

Software Reliability and Safety

CS 8317 — Fall 2020

Prof. Jeff Tian, tian@engr.smu.edu
CS, SMU, Dallas, TX 75275
(214) 768-2861; Fax: (214) 768-3085
www.engr.smu.edu/~tian/class/8317.20f

SSE.4: Formal/New Methods for Safety

- Formal Methods: Axiomatic etc.
— SQP Chapter 15 and related slides
- Applications in SSE: PSC, etc.
- New Development: STAMP related
- CPS/IoT/HCI/etc. Quality Concerns

FM in SSE

- Leveson approach
 - ▷ Focused verification
 - ▷ Driven by hazard analysis
 - ▷ Distributed over development phases
 - ▷ Which FM? ad hoc

- Specific FM: SQE Ch.15 (slides!)
 - but with a safety focus/perspective

- Other applications
 - ▷ Need automation ⇒ model checking.
 - ▷ Less formality
 - ⇒ Parnas/tabular method & formal insp.
 - ▷ With statistical testing ⇒ Cleanroom
 - ▷ Yih/Tian: PSC (next module)

FM: 7 Myths and 10 Commandments

- Seven myths (Hall, 1990)
 - ▷ FM guarantee that software is perfect
 - ▷ They work by proving correctness
 - ▷ Only highly critical system benefits
 - ▷ FM involve complex mathematics
 - ▷ FM increase cost of development
 - ▷ They are incomprehensible to client
 - ▷ Nobody uses them for real projects

- Refutations and discussions

- However, some validity/quantified

FM: 7 Myths and 10 Commandments

- 10 Commandments ... 10 Years Later
(Bowen and Hinchey, 2006)
 - I. Thou shalt choose
an appropriate notation
 - II. Thou shalt formalize
but not overformalize
 - III. Thou shalt estimate costs
 - IV. Thou shalt have a FM guru on call
 - V. Thou shalt not
abandon thy trad. dev. methods
 - VI. Thou shalt document sufficiently
 - VII. Thou shalt not
compromise thy quality standards
 - VIII. Thou shalt not be dogmatic
 - IX. Thou shalt test, test, and test again
 - X. Thou shalt reuse

- Still valid after 10 years!

PSC and Safety

- Why?
 - ▷ Accident reports/empirical data:
 - mostly interface/interaction problems
 - ▷ Need systematic analysis
 - ▷ Existing approaches: combined idea?

- How?
 - ▷ Model: TFM (two-frame model)
 - ▷ Analysis of interfaces/interactions
 - ▷ Root cause of I/I problems:
 - physical vs. logical frame consistency
 - ▷ FM and particularly model checking ideas

- Slides SQE 16.5

STAMP and STPA

- Leveson's recent work:
 - ▷ After "Safeware"
 - ▷ Roots in systems and control theory
 - ▷ STAMP: Systems-Theoretic Accident Model and Processes
 - ▷ STPA: STamP Analysis
- Several papers and some online slides.
- New book by Nancy G. Leveson:
"Engineering A Safer World: Systems Thinking Applied to Safety,"
MIT Press, 2011.
ISBN: 9780262016629

Other Recent Work

- Survey of new accident:
 - similar findings
- FM-related work:
 - larger systems and applications
- Safety as part of dependability:
 - dependable and secure computing
 - safety trade-off
 - diversity and dependability (and safety)
 - integrating safetyreliability/usability
- New application domains:
 - net-centric: DoD/DARPA/etc.
 - NASA work
 - IoT/Big-Data and safety
 - many others
- Many active new frontiers for SSE research