Provably-Correct and Comfortable Adaptive Cruise Control

Matthias Althoff, Sebastian Maierhofer, and Christian Pek

***Abstract*—Adaptive cruise control is one of the most common comfort features of road vehicles. Despite its large market penetration, current systems are not safe in all driving conditions and require supervision by human drivers. While several previous works have proposed solutions for safe adaptive cruise control, none of these works considers comfort, especially in the event of cut-ins. We provide a novel solution that simultaneously meets our specifications and provides comfort in all driving conditions, including cut-ins. This is achieved by an exchangeable nominal controller ensuring comfort, combined with a provably correct fail-safe controller that gradually engages an emergency maneuver—this ensures comfort, since most threats are already cleared before emergency braking is fully activated. As a consequence, one can easily exchange the nominal controller without having to have the overall system safety re-certified. We also provide the first user study into a provably-correct adaptive cruise controller. It shows that even though our approach never causes an accident, passengers rate the performance as good as a state-of-the-art solution that does not ensure safety.**

***Index Terms*—Adaptive cruise control, formal verification, fail-safe control, cut-ins, and user study.**

I. Introduction

FOLLOWING other vehicles is one of the most frequently-performed tasks in road traffic situations. To relieve drivers from what is often perceived as a tedious task, many vehicles are equipped with adaptive cruise control. Current systems require drivers to take over in dangerous situations, since a rigorous solution is expensive to develop and have certified. However, 14.6 % of accidents were rear-end collisions in Germany in 2007 [1, Table 1], which could be avoided through the use of provably-safe adaptive cruise control. In a recent study, we showed that many non-formal techniques claiming to provide safe solutions are in fact not safe, while only formal methods could not be falsified [2].

Manuscript received December 20, 2019; revised March 23, 2020; accepted April 1, 2020. Date of publication May 12, 2020; date of current version February 24, 2021. This work was supported in part by the German Research Foundation (DFG) under Grant AL 1185/7-1, in part by the project justITSELF funded by the European Research Council (ERC) under Grant 817629, and in part by the project interACT within the EU Horizon 2020 program under Grant 723395. We would also like to thank the BMW Group for allowing us to test our algorithms in their simulator. *(Corresponding author: Matthias Althoff.)*

The authors are with the Department of Computer Science, Technical University of Munich, 85748 Garching, Germany (e-mail: althoff@tum.de.; sebastian.maierhofer@tum.de; christian.pek@tum.de).

This article has supplementary downloadable material available at https://ieeexplore.ieee.org, provided by the authors.

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIV.2020.2991953

Provably-correct adaptive cruise control is not only beneficial as a driver-assistance system, but also a major building block for automated vehicles. Since following other vehicles requires a tight perception-action loop, a bespoke solution is often designed to circumvent complicated motion planning algorithms [3], [4]. Safe adaptive cruise control would not invite other drivers to cut in [5], despite the common misconception to the contrary. Furthermore, if a provably-safe adaptive cruise controller can be activated, an automated vehicle is in an invariably safe state, which ensures safety beyond finite planning horizons [6].

Research on adaptive cruise control already started back in the 1960s [7]. Below, we review the state of the art in adaptive cruise control in the following categories: influence on traffic flow, control concepts, full-range adaptive cruise control, and formal methods. To limit our literature survey, we intentionally exclude improved fuel economy [8], improved performance through cooperative adaptive cruise control [9], vehicle platooning [10], and string stability [11].

a) Influence on Traffic Flow: Several studies have shown that adaptive cruise control has a positive effect on traffic flow since its control actions are typically smoother than those of human drivers, see e.g., [12], [13]. The positive effect is dominated by the spacing policy, which determines the reference value for the adaptive cruise controller [14]. Two different policies are compared in [15]—constant spacing and constant headway; constant spacing can provide better throughput, but requires communication between vehicles, while only constant headway ensures string stability if no communication is used. An improved nonlinear spacing policy is manually derived in [16]. A similar work uses optimization procedures with traffic flow and stability constraints to obtain a nonlinear spacing policy [17]. Well-designed spacing policies can even eliminate traffic congestion in simulation studies if only 25% of the vehicles engage adaptive cruise control [18]. Also, the high market penetration of cooperative adaptive cruise control (which receives information from the vehicle in front) improves traffic flow even further [19]. Additional improvements can be expected when vehicles inform other vehicles about lane-change intentions ahead of time [20].

b) Control Concepts: Next, we review methods to realize the aforementioned spacing policies. It has been shown, through simulations and real experiments, that even a standard PID controller achieves satisfactory performance when no safety guarantees are required [21]. A more advanced adaptive control algorithm in [22] also ensures string stability. Model predictive control further improves control performance, despite constraints originating from actuators, comfort requirements, fuel

consumption, and string stability. Most approaches use a hierarchical concept, where the model predictive controller provides the high-level commands (typically acceleration), while low-level commands are effected via classical feedback loops [23]. To achieve real-time capability of model predictive control, explicit model predictive control was investigated in [24] and a scale reduction framework applied in [25]. Several works have also explicitly considered cut-in vehicles [26], [27]. However, the aforementioned methods are not rigorously safe, in the sense that they may exclude accidents for the entire velocity range of the automated vehicle, since bounds on control errors are not proven regardless of sensor noise, disturbances, and the behavior of surrounding vehicles [28], [29].

c) Full-Range Adaptive Cruise Control: Most available adaptive cruise control systems do not provide sufficient braking in emergency situations and/or cannot be engaged in stop-and-go traffic. This shortcoming is addressed by full-range adaptive cruise control operating across the entire velocity range. In [24], [30], model predictive control is used to achieve adaptive cruise controllers with a full range. A fuzzy-control concept is presented in [31]; due to the lack of ordinary differential equations describing the closed-loop dynamics of such controllers, they are not suitable for proving collision avoidance. This also applies to approaches achieving full-range adaptive cruise control through training neural networks [32]. A hybrid control method is achieved in [33] with the control modes *comfort mode*, *large deceleration mode*, and *severe braking mode*. Another hybrid approach switches between adaptive cruise control and collision avoidance, such that jerky maneuvers are avoided [34].

d) Formal Methods: In contrast to all previous methods, formal methods provide a mathematical proof that designed systems rigorously meet formal specifications, despite any uncertainty originating from various sources, such as sensor noise, disturbances, and modeling errors [35], [36]. Formal methods have not only been applied to adaptive cruise control, but also to intelligent intersections [37]–[39], ground vehicles in unstructured environments [40], [41], cooperative driving [42], [43], and automated vehicles [44].

One of the first works to provide a provably-safe adaptive cruise controller, uses handwritten proofs [45]. This work was later extended by game-theoretic techniques to better deal with cooperative controlled vehicles [46]. Handwritten proofs are also provided in [47], [48] to ensure the safety of vehicle platoons. To avoid mistakes in handwritten proofs, a theorem prover is used in [49], [50]; this, however, requires all vehicles to be automated.

Another method for avoiding mistakes in handwritten proofs is to use reachability analysis, which computes the set of reachable states. If no reachable state of the adaptive cruise controller is unsafe, the correct behavior is ensured given the assumptions on the modeled behavior of the own vehicle and other vehicles [10], [51]. To avoid computing the reachable set of the entire state space, a counterexample-guided verification procedure is presented for a cruise control system in [52]. A special case of reachable sets are invariant sets, in which a system stays indefinitely. If the invariant set of the adaptive cruise controller does not contain any unsafe states, correctness can be argued as for reachable sets [53]–[55], where [56] can also be applied to path-following.

Barrier certificates are another concept to prove that one cannot transition from a safe set of states to an unsafe one; an extension of barrier certificates by control Lyapunov functions is presented in [57] for adaptive cruise control, and has been experimentally validated [58]. The work of [57] has been extended in [59] to the case where the velocity of the leading vehicle is variable and compared to a controller synthesized by the tool PESSOA [60]. This work is further extended in [61] by adding provably-correct lane-keeping.

Another line of research safeguards exchangeable nominal controllers, by embedding them in an emergency controller that only engages if the nominal controller would perform an unsafe action [62]. However, switching between controllers can result in discomfort for the passengers, so we developed a safe and smooth switching strategy in our previous work [63]. This work was later also applied to vehicle platooning [64].

e) Summary: While formal methods ensure provably-safe adaptive cruise controllers, they are not tuned for comfort. Especially when vehicles cut in, their behavior is either extreme in the sense that full braking is applied or their behavior is unspecified for that use case. Cut-ins are particularly challenging since the automated vehicle is temporarily in an unsafe situation. No previous publication even specifies the desired behavior in the event of a cut-in—this would be the minimum requirement for a provably-correct solution. There also exists no user study of adaptive cruise controllers designed using formal methods measuring comfort and perceived safety.

f) Contributions: We present a provably-correct, full-range adaptive cruise controller. Our approach is based on the emergency controller concept of our previous work [63]. In contrast to previous work, our work is the only one that simultaneously achieves the following properties:

- We specify and ensure the intended behavior in the event of a cut-in.
- Our approach considers measurement uncertainties, disturbances, and model uncertainties.
- We automatically identify safety-relevant vehicles to ensure the soundness of our approach.
- Our approach has limited hardware-requirements compared to correct-by-construction methods, which often require multiple gigabytes of memory [65, Table 1].
- The nominal controller of our approach can be replaced without having to have the system re-certified. Thus, methods from machine learning can be easily integrated in our approach, in contrast to most reviewed formal approaches.
- The jerk profile in emergency situations can be fully specified to ensure comfort without jeopardizing safety.
- We have conducted the only user study on a provably-correct adaptive cruise controller.

g) Organization: After presenting the required preliminaries in Section II, we introduce our system specification and our solution concept in Section III. Our safety controller for the case without cut-ins is presented in Section IV, and with cut-ins in Section V; both controllers are evaluated in Section VI. We draw final conclusions in Section VII.

II. PRELIMINARIES

Longitudinal vehicle control typically consists of two control loops: an inner control loop compensating the nonlinear vehicle dynamics, and an outer control loop commanding the desired acceleration. In this work, we will focus on the outer loop—this does not impede the verifiability of the results since established methods exist to verify the inner control loop as, e.g., demonstrated in [66]. The errors from the inner control loop can be added to our proposed approach as an additional model uncertainty (see Section IV-C2). We also assume that we receive the positions and velocities of all surrounding vehicles from the perception module of the vehicle, including measurement uncertainties.

The lane of the controlled vehicle—referred to as the *ego vehicle* from now on—is referred to as the *ego lane*, and we denote the set of points of that lane as $\mathcal{L}_{ego}$. We use V_i, $i \in \{1, 2, \dots, N\}$ to denote vehicles partially occupying the ego lane and preceding the ego vehicle, where a larger index means that the vehicle is further ahead. All variables associated to a preceding vehicle are denoted by the subscript $\square_p$.

We consider scenarios where the ego vehicle drives on multi-lane roads with motorized traffic driving in the same direction and where the lateral dynamics can be neglected; it thus suffices to use the distance s along the considered lane in the driving direction. The state of a vehicle is denoted by $x \in \mathbb{R}^n$ and its initial state by $x_0 \in \mathbb{R}^n$. In this work, the state of the ego vehicle $x = [s \quad v \quad a]^T$ consists of position s, velocity v, and acceleration a; the state of preceding vehicles only consists of position and velocity: $x_p = [s \quad v]^T$. We also introduce the relative position $\Delta s = s_p - s$ and the relative velocity $\Delta v = v_p - v$. For a given initial state, an input trajectory $u(\cdot)$, and a disturbance trajectory $w(\cdot)$, we introduce the solution of the model $\dot{x} = f(x, u, w)$ of the ego vehicle over time t as $\xi(t; x_0, u(\cdot), w(\cdot))$. Since disturbances are later considered in Section IV-C2, we simply write $\xi(t; x_0, u(\cdot))$ for ease of notation. The time at which a safe state is reached for $u(\cdot)$, given the system dynamics and x_0, is denoted by $t_s(u(\cdot))$; we consider a state to be safe when one can stay in it indefinitely without causing a collision [6]. We also require the set of possible input trajectories $\tilde{\mathcal{U}}$ that reach a safe state for a given set of possible inputs $\mathcal{U}$: $\tilde{\mathcal{U}} = \{u(\cdot) | \forall t : u(t) \in \mathcal{U}, \exists t_s(u(\cdot)) \in [0, \infty[\}$. We denote a braking input by $u_{brake}(\cdot)$.

The occupancy of a vehicle for a given state x is denoted by $\mathcal{O}(x(t))$ and the time-varying occupancy of all surrounding traffic participants as $\mathcal{O}_{tp}(t)$. The operator $\mathrm{proj}()$ projects a state to a position s. Please note that the position of the preceding vehicle $s_p = \mathrm{proj}(x_p)$ is measured from the rear bumper, while the position of the ego vehicle $s = \mathrm{proj}(x)$ is measured from the front bumper; this makes it possible to demand that $s_p - s > 0$ for collision avoidance, without having to specify the vehicle dimensions.

