15-819/18-879: Logical Analysis of Hybrid Systems
18: European Train Control System Verification

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA
Outline

1 Train Control
   - Separation Principle
   - Parametric ETCS

2 Parametric European Train Control System
   - Controllability
   - Reactivity
   - Refined Control
   - Safety
   - Liveness

3 Enhancements

4 Summary
Outline

1 Train Control
   • Separation Principle
   • Parametric ETCS

2 Parametric European Train Control System
   • Controllability
   • Reactivity
   • Refined Control
   • Safety
   • Liveness

3 Enhancements

4 Summary
Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid Systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

More than computers: no NullPointerException ⇒ safe

Joint dynamics requires:
$$SB \geq \frac{v^2}{2} \leq 2b(m-z) \neq safe$$
Hybrid Systems Analysis: Train Control

**Challenge**

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers:

   no NullPointerException ⇒ safe

2. More than physics:

   braking control \( v^2 \leq 2b(m - z) \) ⇒ safe
Hybrid Systems Analysis: Train Control

**Challenge**

Hybrid Systems
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

1. More than computers: no NullPointerException ⇒ safe
2. More than physics: braking control $v^2 \leq 2b(m - z) \not\Rightarrow$ safe
3. Joint dynamics requires:

$$SB \geq \frac{v^2}{2b} + \frac{a^2 \varepsilon^2}{2b} + \frac{a}{b} \varepsilon v + \frac{a}{2} \varepsilon^2 + \varepsilon v \ldots$$
Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Challenge

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)
Hybrid Systems Analysis: Train Control

**Challenge**

Hybrid Systems

- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

\[
SB \geq \frac{v^2}{2b} + \frac{a^2 \varepsilon^2}{2b} + \frac{a}{b} \varepsilon v + \frac{a}{2} \varepsilon^2 + \varepsilon v
\]
Objectives

1. Collision free
2. Maximise throughput & velocity (300 km/h)
3. $2.1 \times 10^6$ passengers/day

Overview

1. No static partitioning of track
2. Radio Block Controller (RBC) manages movement authorities dynamically
3. Moving block principle
Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

∀ \( m.e \) \exists \( SB \) “train always safe”
Parametric Hybrid Systems

continuous evolution along differential equations + discrete change
Parametric Hybrid Systems

continuous evolution along differential equations + discrete change
Example

Precondition \[ \tau.p \] \[ \begin{matrix} \rightarrow \\ \tau.V \end{matrix} \] Operation model \[ m.e \] Property
Example

\[ \tau.v^2 \leq 2b(m.e - \tau.p) \rightarrow [ (\tau.p \leq m.e) ] \]

Precondition: \( \tau.v^2 \leq 2b(m.e - \tau.p) \)

Operation model: \[ (\tau.p \leq m.e) \]

Property: \( \tau.p \leq m.e \)
Example

\[ \tau.v^2 \leq 2b(m.e - \tau.p) \rightarrow [\tau.p' = \tau.v, \tau.v' = \tau.a, (\tau.p \leq m.e)] \]

Precondition

Operation model

Property

Continuous evolution: differential equation
Differential Dynamic Logic (dL)

Example

\[
\tau.v^2 \leq 2b(m.e - \tau.p) \rightarrow [\tau.a := \ast; \tau.p' = \tau.v, \tau.v' = \tau.a](\tau.p \leq m.e)
\]

Precondition

Operation model

Property

Random assignment
Differential Dynamic Logic (dL)

Example

\[ \tau.v^2 \leq 2b(m.e - \tau.p) \rightarrow [\tau.a := *; \ ?\tau.a \leq -b; \ \tau.p' = \tau.v, \tau.v' = \tau.a](\tau.p \leq m.e) \]

- **Precondition**

- **Operation model**

- **Property**

**Test**
Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep recommended speed $\mathbf{m}.r$.
Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}_e$ train not faster than $\mathbf{m}_d$.
- Train should try to keep recommended speed $\mathbf{m}_r$
Vectorial MA $\mathbf{m} = (d, e, r)$:

- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep recommended speed $\mathbf{m}.r$.
Vectorial MA $\mathbf{m} = (d, e, r)$:

- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$
Vectorial MA $m = (d, e, r)$:

- Beyond point $m.e$ train not faster than $m.d$.
- Train should try to keep recommended speed $m.r$.
Vectorial MA $m = (d, e, r)$:
- Beyond point $m.e$ train not faster than $m.d$.
- Train should try to keep *recommended speed* $m.r$.
Vectorial MA $\mathbf{m} = (d, e, r)$:

- Beyond point $\mathbf{m.e}$ train not faster than $\mathbf{m.d}$.
- Train should try to keep recommended speed $\mathbf{m.r}$
Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities

\( \Rightarrow \) trains can never collide.
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities

\[ \Rightarrow \text{trains can never collide.} \]

Proof.

To simplify notation, assume trains are points. Consider any point in time \( \zeta \).

For \( n \in \mathbb{N} \), let \( z_1, \ldots, z_n \) be positions of all the trains 1 to \( n \) at \( \zeta \).

Let \( M_i \) be the MA-range, i.e., the set of positions on the track for which train \( i \) has currently been issued MA.

Suppose there was a collision at time \( \zeta \).

Then \( z_i = z_j \) at \( \zeta \) for some \( i, j \in \mathbb{N} \).

However, by assumption, \( z_i \in M_i \) and \( z_j \in M_j \) at \( \zeta \), thus \( M_i \cap M_j \neq \emptyset \),

This contradicts the assumption of disjoint MA.

André Platzer (CMU)
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities $\Rightarrow$ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities
⇒ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time $\zeta$. 
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities

⇒ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time $\zeta$.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to $n$ at $\zeta$. 
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities
\[ \Rightarrow \text{trains can never collide.} \]

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time \( \zeta \).
- For \( n \in \mathbb{N} \), let \( z_1, \ldots, z_n \) be positions of all the trains 1 to \( n \) at \( \zeta \).
- Let \( M_i \) be the MA-range, i.e., the set of positions on the track for which train \( i \) has currently been issued MA.
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities
⇒ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time $\zeta$.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to $n$ at $\zeta$.
- Let $M_i$ be the MA-range, i.e., the set of positions on the track for which train $i$ has currently been issued MA.
- Suppose there was a collision at time $\zeta$. 
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities

⇒ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time $\zeta$.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to $n$ at $\zeta$.
- Let $M_i$ be the MA-range, i.e., the set of positions on the track for which train $i$ has currently been issued MA.
- Suppose there was a collision at time $\zeta$.
- Then $z_i = z_j$ at $\zeta$ for some $i, j \in \mathbb{N}$. 
Separation Principle

Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities
⇒ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time $\zeta$.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to $n$ at $\zeta$.
- Let $M_i$ be the MA-range, i.e., the set of positions on the track for which train $i$ has currently been issued MA.
- Suppose there was a collision at time $\zeta$.
- Then $z_i = z_j$ at $\zeta$ for some $i, j \in \mathbb{N}$.
- However, by assumption, $z_i \in M_i$ and $z_j \in M_j$ at $\zeta$, thus $M_i \cap M_j \neq \emptyset$. 
Lemma (Principle of separation by movement authorities)

Each train respects its movement authority and the RBC partitions into disjoint movement authorities

⇒ trains can never collide.

Proof.

- To simplify notation, assume trains are points.
- Consider any point in time $\zeta$.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to $n$ at $\zeta$.
- Let $M_i$ be the MA-range, i.e., the set of positions on the track for which train $i$ has currently been issued MA.
- Suppose there was a collision at time $\zeta$.
- Then $z_i = z_j$ at $\zeta$ for some $i, j \in \mathbb{N}$.
- However, by assumption, $z_i \in M_i$ and $z_j \in M_j$ at $\zeta$, thus $M_i \cap M_j \neq \emptyset$.
- This contradicts the assumption of disjoint MA.
Model/State Variables

Train $\tau$:
- $\tau.v$ Position
- $\tau.v$ Speed
- $\tau.a$ Acceleration
- $(t\ \text{model time})$

RBC + MA:
- $m.e$ End of Authority
- $m.d$ Speed limit
- $m.r$ Recommended speed
- $rbc.message$ Channel

