"An Investigation of the Therac-25 Accidents"

by Nancy G. Leveson and Clark S. Turner

slides adapted from the article and a graduate presentation by Catherine Schell

Development of the Therac-25

- Early 1970's
  - AECL and CGR (Fr.) collaborated
    - developed Therac-6: 6 MeV accelerator that produced X-rays only (cobalt)
  - Later, developed Therac-20: 20 MeV dual-mode accelerator
    - Both versions of older CGR machines
      - augmented with computer control

Development of the Therac-25 cont'd

- Mid 1970's: AECL "double-pass"
  - used in design of Therac-25
    - what was good about it?
- 1976: first hardwired prototype Therac-25
- 1981: AECL and CGR broke up :-)

Development of the Therac-25 cont'd

- 1982: Commercial version of Therac-25
- March 1983: AECL *safety analysis* assumptions:
  - Programming errors reduced by extensive testing;
    - software errors not included in analysis
  - Software does not degrade or wear out
  - Computer execution errors caused by faulty hardware and random errors due to noise

Important Features of the Therac-25

- AECL designed Therac-25 to depend on computer control
  - Th-6 and Th-20 had could function without computer control
- Th-25 software replaced much hardware in safety functionality
  - why?
- Software in the Th-6 and Th-20 was reused in the Th-25
  - why?

Therac-25 Software

- Real time exec, PDP-11 ass'y code
  - Four major components:
    - Stored data
    - Scheduler
    - Set of critical and non-critical tasks
    - Interrupt services
- Exec allows concurrent access to shared memory
  - Synchronization using data stored in shared variables
  - "Test" and "set" operations for shared variables are not indivisible

Major Event Timeline: 1985

- June
  - 3rd: Marietta, GA "problem"
    - Hospital phys called AECL - ask if overdose possible
    - AECL reply three days later: "NO!"
- July
  - 26th: Hamilton, Ontario, Canada mild overdose seen
    - machine shut down with "H-tilt" message
    - AECL notified, cause surmised to be microswitch failure
      - AECL could not repeat the error condition though
- August
  - 1st: Four users in US advised
    - check ionization chamber to verify postion
    - treatment should be discontinued if "H-tilt" error message
      - and incorrect dosage displayed

Major Event Timeline: 1985 cont'd

- September
  - AECL "fixes" microswitch "problem"
    - notifies users of radical improvement in safety
  - Independent consultant (Hamilton) recommends potentiometer on turntable
    - analog (redundant) indication of position
- October
  - Georgia patient files suit against AECL and hospital
    - still not known that it was a Th-25 accident

Major Event Timeline: 1985 cont'd

- November
  - 8th: Letter from CRPB to AECL
    - asks for hardware interlocks and software changes
      - redesign microswitch
      - cancel treatment in event of dose rate errors
      - change to treatment "pause" to "suspend" with serious errors and after one try
      - new test procedures and command formats (UI)
- December
  - Yakima, WA mild overdose
    - looked like "water bottle" burns to MD's

Major Event Timeline: 1986

- January
  - Atty (Hamilton) demands potentiometer on turntable
    - how hard is this?
- 31st:AECL from Yakima: possibility of overdose
- February
  - 24th: AECL to Yakima: "overdose not possible, no other incidents had occurred…"

Major Event Timeline: 1986 cont'd

- March
  - 21st: Tyler, TX overdose: AECL notified; AECL claims overdose impossible, no other accidents occurred, suggests electrical problem in hospital as cause
- April
  - 7th: Tyler machine put back in service after no electrical problem found
  - 11th: Second Tyler overdose: AECL notified; AECL finds software problem
  - 15th: AECL files accident report with the FDA

Major Event Timeline: 1986 cont'd

- May
  - 2nd: FDA declares Therac-25 defective; FDA asks for CAP and proper notification of users
- June
  - 13th: AECL submits CAP to FDA
- July
  - 23rd: FDA responds, asks for more info
- August
  - First user group meeting

Major Event Timeline: 1986 cont'd

- September
  - 26th: AECL sends FDA additional info
- October
  - 30th: FDA requests more info
- November
  - 12th: AECL submits revision of CAP
- December:
  - Therac-25 users notified of software bug
  - 11th: FDA requests further changes to CAP
  - 22nd: AECL submits second revision of CAP

Major Event Timeline: 1987

- January
  - 17th: Second Yakima, WA overdose
  - 26th: AECL sends FDA revised test plan
- February
  - Hamilton clinic investigates first accident, concludes overdose occurred
  - 3rd: AECL announces changes to Therac-25
  - 10th: FDA notifies AECL of adverse findings declaring Therac-25 defective under US law, asks AECL to notify users not to use it for routine therapy; Health Protection Branch of Canada does the same.

Major Event Timeline: 1987 cont'd

- March
  - Second user group meeting
  - 5th: AECL submits third revision of CAP
- April
  - 9th: FDA requests additional info from AECL
- May
  - 1st: AECL submits fourth revision of CAP
  - 26th: FDA approves CAP subject to final testing and safety analysis

Major Event Timeline: 1987 cont'd

- June
  - 5th: AECL sends final test plan and draft of safety analysis to FDA
- July
  - Third user group meeting
  - 21st: AECL submits fifth revision of CAP

Major Event Timeline: 1988

- January
  - 29th: Interim safety analysis report issued
- November
  - 3rd: Final safety analysis report issued

Lessons Learned

- Do not put too much confidence in the software.
- Do not remove standard hardware interlocks when adding computer (software) control.
- Software should not be solely responsible for safety.

Lessons Learned cont'd

- Systems should not be designed wherein a single software error can be catastrophic.
- Software error should not be the last possibility investigated in an accident.
- Engineers need to design for the worst case.

Lessons Learned cont'd

- Companies building hazardous equipment should include
  - hazard logging and tracking
  - incident reporting
  - incident analysis

  as part of quality control procedures.
- Risk assessment numbers should be meaningful, and statistics should be treated with caution.

Lessons Learned cont'd

- Documentation is important.
- Software quality assurance practices and standards should be established.
- Designs should be simple.
- Error logging or software audit trail reporting should be designed into the software from the beginning.
- System testing alone is not adequate; there should also be testing and formal analysis at the module and software levels.

Lessons Learned cont'd

- Safety-critical software projects must incorporate safety-analysis and design procedures.
- Reusing software modules does not guarantee safety in the new system.
- Software engineers need additional training and experience when working on safety-critical systems.

Lessons Learned cont'd

- Software engineers need
  - better training in interface design, or
  - more input from human factors engineers.
- There must be recognition of the potential conflict between user-friendly interfaces and safety.

Lessons Learned cont'd

- Reasons for design decisions must be recorded.
- Users of safety-critical systems should be involved in resolving problems.