6.033 Computer System Engineering
Spring 2009

One-pager #1: Due in Recitation 3

Read *An Investigation of the Therac-25 Accidents* by Leveson and Turner. Also read the following two brief reports that are available only on-line:

- Nuclear Regulatory Commission Information Notice 2001-8
- Multidata response.

Although there are many cases in which software design and failure has led to the loss of life, the case of the Therac-25 is among the best known and most widely cited because of the depth of analysis that was performed by professor Nancy Leveson and her graduate student Clark Turner. The Leveson paper is quite long, and not all parts are equally important. This is a good opportunity for you to begin practicing how to get the interesting stuff out of a paper without getting bogged down in minor detail:

- Start with a quick pass, just reading the section headings and the figure captions, to get an idea of the layout of the paper and what kinds of things the authors seem to be trying to communicate.
- Next, skim it quickly, looking primarily at the first and last paragraph of each section.
- Read disconnected sections (sometimes called *boxes*) or *sidebars* on pp. 20-21, p. 24 and p. 25. These sections contain technical information that both stands on its own and that the authors couldn't figure out how to gracefully integrate into the main text of the article. Often on a long article or book chapter, the sidebars give you background material that makes the main text easier to understand.

Now ask yourself why it was assigned as a 6.033 reading, and with that in mind, start working your way through the meat of the paper. Some sections can be skimmed quickly, while other parts require careful study. Not surprisingly, there is also some redundant information that you can ignore.

As you read the paper, try to distinguish solid technical facts from higher-level statements that the authors are trying to make about process, procedures and policy. You might find it useful to note the places where you agree or disagree with the authors' analysis.

Finally, don't be dismayed by unfamiliar technical jargon; make a guess about what it means and move on. The authors may explain it two paragraphs later, or two pages later, or perhaps never get around to it. There is a good chance that you will discover that it didn't actually matter. But if it does, you have something to ask about in recitation.

After reading the Leveson paper, write a one-page memo:

Alice Abramov is the head of product development in a company that wants to design a new medical linear accelerator, similar to the Therac-25 but hopefully safer. Ms. Abramov is alarmed that the Therac-25 suffered many failures, despite multiple safety analyses purporting to show that failure was astronomically unlikely. In fact, many elements of the Therac-25 design and corresponding safety analyses gave a misleading *appearance* of safety.

Ms. Abramov hires you as a consultant to help her company identify potential areas of flawed analysis.

Your job is first to choose one of the following three aspects of the Therac-25 design:

- Real-time executive and use of concurrency
- Software safety interlocks
- User interface

You are then to write a memo to Ms. Abramov explaining:

1. How that feature and its safety analysis provided the system designers with a false sense of security,
2. In what way(s) the analysis was flawed,
3. How the problems in testing and analysis could have been effectively addressed.

Remember, **use no more than one sheet of paper for your memo.** (Consult the 6.033 FAQ for formatting specifications.) We care more about quality and conciseness than the amount of content in your memo. You will not be able to address every issue in one page, so you will have to make your best argument and judiciously choose supporting facts.

***Two copies* of this assignment are due at the beginning of recitation**. The second copy will be forwarded to the writing program for evaluation.

Grading:

Your submission will be graded by both the 6.033 staff and the Writing Program. The staff grade will focus on your identification of failed analyses, your suggestion of reasonable methods to address these failures, and on how well you articulate your argument. The Writing Program grade will focus on the style and clarity of your memo, according to the following key areas:

1. **Completeness of Ideas.** Has the reader been provided with all the information necessary to understand the failures in analysis and suggestions for improvements?
2. **Sequencing.** Has the information been sequenced in a way that facilitates fast and accurate assimilation and assessment?
3. **Language & Syntax.** Is the memo well proofread and substantially free of surface errors?
4. **Format.** Does the assignment adhere to standard memo format and conventions?
5. **Visual Organization.** Does the use of segmentation, white space, and other visual characteristics facilitate the clear transmission of the information in the memo?