Software Disasters Case Studies

CSCI 3300/5300

Note: This lecture may contain sensitive material, as it discusses system failures that resulted in the loss of human life

Boeing 737 Max Crashes

As part of the upgrade, Boeing will install an extra warning system on all 737 Max aircraft, which was previously an optional safety feature.

Neither of the planes, operated by Lion Air in Indonesia and Ethiopian Airlines, that were involved in the fatal crashes carried the alert systems, which are designed to warn pilots when sensors produce contradictory readings.

GETTY IMAGES

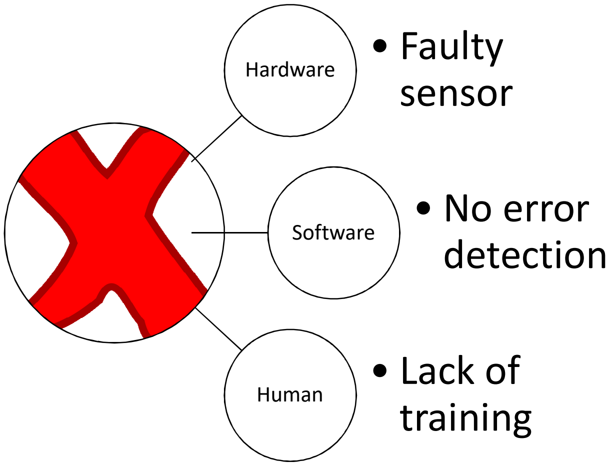
Debris from Ethiopian Airlines flight 302

Boeing has issued changes to controversial control systems linked to two fatal crashes of its 737 Max planes in the past five months.

What we know about 737 Max issues

- October 29, 2018 – Lion Air Jet crash in Indonesia
- Automated flight control system forced the nose of the plane down
  - MCAS – Maneuvering Characteristics Augmentation System
  - System acted on erroneous data from a faulty sensor
  - Pilots were unable to counteract or disengage the system
- MCAS did not exist on previous versions of 737
- Pilots were not aware of the new feature and were not trained on it
- March 10, 2019 – Ethiopian Airlines crash
  - Investigation report is expected this week

System Failure



Hardware
- Faulty sensor

Software
- No error detection

Human
- Lack of training

Therac-25

- Computer controlled radiation therapy machine
- Electron mode
  - Low energy electrons well suited at killing shallow tissue (skin cancer)
  - **Scanning magnets spread the electron beam**
- High power X-Ray mode
  - Beam of high energy X-Ray photons for treating deeper tissues (lung cancer)
  - Rotated four components into the beam

Therac-25

- 6 accidents where patients were given massive overdoses of radiation
- Prior versions Therac-6 and Therac-20
  - Manual control: operator did all the set-up
  - Hardware interlocks: prevented operator from doing dangerous operations
- New version: Therac-25
  - Many manual controls removed
  - Software control to prevent dangerous operations
  - Hardware interlocks removed

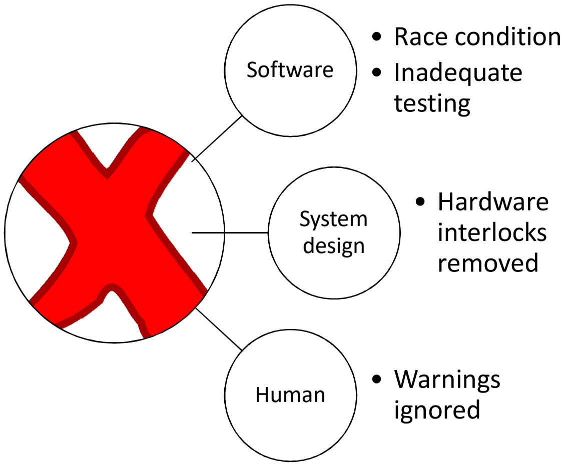
Malfunction 54

- x – for X-Ray mode, e – for Electron mode
- Operator typed 'x' instead of 'e'
- Quickly used up arrow to select the correct mode
- Machine shut down with "Malfunction 54" error message
- Treatment pause errors were frequent and ignored
- Operator continued the treatment

Race condition: When mode of operation was switched in less than 8 seconds from x to e, scanning magnets required for electron mode were not positioned correctly

