Towards Formal Verification of Freeway Traffic Control

Stefan Mitsch
Marshall-Plan Scholar
Johannes Kepler University
Linz, Austria
stefan@tk.jku.at

Sarah M. Loos, André Platzer
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA, USA
{*sloos,aplatzer*}*@cs.cmu.edu*

***Abstract*—We study how CPS technology can help improve freeway traffic by combining local car GPS positioning, traffic center control decisions, and communication to achieve more tightly coupled feedback control in intelligent speed adaptation. We develop models for an intelligent speed adaptation that respects variable speed limit control and incident management. We identify safe ranges for crucial design parameters in these systems and, using the theorem prover KeYmaera, formally verify safety of the resulting CPSs. Finally, we show how those parameter ranges can be used to decide trade-offs for practical system implementations even for design parameters that are not modeled formally.**

***Keywords*-Freeway traffic control, intelligent speed adaptation, hybrid system**

I. Introduction

Traffic centers have the goal of ensuring global functioning and safety of a freeway or highway network. The available control options comprise, for instance, variable speed limits, ramp metering, lane closures, detours, arterial traffic light control, and warning signs displaying traffic incident information (e.g., traffic jams, construction sites, or driving conditions). A number of theoretical and experimental results have shown that such global highway and freeway traffic control increases safety [1], [2], homogenizes traffic flow [3], and may increase the flow during peak periods [4], [5]. Today's highway and freeway traffic control is centralized in traffic centers (e.g., on a per state level) with little direct influence on the behavior of cars, making it an open-loop control system. Typically, advice to drivers is displayed on dynamic traffic signs mounted on gantries, broadcasted via radio stations, or to GPS navigation systems.

With the advent of more precise and pervasive sensing as well as car-to-car (C2C) and car-to-infrastructure (C2I) communication, a large amount of dynamic traffic information about individual cars becomes available. It is a promising idea to exploit such dynamic traffic information and complement the (geographically) static road infrastructure with dynamic infrastructure-to-car communication. As a result, custom traffic advice could be provided to each car individually, broadcast to all cars in an area, and, in the futre, may even be fed directly as set values into the controllers of (semi-)automatic driver assistance technology in the cars.

At this point, at the latest, the scenario is a prototypical *cyber-physical system* (CPS) case. On the one hand, we find the physics of the movement of a car or a collection of cars down the streets. On the other hand, we have onboard computers embedded in the car and various of its controllers as well as computers in the traffic center that analyze dynamic traffic flow information and support humans with traffic management decisions. In the middle, we find the communication that sends status, traffic, and flow information from the roadside sensor infrastructure and the car GPS's to the traffic centers and the communication that broadcasts, e.g., variable speed limit decisions back to cars and dynamic traffic signs. The CPS is especially interesting when we close the loop and use car information to enhance traffic center decisions and provide traffic center control for individual cars, both connected via C2I communication. The hope is that integrated CPS could direct the fleet of cars more efficiently than a relatively uninformed traffic center without means for direct feedback.

This technology would not be particularly useful if it lead to vastly suboptimal or incorrect control decisions, possibly even endangering safety on the road instead of improving it. For one thing, decision time delays, which may be negligible in more local control scenarios, have a serious impact on the overall CPS dynamics and its behavior over time given the long-range communication and control loop. One particularly interesting challenge to help develop such next generation road traffic control, thus, is the question of how to ensure correct functioning and reliability of such a system. Another challenge is to identify safe margins on the system within which traffic flow can be optimized without endangering safety. First steps towards the verification of safety in road traffic control have been taken by verifying that cars with local adaptive cruise control cannot collide [6]. As a next step, we introduce global control by highway authorities. Our main contribution is a model of a distributed intelligent speed adaptation system and a formal proof that this system correctly disseminates speed limit information and guarantees for cars adhering to the speed limit. For this, we identify constraints on the input and output parameters that car and traffic center controllers need to obey to remain within the safely operable bounds of the system.

These constraints are also relevant in local control loops that replace the traffic center with in-car driver assistance systems, such as traffic sign, pedestrian, or obstacle detectors, picking up control decisions from roadside infrastructure or detecting incidents along the road. The constraints can serve as a basis for precise requirements for driver assistance systems with regard to, for instance, image resolution, focal length of the camera lense, and computation time. In combination with car control, this scenario represents a fully autonomous, active intelligent speed adaptation system [7].

In summary, our contributions are (i) a model of a distributed intelligent speed adaptation system obtaining speed advice from traffic centers, traffic sign detectors, or obstacle detectors, (ii) lower and upper bounds on the position of speed limit area beginnings relative to the position of a car, and (iii) requirements for the implementation of such systems that directly follow from the bounds.

This paper is organized as follows. In the next section, we discuss related research concerning global control in traffic centers and local control with in-car driver assistance technology, with a focus on formal verification. Section III recalls differential dynamic logic as a modeling formalism for the behavior and the safety constraints of our system. In Sect. IV we discuss the challenges in intelligent speed adaptation and, from these, derive the input and output parameters and the general structure of the system. Section V then presents a model and verification of a lower bound for speed limit choices, and Sect. VI extends this model with an upper bound becoming necessary when incidents moving towards cars make speed limits mandatory. Finally, Sect. VII concludes the paper with an outlook on future work.

II. Related Work

We discuss related work from the application areas that we focus on: firstly concerning global control in traffic centers from the viewpoint of intelligent speed adaptation, secondly considering advanced driver assistance systems, and, finally, concerning formal verification of traffic control systems.

Lu et al. [8] demonstrate with simulations that higher-level control strategies, such as variable speed limits, can help increase traffic flow and reduce congestion in bottleneck areas. Dia et al. [9] also used simulation to assess the impact of incident management techniques such as ramp metering, route diversion, and variable speed limits. We verify that such variable speed limits can be disseminated to cars in a safe manner, and that these cars comply with the speed limit at all times. Intelligent speed adaptation [10] and variable speed limit sign systems [1] have increasingly gained attention as a means to increase road traffic safety. Related research in these areas, however, (i) focuses on experiments and simulations of traffic behavior [4], [5] and models for determining optimal speed limits [11], (ii) shows the effectiveness of speed adaptation in terms of reducing casualties [1], [12], homogenizing speed [3], increasing compliance with speed limits [10], as well as (iii) discusses impacts on travel time and throughput. We, instead, investigate constraints that implementations of such a system must respect and verify the safety that can be guaranteed under these constraints.

