



COURSE REVIEW

Course Review: System Safety, by Prof Nancy Leveson

This course is available through MIT's OpenCourseWare:

<http://ocw.mit.edu/OcwWeb/Aeronautics-and-Astronautics/16-358JSystem-SafetySpring2003/CourseHome/index.htm>

The course is based largely on a popular book by Prof. Leveson entitled "**Safeware: System Safety and Computers**" (Addison-Wesley, 1995) and its new version which is available on-line, and covers the analysis and design of safety-critical systems involving computers. Upon accessing the website for the course, the usual information such as syllabus, assignments and projects can be viewed. There are also extensive readings (mostly from the above-mentioned book) and course notes, which can be read on-line or downloaded.

The notes and readings are very useful. The author begins from the premise that the traditional reliability engineering approach to safety planning and design assumes that accidents are the result of quantifiable component failures. However, in the case of computer-operated and computer-controlled systems, accidents may occur without any component "failure", for example equipment operating outside their set parameters or time limits or by interactions of components all operating according to specification. To take the argument further, the standard recommendations such as preventing failure events through redundancy, increasing component reliability and learning from experience will not work in the case of software and computer system failures.

The author therefore propounds a holistic view of System Safety through an iterative process of hazard analysis and control, which is applicable for all safety-critical systems involving computer systems and software. Interesting topics covered include Accident Models, Software Integrity (why software "fails"), and Design for Safety (including software and the human-computer interface). There are numerous practical examples and case studies scattered throughout the course notes and textbook, ranging from Bhopal to aircraft instrument landing system failures.

By Reginald Tan