

MONDAY
APRIL 2, 2007

Scaife Hall Auditorium
Room 125

3:00 PM
Refreshments—2:30 PM

NOTE SPECIAL TIME AND DAY



JOHN KNIGHT
UNIVERSITY OF VIRGINIA

John Knight is a professor of computer science at the University of Virginia. He holds a B.Sc. (Hons) in Mathematics from the Imperial College of Science and Technology (London) and a Ph.D. in Computer Science from the University of Newcastle upon Tyne. Prior to joining the University of Virginia in 1981, he was with NASA's Langley Research Center.

Dr. Knight's research interests are in software dependability. He is currently working on projects in safety-critical embedded systems and the survivability of critical networked applications. Specific research topics include the use of natural language in specification, tool support for comprehensive specification development and analysis, formal verification, assurance arguments, and network survivability architectures.

From 2001 to 2005 Dr. Knight served as Editor in Chief of the IEEE Transactions on Software Engineering, he is a member of the editorial board of the Empirical Software Engineering Journal, and he is the General Chair of the 2007 International Conference on Software Engineering.

ASSURANCE BASED DEVELOPMENT OF CRITICAL SYSTEMS

Assurance-Based Development (ABD) is the synergistic construction of a critical computing system and its assurance case. The assurance case is an argument that sets out the dependability goal for the system, the evidence needed to support it, and how that evidence is combined to justify the assurance claim. Because the system and its assurance case are developed in parallel, software developers can make technology choices that address the specific dependability goal of each component.

This approach gives developers: (1) confidence that the technologies selected will support the system's dependability goal and (2) flexibility to deploy expensive technology, such as formal verification, only on components whose assurance needs demand it. ABD simplifies the detection—and thereby avoidance—of potential assurance difficulties as they arise, rather than after development is complete.

In this presentation, I will present the details of Assurance Based Development together with a detailed example of its use.