Verified Train Controllers for the Federal Railroad Administration Train Kinematics Model:

Balancing Competing Brake and Track Forces

Aditi Kabra Stefan Mitsch André Platzer

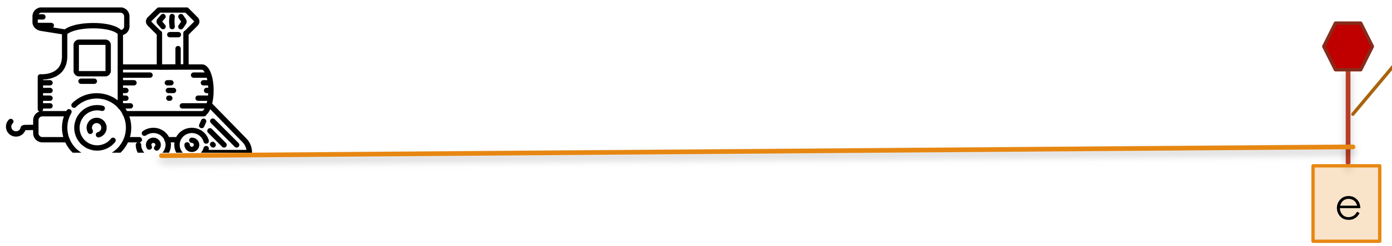
Computer Science Department,
Carnegie Mellon University

INTERNATIONAL CONFERENCE ON EMBEDDED SOFTWARE 2022

Supported by FRA contract number 693JJ620C000025

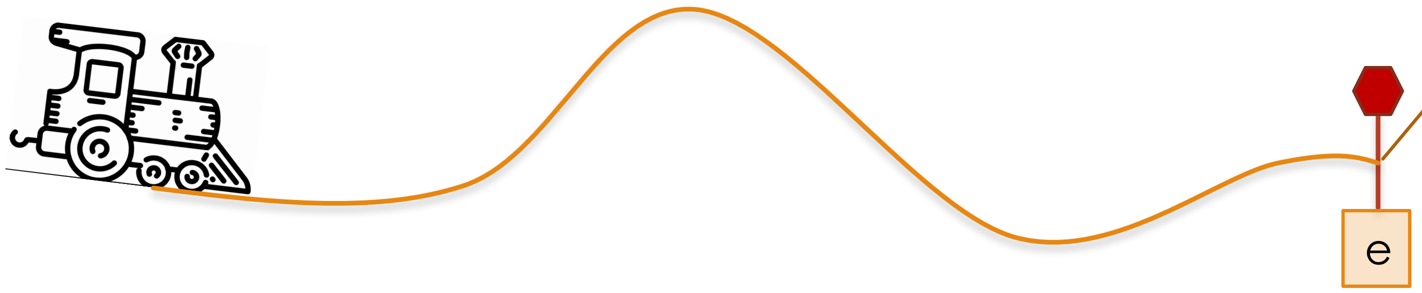

M
M.

Train Control: Complicated



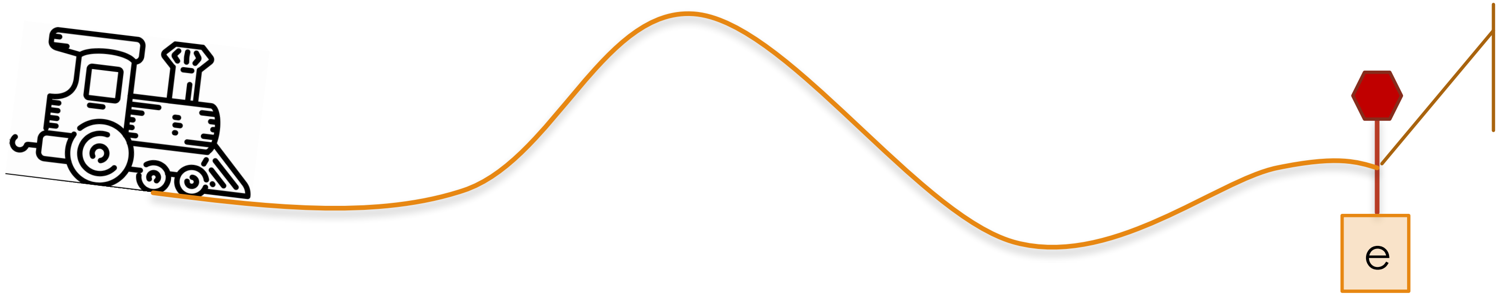
End of *movement authority*: the train must stop by this point

Train Control: Complicated

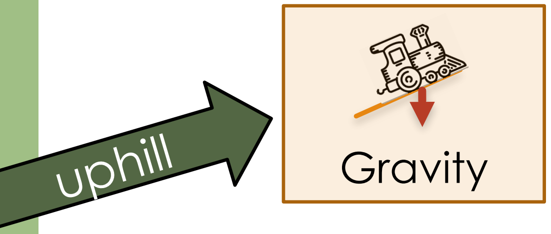


End of *movement authority*: the train must stop by this point

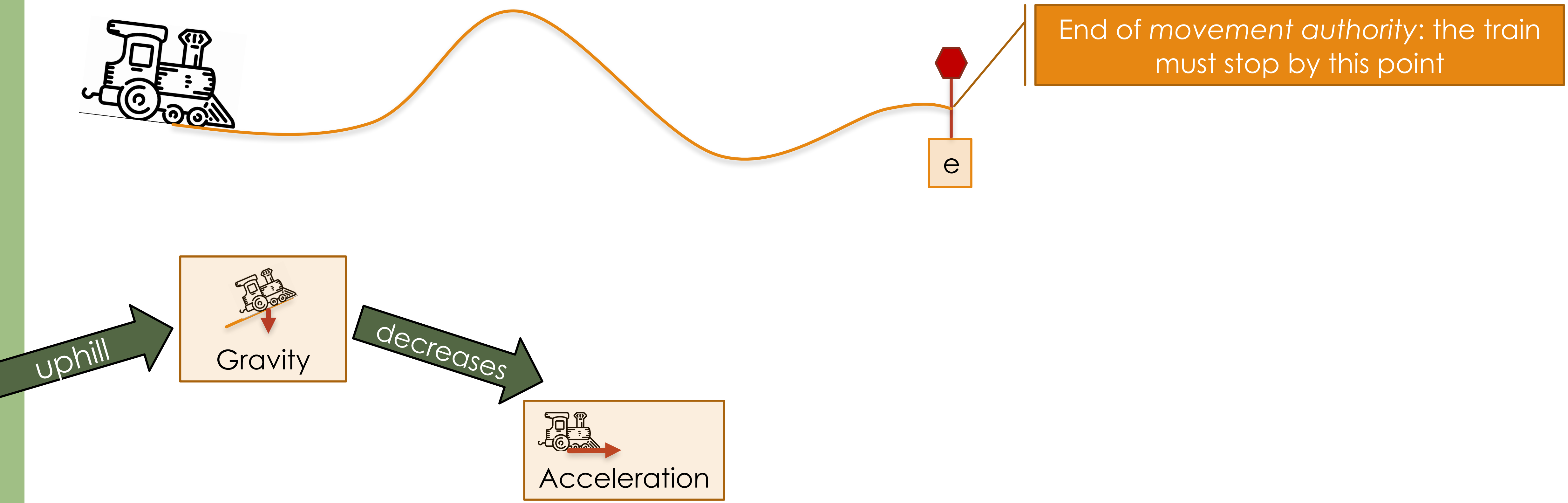
Train Control: Complicated



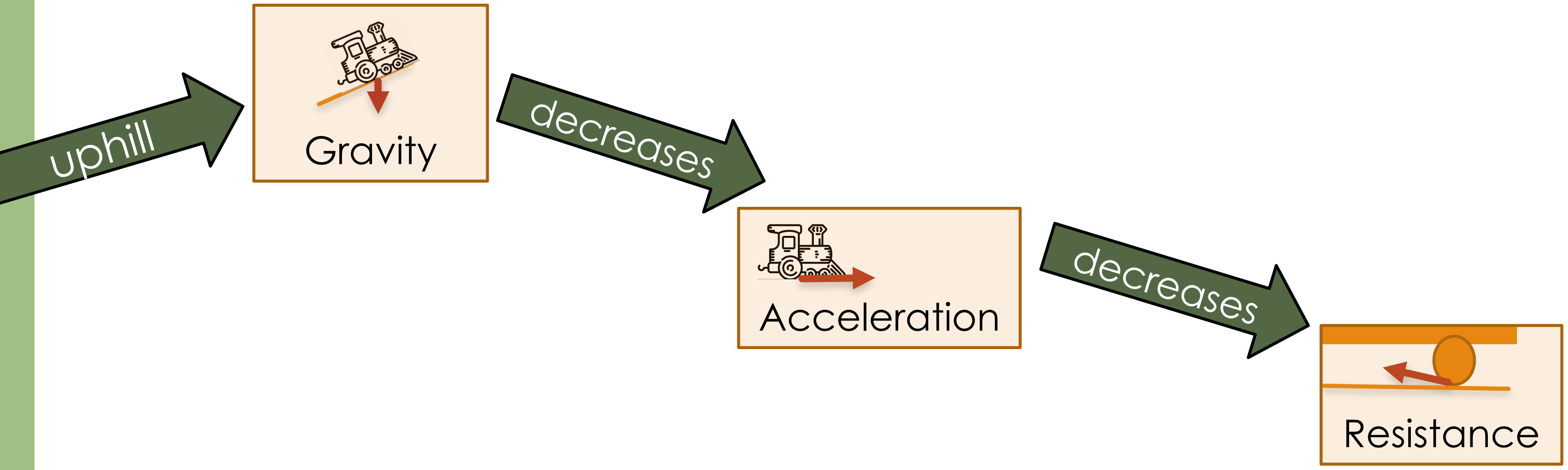
End of *movement authority*: the train must stop by this point