Definition II.1 (Safe distance): The distance $d_{safe}(x, v_p)$ is the minimum distance the ego vehicle has to keep to a preceding vehicle to be able to stop without a collision occurring if the preceding vehicle fully brakes:

$$\begin{aligned} d_{safe}(x, v_p) = \min\{d | \forall t \in [0, t_s(u_{brake}(\cdot))] : \\ \mathrm{proj}(\xi_p(t; [d + \mathrm{proj}(x), \, v_p]^T, u_{p,brake}(\cdot))) \\ - \, \mathrm{proj}(\xi(t; x, u_{brake}(\cdot))) > 0\}. \end{aligned}$$

The braking trajectory $u_{brake}(\cdot)$ of the ego vehicle is user-defined (see Section IV), while $u_{p,brake}(\cdot)$ represents immediate full braking.

Definition II.2 (Inevitable collision state [40, eq. 3]): The ego vehicle is in an inevitable collision state if a collision with an obstacle is inevitable regardless of the control action of the ego vehicle. The set of inevitable collision states is

$$\begin{aligned} \mathcal{ICS} = \{x | \forall u(\cdot) \in \tilde{\mathcal{U}} \;\; \exists t \in [0, t_s(u(\cdot))] : \\ \mathcal{O}(\xi(t; x, u(\cdot))) \cap \mathcal{O}_{tp}(t) \neq \emptyset\}. \end{aligned}$$

Definition II.3 (Cut-in): A *cut-in* occurs when another vehicle enters the ego lane without respecting the safe distance to the ego vehicle. The following predicate is true in the event of the cut-in:

$$\begin{aligned} &\mathtt{cut-in}(x(t), x_p(t)) \Leftrightarrow \mathcal{O}(x_p(t)) \cap \mathcal{L}_{ego} \neq \emptyset \wedge \\ &\lim_{\delta \to 0} \mathcal{O}(x_p(t - \delta)) \cap \mathcal{L}_{ego} = \emptyset \wedge \\ &\mathrm{proj}(x_p(t) - \mathrm{proj}\, x(t)) \leq d_{safe}(x(t), v_p(t)). \end{aligned}$$

Definition II.4 (Clearing time): The time $t_c(x(t), x_p(t))$ defines how much time remains for the ego-vehicle to establish a safe distance after a cut-in. This time is user-defined and depends on the ego vehicle state and the state of the cut-in vehicle at the time of the cut-in. For a concise notation, the dependency of $x(t)$ and $x_p(t)$ is often omitted and we simply write t_c.

A. Ego Vehicle Model

As previously mentioned, we assume that we can command acceleration to low-level controllers that effect the commanded acceleration with some margin of error. Our model considers maximum tire forces, limited engine power, aerodynamic drag, and forces acting on the vehicle due to an incline. Minor effects, such as roll resistance of tires are considered by ensuring conformance as described in Section IV-C2.

In order to ensure comfortable motions, we use jerk j as the input to our vehicle model [67], [68]. Furthermore, we require several vehicle parameters: mass m, drag coefficient c_d, the frontal area A, and the velocity v_S above which the engine power is not great enough to cause wheel slip. We also require the air density ρ, the road incline angle α, the gravity constant g, and the headwind velocity v_{wind}. We denote by $\underline{\square}$ the minimum possible value and by $\overline{\square}$ the maximum possible value of a variable. Due to speed limits for forward and backwards driving, we obtain the constraint

$$v \in [\underline{v}, \overline{v}].$$

One can obviously restrict backwards driving by setting $\underline{v} = 0$. Acceleration a_{pow} due to engine power and braking power is constrained by [69, Section III-B], where

$$a_{pow} \in [\underline{a}, \overline{a}(v)], \quad \overline{a}(v) = \begin{cases} a_{\max} \frac{v_S}{v} & \text{for } v > v_S, \\ a_{\max} & \text{otherwise.} \end{cases}$$

The negative acceleration caused by drag is $a_{dr} = -\frac{1}{2m}\rho c_d A (v + v_{wind})^2$ and that due to an incline is $a_i = -g\sin(\alpha)$ [70, Ch. 4]. To ensure that a vehicle does not accelerate beyond $\overline{v}$ and decelerate beyond $\underline{v}$, we introduce the condition C for zero acceleration:

$$C \equiv (v \leq \underline{v} \wedge a \leq 0) \vee (v \geq \overline{v} \wedge a \geq 0).$$

Based on the previous formulas, we can now present the vehicle dynamics $\dot{x} = f(x, u, w)$ for the state $x = [s \quad v \quad a]$, the input $u = j$, and the disturbance $w = [\alpha, v_{wind}]$:

$$\dot{x}_1 = x_2$$

$$\dot{x}_2 = \begin{cases} 0 & \text{for } C, \\ \underline{a} + a_{dr} + a_i & \text{for } \neg C \wedge x_3 \leq \underline{a} + a_{dr} + a_i, \\ \overline{a}(v) + a_{dr} + a_i & \text{for } \neg C \wedge x_3 \geq \overline{a}(v) + a_{dr} + a_i, \\ x_3 & \text{otherwise.} \end{cases}$$

$$\dot{x}_3 = u. \tag{1}$$

Please note that while the ego vehicle input is jerk to ensure comfort, the input of preceding vehicles u_p refers to their acceleration. Also, we forward the acceleration x_2 as the input to the underlying acceleration controller of the ego vehicle.

B. Nominal Controller

While our concept safeguards any nominal controller—even neural networks—we chose model predictive control, as it already takes into consideration the constraints based on the assumed behavior of preceding vehicles. If the assumption as to the behavior is incorrect, our emergency controller takes over and ensures collision avoidance.

Our model predictive controller assumes constant velocity for preceding vehicles beginning from the time t_0 of the last measurement update: $s_p(t + t_0) = v_p(t_0)\, t + s_p(t_0)$. Since the nominal controller does not ensure safety requirements, we use a simple point-mass model for the model predictive controller, in order to save computational resources. The point mass model for the state of the nominal controller $x_n = [\Delta s \quad \Delta v \quad a]$ and the input $u = j$ is

$$\dot{x}_n = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{bmatrix} x_n + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u.$$

Our model predictive controller optimizes the inputs for discrete, equidistant points in time $t_k = k\,\Delta t$, where $k \in \mathbb{N}$ is the time step and $\Delta t \in \mathbb{R}^+$ is the time increment. For a concise notation, we define $\tilde{x}_n(t_k) = x_n(t_k) - [d_{safe}(t_k), 0, 0]^T$ and $\tilde{x}_{n,k} := \tilde{x}_n(t_k)$, which is also used for other variables, e.g., u_k. Please note that the computation of d_{safe} as defined in Def. II.1 is detailed later in Prop. IV.5. Using the weighting matrix Q for state errors and the weight r for input efforts, we choose the cost function for the time horizon h to be a standard quadratic function:

$$u_{opt}(\cdot) = \operatorname{argmin}_{u(\cdot)} \sum_{k=1}^{h} \tilde{x}_{n,k}^T Q \tilde{x}_{n,k} + r\, u_k^2 \tag{2}$$

subject to the constraints $\forall t \in [0, t_h]$

$$d_{safe}(x_0, v_{p,0}) \leq x_{n,1}(t) \text{ (safety)} \tag{3}$$

$$\underline{v} \leq v_p(t) - x_{n,2}(t) \leq \overline{v} \text{ (velocity limits)} \tag{4}$$

$$\underline{a} \leq x_{n,3}(t) \leq \overline{a}(v) \text{ (acceleration limits)} \tag{5}$$

$$\underline{j} \leq u(t) \leq \overline{j} \text{ (comfort)} \tag{6}$$

where the computation of constraint (3) is detailed in Prop. IV.5. Also, the time is reset to zero for each new optimization, and we do not recompute $d_{safe}(x_0, v_{p,0})$ for different times, for the sake of computational efficiency—safety is later ensured by the emergency controller. The quadratic cost function subject to linear dynamics and constraints forms a quadratic programming problem. For each time step, the model predictive controller solves the quadratic program and only performs the first part of the optimal input trajectory in each time step. To save computation time, we follow the batch approach in [71, Ch. 8.2].

When several automated vehicles should follow each other, one also requires string stability [72]. While this is not the focus of this work, we briefly introduce a possible additional constraint for string stability [73, eq. 26]:

$$\forall k \in \{0, \ldots, h\}: \quad x_{3,k} \leq \gamma \max_{\tilde{k} \in \{-\tilde{h}, \ldots, 0\}} |a_{p,\tilde{k}}|,$$

where $\gamma \in]0, 1[$ and $\tilde{h}$ can be chosen by the user such that it is large enough to account for delays arising in the vehicle stream. Negative time steps refer to values before the current measurement.

C. Lane-Change Prediction

Our nominal controller uses lane-change prediction to further increase comfort by adjusting the velocity in a foresighted manner. Any lane-change prediction method can be used, e.g., those described in [74]–[76]. To focus on the novel aspects of this paper, we have used a simple lane-change prediction method which demonstrated a good level of performance in our experiments. Let us introduce some variables with respect to the current lane of a preceding vehicle: the lateral deviation from the lane center s_{lat}, the orientation deviation from the lane center θ, the user-defined thresholds s_c and θ_c, and the time horizon λ. We predict a cut-in if

$$\forall t \in [t_0 - \lambda, t_0]: |s_{lat}(t)| > s_c \wedge |\theta(t)| > \theta_c.$$

As soon as the above formula is true, we assume that the vehicle is already in the ego lane, so that the nominal controller can adjust the velocity, even though the vehicle has not yet completed the lane change. We use the same cut-in prediction not only for the nominal controller, but also for the emergency

controllers presented later. In the following section, we provide the specifications and build a safety layer around the nominal system to ensure that the specifications are always met.

III. System Specification and Solution Concept

As already discussed in the introduction, there is no holistic concept that guarantees safety across the entire velocity range whilst ensuring comfort and working as specified in the event of cut-ins. We formalize these specifications and later present our solution concept.

A. System Specification

Based on the previously introduced variables and definitions, we list—using first-order logic—the specifications that our approach provably ensures. Specifying the behavior of adaptive cruise controllers is part of a larger effort to formalize traffic rules, so that the intended behavior of automated vehicles can be formally specified [77].

Specification III.1 (Clearing time for cut-ins): When a vehicle cuts in (see Def. II.3) and the ego vehicle is not in an inevitable collision state, the ego vehicle has to establish a safe distance within a user-specified clearing time $t_c(x(t), x_p(t))$ (see Def. II.4) under the assumption that the cut-in vehicle does not brake more sharply than $\underline{a}_{cut-in}$:

$$\forall t : x(t) \notin \mathcal{ICS} \wedge \texttt{cut} - \texttt{in}(x(t), x_p(t)) \wedge$$
$$\forall \tilde{t} \in [t, t + t_c] : u_p(\tilde{t}) \geq \underline{a}_{cut-in} \Longrightarrow \text{proj}(x_p(t + t_c))$$
$$- \text{proj}(x(t + t_c)) \geq d_{safe}(x(t + t_c)), v_p(t + t_c)).$$

This specification is ensured by Prop. V.1.

We additionally try to obtain a comfortable acceleration through obtaining $u_{opt}(\cdot)$ from (2), but this is not a formal constraint. To ensure that $t_c(x(t), x_p(t))$ is feasible with respect to Spec. III.1, one can compute offline for uniformly sampled combinations of the state variables whether $t_c(x(t), x_p(t))$ is feasible. If a sample is infeasible, we conservatively also declare the region of states infeasible that is spanned by neighboring samples whose relative distance is larger and whose relative velocity is smaller.

Please note that in a very small number of cases, t_c cannot be met when the cutting-in vehicle decelerates more sharply than $\underline{a}_{cut-in}$. We denote the earliest possible time that safety is re-established as $\tilde{t}_c \geq t_c$.

