Computer Reliability

Lecture 8-1

Computers & Society (CPSC 430)

Kevin Leyton-Brown (Section 101)
Giulia Toti and Melissa Lee (Section 102)
https://www.cs.ubc.ca/~kevinlb/teaching/cs430

Computer Reliability

- Data-Entry and Retrieval errors
  - Voter logs
  - Long gun registry
  - False arrests
  - Credit records

- *What responsibility does the maintainer of a database have for the integrity of the data in it? What rights should the people about whom data is stored have to access it, and to have the data corrected?*
- *There is a trade-off between making a crime database more extensive and more accurate. How should this trade-off be managed?*

Dataset errors – protected words and invalid characters

- In 2016, a security researcher from California named Joseph Tartaro decided to get a vanity license plate. His choice: NULL
- He low-key hoped that would get him out of tickets, since NULL means "undefined" in many databases
- He ended up collecting fines for all people with missing license plates ($12,049 total)
- Christopher Null, a journalist for WIRED, commented: "He had it coming"
- Sources:
  - https://radiolab.org/episodes/null
  - https://www.wired.com/story/null-license-plate-landed-one-hacker-ticket-hell/

Software and Billing Errors

- System Malfunctions
  - Huge bills in the mail
  - Errors in government statistics
  - Mail undelivered
  - Rent system charged people too much
- System Failures
  - 911 system had huge delays
  - Errors in stock exchange platforms
  - Air traffic control systems
  - Emergency room scheduling systems
  - Airline scheduling software crash leads to 1100 canceled flights
  - Boeing 777 autopilot malfunction led to erratic flying
    - More recently, Boeing had issues with their MAX model and MCAS software
    - https://en.wikipedia.org/wiki/Maneuvering_Characteristics_Augmentation_System

Embedded Systems

- Patriot missiles
  - Accumulating floating point truncation errors led them not to fire at incoming missiles
- Ariane 5
  - Floating point to integer conversion error led rocket to explode
- Mars climate orbiter
  - Imperial/metric unit conversion led to crash
- Denver International Airport
  - $311 million automated baggage system never worked, eventually replaced with a $71 million traditional system
- Tokyo stock exchange
  - Accepted an order for selling 610,000 shares at 1 yen, instead of 1 share at 610,000 yen. Then wouldn’t cancel the order.

More Embedded Systems

- Electronic Voting Machines
  - Fails to record various ballots
  - Records way too many votes
  - Records way too few votes
  - Votes recorded correctly but counted wrong (integer overflow)
  - Votes were changed at the confirmation screen
- Therac-25
  - A linear accelerator used to for cancer radiation therapy
  - Occasionally gave patients way too much radiation
  - Traced to various software errors, including two race conditions

- *How much should be done to prevent such problems?*
- *How should we decide that a system is safe?*

Self driving vehicles

- SAE International:
  - SAE Level 0 – No Automation
  - SAE Level 1 – Driver Assistance (adjustments to steering or acceleration/deceleration)
  - SAE Level 2 – Partial Automation: (adjustments to both steering and acceleration/deceleration)
  - SAE Level 3 – Conditional Automation: "the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene"
  - SAE Level 4 – High Automation: automated driving system with occasional requests for intervention from the human driver (not crucial)
  - SAE Level 5 – Full Automation

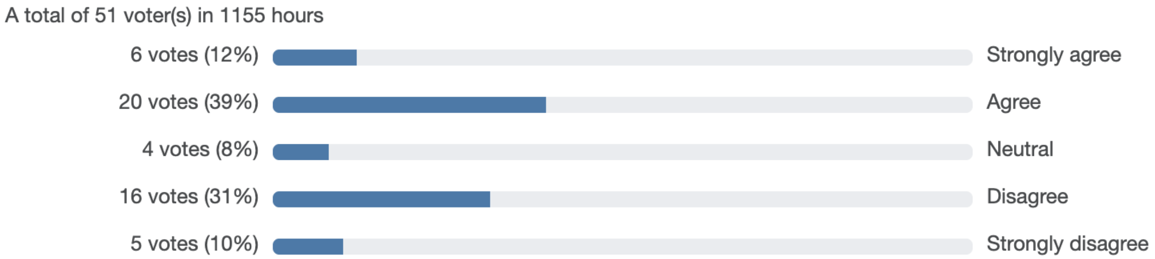
- SAE level 3 creates the "hands off problem"; Ford, Volvo and Google decided to skip this step. Do you agree?

- Do you agree with Quinn's assessment that Tesla Motor is partially responsible for Joshua Brown's death?

Computer Reliability

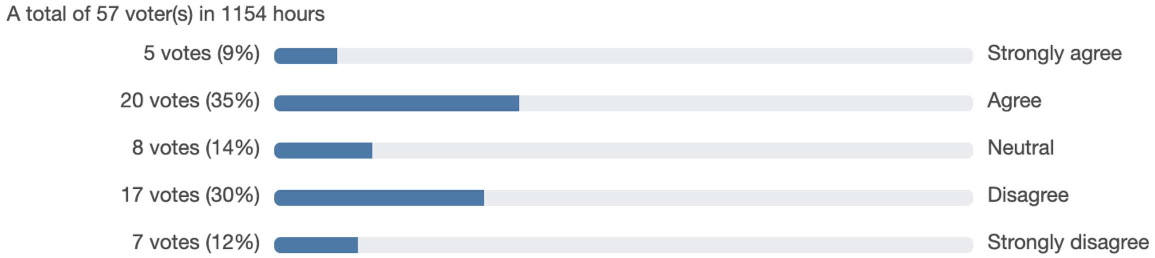
"Self-driving cars should be allowed to operate on public roads once they have been shown to be at least slightly safer than the average human driver."

Section 101



A total of 51 voter(s) in 1155 hours

Section 102



A total of 57 voter(s) in 1154 hours

Computer Simulations

- Simulations are used to answer questions about scenarios that can’t be easily observed in the real world
  - Hurricanes
  - Nuclear explosions
  - Climate change
  - Car crashes
- Models are only useful if they accurately describe reality
- *What would you need to see to trust a simulation?*
- *How accurate does a simulation have to be to be useful?*

Software Warranties

- Software companies tend to write license agreements saying that the software may not perform as promised
  - “we expressly disclaim … the implied warranties of merchantability and fitness for a particular purpose”
- Why is this reasonable?
  - Software is expensive
  - Other expensive goods are backed up by warranties
- *Should software come with warranties? If so, what should these warranties cover?*
- *Do software makers have a moral obligation to produce software that does what it promises?*