Formal Verification of Train Control with Air Pressure Brakes*

Stefan Mitsch[1], Marco Gario[2], Christof J. Budnik[2], Michael Golm[2], and André Platzer[1]

[1] Computer Science Department, Carnegie Mellon University, Pittsburgh PA 15213, USA
{smitsch,aplatzer}@cs.cmu.edu
[2] Siemens Corporate Technology, Princeton, NJ, USA
{marco.gario,christof.budnik,michael.golm}@siemens.com

Abstract. Train control technology enhances the safety and efficiency of railroad operation by safeguarding the motion of trains to prevent them from leaving designated areas of operation and colliding with other trains. It is crucial for safety that the trains engage their brakes early enough in order to make sure they never leave the safe part of the track. Efficiency considerations, however, also require that the train does not brake too soon, which would limit operational suitability. It is surprisingly subtle to reach the right tradeoffs and identify the right control conditions that guarantee safe motion without being overly conservative.
In pursuit of an answer, we develop a *hybrid system* model with *discrete control decisions* for acceleration, brakes, and with *continuous differential equations* for their physical effects on the motion of the train. The resulting hybrid system model is systematically derived from the Federal Railway Administration model for flat terrain by *conservatively* neglecting minor forces.
The main contribution of this paper is the identification of a controller with control constraints that we formally verify to always guarantee collision freedom in the FRA model. The safe braking behavior of a train is influenced not only by the train configuration (e.g., train length and mass), but also by physical characteristics (e.g., brake pressure propagation and reaction time). We formalize train control safety properties in differential dynamic logic and prove the correctness of the train control models in the theorem prover KeYmaera X.

1 Introduction

Train control (TC) technology is meant to safeguard the control of trains such that they cannot collide with other trains, cannot move into unauthorized track segments, and cannot derail because of excessive speed. While they do not prevent accidents caused by mechanical failures like axle breakage, train protection systems are the major safety technology controlling the safety of the motion of trains.

Train protection systems monitor the motion and the operator's control decisions and take infrastructure information into account to stop the train before reaching the position of other trains or otherwise moving into unauthorized track segments. Of course, TC needs to initiate the brakes early enough in order to make sure the train finally comes

* This material is based upon work supported by Siemens Corporate Technology.

to a stop safely (or below the speed limit) before the unsafe track position. At the same time, railway operation would be disrupted substantially if an automatic train protection system were to frequently cause a train to brake unnecessarily.

Consequently, it is useful to find out how late the train brakes can still be applied without losing guaranteed stopping capabilities of the train. More generally, the challenge is to identify a maximally permissive train protection controller that gives the operator and other train controllers maximal degrees of freedom in operating the train, while still always ensuring that the train brakes will automatically be applied early enough so that the train will come to a stop before reaching any unsafe track positions.

Trains can perform different types of braking, e.g., through traction of the motors in the locomotive, and magnetic or pneumatic brake shoes on the train's cars. Combined with various ways of triggering the brakes (e.g., electronically or through air pressure pipes), we get a range of available brake forces and durations until full braking force is available. For example, air pressure propagation along the train causes the effective braking force to change and ramp up slowly over time. This complicates the safety analysis and requires safe TC controllers to be aware of the worst-case influence of the various train parameters on the guaranteed safe stopping distance. Some parameters (e.g., train length) have significant influence on the pressure propagation and in turn on the stopping distance, while others (e.g., aerodynamic drag) can be approximated by either their upper or lower bound, depending on the direction of their influence.

Approach. In order to discover the right safety constraints and justify their safety with mathematical rigor, we develop a controller for a mathematical model based on the physics of the *Federal Railway Administration* (FRA) model [6]. This results in a *hybrid systems* model, because it includes differential equations for the continuous physical effects of motion and the discrete control decisions of when to accelerate, when to apply moderate braking in normal operation, and when to begin or stop applying maximum brakes. The model considers train length and mass, reaction times, brake pressure propagation, penalty brake force, service brake force, and acceleration force. Unlike the FRA model, we ignore roll resistance, air resistance, and curve resistance, because these are negligible for freight trains and only make the train stop earlier (so the controller is safer). As a first step, we simplify the model to consider flat terrain only, leaving more complex terrain profiles as future work.

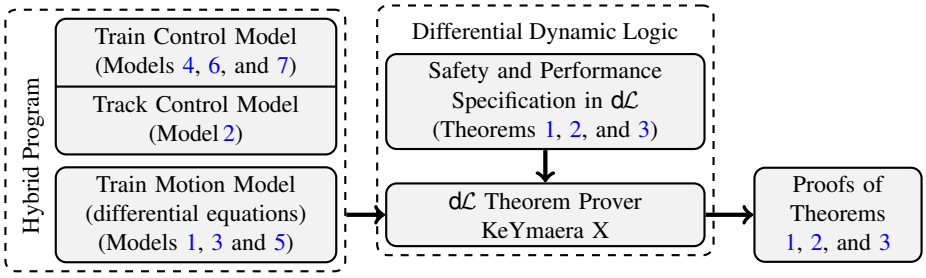


Fig. 1: Overview of formal verification process in dℒ and artifacts

We formalize safety of the TC controller as a formula in differential dynamic logic dℒ [19,20,21,22], which is the logic for hybrid systems. Besides the identification of the safety conditions for the TC controller, our main contribution is its rigorous mathematical justification by providing a proof in the dℒ theorem prover KeYmaera X [13]. Formalizing and proving motion and controller together in a hybrid systems model has the additional benefit of *identifying constraints* on the decisions that a controller has to make *ahead of time for any subtle combination of system state and control choice*. Fig. 1 summarizes our formal verification approach and the artifacts of this paper. These findings are part of an ongoing effort to rigorously formalize the safety of train controllers.

2 Preliminaries: Differential Dynamic Logic

We use *differential dynamic logic* dℒ [19,20,21,22] to verify safe braking behavior. Differential dynamic logic has a notation for hybrid systems as *hybrid programs*, which use differential equations as program statements to describe continuous behavior in addition to discrete computations.

One of the challenges of developing a safe braking controller is to analyze its safety over a broad range of possible control decisions that were taken prior to braking, where a train should be allowed to speed up or slow down in any appropriate way. In addition to programming constructs familiar from other languages (e.g., assignments and conditional statements), hybrid programs provide nondeterministic operators that allow us to describe such unknown prior behavior concisely. Nondeterminism has the additional benefit that later optimization (e.g., use better sensors or implement a faster algorithm) may be possible without re-verification as variations are already covered.

