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

SRE.1: SRE Basics

- SRE Overview and Approaches
  – see Slides for SQE Chapter 22.

- SRE Activities and Context

- Analyses beyond reliability modeling

- General problems/issues

SRE Activities

- Analysis/modeling activities:
  - ▷ Predicting (prescriptive) reliability:
    - – product/process characteristics
    - – Musa's work at AT&T
  - ▷ Estimating (descriptive) reliability:
    - – s/w reliability growth models (SRGMs)
    - – other models
  - ▷ SRE practice: focus on latter (prescriptive models not mature yet)

- Modeling sub-activities:
  - ▷ Observations/measurement
  - ▷ Choice of models for goal/data
  - ▷ Modeling result evaluation
  - ▷ Applying results in process/decisions
  - ▷ Followup and improvement

SRE Activities

- In-process activities:
  - ▷ OP construction:
    - – start with requirement
    - – end with testing
    - – procedures and techniques
  - ▷ Prepare/execute random testing
  - ▷ Design for reliability:
    - – similar to design for safety
  - ▷ Process management & improvement
    - – manage by reliability goals

- In-field activities:
  - ▷ Measurement and data gathering
  - ▷ Availability management

$$\text{Availability} = \frac{MTTF}{MTTF + MTTR}$$

increase MTTF and decrease MTTR

Link to Software Process & QA

- Direct link to testing
  - ▷ Testing techniques and reliability
  - ▷ Measurement for reliability analysis
  - ▷ Repeated random sampling
    – IDRMs: Nelson model etc.
  - ▷ Fault seeding (& models)

- Other in-process measurement/analysis
  - ▷ Requirement and specification link to operational profile
  - ▷ Design and code measurement link to fault characteristics
  - ▷ Early remedial/preventive actions

Link to Other Activities

- Other QA activities and reliability
  - ▷ Fault tolerance/avoidance
  - ▷ Defect/fault removal process
  - ▷ Defect classification and analysis
  - ▷ Root cause analysis
  - ▷ Inspections
  - ▷ Program (formal) verification
  - ▷ Process for defect prevention

- Systems engineering
  - ▷ Hardware reliability
  - ▷ System composition/trade-offs
  - ▷ Maximize *system* reliability
  - ▷ Lyu-book: Chapter 2 (s/w vs sys.)

SRE and related analyses

- *Reliability:* Prob(failure-free operation)
  - ▷ Time: how to measure ⇒ SRGMs
  - ▷ Input: seeding, testing techniques and coverage metrics
  - ▷ Failures: defect analysis
  - ▷ Environment: specific techniques

- Related concepts (-ilities):
  - ▷ Quality and defect
  - ▷ Availability: failure and repair
  - ▷ Safety: emphasize on impact
  - ▷ Others: usability, portability

Defect Analysis

- Causal analysis
  - ▷ Domain knowledge: operation/usage
  - ▷ Product knowledge: internal structure
  - ▷ Reverse engineering tools
- Classification/distribution
  - ▷ Severity and characteristics
  - ▷ Error/fault/failure view
- Predictive modeling
  - ▷ Internal measurement to defects
  - ▷ Corrections: design for reliability
- SQE Part IV (esp. Ch.20)

Orthogonal Defect Classification

- Background and motivation
  - ▷ Developed and applied at IBM.
  - ▷ Bridging gap between causal analysis and statistical quality models.
  - ▷ Approach: classification and analysis.
  - ▷ Orthogonal, multi-phases/products.
  - ▷ Analysis technique: attribute focusing.
  - ▷ Applicability: inspection and testing.

- Key attributes of defects
  - ▷ Views: both failure and fault.
  - ▷ Cause: type, trigger
  - ▷ Effect: severity, effect, etc.

- (Lyu, 1995a):Ch.9 & SQE:Ch.20.

Improvement & Predictive Modeling

- Improvement focus
  - ▷ Risk: identification/correction
  - ▷ Techniques for improvement:
    - – analytical: favorable preconditions
    - – empirical: early indicators
  - ▷ Validation: external metrics
    - – quality, reliability, defects
    - – effort, schedule, cost

- Predictive modeling
  - ▷ Risk identification techniques
    - – SQE book, Ch. 21.
  - ▷ What measurement to take
    - – empirically based
    - – SQE book, Ch. 18 and 19.

SRE Issues: What and How

- Usage and effectiveness
  - ▷ Good assessment vehicle
  - ▷ Prediction varies w/ OP quality
  - ▷ Limited control ability
  - ▷ Dependency on data/environment

- Models and development
  - ▷ SRGMs: overall picture
  - ▷ Combinatorial: snapshots, focus
  - ▷ Integrated: promising
  - ▷ Data/tools/experience
  - ▷ Integration with other initiatives

SRE Issues: Where and When

- Products and environments
  - ▷ Medium reliable software: SRE
  - ▷ Safety critical: safety eng.
  - ▷ Mass market: focus on usability
  - ▷ Spectrum: (-ilities)...(SRE)...(safety)
  - ▷ Tailoring/adaptation/adoption

- When it is useful
  - ▷ OP-based random testing
  - ▷ Late in development cycle
  - ▷ Too late? What to do?
  - ▷ Learn from hardware RE.

SRE Issues: Improvement

- Improvement potential
  - ▷ Risk identification
  - ▷ Remedial actions
  - ▷ Prevention: design for reliability
  - ▷ Learn from experience

- More data and analyses
  - ▷ Defect: Classification/distribution
  - ▷ Internal measurement
  - ▷ Linkage: predictive analysis/modeling
  - ▷ Analysis techniques
    - – statistical: regression, NN, TBM etc.
    - – analytical: trace, causing, FT etc.
  - ▷ Linkage to subsequent topics