

Clayton School of Information Technology
FIT3013 Assignment 2
Refining the Railways
Refined Specification

Due Date: 12noon, 18 May 2009

This assignment is about refining the simple railway signalling specification started in Assignment 1. You are to use the RODIN tool to build the specification.

The main refinement to be added is the addition of intermediate stations. These stations have the advantage that they have two tracks, allowing trains in opposing directions to pass each other safely. Trains travelling towards Huntingdale are called **up** trains, and trains travelling towards Rowville are said to be **down** trains.

Between any two stations is a single line track called a *section*, and is referred to as “sectionAB” where A and B are the two stations at each end of the section. A section has a signal at each end facing entering trains (known as the *starting signal*), and shows a red or green aspect. Hence there are two sets of signals at each station: the **up starter** (for trains travelling towards Huntingdale) and the **down starter** (for trains travelling towards Rowville). Since there are two platforms at intermediate stations, we need a total of four starting signals (one on each end of each platform).

The signals thus allow trains to treat the sections between stations in the same way as the single section between Huntingdale and Rowville developed in *A1_SignallingMachine* – in particular, allowing trains to follow one another, and to pass trains in the opposing direction.

The rules for allowing a train to enter a section (turning a signal to green) are that the signal for entering the section from the opposite direction must be red, and that there are no trains already in the section (travelling in either direction). Be sure to make a clear distinction between the events of changing a signal, and a train entering a section.

1. We start this refinement by adding just one intermediate station: Monash University. This station is connected in each direction to Huntingdale and Rowville by two sections, each a single line track, thus requiring any passing or overtaking manoeuvres to take place at Monash, where there are two platforms A and B (each with their own track). Each platform can connect with each section. At each end of each platform is a starter signal, which allows a train standing at the platform to leave the platform and enter the section.

We also modify Huntingdale and Rowville so that they have two platforms each, but Huntingdale only has down starter signals, and Rowville only has up starter signals.

- (a) Assuming that *A1_SignallingContext* defines a set $SIGNAL = \{red, green\}$, define an invariant for the state variables *downStarter* and *upStarter*. (Remember that there are two down starters and two up starters.)
- (b) What is/are the variable(s) that you will use to describe trains in transit between any two stations i and $i + 1$ (counting Huntingdale as $station_0$ and Rowville as $station_2$) Remember to distinguish the direction of travel!
- (c) state the invariant that you use to ensure safety, that is, that there cannot be more than one train (in either direction) in a section at any one time.
- (d) State the invariant that you use to ensure that the signals cannot allow the safety condition to be violated.
- (e) Design a new machine *A2_SignallingMachine* that is a refinement of *A1_SignallingMachine*. You can access a fair copy of the assignment 1 project by downloading <http://www.csse.monash.edu.au/~ajh/teaching/fit3013/2009/assessment/assignment1/A1-Sol.pdf> (also available from the Moodle page).

2. (Generalization) Model the stretch of railway line from Huntingdale to Rowville as a collection of n stations (where Huntingdale is $station_0$, and Rowville is $station_{n-1}$), connected by $n - 1$ sections (where Huntingdale to $station_1$ is $section_1$, and $station_{n-2}$ to Rowville is $section_{n-1}$. (Since this is an isolated line with no junctions, we can simplify the rule for naming sections to be just “sectionB” without loss of generality.)
 - (a) Design a new machine $A2_GeneralSignalling$ that is a refinement of $A2_SignallingMachine$.
 - (b) Discuss how your modelling needs to change to accomodate this refinement.

Submit your solution as a fully commented Rodin export file through the Moodle submission mechanism. Include L^AT_EX generated pdf files of your project components, as described in lectures.