Our new job

- USF has taken on a consulting job, and assigned this class to develop a prototype.
- We are to build the software for a pacemaker.
- Requirements - the pacemaker must listen for the patient’s heartbeat and deliver an electrical current to the patient’s heart exactly once a second, or the person will die.
- Write pseudocode for the pacemaker controller.
- You may assume that you have the following primitive available:
  - deliverCurrent()
Solution?

Does your solution look like this?

```python
while (True) {
    deliverCurrent()
    sleep(1)
}
```

If so, please report to the legal department.
**Issues**

- Does `sleep()` always take exactly one second?
- What if an error of some sort occurs?
Solution?

What about this sort of solution?

```java
long i = 1;
while (i > 0) {
    i++;
    sleep(1)
    deliverCurrent();
}
```

What additional problems might this have?
Reliability

- The fundamental issue up for discussion here is reliability.
- If we are to entrust hardware or software with critical tasks, we must be ensured that they function properly.
- Corollary:
  - As builders of software or hardware, we have a responsibility to ensure that the tools we create do not malfunction.
Risk

- The flip side of reliability is risk.

- We put our safety in the hands of other people and technologies all the time.

- Would you:
  - Go skydiving?
  - Cross a busy intersection?
  - Fly in an airplane?
    - landed by a computer program?
  - Ride in a computer-controlled train?
  - Let a computer determine your credit rating?
  - Let a computer program manage your bank account?
  - Let a computer program administer a medical procedure?
Therac-25

Therac-25 was a software-controlled radiation-therapy machine.
- Between 1985 and 1987, it gave radiation overdoses to six patients
- Fully automated and software-controlled.
- Replacement for an earlier system that provided software assistance to a human.
- Useful as a case study because it’s been so well documented.
Therac-25

- What were the problems?
  - Design issues - malfunctions, unhelpful error messages, little documentation.
  - Software bugs
    - Overflow in counter
    - Incorrect processing of input (race condition)
  - Many problems stem from the interaction of multiple components.
    - Just unit testing is not sufficient.
Why did these problems occur?

- No fail-safe in the system
- No detection or monitoring of errors
- Little useful documentation to assist human operators
- Inappropriate code reuse
Reliability and dependency

What are other examples of systems in which an undiscovered problem might have serious consequences?

(not necessarily life-threatening ...)
Reliability and dependency

- What are other examples of systems in which an undiscovered problem might have serious consequences?
  - Electronic voting - 2000 election
  - NCIC criminal database, FBI watch list
  - Missile guidance systems - Patriot missile in Gulf War I
  - Pricing and billing software
  - Denver Airport baggage
  - Simulations - economics, car crashes, nuclear weapons
You may remember about 8 years ago, there was a great deal of concern about the Y2K problem.

What was this?
Y2K

You may remember about 8 years ago, there was a great deal of concern about the Y2K problem.

What was this?

Many legacy systems had the date represented as a two-year number.

Billions of dollars spent to fix this.

What other sorts of Y2K-style problems might be lurking out there?
Software Engineering

What can we as software designers do to minimize these sorts of risks?
Software Engineering

What can we as software designers do to minimize these sorts of risks?

- Careful attention to UI and human role in the system
- Careful attention to the system’s possible uses
- Components that explicitly check for and handle errors
- Testing of individual components
- Testing of the system as a whole
- Field testing and evaluation
- Redundancy
- Independent validation and verification (who does the testing?)
Ethical Responsibility

- An underlying issue in these discussions is ethical responsibility - who is responsible when things go wrong?
  - This is different from legal responsibility.

- Ethicists often argue that, in order to be morally responsible, two conditions must hold:
  - The actions or inactions of a person must have caused the harm.
  - The actions must have been intended by the person. (note: they don’t need to have intended the consequences, just the initial actions. Carelessness or negligence counts here.)
Electronic Voting

- After the 2000 US Presidential Election, there was a great deal of concern about inconsistencies on the tallying of votes.
- In the US, election law is governed by each state.
- Elections are administered at the county level.
- Different areas had different technologies, budgets, methods.
HAVA

- In 2002, Congress passed HAVA (Help America Vote Act)
- Required replacement of punch card machines
- Set up a “provisional vote” system
- Requires that voting machines be auditable and produce a paper trail.
HAVA

- Many states had to move very quickly to replace large numbers of disallowed machines before the 2004 election.
- Diebold is one of the largest makers of electronic voting machines.
- Several states turned over the deployment and conduct of elections to Diebold.
Electronic Voting

http://itpolicy.princeton.edu/voting/
Exercise

Let’s suppose that the state of California hires us as consultants.

They’d like to implement electronic voting machines in California.

They want specific suggestions for things that Diebold could do to address security concerns.

What would you suggest?
Suggestions

- Open software/architecture
- Paper record for each vote
- Better security/construction for machines
- Access by security professionals
- More government oversight
- Digital signing of software updates
- Testing of machines in “vote” mode
Exercise

- In 2003, Amazon inadvertently advertised a PDA for $10, rather than almost $500.
- Many people found this through bargain-hunter sites before it was changed.
- Amazon refused to sell the PDAs for the lower price.
- Were they justified in doing so?
- What if the gap was smaller? When would Amazon be justified in arbitrarily changing the price it charges for something?