The Therac 25
A case study in safety failure

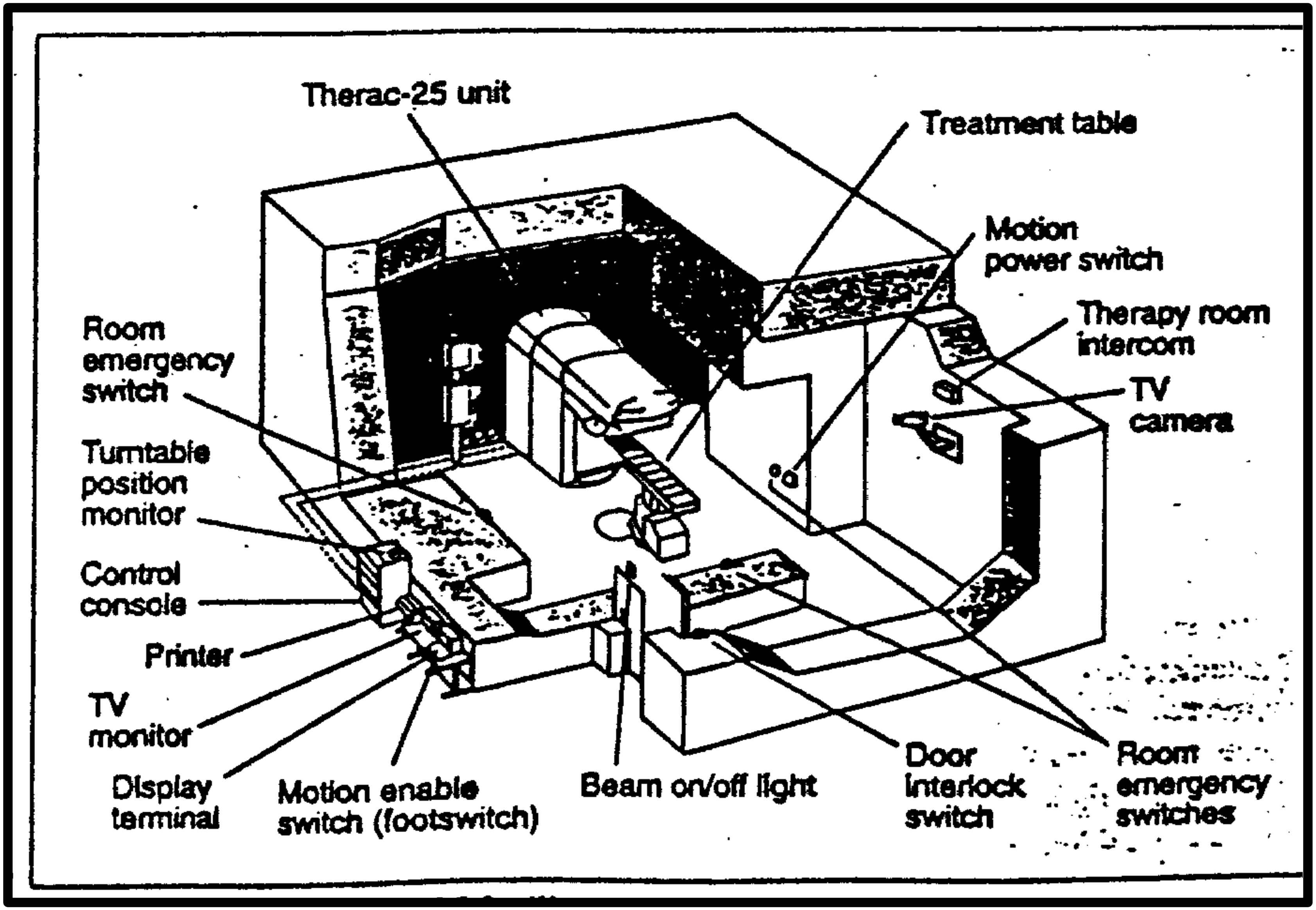
- Radiation therapy machine
- “The most serious computer-related accidents to date”
- People were killed
- Reference:

  Nancy Leveson and Clark Turner, “The Investigation of the Therac-25 Accidents”, Computer, 26, 7 (July 1993) pp 18-41.

Therac 25 Background

- Medical linear accelerator developed by Atomic Energy of Canada, Ltd. in mid-1970s
- Delivers 25 MeV photons or electrons of various energies
- Controlled by PDP-11 minicomputer
- Software responsible for safety
- Software adapted from earlier Therac-6 & Therac 20 systems, which had hardware interlocks for safety

