How to Write Better Programs

Rafael Castro

27/10/2023

Bugs are annoying

- why they happen?

Therac-25: The killing radiation therapy machine

People got hurt

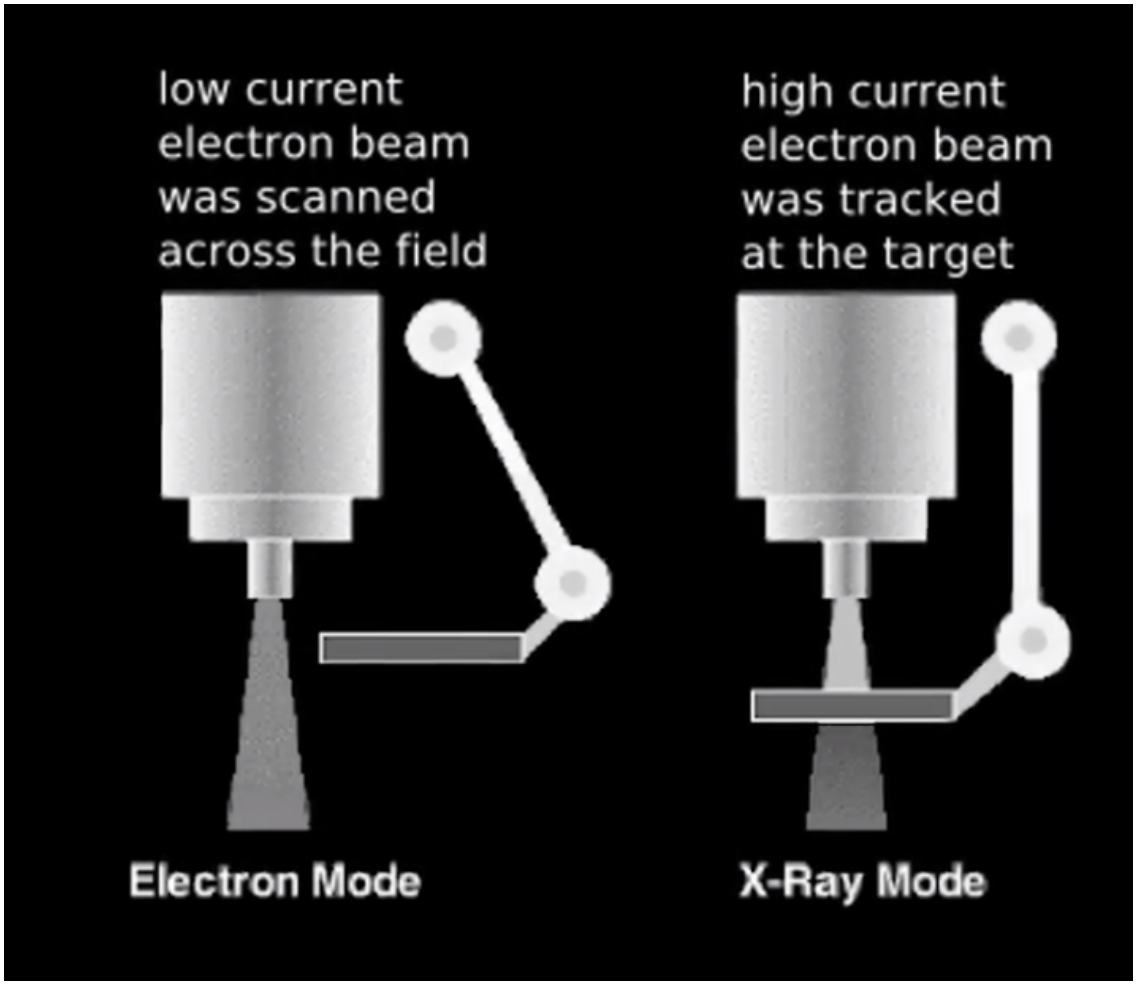
- At least 6 accidents between 1985 and 1987, 3 died later

