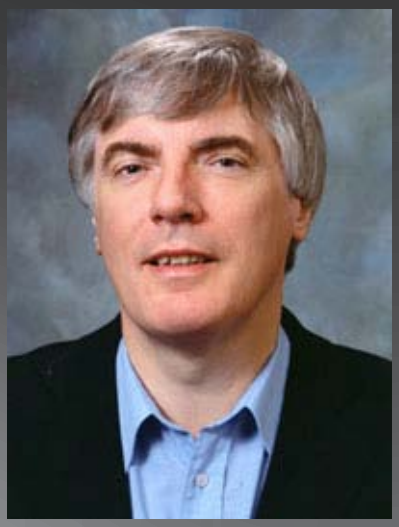
中央研究院 資訊科學研究所
Institute of Information Science, Academia Sinica

Distinguished Lecture Series

# What is Software Assurance?



**Monday, February 14th, 2011 10:00am**
**Auditorium 106 at New IIS Building**


## Dr. John Rushby

**Program Director, Formal Methods and Dependable Systems, Computer Science Laboratory, SRI International**



## Abstract

Safety-critical systems must be supplied with strong assurance that they are, indeed, safe. Top-level safety goals are usually stated quantitatively--for example, "no catastrophic failure in the lifetime of all airplanes of one type"--and these translate into probabilistic requirements for subsystems, and hence for software. In this way, we obtain quantitative reliability requirements for software: for example, the probability of failure in flight-critical software must not exceed $10^{-9}$ per hour.

But the methods by which assurance is developed for critical systems are mostly about correctness (inspections, formal verification, testing etc.) and these do not seem to support quantitative reliability claims. Furthermore, more stringent reliability goals require more extensive correctness-based assurance. How does more assurance of correctness deliver greater reliability?

I will resolve this conundrum by arguing that what assurance actually does is provide evidence for assessing a probability of "possible perfection." Possible perfection does relate to reliability and has other attractive properties that I will describe. In particular, it allows assessment of the reliability of certain fault-tolerant architectures. I will explain how formal verification can allow assessment of a probability of perfection, and will discuss plausible values for this probability and consequences for correctness of verification systems themselves.

This is joint work with Bev Littlewood of City University, London UK.


For more infomation: http://www.iis.sinica.edu.tw/