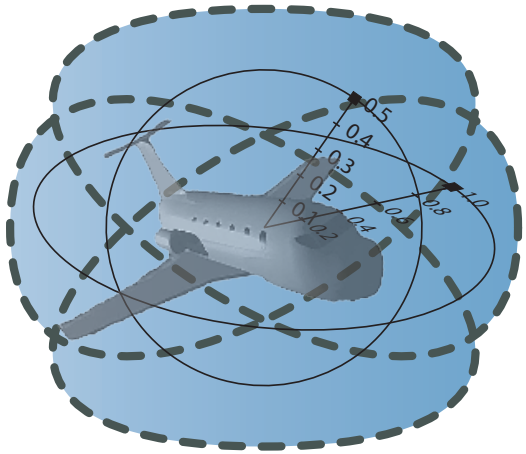
15-819/18-879: Logical Analysis of Hybrid Systems

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

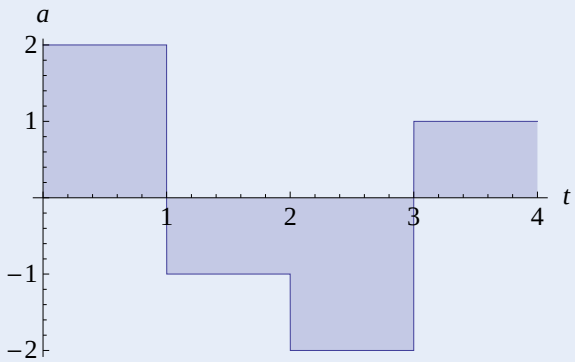
Outline

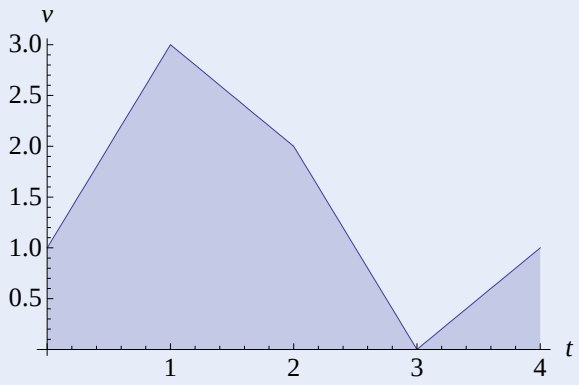
1. Train Control
   - Separation Principle
   - Parametric ETCS
2. Parametric European Train Control System
   - Controllability
   - Reactivity
   - Refined Control
   - Safety
   - Liveness
3. Enhancements
4. Summary

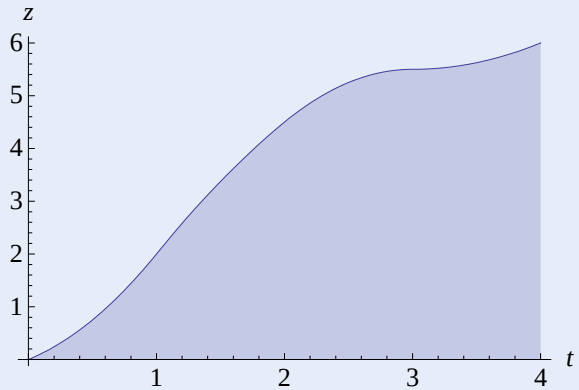
Challenge

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)

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe

Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(\mathbf{m} - z)$ $\not\Rightarrow$ safe

Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

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

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

$$SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v \ldots$$

Challenge

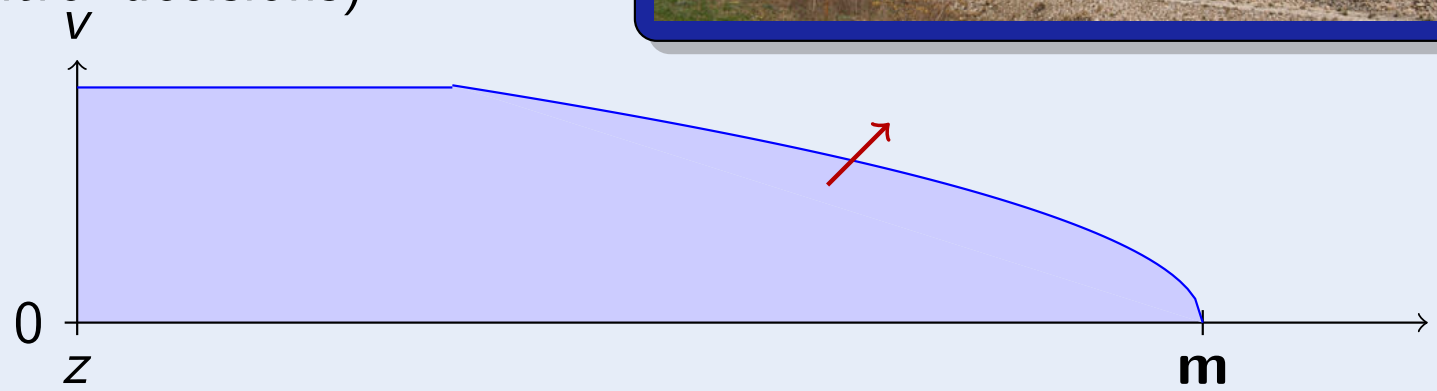
Hybrid Systems

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

Challenge

Hybrid Systems

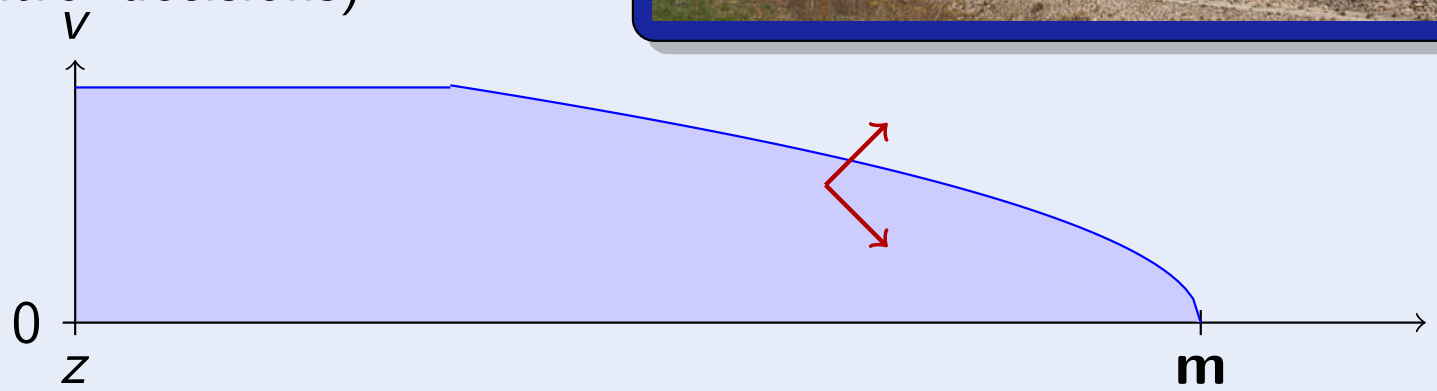
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid Systems

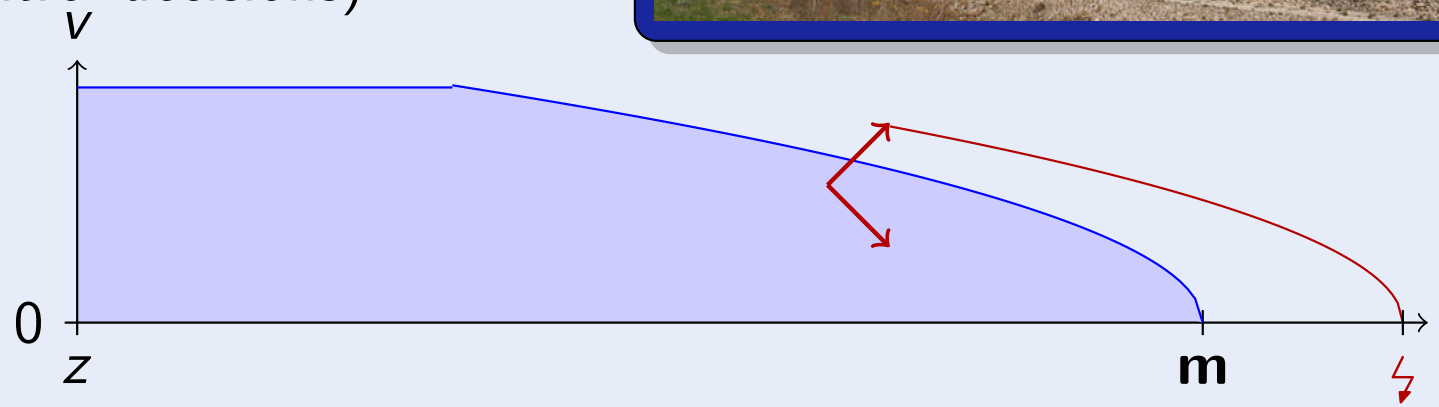
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid Systems

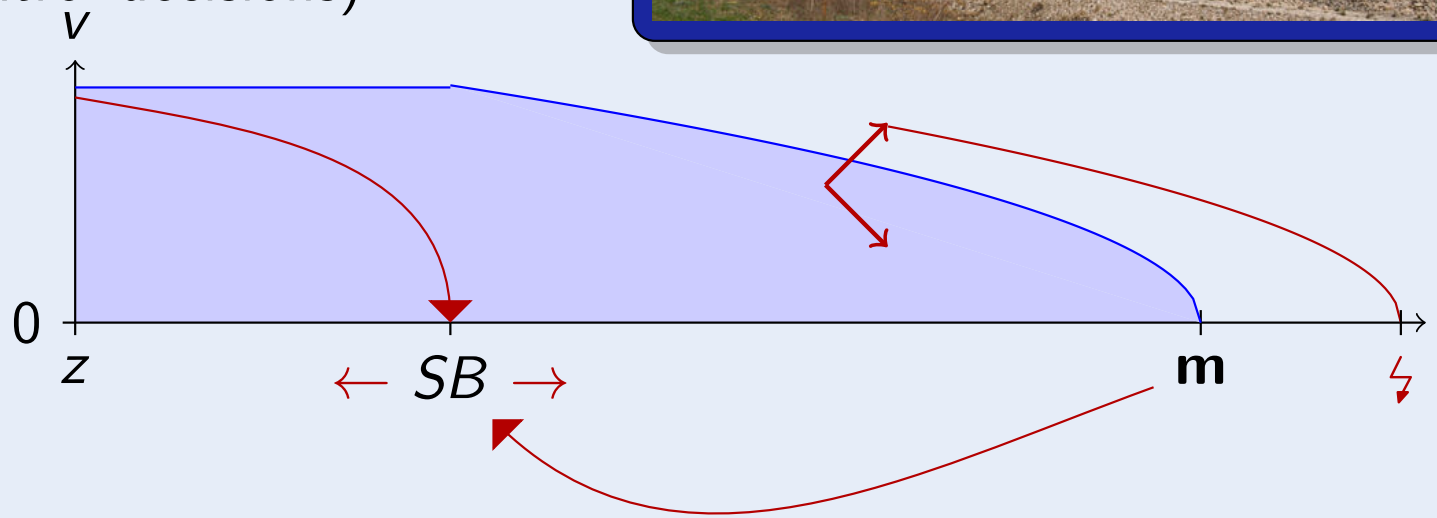
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid Systems

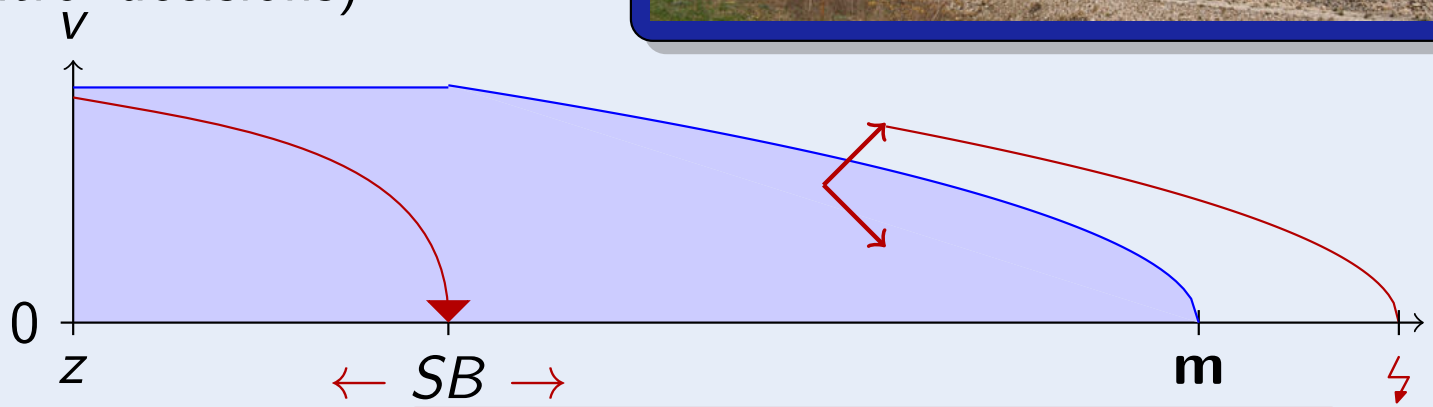
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

