Received 15 March 2024; accepted 3 April 2024. Date of publication 12 April 2024;
date of current version 26 April 2024. The review of this article was coordinated by Editor Lei Zhang.

Digital Object Identifier 10.1109/OJVT.2024.3387414

A Formal Approach to Road Safety Assessment Using Traffic Conflict Techniques

OUMAIMA BARHOUMI [1], MOHAMED H. ZAKI [2] (Member, IEEE), AND SOFIÉNÉ TAHAR [1] (Senior Member, IEEE)

[1] Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada
[2] Department of Civil and Environmental Engineering, Western University, London, ON N6A 3K7, Canada

CORRESPONDING AUTHOR: MOHAMED H. ZAKI (e-mail: mzaki9@uwo.ca).

ABSTRACT Traffic conflict techniques enable a comprehensive assessment of traffic safety analysis. Formal methods allow the identification of factors that contribute to traffic safety issues and provide evidence of potential safety degradation. As such, formal methods provide a novel way to model traffic rules and verify road users' compliance. The paper proposes formalizing a traffic safety rule in differential dynamic logic and using KeYmaera theorem prover for verification. This rule considers time-to-collision (TTC), space headway (SHW), and shockwave speed (SWV). To validate the effectiveness of this rule in realistic traffic scenarios, we conducted a study using calibrated microsimulation data from the SR528 highway in Orlando, Florida. Our analysis examined the TTC, SHW, and SWV values for vehicle platoons on the highway and demonstrated how smaller TTC and SHW values indicate shockwaves and subsequent conflicts. Furthermore, we observed that shockwave speed could contribute to traffic conflicts by enabling evasive actions such as sudden braking or lane changes as the risk of collisions increases. By highlighting these findings, we aim to provide valuable insights into the real-world applicability of formal methods for traffic safety and their potential in promoting safer driving practices that can help create reliable autonomous vehicle control systems.

INDEX TERMS Transportation safety, time-to-collision, space headway, shockwaves, formal verification.

I. INTRODUCTION

Scope: Around 1.35 million road traffic deaths are registered every year in the world, as reported by the National Highway Traffic Safety Administration [1]. Furthermore, 42,915 lost lives were registered in 2021 by the National Highway Traffic Safety Administration (NHTSA) [1]. In this context, a conventional practice in road safety to prevent future crashes is to rely on historical crash data. Although beneficial and generally effective, this approach can be unreliable due to shortcomings, such as the scarcity of collected data and the poor quality of available records [2]. As an alternative, Traffic Conflict Techniques (TCTs), such as Time-To-Collision (TTC), have emerged to address many shortcomings of crash data analysis. TCTs are introduced as a direct evaluation of traffic safety by studying their nature and observing their variations, whether in a normal flow or a traffic conflict situation [3]. In this context, a traffic conflict is defined as an interaction between two or multiple vehicles in which one of the vehicles must take evasive action to avoid the collision [3]. It is worth noting that the nature of the conflict differs depending on the contributing factors to its occurrence and the vehicle's surrounding environment at the moment of the conflict. Therefore, ensuring the appropriate use of TCTs in different traffic conflicts is the first step in conducting an accurate analysis.

Traditionally, the accuracy of transportation systems relies on the analysis of real traffic data and the use of calibrated simulation-based tools. However, with the increasing complexity in transportation networks, simulation can be insufficient to thoroughly verify the safety of the transportation system, given the constrained time horizon and limited coverage. One promising approach to enhancing confidence in transportation systems is to combine simulation-based tools with rigorous modelling and analysis techniques such as formal methods. Formal methods employ mathematical reasoning and thorough mathematical analysis to create models and verify the functionality of a system based on its intended specifications [4]. By utilizing logical procedures, formal methods can prove or disprove the correctness of the model in relation to the specifications.

Different variants of formal-based verification tools span various logical formalisms and automation. For example, model checking [5] is an approach in which the automation of the verification process is rendered possible as the system model is described using finite state machines and the state space is explored in an exhaustive manner to check whether the specification, usually written in temporal logic, is satisfied or not for a given set of initial conditions. However, because of the interaction between their continuous and discrete state transitions, vehicles are modelled as hybrid systems known for their infinite state spaces. These state spaces cannot be partitioned into finitely relevant regions for deciding reachability [6], making model checking incapable of verifying hybrid systems given their state space explosion problem.

Theorem proving [7] is introduced as a technique applied to formally verify that a design implementation satisfies its specification. Thanks to their underlying logic, e.g., first-order logic and higher-order logic, theorem proving is capable of analyzing large and complex systems. Therefore, it is a convenient formal verification method to achieve sound and verified designs. Based on the expressiveness of the underlying logic, the theorem prover can be fully automated, e.g., KeYmaera [8] or interactive, e.g., Isabelle/HOL [9]. In the case of an interactive theorem prover, user intervention is needed to guide the verification process. Theorem proving has been successful in uncovering bugs in computer systems [10] but has also been used to ensure the verification of avionics systems [11]. Most recently, theorem proving was applied in the verification of transportation systems [12]. Through its detailed approach to modeling and verifying complex systems, theorem proving provides an effective tool for deriving traffic rules and verifying the safety of interactions between road users under designated traffic conditions.

Approach Overview: Building upon established best practices, particularly those outlined in [13], [14], we advocate for the analysis of TCTs as a current approach for traffic safety assessment. In car following models [15], rear-end crashes frequently occur due to different traffic events such as shockwaves. Shockwaves are traffic events that occur due to predicted, and non-predicted changes in the traffic state, such as crashes and signalized intersections [16]. A shockwave can be identified by a platooning of stationary vehicles or slowed vehicles on a certain road segment. Therefore, we introduce the Shockwave Speed (SWV) indicator as a traffic conflict indicator identifying the occurrence of shockwaves in a traffic flow by studying its variation compared to pre-defined bounds from the literature. In order to further study the impact of shockwaves on the traffic state, we analyze the variation of two significant traffic conflict techniques (TCT), namely Time-To-Collision (TTC) and Space Headway (SHW). These indicators are utilized to assess minor disruptions in traffic flow by comparing their values with predefined boundary conditions.

In this paper, we apply theorem proving to formally verify a traffic safety rule that combines different TCTs to build reliable, advanced and autonomous vehicle control systems. In this context, vehicles are modelled as hybrid systems because of the interaction between their continuous and discrete state transitions. Therefore, we propose to use the KeYmaera theorem prover as a deductive verification tool that deals with hybrid systems [17]. KeYmaera supports differential dynamic logic (dL), a real-valued first-order dynamic logic for hybrid programs. Furthermore, dL is used as a program notation for hybrid automata [6]. Using KeYmaera, we aim to prove the correctness of the traffic safety rule that integrates TTC, SHW and, SWV. By studying the interplay between TTC and space headway during shockwaves, we gain a more comprehensive understanding of the factors contributing to the event. This dual-metric approach allows for a nuanced assessment of traffic conflicts, considering both time and space components, and facilitates a more precise analysis of the conditions leading to and evolving within shockwave occurrence. Based on this assessment, we can identify convenient measures to reduce the severity of traffic conflicts, avoid them and reduce the occurrence of crashes.

Contributions: The contributions of this paper can be summarized as follows:

- We examine how indicators like Time-To-Collision (TTC), Space Headway (SHW), and Shockwaves (SWV) are interconnected. Our goal is to establish a traffic safety rule that can effectively mitigate severe traffic conflicts and minimize the risk of collisions.
- We formalize and verify a traffic safety rules using Differential Dynamic Logic (dL) and the KeYmaera Automated Theorem Prover.
- We conduct a case study to illustrate the effectiveness of the formalized traffic safety rule that links Time-To-Collision (TTC), Space Headway (SHW), and Shockwaves (SWV). The study uses traffic platooning simulation data calibrated from a real-life traffic dataset obtained from the SR528 highway in Orlando, Florida, USA.

Traffic safety is evaluated based on the severity of the conflict, therefore, the use of specific metrics in these cases is extremely helpful in reflecting the severity of the situation. Regardless of whether a traffic conflict is extreme or mild, interventions such as evasive actions or speed adjustments become necessary. The distinction lies in the intensity of the required actions. In the case of a mild conflict, the interventions may be less severe and could involve minor adjustments to speed or lane positioning to avoid a potential collision. On the other hand, in the case of an extreme conflict where the risk of collision is higher, interventions need to be more intense and immediate. In both scenarios, the fundamental principle is to address the conflict and take appropriate actions to ensure the safety of all road users, but the degree of urgency and the magnitude of the required interventions vary based on the severity of the conflict. Therefore, the primary goal of this paper is to improve the accuracy of road safety evaluation by integrating traffic measures and conflict indicators into a rule-based formal method framework. Moreover, the use of theorem-proving in transportation, as proposed in this paper, can play a critical role in identifying inconsistencies in vehicles' decision-making process and provide a road map for a safe-by-design driver controller for autonomous vehicles. An example that illustrates the potential impact that a formally verified system can have on the safety of autonomous vehicles is explained in [18]. The crash caused by the Zoox vehicle's autonomous system that misjudged its clearance from parked vehicles could have been avoided if the system had undergone formal verification.