Table 1 summarizes the syntax of hybrid programs together with an informal semantics. We briefly describe each operator with an example. Sequential composition $\alpha;\beta$ says that program β starts after α finishes (e.g., first determine track grade, then let the train choose acceleration). The nondeterministic choice $\alpha \cup \beta$ follows either α or β (e.g., the train may be in normal operation or in braking mode). The nondeterministic repetition operator α^* repeats α zero or more times (e.g., the train's target speed may be revised over and over again, but we do not know exactly how often). Assignment $x := \theta$ instantaneously assigns the value of the term θ to variable x (e.g., let the train choose maximum braking). Instead $x := *$ assigns an arbitrary value to x (e.g., the track grade may change arbitrarily, we do not know which value exactly). $x' = \theta \,\&\, F$ describes a continuous evolution of x along the differential equation $x' = \theta$ of arbitrary duration (even zero time). The evolution domain F can be used to restrict the continuous evolution to a certain region in space-time (e.g., restrict duration to at most $5s$). The test $?F$ checks that a particular condition F holds and aborts if it does not (e.g., continue accelerating only when the distance to the track position limit is large enough). Execution of hybrid programs with backtracking is a good intuition, since other nondeterministic choices may still be possible if one run fails. A typical pattern that involves assignment and tests is to limit the assignment of arbitrary values by their bounds (e.g., limit acceleration to the normal operation conditions, as in $f_a := *;\ ? - F_{sb} \leq f_a \leq A$, which assigns to f_a any value between the service brake force $-F_{sb}$ and acceleration force A).

Table 1: Hybrid program representations of hybrid systems

Statement	Effect
$\alpha;\ \beta$	sequential composition, first run program α, then β
$\alpha\ \cup\ \beta$	nondeterministic choice, following either program α or β
α^*	nondeterministic repetition, repeats program α any $n \geq 0$ times
$x := \theta$	assign value of term θ to variable x (discrete jump)
$x := *$	assign any arbitrary real number to variable x nondeterministically
$?F$	check that formula F holds at the current state, and abort if it does not
$\{x_1' = \theta_1, \ldots, x_n' = \theta_n\ \&\ F\}$	evolve x_i along differential equation system $x_i' = \theta_i$ restricted to maximum evolution domain F for any duration $r \in \mathbb{R}$

The set of dL formulas is generated by the following grammar ($\sim$ is any operator in $\{<, \leq, =, \neq, \geq, >\}$, θ_1, θ_2 are arithmetic expressions in $+, -, \cdot, /$ over the reals):

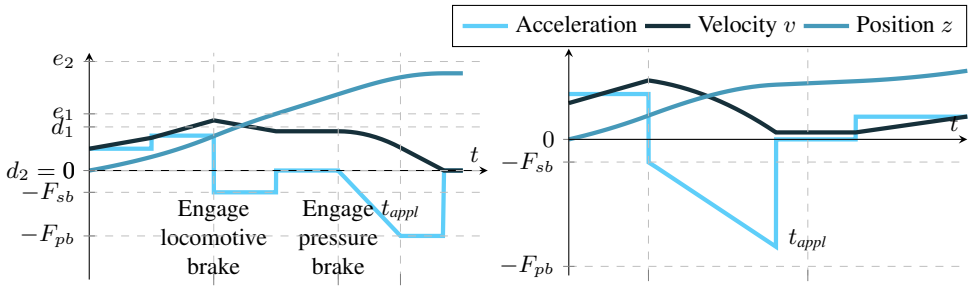
$$\phi ::= \theta_1 \sim \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \phi \vee \psi \mid \phi \rightarrow \psi \mid \phi \leftrightarrow \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

To specify the desired correctness properties of hybrid programs, a dL formula $F \rightarrow [\alpha]G$ means that if started at an initial state in which formula F is true, then all executions of the hybrid program α only lead to states in which formula G is true. Differential dynamic logic comes with a formal verification technique to prove these and other correctness properties. We did all our proofs in the verification tool KeYmaera X [13], which implements the dL verification technique [19,21,22]. The dL verification technique is sound, which means that a formula that has a proof is *valid*, i.e., true in all states. For high confidence, the dL verification technique has been cross-verified [3] in the Isabelle and Coq theorem provers. This gives dL-based verification results an extraordinarily strong degree of reliability for high confidence safety assurance cases.

3 Train Control Models

In normal operation, trains may speed up or slow down at will. The brakes are then typically operated with moderate braking force, referred to as *service braking*. When a train is about to violate the track position limit or speed limit in normal operation, the goal of TC is to ensure safety by switching to *penalty braking* with maximum brake force. The air pressure brakes on a train exert strong braking force but require some time to build up maximum brake force by propagating air pressure along the train. For fail-safety reasons, air brakes along a train apply pressure brakes in proportion to how the air pressure from the locomotive is lost instead of increased, but they are, nevertheless, subject to slow propagation and build-up of braking force along the train.

Figure 2 illustrates the behavior that we model. In free driving—i.e., when the train respects the speed limit and is at a safe distance from the track position limit e—the train may speed up or slow down at will (e.g., according to the train driver's decisions or those of other optimizing controllers). At time $t = 1$, the train receives a speed limit $d_1 = 1$ that is in place from e_1 onwards, so it engages its service brakes $-F_{sb}$ and afterwards decides to coast to respect the speed limit. Later, the speed limit changes to



(a) Free driving, service brakes $-F_{sb}$ to respect speed limit d_1 at e_1, and penalty brake $-F_{pb}$ to stop before track position limit e_2

(b) Engage locomotive brake and pressure brakes at the same time. Later release brakes before full stop and continue driving

Fig. 2: Braking with instantaneous service brakes and air pressure penalty brakes

a full stop $d_2 = 0$ at e_2. The remaining distance to e_2 is too small to stop safely just using the service brakes. Therefore, at time $t = 2$ the train engages its penalty brakes, which, however, need time t_{appl} until they are operational at full force $-F_{pb}$. The train then continues braking with full brake force $-F_{pb}$ until it is fully stopped. This scenario includes the following model components (detailed subsequently):

- A track controller may repeatedly issue new speed limits d that are in place from a position e onwards. Limit $d = 0$ means stop at e. It should not demand physically impossible maneuvers (e.g., ask a freight train traveling at 60mph to stop in 3ft).
- A train controller decides between free driving (using arbitrary engine acceleration and the service brakes) and penalty braking using maximum brake force. The decision is based on the resulting slowdown/stopping distance from its current speed v to speed limit d and the remaining safety distance to track position e.
- The safety margins follow from a motion model of the train, whose behavior depends on train parameters (e.g., length) and external conditions (e.g., track grade).
- Acceleration and service brake via the train's engine have immediate but limited effect. Penalty brakes provide higher overall braking force at the cost of pressure propagation time along the individual freight or passenger cars of the train.