Automated highway control has been the focus, for instance, of the California PATH project (for an overview see [13]), which also investigated the integration of vehicles and roadside infrastructure [14]. Particularly relevant is the work of Ioannou et al. [15] on an integrated roadway/adaptive cruise control system, which was shown to improve travel times and smoothen traffic flow. Similarly, Baskar et al. [16] combined automated vehicle platooning with conventional traffic control in a hierarchy of cooperating controllers with different responsibilities. Again, these works tested safety only partially (mostly using simulation), and do not derive constraints for implementation. Our model is similar, in that it also divides responsibilities between distributed controllers. However, our verification results allow us to derive constraints for the cooperation between higher-level controllers, such as area, regional, or super-regional controllers [16] and highway traffic management control [15] (i.e., traffic centers), and lower-level platoon and vehicle controllers.

With the recent commercialization of advanced driver assistance systems, such as adaptive cruise control, braking assistants, and lane guard systems, also research on traffic sign, crosswalk, and pedestrian detection (cf., for instance, [17], [18], [19], [20], [21]) gained popularity. Such systems are also vital in realizing the vision of fully autonomous vehicles [22]. While investigating detection quality and computation speed, both being undisputedly important characteristics of these systems, none of the works focused on determining the necessary bounds within which such a system can be operated safely.

Verification of safety has been the focus of Loos et al. [6] in their work on adaptive cruise control. Their model focused on mutual safety of cars following each other on a highway. In contrast, we discuss the interplay of cars and roadside infrastructure. Traffic centers disseminating virtual information that may change arbitrarily (i.e., whose positions are not constrained by physical limits and continuity). We, thus, need to find appropriate bounds for traffic center decisions. Moreover, our model allows physical entities on a freeway (e.g., incidents) to move opposite to the driving direction, which was assumed not to happen in [6]. Movement authorities, which are somewhat similar to speed limits, have been used in verifying the European train control system [23]. They are issued centrally at frequent intervals and trains are not allowed to move without frequent clearance. These results are not applicable to road traffic, because permanent negotiation for movement clearance does not scale to the vast number of cars on a highway (in comparison to the small number of trains on a railroad network). Also, motion was

Table I
STATEMENTS OF HYBRID PROGRAMS

Statement	Effect
$\alpha;\ \beta$	sequential composition, first performs α and then β afterwards
$\alpha\ \cup\ \beta$	nondeterministic choice, following either α or β
α^*	nondeterministic repetition, repeating α $n \geq 0$ times
$x := \theta$	discrete assignment of the value of term θ to variable x (jump)
$x := *$	nondeterministic assignment of an arbitrary real number to x
$\big(x_1' = \theta_1, \ldots,$ $x_n' = \theta_n\ \&\ F\big)$	continuous evolution of x_i along differential equation system $x_i' = \theta_i$, restricted to maximum domain or invariant region F
$?F$	check if formula F holds at current state, abort otherwise
if(F) then α else β	perform α if F holds, perform β otherwise

only allowed in accordance with the driving direction of a railroad link. In [24], online verification techniques are presented to derive collision probabilities for autonomous cars. However, deriving bounds and implementation requirements has not been the focus in their work.

III. PRELIMINARIES: DIFFERENTIAL DYNAMIC LOGIC

For specifying and verifying correctness statements about hybrid systems, we use *differential dynamic logic* dL [25], [26].

Differential dynamic logic supports *hybrid programs* [25], [26] as a program notation for hybrid systems. The syntax of hybrid programs is summarized together with an informal semantics in Tab. I. We use hybrid programs to describe our system models. The sequential composition $\alpha;\ \beta$ expresses that β starts after α finishes (e.g., first let a traffic center choose a maximum speed, then a position for a speed limit area). The nondeterminic choice $\alpha\ \cup\ \beta$ follows either α or β (e.g., let a traffic center decide nondeterministically between keeping an existing speed limit or choosing a new one). The nondeterministic repetition operator α^* repeats α zero or more times (e.g., let a traffic center choose new speed limits arbitrarily often, not just once). Discrete assignment $x := \theta$ instantenously assigns the value of the term θ to the variable x (e.g., let a car choose a particular acceleration), while $x := *$ assigns an arbitrary value to x (e.g., let a car choose any acceleration). $x' = \theta\ \&\ F$ describes a continuous evolution of x within the evolution domain F (e.g., let the velocity of a car change according to its acceleration, but always be greater than zero). The test $?F$ checks that a particular condition expressed by F holds, and aborts if it does not (e.g., check that an arbitrarily chosen acceleration stays within the physical limits of a car because physically impossible accelerations are never considered). Finally, if(F) then α else β is a deterministic choice that executes α if F holds, and β otherwise (e.g., let a traffic center decide upon the position of a car whether or not a speed limit should be issued).

To specify the desired correctness properties of the hybrid programs, differential dynamic logic (dL) provides modal operators $[\alpha]$ and $\langle\alpha\rangle$, one for each hybrid program α. When ϕ is a dL formula (e.g., a simple arithmetic constraint) describing a safe state and α is a hybrid program, then the dL formula $[\alpha]\phi$ states that all states reachable by α satisfy ϕ. Dually, formula $\langle\alpha\rangle\phi$ expresses that there is a state reachable by the hybrid program α that satisfies formula ϕ. The dL formulas are generated by the following EBNF grammar (where $\sim \in \{<, \leq, =, \geq, >\}$ and θ_1, θ_2 are arithmetic expressions in $+, -, \cdot, /$ over the reals):

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

Differential dynamic logic is not only a specification language for hybrid systems (as hybrid programs) and desired correctness properties (as dL formulas), but also comes with a verification technique to prove those correctness properties. We use this verification technique [25], [26], which is a proof calculus implemented in the verification tool KeYmaera.

IV. CHALLENGES IN INTELLIGENT SPEED ADAPTATION

A typical application of intelligent speed adaptation with variable speed limits is to lower and homogenize speed in the area of traffic incidents [1]. For example, Lu et al. [8] use variable speed limit control to maximize bottleneck flow in an area of a lane drop, such as encountered when lanes merge or lanes are closed due to road work. The nature of traffic incidents in conjunction with the distributed setting of cars and traffic centers, however, poses several challenges on the integration of roadside infrastructure and vehicle control in general, and on the implementation of intelligent speed adaptation systems in particular, as detailed below.

