CS6150: RELIABLE COMPUTING

Course Description

Techniques for writing reliable software including n-version programming, fault-tolerant data structures and formal proofs of correctness. Rollback and recovery methods. Fault-tolerant hardware and methods of hardware error detection and correction. Prerequisites: Admission to MS in CS program, or consent of department, plus CS 3350 or equivalent.

Course Syllabus

- **Fault-Tolerant Hardware**
  - Tandem Computer Architecture(*)
  - Stratus computer architecture(*)
  - The (4,2) computer architecture
  - Hardware error detection & correction through coding(*)
  - Redundant array of inexpensive disks (RAID)(*):

- **Fault-Tolerant Software**
  - Formal proofs of correctness(*)
    - Axiomatic semantics and proof rules
      - weakest precondition
      - strongest post condition
      - invariants and assertions
    - Formal specification - an overview
      - VDM or Z
      - Algebraic specification and data types
    - Roll back and recovery, check pointing(*)
    - Software safety
    - N-version techniques(*)
    - Fault tolerant data structures and scrubbing(*)
    - Use of error detection codes in software
    - Data integrity in distributed transactions
      - Validation protocols for transactions
      - Distributed check pointing

- **Estimation of Mean Time Between Failures (MTBF)**
  - Numerical aspects of software testing
  - Domain testing
  - Effect of redundant components
  - Effect of scrubbing
  - Standards for software fault-tolerance

(*)These topics are core material to be covered every time the course is taught.