The paper is structured as follows. Section II presents previous work related to TCTs and formal verification. In Section IV, we provide an overview of the proposed methodology and a brief introduction to the KeYmaera theorem prover. Section V covers the process of formalizing the introduced traffic safety rule, and Section VII presents a case study evaluating the safety rule against calibrated traffic simulation data. We conclude this work in Section VIII.

II. RELATED WORK

A. TRAFFIC CONFLICTS FOR TRAFFIC SAFETY EVALUATION

The use of traffic conflicts to diagnose traffic safety has gained approval as a more efficient approach than relying on historical collision data records. The correlation between the occurrence of traffic conflicts and the frequency of traffic collisions is illustrated in [19], [20]. In fact, the failure mechanism in a system can lead to both events, that is, a traffic conflict followed by a traffic collision depending on the severity of the conflict. Consequently, the use of traffic conflicts as surrogates for collisions in safety analysis can offer valuable insights into the underlying causes of road collisions. This approach opens the possibility of reducing the frequency of traffic collisions by addressing and mitigating traffic conflicts [21].

Traffic conflicts can be employed to study critical behaviors by analyzing road users' actions in safety-critical situations. The safety level of the observed behaviors is then determined based on the frequency and severity of traffic conflicts. Numerous works in the literature, such as [22], [23], [24], demonstrate this type of application. A significant implication of employing traffic conflicts lies in conducting before-after safety analysis to assess the effectiveness of applied treatments in enhancing safety. This involves comparing the frequency and/or severity of traffic conflicts in the "after" period to those in the "before" period, as illustrated in [13], [25], [26]. Defined as "an observable situation in which two or more road users approach each other in space and time to an extent that there is a risk of collision if their movements remain unchanged" [27], traffic conflicts play a crucial role in proactive road safety management systems. They can be applied as real-time safety prediction approaches by monitoring the ongoing safety level, reflected in factors like traffic conflict frequency, and/or conflict-derived indicators such as TTC, SHW, etc. In this context, various applications are detailed in [28], [29], [30].

While the above works advocate for the use of traffic conflicts for traffic safety evaluation, they mainly focus on the analysis of one traffic safety indicator at a time to analyze the occurring traffic conflict. In our study, we propose a before/after analysis that employs a combination of TCTs, namely Time-To-Collision (TTC), Space Headway (SHW), and Shockwave Speed (SWV), as a one traffic safety rule, to examine shockwave events occurring within platooning scenarios.

B. TRAFFIC CONFLICT TECHNIQUES AS MEASURES FOR TRAFFIC CONFLICTS

In order to study traffic conflicts, their severity and their impact on the traffic flow, several traffic conflict techniques (TCTs) were introduced as a direct evaluation of traffic safety [3]. An accurate analysis of TCTs is capable of providing a correct evaluation of traffic state and vehicles' interactions. For instance, Time-To-Collision (TTC) as a safety indicator in traffic flow has been widely studied and has been shown to be effective in identifying potential collisions. TTC was first introduced by Hayward in 1971 as a temporal-proximity measure that predicts the time it would take for two vehicles to collide if no preventative measures are taken [31]. In a subsequent study by Hayward in 1972 [32], it was shown that TTC has an impact on the speed of the vehicle and can be used to prevent collisions by alerting drivers to potential hazards.

Based on a study conducted in 1994 [33], TTC has been identified as the primary indicator used in the design of collision avoidance systems. This highlights the importance of TTC in ensuring the safety of drivers and passengers on the road and underscores its significance as a critical safety indicator in traffic flow. In [34], the authors conduct a case study to assess the accuracy of time-to-collision (TTC) as an indicator for detecting rear-end collisions under different assumptions of constant velocity, constant acceleration, and linear acceleration for leading and following vehicles. Based on their findings, applying TTC based on the assumption of linear acceleration in collision avoidance systems helps decrease driver errors more than other cases. Introduced first by [31] in 1971, various modifications were introduced to TTC over time, such as [35], [36], [37]. For instance, in [36], the authors review these modifications to propose a comprehensive framework for the numerous applications of TTC for different types of traffic conflicts. The efficacy of the framework is evaluated using microscopic traffic data collected in Tehran. The findings of this work demonstrate the usefulness of different versions of TTC in increasing the precision and accuracy of detecting dangerous encounters.

Unlike TTC, the Space Headway indicator (SHW) [38], defined as a spatial-proximity safety indicator, is described as the physical distance separating two consecutive vehicles and its value is determined as the difference between the position of the front of the leading vehicle and the position of the front of the following vehicle. Among numerous works, SHW was studied in [39] in order to estimate the average space headway using a model-based approach with special reference to congestion prediction for intelligent transportation systems (ITS) applications. Furthermore, it was used in [40] to describe a safe traffic flow where the shockwave occurrence is improbable for a series of equal space headways over a platooning of vehicles.

The occurrence of shockwaves in traffic flow can have a significant impact on the safety of drivers on the road. One way to measure the occurrence of shockwaves is through the Shockwave Speed (SWV) indicator. SWV reflects the speed at which a shockwave propagates through traffic flow, and it can be used as a safety indicator to evaluate the risk of collisions caused by shockwaves. In [16], the main focus of the authors was on investigating the frequency of rear-end crashes in congested freeways in the presence of a downstream shockwave. The latter was used as an environmental situation that can be a factor in rear-end crashes. In the work of Machiani et al. [41], a novel surrogate safety measure called safety surrogate histogram (SSH) was developed by taking into consideration the frequency of Dilemma Zone (DZ)-related crashes. The concept of SSH is related to the behavior of traffic passing through the forming shockwave at the intersection without providing the characteristics or the parameters of a shockwave. However, none of these studies evaluated the occurrence of shockwaves by comparing the computed shockwave speed to a pre-defined bound. This approach could provide a more quantitative and standardized way to assess the risk associated with shockwaves in traffic flow. By defining bounds for SWV, it would be possible to identify situations where the shockwave speed exceeds the safe limit in order to take appropriate measures to mitigate the risk of collisions.

C. FORMAL VERIFICATION FOR TRANSPORTATION

When it comes to dealing with safety-critical systems, such as transportation systems, it is vital to make sure that no human errors or bugs go undiscovered during the realization and testing phase of the system. Considering the case of system failures, the outcome will not be limited to financial losses and equipment damages only, it might also cause human life losses. Therefore, conventional methods such as simulation tools and paper and pencil analysis are no longer sufficient to guarantee the correctness of large and complex systems, such as transportation systems. In this context, formal verification methods are introduced as rigorous methods that are capable of guaranteeing a very high level of accuracy by formally verifying that the defined mathematical model of a system meets its specifications to function correctly [4].

Formal methods and verification tools have been used in the engineering of safety-critical transport systems for well over 30 years [42]. They have been used in railway, avionics and automotive to demonstrate, with the highest levels of assurance, the correct functioning of the systems involved. Our interest will be in the application of formal verification to vehicles and traffic systems. For instance, in [43], a specification-based monitoring approach is proposed in order to define traffic parameters. Furthermore, the authors used signal temporal logic as a formal language to analyse these traffic rules. The authors in [44] applied formal methods to develop a runtime monitoring of a cooperative adaptive cruise control (CACC) system. Toward this goal, they defined temporal specifications for the safe operation of CACC and results showed that their approach successfully captured specification violations. Furthermore, formal verification techniques were also applied to guarantee that an autonomous vehicle will avoid static objects, as well as dynamic obstacles on the road, [45]. When it comes to the verification of the entirety of the traffic system, Loos et al. [46] developed a distributed car control system and formal proof that this system is collision-free for arbitrarily many cars.

The work of Mitsch et al., in [47], was one of the first attempts to utilize formal verification tools in the modeling of freeway dynamics. The objective was to ensure that the system correctly calculates the appropriate speed limit and communicates this information to vehicles in certain regions of interest. Differential dynamic logic was used to formulate and verify the system specifications in [47]. Seeing the importance of the macroscopic model in planning strategies in allocating resources for implementing optimized and balanced transportation systems, Rashid et al. in [12], opted to formalize some foundation concepts of macroscopic models using the higher-order-logic theorem prover HOL Light [48]. Finally, the authors of [49] provided a formally proved checker of the safe distance rule in order to check if an autonomous vehicle complies with the traffic rules.

D. KNOWLEDGE GAPS

The studies mentioned have explored different aspects of verifying transportation systems, with a focus on safety-related concerns related to the vehicle or its interaction with the environment. However, there has been no prior research into formalizing and verifying Traffic Conflict Techniques (TCT) - which serve as safety measures for traffic interactions. To fill some of these gaps, this paper proposes a formal analysis of traffic conflicts and their occurrence by defining a TCT-based traffic safety rule. This rule examines the impact of shockwaves on Time-to-collision and Space Headway variations and vice versa. To ensure accuracy, we rely on formal verification methods and traffic simulation to prove the correctness of this rule.

