Social Dimensions of Reliability of Complex Systems

Chaired by
SEVERO M. ORNSTEIN, *Computer Professionals for Social Responsibility*
Panel:
PETER NEUMANN, *SRI International*
ALAN BORNING, *University of Washington*
GREG NELSON, *Digital Equipment Corporation*
NANCY LEVESON, *University of California, Irvine*

Session Summary

The purpose of this panel is to explore the limits of our ability to build fully reliable systems and the consequences thereof. As we come to depend more and more on sophisticated computer-based systems, certain of society's functions are placed in jeopardy. In general our dependence grows gradually as we adjust our degree of trust based on incremental experience. But, there some tendency to get into trouble by trusting too much too soon. This panel investigates these issues and raises questions about what society might do to deal with them more thoughtfully.

Dr. Peter Neumann of SRI will open the panel by discussing examples of computer failures that demonstrate the prevalance of the problem. These examples illustrate the fact that a root difficulty lies our inability to foresee events and understand seemingly improbable connections. Dr. Neumann will briefly discuss SRI's SIFT project to develop an ultra-reliable aircraft control computer system -- clearly a life-critical system. Dr. Alan Borning of the University of Washington will discuss the U.S. missile attack warning system and describe some computer failures that have occurred in that system. He will then discuss concerns about the role of computer failure in precipitating an unintentional nuclear war, in particular "launch on warning" strategies and the dangers of interacting, escalating alerts. Dr. Nancy Leveson of the University of California Irvine will then try to lend some structure to the problem by defining terms and outlining general approaches to analysis and verification of software safety. Unfortunately enhancing safety often "costs" in terms of money, performance, overall functional reliability, etc. This opens questions about how much society is willing to pay for safety, how best to ensure that tradeoff decisions are made on the side of safety, and where the ultimate decision-making authority concerning safety issues should rest. Finally Dr. Greg Nelson, of Digital Equipment Corporation's System Research Center, will discuss the tools, such as program verification, that are available to us for dealing with these problems. He will describe the current level of their effectiveness, what problems they present in implementation, and will try to predict what we can expect over the next few years.

-- Severo M. Ornstein

Chairman, Computer Professionals for Social Responsibility