Verification of multiple models of a safety-critical motor controller in railway systems

José Proença (ISEP), Sina Borrami (Alstom), Jorge Sanchez de Nova (Alstom), David Pereira (ISEP), Giann Nandi (ISEP)

1 June 2022

Public
Verification of a motor controller in signalling systems

Dashboard \(\rightarrow\) commands \(\rightarrow\) status \(\leftarrow\) Circuit

Controller

Development team

Verification team

ALSTOM

ISEP
Verification of a motor controller in signalling systems

- Dashboard
- Controller
- Circuit

- Check HW
- Self Test
- Idle
- Ready
- Left
- Right
- Fall-back

- commands
- status
- commands
- status
Overview of this talk

1. Model **behaviour** in UPPAAL model checker

2. Specify **requirements** (temporal formula)

3. Configure **instances** of the models and requirements in Excel

4. Verify **all** instances and **all** requirements in one go

Verification of multiple models of a safety-critical motor controller in railway systems
The Controller

Model-checker of
Real-time properties

Verification of multiple models of a safety-critical motor controller in railway systems
Component architecture

16x Automata
Verification of multiple models of a safety-critical motor controller in railway systems
Model = Requirements + Network of Automata

<table>
<thead>
<tr>
<th>Config.</th>
<th>State</th>
<th>Trigger</th>
<th>Comp.</th>
<th>Expected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conf₁</td>
<td>controller₁ is ready</td>
<td>decoder receives a left command</td>
<td>controller₁</td>
<td>send a left command within 100ms</td>
</tr>
<tr>
<td>Conf₂</td>
<td></td>
<td>monitor₁ or reader₁ fail</td>
<td>controller₂</td>
<td>go to a fallback state within 100ms</td>
</tr>
<tr>
<td>Conf₃</td>
<td></td>
<td>controller₁ fails</td>
<td>controller₂</td>
<td>go to a fallback state within 100ms</td>
</tr>
<tr>
<td>Conf₄</td>
<td></td>
<td>controller₁ receives an error message</td>
<td>controller₁</td>
<td>send immediately a stop command to the circuit</td>
</tr>
<tr>
<td>Conf₅</td>
<td>dashboard can send messages</td>
<td>controller₁ receives an error message</td>
<td>encoder₁</td>
<td>notify the dashboard within 100ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>full system</td>
<td>full system</td>
<td>never get stuck</td>
</tr>
</tbody>
</table>

Verification of multiple models of a safety-critical motor controller in railway systems
Examples of Configurations

**Configuration 1**
- The motor takes exactly 4.5s to move left or right (OK)
- The dashboard starts at 2s, asks to move left at 5s, and asks to move right at 10s
- No fault is injected

**Configuration 2**
- The motor takes 6s to move left (not OK)
- (rest as Conf. 1)

**Configuration 3**
- The monitor1 components becomes faulty after 5s
- Buffer is smaller
- Heartbeats are off
- (rest as Conf 1.)
Uppex: Challenges and Workflow

- Large model that can be refined
- Variability (unfixed parameters)

- Understanding & Maintenance
- Developers + Modellers

https://cister-labs.github.io/uppex
Demo: A look into the configurations

<table>
<thead>
<tr>
<th>Name</th>
<th>Min-1</th>
<th>Min-2</th>
<th>Max-1</th>
<th>Max-2</th>
<th>Control: time to run</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>50</td>
<td>50</td>
<td>70</td>
<td>70</td>
<td>control: time</td>
<td></td>
</tr>
<tr>
<td>Check</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>control: max</td>
<td></td>
</tr>
<tr>
<td>SelfTest</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>200</td>
<td>time to run: Self</td>
<td></td>
</tr>
<tr>
<td>SelfTest</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>200</td>
<td>time to run: Self</td>
<td></td>
</tr>
</tbody>
</table>

@Global @Local @TimeBounds @Configurations @Scenarios

Formula: A[] (not deadlock) || Dash.StopSce ChckDeadlock Monitor1fails Controller1 is ready

Dashboard can send

Decoder receives a GOLEFT

Circuit

Monitor1 fails Controller2

Mon1.Fails --> (Ct2.FallBack && Mc FailMon10

@Configurations @Scenarios <queries> @Global @Local @TimeBounds @DataT

Verification of multiple models of a safety-critical motor controller in railway systems

1 June 2022
Wrap up

1. **Annotate** Uppaal model

2. **Configure** annotations in Excel

3. **Intantiate & Verify** many configurations

Development team  Verification team

1 June 2022

Verification of multiple models of a safety-critical motor controller in railway systems
Verification and Validation of Automated Systems’ Safety and Security

www.valu3s.eu

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876852. The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey.

Disclaimer: The ECSEL JU and the European Commission are not responsible for the content on this presentation or any use that may be made of the information it contains.