III. PRELIMINARIES: KEYMAERA THEOREM PROVER

As a deductive verification tool that deals with hybrid systems, KeYmaera handles hybrid systems' arithmetic by using real quantifier elimination. In handling differential equations of continuous evolutions, KeYmaera applies symbolic computations in computer algebra systems [6]. As an automated

TABLE 1. Syntax of Differential Dynamic Logic (dL) [6]

Statement	Effect
$\alpha;\beta$	sequential composition, first performs α and then β afterwards
$\alpha \cup \beta$	nondeterministic choice, following either α or β
α^*	nondeterministic repetition, repeating α $n \geq 0$ times
$x := \theta$	discrete assignment of the value of term θ to variable x (jump)
$x := *$	nondeterministic assignment of an arbitrary real number to x
$x'_1 = \theta_1,..., x'_n = \theta_n, F$	continuous evolution of x'_i along differential equation system $x'_i = \theta_i$, restricted to a maximum domain or an invariant region F
$?F$	check if formula F holds at current state, abort otherwise
if (F) then α	perform α if F holds, do nothing otherwise
if (F) then α else β	perform α if F holds, perform β otherwise

and interactive theorem prover for a natural specification and verification logic for hybrid systems, KeYmaera supports differential dynamic logic (dL), i.e., a real-valued first-order dynamic logic for hybrid programs. The operational behavior of hybrid systems can be described using hybrid automata that can be embedded into hybrid programs. An overview of the syntax and informal semantics of hybrid programs is given in Table 1, where F is a formula of first-order real arithmetic.

The input for KeYmaera consists of a single formula in Differential Dynamic Logic, which combines both the system description and the property under consideration. To establish the validity of this formula, it is divided into multiple subtasks in accordance with the proof rules of dL. The Boolean structure of the input formula is systematically converted into a proof tree whenever applicable. Programs are managed through symbolic execution, meaning that for each program construct, there exists a proof rule that computes its effect. For instance, managing assignments such as $x := \theta$ can be accomplished by substituting each occurrence of x with its updated value θ in the postcondition. KeYmaera's strength lies in its capability to conduct automated proof searches while also enabling user interaction to guide the prover in situations where automated proof procedures fall short. An impressive feature of KeYmaera is its automated breakdown of the initial verification problem into smaller subtasks while preserving a transparent link to the original problem. This approach permits users to concentrate on challenging cases that demand interaction, while leaving routine steps to be handled automatically by the prover.

IV. PROPOSED METHODOLOGY

In this paper, our aim is to improve the accuracy of safety evaluation by integrating traffic conflict indicators within a rule-based formal method framework. Therefore, we employ shockwave Speed (SWV), Time-To-Collision (TTC) and Space Headway (SHW) as traffic conflict indicators to define a traffic safety rule that takes into account the potential for traffic conflicts based on speed, time, and space. Initially, we start by mathematically defining the applied TCTs as shown in Fig. 1 [50]. In order to construct a formal model of the proposed traffic safety rule, we provide a formalization of the introduced traffic conflict indicators using differential dynamic logic (dL). Subsequently, we examine the bidirectional causal relationship between Shockwave Speed (SWV), Time-To-Collision (TTC), and Space Headway (SHW). Specifically, we investigate how violating the TTC and SHW thresholds affects the occurrence of shockwaves and how shockwave speed impacts the TTC and SHW indicators. By analyzing these variables using Keymaera, we can identify situations where the TTC is very low and there is a high risk of collision or where the space headway is too small, increasing the risk of a rear-end collision. Additionally, analyzing shockwave speed can help identify situations in which a disturbance in traffic flow can lead to a chain reaction of collisions. Consequently, we formalize and verify the traffic safety rule within the KeYmaera theorem prover. Towards achieving this goal, the first step is to introduce the initial pre-conditions for the system's variables, followed by modeling the hybrid system using an ordinary differential equation (ODE) due to the continuous evolution of the system. Finally, we define the post-conditions responsible for setting the expected behavior. These conditions must be met for the safety rule to be valid. Using KeYmaera to verify these post-conditions, we can ensure that the safety rule is reliable in capturing the safety events.

V. VERIFICATION OF THE TRAFFIC SAFETY RULE

In an earlier study, the authors of [16] identified shockwave occurrence as a primary cause of rear-end crashes. Shockwaves are defined by propagation of traffic congestion from one traffic region to the next. This congestion state mostly impacts vehicles driving fast and/or joining the queue recently and inattentive drivers, such as tired or distracted drivers. In these situations, the driver ends up eventually crashing into the vehicle ahead. The damages registered by this type of collision might seem light, however, it is based on certain traffic parameters and their intensity that the collision might be considered serious. We propose Time-To-Collision (TTC), Space Headway (SHW) and Shockwaves speed (SWV) as the main parameters that are analyzed to study these situations. TTC and SHW represent temporal and spatial proximity indicators, respectively, that are considered by multiple works in the literature as convenient indicators to reflect the change in driving behavior in platoons. The analysis of these indicators can identify the occurrence of shockwaves and reflect the severity of the conflict.

A. EQUATION-BASED MODELING OF TCTS

In this part, we provide the mathematical representation of the TCTs forming the traffic safety rule, i.e., TTC, SHW and

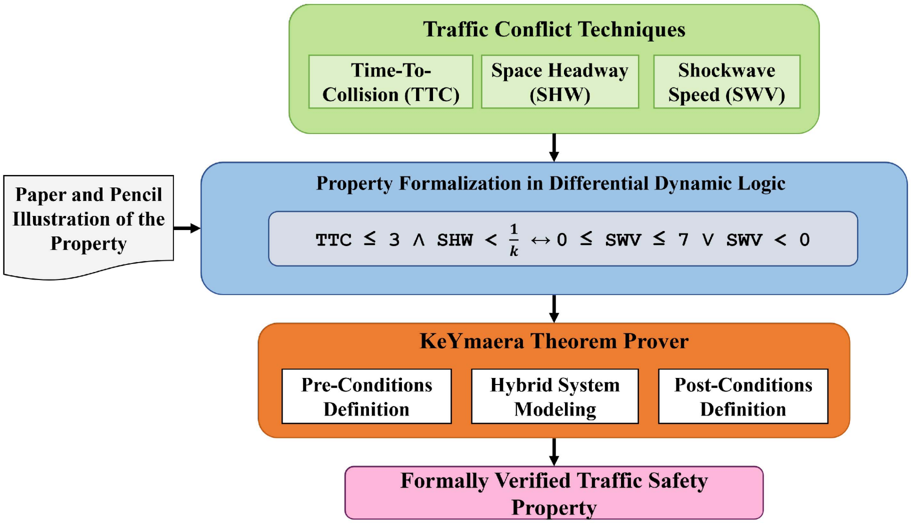
Traffic Conflict Techniques
Time-To-Collision (TTC)
Space Headway (SHW)
Shockwave Speed (SWV)
Paper and Pencil Illustration of the Property
Property Formalization in Differential Dynamic Logic
TTC ≤ 3 ∧ SHW < 1/k ↔ 0 ≤ SWV ≤ 7 ∨ SWV < 0
KeYmaera Theorem Prover
Pre-Conditions Definition
Hybrid System Modeling
Post-Conditions Definition
Formally Verified Traffic Safety Property

FIGURE 1. Methodology for the verification of the TCT-based safety rule [50].

SWV, in car following models. The latter is reflected by platoons of vehicles where every vehicle can be a leader and/or a following vehicle.

1) TIME-TO-COLLISION

In order to mathematically model the TTC indicator, the number of vehicles is generic as given in (1) [51].

$$TTC = \frac{x_i - x_{i+1} - L_i}{v_{i+1} - v_i}, \qquad v_{i+1} > v_i \tag{1}$$

where vehicles i and $i+1$ are the leading and following vehicles, respectively, x_i, x_{i+1}, v_i and v_{i+1} are the positions and velocities of vehicles i and $i+1$, respectively, and L is the length of vehicle i.

2) SPACE HEADWAY

The Space Headway indicator (SHW) describes the physical distance separating the front bumps of every two consecutive vehicles. The space headway is the position difference between vehicle i and $i+1$ can be mathematically defined in (2) as follows:

$$SHW = x_i - x_{i+1} \tag{2}$$

where x_i and x_{i+1} are the positions of vehicle i, the leading vehicle, and the following vehicle $i+1$, respectively.

3) SHOCKWAVE SPEED

A shockwave is a macroscopic event that occurs during a traffic flow due to different factors such as signalized intersection, aggressive lane change causing the following vehicles to brake sharply, or a collision downstream the platoon of vehicles. A shockwave can be identified by a platooning of stationary vehicles or slowed vehicles on a certain road segment. Mathematically, the occurrence of shockwaves can be detected by computing the Shockwave Speed (SWV) defined over a range of consecutive vehicles, the formula in the macroscopic model is given in (3) [40].

$$SWV = \frac{q_i - q_j}{k_i - k_j} \tag{3}$$

where q_i, q_j, k_i and k_j represent the traffic flow and flow density for traffic state i representing the congested state, and for traffic state j representing the uncongested state, respectively. However, due to the scarcity of the traffic data or its delay, we opted for analyzing shockwave events at the microscopic level. Furthermore, conducting the traffic analysis at a microscopic level has its advantages when it comes to capturing the vehicles' dynamics as well as the drivers' actions in order to conduct a road safety analysis. Therefore, the Shockwave Speed indicator is now defined at the microscopic level using the dynamics of a range of consecutive vehicles on a road segment. Based on the work done in [40], the flow density (k), as shown below in (4), is found to be equal to the inverse of the headway distance (SHW) that is defined as the physical distance separating two consecutive vehicles, for example, the second and third vehicles in row.

$$k = \frac{1}{SHW} \tag{4}$$

Furthermore, using the conventional definition of traffic flow in engineering, the traffic flow (q) is reduced to the vehicle's speed multiplied by the flow density (k) as shown in (5).

$$q = v * k \tag{5}$$

However, by substituting (4) into (5) yields (6) as the microscopic expression for traffic flow [40].

$$q = \frac{v}{SHW} \tag{6}$$

Redefining SWV at the microscopic level as the shockwave speed of a platoon of vehicles in a car following model, we replace (4) and (6) into (3) to yield (7) [40].

$$SWV = \frac{\dfrac{v_i}{SHW_i} - \dfrac{v_j}{SHW_j}}{\dfrac{1}{SHW_i} - \dfrac{1}{SHW_j}} \tag{7}$$

where v_i and v_j represent the speed of vehicles i and j, respectively. As for SHW_i and SHW_j, they represent the distance separating vehicles i and $i+1$, and vehicles j and $j+1$, respectively, with $i \neq j$.

