

**Safety-Critical Computing:  
Hazards, Practices, Standards  
and Regulation**  
from Jon Jacky  
<http://staff.washington.edu/~jon/pubs/safety-critical.html>

CIS 381

---

---

---

---

---

---

---

---

**Event (1)**

On March 21, 1986, oilfield worker Ray Cox visited a clinic in Tyler, Texas, to receive his radiation treatment. Cox knew from his previous visits that the procedure should be painless--but that day, he felt a jolt of searing heat. Outside the shielded treatment room, the therapy technologist was puzzled. The computer terminal used to operate the radiation machine displayed the cryptic message, "Malfunction 54," indicating the incorrect dose had been delivered. Clinic staff were unable to find anything wrong with the machine, so they sent Cox home and continued treating other patients.

---

---

---

---

---

---

---

---

**Event (2)**

Cox's condition worsened. Spitting blood, he checked into a hospital emergency room. Clinic staff suspected Cox had received an electrical shock, but specialists were unable to locate any hazard. Less than a month later, malfunction 54 occurred again--this time striking Verdon Kidd, a 66-year-old bus driver. Kidd died in May, reportedly the first fatality ever caused by an overdose during a radiation treatment. Meanwhile, Cox became paralyzed and lapsed into a coma. He died in a Dallas hospital in September 1986.

---

---

---

---

---

---

---

---

## Background

- As news of the Tyler incidents spread, reports of other accidents surfaced. A patient in Canada, another in Georgia, and a third in Washington state had received mutilating injuries in 1985. Another overdose occurred in Washington state in January 1987. All victims had been treated with the Therac-25, a computer-controlled radiation machine called a linear accelerator manufactured by Atomic Energy of Canada, Ltd (AECL).

---

---

---

---

---

---

---

---

- Different problems with the Therac-25 and its predecessor, the Therac-20, had been turning up for years prior to the Tyler accidents but were not widely known.
- Injured patients had been largely ignored and machines kept in use.
- Fixes requested by the Canadian government in the wake of one accident had never been installed.
- After the Tyler clinic staff explained the cause of the problems, Therac-25s were not withdrawn from service; instead, warnings were circulated and a makeshift temporary fix was recommended.

---

---

---

---

---

---

---

---

- Physicist Fritz Hager and therapy technologists at the Tyler clinic discovered that the accidents were caused by errors in the computer programs that controlled the Therac-25.
- Cox and Kidd had been killed by software.

---

---

---

---

---

---

---

---

## Position

- **Using computers to control hazardous machinery raises difficult questions. Some are specific to computing:**
  - Why use computers at all, if satisfactory techniques already exist?
  - Do computers introduce new kinds of problems unlike those encountered in traditional control systems?
  - What techniques exist now for creating safe and reliable computer-controlled systems, and could they be improved?

---

---

---

---

---

---

---

- **Other questions are perennial for society at large but are only now beginning to be considered in the computing field:**
  - How are we to decide whether a product is safe enough to place on the market?
  - How can we ensure that product developers and service providers are competent and that poor practices are discouraged?
  - Who is held responsible when systems fail and people get killed?

---

---

---

---

---

---

---

## How?

- **The million-dollar Therac-25, introduced in 1982, was thought to be among the best available and was one of the first of a new generation of computer-controlled machines.**
- **The traditional operator's control panel was replaced by a computer video display terminal, and much of the internal control electronics was replaced by a computer. This was intended to make operation more convenient, improve the accuracy of treatments, and decrease the time needed to treat each patient.**

---

---

---

---

---

---

---

- A particular innovation of the Therac-25 was the use of the computer to perform many of the safety functions traditionally allocated to independent, or hard-wired, electromechanical circuits called interlocks.

---

---

---

---

---

---

---

**Facts**

- Linear accelerators, including the Therac-25, can produce two kinds of radiation beams: electron beams and X-rays. Patients are treated with both kinds. First, an electron beam is generated. It may irradiate the patient directly; alternatively, an X-ray beam can be created by placing a metal target into the electron beam: as electrons are absorbed in the target, X-rays emerge from the other side. However, the efficiency of this X-ray-producing process is very poor, so the intensity of the electron beam has to be massively increased when the target is in place.

