Reliability and Risk

EJ Jung

Examples

- N.S. woman tired of getting declared of being dead
- Woman declared dead, but she's not
- Diebold voting machine flaws

Case Study

- The Therac-25
  - 6 overdoses at 4 medical centers bet'n `85-`87
  - 3 deaths
- Two programming errors
  - fast typing of prescription caused ignoring edits
  - using 1 byte to store counter caused wrap-around
- Killed by Code: Software Transparency in Implantable Medical Devices

Design and Development factors

- Carelessness
  - not knowing potential safety risks
  - not expecting all possible inputs
- Interaction with physical devices
- Incompatibility between sw and hw
- Insufficient testing
  - reuse of old sw
- Overconfidence in SW

Management and use

- Data errors
  - entry error
  - maintenance error
- Inadequate training of users
- Interpretation errors
- Overconfidence by users
- No plan B

Others

- Inadequate response to problems
  - admin cannot recreate the error
- Insufficient market or legal incentives

User Interfaces and Human Factors

- “Fool-proof” software

Redundancy and Self-checking

- N-version programming
  - the same initial spec
  - independent coding
  - hope for different errors

Testing

- Independent Verification and Validation
  - red-team, penetration testing
- Beta-testing
- Formal verification

Criminal and Civil Penalties

- liability laws
- 2003 lawsuit against Microsoft
  - MS software had security holes
  - Criminals are responsible for attacks
- Who is liable for bugs and security flaws in software?
- Warranties for SW

Regulation and safety-critical apps

- FDA regulates software in medical devices
- Licensing programmers?