B. TRAFFIC SAFETY RULE SPECIFICATION

In this section, we study the interplay between TTC and space headway during shockwaves to gain a more comprehensive understanding of the factors contributing to the event. To achieve this objective, we propose the incorporation of a bidirectional relationship that integrates three key traffic safety indicators, specifically Time-to-Collision (TTC), Space Headway (SHW), and Shockwave Speed (SWV). This integrated relationship is consistently referred to as the traffic safety rule in the entirety of this paper. Time to Collision (TTC) is primarily utilized to assess potentially hazardous situations based on its numerical value and a comparison to a predefined threshold of 3 seconds. By setting a threshold of 3 seconds, we establish a benchmark to identify situations where the time available before a potential collision is relatively limited. Paired with space headway as an additional indicator, we investigate the variation of these two metrics in the context of a specific traffic event, specifically shockwaves. In the analysis of shockwaves, the combination of TTC and space headway provides insights into the dynamics of the traffic situation. A decrease in TTC below the threshold indicates a reduced time available before potential conflicts, highlighting areas of heightened risk. Simultaneously, examining space headway, which represents the distance between vehicles, contributes to understanding the spatial aspects of the traffic flow. The sketch of the traffic safety rule is given by:

$$Violated\ Indicators(Ind_{violated}) \longleftrightarrow$$
$$Shockwave\ Occurrence(SWV_{speed})$$

where TTC and SHW below their respective thresholds is referred to by *Violated Indicators*. To verify this rule, it is necessary to investigate the bidirectional relationship between the variables and demonstrate that the bi-implication holds in both directions. Initially, we start by initializing the system parameters and defining their bounds, i.e., *init*. Subsequently, we formally identify our system as a hybrid model, i.e., *dyn*, represented by an Ordinary Differential Equation (ODE). Once this is established, we introduce the rule by expressing it in the formal language dL. Subsequently, we introduce a set of defined preconditions on system variables, i.e., $ind_{violated}$, followed by defining the bounds of the shockwave speed indicator given by SWV_{speed}.

Formalization of pre-conditions and bounds: In order to ensure a proper representation of the system, the formalization of the pre-conditions and their respective bounds, i.e., *init*, in dL, is given by :

Definition 1: Pre-conditions (init)

$$
\begin{aligned}
&\vdash \forall\ \mathtt{C}\ \mathtt{i}.\\
&\quad \forall\ \mathtt{C}\ \mathtt{j}.\\
&\quad ((\mathtt{i} \neq \mathtt{j}) \wedge (\mathtt{v(i)} > 0) \wedge (\mathtt{v(j)} > 0) \wedge\\
&\quad (\mathtt{A} > 0) \wedge (\mathtt{C} > 0) \wedge (\mathtt{L} > 0) \wedge\\
&\left(k = \frac{N}{1000}\right) \wedge\\
&\quad (\mathtt{x(i)} < \mathtt{x(j)}) \wedge (\mathtt{v(i)} > \mathtt{v(j)}) \wedge\\
&\quad (\forall\ \mathtt{C}\ \mathtt{k}.\ ((\mathtt{k} \neq \mathtt{j}) \wedge (\mathtt{k} \neq \mathtt{i}) \longrightarrow\\
&\quad (\mathtt{x(j)} < \mathtt{x(k)}) \wedge (\mathtt{v(k)} > 0))\wedge\\
&\quad (\mathtt{SHW} = \mathtt{x(j)} - \mathtt{x(i)})\wedge\\
&\quad (\mathtt{d(i)} = \mathtt{x(j)} - \mathtt{x(i)})\wedge\\
&\quad (\mathtt{d(k)} = \mathtt{x(k)} - \mathtt{x(j)})\wedge\\
&\quad \left(\mathtt{SWV} = \left(\frac{v(k)}{d(k)} - \frac{v(i)}{d(i)}\right) / \left(\frac{1}{d(k)} - \frac{1}{d(i)}\right)\right)\wedge\\
&\quad (\mathtt{TTC} = \frac{SHW - L}{v(i) - v(j)})))
\end{aligned}
$$

where the universal quantifier ∀ C reflects that the formalization is carried out for all objects of sort C, with C being a built-in sort in KeYmaera used here to represent cars [52]. The employed indicators are formalized in dL, along with defining the bounds of the used variables, e.g., vehicles' positions x and speeds v. Furthermore, N represents the number of vehicles using the road section, k is the density defined as the average number of vehicles that occupy one mile or one kilometer of road space and L is the length of the leading vehicle in a platoon.

Formalization of the system model: We model the dynamics of the vehicles by their positions x_i, velocities v_i and accelerations a_i in dL. The formalization of the ODE linking these parameters in KeYmaera is given as:

Definition 2: Vehicle Dynamics (dyn)

$$
\begin{aligned}
&\vdash \forall\ \mathtt{C}\ \mathtt{i}.\ (\mathtt{x(i)'}) = (\mathtt{v(i)}),\\
&\quad\ \forall\ \mathtt{C}\ \mathtt{i}.\ (\mathtt{v(i)'}) = (\mathtt{a(i)}),\ (\mathtt{t'}) = (\mathtt{1})
\end{aligned}
$$

where the derivative x_i' of x_i and v_i' of v_i over time are $\frac{dx_i}{dt}$ and $\frac{dv_i}{dt}$, respectively, and the continuous dynamics of the vehicle given by the derivative *t'* equal to a constant.

Formalization of TTC and SHW constraints: In this part, we define the thresholds of the temporal proximity indicator, i.e., TTC, along with the spatial proximity indicator, i.e., SHW, in dL in order to set the safety constraints for vehicles driving in a zone where a shockwave is detected. The formalization is given below:

Definition 3: Violated Indicators ($Ind_{violated}$)

$$
\begin{aligned}
&\vdash \forall\ \mathtt{C}\ \mathtt{i}.\\
&\quad \forall\ \mathtt{C}\ \mathtt{j}.\\
&\quad ((\mathtt{i} \neq \mathtt{j})\wedge(\mathtt{TTC} < \mathtt{3})\wedge(\mathtt{SHW} < \frac{1}{k}))
\end{aligned}
$$

Formalization of SWV constraints: In this formalization, the shockwave speed threshold is formally defined for all cars as follows:

Definition 4: Shockwave Speed (SWV_{speed})

$$\vdash \forall\ \mathtt{C}\ \mathtt{i}.\ \forall\ \mathtt{C}\ \mathtt{j}.\ ((\mathtt{i} \neq \mathtt{j}) \wedge (0 \leq \mathtt{SWV} \leq 7) \vee (\mathtt{SWV} < 0))$$

1) THE IMPACT OF TIME-TO-COLLISION AND SPACE HEADWAY ON SHOCKWAVES

During the existence of a platooning of vehicles on a road section, the density k is defined as the average number of vehicles that occupy one mile or one kilometer of road space and expressed in vehicles per mile or per kilometer. The mathematical modeling of the density is given by (8), where N is the number of vehicles using the road section.

$$k = \frac{N}{1000} \tag{8}$$

In a conflict-free traffic flow, SHW is calculated as the inverse of the density of a certain road section as defined by (9). For safe spacing between vehicles, the SHW value should be greater than or at least equal to $\frac{1}{k}$.

$$SHW \geq \frac{1}{k} \tag{9}$$

To measure the severity of a traffic conflict, TTC, as defined in (1), is used to determine if a situation is critical or not based on its calculated value. A TTC value in a range of 0 to 3 seconds indicates an endangering traffic situation that requires the immediate attention of the involved car driver. However, to achieve an accurate traffic flow analysis, we introduce SHW as an additional indicator reflecting the spatial proximity between following vehicles to be combined with TTC to accurately analyze a traffic conflict. Consequently, we deduce that a TTC of less than 3 seconds, accompanied by a SHW less than its defined threshold, will have noticeable implications on traffic flow. The main consequence of these conditions is the formation of congested areas where the flow diminishes, vehicles slow down, and add up to form a queue characterizing a shockwave formation. The occurrence of a shockwave can be detected by determining its speed. Based on the work by Ibrahim et al. in [53], a shockwave speed of 7 m/s, i.e., 25.2 km/h, calculated between the ith and jth vehicles in a platoon of vehicles, where $i \neq j$ identifies a shockwave. The detected shockwave can propagate either upstream or downstream, depending on the sign of the speed value. For a speed value:

- SWV < 0 : the shockwave propagates in the same direction as the traffic stream, i.e., upstream.
- SWV ≥ 0 & SWV < 7 : the shockwave propagates against the traffic stream, i.e., downstream.

