Failure Reports
5/9/01 Lecture #34 16.070

- Examine failure reports due to software
  - Mars Pathfinder
  - Ariane V
  - Mars Polar Lander
  - Therac 25

Mars Pathfinder Priority Inversion

- A few days after landing, spacecraft began experiencing total system resets, each resulting in losses of data
- Pathfinder contained an "information bus" -- shared memory area used to pass info between tasks
  - Access to bus was synchronized with mutual exclusion locks (mutexes)
  - Bus mgmt task: frequent, high priority to move data in/out of info bus
  - Meteorological data gathering task: infrequent, low priority. Acquires info bus mutex, writes to bus, then releases mutex
  - If interrupt caused bus mgmt task to be scheduled while mutex was held, and if bus mgmt task then attempted to acquire same mutex, bus mgmt task is blocked, waiting until meteorological task releases mutex
  - Problem: Medium priority communications task (long-running) scheduled while high-priority bus mgmt task is blocked.

Flight #1 of the Ariane V - The Controller Design

- Flight Control System
  - ➢ On-Board Computer executes flight program and controls solid booster nozzles and Vulcain cryogenic engine, via servo-valves and hydraulic actuators
  - ➢ Inertial Reference System (SRI)
    - Measures launcher attitude and movements in space
    - Has internal computer which calculates angles and velocities based on info from a "strap-down" inertial platform, with laser gyros and accelerometers
    - Data from SRI transmitted through data-bus to On-Board Computer (OBC)