Ten Diverse Formal Models for a CBTC Automatic Train Supervision System

Franco Mazzanti
ISTI CNR Pisa Italy
Origins of the study

Trace-IT

Define an ATS scheduling approach to achieve deadlock free train dispatching.

Case Study: a project defined CBTC scenario

ASTRail

Investigate and experiment with a rich set of formal methods an tools to compose a survey on the suggested use of formal methods in the railway field.

Trace-IT case study re-used as one of the experiments.

Official Disclaimer: The opinions and results discussed in this presentation reflects only the author’s view and the Shift2Rail Joint Undertaking is not responsible for any use that may be made of the presented information.
The Trace-IT goal

- We have a metro layout.
- We have an automatic (unmanned) metro service.
- Each train has its mission statically defined, provided to the ATS as static configuration data (timetable).
- We have to design the logic of the ATS scheduling kernel, to successfully dispatch all the trains, leading them to destination avoiding deadlocks (also in case of arbitrary delays).
The Trace-IT project demonstrator case study

- 8 trains providing circular services
Itineraries vs circuits

Segments correspond to entry/exit itineraries of stations

Itineraries are composed of several track circuits
Handling the problem size

SECTION 1

SECTION 2

SECTION 3
The Section 2 layout and train missions.
The Section 2 layout and train missions.
The Section 2 layout and train missions.
The Section 2 layout and train missions.
The Trace-IT case study
The Section 2 layout and train missions.
The Section 2 layout and train missions.
The Section 2 layout and train missions.
The Section 2 layout and train missions.
A sample deadlock occurrence
The Trace-IT solution

Ten Diverse Formal Models …

Thessaloniki, 20 April 2018

RA = current occupation count
LA = max occupation count = 7

T0 = [1, 9, 10, 13, 15, 20, 23] Mission for train0
A0 = [0, 0, 0, 1, 0, -1, 0] Region-A Constraints for train0
The progression rule (e.g. for train0)

\[
\begin{align*}
T_0 &= [1, 9, 10, 13, 15, 20, 23] \quad \text{Mission for train0} \\
A_0 &= [0, 0, 0, 1, 0, -1, 0] \quad \text{Region-A Increments/Decr. for train0} \\
P_0 &= n \quad \text{current progress point of train0 (index in } T_0) \\
R_A &= n \quad \text{current degree of occupancy of region } A \\
L_A &= 7 \quad \text{maximum degree of occupancy for region } A
\end{align*}
\]

when <next endpoint of train0 is free>

i.e. for all \( i \): \( T_0[P_0+1] \neq T_i[P_i] \)

and <train0 move does not saturate any region>

i.e. for all regions \( A \), … : \( R_A + A_0[P_0+1] \leq L_A \)

the train can advance: i.e. \( P_0 = P_0+1, \quad R_A = R_A + A_0[P_0] \)
### The reference structure of the model

<table>
<thead>
<tr>
<th>Global Constants</th>
<th>Train Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0 = [1, 9, 10, 13, 15, 20, 23]; A0 = [0, 0, 0, 1, 0, -1, 0]; B0 = [0, 0, 0, 1, 0, -1, 0]; ...</td>
<td></td>
</tr>
<tr>
<td>T7 = [26, 22, 17, 18, 12, 27, 7]; A7 = [1, 0, 0, -1, 0, 0, 0]; B7 = [1, 0, 0, -1, 0, 0, 0]; LA = 7; LB = 7</td>
<td></td>
</tr>
<tr>
<td>Global Variables</td>
<td></td>
</tr>
<tr>
<td>P0, P1, ..., P7 := 0; RA := 1, RB := 1</td>
<td></td>
</tr>
<tr>
<td>Train0: [guard train0] / actions train0</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>Train7: [guard train7] / actions train7</td>
<td></td>
</tr>
</tbody>
</table>

---

**Global Constants**

- \( T_0 = [1, 9, 10, 13, 15, 20, 23] \)
- \( A_0 = [0, 0, 0, 1, 0, -1, 0] \)
- \( B_0 = [0, 0, 0, 1, 0, -1, 0] \)

