CASE STUDY: THERAC-25

Machine:

- SW controlled radiation therapy
- dual-mode
  - electron beam
  - xray
  - visible light beam

- developed from Therac-6 & Therac-20
- eliminated HW safety interlocks of preceding designs
- reuse of some SW of preceding designs

Operation Failures:

- massive overdoses to 6 patients (3 deaths)
- frequent malfunctions ($\leq$40 dose /day)

- mostly underdoses
- operators became inured to frequent error messages
  - messages didn't indicate safety hazards
  - error #'s
  - obscure messages
  - explanations not documented in user manuals
  - severity not indicated by effort to continue operation
- little documentation of development of SW specifications and testing plan

Bugs:

- overdoses traced to 2 specific SW bugs
- set up test procedure, called potentially 100's of times
  - based on a flag variable
  - variable incremented
  - value of zero indicates completion
  - 1 byte storage
  - overflow to zero

- race conditions
  - machine could ignore typed (edited) operator input
  - edited info failed to propogate
  - occurrence if experienced operator edited quickly

Why Multiple Incidents:

- operator uncertain of source of patient injuries
- manufacturer denial, incredulity & prevarication

- changes made not knowing if they solved the critical problems
- bogus reliability improvement figure declared by manufacturer (10^5)
- clinics maintained use based on incomplete or false info
- internal investigation
- external recommendations not implemented
- manufacturer responsible for notifying users that machine declared defective by FDA

- one year to negotiate changes
- external clinic video & audio monitoring failure

Overconfidence:

- operator incredulity
- manufacturer overconfidence in SW
- clinics assumed machine safe

- error messages ignored due to frequency

Conclusion:

- Manufacturer irresponsibility
  - carelessness
  - corner cutting
  - avoidance of responsibility

- Remedy:

- good SW development procedures
- individual initiative & responsibility
- training & education
- accountability
- management responsibility