**Case Study 17: Therac 25 (design/use of software in safety-critical applications)**

**[Extracts from: http://www.computingcases.org/case\_materials/therac/therac\_case\_intro.html]**

Therac-25 was a medical linear accelerator made by AECL. The Therac-25 was a device that targeted electron or X-ray beams on cancerous tissue to destroy it. Electron beams were used to treat shallow tissue, while photon beams could penetrate with minimal damage to treat deep tissue. Even though operators were told that there were "so many safety mechanisms" that it was "virtually impossible" to overdose a patient, this is exactly what did occur in six documented cases

The major innovations of Therac-25 were the double pass accelerator (allowing a more powerful accelerator to be fitted into a small space, at less cost) and the move to more complete computer control. The move to computer control allowed operators to set up the machine more quickly, giving them more time to speak with patients and making it possible to treat more patients in a day. Along with the move to computer control, most of the safety checks for the operation of the machine were moved to software and the hardware safety interlocks removed.

Before release of Therac-25 on the US market in 1983, AECL obtained approval to market it from the FDA. This approval was obtained by declaring what FDA called pre-market equivalence. Since the software was based on software already in use, and the linear accelerator was a minor modification of existing technology, designation of Therac-25 as equivalent to this earlier technology meant that Therac-25 bypassed the rigorous FDA testing procedures. In 1984, 94% of medical devices entered the market in this manner. This declaration of pre-market equivalence seems optimistic in that most of the safety mechanisms were moved into the software, a major change from previous version of the machine.

In July of 1985, AECL was notified that a patient in Hamilton had been overdosed. AECL sent a service engineer to the site to investigate. AECL also informed the United States Food and Drug Administration (FDA), and the Canadian Radiation Protection Board (CRPB) of the problem. In addition they notified all users of the problem and issued instructions that operators should visually confirm hardware settings before each treatment. AECL could not reproduce the malfunction, but its engineers suspected that a hardware failure in a micro switch was at fault. They redesigned the hardware and claimed that this redesign improved the safety of the machine by five orders of magnitude. After modifications were made in the installed machines, AECL notified sites that they did not need to manually check the hardware settings anymore.

In November of 1985, AECL heard of another incident in Georgia. The patient in that incident (Linda Knight) filed suit that month based on an overdose that occurred in June. In January of 1986, AECL heard from a hospital in Yakima, Washington that a patient had been overdosed. The AECL technical support supervisor spoke with the Yakima hospital staff on the phone, and contacted them by letter indicating that he did not think the damage they reported was caused by the Therac-25 machine. He also notified them that there have "apparently been no other instances of similar damage to this or other patients."

In March of 1986, AECL was notified that the Therac-25 unit in Tyler, Texas had overdosed a patient. They sent both a local Texas engineer and an engineer from their Canada home office to investigate the incident the day after it occurred. They spent a day running tests on the machine but could not reproduce the specific error. The AECL engineer suggested that perhaps an electrical problem had caused the accident. He also said that AECL knew of no accidents involving radiation overexposure with the Therac-25. An independent engineering firm checked out the electric shock theory and found that the machine did not seem capable of delivering an electric shock to a patient.

On April 11th of 1986, AECL was alerted to another overdose that had occurred in Tyler. After communication with the medical physicist at Tyler, AECL engineers were able to reproduce the overdose and the sequences leading up to it.

AECL filed a medical device report with the FDA on April 15, 1986 to notify them of the circumstances that produced the two Tyler accidents.

In January 1987, AECL was notified of another overdose occurring again at the Yakima, Washington hospital. After sending an engineer to investigate this incident, AECL concluded that there was a different software problem that allowed the electron beam to be turned on without the device that spread it to a safe concentration being placed in the beam.

In February, 1987, the FDA and its Canadian counterpart cooperated to require all units of Therac-25 to be shut down until effective and permanent modifications were made. After another 6 months of negotiation with the FDA, AECL received approval for its final corrective action plan. This plan included numerous software fixes, the installation of independent, mechanical safety interlocks, and a variety of other safety related changes.

Several of the surviving victims or the deceased victim’s families filed suit in US courts against AECL and the medical facilities using Therac-25. All of these suits were settled out of court.

**Discussion**

1. What are the responsibilities of the organizations and individuals involved? (operator who administered the overdose/software developers/system engineers/manufacturer/government)

2. What design decisions could have prevented these outcomes?

3. Was there too much faith placed in the *software* and not enough emphasis on real-world effects or situations?

Author: These massive radiation overdoses were the result of a convergence of many factors including

* simple programming errors
* inadequate safety engineering
* poor human computer interaction design
* a lax culture of safety in the manufacturing organization
* inadequate reporting structure at the company level and as required by the U.S. government