Formal Verification of Train Control with Air Pressure Brakes

Stefan Mitsch¹  Marco Gario²  Christof J. Budnik²  Michael Golm²  André Platzer¹

¹Computer Science Department, Carnegie Mellon University
²Siemens Corporate Technology, Princeton, NJ, USA

Reliability, Safety and Security of Railway Systems
November 15, 2017
Railroad Safety: Train Separation and Train Control

Train separation requires verified train control and motion!

Federal Railroad Administration (FRA): motion and brake models

But underspecified control conditions

Safe train separation requires verified train control and motion!
Train separation and train control require verified train control and motion.
Railroad Safety: Train Separation and Train Control

Movement authority

Train separation

Interlocking

Safe train separation requires verified train control and motion!
Interlocking

Movement authority

Train separation

Train control requires verified train control and motion!

Federal Railroad Administration (FRA): motion and brake models

No overshoot

Limited undershoot

But underspecified control conditions

Approach Safe train separation requires verified train control and motion!
Train control requires! Train separation

Interlocking

Federal Railroad Administration (FRA): motion and brake models

No overshoot
Limited undershoot

But underspecified control conditions

Safe train separation requires verified train control and motion!
Design **provably safe train control** considering physical train motion

Federal Railroad Administration (FRA): motion and brake models

No overshoot

Limited undershoot
Design **provably safe train control** considering physical train motion

Federal Railroad Administration (FRA): motion and brake models

No overshoot

Limited undershoot

**But underspecified control conditions**
Safe train separation requires verified train control and motion!

Design provably safe train control considering physical train motion.

Federal Railroad Administration (FRA): motion and brake models.

No overshoot.

Limited undershoot.

But underspecified control conditions.
Approach: Hybrid Systems Theorem Proving

Analyze the physical effect of software

Hybrid System
Model
KeYmaera X
Control
Conditions
Proof
Control
Sensors Actuators

Discrete computation + continuous physics
Approach: Hybrid Systems Theorem Proving

Theorem proving ensures correct model

Proof Strategy
Hybrid System
Model
KeYmaera X
Control
Conditions
Proof
Control
Sensors Actuators

Main results for

Certification: Proofs
System architecture and implementation: Models
Control engineering and testing: Control conditions
Train Motion and Brake Model

\[ x' = v, \quad v' = \frac{1}{m}( - (F_g + F_r + F_c) + f_a) \]

\[ f_a' \leq f_a \]

Underspecified:
- What are safe control choices?
- How important is brake model fidelity?

Train Motion and Brake Model

Accelerate

Instant brake

Limited, but almost instant effect

Train Motion and Brake Model

Accelerate Instant brake

Air brake

Brake effect increases, time depends on train length

Accelerate Instant brake

$\dot{v} = \frac{1}{m} \left( \begin{array}{cc} f_a & \end{array} \right)\right)$

Train Motion and Brake Model

\[ v' = \frac{1}{m} \left( -F_{gb} - F_{fr} - F_{rc} + f_a \right) \]

\[ f'_a = j & -F_{pb} \leq f_a \]

Train Motion and Brake Model

\[ v' = \frac{1}{m} \left( - (F_g + F_r + F_c) + f_a \right), \quad f'_a = j \quad \& \quad -F_{pb} \leq f_a \]

Train Motion and Brake Model

\[
x' = v, \quad v' = \frac{1}{m} \left( - (F_g + F_r + F_c) + f_a \right), \quad f'_a = j \land -F_{pb} \leq f_a
\]

Train Motion and Brake Model

\[ x' = v, \quad v' = \frac{1}{m} \left( - (F_g + F_r + F_c) + f_a \right), \quad f'_a = j \land -F_{pb} \leq f_a \]

Underspecified:

- What are safe control choices?
- How important is brake model fidelity?

Train Motion and Brake Model

\[ x' = v, \quad v' = \frac{1}{m} \left( - (F_g + F_r + F_c) + f_a \right) \], \quad f'_a = j \& -F_{pb} \leq f_a

Underspecified:
What are safe control choices?
How important is brake model fidelity?