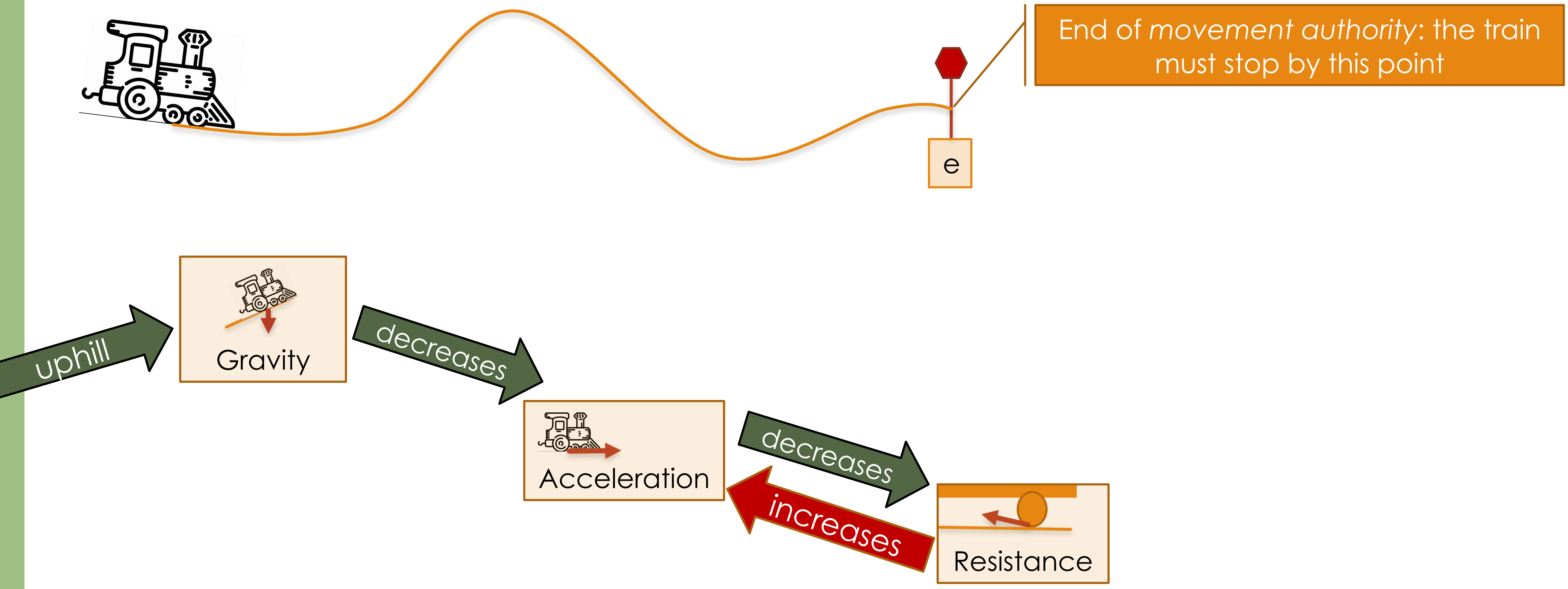
Train Control: Complicated



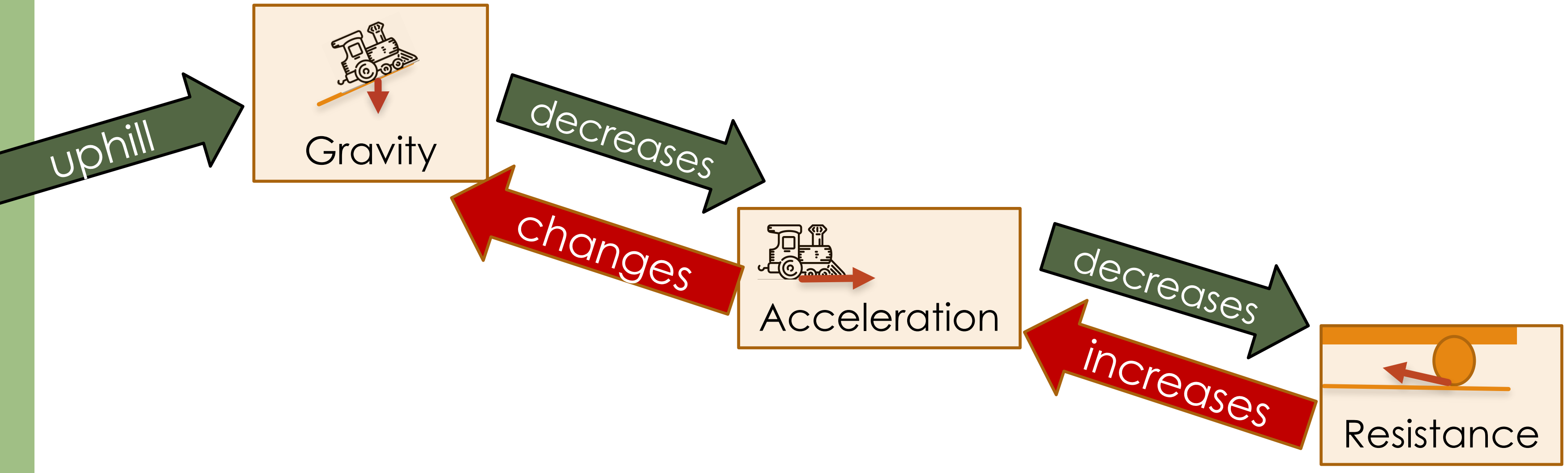
Train Control: Complicated



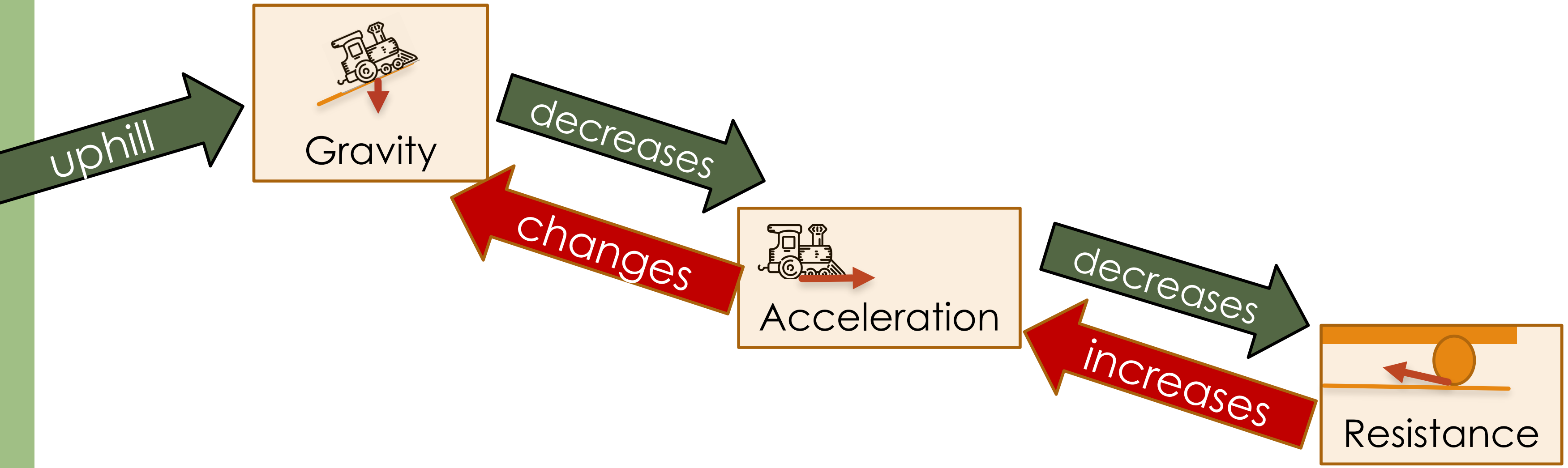
Train Control: Complicated

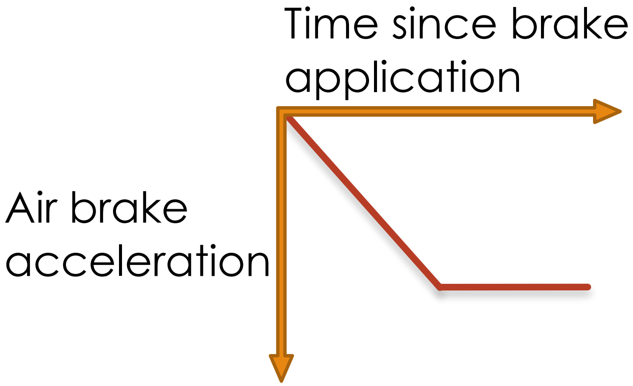


Train Control: Complicated

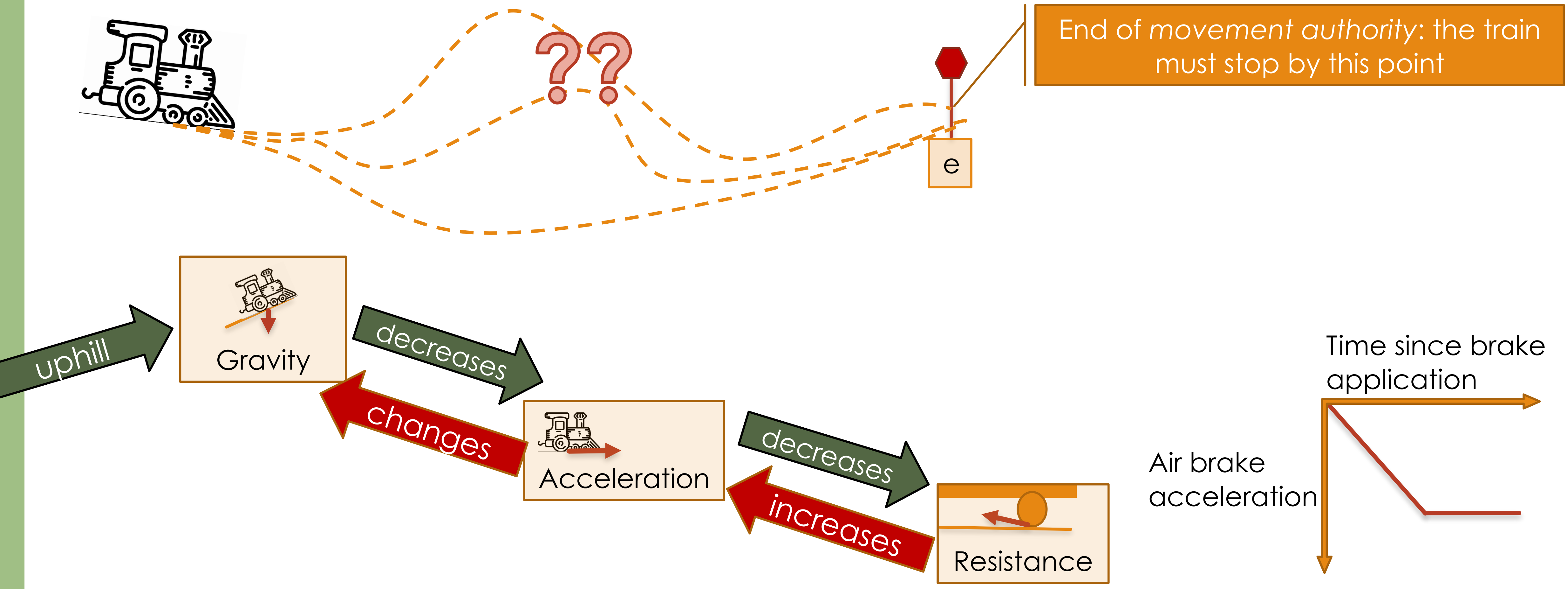


Train Control: Complicated