Traffic incidents can not only occur at a geographically fixed position (i.e., be static, such as construction sites), but also change their position (e.g., traffic jams, wrong-way drivers) in the worst case in the opposite direction of traffic on a freeway. Often, motion of traffic incidents can only be approximated using complex models (e.g., shock waves traveling opposite to the driving direction on a freeway [27]). However, estimations about the velocity of incidents can be made, for instance, on the basis of traffic operator experience, or from traffic throughput measurings of induction loop detector arrays.

Nevertheless, the positions and points in time at which incidents occur are completely nondeterministic. As a result, special focus must be laid on the trade off that traffic centers

have to make upon occurrence of an incident: as many cars as possible should be warned, which means that speed limits have to be enacted as close as possible to an incident, while at the same time speed limits should only be enacted at safe positions (i.e., at positions that guarantee for cars being able to meet the speed limit).

These matters are even made worse by the fact that the communication delay between a traffic center and a car is non-negligible. During this communication delay, the car moves and the incident changes its position. In order to be effective, variable speed limits must be enacted (from the viewpoint of cars traveling on a freeway) in front of an incident. As a consequence, the traffic center has to estimate a latest speed limit position, which ensures that a car receives its speed limit in any case before it meets an incident.

The promising effects of roadside infrastructure and vehicle integration demonstrated in [15] in terms of better managed traffic with reduced travel times and smoothened traffic flow, which in turn may lead to improvements in safety and environment, however, make it worthwile to accept these challenges.

The result of this paper is a formally verified model of a straight stretch of highway (which may comprise traffic incidents, such as accidents, construction sites, and traffic jams) controlled by a traffic center and a car following its local control and the variable speed limit issued by the traffic center (i.e., the car does not purposefully violate speed limits). The car has a position, velocity, and acceleration and must obey the laws of physics. The model additionally accounts for sensor and actuator delay within the car, communication between the car and the traffic center, and computation in both. The possible delays caused by communication with central facilities are non-negligible.

Complex maneuvers, such as lane changes, and cars entering and leaving the highway, are not essential for the purpose of our proofs and therefore omitted in the model. It is of utmost importance that the control choices of the car and the traffic center at all times ensure safety of the car, that is, make it possible for the car to meet the speed limit, and safety of the traffic center decision—i.e., set the speed limit at a position on the lane that is between the car and the incident. In Sect. V, we prove that the speed limit choices of the traffic center can at all times be followed by the car. In Sect. VI, we introduce a static or moving incident (such as an actual or virtual lane drop, e.g., a construction site, or a traffic jam) and prove safety of the speed limit choices.

V. Variable Speed Limit Control

As a first step towards verifying traffic control, the problem that we are solving is: a car on a straight lane can accelerate, coast and brake and we prove that it will not exceed the speed limit set by the traffic center or indicated by a traffic sign detector at any point. This system contains discrete and continuous dynamics, thus it is a hybrid system. Alone, the necessity for issuing a speed limit may arise at any time. As a consequence, both the traffic center and the traffic sign detector can repeatedly issue new speed limits—comprising a maximum speed and a position denoting the speed limit area—or decide to stick with already set ones. Newly issued speed limits are communicated to the car controller (in the case of the traffic center, e.g., wirelessly or via conventional roadside infrastructure), which, anyway, takes time. In the meantime, of course, the car's position evolves according to its velocity and acceleration. As a consequence, the traffic center must take into account the car's position, velocity, and acceleration, and the time needed for communicating to and processing the decision in the car when choosing the maximum speed and position of a speed limit area, in order to avoid issuing speed limits that cannot be complied with (e.g., we cannot demand the car to brake from 30 m/s to 20 m/s within 1 m). Likewise, a traffic sign detector must be able to correctly recognize a speed limit sign at a distance depending on the car's velocity and acceleration, and the time needed for processing the speed limit sign image, communicating to and processing the speed limit in the car controller. At the cost of more conservative decisions and distance/processing bounds, this information demand can be relaxed by assuming generic maximum values for velocity, acceleration, and communication and processing time.

Here, we abstract from the details of traffic centers and traffic sign detectors by modeling the relevant characteristics of the decisions both have to make (i.e., the maximum speed allowed in and the geographical position of the speed limit area), as described in the following paragraph. Formal verification of the model guarantees safety in all considered situations. This allows us to derive from the model the bounds for (i) maximum speed and geographical position relevant for the traffic center, and (ii) distance and processing time of a traffic sign detector. Since we use individual speed limits for each car (realized with direct communication between traffic centers and cars, or with traffic sign detectors inside the car), we can safely simplify our model to a single car.

Modeling: Based on the adaptive cruise control model of Loos et al. [6], we develop a formal model of a distributed intelligent speed adaptation system as a hybrid program (HP). The car has state variables describing its current position (x_c), velocity (v_c), and acceleration (a_c). The continuous dynamics of the car is described by the differential equation system of ideal-world dynamics for longitudinal position changes ($x_c' = v_c, v_c' = a_c$). We assume bounds for acceleration a_c in terms of a maximum acceleration $A \geq 0$ and a minimum positive braking power $b > 0$. We introduce a constant ε that provides an upper bound for sensor and actuator delay, communication between the traffic center or traffic sign detector and the car controller, and computation

Model 1 Variable speed limit control (vsl)

$$vsl \equiv (ctrl; dyn)^* \tag{1}$$
$$ctrl \equiv ctrl_{car} || ctrl_{ctr}; \tag{2}$$
$$ctrl_{car} \equiv (a_c := -b) \tag{3}$$
$$\cup \left(?Safe_{\underline{x_{sl}}}; a_c := *; ?(-b \leq a_c \leq A)\right) \tag{4}$$
$$\cup \left(?x_c \geq x_{sl}; a_c := *; ?(-b \leq a_c \leq A \wedge a_c \leq \frac{v_{sl} - v_c}{\varepsilon})\right) \tag{5}$$
$$\cup (?v_c = 0; a_c := 0) \tag{6}$$
$$Safe_{\underline{sl}} \equiv x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \tag{7}$$
$$+ \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \leq x_{sl} \tag{8}$$
$$ctrl_{ctr} \equiv (x_{sl} := x_{sl}; v_{sl} := v_{sl}) \tag{9}$$
$$\cup \left(x_{sl} := *; v_{sl} := *; ?(v_{sl} \geq 0 \wedge Safe_{\underline{sl}})\right) \tag{10}$$
$$dyn \equiv (t := 0; x_c' = v_c, v_c' = a_c, t' = 1 \tag{11}$$
$$\& v_c \geq 0 \wedge t \leq \varepsilon) \tag{12}$$

in both. The car controller[1] and the traffic center may react and exchange messages as quickly as they want, but they can take no longer than ε.

