Formal Verification of the Danish Railway Interlocking Systems

Linh H. Vu* (lvho@dtu.dk)
Anne E. Haxthausen* (aeha@dtu.dk)
Jan Peleska** (jp@informatik.uni-bremen.de)

* Technical University of Denmark, Denmark
** University of Bremen, Germany
Background

• **Context:** The Danish Signalling Programme\(^1\) (2009-2021) - replace the railway signalling systems in the entire country with standardized ERTMS/ETCS Level 2

• **ERTMS/ETCS:** European standardized railway traffic management/train control systems → seamless railway travel through Europe

• **RobustRailS:** (Robustness in Railway OperationS\(^2\))
  - Funded by the Danish Strategic Research Council
  - Accompanies the Danish Signalling Programme on a scientific level

• **(One of the) goals:** Provide methods and tools supporting *efficient* development and verification of railway control systems (WP.4.1)

→ *How we did that for a case study*…

Source: ertms.net

\(^1\) [http://www.bane.dk/signalprogrammet](http://www.bane.dk/signalprogrammet)

\(^2\) [http://robustrails.man.dtu.dk](http://robustrails.man.dtu.dk)
Agenda

1. Background

2. Case Study

3. Toolchain and Model

4. Verification Technique

5. Conclusion
Interlocking Case Study

- **Interlocking system**: A component of the signalling system that guides trains safely through the (fraction of) railway network under its control

- **Safety-critical**: A vital component with highest safety integrity level (SIL4)

- **Our goal**: Verify high-level safety properties (no collisions, no derailments) for the new Danish interlocking systems

- **Approach**:
  - Formal methods (FM) based - strongly recommended by CENELEC 50128 standard
  - Domain-specific languages to encapsulate FM
  - Support automation

Source: wikipedia.org, skynet.be
Route-based Interlocking Systems

- Reserve a fraction of the network - a route - for a train at a time
- Specification of a route-based interlocking system consists of
  1. A railway network layout under control
  2. A corresponding interlocking table

<table>
<thead>
<tr>
<th>ID</th>
<th>src</th>
<th>dest</th>
<th>overlaps</th>
<th>points</th>
<th>signals</th>
<th>path</th>
<th>conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mb11</td>
<td>mb13</td>
<td>t11:p;t13:m</td>
<td>mb12;mb20</td>
<td>t11;t12</td>
<td>2;3;4;5;7</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>mb11</td>
<td>mb21</td>
<td>t11:m;t13:p</td>
<td>mb12;mb20</td>
<td>t11;t20</td>
<td>1;3;6;7;8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>mb12</td>
<td>mb10</td>
<td>t11:p</td>
<td>mb11;mb20</td>
<td>t11;t10</td>
<td>1;2;5;7</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>mb13</td>
<td>mb15</td>
<td>t13:p</td>
<td>mb14;mb21</td>
<td>t13;t14</td>
<td>1;5;6;8</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>mb14</td>
<td>mb12</td>
<td>t11:m;t13:p</td>
<td>mb13;mb21</td>
<td>t13;t12</td>
<td>1;3;4;6;8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>mb14</td>
<td>mb20</td>
<td>t11:p;t13:m</td>
<td>mb13;mb21</td>
<td>t13;t20</td>
<td>2;4;5;7;8</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>mb20</td>
<td>mb10</td>
<td>t11:m</td>
<td>mb11;mb12</td>
<td>t11;t10</td>
<td>1;2;3;6</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>mb21</td>
<td>mb15</td>
<td>t13:m</td>
<td>mb13;mb14</td>
<td>t13;t14</td>
<td>2;4;5;6</td>
<td></td>
</tr>
</tbody>
</table>
Railway Network Layout

- Geographical arrangement of track-side elements
  - linear sections (t10)
  - points (t11): PLUS (straight) or MINUS (siding) positions
  - marker boards (mb11)
Virtual Signal Concept

- **ETCS Level 2**: No physical signals on the tracks; instead movement authorities are communicated via on-board computers → modeling concept of virtual signals associated with marker boards
Interlocking Tables

• An interlocking table specifying routes and conditions for setting (reserving) them