Parameters:
- $SB$ Start Braking
- $ST$ Start Talking
- $b$ Braking power/deceleration
- $a$ Maximum acceleration
- $\varepsilon$ Maximum cycle time
- $\Delta$ Maximum expected communication delay
Parametric Skeleton of ETCS

Read from the informal specification...

\[ ETCS_{skel} : (train \cup rbc)^* \]

\[ train : spd; atp; drive \]

\[ spd : \begin{align*}
& (\tau. v \leq m.r; \tau.a := \ast; \ ? - b \leq \tau.a \leq a) \\
& \cup (\tau. v \geq m.r; \tau.a := \ast; \ ? - b \leq \tau.a \leq 0)
\end{align*} \]

\[ atp : \text{if}(m.e - \tau.p \leq SB \lor rbc.message = \text{emergency}) \tau.a := -b \]

\[ drive : t := 0; (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \land \tau.v \geq 0 \land t \leq \varepsilon) \]

\[ rbc : (rbc.message := \text{emergency}) \cup (m := \ast; \ ?m.r > 0) \]
Parametric Skeleton of ETCS

As transition system...

\[ m_0 := m \quad m := * \]

\[ rbc.message := \text{emergency} \]

\[ t := 0 \]

\[ \tau.p' = \tau.v, \quad \tau.v' = \tau.a, t' = 1 \]

\[ \tau.v \geq 0 \land t \leq \varepsilon \]

\[ \tau.a := -b \]

\[ ?(m.e - \tau.p \leq SB \lor rbc.message = \text{emergency}) \]

\[ ?m.e - \tau.p \geq SB \land rbc.message \neq \text{emergency} \]

Example (Taks)
Verify safety
Specification \[ \text{ETCS skel} \]

\[ \tau.p \geq m.e \rightarrow \tau.v \leq m.d \]

Issue
Lots of counterexamples!
Parametric Skeleton of ETCS

\[ ETCS_{skel} : (\text{train} \cup \text{rbc})^* \]

\text{train} : \text{spd}; \text{atp}; \text{drive}

\text{spd} : (\omega \text{.} v \leq m.r; \omega \text{.} a := \star; \omega - b \leq \omega \text{.} a \leq a)
\quad \cup (\omega \text{.} v \geq m.r; \omega \text{.} a := \star; \omega - b \leq \omega \text{.} a \leq 0)

\text{atp} : \text{if}(m.e - \omega \text{.} p \leq SB \lor \text{rbc.message} = \text{emergency}) \omega \text{.} a := -b

\text{drive} : t := 0; (\omega \text{.} p' = \omega \text{.} v, \omega \text{.} v' = \omega \text{.} a, t' = 1 \land \omega \text{.} v \geq 0 \land t \leq \varepsilon)

\text{rbc} : (\text{rbc.message} := \text{emergency}) \cup (m := \star; ?m.r > 0)

Example (Taks)

Verify safety
Parametric Skeleton of ETCS

\[ ETCS_{skel} : (\text{train} \cup \text{rbc})^* \]

- **train**: \( \text{spd}; \ \text{atp}; \ \text{drive} \)
- **spd**: \( (?\tau.v \leq m.r; \ \tau.a := *; \ ? - b \leq \tau.a \leq a) \)
  \( \cup (?\tau.v \geq m.r; \ \tau.a := *; \ ? - b \leq \tau.a \leq 0) \)
- **atp**: \( \text{if}(m.e - \tau.p \leq SB \lor \text{rbc.message} = \text{emergency}) \ \tau.a := -b \)
- **drive**: \( t := 0; \ (\tau.p' = \tau.v, \ \tau.v' = \tau.a, \ t' = 1 \land \tau.v \geq 0 \land t \leq \varepsilon) \)
- **rbc**: \( (\text{rbc.message} := \text{emergency}) \ \cup \ (m := *; \ ?m.r > 0) \)

Example (Taks)

Verify safety

Specification

\[ [ETCS_{skel}](\tau.p \geq m.e \rightarrow \tau.v \leq m.d) \]
**Parametric Skeleton of ETCS**

\[ ETCS_{skel} : (\text{train} \cup \text{rbc})^* \]

