Software Modeling and Verification
Lehrstuhl für Informatik 2
RWTH Aachen University

Prof. Dr. Ir. J.-P. Katoen
Priv.-Doz. Dr. T. Noll
T. Han, M. Neuhäußer

Modeling Concurrent and Probabilistic Systems

Winter Term 07/08

– Series 2 –

Hand in until November 02 before the exercise class.

Exercise 1 (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.

Design a corresponding process definition and give its transition system!

Exercise 2 (1+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:

$$Elevator(req, fl_1, \ldots, fl_5) = req.fl_1.Elevator(req, fl_1, \ldots, fl_5) + \cdots + req.fl_5.Elevator(req, fl_1, \ldots, fl_5).$$

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

$$Elevator(req, fl_1, \ldots, fl_5) = req.(fl_1.Elevator(req, fl_1, \ldots, fl_5) + \cdots + fl_5.Elevator(req, fl_1, \ldots, fl_5)).$$

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:

$$User(req, fl_4) = \overline{req}.\overline{fl}_4.\mathsf{nil}.$$

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