Formal Analysis of Vehicular Crash Severity using KeYmaera X

Oumaima Barhoumi[1], Mohamed H Zaki[2], and Sofiène Tahar[1]

[1] Concordia University, Montreal, Quebec, Canada
{o_barh,tahar}@ece.concordia.ca
[2] Western University, London, Ontario, Canada
mzaki9@uwo.ca

Abstract. In this paper, we integrate formal methods with traffic conflict techniques such as Time-To-Collision and Deceleration Rate, and evasive action indicators, like Jerk Profile and Yaw Rate in order to introduce a practical traffic safety rule. We propose the use of formal methods to prove the correctness of this traffic safety rule and verify road users' compliance with it. To this end, we utilize differential dynamic logic and the KeYmaera X theorem prover for the formalization and verification of this rule. Furthermore, we conduct a formal analysis of crash severity applied to different traffic collision scenarios to determine the optimal evasive actions to be taken during a traffic conflict, along with their appropriate intensity. Using KeYmaera X, we are able to automatically verify the proposed traffic safety rule in three traffic collision scenarios, namely rear-end and head-on and left-side collisions.

Keywords: Formal Verification · Traffic Conflict Techniques · Transportation Safety · Crash Severity · KeYmaera X.

1 Introduction

Urban mobility is witnessing a growing reliance on advanced driver-assistance systems for traffic safety mitigation. Yet, these systems and the anticipated deployment of driverless vehicles expose the traffic network to an unprecedented level of technologies that might not be fully mature to deal with the complex nature of the traffic culture. While Artificial Intelligence (AI) systems are known for their complexity and advanced capabilities, a lesser-known fact is that both actual self-driving cars and vehicles equipped with advanced driving-assistance systems (ADAS) operate on principles similar to those underlying ChatGPT and other large language models (LLMs) [13]. Both types of AI leverage statistical reasoning to predict the next word, phrase, or steering input, which places significant emphasis on recently used words or actions in their calculations. This kind of AI lacks a true understanding of the situation, context, or unobserved factors that a human would naturally consider in similar circumstances. However, the critical distinction is that while a language model might produce nonsensical or irrelevant output, a self-driving car has the potential to be fatal [13]. One relevant example is the 2018 Uber driverless vehicle fatal incident, where the vehicle

could not perform the evasive actions necessary to avoid a pedestrian [19]. Conventional methods for system verification, often relying on testing and simulation, differ significantly from formal verification tools like KeYmaera X and lack the mathematical rigor and formal guarantees provided by tools based on formal methods. Typically, they involve manual testing and debugging, which may not comprehensively address the intricate interactions within hybrid systems that combine discrete events and continuous dynamics. Formal methods refer to mathematically based techniques for the specification, design, verification, and validation of software and hardware systems. These methods use mathematical languages and tools to model and analyze systems, helping to ensure their correctness and reliability. Verification and validation of algorithms for perception, decision-making, and control using formal methods can help ensure that these systems operate safely and reliably. This is particularly important for avoiding accidents and minimizing risks associated with autonomous vehicles navigating in complex traffic scenarios. Therefore, the use of formal methods is essential in addressing safety-related challenges anticipated in road transportation while simultaneously establishing a well defined specification for traffic rules [5].

In the literature, established traffic safety rules define what constitutes safe conditions. However, the deployment of connected autonomous vehicles (CAVs) is presenting unprecedented challenges in adhering to these rules. This challenge is evident in the rising number of rear-end collisions involving automated vehicles compared to conventional human-driven vehicles in 2023 [13]. In this study, we have decided to focus not on defining safe conditions as a safety specification, but rather on identifying unsafe conditions that lead to collisions. Our objective with this approach is to establish a foundational framework that will enable further research to enhance CAVs by identifying clear and well-defined safe regions for operation, informed by understanding the unsafe conditions. To do so, we chose to dive deeper into the causes of these collisions by concentrating on a crucial phase that precedes a collision: traffic conflicts and the actions taken during them. Therefore, we conduct our analysis assuming that the vehicle is already in a traffic conflict. Hence, preventing these conflicts from leading to crashes is one of the main axes to focus on. In this context, Traffic Conflict Techniques (TCTs), also referred to as traffic safety indicators, are employed as a set of methods for identifying, assessing, and analyzing traffic conflicts. By adopting a broader perspective, TCTs enable a reliable traffic analysis that can offer insights into the underlying causes and risk factors associated with traffic conflicts. In this paper, we introduce a practical traffic safety rule based on the combination of TCTs such as Time-To-Collision and Deceleration Rate, and evasive-actions-based indicators, like Jerk Profile and Yaw Rate. Additionally, we propose to formally verify the developed rule using an automated prover in order to conduct a formal analysis of vehicular crashes and their anticipated severity.

In this work, we consider a temporal-proximity and two speed-related traffic safety indicators, namely Time-to-Collision (TTC), Delta-V and Extended Delta-V, respectively. TTC is a temporal proximity indicator [22] that is defined as the time remaining for a collision to take place between two involved

vehicles if no action is taken. Whereas, Delta-V (ΔV) represents the velocity variation of the vehicles prior and post-crash [9]. Extended Delta-V is a more precise indicator for predicting the likelihood and severity of a crash [9], as it calculates a hypothetical value of Delta-V instead of using the true value. In addition to these indicators, evasive action-based indicators such as jerk profile and yaw rate are also utilized to conduct a more accurate analysis of traffic conflicts and assess the success of a maneuver based on the intensity of these indicators. The jerk profile [6] provides a detailed insight into a vehicle's temporal acceleration dynamics. This metric is calculated as the derivative of the vehicle's acceleration, allowing us to capture rapid changes in acceleration over time. The yaw rate [6] quantifies the extent of swerving or rotational motion exhibited by a vehicle during maneuvers. Understanding the yaw rate is essential for evaluating the intensity of a vehicle's response when evading obstacles, navigating curves, or making sharp turns. Our research aims to investigate the effectiveness of these evasive action-based indicators in resolving traffic conflicts by conducting a formal analysis of their intensity using formal methods. The main contribution of the paper lies in the integration and application of formal methods to solve specific safety challenges in transportation by (1) proposing a novel traffic rule established using temporal and spatial indicators along with evasive actions; and (2) using formal methods tool, KeYmaera X, to formally verify the proposed traffic rule in three different traffic scenarios.