The Therac 25



Therac 25 Turntable

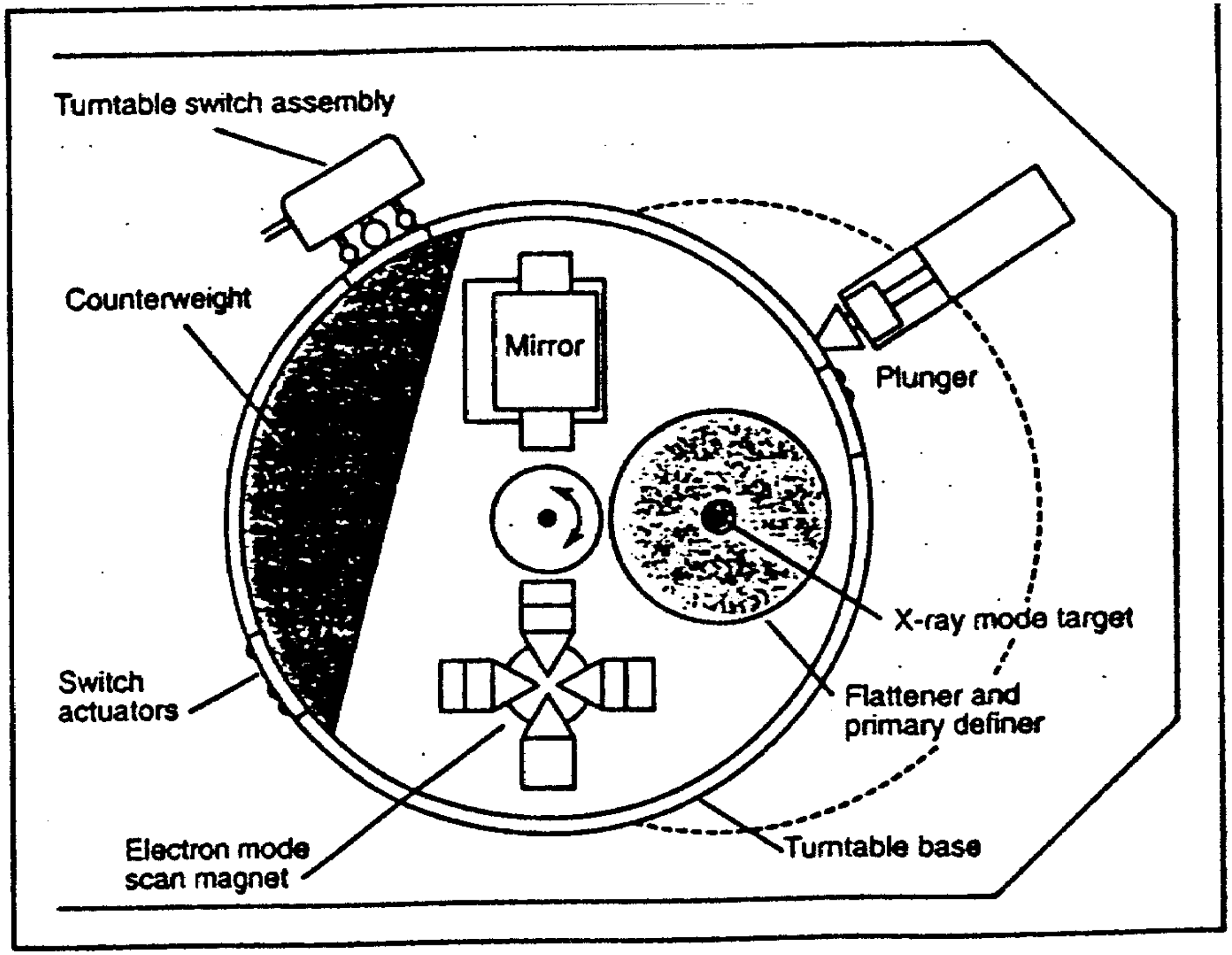

Turntable switch assembly
Counterweight
Mirror
Plunger
X-ray mode target
Flattener and primary definer
Switch actuators
Electron mode scan magnet
Turntable base

Figure B. Upper turntable assembly.

Therac 25 Turntable

- Electron mode
  - 5-25 MEV
  - Magnets spread beam
  - Ion chamber monitor
- X-ray mode
  - 25 MEV electrons hit target
  - “Beam flattener” attenuates
  - 100x beam current
  - Ion chamber monitor
- Field-light mode
  - No current
  - Mirror & light used to check alignment
  - No ion chamber (since not treating)

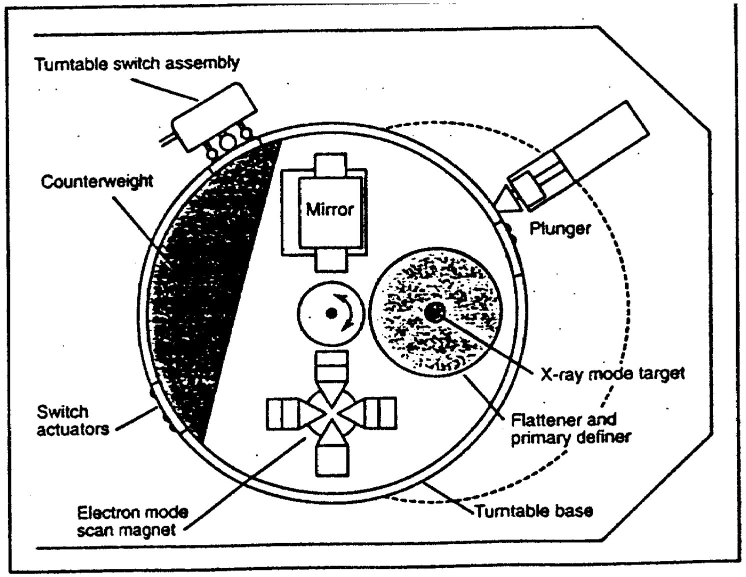

Turntable switch assembly
Counterweight
Mirror
Plunger
X-ray mode target
Switch actuators
Flattener and primary definer
Electron mode scan magnet
Turntable base

Figure B. Upper turntable assembly.

