European Train Control System: A Case Study in Formal Verification

André Platzer Jan-David Quesel

Carnegie Mellon University, Pittsburgh, PA

October 23, 2013

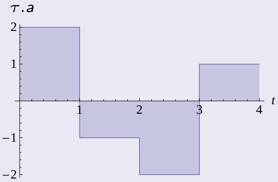
Deutsche Forschungsgemeinschaft DFG

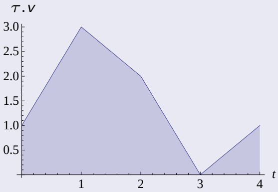
ETCS Control Verification

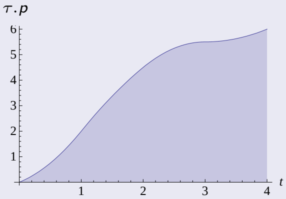
Problem

Hybrid System

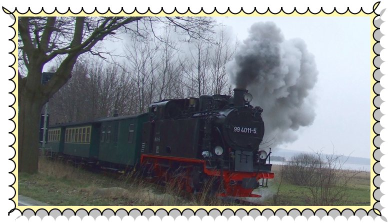
- Continuous evolutions (differential equations)
- Discrete jumps (control decisions)

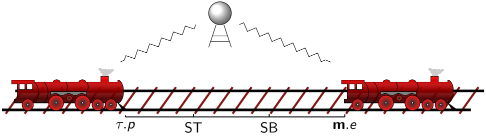






European Train Control System





Objectives

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

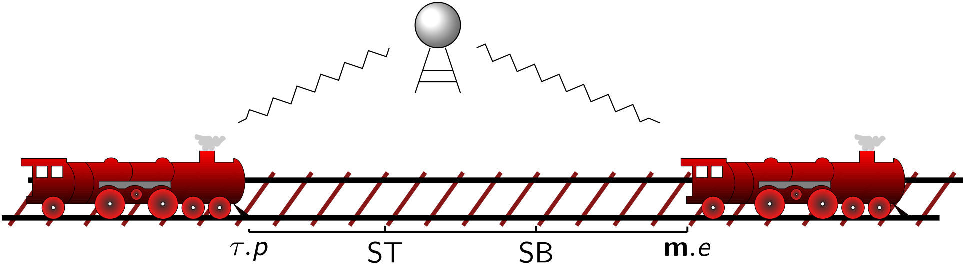
Overview

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

Separation Principle

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.*



Separation Principle

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.

$\square$

Separation Principle

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.

Separation Principle

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.
- Consider any point in time ζ.

Separation Principle

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.
- Consider any point in time ζ.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to n at ζ.

Separation Principle

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.
- Consider any point in time ζ.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to n at ζ.
- 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.

Separation Principle

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.
- Consider any point in time ζ.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to n at ζ.
- 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 ζ.

Separation Principle

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.
- Consider any point in time ζ.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to n at ζ.
- 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 ζ.
- Then $z_i = z_j$ at ζ for some $i, j \in \mathbb{N}$.

$\square$

Separation Principle

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.
- Consider any point in time ζ.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to n at ζ.
- 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 ζ.
- Then $z_i = z_j$ at ζ for some $i, j \in \mathbb{N}$.
- However, by assumption, $z_i \in M_i$ and $z_j \in M_j$ at ζ, thus $M_i \cap M_j \neq \emptyset$, $\square$

Separation Principle

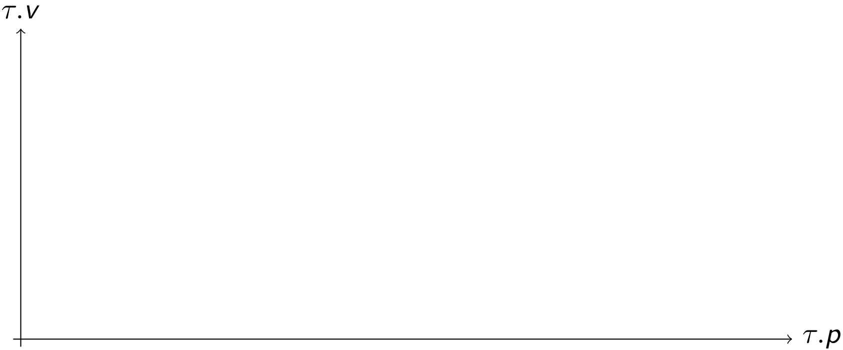
Lemma (Principle of separation by movement authorities)

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

Proof.

