IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 June 2023, accepted 20 July 2023, date of publication 1 August 2023, date of current version 5 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3300423

APPLIED RESEARCH

Online Safety Verification of Autonomous Driving Decision-Making Based on Dynamic Reachability Analysis

FEI GAO[1], CHENG LUO[2], FANGYUAN SHI[3], XIANQING CHEN[3], ZHENHAI GAO[1], AND RUI ZHAO[1], (Member, IEEE)

[1]State Key Laboratory of Automotive Simulation and Control, Jilin University, Changchun, Jilin 130025, China
[2]School of Automotive Studies, Tongji University, Shanghai 201804, China
[3]Chongqing Chang'an Automobile Company Ltd., Chongqing 400023, China

Corresponding author: Rui Zhao (rzhao@jlu.edu.cn)

This work was supported by the National Science Foundation of China under Grant 52202494 and Grant 52202495.

ABSTRACT Addressing decision safety in the unpredictable arena of complex traffic scenarios represents a significant hurdle for autonomous driving systems. Considering the inherent spatial-temporal uncertainties associated with the future actions of surrounding traffic participants, real-time safety verification of autonomous driving decisions is crucial to maintaining vehicular safety. Existing online verification methodologies, such as Responsibility Sensitive Safety (RSS) and Safety Force Field (SFF), ensure driving safety by formalizing human safe-driving rules and constraining the vehicle to maintain safe lateral and longitudinal distances in real-time. While these methods effectively prevent collisions instigated by the autonomous vehicle itself, they lack sufficient foresight and often result in less smooth driving trajectories. To address these limitations, we propose an innovative, interpretable, formal safety verification framework. This approach integrates both explicit and implicit traffic rules to anticipate all legally acceptable transitions of traffic scenarios. It builds the lawful, short-term reachable region for each vehicle, and verifies the safety of autonomous vehicle decisions by assessing whether the regions these vehicles inhabit, in accordance with the expected trajectory, overlap with the accessible zones of other vehicles. Furthermore, in scenarios presenting potential danger, a backup smooth safety trajectory is derived from the autonomous vehicle's legal reachability domain as a preventive measure to degrade safety threats. As a cornerstone of safety for autonomous vehicles, our proposed method ensures a continual safe trajectory in all traffic scenarios, provided that other participants adhere to traffic rules. Experimental outcomes, grounded in the ISO 34502 standard and real-world critical safety scenarios, demonstrate the method's efficacy in identifying potentially dangerous decisions and mitigating autonomous vehicle-induced traffic accidents.

INDEX TERMS Autonomous driving, online safety verification, reachability analysis, decision planning, alternate safety trajectory.

I. INTRODUCTION

While autonomous driving technology promises to eliminate human error, augment traffic safety, enable mobility for the disabled, alleviate traffic congestion, and significantly enhance the future transportation system's intelligence, the technology in its current form struggles to ensure safe driving under all weather and scenario conditions. The perception and decision-making functionalities of autonomous driving systems exhibit certain limitations in dense and complex traffic scenarios and extreme weather conditions, leading to potentially unsafe driving strategies [1]. These strategies not only pose serious threats to the lives and property of drivers and associated parties, but also provoke a crisis of public

The associate editor coordinating the review of this manuscript and approving it for publication was Cinzia Bernardeschi.

confidence, thus, impeding the broader adoption of autonomous driving technology. To ensure that the autonomous vehicle can skillfully and safely respond to any intricate traffic scenarios encountered in real-world conditions, and to prevent such vehicles from actively causing accidents, it is critical to rigorously verify the safety of decisions produced by autonomous driving systems.

Currently, most safety verification of such decision-making systems is conducted offline, predominantly relying on simulation and actual vehicle verification methodologies [2]. Real-road vehicle safety verification primarily employs statistical principles to assert that autonomous vehicles are statistically safer than their human-driven counterparts, with one evaluative metric being the disengagement rate [3]. While this methodology is effective, it still harbors limitations. Firstly, to prove that the safety of autonomous vehicles matches or exceeds that of human-driven vehicles, these vehicles are required to maintain an accident-free record over an astounding distance of 240 million kilometers [4]. This stipulation significantly extends the verification period. Secondly, ensuring that any updates to the algorithms will not introduce new accidents within the mileage already tested presents a complex task. Consequently, this real-vehicle safety verification method encounters a bottleneck in persistently guaranteeing the safety of autonomous driving decision-making.

Simulation-based safety verification for autonomous driving harnesses model-in-the-loop, hardware-in-the-loop, and vehicle-in-the-loop testing [5], [6]. Model-in-the-loop testing mandates that autonomous driving algorithms demonstrate a safety performance akin to human-operated vehicles [7]. Hardware-in-the-loop testing encompasses continuous, combination, and scalability testing [8]. Closed-field vehicle-in-the-loop and hub-and-spoke platform vehicle-in-the-loop are primarily used in vehicle-in-the-loop testing [9]. Yet, these methods struggle with replicating dense, dynamic, and complex traffic scenarios reflecting real-world conditions. Researchers have made attempts to address this. Zhao et al. [10] created lane change models based on extensive natural driving data, facilitating more rapid evaluation of autonomous vehicle performance through estimating conflict, collision, and injury rates. Li et al. [11] and Sinha et al. [12] leveraged simulation engines and exploration techniques, respectively, to generate safety verification scenarios. Feng et al. [13] employed deep reinforcement learning to train background vehicles via neural networks, thus crafting an AI-based adversarial testing environment that drastically reduces necessary test miles. Despite these advancements, challenges persist. Validating the accuracy of these virtual environments in reproducing realistic traffic scenarios remains difficult, as does confirming the consistency of autonomous decision-making error rates between virtual and real environments. Moreover, these approaches predominantly rely on offline data, such as position velocity of the autonomous vehicle and other vehicles, for performance evaluation. This limits their capacity for online correction of decision algorithms, posing a potential risk to maintaining strict safety standards [14], [15].

Online verification, as a supplement to offline methods, can authenticate the real-time safety of autonomous vehicles. Prevalent online verification approaches include Mobileye's Responsibility Sensitive Safety (RSS) model and Nvidia's Safety Force Field (SFF) model. Oboril and Scholl [16] fused an online driving risk assessment methodology with RSS to estimate the potential for accidents via a risk model, subsequently expanding RSS [17] to evaluate all safety scenarios based on the probable future actions of other traffic participants. They further calculated and assessed whether the associated collision risk value was sufficiently low to evaluate vehicular safety. Several researchers [18], [19], [20], [21] have sought to refine RSS parameter ranges based on physical constraints, legal requirements, and human driving behavior, to enhance the practicality of RSS models. Pasch et al. [22] conducted an extensive parameter assessment of vulnerable road users within the RSS scope, illustrating how RSS parameter values significantly influence the model's usability. However, these methodologies, while based on predefined driving rules such as maintaining a safe distance, can only verify whether the vehicle's state meets the established rules at a given moment. They fail to guarantee the safety of the vehicle's continuous trajectory and do not propose alternative strategies to guide the vehicle into a safe state.

A number of studies have sought to authenticate the safety of autonomous vehicle trajectories based on the reachability analysis of traffic participants. Koschi et al. [23] scrutinized pedestrian reachability, while Althoff and Magdici [24] computed the reachable regions of surrounding traffic participants predicated on acceleration and lane-following reachability. Manzinger et al. [25] amalgamated reachability analysis with a trajectory planner to compute driving corridors and trajectories online. Pek et al. [26] incorporated reachability analysis to evaluate the legality and safety of the ego vehicle's expected trajectory, providing an alternative trajectory in hazardous situations. However, these methodologies inadequately account for implicit traffic rules, such as social interaction information and road rights information pertinent to cooperative driving. As such, these approaches do not effectively correspond to cooperative driving in real-world road conditions and neglect factors such as road signs or temporary traffic restrictions present in actual traffic environments. They remain ill-equipped to handle the shifting road environment in the real world. Concurrently, these methods overlook the occupancy rate engendered by the size of the ego vehicle on the expected trajectory, resulting in an overestimation of the safety of the ego vehicle's anticipated trajectory.

In an endeavor to bridge the gaps outlined above, we present a formalized, online safety verification methodology for autonomous driving decision-making. This approach acts as a safety foundation for the existing motion planning layer, combining explicit, and implicit traffic regulations to

formally predict the legal reachable region for traffic participant vehicles. Subsequently, it verifies the safety of the vehicle's anticipated trajectory and provides an alternative safe trajectory. Through real-time online verification, this method corrects autonomous driving decisions, displaying a robust generalization ability to adapt to all traffic scenarios. The primary contributions can be summarized as follows:

1. Firstly, our method holistically amalgamates both explicit and implicit traffic regulations to calculate the reachable regions for our vehicle and surrounding traffic participants. It verifies in real-time and continuously if the space occupied by the ego vehicle intersects with the reachable regions of other traffic participant vehicles. This process aids in evaluating the safety of the trajectory produced by the decision-making layer and helps avoid dangerous situations. The calculation of reachable regions takes into account regulations tied to road traffic, vehicle motion, and cooperative driving, allowing the derived reachable regions to adapt to changing road environments. Furthermore, these rules are reusable, scalable, and can be generalized to all traffic scenarios.

2. Secondly, our approach can generate redundant and smooth alternative safety trajectories based on the ego vehicle's legal reachable region. These trajectories serve as fallback safety measures in precarious situations, ensuring the strict safety standards of the vehicle's journey.

3. Thirdly, we conducted extensive experiments to demonstrate the effectiveness and real-time performance of the proposed method. According to the ISO 34502 test scene standard for autonomous driving systems and the real-world critical safety events, six random hazardous scenarios were constructed for simulation analysis. The results indicate that our method utilizes minimal computational resources while displaying robust real-time performance. It can complete the safety verification of the expected trajectory and generate a smooth alternative safety trajectory promptly, ensuring the vehicle's driving safety while maximizing comfort.

The remainder of this paper is structured thusly: Section II delineates the model and system problematics; Section III elucidates the paper's framework; Section IV introduces safety verification of the expected trajectory, rooted in a reachable region, and explicates the derivation of an alternate safety trajectory; Section V outlines the experimental design and reports the resulting data; the manuscript culminates in Section VI, which presents the conclusion.

II. SYSTEM MODELING AND PROBLEM FORMULATION

A. VEHICLE AND ROAD MODELING

Vehicle classifications consist of ego vehicle and those participating in traffic, the latter of which are subdivided into motorized and non-motorized categories as illustrated in Fig. 1. Employing a point-mass model, all vehicles are accounted for, incorporating a degree of measurement uncertainty. The ego vehicle is conceptualized as a rectangle defined by length l_{ego} and width w_{ego}, with the reference point

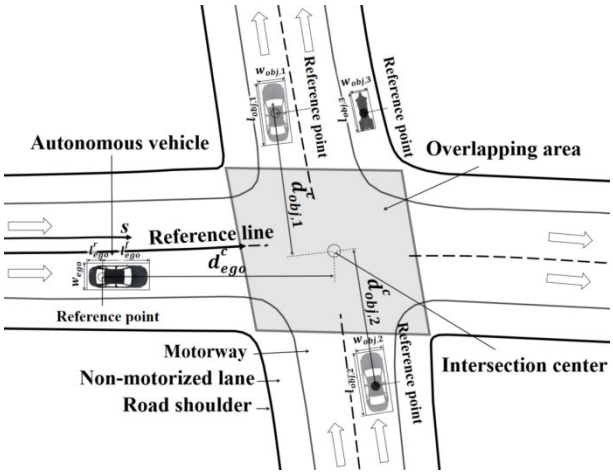


FIGURE 1. Schematic of vehicle and road models.

situated at the rear axle's center. The rectangle's front end maintains a distance l_{ego}^{f} from this reference point, while the distance from the rear end is denoted as l_{ego}^{r}. The $i(i = 1, 2, \ldots, N_{obj})$ traffic participant is characterized by a rectangular model with length $l_{obj,i}$ and width $w_{obj,i}$, its reference point being the rectangle's center. We define the vehicle's kinematic model using a second-order integrator:

$$\begin{bmatrix} p_x \\ p_y \end{bmatrix} = \begin{bmatrix} p_{x,0} \\ p_{y,0} \end{bmatrix} + \begin{bmatrix} v_{x,0} \\ v_{y,0} \end{bmatrix} (t - t_0) + \frac{1}{2} \begin{bmatrix} a_{x,0} \\ a_{y,0} \end{bmatrix} (t - t_0)^2 \tag{1}$$

where p_x and p_y represent the X and Y coordinates of the vehicle reference point at time t, while $p_{x,0}$ and $p_{y,0}$ correspond to the x and y coordinates of the same point at time t_0. Similarly, $v_{x,0}$ and $v_{y,0}$ denote the velocities in the x and y directions, respectively, of the vehicle reference point at time t_0. The terms $a_{x,0}$ and $a_{y,0}$ stand for the accelerations in the x and y directions of the vehicle reference point at time t_0.

