

How to Write Better Programs

Rafael Castro

27/10/2023

Bugs are annoying

Windows

An error has occurred. We don't even know what it is. So can't fix it ,
and you have to restart your computer. By the way if you restart your ,
computer you will lose any unsaved information in all open applications.
In the other hand you don't have any other option :)

Press Enter to return to Windows (It won't work), or

Press CTRL+ALT+DEL to restart your computer.

Error : 0E : 016F : BFF9B3D4

Uni.Q Design

• why they happen?

Therac-25: The killing radiation therapy machine



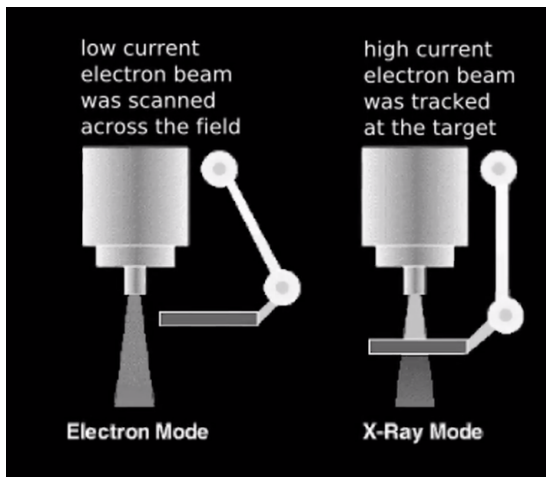
Malfunction messages

- Malfunction messages from 1 to 64, with no extra information

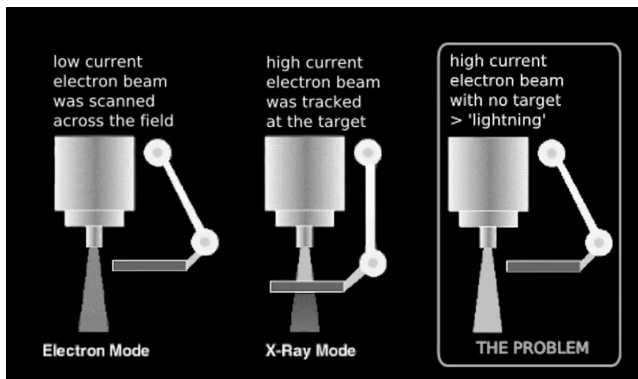


The machine a bug

- The machine had three modes: field light, direct electron beam, x-ray



The machine a bug



How to cause the bug

```
PATIENT NAME: John
TREATMENT MODE: FIX      BEAM TYPE: E      ENERGY (KeV):      10

                        ACTUAL      PRESCRIBED
UNIT RATE/MINUTE      0.000000      0.000000
MONITOR UNITS          200.000000      200.000000
TIME (MIN)             0.270000      0.270000

GANTRY ROTATION (DEG)      0.000000      0.000000      VERIFIED
COLLIMATOR ROTATION (DEG)  359.200000      359.200000      VERIFIED
COLLIMATOR X (CM)         14.200000      14.200000      VERIFIED
COLLIMATOR Y (CM)         27.200000      27.200000      VERIFIED
WEDGE NUMBER              1.000000      1.000000      VERIFIED
ACCESSORY NUMBER          0.000000      0.000000      VERIFIED

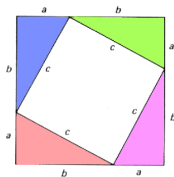
DATE: 2012-04-16      SYSTEM: BEAM READY      OP.MODE: TREAT      AUTO
TIME: 11:48:58        TREAT: TREAT PAUSE      X-RAY          173777
OPR ID: 033-tfs3p     REASON: OPERATOR      COMMAND: █
```


How to write software that don't cause catastrophic failures?

- Formal Methods!
- There are many techniques: type systems, model checking and formal proving

What is to prove something?

- Establishing mathematical facts that are universally true
- You know some: Pythagoras theorem: $\forall abc. c^2 = a^2 + b^2$



Two ways to calculate this area:

① $(a + b)(a + b) = a^2 + ab + ab + b^2$

② $4(ab)/2 + c^2$

they should be the same!

$$a^2 + ab + ab + b^2 = 4(ab)/2 + c^2$$

$$a^2 + b^2 = c^2$$

- How can you be sure that there is no mistake in the proof?

- Programs that verify if your proof is correct!
- We trust the verifier!
- I use a proof assistant called Isabelle/HOL to verify programs
- How my research works:
 - ① I write a specification of the program: what it should do, and what it should **not** do
 - ② I write the program
 - ③ I write a proof that the program respects the specification