- ... (omitted)

- \( T_7 = [26, 22, 17, 18, 12, 27, 7] \)
- \( A_7 = [1, 0, 0, -1, 0, 0, 0] \)
- \( B_7 = [1, 0, 0, -1, 0, 0, 0] \)

- \( \text{LA} = 7; \text{LB} = 7 \)

---

**Global Variables**

- \( P_0, P_1, ..., P_7 := 0; \)
- \( \text{RA} := 1, \text{RB} := 1 \)

---

**Train Rules**

- \( \text{Train0: [guard train0] / actions train0} \)
- ... (omitted)
- \( \text{Train7: [guard train7] / actions train7} \)
The encoding of the model: UMC

\[
\text{train0: s1 -> s1}
\]
{ \hspace{10pt} \begin{align*}
&P0 < 6 \quad & T0[P0+1] \neq T5[P5] \quad \& \ldots \& \quad T0[P0+1] \neq T7[P7] \quad \& \\
&RA + A0[P0+1] \leq LA \quad \& \quad RB + B0[P0+1] \leq LB \\
&P0 := P0 + 1; \\
&RA := RA + A0[P0]; \quad \text{RB} := RB + B0[P0]; \\
\end{align*} \}

\[
\text{...}
\]

\[
\text{train7: s1 -> s1}
\]
{ \hspace{10pt} \begin{align*}
&\ldots
\end{align*} }
The encoding of the model: SPIN

\[
\begin{align*}
do &:: atomic \{ \\
& (P0<6 \ & \ & T0[P0+1] != T1[P1] \ & \ & \ldots \ & \ & \ldots \ & \ & T0[P0+1] != T7[P7] \ & \ & \&
(RA+A0[P0+1]) <= LA \ & \ & \& (RB+B0[P0+1] <= LB) \\
& ) - > \\
& P0 = (P0+1); \\
& RA = RA+A0[P0]; \\
& RB = RB+B0[P0];
\}
\end{align*}
\]

:: atomic 

};

od;
The encoding of the model: CADP/LNT

loop
  select
    only if
      P0<6 and T0[P0+1] != T1[P1] and ... and T0[P0+1] != T7[P7] and
      (RA+A0[P0+1]) <= LA and (RB+B0[P0+1] <= LB)
    then
      MOVE (0 of Train_Number);
      P0 := (P0+1);
      RA := RA+A0[P0];  RB := RB+B0[P0];
    end if
  [ ]
    only if
      ...
  end select
end loop
The encoding of the model:  ProB

OPERATIONS

move0 =

PRE
P0<6  &  T0(P0+1) /=T1(P1)  &...&  T0(P0+1) /=T7(P7)  &
RA+A0(P0+1)<=LA  &  RB+B0(P0+1)<=LB

THEN
P0 := P0+1;
RA := RA+A0(P0);  RB := RB+B0(P0);

END;

move1 =  ...
The encoding of the model: NuSMV/ nuXmv

TRANS

RUNNING=0 ->

P0<6 && T0[P0+1] != T1[P1] &&...& T0[P0+1] != T7[P7] &
(RA+A0[P0+1])<=LA & (RB+B0[P0+1])<=LB

? next(P0)=(P0+1) & next(P1)=P1 &&...& next(P7)=P7 &
next(RA)= RA+A0[P0]; next(RB)=RB+B0[P0];

: next(P0)=P0 &&...& next(P7)=P7 & next(RA)=RA & next(RB)=RB

...