The proposed traffic safety rule consists of proving that the presence of a shockwave can be induced by a TTC that is less than 3 seconds and a noticeable reduction of the space headway over a platoon of vehicles. Therefore, the observation of TTC and SHW variations are made over a range of vehicles where the speed variation between vehicles differs according to the traffic environment at hand (signalized intersection, accident occurrence ahead, etc.). Consequently, we derive an implication relation describing the defined preconditions and their consequences over a platoon of vehicles. The formalization of the implication of the right-hand side (RHS) is given by:

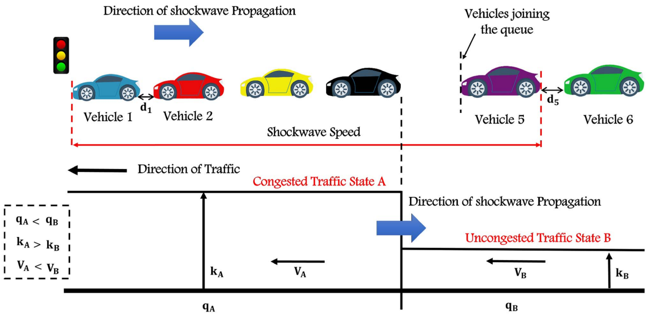
Direction of shockwave Propagation
Vehicles joining the queue
Vehicle 1
d_1
Vehicle 2
Shockwave Speed
Vehicle 5
d_5
Vehicle 6
Direction of Traffic
Congested Traffic State A
Direction of shockwave Propagation
Uncongested Traffic State B
$q_A < q_B$
$k_A > k_B$
$V_A < V_B$
k_A
V_A
V_B
k_B
q_A
q_B

FIGURE 2. Shockwave downstream propagation.

Theorem 1: RHS ($Ind_{violated} \longrightarrow SWV_{speed}$)

$$\vdash \forall\ \mathtt{C}\ \mathtt{i}.\ \forall\ \mathtt{C}\ \mathtt{j}.\ \left((\mathtt{i} \neq \mathtt{j}) \wedge\ (\mathtt{TTC} < 3)\ \wedge \left(SHW < \frac{1}{k}\right)\right) \longrightarrow ((0 \leq \mathtt{SWV} \leq 7)\ \vee\ (\mathtt{SWV} < 0))$$

2) THE IMPACT OF SHOCKWAVES ON TIME-TO-COLLISION AND SPACE HEADWAY

Inspired by this line of thought, we study the presence of the shockwave and its impact on TTC and SHW. This investigation proves fruitful by noticing the reduction of the spacing between consecutive vehicles leading to a reduced time-to-collision over a platoon of vehicles in the presence of a shockwave. Therefore, the impact of the shockwave is confirmed by focusing on the vehicles that form the queue. However, its propagation is observed by monitoring the vehicles that recently joined the platoon and analyzing their related TTC and SHW. As a demonstration example, Fig. 2 presents a downstream propagation of a shockwave. Mathematically, the direction of propagation can be determined based on the sign of the shockwave speed, for example, a negative sign confirms a downstream propagation. In this case, the vehicles entering a signalized intersection where the long light duration causes the formation of a queue of stand-by vehicles. Region A (left side of Fig. 2) is a congested area, while region B (right side of Fig. 2) is an uncongested area where the traffic flow runs smoothly and uninterrupted. As a result, the traffic flow in the congested area is lower than the traffic flow in the uncongested region, i.e., $q_A < q_B$. Furthermore, this traffic event will impact the mean speed by causing its reduction in the congested area, i.e., $V_A < V_B$ in addition to an increase of traffic density in state A compared to state B, i.e., $k_A > k_B$. For the vehicles joining with high speed, their braking will be abrupt and strong in order to stop the vehicle without colliding with the front vehicle. This will leave a small spacing between the two vehicles in addition to a smaller time to collision.

Based on the computed values of the two indicators, in this condition, i.e., the occurrence of a shockwave, this traffic situation is considered as a traffic conflict where certain measures should be taken to mitigate it safely. The formalization of the left-hand side (LHS) implication for all objects of sort C can be described as:

Theorem 2: LHS ($SWV_{speed} \longrightarrow Ind_{violated}$)

$$\begin{aligned}&\vdash \forall\ \mathtt{C\ i.}\\ &\quad \forall\ \mathtt{C\ j.}\\ &\quad ((0\ \le\ \mathtt{SWV}\ \le\ 7)\ \lor\ (\mathtt{SWV}\ < 0)) \longrightarrow\\ &\quad \left((\mathtt{i}\ \neq\ \mathtt{j}) \land\ (\mathtt{TTC}\ <\ 3)\ \land\ \left(SHW\ <\ \frac{1}{k}\right)\right)\end{aligned}$$

Based on the formalization and verification of the implication in both directions as given by Theorems 1 and 2, we define the traffic safety rule as a bidirectional relation between TTC, SHW and SWV. We provide the formalization of this rule using the formal language dL in Theorem 3. We aim to formally verify the depicted safety rule using a set of automated procedures in KeYmaera using automatic proof strategies. One of these strategies involves solving the dynamics of hybrid systems, such as vehicles, which are described by differential equations. The solutions obtained from this process are then used to verify each sub-goal of the rule until the main goal is reached.

Theorem 3: Traffic Safety Rule

$$\vdash \mathtt{init}\ \longrightarrow\ [(\mathtt{dyn})^*](\mathtt{Ind}_{violated}\ \longleftrightarrow\ \mathtt{SWV}_{speed})$$

KeYmaera's verification process is exhaustive in the sense that it rigorously examines all potential combinations of the provided initial conditions to establish the validity of the specified theorems within the given system. In our work, Definition 1 articulates these initial conditions, denoted as pre-conditions. KeYmaera is designed to handle hybrid systems, which involve both continuous variables (described by differential equations) and discrete transitions (triggered by events or conditions). Its verification logic, i.e., Differential Dynamic Logic (dL), serves the purpose of formally specifying and reasoning about properties of continuous behaviors and discrete transitions. If the proof is successful, the rule is considered proven. However, if an error is encountered during the process, the prover is disabled from continuing the process.

The boolean structure of the traffic safety rule is transformed into a proof tree as given by Figs. 3 and 4 where the violated thresholds of the TTC and SWV indicators, defined at the top, indicate an upcoming traffic conflict. KeYmaera implements automatic proof strategies that decompose the hybrid system specification symbolically. This compositional verification principle helps scaling up verification, because KeYmaera verifies a big system by verifying properties of subsystems. Therefore, multiple branches are automatically generated and evaluated, where each branch leads to a subgoal that KeYmaera automatically proves. Following the branches and verifying every possibility leads to verifying all sub-goals, thereby proving the correctness of the rule. For example, as highlighted in Fig. 3, in a traffic conflict situation, a *Potential Collision* outcome is obtained when violating TCTs thresholds.

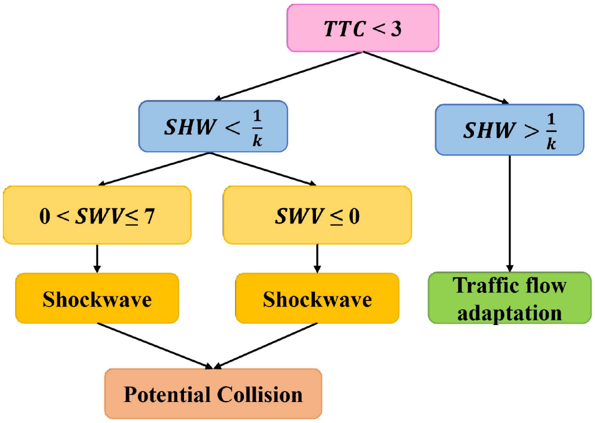

FIGURE 3. Proof tree of the RHS of the traffic safety rule.

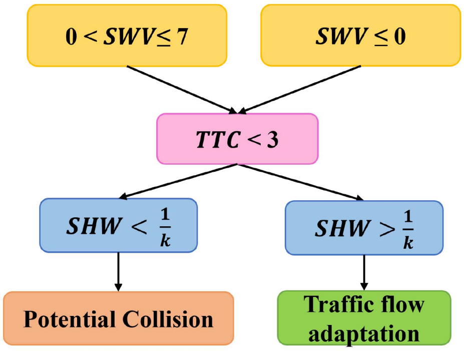

FIGURE 4. Proof tree of the LHS of the traffic safety rule.

VI. SENSITIVITY STUDY

In the work of Hirst et al. [54], 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 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 was collectively decided that setting a TTC threshold at 3 seconds is more appropriate. In this section, we perform a sensitivity study to provide validation and rationale for the selected threshold of 3 seconds for TTC in assessing potential traffic conflicts. Exploiting the traffic data extracted from the SR528 highway in Orlando, Florida, we identified different platoons exhibiting TTC values spanning the range of 2.5, 3, and 3.5 seconds.