Vehicles are complex systems that involve both continuous and discrete dynamics, where the former represents the vehicle's movement and the latter includes events such as gear changes and braking. The behavior of a vehicle in traffic is determined by the interaction between these dynamics. In this paper, we focus on formally verifying the proposed traffic safety rule combining the specified TCTs and evasive actions indicators, i.e., TTC, Extended Delta-V, jerk profile and yaw rate, respectively. To achieve this goal, we require a sufficiently expressive logic capable of reasoning about dynamic behaviors. This is essential for formalizing both the traffic safety indicators and the traffic safety rule, alongside a formal verification tool that ideally supports such logic in an automated fashion. Therefore, first- and higher-order logic theorem proving would be the most convenient formal verification method to achieve this goal. While studying existing automated and interactive theorem provers, we realized that the automated hybrid verification tool KeYmaera X [16] is the most appropriate for our work. In fact, KeYmaera X supports Differential Dynamic Logic (dL) [16] as the specification language, which will enable us to efficiently study the traffic safety rule in different car crash scenarios. Moreover, KeYmaera X provides a rigorous and systematic proof engines suitable for checking whether the vehicle complies with the safety specifications. The TCTs employed in this process will be scrutinized, and based on their evaluation, a decision will be made regarding the safe management of the involved vehicles by determining the appropriate intensity of the evasive actions indicators. In this paper, we aim to improve road safety by developing a better understanding of the causes of traffic conflicts and developing effective strategies to prevent them. This is achieved by adopting

a proactive approach that consists of formally analyzing the severity of traffic conflicts and determining the convenient evasive measures to be taken as well as their intensities to prevent potential vehicular crashes. The proof files for the traffic safety rule formalized in KeYmaera X are available online [3].

The rest of the paper is organized as follows. In Section 2, we review the works done earlier relating TCTs and formal verification. In Section 3, we provide some preliminaries of the employed TCTs and their mathematical representation. Section 4 describes the traffic safety rule formal structure. Whereas Section 5 covers the formalization process of the introduced traffic safety rule. Finally, we conclude this work in Section 6.

2 Related Work

The use of formal methods in the field of transportation is recognized by researchers based on its own merits in verifying safety critical systems such as vehicles. Thanks to their rigorous nature, formal verification aims to deliver sound systems that meet their specifications by applying various techniques, such as runtime monitoring, model checking and interactive or automated theorem proving. For instance, Mao et al. [12], modeled a cooperative adaptive cruise control system using the CHARON modeling language and applied runtime monitoring to check the model against safety properties defined using the temporal logic MEDL through simulation. Although the authors utilize a formal modeling language (MEDL) for specifying the properties, their approach involves a simulation-based case study for monitoring the safety properties. In the work of Althoff et al. [1], algorithmic verification which is an extension of model checking was applied online to make sure that a self-driving vehicle will avoid static objects as well as dynamic obstacles on the road. In this work, the assumption of the other car strictly adhering to road traffic regulations oversimplifies real-world traffic complexity and uncertainty. Unpredictable behavior and distracting factors are also not considered, limiting the proposed approach's ability to capture dynamic traffic scenarios.

The authors of [17] provided a formally verified checker of the safe distance rule in order to verify if an autonomous vehicle complies with traffic rules using the interactive theorem prover Isabelle/HOL. The study neglects to consider the interactions between the subject vehicle and other vehicles, as well as the surrounding environment. These interactions could be indicated by traffic safety indicators like Time-To-Collision. When it comes to the verification of the entirety of the traffic system, Loos et al. [11] developed a formal proof of a distributed car control system to verify that the control model guarantees collision freedom for arbitrarily many cars using the KeYmaera automated theorem prover. While the study successfully provides formal verification results for collision freedom, accounting for uncertainties in the environment, such as the presence of unpredictable objects or obstacles, is crucial for its real-world deployment. Incorporating these factors into the formal verification process can

provide a more accurate assessment of the system's reliability under diverse circumstances. In [14], the work of Mitsch et al. was one of the early attempts to utilize formal verification tools in the modeling of freeway dynamics. The authors used dL for the formulation and verification of the system specifications using KeYmaera. However, it is important to acknowledge that the current approach does not fully address uncertainties in the environment or incorporate real-world constraints and scenarios into the verification process.

The studies mentioned above cover the verification of different safety aspects of the vehicle and its interaction with the outer environment. However, none of them explores the verification of TCTs, which serve as traffic safety indicators. In our work, we are taking interest in the verification of a new traffic safety rule linking TCTs indicators, i.e., TTC, Delta-V, and Extended Delta-V, along with evasive actions indicators, i.e., jerk profile and yaw rate. The formalization of this rule and its verification will introduce accurate safety bounds for driver behaviors during traffic conflicts to avoid collisions by studying different case scenarios and identifying the severity level of crashes if they were to happen. In light of this, and inspired by the work of [11] and [14] using KeYmaera, we will employ the KeYmaera X hybrid theorem prover which is an extension of KeYmaera to conduct the verification process.

3 Preliminaries

To ease the readability of the paper, in this section we provide a preliminary introduction to relevant notions of TCTs and evasive actions indicators along with their mathematical formulations. We also provide an overview of the KeYmaera X theorem prover and a summary of the used differential dynamic logic syntax.

3.1 Traffic Conflict Techniques

In this paper, we apply different TCTs and evasive action indicators, furthermore, we provide their mathematical formulation for different collision scenarios. In this case, the vehicles involved in the collision are assumed to have identical properties, such as length, i.e., $L_1 = L_2 = L$, and mass, i.e., $m_1 = m_2 = m$. Assuming vehicles have equal masses and lengths is essential for simplifying the analysis of crash severity. Without this assumption, we would need to account for various vehicle shapes, sizes (like SUVs, vans, compacts), and weights, leading to a multitude of sub-cases and a wide range of crash severity levels to analyze. Moreover, we only consider the execution of evasive actions, i.e., braking and swerving, in a sequential manner rather than simultaneously.

Time To Collision: TTC is defined as the time required for two vehicles to collide if they continue at their present speed and on the same path [7]. In the work of [8] a TTC of 4 seconds signifies the presence of a conflict situation for a vehicle. However, the same study revealed that TTC values in the range of 4 to 5

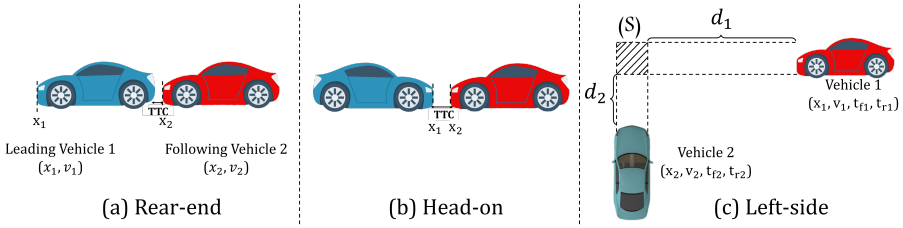

Fig. 1: Collision Scenarios

seconds sometimes led to false positives, indicating potential collisions when, in fact, a typical braking maneuver would have safely resolved the traffic conflict. As a result, it is acknowledged in the literature [8] that setting a TTC threshold at 3 seconds is appropriate for safety evaluation. TTC can be computed for various traffic interactions. In our case, we define TTC in rear-end, head-on, and left-side collision situations, where we use the indexes *1* and *2* to refer to the leading and following vehicles in traffic as shown by Figure 1:

1. **Rear-end collision:** TTC is measured between two consecutive vehicles from the rear bumper of the leading vehicle to the front bumper of the following vehicle as shown by Figure 1.a. The formula to compute TTC for two consecutive vehicles in a rear-end collision scenario is defined as [22]:

$$TTC_1 = \frac{x_1 - x_2 - L_1}{v_2 - v_1}, \qquad v_2 > v_1 \tag{1}$$

   The bumper positions and velocities of vehicles 1 and 2 are represented by the variables x_1, x_2, v_1, and v_2, respectively. Additionally, L_1 represents the length of the leading vehicle, which is vehicle 1, while the following vehicle is represented by vehicle 2.

2. **Head-on collision:** In this collision scenario, TTC is measured between the front bumpers of the two involved vehicles as reflected by Figure 1.b. Therefore, the formula of TTC is modified as [10]:

$$TTC_2 = \frac{x_1 - x_2}{v_1 + v_2} \tag{2}$$

   where x_1, x_2, v_1 and v_2 are the positions and velocities of vehicles 1 and 2, respectively.

3. **Left-side collision:** In this case, the definition of TTC, as illustrated by Figure 1.c, is revised by considering the time instances corresponding to the arrival of the front and rear-ends of both vehicles 1 and 2 at the conflict-to-collision region (S), denoted as t_{f1}, t_{r1}, t_{f2} and t_{r2}, respectively. The TTC in this case is determined as follows [10]:

$$t_{f1} < t_{f2} < t_{r1}; \quad TTC_3 = \frac{d_2}{v_2} \tag{3}$$

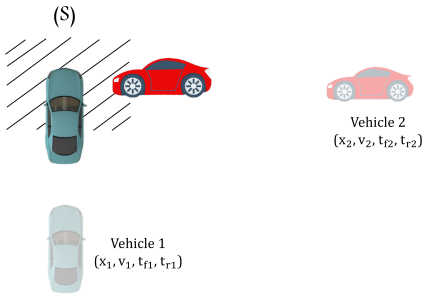

Fig. 2: Left-Side Traffic Conflict

$$t_{f2} < t_{f1} < t_{r2}; \quad TTC_3 = \frac{d_1}{v_1} \tag{4}$$

where v_1 and v_2 represent the vehicles' velocities and d_1 and d_2 are defined as the x-distance and y-distance separating vehicles 1 and 2 from the region (S) respectively.
In this scenario, we are examining a left-side collision, where either vehicle 1 reaches the conflict-to-collision region (S) after vehicle 2, or vice-versa. If TTC is less than 3 seconds, both vehicles are considered to be involved in a traffic conflict. The time intervals specified in Equations 3 and 4 are conditions that define a mathematical formulation of TTC, enabling a continuous TTC calculation during traffic conflicts. In this study, we will proceed with the Time-To-Collision given by Equation 3, i.e., TTC_3, where vehicle 1 arrives at the conflict-to-collision region (S) while vehicle 2 has not yet left this region which leads to a traffic conflict, as shown by Figure 1.c. This is described by the arrival of the front of vehicle 2, i.e., t_{f2}, before the arrival of the rear of vehicle 1, i.e., t_{r1}, and after the arrival of the front of vehicle 1, i.e., t_{f1}, reflecting a traffic conflict during which TTC can be computed as given by Equation 3. This relationship is depicted schematically in Figure 2.

Extended Delta-V: Extended Delta-V (Ext-ΔV) is a speed-related indicator describing the speed reduction rate of vehicles due to an unexpected event, e.g., conflict, collision [9]. It is used as an informative measure of the possibility of a crash occurrence and whether or not a preventive action was taken. The value of this indicator foresees the severity of the collision should it happen. For this, Extended Delta-V represents the theoretical value of Delta-V if the taken evasive action was successful. In the case where the collision takes place, the value of Extended Delta-V converges to the true value of Delta-V. Whereas, Extended Delta-V abides by the same general rule to determine the value of Delta-V, given by Equation 5 to determine its value. The specificity of this indicator compared to the classical Delta-V lies in the vehicle's speed definition prior to a conflict.

This indicator as defined in Equation 6, incorporates braking as an evasive measure linked to a temporal indicator. In a traffic conflict, the chosen temporal

indicator within a collision course is TTC. It gauges the proximity to collision, multiplied by a deceleration rate, in order to determine the required evasive action for crash avoidance. Severity assessment is based on the aggressiveness and remaining time to the collision.

$$\textit{Ext-}\Delta V = V_{post} - V \tag{5}$$

$$V = v_0 - a * TTC \tag{6}$$

Under the assumption that it is an *inelastic collision* [18] and in the case of two vehicles colliding, those vehicles will stick together after the crash, i.e., $\mathrm{V}_{1post} = \mathrm{V}_{2post} = \mathrm{V}_{post}$. Mathematically, an inelastic collision is translated by [18]:

$$m_1 * v_1 + m_2 * v_2 = (m_1 + m_2) * V_{post} \tag{7}$$

Given our assumption that the masses of vehicle 1 and vehicle 2 are equal, i.e., $m_1 = m_2 = m$, V_{post} is deduced as:

$$V_{post} = \frac{v_1 + v_2}{2} \tag{8}$$

Jerk Profile: The studies in [2] and [21] reveal that acceleration patterns in normal driving situations can resemble those in conflict situations. Relying solely on the deceleration profile may not accurately evaluate the severity of vehicle interactions. Instead, the jerk profile, which measures the rate of change of acceleration, can detect transitions from light braking to sudden and intense braking. The jerk profile is defined as a function of the vehicle's acceleration, i.e., a:

$$J = \frac{\mathrm{d}a}{\mathrm{d}t} \tag{9}$$

Analyzing the jerk profile allows differentiation between traffic conflict situations and normal or near-miss situations. For instance, a traffic conflict is characterized by a strong negative value of the jerk, where the highest value computed by the jerk is found to be -15 $\mathrm{m/s^3}$ seeing that any greater value will be considered mechanically unfeasible [21]. As for a situation where normal braking is executed, the highest value of jerk computed is at -8 $\mathrm{m/s^3}$. Based on the findings of multiple researchers, such as [15] and [2], a threshold value of the jerk profile is defined in Equation 10, to be equal to -9.82 $\mathrm{m/s^3}$, as an indicator of safety-critical driving behavior. Mathematically, the jerk profile is defined as follows:

$$-9.82 m/s^3 \leq J < -15 m/s^3 \tag{10}$$

Yaw Rate: Braking, as an evasive action, is not always sufficient to avoid a crash. Swerving is a variation of the heading angle in a chosen direction once the vehicle is found in a conflict situation. The yaw rate is used as the indicator to quantify this, it is used to describe the change of the heading angle in a