Roads are bifurcated into non-overlapping and overlapping categories: non-overlapping roads consist solely of a primary thoroughfare without subsidiary lanes or intersections, while overlapping roads incorporate branching lanes and intersecting areas. The overlap area is defined as the intersection of each subsidiary lane, its centroid taken as the confluence of the centre lines of each branch. The distance from the ego vehicle to this centroid is denoted as d_{ego}^{c}, and the corresponding distance from the i^{th} traffic participant is represented by $d_{obj,i}^{c}$. Roadway typologies encompass motorways, non-motorways, and shoulders. For any given lane, it is presumed that the lane centreline, along with its left and right boundaries, constitute smooth directed curves. Furthermore, the lane centreline is assumed parallel to the left and right boundary lines of the lane, both of which comprise a series of n_{arc} segments.

Within the Frenet coordinate system, the lane centreline serves as the reference line with the lane width symbolized as w_{lane}. The unit normal vector at the reference line position s is denoted as $r^{\perp}(s)$, while the tangential angle corresponding to

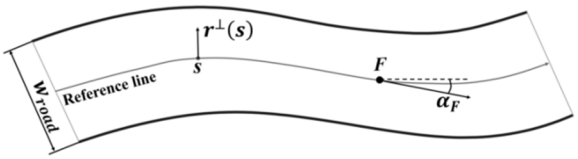


FIGURE 2. Depiction of lane model.

the reference line at point F is α_F, as illustrated in Fig. 2. The set comprising all points enclosed within the lane boundary R is represented as:

$$R = \{r(s) + \gamma w_{lane} r^{\perp}(s) | s \in [s_{min}, s_{max}], \gamma \in [-\frac{1}{2}, \frac{1}{2}]\} \quad (2)$$

In this context, $r(s)$ represents the point corresponding to the reference line position s. The variable γ is a scalar factor ensuring all points are constrained within the lane boundary, with a range of defined values. The parameters s_{min} and s_{max} respectively represent the minimum and maximum magnitudes of the lane reference line lengths. Our approach to road modelling is aligned with the road network standards proposed by OpenDRIVE [27].

B. FORMALIZATION OF TRAFFIC REGULATIONS

To ensure the unambiguous safety compliance of ego vehicle, we articulate the constraints posed by both explicit and implicit traffic regulations on each participant in traffic. Explicit traffic regulations encompass legally mandated rules governing vehicular behavior, whereas implicit traffic regulations pertain to norms typically observed by seasoned drivers, yet not officially codified in regulatory statutes. As delineated in Table 1, constraints on individual traffic participants are categorized into three broad classifications: those related to road traffic, vehicle movement, and cooperative driving.

C. PROBLEM DEFINITION

The issue of real-time safety verification for autonomous driving decision-making premised on dynamic reachability domain can be defined as follows: In each verification cycle, this study computes the accessibility of other vehicles participating in traffic, guided by the established vehicle and road models, along with explicit and implicit traffic regulations. This process relies on comparing the area encompassed by the ego vehicle's anticipated trajectory to the space occupied by the expected trajectories of others. The safety of the ego vehicle's predicted trajectory is assessed based on the presence or absence of overlap between these areas. Furthermore, the legally reachable region for the ego vehicle is calculated, contingent upon the reachability regions of other traffic participants, to derive an alternate safe trajectory. The success of this alternate safety trajectory generation is contingent upon whether the area it occupies falls within the ego vehicle's lawful reachability region. Ultimately, the safety of the anticipated trajectory and the successful generation of an alternate safe trajectory dictate the trajectory of the ego vehicle in the subsequent verification cycle.

TABLE 1. Restrictions imposed on traffic participants.

Restriction	Sign	Description
Road traffic related restrictions	$R_{road\_boundary}$	Prohibition of vehicles from driving outside the boundaries of the road allowed by traffic regulations, such as driving outside the solid line of the lane.
	R_{road_permit}	Vehicles should drive within the drivable area guided by road signs or temporary traffic restrictions.
	$R_{cautious\_driving}$	Under adverse driving conditions, vehicles should drive cautiously, with a speed not exceeding $v_{max}^{cautious}$ and an acceleration not exceeding $a_{max}^{cautious}$.
Vehicle motion-related restrictions	$R_{velocity}$	The vehicle's speed should not exceed $min\{v_{max}^{road}, v_{max}^{mot}\}$, where v_{max}^{road} is the maximum speed allowed by the road and v_{max}^{mot} is the maximum speed allowed by the vehicle's kinematics.
	$R_{acceleration}$	Vehicle acceleration not to exceed a_{max}.
Co-driving related restrictions	$R_{safe\_distance}$	Vehicles should maintain a suitable longitudinal safety distance with the preceding vehicles in the same lane and maintain a suitable longitudinal safety distance with the vehicles on the target lane when changing lanes.
	R_{road_right}	Vehicles must give way to other vehicles that have the right of way.

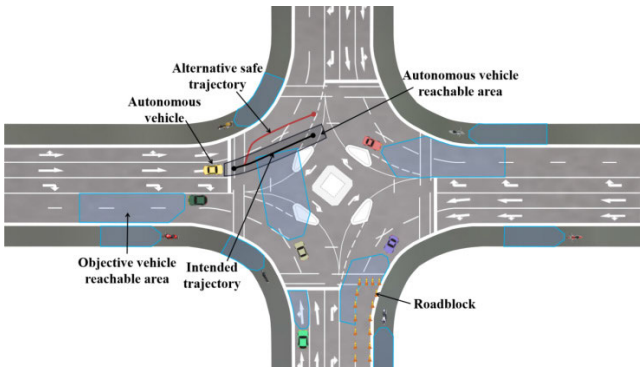


FIGURE 3. Schematic representation of online safety verification.

III. PROCEDURE FOR ONLINE SAFETY VERIFICATION METHOD

The proposed online safety verification method ensures the safety across consecutive verification cycles. This section explains the verification procedure as illustrated in Fig. 3 to Fig. 5. The intended path (represented by a black line) from the ego vehicle's trajectory planner is evaluated for possible intersections with the reachable zones (shown as blue areas) of other traffic entities. In case of a potential hazard, an alternate safe trajectory (depicted by a red line) will be employed

The i^{th} traffic participant's attainable regions encompass: the roadway-related region $\mathcal{A}_{road,i}(t_k, t_{k+1})$ (the green area in Fig. 4a), the vehicular motion-related region $\mathcal{A}_{mot,i}(t_k, t_{k+1})$ (the orange area in Fig. 4b), and the cooperative driving-related region $\mathcal{A}_{coop,i}(t_k, t_{k+1})$ (the blue area in Fig. 4c). The comprehensive attainable region $\mathcal{A}_{obj,i}(t_k, t_{k+1})$ (the area circumscribed by the blue line in Fig. 4d), is the

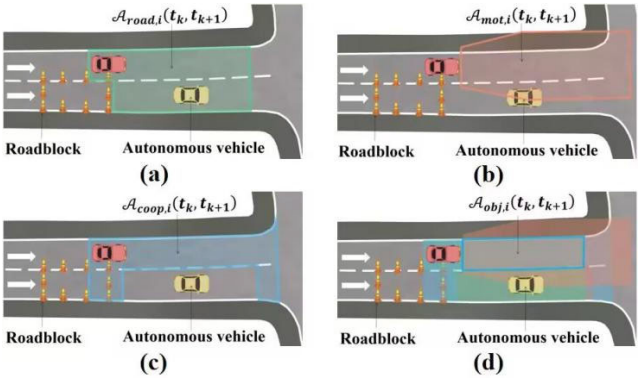


FIGURE 4. Illustration of regions of additional traffic participants: (a) the roadway-related region $\mathcal{A}_{road,i}(t_k, t_{k+1})$, (b) the vehicular motion-related region $\mathcal{A}_{mot,i}(t_k, t_{k+1})$, (c) the cooperative driving-related region $\mathcal{A}_{coop,i}(t_k, t_{k+1})$, (d) the comprehensive attainable region $\mathcal{A}_{obj,i}(t_k, t_{k+1})$.

intersection of these three regions. The collective region $\mathcal{A}_{obj}(t_k, t_{k+1})$ can be derived by concatenating the regions of each traffic participant:

$$\mathcal{A}_{obj}(t_k, t_{k+1}) = \bigcup \mathcal{A}_{obj,i}(t_k, t_{k+1}) \tag{3}$$

The expected trajectory within the interval $[t_k, t_{k+1}]$, denoted as TR_k^{intend}, is verified as safe (TR_k^{safe}) before time t_k. To prevent the deployment of an unsafe path after time t_{k+1}, a continuous alternative safe trajectory TR_k^{alter} is provided, forming a composite trajectory $TR_k^{safe}|TR_k^{alter}$. If both TR_k^{intend} and TR_k^{alter} are successfully verified prior to time t_k, the composite trajectory is deemed valid, thus permitting the ego vehicle to transition into automatic mode and initiate the execution of TR_k^{safe}, as demonstrated in Fig. 5 for validation cycles $i = 1$ and $i = 2$. If the trajectory remains unverified at time t_k, as shown for cycles $i = 3$ and $i = 4$ in Fig. 5, the vehicle continues on the previously verified trajectory $TR_{k-c}^{alter}(0 < c < k)$ until a new valid path emerges. If the duration t_e of the currently active alternate safe trajectory satisfies the condition $t_a \le t_e \le t_b$ (where t_a and t_b are constants and $0 < t_a \le t_b \le T_{alter}$), a legally reachable region from the vehicle at a specific time is computed to generate an alternate safe trajectory for duration T_{alter}. If the vehicle is unable to generate an alternate safe trajectory and $t_e < t_a$, considering the constraint $R_{safe\_distance}$, a path that ensures legal safety is established along the vehicle's current lane centerline, involving maximum deceleration. This pathway is recorded as the subsequent alternate safe trajectory TR_k^{alter}.

IV. ONLINE SAFETY VERIFICATION METHOD BASED ON REACHABILITY ANALYSIS

A. PREDICTION OF REGIONS FOR TRAFFIC PARTICIPANTS

We categorize the region $\mathcal{A}_{obj,i}(t_k, t_{k+1})$ of the i^{th} traffic participant vehicle within the time interval $[t_k, t_{k+1}]$ into three types according to the primary constraints delineated in the traffic statute formalism: the road-traffic-associated region $\mathcal{A}_{road,i}(t_k, t_{k+1})$, vehicle movement-related region

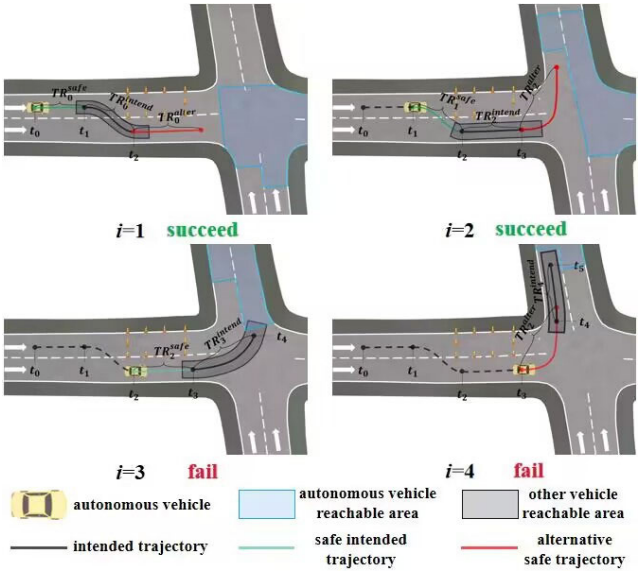


FIGURE 5. Timeline for generation of alternate safety trajectories.

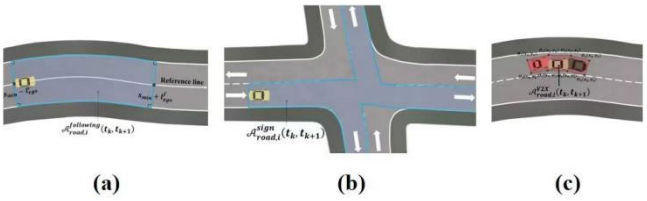


FIGURE 6. Regions in relation to road traffic: (a) the lane-following-based region $\mathcal{A}^{following}_{road,i}(t_k, t_{k+1})$, (b) the road-signage-based region $\mathcal{A}^{sign}_{road,i}(t_k, t_{k+1})$, (c) the V2X cooperation-based region $\mathcal{A}^{V2X}_{road,i}(t_k, t_{k+1})$.

