Train Safety 2 assignment

Peter, Dirk, Johan & Elmar

Software Specification 2006

September 26, 2006

Problem Description

Problem Description

Given a train system consisting of a network of tracks, a set of trains and a control strategy, what does it mean for this control strategy to be reasonable.

Assumptions:

- We assume the previous train safety specification.
- We assume natural laws of physics.
- We assume trains don't break down.
- Trains always stop for a red light.

Definitions

- The railway infrastructure is represented by a directed graph $G(Nodes, Edges)$
- **Edges:** correspond to segments of railway track
- **Nodes:** are "interesting" points along the track:
  - Switches (or "merges")
  - Lights
- Train $= \{t_0, t_1 \ldots t_{n_{trains}}\}$
- Time $= \mathbb{R}^+$
- Pos $= \{(e, d) | e \in Edges, d \in [0, length(e))\}$
- Color $= \{Red, Orange, Green\}$
- LS $= (Color)^{n_{lights}}$
- SS $= (Edges)^{n_{switches}}$

Definitions

- Given a control stategy *ns*, a time and a train, return the position of the train at that time. *position* exists of two components: $position_e$ and $position_d$.

$$
\begin{aligned}
position &: NS \rightarrow Time \rightarrow Train \rightarrow Pos \\
position_e &: NS \rightarrow Time \rightarrow Train \rightarrow Edges \\
position_d &: NS \rightarrow Time \rightarrow Train \rightarrow \mathbb{R}^+
\end{aligned}
$$

- *velocity* is the derivative of *position*.

$$velocity : NS \rightarrow Time \rightarrow Train \rightarrow \mathbb{R}^+$$

Specification

- NS is the set of all reasonable control strategies. A strategy is reasonable if for all time the predicates *safe* and *moving* hold.

$$NS = \{ns | ns : Time \rightarrow (LS, SS), \\ \forall t \in Time \bullet safe(ns, t) \wedge moving(ns, t)\}$$

- Given a control strategy, is it safe at a certain time?

$$safe(ns, t) = \quad \forall train1, train2 \in Train \bullet train1 \neq train2 \Rightarrow \\ position_e(ns, t, train1) \neq position_e(ns, t, train2)$$

- Given a control strategy, is there at least one train moving?

$$moving(ns, t) = \exists train \in Train \bullet velocity(ns, t, train) > 0$$

Specification

Given a control strategy x, x is a reasonable strategy iff $x \in NS$.

Questions?

?