3.1 Safety and Performance Considerations

The main safety objective in train control is to respect speed and track position limits [6]. Predicting the stopping distance is therefore key to a safe and effective controller. Errors in the prediction may let a train run past the track position limit (overshoot), stop unnecessarily early (undershoot), or brake unnecessarily, resulting in undesired effects on the overall railway network operation. The FRA characterizes safety by limiting overshoots, i.e., with 99.9995% probability trains must not overshoot the track position limit [6]. Usually one overestimates the stopping distance by some safe factor. While this can improve the overall safety of the system, it might be detrimental to system performance: trains significantly underperform when train length and weight are not considered in the braking decision [24], and braking frequently or significantly earlier

Model 1 Train Motion Model

$$\mathit{motion} \equiv t := 0;\ \{z' = v,\ v' = \frac{F + f_a}{m},\ t' = 1\ \&\ v \geq 0 \wedge t \leq \varepsilon\} \tag{1}$$

than needed has negative impacts both on energy considerations as well as on the overall throughput of the network. An orthogonal performance objective, therefore, limits undershoots to 500ft for trains at less than 30mph, and 1000ft above 30mph [6].

To find a suitable safety and performance trade-off, we need to consider more realistic (and therefore complex) models of the dynamics to which the train is subject. We compare a simpler model that considers only the delay of brake pressure propagation with a more accurate model of gradual pressure propagation.

3.2 Train Motion and Brake Forces

The model of train motion is developed in Model 1. By Newtonian physics, the time-derivative of the train's position z is its velocity v, which explains differential equation $z' = v$. The derivative of the train's velocity v is the sum of external forces F as well as the controlled acceleration/braking force f_a. Both are subject to the train's mass m to capture motion inertia, giving $v' = \frac{F+f_a}{m}$. Because trains do not move backwards just because they are braking with a negative acceleration, we include $v \geq 0$ as an evolution domain constraint. The system's control cycle duration is modeled with a timer t that is reset to $t := 0$ before the differential equation, evolves with $t' = 1$, and interrupts the differential equation after at most ε time due to the evolution domain $t \leq \varepsilon$. This ensures that the motion will "stop" to give the subsequent controllers a chance to run at the latest after ε time again. The initial values of position z and speed v are unknown.

The forces that act on the train are its own braking force F_b and locomotive traction F_l, as well as the track grade force F_g (incline or decline), the track curvature force F_c, and the bearing, rolling, and aerodynamic resistive forces F_r [6, p. 57]. Model 1 uses f_a to summarize the train's braking force F_b and locomotive tractive effort F_l, so $F = -(F_g + F_r + F_c)$ in (1). The train's acceleration will be limited by a maximum braking force $-F_{pb}$ and a maximum acceleration force A. An important characteristic of air pressure brakes is the time t_{appl} that it takes from initiating braking until the full braking force F_{pb} is available [6]. The time t_{appl} depends on the length l of the train with constants $c_1^{t_{appl}}$ to $c_3^{t_{appl}}$ as follows: $t_{appl} = c_1^{t_{appl}} + c_2^{t_{appl}} l + c_3^{t_{appl}} l^2$ by [6, p. 57].

The resistive forces F_r can be estimated from the train's speed v, weight $W = mg$ with gravity constant $g > 0$, number of cars N and axles n with constants c_1^r to c_4^r using $F_r = c_1^r W + c_2^r n + c_3^r W v + c_4^r N v^2$ [6]. The track curvature force F_c depends on the train's weight W and the average curvature C under the train $F_c = c_1^c CW$ [6]. Since both resistive force and track curvature force oppose forward motion (i.e., improve braking), we can neglect them for safety analysis purposes by assuming $c_i^r = c_i^c = 0$. The track grade force F_g depends on the train's weight and average track grade G under the train by $F_g = c_1^g GW$, so $F_g = 0$ for flat tracks. Additional detail on the external forces acting on trains is in [2]. We take a first step by assuming external forces $F = -(F_g + F_r + F_c) = 0$ to focus solely on the effect of brake pressure propagation on f_a in flat terrain (forces F_r and F_c improve braking, so make our controllers safer).

Model 2 Track Control

$$tc \;\equiv\; e := *;\; d := *;\; ?\left(d \geq 0 \wedge (v^2 - d^2)m \leq 2F_{sb}(e - z)\right) \tag{2}$$

3.3 Track Control

The central track controller *tc* in Model 2 can update speed limits d and track position limit e at any time, as long as it does not demand the train moves backwards (so $d \geq 0$) and the remaining distance between the train's position z and the track position limit e allows the train to respect the speed limit safely within the limits of physics. For a reasonable system design, the track controller should also only choose d and e such that the train can safely follow by just using the service brakes $-F_{sb}$.

Crucially, the condition (2) characterizes the relationship between the train's current speed v and position z, and the speed limit d and track position limit e. Condition (2) can be discovered in KeYmaera X by proving a simplified hybrid program (3) that uses the service brakes $f_a := -F_{sb}$ and neglects other model details (external force $F = 0$):

$$F = 0 \wedge F_{sb} > 0 \wedge m > 0 \rightarrow [f_a := -F_{sb};\; \textit{motion}](z \geq e \rightarrow v \leq d) \tag{3}$$

Formula (3) is not valid but still true in some states, which allows KeYmaera X to find conditions on e and z that make it provable. These conditions can be explained as follows: from $v' = \frac{F+f_a}{m}$ in *motion* we see that, with service brakes, the train needs $\frac{(v-d)m}{F_{sb}}$ time to overcome the difference between its current speed v and speed limit d. The differential equation in *motion* is solvable, so its solution gives the slowdown distance $\int_0^{\frac{(v-d)m}{F_{sb}}} \left(v - \frac{F_{sb}}{m}t\right) dt$, implying $\frac{(v^2-d^2)m}{2F_{sb}}$ as minimum distance between the track position limit e and the train z, see equivalent condition in (2).

3.4 Train Control

The primary safety question in train controller design is finding conditions under which it is safe to drive freely, and when it is necessary to engage the brakes as a last resort safety action. The major safety argument for the controller has to justify why the train will always respect the target speed at the track position limit.

For traceability purposes and for managing the analytic complexity it is beneficial to develop these conditions in increasingly realistic brake pressure propagation models. We first consider a conservative approximation delaying the whole effect of brakes for the entire propagation time (Section 3.5). Then we follow the FRA model that gradually increases the effect of the air pressure brakes with a constant jerk or jolt (Section 3.6).