As demonstrated in Tables 2, 3, and 4, we present the TTC values for each vehicle within the platoons both before and after adjusting the speed of the lead vehicle in each platoon. The analysis of TTC values reveals that when a vehicle's TTC is less than 2.5 seconds, modifying the speed of this vehicle

TABLE 2. Traffic Data From a Vehicle Platooning With TTC < 2.5 Seconds

Time (s)	Vehicle ID	Vehicle Speed (m/s)	Space Headway (m)		TTC (s)	
			Before	After	Before	After
3600	car488.4	5.554	4.26	4.26	0.91	0.91
3600	car490.5	2.912	8.635	8.635	3.26	3.26
3601	car488.4	1.054	5.550	6.090	4.44	3.33
3601	car490.5	4.843	5.43	4.846	1.69	1.27
3602	car488.4	3.014	2.955	2.81	1.09	0.98
3603	car488.4	0.702	5.370	5.330	2.11	2.22
3603	car490.5	2.758	3.620	3.439	1.78	1.76
3604	car488.4	2.524	10.049	10.035	2.13	2.14
3604	car490.5	1.048	5.096	5.005	3.19	3.45
3605	car488.4	5.830	-3.546	-3.567	-4.70	-4.72

TABLE 3. Traffic Data From a Vehicle Platooning With TTC < 3 Seconds

Time (s)	Vehicle ID	Vehicle Speed (m/s)	Space Headway (m)		TTC (s)	
			Before	After	Before	After
3600	car490.3	7.156	7.435	7.435	1.66	1.66
3601	car483.1	7.056	7.826	13.883	2.27	5.31
3601	car490.3	3.613	7.120	15.120	22.64	22.64
3602	car490.3	3.727	3.393	11.393	0.91	17.91
3603	car490.3	0.942	5.568	9.568	2.55	9.55
3604	car490.3	2.426	10.345	12.345	2.16	14.16
3605	car488.4	5.826	-3.551	17.55	-4.70	24.70

TABLE 4. Traffic Data From a Vehicle Platooning With TTC < 3.5 Seconds

Time (s)	Vehicle ID	Vehicle Speed (m/s)	Space Headway (m)	TTC (s)
3600	car490.5	2.912	8.635	3.26
3600	car490.6	2.743	12.234	38.64
3601	car490.6	3.3	5.69	6.57
3602	car490.6	2.55	7.09	8.58
3603	car490.6	2.014	7.21	8.50
3604	car490.6	1.79	5.25	4.74
3605	car490.5	4.56	10.33	8.20
3605	car490.6	1.34	6.98	5.16

results in a reduction of the TTC for the following vehicle leading to new traffic conflicts, as shown by Table II. On the other hand, Table 4 shows that a TTC less than 3.5 seconds leads to the detection of traffic conflicts that are considered false alarms because it sets a relatively sensitive criterion for identifying potential conflicts. In such cases, minor fluctuations in vehicle behavior, such as temporary slowdowns or minor deviations from the normal flow of traffic, can trigger the TTC threshold and be interpreted as conflicts, even if these situations do not pose an actual safety risk.

Setting a lower TTC threshold enhances the likelihood of capturing potential conflicts but can also increase the number of false alarms, which can be problematic for system operators or researchers trying to focus on more critical or significant traffic incidents. Therefore, the choice of a TTC threshold involves a trade-off between sensitivity (capturing potential conflicts) and specificity (avoiding false alarms), and it depends on the specific goals and context of the analysis or system being used. In the context of our platoon analysis, it becomes evident that a TTC threshold of 3 seconds is the most suitable option. This threshold effectively identifies critical incidents while keeping false alarms to a minimum, as shown in Table 3.

VII. EVALUATION

The formal verification of the traffic rule provides a thorough analysis and ensures error-free and reliable behavior. In this section, we will provide a cross-validation using a traffic simulation approach based on real traffic data. By incorporating real-life data into the simulation, we can assess the accuracy and performance of our model in realistic scenarios. This approach allows us to validate and refine predictions from our model while taking advantage of formal guarantees and rigorous analysis provided by formal verification techniques.

FIGURE 5. SR528 highway in Orlando, Florida.

To achieve this goal, we monitor actual traffic flow to extract and analyze TCTs, i.e., TTC, SHW and SWV values.

A. DESCRIPTION OF THE SR528 HIGHWAY

In this section, we use traffic simulation to evaluate the reciprocal relationship between traffic safety indicators to demonstrate the effectiveness of the safety rule in reducing traffic conflicts, as originally claimed. To achieve this goal, we monitored a real-life traffic flow to analyze the variation of the TCTs corresponding to every vehicle. Therefore, we use traffic-related data extracted from loop detectors. These data allow the detection of vehicles passing or arriving at certain points, positioned on a 2-mile section of the SR528 highway in Orlando, Florida, which covers east- and west-bound traffic[1] as seen in Fig. 5. By analyzing the data extracted from this highway using the SUMO traffic simulator [55], we identify different regions of congestion that will focus our attention when conducting the case study. In fact, during these congested periods, we can accurately analyze TTC, SHW and SWV to evaluate the efficiency of the traffic safety rule.

Using the traffic indicators extracted from the real-life dataset, we conduct our analysis based on their calculated values at each time step. Due to the high volume of vehicles involved, our strategy for identifying a platoon entails locating the foremost vehicle and subsequently recognizing the other vehicles following it. In SUMO, each vehicle is assigned a unique vehicle ID, simplifying the process of identifying vehicles in traffic. Additionally, each following vehicle's speed, acceleration, and the leading vehicle's ID, speed, and acceleration are also used to describe them. During this simulation, we extract a list of traffic safety measures, such as TTC and space headway. The shockwave indicator (shockwave speed) is calculated manually by (7). Several vehicles should be considered when calculating the speed to accurately analyze the occurrence of shockwaves. Once a vehicle platoon has been identified, we calculate the shockwave speed to determine if a shockwave exists using the predefined speed thresholds.

B. RESULTS SUMMARY

The validation process described above aims to provide empirical evidence for the effectiveness of the traffic safety property by examining a real-life platoon extracted from a carefully calibrated dataset [50]. In this particular context, our focus is to identify a vehicle platoon present in the real-life dataset, enabling us to conduct a thorough analysis of the extracted indicators values and determine the speed of the shockwave. Table 5 shows the vehicle IDs, speeds, space headways and TTCs extracted values of a sample of vehicles forming a platoon, where each vehicle has its own leader and following vehicle. Based on (7), the shockwave speed is computed for the introduced platoon while taking the vehicle with ID "car432.28" as the leading vehicle and "car447.8" as the vehicle at the end of the presented platoon. Using the extracted parameters values, the shockwave speed is computed by replacing the parameters with their values in (7), which results in (10):

$$\begin{aligned} SWV &= \frac{\frac{v_1}{d_1} - \frac{v_{15}}{d_{15}}}{\frac{1}{d_1} - \frac{1}{d_{15}}} = \frac{\frac{27.817}{38.631} - \frac{24.181}{36.581}}{\frac{1}{38.631} - \frac{1}{36.581}} \\ &= -30\,\text{m/s} < 0 \end{aligned} \tag{10}$$

Per the definition given in Theorem 1, vehicles registering a TTC < 3 and a SHW $< \frac{1}{k}$, i.e., (SHW < 58.823 m), are involved in a traffic conflict. In this case, the calculated shockwave speed indicates the occurrence of a shockwave propagating downstream based on its negative sign. Moreover, analyzing the TTC and space headway values stated in Table 5, it is clear that the thresholds of both indicators are violated by most vehicles in the platoon, which validates the formalized traffic safety rule. This outcome confirms the occurrence of shockwaves whenever the TCTs in question, i.e., TTC and SHW, are below their defined thresholds.

Table 6 provides a comprehensive overview of traffic data, including Shockwave Speed (SWV), Time to Collision (TTC), and Shockwave Speed (SHW) values for each vehicle within a platoon. The computed SWV value, marked by its negative sign and exceeding the defined threshold of 7 m/s, signifies the presence of a shockwave and its downstream propagation. Consequently, a detailed examination of the TTC and SHW values becomes essential to gauge the implications of the observed shockwave on traffic flow. The declining TTC and SHW values, as evident in Table 6, surpassing the respective predefined thresholds for both indicators, corroborate the disruptions and traffic conflicts arising from the occurrence of a shockwave within the traffic flow. By analyzing the behavior of the vehicles within these platoons and extracting the TTC and SHW values, the study seeks to confirm the formalized bidirectional relationship between TTC, SHW, and SWV. This interdependence is characterized by TTC and SHW values violating their thresholds that lead to shockwave occurrences, and conversely, shockwave occurrences also result in violations of TTC and SHW thresholds. This reciprocal

[1] City of Orlando, Florida, USA

TABLE 5. Extracted Time-to-Collision and Space Headway Data From a Vehicle Platooning

Time (s)	Vehicle ID	Vehicle Speed (m/s)	Space Headway (m)	TTC (s)
3600	**car432.28**	27.817	-	-
3600	car446.0	24.877	38.631	10.69
3600	car447.0	25.137	35.359	0.95
3600	car450.4	26.133	117.046	84.24
3600	car446.1	26.592	36.678	0.9
3600	car450.3	26.522	36.576	0.9
3600	car450.2	26.888	36.825	1.15
3600	car447.4	25.273	37.256	1.15
3600	car446.2	23.204	38.181	0.75
3600	car446.3	22.424	45.604	0.75
3600	car446.10	23.209	39.961	16.78
3600	car446.6	23.793	31.661	0.57
3600	car450.6	23.792	34.183	0.57
3600	car447.7	24.582	35.852	1.21
3600	**car447.8**	24.181	34.647	1.21
3600	car450.7	24.545	36.581	0.73

TABLE 6. Extracted Shockwave Data From a Vehicle Platooning

Time (s)	Vehicle ID	Shockwave Speed (m/s)	Space Headway (m)	TTC (s)
3600	**car459.15**	-1.92	30.18	44.948
3600	car468.4		96.42	37.193
3600	car469.0		4.71	52.444
3600	car478.1		4.17	21.580
3600	car468.6		0.63	6.606
3600	car480.0		0.65	3.731
3600	car468.18		1.17	4.934
3600	**car468.23**		2.99	8.883
3600	car468.26		2.78	5.778

relationship is exemplified by the data presented in Tables 5 and 6.