The car is allowed to brake at all times through (3) having no precondition, which is also the only option if there is not enough distance between the car and the speed limit area to maintain speed or accelerate. If the car is still at a safe distance from the speed limit area, it may choose its acceleration freely within the bounds of its braking power and acceleration, cf. (4). Safety of the car is given when (7) and (8) are satisfied, i.e., if the car can drive up to ε time units with any choice of acceleration, and still adhere to the speed limit. For this, the distance between the car's current position x_c and the beginning of the speed limit area x_{sl} must account for two components: first, the car may need to brake from its current velocity v_c down to v_{sl}, and in the course of this travel the distance given in (7). Second, since the car may not notice the speed limit up to ε time units, we must additionally take into account the distance that the car may travel with its current velocity and worst-case acceleration A and the distance needed for compensating its potential acceleration of A during that time with braking power b, see (8). In the speed limit area the car may choose its acceleration within its physical limits and depending on the current velocity difference to the speed limit, see (5). Note that for the implementation of a car controller that computes its acceleration only on the basis of the physical boundaries of the car (i.e., A and b), the additional restriction $a_c \leq \frac{v_{sl} - v_c}{\varepsilon}$ can be used as a precondition using maximum acceleration $v_c + A \cdot \varepsilon \leq v_{sl}$. Finally, the car may choose to stand still if its current velocity is zero already (6), since the continuous dynamics, in accordance with freeway traffic rules, do not allow velocities below zero (i.e., driving opposite to the driving direction on a freeway is prohibited).

The traffic center may choose to keep a current speed limit, cf. (9), or set a new speed limit v_{sl} (which, of course, must not force the car to drive backwards) at a new, safe position x_{sl}; see (10). This safe position guarantees, that the car is still able to meet the speed limit even if it does not receive and cannot react on the new speed limit for up to ε time units. For making this decision, it is essential that the controller in the traffic center knows or can estimate the current position, velocity, braking and acceleration capabilities of the car, and the time needed for reaction. Note that it is only mandatory to communicate the current position of the car (allowing, of course, some inaccuracy) to the traffic center. At the expense of a less stringent speed limit area (i.e., the safety distance may be larger than absolutely necessary), worst case estimations can be used for all other values (e.g., general highway speed limits, typical car acceleration, and minimum braking power demanded by law).

Car and control center can repeatedly choose acceleration and speed limit, respectively, which is represented by the nondeterministic repetition operator * in (1). The controllers of the car and the traffic center operate in parallel, cf. (2). Since the controllers are independent with respect to their read and write variables, the parallel operation can also be modeled using a sequential composition. The order of components in a sequential composition is significant: we model the control of the car followed by the control of the traffic center, and finally the dynamics of the system. As a result, the system evolves before the traffic center decisions reach the car controller at the next iteration, which models communication delay between the traffic center and the car.

The continuous dynamics (11) of the model describe the evolution of the car's position and velocity according to the current acceleration. We use a variable t that evolves with constant slope (i.e., a clock) for measuring time within the upper bound ε, and constrain the evolution of velocity v_c to non-negative values, see (12).

Verification: We verify the safety of a speed limit choice as modeled above, using a formal proof calculus for dL [25], [26]. In this use case, the car must comply with the speed limit inside a speed limit area at all times. The following condition captures this requirement as an invariant that must hold at all times during the execution of the model:

$$c \searrow sl \equiv \left(v_c \leq v_{sl} \vee x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b}\right) \wedge v_c \geq 0 \wedge v_{sl} \geq 0$$

[1]Note that the car controller may also be a human driver, in which case the processing time in the car is mostly attributed to the reaction time of the driver.

The formula states that a speed limit chosen by the traffic center or detected by the traffic sign detector can be complied with when the car's current velocity is already less or equal to the speed limit, or there is still enough distance for the car to brake (and the car must drive forward, and the speed limit not demand driving backwards).

Proposition 1 (Safety of speed limit): If a car is at a safe distance from x_{sl} initially, then it will not exceed the speed limit past the beginning of a speed limit area while the car controller and the traffic center or traffic sign detector follow the `vsl` control model. Compliance with the speed limit is expressed by the provable formula $(c \searrow sl) \rightarrow [vsl](x_c \geq x_{sl} \rightarrow v_c \leq v_{sl})$

We proved Proposition 1 using KeYmaera, a theorem prover for hybrid systems. The resulting proof files are available online as projects in KeYmaera[2].

Safe bounds: The condition $Safe_{\underline{sl}}$, see (7), provides bounds on the minimum distance of a speed limit area to the current position of a car (assuming a certain maximum speed), as well as the maximum speed (assuming a certain minimum distance) of a variable speed limit area. Concerning a traffic sign detector, the worst case minimum distance that a car needs in order to comply with a speed limit is most interesting. This worst case minimum distance, at which a traffic sign detector must be able to identify a speed limit sign at the latest, is given through (13).

$$xsl - x_c \geq \frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right) \quad (13)$$

For instance, with a current velocity of 60 km/h, typical values for maximum acceleration (4 m/s^2) and maximum braking power (9 m/s^2), and assuming a speed limit sign that shows 50 km/h, computation time of 50 ms and another 50 ms for communication and reaction, the distance at which the traffic sign detector must start at the latest is about 8 m from the traffic sign. When applying a comfortable braking power of only 2 m/s^2 [28], the distance grows to over 26 m. Taking a look at the camera and resolution used by Deguchi et al. [17], a speed limit sign of 0.5 m width in a distance of 26 m would be represented in the resulting image with a width of 12 pixels[3], which is below the 15–45 pixels image width used in their evaluation. This is an example where formal analysis can be used to infer design decisions of CPS.