Keeping acceleration constant between decisions significantly simplifies the task of finding the safety distances. The effects of changing accelerations manifest in position constraints: with gradual increase j in braking force we need to solve $z''' = j$. With delayed brake onset $z'' = f_a$ is enough. Fig. 3 illustrates the conservative approximation in comparison to a gradual increase in brake force. Both models behave the same in free driving. When engaging the pressure brakes, the conservative approximation coasts for

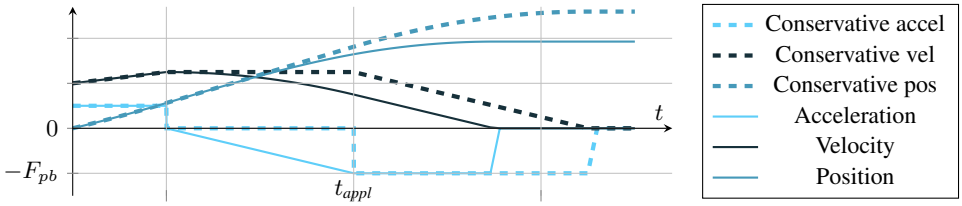


Fig. 3: Delayed brake onset conservatively approximates brake pressure propagation. The train length determines how long (t_{appl}) it takes to reach full braking force $-F_{pb}$.

the entire brake pressure propagation time, while gradual braking force already decelerates the train with limited force while the brake force builds up. Since we prove the safety of both controllers, we can subsequently compare the loss in performance for the more simplistic model compared to the more accurate FRA model with jerk.

3.5 Delayed Braking

The simpler train model that conservatively takes the effect of gradual pressure brake build-up into account simply pretends the pressure brakes would have no effect at all until they finally have full effect after the pressure propagated along the train. This is counterfactual with reality but a conservative approximation, because some braking force already takes effect in the middle of the process of building up braking force from the pressure brakes. Pretending this deceleration would be 0 is inaccurate but only makes the real train brake quicker than the model, so safer.

The train motion in Model 3 follows the motion of Model 1 with changes highlighted in bold. The pressure brake build-up delay is modeled with a timer c with $c' = s$ that can be enabled or disabled by setting its slope s either to 1 (enabled) or to 0 (disabled), but it never exceeds the brake delay ($c \leq t_{appl}$), which is only relevant if $s \neq 0$.

The train controller for delayed brake onset that we develop in Model 4 can (nondeterministically) choose to either *drive* or *brake* (5). The choice is nondeterministic in order to maximize flexibility of the train controller and, thus, also maximize how many concrete train controller implementations are covered by our single safety proof.

When driving freely, in (6) any choice between the train's service brake force $-F_{sb}$ and maximum acceleration force A is allowed by a nondeterministic assignment $f_a := *$ followed by a subsequent test to check that $-F_{sb} \leq f_a \leq A$ is true. The choice of f_a is nondeterministic in order to cover a large variety of concrete controllers under the safety argument (imagine controllers optimizing secondary objectives such as energy consumption or decisions by train conductors that determine the concrete choice of f_a

Model 3 Train Motion Model with Delayed Brake Onset, extends Model 1

$$\mathit{motion} \equiv t := 0;\ \{z' = v,\ v' = \frac{F + f_a}{m},\ t' = 1,\ \boldsymbol{c' = s}\ \&\ v \geq 0 \wedge t \leq \varepsilon \wedge \boldsymbol{c \leq t_{appl}}\} \quad (4)$$

Model 4 Train Controller for Delayed Brake Onset

$$ctrl_z \equiv drive \cup brake \tag{5}$$

$$drive \equiv f_a := *;\ ?(-F_{sb} \leq f_a \leq A); \tag{6}$$

$$c := 0;\ s := 0; \tag{7}$$

$$?\,(e - z \geq margin) \tag{8}$$

$$margin = \frac{(v^2 - d^2)m}{2F_{pb}} + \left(\frac{A}{F_{pb}} + 1\right)\left(\frac{A}{2m}\varepsilon^2 + \varepsilon v\right) + \left(v + \frac{A}{m}\varepsilon\right)t_{appl} \tag{9}$$

$$brake \equiv \begin{cases} \text{if } \left(e - z \geq \frac{(v^2-d^2)m}{2F_{sb}}\right) & f_a := -F_{sb};\ c := 0;\ s := 0 \\ \text{else if } (c \geq t_{appl}) & f_a := -F_{pb};\ s := 0 \\ \text{else if } (c > 0) & f_a := f_a \\ \text{else} & f_a := 0;\ s := 1 \end{cases} \tag{10}$$

during each execution of *drive*). The brake delay timer c is reset ($c := 0$) and turned off ($s := 0$) in (7), because the penalty brakes are not activated when driving freely.

Of course, driving freely or accelerating is not always safe. KeYmaera X points us to the worst possible scenario of this control decision: acceleration with full force A for the maximum allowed time ε and postponing braking for the maximum allowed delay t_{appl}. Condition (8) checks whether or not the remaining distance $e - z$ on the track is large enough to handle this worst-case scenario, i.e., defer braking for yet another control cycle duration ε. If it is large enough, the chosen acceleration force f_a will be made operational. Otherwise (i.e., if (8) does not hold), the controller falls back to executing *brake* as the only remaining option in nondeterministic control choice (5). When introducing brake pressure propagation we will see later that the condition (8) could be improved with separate conditions on braking and accelerating.

Braking is modeled along four increasingly critical cases in (10). The train prefers the service brake over the penalty brakes $f_a := -F_{sb}$ if the remaining distance to e is still enough for service brakes alone to ensure safety. Otherwise, the penalty brakes are used in the following way: If the brake delay has expired ($c \geq t_{appl}$), the full braking force is available with $f_a := -F_{pb}$. If the brake delay has not been reached yet but the train is already waiting for the brakes to activate ($c > 0$), then it just keeps waiting by keeping its current acceleration force $f_a := f_a$. Otherwise, the train turns the engine off to stop accelerating $f_a := 0$ and the brake delay timer is started with $s := 1$.

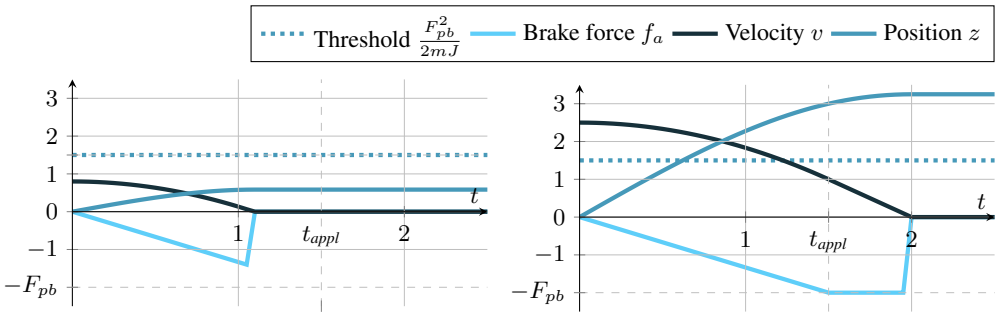
Theorem 1 (Train Controller with Delayed Brake Onset). *The braking controller for motion with delayed brake onset from Model 4 guarantees to observe a maximum speed $v \leq d$ when the train passes the track position limit $z \geq e$. That is, the following* dℒ *formula is proved: assumptions* $\rightarrow [\big(tc \cup (ctrl_z;\ motion)\big)^*](z \geq e \rightarrow v \leq d)$