Specification III.2 (No collision caused by ego vehicle): We only require that the ego vehicle respects the safe distance $d_{safe}(x(t), v_p(t))$ (see Def. II.1) if no vehicle cuts in. Let us denote the j^{th} time interval in which the ego vehicle is potentially unsafe due to a cut-in as

$$\tau_j = [t_{cut,j}, t_{cut,j} + \tilde{t}_c],$$
$$\texttt{cut} - \texttt{in}(x(t_{cut,j}), x_p(t_{cut,j})) = \texttt{true}.$$

We further introduce the union of all potentially unsafe times $\tau_\cup = \bigcup_j \tau_j$ so that we can formulate the specification

$$\forall t \in \mathbb{R} \setminus \tau_\cup : \text{proj}(x_p(t)) - \text{proj}(x(t)) \geq d_{safe}(x(t), v_p(t)).$$

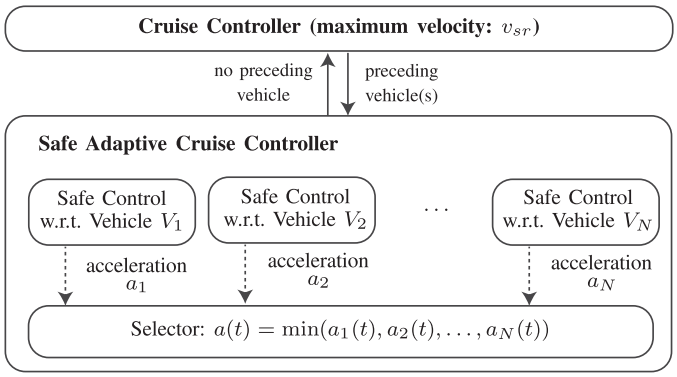


Fig. 1. Overall solution concept.

This specification is ensured by Prop. IV.5.

Specification III.3 (Full braking in ICS): When the state of the ego vehicle is within the set of inevitable collision states $\mathcal{ICS}$ (see Def. II.2), the ego vehicle fully brakes to mitigate the potential collision impact:

$$\forall t : x(t) \in \mathcal{ICS} \Longrightarrow a(t) = \underline{a}.$$

This specification is ensured by the inevitable-collision-state controller in Section V-B.

Specification III.4 (Stopping within the sensor range): The ego vehicle must stay below a velocity v_{sr} to be able to stop within the sensor range:

$$\forall t : v(t) \leq v_{sr}.$$

This specification is ensured by Prop. IV.3.

Specification III.5 (Minimum deceleration): All specifications must be met even if preceding vehicles can brake more sharply than the ego vehicle: $\underline{a}_p \leq \underline{a}$. The value of $\underline{a}_p$ must be chosen based on the best commercially available tire compound. This specification is ensured by considering it as an assumption in all subsequent propositions.

Since the relative performance of tires is rather uniform, choosing the best tire compound is not very conservative [78, Table 4], [79, Fig. 3.2].

B. Solution Concept

Our solution concept is driven by ensuring all formal system specifications, while still realizing all soft constraints, such as comfort. An overview of our solution concept is shown in Fig. 1. When there is no preceding vehicle within the sensor range, we engage a standard cruise controller [12]. The only constraint is that the user cannot set a velocity beyond the safe velocity v_{sr}, to ensure that the vehicle can stop within its sensor range (see Prop. IV.3). Otherwise, the ego vehicle first selects all relevant surrounding vehicles (see Section III-C) and computes a safe acceleration value with respect to (w.r.t.) each one of them (see Section IV). The individual accelerations a_i are collected in the selector, and the smallest acceleration value $a(t) = \min(a_1(t), a_2(t), \ldots, a_N(t))$ is selected to ensure safety.

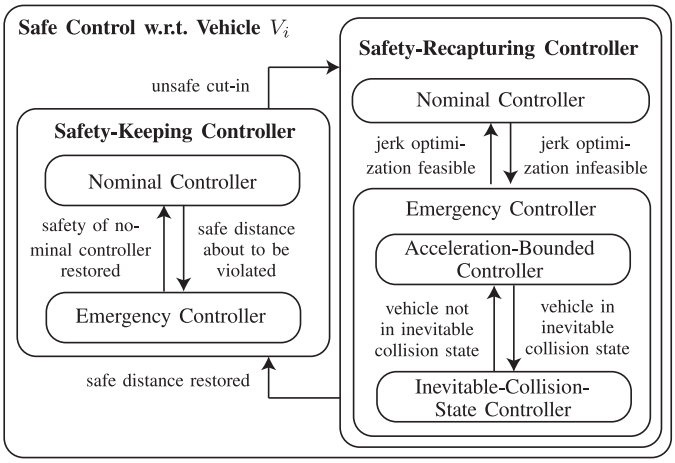


Fig. 2. Solution concept for a single preceding vehicle.

The safe acceleration with respect to each vehicle is effected via a safety-keeping controller consisting of an unverified nominal controller and a verified emergency controller, as shown in Fig. 2. This combination ensures a safe distance if no vehicle cuts in, because an emergency controller ensures the safe distance if it is about to be violated by the nominal controller. When a vehicle cuts into the lane in which the ego vehicle is located, the safety-recapturing controller of the ego vehicle is activated. Since cut-in vehicles cause unsafe situations that are not caused by the ego vehicle, the ego vehicle is not obliged to establish a safe distance at all costs. While our control concept must be safe for any future behavior of preceding vehicles, it is only required to clear the dangerous situation within the clearing time $t_c(x(t), x_p(t))$ given that the other vehicle does not brake more sharply than $\underline{a}_{cut-in}$ as stated in Spec. III.1.

Next, we provide methods to identify safety-relevant vehicles. We present our safe adaptive cruise controller considering the remaining vehicles in Section IV, followed by the safety-recapturing controller in Section V.

C. Selection of Safety-Relevant Vehicles

In order to ensure safety, it is not sufficient to merely consider the vehicle directly in front of the ego vehicle. This first preceding vehicle might perform a lane change due to a stationary vehicle ahead, in which case the latter is the relevant one for the safety controller; see Fig. 12(b). However, considering all vehicles is computationally expensive, so we exclude vehicles that are provably irrelevant. As previously mentioned, the vehicles $V_i, i \in \{1, 2, \dots, N\}$ preceding the ego vehicle are ordered, where a larger index means that the vehicle is further ahead.

In this work, we consider a vehicle to be part of the ego lane as soon as the occupancy of the vehicle intersects with it: $\mathcal{O}(x_p(t)) \cap \mathcal{L}_{ego} \neq \emptyset$ (see Def. II.3). For vehicles leaving the ego lane, we introduce a time lag δ_{leave} during which we still assume that they are in the ego lane, in order to prevent uncomfortable accelerations if they immediately re-enter the ego lane. The reduction in the number of vehicles considered is performed in two steps.

1) Exclusion of Faster Preceding Vehicles: We ignore preceding vehicles V_i at time t if

$$\exists j \in \{1, \dots, i-1\} : \; v_p^{(j)}(t) \leq v_p^{(i)}(t).$$

Due to the assumption that the maximum deceleration potential among other vehicles is identical (Spec. III.5), it is obvious that faster preceding vehicles of V_i stay ahead of V_i if maximum deceleration is applied.

2) Remove Vehicles Behind the Stopping Distance: Given the maximum possible input trajectory $\overline{u}(\cdot)$ of the ego vehicle and its stopping distance $s_{stop}(t)$ in emergency mode, vehicles V_i are ignored at time t if

$$s_p^{(i)}(t) \geq \mathrm{proj}(\xi(\Delta t; x_0, \overline{u}(\cdot))) + s_{stop}(t + \Delta t).$$

Let us justify the above condition using a hypothetical worst-case scenario where a preceding vehicle instantaneously stops at its initial position $s_p^{(i)}(t)$: If the ego vehicle in emergency mode can still stop before hitting the preceding vehicle in the next planning cycle after moving by $\mathrm{proj}(\xi(\Delta t; x_0, u(\cdot)))$, then the preceding vehicle can be ignored by the safety-keeping controller.

D. Overall Algorithm

Alg. 1 summarizes the different computation steps of the safe adaptive cruise controller for a single time interval. The algorithm receives as input the current state of the ego vehicle and of all preceding vehicles. First, vehicles for the safety-recapturing controller $\mathcal{X}_p^{re}$ and vehicles for the safety-keeping controller $\mathcal{X}_p^{ke}$ are selected (line 1-2). If the calculated acceleration of the safety-keeping nominal controller would violate the safe distance, the emergency controller is activated (line 5-8). In the case of an inevitable-collision state caused by a cut-in vehicle, the ego vehicle fully brakes (line 12-14). If the safety-recapturing nominal controller finds no solution, the acceleration-bounded controller is used (line 15-18). If no relevant vehicle exists, the cruise controller is executed (line 22).

IV. Emergency Controller

The purpose of the emergency controller is to take over control if the nominal controller does not provide a safe solution, regardless of sensor noise, disturbances, and the future behavior of surrounding vehicles. We first present the interaction of the emergency controller with the nominal controller in Section IV-A. Next, we show in Section IV-B how to simultaneously ensure safety and comfort.

A. Interaction With Nominal Controller

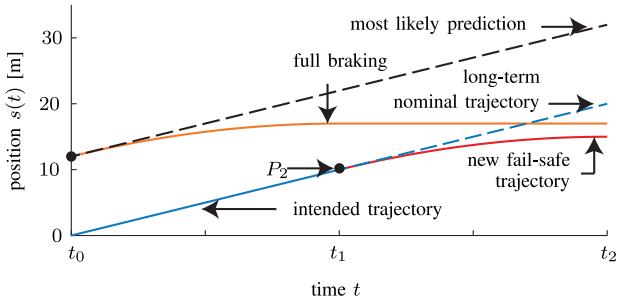
To explain the interaction between the nominal controller and the emergency controller, we first introduce a few different types of trajectories:

- *Long-term nominal trajectory:* A trajectory planned by the nominal controller under certain assumptions on the behavior of surrounding vehicles for a time horizon of typically several seconds.

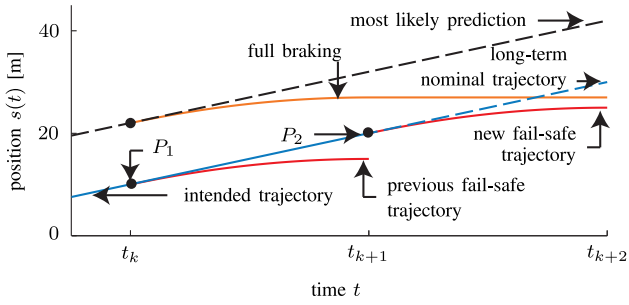
Algorithm 1: Safe Control Outputs for One Time Interval.

Input: Ego vehicle state x, set of preceding vehicle states $\mathcal{X}_p = \{x^{(i)} \mid i \in 1...N\}$
Output: Acceleration for underlying controller

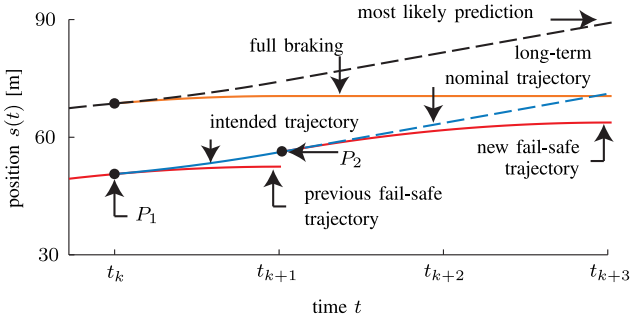
$\mathcal{X}_p^{re} \leftarrow$ CUTINVEHICLES$(\mathcal{X}_p)$ ▷Def. II.3
$\mathcal{X}_p^{ke} \leftarrow$ RELEVANTVEHICLES$(\mathcal{X}_p \setminus \mathcal{X}_p^{re})$ ▷Section III-C
AccList $\leftarrow$ []
for all $x_p \in \mathcal{X}_p^{ke}$ **do**
  a $\leftarrow$ safetyKeeping.NOMINAL(x, x_p) ▷Section II-B
  if safetyKeeping.UNSAFE(a, x, x_p) **then** ▷Section IV-A
    a $\leftarrow$ safetyKeeping.EMERGENCY(x) ▷Section IV-B
  end if
  AccList.APPEND(a)
end for
for all $x_p \in \mathcal{X}_p^{re}$ **do**
  if safetyRecap.ICS(x, x_p) **then** ▷Section V-B1
    return $\underline{a}$ ▷Spec. III.3
  end if
  a $\leftarrow$ safetyRecap.NOMINAL(x, x_p) ▷Section V-A
  if a $= \emptyset$ **then**
    a $\leftarrow$ safetyRecap.BOUNDED(x, x_p) ▷Section V-B2
  end if
  AccList.APPEND(a)
end for
if $\mathcal{X}_p^{ke} \cup \mathcal{X}_p^{re} = \emptyset$ **then**
  a $\leftarrow$ CRUISECONTROL (x)
  return a
end if
return min(AccList)



(a) The adaptive cruise controller can only be engaged if the intended and fail-safe trajectory can be verified as shown in this illustration.



(b) If the next intended trajectory together with its fail-safe trajectory can be verified before approaching P_1, the new intended trajectory can be followed up to P_2.



