

Software Reliability and Safety

CSE 8317 — Spring 2015

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/8317.15s

SSE.2: Hazard Analysis

- Hazard Analyses and Techniques
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Other HA Techniques

Safety Techniques

- Hazard and risk identification:
 - ▷ Accident scenarios: actual/hypothetical
 - starting points for safety
 - ▷ Focus: operations and operational env.

- Hazard analysis and assessment:
 - ▷ Fault trees: (static) logical conditions
 - ▷ Event trees: dynamic sequences
 - ▷ Other analyses/assessment techniques

- Hazard and risk resolution
 - ▷ Hazard elimination
 - ▷ Hazard reduction
 - ▷ Hazard control
 - ▷ Damage control

Hazard Analyses: Types

- Sub-system hazard analyses (SSHA)
 - ▷ Hazard within individual sub-system
 - ▷ Component/sub-system in isolation

- System hazard analyses (SHA)
 - ▷ Focus: interface and interaction
 - ▷ Subsys/env/human effect on system
 - ▷ Throughout development process
 - ▷ Focus on early phases to provide info. for other activities (hazard resolution and safety verification)

- SHA/SSHA in software process
 - ▷ Throughout development process
 - ▷ Focus on early phases to provide info. for other activities (hazard resolution and safety verification)

Hazard Analyses: Techniques

- Primary techniques for SHA/SSHA:
 - ▷ Fault-tree analyses (FTA)
 - ▷ Event-tree analyses (ETA)
 - ▷ SQE Ch.16.4 and Safeware Ch.14.

- Other techniques:
 - ▷ Design reviews & checklists
 - ▷ Hazard indices
 - ▷ Risk trees
 - ▷ Cause-consequence analysis (CCA)
 - ▷ Hazard & operability analysis (HAZOP)
 - ▷ Failure modes and effect analysis (FMEA)
 - ▷ FMECA (FMEA + Criticality), etc.
 - ▷ Above: “Safeware” Ch.14.
 - ▷ Specific to software: “Safeware” Ch.15.

- FTA and ETA slides from SQE Ch.16.4.

Hazard Analysis: SFTA

- SFTA: Software FTA
 - ▷ Same concept applied to software
 - ▷ Actual implementation (white-box)
 - ▷ Language elements (high-level):
 - assignment and function calls
 - branching statement, loops, etc.
 - ▷ Also for specification/architecture
 - black-box control flow diagram
 - equivalent language representation

 - SFTA construction:
 - ▷ Templates/examples for diff. statements
 - ▷ Safeware 18.2.2 (pp.497-507)
- ⇒ Additional work needed,
especially for system design/architecture

Hazard Analysis: ETA & CCA

- ETA alone: trace of accident.
May desire explanation also (from FTA)

- Cause-consequence diagram (CCA):
 - ▷ Combine ETA with FTA
 - ▷ Explaining decisions in ET

- Using ETA and CCA:
 - ▷ Partial vs. total ETA
 - ▷ Focus on main consequences
 - ▷ Details:
 “Safeware” 14.5-14.6 (pp.327-pp.335)