An Approach to Ensure Safety of Autonomous Vehicles in Planned Trajectories

Joelle Abou Faysal, Nour Zalmai, Ankica Barisic, Frédéric Mallet

An Approach to Ensure Safety of Autonomous Vehicles in Planned Trajectories

Joelle Abou Faysal, Nour Zalmai, Ankica Barisic, and Frederic Mallet

***Abstract*—We propose a Model-Based System Engineering (MBSE) approach for the safety of Autonomous Vehicles (AVs) in planned trajectories. It is a simulation environment in which we specify and generate safety rules with priorities. Its objective is to create a resilient and safe driver monitoring system that continuously checks safety rules, and triggers alarms when violations occur. This framework will also help to detect rule inconsistencies for all the feature block decisions.**

***Index Terms*—Operational Design Domain, autonomous vehicles, model development and verification, test and simulation, specific design domains, automotive model-based safety design, formal rules.**

I. Introduction

AUTONOMOUS vehicle is currently one of the most relevant topics nowadays. It remains a substantial challenge for safety due to some wrong decisions taken by the autonomous vehicle. The unavoidable accidents and death caused by autonomous cars have sparked a debate on their safety and the current limits of technology. Automotive industries have started working on improving safety. Their acceptance in an urban environment, by road users as well as by the authorities, depends on the reliability of their behavior. The relatively large number of accidents involving autonomous vehicles and the difficulty in convincing the public are a reason to give scientific arguments that establish the conditions under which an autonomous system will be able to significantly reduce accidents. Self-driving cars can potentially identify hazards better than people in several circumstances. This will help to avoid human mistakes because autonomous vehicles can have good perceptions and can be less vulnerable to incapacitation, such as distraction or tiredness. To do so, they need to be specifically programmed to prioritize safety over factors.

II. Overview

One proposal to assess safety is to test autonomous vehicles in real traffic and observe their behavior. However, it is neither feasible nor sufficient because it poses significant risks to the environment and requires a lot of testing, which makes it non-scalable [1]. An exhaustive listing of dangerous situations is impossible without precisely defining the conditions under which the vehicle operates. Therefore, we need rigorous and comprehensive approaches to ensure operational safety. So the interest is to work on an approach based on modeling, and which is a promising approach because it is an evolutionary solution that can treat complex systems, and which is considered as a means of communication between engineers instead of text documents. Many of the existing solutions use MBSE approaches, but most of the studies are done to create and generate new scenarios or review ones designed by other experts [2]. They ease the scenario creation process but not formal safety rules description. Existing solutions have also provided new approaches without the need to use large mileage test traces. One of these approaches is called Measurable Scenario Description Language (M-SDL) [3]. Despite being released openly, the modeling and simulation tools are proprietary solutions, and there is no way to specify low-level details such as the characteristics of a sensor that are important for decision-making. Another solution is a modeling and simulation environment called RSS [4]. The downsides of their system are that a change in the software will require new data collection, and they lack the interpretability of the violations and rules. This model is not intended to guarantee that a vehicle will not be involved in an accident. It is, therefore, parametric and does not depend on environmental conditions. Building concrete evidence to measure the safety and security of autonomous vehicles is of critical importance. This is why the design process must be based on formal modeling and verification to give sufficient guarantees.

III. Proposed Approach

The proposed approach consists of ensuring the safety of autonomous vehicles (AVs). We have designed a simulation platform that analyzes the environment and trajectory of AVs and verifies safety based on rules and priorities. It is a domain-specific language that expresses safety properties, as well as scenarios to measure how safety properties can be satisfied. This Model-Based System Engineering (MBSE) approach is based on a simulation environment in which we specify and generate a set of safety rules. we will need elementary data necessary for the system which constitutes the perception. We will also need to know the rules to be defined with their types. This is why we used Renault's documentation called "Area2 known unsafe scenarios" which describes the raw data of the abstract scenarios, their risks and the measures to be taken. From these unsafe scenarios, we were able to describe them more concretely, in the form of rules and priorities, alarms, and actions. They are considered as our use case, and have different priorities or levels of urgency, depending on the current mode of operation. The goal of the approach is to dynamically build and update a model of the global scene from formal models typical of the actors involved (scene and traffic rules). This formal model makes it possible to monitor lower-level control systems, including trajectory planning, to ensure that they behave as expected in the context