(c) If the ego vehicle follows a fail-safe trajectory, it is tried to find a new safe intended trajectory. The figure shows that the fail-safe trajectory only has to be executed up to P_1 and the new intended trajectory can be executed up to P_2.

Fig. 3. Interaction between the nominal controller and the emergency controller. If the nominal trajectory plus the fail-safe trajectory can be verified on time, the nominal trajectory is executed, otherwise the fail-safe trajectory is executed.

- *Intended trajectory:* First part of a long-term nominal trajectory subject to formal verification.
- *Fail-safe trajectory:* A trajectory attached to the intended trajectory that brings the vehicle to a safe state [6], [80].
- *Potential trajectory:* Concatenation of an intended trajectory and a fail-safe trajectory, which has not yet been verified.
- *Safe trajectory:* Potential trajectory, which is verified as safe. A safe trajectory is verified for all times, since the ego vehicle is not accountable if it is hit after reaching a safe state at the end of the fail-safe trajectory.

The safety of the nominal controller in combination with the emergency controller is proven by induction. The safe adaptive cruise controller can only be engaged if the potential trajectory (intended trajectory plus fail-safe trajectory) has been verified. The potential trajectory is verified if there is no collision with the preceding vehicle performing full braking as shown in Fig. 3(a). Once the system is safely engaged (base case), we show that the next step is also safe (induction step) as shown in Fig. 3(b). While time progresses within $[t_{k-1}, t_k[$ (open brackets denote the exclusion of endpoints), the ego vehicle verifies whether the new intended trajectory for $[t_k, t_{k+1}[$ together with its fail-safe trajectory is safe, i.e., whether the ego vehicle avoids a crash if the preceding vehicle fully brakes. If it is safe, the intended trajectory is executed for $[t_k, t_{k+1}[$. Otherwise, the fail-safe maneuver is started at t_k (see point P_1 in Fig. 3(b)). In the event that a fail-safe trajectory is engaged, we try to find a new safe trajectory branching off the fail-safe trajectory (see point P_1 in Fig. 3(c)) so that the fail-safe trajectory is executed as shortly as possible if a new safe intended trajectory can be found. Indeed, the new intended trajectory between point P_1 and P_2 in Fig. 3(c) for $[t_k, t_{k+1}[$ together with the new fail-safe trajectory branching off at P_2 can be verified as safe; thus, the fail-safe trajectory no longer has to be executed.

B. Emergency Controller for a Single Preceding Vehicle

We provide methods to efficiently determine whether the proposed fail-safe trajectory indeed avoids a crash if the preceding vehicle immediately brakes. As a result, we obtain the acceleration profile for $[t_k, t_{k+1}[$ with respect to each preceding vehicle. As mentioned in our solution concept in Section III-B, we select the minimum acceleration for each point in time within $[t_k, t_{k+1}[$. In our implementation, we hold the acceleration value within $[t_k, t_{k+1}[$ so that all that remains is to compare one value per vehicle for the considered time interval. To ensure safety for each vehicle, we make use of the concept of monotone dynamics.

Definition IV.1 (Monotone dynamics; see [81, Def. II.1]): The system dynamics is monotone with respect to the initial state x_0 and input trajectories $u(\cdot)$ when the following property holds for the solution $\xi(t, x_0, u(\cdot))$:

$$\begin{aligned}&\forall i, j, t \geq 0 : x_i(0) \leq \overline{x}_i(0), u_j(t) \leq \overline{u}_j(t)\\ &\implies \xi_i(t; x(0), u(\cdot)) \leq \xi_i(t; \overline{x}(0), \overline{u}(\cdot)).\end{aligned}$$

Next, we show that our vehicle model $\dot{x} = f(x, u, w)$ in (1) is monotonic. A constructive method to prove monotonicity is presented in [81, Prop. III.2], which returns monotonicity with respect to x and u.

Proposition IV.1 (Monotonic vehicle dynamics): The vehicle model $\dot{x} = f(x, u, w)$ in (1) is monotonic.

Proof: We first require the non-zero and non-diagonal derivatives of the vehicle model:

$$\frac{\partial f_1}{\partial x_2} = 1$$

$$\frac{\partial f_2}{\partial x_3} = \begin{cases} 1 & \text{for } \neg C \wedge (\underline{a} + a_{dr} + a_i \leq x_3 \leq \overline{a}(v) + a_{dr} + a_i),\\ 0 & \text{otherwise}\end{cases}$$

$$\frac{\partial f_3}{\partial u} = 1.$$

Since all non-zero and non-diagonal derivatives are 1, irrespective of the state and input, the system is monotone; see, e.g., [81, Prop. III.2]. ■

Please note that most systems are not monotonic—including vehicles whereby one jointly considers the longitudinal and the lateral dynamics, as shown in [82, Section IV-B].

Subsequently, we exploit monotonicity by only using stopping distances for two aspects: 1) the safe velocity based on the sensor range and 2) whether a crash can occur. As a preliminary result, we determine the upper bound of reachable positions using zero-order hold.

Proposition IV.2 (Upper bound of reachable position): If $\forall t > 0 : \dot{u}(t) \leq 0$, one obtains an upper bound of the reachable position when using zero-order hold for $u(t)$.

Proof: Let us denote the zero-order hold function as $\tilde{u}(t)$. Since $\dot{u}(t) \leq 0$ we have that

$$\forall k \, \forall t \in [t_k, t_{k+1}[: \tilde{u}(t) = u(t_k) \geq u(t).$$

Thus, due to monotonicity of (1) according to Prop. IV.1, we have that

$$\begin{aligned}&\xi_i(t; x(0), \tilde{u}(\cdot)) \geq \xi_i(t; x(0), u(\cdot))\\ &\implies \text{proj}(\xi_i(t; x(0), \tilde{u}(\cdot))) \geq \text{proj}(\xi_i(t; x(0), u(\cdot))).\end{aligned}$$

■

The previous proposition motivates the use of standard solvers of ordinary differential equations for computing upper bounds on reachable positions. Let us denote the stopping distance obtained by Prop. IV.2 as $\tilde{s}_{stop} = \xi(t_s(\tilde{u}_{brake}(\cdot)); x_0, \tilde{u}_{brake}(\cdot))$, where $\tilde{u}_{brake}(\cdot)$ is the zero-order hold trajectory of $u_{brake}(\cdot)$. The ego vehicle can only drive at a maximum speed that allows it to come to a stop within the sensor range. This ensures that if another vehicle stands at the border of the sensor range, the ego vehicle can avoid a collision. Given the sensor range s_{sr}, the maximum allowed velocity can be determined offline as shown below.

Proposition IV.3 (Safe velocity for sensor range): Given $u_{brake}(\cdot)$ (see Def. II.1) and the sensor range s_{sr}, the ego vehicle is always able to stop within the sensor range if $v \leq v_{sr}$, where the maximum v_{sr} is chosen such that

$$\text{proj}(\xi(t_s(\tilde{u}_{brake}(\cdot)); [0, v_{sr}, \overline{a}]^T, \tilde{u}_{brake}(\cdot))) \leq s_{sr}.$$

Proof: Due to the monotonicity of the vehicle model according to Prop. IV.1, it is sufficient to find the worst-case initial state to determine the maximum braking distance. Since the vehicle dynamics is position-invariant, we can choose $x_1 = 0$ without a loss of generality. The velocity is given as $x_2 = v_{sr}$ so that it remains to choose the worst-case initial acceleration $x_3(t_0) = \overline{a}$. ■

Besides the maximum velocity regarding the sensor range, we also have to respect the speed limit $v_{limit}(t)$ so that

$$\overline{v}(t) = \min(v_{sr}, v_{limit}(t)).$$

Since the speed limit can be violated within small bounds, we do not enforce it with formal methods, and just rely on the nominal controller. However, we enforce v_{sr} for safety reasons. Since the acceleration potential of a vehicle at v_{sr} is small for a decent sensor range, the nominal controller will gradually approach v_{sr} if $v_{limit}(t) > v_{sr}$, so that we immediately limit the acceleration to zero as soon as this speed is reached without causing discomfort.

Subsequently, we make use of the braking distance in order to safely follow preceding vehicles. Before we can do that, we present the relationship between collision avoidance and braking distance for two different cases. In the first case, the preceding vehicle cannot brake as sharply as the ego vehicle. As a consequence, it is not sufficient in that case to consider braking distances to determine whether a crash can occur or not, as illustrated by the following counterexample.

Example IV.1 (Ego vehicle with large deceleration): Let us consider the situation with the following initial states and inputs: $s_{p,0} = 20$ [m], $v_{p,0} = 20$ [m/s], $\forall t \in [0, t_s(a_p(\cdot))] : a_p(t) = -3$ [m/s^2], $s_0 = 0$ [m], $v_0 = 40$ [m/s], and $\forall t \in [0, t_s(a(\cdot))] : a = -10$ [m/s^2]. Since we chose the deceleration of the ego vehicle (at $a = -10$ [m/s^2]) to be larger than that of the preceding

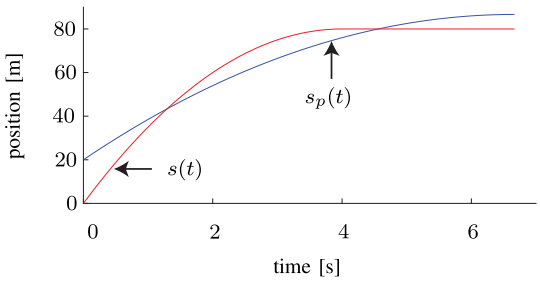


Fig. 4. Counterexample showing that a collision can occur although the ego vehicle would stop behind the preceding vehicle.

vehicle ($a_p = -3$ [m/s^2]), the ego vehicle would stop behind the preceding vehicle, although they collide at an earlier point in time, as shown in Fig. 4. Thus, it is not sufficient to only check whether the ego vehicle comes to a standstill behind the preceding vehicle.

However, in the second case, where the preceding vehicle can brake more sharply than the ego vehicle (Spec. III.5), it is sufficient to merely consider the braking distance as presented next. To simplify the notation, we introduce the stopping time $t_{stop} = t_s(u(\cdot))$.

Proposition IV.4 (Collision detection by stopping distance): When a preceding vehicle brakes at $\underline{a}_p$ and the ego vehicle decelerates less, such that $\forall t : a(t) > \underline{a}_p$, it is sufficient to check whether $s_p(t_{p,stop}) \geq s(t_{stop})$ to conclude that no collision can happen.

Proof: There are two possibilities as to how a crash can occur: the preceding vehicle is stationary when the crash happens, or it is still moving. Let us consider the corner case, where $t_{stop} = t_{p,stop}$ and $s_p(t_{p,stop}) = s(t_{stop})$. When simulating the system backwards in time, this condition can only be reached when

$$s(t) = s_p(t) + \underbrace{\int_t^{t_{p,stop}} \int_t^{\tilde{\tau}} a(\tau) - \underline{a}_p \, \mathrm{d}\tau \mathrm{d}\tilde{\tau}}_{>0},$$

so that it is impossible to achieve $s(t) = s_p(t)$ for any $t < t_{p,stop}$. Thus, to avoid a crash, we only have to check whether the ego vehicle can crash into the preceding vehicle when it has already stopped. Since the position of the preceding vehicle does not change after $t_{p,stop}$ and the position of the ego vehicle might still increase after $t_{p,stop}$ ($s(t_{p,stop}) \leq s(t_{stop})$), no crash can occur if $s_p(t_{p,stop}) \geq s(t_{stop})$. ■

This result can be used to formulate a condition under which the next intended behavior $\xi(t; x_0, u_{int}(\cdot))$ can be verified as safe. To this end, we introduce the state $\hat{x}$ at the beginning of the fail-safe trajectory at time t_{k+1} and the state $\hat{x}_p$ at the beginning of the full-braking trajectory at time t_k. Subsequently, we slightly abuse notation and write $\underline{a}_p$ instead of $u_{p,brake}(\cdot)$ to denote an input trajectory with the constant value $\underline{a}_p$.

Proposition IV.5 (Safe use of nominal controller): If

$$\mathrm{proj}(\xi_p(t_{p,stop}; \hat{x}_p, \underline{a}_p) \geq \mathrm{proj}(\xi(t_{stop}; \hat{x}, \tilde{u}_{brake}(\cdot)), \quad (7)$$

we can continue using the nominal controller during $t \in [t_k, t_{k+1}[$ ensuring the safe distance

$$d_{safe}(x(t_k), v_p(t_k)) = \mathrm{proj}\Big(\hat{x} - x(t_k) + \xi(t_{stop}; \hat{x}, \tilde{u}_{brake}(\cdot))\Big) - \mathrm{proj}\Big(\xi(t_{p,stop}; [\mathrm{proj}(x(t_k)),\ v_p(t_k)]^T, \underline{a}_p)\Big)$$

when no vehicle cuts in, otherwise the emergency controller must be activated at time t_k.