Control Model

Track Control

![Diagram with SPEED LIMIT 25 and an arrow extending e, d]
Control Model

- **Driver**

- **Track Control**

- **Train Control**

  - \( e, d \)

  - Speed limit 25

  - Extend \( e, d \)

  - \( a \downarrow \quad \downarrow - F_{pb} \)
Control Model

- Driver
- Track Control
  - $e, d$
  - $a$
- Train Control
- Actuators

Delay vs. air brake: $\square$
Control Model

Track Control

Train Control

Actuators

Motion

Driver

Delay vs. air brake

extend $e, d$

$a \downarrow, \downarrow - F_{pb}$

S. Mitsch et al.—Formal Verification of Train Control
Formal Verification with dL: No Overshoot

Correctness property: \textit{respect the speed limit}

\[
safe \equiv (z \geq e \rightarrow v \leq 25)
\]
Correctness property: **respect the speed limit**

\[ \text{safe} \equiv (z \geq e \rightarrow v \leq d) \]
Formal Verification with dL: No Overshoot

Correctness property: **respect the speed limit**

\[
\text{safe} \equiv (z \geq e \to v \leq d)
\]

\[
[\![\text{safe}]\!]
\]
Correctness property: **respect the speed limit**

\[ \text{safe} \equiv (z \geq e \rightarrow v \leq d) \]
Formal Verification with dL: No Overshoot

Correctness property: **respect the speed limit**

\[\text{safe} \equiv (z \geq e \rightarrow v \leq d)\]

\[\left[\left(\begin{array}{c}
\text{SPEED LIMIT} \\
d
\end{array}\right) \cup \left\{\begin{array}{c}
\text{Joystick}
\end{array}\right\} ; \left\{\begin{array}{c}
\text{Brake}
\end{array}\right\} ; \left\{\begin{array}{c}
\text{Train}
\end{array}\right\} \right]^*\text{safe}\]
Correctness property: **respect the speed limit**

\[
safe \equiv (z \geq e \rightarrow v \leq d)
\]

\[
\text{init} \rightarrow \left[ \left( \text{SPEED LIMIT } d \right) \cup \text{\_\_\_}; \text{\_\_\_}; \text{\_\_\_} \right)^* \text{safe}
\]
Formal Verification with $\mathcal{dL}$: No Overshoot

Correctness property: **respect the speed limit**

$$\text{safe} \equiv (z \geq e \rightarrow v \leq d)$$

$$\text{init} \rightarrow \left[ (\text{SPEED LIMIT } d) \cup (\text{STOP}) ; \text{ safe} \right]$$
Correctness property: respect the speed limit

\[
\text{safe } \equiv (z \geq e \rightarrow v \leq d)
\]

\[
\text{init } \rightarrow \left[ \left( \left( \text{d} \right) \cup \left( \text{stop} \right) \right); \right]^{*} \text{safe}
\]

\[
\equiv f_a := *; ? - F_{sb} \leq f_a \leq A; ? \left( e - z \geq \frac{(v^2 - d^2)m}{2F_{sb}} + \left( \frac{A}{F_{sb}} + 1 \right) \left( \frac{A}{2m} \varepsilon^2 + v \varepsilon \right) \right)
\]

\[
\left( \text{slow}^- \lor \text{slow}^+ \lor \text{fast}^- \lor \text{fast}^+ \right)
\]

\[
\text{slow}^- \equiv \neg \text{isFast}(v) \land f_a \leq 0 \land e - z \geq v \varepsilon + m \text{Slow}(v)
\]

\[
\text{slow}^+ \equiv [u := v + \frac{f_a \varepsilon}{m}] \left( \neg \text{isFast}(u) \land f_a \geq 0 \land e - z \geq v \varepsilon + \frac{f_a \varepsilon^2}{2m} + m \text{Slow}(u) \right)
\]

\[
\text{fast}^- \equiv \text{isFast}(v) \land f_a \leq 0 \land e - z \geq v \varepsilon + m \text{Fast}(v)
\]

