

Computer Reliability

Lecture 10-1

Computers & Society (CPSC 430)

Hedayat Zarkoob

<https://www.students.cs.ubc.ca/~cs-430/>

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?*

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.”

