Reliability and Dependability and Safety

(oh my!)
Reliability and Dependability

Definitions

- Dependability
  - Reliance may be justifiably placed on the service delivered
  - Reliability, safety, security, availability, performance...

- Reliability
  - A measure of the continuous delivery of correct service – or of the time to failure

What has been done in the past?

- Historical competitive advantage to higher reliability
  - Microsoft is the quintessential software vendor...
- Hardware designed ‘within tolerance’ – predictable physical failure rates
  - Software fails mainly due to design defects

Reliability and Dependability

What can be done now?

- Fault prevention
  - Good process, formal methods, human interaction issues
- Fault removal
  - Test, test, test; regression test after changes (in case new faults were introduced)
- Fault tolerance (fault does not result in failure)
  - Recovery blocks, retry blocks, checkpoint/rollback, redundancy
- Fault/failure forecasting (failure occurs, but with predictable and acceptable cost)
  - Reliability modeling, fault injection

Reliability and Dependability

- Remaining challenges
  - Difficult to assess impact of techniques
    - Good process does not ensure good product...
    - Data is limited and project-specific
  - Difficult to predict reliability at design time
    - Software not easily split into ‘components’
  - Reticent, complicated culture
    - Features, not reliability, sell consumer products
    - Many standards for safety-critical

Safety

Definitions

- Safety
  - Nonoccurrence of accidents
  - (In software, many accidents have simple causes)

- Accident
  - An unplanned event that results in death, injury, illness, damage to or loss of property, or environmental harm

- Hazard
  - State that can lead to an accident
  - Analyzed by criticality and likelihood of occurrence

Safety

What has been done in the past?

- Hazard and Operability analysis (HAZOP)
  - Developed by Imperial Chemical Industries in early 1970s
  - Guide words (‘no’, ‘more of’...), deviation (‘pressure’, ‘temperature’...), causes, consequences, action

- Failure Modes and Effects Analysis (FMEA)
  - Developed in 1960s for analysis of aircraft safety
  - Assesses effects of individual component failure modes on the system (failure -> hazard); originally hardware (eg stuck-at 0)

- Fault Tree Analysis (FTA)
  - Developed 1961-2 to assess and improve reliability of the Minuteman Missile Launch Control System
  - Identify possible event combinations leading to a hazard (hazard -> failure)

Safety

- What can be done now?
  - FMEA, FTA for software (limited applications)
  - Integrated safety, system requirements and toolsets (eg SpecTRM by Leveson)
  - Use formal methods to ensure ‘that doesn’t occur’

- Remaining challenges
  - Seamless integration of design process
  - Education and human interaction study
    - Proven beneficial techniques not widespread
    - Human operators are often the weakest link
  - Safe use and reuse
    - Pay attention to boundary conditions
    - State assumptions about user, environment, operations