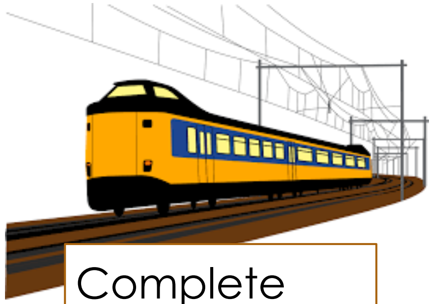




Train Control: Complicated



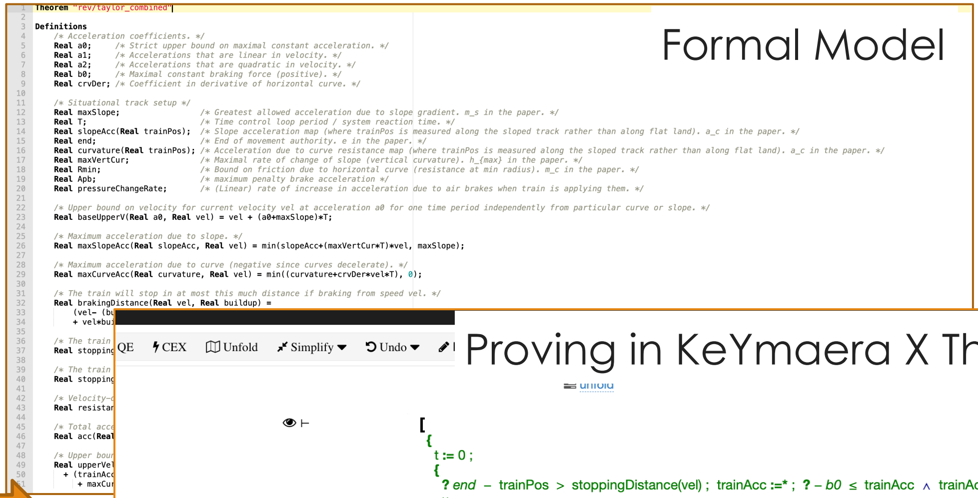
Formal Verification



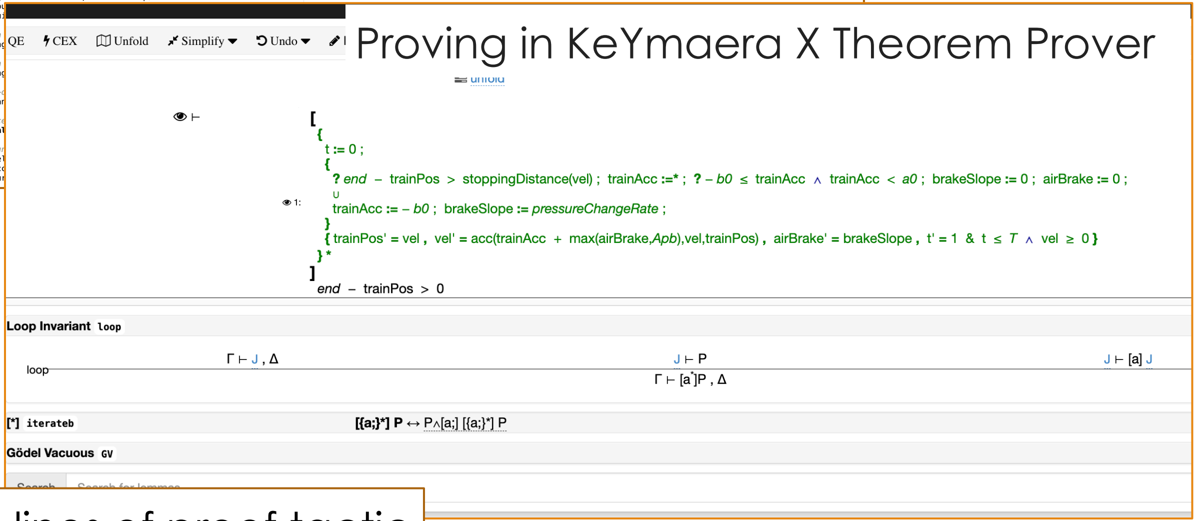
Complete
FRA Model[1]

[1] J. Brosseau and B. M. Ede, "Development of an adaptive predictive braking enforcement algorithm", Federal Railroad Administration, 2009.