$\mathcal{A}_{mot,i}(t_k, t_{k+1})$, and cooperative driving-related region $\mathcal{A}_{coop,i}(t_k, t_{k+1})$. These three types of regions are derived from the stipulations set forth in the traffic statute formalism.

$$\mathcal{A}_{obj,i} = \mathcal{A}_{road,i} \cap \mathcal{A}_{mot,i} \cap \mathcal{A}_{coop,i} \tag{4}$$

The three methodologies we have proposed for region calculation ensure an over approximation of the results. That is, the calculated region surpasses the actual region, thereby strictly verifying the potential for collision between the ego vehicle and other traffic participants. This approach eradicates the possibility of missed detection, thus ensuring the safety of the anticipated trajectory of the ego vehicle.

1) REACHABILITY PERTAINING TO ROAD TRAFFIC

Road-traffic-associated regions $\mathcal{A}_{road,i}(t_k, t_{k+1})$ are contingent upon road geometry, traffic signs, and real-time status. These encompass lane-following-based regions $\mathcal{A}^{following}_{road,i}(t_k, t_{k+1})$, road-signage-based regions $\mathcal{A}^{sign}_{road,i}(t_k, t_{k+1})$, and Vehicle-to-Everything (V2X) cooperation-based regions $\mathcal{A}^{V2X}_{road,i}(t_k, t_{k+1})$, as depicted in Fig. 6.

$$\mathcal{A}_{road,i} = \mathcal{A}^{following}_{road,i} \cap \mathcal{A}^{sign}_{road,i} \bigcap \mathcal{A}^{V2X}_{road,i} \tag{5}$$

The lane-following reachable region $\mathcal{A}_{road,i}^{following}(t_k, t_{k+1})$ primarily considers the influence of the lane boundary constraint $R_{road\_boundary}$ and the vehicle's speed $R_{velocity}$. By imposing the lane boundary constraint along the lane's shortest path, we ensure the maximum possible travel distance is equivalent to or exceeds the vehicle's actual travel distance. Once the maximum travel distance is established, the vehicle is assumed capable of reaching any point within the perpendicular lane boundaries, resulting in a hyper- approximate estimation of the lane-following reachable region. We determine the minimal travel path through a given road segment under the principle of lane network, as depicted in Figure 6(a). In the Frenet coordinate system, the lane's centerline serves as the reference line, with ξ_{s_F} representing the shortest path length at s_F on the reference line. Here, s_F is the reference line's length at point F, while $|\Delta\alpha(s)|$ reflects the absolute alteration in the reference line's tangential angle corresponding to the reference line length s. Consequently, we derive:

$$\xi_{s_F} = s_F - \frac{w_{lane}}{2}\int_0^{s_F} |\Delta\alpha(s)|\, ds \tag{6}$$

The shortest path ξ corresponds to s, thus $s = f(\xi)$. Considering the constraint $R_{velocity}$, assume the furthest reachable distance by other traffic participants within the time interval $[t_k, t_{k+1}]$ is d_{max}. Consequently, the current location s_0 of these traffic participants corresponds to the shortest path ξ_0, and their furthest reachable location s_{max} aligns with the shortest path ξ_{max}. These should satisfy the following equation:

$$\xi_{max} = \xi_0 + d_{max} \tag{7}$$

Thus, we set $s_{max} = f(\xi_{max})$ and, in order to overestimate $\mathcal{A}_{road,i}^{following}(t_k, t_{k+1})$, we set $s_{min} = s_0$. Accounting for the dimensions of the ego vehicle, the construction of a polygon perpendicular to the corresponding lane boundaries between $s_{min} - l_{ego}^{r}$ and $s_{max} + l_{ego}^{f}$ within the lane yields the region $\mathcal{A}_{road,i}^{following}(t_k, t_{k+1})$ pertaining to the lane under consideration.

Therefore, the region $\mathcal{A}_{road,i}^{sign}(t_k, t_{k+1})$ that corresponds to relevant road signs takes into consideration constraints R_{road_permit}, such as lane markings, turn signals, or roadblocks. Each traffic participant is expected to follow the guidance of these road signs and remain within the designated area. We obtain information about permissible lanes based on the directives of these road signs, as depicted in Fig. 6(b). By constructing corresponding polygons along the boundaries of these permissible lanes, we can generate the region that is pertinent to these road signs.

V2X warning messages serve as indicators of non-navigable sectors on the road network, which may include regions compromised by traffic accidents or ongoing construction activities. As delineated in Fig. 6(c), V2X technology is employed to accrue information regarding these non-navigable polygonal regions $O(O_1, O_2, \ldots, O_{n^{pol}})$, subsequently projecting this data onto the spatial domain.

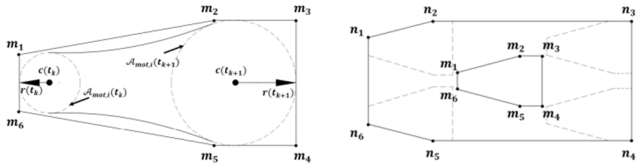


FIGURE 7. Diagram of regions for movement of other traffic participants: (a) without accounting for vehicle size, (b) with consideration of vehicle size.

Thus, the intended depiction of the unreachable region $\mathcal{A}_{road,i}^{V2X}(t_k, t_{k+1})$ within this spatial domain can be deduced through the lens of V2X intelligence.

2) REACHABILITY RELATIVE TO VEHICLE MOTION

The feasible region $\mathcal{A}_{mot,i}(t_k, t_{k+1})$ associated with vehicular motion is contingent upon the vehicle's intrinsic physical and dynamical characteristics, primarily focusing on the constraint $R_{acceleration}$, which signifies the maximum achievable acceleration a_{max}. This realm is derived from the vehicle's physical schema incorporating maximal acceleration data and vehicular geometry; it also takes into account the most recent measured state of the vehicle, encompassing positional information p_0, directional heading H_0, and speed v_0. Consequently, the feasible motion region $\mathcal{A}_{mot,i}(t_k, t_{k+1})$ for the vehicle within a specified time frame is computable. Presuming $p_{x,0} = 0, p_{y,0} = 0, v_{x,0} = v_0, v_{y,0} = 0$ for other vehicles participating in traffic, the feasible region for the reference point at time $[t_k, t_{k+1}]$ is delineated by a circle with center $c(t)$ and radius $r(t)$ [24], as visually represented in Fig. 7(a):

$$c(t) = \begin{bmatrix} p_{x,0} \\ p_{y,0} \end{bmatrix} + \begin{bmatrix} v_{x,0} \\ v_{y,0} \end{bmatrix} \mathrm{t}, r(t) = \frac{1}{2} a_{max} t^2 \tag{8}$$

The boundary delimiting the reachable region is characterized by the two-dimensional function $\left[b_x(t), b_y(t)\right]^T$, where:

$$b_x(t) = v_0 t - \frac{a_{max}^2 t^3}{2v_0},\ b_y(t) = \sqrt{\frac{1}{4} a_{max}^2 t^4 - \left(\frac{a_{max}^2 t^3}{2v_0}\right)^2} \tag{9}$$

The feasible region for other traffic-engaged vehicles within a specified time interval $[t_k, t_{k+1}]$ is demarcated by two circles and a concave boundary at instances t_k and t_{k+1}. A convex hexagon $M(m_1, \ldots, m_6)$, as depicted in Fig. 7(a) by points, can serve as an overestimation of the occupancy zone, disregarding the scale of the vehicle, to provide a conservative approximation of this region:

$$m_1 = \left[c_x(t_k) - r(t_k), c_y(t_k) + r(t_k)\right]^{\mathrm{T}} \tag{10a}$$
$$m_2 = \left[b_x(t_k), c_y(t_{k+1}) + r(t_{k+1})\right]^{\mathrm{T}} \tag{10b}$$
$$m_3 = \left[c_x(t_{k+1}) + r(t_{k+1}), c_y(t_{k+1}) + r(t_{k+1})\right]^{\mathrm{T}} \tag{10c}$$
$$m_4 = \left[c_x(t_{k+1}) + r(t_{k+1}), c_y(t_{k+1}) - r(t_{k+1})\right]^{\mathrm{T}} \tag{10d}$$
$$m_5 = \left[b_x(t_k), c_y(t_{k+1}) - r(t_{k+1})\right]^{\mathrm{T}} \tag{10e}$$

$$m_6 = \left[c_x(t_k)-r(t_k), c_y(t_k)-r(t_k)\right]^{\mathrm{T}} \tag{10f}$$

When accounting for vehicle dimensions within the feasible region, the precise region $\mathcal{A}_{mot,i}(t_k, t_{k+1})$, can be conservatively estimated via an encompassing hexagonal region denoted by $N(n_1, \ldots, n_6)$ as presented in Fig. 7(b), whereby:

$$n_1 = m_1 + \frac{1}{2}\left[-l_{obj,i}, w_{obj,i}\right]^{\mathrm{T}} \tag{11a}$$

$$n_2 = m_2 + \frac{1}{2}\left[-l_{obj,i}, w_{obj,i}\right]^{\mathrm{T}} \tag{11b}$$

$$n_3 = m_3 + \frac{1}{2}\left[l_{obj,i}, w_{obj,i}\right]^{\mathrm{T}} \tag{11c}$$

$$n_4 = m_4 + \frac{1}{2}\left[l_{obj,i}, -w_{obj,i}\right]^{\mathrm{T}} \tag{11d}$$

$$n_5 = m_5 + \frac{1}{2}\left[-l_{obj,i}, -w_{obj,i}\right]^{\mathrm{T}} \tag{11e}$$

$$n_6 = m_6 + \frac{1}{2}\left[-l_{obj,i}, -w_{obj,i}\right]^{\mathrm{T}} \tag{11f}$$

The aforementioned derivation presumes a specific relative position and orientation of other vehicles in traffic with respect to the subject. To facilitate the derivation of an acceleration-based feasible region for any conceivable scenario, this acceleration-centered feasible area is subsequently rotated and transformed in alignment with the authentic initial position and orientation of the other vehicles engaged in traffic. Under adverse weather conditions, the $R_{cautious\_driving}$ constraint ought to be observed, thereby adjusting the vehicle's maximum velocity to $v_{max}^{cautious}$ and the absolute acceleration to $a_{max}^{cautious}$.

3) REACHABILITY ASSOCIATED WITH CO-DRIVING BEHAVIOR

The region $\mathcal{A}_{coop,i}(t_k, t_{k+1})$ associated with vehicle co-driving is determined jointly by the participating vehicles, mainly considering the region $\mathcal{A}_{coop,i}^{dist}(t_k, t_{k+1})$ associated with safe distance unreachable and the region $\mathcal{A}_{coop,i}^{right}(t_k, t_{k+1})$ associated with the right of way. The right-of-way regions and the complement of the relevant safe distance unreachable areas are intersected to obtain the regions associated with vehicle coordination:

The cooperative feasible region $\mathcal{A}_{coop,i}(t_k, t_{k+1})$ associated with vehicular co-driving is ascertained collectively by engaged vehicles, primarily focusing on the safe distance unattainable region $\mathcal{A}_{coop,i}^{dist}(t_k, t_{k+1})$ and the feasible region associated with right-of-way $\mathcal{A}_{coop,i}^{right}(t_k, t_{k+1})$. The intersection of the right-of-way feasible regions and the complement of pertinent safe distance unattainable regions yields the feasible areas associated with vehicular coordination:

$$\mathcal{A}_{coop,i}(t_k, t_{k+1}) = \mathcal{A}_{coop,i}^{right}(t_k, t_{k+1}) \cap \mathcal{A}_{coop,i}^{dist}(t_k, t_{k+1}) \tag{12}$$

Traffic regulations mandate the maintenance of an adequate safe distance between adjacently positioned vehicles, also stipulating that lane transitions must not imperil trailing traffic. Given that $v_{r,0}$ and $v_{f,0}$ represent the initial velocities of the following and leading vehicles respectively, and δ symbolizes the reaction delay time — the interval between the leading vehicle's complete halt from its initial state and the following vehicle's full brake application — we refer to the longitudinal safety distances dictated by the RSS model. In order to secure an overestimated feasible region $\mathcal{A}_{coop,i}(t_k, t_{k+1})$ the corresponding safety distance unattainable area $\mathcal{A}_{coop,i}^{dist}(t_k, t_{k+1})$ is deemed an underestimation. Acknowledging that the reaction time of an autonomous vehicle is comparatively shorter than that of a human, we suitably underestimate the safety distance by assigning the human driver's reaction time $\delta_{human} = 0.5$s and the autonomous vehicle reaction time $\delta_{vehicle}$ within the range of 0 to δ_{human}. The presupposition being that the trailing vehicle reacts promptly to decelerate and brake, maintaining the maximal braking deceleration rate throughout, the safety distance, disregarding the area occupied by the vehicle, is computed in (13), as shown at the bottom of the next page.

