

An Event-B Specification of A2_SignallingMachine
Generated Date: 12 Jun 2009 @ 05:11:01 PM

MACHINE A2_SignallingMachine

This machine defines the Huntingdale-Monash-Rowville railway. It is written so that it can be easily generalized to more stations if required, or even to an arbitrary n stations, where station 0 = Huntingdale, and station n = Rowville

SEES A2_SignallingContext

VARIABLES

stationaryTrains location of all trains in the system
transitTrains trains that are travelling between stations
downStarter signals for town drains
upStarter signals for up trains

INVARIANTS

inv1 : $stationaryTrains \in (STATIONS \rightarrow (PLATFORMS \leftrightarrow TRAINS))$
every station has two platforms (total), which may or may not have a train (partial).
inv2 : $transitTrains \in (SECTIONS \rightarrow (DIR \leftrightarrow TRAINS))$
these are the trains in transit between stations. every section has two directions of travel (total), but at most only one direction can be populated (partial)
inv3 : $downStarter \in (SECTIONS \rightarrow (PLATFORMS \rightarrow SIGNAL))$
total, since all sections have both down and up starters, which must show either red or green
inv4 : $upStarter \in (SECTIONS \rightarrow (PLATFORMS \rightarrow SIGNAL))$
total, since all sections have both down and up starters, which must show either red or green

EVENTS

Initialisation

begin

act1 : $stationaryTrains := \{Hdale \mapsto \{A \mapsto t0, B \mapsto t1\}, Monash \mapsto \emptyset, Rville \mapsto \emptyset\}$
initially two trains, both at Huntingdale. If generalized, just $\{0 \mapsto \{A \mapsto t0, B \mapsto t1\}\}$
act2 : $transitTrains := \{sectionHM \mapsto \emptyset, sectionMR \mapsto \emptyset\}$
generalizes to $\{i \mapsto \{\} : i \in 0..n-1\}$
act4 : $downStarter := \{sectionHM \mapsto (PLATFORMS \times \{red\}), sectionMR \mapsto (PLATFORMS \times \{red\})\}$
initially, all signals are red. generalizes to $\{i \mapsto (PLATFORMS \times \{red\}) : i \in 0..n-1\}$
act5 : $upStarter := \{sectionHM \mapsto (PLATFORMS \times \{red\}), sectionMR \mapsto (PLATFORMS \times \{red\})\}$
initially, all signals are red. generalizes to $\{i \mapsto (PLATFORMS \times \{red\}) : i \in 0..n-1\}$

end

Event $enterSection \hat{=}$

A train t enters a section s leaving platform p at station l in direction d . The relevant signal is automatically reset to prevent followons.

any

t train about to enter section

l location of train
 d direction of train
 s section to be entered
 p platform from which this train is leaving

where

grd2 : $l \in STATIONS$
 enterSection from this station
grd3 : $l \in dom(stationaryTrains)$
 there must be some trains at this station
grd13 : $l \in dom(sections)$
 there must be some sections accessible from this station
grd5 : $d \in DIR$
 direction of travel of this train
grd10 : $d \in dom(sections(l))$
 and it must have a section to enter in this direction of travel
grd6 : $s \in SECTIONS$
 the section to be entered ...
grd7 : $s = sections(l)(d)$
 ... must be the next section in direction d at station l
grd12 : $p \in PLATFORMS$
 train is departing from this platform
grd9 : $p \in dom(stationaryTrains(l))$
 and there must be a train at this platform
grd1 : $t \in TRAINS$
 train to enter the section ...
grd4 : $t = stationaryTrains(l)(p)$
 and the train in question must be at this station and platform!
grd8 : $d = down \Rightarrow (downStarter(s)(p) = green)$
 safety condition to enter this section
grd18 : $d = up \Rightarrow (upStarter(s)(p) = green)$
 safety condition to enter this section
grd14 : $d = down \Rightarrow (s \in dom(downStarter) \wedge p \in dom(downStarter(s)))$
 if down, then downStarters relevant to this section and platform used
grd15 : $d = up \Rightarrow (s \in dom(upStarter) \wedge p \in dom(upStarter(s)))$
 if up, then upStarters relevant to this section and platform used