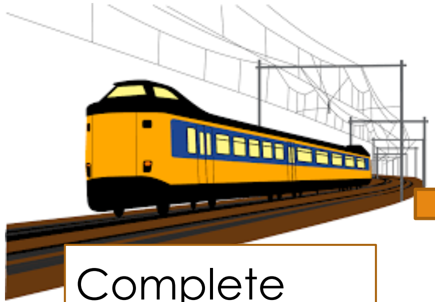
Formal Verification



Formal Model



Proving in KeYmaera X Theorem Prover

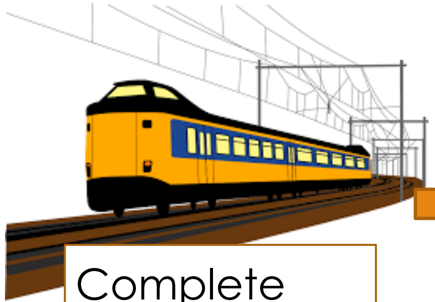


Complete FRA Model[1]

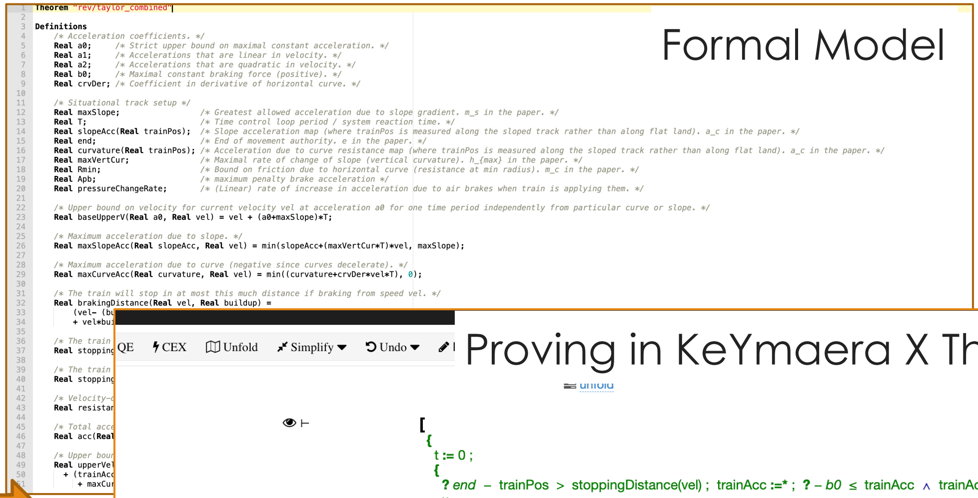
2545 lines of proof tactic

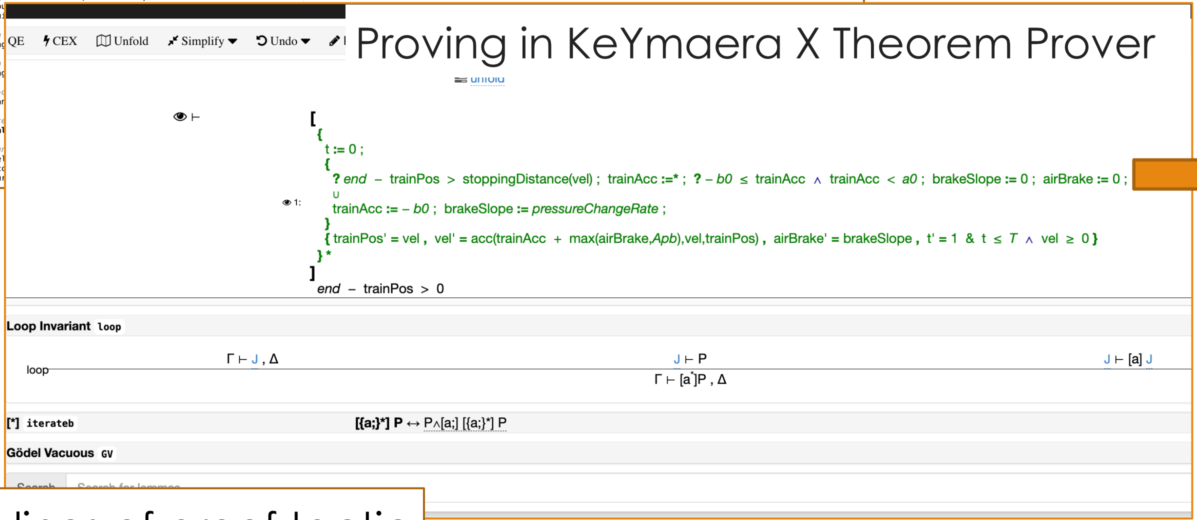
[1] J. Brosseau and B. M. Ede, “Development of an adaptive predictive braking enforcement algorithm”, Federal Railroad Administration, 2009.

Formal Verification



Complete FRA Model[1]





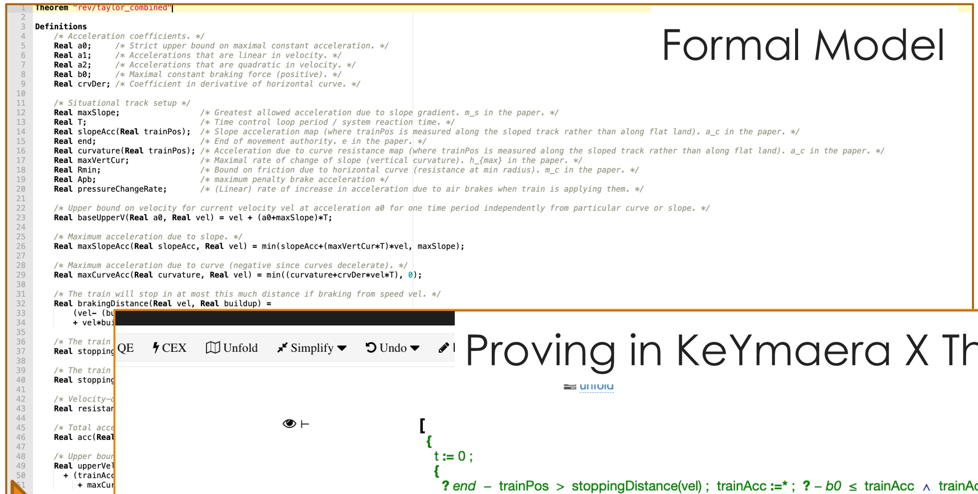
2545 lines of proof tactic

Infinitely many possibilities checked once and for all

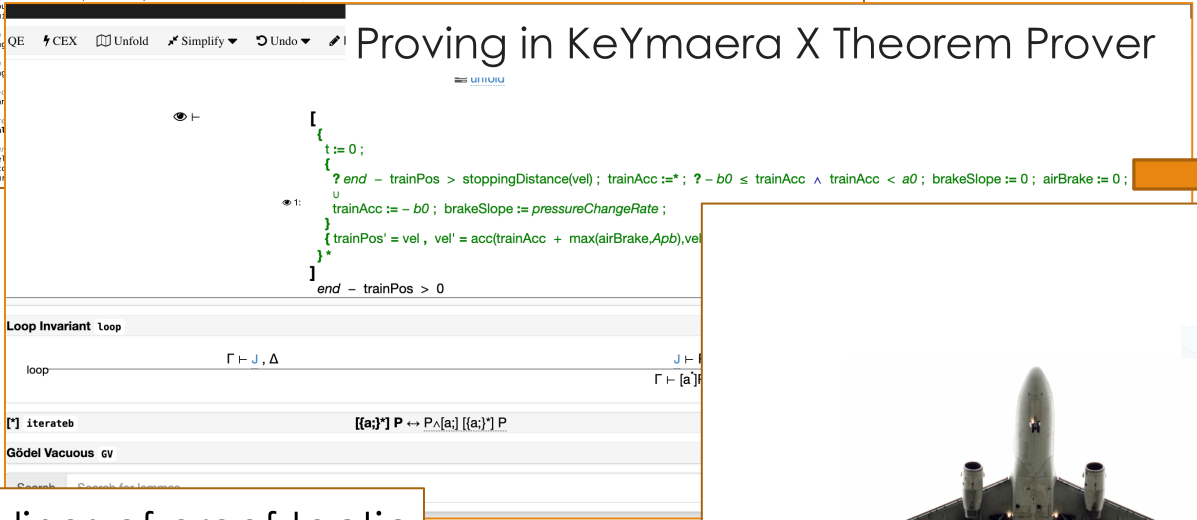
[1] J. Brosseau and B. M. Ede, "Development of an adaptive predictive braking enforcement algorithm", Federal Railroad Administration, 2009.