3.6 Brake Pressure Propagation

The FRA's dynamical model of trains with brake pressure propagation differs in subtle but substantial ways from the simplified delayed braking model. The key differences

Model 5 Train Motion Model with Brake Pressure Propagation

$$\mathit{motion} \equiv t := 0;\ \{z' = v,\ v' = \frac{F + f_a}{m_z},\ \boldsymbol{f_a' = j},\ t' = 1\ \&\ v \geq 0 \wedge \boldsymbol{-F_{pb} \leq f_a} \wedge t \leq \varepsilon\} \quad (11)$$



(a) At slow speed $v \leq \frac{F_{pb}^2}{2mJ}$ the train stops while building up braking force

(b) At high speed $v \geq \frac{F_{pb}^2}{2mJ}$ the train stops after reaching full braking force $-F_{pb}$

Fig. 4: Brake force and stopping distance

of the resulting Model 5, highlighted in boldface, are that the acceleration force f_a is increasing continuously over time along $f_a' = j$ with the jerk j from the pressure brake propagation. The effective force of penalty braking is limited by $-F_{pb}$, reflected in an additional evolution domain constraint $-F_{pb} \leq f_a$, beyond which the subsequently developed physics controller will deactivate jerk and keep constant acceleration force.

Our train controller for brake pressure propagation in Model 6 follows the same basic setup as the controller for brake delay; differences are highlighted in bold. The main difference is condition (13)–(14) and its components (15)–(21) that allow driving with any acceleration, and the control decisions on the brake jerk j in the braking cases. In mode *drive*, penalty braking is deactivated $j := 0$ and the train controller chooses any acceleration between service braking with force $-F_{sb}$ and full acceleration force A. This is safe if service braking later ensures that the train will still always respect the speed limit d (13), or if penalty braking to a full stop with the pressure brakes will later always keep the train inside the track position limit (14). The pressure propagation along the train increases the available brake force over time up to the maximum braking force F_{pb}. As a result, the distance margin for stopping safely splits into two cases, as pointed out by KeYmaera X during the proof: slow trains will stop while the braking force is still ramping up (see Fig. 4a), fast trains will stop after reaching the maximum braking force (see Fig. 4b). In each case, the margin additionally depends on whether the train controller presently wants to slow down $f_a \leq 0$ (*slow*$^-$ (15) and *fast*$^-$ (17)) or speed up $f_a \geq 0$ (*slow*$^+$ (16) and *fast*$^+$ (18)). KeYmaera X points to a subtle combination of the worst-case bounds in margins (20) and (21). Per condition (16), a slow train may accelerate with current force f_a for the maximum allowed duration ε, if the safety margin $e - z$ is large enough for the future higher speed $u = v + \frac{f_a \varepsilon}{m}$. In the

Model 6 Train Controller for Brake Pressure Propagation

$$ctrl_z \equiv drive \cup brake \tag{12}$$

$$drive \equiv \boldsymbol{j := 0};\ f_a := *;\ ?-F_{sb} \le f_a \le A;$$

$$?\Bigg(e - z \ge \frac{(v^2-d^2)m}{2F_{sb}} + \left(\frac{A}{F_{sb}}+1\right)\left(\frac{A}{2m}\varepsilon^2 + v\varepsilon\right) \tag{13}$$

$$\vee\ slow^- \vee slow^+ \vee fast^- \vee fast^+\Bigg) \tag{14}$$

$$slow^- \equiv \neg isFast(v) \wedge f_a \le 0 \wedge e - z \ge v\varepsilon + mSlow(v) \tag{15}$$

$$slow^+ \equiv [u := v + \frac{f_a\varepsilon}{m}]\left(\neg isFast(u) \wedge f_a \ge 0 \wedge e - z \ge v\varepsilon + \frac{f_a\varepsilon^2}{2m} + mSlow(u)\right) \tag{16}$$

$$fast^- \equiv isFast(v) \wedge f_a \le 0 \wedge e - z \ge v\varepsilon + mFast(v) \tag{17}$$

$$fast^+ \equiv isFast(v) \wedge f_a \ge 0 \wedge e - z \ge v\varepsilon + \frac{f_a\varepsilon^2}{2m} + mFast\left(v + \frac{f_a\varepsilon}{m}\right) \tag{18}$$

$$isFast(v) \equiv v \ge \frac{F_{pb}^2}{2mJ} \tag{19}$$

$$mSlow(v) = \frac{2}{3}v\sqrt{2mv/J} \tag{20}$$

$$mFast(v) = \frac{mv^2}{2F_{pb}} + \frac{vF_{pb}}{2J} - \frac{F_{pb}^3}{24mJ^2} \tag{21}$$

$$brake \equiv \begin{cases} \text{if } \left(e - z \ge \frac{(v^2-d^2)m}{2F_{sb}}\right) & \boldsymbol{f_a := -F_{sb}} \\ \text{else if } \boldsymbol{(v \le d)} & \boldsymbol{j := 0};\ f_a := *;\ ?-F_{sb} \le f_a \le 0 \\ \text{else if } \boldsymbol{(f_a \le -F_{pb})} & \boldsymbol{j := 0} \\ \text{else} & \boldsymbol{j := -J};\ \boldsymbol{f_a := \min(f_a, 0)} \end{cases} \tag{22}$$

converse scenario (17), however, KeYmaera X reveals with a counterexample that using the future speed $v + \frac{f_a\varepsilon}{m}$ is unsafe, because all intermediate speeds up to ε time require a larger safety margin (i.e., the current speed v determines the worst-case bound).

Akin to Model 4, braking is structured into increasingly critical cases: the train's main preference is to use service braking $f_a := -F_{sb}$ if the remaining distance is sufficient ($e - z \ge \frac{(v^2-d^2)m}{2F_{sb}}$). If the train is slow enough already ($v \le d$), then penalty braking is disabled $j := 0$ and any level of service braking or coasting is used instead (in the force range $-F_{sb}$ to 0); If the brake pressure propagation is finished, meaning that the brakes are fully engaged ($f_a \le -F_{pb}$), then there will be no further increase in braking force ($j := 0$). Otherwise, the train did not yet build up sufficient braking force, but at least keeps increasing braking force with jerk $j := -J$ and $J = \frac{F_{pb}}{t_{appl}}$ from its current deceleration ($f_a := \min(f_a, 0)$). Note that $\min(f_a, 0)$ also models that the train stops acceleration through its locomotive when it starts the brake pressure propagation. The term $\min(f_a, 0)$ in (22) also covers the case where the train already uses service braking in *drive* but decides to switch to the stronger penalty braking for safety reasons.