As depicted in Fig. 8, when other engaged vehicles are proceeding in the same direction as the ego vehicle, irrespective of whether they occupy the same lane or a distinct lane, or are trailing the ego vehicle in the same lane, they are required to maintain a specific safety distance both in front and behind the ego vehicle. To generate an underestimation of the safety distance, accounting for the effect of the area occupied by the ego vehicle and other traffic-engaged vehicles on the safety margin, we consider that, for time interval $[t_k, t_{k+1}]$, the traffic-engaged vehicles in different lanes at time t_k are positioned ahead of the ego vehicle, and the safety distance is therefore calculated as:

$$d_{safe,front} = d_{safe} + \frac{1}{2}l_{obj} + l_{ego}^{f} \tag{14}$$

Herein, $v_{r,0} = v_{ego,0}$ and $v_{f,0} = v_{obj,0}$, where $v_{ego,0}$ represents the initial speed of the ego vehicle and $v_{obj,0}$ denotes the initial speed of other engaged traffic vehicles.

At instance t_{k+1}, if the traffic-engaged vehicle is deemed to be trailing the ego vehicle, the safety distance is calculated as:

$$d_{safe,rear} = d_{safe} + \frac{1}{2}l_{obj} + l_{ego}^{r} \tag{15}$$

where $v_{r,0} = v_{obj,0}$, $v_{f,0} = v_{ego,0}$.

The calculated safety distances above pertain to values within the Frenet coordinate system. An aggregate underestimation of the safety interval at a specific time instance can be deduced by amalgamating the derived underestimations of safety distances with the starting point at the self-reference point. The unattainable region corresponding to the relevant safety distance $\mathcal{A}_{coop,i}^{dist}(t_k, t_{k+1})$ can be delineated by constructing a polygon perpendicular to the respective lane boundary.

Areas reachable in consideration of the right-of-way $\mathcal{A}_{coop,i}^{right}(t_k, t_{k+1})$ primarily for overlapping roads, incorporate the constraint R_{road_right}: vehicles are obliged to yield to others with right-of-way precedence. Absent traffic signals,

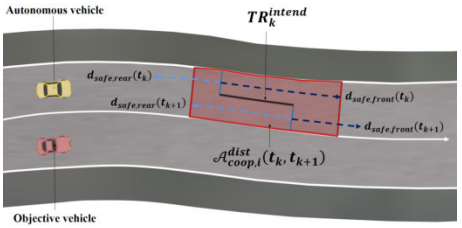
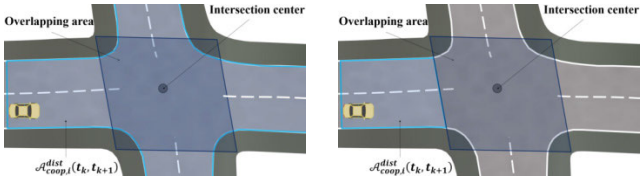


FIGURE 8. Diagram of unreachable area for maintaining safe following distance.



(a) (b)

FIGURE 9. Illustration of region in consideration of right-of-way: (a) entire lane, (b) cut-off to road overlap area.

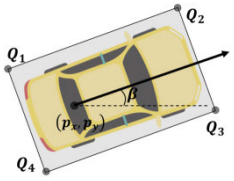


FIGURE 10. Occupied area of the ego vehicle at a given instant.

proximity to the overlap zone confers priority. Initially, the distance to the overlap area's center is determined for each vehicle necessitating intersection crossing. The right-of-way dependent region hinges on whether the vehicle can traverse the overlap zone within the time interval $[t_k, t_{k+1}]$. No other vehicle is permitted to intrude into the overlap zone until the vehicle proximate to the overlap area's center has completed intersection crossing. The right-of-way feasible region for the vehicle closest to the overlap area's center spans the entirety of its current lane, as depicted in Fig. 9(a); whereas, the right-of-way feasible region for other vehicles extends up to the overlap area, as illustrated in Fig. 9(b).

When traffic signals are present at the junction, the right-of-way contingent region $\mathcal{A}^{right}_{coop,i}(t_k, t_{k+1})$ must additionally factor in whether the vehicle can penetrate the road overlap area within the remaining permissible time frame. Given that the distance from the i^{th} traffic participant to the overlap area's center is $d^c_{obj,i}$ and the current speed is $v_{obj,0}$, the corresponding trajectory is verified for a time of $[t_k, t_{k+1}]$. Furthermore, the residual time allowance between the present moment and t_{k+1} is denoted as $t_{passable}$. The i^{th} traffic participant's right-of-way related feasible region corresponding to the $[t_k, t_{k+1}]$ engaged vehicle under various circumstances is illustrated in Table 2.

TABLE 2. Regions for additional traffic participants during the time interval $[T_K, T_{K+1}]$ in consideration of right-of-way.

Traffic scenarios			$\mathcal{A}^{right}_{coop,i}$
No traffic lights	The vehicle closest to the center of the overlapping area	$d^c_{obj,i}=min\{d^c_{ego}, d^c_{obj,1}, d^c_{obj,2}, \ldots\}$	Entire lane
	Vehicles not closest to the centre of the overlapping area	$d^c_{obj,i}\neq min\{d^c_{ego}, d^c_{obj,1}, d^c_{obj,2}, \ldots\}$	Cut-off to overlap area
With traffic lights	With remaining passable time	$t_{passable}>0, v_{obj,0}t_{passable}+\frac{1}{2}a_{max,\ acc}t^2_{passable}\geq d^c_{obj,i}$	Entire lane
		$t_{passable}>0, v_{obj,0}t_{passable}+\frac{1}{2}a_{max,\ acc}t^2_{passable}<d^c_{obj,i}$	Cut-off to overlap area
	No remaining passable time	$t_{passable}=0, v_{obj,0}t_{passable}+\frac{1}{2}a_{max,\ acc}t^2_{passable}<d^c_{obj,i}$	Cut-off to overlap area

B. EXPECTED TRAJECTORY SAFETY VERIFICATION

Predicated on the anticipated trajectory engendered by the ego vehicle's decision system, its occupancy area within the time interval $[t_k, t_{k+1}]$ is calculated. Accommodating for the vehicle's dimensions, as depicted in Fig. 10, the ego vehicle's occupancy area at a given instant is a rectangle $Q(q_1, q_2, q_3, q_4)$, where the coordinates of the reference point of the ego vehicle are (p_x, p_y) and the angle between the longitudinal axis of the vehicle and the x-axis is denoted as β. Utilizing the axis rotation formula, we can derive in (16a)–(16d), as shown at the bottom of the next page.

The ego vehicle's self-occupancy area corresponding to each point of the anticipated trajectory within $[t_k, t_{k+1}]$ can be calculated, and the self-occupied area $\mathcal{A}_{ego}(t_k, t_{k+1})$ can be determined by consolidating the resultant set.

To ascertain whether the anticipated trajectory proposed by the ego vehicle's trajectory planner is safe, it is incumbent to examine whether the ego vehicle's occupied area, engendered by the anticipated trajectory at the respective time, intersects with the regions of other traffic-engaged vehicles. If an anticipated trajectory generates a self-occupied area $\mathcal{A}_{ego}(t_k, t_{k+1})$ that does not intersect with the region $\mathcal{A}_{obj}(t_k, t_{k+1})$ of all other traffic-engaged vehicles at this time, then this anticipated trajectory can be validated as safe; if not, it is deemed unsafe.

C. GENERATION OF ALTERNATIVE SAFETY TRAJECTORIES

The formulation of the alternate safe trajectory chiefly encompasses the selection of the ego vehicle's alternate safe

$$d_{safe} = max\left\{v_{r,0}\delta_{vehicle} - \frac{1}{2}a_{max,brake}\delta^2_{vehicle} + \frac{(v_{r,0} - a_{max,brake}\delta_{vehicle})^2 - v^2_{f,0}}{2a_{max,brake}}, 0\right\} \tag{13}$$

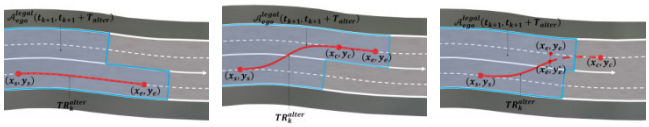
trajectory endpoint and the generation of the ego vehicle's alternate safe trajectory. The endpoint selection for the ego vehicle's alternate safe trajectory serves to select the endpoint of the alternate safe trajectory meeting requisite conditions. The generation of the ego vehicle's alternate safe trajectory employs either the quintic polynomial method or the lane centerline method to create the alternate safe trajectory, contingent upon whether the ego vehicle requires lane change.

1) SELECTION OF TRAJECTORY ENDPOINT

The alternate safe trajectory TR_k^{alter} must satisfy three stipulations: firstly, TR_k^{alter} is required to seamlessly link with TR_k^{safe}, thereby setting the starting point (x_s, y_s) of TR_k^{alter} as the endpoint of TR_k^{safe}; secondly, TR_k^{alter} must guarantee the ego vehicle's legal safety, ensuring that the vehicle's occupancy area along the entire alternate safety trajectory does not intersect with the region of other traffic-engaged vehicles, hence TR_k^{alter} should be within the legally reachable region of the ego vehicle $\mathcal{A}_{ego}^{legal}$:

$$\mathcal{A}_{ego}^{legal} = \mathcal{A}_{road}^{sign} \bigcap \mathcal{A}_{road}^{right} \bigcap \mathcal{A}_{road}^{V2X\complement} \bigcap \mathcal{A}_{obj}^{*\complement} \tag{17}$$

where $\mathcal{A}_{road}^{sign}$ represents the ego vehicle's region concerning road signs $\mathcal{A}_{road,V2X}^{C}$ symbolizes the unreachable area regarding V2X information, and $\mathcal{A}_{obj}^{*\complement}$ denotes the complement of the region $\mathcal{A}_{obj}^{*}$ of all other traffic-engaged vehicles concerning the vehicles and roads. Equation (17) designates all regions corresponding to the time $[t_{k+1}, t_{k+1} + T_{alter}]$. Given that the trajectory of the ego vehicle remains indeterminate, only the reachable regions $\mathcal{A}_{obj}^{*}$ of vehicles and roads related to other traffic-engaged vehicles are calculated. It is then incumbent to select the endpoint (x_e, y_e) of the alternate safety trajectory TR_k^{alter} within $\mathcal{A}_{ego}^{legal}(t_{k+1}, t_{k+1} + T_{alter})$. Lastly, the length of TR_k^{alter} must cater to the requirements of normal driving, enabling the ego vehicle to transition into the safety area. Provided that the speed of the ego vehicle is $v_{ego,0}$ and the maximum braking deceleration is $a_{max,brake}$, to ensure that the alternate safety trajectory TR_k^{alter} allows for sufficient deceleration for the ego vehicle to stop, in the Frenet coordinate system, it is presumed that the starting point (x_s, y_s) of the alternate safety trajectory TR_k^{alter} corresponds to the length of the reference line s_{start}, and the endpoint (x_e, y_e) corresponds to the length of the reference line s_{end}.



(a) (b) (c)

FIGURE 11. Scenarios for generation of alternate safe trajectories: (a) No lane alteration necessitated, (b) The terminal point of the lane shift resides within the legally reachable region of the vehicle, (c) The terminal point of the lane shift falls outside the legally reachable region of the vehicle.

Consequently, s_{end} must satisfy:

$$s_{end} \geq v_{ego,0} T_{alter} + l_{ego}^{f} + s_{start} \tag{18}$$

In consideration of the increased risk associated with lane changes compared to maintaining the current lane, the ego vehicle is programmed to avoid changing lanes unless absolutely necessary. When a lane change is required, it's programmed to choose the adjacent lane with a larger legally reachable region for the maneuver. Initially, the lane centerline of the current lane of the ego vehicle is assessed against formula (18) at the point corresponding to the longest reference line length in the legally reachable region. If it satisfies the formula, the point with a reference line length of s_{end} on the lane centerline is chosen as the endpoint of the alternate safety trajectory. Otherwise, the point corresponding to the longest reference line length in the legally reachable region of the adjacent lane is examined to see if it meets the criteria of formula (18). If it does, the point with the reference line length of s_{end} on the lane centerline is selected as the endpoint of the alternate safety trajectory for the next calculation. If none of these conditions are met, the generation of the alternate safety trajectory fails.

