Software Reliability and Safety

CSE 8317 — Fall 2006

Prof. Jeff Tian, tian@engr.smu.edu
CSE, SMU, Dallas, TX 75275
(214) 768-2861; Fax: (214) 768-3085
www.engr.smu.edu/~tian/class/8317.06f

SSE.3: Formal Methods for Safety

- Formal Methods for Specification and Verification
- Axiomatic Approach
- Functional and Other Approaches
- Applications to Safety Problems

FM in SSE

- Leveson approach
  - ▷ Focused verification
  - ▷ Driven by hazard analysis
  - ▷ Distributed over development phases
  - ▷ Which FM? ad hoc

- Specific FM: SQE Ch.15 (slides!)
  – but with a safety focus/perspective

- Other applications
  - ▷ Need automation ⇒ model checking.
  - ▷ Less formality
    ⇒ Parnas/tabular method & formal insp.
  - ▷ With statistical testing ⇒ Cleanroom
  - ▷ Yih/Tian: PSC (next module)