4

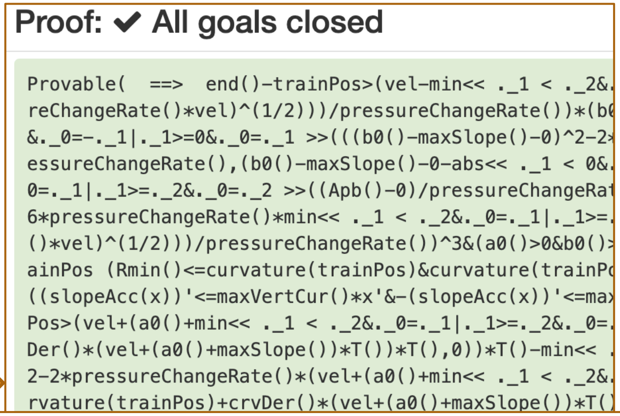
Formal Verification



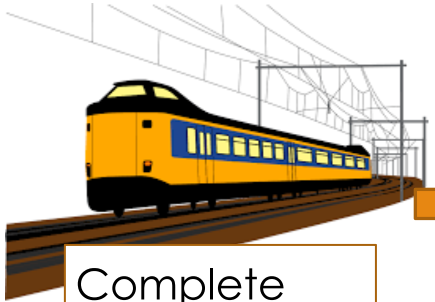
Formal Model



Proving in KeYmaera X Theorem Prover



Proof: ✔ All goals closed



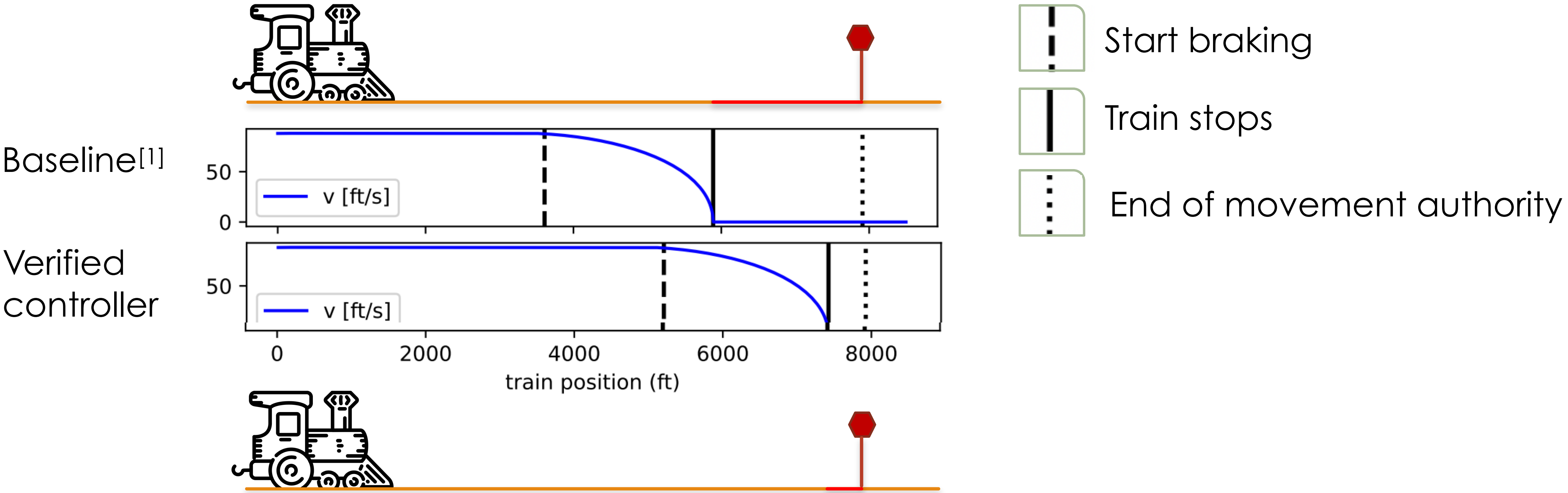
Complete FRA Model[1]

2545 lines of proof tactic

Generalizable

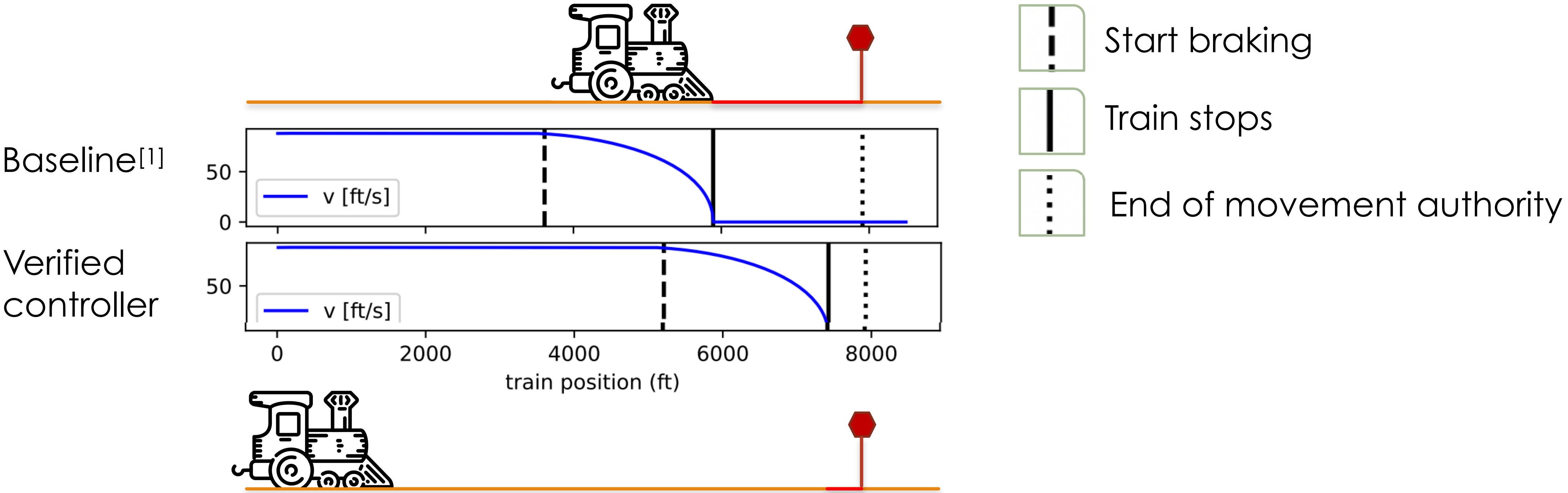
[1] J. Brosseau and B. M. Ede, "Development of an adaptive predicti
Administration, 2009.

Approach: Impact



[1] J. Brosseau and B. M. Ede, "Development of an adaptive predictive braking enforcement algorithm", Federal Railroad Administration, 2009.

Approach: Impact

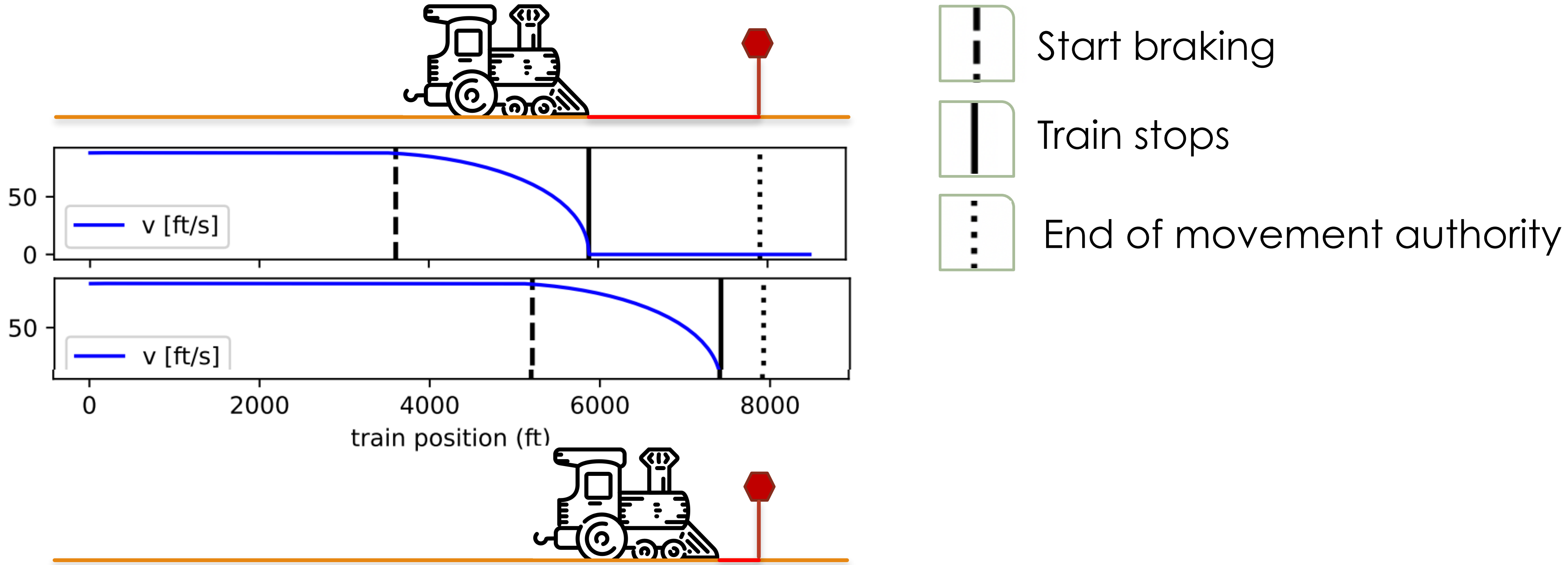


[1] J. Brosseau and B. M. Ede, “Development of an adaptive predictive braking enforcement algorithm”, Federal Railroad Administration, 2009.

