Towards the Verification of Bidirectional Railway Models in CSP||B

Phillip James, Faron Moller, Hoang Nga Nguyen, Markus Roggenbach, Steve Schneider, Helen Treharne

AVoCS 2014
Overview

The verification challenge
Railway modelling in CSP∥B in a nutshell
From uni-directional to bi-directional Scheme Plans
Finitisation
The verification challenge
Governance for Railway Investment Projects (GRIP)

Process prescribed by Network Rail within the UK

The first four GRIP phases define

- track plan
- routes

In phase five (Detailed design) a signalling company

- chooses appropriate track equipment,
- adds control/release tables
- implements the solid state interlocking
Scheme Plan verification

Given: Scheme Plan $SP$, i.e.

- Track Plan:

- Control / Release tables, e.g.

<table>
<thead>
<tr>
<th>Route Name</th>
<th>Normal</th>
<th>Reverse</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>R2</td>
<td></td>
<td>P2, P6</td>
<td>TC6, TC7, TC17, TC19, TC20</td>
</tr>
<tr>
<td>R3</td>
<td>P5, P6</td>
<td></td>
<td>TC14, TC18, TC19, TC20</td>
</tr>
<tr>
<td>R5B</td>
<td>P2, P3</td>
<td></td>
<td>TC9, TC8, TC7, TC6, TC3</td>
</tr>
<tr>
<td>R5C</td>
<td></td>
<td>P3, P5</td>
<td>TC9, TC8, TC17, TC18, TC14, TC13</td>
</tr>
</tbody>
</table>
Scheme Plan verification

Given: Scheme Plan $SP$, i.e.

- Track Plan:

- Control / Release tables, e.g.

<table>
<thead>
<tr>
<th>Route Name</th>
<th>Normal</th>
<th>Reverse</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>R2</td>
<td>P2, P6</td>
<td>TC6, TC7, TC17, TC19, TC20</td>
<td></td>
</tr>
<tr>
<td>R3</td>
<td>P5, P6</td>
<td>TC14, TC18, TC19, TC20</td>
<td></td>
</tr>
<tr>
<td>R5B</td>
<td>P2, P3</td>
<td>TC9, TC8, TC7, TC6, TC3</td>
<td></td>
</tr>
<tr>
<td>R5C</td>
<td>P3, P5</td>
<td>TC9, TC8, TC17, TC18, TC14, TC13</td>
<td></td>
</tr>
</tbody>
</table>

Verify: $SP$ is “safe”, i.e., collision-free, has no run-throughs, and no moving points under trains.
Operation of an interlocking

Controller

Route request, Route release

Interlocking

Request response, Release response

Signal and point settings

Track occupation

Track equipment

Signal aspect

Current movement

Trains

M.Roggenbach: Bidirectional Railway Models; AVoCS 2014
Railway modelling in CSP in a nutshell
The language CSP||B

Event-based & state based modelling: CSP processes control classical B machines

Safety verification: certain B states are not reachable.
Example: CSP controls B via “machine channels”

Machine channels: nextSignal, release, request, move, ...

CSP: \( P(t) = \text{nextSignal}!t?\text{aspect} \rightarrow P'(\text{aspect}) \)

B: \( s \leftarrow \text{nextSignal}(t) = \) 
Pre ...
Then ... \( s := \text{SignalStatus}(\text{homeSignal}(\text{pos}(t))) \)
End
Generic railway modelling in CSP||B

CSP: Controller & Trains

Statefull B: Interlocking

Stateless B: Scheme Plan (specific)

“Double nature” of railways: events & state conditions

M.Roggenbach: Bidirectional Railway Models; AVoCS 2014
From uni-directional to bi-directional Scheme Plans
Unidirectional interlockings

Prevent

• setting of a route that is currently in use,
• setting of conflicting routes
Bidirectional interlockings

Prevent

- setting of a route that is currently in use,
- setting of conflicting routes

Additionally, prevent

- setting of opposing routes
Bidirectional interlockings

Prevent
• setting of a route that is currently in use,
• setting of conflicting routes

Additionally, prevent
• setting of opposing routes

Means: sequential release
= lock track circuites of a route; release locks behind a train
Consequences for our CSP∥B models

- Increase in code complexity
  (as events have to take care of directions)

- Significantly larger state space
  e.g., single junction

  | uni-directional modelling: | 8,646 states |
  | bi-directional modelling:   | 196,284 states |

- Finitisation & decomposition theorems harder to establish
Finitisation
The “algebra” of interlockings

Controller can request or cancel routes.

Claim:

Sometimes, the “effect” of running a train on a route can be mimicked by a route request followed by a route release.
A simulation theorem

Given:

- scheme plan \( SP \)
- a set \( \text{Train} \) of trains
- \( B \subseteq \text{Train} \)

Let \( \sigma \) be a system run of CSP||\( B(SP, \text{Train}) \).

Then \( \text{replace}_B(\sigma) \) is a system run of CSP||\( B(SP, \text{Train} \setminus B) \), provided trains in \( B \) do not violate any safety property in \( \sigma \) but in the last state.
Definition of the replace function

\[ \text{replace}_B(S, e) = \begin{cases} 
  e & \text{``concerns'' a train not in } B \\
  \text{release.r.yes} e = \text{move.b.cp.np} & \text{for some } b \in B \text{ and } b \text{ ``moves over a green signal''} \\
  \text{idle} & \text{otherwise} 
\end{cases} \]

\( S \) : state of the B machine
\( e \) : event
Idea behind the theorem

establish relations between

- the states $S, S', \ldots$ of $\sigma$
- the states $T, T', \ldots$ of $\text{replace}_B(\sigma)$, i.e., after removing trains $B$

\[
\begin{array}{ccccccccc}
S & e & S' & e & S' & \ldots & S' \\
\preceq_B & \preceq_B & \preceq_B & \preceq_B & \preceq_B \\
T & \text{replace}_B(S, e) & T' & \text{replace}_B(S, e) & T' & \ldots & T'
\end{array}
\]
\( \leq_B \) consists out of 11 relations

including

- point positions are the same
- train positions are the same – up to the trains removed
- a \( T \) state has less locks than its corresponding \( S \) state
- for green routes the locks are the same.
- after a route release thanks to a train in \( B \), all locks of this route are empty.
Conclusion
Results

We have achieved:

• Modelling of bi-directional Scheme Plans in CSP||B.
• Finitisation:
  a scheme plan is safe for any number of trains
  if it is safe for two trains.
• Safety proofs are possible for
  simple bi-directional Scheme Plans.
Future work

- Develop bi-directional decomposition.
- Transfer these ideas over to ETCS, level 2.
Announcement
Two open postdoc positions in Swansea

Position 1: smart phone security
- software verification via abstraction to CSP / Timed CSP
- 2 years
- starting early 2015

Position 2: railway safety and capacity
- railway modelling and verification in Real-Time Maude / Timed CSP / Timed (CSP||B)
- 2 years
- starting early 2015.