\[
\text{fast}^+ \equiv \text{isFast}(v) \land f_a \geq 0 \land e - z \geq v \varepsilon + \frac{f_a \varepsilon^2}{2m} + m \text{Fast} \left( v + \frac{f_a \varepsilon}{m} \right)
\]

\[
\text{isFast}(v) \equiv v \geq \frac{F_{pb}^2}{2mJ}
\]

\[
\text{mSlow}(v) = \frac{2}{3} \sqrt{2mv/J}
\]

\[
\text{mFast}(v) = \frac{mv^2}{2F_{pb}} + \frac{vF_{pb}}{2J} - \frac{F_{pb}^3}{24mJ^2}
\]

Result:
Driving with verified control conditions ensures safety

How to find conditions: Proofs!
Correctness property: **respect the speed limit**

\[ \text{safe} \equiv (z \geq e \rightarrow v \leq d) \]

\[ \text{init} \rightarrow \left[ \left( \begin{array}{c} \text{SPEED LIMIT} \; d \\ \cup \end{array} \right) \cup \left( \begin{array}{c} \text{STOP} \\ \cup \end{array} \right) ; \; \left( \begin{array}{c} \text{BAR} \\ \cup \end{array} \right) \right]^* \text{safe} \]

**Result**

**Driving with verified control conditions ensures safety**

**How to find conditions: Proofs!**

\[ \text{slow}^- \equiv \neg \text{isFast}(v) \land f_a \leq 0 \land e - z \geq v\varepsilon + m\text{Slow}(v) \]

\[ \text{slow}^+ \equiv [u := v + \frac{f_a\varepsilon}{m}] \left( \neg \text{isFast}(u) \land f_a \geq 0 \land e - z \geq v\varepsilon + \frac{f_a\varepsilon^2}{2m} + m\text{Slow}(u) \right) \]

\[ \text{fast}^- \equiv \text{isFast}(v) \land f_a \leq 0 \land e - z \geq v\varepsilon + m\text{Fast}(v) \]

\[ \text{fast}^+ \equiv \text{isFast}(v) \land f_a \geq 0 \land e - z \geq v\varepsilon + \frac{f_a\varepsilon^2}{2m} + m\text{Fast} \left( v + \frac{f_a\varepsilon}{m} \right) \]

\[ \text{isFast}(v) \equiv v \geq \frac{F_{pb}^2}{2mJ} \]

\[ m\text{Slow}(v) = \frac{2}{3} \sqrt{2mv/J} \]

\[ m\text{Fast}(v) = \frac{mv^2}{2F_{pb}} + \frac{vF_{pb}}{2J} - \frac{F_{pb}^3}{24mJ^2} \]
Partial model, unknown condition $\mathbf{?true}$

\[
\begin{array}{c}
\text{\includegraphics[width=1cm]{person}} ; \ \mathbf{?true} ; \ \text{\includegraphics[width=1cm]{train}} \ \mathbf{safe}
\end{array}
\]
Systematically Derive Safe Control Conditions in dL

Partial model, unknown condition ?true

\[
\begin{array}{c}
\text{安全} \\
\end{array}
\]

Run and observe “parallel universe”

\[
\begin{array}{c}
\text{安全} \\
\end{array}
\]

test for desired outcome

↓ copy & paste

\[
\begin{array}{c}
\text{安全} \\
\end{array}
\]

\[
\begin{array}{c}
\text{安全} \\
\end{array}
\]
Partial model, unknown condition \(?\text{true}\)
\[
\begin{array}{c}
\text{safe} \\
\text{test for desired outcome}
\end{array}
\]

Run and observe “parallel universe”
\[
\begin{array}{c}
\text{safe} \\
\text{safe}
\end{array}
\]

Obviously true but not helpful for implementation
\[
\begin{array}{c}
\text{safe} \\
\text{safe}
\end{array}
\]

Result

Augment partial model with implementable control conditions derived by proof
Partial model, unknown condition \(?\text{true}\)

\[
\begin{array}{c}
\text{safe} \\
\end{array}
\]