<table>
<thead>
<tr>
<th>ID</th>
<th>src</th>
<th>dest</th>
<th>overlaps</th>
<th>points</th>
<th>signals</th>
<th>path</th>
<th>conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mb11</td>
<td>mb13</td>
<td>t11;p;t13;m</td>
<td>mb12;mb20</td>
<td>t11;t12</td>
<td>2;3;4;5;7</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>mb11</td>
<td>mb21</td>
<td>t11;m;t13:p</td>
<td>mb12;mb20</td>
<td>t11;t20</td>
<td>1;3;6;7;8</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>mb12</td>
<td>mb10</td>
<td>t11:p</td>
<td>mb11;mb20</td>
<td>t11;t10</td>
<td>1;2;5;7</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>mb13</td>
<td>mb15</td>
<td>t13:p</td>
<td>mb14;mb21</td>
<td>t13;t14</td>
<td>1;5;6;7</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>mb14</td>
<td>mb12</td>
<td>t11;m;t13:p</td>
<td>mb13;mb21</td>
<td>t13;t12</td>
<td>1;3;4;6;8</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>mb14</td>
<td>mb20</td>
<td>t11;p;t13:m</td>
<td>mb13;mb21</td>
<td>t13;t20</td>
<td>2;4;5;7;8</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>mb20</td>
<td>mb10</td>
<td>t11:m</td>
<td>mb11;mb12</td>
<td>t11;t10</td>
<td>1;2;3;6</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>mb21</td>
<td>mb15</td>
<td>t13:m</td>
<td>mb13;mb14</td>
<td>t13;t14</td>
<td>2;4;5;6</td>
<td></td>
</tr>
</tbody>
</table>
Sequential Release

- Incrementally releasing route portions that have been traversed by the associated train → concurrency level ↑ → train throughput ↑

E.g.: t11 can be released as soon as the train has passed it while traveling on route 1, then t11 can be used to set route 7

<table>
<thead>
<tr>
<th>ID</th>
<th>src</th>
<th>dest</th>
<th>overlaps</th>
<th>points</th>
<th>signals</th>
<th>path</th>
<th>conflicts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mb11</td>
<td>mb13</td>
<td>t11:p; t13:m</td>
<td>mb12; mb20</td>
<td>t11;t12</td>
<td>2;3;4;5;7</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>mb20</td>
<td>mb10</td>
<td>t11:m</td>
<td>mb11; mb12</td>
<td>t11;t10</td>
<td>1;2;3;6</td>
<td></td>
</tr>
</tbody>
</table>
Agenda

1. Background

2. Case Study

3. Toolchain and Model

4. Verification Technique

5. Conclusion
**Toolchain Overview**

- **Reconfigurable model:**
  - Configuration data of interlocking systems (network + interlocking table)
  - Generic behavioral model and safety properties which can be instantiated with the configuration data
- **2-step verification and validation (V&V)**
  - Validate configuration data by the static checker
  - Verify safety properties for model instances: bounded model checking (BMC) + inductive reasoning
- **Types of identified errors**
  - Errors in the configuration data
  - Errors in the design of interlocking protocol
- **Implemented as a tool-chain using RT-Tester toolbox and SONOLAR SMT solver**

---

3 AG BS, University of Bremen, Germany
Generic Behavioral Model and Properties

1. Generic behavioral model consists of
   - Interlocking controller
   - Its environment: point switching, train movements
   \[ \text{→ (instantiated with configuration data) → model instance - a Kripke structure } K \]
   \[ r : Route \cdot r.MODE = FREE \land r.MODE' = MARKED \]
   instantiated \[ r = r_1 \ldots r_4 \]
   \[ (r_1.MODE = FREE \land r_1.MODE' = MARKED) \lor \]
   \[ (r_2.MODE = FREE \land r_2.MODE' = MARKED) \lor \]
   \[ (r_3.MODE = FREE \land r_3.MODE' = MARKED) \lor \]
   \[ (r_4.MODE = FREE \land r_4.MODE' = MARKED) \]

2. Generic safety properties: no collisions, no derailments
   \[ \text{→ (instantiated) → concrete safety properties - state invariants over variables} \]
   \[ \text{representing vacancy status of sections} \]
High-level Safety Properties

