Reading Questions

The following questions are for thought during your reading assignment and for discussion in class. You do *not* have to hand in written answers.

Safer World, Chapter 1:

1. Which of these factors are true for your field or industry? Are any of them not true?

Safer World, Chapter 2:

- Section 2.1: Think of an example (not in the book) of a system that is reliable but not safe, safe but not reliable, conflicting?
- Section 2.2: Did the accident report you chose use a chain-of-events model? What are some causal factors in that accident that do not fit in an accident chain and are indirectly (or non-linearly) related to the events? Were they included in the accident report as a "cause"? Could a different set of events be given to describe the chain of events leading the accident?
- Section 2.3: Chernobyl had a calculated PRA of 10^{-9} per year (or a mean time between "failure" of 10,000 years) so what do you think went wrong in the analysis? Or did it? (There is a description of what happened at Chernobyl in Safeware Appendix D, but you do not have to read it to answer the question).
- Section 2.4: Did you find any instances of hindsight bias in your accident report? What is an example of an environmental factor that can affect human error? Was there an example in your selected accident report?
- Section 2.5: Consider the hardware definition of failure. Does it make sense to talk about a failure of a pure abstraction like software? In what way could it make sense? I what ways is it different?
- Section 2.6: Was there or might there have been a migration toward higher risk in your selected accident report? What do you think are some of the mechanisms underlying this migration?
- Section 2.7: Why do you think it is so hard for people to let go of the concept of blame? Taking an example of human error in your accident report, what is one reason why it might have made sense (at the time) for the person to act the way they did?
- Are there any other assumptions of the traditional approaches to safety that you think are no longer always true or additional goals for a new approach to safety?

Safer World, Chapter 3:

- What is an example of another emergent system property besides safety? Why is it emergent?
- What is a safety constraint that was violated in your selected accident report?
- What is an example of a system with organized simplicity? Unorganized complexity? Organized complexity?
- Have you ever worked on a safety-critical system project? If so, how was safety handled? Did the project have a system engineering

16.863J / ESD.863J System Safety
Spring 2011