- **train**: \( \text{spd; atp; drive} \)
- **spd**:  
  \( (?\tau.v \leq m.r; \tau.a := *; ? - b \leq \tau.a \leq a) \)  
  \( \cup (?\tau.v \geq m.r; \tau.a := *; ? - b \leq \tau.a \leq 0) \)
- **atp**:  
  \( \text{if}(m.e - \tau.p \leq SB \lor \text{rbc.message} = \text{emergency}) \tau.a := -b \)
- **drive**:  
  \( t := 0; (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \land \tau.v \geq 0 \land t \leq \varepsilon) \)
- **rbc**:  
  \( (\text{rbc.message} := \text{emergency}) \cup (m := *; ?m.r > 0) \)

**Example (Taks)**

Verify safety

**Specification**

\[ \lbrack ETCS_{skel} \rbrack(\tau.p \geq m.e \rightarrow \tau.v \leq m.d) \]

**Issue**

Lots of counterexamples!
Iterative Control Refinement Process

\[ \tau \cdot v \]

\[ m \cdot d \]

\[ \tau \cdot p \]

\[ m \cdot e \]
Iterative Control Refinement Process

1. Controllability discovery
1 Controllability discovery
Controllability discovery
1. Controllability discovery
2. Control refinement
Iterative Control Refinement Process

1. Controllability discovery
2. Control refinement
Iterative Control Refinement Process

1. Controllability discovery
2. Control refinement
Iterative Control Refinement Process

1. Controllability discovery
2. Control refinement
Iterative Control Refinement Process

1. Controllability discovery
2. Control refinement
3. Repeat 2 until safety can be proven
Iterative Control Refinement Process

1. Controllability discovery
2. Control refinement
3. Repeat 2 until safety can be proven
4. Liveness check
Outline

1 Train Control
   • Separation Principle
   • Parametric ETCS

2 Parametric European Train Control System
   • Controllability
   • Reactivity
   • Refined Control
   • Safety
   • Liveness

3 Enhancements

4 Summary
ETCS Controllability

Proposition (Controllability)

\[
[\tau.p' = \tau.v, \tau.v' = -b \land \tau.v \geq 0](\tau.p \geq m.e \rightarrow \tau.v \leq m.d)
\equiv \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.p)
\]
Proposition (RBC Controllability)

\[ m.d \geq 0 \land b > 0 \rightarrow [m_0 := m; rbc] \bigg( m_0.d^2 - m.d^2 \leq 2b(m.e - m_0.e) \land m_0.d \geq 0 \land m.d \geq 0 \bigg) \land \forall \tau \bigg( (\langle m := m_0 \rangle C) \rightarrow C \bigg) \]
**Proposition (Reactivity)**

\[
\left( \forall m.e \forall \tau.p \left( m.e - \tau.p \geq SB \land C \rightarrow [\tau.a := a; \ drive] C \right) \right)
\]

\[
\equiv SB \geq \frac{\tau.v^2 - m.d^2}{2b} + \left( \frac{a}{b} + 1 \right) \left( \frac{a}{2} \varepsilon^2 + \varepsilon \tau.v \right)
\]
ETCS:\ ((\text{train} \cup \text{rbc})^*)

\begin{align*}
\text{train} & : \text{spd}; \text{atp}; \text{drive} \\
\text{spd} & : (\exists \tau.v \leq m.r; \tau.a := *; \exists \tau.a \leq \tau.a \leq A) \\
& \quad \cup (\exists \tau.v \geq m.r; \tau.a := *; \exists \tau.a \geq \exists \tau.a \geq \exists \tau.a \geq -b) \\
\text{atp} & : SB := \frac{\tau.v^2 - m.d^2}{2b} + \left(\frac{a}{b} + 1\right) \left(\frac{a}{2} \varepsilon^2 + \varepsilon \tau.v\right); \\
& \quad \text{if}(m.e - \tau.p \leq SB \lor \text{rbc.message} = \text{emergency}) \tau.a := \exists \tau.a \geq \exists \tau.a \geq \exists \tau.a \geq -b \\
\text{drive} & : t := 0; (\tau.p' = \tau.v, \tau.v' = \tau.a, \tau.t' = 1 \land \exists \tau.v \geq 0 \land t \leq \varepsilon) \\
\text{rbc} & : (\text{rbc.message} := \text{emergency}) \\
& \quad \cup (m_0 := m; m := *; \exists m_0.d^2 = m.d^2 \leq 2b(m.e - m_0.e) \land m.r \geq 0 \land m.d \geq 0) 
\end{align*}
Refined ETCS Control

