Quick Quiz

1. List and briefly describe two cases, discussed in the chapter (other than the Therac case), where insufficient testing was a factor in an error or failure.

2. List and briefly describe one case, discussed in the chapter (other than the Therac case), where lack of accounting for environmental factors contributed to an error or failure.

3. Describe one principle of human-interface design that is particularly important in safety-critical systems.

4. List and briefly describe two of the many responsibilities of technical professionals in developing software.
High Cost of Software Failure

Software bugs are costing the U.S. economy an estimated $59.5 billion each year. Improvements in testing, debugging, and maintenance could reduce this cost by about a third, or $22.5 billion.

(from NIST Estimated Planning Report 02-3)

What Roles Do We Play?

Computer user
- understand limitations of computers, need for proper training and responsible use
- recognize that, as in other areas, there are good products and bad products

Computer professional
- studying computer failures helps us become better professionals (e.g., systems designer, programmers, technical support professional, etc.).
- even if not in these fields, will benefit from understanding sources and consequences of failures

Educated member of society
- many personal decisions or social, legal, and political decisions may depend on our understanding of risks of computer system failures
- could face issues of computing technology on a jury, lobbying for legislation, or deciding whether to use an experimental medical device
What Can Go Wrong?

- What are risks for computer failures?

What Can Go Wrong?

- What are reasons for computer failures?
What Can Go Wrong?

• How much risk must or should we accept?

Categories of Computer Errors and Failures

Computer problems can be organized in many different ways. GF uses the following categories:
• Problems for individuals
• System failures that affect large numbers of people
• Problems in safety-critical applications that could injure or kill people
Professional Responsibilities

What are they?

Professional Techniques

Software engineering has grown up around the principles of developing safe, efficient, and reliable software systems

- Software engineers working on safety-critical applications need special training (Leveson—we can learn from engineers’ experience in building safe electromechanical systems)
- Most software is not safe enough for safety-critical applications
- Accidents not prevented from technological fixes alone (no complete automated system will work)
- For safety-critical systems, expert control of development and operation is necessary
Redundancy and Self-Checking

- Critical applications should be redundant
  - e.g., Space shuttle used four identical but independent computer systems—checked against each other
  - most network infrastructures highly redundant.
- Complex systems can collect information on their own activity
  - for use in diagnosing and correcting errors (instrument to monitor the application.)
  - but sometimes the collection of systems themselves can fail

Testing

- What is the purpose of testing?
Testing

- Adequate and well-planned testing is essential.
- Test suites should be developed that exercise a program in all likely ways it will be used (and even unusual ways) but this is impossible.
- Thus, even if well tested, unforeseen set of circumstances could cause a failure.
- Testing only guarantees correctness for those inputs, environments, etc. executed.
- What other ways can be used to gain confidence in a system?

A Deeper Problem....

- Deeper problem of “under engineered systems”
- Such systems are so complex, use such new techniques, or are operating in such new ways that significant risk is inevitable—e.g., space shuttle
- Systems are experimental systems. Although good management and design practices must be followed with these systems, risk cannot be eliminated.
Law and Regulation

- Criminal and civil penalties are always available for computing systems that fail and cause harm. But this is after the fact.
- Retail sellers of computing hardware usually provide warranties. However, software is usually sold "as-is." What should the law be? Should companies be required by law to pay for bugs (and in what way?) or should they be protected?
- Safety-critical applications are a special case. Perhaps they need FDA-like regulation?
- Do any of them have FDA-like regulation?

Professional Licensing

- Software development professionals could be licensed (like engineers or architects).
- Licensing typically involves specific training, passing of competency exams, ethical requirements, and continuing education.
- But sometimes licensing is used to protect the status-quo rather than to provide better and more ethical service. Economic analysis shows that one effect of licensing is to reduce the number of practitioners in a field and keep prices and income higher than they would otherwise be.
- What is the current status of software-engineering licensing?
**Discussion**

- Are we too dependent on computers?
- How does modeling help improve reliability? What are the problems and risks in modeling?
- Who are the “good guys”—those people or organizations that make systems safer or reduce negative consequences of errors?
- When testing usually produces no failures, managers want to reduce the testing performed. Do you agree or disagree with this approach?

**Discussion**

- How many of you have tried hand gliding or bungee jumping?
- How many of you would ride on a computer controlled train that had no human driver?
- How many of you would ride on a computer controlled train that had no human, on-board pilot?
- How many of you would be among the first to get a computer chip implanted in your brain to aid in memory or computation?
Discussion

• Which models do you think would produce accurate results? Less reliable? Why?
  • Models that predict the position of the moon in relation to the earth 30 years from now
  • Models that predict the speed of a new racing boat hull design under specified wind conditions.
  • Models that predict the effect of an income tax change on government revenue.