Radiation Cancer Therapy Machine Mishaps in 1985-86 due to Safety Critical Software Control Errors

Leadership ViTS Meeting
December 18, 2006

Jim Lloyd
Deputy Chief, Safety and Mission Assurance

Previous Leadership ViTS safety presentations can be found at:
https://sma.nasa.gov/safety-messages

The Mishaps

In a 20-month period between June 1985 and January 1987, Therac-25 radiation therapy machines used in both the US and Canada administered massive overdoses of electron beam radiation to at least six cancer patients, with at least three deaths attributed to radiation overdose.

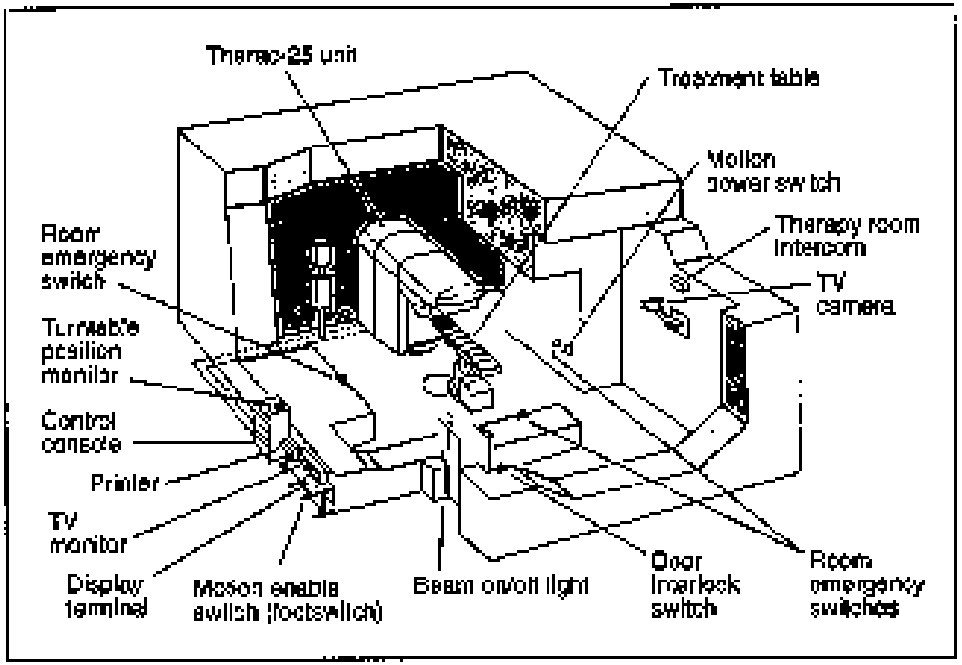

Figure 1. Typical Therac-25 facility.

History of the Therac-25

- Two companies, one in Canada and the other in France collaborated in the 1970s to build two linear accelerators (Therac-6 and Therac-20) to administer controlled doses of radiation for treatment of cancer.
- Both machines were based on the French company's prior designs.
- The Canadian company, working alone, then developed the Therac-25, making a number of design modifications to the hardware and re-using some of the software from the prior two designs, and started shipping units in 1983.
- The US Food and Drug Administration approved the new design based on the heritage design of the previous machines (including the control software).

Design Changes for the Therac-25

- The Therac-25 was capable of operating in two modes (direct electron beam (5 MeV to 25 MeV) and X-ray beam (25 MeV electron beam converted to soft X-rays) .
- X-rays were produced from the electron beam source using a succession of 3 components that converted, shaped and moderated the beam.
- The system (unlike the earlier systems) was designed from the outset to be computer controlled.
- To save cost and increase efficiency, some hardware safety features used in the prior designs were eliminated and the safety functions were believed to be incorporated into the control software.
- The prior software was modified (reused with changes) for this more complex and powerful machine.

Therac-25 Operation and Problems

- **In the x-ray mode of operation:**
  - Required 100 times more input electron energy.
  - A beam flattener provided consistent dose over a larger target area, and kept the radiation dose at a safe level.
  - Patient was exposed to 100 times the required dose if the beam flattener was not engaged.
  - Software controlled the engagement of the beam flattener when x-ray mode was selected.
    - A hardware interlock that had been incorporated in the previous generation of equipment to prevent overdose had been eliminated in the Therac-25.
    - The design had no capability to warn of overdose (open loop).

- **Frequent malfunctions were being reported (up to 40 per day per machine) with no effective manufacturer response or information sharing among users.**

Cause Factors

- **Proximate Cause**
  - Patients received direct electron beam radiation overdose due to operating in the x-ray mode without operator knowing the beam flattener was not engaged.
- **Intermediate Causes**
  - Operators performed setup more quickly than accommodated by design.
  - Software safety interlock had an unknown “race” condition (1/256) that manifested itself only during these “quick” setups.
  - The machine had no safety shutoff feature based on sensed improper high dosage (open loop control).

Contributing Factors

- New system with modified software based on much different older systems.
- System software programmed and reprogrammed, verified and validated entirely by a one individual.
- In developmental phase, fault tree analysis included software as a source of failure, but extremely low failure probabilities were reported and no units were specified for the interval between failures:
  - "Computer selects wrong energy" probability of $1X10^{-11}$ (units?)
  - "Computer selects wrong mode" probability of $4X10^{-9}$ (units?)
- No scenario analysis was conducted using the failure of the software as a pivotal event in a mishap sequence.
- No record of original system testing.
- Frequent malfunctions of the device to the extent that operators no longer reported them.
  - An aside, in 1990, health-care facilities were required by law to report incidents to both the manufacturer and to the FDA.
- Despite the existence of multiple adverse indicators during operation, these problems, issues, and analyses were not evaluated or investigated from a systems perspective.

Lessons for NASA on the Use of Safety Critical Software

- Re-used software code does not guarantee correct code whether or not modified to accommodate other changes.
- Safety critical software:
  - needs to be developed using standards and effective design processes.
  - should be included in any scenario-based risk analysis.
  - should be subject to independent validation of the design requirements and verification that it meets those requirements.
- Safety analyses and testing need to evaluate the full spectrum of system operation (especially when software is performing a safety critical function).
- Assure an appropriate means for evaluation of reported problems and the development of appropriate system corrections.
- Share failure data with the design center and among the user community (problem reporting and corrective action (PRACA), close calls, mishaps, etc.).

References:

Leveson, Nancy, Safeware - System Safety and Computers, Addison Wesley, 1995, Reading, MA, 680 pp.

NASA Standard 8719.13, Software Safety, July 8, 2004

Also, http://sunnyday.mit.edu/papers/therac.pdf

Or simply Google "Therac-25"