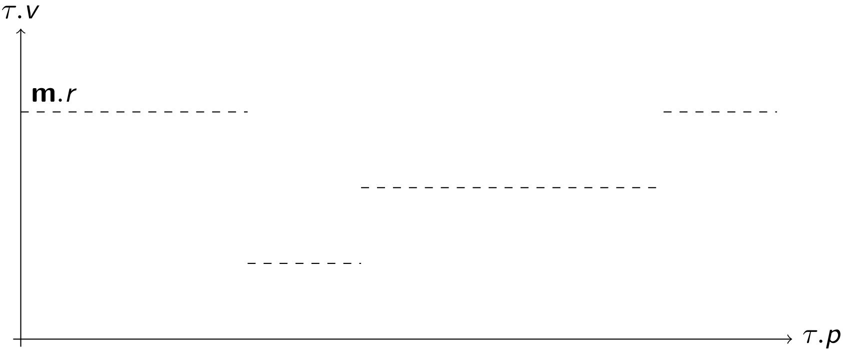
- To simplify notation, assume trains are points.
- Consider any point in time ζ.
- For $n \in \mathbb{N}$, let $z_1, \ldots, z_n$ be positions of all the trains 1 to n at ζ.
- Let M_i be the MA-range, i.e., the set of positions on the track for which train i has currently been issued MA.
- Suppose there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

3D Movement Authorities



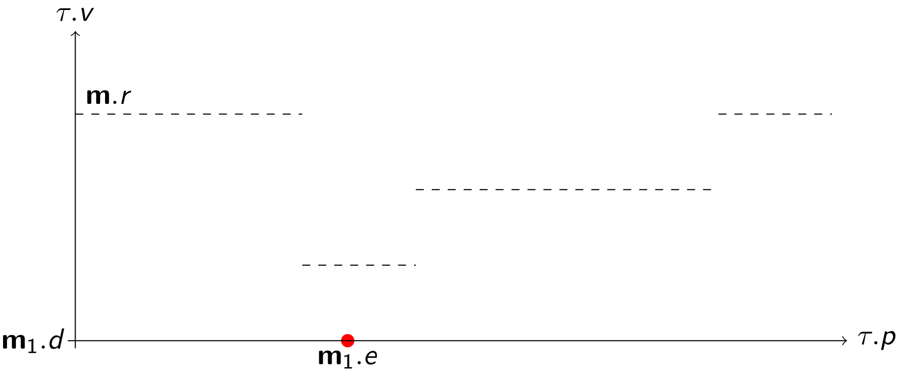
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



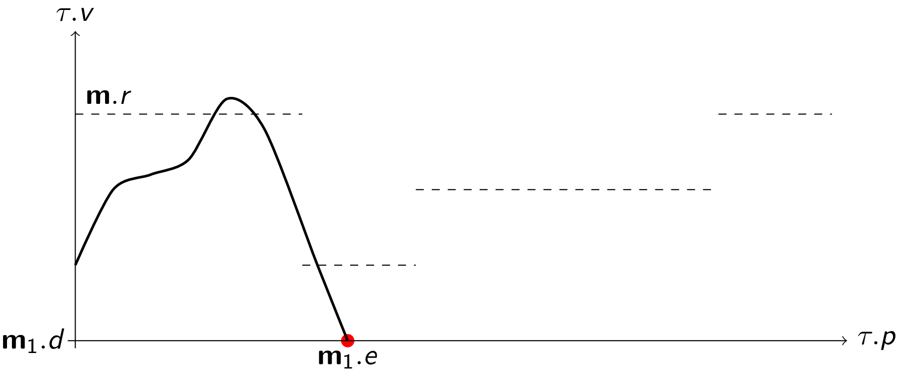
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



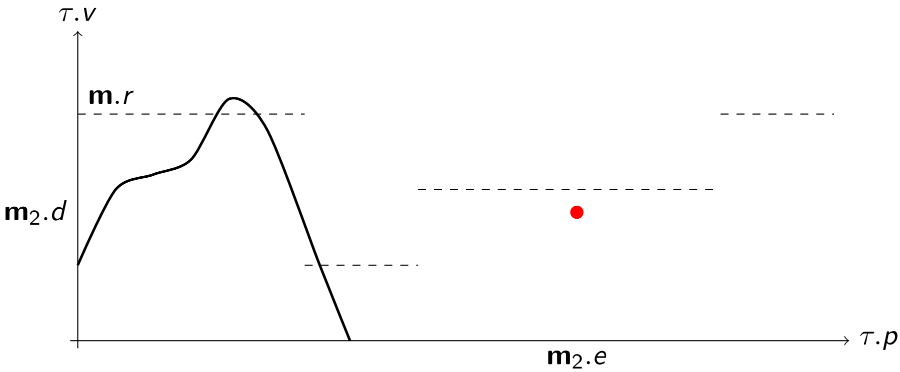
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