Run and observe “parallel universe”

\[
\begin{array}{c}
\text{safe} \\
\end{array}
\]

test for desired outcome

Obviously true but not helpful for implementation

\[
\begin{array}{c}
\text{safe} \\
\end{array}
\]

Symbolically execute program with \(d\mathcal{L}\)

\[
\begin{array}{c}
\text{safe}(z + vt + \frac{f_a}{2m} t^2, v + \frac{f_a}{m} t) \rightarrow [\text{safe}] \\
\end{array}
\]
Partial model, unknown condition \(?\text{true}\)

\[
[ \text{不出} \; ; \; ?\text{true} ; \; \text{车} ] \text{safe}
\]

Run and observe “parallel universe”

\[
[ \text{不出} \; ; \; ?[\text{车}] \text{safe} ; \; \text{车} ] \text{safe}
\]

test for desired outcome

Obviously true but not helpful for implementation

\[
[ \text{不出} ] ( ?[\text{车}] \text{safe} \rightarrow [\text{车}] \text{safe} )
\]

Symbolically execute program with dL

\[
[ \text{不出} ] ( \text{safe}(z + vt + \frac{f_a}{2m} t^2, v + \frac{f_a}{m} t) \rightarrow [\text{车}] \text{safe} )
\]

Use program effects as control conditions

\[
[ \text{不出} \; ; \; ?\text{safe}(z + vt + \frac{f_a}{2m} t^2, v + \frac{f_a}{m} t) ; \; \text{车} ] \text{safe}
\]

Implementable
Systematically Derive Safe Control Conditions in $d\mathcal{L}$

Partial model, unknown condition $\text{true}$

\[
\text{safe} \quad \left[ \begin{array}{c}
\text{true} ; \\
\end{array} \right]
\]

Run and observe “parallel universe”

\[
\text{safe} \quad \left[ \begin{array}{c}
\text{true} ; \\
\end{array} \right]
\]

Result

Augment partial model with implementable control conditions derived by proof

\[
\left( \text{safe}(z + vt + \frac{fa}{2m} t^2, v + \frac{fa}{m} t) \rightarrow \left[ \begin{array}{c}
\text{true} ; \\
\end{array} \right] \text{safe} \right)
\]

Use program effects as control conditions

\[
\left[ \begin{array}{c}
\text{true} ; \\
\end{array} \right] \text{safe}(z + vt + \frac{fa}{2m} t^2, v + \frac{fa}{m} t) \quad \left[ \begin{array}{c}
\text{true} ; \\
\end{array} \right] \text{safe}
\]

Implementable
Proof guarantees correct model

**Proof Strategy**

**Hybrid System**

**Model**

KeYmaera X

**Control**

**Conditions**

Proof

Sensors

Actuators

---

No overshoot ✓

Verified models: safely control brake delay and air brakes

Symbolic control conditions to select between free driving and braking
No overshoot ✓ + Limited undershoot

Verified models: safely control brake delay and air brakes
Symbolic control conditions to select between free driving and braking
Correctness: when done braking, train is after undershoot limit

\[
\text{efficient} \equiv (\text{brakesEngaged} \land v \leq d) \rightarrow (z \geq e - u)
\]
Correctness: **when done braking, train is after undershoot limit**

\[
\text{efficient} \equiv (\text{brakesEngaged} \land v \leq d) \rightarrow (z \geq e - u)
\]

Needs change in control priority

No overshoot: braking allowed but spoils efficiency

\[
\text{init} \rightarrow \left[ \left( (\text{\text{\text{\footnotesize \text{person}}} \cup \text{\text{\text{\footnotesize \text{stop}}}}) ; \text{\text{\text{\footnotesize \text{line}}}} ; \text{\text{\text{\footnotesize \text{train}}}} \right)^* \right] \text{efficient}
\]
Correctness: **when done braking, train is after undershoot limit**

$$\text{efficient} \equiv (\text{brakesEngaged} \land v \leq d) \rightarrow (z \geq e - u)$$

