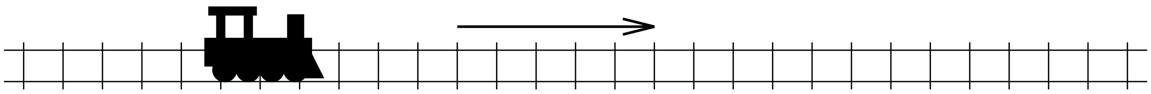
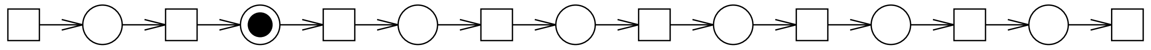
T-79.231 Parallel and distributed digital systems **Autumn 2001**
Home Assignment #2 **Original by Keijo Heljanko**

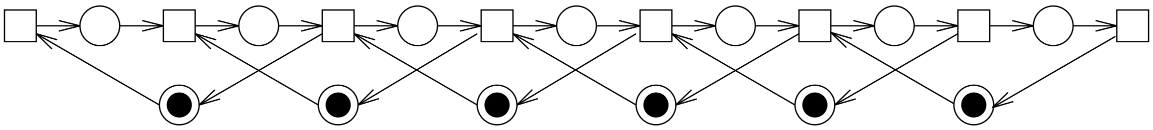
Design and analysis of a safety critical system

A segment of a train track can be modelled as a P/T net. A token represents a train travelling from left to right along the track. There is the problem that trains can collide with each other (from the rear). In the net model this is seen as the unsafeness of the net. The net can be made safe by a complement place construction. A similar signaling can be built on the train track, where a train moves to the next segment of the track only if it is empty.

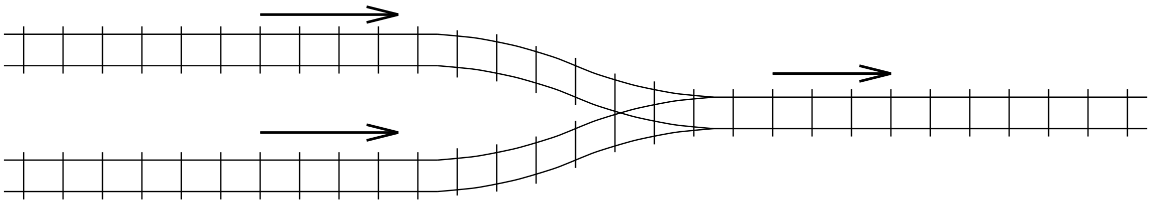


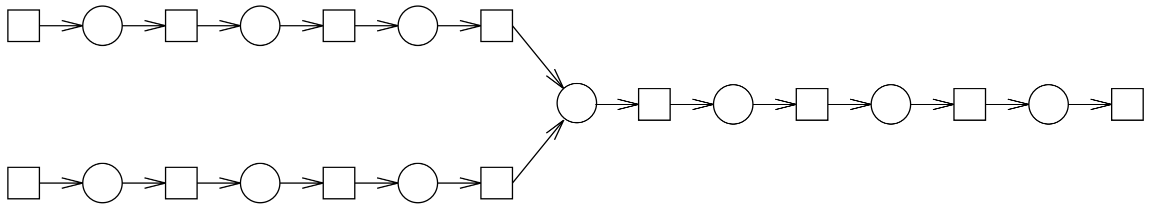


In a real system it s not sufficient for a train collision to be theoretically impossible. In addition, the trains must retain a certain safety distance from each other. In the net below, the signalling is designed so that there is always at least one track segment between any two trains.



(a) Plan a similar signalling in a switch where two tracks merge into one. Trains can arrive to the switch along both tracks from the left, independent of the other track. All trains continue to the right. There must always be at least one empty track segment between two trains arriving along the same track or from different tracks. Additionally, the trains must be allowed to travel as freely as possible. Present the system as a P/T net.





(b) Mark on the net those parts where conflict and confusion occur. Remember that conflict and confusion are dynamic properties.

(c) Assume that trains never stop voluntarily if the signalling permits them to proceed. Is it possible, in your system, for a train to arrive at the switch but never (or not for a very long time) get past it?

(d) Prove that in the straight track model above, there is always at least one empty track segment between two trains. Hint: Use place invariants (S-invariants).

(e) Present the straight track model as a Pr/T net and in the Maria input language when the length of the track is N segments.

N.B.: The home assignment is an individual task. No signs of cooperation shall be visible in the returned assignments.

The deadline for the Home Assignment 2 is Nov 12, 2001; use the post box between rooms B336 and B337 in the Computer Science building. The homework assistant is Jukka Honkola (email:Jukka.Honkola@hut.fi).