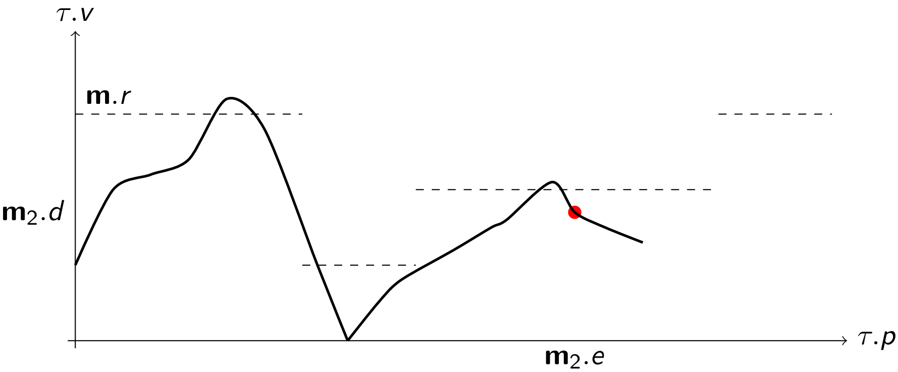
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



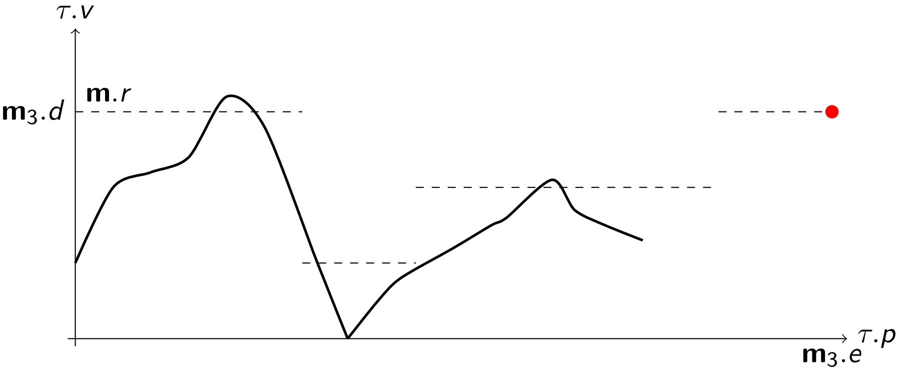
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



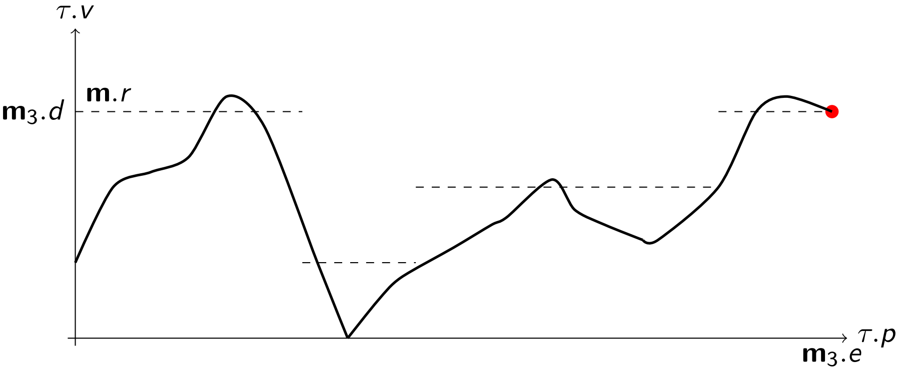
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



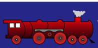
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



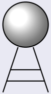
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

Model/State Variables

Train τ ()

- $\tau.p$ Position
- $\tau.v$ Speed
- $\tau.a$ Acceleration
- (t model time)

RBC + MA



- $\mathbf{m}.e$ End of Authority
- $\mathbf{m}.d$ Speed limit
- $\mathbf{m}.r$ Recommended speed
- $rbc.message$ Channel

Parameters

- SB Start Braking
- b Braking power/deceleration
- A Maximum acceleration
- ε Maximum cycle time