Now that we have found safety criteria for determining the minimum distance and maximum speed of a variable speed limit, in the next section we turn our attention to finding an upper bound for the beginning of a speed limit area.

[2]`http://symbolaris.com/info/KeYmaera.html`

[3]Given a chip width (w_{chip}) and focal length (l_{focal}) of both 63 mm and 640 pixels of horizontal image width (w_{image}), using $res = w_{image}/(d \cdot w_{chip}/l_{focal})$, we get a resolution of 24 pixels/m for an object at a distance (d) of 26 m.

VI. Control for Static and Moving Incidents

Typically, variable speed limits are used to lower and homogenize speed in the area of traffic incidents [1], which can be static (i.e., at a geographically fixed position, e.g., construction sites) or moving (e.g., traffic jams, wrong-way drivers). In order to be effective, a variable speed limit therefore must be activated geographically in front of such an incident (from the viewpoint of cars approaching an incident,). If an incident is static, the upper bound for the position of a variable speed limit is at the incident's position. In the case of a moving incident, however, we must also account for the distance that the incident travels while the car approaches the variable speed limit area, which is determined by the worst-case meeting point of the car with the incident, see Fig. 1. Additionally, we define an alert area in front of the incident, which, when a car enters, has a variable speed limit. This alert area also serves the purpose of avoiding to unnecessarily alert cars that may not even reach the incident (i.e., cars outside this alert area are not yet issued a speed limit that warns about the incident). For this, the beginning of the alert area moves with the incident at a fixed distance.

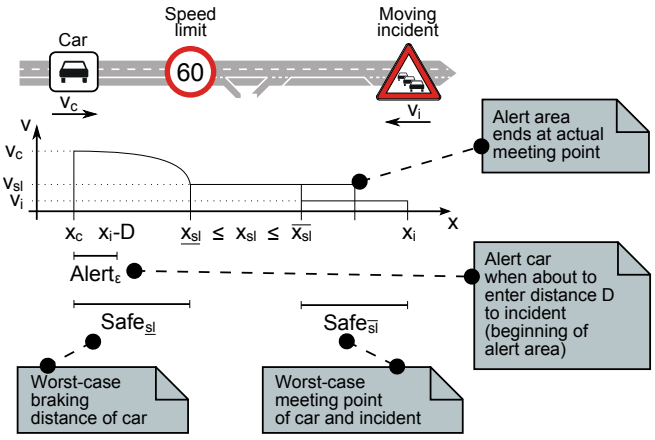

Figure 1. Speed limit control in presence of an incident moving towards a car

Modeling: In Model 2, we provide a model for variable speed limit control in the presence of an incident moving towards a car. Cars in this model follow the same control as in the previous section. They take care to comply with speed limits and potentially satisfy or optimize secondary objectives. Accordingly, the lower bound $Safe_{\underline{sl}}$ of the speed limit remains unchanged. We introduce state variables describing an incident's position (x_i) and its velocity of movement (v_i) towards cars. The system dynamics, see (27) and (28), are extended with motion of an incident. We also introduce a minimum velocity (v_{min}), which is often mandatory on freeways and highways, to exclude unreasonable car behavior from the model (e.g., avoid having a car brake to a complete stand still, wait for the incident to arrive at

Model 2 Variable speed limit control in presence of static and moving incidents (vsli)

$$vsli \equiv (ctrl; dyn)^* \tag{14}$$
$$ctrl \equiv ctrl_{car} || ctrl_{ctr}; \tag{15}$$
$$ctrl_{ctr} \equiv \text{if } (\neg Alert_\varepsilon) \text{ then} \tag{16}$$
$$(x_{sl} := x_{sl}; v_{sl} := v_{sl}) \tag{17}$$
$$\cup \big(x_{sl} := *; v_{sl} := *; ?(v_{sl} \geq 0 \wedge Safe_{\underline{sl}})\big) \tag{18}$$
$$\text{else} \tag{19}$$
$$x_{sl} := *; v_{sl} := *; \tag{20}$$
$$?(v_{sl} \geq v_{min} \wedge Safe_{\underline{sl}} \wedge Safe_{\overline{sl}}) \tag{21}$$
$$\text{fi}; \tag{22}$$
$$Alert_\varepsilon \equiv x_i - D \leq x_c + \left(\frac{v_c^2 - v_{min}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right)\right) \cdot \left(1 + \frac{v_i}{v_{min}}\right) \tag{23}$$
$$\wedge\, x_c \leq x_i \tag{24}$$
$$Safe_{\overline{sl}} \equiv (v_i = 0 \wedge x_{sl} \leq x_i) \tag{25}$$
$$\vee \left(v_i > 0 \wedge x_{sl} \leq \frac{x_i \cdot v_{min} + x_c \cdot v_i}{v_i + v_{min}}\right) \tag{26}$$
$$dyn \equiv (t := 0; x_c' = v_c, v_c' = a_c, x_i' = -v_i, t' = 1 \tag{27}$$
$$\&v_c \geq v_{min} \wedge t \leq \varepsilon) \tag{28}$$

the car's position, just to finally accelerate with maximum acceleration and rush beyond the incident).

A crucial change is in the behavior of the traffic center, cf. (16). Since we now must enact a variable speed limit at a specified latest position, the previously nondeterministic behavior is encapsulated in a deterministic decision between two options. Outside the alert area (i.e., before entering the safety distance D or after the incident), the traffic center may follow the control principle from the previous section, that is, keep existing or issue new speed limits at will, cf. (16)–(18). Otherwise, that is, when the car is about to enter the alert area defined by distance D of an incident's position x_i, the traffic center must enact a variable speed limit, and for this, it decides about the beginning and maximum speed of the variable speed limit area; see (19)–(21). Note that we nondeterministically choose any value between the lower and the upper safety bound, see (21), in order to prove safety for all possible values. In practice, however, the maximum speed limit will often be known beforehand.