Needs change in control priority

No overshoot: braking allowed but spoils efficiency

Limited undershoot: only brake if necessary for safety

$$\text{init} \rightarrow \left[ \left( \text{(if (mustBrake)\ding{55} else \ding{53}) ; \align ; \ding{53} \right) \right]^* \text{efficient}$$
No overshoot ✓ + Limited undershoot ✓

Verified models: safely control brake delay and air brakes
Symbolic control conditions to select between free driving and braking
Control favors free driving for efficiency
Experiments

Compare brake engage distance to endpoint control assuming delayed brakes control assuming air brakes

Instantiate symbolic models with concrete parameters from FRA

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>vs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$l_z$</td>
<td>Length Medium = 2 345ft (40 cars)</td>
<td>short, long</td>
</tr>
<tr>
<td>$m$</td>
<td>Mass Loaded = 10 520klb (263klb/car)</td>
<td>empty</td>
</tr>
<tr>
<td>$v$</td>
<td>Speed Fast = 60mph</td>
<td>slow</td>
</tr>
<tr>
<td>$F_{pb}$</td>
<td>Emergency brake Loaded = 1 430klbf (35 750lbf/car)</td>
<td>empty, unknown</td>
</tr>
<tr>
<td>$t_{appl}$</td>
<td>Time 50 s</td>
<td>length-dependent</td>
</tr>
<tr>
<td>$A$</td>
<td>Acceleration $5 \frac{mph}{min} = 391.91$klbf</td>
<td></td>
</tr>
<tr>
<td>$f_a$</td>
<td>Brake force $1.75 \frac{mph}{min} = 136.76$klbf</td>
<td></td>
</tr>
<tr>
<td>$\varepsilon$</td>
<td>Control cycle 100ms</td>
<td></td>
</tr>
</tbody>
</table>

### Experimental Results: Brake Engage Points

<table>
<thead>
<tr>
<th>Cars</th>
<th>Slow</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Loaded</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Empty</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td><strong>Brake force for unknown load</strong> $F_{pb} = 23,338$ lbf&lt;sub&gt;car&lt;/sub&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>726</td>
<td>1,110</td>
<td>1,942</td>
</tr>
<tr>
<td>Air brakes</td>
<td>541</td>
<td>710</td>
<td>1,017</td>
</tr>
<tr>
<td>Difference</td>
<td>185</td>
<td>400</td>
<td>925</td>
</tr>
<tr>
<td><strong>Brake force for known load, loaded</strong>: $F_{pb} = 35,750$ lbf&lt;sub&gt;car&lt;/sub&gt;, empty: $F_{pb} = 10,575$ lbf&lt;sub&gt;car&lt;/sub&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>597</td>
<td>982</td>
<td>1,814</td>
</tr>
<tr>
<td>Air brakes</td>
<td>409</td>
<td>565</td>
<td>822</td>
</tr>
<tr>
<td>Difference</td>
<td>188</td>
<td>417</td>
<td>992</td>
</tr>
<tr>
<td><strong>Brake force for known load, loaded</strong>: $F_{pb} = 35,750$ lbf&lt;sub&gt;car&lt;/sub&gt;, empty: $F_{pb} = 10,575$ lbf&lt;sub&gt;car&lt;/sub&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>597</td>
<td>982</td>
<td>1,814</td>
</tr>
<tr>
<td>Air brakes</td>
<td>409</td>
<td>565</td>
<td>822</td>
</tr>
<tr>
<td>Difference</td>
<td>188</td>
<td>417</td>
<td>992</td>
</tr>
</tbody>
</table>

**Delay brakes** delay times:
- Slow: 726, 1,110, 1,942, 446, 830, 1,662 lbf<sub>car</sub>
- Fast: 15,436, 17,742, 22,730, 5,369, 7,676, 12,664 lbf<sub>car</sub>

**Air brakes** delay times:
- Slow: 541, 710, 1,017, 239, 345, 503 lbf<sub>car</sub>
- Fast: 14,364, 15,494, 17,880, 4,278, 5,334, 7,383 lbf<sub>car</sub>