Proof: We prove the safety by induction. The base case is that the adaptive cruise controller can only be engaged if the vehicle is in a safe state, i.e., (7) is fulfilled. The induction step is that we stay safe at time t_{k+1} if we are in a safe state at time t_k: We only follow the intended trajectory if the subsequent fail-safe maneuver (see Fig. 3(b)) is safe according to Prop. IV.4, which is formalized by (7). Otherwise, the provably-safe emergency controller is activated at time t_{k+1}.

As a by-product, we maintain a safe distance, i.e., the distance at time t_k such that (7) is barely fulfilled: $\mathrm{proj}(\xi_p(t_{p,stop}; \hat{x}_p, \underline{a}_p) = \mathrm{proj}(\xi(t_{stop}; \hat{x}, \tilde{u}_{brake}(\cdot))$. This results in the safe distance from the proposition. ■

C. Measurement Uncertainties and Conformance Checking

We further make use of monotonicity to easily integrate measurement uncertainties and model uncertainties.

1) Measurement Uncertainties: We assume that the perception module of the vehicle does not only provide the state of each surrounding vehicle (position and velocity), but also an uncertain interval in which the true state lies. To obtain these intervals, one can use set-based observers [83], [84]. These observers ensure that the propagation of the set of uncertain states is physically possible, so that a safe solution can always be found if no vehicle cuts in. An alternative is to use standard stochastic observers, such as Kalman filters, and using confidence intervals, such as 4σ (σ is the standard deviation) in which 99.994% of all measurements would lie, assuming Gaussian distribution. Given the position interval $[\underline{s}_p, \overline{s}_p]$ and the velocity interval $[\underline{v}_p, \overline{v}_p]$ of an arbitrary preceding vehicle, the worst-case position for triggering the emergency controller in (7) is $\underline{s}_p$ and the worst-case velocity is $\underline{v}_p$ due to monotonicity.

Perception modules try to track as many vehicles as possible, e.g., by a diverse set of sensors [85], [86], by reflections of signals [87], [88], and by Vehicle2X communication [89], [90]. However, in some cases, one cannot infer whether a vehicle is in front of another vehicle. In such an event, we assume that a standing vehicle is present at the border of the undetectable region of the ego lane.

2) Conformance Checking: Since the demanded acceleration of the vehicle is not exactly achieved by a real vehicle, we increase the acceleration by a_{corr} when computing solutions of the ego vehicle, such as $\xi(t_{stop}; \hat{x}(t_{k+1}), \tilde{u}_{brake}(\cdot))$. Due to the monotonicity of the dynamics, this results in strictly larger distances. Otherwise, an uncertain interval of values would have to be added, as this is typically done as part of conformance

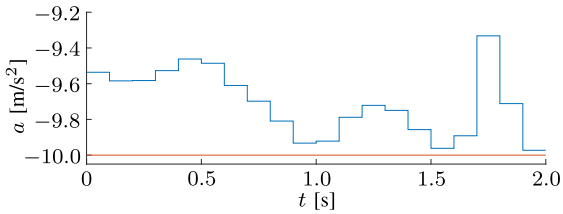


Fig. 5. The executed acceleration by the simulator (blue) deviates from the commanded acceleration of the safe ACC (orange).

checking; see, e.g., [66], [91], [92]. The value of a_{corr} has to be determined in driving experiments, and represents the maximum deviation from the commanded acceleration across all driving experiments. In particular, we have conducted more than 50 experiments with a high-fidelity simulation of the braking system, where an exemplary deviation between the commanded and executed acceleration is shown in Fig. 5. For the simulator study with a high-fidelity simulation of the braking system, we have determined $a_{corr} = 0.75$ [m/s^2]. An appropriate way to limit a_{corr} is too select $|\underline{j}|$ not too large. Due to conformance checking, we also consider the dynamics of inner control loops as discussed in Section II.

V. Safety-Recapturing Controller

While a cut-in brings the ego vehicle to a temporarily unsafe situation, it cannot be demanded that the ego vehicle immediately performs emergency braking—not only since this jeopardizes the safety of following vehicles, but also because the passengers should not suffer from the fault of another driver. Although in most cases no collision occurs if one does not immediately regain a safe distance, one should still react swiftly.

The user-defined clearance time $t_c(x(t), x_p(t))$ from Spec. III.1 specifies the point by which the safe distance has to be regained. As for the safety-keeping controller, we provide a nominal controller and an emergency controller, where the nominal controller can be replaced by any other controller. To simplify the notation, we assume that time is reset to zero as soon as the vehicle for which we run this controller cuts in.

A. Nominal Controller

We propose regaining safety in the nominal case by solving the optimization problem in (2).

Proposition V.1 (Ensuring the clearing time t_c): Without loss of generality, we reset the initial time to zero. We ensure the clearing time t_c as specified in Spec. III.1 under the assumption that the preceding vehicle accelerates more rapidly than $\underline{a}_{cut-in}$, i.e., $\forall t \leq t_c : a_p(t) > \underline{a}_{cut-in}(t)$, by adjusting the constraint in (3) to

$$d_{safe}(x(t_c), v_p(t_c)) \leq x_{n,1}(t_c), \quad v_p(t_c) = v_{p,0} + \underline{a}_{cut-in}\, t_c.$$

Proof: When the modified quadratic programming problem in (3) is feasible, there are solvers that are guaranteed to meet the constraints (here: satisfy the clearance time) while converging to the optimal solution [93]. Obviously, an increase in the velocity of the preceding vehicle would not make the optimization infeasible. ■

To save computation time, all optimizations for Prop. V.1 are only performed up to the clearing time t_c. In the event that the preceding vehicle decelerates more sharply than $\underline{a}_{cut-in}$, we switch to the emergency controller (see Fig. 2), which is described subsequently. Also, the safe distance might be regained faster than t_c if the preceding vehicle decelerates at less than $\underline{a}_{cut-in}$; in this event, we switch to the safety-keeping controller before t_c, as illustrated in Fig 2.

B. Emergency Controller

Unlike the emergency controller for safety-keeping, the emergency controller for safety-recapturing has two modes: the ego vehicle is in an inevitable collision state ($x \in \mathcal{ICS}$) or not.

1) Inevitable-Collision-State Controller: The definition of inevitable collision states does not specify how the occupancy of surrounding obstacles is predicted (see Def. II.2). According to the specification regarding cut-ins, we assume that the preceding vehicle does not brake more sharply than $\underline{a}_{cut-in}$ (Spec. III.1) so that the worst-case prediction for the preceding vehicle is braking with $\underline{a}_{cut-in}$. If the ego vehicle is in an inevitable collision state, assuming the deceleration $\underline{a}_{cut-in}$ of the preceding vehicle, full braking is immediately applied to mitigate the likely collision—we refer to this controller as the inevitable-collision-state controller; the collision can still be avoided if the preceding vehicle accelerates.

2) Acceleration-Bounded Controller: Otherwise, if the ego vehicle is not in an inevitable collision state, a safe solution within the acceleration bounds is still feasible. Since the nominal controller could not find a solution, we remove the jerk constraints in (6)—we refer to this controller as acceleration-bounded controller. Again, as for the nominal controller, we assume that the preceding vehicle does not brake more sharply than $\underline{a}_{cut-in}$.

VI. Evaluation

One of our main goals is to not only ensure provably correct behavior, but also to provide the sensation of safety and comfort, even when other vehicles cut in. To evaluate whether passengers feel safe and comfortable, we conducted a user study in a driving simulator. Before we present the results of the user study, we list the parameterization of the controllers, the achieved computation times, and demonstrate the behavior of the vehicle for selected traffic situations.

A. Parameterization of the Controllers

We briefly list the parameters used in the safe adaptive cruise controller for the subsequent evaluation in Table I, where the subscripts k and r denote weights for the safety-keeping and safety-recapturing nominal controller, respectively. The jerk profile can be freely chosen by the system designer to determine the vehicle acceleration up to the point when the maximum possible deceleration $\underline{a}$ is reached. From that point on, the vehicle

TABLE I
PARAMETERIZATION OF THE NOMINAL AND EMERGENCY CONTROLLERS

Parameter	Value	Parameter	Value
$\bar{j}$	10 $\frac{\text{m}}{\text{s}^3}$	$\underline{j}$	-10 $\frac{\text{m}}{\text{s}^3}$
$\bar{a}$	3 $\frac{\text{m}}{\text{s}^2}$	$\underline{a}$	-10 $\frac{\text{m}}{\text{s}^2}$
$\bar{v}$	51 $\frac{\text{m}}{\text{s}}$	$\underline{v}$	0 $\frac{\text{m}}{\text{s}}$
s_{sr}	200 m	Δt	0.1 s
$\underline{a}_p$	-10.5 $\frac{\text{m}}{\text{s}^2}$	λ	0.5 s
s_c	0.4 m	θ_c	0.035 rad
Q_k	[5 10 50]	r_k	100
Q_r	[15 30 50]	r_r	100
h_k	6.0 s	$\underline{a}_{cut-in}$	-2 $\frac{\text{m}}{\text{s}^2}$
δ_{leave}	1.0 s		

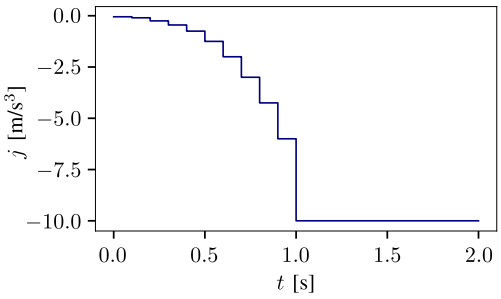


Fig. 6. Predefined jerk profile.

decelerates at $\underline{a}$ until the emergency mode is left or the vehicle is at a standstill. We chose the monotonically decreasing jerk profile shown in Fig. 6 since most situations are quickly resolved, so that we could apply Prop. IV.2.

B. Selected Scenarios

The subsequent evaluations are based on scenarios of the CommonRoad benchmark suite[1] [94]. All simulations were executed on a machine with an Intel Core i7-8650U 1.90 GHz processor and 24 GB of DDR4 2400 MHz memory. Our Python implementation of the safe adaptive cruise control is available at https://gitlab.lrz.de/tum-cps/safe-acc. In the first evaluated scenario, the recapturing controller is activated to restore the safe distance after a cut-in (CommonRoad ID: S=USA_US101-13_5_T-1:2018b). In the second scenario, the safety-keeping nominal controller is not able to maintain the safe distance to a leading vehicle, and therefore the emergency controller is executed (CommonRoad ID: S=USA_US101-3_5_T-1:2018b). In both scenarios, the adaptive cruise controller continues with the safety-keeping nominal controller, after the critical situations have been successfully resolved. The computation time for the cut-in scenario when excluding non-safety relevant vehicles is always less than 0.01 [s], although there are up to eight vehicles within the sensor range (see Fig. 7). This confirms the real-time capability of our approach. The exclusion of non-safety-relevant vehicles decreases the computation time roughly by a factor of four in the considered scenario.

The jerk, acceleration, velocity, and distance trajectories for the cut-in and emergency maneuver scenario are shown in Fig. 8

[1]commonroad.in.tum.de

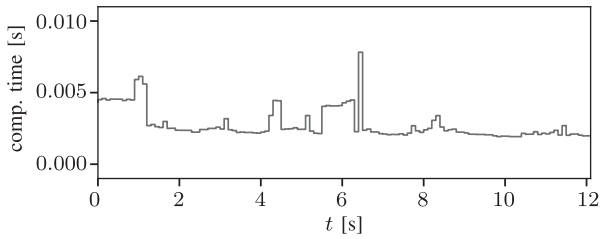


Fig. 7. Computation time for the cut-in scenario (CommonRoad ID: S=USA_US101-13_5_T-1:2018b).

and Fig. 9, respectively. Both scenarios show the high comfort level of our approach, since only when the cut-in vehicle violates the safe distance does the ego vehicle apply $\underline{j}$ for three time steps.

C. User Study

The user study was conducted at the BMW Group in a static driving simulator. Fig. 10 shows the simulator consisting of an actual cockpit from a serial vehicle and three monitors visualizing the environment; a snapshot of the central monitor is shown Fig. 11.

The driver can control the automatic gearbox, the gas pedal, the brake pedal, and the steering wheel. The software for controlling the simulator and creating the scenarios is a proprietary BMW tool called SPIDER. During the user study, the driver only needed to control the steering wheel. Additionally, the participants saw the current velocity on the monitor. All users tested two systems: our novel system and the built-in state-of-the-art adaptive cruise controller, which we briefly describe below.