The alert condition $Alert_\varepsilon$, see (23)–(24) indicates to the traffic center whether or not a car is about to enter the alert area. This area starts at distance D in front of the incident and ends at the position of the incident. To ensure that, in any case, a car within $[x_i - D, x_i]$ will have received a variable speed limit, once again we need to take into account the distance needed for braking from the current velocity v_c to v_{min} (i.e., we are allowed to choose any $v_{sl} \geq v_{min}$), and the distance that may be traveled for up to ε time units and be needed to compensate for maximum acceleration during this period. Alone, in parallel to the actions of the car, the incident also moves towards the car with its velocity v_i, which is accounted for by the additional factor $1 + v_i/v_{min}$. Since the alert area must be large enough to accommodate both the lower and upper bound of the speed limit area, this factor can be derived, as shown below in the discussion on safe bounds, from $Safe_{\underline{sl}} \leq Safe_{\overline{sl}}$.

Finally, the safety condition for the upper bound $Safe_{\overline{sl}}$ of the beginning of the speed limit area is determined by the position of an incident (in case the incident is static, cf. (25)), or by the worst-case meeting point of a car with the incident, see (26)[4].

Verification: We verify the safety of the speed limit choice as modeled above using the formal proof calculus for differential dynamic logic [25], [26]. As specified in Model 2, in this use case, a car must still be able to brake or already comply with the speed limit. Additionally, the traffic center's choices are as follows: (i) the car is outside the alert area when the car has not yet reached the alert area or it is already past the incident (denoted by $\Box$), or (ii) the car is within the alert area (denoted with $\boxdot$), in which case the beginning of the speed limit area must be in front of the static or moving incident, or the car is already inside the speed limit area. The following condition captures this requirement as an invariant that must hold at all times during the execution of the model.

$$\begin{aligned}
(c \rightarrow \boxdot\, sl) \equiv\ & v_c \geq v_{min} \wedge v_{sl} \geq v_{min} \\
& \wedge (x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \vee v_c \leq v_{sl}) \\
& \wedge \big(c \,\Box\, sl \vee c \,\boxdot\, sl\big) \\
(c \,\Box\, sl) \equiv\ & x_c + \frac{v_c^2 - v_{min}^2}{2 \cdot b} \cdot \left(1 + \frac{v_i}{v_{min}}\right) < x_i - D \\
& \vee\, x_c > x_i \\
(c \,\boxdot\, sl) \equiv\ & (v_i = 0 \wedge x_{sl} \leq x_i) \\
& \vee \left(v_i > 0 \wedge x_{sl} \leq x_i \wedge \frac{x_{sl} - x_c}{v_{min}} \leq \frac{x_i - x_{sl}}{v_i}\right) \\
& \vee\, x_c \geq x_{sl}
\end{aligned}$$

Proposition 2 extends Proposition 1 in terms of an additional safety condition that a car within the alert area must

[4]Note that the constraint (25) can be considered to be a special case of (26). This is another indication that we have identified the right constraints without unnecessary slack here. We include both to explicitly model both scenarios.

either already comply with the speed limit or (it will do so because) there is a speed limit area in front of the incident.

Proposition 2 (Safety at incident): If the car is at a safe distance from $x_i - D$ initially, then it will not exceed the speed limit past the beginning of the speed limit area while the car controller and the traffic center or traffic sign detector follow the `vsli` control model. In conjunction, when the car is within the alert area $[x_i - D, x_i]$, the speed limit area is still in front of the incident or the car must already comply with the speed limit. These conditions are expressed by the following provable formula.

$$(c \rightarrow \boxdot\, sl) \rightarrow [vsli]\Big(\big(x_c \geq x_{sl} \rightarrow v_c \leq v_{sl}\big) \wedge \big(x_c \geq x_i - D \wedge x_c \leq x_i \rightarrow (x_{sl} \leq x_i \vee v_c \leq v_{sl})\big)\Big)$$

Note, that Proposition 2 does not explicitly state that a speed limit is enacted and communicated to the car. It only covers our conditions about the actual car behavior (its speed and position in relation to speed limit areas and incidents). These conditions, however, can only be guaranteed when the traffic center in fact issues speed limits. We proved Proposition 2 using KeYmaera, and the proof files are again available online.

Safe bounds: From the viewpoint of a traffic center and an in-car driver assistance system (e.g., obstacle or pedestrian detection [29]), a combination $Safe_{\overline{sl}} \geq Safe_{\underline{sl}}$ is most interesting, since it allows us to derive a minimum distance between an incident and a car that is still safe for braking before meeting the incident. Analogously to above, we define such a safe operating distance in (29), which indicates the latest distance at which a traffic center or an in-car driver assistance system must start processing in order to warn about a (moving) incident in time so that the system can react safely in time.

$$x_i - x_c \geq \left(\frac{v_c^2 - v_{sl}^2}{2 \cdot b} + \left(\frac{A}{b} + 1\right) \cdot \left(\frac{A}{2} \cdot \varepsilon^2 + \varepsilon \cdot v_c\right)\right) \cdot \left(1 + \frac{v_i}{v_{min}}\right) \tag{29}$$

For static incidents (i.e., incidents with $v_i = 0$), (29) is equivalent to (13), which again shows that our system is a conservative extension and increases confidence that the bounds are tight. From the multiplicative factor $1 + \frac{v_i}{v_{min}}$ in (29), however, it follows that coping with fast moving traffic incidents (e.g., wrong-way drivers) is especially challenging. For example, let us assume a velocity of 30 m/s for both car and wrong-way driver. Just to turn an imminent collision into one with minimized impact at "only" the wrong-way driver's velocity, the distance needed for braking to a complete stand still with 9 m/s^2 braking power and 0.1 s reaction time is 54 m. During this braking action, the car has a mean velocity of 15 m/s, which substituted for v_{min} results in a minimum distance of 163 m. For a camera-based detection system, such a distance is already quite challenging. In order to avoid the collision, this distance allows the car 2.7 s to change lanes. With present technology, this can only be turned into a safe system when using a global warning system (e.g., in the form of a traffic center or car-to-car communication) for resolving such incidents.

The lower bound on the distance given in (29) may force the car to apply maximum braking power in order to meet the speed limit. The additional distance parameter D for computing the alert point allows a traffic center to operate the car on a more comfortable setting.