Table 1: Statements of Hybrid Programs [16]

Statement	Effect
$x := e$	discrete assignment of the current value of term e to variable x
$x{:=}*$	nondeterministic assignment of an arbitrary real number to x
$?P$	continue if first-order formula P holds in the current state, abort otherwise
$x'{=}f(x)\ \&\ Q$	follow differential equation $x' = f(x)$ within evolution domain Q for any duration
$\alpha;\beta$	sequential composition, first performs α and then β afterwards
$\alpha \cup \beta$	nondeterministic choice, following either α or β
α^*	nondeterministic repetition, repeating α $n \geq 0$ times

short period. Mathematically, the yaw rate and the vehicle's heading angle θ are defined as follows [20]:

$$r(t) = \frac{\mathrm{d}\theta}{\mathrm{d}t} \tag{11}$$

$$\theta = \frac{x}{rd} \tag{12}$$

with x as the vehicles position and rd representing the radius of the curve. The range of the yaw rate is defined based on the safety of the action after its execution. With regards to resolving a traffic conflict by swerving, we propose a range of [0, 45] degrees, i.e., [0, 0.785] radians [4], for effective maneuvering in response to a traffic conflict while maintaining control of the vehicle:

$$0 < r \leq 0.785 \tag{13}$$

3.2 KeYmaera X Theorem Prover

KeYmaera X is an interactive theorem prover for hybrid systems supporting differential dynamic logic (dL) that is based on first-order logic, along with a program notation for hybrid systems [16]. dL is a single language that integrates operational system models and formulas. In dL, a hybrid program (HP) is a compositional program notation for hybrid systems, which include both discrete and continuous behaviors. A HP consist of various program statements, including differential equations that describe continuous behaviors. A summary of the used syntax and informal semantics of hybrid programs is given in Table 1, where HPs are composed of different elements such as α and β, which are also HPs, x represents variables that can be used within an HP, e denotes a term that may contain x, and P and Q are formulas of first-order logic of real arithmetic [16]. Thanks to its interfacing with several provers and tools that are invoked transparently in the background, e.g., Mathematica or Z3 SMT Solver, KeYmaera X stands out by implementing automatic proof strategies to enable the compositional verification of large systems. To verify the proposed safety traffic rule in KeYmaera X, the proving process is based on a series of applied automatic proof strategies. For instance, the rule of the hybrid program including a differential

equation requires solving the dynamics of hybrid systems, i.e., vehicles. Afterwards, the obtained solutions are used to prove each sub-goal of the rule until reaching the main goal. Eventually, KeYmaera's verification process results in either a proven rule or an error that disables the prover from continuing the process. In our case, the correctness of the rule is proved for the three different scenarios of rear-end, head-on, and left-side collision.

4 Crash Severity Analysis

In this section, we discuss in detail the proposed methodology for crash severity analysis using the KeYmaera X theorem prover, followed by a detailed description of the traffic safety rule specification.

4.1 Proposed Methodology

The proposed methodology for the formal analysis of crash severity is depicted in Figure 3. As illustrated in the figure, the first step of our approach involves the formulation of traffic conflict indicators, including Time-To-Collision, Extended Delta-V, and deceleration rate. Additionally, we define evasive action indicators such as jerk profile and yaw rate. These indicators are then formalized using dL, which serves as the specification logic in our approach. Subsequently, we establish a traffic safety rule that specifies safe conditions, defined by predefined thresholds for each indicator, and the consequences of their violation, i.e., an Imminent collision. In this context, we examine three distinct collision scenarios: rear-end, head-on, and right-side. The collision scenarios presented in this study are illustrative of basic cases, yet they serve as an illustration of potential real-world interactions involving two different vehicles. This traffic safety rule states that"If these thresholds are violated and appropriate evasive actions are not taken with the correct level of intensity, a collision will occur". The first step in defining this rule is to introduce its pre-conditions based on the inputs for the system, such as the vehicle's environment parameters. The next step is to model the hybrid system, given the vehicle's dynamics, using an ordinary differential equation (ODE) due to the continuous evolution of the system. Lastly, the post-conditions are introduced to describe every speed interval and its association with a deceleration variable. These steps are carried out in the KeYmaera X theorem prover where the verification process will take place.

The evaluation of the consequences of violating traffic safety rules is based on predefined thresholds of safety traffic indicators (cf. Section 3.1). The impact of such violations is studied in three distinct traffic scenarios. In each scenario, a formal analysis is conducted to assess the severity of potential crashes based on the specific situation. To deduce the severity level of a crash, we rely on the values of TTC and Delta-V as well as the speeds of the vehicles involved in a traffic conflict. These severity levels include categories such as *property damage only*, *potential injury*, *non-severe injury*, and *severe injury* depending on the speeds of the vehicles involved in the traffic conflict. We achieve this by monitoring the

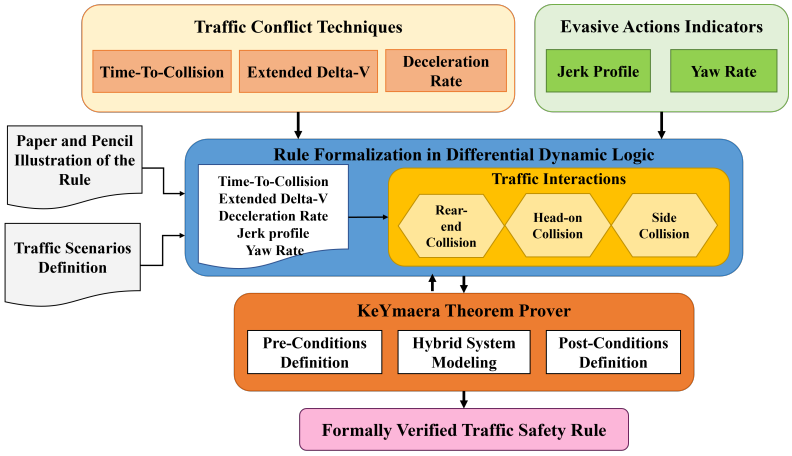

Fig. 3: Methodology for Formal Crash Severity Analysis

variation of the value of Extended Delta-V and the speeds of the two involved vehicles entering the traffic conflict. Once the involved vehicles are found in a traffic conflict, the interpretation of the values of the safety indicators determines the severity level of the crash should it happen.

