Abstract—This paper discusses driving system design based on traffic rules. This allows fully automated driving in an environment with human drivers, without necessarily changing equipment on other vehicles or infrastructure. It also facilitates cooperation between the driving system and the host driver during highly automated driving. The concept, referred to as legal safety, is illustrated for highly automated driving on highways with distance keeping, intelligent speed adaptation, and lane-changing functionalities. Requirements by legal safety on perception and control components are discussed. This paper presents the actual design of a legal safety decision component, which predicts object trajectories and calculates optimal subject trajectories. System implementation on automotive electronic control units and results on vehicle and simulator are discussed.

Index Terms—Decision making, driver assistance, driving automation, electronic control circuit, intelligent vehicles, legal safety, perception, vehicle safety.

I. INTRODUCTION

VEHICLE automation is proposed as one of the solutions that will make transport safer, more comfortable, and more environmentally friendly [1]. Autonomous driving can currently be demonstrated, with highly equipped vehicles under human supervision. The VaMoRs experience [2], ARGO experience [3], Defense Advanced Research Projects Agency (DARPA) Grand Challenges [4], CyberCar [5], CityMobil [6], and CityNetMobil [7] demonstrations presented autonomous vehicles on dedicated infrastructure, with limited interaction with other vehicles. Recently, promising results on automated driving on public roads have been shown by the VisLab and Google teams [8], [9].

For economical, technical, legal, and psychological reasons, vehicle automation is not directly brought to market. It is this paper is organized as follows. Section II presents the legal safety concept and its application to highway environments, based on traffic rules of the Vienna Convention on Road Traffic. Section III discusses the system architecture and presents the perception and control requirements. Sections IV and V explain how the decision component predicts object trajectories and calculates optimal subject trajectories. Section VI presents the system implementation on automotive electronic control units (ECUs) and results on a simulator (SiVIC) and a vehicle (CARLLA) along scenarios that combine ISO, HAVEit, and ABV test cases. Section VII discusses the contribution of this paper and gives a perspective on future work.

II. LEGAL SAFETY ON HIGHWAYS

A. Legal Safety Concept

The word traffic comes from the Arabic taraffafaq, which means “slowly walking along together.” Currently, this is certainly not the most common type of road traffic. Traffic is complex because of the diversity of its participants (e.g., drivers...
personality and vehicle type) and infrastructure (e.g., multiple lanes, junctions, and

t, they will likely need to share the infrastructure with human drivers. A distant future where all vehicles would autonomously be driven would be preceded by a transient period where automated and nonautomated vehicles coexist. One alternative to sharing the infrastructure would be to exclusively assign a part of existing infrastructure to autonomous driving, e.g., dedicated lanes. Another alternative is to create an entirely separated infrastructure for autonomous vehicles. Both alternatives would come at a large cost, reduce the application zone of autonomous driving (e.g., excluding rugged environments and environments with pedestrians and cyclists), and could prove difficult to implement [16]. A solution where driving systems and human drivers share the road seems preferable. This paper discusses the possibility of such a solution.

A legal safety system ensures safety when traffic rules are respected by all traffic participants. In everyday traffic, however, traffic rules are not always respected. A legal safety system uses traffic rules to detect and anticipate the nonlegal behavior of other traffic participants (objects). Several basic defensive driving principles will be discussed. In the case of nonlegal object behavior, a legal safety system prevents an accident if possible and mitigates the accident if not. By definition, a legal safety system allows FA driving. However, FA driving is not allowed by current legislation and raises the ethical question concerning the acceptability of an accident between a legal safety system and a human driver who does not respect traffic rules.

Legal safety system design does not depend on the equipment of other vehicles or infrastructure. A legal safety system can not only cooperate with vehicles that are equipped with compatible vehicle-to-vehicle (V2V) communication and with infrastructure equipped with vehicle-to-infrastructure (V2I) communication but can also share the road with human drivers in a nonequipped environment. The cooperative approach (i.e., with explicit communication) can be seen as a specific case of the independent approach (i.e., without explicit communication), where uncertainty is reduced. For example, V2V can decrease the uncertainty on future object trajectories.

