USING CSP||B AND ProB FOR RAILWAY MODELLING

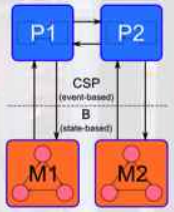
Aims

"Natural modelling" to provide accessible and traceable formal specifications

Tool support for verification with comprehendible feedback

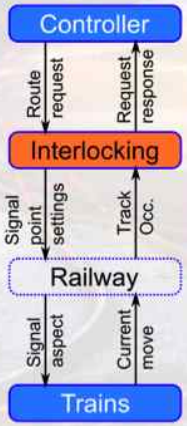
Background

CSP||B Architecture



Railway

hybrid nature



Railway's duality

Event: "*train moves on track T5*"

State condition: "*signal S shows proceed if tracks T1, T2 are free*"

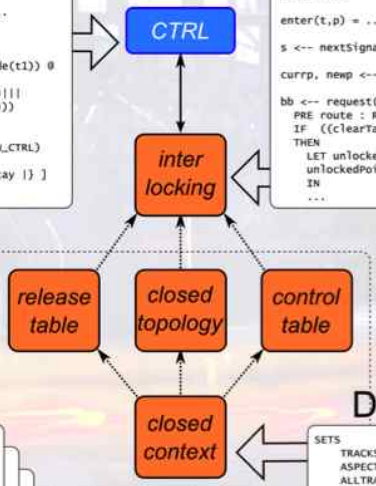
A natural modelling approach

Driving rules

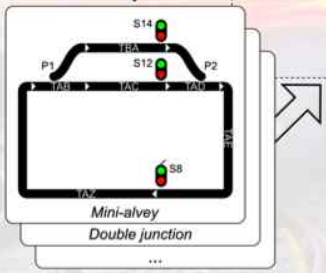
```
RW_CTRL = [] r : ROUTE @
          (request!r -> RW_CTRL)

TRAIN_CTRL(t,currp) =
   nextSignal!t?s ->
   if (s == none or s == green)
   then (move.t.currp?newp -> ...

ALL_TRAINS = [] t1 : TRACK @
   enter.albert.t1 ->
     (([] t2 : diff(TRACK,exclude(t1)) @
        enter.bertie.t2 ->
          TRAIN_CTRL(albert,t1)|||
          TRAIN_CTRL(bertie,t2)))

-TRL  =
   (enter?t?p -> enter?t?p -> RW_CTRL)
   [ {|enter,request |} ||
   {|enter, nextSignal, move, stay |} ]
   ALL_TRAINS
```

Signalling

```
INVARIANT

      pos : TRAIN >+> TRACK &
      ...

OPERATIONS

enter(t,p) = ...

s <-- nextSignal(t) = ...

currp, newp <-- move(t) = ...

bb <-- request(route) =
  PRE route : ROUTE THEN
  IF  ({clearTable(route) <: emptyTracks ))
  THEN
    LET unlockedPoints BE
    unlockedPoints = POINTS-ran(currentLocks)
    IN
    ...
```



Track plans



Datatypes

```
SETS
    TRACKSTATUS = {occ,empty};
    ASPECT = {red,green,none};
    ALLTRACK = {TA2,TAB,TAC,...};
    SIGNAL = {S8,S12,S14};
    TRAIN = {albert,bertie};
    POINTS = {P201,P202};
    POINTPOSITION={normal,reverse};
    POINTSTATUS={locked, unlocked};
    ROUTE = {A8,B8,A12,A14}

CONSTANTS
    SIGNALSTATUS,
    TRACK
...
```

Mini-alvey

Double junction

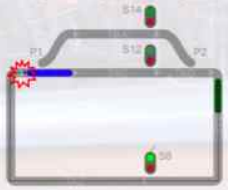
...

Verification

Safety: no collision and no derailment

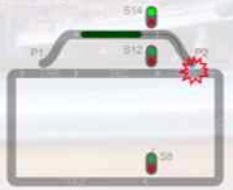
Collision caused by a faulty rule for 8A

(TAB not required to be clear)



Derailment caused by a faulty rule for 14A

(P2 in normal position)



Results

CSP||B models which are

- *understandable and (thus) verifiable by our industrial partners*
- *analysable by current verification technology*

References:

1. Schneider, S. and Treharne, H. *CSP theorems for communicating B machines,* Journal of Formal Aspects of Computing. Volume 17. Pages 390-422. 2005.
2. F. Moller, H. Nguyen, M. Roggenbach, S. Schneider, H. Treharne, *Combining event-based and state-based modelling for railway verification*, Tech. Rep. CS-12-02, University of Surrey (2012).

Swansea University Prifysgol Abertawe

Faron Moller
Hoang Nga Nguyen
Markus Roggenbach

UNIVERSITY OF SURREY

Helen Treharne
Steve Schneider

SafeCap