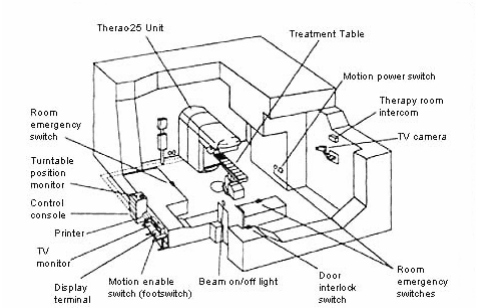
Embedded Systems

Bernd Finkbeiner
Calogero Zarba
Moritz Hahn

Sommersemester 2007

A Safety Failure Example



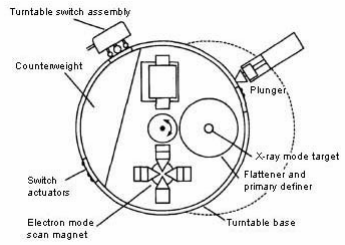


Figure B. Upper turntable assembly

Therac-25

- Computer controlled radiation therapy machine
  Built by Canadian company CMC, used in Canada and US
- Electron beam – treats shallow tissue
- Photon beam – treats deep tissue
  - Also alignment mode for positioning of radiation beam
  - Each mode requires different position of turntable
- Safety failure
  Between 1985 and 1987 6 people wrongly received massive overdoses, 4 died as a result

History

- Therac-6
  Photon beam only, linked to PDP-11,
  but capable of operating without computer

  Safety implemented in hardware
- Therac-20
  Dual mode device, linked to PDP-11,
  but capable of operating without computer

  Safety implemented in hardware
- Therac-25
  Dual mode device, PDP-11 required for operation
  Relies on software for some safety features

  Software written in assembler,
  using software from
  Therac-6 and Therac-20

First Bug (May 1986)

- Feature
  – Changes to parameters allowed during set up
  – Set up takes 8 sec
- Problem
  – Sometimes changes ignored, though shown on the screen
  – Caused by flag being set in the wrong place
- Accident scenario
  – Operator selected photon by mistake, set up was initiated then operator changed energy level within 8 sec
  – Changes ignored, so dosage too high
- Fix
  – Disallow edits during set up
  – Must reset device to change parameters

Second Bug (January 1987)

- Feature
  - Software controlled interlock, prevents activation of the beam when turntable not correctly positioned
- Problem
  - Interlock fails, allowing beam to be activated
  - Caused by flag being set using code:
    flag := flag + 1
  - for an 8-bit integer, so it wrapped around to zero!
- Fix
  - Software fixed
  - Extra hardware interlocks and shutdown system added