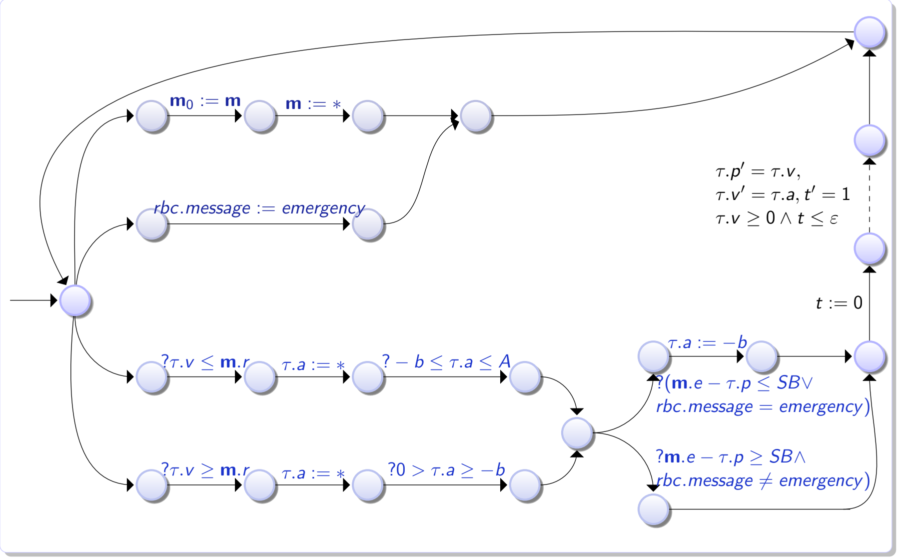
Parametric Skeleton of ETCS

Read from the informal specification...

$$
\begin{array}{ll}
ETCS_{skel} & : (train \cup rbc)^* \\
train & : spd;\ atp;\ drive \\
spd & : \quad (?\tau.v \leq \mathbf{m}.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq A) \\
 & \quad \cup(?\tau.v \geq \mathbf{m}.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq 0) \\
atp & : \mathtt{if}(\mathbf{m}.e - \tau.p \leq SB \lor rbc.message = emergency)\, \tau.a := -b \\
drive & : t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \land \tau.v \geq 0 \land t \leq \varepsilon) \\
rbc & : (rbc.message := emergency)\ \cup\ (\mathbf{m} := *;\ ?\mathbf{m}.r > 0)
\end{array}
$$

Parametric Skeleton of ETCS

As transition system...



Parametric Skeleton of ETCS

$$
\begin{array}{ll}
ETCS_{skel} & : (train \cup rbc)^{*} \\
train & : spd;\ atp;\ drive \\
spd & : \quad (?\tau.v \leq \mathbf{m}.r;\ \tau.a := *;\ ? - b \leq \tau.a \leq A) \\
 & \quad \cup(?\tau.v \geq \mathbf{m}.r;\ \tau.a := *;\ ? - b \leq \tau.a \leq 0) \\
atp & : \mathtt{if}(\mathbf{m}.e - \tau.p \leq SB \vee rbc.message = emergency)\, \tau.a := -b \\
drive & : t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \wedge \tau.v \geq 0 \wedge t \leq \varepsilon) \\
rbc & : (rbc.message := emergency)\ \cup\ (\mathbf{m} := *;\ ?\mathbf{m}.r > 0)
\end{array}
$$

Task

Verify safety

Parametric Skeleton of ETCS

$$
\begin{array}{lll}
ETCS_{skel} & : & (train \cup rbc)^* \\
train & : & spd;\ atp;\ drive \\
spd & : & \quad (?\tau.v \leq \mathbf{m}.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq A) \\
 & & \cup(?\tau.v \geq \mathbf{m}.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq 0) \\
atp & : & \mathtt{if}(\mathbf{m}.e - \tau.p \leq SB \vee rbc.message = emergency)\, \tau.a := -b \\
drive & : & t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \wedge \tau.v \geq 0 \wedge t \leq \varepsilon) \\
rbc & : & (rbc.message := emergency)\ \cup\ (\mathbf{m} := *;\ ?\mathbf{m}.r > 0)
\end{array}
$$