• Formulated as a state invariant $\phi$ over variables representing vacancy status of sections

• $\phi$: free of hazardous situations

\[ \phi \equiv (\bigwedge_{l: Linear} \neg Hazard_l) \land (\bigwedge_{p: Point} \neg Hazard_p) \quad (1) \]

• Hazards:
  
  (a) Head to head collision
  (b) Trains follow others collision
  (c) Derailment on points

- (a) Head to head
- (b) Trains follow others
- (c) Derailment

• Proof obligation: Prove $K \models G(\phi)$, where $K$ is the behavioral model instance
Verification Strategy

- **Strategy**: combine bounded model checking (BMC) with inductive reasoning
- To prove $K \models G(\phi)$:
  - Prove base case: $\phi$ holds for $k$ consecutive states starting from the initial state
  - Prove induction step: if $\phi$ holds for $k$ consecutive states starting from an arbitrary state, then $\phi$ will hold in the $(k + 1)^{th}$ state.
- Base case and induction step are proved using a SMT-based model checker
- $\phi$ not always inductive $\rightarrow$ spurious counter-examples
  $\rightarrow$ strengthening invariant $\psi$: prove $K \models G(\phi \land \psi)$ instead of $K \not\models G(\phi)$
Strengthening Invariant Example

• *Train movement model:* distinguishes situations where the head and/or tail of the train occupy the section

  ![Diagram of train movement model](image)

  \[ \text{t}_1 \quad \text{t}_2 \quad \text{t}_3 \quad \text{t}_4 \]

  \[ \rightarrow \]

→ *Strengthening invariant for train integrity:* if the *head* but not the *tail* of a train is in the *current* section, then we should find the *tail* in one of the *previous sections* (before we find another head or vacant section)

  ![Diagram of train integrity](image)

  (a) × Spurious  \[ \rightarrow \]  (b) ✓ Train integrity
Experimental Results

- Verified the models of interlocking systems controlling networks of realistic size, e.g. Køge st. in Denmark
- Identified errors (if there are any) quickly in the generic behavioral model or configuration data of interlocking systems

<table>
<thead>
<tr>
<th>Case</th>
<th>Lines</th>
<th>Points</th>
<th>Signals</th>
<th>Routes</th>
<th>BR</th>
<th>Vars</th>
<th>Time/sec</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toy</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>6</td>
<td>0.33</td>
<td>35</td>
<td>9</td>
<td>51 MB</td>
</tr>
<tr>
<td>Cross</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>10</td>
<td>0.50</td>
<td>56</td>
<td>64</td>
<td>127 MB</td>
</tr>
<tr>
<td>Mini</td>
<td>4</td>
<td>2</td>
<td>8</td>
<td>12</td>
<td>0.50</td>
<td>58</td>
<td>76</td>
<td>128 MB</td>
</tr>
<tr>
<td>Gt-Hd</td>
<td>18</td>
<td>5</td>
<td>21</td>
<td>30</td>
<td>0.28</td>
<td>179</td>
<td>1826</td>
<td>1171 MB</td>
</tr>
<tr>
<td>Køge</td>
<td>46</td>
<td>23</td>
<td>49</td>
<td>59</td>
<td>0.50</td>
<td>502</td>
<td>33627</td>
<td>4788 MB</td>
</tr>
</tbody>
</table>

- How is it useful?
  - Major number of network fractions in Denmark are smaller than Køge
  - Complex fractions, e.g. central station, can be decomposed into smaller ones, e.g. see Covering Abstraction
  - Automated, gives higher level of confidence than manual verification

---

Conclusion

- Formal model of the forthcoming Danish interlocking systems
  - ETCS Level 2 compatible: *virtual signal* concept → handle assignment of movement authorities in the similar way as physical signals are used
  - Accommodate sequential release → more complex model

- *Pushed the applicability bounds* of FM in verifying interlocking systems further by
  - Encodings of state space, transition relation, and safety properties → can be efficiently evaluated by SMT solvers
  - Verification technique of combining BMC and inductive reasoning

- Implemented the toolchain and verified successfully the configuration data of interlocking systems controlling networks of realistic size.

Thank you for your attention!