2) TRAJECTORY GENERATION METHODOLOGY

The generation method for the alternate safety trajectory reference line is determined by whether a lane change is required. In cases where a lane change is not necessary, as illustrated in Fig. 11(a), the starting and ending points of the alternate safety trajectory are on the same lane centerline. Conversely, in cases where a lane change is required, as shown in Fig. 11(b) and (c), the starting and ending points of the alternate safety trajectory are not on the same lane centerline, necessitating a lane change.

$$q_1 = \left[-l_{ego}^{r} cos\beta - \frac{1}{2} w_{ego} sin\beta + p_x, -l_{ego}^{r} sin\beta + \frac{1}{2} w_{ego} cos\beta + p_y \right]^{\mathrm{T}} \tag{16a}$$

$$q_2 = \left[l_{ego}^{f} cos\beta - \frac{1}{2} w_{ego} sin\beta + p_x, l_{ego}^{f} sin\beta + \frac{1}{2} w_{ego} cos\beta + p_y \right]^{\mathrm{T}} \tag{16b}$$

$$q_3 = \left[l_{ego}^{f} cos\beta + \frac{1}{2} w_{ego} sin\beta + p_x, l_{ego}^{f} sin\beta - \frac{1}{2} w_{ego} cos\beta + p_y \right]^{\mathrm{T}} \tag{16c}$$

$$q_4 = \left[-l_{ego}^{r} cos\beta + \frac{1}{2} w_{ego} sin\beta + p_x, -l_{ego}^{r} sin\beta - \frac{1}{2} w_{ego} cos\beta + p_y \right]^{\mathrm{T}} \tag{16d}$$

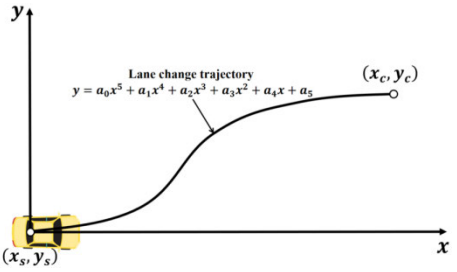


FIGURE 12. Diagram demonstrating prediction of lane change trajectory.

The starting point for the lane change is the starting point (x_s, y_s) of the alternate safety trajectory, and an endpoint (x_c, y_c) for the lane change completion needs to be selected on the centerline of the target lane. In the Frenet coordinate system, it is crucial to reserve enough distance for the lane change. To ensure the distance required from the start to the completion of the lane change is d_{change}, the reference line length s_{change} corresponding to the endpoint (x_c, y_c) should satisfy $s_{change} \geq s_{start} + d_{change}$. By taking $s_{change} = s_{start} + d_{change}$ and retrieving it on the target lane centerline, the lane change endpoint (x_c, y_c) that satisfies the condition can be determined.

When the given alternate safety trajectory endpoint (x_e, y_e) corresponding to the reference line length s_{end} is greater than (x_c, y_c) corresponding to the reference line length s_{change}, as shown in Fig. 11(b), the ego vehicle can continue driving along the target lane centerline from (x_c, y_c) to (x_e, y_e) after completing the lane change. The reference line of the alternate safety trajectory is the curve $(x_s, y_s) - (x_c, y_c) - (x_e, y_e)$. However, if the length s_{end} of the reference line corresponding to (x_e, y_e) is less than the length s_{change} of the reference line corresponding to (x_c, y_c), as shown in Fig. 11(c), only a partial lane change trajectory is generated, and the endpoint (x_e^*, y_e^*) is selected on the generated reference line, so that its corresponding reference line length is s_{end}.

The derivation of the alternate safety trajectory, premised on the centerline method, proceeds as follows: As delineated in Fig. 12(a), the origin and termination points of the alternate safety trajectory reside on the identical lane centerline. The lane centerline spanning from coordinates (x_s, y_s) to (x_e, y_e) is adopted as the reference line for the alternate safety trajectory, as it obviates the necessity for the vehicle to alter lanes.

Subsequently, the generation of the alternate safety trajectory via the quintic polynomial method is characterized as follows: Referencing Fig. 12, a coordinate system is instantiated, its origin residing at the initial position of the ego vehicle's reference point, and its x-axis aligned with the ego vehicle's velocity vector. Given that the lateral velocity of the ego vehicle is presumed negligible, its influence is disregarded. The equation of the reference line dictating the ego vehicle's lane-changing trajectory is defined as:

$$y = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \tag{19}$$

Presuming the current velocity of the vehicle as $v_{ego,0}$, and the transverse pendulum's angular velocity as $\omega_{ego,0}$, the tangent point upon completion of lane change with the target lane centerline is denoted as P_c. The lane line sensor is capable of quantifying the coordinates of the target point on the lane centerline for lane change as (x_c, y_c), as well as the gradient r_c, and the curvature K_c. Within the extant coordinate system, the coordinates of the initial position for lane change point (x_s, y_s) is set as (0,0). The gradient at point (x_s, y_s) is zero, and the corresponding curvature of the reference line at point (x_s, y_s) can be inferred from the vehicle's velocity and the transverse pendulum's angular velocity. Consequently, the equation of the reference line at point (x_s, y_s) ought to satisfy the ensuing conditions:

$$y = 0 \tag{20a}$$
$$y' = 0 \tag{20b}$$
$$K = \frac{y''}{\left(1 + y'^2\right)^{\frac{3}{2}}} = \frac{\omega_{ego,0}}{v_{ego,0}} \tag{20c}$$

At the terminal point of lane change (x_c, y_c) the gradient and curvature of the reference line for the alternate safety trajectory should harmonize with those of the lane centerline at this location. Hence, the equation defining the reference line at point (x_c, y_c) ought to meet the subsequent relationship:

$$y = y_c \tag{21a}$$
$$y' = r_c \tag{21b}$$
$$K = \frac{y''}{\left(1 + y'^2\right)^{\frac{3}{2}}} = K_c \tag{21c}$$

Basing on the preceding pair of equations, we can deduce the quintic polynomial reference line equation for the ego vehicle's lane change. This requires the initial state data of the ego vehicle, the terminus point (x_c, y_c) of the lane change, and the parameters of the target lane centerline pertaining to the lane change:

$$\begin{bmatrix} x_c^5, & x_c^4, & x_c^3 \\ 5x_c^4, & 4x_c^3, & 3x_c^2 \\ 20x_c^3, & 12x_c^2 & 6x_c \end{bmatrix} \begin{bmatrix} a_5 \\ a_4 \\ a_3 \end{bmatrix} = \begin{bmatrix} y_c - \frac{\omega_{ego,0}}{2v_{ego,0}} x_c^2 \\ r_c - \frac{\omega_{ego,0}}{v_{ego,0}} x_c \\ K_c - \frac{\omega_{ego,0}}{v_{ego,0}} \end{bmatrix} \tag{22}$$

where $a_0 = 0, a_1 = 0, a_2 = \frac{\omega_{ego,0}}{2v_{ego,0}}$.

Upon the evaluation of the coefficient matrix, the values for a_3, a_4, and a_5 can be determined. It is essential to underscore that the aforementioned derivation is performed in the specified coordinate system, necessitating a rotational transformation of the coordinates to obtain the equation for the reference line change in global coordinates. The computation of the alternate safety trajectory reference line is thus concluded at this juncture.

Subsequent to this, it becomes imperative to verify whether the ego vehicle's occupied area, generated by the alternate safety trajectory, is encompassed within its legally reachable region. Should the ego vehicle's occupied area lie within its legally reachable region, the generation of the alternate safety trajectory is deemed successful; otherwise, it is considered a failure.

D. ONLINE SAFETY VERIFICATION ALGORITHM

This section presents the online safety verification algorithm for autonomous driving decisions. The pseudocode flow for each verification cycle is characterized as Algorithm1.The initialization parameters requisite for each verification cycle encompass road geometry information I_{road}^{geo}, road travel constraint information I_{road}^{rest}, traffic participant vehicle state information $I_{obj,i}$, and ego vehicle state information I_{ego}. I_{road}^{geo} includes road width w_{road}, the location of the road's center overlap area p_{center}, and lane line information I_{lane}. I_{road}^{rest} encompasses maximum vehicle speed v_{max}, maximum vehicle acceleration a_{max}, remaining passable time $t_{passable}$, road sign information I_{sign}, V2X information I_{V2X}, with $I_{obj,i}$ detailing dimensions $l_{obj,i}$, $w_{obj,i}$ of other traffic participating vehicles, speed $v_{0,i}$, position $p_{0,i}$ and heading angle $H_{obj,i}$. I_{ego} encapsulates the size of the ego vehicle l_{ego}^{f}, l_{ego}^{r}, w_{ego}, speed $v_{ego,0}$, the expected trajectory TR_k^{intend} provided by the trajectory planner, the last successfully generated alternate safety trajectory TR_{k-c}^{alter}, the transverse angular velocity of the ego vehicle $\omega_{ego,0}$, the lane change distance d_{change}, and the time corresponding to the generation of the alternate safety trajectory T_{alter}.

To ascertain the safety of TR_k^{intend}, the algorithm initially calculates three reachable zones for each traffic participant, namely $\mathcal{A}_{mot,i}(t_k, t_{k+1})$, $\mathcal{A}_{road,i}(t_k, t_{k+1})$, and $\mathcal{A}_{coop,i}(t_k, t_{k+1})$. The intersection of these three reachable zones yields the overall region for each traffic participant $\mathcal{A}_{obj,i}(t_k, t_{k+1})$. The intersection of the overall regions of all traffic participants is then determined to obtain the combined reachable zones of all traffic participants $\mathcal{A}_{obj}(t_k, t_{k+1})$. The algorithm then computes the self-occupied area $\mathcal{A}_{ego}(t_k, t_{k+1})$, and differentiates it from $\mathcal{A}_{obj}(t_k, t_{k+1})$ to verify the safety of TR_k^{intend} (lines 2-6).

Assuming TR_k^{intend} is deemed safe, the algorithm then attempts to generate the alternate safe trajectory TR_k^{alter}. Based on TR_k^{intend}, the algorithm can determine the starting point (x_s, y_s) of TR_k^{alter}, compute $\mathcal{A}_{ego}^{legal}$ – the legally reachable region for the vehicle within $[t_{k+1}, t_{k+1} + T_{alter}]$, and subsequently determine the end point (x_e, y_e) of TR_k^{alter} based on $\mathcal{A}_{ego}^{legal}$. If the distance between (x_e, y_e) and (x_s, y_s) is sufficiently large, then TR_k^{alter} is generated and the self-occupied area $\mathcal{A}_{auto}^{alter}$ engendered by TR_k^{alter} is computed. If $\mathcal{A}_{auto}^{alter}$ resides within $\mathcal{A}_{ego}^{legal}$, the alternate safety trajectory is successfully generated and TR_k^{intend} is executed within $[t_k, t_{k+1}]$ (lines 7-14). However, if $\mathcal{A}_{ego}(t_k, t_{k+1})$ intersects with $\mathcal{A}_{obj}(t_k, t_{k+1})$, if (x_e, y_e) is not distanced sufficiently from (x_s, y_s), or if $\mathcal{A}_{auto}^{alter}$ does not belong to $\mathcal{A}_{ego}^{legal}$, then TR_{k-c}^{alter} is executed within $[t_k, t_{k+1}]$ (lines 1-17).

V. TESTING AND EVALUATION

A. EXPERIMENT SETTINGS

Utilizing a co-simulation of PreScan (version 8.6.0) and Matlab (version R2021b), we tested and validated the proposed online safety verification methodology for autonomous driving decision-making. PreScan facilitated the construction of various prototypical traffic scenarios, encompassing road network development, establishment of the road's surrounding environment, parameter setting and trajectory planning for each traffic participant, and the creation of the perception layer. Matlab was utilized for data transmission and processing, implementing the online safety verification algorithm via the M language.

The AIR sensor was employed to gather information about other traffic vehicles, including speed $v_{obj,i}$, heading angle $H_{obj,i}$, distance from the vehicle $R_{obj,i}$, and azimuth angle $\theta_{obj,i}$.

