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

SSE.3: Hazard and Risk Resolution

- Hazard Resolution and Damage Control
- Hazard Resolution Techniques:
  Hazard Elimination/Reduction/Control
- Risk Resolution: Damage Reduction

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 and Risk Resolution

- Generic hazard resolution techniques (in order of their precedence):
  - ▷ Hazard elimination:
    – eliminate (some) hazard sources
  - ▷ Hazard reduction:
    – reduce hazard likelihood/severity
  - ▷ Hazard control:
    – control hazard severity/scope

- Hazard resolution $\Rightarrow$ prob(accident) $\downarrow$

- Related issues:
  - ▷ Basis: hazard identification and analysis via FTA, ETA, FMEA, CCA, etc.
  - ▷ Many specific techniques
  - ▷ Related to QA and SRE
  - ▷ Risk resolution: damage reduction too

Hazard Elimination

- Elimination of hazard
  - ▷ Intrinsically safe (sub-)system
  - ▷ All eliminated: feasibility & cost?
  - ▷ Certain types of hazard eliminated
  - ▷ Direct use of hazard identification and analysis results.

- Specific techniques: "Good SE & SSE"
  - ▷ Component substitution ($\Leftarrow$ FTA)
  - ▷ No single point of failure ($\Leftarrow$ ETA)
  - ▷ Simplification of building blocks
  - ▷ Decoupling of system architecture
  - ▷ Human errors/hazardous material elim.
  - ▷ Component safety certification:
  - ▷ Link to testing/FT/QA activities and SSP process

Hazard Elimination

- FTA derived
  - ▷ Negating/altering logical conditions
  - ▷ Critical component: substitution
  - ▷ Structural change?
- ETA derived
  - ▷ Altering/forcing event sequences
  - ▷ No single point of failure
  - ▷ "rollback" possibility?
- FMEA/etc. derived
  - ▷ Environmental control/influence
  - ▷ Formal verification of component and/or system
  - ▷ STAMP and other approaches: SSE4

Hazard, Controllability, & Observability

- Related to hazard resolution, particularly hazard reduction and control.

- Controllability:
  - ▷ Between any two system states
  - ▷ Desirable/safe states: maintain
  - ▷ Fail ⇒ action ⇒ safe (haz. control)
  - ▷ Controllability limits:
    - system design/structure limit
    - energy/capacity limit

- Observability: observation of system states (and failures), basis for control.

Design for Controllability

- Maintain safe states
  - ▷ Use built-in control
  - ▷ Monitoring: observation $\Rightarrow$ control
  - ▷ Multiple checks $\Leftarrow$ monitoring
  - ▷ Mostly in hazard reduction
- Enhancing control opportunities:
  - ▷ Incremental control: more control points
  - ▷ Intermediate states: more obs. points ($\Rightarrow$ more control opportunities)
  - ▷ Decision aid: easier/more control points
  - ▷ Both in hazard reduction and especially in hazard control

Hazard Reduction

- Hazard reduction:
  - ▷ Severity reduction:
    - change failure characteristics (failure $\wedge \neg$ hazard)
    - various locks/barriers
  - ▷ Likelihood reduction:
    - reduce failure probability
    - in combination with above
    - also: most QA/SRE related techniques

- Specific techniques:
  - ▷ Design for controllability
  - ▷ Barriers and locks (passive)
  - ▷ Failure/hazard probability/severity $\downarrow$ (accident probability$\downarrow$)

Hazard Reduction: Techniques

- Monitoring and checks: Fig 16.2
  - ▷ Hardware checks: lowest level
  - ▷ Code-level checks: assertions
    – connection to PSC (SSE.4)
  - ▷ Audit checks: independent monitoring
  - ▷ Supervisory checks: system/highest level

- Locks and barriers (passive)
  - ▷ Lock-outs (preventing hazard)
  - ▷ Lock-ins (maintaining safety conditions)
  - ▷ Interlocks (correct order/combinations)
  - ▷ Other barriers (extra cap./redundancy/etc.)

Hazard Reduction: Techniques

- Hazard probability minimization:
  - ▷ Design with extra capacity:
    - – safety factors/margins example
    - – melt temp. T_m and margin M
    - – $\Rightarrow$ safety bound $T_s = T_m - M$
  - ▷ Redundancy: similar
  - ▷ QA and SRE: failure $\downarrow$
    - – focused hazard probability min.
    - – with FTA/ETA/etc. help

- Redundancy (FT etc.) $\Rightarrow$ prob(hazard) $\downarrow$:
  - ▷ Hardware redundancy/backup
  - ▷ Software redundancy:
    - – fault tolerance (NVP, & (?) RB)
    - – anticipated input/env. enlargement
    - – "fool-proof" software
  - ▷ Recovery: similar to RB in FT
  - ▷ Hardware/software interlocks

Hazard Resolution: Hw/Sw Interlock

- Interlock software
  - ▷ Software used as safety interlock
    - (s/w usage: data/control/safety)
    - example: emergency shut-down s/w
  - ▷ More stringent safety requirement:
    - most s/w function safety-related
    - should not rely solely on s/w
    - Therac-25 accident lessons

- Hardware/software interlock
  - ▷ Limitation of s/w backups:
    - diversity and independence problems
  - ▷ Hardware backups and interlocks:
    - different characteristics
    - different failure mechanisms
    - more likely to be *independent*
    - passive/active safety devices
  - ▷ Combine the advantages $\Rightarrow$ safety $\uparrow$

Hazard Control

- Hazard control:
  - ▷ Detecting hazard, then control it
  - ▷ Built-in control: by design
  - ▷ Change after detection:
    - (passive) limits
      (mostly outside system)
    - (active) control devices/sub-systems

- Specific techniques:
  - ▷ Limiting exposure (duration↓)
  - ▷ Isolation and containment
  - ▷ Protection systems
  - ▷ Fail-safe design

Hazard Control: Techniques

- Internal system change:
  - ▷ Isolation of hazard event
  - ▷ Containment around hazard event
  - ▷ Fail-safe design (passive)

- System augmentation:
  - ▷ Protection system (PS) added on:
    - – hazard ⇒ PS action ⇒ safe
    - – shut-down or partial shut-down
    - – e.g., automatic coolant injection or pressure relief
  - ▷ Controllability limit (earlier)
  - ▷ Partial solution may be necessary:
    - – reduce the severity
    - – bring to a neighboring state

Risk Resolution: Damage Reduction

- Damage reduction: Why?
  - ▷ Risk factors:
    f(prob(haz), prob(haz→acc), damage)
  - ▷ All the hazard resolution techniques
    ⇒ risk ≠ 0 still!
  - ▷ Damage reduction needed
  - ▷ Passed "point of no return"

- Specific techniques:
  - ▷ Escape routes (lifeboats, fire escapes, evacuation plans, etc.)
  - ▷ Safe abandonment (haz. waste disposal)
  - ▷ Devices for limiting damage:
    – auto safety devices
    – limited melt-down
    – collapsible signpost, etc.

Perspectives

- SSE: Augment S/w Eng.
  - ▷ Analysis to identify hazard
  - ▷ Design for safety
  - ▷ Verify safety constraints (next module)
  - ▷ Leveson's SSP and STAMP

- Dealing with hazard/risk in SSE:
  - ▷ Hazard identification and analysis
  - ▷ Design for safety/hazard resolution:
    – Hazard elimination/reduction/control
  - ▷ Damage reduction
  - ▷ Safety verification
  - ▷ All in SSE context: hazard focus.