Therac 25 Turntable

- Computer adjusts turntable position
- Microswitches detect turntable setting
- 3-bit binary code used to encode turntable setting
- Software checks replace hardware interlocks

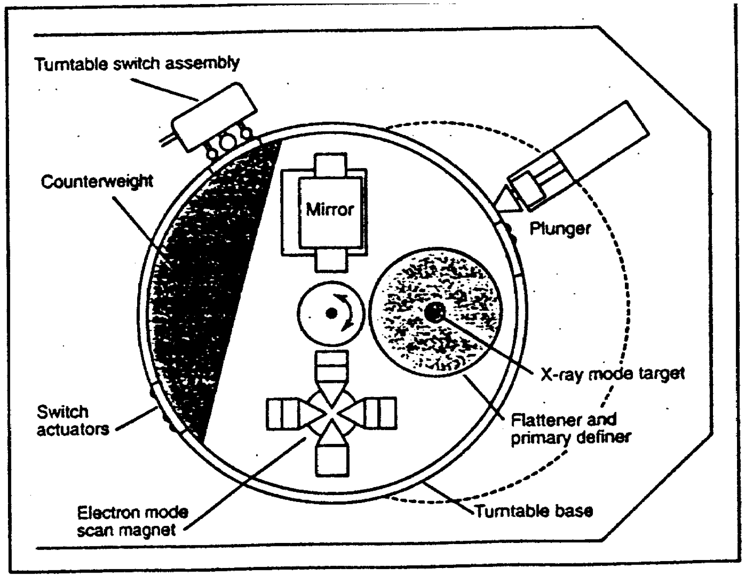

Turntable switch assembly
Counterweight
Mirror
Plunger
X-ray mode target
Flattener and primary definer
Switch actuators
Electron mode scan magnet
Turntable base

Figure B. Upper turntable assembly.

Therac 25 Software Development

- Evolved from Therac 6 system (1972-1976)
- Incorporated some Therac 20 code, as well
- Written in PDP-11 assembler
- Custom operating system
- Little documentation during development
- Minimal unit and software testing
- Q/A testing was 2700 hours of use as integrated system
- Programmer left AECL in 1986, little information available about his background

"I know this may be an awkward time,
but do you recall him ever mentioning source code."

Therac 25 Software Functions

- Monitors machine status
- Sets up machine for treatment
- Turns beam on and off in response to operator
- Monitors interlocks
- If fault, either prevents treatment start or causes a pause/suspend