Algorithm 1 Online Safetyverification

Input: road geometry information I_{road}^{geo} (w_{road}, p_{center}, I_{lane}), road driving restraint information I_{road}^{rest}(v_{max}, a_{max}, $t_{passable}$, I_{sign}, I_{V2X}), traffic participation vehicle status information $I_{obj,i}$($l_{obj,i}$, $w_{obj,i}$, $v_{0,i}$, $p_{0,i}$, , $H_{obj,i}$), ego vehicle status information I_{ego}(l_{ego}^{f}, l_{ego}^{r}, w_{ego}, $v_{ego,0}$, $\boldsymbol{TR}_k^{intend}$, $\boldsymbol{TR}_{k-c}^{alter}$, $\omega_{ego,0}$, d_{change}, T_{alter}),current time t_0, verification time t_k, t_{k+1}

Output: Safety trajectory $\boldsymbol{TR}_k^{exe}$ executed in $[t_k, t_{k+1}]$

1: $\boldsymbol{TR}_k^{exe} \leftarrow \boldsymbol{TR}_{k-c}^{alter}$

2: $\mathcal{A}_{road,i}(t_k, t_{k+1})$, $\mathcal{A}_{mot,i}(t_k, t_{k+1})$, $\mathcal{A}_{coop,i}(t_k, t_{k+1})$ ← calculate three regions (I_{road}^{geo}, I_{road}^{rest}, $I_{obj,i}$, I_{ego})

3: $\mathcal{A}_{obj,i}(t_k, t_{k+1})$ ← calculate the overall region $(\mathcal{A}_{mot,i}(t_k, t_{k+1}), \mathcal{A}_{road,i}(t_k, t_{k+1}), \mathcal{A}_{coop,i}(t_k, t_{k+1}))$

4: $\mathcal{A}_{obj}(t_k, t_{k+1}) \leftarrow \bigcup A_{obj,i}(t_k, t_{k+1})$

5: $\mathcal{A}_{ego}(t_k, t_{k+1})$ ← calculate the area occupied by the ego vehicle(l_{ego}^{f}, l_{ego}^{r}, w_{ego}, $\boldsymbol{TR}_k^{intend}$)

6: **if** $\mathcal{A}_{ego}(t_k, t_{k+1}) \cap \mathcal{A}_{obj}(t_k, t_{k+1}) = \emptyset$ **then**

7: $(x_s, y_s) \leftarrow \boldsymbol{TR}_k^{intend}$

8: $\mathcal{A}_{ego}^{legal}(t_{k+1}, t_{k+1} + T_{alter}) \leftarrow \mathcal{A}_{road}^{sign}(t_{k+1}, t_{k+1} + T_{alter}) \bigcap \mathcal{A}_{road}^{right}(t_{k+1}, t_{k+1} + T_{alter}) \bigcap \mathcal{A}_{road}^{V2XC}(t_{k+1}, t_{k+1} + T_{alter}) \bigcap \mathcal{A}_{obj}(t_{k+1}, t_{k+1} + T_{alter})$

9: (x_e, y_e) ← calculate alternate safety trajectory endpoint $\{\mathcal{A}_{ego}^{legal}(t_{k+1}, t_{k+1} + T_{alter})\}$

10: **if** (x_e, y_e) is far enough away from (x_s, y_s) **then**

11: $\boldsymbol{TR}_k^{alter}$ ← calculate alternate safety trajectory $\{(x_e, y_e), (x_s, y_s)\}$

12: $\mathcal{A}_{auto}^{alter}$ ← calculate occupied area ($\boldsymbol{TR}_k^{alter}$)

13: **if** $\mathcal{A}_{auto}^{alter} \subseteq \mathcal{A}_{ego}^{legal}(t_{k+1}, t_{k+1} + T_{alter})$ **then**

14: $\boldsymbol{TR}_k^{exe} \leftarrow \boldsymbol{TR}_k^{intend}$

15: **end if**

16: **end if**

17: **end if**

We encapsulated the point mass models of other traffic participants in a rectangle with $l_{obj,i}$ of $4m$, and $w_{obj,i}$ of $2m$., and the point mass models of the ego-vehicle in a rectangle with l_{ego}^{f} of $4m$, l_{ego}^{r} of $1.3m$, and w_{ego} of $2m$. The maximum acceleration $a_{max,acc}$ and maximum deceleration $a_{max,brake}$ of the ego-vehicle and other traffic participants were set to $8m/s^2$. The length s_{end} of the reference line corresponding to the termination of the alternate safety trajectory is determined by $v_{ego,0}T_{alter} + l_{ego}^{f} + s_{start}$. The online safety verification replanning period is set at $0.1s$, the duration of each expected trajectory TR_k^{intend} at $0.3s$, and the duration of the alternate safety trajectory T_{alter} at $0.6s$, with t_a as $0.1s$ and t_b as $0.3s$. Assuming that the expected trajectory remains unaltered within a $0.3s$ interval and that the online safety verification replanning period is $0.1s$, the expected trajectory TR_k^{intend} corresponds to a duration of $[t_k, t_k + 0.3s]$. Each expected trajectory needs verification thrice; a single successful instance out of the three leads to a successful verification of TR_k^{intend} and its execution starting from t_k. However, if all three instances of verification fail, TR_k^{intend} will be adjudged a verification failure, and the alternate safe

TABLE 3. Parameter settings for simulation scenarios.

Scenario	$v_{ego,0}$ (m/s)	$v_{ego,end}$ (m/s)	$a_{max,acc}$ (m/s^2)	$a_{max,brake}$ (m/s^2)	n_{obj}	v_{max} (m/s)
Two-way multi-lane	15	20	8	8	5	30
One-way multi-lane	15	15	8	8	2	30
One-way multi-lane with temporary road signs	15	15	8	8	2	30
Crossroad	12	5	8	8	6	30
Y-junction	15	5	8	8	2	30
One-way multi-lane with bad weather	15	15	4	4	2	15

trajectory TR_{k-c}^{alter} from the last successful verification will be executed at time t_k, thus yielding the trajectory to be executed in each cycle.

Based on the ISO 34502 automatic driving system test scene construction standard, common test scenarios in the research and development of automatic driving, and actual road safety-critical traffic scenarios, we created one-way multi-lane, two-way multi-lane, intersections and Y-shaped intersections in PreScan. A typical scene is used as a test. At the same time, the road with temporary road traffic signs and bad weather was tested on the one-way multi-lane. The parameters of each simulation scene are shown in Table 3.

B. SIMULATION AND VERIFICATION OF SPECIFIC AUTONOMOUS DRIVING SCENARIOS

The above-mentioned online safety verification methodologies were individually validated based on the specific typical traffic scenarios defined in the experimental design. The ensuing analysis of the test results primarily encompassed two dimensions: safety and real-time performance. Safety implies that the technology is capable of adapting to a plethora of traffic scenarios, accurately evaluating the safety of the anticipated trajectory, and generating an alternate safe trajectory that can guide the vehicle to a secure state, without actively instigating traffic accidents or violating traffic regulations, thereby ensuring the vehicle's lawful safety. Real-time, on the other hand, indicates the ability of the technology to complete computations and processing within the prescribed time, and promptly verify the safety of the anticipated trajectory and generate an alternate safe trajectory.

1) SIMULATION VALIDATION FOR TWO-WAY MULTI-LANE SCENARIOS

Fig. 13(a) illustrates the initial speed and relative position of each traffic participant in the constructed two-way six-lane straight road scenario, while Fig. 13(b) showcases the online safety verification result for this scenario:

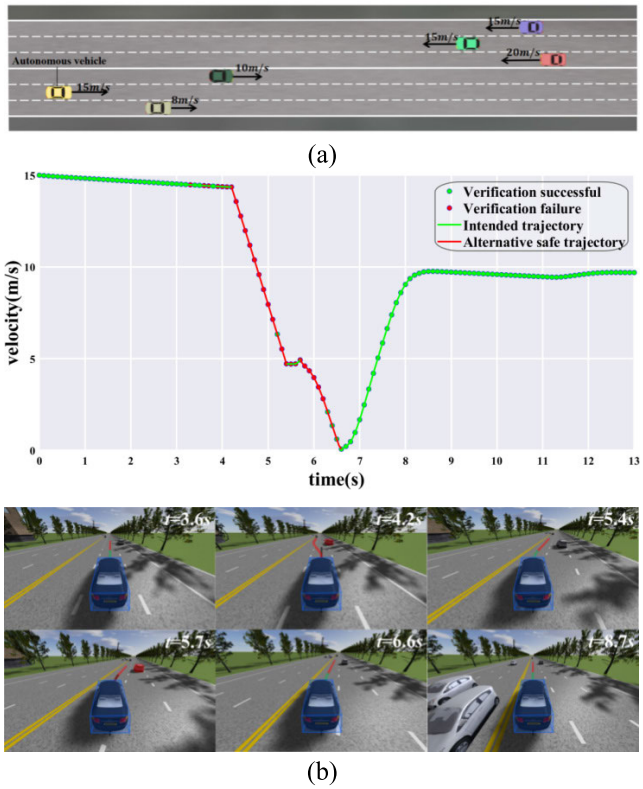


FIGURE 13. Validation of two-way multi-lane scenario: (a) Two-way six-lane straight road scenario, (b) safety verification outcomes for two-way six-lane straight scenario.

At $t = 4.2s$, owing to an anticipated lane change from the vehicle directly ahead on the right, the ego vehicle's proposed trajectory failed to pass verification, prompting the execution of the latest successfully verified alternate safety trajectory from the $3.9s$ - $4.2s$ interval, thus initiating a lane change to the left. At $5.7s$, the expected trajectory for the ego vehicle failed verification, thus invoking the alternate safety trajectory validated in the $5.4s$ - $5.7s$ period. At $3.5s$, $5.4s$, $6.6s$, and $8.7s$, the ego vehicle's proposed trajectory successfully passed verification and was subsequently executed. The ego vehicle adhered to the alternate safety trajectory during the $4.2s$ - $5.4s$ and $5.7s$ - $6.6s$ intervals, while executing the verified expected trajectory for the remaining duration.

2) SIMULATION VALIDATION FOR ONE-WAY MULTI-LANE SCENARIOS

Fig. 14(a) illustrates the initial speed and relative position of each traffic participant in the constructed one-way three-lane curve scenario, while the online safety verification result for this scenario is depicted in Fig. 14(b):

At $t = 4.5s$, the anticipated trajectory verification of the ego vehicle (indicated in blue) fails due to the leading vehicle (marked in red) preparing to change lanes (the anticipated trajectory corresponding to the verification failure is

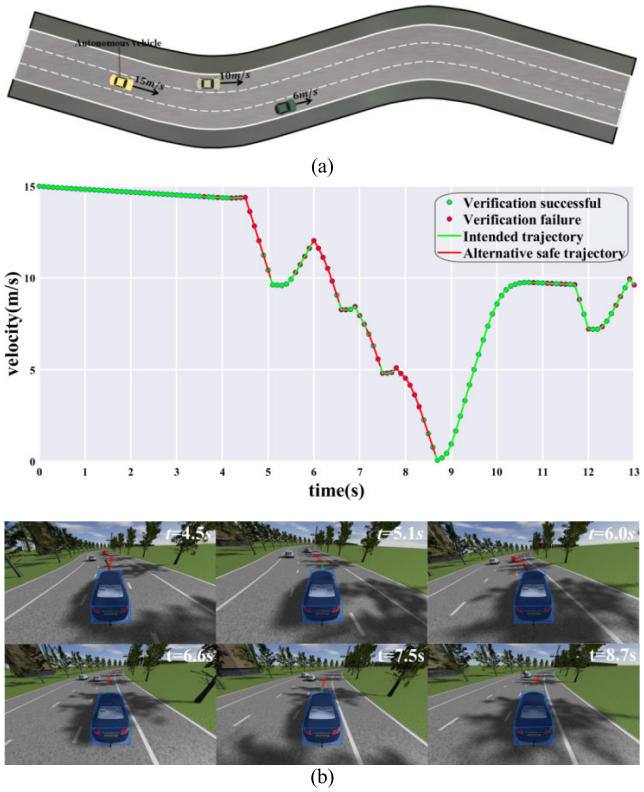


FIGURE 14. Validation of one-way multi-lane scenario: (a) One-way three-lane curved road scenario, (b) safety verification outcomes for one-way three-lane curved scenario.

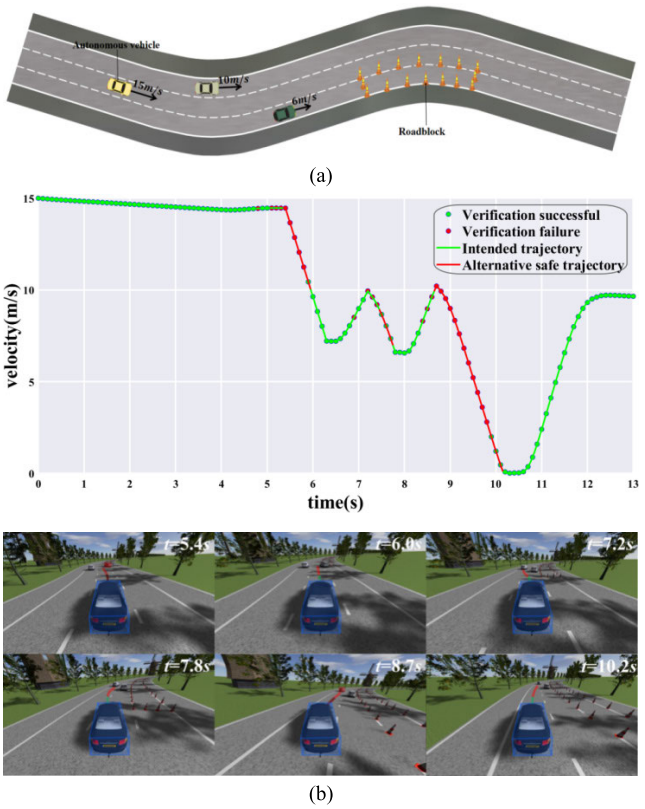


FIGURE 15. Validation of temporary road sign scenario: (a) one-way three-lane curved road scenario with temporary road signs, (b) safety verification outcomes for one-way three-lane curved road scenario with temporary road signs.

delineated in black). Consequently, the latest successfully verified alternate safety trajectory within the time frame of 3.9s - 4.2s (highlighted in red) is executed, initiating the lane change to the immediate right lane. At 6.0s, the verification of the ego vehicle's anticipated trajectory fails, leading to the execution of the most recent successfully verified alternate safety trajectory within the time period of 5.7s - 6.0s. At 5.1s, 6.6s, 7.5s, and 8.7s, the ego vehicle's anticipated trajectory successfully passes the verification, subsequently leading to the execution of the anticipated trajectory. The ego vehicle executes the alternate safety trajectory within the time intervals of 4.5s - 5.1s, 6.0s - 6.6s, 7.2s - 7.5s, and 7.8s - 8.7s, while for the remaining durations, it executes the successfully verified anticipated trajectory.