B. Traffic Rules of the Vienna Convention for Highways

Basic traffic rules are defined by an international treaty under the authority of the United Nations, i.e., the 1968 Vienna Convention on Road Traffic [17]. It has not been signed by all countries, and local variations in practice can be found among signatories. Many of the local specificities do not directly apply to the driving task (e.g., driving under intoxication, day lighting, seat belt use, and tire equipment), but some of them do. However, these local variations are not discussed in this paper.

This paper focuses on the application of the Vienna Convention on highways, as suggested in Fig. 1. The highway might be the first environment where highly (and fully) automated driving will become possible, because its simple lane structure and unidirectional flow of large objects facilitate perception, decision, and control algorithms. The description in this paper assumes that driving is on the right side of the road and translation for left-side driving is straightforward. The environment and conditions (day/night conditions, lane keeping/changing, speed range, right/left-side driving) for which the system is designed are referred to as the application zone.

A concise description of Vienna Convention articles that apply to highways is given as follows. The formulation of the rules is simplified for understandability but intends to reflect the exact article content. The original index of the article in the text of the convention is indicated between parentheses.

Rule 1 (7). Road users should avoid damage to road infrastructure or to other road users.

Rule 2 (8). The (human) driver should be in good physical and mental condition and should always be able to control the vehicle.

Rule 3 (10). Driving should be on the rightmost lane if possible, except for overtaking.

Rule 4 (11, 14). A vehicle shall only be overtaken on its left side, except in congested traffic, where right overtaking is also allowed. An overtaking maneuver can only be started if the vehicles in the front and back of the subject vehicle in the same lane have neither indicated nor started to overtake another vehicle and if vehicles in the target lane are not hindered by the maneuver. An overtaken maneuver shall not be performed if prohibited by a traffic sign, and continuous lane markings should not be crossed. The corresponding indicator must be activated during the entire overtaking maneuver.

Rule 5 (13). Speed must be adapted to road and weather conditions (e.g., visibility and road friction), speed limit signs, and the presence of other vehicles. The distance between vehicles must be such that a collision can be avoided if a vehicle performs an emergency brake. Drivers also must be able to avoid collisions with any foreseeable vehicle outside their perception zone.

Rule 6 (17). Braking should only be performed for safety reasons and must be indicated with braking lights.

Rule 7 (25). Only motor vehicles are allowed on highways. Vehicles shall not travel in reverse or in the opposite direction. Vehicles on the highway have priority over vehicles entering. If the vehicle needs to be stopped for a technical reason, this must be done on the emergency
Rule 8 (32). The lighting of the vehicle should be adapted to visibility conditions.

Rule 9 (34). Priority vehicles are exempt from traffic rules, except from Rule 1 (7).

C. Human Rules

A human driver must always be ready to take over control according to the Vienna Convention (Rule 2). This allows highly automated driving, where the driving system controls the vehicle, and the human driver monitors the situation. The legal consequences of FA driving, where the human driver does not need to continuously monitor the situation, are currently investigated by research institutes and vehicle manufacturers [18]–[20]. For FA driving, adaptations to the Vienna Convention are needed. In anticipation of such adaptations, this paper assumes that the term driver in Rule 2 is extended to a human driver, a driving system, or a combination of both in the application zone. This means that, during FA driving, the driving system must monitor its condition (Rule 2) and be able to come to a safe standstill on the emergency lane if, in cases of system failure, the human driver cannot take over control (Rule 7).

Driver-only (DO), driver-assisted (DA), semiautomated (SA), and highly automated (HA) driving have extensively been studied in the HAVEit and ABV projects [14], [15]. During these automation levels, interaction between the human driver and the driving system is designed according to the horse-rider metaphor (H-metaphor) [21], [22]. Automation-level definition and automation-mode selection according to the projects are summarized in Rules 10 and 11.

