Software Modeling and Verification
Lehrstuhl für Informatik 2
RWTH Aachen University

Prof. Dr. Ir. J.-P. Katoen
Priv.-Doz. Dr. T. Noll
T. Han, D. Klink

Modeling Concurrent and Probabilistic Systems

Summer Term 09

– Series 2 –

Hand in until May 13 before the exercise class.

Exercise 1 (3+3 points)

The aim of this exercise is to develop a (simplified) model of a car's central locking system. Assume the following components:

- a *door* which is either open or closed
- a *locker* for the door which can be activated if the door is not open (otherwise an alarm should be issued), and
- a *key* which controls the whole mechanism.

a) Design a corresponding process definition and give its transition system!

b) Check if the car locking system you developed in Exercise 2.1 has a deadlock. If this is the case, provide a deadlock free specification of the system.

Exercise 2 (2+3 points)

An engineer is charged with developing an elevator control for a building with five floors, starting with a CCS model. His subspecification for requesting the elevator and selecting the target floor looks as follows:

$$\mathit{Elevator}(\mathit{req}, \mathit{fl}_1, \ldots, \mathit{fl}_5) = \mathit{req}.\mathit{fl}_1.\mathit{Elevator}(\mathit{req}, \mathit{fl}_1, \ldots, \mathit{fl}_5) + \cdots + \mathit{req}.\mathit{fl}_5.\mathit{Elevator}(\mathit{req}, \mathit{fl}_1, \ldots, \mathit{fl}_5).$$

A computer scientist who was called for supporting the engineer suggests the following solution instead:

$$\mathit{Elevator}(\mathit{req}, \mathit{fl}_1, \ldots, \mathit{fl}_5) = \mathit{req}.(\mathit{fl}_1.\mathit{Elevator}(\mathit{req}, \mathit{fl}_1, \ldots, \mathit{fl}_5) + \cdots + \mathit{fl}_5.\mathit{Elevator}(\mathit{req}, \mathit{fl}_1, \ldots, \mathit{fl}_5)).$$

a) Are both systems trace equivalent?

b) Test the elevator subsystem together with the specification of a user who would like to reach the fourth floor:

$$\mathit{User}(\mathit{req}, \mathit{fl}_4) = \overline{\mathit{req}}.\overline{\mathit{fl}}_4.\mathsf{nil}.$$

Do both specifications of the elevator guarantee that the user is satisfied?