Approach: Impact

Baseline[1]

Verified controller

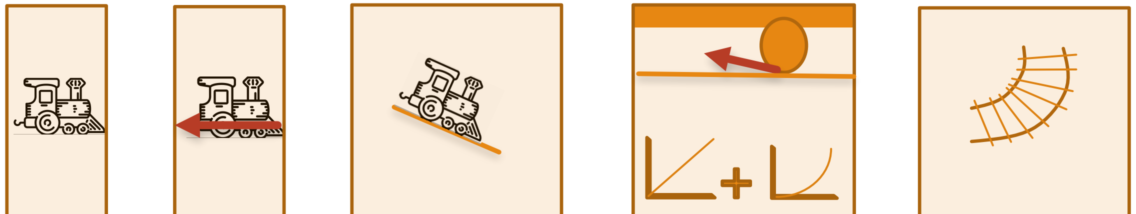


[1] J. Brosseau and B. M. Ede, "Development of an adaptive predictive braking enforcement algorithm", Federal Railroad Administration, 2009.

Overview

- Introduction
- Techniques
- Evaluation
- Summary

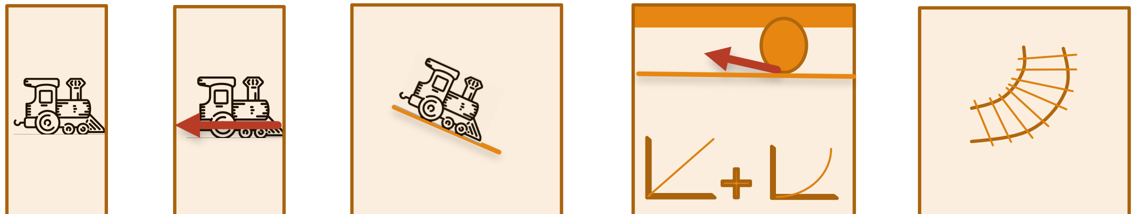
Background: Dynamics



$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

$$\text{with } a_l \in [-b_{\max}, a_{\max}], a_a = max(a_b, a_{b\max})$$

Background: Dynamics



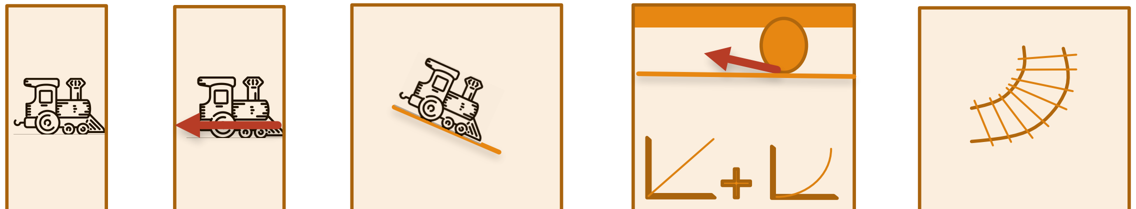
$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

$$\text{with } a_l \in [-b_{\max}, a_{\max}], a_a = max(a_b, a_{b\max})$$

Rate of change of train position is velocity

Background: Dynamics

Rate of change of train velocity is acceleration



$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

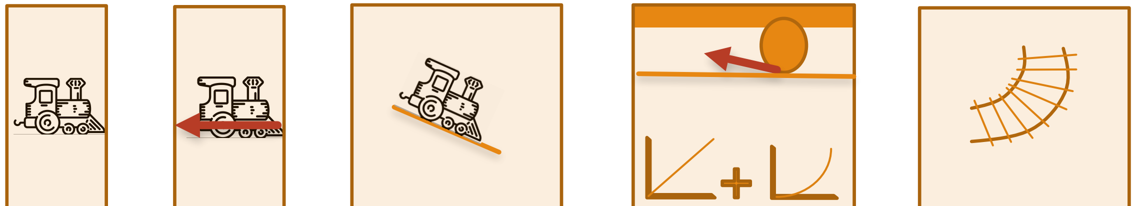
$$\text{with } a_l \in [-b_{\max}, a_{\max}], a_a = max(a_b, a_{b\max})$$

Rate of change of train position is velocity

Background: Dynamics

Rate of change of train velocity is acceleration

Air brakes ramp up



$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

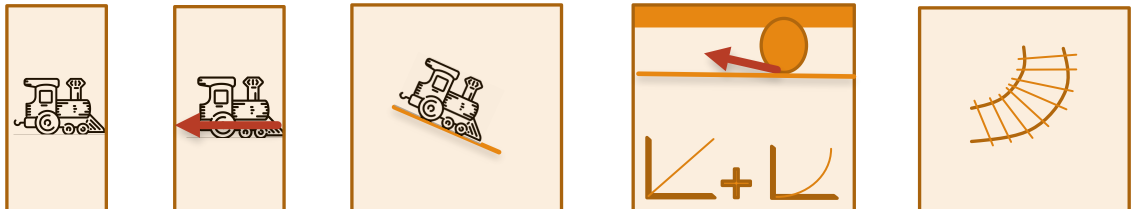
$$\text{with } a_l \in [-b_{\max}, a_{\max}], a_a = max(a_b, a_{b\max})$$

Rate of change of train position is velocity

Background: Dynamics

Rate of change of train velocity is acceleration

Air brakes ramp up



$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

$$\text{with } a_l \in [-b_{\max}, a_{\max}], a_a = max(a_b, a_{b\max})$$

Rate of change of train position is velocity

Unknown functions: slope, curve

$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

Unknown functions: slope, curve

$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

Unknown functions: slope, curve

$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a_b' = m_b$$

Unknown functions: slope, curve

Use worst case value …

$$p' = v, v' = a_l + a_a + a_s(p) + a_r(v) + a_c(p), a'_b = m_b$$

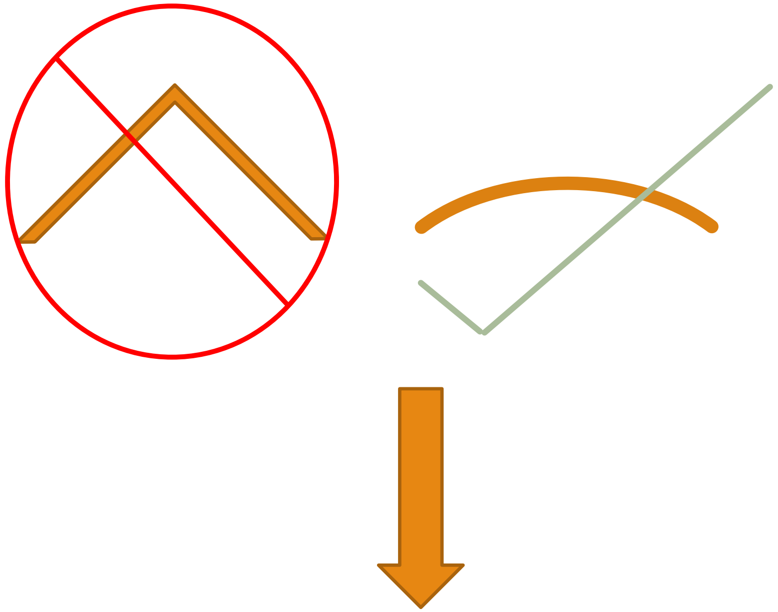
$a_s(p) \rightarrow m_s$, $a_c(p) \rightarrow 0$

