Therac 25

Who is accountable for software failures?

Jayesh Patel

March 21, 2003

Outline

- What is the Therac-25 ?
- Consequences of software failure
- Aftermath and accountability
- Stakeholders and key ethical issues
- Comparison to classical engineering field
- Going forward

What is the Therac-25 ?

- Medical linear accelerator used to treat cancer
- Developed by Atomic Energy Commission Limited (AECL)
- Released in 1983
- More computer control
- Safety checks moved from HW to SW

What is the Therac-25 ?

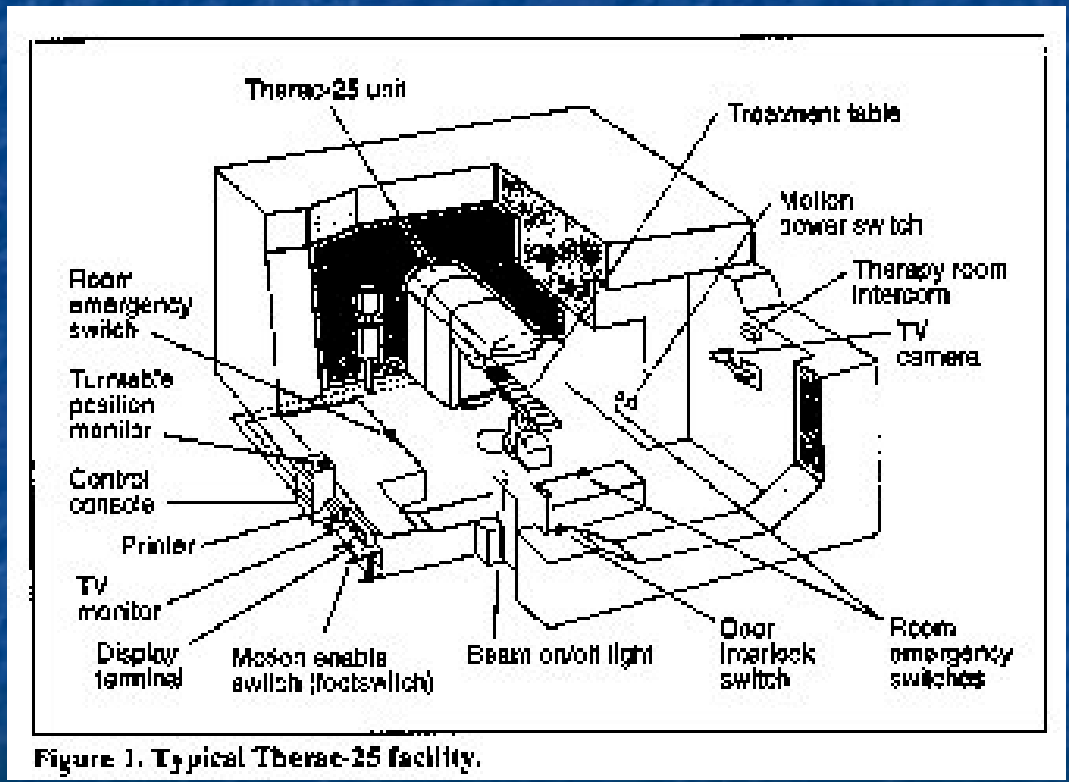

Figure 1. Typical Therac-25 facility.

What Happened

- Possible for computer to lag behind operator orders
  - Resulted in improper setting
  - Focused electrons at full power to a small spot on body

Consequences of Software Failure

- June 1985 to January 1987
  - 6 patients received radiation overdose
  - 3 died soon after overdose

Factors Leading to the Failure

- Poor implementation of software engineering principles
  - One programmer – lack of review, testing
  - No formal test plan
  - Lack of Human-Computer Interface design principles
  - Fundamental programming errors
  - Reuse of code without verification

Factors Leading to the Failure

- Inadequate responses by AECL
- “Pre-market equivalence” approval by FDA
- AECL’s use of Fault Tree Analysis

Aftermath and Accountability

- FDA / CRPB require Therac-25 units to shutdown until AECL makes satisfactory modifications
  - Software fixes
  - Independent mechanical safety interlocks
- No individuals held accountable
- Legal cases settled out of court

Steps Taken to Alleviate Future Occurrences

- FDA adjusts policies to address
  - Communication with medical centres
  - Product approval
- 1990 – health-care facilities required by law to report incidents to manufacturer and FDA

Stakeholders

- Atomic Energy Commission Limited
- Programmer
- FDA (public)
- Machine operators
- Patients
- (Software) engineering profession

Key Ethical Issues

- Engineer's responsibility to the company vs. the consumer (public)
  - Engineers shall be honest
  - Engineers shall expose risks openly to supervisors
  - Engineers shall hold paramount the safety, health, and welfare of the public in the performance of professional duties
- Accountability with respect to computing

Comparison to Classical Engineering Field

- Registered professional engineer would have risked losing license due to
  - Inappropriate action to ensure public welfare and safety
- Ethical principles
  - Engineers shall expose risks openly to supervisors
  - Engineers shall participate in a lifelong learning process regarding the practice of their profession
- More difficult for accountability
  - Many parties involved in development
  - General acceptance of errors in software

Going Forward

- Safety-critical software requires rigorous testing and failure analyses
- Education and recognition of software engineers
- Society will require us to take responsibility for what we build

References

"An Investigation of the Therac-25 Accidents," (1999). Onlineethics.org. Retrieved 28 February 2003 from the World Wide Web: http://onlineethics.org/cases/therac25.html

Boyer, Kevin W. "Ethics and Computing – Living Responsibility in a Computerized World," IEEE Computer Society Press, 1996.

"Computer Ethics: Princeton's Helen Nissenbaum is Helping Develop Emerging Field," (1995). Princeton University. Retrieved 28 February 2003 from the World Wide Web: www.princeton.edu/pr/news/95/q2/0407ethics.html.

Leveson, Nancy G. Safeware – System Safety and Computers – A Guide to Preventing Accidents and Losses Caused by Technology. Addison Wesley, 1995.

"Therac 25 Case Materials," (n.d.) Computingcases.org. Retrieved 3 March 2003 from the World Wide Web: www.computingcases.org/case_materials/therac/therac_case_intro.html.

Questions / Comments ?