Software Reliability and Safety

CS 8317 — Spring 2023

Prof. Jeff Tian, tian@engr.smu.edu
CS, SMU, Dallas, TX 75275
(214) 768-2861; Fax: (214) 768-3085
s2.smu.edu/∼tian/class/8317.23s

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

- Main reference: Lyu/HSRE Ch.6

- Analysis/modeling activities:
  - ▷ Predicting (prescriptive) reliability:
    - based on prod./proc. characteristics
    - Musa's work at AT&T
  - ▷ Estimating (descriptive) reliability:
    - s/w reliability growth models (SRGMs)
    - other models and applications
    - all based on testing/defect/etc. data
  - ▷ SRE practice: mostly latter

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

SRE Activities

- In-process activities:
  - ▷ OP construction:
    – start:requirement — end:testing
  - ▷ Prepare/execute OP-guided testing
  - ▷ Process management & improvement
    – manage by reliability goals
  - ▷ Techniques for above: in 7314
  - ▷ Design for reliability:
    – some additional research

- In-field activities:
  - ▷ Measurement and data gathering
  - ▷ Focus: availability management

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

increase MTTF and decrease MTTR

SRE and System Reliability

- Hardware reliability
  - ▷ Different characteristics
    aging, wear, etc. ⇒ reliability decay
  - ▷ Different models (and distribution functions)
  - ▷ Extensive existing work
    analysis, composition (block-diagram), etc.

- Systems engineering
  - ▷ System composition/trade-offs
  - ▷ Maximize *system* reliability

- Lyu-book: Chapter 2 (s/w vs sys.)

SRE and Quality/Dependability

- Quality attributes beyond reliability and safety:
  - ▷ Usability, safety, security
  - ▷ Many others in ISO 9126 etc.
  - ▷ Share some common analysis techniques

- Dependability
  - ▷ Usually for (software-intensive) systems
    – e.g., SOA, Cloud, Net-Centric
  - ▷ High-assurance systems (HISS):
    – security as one major area
    – reliability, safety
    – availability, fault tolerance, etc.
  - ▷ SRE/SSE as important part of HISS techniques

SRE and Other Analysis

- Quantitative analysis
  - ▷ Defect analysis, risk analysis, etc,
  - ▷ Measurement and data collection
  - ▷ Analysis: assessment/prediction/control – in SRE, SSE, etc.
  - ▷ Statistical and AI-based
- Qualitative analysis
  - ▷ Defect classification, root-cause, etc.
  - ▷ Measurement level: nominal or ordinal
  - ▷ Subjective judgment and process
- Example: usability work at SMU

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(TBRMs etc): promising
  - ▷ Data/tools/experience
  - ▷ Integration with other initiatives

SRE Issues: Where and When

- Products and environments
  - ▷ Medium reliable software: SRE
  - ▷ Safety critical: SSE
  - ▷ Mass market: focus on usability, etc.
  - ▷ Spectrum: (-ilities)...(SRE)...(safety)
  - ▷ Tailoring/adaptation/adoption
- When it is useful
  - ▷ OP-based random testing
  - ▷ Late in development cycle
  - ▷ Too late? What to do? (SRE.2)
  - ▷ Learn from hardware RE.

SRE Issues: Process & QA

- Direct link to testing
  - ▷ Testing techniques affect reliability
  - ▷ Testing measurements in SRE modeling
    - – sampling: Nelson model & other IDRMs
    - – reliability growth over time: SRGMs
    - – fault seeding (& models), etc.

- Other in-process measurement/analysis
  - ▷ Requirements/specs to OP/UBST
  - ▷ Design and code measurement to defect analysis and predictive modeling
  - ▷ Current/historical data from elsewhere
  - ▷ Early remedial/preventive actions

SRE Issues: Improvement

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

- Timing and process for improvement
  - Early risk identification
  - Make time for improvement actions
  - Improvement process: QIP like
  - Feedback and feedback-loop critical

SRE Issues: Improvement

- More data and early
  - ▷ Defect: Classification/distribution
  - ▷ Internal measurement
  - ▷ Linkage: predictive analysis/modeling
  - ▷ Early availability of data
  - ▷ Mixed quantitative and qualitative data

- Analyses
  - ▷ Statistical: regression, NN, TBM etc.
  - ▷ Analytical: trace, causing, FT etc.
    – often qualitative or hybrid (e.g. ODC)
  - ▷ Recent applications of AI/ML in SwEngr.

- Linkage to subsequent topics