Rule 10. In automation-level DO, the system is not active. In automation-level DA, the human driver performs longitudinal and lateral control, and the driving system gives feedback on the optimal speed and optimal lane. In SA, the driving system takes over longitudinal control. In HA, the driving system performs longitudinal and lateral control, whereas the human driver monitors the situation and specifies the target speed and target lane. In FA, the human driver no longer needs to monitor the situation, and lane changes are automatically performed. Optionally, the human can choose the driving style, e.g., normal, sportive, or comfortable.

Rule 11. Outside the application zone, only DO is possible. In the application zone, the system switches from DO to DA. The automation mode can be changed by either the human driver or the driving system. The human driver can switch between consecutive automation levels DA, SA, HA, and FA. If the human performs a decisive action on pedals or the steering wheel, the automation level directly switches to DA. The system automatically switches from DA to SA to avoid a collision by braking. The system switches to HA to avoid lane departure. In the case of a system failure or at the end of the application zone, the system automatically brings the vehicle to a standstill on the emergency lane, unless the human driver takes over control in DA.

Sections III–V discuss the legal safety system design according to the aforementioned traffic and human rules.

III. PERCEPTION AND CONTROL REQUIREMENTS

A. System Architecture

The functional architecture of a legal safety system is shown in Fig. 2. As most driving systems, it imitates human driving functions with perception, decision, and control components. The perception component gives an environment description (lanes, traffic signs, and objects) based on sensors such as cameras and radar. The decision component predicts object trajectories and calculates an optimal subject trajectory according to traffic rules (Section II-B), human rules (Section II-C), and system rules (Section III-B). In this paper, optimality refers to the trajectory with the highest speed that respects the three sets of rules, in the trajectory space that is considered by the decision algorithm. The control component keeps the vehicle on the subject trajectory and gives haptic feedback to the host driver. Human–machine interface (HMI) manages communication between the driving system and the host driver.

All information that is exchanged between the perception, decision, control, and HMI components (continuous and dotted lines in Fig. 2) is described in a subject coordinate system $XY$, with origin at the center of the subject rear wheel axle, $X$ to the front and $Y$ to the left, as shown in Fig. 1.

B. System Rules

Apart from traffic rules and human rules, system rules are imposed on each system component to ensure the integrity of calculations of other components. System rules are shortly described as follows.

Rule 12. Within the perception zone, the error on subject, lane, and object descriptions by perception must be within bounds.

Rule 13. Subject trajectories calculated by the decision component must be feasible for control.

Rule 14. The control keeps the subject on a trajectory with a bounded error. The accuracy of control is such that lane
changes are performed within a certain distance and that the vehicle can be kept within the target lane.

Rule 15. All information communicated between components has a bounded number of elements. Perception describes a maximum of the following three lanes: left, subject, and right lanes. Perception describes a maximum of eight objects, as shown in Fig. 3. Nearest objects ahead of and behind the subject in each of the three lanes and objects on either side of the subject are described. The decision component describes a maximum of four trajectories: one optimal trajectory in each lane and one trajectory that brings the vehicle to a standstill during failure functioning. In addition, the calculation time of perception, decision, and control meets predefined bounds.

The remainder of Section III discusses legal safety requirements (i.e., traffic, human, and system rules) with respect to the perception component (see Section III-C) and the control component (see Section III-D). This paper keeps the description of the perception and control components on a requirement level and compares with state-of-the-art technology. It does not aim at contributing to the actual design of these components.

C. Perception Requirements

The organization of the environment in lanes forms the basis for the interaction between traffic participants. Traffic rules (Rules 1, 3, 4, and 7), human rules (Rule 10), and system rules (Rule 12) make reference to the right, subject, and left lanes. These three lanes must be described by perception. In this paper, the lanes are labeled A, B, and C, respectively, as shown in Fig. 3. Lane indices A, B, and C change when the origin of XY crosses a lane marking. Lane description must be available ahead of and behind the subject.