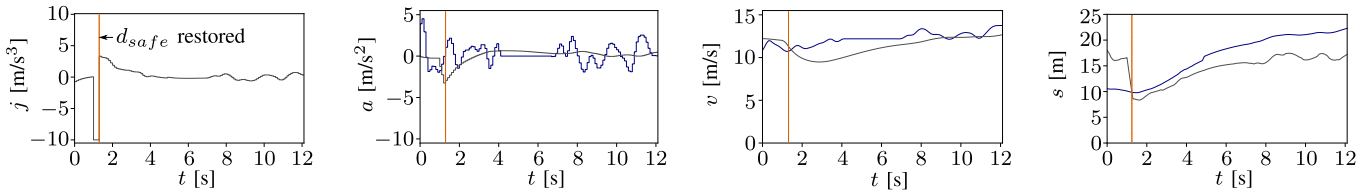
The goal of the user study was to evaluate the following hypotheses:

1) The feeling of safety provided by the safe adaptive cruise controller is at least as high as that of a state-of-the-art adaptive cruise controller.
2) The comfort of the safe adaptive cruise controller is at least as good as that of a state-of-the-art adaptive cruise controller.

To evaluate these hypotheses, the user was asked six different questions after each scenario and, additionally, the braking force applied to the pedal was evaluated. In the following, the six questions are listed with the possible answer options in parentheses:

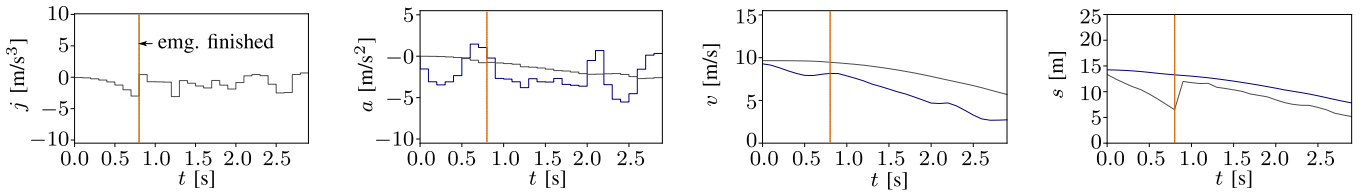
1) How do you rate the distance to the leading vehicle? (very short, short, appropriate, large, very large)
2) How do you rate the feeling of safety provided by the algorithm? (very low, low, middle, high, very high)
3) Did you want to intervene, but refrained from doing so in the end? (no, yes)
4) Did the algorithm slow down unnecessarily or slow down too rapidly? (no, yes)
5) How do you rate the comfort of this algorithm? (very low, low, appropriate, high, very high)
6) How do you assess the timing of the braking maneuver? (very early, early, appropriate, late, very late)

The answers for the questions with five options have been encoded with numerical values ranging from 1 to 5 and the answers



(a) Jerk of the ego vehicle. (b) Acceleration of the ego vehicle (gray) and a cut-in vehicle (blue). (c) Velocity of the ego vehicle (gray) and a cut-in vehicle (blue). (d) Relative (blue) and safe distance (gray).

Fig. 8. The safety-recapturing controller restores the safe distance comfortably (CommonRoad ID: S=USA_US101-13_5_T-1:2018b).



(a) Jerk of the ego vehicle. (b) Acceleration of the ego vehicle (gray) and a cut-in vehicle (blue). (c) Velocity of the ego vehicle (gray) and a cut-in vehicle (blue). (d) Relative (blue) and safe distance (gray).

Fig. 9. The emergency controller is activated since the safe distance is about to be violated (CommonRoad ID: S=USA_US101-3_5_T-1:2018b).

Fig. 10. The BMW driving simulator consisting of a cockpit and three monitors visualizing the environment.

Fig. 11. Snapshot of a scene in the driving simulator displayed at the central screen.

for questions with yes or no options have been encoded with 0 and 1. Questions 2 and 5 ask directly for an evaluation of the corresponding hypothesis. Question 1 has the goal of showing that the safe adaptive cruise controller is not too conservative. Question 3 is related to the feeling of safety, and questions 4 and 6 are related to comfort. In addition to the questions previously mentioned, the user could give general feedback on the performance of the adaptive cruise controllers.

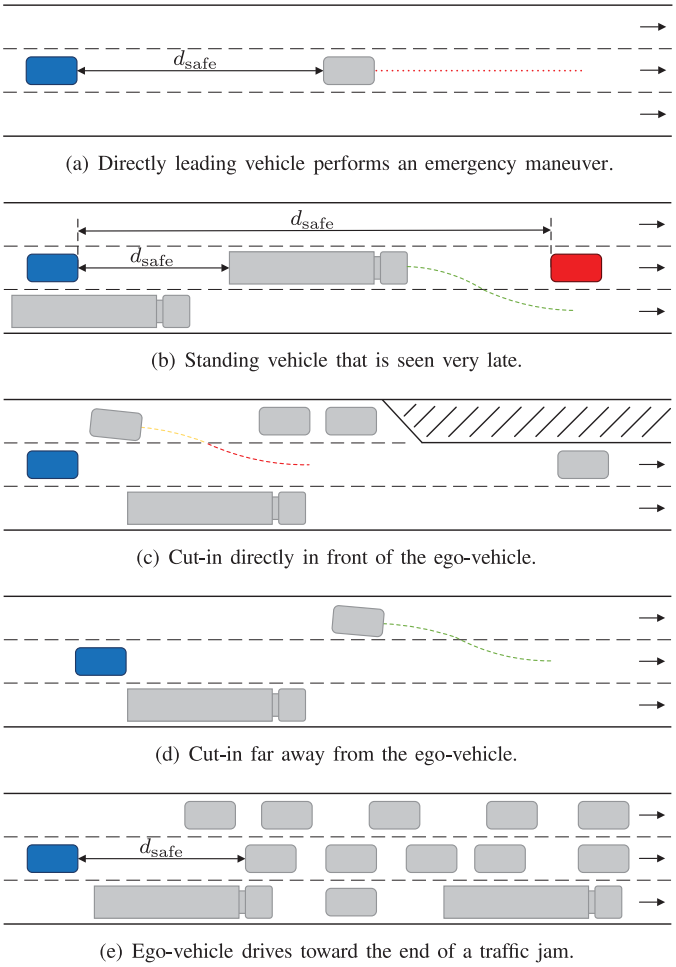
1) State-of-the-Art Adaptive Cruise Controller: Instead of trying to keep a safe distance d_{safe}, the state-of-the-art adaptive cruise controller tries to keep the distance d_{rec}, which is half of the ego vehicle's velocity in $\frac{\text{km}}{\text{h}}$, which is the recommended minimum distance according to German traffic rules:

$$d_{\text{rec}} = 1.8\, v.$$

The state-of-the-art adaptive cruise controller considers only a single leading vehicle and no cut-in vehicles. If the state-of-the-art adaptive cruise controller does not find a valid input to the lower-level vehicle controller because constraints cannot be fulfilled, a linear deceleration occurs until the model predictive controller finds a valid input once again. Next, we describe the scenarios considered in the user study.

2) Test Scenarios: For the evaluation of the safe adaptive cruise controller, five different test scenarios were created. In all scenarios, the ego vehicle starts with a velocity of zero and in a safe state. Fig. 12 illustrates the scenarios from a top view and the following list describes the settings and goals of the scenarios:

1) *Full braking of the first leading vehicle:* The ego vehicle drives behind a leading vehicle that, after a while, suddenly



(a) Directly leading vehicle performs an emergency maneuver.

(b) Standing vehicle that is seen very late.

(c) Cut-in directly in front of the ego-vehicle.

(d) Cut-in far away from the ego-vehicle.

(e) Ego-vehicle drives toward the end of a traffic jam.

Fig. 12. Test scenarios for the evaluation of the safe adaptive cruise controller. The ego vehicle is marked in blue, surrounding vehicles are gray and stationary vehicles are red.

fully brakes to a standstill. The goal of this scenario is to evaluate vehicle-following and the ability to react to a sudden full braking maneuver.

2) *Full braking of the second leading vehicle:* The ego vehicle follows a small transporter approaching a standing vehicle. The participant cannot see the standing vehicle because the transporter is blocking the view. After the transporter performs an unexpected lane change to prevent colliding with the standing vehicle, the standing vehicle suddenly appears in front of the ego vehicle. This scenario tests the behavior while following another vehicle, the ability of the safe adaptive cruise controller to consider more than one leading vehicle, and the reaction when a standing vehicle enters the field of view.
3) *Aggressive cut-in:* A vehicle from an adjacent lane performs an aggressive cut-in. The merging vehicle has a lower velocity than the ego vehicle and brakes during the cut-in. The goal of the scenario is to demonstrate the ability to react to cut-in vehicles and to evaluate the behavior of the ego vehicle in this situation.
4) *Smooth cut-in:* A vehicle from an adjacent lane performs a smooth cut-in. The cut-in vehicle has a higher velocity than the ego vehicle and accelerates during the cut-in. This scenario has the same goals as those of the aggressive cut-in.
5) *Approaching tail of traffic jam:* The ego vehicle reaches the tail of a traffic jam and drives at $\overline{v}$. This scenario demonstrates the ability to come to a standstill if the ego vehicle drives fast and a standing vehicle enters the field of view.

Please note that we additionally inserted further random vehicles in the scenarios to create realistic scenarios with sufficient traffic. For each scenario, we changed the number of vehicles driving in the background, the vehicle types, and the motion of the surrounding vehicles. The order of the scenarios was different for each user to prevent bias in the user evaluations. For the same reason, we also slightly modified the scenarios for our adaptive cruise controller and the state-of-the-art version.

3) Results: Overall, 31 participants took part in the user study. For the evaluation of the two hypotheses, the Wilcoxon signed-rank t-test [95, Ch. 26] is used, because the data has an ordinal scale of measurement and the data distribution for both adaptive cruise controllers is nearly identical. The *Z-value* and *p-value* for the two hypotheses based on the Wilcoxon signed-rank t-test are listed in Table II. A *p-value* of less than or equal to 0.05 indicates significant results.

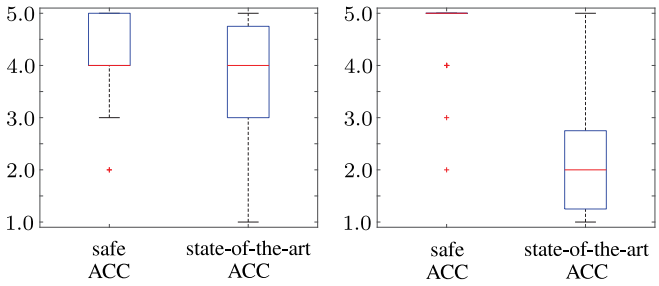
TABLE II
RESULTS OF THE WILCOXON SIGNED-RANK T-TEST FOR THE TWO HYPOTHESES

Scenario	Question	Z-value	p-value
1	Safety feeling	110.00	0.431
1	Comfort	170.50	0.159
2	Safety feeling	205.00	0.019
2	Comfort	383.00	0.001
3	Safety feeling	225.50	0.014
3	Comfort	201.00	0.026
4	Safety feeling	136.00	0.001
4	Comfort	403.50	0.001
5	Safety feeling	165.00	0.034
5	Comfort	124.50	0.107

The Wilcoxon signed-rank t-test indicates significant results for the hypothesis regarding the feeling of safety in Scenarios 2, 3, 4, and 5 and for the comfort hypothesis in Scenarios 2, 3, and 4. For the other scenarios, no significant results were generated; therefore, they are not discussed here in further detail. However, this does not mean that the safe adaptive cruise controller is worse than the state-of-the-art adaptive cruise controller in these scenarios. For the hypothesis-related questions regarding safety feeling and comfort, the mean of the safe adaptive cruise controller is at least as good as for the state-of-the-art adaptive cruise controller in all scenarios (see Table III). In Scenarios 1 and 5, no significant results were achieved, because the behavior of the safe adaptive cruise controller was not different enough from the state-of-the-art approach. In both scenarios, the main part consists of a full braking maneuver; therefore, the users were not able to detect significant differences. In all scenarios, the mean of the distance evaluated is always close to the optimal value (see Table III), which indicates that the safe adaptive cruise controller was not too conservative while achieving these

TABLE III
MEAN AND STANDARD DEVIATION OF ALL SCENARIOS

	Scenario 1				Scenario 2				Scenario 3				Scenario 4				Scenario 5			
Question	$\bar{x}_a$	$\bar{x}_b$	s_a	s_b	$\bar{x}_a$	$\bar{x}_b$	s_a	s_b	$\bar{x}_a$	$\bar{x}_b$	s_a	s_b	$\bar{x}_a$	$\bar{x}_b$	s_a	s_b	$\bar{x}_a$	$\bar{x}_b$	s_a	s_b
Distance	3.10	3.10	0.79	0.70	3.10	3.32	0.65	0.83	3.13	2.90	0.81	0.91	3.29	3.90	0.78	1.04	2.32	2.35	0.83	0.71
Safety feeling	4.16	4.13	0.90	0.99	4.19	3.58	0.91	1.18	3.68	3.06	1.05	1.03	4.94	3.97	0.25	1.14	2.32	1.97	1.05	0.98
Intervene	0.29	0.29	0.46	0.46	0.29	0.32	0.46	0.54	0.45	0.52	0.96	0.57	0.00	0.00	0.00	0.00	0.74	0.77	0.44	0.43
Unnec. braking	0.03	0.35	0.18	0.55	0.03	0.84	0.18	0.73	0.35	0.61	0.66	1.12	0.03	0.81	0.18	0.40	0.10	0.06	0.30	0.25
Comfort	3.87	3.58	0.96	1.15	4.16	2.52	0.90	1.06	3.35	2.81	1.05	1.11	4.68	2.19	0.70	1.11	2.10	1.87	1.11	0.85
Braking time	3.35	3.52	0.49	0.81	3.23	3.32	0.62	0.94	3.35	3.55	0.75	0.93	2.94	3.16	0.51	1.32	4.58	4.61	0.81	0.67
Braking force	0.11	0.10	0.29	0.26	0.07	0.06	0.25	0.25	0.03	0.12	0.18	0.31	0.00	0.00	0.00	0.00	0.30	0.36	0.45	0.47



(a) Boxplot of safety feeling in Scenario 2.