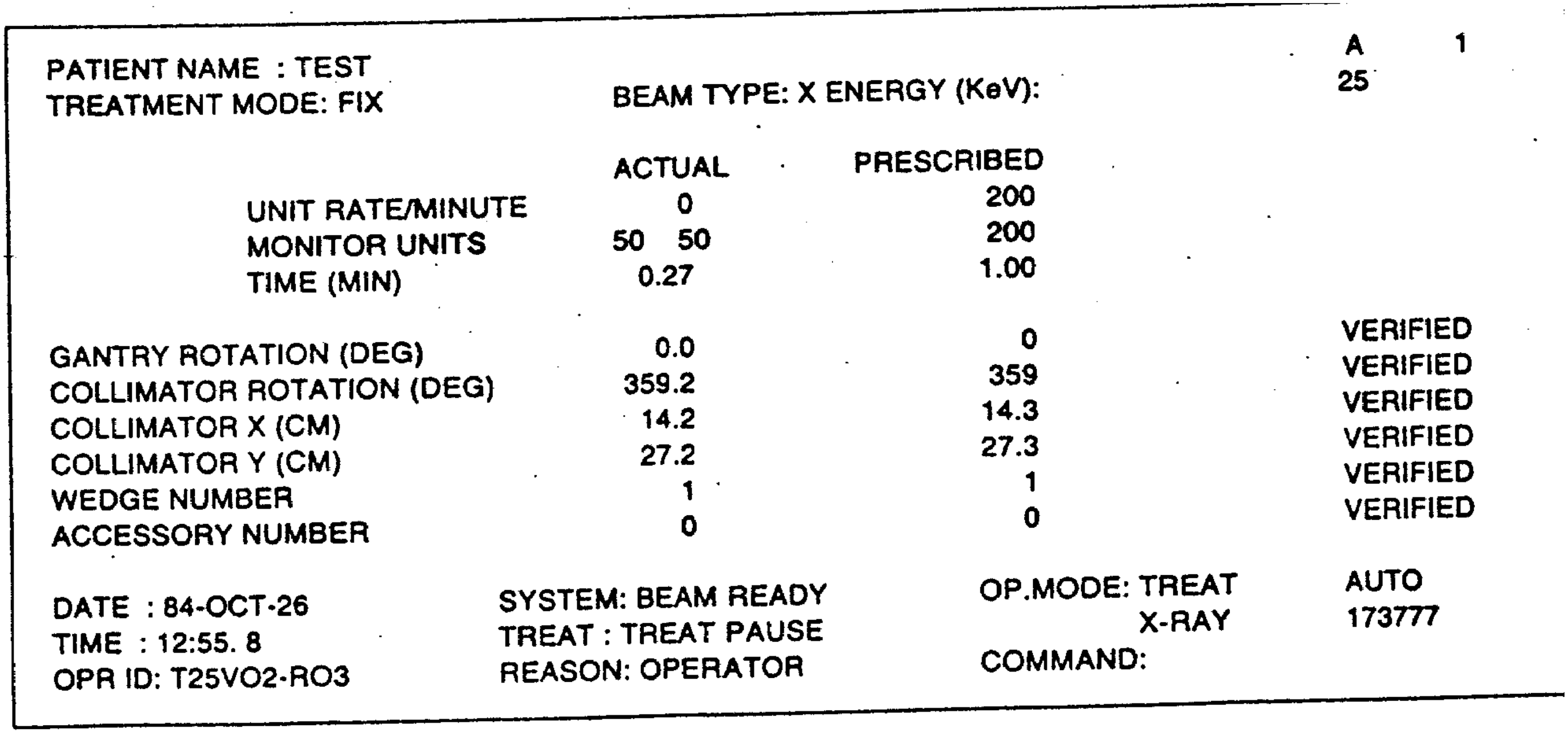
Therac 25 Software Structure

- Critical tasks:
  - Treatment monitor
  - Servo
  - Housekeeping
- Non-critical tasks:
  - Checksum
  - Keyboard
  - Calibration
  - etc.
- Concurrent access to shared memory, “test” and “set” of variables not indivisible, race conditions

Operator Procedures

- Position patient on table
- Manually set treatment field size and gantry rotation; attach accessories
- Leave room
- Use VT-100 console to enter patient data, dose data, etc.
- (System compares manual settings with system values)
- If “verified”, operator can start machine
- Else must re-enter data

Operator Screen Layout



```
                                                                                A         1
PATIENT NAME  : TEST                                                            25
TREATMENT MODE: FIX              BEAM TYPE: X ENERGY (KeV):

                                 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: T25VO2-RO3          REASON: OPERATOR          COMMAND:
```

Figure A. Operator interface screen layout.

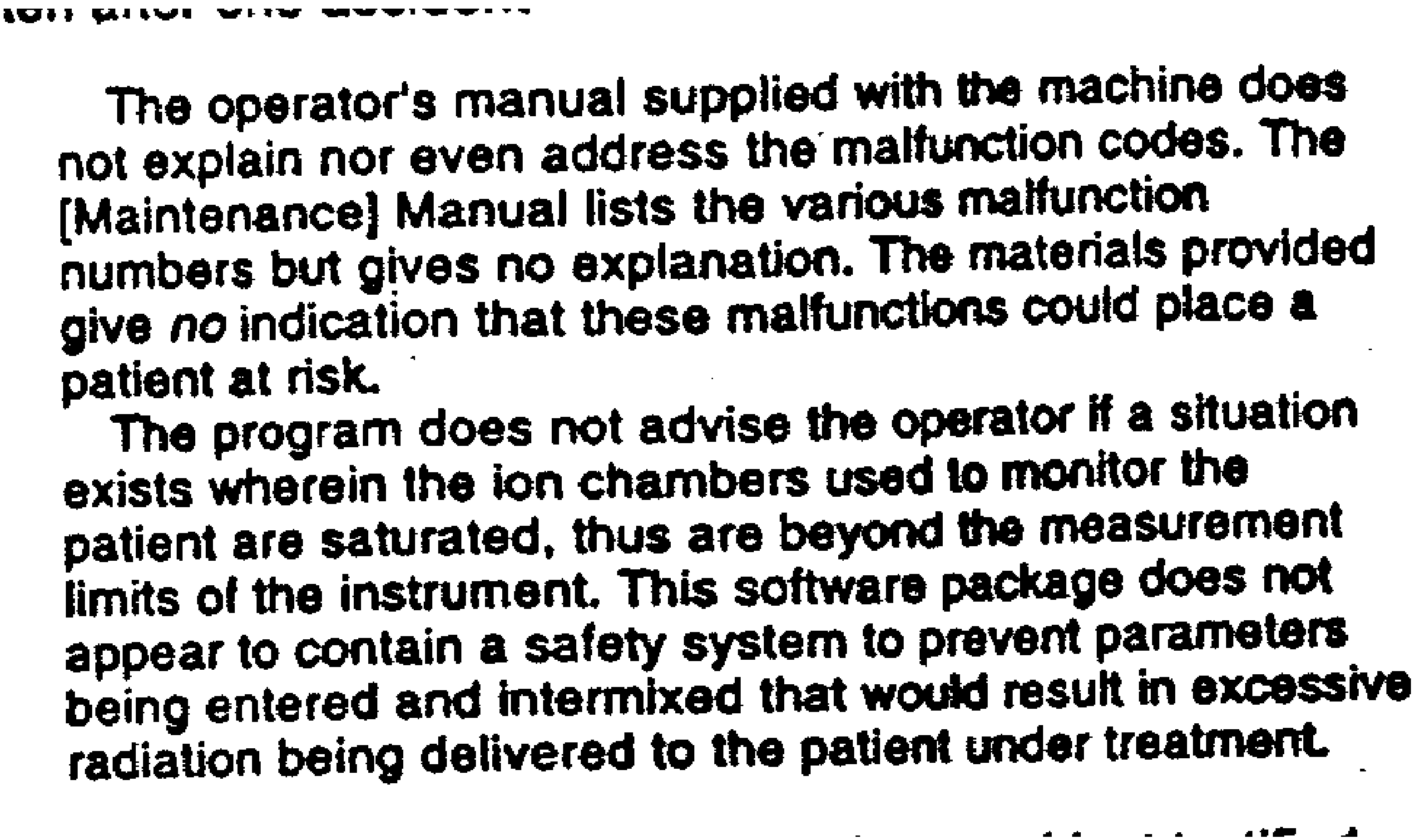
Operator Procedures

- **Complaint**
  - Re-entering all that data manually is very tedious
- **Response**
  - Set things up so that “carriage return” copies previous data for entry
  - Series of carriage returns effectively permits fast re-entry of unchanged parts of data