In recent years, extensive research on lane perception based on different types of sensors has been presented. The camera is probably least expensive and best suited for a complete lane description. Vision-based perception of the subject lane is already available on the market as part of LKAS. Research currently investigates the perception of right and left lanes [23]. Perception must distinguish continuous from discontinuous lane markings for Rule 4 and must differentiate normal lanes, emergency lanes, entrance ramps, and exit ramps for Rule 7.

Rule 5 requires the perception of traffic signs, i.e., speed limits, overtaking prohibitions, and lane closures. Both the content and distance of traffic signs are required. Traffic sign recognition by vision has been studied during the last years [24] and currently has first commercial applications such as ISA. Rule 5 also demands adapting the vehicle speed to the road friction. Electronic stability control (ESC) sensors or other proprioceptive sensors could give quite accurate road friction estimation [25] but could not predict a drop of road friction ahead, e.g., caused by oil on the road, ice, snow, or aquaplaning. Similar to the human driver, the system could estimate friction in front with a camera [26].

The perception of position, size, speed, and acceleration of objects in subject, right, and left lanes, ahead of and behind the subject, is required for Rules 1, 4, 5, 6, 7, and 9. At night, at least objects with appropriate lighting should be detected by Rule 8. Object perception is possible with a variety of sensors such as the radar [27], LIDAR [28] and camera [29]. The camera is essential for indicator detection [30] of objects in the subject lane (behind and ahead of subject) for Rule 4. The knowledge of indicator status of objects in right and left lanes is not strictly needed according to traffic rules but helps in defensive driving. The camera also allows increasing the accuracy of lateral object position in the lane, which is determinant for subject trajectory optimality, as will be explained in Section IV.

Apart from information that comes from the aforementioned exteroceptive sensors (e.g., camera and radar), additional information from V2V and V2I communication can be integrated, if available. However, as explained in Section II, a legal safety system must also be capable of FA driving if other vehicles and infrastructure do not have communication equipment.

Perception combines subject, lanes, and objects description into a complete environment model, as shown in Fig. 3. The environment model is communicated to the decision component (see the continuous line in Fig. 2), and subject description is communicated to the control component (see the dotted lines in Fig. 2).

Providing a complete and robust environment perception is the main challenge of a legal safety system. Many requirements that were presented in this section cannot yet be met with state-of-the-art technology. However, research on this topic is intensifying. Reliability and accuracy increase under the impulse of first ADASs such as ACC, LDWS, and LKAS. The estimate is that legal safety perception could be achievable in medium terms.

D. Control Requirements

This section shortly mentions requirements on legal safety control and compares with state-of-the-art technology. For a natural feeling, Rules 10 and 11 require that control is performed through haptic feedback that can be overpowered by the human driver. The control component must be able to handle these disturbances.

Rules 4 and 5 imply lateral control for lane keeping and lane changing and longitudinal control, which, in the extreme case, performs emergency braking. Vehicle control is probably the domain that is most advanced with respect to legal safety. With state-of-the-art technology, limits of perception integrity are usually reached earlier than limits of control; for example, only slow lane changes ensure the integrity of lane tracking. In this case, vehicle dynamics can be assumed linear, which facilitates the task of control. Legal safety control can be based
on longitudinal control [31] and lateral control [32], which are part of existing ADASs.

IV. PREDICTION OF THE OBJECT AND PHANTOM TRAJECTORIES

A. Overview of Approaches

One common approach for object trajectory prediction is to assume that the object will continue its current movement, without taking into account the lane structure. For example, a Kalman filter or one of its variants is used, together with motion models such as constant turning rate and acceleration [33]. In this approach, object behavior is assumed deterministic, i.e., one trajectory per object is computed.

