Increasing Reliability and Safety

What Goes Wrong?

- Overconfidence: unrealistic or inadequate understanding of the risks of a complex system.
- safety-critical systems have failed when using fail-safe controls
- risks of failure can be analyzed and quantified
- use techniques for developing estimates carefully

- redundant SW systems designed by separate teams
- working separately, many common errors recur, often revealing failures in specs
- business or political *pressure* to hide flaws to avoid threat of bad publicity and/or the expense of correction and litigation
- be skeptical regarding risk estimates (e.g. Challenger)

Professional Techniques

Software engineering and professional responsibility

- use good SW eng. tech. at *all* stages of development
  - specifications
  - design
  - implementation
  - documentation
  - testing

- programmers and managers:
  - study and use the available SW Eng. tech and tools
  - learn about the application field
  - know the SW and systems used to anticipate potential problems
- e.g. Clearinghouse IPS:
  - years on specs for upgrade
  - months on programming
  - performed realistic and extensive tests

- SW developers tend to:
  - skimp on planning, spec, and design phases
  - too quickly commence programming
  - inadequate testing before release
- Subfield of CSCI: safety critical SW design, development and analysis
  - safety designed in from inception
  - techniques of hazard analysis to identify and protect against risks

- accidents usually from failure to apply well-known standard engineering practices – not unknown sci. prin.
- tech. fixes alone cannot prevent accidents.
- SW developers must accept limitations of SW
- turn control over to SW only after careful analyses
- HW mech. are still useful – omit only with extreme justification

User Interfaces and Human Factors

- well-designed user interfaces can help avoid many computer-related problems
- there are known practices for quality UI
- input from psychology and human factors experts
- eg: automated flight system:
  - pilot needs feedback at all times to understand status

- system should perform as pilot does
- low workload leads to inattentiveness

Redundancy and self-checking

- e.g. space shuttles' voting and independent systems
- complex sys. collect info on own activity to diagnose and correct errors
- e.g. telephone SW sys.: half of operation devoted to err checking

- bugs in err and exception handling SW hard to diagnose and can have extensive effects

- bug-free complicated systems cannot be guaranteed even via best SW eng. practice

Testing

- testing not arbitrary: known principles and tech for quality

- e.g. NASA: SW passed tests so NASA wanted to reduce testing!

- IV&V: Independent verification and validation
  - SW tested and validated by company other than customer and developer
  - IV&V team acts adversarially to find flaws

Law and Regulation

- Criminal and civil penalties
  - suits against developer and seller
  - criminal charges for fraud & negligence
  - contracts limit liability to cost of sys and are upheld in court
  - laws too extreme discourage innovation
  - instead provide incentive for safety
  - entities that don't pay for mistakes will make more

- US liability law flawed

- Warranties for consumer SW:
  - *shrink-wrap* licencing agreements offer SW *as-is*
  - Uniform Computer Information Transactions Act (UCITA) accepts these agreements as binding
  - consumer advocates: mandatory warranties on SW, making companies liable for their bugs
  - pro:
    * encourages SW responsibility and ultimately better SW

    - consumer protection against large indifferent companies
  - con:
    - more expensive SW
    - burden worse for small developers
    - reduction in innovation and development of SW
    - error-free SW infeasible to produce
  - liability standards differ between SW & HW

- Regulation:

- testing requirements
- Gov. agency approval
- pro:
  * profit motive encourages safety skimping – the Gov. should prevent that
  * better to be proactive than reactive
  * most users at risk do not have expertise to judge risk
  * infeasible for ordinary people to sue large companies successfully
- con:

    * approval process expensive & slow
    * inhibition of innovation via requirements for specific procedures or materials
    * goals of regulation get lost in details of paperwork
    * political concerns affect approval process

- Licencing:
  - specific training
  - exams
  - ethical requirements

- continuing education
- violates *freedom to work*
- reduces number of practitioners in field
- prices & income inflated
- objections apply primarily if licencing involuntary
- voluntary: diplomas & certificates

- Taking Responsibility
  - business pressure for good customer relations and reputation for quality and service

– pay more for higher reliability