College Specification and analysis of Embedded Systems, 2R770, Spring 2002

Jan Friso Groote (J.F.Groote@win.tue.nl, www.win.tue.nl/~jfg, 040-247 5003/5010)

Goal

This course provides a number of techniques to model and analyse interacting, parallel systems, finding their roots in process algebra and logic. These techniques can be used to master the more complex problems of embedded system design: to understand the problem for which an embedded system is to be made and to understand how cooperation of individual systems does actually yield a solution for this problem. This is a field heavily under research at the moment. The course does address the research that is currently going on, while in the meantime students are working on the specification of an embedded system application that must meet certain quality standards.

Course material

There will be handouts during the course, including the following.

- Modelling Concurrent Systems: Protocol Verfication in μCRL. W.J. Fokkink, J.F. Groote and M.A. Reniers. (draft).
- A.G. Wouters. Manual for the μCRL tool set (version 2.8.2). Technical report SEN-R0130, December 2001.
- S.P. Luttik. Description and Formal Specification of the Link Layer of P1394. Technical Report SEN-R9706, CWI, Amsterdam, 1997.

Prerequisites

Process algebra 2M920. Preferably: Automated Reasoning (2R880).

Examination

Students are asked to design a control system for a vacuum chamber that will be part of the next generation wafer stepper at ASML. In cooperation with the teacher students must develop a plan to model and analyse this embedded system. An important aspect in this modelling phase is to select the right level of modelling. If the model is too detailed it might be too complex to gain insight. If the model is too simple, not all adequate aspects of the real system and its requirements can be studied. The result must be properly documented in the form of a technical report, showing that the design meets the quality standards, which have to be set a priori.

The requirements for the design will be formulated by ASML during a visit that will take place on either April 22 or April 26 from 14:00 onwards. An sketch of the design must be handed in before the week starting at May 6, including a full set of requirements that the design must satisfy. At May 20 a full formalized design must be finished. On June 24 a technical report must be handed in, including a full analysis that the design meets its requirements.

Weekly content (indicative)

April 8 Introduction into μCRL. Syntax, axioms and CL-RSP. Data types. Rewrite rules.

April 15 Weak and branching bisimulation. Elementary calculations and specifications.

April 22 Linear Process Operator. Greibach Normal Form. Linearising μCRL. Optimisation techniques for LPOs.

May 6 Toolset of μCRL. State space generation. Visualisation of large data spaces. Optimisations of linear process operators (constelm, parelm, structelm).

May 27 Confluence; EQ-BDDs. Local confluence.

June 3 Modal logic. Specification of properties and analysis of algorithms.

June 10 Cones and Foci theorem. Firewire configuration protocol.

June 17 Reserve and examples: Hef system. Bounded Retransmission Protocol (RC6), P1394. Euris. Safety system of Woerden Harmelen.