Software Engineering Disasters

EECS 2031

AT&T Lines Go Dead (1990)

- **Cost**: <u>75 million phone calls missed</u>, 200 thousand airline reservations lost

- **Disaster**: A single switch at one of AT&T's 114 switching centers suffered a minor mechanical problem and shut down the center. When the center came back up, it sent a message to other switching centers, which in turn caused them to shut down and <u>brought down the entire AT&T network for 9 hours</u>.

- **Cause**: <u>A single line of buggy code in a complex software upgrade</u> implemented to speed up calling caused a ripple effect that shut down the network.

Mariner Rocket Was Destroyed

- **Cost**: $18.5 million (1962)
- **Disaster**: The Mariner 1 rocket with a space probe headed for Venus diverted from its intended flight path shortly after launch. Mission Control <u>destroyed the rocket 293 seconds after liftoff</u>.
- **Cause**: A programmer incorrectly transcribed a handwritten formula into computer code, <u>missing a single superscript bar</u>. Without the smoothing function indicated by the bar, the software treated normal variations of velocity as if they were serious, causing faulty corrections that sent the rocket off course.

Hartford Coliseum Collapse (1978)

- **Cost**: $70 million, plus another $20 million damage to the local economy
- **Disaster**: Just hours after thousands of fans had left the Hartford Coliseum, the steel-latticed <u>roof collapsed under the weight of wet snow</u>.
- **Cause**: The programmer of the CAD software used to design the coliseum <u>incorrectly assumed the steel roof supports would only face pure compression</u>. But when one of the supports unexpectedly buckled from the snow, it set off a chain reaction that brought down the other roof sections like dominoes.

World War III... Almost (1983)

- **Cost**: Nearly all of humanity
- **Disaster**: The Soviet early warning system <u>falsely indicated the U.S. had launched five ballistic missiles</u>. Fortunately the Soviet duty officer had a "funny feeling in my gut" and reasoned if the U.S. was really attacking they would launch more than five missiles, so he reported the apparent attack as a false alarm.
- **Cause**: <u>A bug in the Soviet software failed to filter out false missile detections</u> caused by sunlight reflecting off cloud-tops.

Patriot Fails Soldiers (1991)

- **Cost**: <u>28 soldiers dead</u>, 100 injured
- **Disaster**: During the first Gulf War, an American Patriot Missile system in Saudi Arabia <u>failed to intercept an incoming Iraqi Scud missile</u>. The missile destroyed an American Army barrack.

- **Cause**: <u>A software rounding error incorrectly calculated the time</u>, causing the Patriot system to ignore the incoming Scud missile.

Medical Machine Kills (1985)

- **Cost**: <u>Three people dead</u>, three people critically injured

- **Disaster**: Canada's Therac-25 radiation therapy machine <u>malfunctioned and delivered lethal radiation doses</u> to patients.

- **Cause**: Because of <u>a subtle bug called a race condition</u>, a technician could accidentally configure Therac-25 so the electron beam would fire in high-power mode without the proper patient shielding.

Cancer Treatment to Die For (2000)

- **Cost**: <u>Eight people dead</u>, 20 critically injured (Panama)
- **Disaster**: Radiation therapy software by Multidata Systems International <u>miscalculated the proper dosage</u>, exposing patients to harmful and in some cases <u>fatal levels of radiation</u>. The physicians, who were legally required to double-check the software's calculations, <u>were indicted for murder</u>.
- **Cause**: The software calculated radiation dosage based on the order in which data was entered, sometimes <u>delivering a double dose of radiation</u>.