(b) Boxplot of comfort in Scenario 4.

Fig. 13. Example boxplots of significant hypotheses.

significant results. Fig. 13 illustrates two example boxplots for the feeling of safety in Scenario 2, and for comfort in Scenario 4. The medians of the safety feelings in Scenario 2 are almost the same, but the interquartile ranges of the state-of-the-art adaptive cruise controller are larger. The median of the comfort in Scenario 4 is much higher than that of the state-of-the-art adaptive cruise controller, and the interquartile range is also very low for the safe adaptive cruise controller compared to the state-of-the-art approach.

This study reveals that provably-correct controllers cannot only ensure safety, but also provide a comfortable ride, and increase the perceived safety, while not increasing the distance to preceding vehicles.

VII. CONCLUSIONS

We have presented the first approach for a provably-correct adaptive cruise controller that ensures comfort, even in the event of cut-ins. Our concept of using a nominal controller that is safeguarded by a provably-correct fail-safe controller makes it possible to exchange the nominal controller without having to have the vehicle's safety re-certified. This makes our approach particularly attractive for over-the-air updates concerning nominal behavior. Compared to previous work on provably-correct adaptive cruise control, we ensure safety by gradually engaging fail-safe maneuvers and providing a strategy for cut-ins—previous provably-correct approaches would apply full braking if a cut-in occurs. Our user study shows that our approach does not impede user satisfaction, despite ensuring that the vehicle does not cause a collision, and that a safe gap is swiftly regained following a cut-in.

REFERENCES

[1] N. Kaempchen, B. Schiele, and K. Dietmayer, "Situation assessment of an autonomous emergency brake for arbitrary vehicle-to-vehicle collision scenarios," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 4, pp. 678–687, Dec. 2009.

[2] M. Koschi, C. Pek, S. Maierhofer, and M. Althoff, "Computationally efficient safety falsification of adaptive cruise control systems," in *Proc. 22nd Int. IEEE Conf. Intell. Transp. Syst.*, 2019, pp. 2879–2886.

[3] A. Vahidi and A. Eskandarian, "Research advances in intelligent collision avoidance and adaptive cruise control," *IEEE Trans. Intell. Transp. Syst.*, vol. 4, no. 3, pp. 143–153, Sep. 2003.

[4] L. Xiao and F. Gao, "A comprehensive review of the development of adaptive cruise control systems," *Veh. Syst. Dyn.*, vol. 48, no. 10, pp. 1167–1192, 2010.

[5] M. Althoff and R. Lösch, "Can automated road vehicles harmonize with traffic flow while guaranteeing a safe distance?" in *Proc. 19th Int. IEEE Conf. Intell. Transp. Syst.*, 2016, pp. 485–491.

[6] C. Pek and M. Althoff, "Efficient computation of invariably safe states for motion planning of self-driving vehicles," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2018, pp. 3523–3530.

[7] W. Levine and M. Athans, "On the optimal error regulation of a string of moving vehicles," *IEEE Trans. Autom. Control*, vol 11, no. 3, pp. 355–361, Jul. 1966.

[8] B. Asadi and A. Vadihi, "Predictive cruise control: Utilizing upcoming traffic signal information for improving fuel economy and reducing trip time. *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 3, pp. 707–714, May 2011.

[9] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 296–305, Feb. 2014.

[10] A. Alam, A. Gattami, K. H. Johansson, and C. J. Tomlin, "Guaranteeing safety for heavy duty vehicle platooning: Safe set computations and experimental evaluations," *Control Eng. Practice*, vol. 24, pp. 33–41, 2014.

[11] J. Zhou and H. Peng, "String stability conditions of adaptive cruise control algorithms," in *Proc. IFAC Symp. Adv. Automot. Control*, vol. 37, no. 22, pp. 649–654, 2004.

[12] P. A. Ioannou and C. C. Chien, "Autonomous intelligent cruise control," *IEEE Trans. Veh. Technol.*, vol. 42, no. 4, pp. 657–672, Nov. 1993.

[13] P. A. Ioannou and M. Stefanovic, "Evaluation of ACC vehicles in mixed traffic: Lane change effects and sensitivity analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 1, pp. 79–89, Mar. 2005.

[14] S. Darbha and K. R. Rajagopal, "Intelligent cruise control systems and traffic flow stability," *Transp. Res. Part C: Emerg. Technol.*, vol. 7, no. 6 pp. 329–352, 1999.

[15] D. Swaroop, J. K. Hedrick, C. C. Chien, and P. A. Ioannou, "A comparision of spacing and headway control laws for automatically controlled vehicles," *Veh. Syst. Dyn.*, vol. 23, no. 1, pp. 597–625, 1994.

[16] K. Santhanakrishnan and R. Rajamani, "On spacing policies for highway vehicle automation," *IEEE Trans. Intell. Transp. Syst.*, vol. 4, no. 4, pp. 198–204, Dec. 2003.

[17] J. Zhou and H. Peng, "Range policy of adaptive cruise control vehicles for improved flow stability and string stability," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 2, pp. 229–237, Jun. 2005.

[18] A. Kesting, M. Treiber, M. Schönhof, and D. Helbing, "Adaptive cruise control design for active congestion avoidance," *Transp. Res. Part C: Emerg. Technol.*, vol. 16, no. 6, pp. 668–683, 2008.

[19] B. van Arem, C. J. G. van Driel, and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow characteristic," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 4, pp. 429–436, Dec. 2006.

[20] L. C. Davis, "Effect of adaptive cruise control systems on mixed traffic flow near an on-ramp," *Physica A: Statist. Mech. Appl.*, vol. 379, no. 1, pp. 274–290, 2007.

[21] P. Ioannou, Z. Xu, S. Eckert, D. Clemons, and T. Sieja, "Intelligent cruise control: Theory and experiment," in *Proc. 32nd IEEE Conf. Decis. Control*, vol. 2, pp. 1885–1890, 1993.

[22] C.-Y. Liang and H. Peng, "Optimal adaptive cruise control with guaranteed string stability," *Veh. Syst. Dyn.*, vol. 32, nos. 4–5, pp. 313–330, 1999.

[23] S. Li, K. Li, R. Rajamani, and J. Wang, "Model predictive multi-objective vehicular adaptive cruise control," *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 3, pp. 556–566, May 2011.

[24] G. J. L. Naus, J. Ploeg, M. J. G. Van de Molengraft, W. P. M. H. Heemels, and M. Steinbuch, "Design and implementation of parameterized adaptive cruise control: An explicit model predictive control approach," *Control Eng. Practice*, vol. 18, no. 8, pp. 882–892, 2010.

[25] S. E. Li, Z. Jia, K. Li, and B. Cheng, "Fast online computation of a model predictive controller and its application to fuel economy-oriented adaptive cruise control," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1199–1209, Jun. 2015.

[26] V. L. Bageshwar, W. L. Garrard, and R. Rajamani, "Model predictive control of transitional maneuvers for adaptive cruise control vehicles," *IEEE Trans. Veh. Technol.*, vol. 53, no. 5, pp. 1573–1585, Sep. 2004.

[27] P. Liu and U. Özgüner, "Predictive control of a vehicle convoy considering lane change behavious of the preceding vehicle," in *Proc. IEEE Amer. Control Conf.*, 2015, pp. 4374–4379.

[28] J. Marzbanrad and N. Karimian, "Space control law design in adaptive cruise control vehicles using model predictive control," in *Proc. Inst. Mech. Eng., Part D: J. Automobile Eng.*, vol. 225, no. 7, pp. 870–884, 2011.

[29] F. E. Sancar, B. Fidan, J. P. Huissoon, and S. L. Waslander, "MPC based collaborative adaptive cruise control with rear end collision avoidance," in *Proc. IEEE Intell. Veh. Symp.*, 2014, pp. 516–521.

[30] J. Martinez and C. C. de Wit, "A safe longitudinal control for adaptive cruise control and stop-and-go scenarios," *IEEE Trans. Control Syst. Technol.*, vol. 15, no. 2, pp. 246–258, Mar. 2007.

[31] C.-C. Tsai, S.-M. Hsieh, and C.-T. Chen, "Fuzzy longitudinal controller design and experimentation for adaptive cruise control and stop&go," *J. Intell. Robot. Syst.*, vol. 59, no. 2, pp. 167–189, 2010.

[32] D. Zhao, Z. Hu, Z. Xia, C. Alippi, Y. Zhu, and D. Wang, "Full-range adaptive cruise control based on supervised adaptive dynamic programming," *Neurocomputing*, vol. 125, pp. 57–67, 2014.

[33] S. Moon, I. Moon, and K. Yi, "Design, tuning, and evaluation of a full-range adaptive cruise control system with collision avoidance," *Control Eng. Practice*, vol. 17, no. 4, pp. 442–455, 2009.

[34] F. A. Mullakkal-Babu, M. Wang, B. van Arem, and R. Happee, "Design and analysis of full range adaptive cruise control with integrated collision a voidance strategy," in *Proc. 19th Int. Conf. Intell. Transp. Syst.*, 2016 pp. 308–315.

[35] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems," in *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012.

[36] S. Mitra, T. Wongpiromsarn, and R. M. Murray, "Verifying cyber-physical interactions in safety-critical systems," *IEEE Secur. Privacy*, vol. 11, no. 4, pp. 28–37, Jul./Aug. 2013.

[37] H. Kowshik, D. Caveney, and P. R. Kumar, "Provable systemwide safety in intelligent intersections," *IEEE Trans. Veh. Technol.*, vol. 60, no. 3, pp. 804–818, Mar. 2011.

[38] M. Asplund, A. Manzoor, M. Bouroche, S. Clarke, and V. Cahill, "A formal approach to autonomous vehicle coordination," in *Proc. FM 2012: Formal Methods*, 2012, pp. 52–67.

[39] E. S. Kim, M. Arcak, and S. A. Seshia, "Compositional controller synthesis for vehicular traffic networks," in *Proc. 54th IEEE Conf. Decis. Control*, 2015, pp. 6165–6171.

[40] S. Bouraine, T. Fraichard, and H. Salhi, "Provably safe navigation for mobile robots with limited field-of-views in dynamic environments," *Auton. Robots*, vol. 32, no. 3, pp. 267–283, 2012.

[41] S. Mitsch, K. Ghorbal, and A. Platzer, "On provably safe obstacle avoidance for autonomous robotic ground vehicles," in *Proc. Robot.: Sci. Syst. IX*, 2013.

[42] W. Damm, H. J. Peter, J. Rakow, and B. Westphal, "Can we build it: Formal synthesis of control strategies for cooperative driver assistance systems," *Math. Structures Comput. Sci.*, vol. 23, no. 4, pp. 676–725, 2013.

[43] M. Althoff, D. Althoff, D. Wollherr, and M. Buss, "Safety verification of autonomous vehicles for coordinated evasive maneuvers," in *Proc. IEEE Intell. Veh. Symp.*, 2010, pp. 1078–1083.

[44] M. Althoff and J. M. Dolan, "Online verification of automated road vehicles using reachability analysis," *IEEE Trans. Robot.*, vol. 30, no. 4, pp. 903–918, Aug. 2014.