Theorem 2 (Train Controller with Brake Pressure Propagation is Safe). *Model 6 with brake pressure propagation stays within a maximum speed $v \leq d$ beyond track position limit $z \geq e$. That is, the following dL formula is proved in KeYmaera X:*

$$\mathit{assumptions} \rightarrow [(\mathit{tc} \cup (\mathit{ctrl}_z;\ \mathit{motion}))^*](z \geq e \rightarrow v \leq d)$$

4 Performance Analysis

The safety analysis proved train control is safe both with delayed braking (Model 4) and with pressure brake propagation models (Model 6). While the former was much easier to design and prove safe, its controller suffers an additional safety margin because it neglects that real brakes already have partial effect while pressure is still propagating along the train. Model 6 is certainly the more realistic model while Model 4 is further away from the FRA model. It might still be a better tradeoff to settle for a conservative overapproximation that is easier to analyze than a full-blown realistic model.

To analyze this tradeoff we use the FRA performance objective [6] of not stopping too early (but still before a certain critical point). The performance objective can be analyzed in the following ways. *(i)* Comparing the performance objective of motion models Model 3 and Model 5 through simulation of some scenarios, e.g., as illustrated in Fig. 3. *(ii)* More systematic characterization by comparing the symbolic safety margins of the models, see Section 5. *(iii)* Full formal guarantees for *all* permitted behaviors when proving a lower bound on the stopping point of the train, dual to the upper bounds from the safety proofs (this section). Intuitively, a train controller has a good performance if it does not stop "too early" but without ever endangering safety.

For proving performance it is important to only engage penalty braking when it is absolutely necessary to avoid overshoot, i.e., when (8) is no longer satisfied, but not earlier. Braking for any other reason at any earlier point is detrimental to proving performance bounds, but allowed in Model 4 for flexibility, so that train operators can do so to react to other unforeseen events along the track or to simply stop at a station. For a performance proof, Model 7 adapts Model 4 to favor free driving over braking by

Model 7 Train Controller for Late Braking

$$\mathit{ctrl}_z \equiv \textbf{if } (\boldsymbol{e - z \geq \mathit{margin}}) \ \{\boldsymbol{\mathit{drive}}\} \textbf{ else } \{\boldsymbol{\mathit{brake}}\} \tag{23}$$

$$\boldsymbol{\mathit{drive}} \equiv f_a := *;\ ?(-F_{sb} \leq f_a \leq A);\ c := 0;\ s := 0 \tag{24}$$

$$\mathit{accMargin}(v) = \left(\frac{A}{F_{pb}} + 1\right)\left(\frac{A}{2m}\varepsilon^2 + \varepsilon v\right) + \left(v + \frac{A}{m}\varepsilon\right) t_{\mathit{appl}} \tag{25}$$

$$\mathit{margin} = (v^2 - d^2)m/(2F_{pb}) + \mathit{accMargin}(v) \tag{26}$$

$$\mathit{brake} \equiv \begin{cases} \text{if } \left(e - z \geq \frac{(v^2-d^2)m}{2F_{sb}}\right) & f_a := -F_{sb};\ c := 0;\ s := 0 \\ \text{else if } (c \geq t_{\mathit{appl}}) & f_a := -F_{pb};\ s := 0 \\ \text{else if } (c > 0) & f_a := f_a \\ \text{else} & f_a := 0;\ s := 1;\ \boldsymbol{v_0 := v} \end{cases} \tag{27}$$

making the nondeterministic choice *drive* $\cup$ *brake* deterministic (23). This deterministic choice implies that, at the start of the braking maneuver, the safety margin to the track position limit e is at most $\frac{(v^2-d^2)m}{2F_{pb}} + \mathit{accMargin}(v)$, cf. (26). The model keeps track of this margin by remembering the initial speed v_0 at the beginning of the brake maneuver.

For safety reasons, the train assumes all aspects in *accMargin* might be disadvantageous for the train (e.g., just a split-second later accelerating may no longer be safe). As a result, if all aspects in *accMargin* turn out in favor of the train (e.g., if the train could still have accelerated almost the full ε time later), the train will stop with $\mathit{accMargin}(v_0)$ distance to the track position limit e. Theorem 3 formalizes this intuition. Note that we neglect track control *tc* here, since it issues stopping points for the service brakes.

Theorem 3 (Late Braking of Train Controller with Brake Delay). *Model 7 ensures that the train stops no earlier than point* $e - \mathit{accMargin}(v_0)$ *when it uses pressure brakes. The following formula is proved in KeYmaera X:*

$$\mathit{assumptions} \rightarrow [(\mathit{ctrl}_z;\ \mathit{motion})^*]\Big(\underbrace{c > 0}_{\text{Pressure brake engaged}} \wedge \underbrace{v \leq d}_{\text{Braking finished}} \rightarrow z \geq \underbrace{e - \mathit{accMargin}(v_0)}_{\text{Earliest stopping point}}\Big)$$

5 Experimental Results

Simulation (Fig. 3) of the motion models suggests that, for safety reasons, the symbolic safety margin (9) of the brake delay model (Model 4) needs to be more conservative than the margins (15)–(18) of the pressure propagation model (Model 6). The difference in safety margins to the latest stopping point is characterized by this brake performance:

$$\mathit{margin} - \begin{cases} v\varepsilon + \mathit{mSlow}(v) & \text{if } \neg\mathit{isFast}(v) \wedge f_a \leq 0 \\ v\varepsilon + \frac{f_a\varepsilon^2}{2m} + \mathit{mSlow}\left(v + \frac{f_a\varepsilon}{m}\right) & \text{if } \neg\mathit{isFast}(v) \wedge f_a \geq 0 \\ v\varepsilon + \mathit{mFast}(v) & \text{if } \mathit{isFast}(v) \wedge f_a \leq 0 \\ v\varepsilon + \frac{f_a\varepsilon^2}{2m} + \mathit{mFast}\left(v + \frac{f_a\varepsilon}{m}\right) & \text{if } \mathit{isFast}(v) \wedge f_a \geq 0 \end{cases} \tag{28}$$

We use formula (28) to compare the performance of Model 4 to Model 6 on parameters chosen according to standard configurations [6], see Table 2. Using these parameters, the net stopping distance with full braking force $-F_{pb}$ when neglecting brake pressure propagation is $\frac{v^2 m}{2F_{pb}}$ (e.g., 8 682ft for a fast, long, loaded train, which is close to the stopping distances in [6, Fig. 10]). With brake pressure propagation, the proofs of Theorem 1 and Theorem 2 show that an additional safety margin is needed to avoid overshoot. The resulting stopping distances including these safety margins are summarized for various configurations in Table 3. Note that F_{pb} in [6] is approximated with $23\,338\frac{\text{klbf}}{\text{car}}$ for unknown load, i.e., when trains are not equipped with sensors to determine whether or not their cars are empty. This approximation "improves" the brakes of empty cars, so in Table 3 empty trains with $F_{pb} = 23\,338\frac{\text{klbf}}{\text{car}}$ for unknown load stop sooner than those with $F_{pb} = 10\,575\frac{\text{klbf}}{\text{car}}$ for known load. The brake pressure propagation time t_{appl} is much larger than control cycle time ε, so the additional safety margin of the conservative model is dominated by the train's speed and the brake pressure propagation time. After all, the delay term $(v + \frac{A}{m}\varepsilon)t_{appl}$ implies that the train controller

