KORSO — Korrekte Software durch formale Methoden

M. Broy* S. Jähnichen†

29. November 1996

Zusammenfassung

Von Februar 1990 bis Juni 1994 arbeiteten 15 Partner im BMFT–Verbundprojekt KORSO an der Weiterentwicklung und Umsetzung formaler Software–Entwicklungsmethoden. Dieser Artikel gibt einen Überblick über die Ziele und die wesentlichen Ergebnisse des Projekts.

1 Einleitung

Korrektheit ist eine entscheidende Eigenschaft von Software–Systemen. Technisch gesprochen steht der Begriff der Korrektheit für die Konsistenz eines Software–Systems mit seinen formellen Anforderungen; in einem eher pragmatischen Sinn umfaßt Korrektheit zusätzlich die Adäquatheit der Anforderungen selbst. Formale Methoden erlauben eine rigorose Herangehensweise an das Problem, die Korrektheit eines Systems zu erreichen und nachzuweisen. Da vollständige Konsistenztests für große Software–Systeme nicht praktikabel sind, ist der Einsatz formaler Methoden für sicherheitskritische Anwendungen ein wesentlicher Beitrag zur Erhöhung der Zuverlässigkeit. Erforderlich ist letztendlich ein Einfügen formaler Methoden
in das Vorgehensmodell zur schrittweisen Entwicklung. Schlüsselfunktionen haben Verfeinerungskonzepte und der Beweis der Korrektheit der Verfeinerungsschritte.

Von Februar 1990 bis Juni 1994 arbeiteten 15 Partner im BMFT–Verbundprojekt KORSO [2] an der Weiterentwicklung und Umsetzung formaler Software–Entwicklungsmethoden. Dieses Projekt wurde bewußt an Partner mit unterschiedlichen Wissensprofilen und technischen Ausrichtungen vergeben, um eine Übersicht über die verfügbaren relevanten Methoden und — wichtiger — einen Nachweis ihrer praktischen Durchführbarkeit zu erhalten. Das Projekt arbeitete als eine koordinierte Gruppe individueller Partner mit individuellen Zielen, aber auch mit enger Zusammenarbeit über spezifische gemeinsame Forschungsthemen.

Das Hauptziel des KORSO–Projekts war es, die theoretischen Grundlagen für eine Verbesserung der Software–Qualität zu prüfen und zu verbessern, und bekannte Techniken an praktisch relevanten Anwendungen zu erproben. Es ging nicht um die Erstellung marktfähiger Werkzeuge für die Unterstützung formaler Methoden, was angesichts des damaligen Stands der Kunst als ein eher waghalsiges Unterfangen hätte erscheinen müssen. Vielmehr ist KORSO ein evolutionäres, prototyporientiertes Projekt angelegt worden, das die Grundlagen für einen systematischen und qualitätsorientierten Software–Entwicklungsprozeß der Zukunft legen half. Die evolutionäre Natur des Projekts ergab sich vor allem aus der Einsicht, daß neue Konzepte nur dann erfolgreich eingeführt werden können, wenn gleichzeitig traditionelle bewährte Methoden berücksichtigt und mit den neuen Konzepten integriert werden.

Die Arbeiten des KORSO–Projekts gliedern sich in folgende Schwerpunkte:

- Konzeption eines allgemeinen methodischen Rahmens für die Software–Produktion,
- Definition einer generischen Beschreibungs- und Modellierungssprache,

*TU München
†TU Berlin