Operator Procedures

- **Error Conditions**
  - – “Treatment suspend” requires complete machine reset
  - – “Treatment pause” can be resumed if operator types “P” at console
  - – Machine insists on reset after 5 “P”s
  - – Malfunction messages fairly common & usually do not affect safety
- **Error Messages**
  - – Cryptic
  - – Some were of the form “Malfunction NN”

FDA Comment on Manual



ion after the accident.

The operator's manual supplied with the machine does not explain nor even address the malfunction codes. The [Maintenance] Manual lists the various malfunction numbers but gives no explanation. The materials provided give *no* indication that these malfunctions could place a patient at risk.

The program does not advise the operator if a situation exists wherein the ion chambers used to monitor the patient are saturated, thus are beyond the measurement limits of the instrument. This software package does not appear to contain a safety system to prevent parameters being entered and intermixed that would result in excessive radiation being delivered to the patient under treatment.

Accident History

- 11 Therac 25’s installed (5 US, 6 Canada)
- Six accidents involving massive overdoses between 1985 and 1987
- Machines recalled in 1987
- Related problems in Therac 20 discovered later but hardware interlocks prevented injuries

E.g., East Texas, March 1986

- History of 500 patients treated successfully
- Prescribed: 22MeV electrons, 180 rads
- Operator selected x-rays by mistake, used cursor keys to change to electrons
- Machine tripped with “Malfunction 54”
  - Documentation explains this is “dose input 2” error
- Operator proceeded; machine tripped again

E.g., East Texas, March 1986

- Patient felt something wrong on first jolt, tried to get up
- Video/audio links to room not functioning
- Patient felt jolt on arm while getting up, pounded on door
- Treatment cancelled for day
- Calibration checks seemed normal
- Later found patient had gotten 16,500-25,000 rads over 1 cm square
- Patient eventually died after 5 months

E.g., East Texas, March 1986

- AECL engineers could not replicate a Malfunction 54
- AECL home office engineer said machine could not overdose patient
- AECL suggested patient got an electric shock
- No grounding problems found
- Machine returned to service April 7, 1986

East Texas/ April 11,1986

- Prescription 10 MeV, area 7 x 10 cm
- Operator used cursor keys to change x-rays to electrons, saw “beam ready”, and turned machine on
- Loud noise, shutdown, malfunction 54
- Patient in great pain
- Patient died three weeks later

East Texas/ April 11,1986

- Machine taken out of service
- ETCC eventually reproduced malfunction 54
  - Data entry speed critical factor
  - Observed 4000 rad dose
- AECL later measured 25,000 rads
- In lawsuit, earlier “cursor up” problems reported, which AECL believed to have been fixed

Yakima Valley, January 1987

- Plan: 2 film verification exposures (3 & 4 rads) + 79 rad photon treatment
- Performed two film exposures
- Operator used hand controls to rotate table to field-light position & check alignment
- Operator set machine but forgot to remove film
- Operator turned beam on, machine showed no dose & displayed fleeting message
- Operator proceeded from pause

Yakima Valley, January 1987

- After another machine pause, operator reentered room.
- Patient complained of burning sensation
- Patient developed severe striped burns
- Patient died in April
- Hospital obtained similar pattern on film by running machine with turntable in field light position

Responses

- Voluntary Class II recall 8/1/85
- AECL accident report April 15, 1986
- First version of corrective action plan 6/13/86
- Second Yakima overdose 1/17/87
- Fifth (final) corrective action plan 7/21/87
- Interim safety analysis report 1/29/88
- Final safety analysis report 11/3/88