VIII. CONCLUSION

In this paper, our focus is on investigating the reciprocal impact between shockwaves and Time-to-Collision (TTC) along with space headway (SHW) to assess traffic safety during shockwave events. To this end, we provide a detailed formalization and verification of a traffic safety rule that incorporates the relevant TCTs. We initiate our analysis by introducing the bidirectional relationship between time-to-collision (TTC), space headway (SHW), and shockwave speed (SWV) using differential dynamic logic (dL). To ensure the correctness of the traffic safety rule, we use an automated theorem prover called KeYmaera, instead of traditional methods like simulation and paper and pencil-based analysis. To validate the effectiveness of the verified traffic safety rule in real-world traffic scenarios, we conducted a rigorous validation study using the SUMO traffic simulator using a calibrated dataset from the SR528 highway in Orlando, Florida, USA. This approach enables a more precise analysis of the conditions that give rise to and evolve within shockwave occurrences, providing a deeper insight into the intricacies of this traffic event. Moreover, this method provides the driver (or future autonomous vehicle controllers) with sufficient time to react and adjust its behavior according to the traffic conditions in order to safely mitigate traffic conflicts, thereby contributing to a decreased likelihood of collisions.

Limitations:

- The proposed traffic safety rule in this work focuses on the car following models, where vehicles are assumed to drive in a straight line. However, considering different traffic behaviors during shockwaves, such as lane change, will add realism to the proposed approach.
- The work presented in this paper is limited to analyzing vehicle interactions in traffic conflicts between pairs of vehicles. In reality, conflicts can occur between more than two vehicles and secondary crashes due to driver's behavior need to be accounted for to provide a more realistic approach for safety verification.

Future Directions:

- We aim to broaden the scope of our analysis and develop a formal model for the inter-connectivity of vehicles (i.e., connected vehicles) and to assess the effects of main factors such as communication penetration rate, signal power management, and packet loss on traffic delays.
- A future goal is to establish a formal modeling approach for lane change behavior and weaving and to evaluate their effect on traffic safety in different traffic scenarios, such as lane closures in work zones and shockwaves [56].
- The emergence of machine learning (ML) techniques shows promise in addressing transportation issues. However, challenges, such as data bias during training, may result in poor model performance and biased predictions. Furthermore, model drift is a phenomenon in which the data distribution changes over time, leading to a degradation in the performance of the ML model. Despite ongoing efforts to address these concerns, ML algorithms remain black boxes that require further verification. It is also important to note that combining ML with formal verification remains an open research question in the literature [57], [58]. As future work, we aim to connect the fields of formal verification and machine learning by using formal methods to ensure the safety of ML-dependent transportation systems. The research will explore possible methods for merging formal methods and machine learning in autonomous vehicle control models. In particular, we aim to integrate the formally verified traffic rule in this work and Reinforcement Learning to develop a coordinated traffic management system for platooning.

ACKNOWLEDGMENT

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 and their helpful explanations during this work. We would also like to express our gratitude to Mariam Nour (University of Central Florida) for her help with the traffic simulation dataset and her insights during the early draft of the paper.

REFERENCES

[1] T. Stewart, "Overview of motor vehicle crashes in 2020," U.S. Department of Transportation, National Highway of Traffic Safety Administration, Washington, DC, USA, Tech. Rep. DOT HS 813 266, 2022.

[2] L. Zheng, K. Ismail, and X. Meng, "Traffic conflict techniques for road safety analysis: Open questions and some insights," *Can. J. Civil Eng.*, vol. 41, no. 7, pp. 633–641, 2014.

[3] S. R. Perkins and J. L. Harris, "Traffic conflict characteristics-accident potential at intersections," *Highway Res. Rec.*, vol. 225, pp. 35–43, 1968.

[4] O. Hasan and S. Tahar, "Formal verification methods," in *Encyclopedia of Information Science and Technology*, 3rd ed. Hershey, PA, USA: IGI Global, 2015, pp. 7162–7170.

[5] C. Baier and J.-P. Katoen, *Principles of Model Checking*. Cambridge, MA, USA: MIT Press, 2008.

[6] A. Platzer and J.-D. Quesel, "Keymaera: A hybrid theorem prover for hybrid systems (system description)," in *Automated Reasoning*, vol. 5195. Berlin, Germany: Springer, 2008, pp. 171–178.

[7] J. Harrison, *Theorem Proving With the Real Numbers*. Berlin, Germany: Springer Science & Business Media, 2012.

[8] A. Platzer, "Home," 2022. [Online]. Available: https://symbolaris.com/info/KeYmaera.html

[9] T. Nipkow, M. Wenzel, and L. C. Paulson, *Isabelle/HOL: a proof assistant for higher-order logic*. Springer, 2002

[10] B. Akbarpour, A. T. Abdel-Hamid, S. Tahar, and J. Harrison, "Verifying a synthesized implementation of IEEE floating-point exponential function using HOL," *Comput. J.*, vol. 53, no. 4, pp. 465–488, 2010.

[11] C. Muñoz et al., "DAIDALUS: Detect and avoid alerting logic for unmanned systems," in *Proc. IEEE/AIAA 34th Digit. Avionics Syst. Conf.*, 2015, pp. 5A1-1–5A1-12.

[12] A. Rashid, M. Umair, O. Hasan, and M. H. Zaki, "Toward the formalization of macroscopic models of traffic flow using higher-order-logic theorem proving," *IEEE Access*, vol. 8, pp. 27291–27307, 2020.

[13] L. Zheng, T. Sayed, and A. Tageldin, "Before-after safety analysis using extreme value theory: A case of left-turn bay extension," *Accident Anal. Prevention*, vol. 121, pp. 258–267, 2018.

[14] A. Arun, M. M. Haque, A. Bhaskar, S. Washington, and T. Sayed, "A systematic mapping review of surrogate safety assessment using traffic conflict techniques," *Accident Anal. Prevention*, vol. 153, 2021, Art. no. 106016.

[15] P. G. Gipps, "A behavioural car-following model for computer simulation," *Transp. Res. Part B, Methodological*, vol. 15, no. 2, pp. 105–111, 1981.

[16] I. Chatterjee and G. A. Davis, "Analysis of rear-end events on congested freeways by using video-recorded shock waves," *Transp. Res. Rec.*, vol. 2583, no. 1, pp. 110–118, 2016.

[17] A. Platzer, "Differential dynamic logic for verifying parametric hybrid systems," in *Proc. Int. Conf. Automated Reasoning Analytic Tableaux Related Methods*, 2007, vol. 4548, pp. 216–232.

[18] P. Brown, "Only 2 accidents involving self-driving cars caused by poor systems," Oct. 2021. [Online]. Available: http://www.avamerica.org/only-2-accidents-involving-self-driving-cars-caused-by-poor-systems/

[19] E. Sacchi, T. Sayed, and P. Deleur, "A comparison of collision-based and conflict-based safety evaluations: The case of right-turn smart channels," *Accident Anal. Prevention*, vol. 59, pp. 260–266, 2013.

[20] K. El-Basyouny and T. Sayed, "Safety performance functions using traffic conflicts," *Saf. Sci.*, vol. 51, no. 1, pp. 160–164, 2013.

[21] A. Tageldin, M. H. Zaki, and T. Sayed, "Examining pedestrian evasive actions as a potential indicator for traffic conflicts," *IET Intell. Transport Syst.*, vol. 11, no. 5, pp. 282–289, 2017.

[22] T. K. O. Madsen and H. Lahrmann, "Comparison of five bicycle facility designs in signalized intersections using traffic conflict studies," *Transp. Res. Part F, Traffic psychol. Behav.*, vol. 46, pp. 438–450, 2017.

[23] Y. Ma, X. Qin, O. Grembek, and Z. Chen, "Developing a safety heatmap of uncontrolled intersections using both conflict probability and severity," *Accident Anal. Prevention*, vol. 113, pp. 303–316, 2018.

[24] D. Beitel, J. Stipancic, K. Manaugh, and L. Miranda-Moreno, "Assessing safety of shared space using cyclist-pedestrian interactions and automated video conflict analysis," *Transp. Res. Part D, Transp. Environ.*, vol. 65, pp. 710–724, 2018.

