



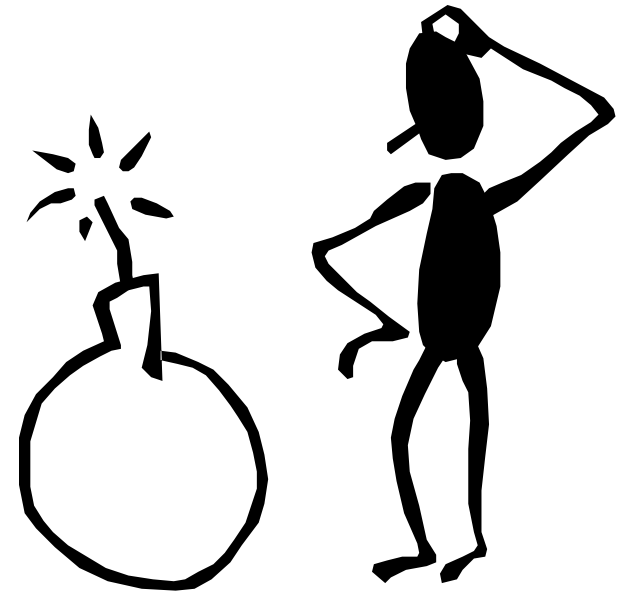
**Software Reliability:  
How good is good enough?**

---

**CSci 110**  
**Updated Summer 2006**

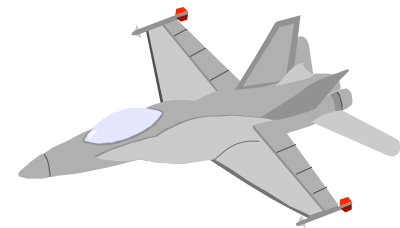
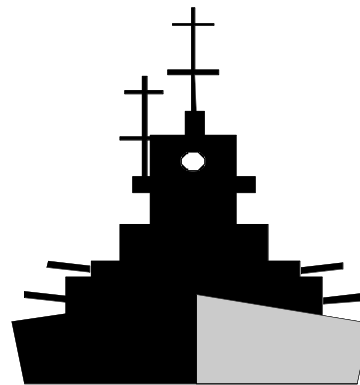
# Issues to consider...

- **Software Engineering (SE) Disasters**
- **SE as a Social Contract**
- **Risk**
- **Responsibility**
- **Accountability**
- **Liability**
- **User-Centered Design**



# Software Engineering Track Record

- 1985 Therac-25 Radiation Therapy
- \$9 billion Hubble Space Telescope
- 1988 USS Vincennes - shot down airliner
- 1990 AT&T 9 hour system failure
- Mars lander
- Auto safety recalls due to software problems



# Therac-25 Case - Product Liability

- See <http://en.wikipedia.org/wiki/Therac-25>
- Radiotherapy machine for cancer patients
- Responsible for several deaths in mid 1980's
- Therac-6 -> Therac-20 -> Therac 25
- Highly regarded line of equipment
- Two modes - X-ray and Electron mode
- Relied heavily on sophisticated SW for safety - hardware interlocks eliminated
- 11 Therac-25's sold - delivered fatal doses of radiation to several patients - AECL denied blame
- Made some SW patches - did not fully investigate the problem - a classic complexity problem!
- A set of subtle events: machine got confused if operators typed corrections too quickly

# Auto Safety Recalls due to Software (just a few examples)

## ■ 1998 GM Airbag Software Problems

- In 1998 General Motors Corp. recalled nearly 1 million cars with air bags that can deploy inadvertently, company officials said today. About 863,000 GM [cars] from the 1996 and 1997 model years are being recalled, along with 103,000 ... cars from model year 1995...
- The National Highway Traffic Safety Administration was investigating 96 complaints involving ... air bags inadvertently deploying while the cars were being driven under normal conditions over paved roads. GM told the agency there was an increased risk of an air bag deployment in a low-speed crash or when an object strikes the car's floor. An agency report said there were complaints of 10 crashes and 53 injuries.
- *The autos were recalled to change the software programming for the air bag computer....*

## ■ 2004 Cadillac SRX

<http://www.autosite.com/content/own/service/index.cfm/action/RecallsView/seriesid/31921>

- Antilock brakes might not respond as quickly as expected, resulting in increased stopping distance.
- Remedy: Have dealer reprogram ABS electronic control unit. [in other words, software error]

## ■ 2004 Chrysler Pacifica

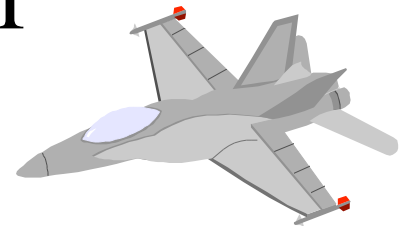
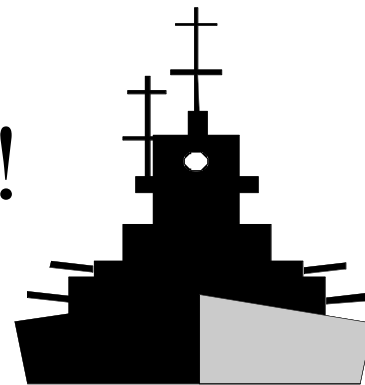
<http://www.autosite.com/content/own/service/index.cfm/action/RecallsView/seriesid/33691>

- Engine could stall suddenly, increasing risk of crash.
- Remedy: Have dealer install revised engine controller software, which will eliminate stall-out condition. [in other words, software error]

## ■ 2004-2005 Prius engine control [http://money.cnn.com/2005/05/16/Autos/prius\\_computer/](http://money.cnn.com/2005/05/16/Autos/prius_computer/)


# USS Vincennes Disaster

- A user interface problem
- Too much going on at once on the screen
- Data not positioned correctly
- Wrong decision made under pressure
- Shot down airliner!