---

---

---

---

---

---

---

- In most of today's accelerators, hard-wired electromechanical interlocks ensure that high electron beam intensity cannot be attained unless the X-ray target is in place. In the Therac- 25, however, both target position and beam intensity were controlled solely by the computer. When the operator switched the machine from Xray to electron mode, the computer was supposed to withdraw the target and set the beam to low intensity.

---

---

---

---

---

---

---

- If the operator selected X-rays by mistake, realized her error, and then selected electrons--all within 8 seconds--the target was withdrawn but the full-intensity beam was turned on. This error--trivial to commit-- killed Cox and Kidd.

---

---

---

---

---

---

---

---

### Product Problems

- The problems with the X-ray target were the immediate cause of the accidents. But those were exacerbated by a poor "user interface" that encouraged technologists to operate the machine in a hazardous fashion. According to therapists, the Therac-25 often issued up to 40 diagnostic messages a day, indicating something was wrong. Most of these messages simply indicated that the beam intensity was slightly less than expected. It was possible to cancel the message and proceed with treatments by pressing the "P" key, and operators quickly learned to respond this way to almost any diagnostic message--which were hard to tell apart, since they were numerical codes rather than English text.

---

---

---

---

---

---

---

---

### Oops!

- In Tyler, the only indication of trouble that the operators saw was the cryptic message, "Malfunction 54." They repeatedly pushed "P" and turned the beam on again and again, dosing Ray Cox three times (investigators concluded that the first dose alone was fatal).

---

---

---

---

---

---

---

---

### **Vendor Problems**

- **AECL allowed a very hazardous product to reach the market. The central problem was not that some individual made a couple of mistakes while writing the computer code that handled the X-ray target. The problem was that AECL failed as an organization; it was unable to protect its customers from the errors of one of its staff.**

---

---

---

---

---

---

---

### **Customer Problems**

- **Clinic staff discounted injured patients' complaints and kept using the machines. Tyler continued treating after Cox's injuries were apparent, and Kidd was killed in the next month. In June 1985 Katy Yarbrough was badly injured by the Therac-25. After the treatment, crying and trembling, she told the treatment technologist, "You burned me." "I'm sorry," the technologist replied, "but that's not possible, it's just not possible."**

---

---

---

---

---

---

---

### **Regulatory Problems**

- **The FDA was sensitive to the clinics' plight. Asked after the fifth accident whether the FDA was considering a total ban, Edwin Miller of the Office of Compliance in the agency's Division of Radiological Products replied, "No such action is planned at this time. A complete ban would require an extensive study of risk assessment".**

---

---

---

---

---

---

---

## Safety-Critical Applications

- The FDA estimated that by 1990, virtually all devices produced by the \$11-billion-per-year medical electronics industry included embedded micro- or minicomputer.
- The medical equipment industry recalls about 400 products a year. Not all recalls involve life-threatening problems, but each implies that the product has serious problems inherent in its design.
- Twice as many computer-related recalls occurred in 1984 as in 1982 or any prior year. Most computer-related recalls were caused by software errors. There were 84 software-related recalls from 1983 through 1987.

---

---

---

---

---

---

---

---

## Update

- The FDA's analysis of 3140 medical device recalls conducted between 1992 and 1998 reveals that 242 of them (7.7%) are attributable to software failures. Of those software related recalls, 192 (or 79%) were caused by software defects that were introduced when changes were made to the software after its initial production and distribution.

---

---

---

---

---

---

---

---

## Samples

- A blood analyzer displayed incorrect values because addition, rather than subtraction, had been programmed into a calibration formula.
- A multiple-patient monitoring system mixed up patients' names with the wrong data.
- An infusion pump would continually infuse insulin if the operator entered "0" as the maximum value to be infused.
- Another pump would ignore settings of less than 1.0 milliliter per hour and deliver instead whatever the previous setting was, up to 700 milliliters per hour.
- If a certain command sequence was entered into one pacemaker programmer, the pacemaker would enter a random unpredictable state.
- In one ventilator, the patient disconnect alarm could fail to sound when needed, and the gas concentrations (like oxygen) could decrease without activation of an alarm or indication on the display.

---

---

---

---

---

---

---

---