TRANS

RUNNING=7 ->
The encoding of the model: FDR4 / CSPm

AllTrains \((P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7, RA, RB) = \)

\[
\begin{align*}
& \text{( } P_0 < 6 \text{ and } \\
& \quad \text{el}(T_0,P_0+1) \neq \text{el}(T_1,P_1) \text{ and } \ldots \text{ and } \text{el}(T_0,P_0+1) \neq \text{el}(T_7,P_7) \text{ and } \\
& \quad RA + \text{el}(A_0,P_0+1) \leq LA \text{ and } RB + \text{el}(B_0,P_0+1) \leq LB \text{ ) } & \\
& \text{)} \ \& \\
& \text{move0 } \rightarrow \\
& \quad \text{AllTrains}(P_0+1,P_1,P_2,P_3,P_4,P_5,P_6,P_7, \ RA+\text{el}(A_0,P_0+1), \ RB+\text{el}(B_0,P_0+1)) \\
& \text{[ ] } \text{ ( } P_1 < 6 \text{ and } \\
& \quad \ldots \text{ )} \end{align*}
\]
The encoding of the model: mCRL2

proc AllTrains(P0,P1,P2,P3,P4,P5,P6,P7:Nat, RA,RB: Int) =

( P0 < 6 &&
  T0(P0+1) != T1(P1) &&… && T0(P0+1) != T7(P7) &&
  RA+A0(P0+1) <= LA && RB+ B0(P0+1)<=LB
 ) &
move(0) ->
  AllTrains(P0+1,P1,P2,P3,P4,P5,P6,P7, RA+A0(P0+1), RB+B0(P0+1))

[ ]
( P1 < 6 &&
  ...

The encoding of the model: TLAplus

Move0 == \ 
    P0 < 6 \& T0[P0+2] /= T1[P1+1] \& ... \& T0[P0+2] /= T7[P7+1] \& 
    RA + A0[P0+2] <= LA \& RB + B0[P0+2] <= LB \& 
    P0' = (P0+1) \& 
    RA' = RA+A0[P0+2] \& RB' = RB+B0[P0+2] \& 
    UNCHANGED <<P1,P2,P3,P4,P5,P6,P7>>

Move1 ==

... 

Next == Move0 \ Move1 \ Move2 \ Move3 \ Move4 \ Move5 \ Move6 \ Move7
Considerations:

So what ????
### Considerations:

| Blackboard models / Event-Condition-Action models / Guard-Transition models / | can have a common reference baseline |
Considerations:

Blackboard models / Event-Condition-Action models / Guard-Transition models / can have a common reference baseline

**Diversity** in tool selection / model encoding: more trustable verification results
Considerations:

Blackboard models / Event Condition Action models / Guard Transition models / can have a common baseline

Diversity in tool selection / model encoding
more trustable verification results
better exploitation of the verification features of multiple existing frameworks.

e.g. Branching vs. Linear vs. Refinements vs. Compositional

e.g. tool. friendliness vs. ability to deal with very large models

e.g. timed vs untimed
Further Works:

More frameworks taken into consideration: Simulink / SCADE / SAL / UPPAAL / ....

More features compared:

- Code Generation?
- Customer Support
- Language Expressiveness
- Simulation?
- Model-based Testing?
- Documentation
- Maturity
- Time Related Aspects?
- Industrial Diffusion
- Report Generation?
- Inport/Export
- Standard input format?
- Modularity
- Certification
- Probability?
Thessaloniki, 20 April 2018

Ten Diverse Formal Models…

This work has received funding from the S2RJU under the European Union’s Horizon 2020 research and innovation programme under grant agreement No 777561.

The opinions and results discussed in this presentation reflect only the author’s view and the Shift2Rail Joint Undertaking is not responsible for any use that may be made of the presented information.
THANK YOU!

CONTACTS
Franco Mazzanti
Senior Researcher
ISTI-CNR Via Moruzzi 1, Pisa, Italy
http://fmt.isti.cnr.it/~mazzanti

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No 777561

Call identifier: H2020-S2RJU-2017
Topic: S2R-OC-IP2-01-2017 – Operational conditions of the signalling and automation systems; signalling system hazard analysis and GNSS SIS characterization along with Formal Method application in railway field
The incremental design/verification approach:

- Train Missions
- Initial model (handling basic deadlocks)
- Model Checking
- New sections, counters, and updated missions
- No more deadlocks
- Validated ATS Data
- New deadlocks