**Difference** delay times:
- Slow: 185, 400, 925, 207, 485, 1,161 lbf<sub>car</sub>
- Fast: 1,072, 2,248, 4,850, 1,091, 2,342, 5,281 lbf<sub>car</sub>
### Experimental Results: Brake Engage Points

<table>
<thead>
<tr>
<th></th>
<th>Slow</th>
<th>Loaded</th>
<th>Empty</th>
<th>Fast</th>
<th>Loaded</th>
<th>Empty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cars</td>
<td>10</td>
<td>40</td>
<td>100</td>
<td>10</td>
<td>40</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>726</td>
<td>1,110</td>
<td>1,942</td>
<td>446</td>
<td>830</td>
<td>1,662</td>
</tr>
<tr>
<td>Air brakes</td>
<td>541</td>
<td>710</td>
<td>1,017</td>
<td>239</td>
<td>345</td>
<td>503</td>
</tr>
<tr>
<td>Difference</td>
<td>185</td>
<td>400</td>
<td>925</td>
<td>207</td>
<td>485</td>
<td>1,161</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brake force for unknown load ( F_{pb} = 23,338 \text{ lbf} )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>15,436</td>
<td>17,742</td>
<td>22,730</td>
<td>5,369</td>
<td>7,676</td>
<td>12,664</td>
</tr>
<tr>
<td>Air brakes</td>
<td>14,364</td>
<td>15,494</td>
<td>17,880</td>
<td>4,278</td>
<td>5,334</td>
<td>7,383</td>
</tr>
<tr>
<td>Difference</td>
<td>1,072</td>
<td>2,248</td>
<td>4,850</td>
<td>1,091</td>
<td>2,342</td>
<td>5,281</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brake force for known load, loaded: ( F_{pb} = 35,750 \text{ lbf} )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>10,817</td>
<td>13,123</td>
<td>18,111</td>
<td>9,277</td>
<td>11,583</td>
<td>16,571</td>
</tr>
<tr>
<td>Air brakes</td>
<td>9,743</td>
<td>10,859</td>
<td>13,188</td>
<td>8,200</td>
<td>9,309</td>
<td>11,602</td>
</tr>
<tr>
<td>Difference</td>
<td>1,074</td>
<td>2,264</td>
<td>4,923</td>
<td>1,077</td>
<td>2,274</td>
<td>4,969</td>
</tr>
</tbody>
</table>
Experimental Results: Brake Engage Points

Air brake control conditions engage brakes considerably later

### Fast trains

<table>
<thead>
<tr>
<th>Cars</th>
<th>Loaded</th>
<th>Empty</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>Brake force for known load, loaded: $F_{pb} = 35\ 750\ \text{lbf}\text{car}^{-1}$, empty: $F_{pb} = 10\ 575\ \text{lbf}\text{car}^{-1}$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delay brakes</td>
<td>10,817</td>
<td>13,123</td>
</tr>
<tr>
<td>Air brakes</td>
<td>9,743</td>
<td>10,859</td>
</tr>
<tr>
<td>Difference</td>
<td>1,074</td>
<td>2,264</td>
</tr>
</tbody>
</table>

Difference exceeds FRA requirement of at most 1000ft undershoot!
Theorem proving ensures correct model

Proof guarantees correct model

Proof Strategy
Hybrid System
Model
KeYmaera X
Code
Control
Conditions
Proof
Control
Sensors Actuators Sensors
Control
Monitor
Actuators

No overshoot ✓ + Limited undershoot ✓

Proofs for certification
Models and code for system architecture and implementation
Control conditions for runtime monitoring and testing
Transfer safety of model to controller implementation

Monitor desired effect + safe environment

ModelPlex synthesizes and proves monitors for model compliance

Runtime: ensure safety and detect anomalies

Testing: generate and analyze test cases

www.keymaeraX.org

Stefan Mitsch
Computer Science Department, Carnegie Mellon University
smitsch@cs.cmu.edu