Case Study: Therac-25

Therac-25 was a computer controlled machine for administering radiation treatment to cancer patients, manufactured by Atomic Energy Canada Limited (AECL). Therac-25 had two modes: a lower energy electron mode designed to focus on a specific part of the body, and a high energy x-ray mode designed to distribute energy over a wider area of the body. A tungsten shield moved into place during the x-ray mode to protect the patient from harm. The shield was not needed during the lower energy electron mode. Therac-25 was first used in 1982 and reused software from Therac-6 and Therac-20. Because there had been no problems with those previous machines, the Therac-25 designers removed hardware safety locks which physically prevented certain erroneous conditions. This was to be a critical mistake.

Accident 1, June 1985. This accident caused a large overdose to be given to a breast cancer patient. A nurse noticed the patient was 'warm' after treatment but the hospital denied any mistake. Indeed, the patient was sent for future treatments. However, she had been severely injured, lost the use of one of her arms, and had to have both breasts removed.

Accident 2, July 1985. A Therac-25 machine gave an error message during treatment. The machine displayed the message 'No Dose', prompting the hospital technician to start the machine again. The technician did this five times, not realising that each time, the patient ***had*** in fact been given a radiation dose. Overall, the patient received 13,000 – 17,000 rads (200 rads is a typical dose and 1000 rads can be fatal). After this accident, an AECL engineer investigated the Therac-25 machine but was unable to determine the cause of the fault.

Accident 3, December 1985. Accident three was similar to accident 1. The patient eventually recovered from his injuries. After this accident, hospital staff contacted AECL about problems with the Therac-25 machine. A month later AECL replied, stating *'After careful consideration, we are of the opinion that this damage could not have been produced by any malfunction of the Therac-25 or by any operator error'* and *'[there have] been no other instances of similar damage to other patients.'*

Accident 4, March 1986. This accident was one of the most severe: a Therac-25 machine paused with a 'Malfunction 54' error during the treatment. As in accident 2, the technician was prompted to restart the machine, and did so. Unfortunately she had stumbled onto two faults in Therac-25 at the same time: one which gave a (single) overdose to a patient, and the 'No Dose' error. The patient received two large overdoses and died five months later. A contributing factor was broken audio/visual equipment, stopping the nurse seeing that the patient was hurt and trying to escape the room.

Accident 5, April 1986. In the same hospital as accident 4, with the same technician, the same 'Malfunction 54' error occurred. This time the technician stopped treatment immediately, but it was too late: the patient received an overdose, suffered severe neurological damage, and died three weeks later. After this accident the operator remembered the sequence of input she had made to cause the 'Malfunction 54' error message. Working with the hospital's physicist, she was able to eventually reproduce the error message at will. The speed at which the data was entered was critical in causing the error to occur. If data was entered and then quickly altered, the error would occur. The next day they reported this to an AECL engineer and two days later AECL acknowledged the error. Further testing revealed the dosage during the error to be up to 25 times higher than the amount required to kill a person.

Accident 6, January 1987. Despite the cause of the fatal overdoses being known, a Therac-25 machine at the same hospital as accident 3 was still in use. A technician received an error message during treatment of a patient and an overdose was administered. The patient died three months later.

By the time Therac-25 was removed from service, three people had been killed and three more seriously injured. The system had two main faults. The first, 'Malfunction 54', gave an overdose to the patient because the software did not move the tungsten shield into place during the high powered x-ray mode. The second error, 'No dose', caused a false message to be displayed, even though a radiation dose ***had*** been delivered. This fooled the operators into giving a second (normal) dose, thus causing an overdose. Accident 4 was particularly unfortunate because both errors occurred, giving the patient multiple overdoses. The tragedy of Therac-25 is that the programming errors were very simple errors, and existed in all previous versions of Therac but had been prevented by the hardware safety locks — the same safety features the Therac-25 designers removed because of the unbroken safety record of Therac-6 and Therac-20[5,6,7].