Measuring Railway Capacity in Timed CSP for solid state interlockings

Markus Roggenbach
Faron Moller, Hoang Nga Nguyen, Yoshinao Isobe

WG “FM s in Railway Control”, January 2015
Motivation

State of the art:
• Experienced engineers “see” the patterns in railway design which lead to high or low capacity.

Open questions:
• Can we give scientific foundations to their experience?
• Can we turn such foundations to an engineering practice?

From the SafeCap project proposal (2010)
A pictorial description
Overview

A simple example
A definition of line capacity
Measuring line capacity in Timed CSP
A simple example
Design 1 – overlaps in the control table

Track plan

Control table

<table>
<thead>
<tr>
<th>Route</th>
<th>Normal</th>
<th>Reverse</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>3A</td>
<td>P101</td>
<td>AB, AC, AD, AE</td>
<td></td>
</tr>
<tr>
<td>3B</td>
<td>P101 P102*</td>
<td>AB, AC, BW, CM, CL</td>
<td></td>
</tr>
<tr>
<td>4A</td>
<td>P101* P102</td>
<td>BV, BW, BX, BY, BZ</td>
<td></td>
</tr>
<tr>
<td>16A</td>
<td>P102</td>
<td>DR, BX, BY, BZ</td>
<td></td>
</tr>
</tbody>
</table>
Design 2 – no overlaps, due to ATP

Track plan

Control table 2

<table>
<thead>
<tr>
<th>Route</th>
<th>Normal</th>
<th>Reverse</th>
<th>Clear</th>
</tr>
</thead>
<tbody>
<tr>
<td>3A</td>
<td>P101</td>
<td></td>
<td>AB, AC, AD, AE</td>
</tr>
<tr>
<td>3B</td>
<td>P101 P102*</td>
<td>AB, AC, BW, CM, CL</td>
<td></td>
</tr>
<tr>
<td>4A</td>
<td>P101* P102</td>
<td>BV, BW, BX, BY, BZ</td>
<td></td>
</tr>
<tr>
<td>16A</td>
<td>P102</td>
<td>DR, BX, BY, BZ</td>
<td></td>
</tr>
</tbody>
</table>

* flank protection
The example in the world of rail engineers

- Design 1 is what UK legislation requires.
- Design 2 is currently against UK legislation.

Observations:
- Taking overlaps out should increase capacity.
- ATP says: safety should not be compromised.
- Engineers are only “half” comfortable to take overlaps out.
- Safety and capacity are two sides of one coin.

Question:
Does the gain in capacity justify change of regulations?
Scientific questions

Given a scheme-plan (track plan + ctrl tables)
• How to prove safety? $\leadsto$ e.g. Helen’s talk
• How to define a capacity measure to quantify the effect?
• How to actually measure capacity?
A definition of line capacity
Context

**Analytic:** Model railway infrastructure by means of mathematical formulae and predict theoretical capacity [UIC 405].

**Optimisation:** Maximise railway capacity by optimising given time tables [UIC 406].

**Simulation:** Imitate the operation of real world railway systems over time [Barber et al 2007].

**Fantechi:** this afternoon.
Our approach

Consider all finite runs of a timed railway model, extending K. Winter’s CSP modelling of scheme-plans:

- Open train systems,
- Timed CSP-modelling,
- Train length & speed,
- Track length.

Observations on trains: front and rear movements

\[
\text{moveff.TA.TB} \quad \text{moverr.TA.TB}
\]
Line capacity - informal

Capacity determines the maximum number of trains that would be able to operate on a given railway infrastructure, during a specific time interval, given the operational conditions. [Abril et al 08]
A space-time diagram of a line

Assumption: infinite supply of ready-to-go trains “on the entry”

(all trains at the same, constant speed; track-length ∼ 3 train-length)
Diagram with observation window

Window-parameters: duration “Delta” & starting time “ST”
Measuring line capacity: Delta = 12, ST = 0

Number of observed trains = 3
Measuring line capacity: Delta = 12, ST = 6

Number of observed trains = 5
Measuring line capacity: Δ = 12, ST = 7

Number of observed trains = 4
Maximum of observed trains, over all starting times: 5.
Definition: “line capacity” in Timed-CSP

Given a Timed-CSP process $TS$ modelling a line of a train system and an observation length $\delta > 0$:

$$cap(TS, \delta) = \max \{ storage(s_1) + increase(s_2) \mid s_1 \triangleright s_2 \in \mathcal{T}_{[0]}[TS] \land \text{duration}(s_2) \leq \delta \}$$

- $storage(s) = s \downarrow entering - s \downarrow leaving$
- $increase(s) = s \downarrow entering$

Given a line with first track F and last track L.

- $entering$ – set of timed events of the form moveff.*.F
- $leaving$ – set of timed events of the form moverr.L.*
Measuring line capacity in Timed CSP
Characterising line capacity via refinement

Theorem
Let $\delta$ be the length of the observation window.
Let $n$ be a natural number.
Let $\delta$ be a rational time length. Then it holds:

$$\text{cap}(\text{TrainSystem}, \delta) = n$$

iff

for all $k \geq n$: $\text{CapFrom}(k, \delta) \subseteq_{TT} \text{TrainSystem'} \land$

for all $k < n$: $\text{CapFrom}(k, \delta) \not\subseteq_{TT} \text{TrainSystem'}$.

$$\text{CapFrom}(k, \delta) = \bigcap_{n \in \{0..n\}} \text{startObs}.\delta \rightarrow \text{infoCap}.n \rightarrow \text{Stop}$$
Verification process for each line

- FDR: to check safety of both scenarios.
- Timed-CSP Simulator: to estimate a small enough $\delta$ to differentiate line capacity of the two designs.
- FDR: to verify the different line capacities.
Results for the double junction designs

- **Safety**: both designs are collision-free (considering each line in isolation)
- **Line capacity**: “one more train every six minutes”

<table>
<thead>
<tr>
<th>Path</th>
<th>Window length</th>
<th>Capacity in Design 1</th>
<th>Capacity in Design 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line from A to E</td>
<td>397s</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>Line from A to B</td>
<td>379s</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>Line from D to C</td>
<td>399s</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>Line from F to C</td>
<td>328s</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

(model-checking takes about 40 seconds for each line)
Snapshot from FDR2
Limitations as of 2012

using FDR2:

• lines of 6–8 tracks could be analysed for safety & capacity
• analysing the double junction as a whole was out of scope

i.e., the approach does not scale.
Reduction of model complexity is possible

• Clearer model architecture

• No train-length
  (2014 paper in SCP discussing the topic for safety)

• Work with move rather than with moveff, moverr
  ○ we have a proof that w.r.t. safety both modelling approaches are equivalent (in CSP)
  ○ experiments show that model-checking with move is far cheaper
New insights – Part II: Abstraction & Tool

Abstractions for safety
(finitisation and covering were originally discovered in the context of CSP modelling)

Better tool support: FDR3 is more powerful than FDR2
New insights – Part III: Network Capacity

Observation window of 300 seconds (result via simulation)
Conclusion
Summary

- The problem of theoretical capacity is still open.
- **Line Capacity:**
  - working definition in Timed CSP
  - tool support needs improvement
- **Network Capacity:**
  - suggestion for a definition in Timed CSP
  - tool support is open
Future work on capacity @ Swansea

For solid state interlockings:

- Mike Smith will take a fresh look at things
- also using alternative tools & languages such as PRISM.

For ERTMS:

- Ditto project (RA position from March 2015):
  - adapt results from solid state interlockings &
  - look into alternatives
- Monika’s talk provides an alternative view.
this presentation has been based on our publication