Task

Verify safety

Specification

$[ETCS_{skel}](\tau.p \geq \mathbf{m}.e \to \tau.v \leq \mathbf{m}.d)$

Parametric Skeleton of ETCS

$$
\begin{array}{lll}
ETCS_{skel} & : & (train \cup rbc)^* \\
train & : & spd;\ atp;\ drive \\
spd & : & \quad (?\tau.v \leq \mathbf{m}.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq A) \\
 & & \cup(?\tau.v \geq \mathbf{m}.r;\ \tau.a := *;\ ?-b \leq \tau.a \leq 0) \\
atp & : & \mathtt{if}(\mathbf{m}.e - \tau.p \leq SB \vee rbc.message = emergency)\, \tau.a := -b \\
drive & : & t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \wedge \tau.v \geq 0 \wedge t \leq \varepsilon) \\
rbc & : & (rbc.message := emergency)\ \cup\ (\mathbf{m} := *;\ ?\mathbf{m}.r > 0)
\end{array}
$$

Task

Verify safety

Specification

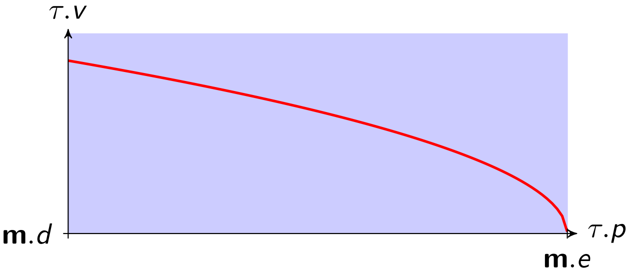
$[ETCS_{skel}](\tau.p \geq \mathbf{m}.e \rightarrow \tau.v \leq \mathbf{m}.d)$

Issue

Lots of counterexamples!

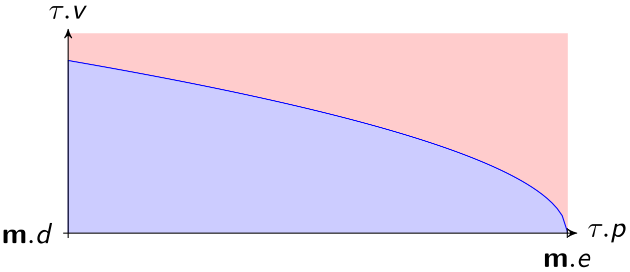
Iterative Control Refinement Process

Iterative Control Refinement Process



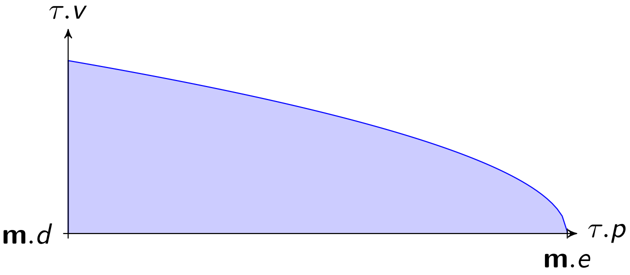
1. Controllability discovery

Iterative Control Refinement Process



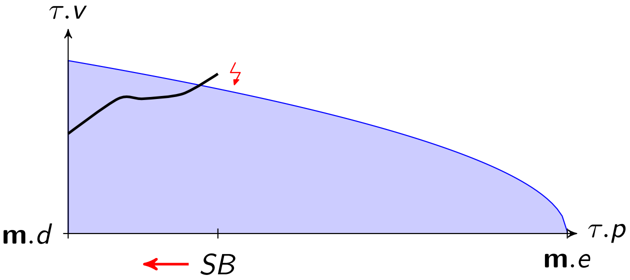
1. Controllability discovery

Iterative Control Refinement Process



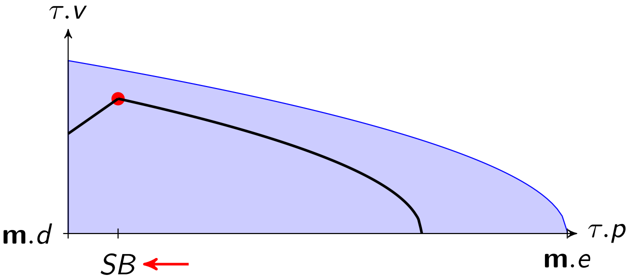
1. Controllability discovery

Iterative Control Refinement Process



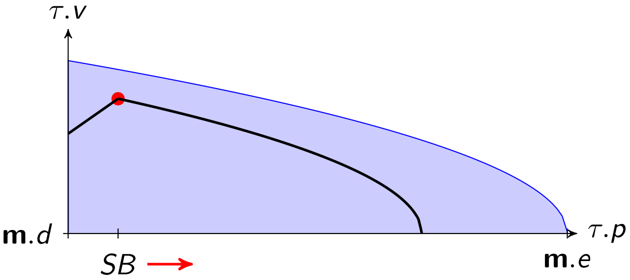
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



