Software Reliability and Safety

CSE 8317 — Spring 2013

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/8317.13s

SSE.4: SSE Frontier

- CCSCS, TFM and Safety
- Prescriptive Specification Checking (PSC)
- STAMP and STPA
- Other New Development

PSC and Safety

- Why?
  - ▷ Accident reports/empirical data:
    – mostly interface/interaction problems
  - ▷ Need systematic analysis
  - ▷ Existing approaches: combined idea?

- How?
  - ▷ Model: TFM (two-frame model)
  - ▷ Analysis of interfaces/interactions
  - ▷ Root cause of I/I problems:
    – physical vs. logical frame consistency
  - ▷ FM and particularly model checking ideas

- Slides SQE 16.5

STAMP and STPA

- Leveson's recent work:
  - ▷ After "Safeware"
  - ▷ Roots in systems and control theory
  - ▷ STAMP: Systems-Theoretic Accident Model and Processes
  - ▷ STPA: STamP Analysis

- Several papers

- New book by Nancy G. Leveson:
  "Engineering A Safer World: Systems Thinking Applied to Safety,"
  MIT Press, 2011.
  ISBN: 9780262016629

Other Recent Work

- Survey of new accident:
  - similar findings

- FM-related work:
  - larger systems and applications

- Safety as part of dependability:
  - dependable and secure computing
  - safety trade-off
  - diversity and dependability (and safety)

- New application domains:
  - net-centric systems
  - defense related DoD/DARPA/etc.
  - NASA work
  - IoT (internet of Things) and safety
  - many others

- Many active new frontiers for SSE research