\(\text{ETCS}_r: \ (\text{train} \cup \text{rbc})^*\)

\(\text{train}: \ \text{spd}; \ \text{atp}; \ \text{drive}\)

\(\text{spd} : \ (??\tau.v \leq m.r; \ \tau.a := \ast; \ ? - b \leq \tau.a \leq A)
\cup (??\tau.v \geq m.r; \ \tau.a := \ast; \ ?0 > \tau.a \geq -b)\)

\(\text{atp} : \ SB := \frac{\tau.v^2 - m.d^2}{2b} + \left(\frac{a}{b} + 1\right) \left(\frac{a}{2} \varepsilon^2 + \varepsilon \ \tau.v\right)\)
\ :
\quad \text{if}(m.e - \tau.p \leq SB \lor \text{rbc.message} = \text{emergency}) \ \tau.a := -b\)

\(\text{drive} : \ t := 0; \ (\tau.p' = \tau.v, \ \tau.v' = \tau.a, \ t' = 1 \land \tau.v \geq 0 \land t \leq \varepsilon)\)

\(\text{rbc} : \ (\text{rbc.message} := \text{emergency})\)
\quad \cup (m_0 := m; \ m := \ast;\)
\quad \quad ?m_0.d^2 - m.d^2 \leq 2b(m.e - m_0.e) \land m.r \geq 0 \land m.d \geq 0)\)

**Specification**

\[\tau.v^2 - m.d^2 \leq 2b(m.e - \tau.p) \rightarrow [\text{ETCS}_r](\tau.p \geq m.e \rightarrow \tau.v \leq m.d)\]
Refined ETCS Control

**ETCS**_r_: (train ∪ rbc)*

- **train**: spd; atp; drive
- **spd**: (?τ.v ≤ m.r; τ.a := *; ? − b ≤ τ.a ≤ A)
  ∪ (?τ.v ≥ m.r; τ.a := *; ?0 > τ.a ≥ −b)
- **atp**: SB := \( \frac{\tau.v^2 - m.d^2}{2b} + \left( \frac{a}{b} + 1 \right) \left( \frac{a}{2} \varepsilon^2 + \varepsilon \tau.v \right) \);
  if(m.e − τ.p ≤ SB ∨ rbc.message = emergency) τ.a := −b
- **drive**: t := 0; (τ.p′ = τ.v, τ.v′ = τ.a, t′ = 1 ∧ τ.v ≥ 0 ∧ t ≤ ε)
- **rbc**: (rbc.message := emergency)
  ∪ (m0 := m; m := *;
  ?m0.d^2 − m.d^2 ≤ 2b(m.e − m0.e) ∧ m.r ≥ 0 ∧ m.d ≥ 0)

**Specification**

\( \tau.v^2 - m.d^2 \leq 2b(m.e - \tau.p) \rightarrow [ETCS_\text{r}](\tau.p \geq m.e \rightarrow \tau.v \leq m.d) \)
Proposition (Safety)

\[ C \rightarrow [ETCS](\tau.p \geq m.e \rightarrow \tau.v \leq m.d) \]
Proposition (Liveness)

\[ \tau.v \geq 0 \land \varepsilon > 0 \rightarrow \forall P \langle ETCS_r \rangle \tau.p \geq P \]
Outline

1. Train Control
   - Separation Principle
   - Parametric ETCS

2. Parametric European Train Control System
   - Controllability
   - Reactivity
   - Refined Control
   - Safety
   - Liveness

3. Enhancements

4. Summary
SO FAR: NO WIND, FRICTION, ETC.

DIRECT CONTROL OF THE ACCELERATION

ISSUE

THIS IS UNREALISTIC!

SOLUTION

TAKE DISTURBANCES INTO ACCOUNT.

