Prof. Dr. P. Liggesmeyer
Dipl.-Inf. Max Steiner

Technical University of Kaiserslautern
Dept. of Computer Sciences
AG Software Engineering: Dependability

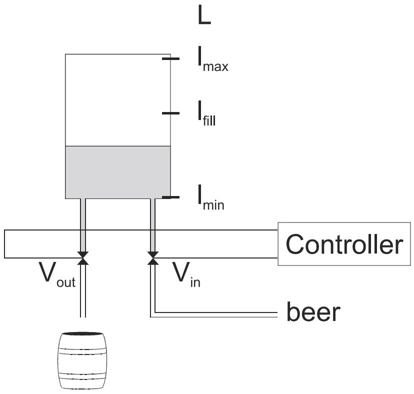
Safety and Reliability of Embedded Systems
(WS 11/12)

Problem Set 7

Due Thursday, February 2nd, 2012

Problem 1: Symbolic model checking

A brewery runs a simple system that measures the amount of beer to be filled into beer-barrels. The equipment contains a tank, an input valve, an output valve, and the controller. In the initial state the tank is empty (l_{min}) and both valves are closed. Then, the input valve is opened and the beer-level in the tank rises. When it reaches the level l_{fill}, the input valve is closed and the output valve is opened in order to fill the barrel. The beer level in the tank now drops until it is empty (l_{min}). Finally, the output valve is closed and the cycle starts again.



The system contains a sensor L that measures the beer-level in the tank. Its values are l_{min}, l_{fill}, and l_{max}. The input valve V_{in} and the output valve V_{out} are actuators. The values are *open* and *closed.*

a) Develop an appropriate finite state machine that defines the behavior of the system described above.

b) It is required that the system fulfills the following safety requirements:

   i. It is prohibited that both valves are open at the same time.
   ii. Level l_{max} does not occur.

   Please specify each of the safety requirements in CTL.

c) Determine the set **E** of reachable states.

d) Represent the set **E** as a Boolean function *e* (OBDD). Please use the following binary coding and the variable order $l_0 \rightarrow l_1 \rightarrow v_i \rightarrow v_o$.

L	l_1	l_0
l_{min}	0	0
l_{fill}	0	1
l_{max}	1	0
-	1	1

V_{out}	v_O
closed	0
open	1

V_{in}	v_i
closed	0
open	1

e) Draw an OBDD-representation of each of the sets of unsafe states $\mathbf{U_i}$ and $\mathbf{U_{ii}}$.

f) Determine whether the safety requirements are fulfilled.