Table 2: Experiment parameter choices (in FRA standard units)

Parameter		Value	Description	Source
l_z	Short	753ft	10 cars	[6, Fig. 20]
	Medium	2 345ft	40 cars	[6, Fig. 20]
	Long	5 531ft	100 cars	[6, Fig. 20]
m	Loaded	$263\frac{\text{klb}}{\text{car}}$	e.g., medium train 10 520klb	[6, Tab. 2]
	Empty	$64\frac{\text{klb}}{\text{car}}$	e.g., medium train 2 560klb	[6, Tab. 2]
v	Slow, Fast	10, 60mph		[6, Tab. 2]
F_{pb}	Loaded	$35\,750\frac{\text{lbf}}{\text{car}}$	e.g., medium train 1 430klbf	[6, p. 22]
	Empty	$10\,575\frac{\text{lbf}}{\text{car}}$	e.g., medium train 423klbf	[6, p. 22]
	Unknown	$23\,338\frac{\text{lbf}}{\text{car}}$	e.g., medium train 933.5klbf	[6, p. 22]
t_{appl}			$12.22 + 0.0156l_z + 0.000000278l_z^2$	[6, Fig. 20]
A		$5\frac{\text{mph}}{\text{min}}$	Force by $\frac{0.44704A}{60}m$, e.g., medium train 391.91klbf	[6, Fig. 27]
f_a		$1.75\frac{\text{mph}}{\text{min}}$	e.g., medium train 136.76klbf	[6, Fig. 27]
ε		100ms		

Table 3: Stopping distance with brake pressure propagation (in ft, lower is better); bold differences exceed the performance objective of [6] (slow: 500ft, fast: 1000ft)

	Slow						**Fast**					
	Loaded			**Empty**			**Loaded**			**Empty**		
Cars	10	40	100	10	40	100	10	40	100	10	40	100
Brake force for unknown load $F_{pb} = 23\,338\frac{\text{lbf}}{\text{car}}$												
Model 4	726	1,110	1,942	446	830	1,662	15,436	17,742	22,730	5,369	7,676	12,664
Model 6	541	710	1,017	239	345	503	14,364	15,494	17,880	4,278	5,334	7,383
Difference	185	400	**925**	207	485	**1,161**	**1,072**	**2,248**	**4,850**	**1,091**	**2,342**	**5,281**
Brake force for known load, loaded: $F_{pb} = 35\,750\frac{\text{lbf}}{\text{car}}$, empty: $F_{pb} = 10\,575\frac{\text{lbf}}{\text{car}}$												
Model 4	597	982	1,814	554	939	1,771	10,817	13,123	18,111	9,277	11,583	16,571
Model 6	409	565	822	364	512	746	9,743	10,859	13,188	8,200	9,309	11,602
Difference	188	417	**992**	190	427	**1,025**	**1,074**	**2,264**	**4,923**	**1,077**	**2,274**	**4,969**

assumes it might be driving with its current speed for the entire brake propagation time t_{appl}. The effect is even more pronounced for empty trains, because a larger fraction of the entire braking process occurs while pressure is still propagating. The remaining improvements of Model 6 over Model 4 target effects during the control cycle time (e.g., distinguish between accelerating and braking, account for the actual chosen acceleration instead of worst-case acceleration), so could be neglected without much impact on the performance for the specific values of our experiments. The cases highlighted in bold indicate cases where just the additional error incurred by the delay model exceeds the FRA's performance objective goal. This indicates the potential for using more advanced control algorithms.

Table 4: Proof statistics

Main tactic purpose		Tactic size		Proof steps	Time	Performance
		LOC	Steps		$[s]$	$[\frac{\text{Steps}}{s}]$
Theorem 1	Case-splitting (loop invariant $\max$)	107	200	35,740	100	357
Theorem 2	Arithmetic simplifications	216	624	59,998	270	222

Proof Effort From an engineering viewpoint, more realistic models are certainly desirable. However, higher modeling fidelity often results in higher proof complexity, especially in the resulting arithmetic. Proofs in KeYmaera X consist of three main aspects: (i) find invariants for loops and differential equations, (ii) symbolically execute programs to determine their effect (results in formulas in real arithmetic), and finally (iii) verify the resulting real arithmetic with external solvers. High modeling fidelity becomes expensive in the arithmetic parts of the proof, since real arithmetic is decidable but of high complexity. As a result, proofs of high-fidelity models may require arithmetic simplifications (e.g., reduce the number of variables by abbreviating complicated terms, or by hiding irrelevant facts) before calling external solvers. The proof process in KeYmaera X can be scripted with tactics to provide human guidance when necessary.

The main insights of doing the proofs are reflected in the model in terms of the control constraints that switch between driving and braking. We illustrated how to obtain such constraints systematically from the motion model of the train when designing the track control. Further guidance provided in the proof tactics of Theorem 1 and Theorem 2 are related to arithmetic simplifications, deferred case splitting to avoid duplicate proof effort, and to speed up rerunning proofs over automated tactics.

The proof of Model 4 was mostly automated with minor case-splits. The tactics nevertheless script differential equation handling to speed up rerunning the proofs. Model 6, in contrast, required arithmetic simplifications to become tractable, and even then resulted in significantly lower proof performance. Table 4 summarizes the proof statistics.

6 Related Work

Train interlocking systems check that trains are not *scheduled to share* route sections at the same time. Formal verification techniques was used in academia [16,8] and industry [5]. Formal methods provide an effective way to satisfy certification requirements such as CENELEC EN-50126 [7]. The properties are phrased as safety properties in temporal logic, and analyzed by model checking, e.g., in SystemC [14], or Simulink [12,4]. High-level safety specifications can also be linked to interlocking rules represented in lookup tables through assurance case arguments [17]. At industrial scale, discrete aspects of train control were formally specified and with the B method [1] preserved along refinements to implementations, e.g., in the Paris METEOR project and the New York City Canarsie line [10], or for analyzing railway network topology [11]. Safety of approaching and passing railroad crossings was analyzed with timed automata (e.g., [15,18]), with motion represented, if at all, as jumps at discrete time steps. These approaches provide guarantees on the discrete train coordination but not the motion.