Malfunction messages

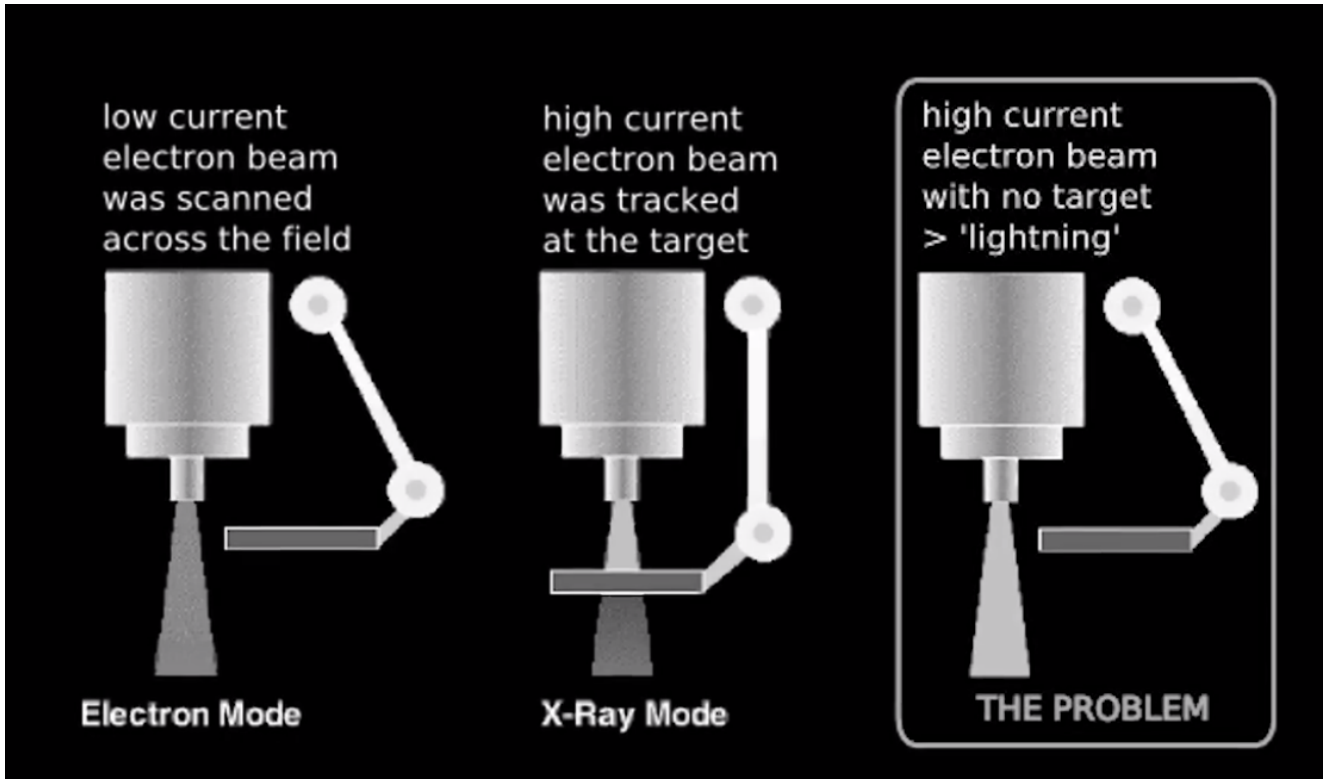
- Malfunction messages from 1 to 64, with no extra information