Tyler Accident Race Condition

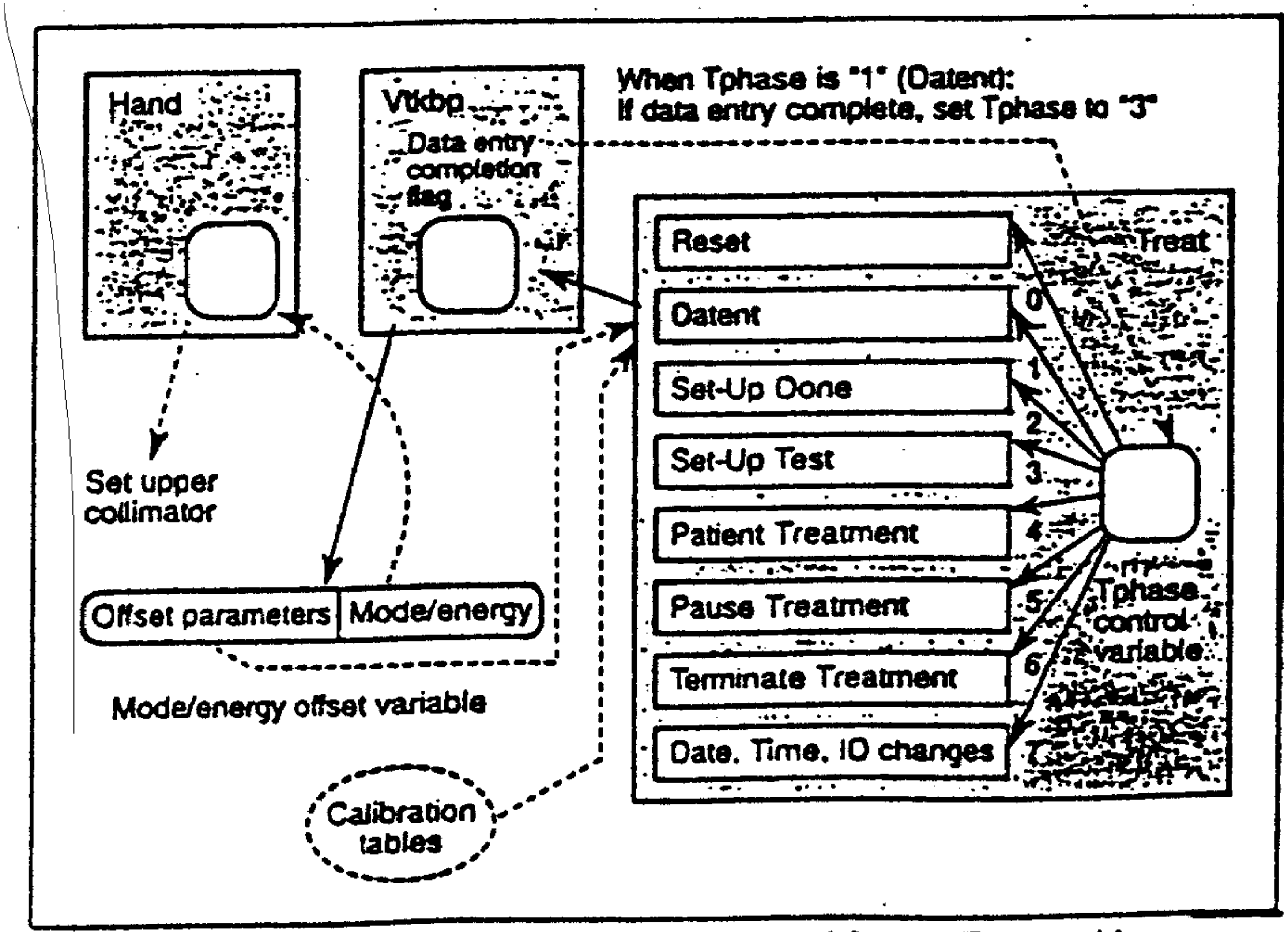
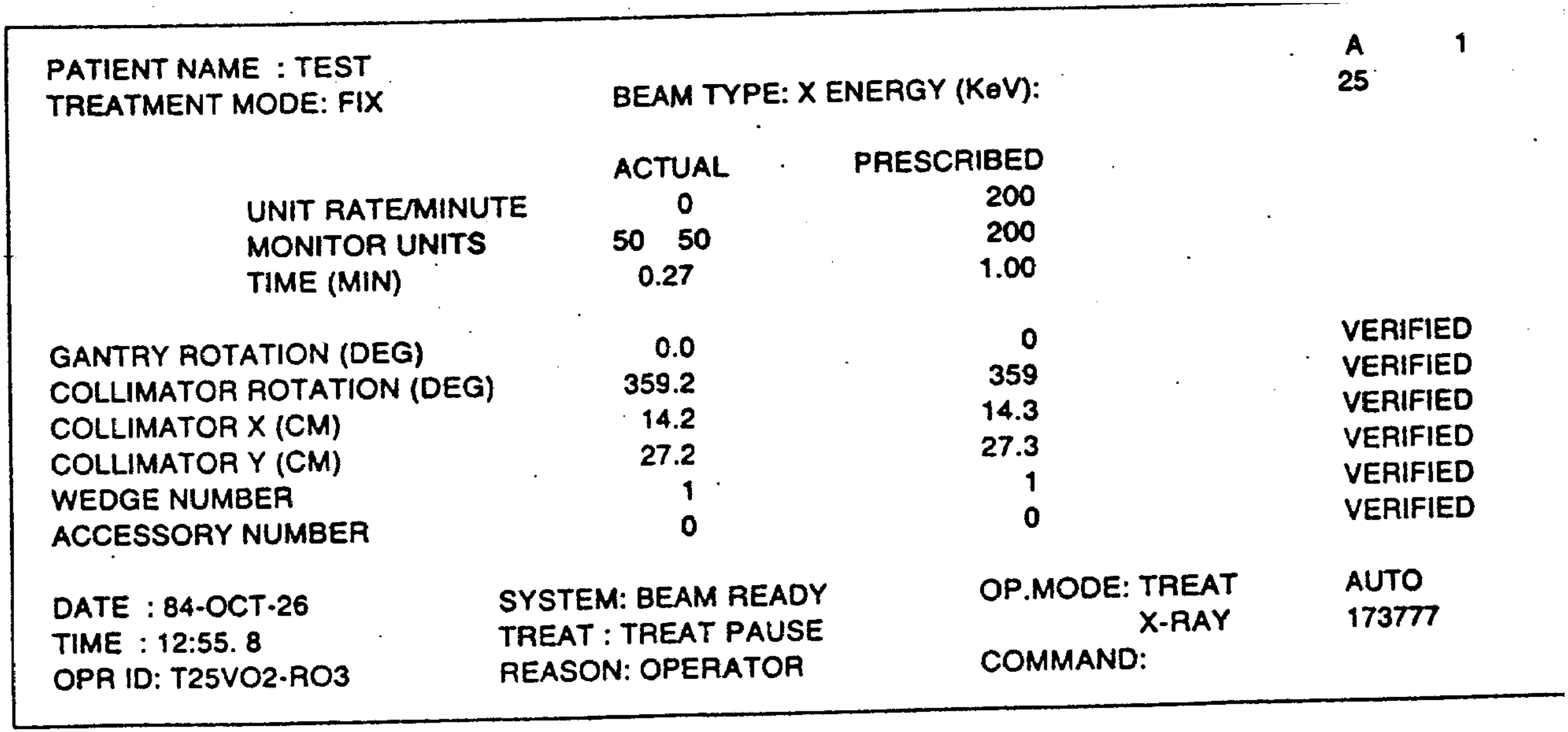


