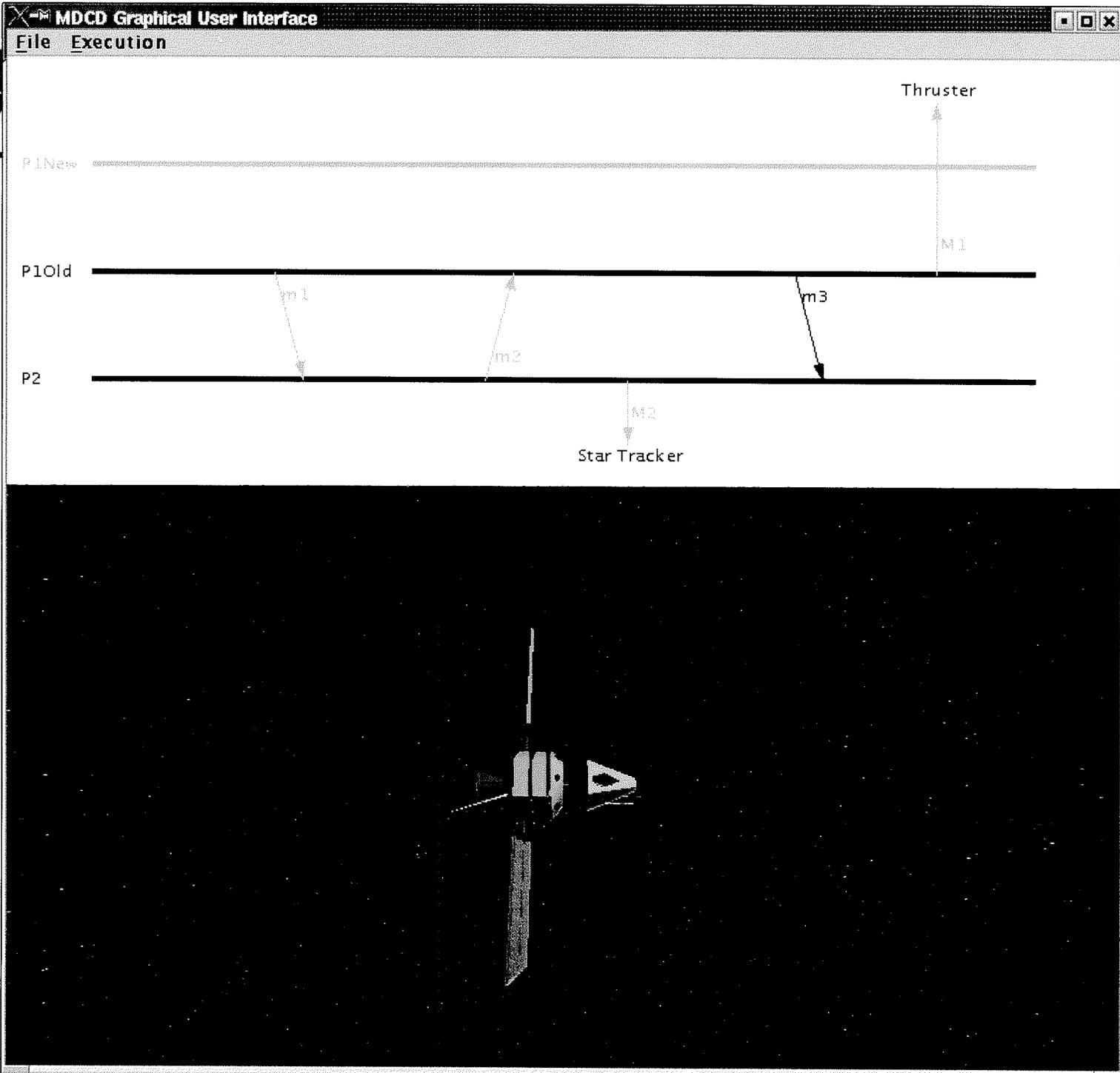


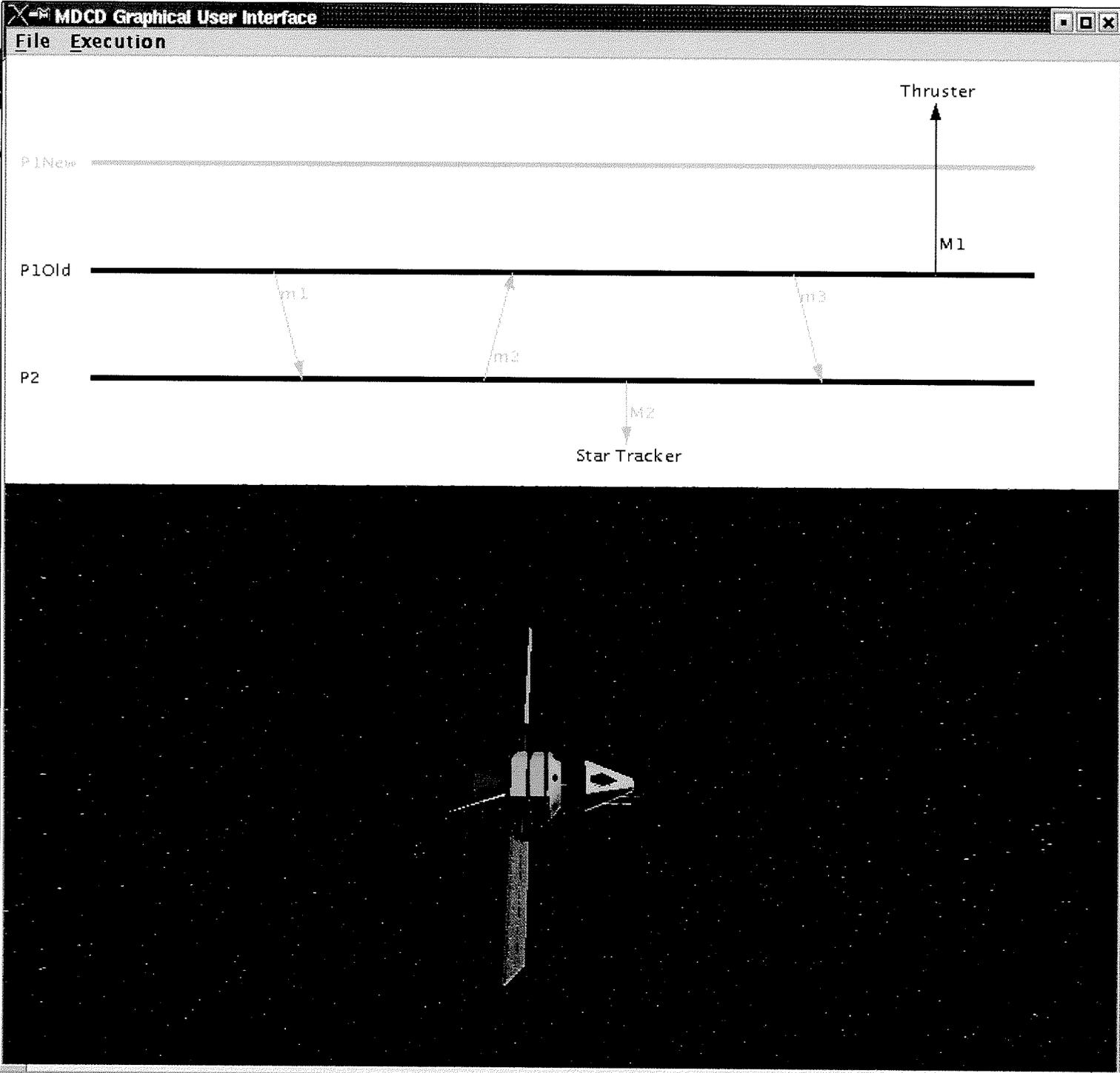














Direction of Dependable Computing Researches for Future Flight Missions



- 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