The machine a bug

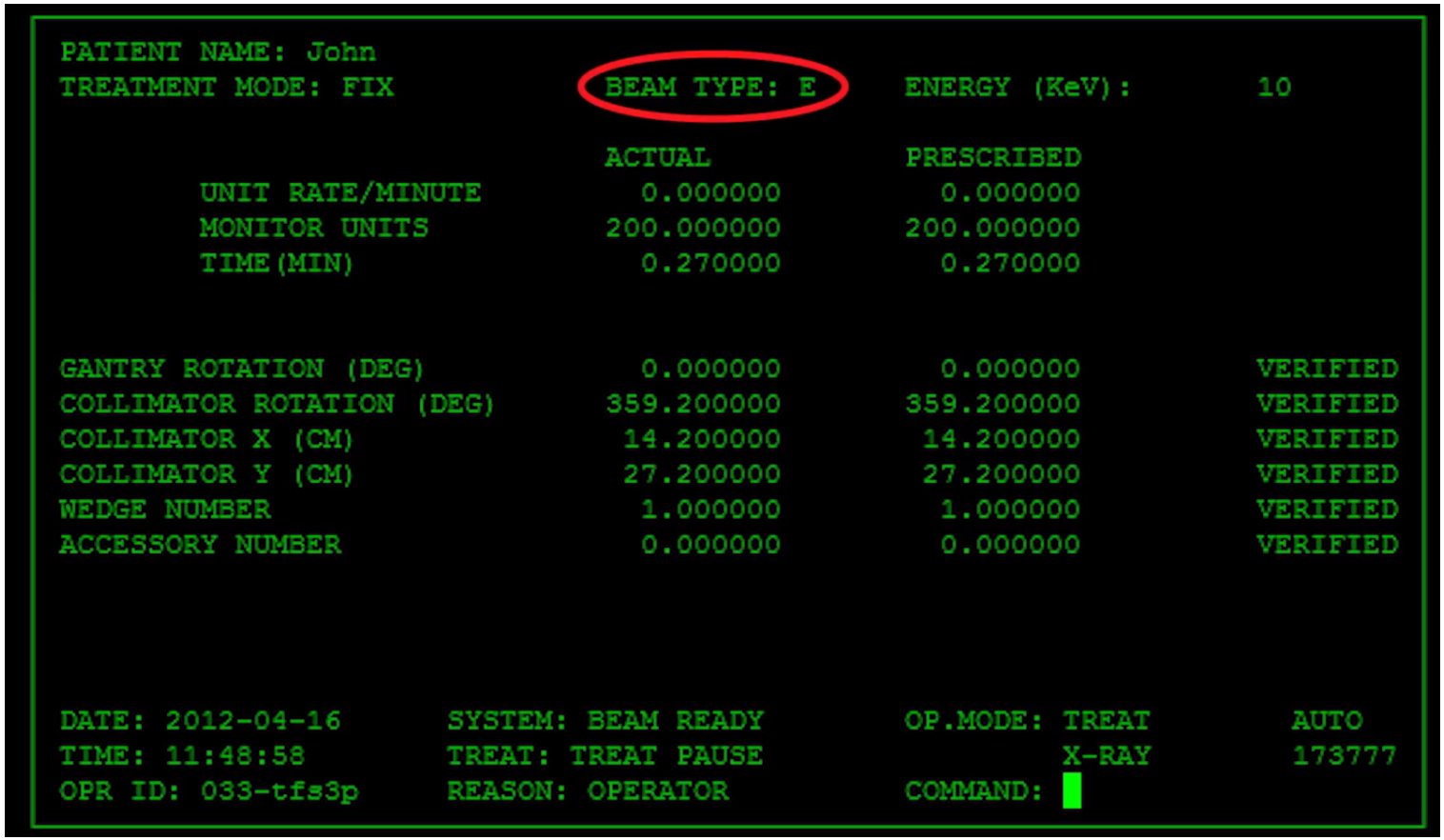
- The machine had three modes: field light, direct electron beam, x-ray



The machine a bug



How to cause the bug

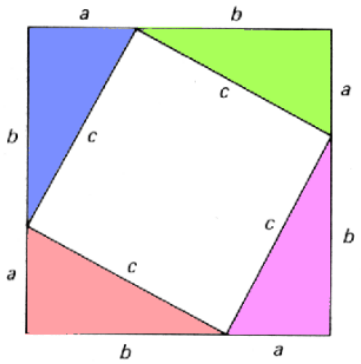


How to write software that don't cause catastrophic failures?

- 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: Pythoragoras 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?

Proof assistants

- 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