

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

OV.2. Review

- QA Alternatives/Activities and Their Relation to CSE 8317
- Fault Tolerance in SSE: SQE Ch.16a
- Common Techniques: SQE Ch.20 & 21

Review: QA Alternatives

- Defect prevention/removal/tolerance
 - ▷ SQE/slides online:
 - Part I (particularly Chapter 3)
 - Parts II and III (high-level only)

- Defect prevention:
 - ▷ Error source elimination
 - ▷ Error blocking

- Defect removal: Inspection/testing/etc.

- Defect tolerance:
 - ▷ Fault tolerance (failure↓)
 - ▷ Damage minimization (safety)

QA Alternatives and 8317

- SRE relation/applications:
 - ▷ QA alternatives directly work with SRE
 - ▷ Functional relation: reliability \sim failure
 - ▷ Remember? error \Rightarrow fault \Rightarrow failure
 - ▷ All will affect the end results/failures
 - ▷ Closer to failure
 - \Rightarrow closer to SRE activities
 - (e.g., system and acceptance testing)

- SSE relation/applications:
 - ▷ More focused (not as broad)
 - ▷ Hazard focus (small subset of failures)
 - ▷ Specifics to be examined later

QA Alternatives and 8317

- Inspection:
 - ▷ Wide applicability (diff periods/artifacts)
 - ▷ Conceptual/static faults
 - ▷ Human intensive, varied cost

- Applications in SRE and SSE
 - ▷ Fault eliminations:
 - helps both reliability and safety
 - for SRE/SSE – high/low fault density cases
 - ▷ Scenario-based (focused) inspection:
 - for SRE – common usage scenarios
 - for SSE – FTA/ETA-based scenarios/elements
 - ▷ Early reliability prediction
 - ▷ Safety constraints and inspection

QA Alternatives and 8317

- Formal verification: SQE Ch.15
 - ▷ Works on code with formal spec.
 - ▷ Practicality: high cost → benefit?
 - ▷ Human intensive, rigorous training

- Applications in SRE and SSE
 - ▷ High cost ⇒ mostly in SSE
 - ▷ Module SSE.3
 - ▷ Focus through FTA and/or ETA
 - ▷ Leveson's approach:
 - safety and other constraints
 - carried through dev. process
 - ▷ Other adaptations:
 - table-driven, model checking, etc
 - PSC, module SSE.4

QA Alternatives and 8317

- Testing:
 - ▷ Dynamic/run-time/interaction problems
 - ▷ BBT/WBT and coverage/usage questions

- Applications in SRE and SSE
 - ▷ Chief application domain for SRE
 - ▷ OP-based testing (UBST):
 - basis for reliability modeling
 - ▷ Earlier phases: WBT/BBT with coverage
 - ▷ Indirect link to SSE

QA Alternatives and 8317

- Fault tolerance:
 - ▷ Dynamic problems
 - ▷ Technique problems (independent NVP?)
 - ▷ Process/technology intensive
 - ▷ High cost

- Applications in SRE and SSE
 - ▷ Too expensive for regular SRE
 - ▷ As hazard reduction/control in SSE
 - ▷ Other related SSE techniques:
 - general redundancy
 - substitution/choice of modules
 - barriers and locks
 - analysis of FT