

ECS 188

Ethics and the Information Age

Therac-25

Phillip Rogaway
Winter 2004

Background

- Jun 85—Jan 87, Therac-25, dual-mode (electron mode, photon mode) medical linear accelerator massively overdose of 6 people, 2 died. 11 machines.
- - Therac-6
 - Therac-20
 - Therac-25
 - AECL—Atomic Energy of Canada, Ltd
 - Used PDP-11 controller, moved HW safety features into SW
- X-ray treatment:
Electron source -> ion chamber -> flattening filter
->patient

Background, cont

1. 25,000 rad (500 rad whole-body LD-50)
2. Some of the account horrifying (p. 18, bottom)

A. What the engineers did wrong

1. Dangerous basic design: "dual mode" (electrons or photons), photonic energy levels (25 MeV) without beam flattener potentially lethal.
2. HW interlocks -> SW checks
3. UI: Treatment pause; proceedⓅ
4. UI: Malfunction 54 -> Dose input 2 (dose too high or too low).
5. <cr> <cr> <cr> to use old previous treatment parameters
6. Manual didn't describe malfunctions or say that some of them were potentially life-threatening

A. What the engineers did wrong, cont

7. Software had no safety system to prevent parameters being entered that would result in excessive radiation.
8. Program extremely buggy; 40 dose-rate malfunctions per day.
9. Meaningless fault-tree hazard analysis:
 - a. ignored SW errors
 - b. picked numbers from the air,
 10^{-11} "wrong energy" 4×10^{-9} "wrong mode"
10. 1-bit error in microswitches could result in bad settings.

A. What the engineers did wrong, cont

11. Plunger-lock could read locked when table way out of position
12. Hacked something that wasn't real and only cause.
13. Made minor changes, claimed safety increased 100,000 fold. At the same time, told FDA "cannot be firm on the exact cause of the accidents but can only suspect". Couldn't reproduce error.
- 14 . "It's not possible to overdose a patient"—closed mindedness.
15. trash on screen
16. no test plan, even after much prodding from FDA
17. Lack of documentation on SW specifications

A. What the engineers did wrong, cont

- 18. Ion chambers could not handle high-density electron beams, became saturated, gave an indication of low dosage.
- 19. See lessons for “bigger-picture” problems
- 20. No real documentation.
- 21. No real SW quality processes.
- 22. Complex design.
- 23. Error detection, audit needs to be designed-in from the beginning.
- 24. Inadequate testing. No regression testing
*BUT—testing would not have found these problems;
needed new SW design.*

B. What the company (AECL) did wrong

1. Apparently incompetent engineering
2. Jun 85: Learned of questions from hospital physicist, didn't investigate.
3. Jun 85: Learned of lawsuit, didn't investigate
4. AECL warned users to visually confirm turntable alignment, but never said death/injury had occurred.
5. Blamed "transient failure of microswitch"
6. Didn't implement the Canadian demands (machine must stop if dose-rate malfunction; changed to allow 3 failures instead of 5).

B. What the company did wrong, cont.

7. Ontario Cancer Foundation study: install independent position-detection system. Did not comply. (Some clinics modified the machines themselves.)
8. Repeatedly wouldn't accept that machine responsible
9. Lied to hospital physics support that there had been no other incidents reported.
10. "Remove the cursor-UP key"—doesn't say what is the defect or its results.
11. Lack of information propagation, users felt
12. "Reviewed by two outside experts"; couldn't/wouldn't provide their names.

B. What the company did wrong, cont.

- 13. Wouldn't release code
- 14. New fault-tree analysis; assumes all SW errors equally likely.
- 15. No audit trail, no formal system for incident analysis.

C. What the operators did wrong

1. Taught "so many safety mechanisms" she understood impossible to overdose a patient
2. June 85: Didn't believe patients: "You burned me" "That's not possible"
3. June 85: Operator reported problem to AECL, but not in the form of a formal written report.
4. June 85: Operator did not report malfunction to FDA
5. Jun 85: treatment prescription printout disabled during accident.

C. What the operators did wrong, cont

6. Jul 85: HTILT error, P, P, P, P—accustomed to malfunctions.
7. Mar 86: video display unplugged, audio monitor broken

D. What the government did wrong

1. Operators not required to report deaths, serious injuries, malfunctions to FDA. Manufacturers were required to do so. GAO study said that less than 1% of malfunctions reported.
2. FDA called problem "class-2 recall" (probability of serious injury remote).
3. Canada: demanded changes, didn't enforce.
4. Accepted that Therac-25 "substantially equivalent" to Therac-20
5. Accepted poor Corrective Action Plans and allowed machines to continue operating; very slow to order machines shutdown.

And the Good, too

- Hospitals modifying the machines on their own.
- Dec 85: Striped-pattern radiation burned investigated (x-rayed heating pad, contacted AECL)
- Hospital physicist Fritz Hagar (East Texas Cancer Center) put it together. Figured out data-entry speed during edits a critical factor.
- University of Chicago: Frank Borger figured out that "creative methods" of editing caused fuses to blow in the machine.
- FDA eventually changed added reporting rules and got more with-it.

Lessons

1. Focusing on a particular SW bug is not the way to make a safe system.
2. Particular coding error is not as important as general design safety.
3. Overconfidence in SW
4. Reliability doesn't imply safety
5. Lack of defensive design
6. Machine didn't monitor problems (patients were used to see if the thing was overdosing)
7. No worst-case design
8. Eagerness to believe that cause of problem has been identified without strong evidence.

Lessons

- 9. It is a mistake to patch one causal factor; what is the root cause.
- 10. Inadequate investigation, follow-up
- 11. Safety is a property of the system, not the SW

Question

- Why do you think that the users were more effective in figuring out safety problems and correcting them than the manufacturer?

Today

- Atomic Energy of Canada Ltd is a thriving company (www.aecl.com)
- Main business is building nuclear reactors. They have 34 nuclear power plants worldwide.
- A search for "Therac" on www.aecl.com:
In 1983, the Toronto-Bayview Clinic became the world's first cancer treatment center to switch on a new therapy machine—Therac 25—a linear accelerator designed and developed by AECL to deliver a higher dose of radiation to the interior of the body with minimal damage to tissue surrounding tumors.