

Verifikation realer Software

Prof. Dr. W. J. Paul
Universität des Saarlandes

Kurzfassung

Im Projekt VERISOFT sollen komplette Computersysteme einschließlich Hardware, Systemsoftware, Kommunikationssystemen und Anwendungsprogrammen durchgängig formal verifiziert werden. Die technische Arbeit hat drei Stoßrichtungen:

- 1) Lücken zwischen bereits existierenden Theorien werden mit mathematisch orientierter Grundlagenarbeit geschlossen.
- 2) Interaktive Beweissysteme werden mit zahlreichen automatischen Werkzeugen gekoppelt.
- 3) In Zusammenarbeit mit Industriepartnern werden verifizierte Demonstratorsysteme erstellt.

In diesem Vortrag berichten wir über die Ergebnisse des ersten Jahrs der Projektarbeit. Wir behandeln ausführlich die Verifikation eines Betriebssystemkerns mit Multitasking und virtuellem Speicher.