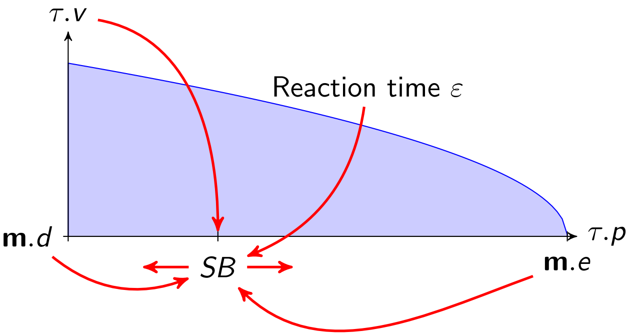
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



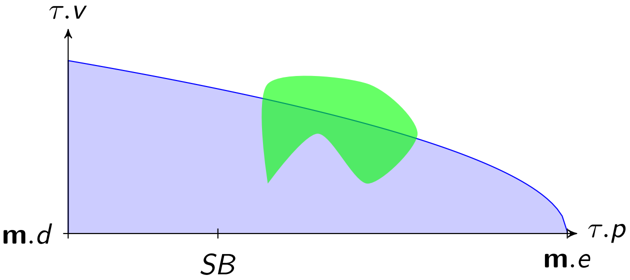
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



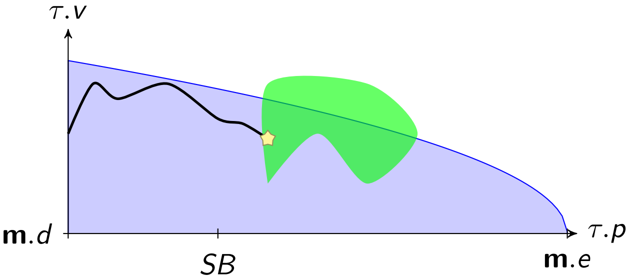
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



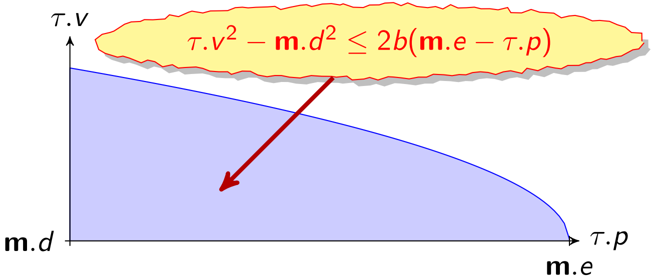
1. Controllability discovery
2. Control refinement
3. Repeat 2 until safety can be proven

Iterative Control Refinement Process



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

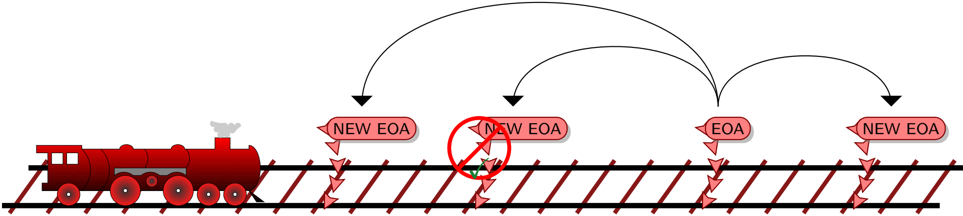
ETCS Controllability



Proposition (Controllability)

$$[\tau.p' = \tau.v, \tau.v' = -b \wedge \tau.v \geq 0](\tau.p \geq \mathbf{m}.e \rightarrow \tau.v \leq \mathbf{m}.d)$$
$$\equiv \tau.v^2 - \mathbf{m}.d^2 \leq 2b(\mathbf{m}.e - \tau.p) \qquad (\mathcal{C})$$