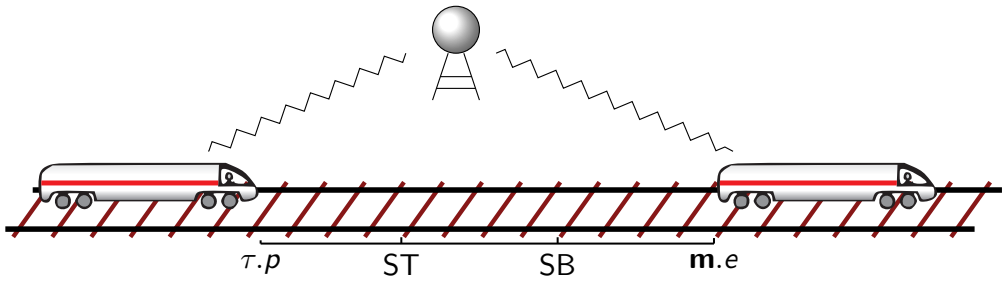
Hybrid Systems

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



$$SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v$$

European Train Control System



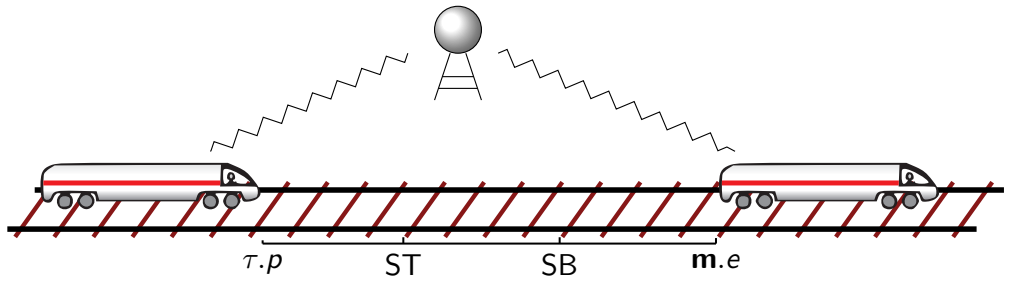
Objectives

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

Overview

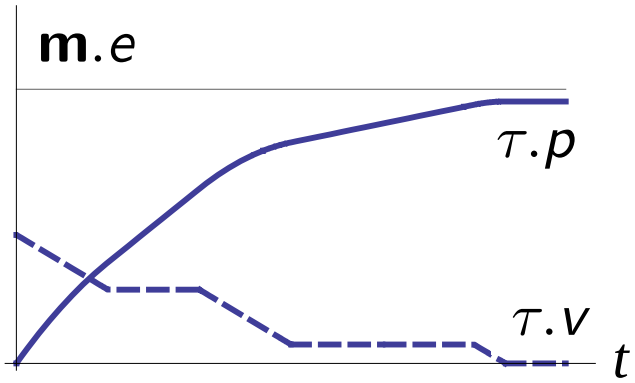
1. No static partitioning of track
2. Radio Block Controller (RBC) manages movement authorities dynamically
3. Moving block principle

European Train Control System

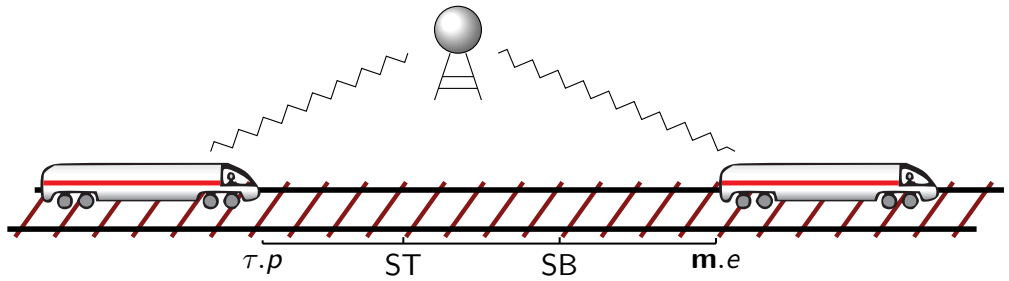


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

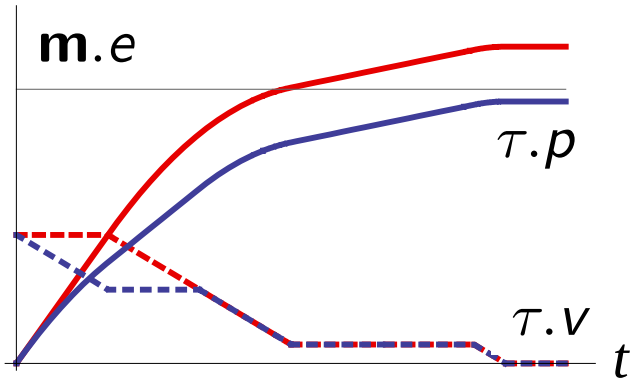


European Train Control System

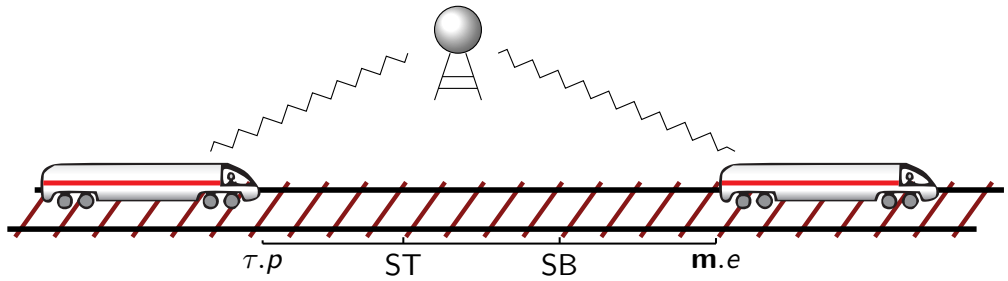


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change

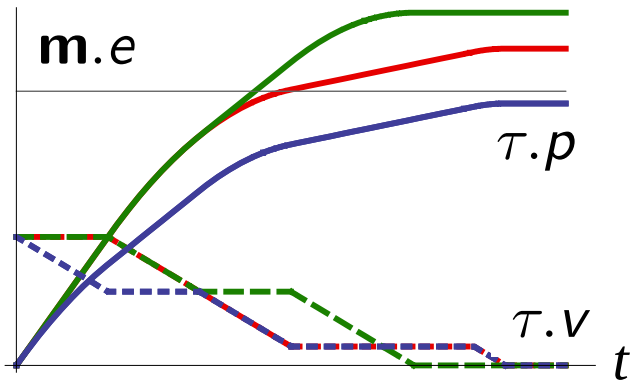


European Train Control System

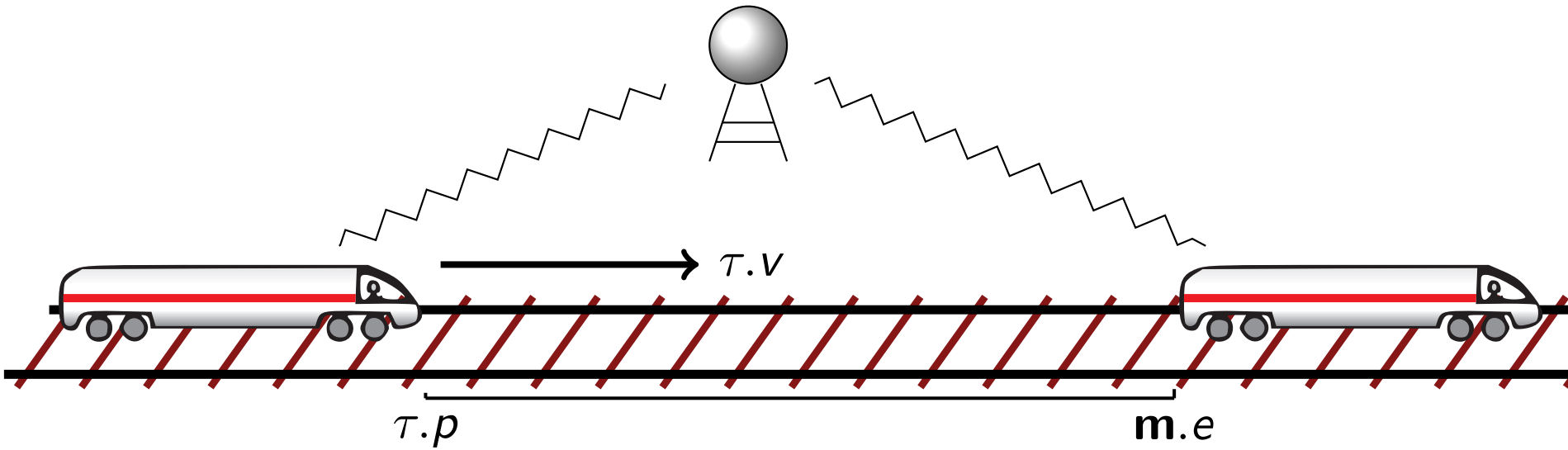


Parametric Hybrid Systems

continuous evolution along differential equations + discrete change



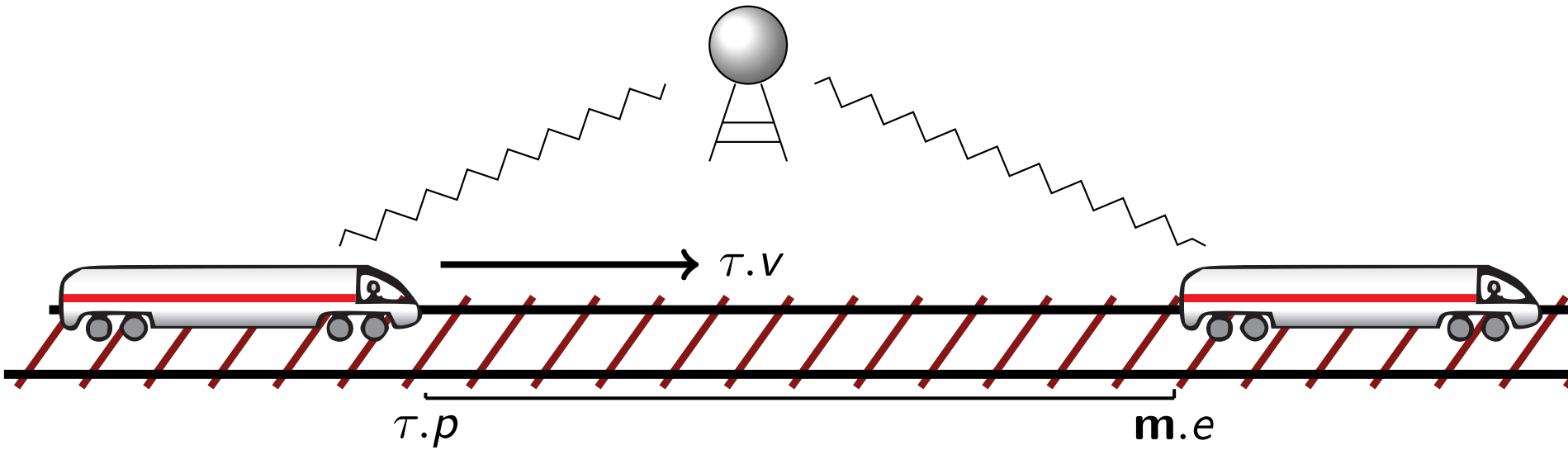
Differential Dynamic Logic (d$\mathcal{L}$)



Example

$$\underbrace{}_{\text{Precondition}} \rightarrow [\underbrace{}_{\text{Operation model}}](\underbrace{}_{\text{Property}})$$

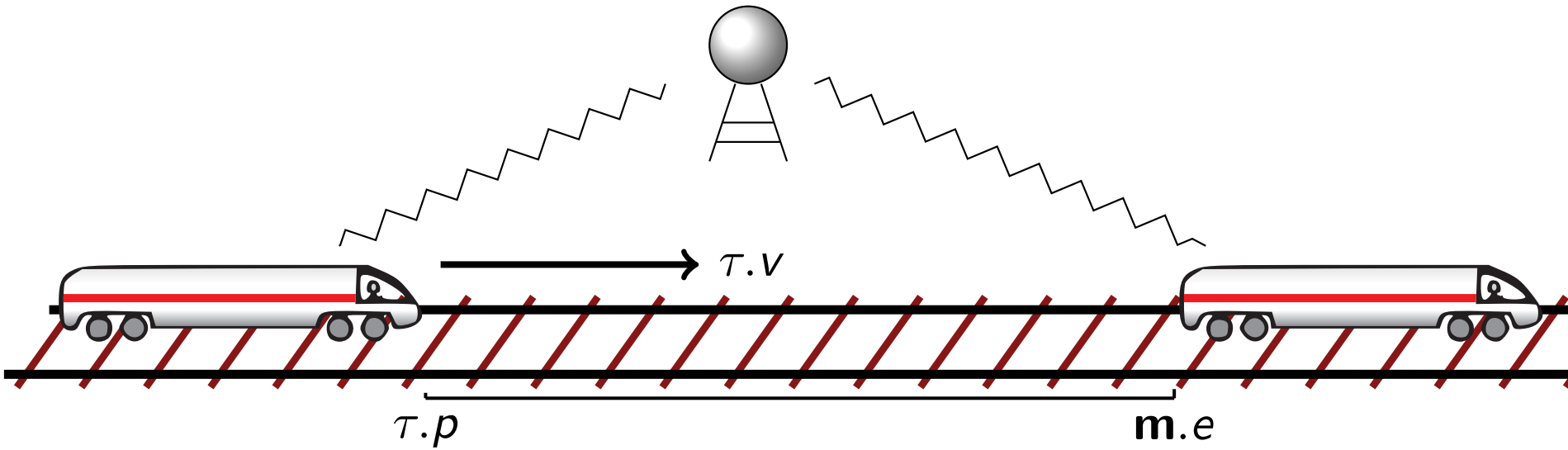
Differential Dynamic Logic (dℒ)



Example

$$\underbrace{\tau.v^2 \leq 2b(\mathbf{m}.e - \tau.p)}_{\text{Precondition}} \rightarrow [\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\text{Operation model}}](\underbrace{\tau.p \leq \mathbf{m}.e}_{\text{Property}})$$

Differential Dynamic Logic (dℒ)

