Software Reliability and Safety

CSE 8317 — Spring 2005

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/8317.05s

O. Overview and QA Review

- About CSE 8317
- Reliability and Safety Overview
- Review: QA Alternatives/Activities and Their Relation to CSE 8317

Quality: Views and Aspects

View	Attribute	
	Correctness	Effectiveness
Customer (external)	Failures: reliability safety	Usability Maintainability Portability Performance Installability Readability
Developer (internal)	Faults: count distr class hazard	Design Size Change Complexity control data presentation

- 8317: Reliability/safety focus

- Things contribute to reliability/safety

What Is Reliability?

- *Reliability:* Probability of failure-free operation for a specific time period or for a given set of input conditions under a specific environment
  - ▷ Failure: behavioral deviations
  - ▷ Time: how to measure?
  - ▷ Input: sampling and measurement
  - ▷ Environment: OP

- Software reliability engineering (SRE):
  - ▷ Failure detection and fault removal
  - ▷ Measurement and data collection
  - ▷ Reliability assessment
  - ▷ Reliability and other predictions
  - ▷ Decision making and management
  - ▷ Reliability and process improvement

What Is Safety?

- *Safety:* The property of being accident-free for (embedded) software systems.
  - ▷ Accident: failures with severe consequences
  - ▷ Hazard: condition for accident
  - ▷ Special case of reliability
  - ▷ Specialized techniques

- Software safety engineering (SSE):
  - ▷ Failure prevention and fault tolerance
  - ▷ Hazard identification/analysis techniques
  - ▷ Hazard resolution alternatives
  - ▷ Safety and risk assessment
  - ▷ Qualitative focus
  - ▷ Safety and process improvement

Reliability, Safety and Defects

- Defect/bug definition/clarification
  - ▷ Failure: external behavior
    – deviation from expected behavior
  - ▷ Fault: internal characteristics
    – cause for failures
  - ▷ Error: missing/incorrect actions
  - ▷ Relations (not necessarily 1-1)
  - ▷ Safety-related: accident & hazard

- Defect and quality assurance/analysis
  - ▷ Quality (reliability/safety) analysis
  - ▷ Preventive actions based on analysis
  - ▷ Fault removal: insp./testing/verification
  - ▷ Fault tolerance

Measurement, Analysis, & Modeling

- Measurement data
  - ▷ Result: success/failure/accident/etc.
  - ▷ Activity: testing/usage/etc.
  - ▷ Product internal: static/dynamic
  - ▷ Environmental: process/people/setup/etc.
- Analysis and modeling:
  - ▷ Data ⇒ safety & reliability.
  - ▷ Based on reliability/safety models
  - ▷ Followup actions:
    - – management decisions
    - – problematic areas identification
    - – reliability/safety/process improvement

Reliability Analyses and Models

- Time domain approach
  - ▷ Failure arrival process
  - ▷ Statistical modeling
  - ▷ Failure count/interval/rate data
  - ▷ Time and other measurements
  - ▷ SRGMs: s/w reliability growth models
  - ▷ Assessment/prediction/decisions
- Input domain approach
  - ▷ Repeated random sampling
  - ▷ Related definitions and models
    – input domain reliability models
  - ▷ Fault seeding models

Reliability Analyses and Models

- TBRMs: tree-based reliability models
  - ▷ Both time/input domain info.
  - ▷ Additional benefit:
    - – risk identification
    - – guide for focused remedial actions
  - ▷ Technique: tree-based modeling
  - ▷ Development/application/SMU research
  - ▷ Major focus in 8317

- Other related issues
  - ▷ Implementation & applications
  - ▷ OP development & QA activities
  - ▷ Fault/defect modeling
  - ▷ Data treatment

Safety Analysis & Improvement

- Hazard analysis:
  - ▷ Hazard: condition for accident
  - ▷ Fault trees: (static) logical conditions
  - ▷ Event trees: dynamic sequences
  - ▷ Combined and other analyses
  - ▷ Generally qualitative
  - ▷ Related: hazard and risk assessment

- Hazard resolution
  - ▷ Hazard elimination
  - ▷ Hazard reduction
  - ▷ Hazard control
  - ▷ Related: damage reduction

Hazard Elimination

- Fault prevention activities:
  - ▷ Preventive actions:
    – education/process/technology/etc
  - ▷ Formal specifition & verification

- Fault removal activities:
  - ▷ Rigorous testing
  - ▷ Inspection and verification
  - ▷ Static/dynamic analyses

- Other hazard elimination:
  - ▷ Above $\in$ traditional QA activities
  - ▷ "Safe" designs etc.

Hazard Reduction & Control

- Hazard reduction
  - ▷ Barrier and safety margins
  - ▷ Redundancy and fault tolerance
  - ▷ “passive” or “reactive”
- Hazard control
  - ▷ Isolation and containment
  - ▷ Protection system
  - ▷ “active”
- Related: post-accident damage reduction

How CSE 8317 Fits In?

- Software reliability engineering (SRE):
  - ▷ Observation-driven SRGMs/IDRMs;
  - ▷ Progress towards measurement-driven TBRMs and other models;
  - ▷ Statistical analysis techniques:
    - – stochastic processes and curve fitting
    - – predictive risk management
    - – tree-based models & other techniques
  - ▷ reliability measurement and improvement.

- Software safety engineering (SSE):
  - ▷ Fault/event tree analyses, etc.;
  - ▷ Hazard elimination/reduction/control;
  - ▷ Process-based approach;
  - ▷ Formal verification and fault tolerance;
  - ▷ Prescriptive specification checking.

Review: QA Alternatives

- Defect prevention/removal/tolerance
  - ▷ Tian-SQP paper online.
  - ▷ Tian-SQEbook/slides online:
    - – Part I (particularly Chapter 3)
    - – Part 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

- Applicability, effectiveness, and cost

- Inspection:
  - ▷ Good throughout dev. process
  - ▷ Works on many software artifacts
  - ▷ Conceptual/static faults
  - ▷ High fault density situations
  - ▷ Human intensive, varied cost

- Applications in SRE and SSE
  - ▷ Fault eliminations:
    - – helps both reliability and safety
  - ▷ Early reliability prediction
  - ▷ Safety constraints and inspection
  - ▷ Leveson's process-based approach

QA Alternatives and 8317

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

- Applications in SRE and SSE
  - ▷ High cost ⇒ most in SSE
  - ▷ Module VIII of CSE 8317
  - ▷ Focus through FTA and/or ETA
  - ▷ Leveson's approach:
    – safety and other constraints
    – carried through dev. process
  - ▷ Other adaptations:
    – table driven approach
    – PSC, module IX

QA Alternatives and 8317

- Testing:
  - ▷ Important link in dev. process
  - ▷ Activities spilt over to other phases
    - – OP/testcase development
  - ▷ Dynamic/run-time/interaction problems
  - ▷ Test tools and execution support
  - ▷ Technique: analysis/behavior-based
  - ▷ Coverage vs. reliability focus

- Applications in SRE and SSE
  - ▷ Chief application domain for SRE
  - ▷ OP-based testing:
    - – basis for reliability modeling
  - ▷ 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 technique in SSE
  - ▷ Other related SSE techniques:
    - – general redundancy
    - – substitution/choice of modules
    - – barriers and locks
    - – analysis of FT