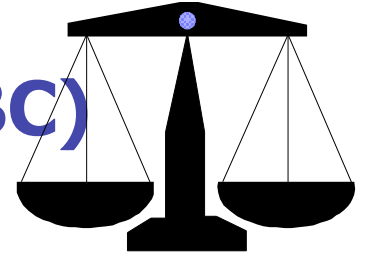
# **Ethical Software Development: A "Social Contract"**

---

- 
- **Software provider - creator**
  - **Software user - actually uses system**
  - **Software penumbra - all stakeholders**
  - **Rawlesian general principles**
    - **least advantaged**
    - **risking harm**
    - **publicity test**

# Code of Hammurabi(1795-1750 BC)

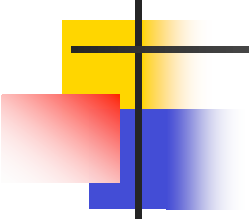
<http://www.fordham.edu/halsall/ancient/hamcode.html>



**Hammurabi was the ruler who chiefly established the greatness of Babylon (present-day Iraq!), the world's first metropolis. By far the most remarkable of the Hammurabi records is his code of laws, the earliest-known example of a ruler proclaiming publicly to his people an entire body of laws, arranged in orderly groups, so that all men might read and know what was required of them. The code was carved upon a black stone monument, eight feet high, and clearly intended to be reared in public view. The code regulates in clear and definite strokes the organization of society. The judge who blunders in a law case is to be expelled from his judgeship forever, and heavily fined. The witness who testifies falsely is to be slain. Indeed, all the heavier crimes are made punishable with death. Even if a man builds a house badly, and it falls and kills the owner, the builder is to be slain. If the owner's son was killed, then the builder's son is slain. These grim retaliatory punishments take no note of excuses or explanations, but only of the fact.**



# ACCOUNTABILITY

- 
- Responsible (assume)
  - Answerable (directed)
  - Blameworthy (cause)
  - Liable (financial)
  - Strict Liability (compensate for harm)

# Barriers to Accountability

- **Many Hands Syndrome**

- obscurs responsibility
- increased complexity
- no one knows all

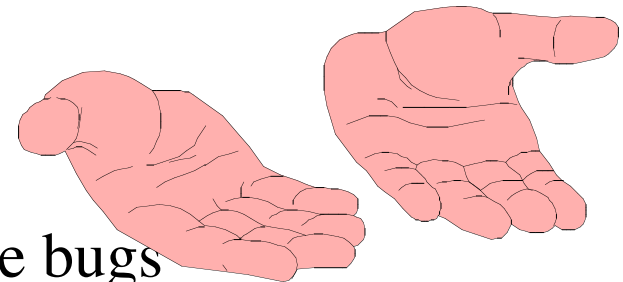
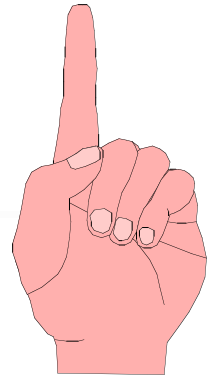
- **Inevitability of SW Bugs**

- natural hazards vs avoidable bugs

- **Computer as Scapegoat** - impute human agency

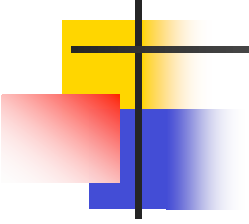
- **Ownership without Liability** (shrinkwrap mentality)  
rights vs responsibility

- **Read the examples of software licenses** - these are real but the company and product names are deleted. They are typical.



# Can Computers Be Moral Agents?

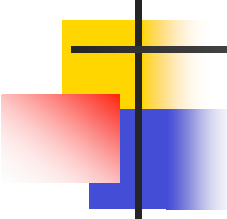
---

- 
- Intentionality causes action
  - Responsibility, accountability relate to moral agency
  - Humans are moral agents, morally responsible
  - Systems should not defer agency
    - anthropomorphic
    - delegated decision-making
    - delegated instruction

# **IEEE/ACM SE Code of Ethics**

## **(see Spinello, p. 535-544)**

---

- 
- 1. Public - act in public interest.**
  - 2. Client or Employer - act in best interest, consistent with #1.**
  - 3. Product - highest possible quality standards.**
  - 4. Judgment - integrity/ independence of professional judgment**
  - 5. Management - ethical approach to managing**
  - 6. Profession - advance integrity, reputation of profession, consistent with #1.**
  - 7. Colleagues - fair and supportive**
  - 8. Self -lifelong learning of skills, ethics**

# #1: PUBLIC

---

**1.01** accept full responsibility

**1.02** mediate interests of developer, client, user

**1.03** approve sw only if sure it is safe

**1.04** disclose any danger

**1.05** cooperate to address public concern

**1.06** be fair - avoid deception

**1.07** consider issues of physical disability

**1.08** volunteer professional skills

# SW Development Ethics Issues



- **Technical Hype vs Trust - vaporware**
- **Responsibility (cause)**
- **Liability (payback)**
- **Safe testing - time, risk, false data**
- **Working Conditions**
  - **stress**
  - **dysfunctional teams**
  - **angry employees / new hires**
- **Conflict of Interest**