Keeping track of alerted cars: Note that our formal model and verification illustrates another interesting phenomenon. Our model is general enough to allow the control center to issue dynamic updates of speed limits at any time. The constraint we have identified under which circumstance those updates are safe is $Alert_\varepsilon$. But once $Alert_\varepsilon$ has been satisfied, it stays satisfied (recall, that cars cannot move backwards). As depicted in Fig. 2, the traffic center would therefore always be able to issue a new speed limit, with the lower bound of the speed limit area—due to the possibility that a car may not fully accelerate during the previous iteration—moving the speed limit closer and closer towards the car and so on ad infinitum. This would force the car to drive in an abnormal way. In order to avoid such Zeno effects with an annoying series of high-frequency multiple speed limit updates, a traffic center may additionally want to keep track of whether or not a particular car has already been alerted. In an actual implementation, this solution or similar solutions that ensure sufficient stability in decisions is necessary to prevent undesired Zeno-type effects.

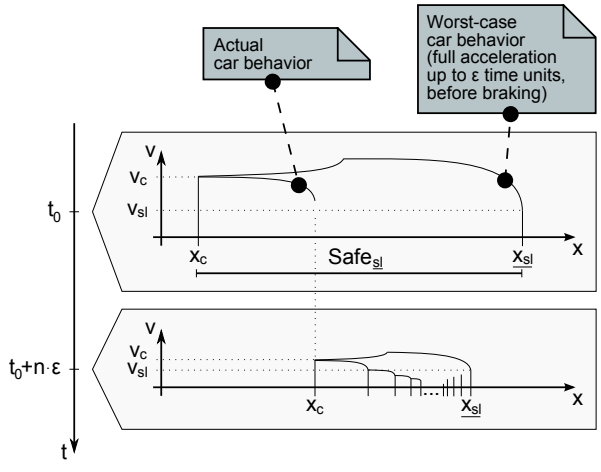

Figure 2. Repeated variable speed limits

We have introduced a corresponding $alerted$ flag in the model below, which is set to false in case the car is still

Model 3 Keeping track of alerted cars

$$
\begin{aligned}
ctrl_{ctr} \equiv\ & \text{if } (\neg Alert_{\varepsilon}) \text{ then} && (30)\\
& \quad alerted := false; && (31)\\
& \quad \textit{/* then branch from Model 2 */} && (32)\\
& \text{else if } (\neg alerted) && (33)\\
& \quad alerted := true; && (34)\\
& \quad \textit{/* else branch from Model 2 */} && (35)\\
& \text{fi fi;} && (36)
\end{aligned}
$$

outside the alert area or has already passed the incident. Within the alert area, the flag is set to true upon first notification of the car and hence, inhibits multiple concurrent speed limits.

For verification, the flag indicating the alert status of a car has to be also reflected in the invariant, as listed below.

$$
\begin{aligned}
(c \rightarrow\!\boxdot\ sl) \equiv\ & v_c \geq v_{min} \wedge v_{sl} \geq v_{min}\\
& \wedge (x_{sl} \geq x_c + \frac{v_c^2 - v_{sl}^2}{2 \cdot b} \vee v_c \leq v_{sl})\\
& \wedge \big((\neg alerted \wedge c \,\square\, sl) \vee (alerted \wedge c \boxdot sl)\big)
\end{aligned}
$$

This invariant states, that cars outside the alert area are not alerted, whereas those within the alert area are alerted. Note, that for cars outside the alert area, the traffic center may nevertheless issue arbitrarily many speed limits. A possible extension of the system could include a minimum time that needs to pass between speed limit updates, in order to not overload communication channels and force cars into abnormal behavior by issuing speed limits too often. Of course, this modified traffic center behavior should not influence safety on the road, and, hence, the safety condition of Proposition 2 remains unchanged. Again, we proved Proposition 2 with the altered invariant using KeYmaera.

VII. Conclusion and Future Work

Traffic centers focus on the global functioning of a freeway or highway network and, for this, impose dynamic constraints (e.g., variable speed limits) on the control choices of car controllers. At the same time, sensor and driver assistance systems make cars increasingly aware of their environment, and enable them to react autonomously (e.g., adaptive cruise control, or obstacle detection that initiates emergency braking). It is a promising idea to combine global traffic control choices—which could be communicated directly from a traffic center to a car, or sensed by driver assistance systems—and car control into a fully autonomous system. Yet, such a combination is only economically feasible without costly post-deploy upgrades or even possible hazards when its safety can be ensured.

In this paper, we presented a distributed intelligent speed adaptation system comprising a car controller and a speed limit controller (e.g., a traffic center or a driver assistance system) with direct communication in-between. We presented formal verification results that guarantee safe operation of cars (i.e., cars always comply with speed limits), even in the presence of incidents moving towards cars that restrict the position of a speed limit area. In the process of verification, we found important invariants, which are needed to ensure such safe operation if implemented in actual physical controllers. These invariants comprise bounds on the distance between cars and speed limit areas. They can be further transformed into precise requirements and help decide trade-offs even for design parameters of traffic centers and driver assistance systems that are not modeled formally (e.g., image resolution, focal length, and computation time of driver assistance systems).

Future work includes addressing arbitrarily many incidents, and homogenizing speed with consecutively arranged speed limits of decreasing maximum speed. Also, the models discussed in this paper will be further refined by introducing explicit communication channels, which allows multiple control decisions during one communication roundtrip.

Acknowledgments

This work has been partly funded by Marshall-Plan Foundation. This material is based upon work supported by the National Science Foundation under NSF CAREER Award CNS-1054246 and NSF EXPEDITION CNS-0926181 as well as Grant Nos. CNS-1035800, and CNS-0931985.

References

[1] P. Allaby, B. Hellinga, and M. Bullock, "Variable speed limits: Safety and operational impacts of a candidate control strategy for freeway applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 8, no. 4, pp. 671 – 680, 2007.

[2] F. Lu and X. Chen, "Analyzing the speed dispersion influence on traffic safety," in *International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, vol. 3. IEEE, 2009, pp. 482 –485.

[3] E. van den Hoogen and S. Smulders, "Control by variable speed signs: results of the dutch experiment," in *7th International Conference on Road Traffic Monitoring and Control*. IEEE, 1994, pp. 145–149.

[4] R. Bertini, S. Boice, and K. Bogenberger, "Using ITS data fusion to examine traffic dynamics on a freeway with variable speed limits," in *Proceedings of Intelligent Transportation Systems*. IEEE, 2005, pp. 1006–1011.