Another approach is to calculate the probability of all possible object movements, e.g., with Gaussian distribution [34]. The subject trajectory is then calculated as a tradeoff between subject speed and the number of collisions with the randomly moving objects. This approach seems reasonable for collision mitigation and avoidance systems, which estimate all possible (i.e., realistic and nonrealistic) object trajectories to avoid premature system activation. For HA and FA driving, however, it is not clear what an acceptable threshold for this collision risk can be. It seems difficult to defend that reasonably foreseeable object behavior and not reasonably foreseeable object behavior are considered on an equal basis.

Object trajectory prediction approaches that do not take traffic rules into account frequently underestimate or overestimate the danger that an object represents. For example, when an object is moving straight and has its indicators activated, lane changing can be expected, but lane keeping is predicted according to a motion model. With the assumption of random object behavior, danger is usually overestimated in safe situations and underestimated in dangerous situations.

This paper proposes an approach to object prediction that is different from the aforementioned approaches. Section IV describes the legal safety prediction of object trajectories based on traffic rules. The legal safety decision component considers not only legal object behavior but also reasonably foreseeable nonlegal behavior, i.e., defensive driving is promoted. It should, however, not anticipate unforeseeable nonlegal behavior but only act when this behavior actually occurs. A minimum amount of confidence must exist between drivers (i.e., driving systems or human drivers) to allow sharing the road.

B. Lane Coordinate System

The curvilinear lane coordinate system \( UW \), with the same origin as the subject coordinate system \( XY \), \( U \)-axis parallel to the middle of each lane and \( W \)-axis perpendicular on \( U \), is a natural environment for calculations with subject and object trajectories. The lane coordinate system \( UW \) and the subject coordinate system \( XY \) are illustrated in Fig. 3. In the lane coordinate system \( UW \), lanes centers have a constant \( W \)-coordinate. Subject and object trajectories that target the lane center can be represented by a transient section (with a varying \( W \)-coordinate) and a permanent section (with a constant \( W \)-coordinate). Calculations with constant \( W \)-coordinates are much easier and faster than calculations in the actual lane geometry in \( XY \), which is usually (but not necessarily) based on a combination of lines, clothoids, and circles [35].

The first step of the decision algorithm consists of transforming the environment description by perception from \( XY \) to \( UW \). All subject and object trajectory calculations are performed in \( UW \). In the final step, the decision component applies an inverse transformation from \( UW \) to \( XY \) to describe trajectories for control and HMI.

C. Zone Model for Subject and Object Trajectories

Many alternatives exist for the mathematical description of subject and object trajectories, e.g., polynomials, circular arcs, splines, and sinusoids [36]. To ensure that trajectory descriptions are precise, these alternatives are usually based on a vehicle model such as a bicycle or a Dubins car [37]. However, no single exact trajectory can realistically describe subject movement due to perception and control errors (Rules 12 and 14). Object movement cannot be represented by an exact trajectory due to perception errors and uncertainty on object behavior. According to legal safety, both subject and object trajectories are uncertain. However, for HA and FA driving, an unbounded uncertainty on subject and object trajectories (e.g., with a Gaussian description) is difficult to defend; no threshold on the probability of collisions between subject and objects seems low enough. This paper proposes a zone model for subject and object trajectories, which represents a bounded and uniform uncertainty. In this paper, the zone model for the subject and objects is described by linear minimum and maximum speed profiles (for longitudinal movement, dotted lines in Figs. 5 and 7) and linear minimum and maximum trajectories (for lateral movement, dotted lines in Figs. 4, 6, and 8). This corresponds to a constant acceleration after a reaction time and to a constant lateral movement toward the target lane after a reaction distance. The lane-based zone model facilitates the implementation of traffic, human, and system rules, as described in Sections IV-D and V-B and C.
D. Trajectory Prediction

Fig. 4 presents possible trajectories for the eight potential objects (1–8) around the subject (0) according to traffic rules. The default trajectory for objects corresponds to lane keeping. Only for 2 is the lane keeping trajectory not calculated. Object 2 is assumed to keep an appropriate distance from the subject (even if the subject performs emergency braking) according to Rule 5. Adapting to the lane-keeping trajectory of object 2 probably goes beyond reasonably limits of defensive driving.