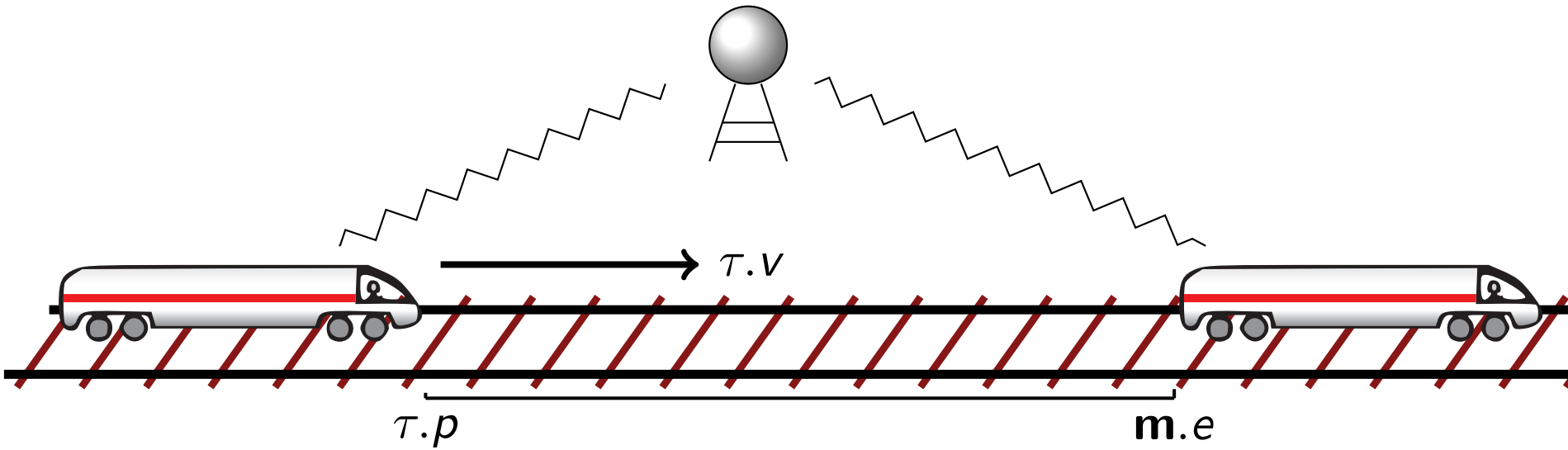


Example

$$\underbrace{\tau.v^2 \leq 2b(\mathbf{m}.e - \tau.p)}_{\text{Precondition}} \rightarrow [\underbrace{\tau.p' = \tau.v, \tau.v' = \tau.a}_{\text{Operation model}}](\underbrace{\tau.p \leq \mathbf{m}.e}_{\text{Property}})$$

Continuous evolution: differential equation

Differential Dynamic Logic (dℒ)

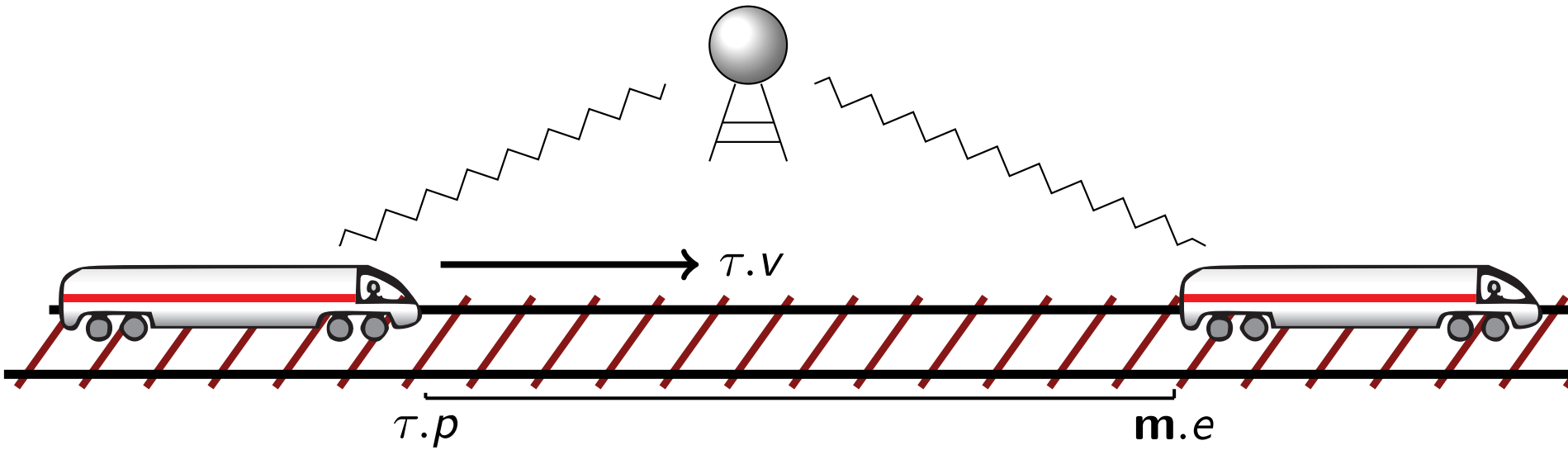


Example

$$\underbrace{\tau.v^2 \leq 2b(\mathbf{m}.e - \tau.p)}_{\text{Precondition}} \rightarrow [\underbrace{\tau.a := *; \quad \tau.p' = \tau.v, \tau.v' = \tau.a}_{\text{Operation model}}](\underbrace{\tau.p \leq \mathbf{m}.e}_{\text{Property}})$$

Random assignment

Differential Dynamic Logic (dℒ)

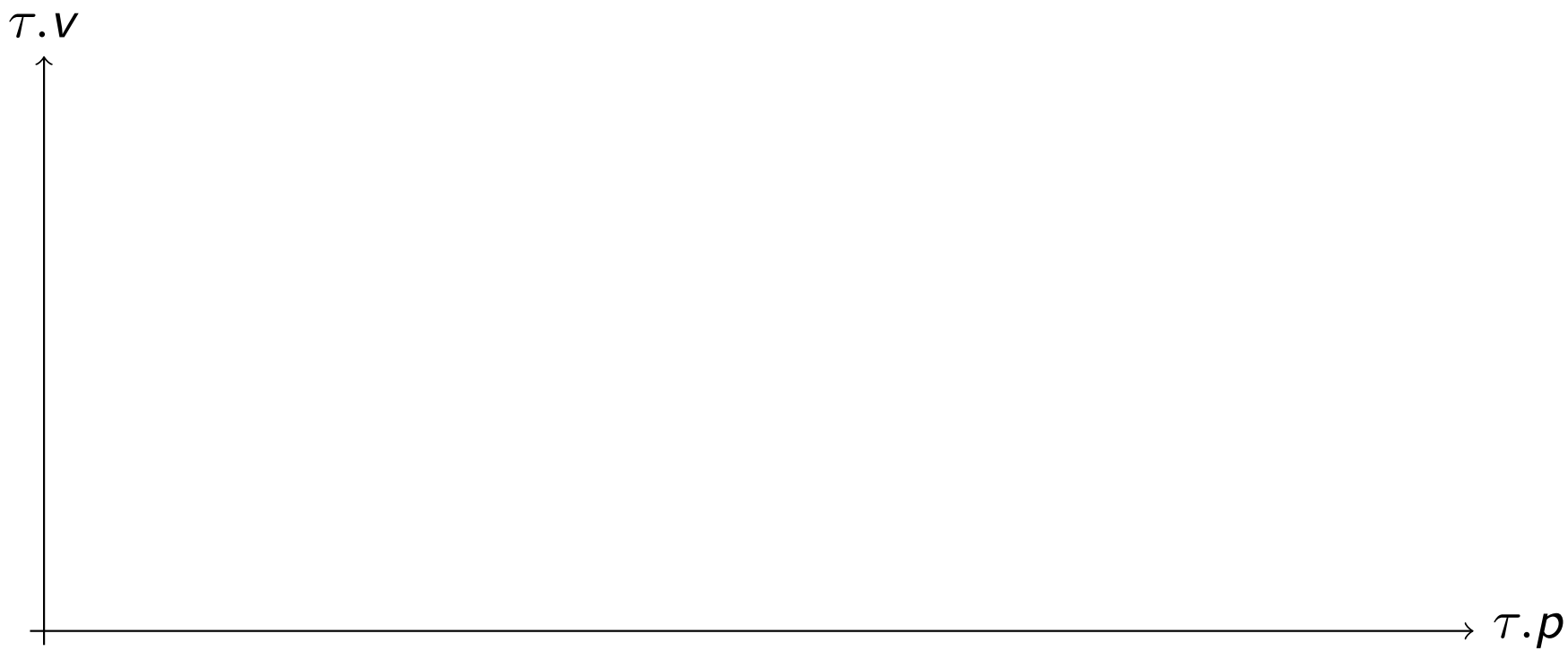


Example

$$\underbrace{\tau.v^2 \leq 2b(\mathbf{m}.e - \tau.p)}_{\text{Precondition}} \rightarrow [\underbrace{\tau.a := *;\ ?\tau.a \leq -b;\ \tau.p' = \tau.v, \tau.v' = \tau.a}_{\text{Operation model}}](\underbrace{\tau.p \leq \mathbf{m}.e}_{\text{Property}})$$

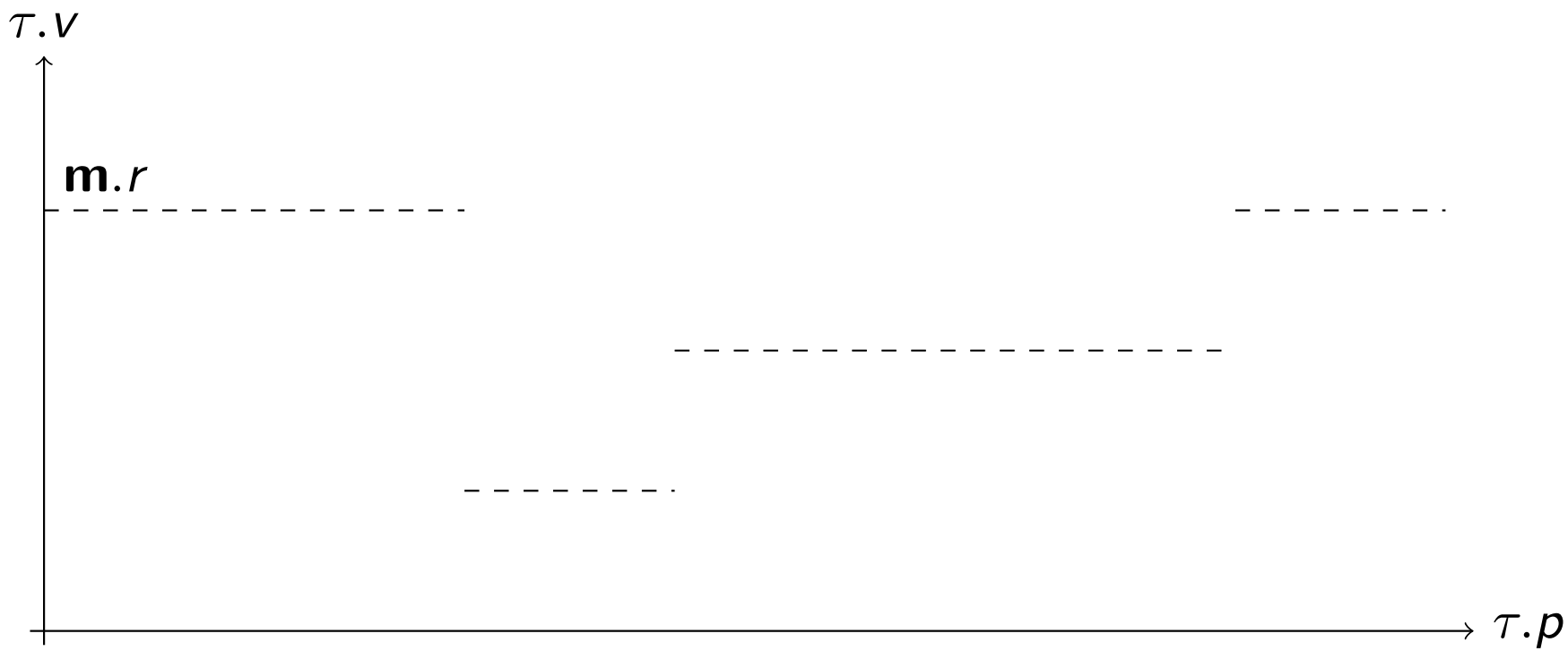
Test

3D Movement Authorities



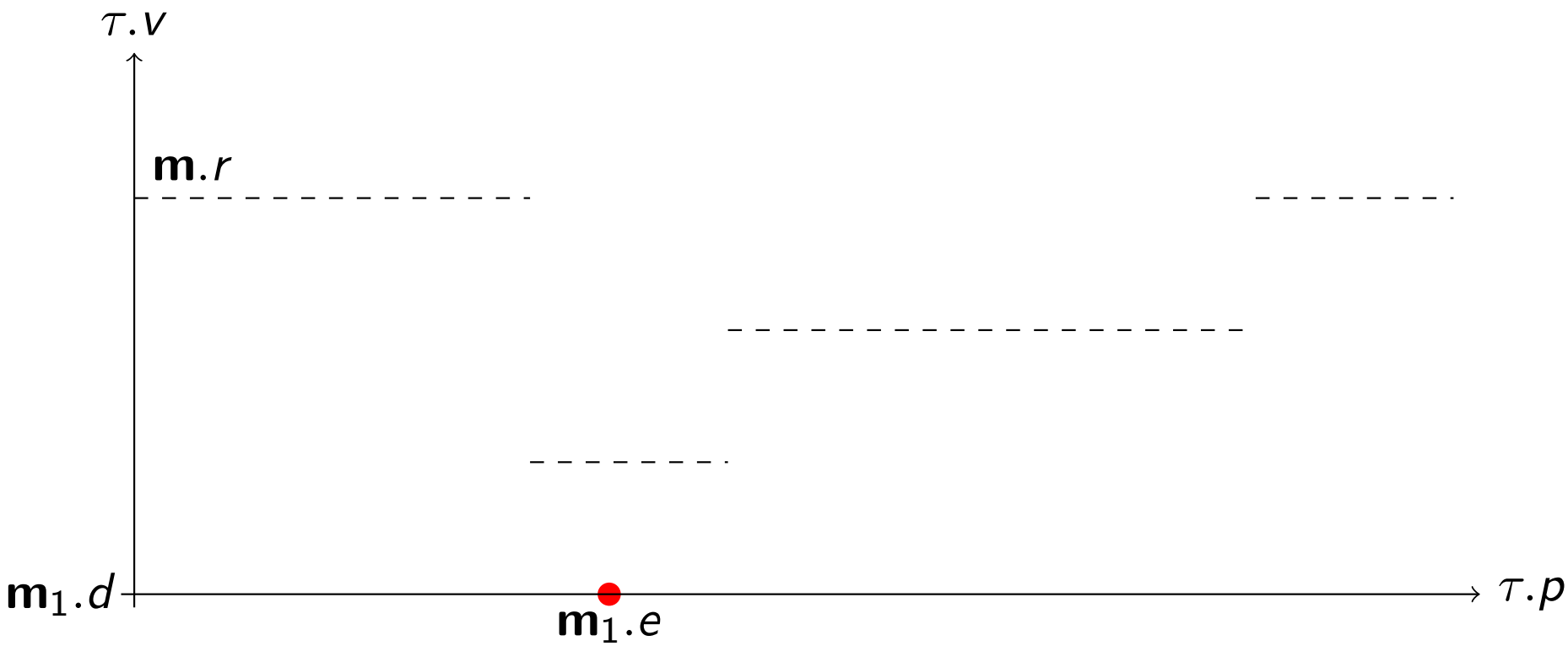
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



