

# Software Reliability and Safety

## CSE 8317 — Fall 2006

Prof. Jeff Tian, [tian@engr.smu.edu](mailto:tian@engr.smu.edu)  
CSE, SMU, Dallas, TX 75275  
(214) 768-2861; Fax: (214) 768-3085  
[www.engr.smu.edu/~tian/class/8317.06f](http://www.engr.smu.edu/~tian/class/8317.06f)

### **OV.1. Overview**

- About CSE 8317
- Defining Quality, Reliability, and Safety
- SRE: Software Reliability Engineering
- SSE: Software Safety Engineering

## 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 and other measurement/data
  - ▷ 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

---

- Measurements: SQE Ch.18
  - ▷ Result: success/failure/accident/etc.
  - ▷ Indirect measurements, as predictors:
    - activity/product internal/environment
  
- Analysis and modeling:
  - ▷ Model categories/context: SQE Ch.19
  - ▷ Defect analysis: SQE Ch.20
  - ▷ Risk identification: SQE Ch.21
  - ▷ Common basis for SRE & SSE
  
- 8317 focus:
  - ▷ SRE/SSE models: Data  $\Rightarrow$  safety & reliability
  
  - ▷ Followup/resolution for reliability/safety assurance and improvement

---

## Reliability Analyses and Models

---

- SRE.2: model = function relations  
e.g., failure  $\sim$  time or input.
  
- 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 (SRE.3)
  
- Other related issues: SRE.4
  - ▷ Implementation & applications
  - ▷ OP development & QA activities
  - ▷ Fault/defect modeling
  - ▷ Data treatment



---

## Safety Analysis & Improvement

---

- Hazard analysis and resolution (SSE.2)
  - ▷ Focus: accidents and pre-conditions (hazards), not other failures
  - ▷ “Safeware” Ch.13-16 & SQE Ch. 16.4
  - ▷ Identification and analysis
  - ▷ Resolution: elimination/reduction/control
  - ▷ Integration in development process
    - SSP (software safety program)
    - “Safeware”, Part IV (Ch.11-18)
  
- Formal verification related:
  - ▷ Main part: SSE.3, SQE Ch. 15.
  - ▷ PSC: SSE.4, SQE Ch. 16.5

## Safety Analysis & Improvement

---

- Hazard analysis:
  - ▷ Fault trees: (static) logical conditions
  - ▷ Event trees: dynamic sequences
  - ▷ Other analyses
  - ▷ Generally qualitative
  - ▷ Related: hazard and risk assessment
  
- Hazard resolution (pre-accident)
  - ▷ Negate/block/mitigate/etc.
  - ▷ Hazard elimination/reduction/control
  
- Related: damage reduction (post-accident)

---

## Safety Assurance & Improvement

---

- **Eliminate** identified hazard sources in material/component/software/etc.
- **Reduce** hazard severity/likelihood via:
  - ▷ Creating hazard barriers,
  - ▷ Minimizing failure probability, etc.
- **Control** or limit hazard scope via:
  - ▷ Isolation and containment,
  - ▷ Fail-safe design, etc.
- **Reduce** damage (post-accident, as compared to pre-accident for the above)

---

## 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.