Introduction

CSSE 373 – Formal Methods

Curt Clifton

Introductions

- Name
- Hometown
- Favorite flavor of ice cream and **why**

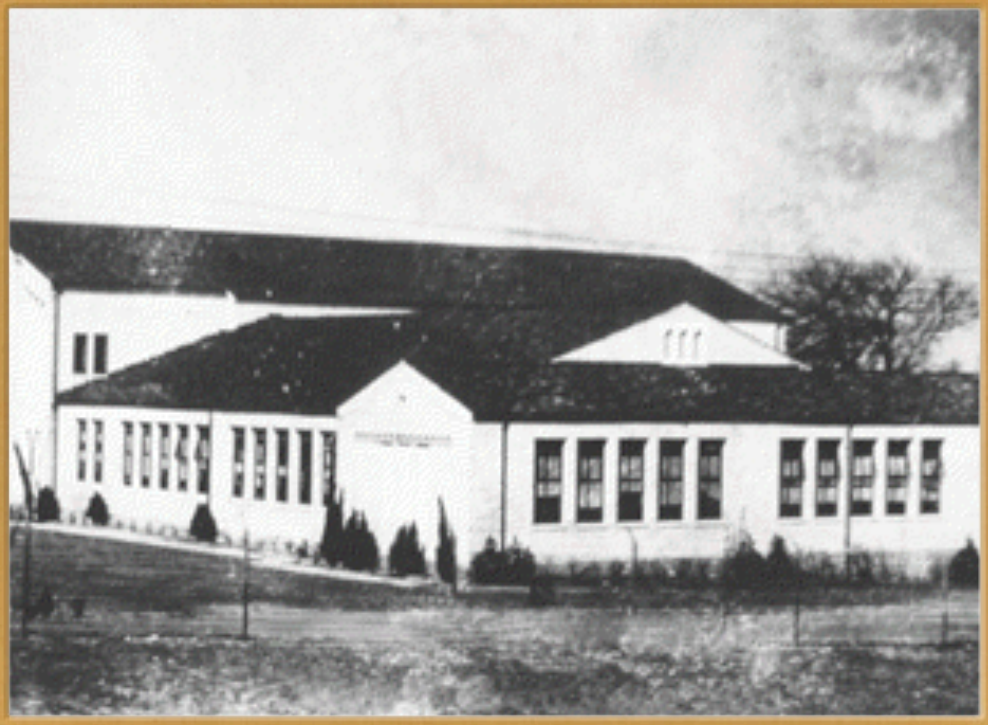
Administrivia

- Course Angel page
- Syllabus
- Schedule, due dates

Homework Submission

- Check out your individual SVN repo:
  - http://svn.csse.rose-hulman.edu/repos/csse373-200930-username
- Add your solution as a **PDF file** to the appropriate subdirectory (e.g., HW1)
- Don't forget to add and commit!

New London School



Before

Heating System

- Original plan:
  central boilers and steam radiators
- Money saving change
  - 72 separate natural gas heaters
  - Had plumber install tap into residue line
  - “Free” heat

Jeremy Hardies—Stone/Getty Images

"Flaring Off"

March 18, 1937

- Around 600 students, 40 teachers in building

The Explosion

- Walls bulged out
- Roof lifted into the air then crashed down
- 2 ton concrete block thrown clear, crushing a car
- Between 296 and 319 killed
- Only 130 escaped without serious injury

After

Aftermath

- US Bureau of Mines experts investigated
  - Determined faulty residue tap was cause
- Texas legislature met in emergency session
  - Concerned that public couldn't tell who was qualified to do engineering work
  - Enacted the "Engineering Registration Act"
  - Only professionally certified engineers may use the title "engineer"

What About Software?

- June 16 -17, 1998
- Texas Board of Professional Engineers ...
  - adopted Software Engineering as a discipline

Consider

- Should society require professional licensure for software engineers?
- Why or why not?

Therac-25

Therac-25

- Radiation therapy device
- Used for cancer treatment
- Two treatment modes
  - Electron-beam burst
  - Longer-exposure X-rays via "target" placed in electron-beam path

First Incident

- Large radiation overdose
  - 100–200 times the prescribed amount
- Hospital denied wrongdoing
- Patient required double mastectomy and lost all use of right arm
- No causal investigation performed

Second Incident

- Machine stopped 5 seconds into treatment with an unidentified error
- User interface reported "No Dose"
- Technician hit 'P' to proceed with the dose
- Repeated this 5 times, delivering a potentially fatal dose each time
- Patient died of original cancer, had she lived would have needed full hip replacement
- Manufacturer suspected a faulty switch, added error correction

Third Incident

- Patient received radiation burns
- Later recovered fully
- Accident not investigated thoroughly

Fourth Incident

- Patient face down on table for back treatment
- Technician very experienced – fast typist
- On confirmation screen noticed she had entered ‘x’ for x-ray rather than ‘e’ for electron beam – arrowed up and changed it
- Machine showed error code and incomplete dose
- Proceeded, with same error
- Patient died of radiation poisoning

Fifth incident

- Same hospital, audio equipment now working
- Same fast typist, same scenario
- Single dosage to face

Within a few seconds the machine shut down, making a loud noise audible via the (now working) intercom. The display showed MALFUNCTION 54 again. The operator rushed into the treatment room, hearing her patient moaning for help. He began to remove the tape that had held his head in position and said something was wrong. She asked him what he felt, and he replied, "fire" on the side of his face. She immediately went to the hospital physicist and told him that another patient appeared to have been burned. Asked by the physicist to described what had happened, the patient explained that something had hit him on the side of the face, he saw a flash of light, and he heard a sizzling sound reminiscent of frying eggs. He was very agitated and asked, "What happened to me, what happened to me?"

Sixth Incident

- Another error message during treatment
- Technician proceeded
- Another overdose
- Patient died 3 months later

Finally They Realized the Seriousness

- All machines taken out of service
- 13 different corrective actions taken
- No incidents reported since

Causal Factors

- Overconfidence in software
- Confusing reliability with safety
- Lack of defensive design
- Failure to eliminate root causes
- Complacency
- Unrealistic risk assessments
- Inadequate followup
- Inadequate software engineering practices
- Software Reuse
- Safe vs. friendly UI