

The Importance of Safety

CS439: Principles of Computer Systems

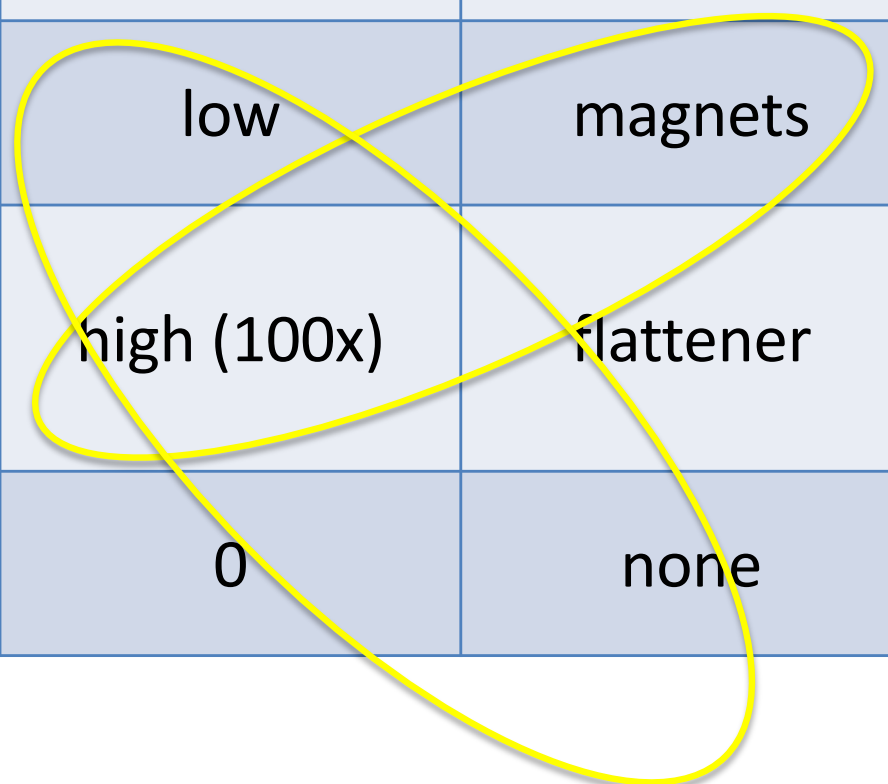
Therac-25

What is the Therac-25?

- Linear accelerator
- Used to treat patients ...

Modes of Operation

	Beam Energy	Beam Current	Beam Modifier
For electron therapy	5-25 MeV	low	magnets
For X-ray therapy, photo mode	25 MeV	high (100x)	flattener
For field light mode	0	0	none



What Went Wrong?

- Two (major) software problems
- Tons of bad software design/human failures that might have prevented this:
 - False alarms
 - Errors reported by number only *and there was no documentation!*
 - No clearinghouse for mistakes *and company hid failures from other users*
 - No end-to-end consistency checks
 - No quality control
 - Don't trust software---hardware should have prevented this, too

What about more recent disasters?

- We don't know for sure
- Possibly software lost treatment plan and defaulted to “all leaves open”
- Software should have sensible defaults!

Lessons

- Complex systems fail for complex reasons
- Be tolerant of inputs
- Be strict on outputs
- Assume buggy software and protect against it!



Doug Collins
@DougCollinsUX



Never count on users to follow instructions. [#ux](#) [#design](#)

