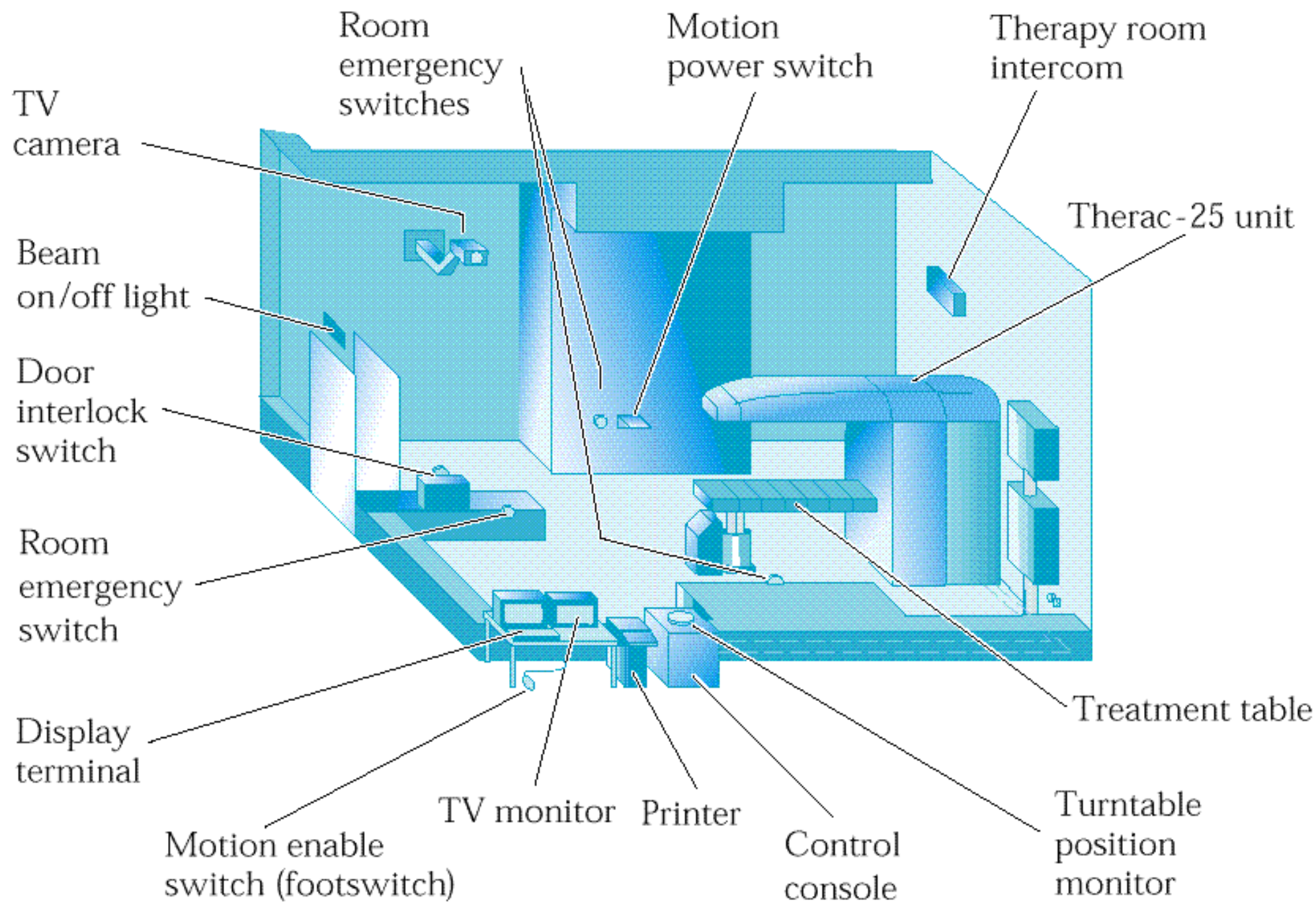


Nancy G. Leveson and Clark S. Turner, “An Investigation of the Therac-25 Accidents”.
Computer **26(7)**, pp. 18-41, Jul 1993.