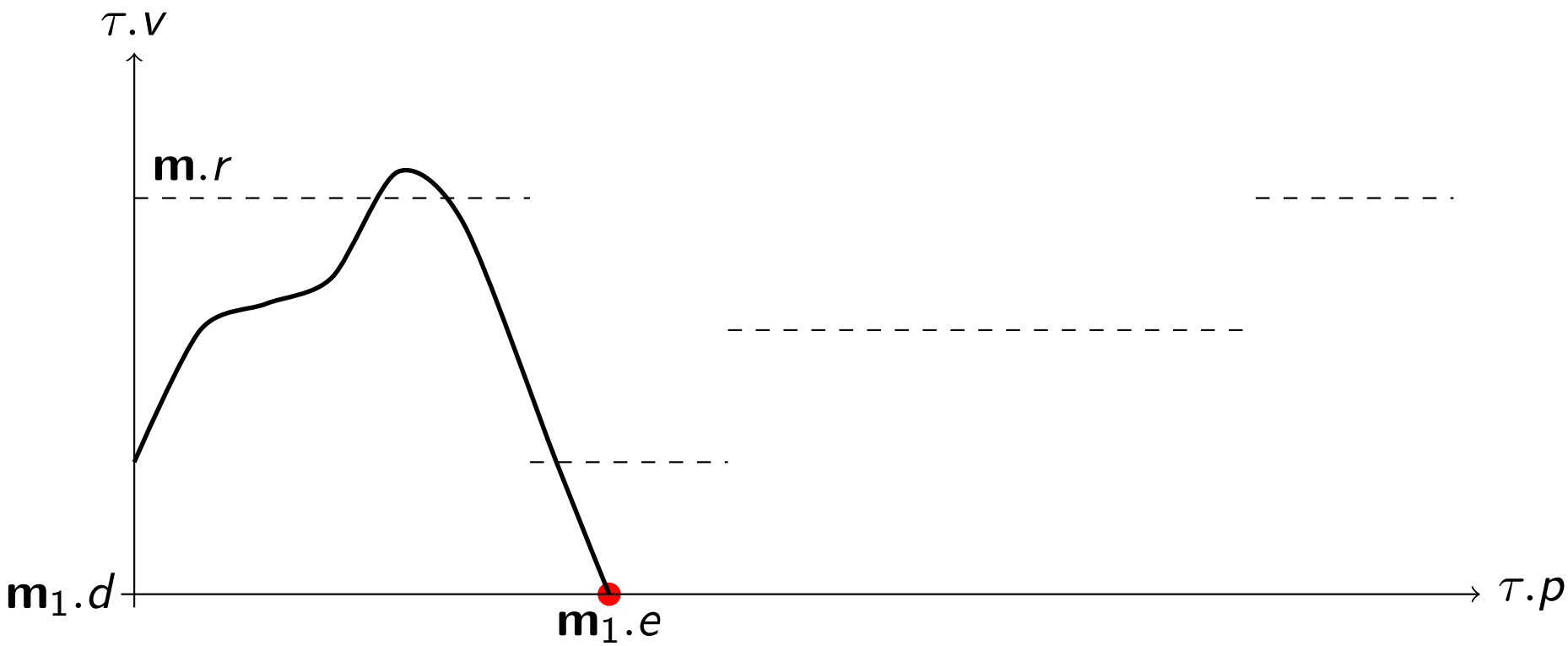
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



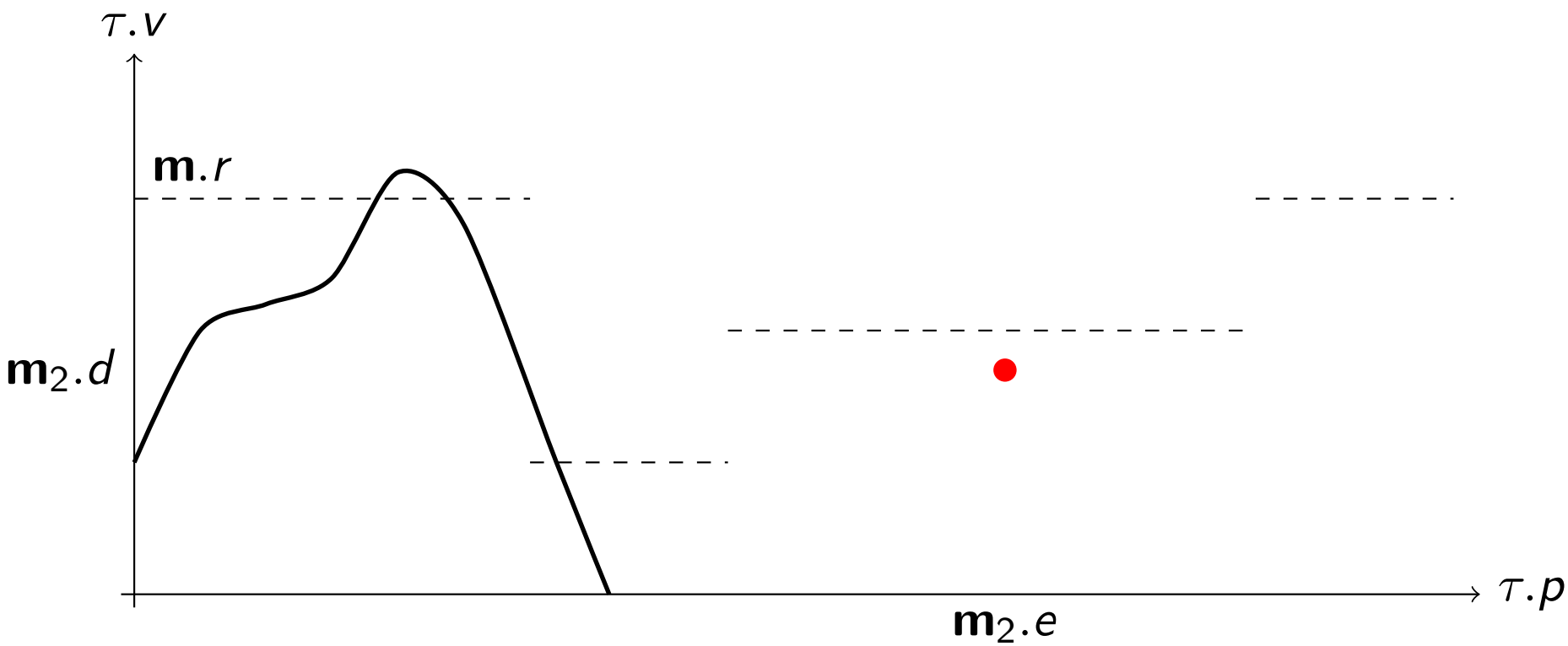
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



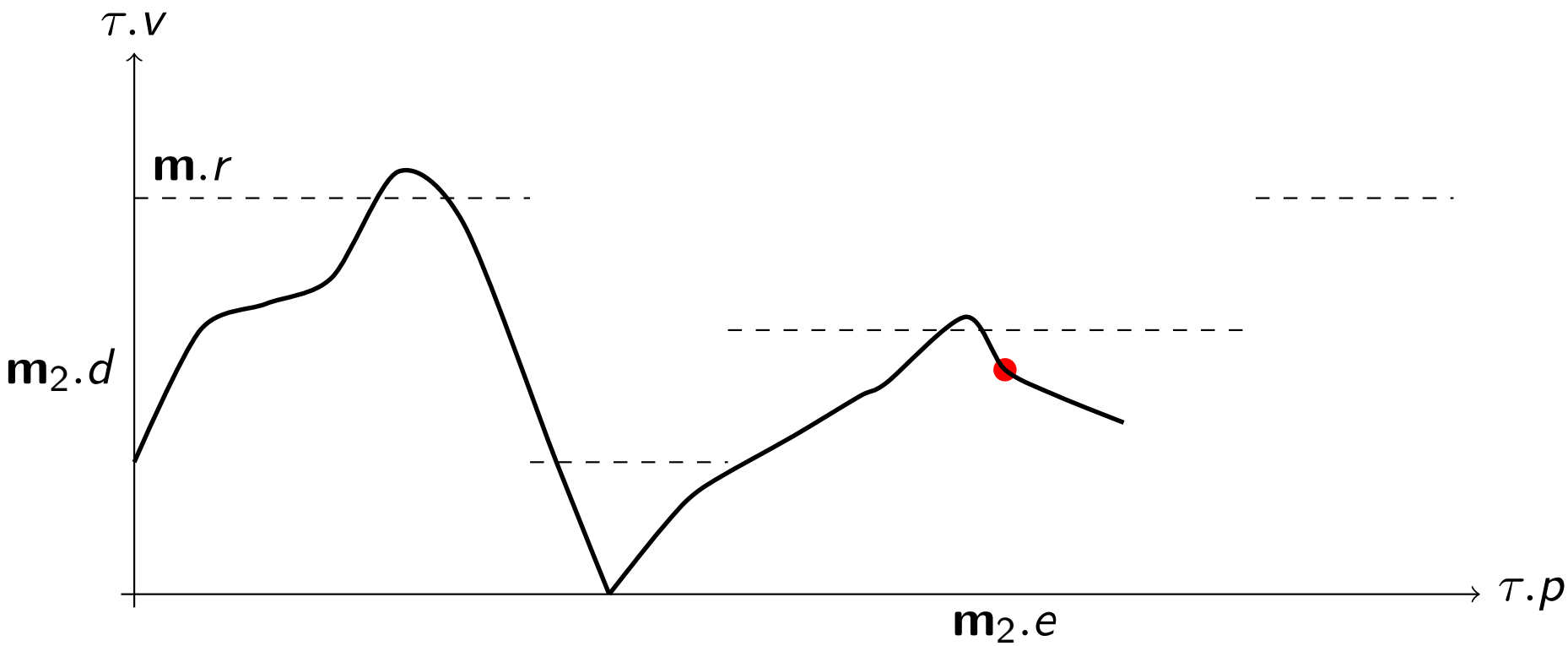
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



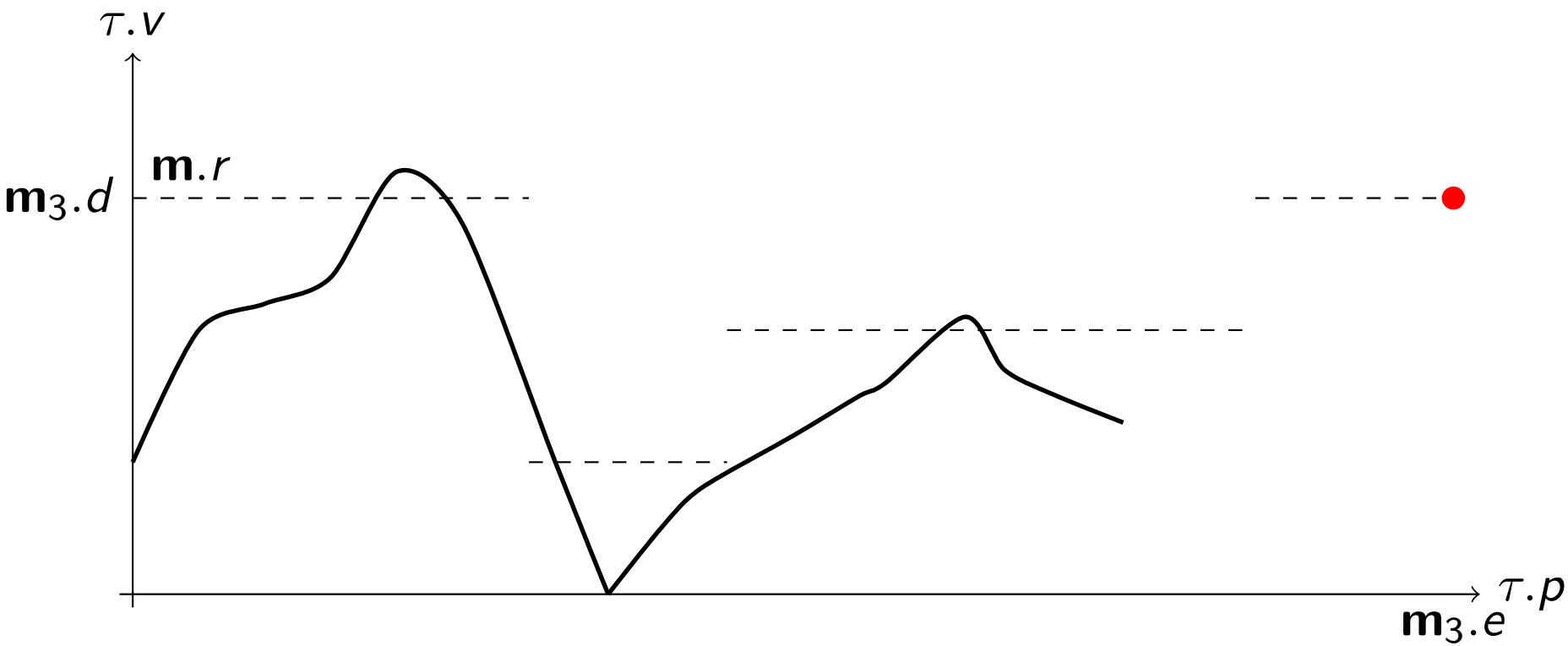
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