In this study, we evaluate crash severity by categorizing involved vehicles into speed intervals. The speed ranges are as follows, increasing in 20 km/h increments: [0, 20), [20, 40), [40, 60), [60, 80). The final interval, [80, 150), encompasses speeds starting from 80 km/h, and extends up to 150 km/h. This range is chosen to represent speeds for standard vehicles, with 150 km/h being the maximum speed considered for this category. While formalizing speed and defining deceleration as a function of speed can result in a more concise and self-contained formalization, in our approach, we opted for explicitly representing speed values to emphasize the significance of the severity analysis and its importance. In the course of our study, we consider different speed intervals to account for different deceleration rates as given by Equation 14, which is applied in the event of a traffic conflict, where the variable a refers to the assigned deceleration and $b_0 < b_1 < b_2 < b_3 < b_4$. However, it is important to note that these rates are approximations, as the precise intensity of braking cannot be determined without additional information about the surrounding conditions and environment of the conflict.

$$a = \begin{cases} b_0, & 0 < v \leq 20 \\ b_1, & 20 < v \leq 40 \\ b_2, & 40 < v \leq 60 \\ b_3, & 60 < v \leq 80 \\ b_4, & 80 < v \end{cases} \tag{14}$$

4.2 Traffic Safety Rule Specification

The traffic safety rule is formulated based on the Extended Delta-V, as described in Equation 6, and incorporates various traffic conflict indicators, including Time-to-Collision (TTC), jerk profile, and yaw rate. This comprehensive rule addresses multiple collision scenarios in order to provide a robust and thorough approach for ensuring traffic safety. While traditional traffic safety rules typically aim to establish safe conditions for vehicles to navigate traffic conflicts successfully, our approach stands out by proposing a traffic safety rule that delineates non-safe conditions. In other words, it focuses on identifying traffic conflicts wherein the involved vehicles could potentially collide if appropriate evasive measures are not taken with the right intensity. A traffic conflict happens if one or all of the involved vehicles violate a traffic rule, show signs of bad driving, or simply join a zone where a conflict is already taking place. In this context, our reasoning is based on the TTC value and its defined threshold to start studying the safety of the involved vehicles. Once the computed value of TTC is less than 3 sec, the first tested evasive action is braking. The rate of deceleration is chosen based on the speed of the vehicle. Furthermore, the intensity of this rate is evaluated using the jerk profile to determine the sufficiency of the action. Should the deceleration rate prove inadequate to prevent a collision, an additional evasive action must be undertaken to ensure that the collision does not occur. The complementing action, i.e., swerving, is inspected using the defined yaw rate indicator, and its effectiveness is also evaluated. In the analysis, the speed of the involved vehicles plays a crucial role in determining the type and intensity of the required evasive action. In instances where these actions fall short, a potential collision becomes likely. The severity level of each collision is established by considering the speeds of the vehicles involved at the time of the traffic conflict. The sketch of the defined traffic safety rule is represented as follows: $\texttt{(Initial State} \wedge \texttt{TCTs thresholds violated)} \longrightarrow \big[\{\texttt{(control);(Vehicles' Dynamics)}\}*\big]\texttt{(TCTs thresholds violated)} \longrightarrow \texttt{Collision)}$, starting from an initial state, i.e., `Initial State`, where the thresholds defined for the TCTs indicators are violated, i.e., `TCTs thresholds violated`, a collision, i.e., `Collision`, is bound to take place. This occurs if the execution of the control part, `control`, reflected by the braking and/or governed by its dynamics (`Vehicles' Dynamics`), proves insufficient in safely mitigating the traffic conflict [3].

5 Verification of the Traffic Safety Rule

In this section, a formal description of the traffic safety rule structure is detailed along with its formalization in differential Dynamic Logic (dL). Furthermore, the verification process of the formalized rule in KeYmaera X is described in different traffic scenarios.

5.1 Formal Specification of the Traffic Safety Rule

In this section, we provide a description of the conditions that can lead to a collision, where we cover the corner cases that a driver can face during a traffic conflict. Furthermore, we present a comprehensive formal definition that provides a formalized understanding of these conditions. For a TTC less than 3 sec, we consider the following corner cases.

1. **Ext-Δ V_p < Ext-ΔV:** In this context, Ext-ΔV_p represents the speed change calculated after deceleration. This condition specifies that when a conflict is detected, an imminent collision is likely if the speed variation, denoted as Ext-ΔV_p, is less than the initial Extended-Delta V value, denoted as Ext-ΔV, which is typically computed under normal traffic conditions. This situation prompts further investigation into the following scenarios:
2. **(Jerk profile $\geq$ 0) $\wedge$ ((Yaw rate $\leq$ 0) $\vee$ (Yaw rate > 0.785)):** These values represent the failure to execute evasive actions; no braking and no swerving which leads immediately to an accident, should the situation remain unchanged during the conflict situation.
3. **(-9.9 < Jerk profile < 0) $\wedge$ ((Yaw rate $\leq$ 0) $\vee$ (Yaw rate > 0.785)):** In this case, the braking action reflects a deceleration rate demonstrating a normal braking situation which is not substantial enough to mitigate the conflict at hand safely. Furthermore, the yaw rate indicates that the trajectory was unchanged meaning no swerving was done. Once combined, these conditions eventually will lead to a collision that may or may not be severe depending on the involved vehicles' speed.
4. **(-15 < Jerk profile $\leq$ -9.9) $\wedge$ ((Yaw rate $\leq$ 0) $\vee$ (Yaw rate > 0.785)):** A jerk profile falling in the defined interval does not necessarily translate into a successful deceleration rate. In fact, the braking might not be enough to stop the vehicle before engaging in the collision. For this to be avoided, the deceleration can be accompanied with a minimum of swerving to make sure that the accident is avoided. The absence of the swerving in this case might be critical and can even lead to a collision that will have a certain impact depending on the vehicles' speeds.

The four aforementioned corner cases are formally represented in dL as follows, where J indicates the jerk profile, while r represents the yaw rate.

Definition 1: $\texttt{TCT}_{violated} \equiv \texttt{(TTC} \leq \texttt{3)} \wedge \texttt{(Ext-}\Delta\texttt{V}_p < \texttt{Ext-}\Delta\texttt{V)} \wedge \Big(\texttt{((J} \geq \texttt{0)} \vee \texttt{((r} \leq \texttt{0)} \vee \texttt{(r} > \texttt{0.785))}\Big) \vee \Big(\texttt{(-9.9} < \texttt{J} < \texttt{0)} \wedge \texttt{((r} \leq \texttt{0)} \vee \texttt{(r} > \texttt{0.785))}\Big) \vee \Big(\texttt{(-15} < \texttt{J} \leq \texttt{-9.9)} \wedge \texttt{((r} \leq \texttt{0)} \vee \texttt{(r} > \texttt{0.785))}\Big)\Big)$

5.2 Formalization of Traffic Collision Scenarios

For every traffic interaction, i.e., rear-end, head-on and left-side collision, the mathematical modeling of the pre-conditions and vehicle dynamics differ. Therefore, the formalization of *Pre-conditions (init)* and *Vehicle Dynamics (dyn)* is given below for every traffic interaction.