Presented by Dror Feitelson

The Big Picture

- The Therac-25 was a computerized radiation therapy machine
- 11 machines were installed (US and Canada)
- In 1985-1987 there were 6 known accidents where massive overdoses were made (patients died or suffered serious injuries)
- These were traced to race conditions in reading operator input
- Unique early investigation of safety-critical software



Operation Modes

- Accelerator produces high-energy electron beam
- Electron-beam treatment
 - Direct irradiation with 5-25 MeV energy but low flux
 - Use scanning magnets to spread beam
- X-ray treatment
 - 25 MeV energy at high flux (100X)
 - X-ray target and beam flattener turn the electron beam into an X-ray beam

Software Responsibility

- Designed to be controlled by a PDP-11
- Accept operator input of treatment parameters
- Operate the beam
- Control and monitor machine configuration and status
 - Including scanning magnets vs. X-ray target
- Software replaces some earlier hardware monitors and safety measures
 - No *known* problems so hardware monitors considered unnecessary

Software Development

- By a single programmer with unknown background
- Done in PDP-11 assembler
- Little documentation
- Tested mainly as an integrated system

Software Structure

- Four major components:
 - Stored data tables
 - Scheduling service
 - Critical and non-critical tasks
 - Interrupt service

Scheduler

- Operates at a rate of 10Hz
- Priority to critical tasks

Critical Tasks

- Treat – the main routine (described later)
- Servo – setup and monitoring of the beam gun
- Housekeeping

User Interface

Using DEC VT100 terminal



```
PATIENT NAME      : JOHN DOE
TREATMENT MODE   : FIX      BEAM TYPE: X      ENERGY (MeV): 25
                                ACTUAL      PRESCRIBED
UNIT RATE/MINUTE           0           200
MONITOR UNITS              50  50       200
TIME (MIN)                 0.27        1.00
GANTRY ROTATION (DEG)      0.0          0      VERIFIED
COLLIMATOR ROTATION (DEG) 359.2         359     VERIFIED
COLLIMATOR X (CM)         14.2         14.3     VERIFIED
COLLIMATOR Y (CM)         27.2         27.3     VERIFIED
WEDGE NUMBER              1            1      VERIFIED
ACCESSORY NUMBER          0            0      VERIFIED
DATE      : 84-OCT-26   SYSTEM : BEAM READY   OP.MODE: TREAT AUTO
TIME     : 12:55. 8    TREAT  : TREAT PAUSE           X-RAY 173777
OPR ID   : T25V02-R03  REASON  : OPERATOR      COMMAND:
```

User Interface

- Use “return” to note that current value is correct
- Use up-cursor key to move up and edit
- “Verified” means input corresponds to manual hardware settings
- Keyboard command “b” turns beam on

```
PATIENT NAME   : JOHN DOE
TREATMENT MODE : FIX      BEAM TYPE: X      ENERGY (MeV): 25
                                ACTUAL      PRESCRIBED
    UNIT RATE/MINUTE           0           200
    MONITOR UNITS              50  50       200
    TIME (MIN)                 0.27        1.00
GANTRY ROTATION (DEG)         0.0          0      VERIFIED
COLLIMATOR ROTATION (DEG)    359.2         359     VERIFIED
COLLIMATOR X (CM)           14.2          14.3     VERIFIED
COLLIMATOR Y (CM)           27.2          27.3     VERIFIED
WEDGE NUMBER                 1            1      VERIFIED
ACCESSORY NUMBER             0            0      VERIFIED
DATE       : 84-OCT-26   SYSTEM : BEAM READY   OP.MODE: TREAT AUTO
TIME      : 12:55. 8    TREAT  : TREAT PAUSE      X-RAY 173777
OPR ID    : T25V02-R03  REASON  : OPERATOR     COMMAND:
```

Error Conditions

- Suspend treatment
 - Requires resetting the machine
- Pause treatment
 - Typically full dose was not administered
 - Treatment parameters stay in effect
 - Retry using “p” key (proceed)
- Up to 40 such events in a day's work
 - Cryptic error messages (“malfunction 54”)
- Operators become insensitized to error
 - Errors thought not to jeopardize patients

Accident Scenario I

- Operator enters mode X and energy
- Enter all other relevant fields
- Move up to change X to E
- Multiple returns to command line
- Beam on
- All within 8 seconds

