

INTRODUCTION

CSSE 373 – FORMAL METHODS

CURT CLIFTON

INTRODUCTIONS

- **NAME**
- **HOMETOWN**
- **FAVORITE FLAVOR OF ICE CREAM AND WHY**

ADMINISTRIVIA

- **COURSE ANGEL PAGE**

- **COURSE WEB PAGE**

<http://www.rose-hulman.edu/class/csse/csse373/current/>

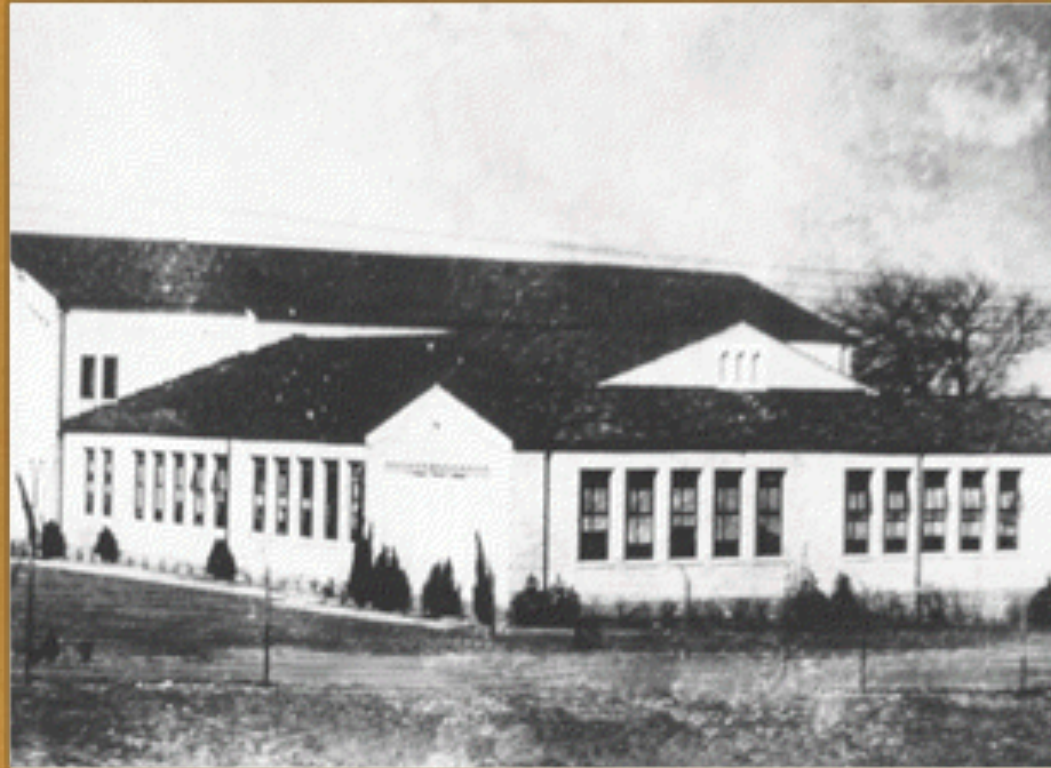
- **SYLLABUS**

- **SCHEDULE, DUE DATES**

HOMWORK SUBMISSION

- CHECK OUT YOUR INDIVIDUAL SVN REPO:
 - <http://svn.csse.rose-hulman.edu/repos/csse373-201030-USERNAME>
- ADD YOUR SOLUTION AS A **PDF FILE** TO THE APPROPRIATE SUBDIRECTORY (E.G., HWO1)
- 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?

THE RAC-25

THE RAC-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 describe 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
- UNREALISTIC RISK ASSESSMENTS
- CONFUSING RELIABILITY WITH SAFETY
- INADEQUATE FOLLOWUP
- LACK OF DEFENSIVE DESIGN
- INADEQUATE SOFTWARE ENGINEERING PRACTICES
- FAILURE TO ELIMINATE ROOT CAUSES
- SOFTWARE REUSE
- COMPLACENCY
- SAFE VS. FRIENDLY UI

OLD NEWS?

The New York Times

February 24, 2010

Radiation Errors Reported in Missouri

By [WALT BOGDANICH](#) and [REBECCA R. RUIZ](#)

A hospital in Missouri said Wednesday that it had overdosed patients, the vast majority with brain cancer, during a procedure because powerful new radiation equipment had been used, even with a representative of the manufacturer watching the procedure.

The hospital, CoxHealth in Springfield, said half of all patients undergoing a particular type of treatment — stereotactic radiosurgery — were overdosed by about 50 percent after a medical physicist at the hospital miscalibrated the new equipment. Routine checks over the next five years failed to catch the error.

The revelation comes at a time of growing concern about safety procedures for a new generation of powerful, computerized medical radiation equipment.

February 27, 2010

At Hearing on Radiation, Calls for Better Oversight

By [WALT BOGDANICH](#)

WASHINGTON — A dozen witnesses, including representatives of virtually all of the leading professional groups in medical radiation, told a House subcommittee during a hearing Friday that more needed to be done to make sure that radiation continues to help, not harm, patients.

The call for a more standardized, comprehensive method of overseeing medical radiation, both diagnostic and therapeutic, came from radiation oncologists, radiologists, therapists, researchers, medical physicists and equipment manufacturers.

Saying that recent news reports about radiation accidents had “raised huge concerns for me,” [Frank Pallone Jr.](#), the New Jersey Democrat who is the chairman of the Energy and Commerce subcommittee on health care, said he was shocked that the people who operate radiologic devices need not be licensed in many states and that “the requirements to report errors and the penalties for making errors are basically nonexistent or not enforced.”

OLD NEWS?

The New York Times



Toyota has insisted on several occasions to customers as well as to Congress that it has rigorously tested and found no flaws in the electronic throttle control systems, which substitute for a mechanical link between the accelerator pedal and the engine in Toyotas and many other vehicles.

Toyota hired a consulting firm to study whether electronic problems could cause unintended acceleration. The firm, Exponent Inc., released an interim report that has found no link between the two. But committee investigators have said the Exponent test was flawed because it studied only a small number of Toyota vehicles.

[HTTP://UNCONFIRMEDSOURCES.COM/?ITEMID=4272](http://unconfirmedsources.com/?itemid=4272)

This month, Toyota released a study of vehicles it had commissioned from Exponent, a research company, that said electronics were not to blame.

But in the letter to Mr. Lentz, Mr. Waxman and Mr. Stupak said Toyota had dismissed the idea and had not investigated it properly. Further, it said the six vehicles involved in Exponent's study, none of which were shown to have problems with their electronic systems, made up too small a sample from which to draw a conclusion.