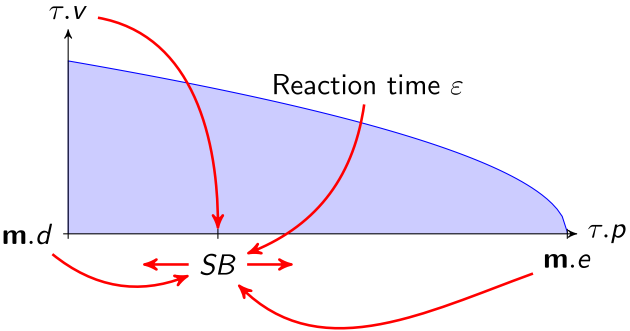
ETCS RBC Controllability



Proposition (RBC Controllability)

$$\mathbf{m}.d \geq 0 \wedge b > 0 \rightarrow [\mathbf{m}_0 := \mathbf{m};\ rbc] \Big(\mathbf{m}_0.d^2 - \mathbf{m}.d^2 \leq 2b(\mathbf{m}.e - \mathbf{m}_0.e) \wedge \mathbf{m}_0.d \geq 0 \wedge \mathbf{m}.d \geq 0 \leftrightarrow \forall \tau \left((\langle \mathbf{m} := \mathbf{m}_0 \rangle \mathcal{C}) \rightarrow \mathcal{C} \right) \Big)$$

ETCS Reactivity



Proposition (Reactivity)

$$\Big(\forall \mathbf{m}.e\, \forall \tau.p\, \big(\mathbf{m}.e - \tau.p \geq SB \land \mathcal{C} \rightarrow [\tau.a := A;\ drive]\, \mathcal{C}\big)\Big)$$

$$\equiv SB \geq \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\, \tau.v\right)$$

Refined ETCS Control

$$
\begin{array}{lll}
ETCS_r\colon & (train \cup rbc)^* \\
train & : & spd;\ atp;\ drive \\
spd & : & (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ?-b \le \tau.a \le A) \\
 & & \cup(?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b) \\
atp & : & SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\,\tau.v\right); \\
 & : & \mathtt{if}(\mathbf{m}.e - \tau.p \le SB \lor rbc.message = emergency)\,\tau.a := -b \\
drive & : & t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \land \tau.v \ge 0 \land t \le \varepsilon) \\
rbc & : & (rbc.message := emergency) \\
 & & \cup\ \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *; \\
 & & \quad ?\mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e) \land \mathbf{m}.r \ge 0 \land \mathbf{m}.d \ge 0\big)
\end{array}
$$

Refined ETCS Control

$$
\begin{array}{lll}
ETCS_r: & (train \cup rbc)^* \\
train & : & spd;\ atp;\ drive \\
spd & : & (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ?-b \le \tau.a \le A) \\
 & & \cup(?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b) \\
atp & : & SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\ \tau.v\right); \\
 & : & \mathtt{if}(\mathbf{m}.e - \tau.p \le SB \lor rbc.message = emergency)\, \tau.a := -b \\
drive & : & t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \land \tau.v \ge 0 \land t \le \varepsilon) \\
rbc & : & (rbc.message := emergency) \\
 & & \cup \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *; \\
 & & \quad ?\mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e) \land \mathbf{m}.r \ge 0 \land \mathbf{m}.d \ge 0\big)
\end{array}
$$

Specification

$$\tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \to [ETCS_r](\tau.p \ge \mathbf{m}.e \to \tau.v \le \mathbf{m}.d)$$

Refined ETCS Control

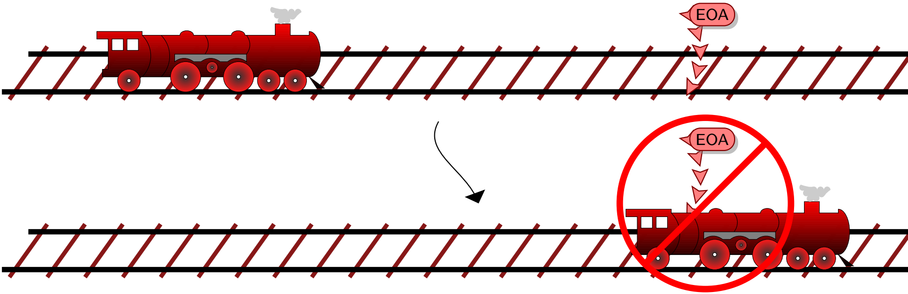
Necessary for safety

$$
\begin{array}{lcl}
ETCS_r & : & (train \cup rbc)^* \\
train & : & spd;\ atp;\ drive \\
spd & : & (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ?-b \le \tau.a \le A) \\
 & & \cup(?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b) \\
atp & : & SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\ \tau.v\right); \\
 & : & \mathtt{if}(\mathbf{m}.e - \tau.p \le SB \vee rbc.message = emergency)\ \tau.a := -b \\
drive & : & t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \wedge \tau.v \ge 0 \wedge t \le \varepsilon) \\
rbc & : & (rbc.message := emergency) \\
 & & \cup\ \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *; \\
 & & \quad ?\mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e) \wedge \mathbf{m}.r \ge 0 \wedge \mathbf{m}.d \ge 0\big)
\end{array}
$$

