Chapter 8: Errors, Failures, and Risks
What We Will Cover

- Failures and Errors in Computer Systems
- Case Study: The Therac-25
- Increasing Reliability and Safety
- Dependence, Risk, and Progress
Failures and Errors in Computer Systems

- Most computer applications are so complex it is virtually impossible to produce programs with no errors.
- The cause of failure is often more than one factor.
- Computer professionals must study failures to learn how to avoid them.
- Computer professionals must study failures to understand the impacts of poor work.
Failures and Errors in Computer Systems (cont.)

Individual Problems:
• Billing errors
• Inaccurate and misinterpreted data in databases
  – Large population where people may share names
  – Automated processing may not be able to recognize special cases
  – Overconfidence in the accuracy of data
  – Errors in data entry
  – Lack of accountability for errors
Failures and Errors in Computer Systems (cont.)

System Failures:
- AT&T, Amtrak, NASDAQ
- Businesses have gone bankrupt after spending huge amounts on computer systems that failed
- Voting system in 2000 presidential election
- Denver Airport
- Ariane 5 Rocket
Failures and Errors in Computer Systems (cont.)

Denver Airport:

- Baggage system failed due to real world problems, problems in other systems and software errors
- Main causes:
  - Time allowed for development was insufficient
  - Denver made significant changes in specifications after the project began
Failures and Errors in Computer Systems (cont.)

High-level Causes of Computer-System Failures:
- Lack of clear, well thought out goals and specifications
- Poor management and poor communication among customers, designers, programmers, etc.
- Pressures that encourage unrealistically low bids, low budget requests, and underestimates of time requirements
- Use of very new technology, with unknown reliability and problems
- Refusal to recognize or admit a project is in trouble
Failures and Errors in Computer Systems (cont.)

Safety-Critical Applications:

• A-320: "fly-by-the-wire" airplanes (many systems are controlled by computers and not directly by the pilots)
  – Between 1988-1992 four planes crashed
• Air traffic control is extremely complex, and includes computers on the ground at airports, devices in thousands of airplanes, radar, databases, communications, and so on - all of which must work in real time, tracking airplanes that move very fast
• In spite of problems, computers and other technologies have made air travel safer
Case Study: The Therac-25

Therac-25 Radiation Overdoses:

• Massive overdoses of radiation were given; the machine said no dose had been administered at all
• Caused severe and painful injuries and the death of three patients
• Important to study to avoid repeating errors
• Manufacturer, computer programmer, and hospitals/clinics all have some responsibility
Case Study: The Therac-25 (cont.)

Software and Design problems:
- Re-used software from older systems, unaware of bugs in previous software
- Weaknesses in design of operator interface
- Inadequate test plan
- Bugs in software
  - Allowed beam to deploy when table not in proper position
  - Ignored changes and corrections operators made at console
Why So Many Incidents?
• Hospitals had never seen such massive overdoses before, were unsure of the cause
• Manufacturer said the machine could not have caused the overdoses and no other incidents had been reported (which was untrue)
• The manufacturer made changes to the turntable and claimed they had improved safety after the second accident. The changes did not correct any of the causes identified later
Case Study: The Therac-25 (cont.)

Why So Many Incidents? (cont.)

- Recommendations were made for further changes to enhance safety; the manufacturer did not implement them
- The FDA declared the machine defective after the fifth accident
- The sixth accident occurred while the FDA was negotiating with the manufacturer on what changes were needed
Case Study: The Therac-25 (cont.)

Observations and Perspective:

- Minor design and implementation errors usually occur in complex systems; they are to be expected
- The problems in the Therac-25 case were not minor and suggest irresponsibility
- Accidents occurred on other radiation treatment equipment without computer controls when the technicians:
  - Left a patient after treatment started to attend a party
  - Did not properly measure the radioactive drugs
  - Confused micro-curies and milli-curies
Case Study: The Therac-25
Discussion Question

• If you were a judge who had to assign responsibility in this case, how much responsibility would you assign to the programmer, the manufacturer, and the hospital or clinic using the machine?
Increasing Reliability and Safety

What goes Wrong?

- Design and development problems
- Management and use problems
- Misrepresentation, hiding problems and inadequate response to reported problems
- Insufficient market or legal incentives to do a better job
- Re-use of software without sufficiently understanding the code and testing it
- Failure to update or maintain a database
Increasing Reliability and Safety (cont.)

Professional techniques:
• Importance of good software engineering and professional responsibility
• User interfaces and human factors
  – Feedback
  – Should behave as an experienced user expects
  – Workload that is too low can lead to mistakes
• Redundancy and self-checking
• Testing
  – Include real world testing with real users
Increasing Reliability and Safety (cont.)

Law, Regulation and Markets:
• Criminal and civil penalties
  – Provide incentives to produce good systems, but shouldn't inhibit innovation
• Warranties for consumer software
  – Most are sold ‘as-is’
• Regulation for safety-critical applications
• Professional licensing
  – Arguments for and against
• Taking responsibility
Dependence, Risk, and Progress

- Are We Too Dependent on Computers?
  - Computers are tools
  - They are not the only dependence
    - Electricity
- Risk and Progress
  - Many new technologies were not very safe when they were first developed
  - We develop and improve new technologies in response to accidents and disasters
  - We should compare the risks of using computers with the risks of other methods and the benefits to be gained
Dependence, Risk, and Progress

Discussion Questions

• Do you believe we are too dependent on computers? Why or why not?
• In what ways are we safer due to new technologies?