3) SIMULATION VALIDATION FOR TEMPORARY ROAD SIGN SCENARIOS

Fig. 15(a) presents the initial speeds and relative positions of each traffic participant in the constructed scenario of a one-way, three-lane curved road with temporary road signs. The online safety verification results for this scenario are shown in Fig. 15(b).

At $t = 5.4s$, due to a roadblock causing the vehicle ahead to prepare to change lanes, the expected trajectory verification for the ego vehicle fails. As a response, the latest successfully verified alternate safety trajectory within the time range of 5.1s - 5.4s is executed, resulting in a reduction in the vehicle's speed. At 8.7s, as the ego vehicle is too close to the vehicle in front, the expected trajectory verification fails again, leading to the execution of the latest successfully verified alternate safety trajectory within the time range of 8.4s - 8.7s. At 6.0s, 7.2s, 7.8s, and 10.2s, the expected trajectory of the ego vehicle successfully passes the verification, and thus is executed. The ego vehicle executes the alternate safety trajectory within the time ranges of 5.4s-6.0s, 7.5s-7.8s, and 8.7s-10.2s, and for the rest of the time, executes the expected trajectory which has successfully passed the verification.

4) SIMULATION VALIDATION FOR INTERSECTION SCENARIOS

Fig. 16(a) displays the initial speeds and relative positions of each participating vehicle in the constructed two-lane intersection scenario, while Fig. 16(b) presents the results of the online safety verification for this scenario.

At $t = 4.8s$, the anticipated trajectory of the ego vehicle failed to pass the verification test due to a vehicle proceeding through the intersection from the front-left. As a result, the most recently validated alternate safety trajectory within the interval of 3.5s - 4.8s was executed, leading to a deceleration of the vehicle. At $t = 5.7s$, with a vehicle on the right infringing on the right-of-way through the intersection, the proposed

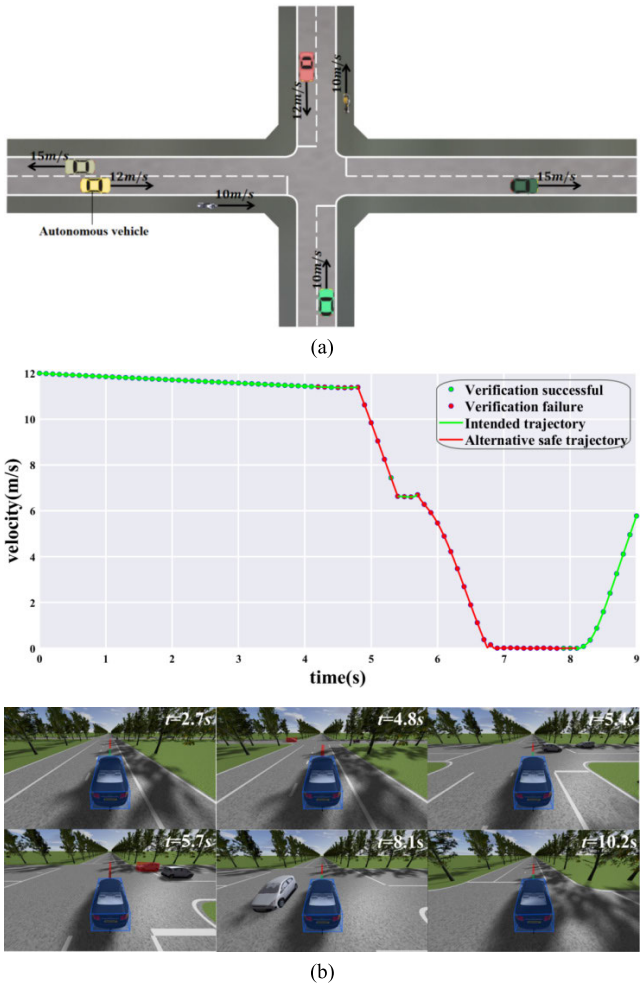


FIGURE 16. Validation of intersection scenario: (a) Two-lane crossroads scenario, (b) safety verification outcomes for two-lane intersection scenario.

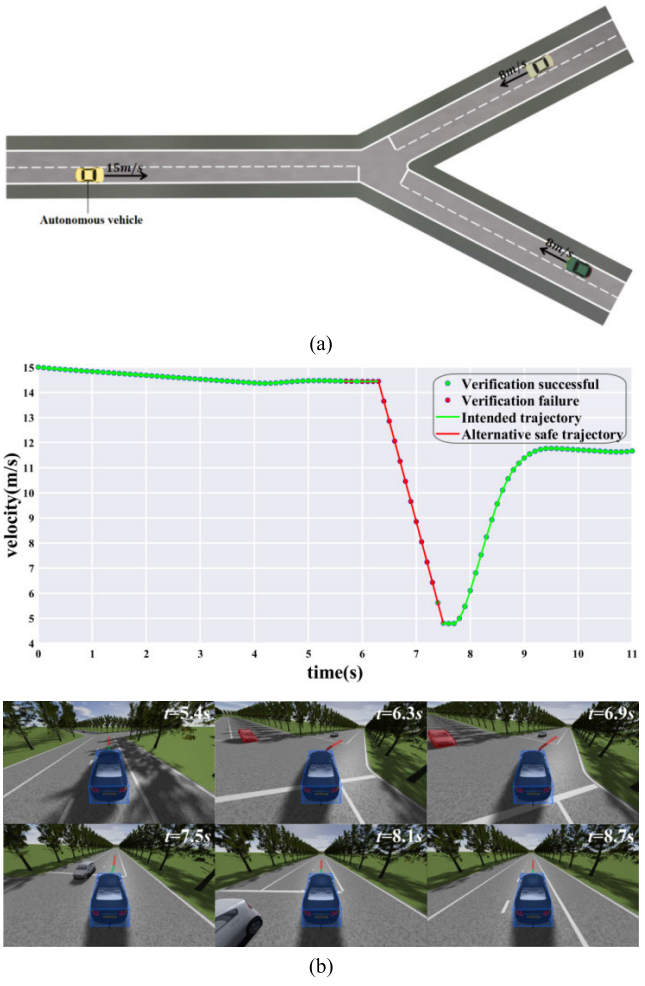


FIGURE 17. Validation of Y-junction scenario: (a) Two-lane y-shaped intersection scenario, (b) safety verification outcomes for two-lane y-shaped intersection scenario.

trajectory for the ego vehicle again failed the verification, which led to the execution of the most recently validated alternate safety trajectory during the 5.4s - 5.7s timeframe, again slowing the vehicle. At t = 2.7s, 5.4s, 8.1s, and 10.2s, the ego vehicle's anticipated trajectory successfully passed the verification and was subsequently executed. The ego vehicle adhered to the alternate safety trajectory during the 4.8s - 5.4s and 5.7s - 8.1s intervals, while executing the verified expected trajectory for the rest of the time.

5) SIMULATION VALIDATION FOR Y-JUNCTION SCENARIOS

Fig. 17(a) displays the initial speeds and relative positions of each participating vehicle in the constructed two-lane Y-intersection scenario, while Fig. 17(b) showcases the results of the online safety verification for this scenario.

At $t = 6.3s$, the expected trajectory of the ego vehicle fails the verification due to a vehicle on the left-front crossing the intersection against the right-of-way. As a result, the latest successfully verified alternate safety trajectory from the 6.0s - 6.3s interval is executed, slowing down the vehicle. At 6.9s, the expected trajectory of the ego vehicle again fails the verification and the latest successfully verified alternate safety trajectory continues to be executed, resulting in further deceleration. At 5.4s, 7.5s, 8.1s, and 8.7s, the expected trajectory of the ego vehicle is successfully verified and executed. The ego vehicle follows the alternate safe trajectory between 6.3s - 7.5s, while for the remaining time, it executes the expected trajectory which has passed verification.

6) SIMULATION VALIDATION FOR SEVERE WEATHER SCENARIOS

Fig. 13(a) illustrates the initial speeds and relative positions of each traffic participant in the constructed scenario of a one-way, three-lane curved road under adverse weather conditions. The online safety verification results for this scenario are shown in Fig. 18.

At $t = 5.1s$, due to the vehicle ahead preparing to change lanes, the expected trajectory verification of the ego vehicle fails. The latest successfully verified alternate safety trajectory within 4.8s-5.1s is then executed. At 9.0s and 11.1s,

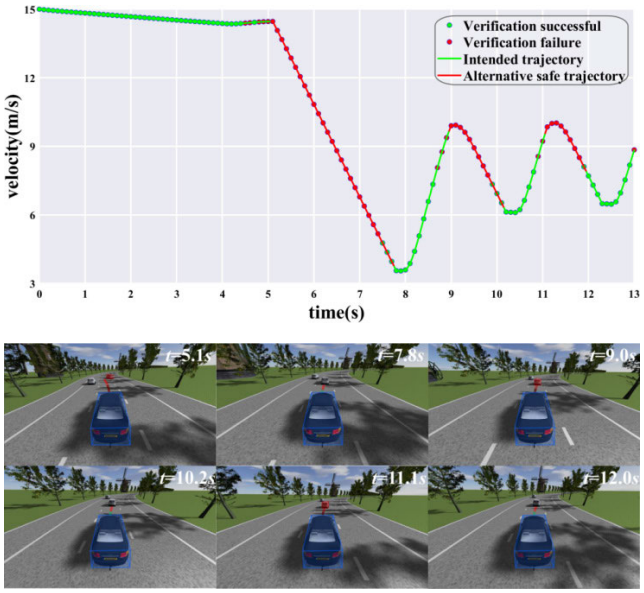


FIGURE 18. Safety verification outcomes for one-way three-lane curved road scenario under adverse weather conditions.

TABLE 4. Computational time for simulation validation.

Scenario	Average time for security verification of expected trajectories	Average time spent on alternate safety trajectory generation	Average total time spent	Overall variance of total time spent
Two-way multi-lane	24.41ms	34.16ms	58.57ms	1.78
One-way multi-lane	23.05ms	32.58ms	55.63ms	1.58
One-way multi-lane with temporary road signs	23.34ms	32.73ms	56.07ms	1.99
Crossroad	24.90ms	34.56ms	59.47ms	2.05
Y-junction	23.81ms	33.94ms	57.75ms	2.14
One-way multi-lane with bad weather	22.99ms	32.59ms	55.58ms	1.72

the ego vehicle gets too close to the vehicle in front, causing the expected trajectory verification to fail again, leading to the execution of the latest successfully verified alternate safety trajectory within 8.7s-9.0s. At 7.8s, 10.2s, and 12.0s, the expected trajectory of the ego vehicle passes the verification and is thus executed. The ego vehicle executes the alternate safety trajectory within 5.1s-7.8s, 9.0s-10.2s, and 11.1s-12.0s, while for the rest of the time, it executes the expected trajectory that has passed the verification.

To further understand the efficiency of the safety verification method, we conducted 10 repeated measurements for the calculation time involved in the expected trajectory safety verification and the alternate safety trajectory generation for the six different scenarios. We calculated the average time for both the expected trajectory safety verification and the generation of the alternate safety trajectory across these six scenarios. We also determined the average of the total time value along with its overall variance. The results of these calculations are shown in Table 4.

These simulation tests were conducted on a computer featuring a 2.60GHz AMD Ryzen 3 3200U processor and 8GB of memory. Given that the computing power of the testing hardware used is lower than what most manufacturers typically use, these results should have a strong practical relevance.

The simulation analysis conducted across the aforementioned six scenarios demonstrates the capability of our proposed online safety verification technique. It can adeptly adapt to a wide array of complex traffic scenarios and accurately judge the safety of the expected trajectory. This ensures that our ego vehicle maintains legal safety under hazardous operating conditions and does not actively instigate traffic accidents. The alternate safety trajectories generated can effectively guide the ego vehicle towards a safe state. Furthermore, the computation time for each scenario can be contained within a 100ms replanning cycle, indicating that our proposed online safety verification technology can promptly complete the safety verification of the expected trajectory and generate the alternate safety trajectory. The current simulation verification time is influenced by the software overhead of the high-level language and the simulation environment. When this method is ported to an embedded environment, the real-time performance can be further improved, optimizing the process even further.