We analyze the complementary question whether the physical motion of trains respects the instructions issued by a correct route interlocking protocol. The combination of both answers is required for safe control. The job of interlocking approaches is to guarantee that disjoint movement authorities are issued to trains. Our results guarantee that the train controllers with their continuous dynamics ensure that the trains never move outside these permitted areas, without which the system would not be safe.

ETCS verification [23,20] formally verifies collision freedom between trains when following the movement authorities issued by a radio-block controller. The protocol is modeled as a hybrid systems model, including motion of the train. The ETCS proofs were the basis for a case study on the Chinese train control system [25]. Similar motion models were used for safety verification of railroad crossings with hybrid automata [9].

Here, we focus on significantly more detailed physical models for train braking, which are the gold standard by the Federal Railway Authority. Their additional considerations of mass, length of the train, their effect on pressure brake propagation, and resulting jerk on the dynamics leads to a more realistic yet also more challenging verification result. We analyze the models both for safety and performance objectives.

7 Conclusion

We analyzed the safety of train control by formalizing hybrid systems models of control decisions and their physical effect in terms of stopping distance under two braking models. We studied a lower-fidelity braking model that conservatively approximates pressure propagation with delayed brake onset, and a higher-fidelity braking model with gradual braking force increase during pressure propagation. Our proofs in the hybrid systems prover KeYmaera X show that safety is achievable in both braking models with appropriate control constraints that indicate when free driving is safe and when braking is required for safety. We developed these constraints alongside the proof.

Conservative approximation in braking controllers may degrade performance and engage brakes unnecessarily early, but more complex controller designs and physics models may increase verification/implementation complexity and runtime resource consumption. We analyzed the trade-off between modeling fidelity and verification complexity: the performance comparison between the two models indicates a significantly better performance (i.e., lower stopping distance) in the higher-fidelity model. However, in this case higher modeling fidelity also results in higher proof complexity, especially in the resulting arithmetic. KeYmaera X provides support for scripting proofs with tactics to provide the necessary human guidance in a machine-repeatable way.

References

1. Abrial, J.: The B-book - assigning programs to meanings. Cambridge University Press (2005)
2. Ahmad, H.A.: Dynamic braking control for accurate train braking distance estimation under different operating conditions (2013)
3. Bohrer, B., Rahli, V., Vukotic, I., Völp, M., Platzer, A.: Formally verified differential dynamic logic. In: Bertot, Y., Vafeiadis, V. (eds.) Certified Programs and Proofs - 6th ACM SIGPLAN Conference, CPP 2017, Paris, France, January 16-17, 2017. pp. 208–221. ACM (2017)

4. Bonacchi, A., Fantechi, A., Bacherini, S., Tempestini, M., Cipriani, L.: Validation of railway interlocking systems by formal verification, A case study. In: SEFM. LNCS, vol. 8368, pp. 237–252. Springer (2013)
5. Borälv, A.: Case study: Formal verification of a computerized railway interlocking. Formal Aspects of Computing 10(4), 338–360 (1998)
6. Brossaeu, J., Ede, B.M.: Development of an adaptive predictive braking enforcement algorithm. Tech. Rep. FRA/DOT/ORD-9/13, Federal Railroad Administration (2009)
7. Cimatti, A., Corvino, R., Lazzaro, A., Narasamdya, I., Rizzo, T., Roveri, M., Sanseviero, A., Tchaltsev, A.: Formal verification and validation of ERTMS industrial railway train spacing system. In: CAV. LNCS, vol. 7358, pp. 378–393. Springer (2012)
8. Cimatti, A., Giunchiglia, F., Mongardi, G., Romano, D., Torielli, F., Traverso, P.: Model checking safety critical software with SPIN: an application to a railway interlocking system. In: SAFECOMP. LNCS, vol. 1516, pp. 284–295. Springer (1998)
9. Damm, W., Hungar, H., Olderog, E.: On the verification of cooperating traffic agents. In: FMCO. LNCS, vol. 3188, pp. 77–110. Springer (2003)
10. Essamé, D., Dollé, D.: B in large-scale projects: The Canarsie line CBTC experience. In: B 2007. LNCS, vol. 4355, pp. 252–254. Springer (2007)
11. Falampin, J., Le-Dang, H., Leuschel, M., Mokrani, M., Plagge, D.: Improving railway data validation with ProB. In: Industrial Deployment of System Engineering Methods, pp. 27–43. Springer (2013)
12. Ferrari, A., Fantechi, A., Magnani, G., Grasso, D., Tempestini, M.: The Metrô Rio case study. Sci. Comput. Program. 78(7), 828–842 (2013)
13. Fulton, N., Mitsch, S., Quesel, J.D., Völp, M., Platzer, A.: KeYmaera X: An axiomatic tactical theorem prover for hybrid systems. In: Felty, A., Middeldorp, A. (eds.) CADE. LNCS, vol. 9195, pp. 527–538. Springer (2015)
14. Haxthausen, A.E., Peleska, J., Kinder, S.: A formal approach for the construction and verification of railway control systems. Formal Asp. Comput. 23(2), 191–219 (2011)
15. Heitmeyer, C.L., Lynch, N.A.: The generalized railroad crossing: A case study in formal verification of real-time systems. In: RTSS. pp. 120–131. IEEE Computer Society (1994)
16. Hong, L.V., Haxthausen, A.E., Peleska, J.: Formal modelling and verification of interlocking systems featuring sequential release. Sci. Comput. Program. 133, 91–115 (2017)
17. Iliasov, A., Romanovsky, A.: Formal analysis of railway signalling data. In: HASE 2016. pp. 70–77. IEEE Computer Society (2016)
18. Ortmeier, F., Reif, W., Schellhorn, G.: Formal safety analysis of a radio-based railroad crossing using deductive cause-consequence analysis (DCCA). In: EDCC. LNCS, vol. 3463, pp. 210–224. Springer (2005)
19. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reas. 41(2), 143–189 (2008)
20. Platzer, A.: Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics. Springer, Heidelberg (2010)
21. Platzer, A.: Logics of dynamical systems. In: LICS. pp. 13–24. IEEE (2012)
22. Platzer, A.: A complete uniform substitution calculus for differential dynamic logic. J. Autom. Reas. 59(2), 219–265 (2017)
23. Platzer, A., Quesel, J.D.: European Train Control System: A case study in formal verification. In: Breitman, K., Cavalcanti, A. (eds.) ICFEM. LNCS, vol. 5885, pp. 246–265. Springer (2009)
24. Polivka, A., Ede, B.M., , Drapa, J.: North american joint positive train control project. Tech. Rep. DOT/FRA/ORD-09/04 (2009)
25. Zou, L., Lv, J., Wang, S., Zhan, N., Tang, T., Yuan, L., Liu, Y.: Verifying chinese train control system under a combined scenario by theorem proving. In: VSTTE. LNCS, vol. 8164, pp. 262–280. Springer (2013)