Software Reliability and Safety

CSE 8317 — Fall 2009

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/8317.09f

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)

FM: 7 Myths and 10 Commandments

- Seven myths (Hall, 1990)
  - ▷ FM guarantee that software is perfect
  - ▷ They work by proving correctness
  - ▷ Only highly critical system benefits
  - ▷ FM involve complex mathematics
  - ▷ FM increase cost of development
  - ▷ They are incomprehensible to client
  - ▷ Nobody uses them for real projects
- Refutations and discussions
- However, some validity/quantified

FM: 7 Myths and 10 Commandments

- 10 Commandments ... 10 Years Later (Bowen and Hinchey, 2006)

  I. Thou shalt choose
  an appropriate notation
  II. Thou shalt formalize
  but not overformalize
  III. Thou shalt estimate costs
  IV. Thou shalt have a FM guru on call
  V. Thou shalt not
  abandon thy trad. dev. methods
  VI. Thou shalt document sufficiently
  VII. Thou shalt not
  compromise thy quality standards
  VIII. Thou shalt not be dogmatic
  IX. Thou shalt test, test, and test again
  X. Thou shalt reuse

- Still valid after 10 years!