Figure 2. Tasks and subroutines in the code blamed for the Tyler accidents.

Operator Screen Layout



```
                                                                                    A       1
PATIENT NAME  : TEST                                                                25
TREATMENT MODE: FIX               BEAM TYPE: X ENERGY (KeV):

                                  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: T25VO2-RO3         REASON: OPERATOR         COMMAND:
```

Figure A. Operator interface screen layout.

Yakima Accident Race Condition

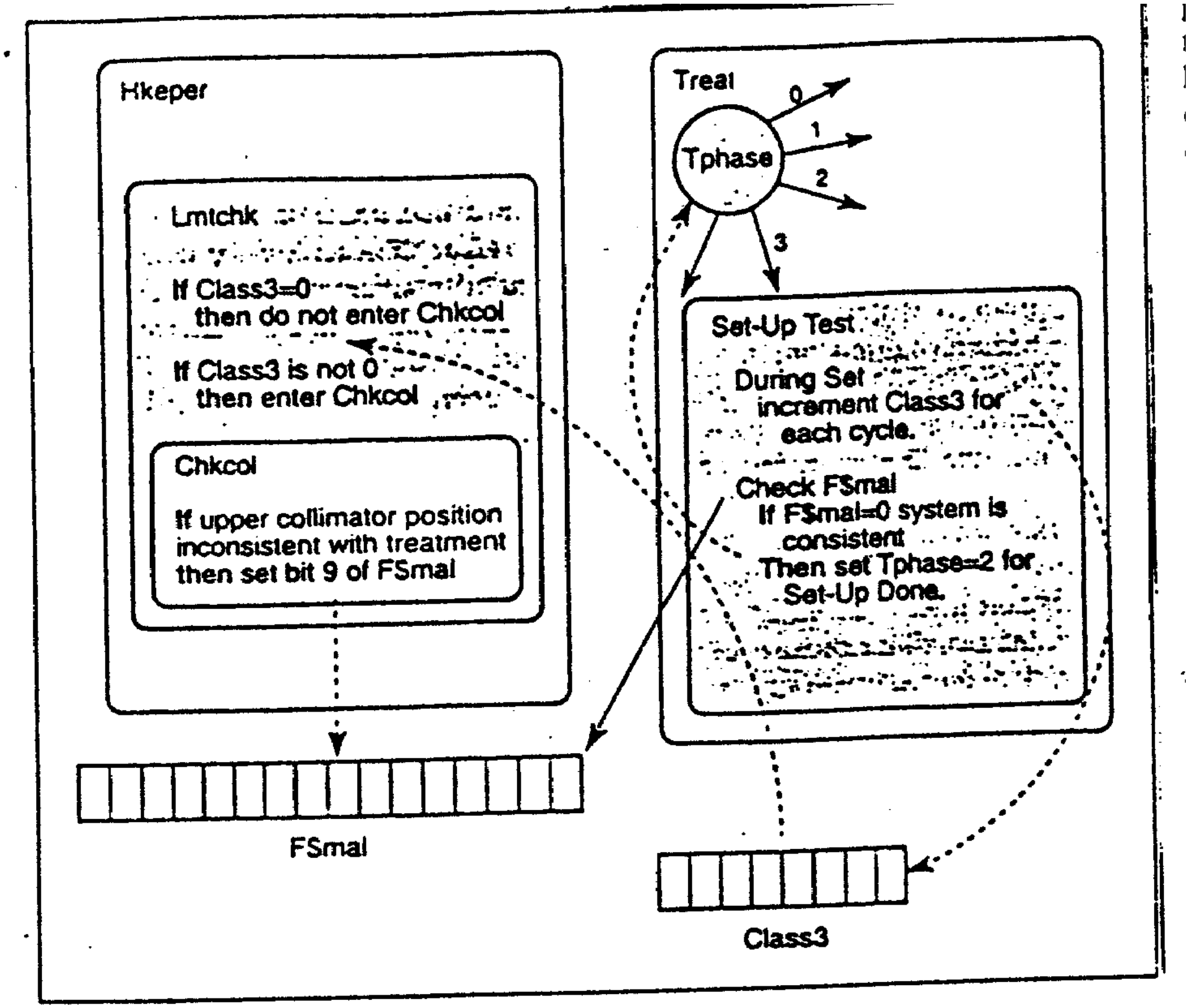


Figure 4. Yakima software flaw.