C. SIMULATION VERIFICATION FOR FULL RANDOMIZED SCENARIOS

This section comprehensively evaluates the performance of the proposed method in continuous random scenarios. Each participating vehicle was assigned a distinct closed-loop trajectory $\mathbf{TR}_i$, aligned with the corresponding road centerline. The initial velocity v_0 for each participating vehicle was set to 15 m/s, while ensuring that the maximum velocity $v_{\max}$ was limited to 30 m/s. The acceleration a_i for each participating vehicle was confined to the range [8, -8] m/s^2, and the duration of each a_i, represented by t_{a_i}, varied within the range of [1, 3] s. In the Frenet coordinate system, the lateral offset d_i, between each participating vehicle and $\mathbf{TR}_i$ was defined as $d_i \in \{d_0, d_1, \ldots, d_k\}$, where $d_0, d_1, \ldots, d_k$ denote the offsets corresponding to each lane centerline relative to $\mathbf{TR}_i$. The duration of this offset t_{d_i}, ranged from [10, 30] s.

For this scenario, random values conforming to a normal distribution were assigned to a_i, t_{a_i}, d_i, and t_{d_i}. Different quantities of participating vehicles were introduced into the simulation test over a duration of three hours to validate our online safety verification algorithm. The experimental results obtained from this simulation are presented in Table 5.

TABLE 5. Computational time for simulation validation.

Traffic participation vehicle	Average validation time per validation cycle	Hazardous scenarios	Satisfying legal safety
2	54.16 ms	4.52%	100%
4	58.89 ms	6.57%	100%
6	63.27 ms	8.93%	100%
8	66.26 ms	11.61%	100%
10	70.57 ms	14.68%	100%

As other participating vehicles comply with traffic regulations during their travel, their driving area consistently remains within the predicted reachable region. With the application of our online safety verification algorithm, we can ensure the legality and safety of ego vehicle at all times.

The simulation analysis conducted across the aforementioned scenarios demonstrates the capability of our proposed online safety verification technique. It can adeptly adapt to a wide array of complex traffic scenarios and accurately judge the safety of the expected trajectory. This ensures that our ego vehicle maintains legal safety under hazardous operating conditions and does not actively instigate traffic accidents. The alternate safety trajectories generated can effectively guide the ego vehicle towards a safe state. Furthermore, the computation time for each scenario can be contained within a 100 ms replanning cycle, indicating that our proposed online safety verification technology can promptly complete the safety verification of the expected trajectory and generate the alternate safety trajectory. The current simulation verification time is influenced by the software overhead of the high-level language and the simulation environment. When this method is ported to an embedded environment, the real-time performance can be further improved, optimizing the process even further.

VI. CONCLUSION

We present an innovative method for real-time online safety verification in automated driving decision-making. This methodology employs a synergy of both explicit and implicit traffic regulations to systematically predict all legal permutations of traffic scenarios. Following this prediction, it calculates the potential reachability area for each traffic participant, and subsequently verify the validity of the expected trajectory against legal safety measures, creating an alternative safety trajectory where necessary. The efficacy of our proposed online safety verification approach, particularly its safety and real-time performance, is evaluated using the PreScan and Matlab platforms within a simulated environment. Its robustness is tested across characteristic traffic scenarios, demonstrating the method's ability to uphold a safe trajectory for the autonomous vehicle, thereby averting potential hazards. The proposed method effectively addresses the safety "long tail" problem of autonomous driving decision-making in unfamiliar and complex traffic scenarios. It can be integrated into autonomous driving systems, running in parallel with existing decision-making systems, to continuously verify the safety of the current decision-making process in real-time. Additionally, it enables the system to switch to alternative trajectories promptly in hazardous situations, providing crucial support for the safety and reliability of autonomous driving decision-making.

In future investigations, we aim to expand the complexity of the traffic scenarios, examine the regions for pedestrians, and explore the potential use of machine learning algorithms to compute alternative safe trajectories within the legally reachable region of the autonomous vehicle.

REFERENCES

[1] S. Zang, M. Ding, D. Smith, P. Tyler, T. Rakotoarivelo, and M. A. Kaafar, "The impact of adverse weather conditions on autonomous vehicles: How rain, snow, fog, and hail affect the performance of a self-driving car," *IEEE Veh. Technol. Mag.*, vol. 14, no. 2, pp. 103–111, Jun. 2019.

[2] Y. Ma, C. Sun, J. Chen, D. Cao, and L. Xiong, "Verification and validation methods for decision-making and planning of automated vehicles: A review," *IEEE Trans. Intell. Vehicles*, vol. 7, no. 3, pp. 480–498, Sep. 2022.

[3] A. Christensen, A. Cunningham, and J. Engelman, "Key considerations in the development of driving automation systems," in *Proc. 24th Enhanced Safety Vehicles Conf.*, Gothenburg, Sweden, 2015, pp. 1–9.

[4] M. Benmimoun, "Effective evaluation of automated driving systems," SAE, Warrendale, PA, USA, Tech. Paper, 2017.

[5] M. Quinlan, T.-C. Au, J. Zhu, N. Stiurca, and P. Stone, "Bringing simulation to life: A mixed reality autonomous intersection," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, Oct. 2010, pp. 6083–6088.

[6] Y. M. Liu, J. Su, and H. D. Pan, "Application of virtual instrument technology in automobile performance test," *China J. Highway Transp.*, vol. 18, no. 2, pp. 112–115, 2005.

[7] O. Kirovskii, "Determination of validation testing scenarios for an ADAS functionality: Case study," SAE, Warrendale, PA, USA, Tech. Paper, 2019.

[8] S. Otten, J. Bach, and C. Wohlfahrt, "Automated assessment and evaluation of digital test drives," in *Advanced Microsystems for Automotive Applications 2017: Smart Systems Transforming the Automobile*. New York, NY, USA: Springer, 2018, pp. 189–199.

[9] Y. Zhang, S. Lu, Y. Yang, and Q. Guo, "Internet-distributed vehicle-in-the-loop simulation for HEVs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3729–3739, May 2018.

[10] D. Zhao, H. Lam, H. Peng, S. Bao, D. J. LeBlanc, K. Nobukawa, and C. S. Pan, "Accelerated evaluation of automated vehicles safety in lane-change scenarios based on importance sampling techniques," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 595–607, Mar. 2017.

[11] L. Li, X. Wang, K. Wang, Y. Lin, J. Xin, L. Chen, L. Xu, B. Tian, Y. Ai, J. Wang, D. Cao, Y. Liu, C. Wang, N. Zheng, and F.-Y. Wang, "Parallel testing of vehicle intelligence via virtual-real interaction," *Sci. Robot.*, vol. 4, no. 28, Mar. 2019, Art. no. eaaw4106.

[12] A. Sinha, M. O'Kelly, R. Tedrake, and J. C. Duchi, "Neural bridge sampling for evaluating safety-critical autonomous systems," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 33, 2020, pp. 6402–6416.

[13] S. Feng, H. Sun, X. Yan, H. Zhu, Z. Zou, S. Shen, and H. X. Liu, "Dense reinforcement learning for safety validation of autonomous vehicles," *Nature*, vol. 615, no. 7953, pp. 620–627, Mar. 2023.

[14] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 1, pp. 90–96, Jan. 2017.

[15] N. Kalra and S. M. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?" *Transp. Res. A, Policy Pract.*, vol. 94, pp. 182–193, Dec. 2016.

[16] F. Oboril and K.-U. Scholl, "Risk-aware safety layer for AV behavior planning," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Oct. 2020, pp. 1922–1928.

[17] F. Oboril and K.-U. Scholl, "RSS+: Pro-active risk mitigation for AV safety layers based on RSS," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jul. 2021, pp. 99–106.

[18] M. Naumann, F. Wirth, F. Oboril, K. Scholl, M. S. Elli, I. Alvarez, J. Weast, and C. Stiller, "On responsibility sensitive safety in car-following situations—A parameter analysis on German highways," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jul. 2021, pp. 83–90.
[19] H. Königshof, F. Oboril, K.-U. Scholl, and C. Stiller, "A parameter analysis on RSS in overtaking situations on German highways," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2022, pp. 1081–1086.
[20] A. Rodionova, I. Alvarez, M. S. Elli, F. Oboril, J. Quast, and R. Mangharam, "How safe is safe enough? Automatic safety constraints boundary estimation for decision-making in automated vehicles," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Oct. 2020, pp. 1457–1464.
[21] B. Gassmann, F. Oboril, C. Buerkle, S. Liu, S. Yan, M. S. Elli, I. Alvarez, N. Aerrabotu, S. Jaber, P. van Beek, D. Iyer, and J. Weast, "Towards standardization of AV safety: C++ library for responsibility sensitive safety," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2019, pp. 2265–2271.
[22] F. Pasch, F. Oboril, B. Gassmann, and K.-U. Scholl, "Vulnerable road users in structured environments with responsibility-sensitive safety," in *Proc. IEEE Int. Intell. Transp. Syst. Conf. (ITSC)*, Sep. 2021, pp. 270–277.
[23] M. Koschi, C. Pek, M. Beikirch, and M. Althoff, "Set-based prediction of pedestrians in urban environments considering formalized traffic rules," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 2704–2711.
[24] M. Althoff and S. Magdici, "Set-based prediction of traffic participants on arbitrary road networks," *IEEE Trans. Intell. Vehicles*, vol. 1, no. 2, pp. 187–202, Jun. 2016.
[25] S. Manzinger, C. Pek, and M. Althoff, "Using reachable sets for trajectory planning of automated vehicles," *IEEE Trans. Intell. Vehicles*, vol. 6, no. 2, pp. 232–248, Jun. 2021.
[26] C. Pek, S. Manzinger, M. Koschi, and M. Althoff, "Using online verification to prevent autonomous vehicles from causing accidents," *Nature Mach. Intell.*, vol. 2, no. 9, pp. 518–528, Sep. 2020.
[27] OpenDRIVE. (2021). *ASAM OpenDRIVE V1.6.1 User Guide*. Accessed: Mar. 1, 2022. [Online]. Available: http://www.opendrive.org/

FEI GAO received the B.S. and Ph.D. degrees in automotive engineering from Jilin University, Changchun, China, in 2011 and 2017, respectively. From 2014 to 2015, she was a Visiting Student in Berkeley, CA, USA.

She is currently an Associate Professor with the State Key Laboratory of Automotive Simulation and Control Automotive Engineering, Jilin University. Her research interests include automotive human engineering and motion sickness. She is the coauthor of three books, more than 20 articles, and more than ten inventions. She is a member of the Society of Automotive Engineers.

CHENG LUO was born in Bijie, Guizhou, China, in 2000. He received the B.Sc. degree from Jilin University, in 2022. He is currently pursuing the master's degree with Tongji University.

His main research field is automotive cyber security, including the analysis and assessment of potential threats and risks, the generation of onboard network datasets along with their corresponding intrusion detection, and the development of robust platforms designed for comprehensive security testing.

FANGYUAN SHI received the master's degree in vehicle engineering from Chongqing University, in December 2010.

Since 2011, he has been engaged in vehicle collision safety research and development with Chongqing Chang'an Automobile Company Ltd. His research areas include full-vehicle structural collision simulation, material fracture failure models, and battery mechanical impact safety. His current research focus is on collision risk prediction.

XIANQING CHEN received the master's degree in mechanical design and theory from Tianjin University, in June 2007. Since 2007, he has been involved in vehicle collision safety research and development with Chongqing Chang'an Automobile Company Ltd. His research areas encompass full-vehicle structural durability and characterization of material mechanical properties. His current research focus is on occupant protection control algorithms.

ZHENHAI GAO was born in Changchun, Jilin, China, in 1973. He received the Ph.D. degree in automotive engineering from Jilin University.

He is currently the Deputy Dean of Automotive Engineering and the Director of the State Key Laboratory of Automotive Simulation and Control Automotive Engineering at Jilin University. His research interests include autopilot technology and human engineering. He is the coauthor of three books. More than 100 articles have been published and 20 invention patents have been authorized.

Prof. Gao is a Distinguished Member of the Expert Committee Intelligent Connected Vehicle Innovation Alliance, the Chairperson of the Industrial Design Association in Jilin Province, and the Editorial Board Member of the *International Journal of Human Factors Modelling and Simulation*.

RUI ZHAO (Member, IEEE) was born in Liaoyuan, Jilin, China, in 1986. She received the B.S. degree in computer science and technology from Northeast Normal University, in 2009, and the Ph.D. degree in computer science and technology from Jilin University, Changchun, China, in 2017.

She is currently an Associate Professor with the College of Automotive Engineering, Jilin University. Her research focuses on cooperative control, functional safety, cybersecurity, and safety reinforcement learning for connected and automated vehicles. She has authored about 30 journal articles and ten patents in China. She authored the monograph "Cyber Security Technology for Intelligent Automotive."

Prof. Zhao holds membership in the Society of Automotive Engineers.