Unknown function: replace with worst case value m_s

Unknown function: replace with worst case value 0

Unknown functions: slope, curve

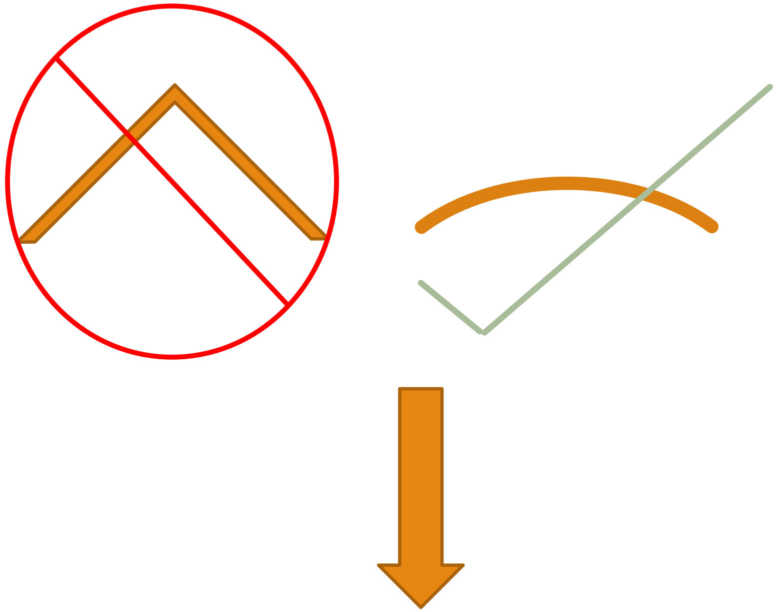
… with improving estimates.



$$a_s(p) \leq \bar{a}_s(p_0) = \min(m_s, a_s(p_0) + u \cdot h_{\max} \cdot T)$$

Unknown functions: slope, curve

… with improving estimates.

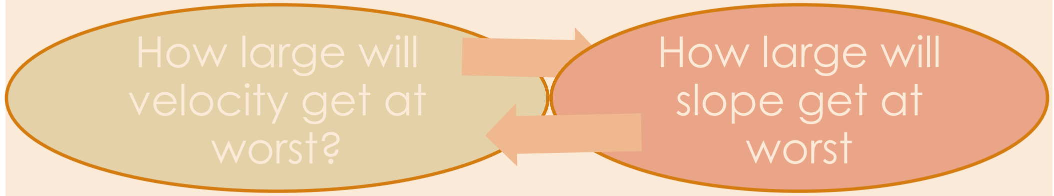


$$a_s(p) \leq \bar{a}_s(p_0) = \min(m_s, a_s(p_0) + u \cdot h_{\max} \cdot T)$$

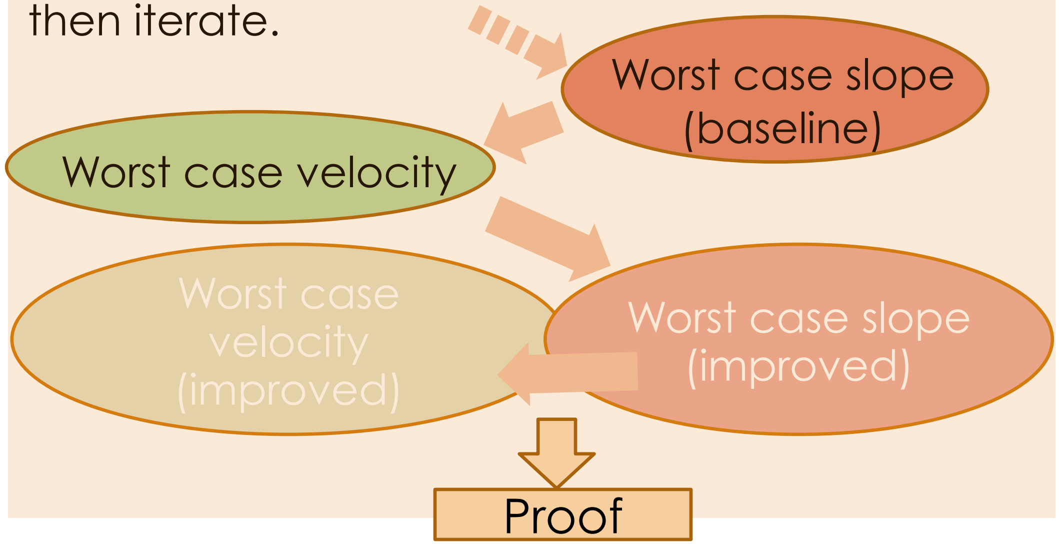
Other Techniques

Circular Dependencies

Problem: Circular dependence while estimating worst case values.



Solution: Bootstrap cycle with naive values, then iterate.



Taylor Polynomial

Problem: Davis resistance integrates poorly.

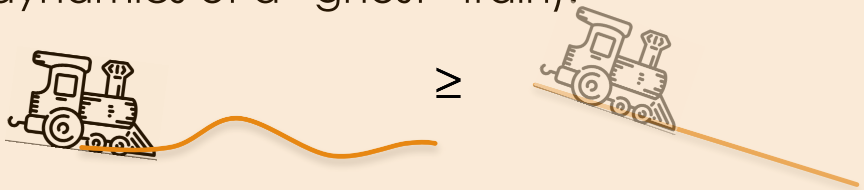
$$\frac{\left(\sqrt{4(a_l+m_s)a_2-a_1^2}\right)\cdot \tan\left(t\frac{\sqrt{4(a_l+m_s)a_2-a_1^2}}{2}+\tan^{-1}\left(\frac{a_1+2a_2v_0}{\sqrt{4(a_l+m_s)a_2-a_1^2}}\right)\right)-a_1}{2a_2}$$

Solution: Taylor polynomial approximation.

Ghost Trains

Problem: Intermediate reasoning steps transcendental.

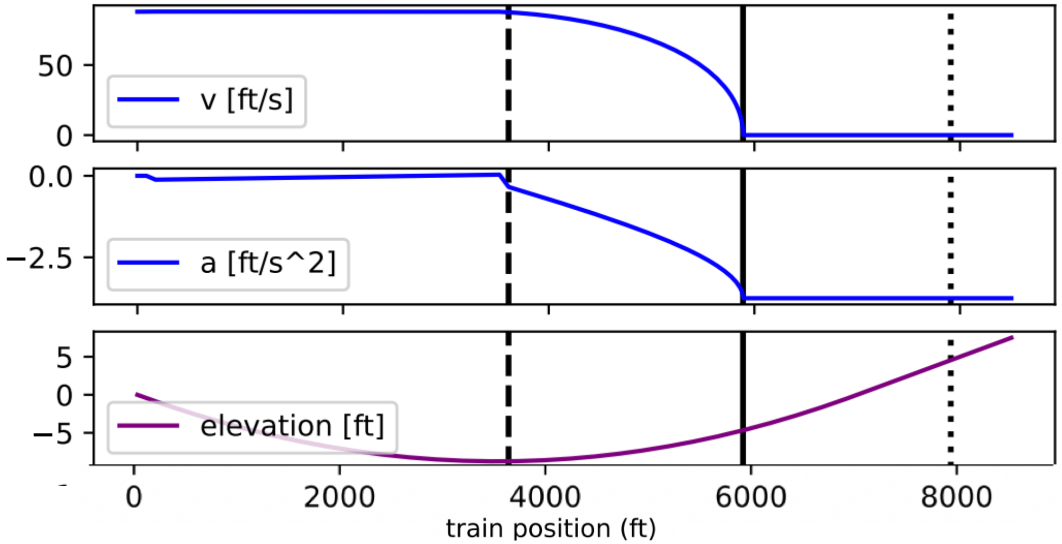
Solution: Reason about as ODE (here represents dynamics of a "ghost" train).

