Resource Access Control in Real-Time Systems

- Resources, Resource Access, and How Things Can Go Wrong: The Mars Pathfinder Incident

- Resources, Critical Sections, Blocking

- Priority Inversion, Deadlocks

- Nonpreemptive Critical Sections

- Priority Inheritance Protocol

- Priority Ceiling Protocol

- Stack-Based Protocols

Mars Pathfinder Incident

- Landing on July 4, 1997
- “experiences software glitches”
- Pathfinder experiences repeated RESETs after starting gathering of meteorological data.

- RESETs generated by watchdog process.
- Timing overruns caused by priority inversion.

- Resources:
  research.microsoft.com/~mbj/Mars_Pathfinder/Mars_Pathfinder.html
Priority Inversion on Mars Pathfinder

Task `bc_dist` becomes active and blocks on mutex. Other low-priority tasks start and are preempted. Task `ASI/MET` starts and locks mutex. Task `bc_sched` detects overrun.

Diagram:

- Task `bc_dist` (high priority)
- Other tasks (low priority)
- Task `ASI/MET` (low priority)