1. **Rear-end Collision:** For a rear-end collision, the speed of the following vehicle and its evasive actions in a traffic conflict play a crucial role in assessing the potential crash severity. Denoting the assumed speeds of vehicles 1 and 2 as v_1 and v_2, respectively (where $v_2 > v_1$), the process begins with the calculation of the Extended Delta-V before a conflict. The monitoring of Time-To-Collision, i.e., TTC_1, comes into play, and when it equals or falls under 3 sec [8], an evasive action will be taken based on the value of v_2. Subsequently, the Extended Delta-V is recalculated and compared to the initial value to determine its strength in averting a potential collision. The formalization of the pre-conditions in dL, i.e., *init*, given below, establishes different bounds for the defined parameters.

Definition 2: $\texttt{init} \equiv (\texttt{v}_0 > 0) \wedge (\texttt{v}_{post} \geq 0) \wedge (\texttt{v}_1 \geq 0) \wedge (\texttt{v}_2 \geq 0) \wedge (\texttt{b}_0 > 0) \wedge (\texttt{b}_1 > \texttt{b}_0) \wedge (\texttt{b}_2 > \texttt{b}_1) \wedge (\texttt{b}_3 > \texttt{b}_2) \wedge (\texttt{b}_4 > \texttt{b}_3) \wedge (\texttt{m}_1 > 0) \wedge (\texttt{m}_2 > 0)\ (\texttt{rd} > 0) \wedge (\texttt{x}_2 < \texttt{x}_1) \wedge (\theta_2 = \frac{x_2}{rd}) \wedge (\texttt{TTC}_1 = \frac{x_1 - x_2 - L_1}{v_2 - v_1})$

The dynamics of the vehicle, given below, are modeled using its position x_2, velocity v_2 and acceleration a_2. The formalization of the ordinary differential equation (ODE) linking these parameters in KeYmaera X is given along with the derivation of the jerk profile J_2 and yaw rate r_2.

Definition 3: $\texttt{dyn} \equiv \texttt{x}_2\texttt{'} = \texttt{v}_2,\ \texttt{v}_2\texttt{'} = \texttt{a}_2,\ \texttt{a}_2\texttt{'} = \texttt{J}_2,\ \theta_2\texttt{'} = \texttt{r}_2$

The proof structure of the traffic safety rule in this collision scenario is depicted in Figure 4, where achieving a *No Collision* outcome (represented by the green leaf) is contingent on adhering to the TCTs thresholds and executing the required evasive actions. Failure to comply may lead to a collision, the severity of which can be determined by assessing the value of TTC_1, the speed of the vehicles and the Extended Delta-V value, as well as considering whether an evasive maneuver was attempted.

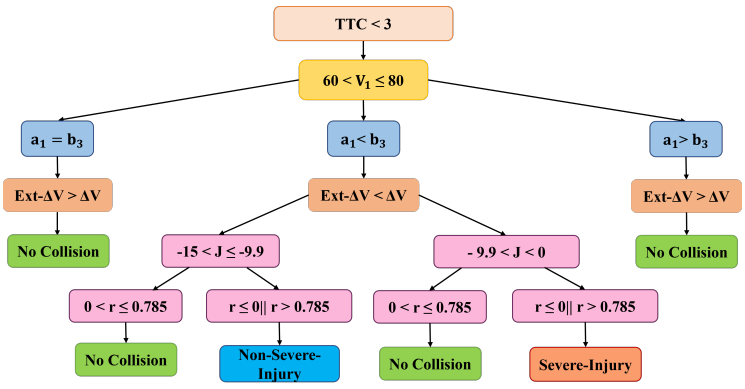

Fig. 4: Proof Structure and Formal Analysis of Crash Severity in a Rear-end Collision Scenario

2. **Head-on Collision:** For a head-on collision, once a traffic conflict situation is identified by Time-To-Collision $\text{TTC}_2 < 3$, the magnitude of the evasive action is carried out based on the speed interval. This magnitude is analyzed to conclude if the crash will happen or not and determine its severity in both cases. Based on the computed value of Extended Delta-V, a series of actions, i.e., braking and swerving, are executed to avoid the conflict safely. However, the execution of evasive actions in some cases proves either insufficient to avoid a collision or too strong for the situation at hand leading to further complications. For this, we build our study on analyzing the intensity of the taken actions by analyzing the obtained values for the rates indicators, jerk profile, and yaw rate, as measures for braking and swerving intensities, respectively. The formalization of the pre-conditions definition for this traffic scenario is described below:

Definition 4: $\texttt{init} \equiv (\texttt{v}_0 > 0) \wedge (\texttt{v}_{post} \geq 0) \wedge (\texttt{v}_1 \geq 0) \wedge (\texttt{v}_2 \geq 0) \wedge (\texttt{b}_0 > 0) \wedge (\texttt{b}_1 > \texttt{b}_0) \wedge (\texttt{b}_2 > \texttt{b}_1) \wedge (\texttt{b}_3 > \texttt{b}_2) \wedge (\texttt{b}_4 > \texttt{b}_3) \wedge (\texttt{m}_1 > 0) \wedge (\texttt{m}_2 > 0) \wedge (\texttt{rd} > 0) \wedge (\texttt{x}_2 \neq \texttt{x}_1) \wedge (\theta_1 = \frac{x_1}{rd}) \wedge (\theta_2 = \frac{x_2}{rd}) \wedge (\texttt{TTC}_2 = \frac{x_1 - x_2}{v_1 + v_2})$

As for modeling the system dynamics, the corresponding ODE is given for the involved vehicles, i.e., vehicle 1 and vehicle 2, using their positions x_1 and x_2, velocities v_1 and v_2, and accelerations a_1 and a_2, respectively. Furthermore, the jerk profile and yaw rate are computed for both vehicles and denoted as J_2, J_2, r_1 and r_2, respectively. The formalization of the dynamics of the system in dL is given below:

Definition 5: $\texttt{dyn} \equiv \texttt{x}_1\texttt{'} = \texttt{v}_1, \texttt{v}_1\texttt{'} = \texttt{a}_1, \texttt{a}_1\texttt{'} = \texttt{J}_1, \theta_1\texttt{'} = \texttt{r}_1, \texttt{x}_2\texttt{'} = \texttt{v}_2, \texttt{v}_2\texttt{'} = \texttt{a}_2, \texttt{a}_2\texttt{'} = \texttt{J}_2, \theta_2\texttt{'} = \texttt{r}_2$

3. **Left-side Collision:** A conflict situation taking place from the driver's left/right side on the main street is prone to happen under many favorable conditions. In this scenario, the defined Delta-V formula explicitly defines the angle using its *cosine* value. Using the formula defined in [9], the Extended Delta-V is calculated as:

$$Ext - \Delta V_i = \frac{m_i}{m_1 + m_2} . \sqrt{v_1^2 + v_2^2 - 2 v_1 v_2 \cos \alpha} \tag{15}$$

where m_i and v_i denote the mass and speed of vehicle i, with $i \in \{1, 2\}$ representing either vehicle 1 or 2, and α is the approaching angle. In this traffic scenario, Time-To-Collision, i.e., TTC_3, is defined based on on vehicles positioning, as described by Equations 3 and 4. For this case, $\alpha = 90^\circ$ is used to simplify things with a conflict-to-collision region, where the two involved vehicles will intercept each other if the crash is not avoided as shown by Figure 1.c. The formalization of the defined parameters as pre-conditions, *init*, is given below.

Definition 6: $\texttt{init} \equiv (\texttt{v}_0 > 0) \land (\texttt{v}_{post} \geq 0) \land (\texttt{v}_1 \geq 0) \land (\texttt{v}_2 \geq 0) \land (\texttt{b}_0 > 0) \land (\texttt{b}_1 > \texttt{b}_0) \land (\texttt{b}_2 > \texttt{b}_1) \land (\texttt{b}_3 > \texttt{b}_2) \land (\texttt{b}_4 > \texttt{b}_3) \land (\texttt{m}_1 > 0) \land (\texttt{m}_2 > 0) \land (\texttt{c} \geq \texttt{-1}) \land (\texttt{t}_{f1} > 0) \land (\texttt{t}_{f2} > 0) \land (\texttt{t}_{r1} > 0) \land (\texttt{t}_{r2} > 0) \land (\texttt{t}_{r1} > \texttt{t}_{f1}) \land (\texttt{t}_{r2} > \texttt{t}_{f2}) \land (\texttt{x}_2 \neq \texttt{x}_1) \land (\texttt{c} \leq 1) \land (\texttt{rd} > 0) \land (\theta_1 = \frac{x_1}{rd}) \land (\theta_2 = \frac{x_2}{rd}) \land (\texttt{TTC}_3 = \frac{d_2}{v_2})$

The formalization of the ODE modeling the system dynamics is given below for the involved vehicles, i.e., vehicle 1 and vehicle 2, using their positions x_1 and x_2, velocities v_1 and v_2, and accelerations a_1 and a_2, respectively. Moreover, the jerk profile and yaw rate are computed for both vehicles and denoted as J_1, J_2, r_1 and r_2, respectively.

Definition 7: $\texttt{dyn} \equiv \texttt{x}_1\texttt{'} = \texttt{v}_1, \texttt{v}_1\texttt{'} = \texttt{a}_1, \texttt{a}_1\texttt{'} = \texttt{J}_1, \theta_1\texttt{'} = \texttt{r}_1, \texttt{x}_2\texttt{'} = \texttt{v}_2, \texttt{v}_2\texttt{'} = \texttt{a}_2, \texttt{a}_2\texttt{'} = \texttt{J}_2, \theta_2\texttt{'} = \texttt{r}_2$

5.3 Formal Verification of the Traffic Safety Rule

When the conditions outlined in Definition 1 are met, it indicates an inevitable collision between the vehicles involved in the traffic conflict. In the context of a head-on collision, this is formally defined when the position of front bumper of vehicle 1, denoted as x_1, is equal to the position of the front bumper vehicle 2, denoted as x_2, as defined in Definition 8.

Definition 8: $\texttt{Collision} \equiv \texttt{x}_1 = \texttt{x}_2$

The same definition is valid for a left-side collision as given below:

Definition 9: $\texttt{Collision} \equiv \texttt{x}_1 = \texttt{x}_2$

In a rear-end collision, it is, however, important to note that the impact takes place at the rear bumper of the leading vehicle. Therefore, a collision is defined by the position of the rear bumper of vehicle 1 (x_1 - L_1) being equal to the position of the front bumper of vehicle 2 (x_2) as given by Definition 10.

Definition 10: $\texttt{Collision} \equiv \texttt{x}_1 - \texttt{L}_1 = \texttt{x}_2$

Using Definitions 1-10, we express in KeYmaera X the following main theorem as the target traffic safety rule. The proposed traffic safety rule is composed of three parts: (1) initial state characterization; (2) definition of multiple speed intervals with the severity level associated with each interval; and (3) post-condition as an expression of the expected outcome if the rule holds.

Theorem:
$\vdash \texttt{init} \land \texttt{TCT}_{violated} \longrightarrow [\{\texttt{(ctrl);(dyn)}\}^*](\texttt{TCT}_{violated} \longrightarrow \texttt{Collision})$

The traffic safety rule is given by the above theorem where `init` is determined based on the collision scenario, as described in Definitions 2, 4, and 6. Definition 1 provides the formal definition of $\texttt{TCT}_{violated}$. The control component, represented as `ctrl`, involves the allocation of specific deceleration rates along

with swerving maneuvers, contingent upon the speed of the vehicles. For more detailed information, please refer to the proof files [3]. Definitions 3, 5, and 7 specify the vehicle dynamics `dyn` depending on the collision scenario. Since there are no evolution domain constraints in `dyn` that limit the duration, each continuous evolution has an arbitrary duration $t \in \mathbb{R}_{\geq 0}$. The operator *, as described in Table 1, signifies a nondeterministic repetition of the program. Lastly, the collision definition `Collision` is given by Definitions 8, 9 and 10. The symbol $\longrightarrow$ denotes an implication relation connecting two formulas, the antecedent and the consequent. It asserts that the truth of the antecedent implies the truth of the consequent.

5.4 Discussion

We succeeded in verifying the above theorem in KeYmaefra X (version 5.0.1). The considered collision scenarios exhibit varying levels of complexity given the number of vehicles involved. In our formalization, we consider the dynamics of all involved vehicles as well as their potential evasive actions based on their respective speeds which adds more complexity to the verification process. This complexity is reflected by the number of tactics needed to prove the theorem as well as the verification time. For instance, the verification of the head-on collision scenario involves modeling the two vehicles implicated and the possible actions executed by each vehicle. This led to applying more tactics and rules to prove this scenario in KeYmaera X. As for rear-end and left side-collision, the systems modeled are less complicated, and therefore, easier to be verified. The verification process was carried out using KeYmaera X's automated strategies, which allowed for a fully automated process. This means that no manual intervention was required during the verification process, which resulted in a more efficient and accurate verification. The KeYmaera X proof files are available online [3].

