Software Reliability and Safety

CSE 8317 — Fall 2007

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/8317.07f

OV.2. QA Review and Common Analyses

- QA Relation to CSE 8317
- Fault Tolerance in SSE: SQE Ch.16a
- Defect Analysis and ODC:
  SQE Ch.20 and Ma/Tian Web-ODC Paper
- Risk Identification: SQE Ch.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:
  - ▷ Functional relation: reliability $\sim$ failure
  - ▷ QA alternatives directly work with SRE
  - ▷ QA affects results/failures via causal chain
    error $\Rightarrow$ fault $\Rightarrow$ failure
  - ▷ 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)
  - ▷ SSP: QA throughout dev. process

- 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
    - SRE/SSE $\sim$ high/low fault densities
  - ▷ Scenario-based (focused) inspection:
    - SRE: common usage
    - SSE: FTA/ETA-based
  - ▷ 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: external vs internal focus
  - ▷ Coverage/usage: termination criteria

- 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