then

act1 : $transitTrains(s) := \{d \mapsto t\}$
 update the trains in transit
act2 : $stationaryTrains(l) := \{p\} \triangleleft stationaryTrains(l)$
 and train is no longer stationary
act3 : $downStarter : |(d = down \Rightarrow downStarter' = downStarter \triangleleft \{s \mapsto \{p \mapsto red\}\}) \wedge (d = up \Rightarrow downStarter' = downStarter)$
 reset the downStarter if cleared
act4 : $upStarter : |(d = up \Rightarrow upStarter' = upStarter \triangleleft \{s \mapsto \{p \mapsto red\}\}) \wedge (d = down \Rightarrow upStarter' = upStarter)$
 reset the upStarter if cleared

end

Event $leaveSection \hat{=}$
 trains arrives at a platform, leaving a section

any

p platform to arrive at

l station to arrive at
 t train in transit that is leaving the section s in direction d
 d direction of travel
 s section train is travelling in

where

grd1 : $p \in PLATFORMS$
 which platform are we arriving at?
grd2 : $l \in STATIONS$
 and which station?
grd3 : $(l \in dom(stationaryTrains)) \Rightarrow (p \notin dom(stationaryTrains(l)))$
 platform must be empty
grd4 : $d \in DIR$
grd5 : $s \in SECTIONS$
grd6 : $s \in dom(transitTrains)$
 there must be a train in transit in this section
grd7 : $d \in dom(transitTrains(s))$
 and going in this direction
grd8 : $t \in TRAINS$
grd9 : $t = transitTrains(s)(d)$
 this is the train in transit, in this section, going in this direction

then

act1 : $transitTrains(s) := \emptyset$
 no train in this section anymore
act2 : $stationaryTrains(l) := \{p \mapsto t\}$
 this train t now at the platform p in station l

end

Event *clearSignal* $\hat{=}$

Set a signal to green. Various safety conditions must be met.

any

p platform to clear for departure
 l station at which signal is to be cleared
 d direction of travel
 s section to be entered

where

grd1 : $p \in PLATFORMS$
grd2 : $l \in STATIONS$
grd3 : $d \in DIR$
grd4 : $s \in SECTIONS$
grd5 : $l \in dom(sections)$
grd6 : $d \in dom(sections(l))$
grd7 : $s = sections(l)(d)$
grd8 : $s \in dom(transitTrains)$
 there must be a train in this section
grd9 : $transitTrains(s) = \emptyset$
 safety condition: no trains in this section (in either direction)
grd10 : $d = down \Rightarrow upStarter(s) = PLATFORMS \times \{red\}$
 safety condition: both opposing signals must be red
grd11 : $d = up \Rightarrow downStarter(s) = PLATFORMS \times \{red\}$
 safety condition: both opposing signals must be red

grd12 : $d = \text{down} \Rightarrow \text{downStarter}(s)(\text{opp}(p)) = \text{red}$
 safety condition: adjacent starter must be red

grd13 : $d = \text{up} \Rightarrow \text{upStarter}(s)(\text{opp}(p)) = \text{red}$
 safety condition: adjacent starter must be red

then

act1 : $\text{downStarter} : |(d = \text{down} \Rightarrow (\text{downStarter}' = \text{downStarter} \triangleleft \{s \mapsto \{p \mapsto \text{green}\}\})) \wedge$
 $(d = \text{up} \Rightarrow (\text{downStarter}' = \text{downStarter}))$

change up or down Starter according to the direction of travel

act2 : $\text{upStarter} : |(d = \text{up} \Rightarrow (\text{upStarter}' = \text{upStarter} \triangleleft \{s \mapsto \{p \mapsto \text{green}\}\})) \wedge (d =$
 $\text{down} \Rightarrow (\text{upStarter}' = \text{upStarter}))$

end

END