3D Movement Authorities



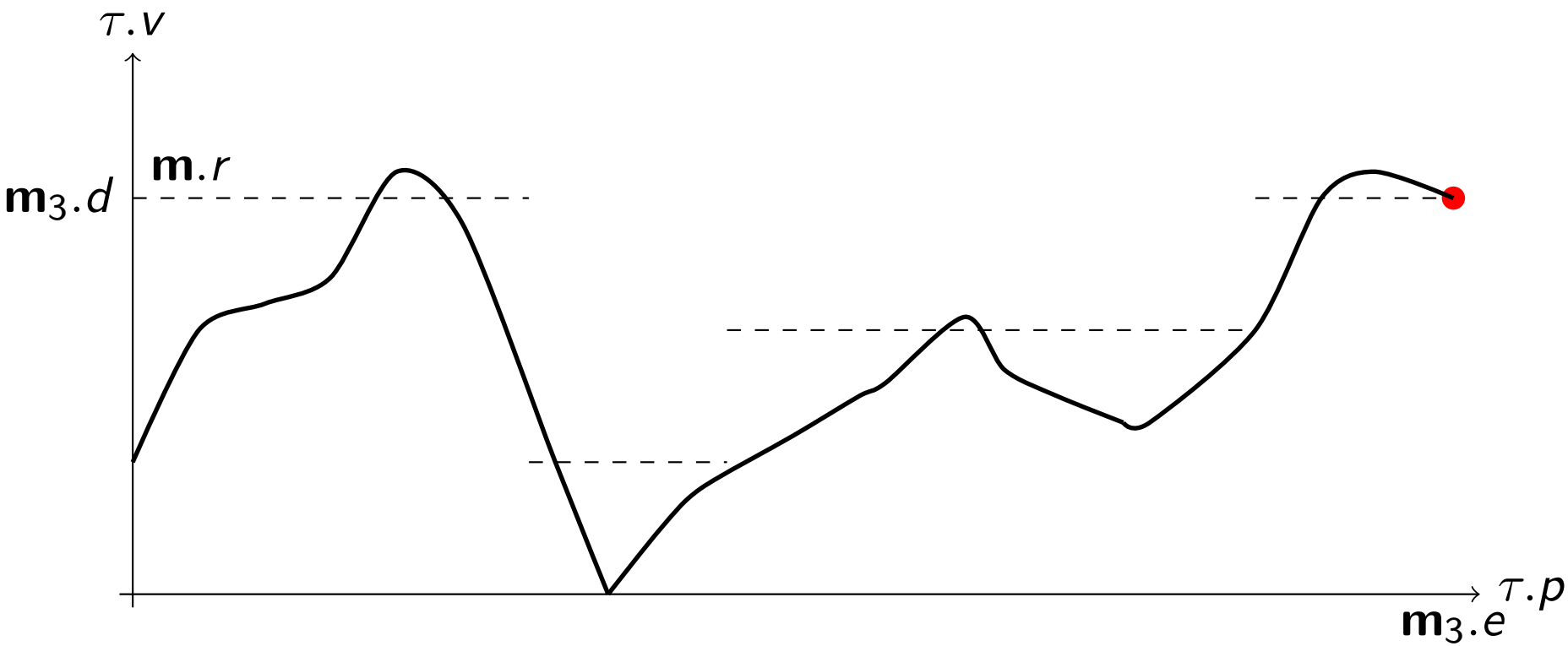
- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

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

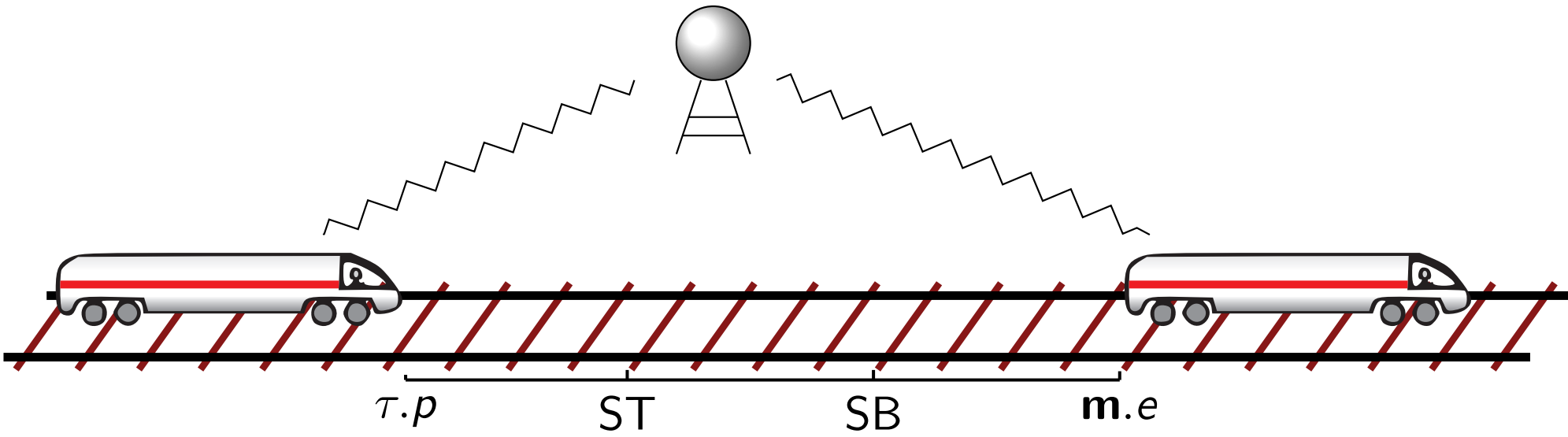


- Vectorial MA $\mathbf{m} = (d, e, r)$:
- Beyond point $\mathbf{m}.e$ train not faster than $\mathbf{m}.d$.
- Train should try to keep *recommended speed* $\mathbf{m}.r$

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.

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 $i, j \in \mathbb{N}$.

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 $M_i \cap M_j \neq \emptyset$,

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. $\square$

Model/State Variables

Train τ:

- $\tau.v$ 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:

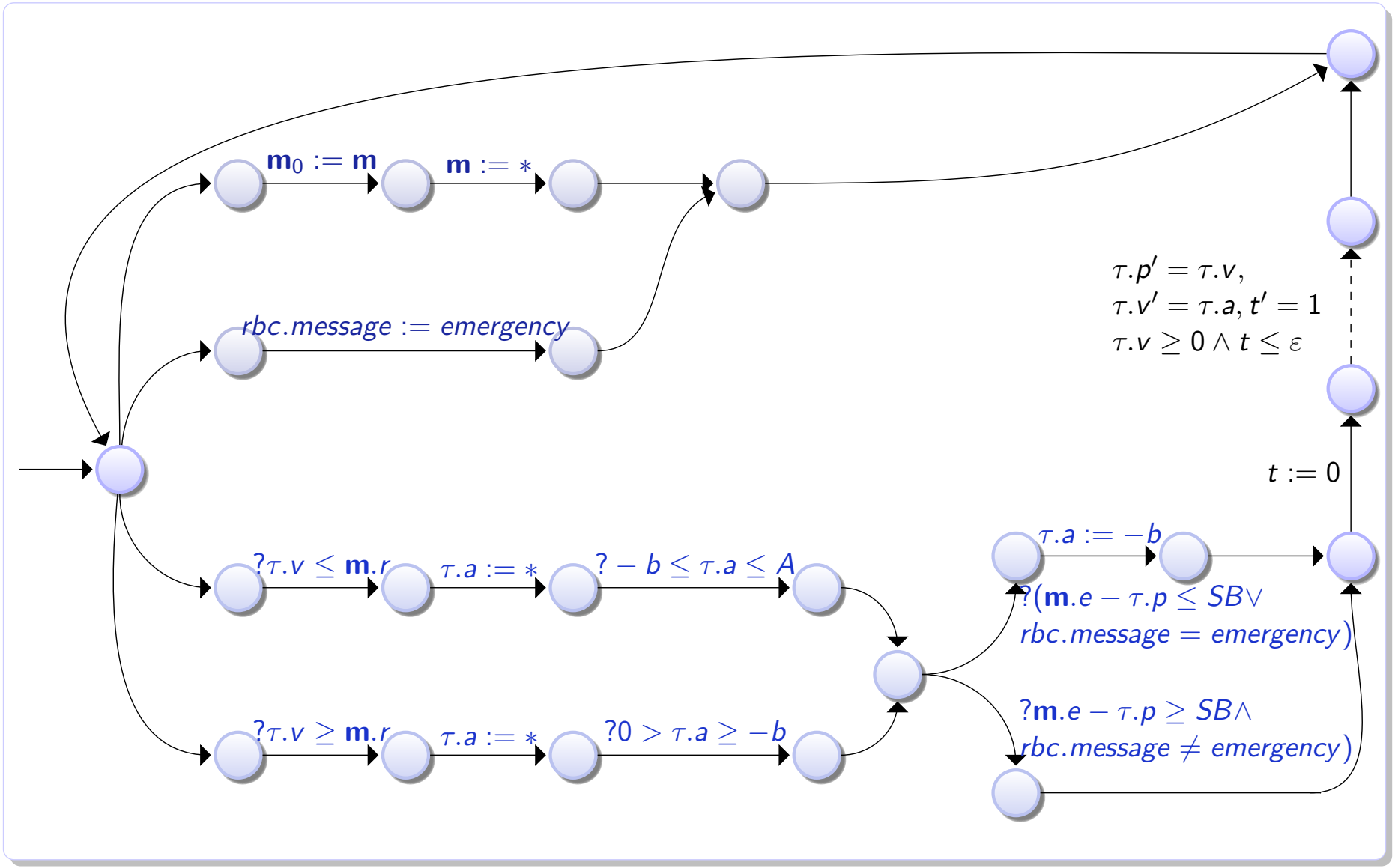
- SB Start Braking
- ST Start Talking
- b Braking power/deceleration
- a Maximum acceleration
- ε Maximum cycle time
- Δ Maximum expected communication delay

Parametric Skeleton of ETCS

Read from the informal specification...

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

As transition system...



Parametric Skeleton of ETCS

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

Example (Taks)

Verify safety

Parametric Skeleton of ETCS

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

Example (Taks)

Verify safety

Specification

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

Parametric Skeleton of ETCS

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

Example (Taks)

Verify safety

Specification

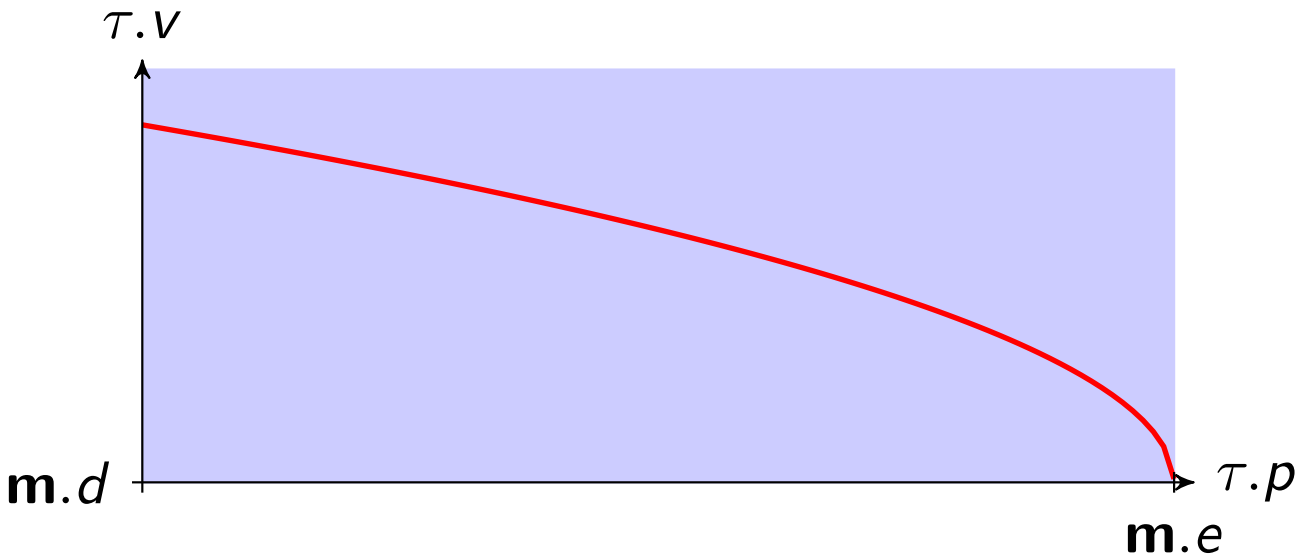
$[ETCS_{skel}](\tau.p \geq \mathbf{m}.e \rightarrow \tau.v \leq \mathbf{m}.d)$

Issue

Lots of counterexamples!