Specification

$$\tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \to [ETCS_r](\tau.p \ge \mathbf{m}.e \to \tau.v \le \mathbf{m}.d)$$

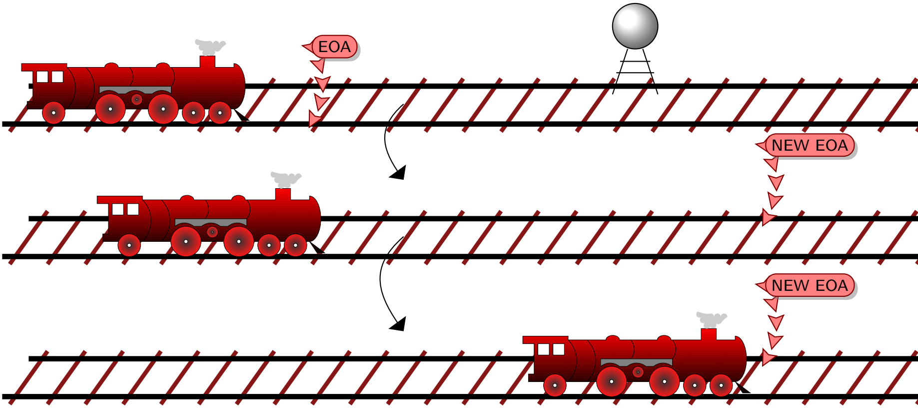
ETCS Safety



Proposition (Safety)

$$\mathcal{C} \rightarrow$$
$$[ETCS](\tau.p \geq \mathbf{m}.e \rightarrow \tau.v \leq \mathbf{m}.d)$$

ETCS Liveness



Proposition (Liveness)

$$\tau.v \geq 0 \land \varepsilon > 0 \rightarrow \forall P \, \langle ETCS_r \rangle \, \tau.p \geq P$$

Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

Issue

This is unrealistic!

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.

Safety Despite Disturbances

So far: no wind, friction, etc.

Direct control of the acceleration

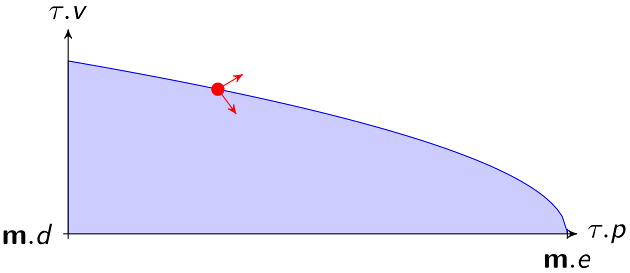
Issue

This is unrealistic!

Solution Take disturbances into account.

Theorem

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



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

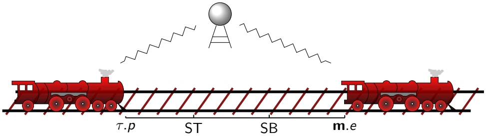
The system now contains $\tau.a - l \leq \tau.v' \leq \tau.a + u$ instead of $\tau.v' = \tau.a$.

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

$\leadsto$ Use differential invariants for approximation. For details see paper.

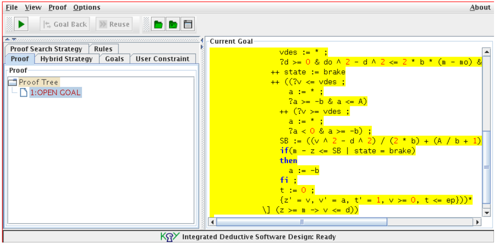
Platzer, A.:
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput. (2008) DOI 10.1093/logcom/exn070.

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



Literature

Platzer, A., Quesel, J.D.:

KeYmaera: A hybrid theorem prover for hybrid systems.

In Armando, A., Baumgartner, P., Dowek, G., eds.: IJCAR. Volume 5195 of LNCS., Springer (2008) 171–178
`http://symbolaris.com/info/KeYmaera.html`.

Platzer, A., Quesel, J.D.:

European train control system: A case study in formal verification.

In Karin Breitman and Ana Cavalcanti, editors, 11th International Conference on Formal Engineering Methods, ICFEM, Rio de Janeiro, Brasil, Proceedings, volume 5885 of LNCS, pages 246-265. Springer, 2009.

Platzer, A., Quesel, J.D.:

European train control system: A case study in formal verification.

Report 54, SFB/TR 14 AVACS (2009) ISSN: 1860-9821, avacs.org.