6 Conclusion

In this paper, we proposed to integrate formal methods with TCTs in order to obtain guarantees of a rigorous analysis of vehicular crash severity. In particular, we provided the formalization and verification of a traffic safety rule using the hybrid theorem prover KeYmaera X. The proposed rule combines crucial TCTs, namely Time-To-Collision and Extended Delta-V, along with relevant evasive actions indicators, i.e., jerk profile and yaw rate. These indicators are employed to formally analyze crash severity based on their computed values. By performing a comprehensive analysis of traffic conflict techniques, the proposed traffic safety rule helps in identifying the suitable evasive actions with the right intensity. This proactive approach holds the potential to significantly reduce the occurrence of actual traffic crashes. However, knowing that traffic conflicts differ from one situation to another, we proposed to conduct our analysis in three different traffic scenarios, i.e., rear-end, head-on, and left-side collision. The work developed in this paper demonstrates the importance of combining different traffic conflict

indicators as a unified safety rule, where each indicator provides a complementary safety aspect of the interactions. The use of formal methods to formally verify the safety rule is of great importance to guarantee the reliability and soundness of the system. This work can be a great asset in the decision-making process for autonomous vehicles during traffic conflicts. As future work, we plan to extend the proposed crash analysis to incorporate connectivity by considering autonomous and connected vehicles, including the inter-communication between them. It will also be interesting to consider other traffic behaviors than those presented in this paper, such as lane changing or weaving.

Future Directions: Considering that AI is increasingly becoming the dominant technology underlying many systems, particularly safety-critical systems, our future work aims to explore the integration of traffic safety rules as formal safety constraints directly into the objective function of Reinforcement Learning algorithms. This approach is intended to ensure that safety becomes an inherent and prioritized aspect of AI algorithms, especially in the context of autonomous systems and intelligent decision-making processes.

Acknowledgement: We would like to extend our thanks to Dr. André Platzer (Karlsruhe Institute of Technology) and Dr. Stefan Mitsch (DePaul University) for their availability to answer our inquiries about KeYmaera.

References

1. Althoff, M., Stursberg, O., Buss, M.: Safety assessment of autonomous cars using verification techniques. In: American Control Conference, pp. 4154–4159 (2007)
2. Bagdadi, O., Várhelyi, A.: Jerky driving—an indicator of accident proneness? In: Accident Analysis & Prevention **43**(4), 1359–1363 (2011)
3. Barhoumi, O.: KeYmaera X proof files for the traffic safety rule. `https://github.com/OumaimaBarhoumi/Traffic-Safety-Rule/`, [Online]
4. Cao, X., Young, W., Sarvi, M.: Exploring duration of lane change execution. In: Australasian Transport Research Forum, pp. 1–17 (2013)
5. Garcia, J., Feng, Y.: A comprehensive study of autonomous vehicle bugs. In: International Conference on Software Engineering, pp. 385–396. ACM (2020)
6. Guo, Y., Sayed, T., Zaki, M.H.: Exploring evasive action–based indicators for ptw conflicts in shared traffic facility environments. In: Journal of Transportation Engineering, Part A: Systems **144**(11), 04018065 (2018)
7. Hayward, J.: Near-miss determination through use of a scale of danger pp. In: Highway Research Record, 24–34 (1972)
8. Hirst, S., Graham, R.: The format and presentation of collision warnings. In: Ergonomics and Safety of Intelligent Driver Interfaces, pp. 203–219. CRC Press (1997)
9. Laureshyn, A., De Ceunynck, T., Karlsson, C., Svensson, Å., Daniels, S.: In search of the severity dimension of traffic events: Extended Delta-V as a traffic conflict indicator. In: Accident Analysis & Prevention **98**, 46–56 (2017)
10. Laureshyn, A., Svensson, Å., Hydén, C.: Evaluation of traffic safety, based on micro-level behavioural data. In: Accident Analysis & Prevention **42**(6), 1637–1646 (2010)

11. Loos, S.M., Platzer, A., Nistor, L.: Adaptive cruise control: Hybrid, distributed, and now formally verified. In: Formal Methods. vol. 6664 of LNCS, pp. 42–56. Springer (2011)
12. Mao, J., Chen, L.: Runtime monitoring for cyber-physical systems: A case study of cooperative adaptive cruise control. In: International Conference on Intelligent System Design and Engineering Application, pp. 509–515 (2012)
13. Mary, L.: 5 conclusions from an automation expert with firsthand knowledge of highway regulation what self-driving cars tell us about ai risks: "missy" cummings. IEEE Spectrum **60**(10), 30–35 (2023)
14. Mitsch, S., Loos, S.M., Platzer, A.: Towards formal verification of freeway traffic control. In: International Conference on Cyber-Physical Systems, pp. 171–180 (2012)
15. Nygård, M.: A method for analysing traffic safety with help of speed profiles. Ph.D. thesis, Tampere University of Technology, Finland (1999)
16. Platzer, A.: Differential dynamic logic for verifying parametric hybrid systems. In: Automated Reasoning with Analytic Tableaux and Related Methods. vol. 4548 of LNCS, pp. 216–232. Springer (2007)
17. Rizaldi, Albert and Immler, Fabian and Althoff, Matthias: A formally verified checker of the safe distance traffic rules for autonomous vehicles. In: NASA Formal Methods. vol. 9690 of LNCS, pp. 175–190. Springer (2016)
18. Shelby, S.: Delta-V as a measure of traffic conflict severity. In: International Conference on Road Safety and Simulation, pp. 14–16 (2011)
19. Stanton, N.A., Salmon, P.M., Walker, G.H., Stanton, M.: Models and methods for collision analysis: a comparison study based on the uber collision with a pedestrian. In: Safety Science **120**, 117–128 (2019)
20. Tageldin, A., Sayed, T., Wang, X.: Can time proximity measures be used as safety indicators in all driving cultures? In: Transportation Research Record **2520**(1), 165–174 (2015)
21. Zaki, M.H., Sayed, T., Shaaban, K.: Use of drivers' jerk profiles in computer vision–based traffic safety evaluations. In: Transportation Research Record **2434**(1), 103–112 (2014)
22. Zheng, L., Ismail, K., Meng, X.: Traffic conflict techniques for road safety analysis: open questions and some insights. In: Canadian Journal of Civil Engineering **41**(7), 633–641 (2014)