According to Rule 4, objects 2 and 7 have priority on the subject when changing lanes if their indicators are activated and if subject indicators have not been activated. In this case, a lane change is predicted for these objects. Other objects that change lanes must give priority to the subject. As will be explained in Section V, this guarantees that a legal safety trajectory in the subject lane always exists, corresponding to lane keeping at a safe distance from object 7. In principle, lane-changing trajectories of objects other than 2 and 7 should not be predicted. However, to promote defensive driving, the subject also predicts that objects 2, 6, 7, and 8 nonlegally change lanes when they are crossing a lane marking, regardless of whether these lane markings are continuous. For objects 1 and 3–5 behind and on the side of the subject, lane-changing trajectories to B are not predicted for a similar reason as for the aforementioned lane-keeping trajectories of object 2.

The prediction of object trajectories illustrates the importance of an accurate estimation of lateral object position in the lane. Note that, for an object with a minimum/maximum trajectory for lane changing, the other maximum/minimum trajectory corresponds to lane keeping. The object evolves between both trajectories if it were expanding in the future. This reflects the uncertainty on whether the lane change will actually take place. Because the dynamism of the lane change cannot be known, a fast lane change is assumed.

Fig. 5 illustrates the prediction of object speed profiles. For objects behind and on the side of the subject (1–5), a minimum speed profile corresponds to keeping speed. If these objects are accelerating, their maximum speed profile continues the acceleration until the maximum speed. If objects behind or on the side are keeping speed or are decelerating, both minimum and maximum speed profiles correspond to keeping speed. The driving system is conservative by not relying on the fact that these objects keep decelerating. An opposite logic is followed for the prediction of speed profiles of objects on the side and ahead (4–8). These objects are either keeping speed or keep decelerating, as shown in Fig. 5.

The decision algorithm is more defensive than strictly needed by traffic rules. It assumes that objects can offend traffic rules, e.g., by overtaking other objects (including the subject) on the right and exceed speed limits.

Rule 5 stipulates that the subject must be able to avoid collisions with potential objects outside the perception zone. For this purpose, trajectories of phantoms, worst case objects at both ends of the perception zone, are calculated. Figs. 5 and 6 illustrate phantom speed profiles and trajectories. Because driving in the opposite direction is prohibited on highways by Rule 7, worst-case phantoms ahead of the subject correspond to still-standing objects, labeled IV, V, and VI. By considering phantoms, the legal safety system limits its speed such that it can come to a standstill before a traffic congestion that appears at the end of the perception horizon, as will be explained in Section V.

Behind the subject, worst case phantoms I and III correspond to vehicles at the end of the perception zone that travel at speed limit. This prevents the subject from overtaking a slower vehicle when the subject speed and the perception horizon to the rear are low, as will be explained in Section V. In noncongested traffic, the phantom I on the right lane could be ignored, because no object is allowed to right overtake the subject by Rule 4. Phantom II is never considered, because the subject vehicle has priority over vehicles that come from behind on the subject lane by Rule 5.

**Conclusion**

This paper proposed driving system design based on traffic rules, which allows FA driving in traffic with human drivers, without necessarily changing equipment on other vehicles or infrastructure. The legal safety concept also facilitates the cooperation between driving system and host driver during HA driving according to current legislation.

Requirements for legal safety system design for driving on highways were presented in the following three sets of rules: 1) traffic rules for the interaction between driving system and
authors would like to thank the anonymous reviewers for their constructive comments.

REFERENCES