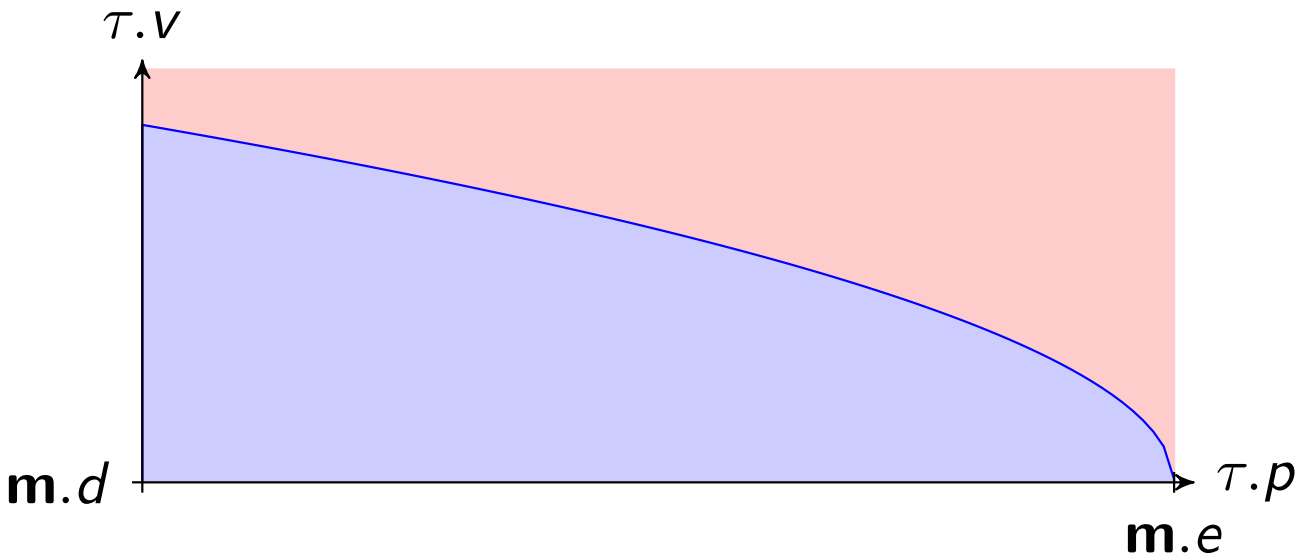
Iterative Control Refinement Process

Iterative Control Refinement Process



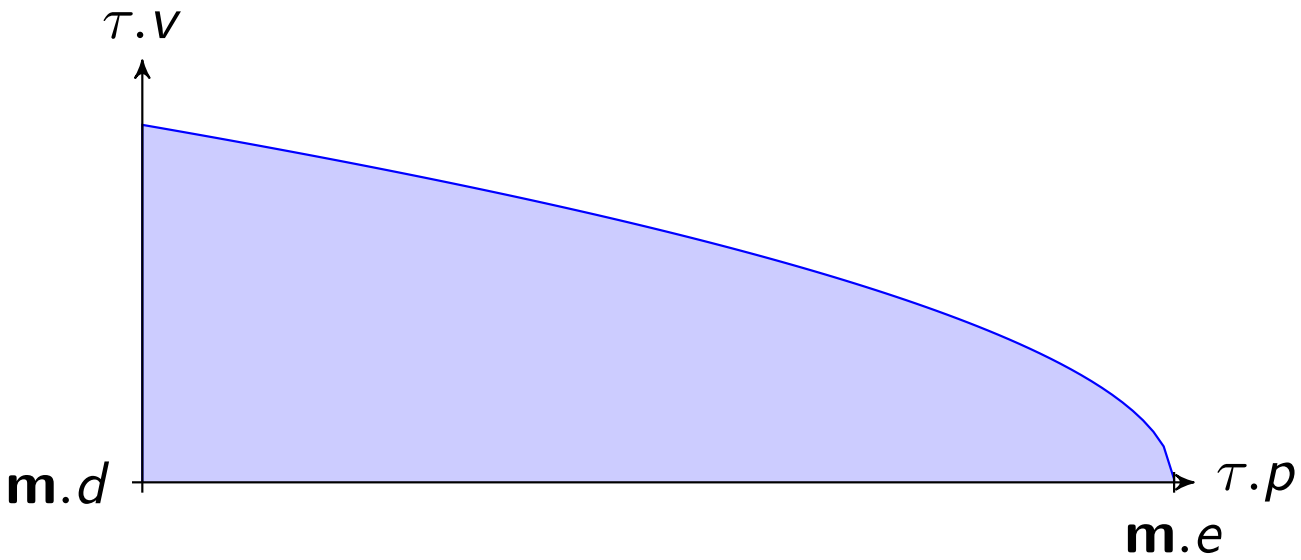
1. Controllability discovery

Iterative Control Refinement Process



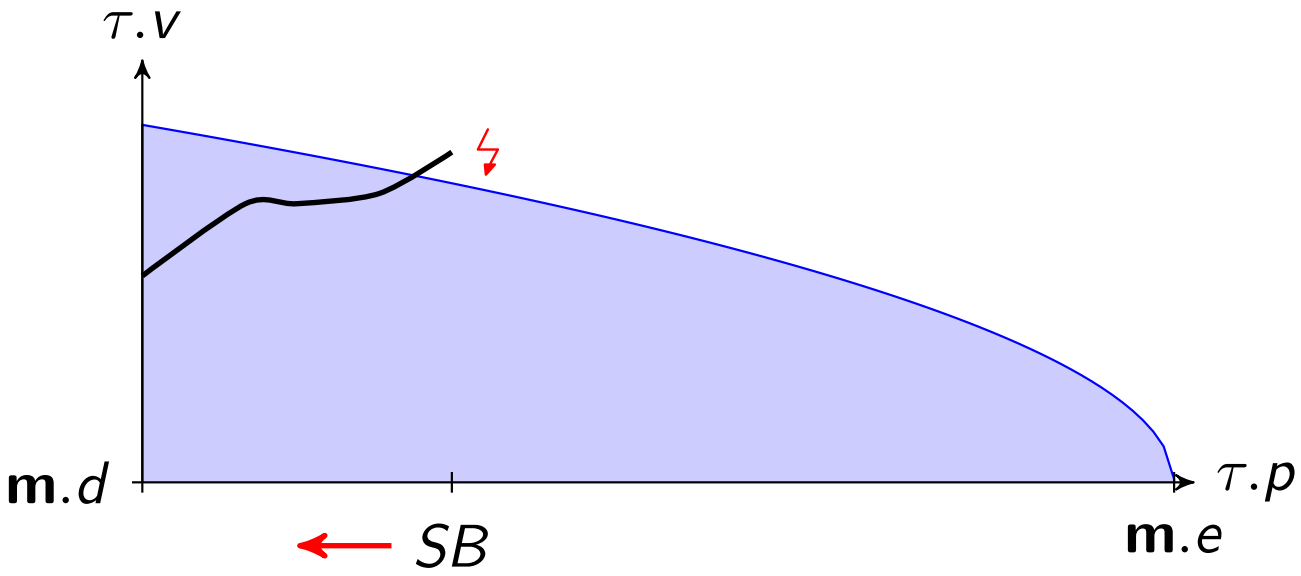
1. Controllability discovery

Iterative Control Refinement Process



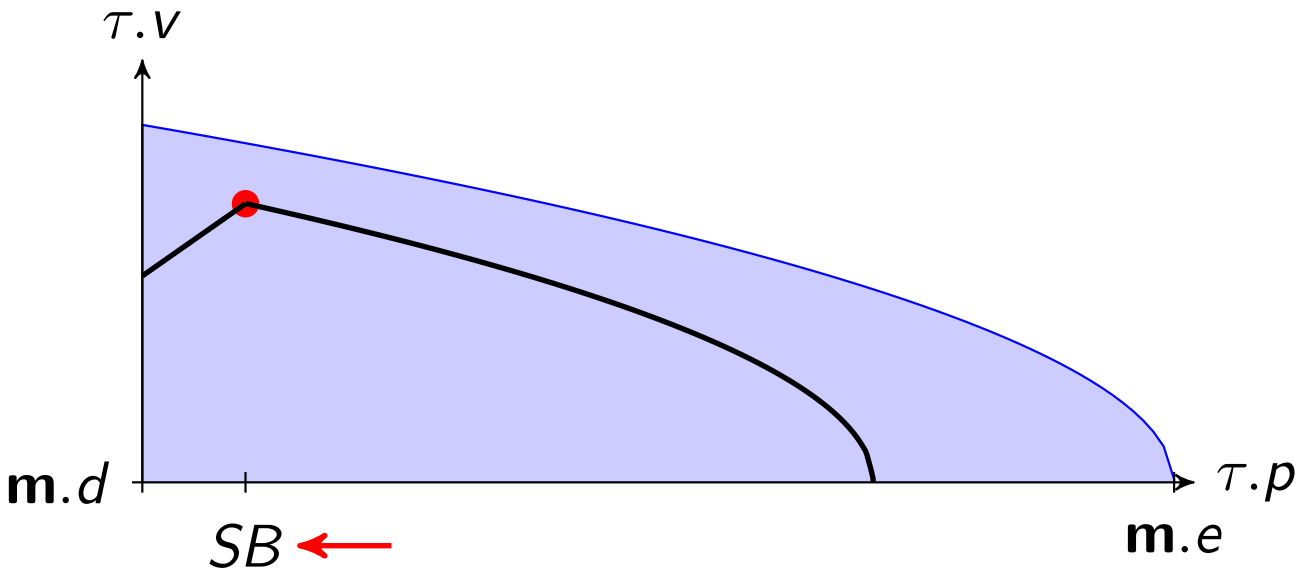
1. Controllability discovery

Iterative Control Refinement Process



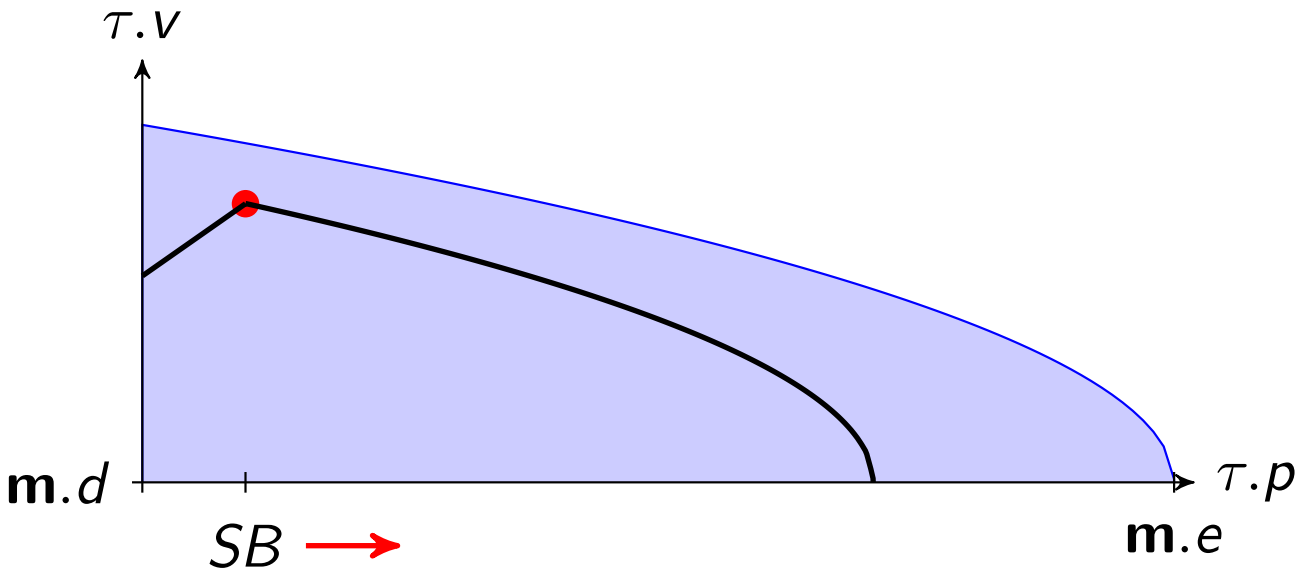
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



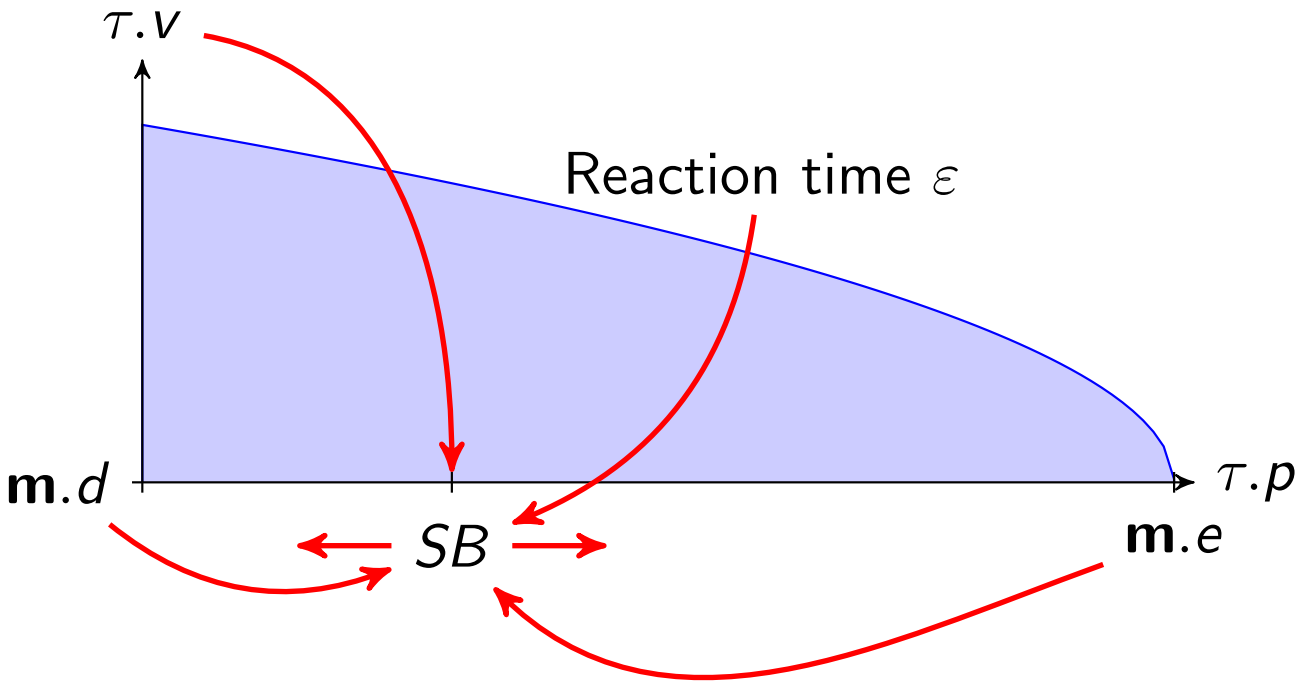
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



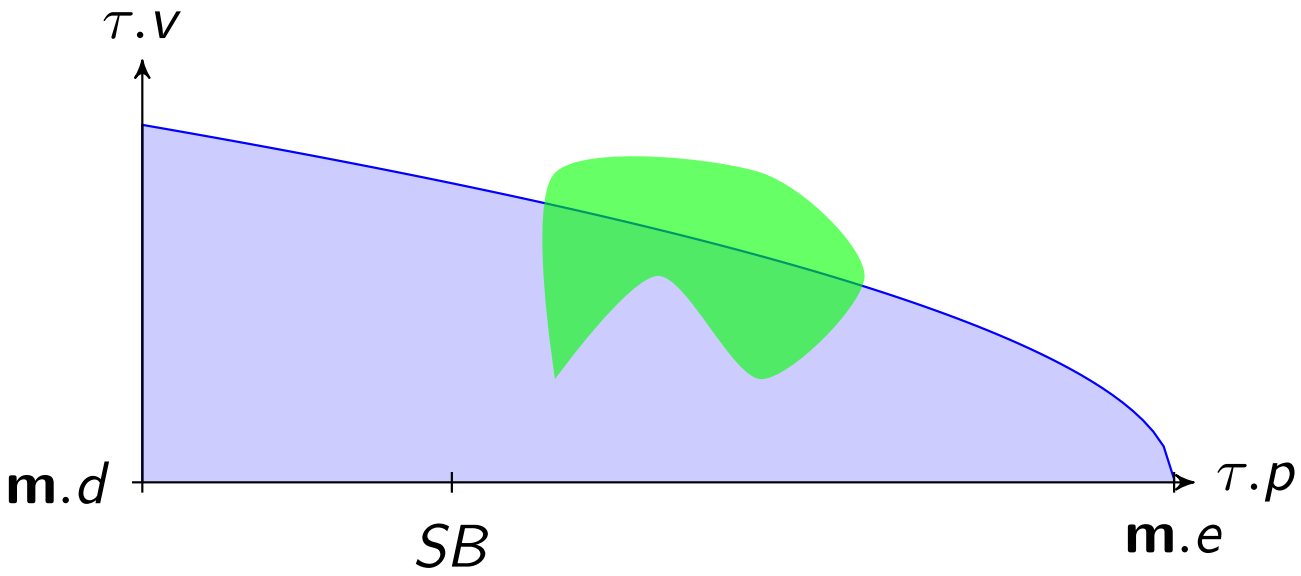
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



