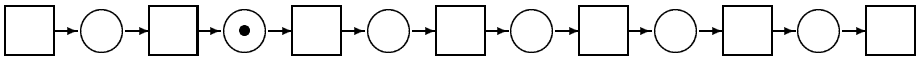
T-79.231 Parallel and Distributed Digital Systems
Homework Assignment 2, October 6, 2003 **Marko Mäkelä**

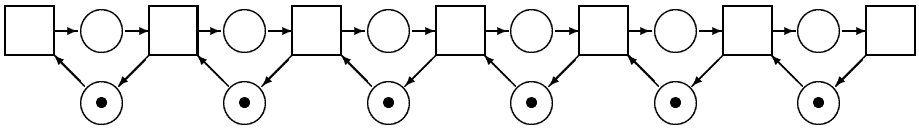
Designing and Verifying a Safety Critical System

Railway track can be modelled with a place/transition system. The token represents a train moving from left to right from one section of track to another.

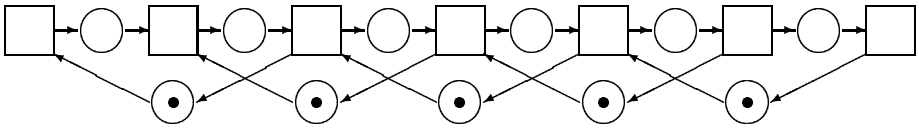


The system does nothing to prevent situations where a fast train appears from the left and collides into a slower train travelling somewhere on the middle of the track.

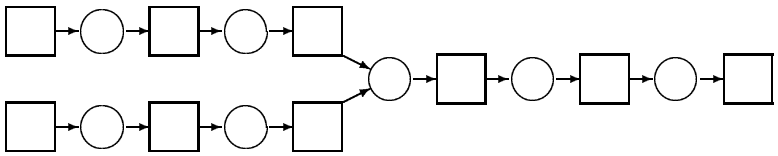
The model can be made safe by introducing complement places. These complement places would correspond to the signalling of the railway interlocking system.



The safety can be improved further by requiring that there must be at least one empty track section between trains.



1. Below is an intersection that merges two tracks into one. Augment it with a signalling system that guarantees that there will be an empty section between trains, and lets the trains move as freely as possible.



2. In which reachable markings of your solution is there a conflict?
3. Let us assume that trains do not stop voluntarily if the signals let them move along. Is it possible in your system that an arriving train is unable to proceed at all (or for a long time)?
4. Give a high-level net and a Maria model for a straight track of n segments that guarantees (a) one empty section, (b) two empty sections between successive trains.
5. Prove that the safety margins hold in your model. Hint: use `reject` formulae.

Return the assignment to the mailbox located between rooms B 336 and B 337 in the Computer Science Building, 3rd floor by 8 p.m. on November 3, 2003. You may also return the answer in Postscript or PDF form to Jukka.Honkola@hut.fi.