[5] R. L. Bertini, S. Boice, and K. Bogenberger, "Dynamics of variable speed limit system surrounding bottleneck on german autobahn," *Transportation Research Record: Journal of the Transportation Research Board*, no. 1978, pp. 149–159, 2006.

[6] S. M. Loos, A. Platzer, and L. Nistor, "Adaptive cruise control: Hybrid, distributed, and now formally verified," in *17th International Symposium on Formal Methods (FM)*, ser. LNCS, M. Butler and W. Schulte, Eds., vol. 6664. Springer, 2011, pp. 42–56.

[7] M. Paine, D. Paine, M. Griffiths, and G. Germanos, "In-vehicle intelligent speed advisory systems," in *Proceedings of the 20th International Conference on the Enhanced Safety of Vehicles*, 2007.

[8] X.-Y. Lu, P. Varaiya, R. Horowitz, D. Su, and S. Shladover, "A new approach for combined freeway variable speed limits and coordinated ramp metering," in *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on*. IEEE, 2010, pp. 491 –498.

[9] H. Dia, W. Gondwe, and S. Panwai, "Traffic impact assessment of incident management strategies," in *Intelligent Transportation Systems, 2008. ITSC 2008. 11th International IEEE Conference on*, 2008, pp. 441–446.

[10] N. Agerholm, R. Waagepetersen, N. Tradisauskas, and H. Lahrmann, "Intelligent speed adaptation in company vehicles," in *Proceedings of the IEEE Intelligent Vehicles Symposium*. IEEE, 2008, pp. 936 –943.

[11] R. Gallen, N. Hautiere, and S. Glaser, "Advisory speed for intelligent speed adaptation in adverse conditions," in *Intelligent Vehicles Symposium (IV), 2010 IEEE*, 2010, pp. 107 –114.

[12] M. Paine, D. Paine, and I. J. Faulks, "Speed limiting trials in Australia," in *Proceedings of the 21st International Technical Conference on the Enhanced Safety of Vehicles*, 2009. [Online]. Available: http://www-nrd.nhtsa.dot.gov/departments/esv/21st/

[13] S. Shladover, "PATH at 20—history and major milestones," *Transactions on Intelligent Transportation Systems*, vol. 8, no. 4, pp. 584–592, 2007.

[14] J. Misener and S. Shladover, "Path investigations in vehicle-roadside cooperation and safety: A foundation for safety and vehicle-infrastructure integration research," in *Proceedings of the Intelligent Transportation Systems Conference (ITSC)*. IEEE, 2006, pp. 9–16.

[15] P. Ioannou, Y. Wang, and H. Chang, "Integrated roadway/adaptive cruise control system: Safety, performance, environmental and near term deployment considerations," California PATH program, Institute of transportation studies, University of California, Berkeley, Tech. Rep. UCB-ITS-PRR-2007-08, 2007.

[16] L. Baskar, B. De Schutter, and H. Hellendoorn, "Dynamic speed limits and on-ramp metering for ivhs using model predictive control," in *Proceedings of the 11th International IEEE Conference on Intelligent Transportation Systems (ITSC)*. IEEE, 2008, pp. 821–826.

[17] D. Deguchi, M. Shirasuna, K. Doman, I. Ide, and H. Murase, "Intelligent traffic sign detector: Adaptive learning based on online gathering of training samples," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, 2011, pp. 72 –77.

[18] A. Broggi, P. Cerri, S. Ghidoni, P. Grisleri, and H. G. Jung, "A new approach to urban pedestrian detection for automatic braking," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 10, no. 4, pp. 594 –605, dec. 2009.

[19] A. Haselhoff and A. Kummert, "On visual crosswalk detection for driver assistance systems," in *Intelligent Vehicles Symposium (IV), 2010 IEEE*, 2010, pp. 883 –888.

[20] R. Kastner, T. Michalke, T. Burbach, J. Fritsch, and C. Goerick, "Attention-based traffic sign recognition with an array of weak classifiers," in *Proceedings of the 2010 Intelligent Vehicles Symposium (IV)*. IEEE, 2010, pp. 333 –339.

[21] L. Oliveira and U. Nunes, "Context-aware pedestrian detection using lidar," in *Intelligent Vehicles Symposium (IV), 2010 IEEE*, 2010, pp. 773 –778.

[22] J. Levinson, J. Askeland, J. Becker, J. Dolson, D. Held, S. Kammel, J. Kolter, D. Langer, O. Pink, V. Pratt, M. Sokolsky, G. Stanek, D. Stavens, A. Teichman, M. Werling, and S. Thrun, "Towards fully autonomous driving: Systems and algorithms," in *Intelligent Vehicles Symposium (IV), 2011 IEEE*, 2011, pp. 163 –168.

[23] A. Platzer and J.-D. Quesel, "European Train Control System: A case study in formal verification," in *ICFEM*, ser. LNCS, K. Breitman and A. Cavalcanti, Eds., vol. 5885. Springer, 2009, pp. 246–265.

[24] M. Althoff, O. Stursberg, and M. Buss, "Safety assessment of autonomous cars using verification techniques," in *Proceedings of the American Control Conference (ACC)*, 2007, pp. 4154–4159.

[25] A. Platzer, "Differential dynamic logic for hybrid systems." *J. Autom. Reas.*, vol. 41, no. 2, pp. 143–189, 2008.

[26] ——, *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Heidelberg: Springer, 2010.

[27] M. R. Flynn, A. R. Kasimov, J.-C. Nave, R. R. Rosales, and B. Seibold, "Self-sustained nonlinear waves in traffic flow," *Physical Review E*, vol. 79, p. 056113, May 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevE.79.056113

[28] G. Anagnostopoulos, M. Coltman, and R. Suever, "Compendium of executive summaries from the maglev system concept definition final reports," U.S. Department of Transportation, Tech. Rep. DOT/FRA/NMI-93/02, 1993.

[29] C. Wakim, S. Capperon, and J. Oksman, "Design of pedestrian detection systems for the prediction of car-to-pedestrian accidents," in *Proceedings of the 7th International IEEE Conference on Intelligent Transportation Systems*. IEEE, 2004, pp. 696–701.