Hardware interlocks would have prevented machine from operating in such mode

System Failure



- Race condition
- Inadequate testing

- Hardware interlocks removed

- Warnings ignored

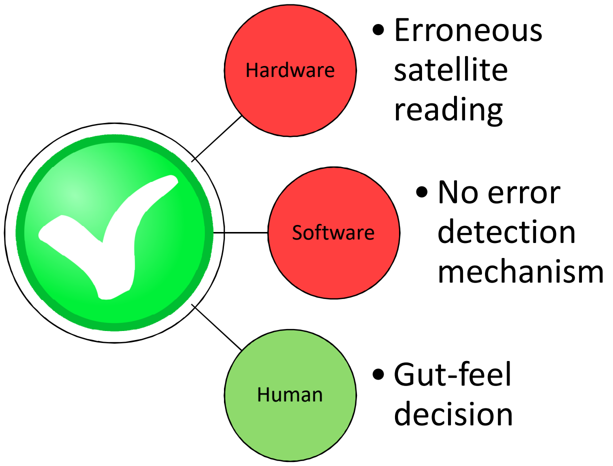
Soviet Nuclear Missile False Alarm

- 1980 – Cold War era
- Nuclear arms race
- Tense relations between Soviet Union and the United States
- Both sides are ready to respond with a counter-attack
- USSR used satellite early warning network to monitor for attacks
- Impending missile attacks must be reported to superiors
- If attack is detected, USSR's strategy was to launch a counter-attack, causing mutual assured destruction
- September 26, 1983 – Lieutenant colonel Stanislav Petrov on duty, observing early warning system

Interview with Stanislav Petrov

Satellite had mistaken the sun's reflection off the tops of the clouds for a missile launch

System Near Failure



Hardware
- Erroneous satellite reading

Software
- No error detection mechanism

Human
- Gut-feel decision

REMEMBER

Turn your computer off before midnight on 12/31/99.

What do Facebook and Y2K have in common?

No Pilots for the Holidays (2017)

- Glitch in scheduling system
- Too many pilots from a certain airline were scheduled to take time off the week of Christmas
- Glitch was caught and flight delays were prevented
  - Pilots were paid time and a half

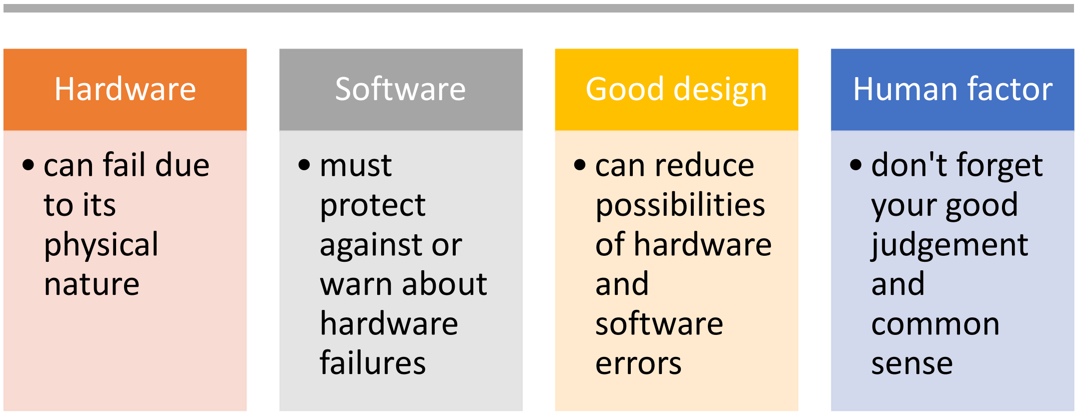
Lucky Christmas (2017)

- Software failure in South Carolina Lottery
- Thousands of winning lottery tickets printed on Christmas day
- Winnings totaling $19.6 Million (if all were validated)
- Lottery was shut down
  - 7 or 8 people won hundreds of dollars each

How to Lose $440 Million in 45 Minutes

- Aug 2, 2012
- Knight Capital Group lost $440 Million in 45 minutes
- Software upgrade is blamed for the loss
- Company rapidly bought and sold millions of shares of over 100 stocks
- Rapid activity on a stock impacts the price
- Company ended up selling shares it bought at an overvalued price back into the market at a lower price

Multiple Layers of Failure



Hardware

- can fail due to its physical nature

Software

- must protect against or warn about hardware failures

Good design

- can reduce possibilities of hardware and software errors

Human factor

- don't forget your good judgement and common sense