[45] J. Lygeros, D. N. Godbole, and S. Sastry, "A verified hybrid controller for automated vehicles," in *Proc. 35th Conf. Decis. Control*, 1996, pp. 2289–2294.

[46] J. Lygeros, D. N. Godbole, and S. Sastry, "Verified hybrid controllers for automated vehicles," *IEEE Trans. Autom. Control*, vol. 43, no. 4, pp. 522–539, Apr. 1998.

[47] E. Dolginova and N. Lynch, "Safety verification for automated platoon maneuvers: A case study," in *Proc. Int. Workshop Hybrid Real-Time Syst.*, 1997, pp. 154–170.

[48] L. Alvarez and R. Horowitz, "Safe platooning in automated highway systems part I: Safety regions design," *Veh. Syst. Dyn.*, vol. 32, no. 1, pp. 23–55, 1999.

[49] S. M. Loos, A. Platzer, and L. Nistor, "Adaptive cruise control: Hybrid, distributed, and now formally verified," in *Proc. 17th Int. Symp. Formal Methods*, 2011, pp. 42–56.

[50] S. M. Loos, D. Witmer, P. Steenkiste, and A. Platzer, "Efficiency analysis of formally verified adaptive cruise controllers," in *Proc. 16th Int. IEEE Conf. Intell. Transp. Syst.*, 2013, pp. 1565–1570.

[51] J. Park and Ü. Özgüner, "Model based controller synthesis using reachability analysis that guarantees the safety of autonomous vehicles in a convoy," in *Proc. IEEE Int. Conf. Veh. Electron. Safety*, 2012, pp. 134–139.

[52] O. Stursberg, A. Fehnker, Z. Han, and B. H. Krogh, "Verification of a cruise control system using counterexample-guided search," *Control Eng. Pract.*, vol. 12, no. 10, pp. 1269–1278, 2004.

[53] S. Dai and X. Koutsoukos, "Safety analysis of automotive control systems using multi-modal port-Hamiltonian systems," in *Proc. 19th Int. Conf. Hybrid Syst.: Comput. Control*, 2016, pp. 105–114.

[54] S. W. Smith, P. Nilsson, and N. Ozay, "Interdependence quantification for compositional control synthesis with an application in vehicle safety systems," in *Proc. 55th IEEE Conf. Decis. Control*, 2016, pp. 5700–5707.

[55] S. Sadraddini, S. Sivaranjani, V. Gupta, and C. Belta, "Provably safe cruise control of vehicular platoons," *IEEE Control Syst. Lett.*, vol. 1, no. 2, pp. 262–267, Oct. 2017.

[56] T. Wongpiromsarn, S. Mitra, R. Murray, and A. Lamperski, "Verification of periodically controlled hybrid systems: Application to an autonomous vehicle," *ACM Trans. Embedded Comput. Syst.*, vol. 11, no. S2, pp. 1–24, 2012.

[57] A. D. Ames, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *Proc. 53rd IEEE Conf. Decis. Control*, 2014, pp. 6271–6278.

[58] A. Mehra, W. Ma, F. Berg, P. Tabuada, J. W. Grizzle, and A. D. Ames, "Adaptive cruise control: Experimental validation of advanced controllers on scale-model cars," in *Proc. Amer. Control Conf.*, 2015, pp. 1411–1418.

[59] P. Nilsson *et al.*, "Correct-by-construction adaptive cruise control: Two approaches," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 4, pp. 1294–1307, Jul. 2016.

[60] M. Mazo, A. Davitian, and P. Tabuada, "PESSOA: A tool for embedded controller synthesis," in *Proc. Comput. Aided Verification*, 2010, pp. 566–569.

[61] X. Xu, J. W. Grizzle, P. Tabuada, and A. D. Ames, "Correctness guarantees for the composition of lane keeping and adaptive cruise control," *IEEE Trans. Automat. Sci. Eng.*, vol. 15, no. 3, pp. 1216–1229, Jul. 2018.

[62] R. Mayr and O. Bauer, "Safety issues in intelligent cruise control," in *Proc. IEEE/IEEJ/JSAI Int. Conf. Intell. Transp. Syst.*, 1999, pp. 970–975.

[63] S. Magdici and M. Althoff, "Adaptive cruise control with safety guarantees for autonomous vehicles," in *Proc. 20th World Congr. Int. Federation Autom. Control*, 2017, pp. 5774–5781.

[64] J. Ligthart, E. Semsar-Kazerooni, J. Ploeg, M. Alirezaei, and H. Nijmeijer, "Controller design for cooperative driving with guaranteed safe behavior," in *Proc. IEEE Conf. Control Technol. Appl.*, 2018, pp. 1460–1465.

[65] M. Khaled and M. Zamani, "pFaces: An acceleration ecosystem for symbolic control," in *Proc. 22nd ACM Int. Conf. Hybrid Syst. Comput. Control*, 2019, pp. 252–257.

[66] B. Schürmann, D. Heß, J. Eilbrecht, O. Stursberg, F. Köster, and M. Althoff, "Ensuring drivability of planned motions using formal methods," in *Proc. 20th IEEE Int. Conf. Intell. Transp. Syst.*, 2017, pp. 1–8.

[67] L. L. Hoberock, "A survey of longitudinal acceleration comfort studies in ground transportation vehicles," *J. Dyn. Syst., Meas. Control*, vol. 99, no. 2, pp. 76–84, 1977.

[68] M. Elbanhawi, M. Simic, and R. Jazar, "In the passenger seat: Investigating ride comfort measures in autonomous cars," *IEEE Intell. Transp. Syst. Mag.*, vol. 7, no. 3, pp. 4–17, Fall 2015.

[69] M. Althoff and S. Magdici, "Set-based prediction of traffic participants on arbitrary road networks," *IEEE Trans. Intell. Veh.*, vol. 1, no. 2, pp. 187–202, Jun. 2016.
[70] R. Rajamani, *Vehicle Dynamics and Control*. Berlin, Germany: Springer, 2012.
[71] F. Borrelli, A. Bemporad, and M. Morari, *Predictive Control for Linear and Hybrid Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.
[72] J. Zhou and H. Peng, "Range policy of adaptive cruise control vehicles for improved flow stability and string stability," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 2, pp. 229–237, Jun. 2015.
[73] R. Kianfar, P. Falcone, and J. Fredriksson, "A receding horizon approach for designing string stable cooperative adaptive cruise control," in *Proc. 14th Int. IEEE Conf. Intell. Transp. Syst.*, 2011, pp. 734–739.
[74] N. Deo, A. Rangesh, and M. M. Trivedi, "How would surround vehicles move? A unified framework for maneuver classification and motion prediction," *IEEE Trans. Intell. Veh.*, vol. 3, no. 2, pp. 129–140, Jun. 2018.
[75] J. Schlechtriemen, A. Wedel, J. Hillenbrand, G. Breuel, and K. Kuhnert, "A lane change detection approach using feature ranking with maximized predictive power," in *Proc. IEEE Intell. Veh. Symp.*, 2014, pp. 108–114.
[76] D. Kasper *et al.*, "Object-oriented Bayesian networks for detection of lane change maneuvers," *IEEE Intell. Transp. Syst. Mag.*, vol. 4, no. 3, pp. 19–31, Fall 2012.
[77] A. Rizaldi and M. Althoff, "Formalising traffic rules for accountability of autonomous vehicles," in *Proc. 18th IEEE Int. Conf. Intell. Transp. Syst.*, 2015, pp. 1658–1665.
[78] L. Segel, Tire Traction on Dry, Uncontaminated Surfaces, in *The Physics of Tire Traction.* Berlin, Germany: Springer, 1974, pp. 65–98.
[79] C.-G. Wallman and H. Åström, "Friction measurement methods the correlation between road friction traffic safety," *iVTI meddelande*., Linköping, Sweden Swedish National Road and Transport Research Institute, 2001.
[80] S. Magdici and M. Althoff, "Fail-safe motion planning of autonomous vehicles," in *Proc. 19th Int. IEEE Conf. Intell. Transp. Syst.*, 2016, pp. 452–458.
[81] D. Angeli and E. D. Sontag, "Monotone control systems," *IEEE Trans. Autom. Control*, vol. 48, no. 10, pp. 1684–1698, Oct. 2003.
[82] M. Althoff, D. Heß, and F. Gambert, "Road occupancy prediction of traffic participants," in *Proc. 16th Int. IEEE Conf. Intell. Transp. Syst.*, 2013, pp. 99–105.
[83] A. Lambert, D. Gruyer, B. Vincke, and E. Seignez, "Consistent outdoor vehicle localization by bounded-error state estimation," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, 2009, pp. 1211–1216.
[84] A. Gning and P. Bonnifait, "Constraints propagation techniques on intervals for a guaranteed localization using redundant data," *Automatica*, vol. 42, no. 7, pp. 1167–1175, 2006.
[85] M. Grinberg, F. Ohr, and J. Beyerer, "Feature-based probabilistic data association (FBPDA) for visual multi-target detection and tracking under occlusions and split and merge effects," in *Proc. 12th Int. IEEE Conf. Intell. Transp. Syst.*, 2009, pp. 291–298.
[86] R. Labayrade, C. Royere, D. Gruyer, and D. Aubert, "Cooperative fusion for multi-obstacles detection with use of stereovision and laser scanner," *Auton. Robots*, vol. 19, no. 2, pp. 117–140, 2005.
[87] R. Zetik, M. Eschrich, S. Jovanoska, and R. S. Thoma, "Looking behind a corner using multipath-exploiting UWB radar," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 3, pp. 1916–1926, Jul. 2015.
[88] L. B. Fertig, J. M. Baden, and J. R. Guerci, "Knowledge-aided processing for multipath exploitation radar (MER)," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 10, pp. 24–36, Oct. 2017.
[89] S. Kim *et al.*, "Multivehicle cooperative driving using cooperative perception: Design and experimental validation," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 663–680, Apr. 2015.
[90] S. Kim, W. Liu, M. H. Ang, E. Frazzoli, and D. Rus, "The impact of cooperative perception on decision making and planning of autonomous vehicles," *IEEE Intell. Transp. Syst. Mag.*, vol. 7, no. 3, pp. 39–50, Fall 2015.
[91] M. Althoff and J. M. Dolan, "Reachability computation of low-order models for the safety verification of high-order road vehicle models," in *Proc. Amer. Control Conf.*, 2012, pp. 3559–3566.
[92] H. Roehm, J. Oehlerking, M. Woehrle, and M. Althoff, "Reachset conformance testing of hybrid automata," in *Proc. Hybrid Syst.: Comput. Control*, 2016, pp. 277–286.
[93] M. Frank and P. Wolfe, "An algorithm for quadratic programming," *Naval Res. Logistics Quart.*, vol. 3, pp. 95–110, 1956.
[94] M. Althoff, M. Koschi, and S. Manzinger, "CommonRoad: Composable benchmarks for motion planning on roads," in *Proc. IEEE Intell. Veh. Symp.*, 2017, pp. 719–726.
[95] D. Freedman, R. Pisani, and R. Purves, *Statistics*. New York, NY, USA: Norton, 2007.

Matthias Althoff is an Associate Professor in Computer Science at the Technical University of Munich, Germany. He received his diploma engineering degree in Mechanical Engineering in 2005, and his Ph.D. degree in Electrical Engineering in 2010, both from the Technical University of Munich, Germany. He is an Associate Professor in Computer Science at the Technical University of Munich, Germany. From 2010 to 2012 he was a Postdoctoral Researcher at Carnegie Mellon University, Pittsburgh, USA, and from 2012 to 2013 an Assistant Professor at Technische Universität Ilmenau, Germany. His research interests include the formal verification of continuous and hybrid systems, reachability analysis, planning algorithms, nonlinear control, automated vehicles, and power systems.

Sebastian Maierhofer is currently a Ph.D. candidate at the Technical University of Munich in the Cyber-Physical Systems Group. He received a B.Sc. degree in Technical Computer Science from the University of Applied Science Regensburg, Germany, in 2016.

He graduated with a M.Sc. degree in Automotive Software Engineering from the Technical University of Munich, Germany, in 2019. His research interests include the formalization of traffic rules, motion planning considering traffic rules, and the falsification of motion planners.

Christian Pek has been a researcher in the Cyber-Physical Systems Group at the Technical University of Munich under Prof. Dr.-Ing. Matthias Althoff since 2015. He was a research assistant in the motion planning group at the BMW Group Autonomous Driving Department from 2015 until 2019. Christian graduated with an M.Sc. in Computer Science and Robotics from the Technical University of Braunschweig, Germany, and the University of Auckland, New Zealand, in 2015.

His vision is a future of robots which robustly and safely accomplish tasks with and around humans. Currently, Christian's research focuses on safe motion planning for mobile robots, in particular automated vehicles.