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

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 and applications
  - ▷ SRE practice: focus on latter

- Modeling sub-activities:
  - ▷ Observing/measuring
  - ▷ Choosing models for goal/data
  - ▷ Evaluating modeling result
  - ▷ Applying results in process/decisions
  - ▷ Followup and improvement

SRE Activities

- In-process activities:
  - ▷ OP construction:
    – start:requirement — end:testing
  - ▷ Prepare/execute random testing
  - ▷ Process management & improvement
    – manage by reliability goals
  - ▷ Techniques for above: in 7314
  - ▷ Design for reliability:
    – similar to design for safety (later)

- 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 affect reliability
  - ▷ Testing measurements in SRE modeling
  - ▷ Repeated random sampling
    – in Nelson model and other IDRMs
  - ▷ Fault seeding (& models)

- Other in-process measurement/analysis
  - ▷ Requirements/specs to OP/UBST
  - ▷ Design and code measurement to defect analysis and predictive modeling
  - ▷ Data from other QA activities
  - ▷ Early remedial/preventive actions

SRE and System Reliability

- Hardware reliability
  - ▷ Different characteristics
  - ▷ Different models (reliability decay)
  - ▷ Extensive existing work
- Systems engineering
  - ▷ System composition/trade-offs
  - ▷ Maximize *system* reliability
- Lyu-book: Chapter 2 (s/w vs sys.)

SRE Issues: What and How

- Usage and effectiveness
  - ▷ Good assessment vehicle
  - ▷ Prediction varies w/ OP quality
  - ▷ Limited control capability
  - ▷ 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