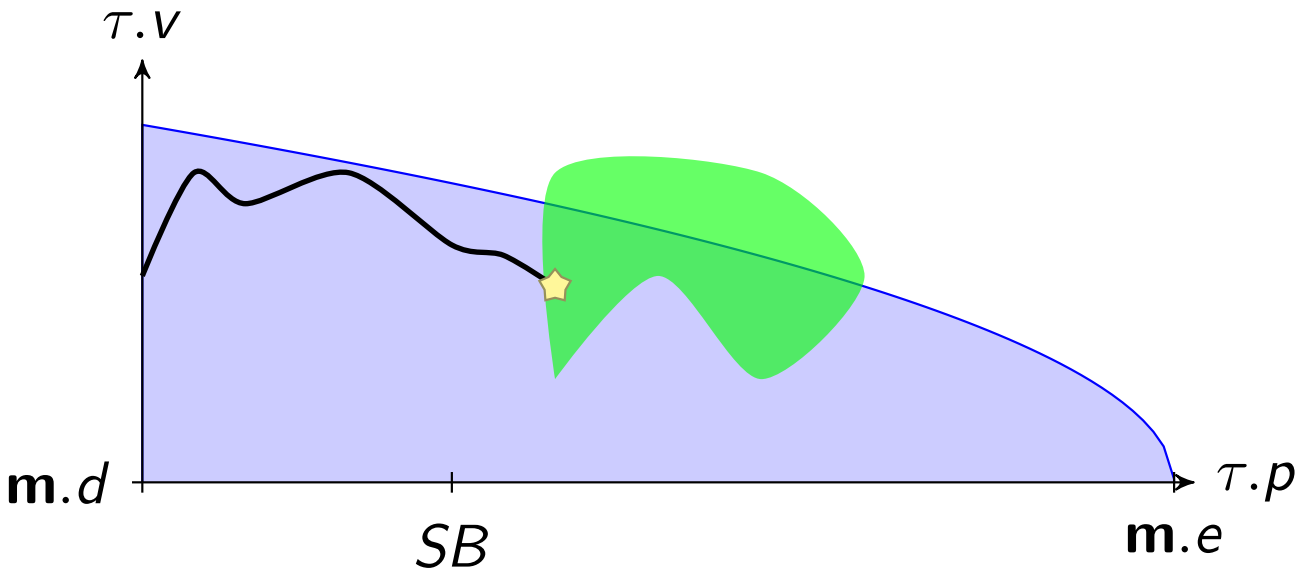
1. Controllability discovery
2. Control refinement

Iterative Control Refinement Process



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

Iterative Control Refinement Process

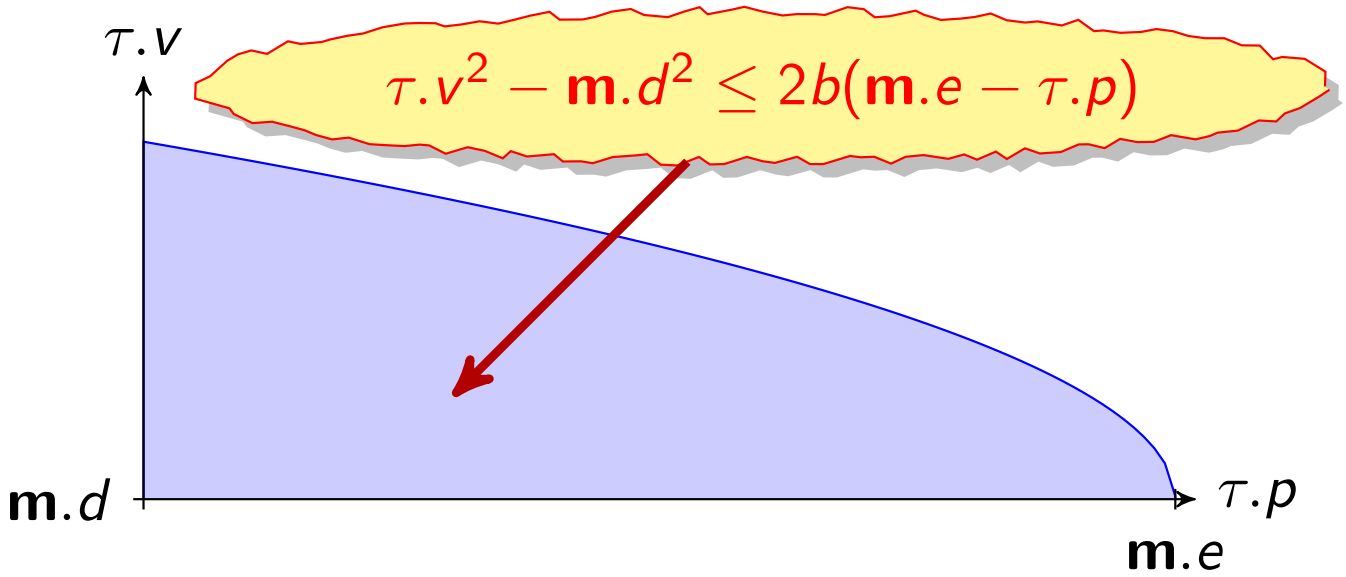


1. Controllability discovery
2. Control refinement
3. Repeat 2 until safety can be proven
4. Liveness check

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

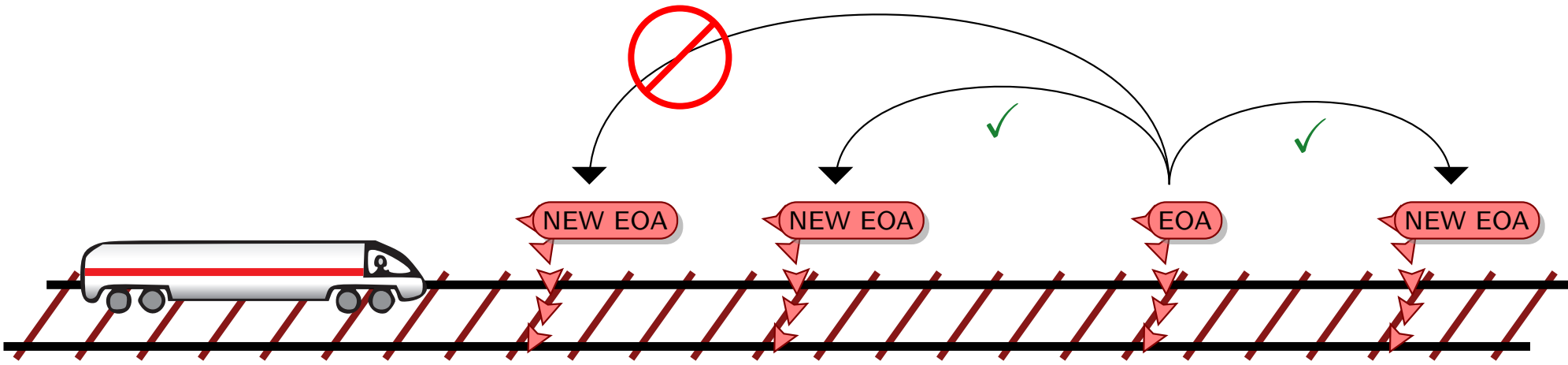


Proposition (Controllability)

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

$$\equiv \quad \tau.v^2 - \mathbf{m}.d^2 \leq 2b(\mathbf{m}.e - \tau.p) \qquad (\mathcal{C})$$

ETCS RBC Controllability



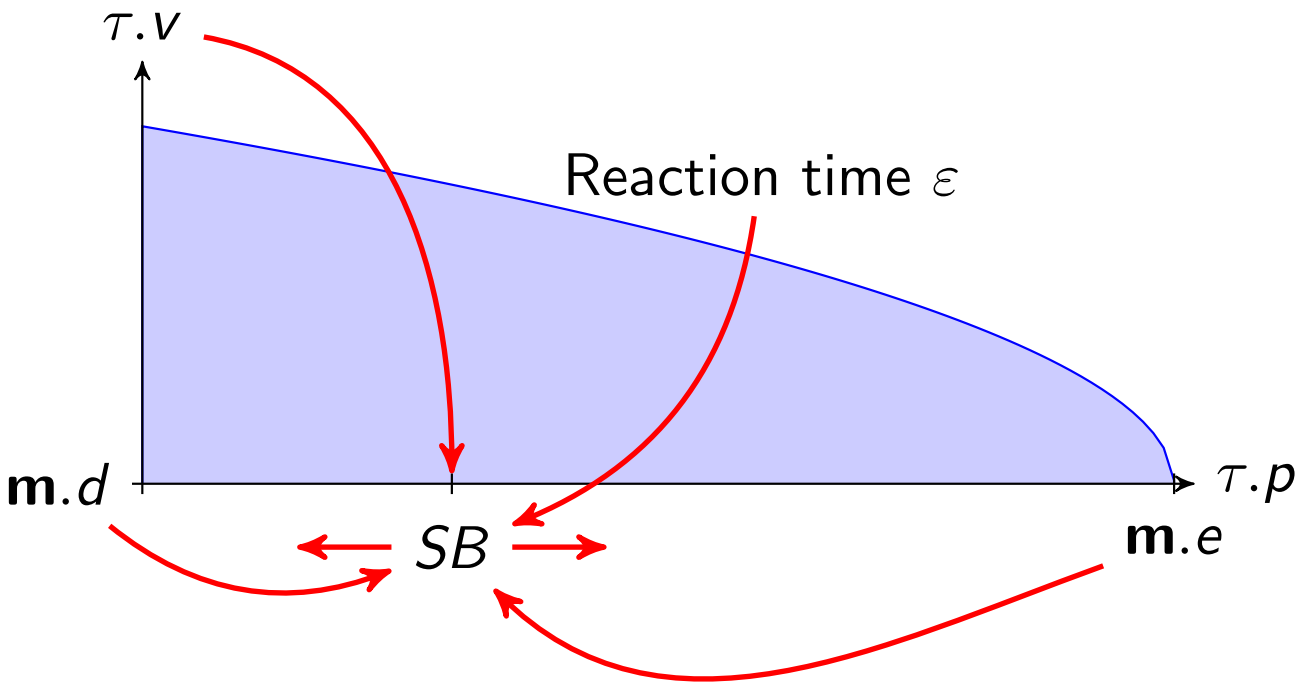
Proposition (RBC Controllability)

$$\mathbf{m}.d \geq 0 \wedge b > 0 \rightarrow [\mathbf{m}_0 := \mathbf{m};\ rbc] \Big($$

$$\mathbf{m}_0.d^2 - \mathbf{m}.d^2 \leq 2b(\mathbf{m}.e - \mathbf{m}_0.e) \wedge \mathbf{m}_0.d \geq 0 \wedge \mathbf{m}.d \geq 0 \leftrightarrow$$

$$\forall \tau \left((\langle \mathbf{m} := \mathbf{m}_0 \rangle \mathcal{C}) \rightarrow \mathcal{C} \right) \Big)$$

ETCS Reactivity



Proposition (Reactivity)

$$\left(\forall \mathbf{m}.e\, \forall \tau.p\, \left(\mathbf{m}.e - \tau.p \geq SB \wedge \mathcal{C} \rightarrow [\tau.a := a;\ drive]\, \mathcal{C}\right)\right)$$

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

Refined ETCS Control

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

Refined ETCS Control

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

Specification

$$\tau.v^2 - \mathbf{m}.d^2 \leq 2b(\mathbf{m}.e - \tau.p) \rightarrow [ETCS_r](\tau.p \geq \mathbf{m}.e \rightarrow \tau.v \leq \mathbf{m}.d)$$

Refined ETCS Control

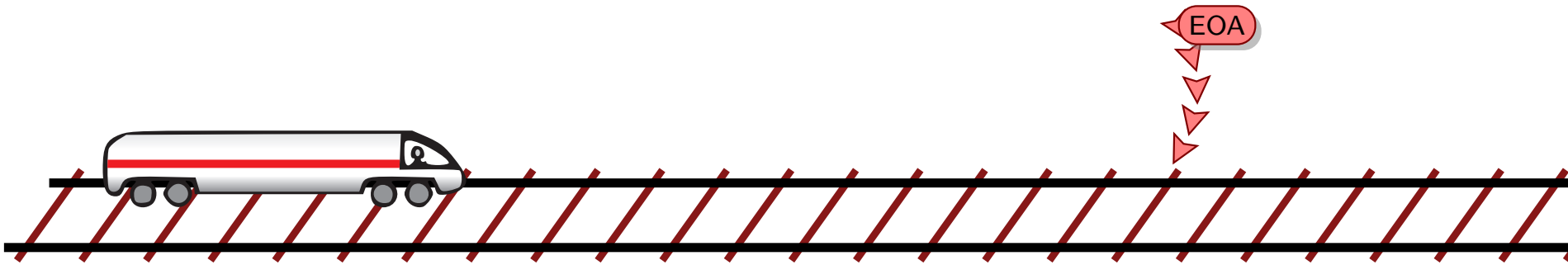
$$
\begin{array}{lcl}
ETCS_r: & & (train \cup rbc)^* \\
train & : & spd;\ atp;\ drive \\
spd & : & (?\tau.v \leq \mathbf{m}.r;\ \tau.a := *;\ ? - b \leq \tau.a \leq A) \\
 & & \cup (?\tau.v \geq \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \geq -b) \\
atp & : & SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b}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

Necessary for safety

Specification

$$\tau.v^2 - \mathbf{m}.d^2 \leq 2b(\mathbf{m}.e - \tau.p) \rightarrow [ETCS_r](\tau.p \geq \mathbf{m}.e \rightarrow \tau.v \leq \mathbf{m}.d)$$

