Speaker: Jan Peleska, University of Bremen and Verified Systems International GmbH, Bremen, jp@verified.de

Title: Industrial verification of avionic, automotive, and railway systems- practical application and theoretical foundations

Abstract:
The verification of safety-critical systems requires considerable effort. For systems of the highest criticality - such as railway interlocking systems, aircraft engine controllers, or anti-lock braking systems in cars - this verification effort is well-known to surpass the development effort, that is, the amount of hours needed to specify, design, and program the software. Since the complexity of safety-critical applications continuously increases, their thorough verification requires automation: otherwise it could never be performed within the tight financial budgets and time frames that are typical for such projects. In this presentation it is highlighted how theoretical foundations in the fields of mathematics and computer science help to solve this problem - sometimes in quite a surprising way: mathematical models originally intended only for increasing the insight into complex system behaviours have been found to be representable in computers and exploitable for automated verification purposes. Starting from practical industrial verification problems, it is highlighted how automated model checking can be applied to verifying highly complex system designs involving concurrency and real-time properties. We show how tests can be automatically generated from mathematical models, so that the whole process of test case identification and test procedure programming can be fully automated, allowing even to prove the correctness of the system under test, under certain hypotheses.

The material presented in this talk is based on projects performed by Verified Systems International, a company providing tools and services for verification and validation of safety-critical systems. The theoretical foundations have been

elaborated at the University of Bremen, in collaboration with many research partners world-wide.