Railroad Crossing

Railroad Crossing Our sample model is derived from the verification of collision avoidance protocols for train applications [1]. The system model consists of two parts, the speed supervision of the train and a cooperation protocol between the train and a Radio Block Center (RBC).

Speed Controller The speed controller drives the current speed v towards a desired speed v_d. In the *Normal* mode the acceleration is computed by $\dot{v} = 0.1(v_d - v)$. If the computed acceleration exceeds the maximal or minimal acceleration, that is, if $\dot{v} \geq 1.0$ or $\dot{v} \leq -1.5$ the controller switches to the *Acceleration* or *Braking* mode. The *Acceleration* mode sets the acceleration to the fixed value $\dot{v} = 1.0$ and allows a transition back to the *Normal* mode if $0.1(v_d - v) \leq 0.8$ is reached. The *Braking* mode behaves similarly with the fixed deceleration $\dot{v} = -1.5$; it is left if $0.1(v_d - v) \geq -1.2$. In addition the controller provides an *Emergency* mode with maximum deceleration of $\dot{v} = -3$. The *Emergency* mode is entered if the cooperation protocol signals a failure.

Cooperation Protocol The cooperation protocol distinguishes different phases. These phases are modelled position dependent. In the *Far* phase the train receives optionally an *isCrossing* message. In this case it sends a *lockCrossing* request to the railroad crossing and switches to the *Request* phase. The railroad crossing has to acknowledge the request and starts locking the crossing. In the *Negotiation* phase the train gets the signals *isLockedCrossing* and *newEOA*. If the crossing is not locked or no new *End of Authority* (EOA) is provided the train has to stop before reaching the current EOA. The protocol also maintains some error control and signals a failure to the speed supervision.

Safety Property The safety property of the model is

$$\textit{Emergency} \text{ mode activated} \rightarrow p \leq EOA, \tag{1}$$

i.e. if the *Emergency* mode is activated the position of train does not exceed EOA.

On the other hand we wanted to ensure that the train crosses the EOA if no failure occurs, thus we showed that the target

$$\text{not } \textit{Emergency} \text{ mode activated} \rightarrow p \leq EOA, \tag{2}$$

is not always globally true, i.e. the train crosses EOA if *Emergency* is not activated.

Results For target (1) we ran two variants with different disturbances of the acceleration on an Intel Core 2 Duo T7500, 2.2 GHz, 2 GB RAM using one processor. As expected it turned out, that for smaller disturbances the target is safe and for higher disturbances the target is unsafe. We measured running times varying form 286 to 320 sec.

For target (2) we measured a running time of 164 sec.

References

[1] Werner Damm, Alfred Mikschl, Jens Oehlerking, Ernst-Rüdiger Olderog, Jun Pang, André Platzer, Marc Segelken, and Boris Wirtz. Automating verification of cooperation, control, and design in traffic applications. In *Formal Methods and Hybrid Real-Time Systems*, volume 4700 of *LNCS*, pages 115–169. Springer, 2007.