Therac 25 Turntable

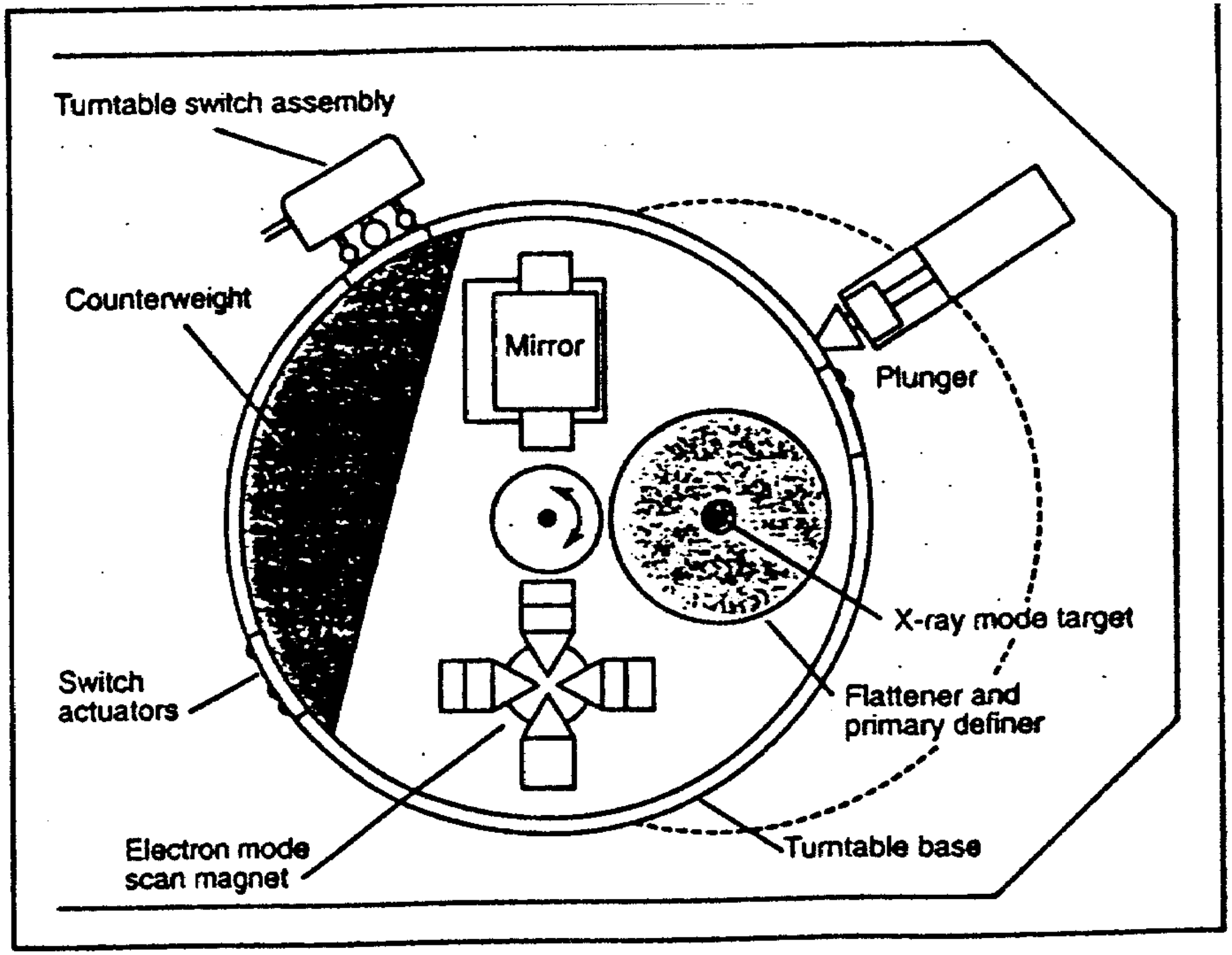

Turntable switch assembly
Counterweight
Mirror
Plunger
X-ray mode target
Flattener and primary definer
Switch actuators
Electron mode scan magnet
Turntable base

Figure B. Upper turntable assembly.

Corrective Action Plan

- Numerous hardware and software changes
- All interruptions related to dosimetry not continuable
- independent hardware & software shutdowns
- potentiometer on turntable
- hardware interlocks
- “dead man switch” motion enable
- Fix documentation, messages, & user manuals
- etc

Lessons (Leveson & Turner)

- Complacency
- Assumption that problem was understood without adequate evidence (“the last bug” fallacy).
- Sole reliance on software for safety
- Systems engineering practices

Lessons (Leveson & Turner)

- Documentation key from beginning
- Use established software engineering practices
- Keep designs simple
- Build in software error logging & audit trails
- Extensive software testing and formal analysis at all levels
- Revalidate reused software
- Don’t rely only on software for safety
- Do incorporate redundancy
- Pay careful attention to human factors
- Involve users at all phases