Treat Task

- Composed of 8 subroutines
 - Upon invocation, call subroutine identified by “Tphase”
 - Upon return, re-schedule
- 1) Reset
 - 2) Data entry
 - 3) Setup done
 - 4) Setup test
 - 5) Patient treatment
 - 6) Treatment pause
 - 7) Treatment end
 - 8) Date/time/ID change

Race Conditions

Operator

- Mode=X
- Fill other fields
- Correct mode=E
- End input

Hand

- Set position X
- Set position E

Treat

- Call datent
 - Set params for mode X
 - Set bending magnets (8 sec)
 - Input ended?
Tphase=3
- Call SetupTest

Bug1: check change in mode, but only during setting of first magnet

Bug2: flag end when cursor reached end even if didn't stay there

Accident Scenario II

- Operator inputs params
- Operator completes setup in treatment room using light mode (show light where beam will go)
- Operator hits “set” to replace light mirror with correct beam device
 - Device is not replaced
- Beam goes through mirror without proper attenuation or spreading

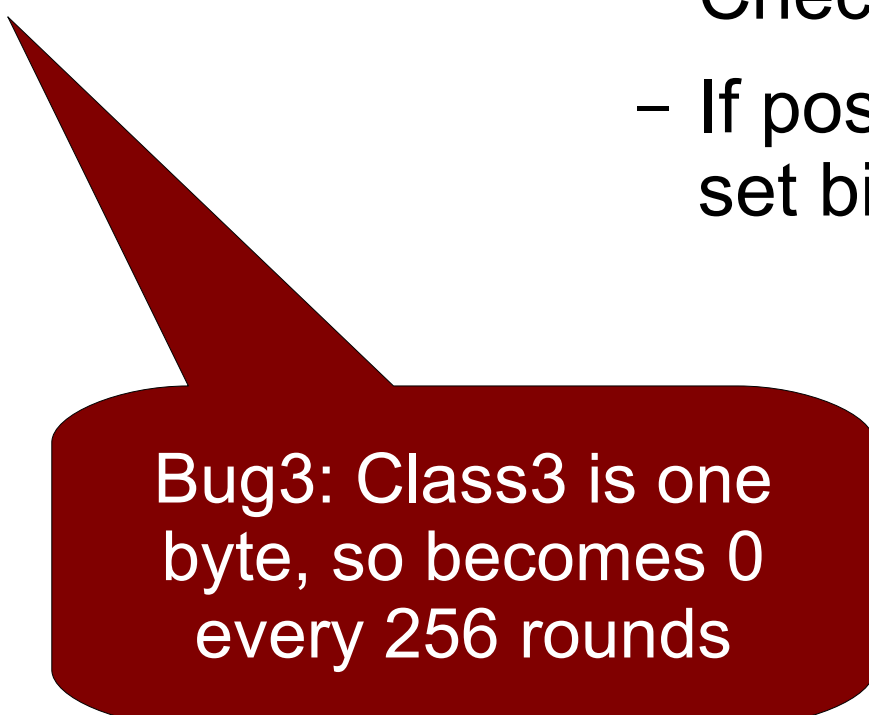
Race Condition

Treat

- Call SetupTest
 - Class3++
 - F\$mal=0?
Tphase=2
- Reschedule

Housekeeper

- If Class3>0
 - Check collimator
 - If position wrong
set bit 9 in F\$mal



Bug3: Class3 is one byte, so becomes 0 every 256 rounds

System Engineering Problems

- Initial safety analysis did not include software
- Software trusted to replace hardware interlock facilities (beam operable only if collimator in correct position)
- Lack of adequate monitoring (no indication of saturation in ion-chambers used to measure radiation)

Societal Problems

- Operator behavior
 - Automatically hit “p” in case of trouble
 - Video camera in room disconnected
- Vendor and regulatory bodies
 - Propagate information about malfunction

Programming Problems

- Complicated concurrent program
- Race conditions
- Error messages to operators

Software Engineering Problems

- Complex design
- Audit trails should be designed into the software
 - What actually happened?
- Employ extensive testing and formal verification
- Documentation
 - Users need to understand error conditions
 - Also documentation of code