Design Studio 7: Software Safety, The Therac-25 Software Accidents

Based on Nancy Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, 1995.

For CS314, Colorado State Univ.
2016

DS6-1

Context

- Linear accelerators can create high-energy beams of electrons or higher energy x-rays to destroy tumors.
- "Between June 1985 and January 1987, a computer-controlled radiation therapy machine, called the Therac-25, massively overdosed six people. These accidents have been described as the worst in the 35 year history of medical accelerators." [Leveson 1995]
- No official investigation was conducted: Leveson account and analysis was gleaned (and reverse engineered) from various sources.

DS5-2

Therac-25 Turntable

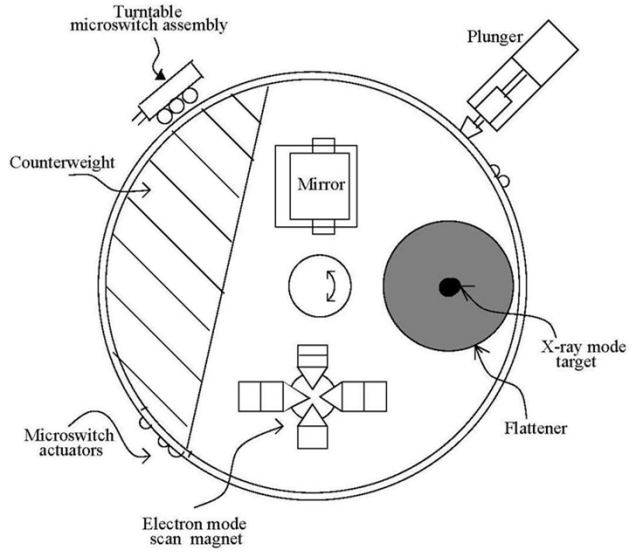


Figure 1: Upper turntable assembly.

DS5-3

Hazard

"If the machine should produce a photon beam with the beam flattener not in position, a high output dose to the patient results. This is the basic hazard of dual-mode machines: If the turntable is in the wrong position, the beam flattener will not be in place." [Leveson, p. 5]

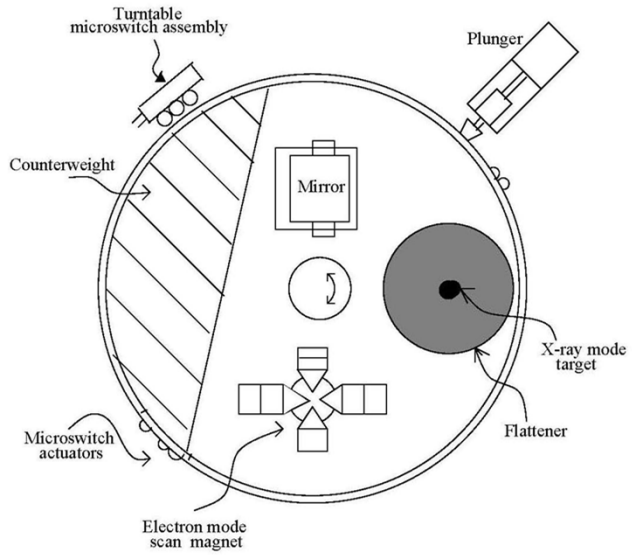


Figure 1: Upper turntable assembly.

DS5-4

"The Therac-25 computer positions the turntable so that a target flattening filter, and xray-ion chamber are in the beam path… No accelerator beam is expected in the field light (mirror) position." [Leveson, p. 5]

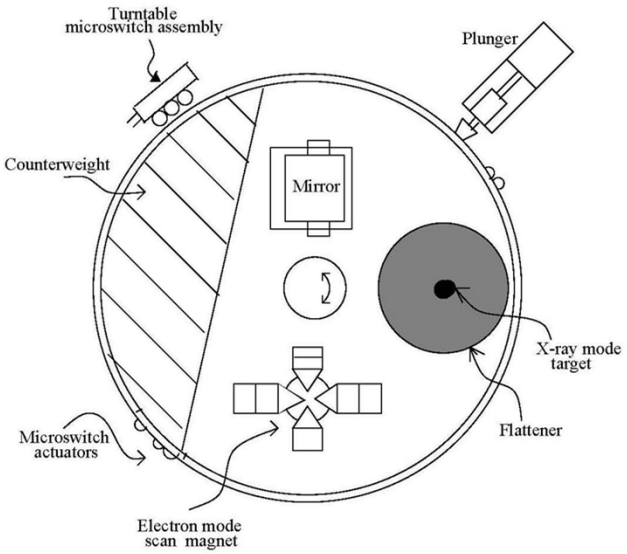


Figure 1: Upper turntable assembly.

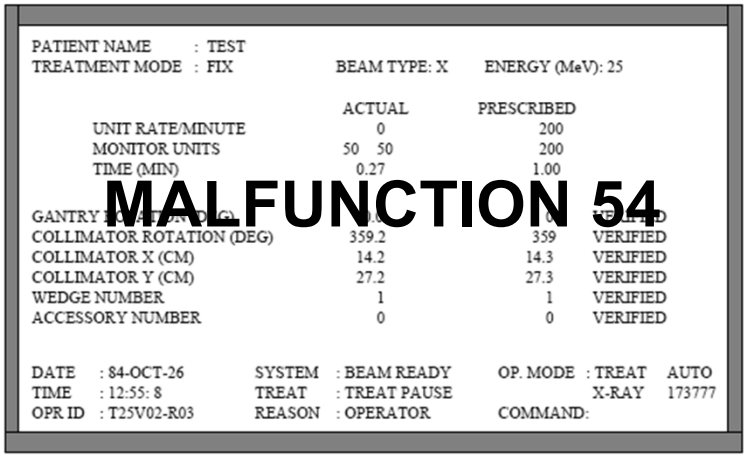
DS5-5

Operator interface screen layout (Fig. 2)

```
PATIENT NAME      : TEST
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:
```

DS5-4

Operator interface screen layout (Fig. 2)



DS5-4

Therac-25 Software

- Written in PDP-11 assembly language.
- Tasks controlled by interrupts:
  - Treatment monitor (Treat) task, with 8 phases.
  - Keyboard processing task.
- How do these tasks communicate?

DS5-8