THEOREM

ETCS IS CONTROLLABLE, REACTIVE, AND SAFE IN THE PRESENCE OF DISTURBANCES.

PROOF SKETCH

THE SYSTEM NOW CONTAINS $\tau_a - l \leq \tau_v$.

$\dot{v} \leq \tau_a + u$ INSTEAD OF $\tau_v$.

WE CANNOT SOLVE THE DIFFERENTIAL EQUATIONS ANYMORE.

USE DIFFERENTIAL INVARIANTS FOR APPROXIMATION. FOR DETAILS SEE LATER.

So far: no wind, friction, etc.

Direct control of the acceleration

**Issue**

This is unrealistic!

---

**Theorem**

ETCS is controllable, reactive, and safe in the presence of disturbances.

**Proof sketch**

The system now contains $\tau. a - l \leq \tau. v' \leq \tau. a + u$ instead of $\tau. v' = \tau. a$.

We cannot solve the differential equations anymore.

Use differential invariants for approximation. For details see later.

So far: no wind, friction, etc.
Direct control of the acceleration

Issue
This is unrealistic!

Solution
Take disturbances into account.

Theorem
ETCS is controllable, reactive, and safe in the presence of disturbances.
Safety Despite Disturbances

So far: no wind, friction, etc.
Direct control of the acceleration

Issue
This is unrealistic!

Solution
Take disturbances into account.

Theorem
ETCS is controllable, reactive, and safe in the presence of disturbances.

\[
\tau.v \\
m.d \\
\tau.p \\
m.e
\]

Proof sketch
The system now contains \( \tau.a - l \leq \tau.v' \leq \tau.a + u \) instead of \( \tau.v' = \tau.a \).
We cannot solve the differential equations anymore.
Use differential invariants for approximation. For details see later.

Safety Despite Disturbances

---

So far: no wind, friction, etc.

Direct control of the acceleration

Issue

This is unrealistic!

Solution

Take disturbances into account.

Theorem

ETCS is controllable, reactive, and safe in the presence of disturbances.

Proof sketch

The system now contains $\tau \cdot a - l \leq \tau \cdot v' \leq \tau \cdot a + u$ instead of $\tau \cdot v' = \tau \cdot a$.

$\Rightarrow$ We cannot solve the differential equations anymore.

$\Rightarrow$ Use differential invariants for approximation. For details see later.

---

So far

Almost completely non-deterministic control.
So far
Almost completely non-deterministic control.

Issue
This is unrealistic!
Realistic Speed Control

So far
Almost completely non-deterministic control.

Issue
This is unrealistic!

Solution
Verify proportional-integral (PI) controllers used in trains.
So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

Solution

Verify proportional-integral (PI) controllers used in trains.

\[ \begin{align*}
&\text{Controller} \\
&v0-v \quad a \\
&\text{PI Output} \\
&\text{Truncate} \\
&\text{In} \\
&\text{min} \\
&\text{max} \\
&\text{Out1} \\
&\text{Plant} \\
&\frac{1}{s} \\
&\text{Speed}
\end{align*} \]
Realistic Speed Control

So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

Solution

Verify proportional-integral (PI) controllers used in trains.

Differential equation system

\[ \tau \cdot v' = \min\left(a, \max\left(-b, \ell (\tau \cdot v - m.r) - i s - c m.r\right)\right) \land s' = \tau \cdot v - m.r \]
Realistic Speed Control

So far
Almost completely non-deterministic control.

Issue
This is unrealistic!

Solution
Verify proportional-integral (PI) controllers used in trains.

Theorem
The ETCS system remains safe when speed is controlled by a PI controller.

Proof sketch
Cannot solve differential equations really. Use differential invariants! For details see later.

Platzer, A.:
Differential-algebraic dynamic logic for differential-algebraic programs.
1 Train Control
   • Separation Principle
   • Parametric ETCS

2 Parametric European Train Control System
   • Controllability
   • Reactivity
   • Refined Control
   • Safety
   • Liveness

3 Enhancements

4 Summary
Formally verified a major case study with KeYmaera:

- discovered necessary safety constraints
- controllability, reactivity, safety and liveness properties
- Extensions for ETCS with disturbances and for ETCS with PI control