[25] K. Ismail, T. Sayed, and N. Saunier, "Automated analysis of pedestrian–vehicle conflicts: Context for before-and-after studies," *Transp. Res. Rec.*, vol. 2198, no. 1, pp. 52–64, 2010.

[26] J. Autey, T. Sayed, and M. H. Zaki, "Safety evaluation of right-turn smart channels using automated traffic conflict analysis," *Accident Anal. Prevention*, vol. 45, pp. 120–130, 2012.

[27] Workshop on Traffic Conflicts, *Proceedings 1st Workshop on Traffic Conflicts Oslo 77*. Oslo, Norway: Norwegian Council for Scientific and Industrial Research, 1977.

[28] M. Essa and T. Sayed, "Traffic conflict models to evaluate the safety of signalized intersections at the cycle level," *Transp. Res. Part C, Emerg. Technol.*, vol. 89, pp. 289–302, 2018.

[29] M. Essa and T. Sayed, "Full Bayesian conflict-based models for real time safety evaluation of signalized intersections," *Accident Anal. Prevention*, vol. 129, pp. 367–381, 2019.

[30] N. Formosa, M. Quddus, S. Ison, M. Abdel-Aty, and J. Yuan, "Predicting real-time traffic conflicts using deep learning," *Accident Anal. Prevention*, vol. 136, 2020, Art. no. 105429.

[31] J. Hayward, *Near Misses as a Measure of Safety at Urban Intersections*. Harrisburg, PA, USA: Pennsylvania Transportation and Traffic Safety Center, USA, 1971.

[32] J. C. Hayward, “Near miss determination through use of a scale of danger,” *Highway Res. Rec.*, vol. 384, pp. 24–35, 1972.

[33] R. V. d. Horst and J. Hogema, “Time-to-collision and collision avoidance systems,” in *Proc. Workshop Int. Cooperation Theories Concepts Traffic Saf.*, 1993, pp. 109–121.

[34] M. Saffarzadeh, N. Nadimi, S. Naseralavi, and A. R. Mamdoohi, “A general formulation for time-to-collision safety indicator,” *Proc. Institution Civil Engineers-Transport*, vol. 166, no. 5, pp. 294–304, 2013.

[35] C. Johnsson, A. Laureshyn, and T. D. Ceunynck, “In search of surrogate safety indicators for vulnerable road users: A review of surrogate safety indicators,” *Transport Rev.*, vol. 38, no. 6, pp. 765–785, 2018.

[36] N. Nadimi, D. R. Ragland, and A. M. Amiri, “An evaluation of time-to-collision as a surrogate safety measure and a proposal of a new method for its application in safety analysis,” *Transp. Lett.*, vol. 12, no. 7, pp. 491–500, 2020.

[37] A. Varhelyi, “Drivers’ speed behaviour at a zebra crossing: A case study,” *Accident Anal. Prevention*, vol. 30, no. 6, pp. 731–743, 1998.

[38] S. P. Hoogendoorn, H. Botma, and M. Minderhoud, *Traffic flow theory and simulation*. Delft University of Technology: Delft, The Netherlands, 2006.

[39] A. Salim, L. Vanajakshi, and S. Subramanian, “Estimation of average space headway under heterogeneous traffic conditions,” *Int. J. Recent Trends Eng. Technol.*, vol. 3, no. 5, pp. 6–10, 2010.

[40] H. Suzuki and K. Matsunaga, “New approach to evaluating macroscopic safety of platooned vehicles based on shockwave theory,” in *Proc. IEEE SICE Annu. Conf.*, 2010, pp. 925–929.

[41] S. G. Machiani and M. Abbas, “Safety surrogate histograms (SSH): A novel real-time safety assessment of dilemma zone related conflicts at signalized intersections,” *Accident Anal. Prevention*, vol. 96, pp. 361–370, 2016.

[42] M. H. Beek, S. Gnesi, and A. Knapp, “Formal methods for transport systems,” *Int. J. Softw. Tools Technol. Transfer*, vol. 20, no. 3, pp. 237–241, 2018.

[43] M. Nour and M. Zaki, “Towards formalization and monitoring of microscopic traffic parameters using temporal logic,” *Transp. Res. Rec.*, vol. 2677, pp. 625–638, 2023.

[44] J. Mao and L. Chen, “Runtime monitoring for cyber-physical systems: A case study of cooperative adaptive cruise control,” in *Proc. IEEE Int. Conf. Intell. Syst. Des. Eng. Appl.*, 2012, pp. 509–515.

[45] M. Althoff, O. Stursberg, and M. Buss, “Safety assessment of autonomous cars using verification techniques,” in *Proc. IEEE Amer. Control Conf.*, 2007, pp. 4154–4159.

[46] S. M. Loos, A. Platzer, and L. Nistor, “Adaptive cruise control: Hybrid, distributed, and now formally verified,” in *Formal Methods*, vol. 6664. Berlin, Germany: Springer, 2011, pp. 42–56.

[47] S. Mitsch, S. M. Loos, and A. Platzer, “Towards formal verification of freeway traffic control,” in *Proc. IEEE Int. Conf. Cyber-Phys. Syst.*, 2012, pp. 171–180.

[48] J. Harrison, “HOL light: A tutorial introduction,” in *Proc. Int. Conf. Formal Methods Comput.-Aided Des.*, 1996, pp. 265–269.

[49] R. Albert, F. Immler, and M. Althoff, “A formally verified checker of the safe distance traffic rules for autonomous vehicles,” in *NASA Formal Methods*, vol. 9690. Berlin, Germany: Springer, 2016, pp. 175–190.

[50] O. Barhoumi, “Formal analysis of traffic conflicts severity using keymaera,” Master’s thesis, Concordia University Montréal, Montréal, QC, Canada, 2022.

[51] M. M. Minderhoud and P. H. Bovy, “Extended time-to-collision measures for road traffic safety assessment,” *Accident Anal. Prevention*, vol. 33, no. 1, pp. 89–97, 2001.

[52] A. Platzer, “Quantified differential dynamic logic for distributed hybrid systems,” in *Proc. Int. Workshop Comput. Sci. Log.*, 2010, pp. 469–483.

[53] A. Ibrahim, M. Čičič, D. Goswami, T. Basten, and K. H. Johansson, “Control of platooned vehicles in presence of traffic shock waves,” in *Proc. IEEE Intell. Transp. Syst. Conf.*, 2019, pp. 1727–1734.

[54] S. Hirst and R. Graham, “The format and presentation of collision warnings,” in *Ergonomics and Safety of Intelligent Driver Interfaces*. Boca Raton, FL, USA: CRC, 2020, pp. 203–219.

[55] P. A. Lopez et al., “Microscopic traffic simulation using SUMO,” in *Proc. IEEE Int. Conf. Intell. Transp. Syst.*, 2018, pp. 2575–2582.

[56] M. S. Rahman, M. Abdel-Aty, J. Lee, and M. H. Rahman, “Safety benefits of arterials’ crash risk under connected and automated vehicles,” *Transp. Res. Part C, Emerg. Technol.*, vol. 100, pp. 354–371, 2019.

[57] B. Thuraisingham, “Trustworthy machine learning,” *IEEE Intell. Syst.*, vol. 37, no. 1, pp. 21–24, Jan./Feb. 2022.

[58] K. Larsen, A. Legay, G. Nolte, M. Schlüter, M. Stoelinga, and B. Steffen, “Formal methods meet machine learning (F3ML),” in *Proc. Int. Symp. Leveraging Appl. Formal Methods*, 2022, pp. 393–405.

OUMAIMA BARHOUMI received the B.Sc. degree in electrical engineering from the National Engineering School of Tunis, Tunis, Tunisia, in 2020, and the M.Sc. degree in electrical and computer engineering from Concordia University, Montreal, QC, Canada, in 2022. She is currently working toward the Ph.D. degree in electrical and computer engineering with Concordia University, under the supervision of Prof. Sofiéné Tahar and co-supervision of Dr. Mohamed H Zaki. She is doing an internship at the National Research Council (NRC) of Canada, where she is working on autonomous driving simulation environments.

MOHAMED H. ZAKI (Member, IEEE) received the Doctoral degree from the Hardware Verification Group, Concordia University, Montreal, QC, Canada, in 2008. He is currently an Assistant Professor with the Civil and Environmental Engineering Department, Western University, London, ON, Canada. He was an Assistant Professor with the Civil, Environmental & Construction Engineering Departmen, University of Central Florida, Orlando, FL, USA. He studies road safety and road-users’ behavior through automated traffic data analysis. Dr. Zaki serves on the Transportation Research Board (TRB) AED50 Committee on Artificial Intelligence and Advanced Computing Applications.

SOFIÉNÉ TAHAR (Senior Member, IEEE) received the Engineering Diploma degree from the University of Darmstadt, Darmstadt, Germany, in 1990, and the Ph.D. degree (Hons.) from the University of Karlsruhe, Karlsruhe, Germany, in 1994. He is currently a Professor and Senior Research Chair in formal verification of systems-on-chip with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada. He is the Founder and Director of the Hardware Verification Group with a research interest in formal verification of hardware and physical systems, and safety and reliability analysis.