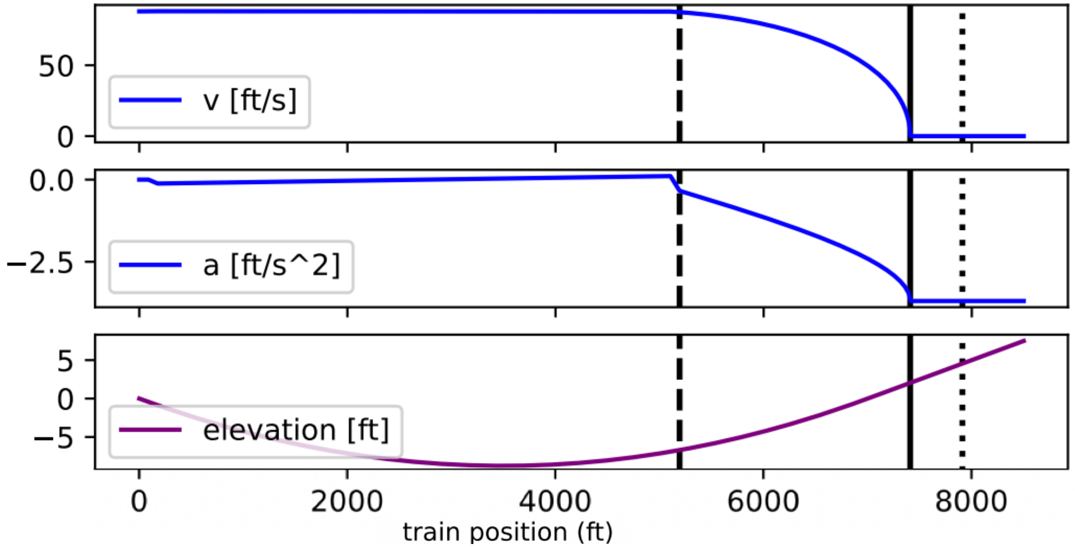


Overview

- Introduction
- Techniques
- Evaluation
- Summary

Limiting Undershoot while Maintaining Safety





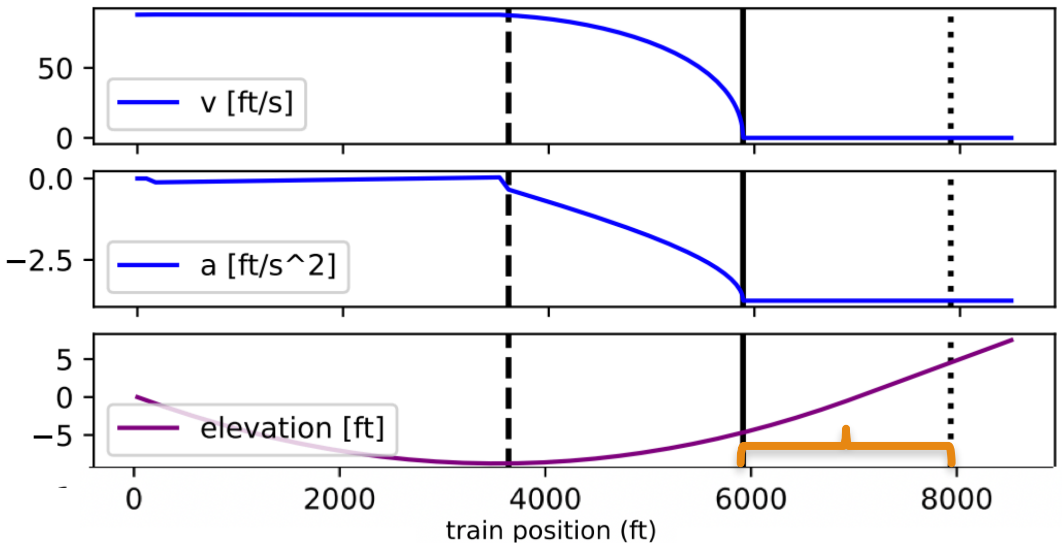
Start braking

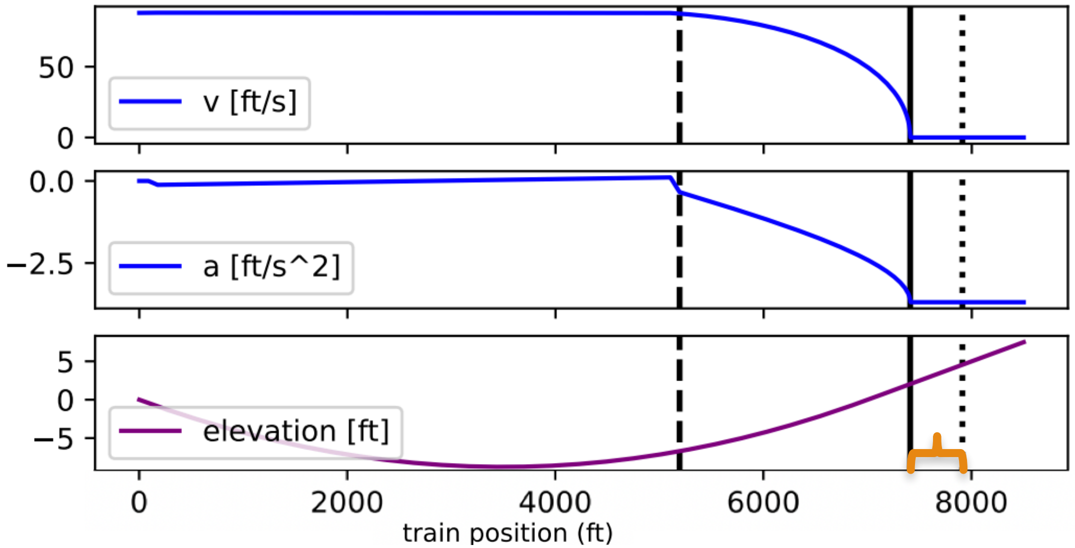
End of movement authority

Train stops

[1] J. Brosseau and B. M. Ede, "Development of an adaptive predictive braking enforcement algorithm", Federal Railroad Administration, 2009.

Limiting Undershoot while Maintaining Safety





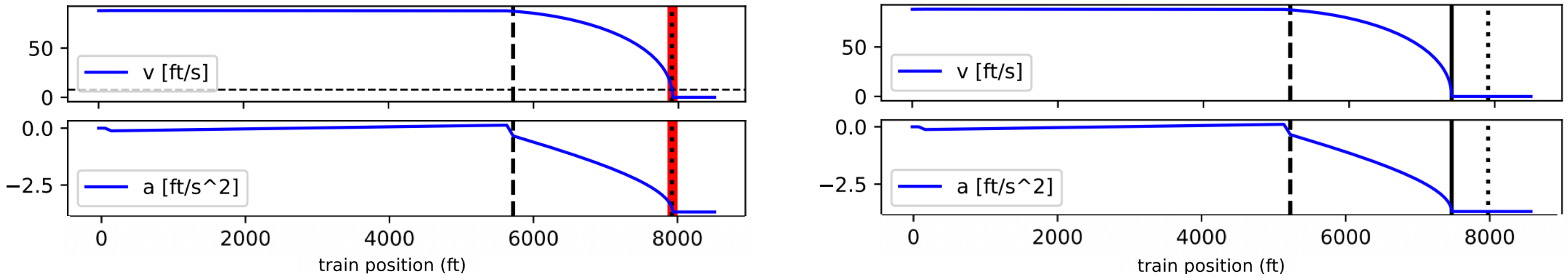
Start braking

Train stops

End of movement authority

[1] J. Brosseau and B. M. Ede, “Development of an adaptive predictive braking enforcement algorithm”, Federal Railroad Administration, 2009.

Limiting Undershoot while Maintaining Safety



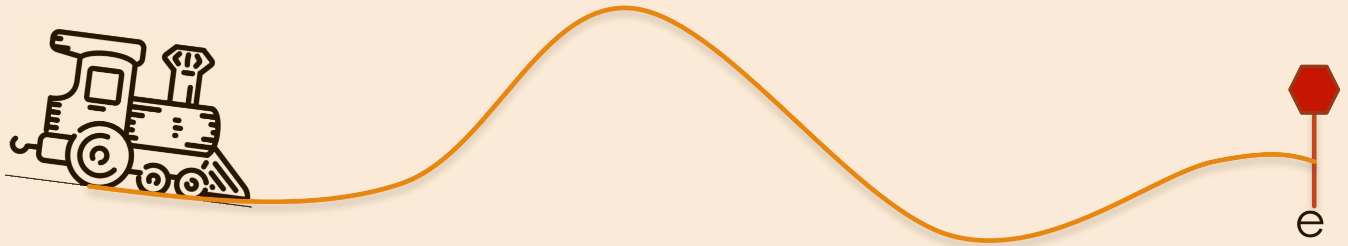
Start braking

End of movement authority

Train stops

[1] J. Brosseau and B. M. Ede, "Development of an adaptive predictive braking enforcement algorithm", Federal Railroad Administration, 2009.

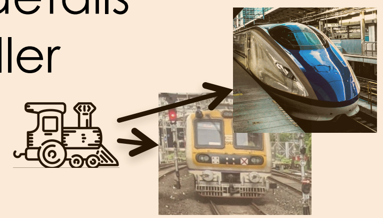
Summary



Verified controller for full FRA model dynamics. KeYmaera X proofs available online

Generalizable Techniques
- Dealing with unknown functions
- Circular dependencies
- Taylor polynomials
- Ghost dynamics

Verified Model Generalizability
- Abstraction of physical details
- Nondeterministic controller



Experiments

Controller limits undershoot while maintaining safety