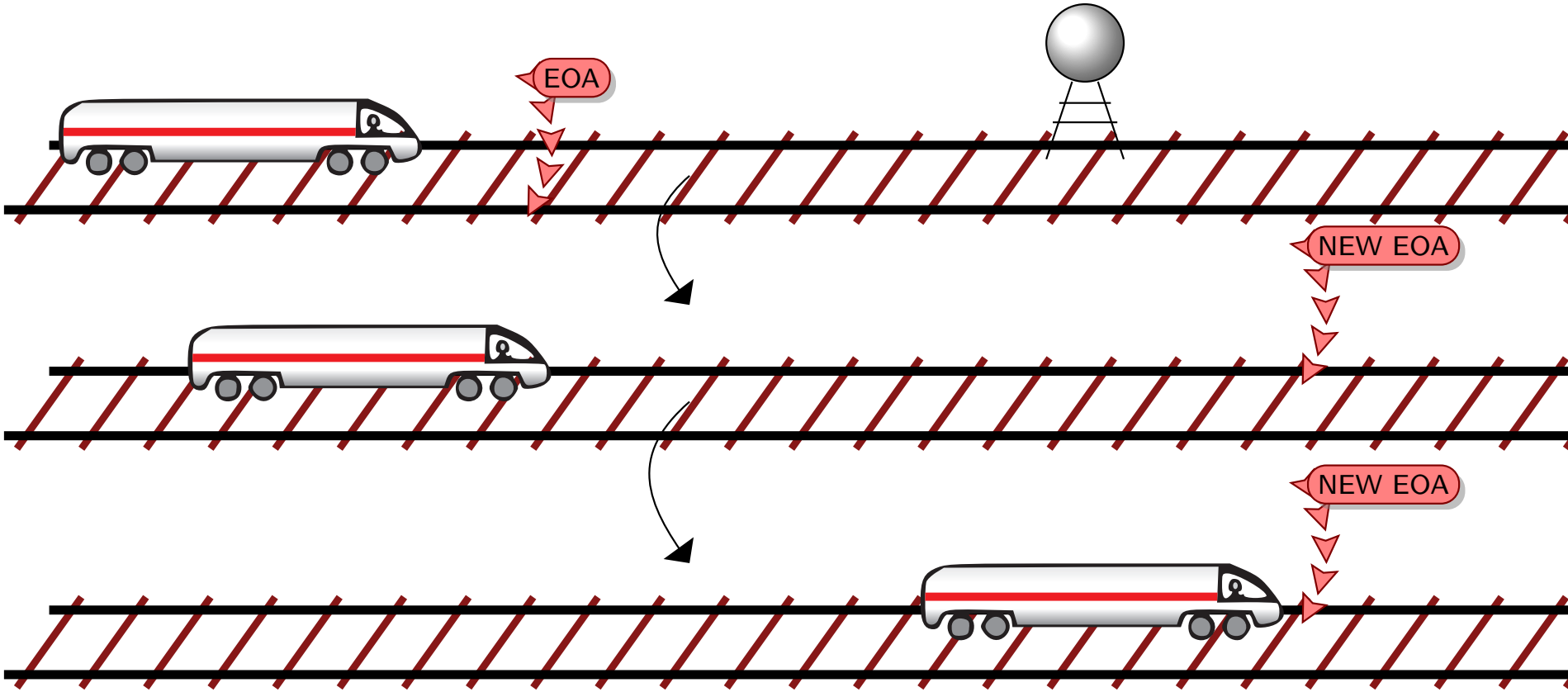
ETCS Safety



Proposition (Safety)

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

ETCS Liveness



Proposition (Liveness)

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

Outline

1. Train Control
   - Separation Principle
   - Parametric ETCS
2. Parametric European Train Control System
   - Controllability
   - Reactivity
   - Refined Control
   - Safety
   - Liveness
3. Enhancements
4. Summary

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

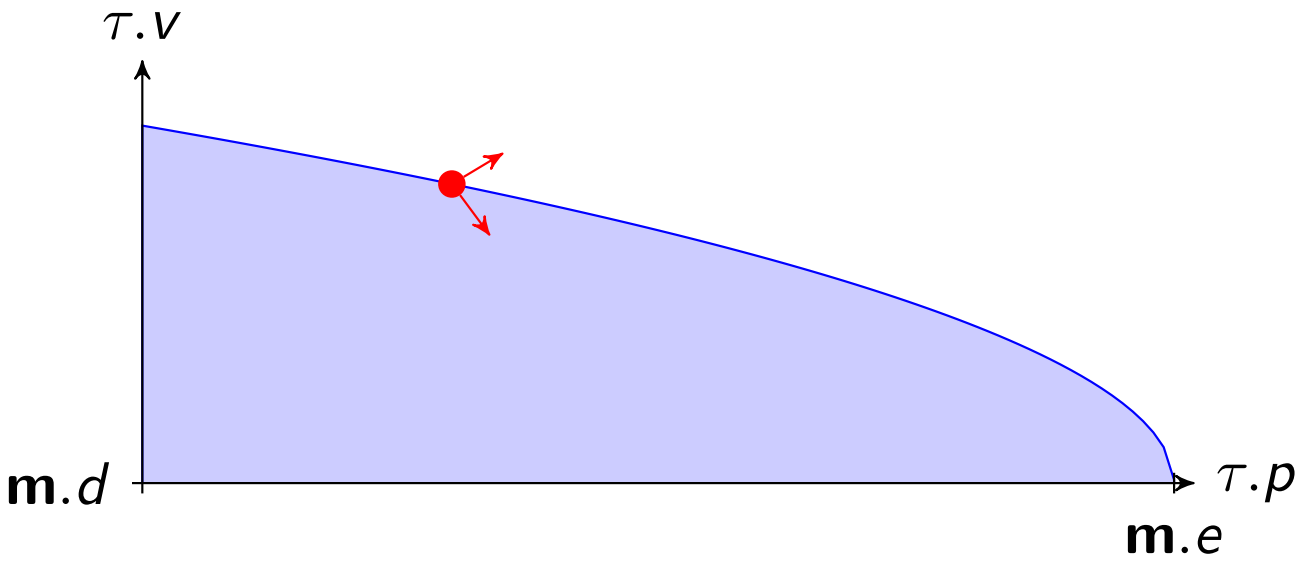
Issue

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 $\tau.v' = \tau.a$.

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

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

Platzer, A.:
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput. **20**(1) (2010) DOI 10.1093/logcom/exn070.

Realistic Speed Control

So far

Almost completely non-deterministic control.

Realistic Speed Control

So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

Realistic Speed Control

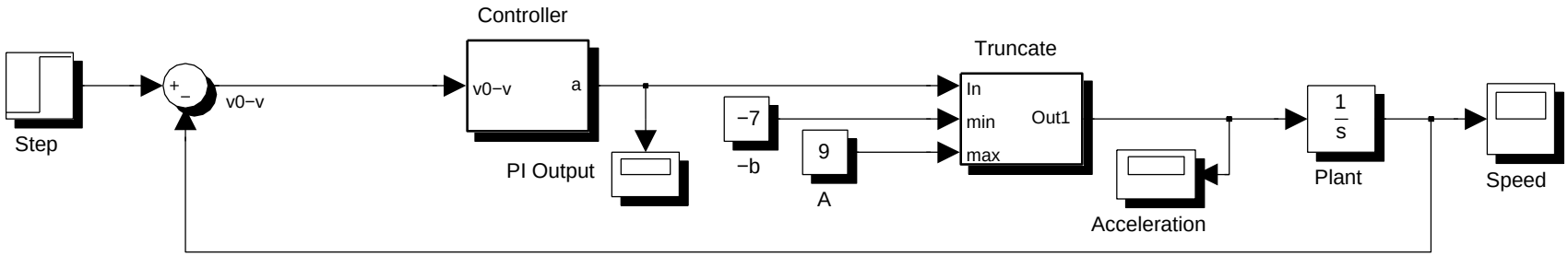
So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

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



Realistic Speed Control

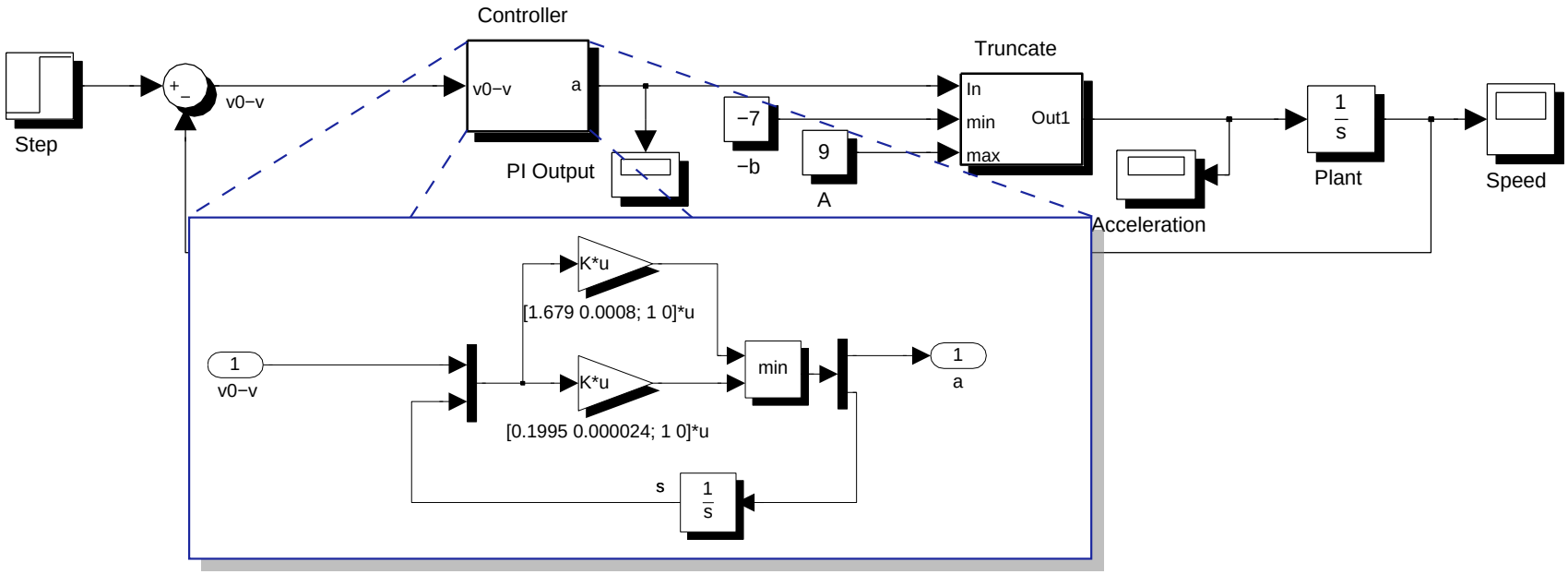
So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

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



Realistic Speed Control

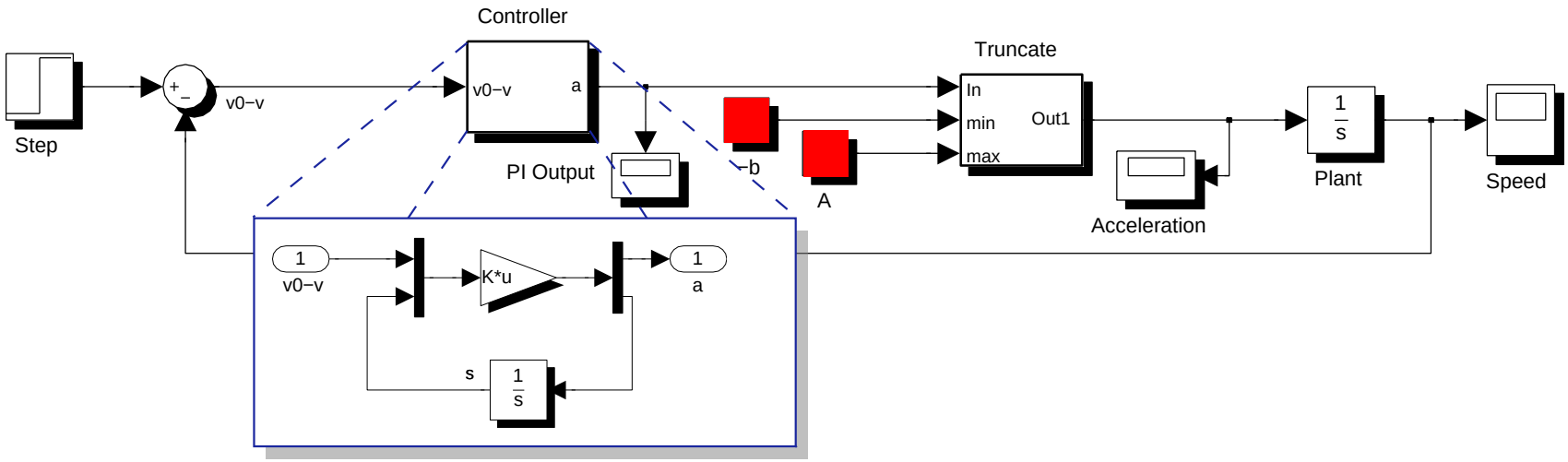
So far

Almost completely non-deterministic control.

Issue

This is unrealistic!

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



Differential equation system

$$\tau.v' = \min\Big(a, \max\big(-b,\ \ell(\tau.v - \mathbf{m}.r) - i\,s - c\,\mathbf{m}.r\big)\Big) \wedge s' = \tau.v - \mathbf{m}.r$$

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

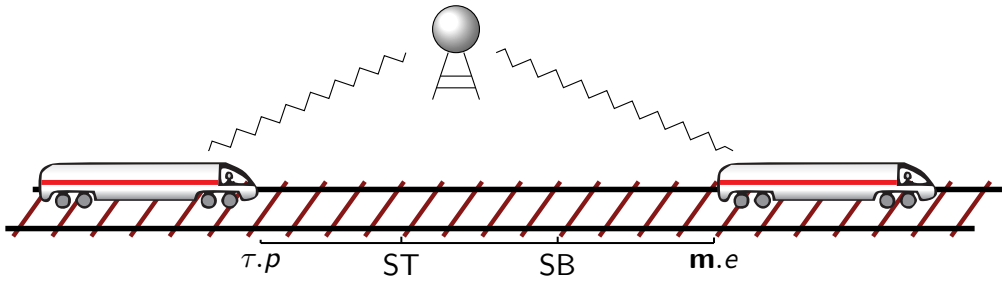
Cannot solve differential equations really. Use differential invariants! For details see later.


Platzer, A.:
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput. **20**(1) (2010) DOI 10.1093/logcom/exn070.

Outline

1. Train Control
   - Separation Principle
   - Parametric ETCS
2. Parametric European Train Control System
   - Controllability
   - Reactivity
   - Refined Control
   - Safety
   - Liveness
3. Enhancements
4. Summary

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