Justin Garrard
Homework 1 Writing Assignment
1/22/2018

Therac Analysis

I recently watched a clip from an interview with Margaret Hamilton, the "first Software Engineer", who developed system control software for the Apollo moon landing missions[1]. One of the most striking parts of the interview was the anecdote about how her daughter discovered a critical flaw in the software design that caused the system to crash if an astronaut were to accidentally initiate the launch sequence after already in flight. In the Therac article, Nancy Leveson puts into words the problem with software safety that evoked a natural uneasiness from the Hamilton story. In the "Confusing Reliability With Safety" section, Leveson describes that for electro-mechanical systems safety can be proven by running the system to exhaustion; however, for software dependent critical systems, reliability isn't a substitute for safety. The problem is inherently different because to test for software safety you essentially need to exhaust every possible user interaction for safety, but in testing you might not imagine some of the ways it could be misused by a user.

For that reason, I found Leveson's assertion that systems should make getting to a safe state very easy while making it hard for a user to move a system into a dangerous state. In developing UAV applications, I would say this translates to building in default safe behaviors when connections to transmitters are lost or when unstable control instructions are sent by the user. This could be a hover or return to launch default.

Why I Took This Course

Throughout my computer science education, I haven't had much of an opportunity to work with hardware or systems. Most of my projects and courses have been focused on software development for a user experience or data analysis goal. Through a number of summer internships I have discovered that these things don't interest me as much as understanding how digital systems work at a lower level. I took this course because I wanted gain experience with embedded systems analysis and development. This would be a success for me if I learn to control the drones using a lower-level programming language and get to study how this actually interacts with the hardware.

[1] https://www.youtube.com/watch?time_continue=12&v=kTn56jJW4zY; "Margaret Hamilton, NASA's First Software Engineer"