

## CSMISS IT Seminar Series



# *A Design Environment for Software- Intensive, Autonomous Spacecraft Systems*

*by*

***Dr. Nancy Leveson***  
*Professor of Aerospace  
Software Engineering,  
Aeronautics and  
Astronautics Dept.,  
the Massachusetts Institute  
of Technology (MIT)*

***Monday,  
March 11, 2002  
12:00 – 1:00 P.M.  
180-101***

Most errors in operational software as well as the vast majority of actual accidents and losses related to software stem from the early conceptual and requirements stages of system development. Yet this is also the time when the fewest tools are available to help with system engineering decisions. A lack of common modeling and other communication mechanisms among engineers with varying backgrounds and expertise has been implicated in recent spacecraft accidents. In this talk, I will describe an approach to requirements modeling and system engineering analysis that is focused on software-based control systems and can be used in the design of autonomous systems. While the models have a formal foundation, they can be easily read and reviewed with a few minutes training by engineers and controllers. The specification environment allows traceability and specification of design rationale so that changes can be incorporated more easily as the design and development of the system evolves. The formal foundation allows the models to execute (thus providing early simulation capabilities) and to be formally analyzed for various types of common errors. Our current analysis tools include checking for consistency and completeness, robustness, hazard analysis, and potential for mode confusion and other types of human errors by operators interacting with the system. We are currently working on providing a domain-specific spacecraft design environment (specification and modeling languages) that we believe will not only increase reliability and safety but will allow reuse of engineering knowledge, design and analysis in subsequent missions.

Bio: Dr. Nancy Leveson is Professor of Aerospace Software Engineering in the Aeronautics and Astronautics Dept. at the Massachusetts Institute of Technology. Previously she was Boeing Professor of Computer Science and Engineering at the University of Washington. Dr. Leveson is a consultant to the NASA Aerospace Safety Advisory Panel (ASAP), a Fellow of the ACM, and a member of the National Academy of Engineering. She received the 1995 AIAA Information Systems Award for "developing the field of software safety and for promoting responsible software and system engineering practices where life and property are at stake" and the 1999 ACM Allen Newell Award for research contributions in computer science. She is author of a book, "Safeware: System Safety and Computers," which describes the changes that are necessary to traditional engineering techniques when computers are used to control physical systems.



**CSMISS IT Seminar Series:  
Highlighting information technology,  
methodologies, tools, and best practices  
used in industry and academia.**