of usage scenarios under rules accepted by the authorities, manufacturers, and users. The rules will naturally take into account avoidance and safety behaviors in high-risk situations. The objective is, therefore, to establish a formal verification at run-time, with possible alerts. The behavior of an autonomous vehicle must be tested and verified to meet all requirements. More specifically, we firstly provided a metamodel with an abstract syntax of our safety rules and libraries using EMF technology which describes the Ecore implementation and acts as a meta-model in the UML way, as seen in Fig.1. This is done by perceiving its environment which constitutes the scene, the alarms, the actions, and the properties defined in the libraries. Then, we described safety rules and priorities while providing unlimited user interaction. This is done by using Xtext that helped defining all aspects of a complete language infrastructure. After that, we generate monitors to analyze the solution and detect problems using Xtend technology. We generated a document for the rules and libraries for each modification, and we also generated the code allowing us to adapt the scenarios or the simulator with the described rules. The objective after all is to test, check and graphically display rule violations and inconsistencies using CCSL and Sirius. All those technologies and functions are grouped in the GEMOC tool. Our language, therefore, aims to help safety engineers to verify operational safety issues. Its objective is to ensure the solution proposed by the Advanced Driver Assistant Systems (ADAS) teams. To study the consistency of the rules, we must compare the output of our safety checker module with the output of a feature block after applying perception algorithms, in our use case we will take the Automatic Emergency Braking (AEB) feature block. This will help us compare, in the event of braking, if there is consistency with our actions in an unsafe situation.

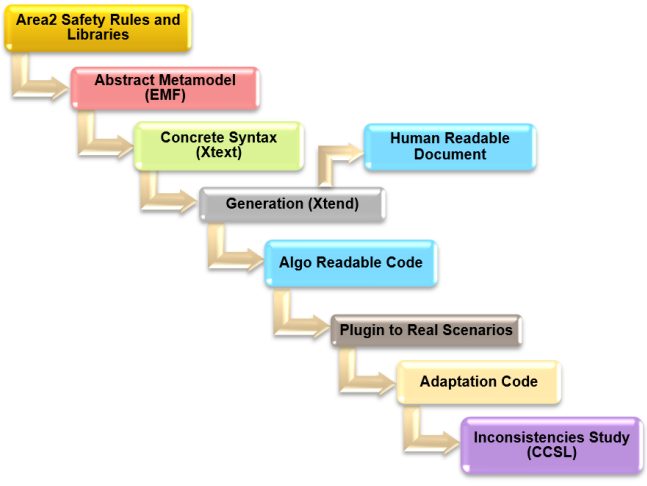

Fig. 1. Overview of the approach with the used technologies.

The use of logical time to coordinate models is highlighted in the GEMOC initiative tool under Eclipse. This is why we used GEMOC to cover all aspects of a Domain Specific Language (DSL) from abstract and concrete syntax to semantic operations. It is also interesting to note that the GEMOC framework generates Java code easily. It generates an IDE with syntax checking.

IV. Conclusion

The goal of the proposed approach is to develop a resilient and safe driver monitoring system that continues to operate safely as long as the assumptions about the Operational Design Domain (ODD) are met. The backbone of the proposal is that it is an evolutionary system compared to others, and it uses GEMOC that is open-source. We want to let the user take control of creating new rules, adding on old ones, or even deleting existing ones. The simulation environment enables safety experts to detect rule breaches by analyzing problems at run-time using generated monitors. Interfacing this model with Renault's simulator with real scenarios is an ongoing work, and this will be helpful later to study inconsistencies between rules and feature blocks. This approach will also be used to find new scenarios or rules to complete the verification of the operational safety on the databases.

References

[1] N. Kalra and S. M. Paddock, "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?" *Transportation Research Part A: Policy and Practice*, vol. 94, pp. 182–193, 2016.

[2] B. Schütt, T. Braun, S. Otten, and E. Sax, "Sceml: a graphical modeling framework for scenario-based testing of autonomous vehicles," in *Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems*, 2020, pp. 114–120.

[3] J. Shenoy, E. Kim, X. Yue, T. Park, D. Fremont, A. Sangiovanni-Vincentelli, and S. Seshia, "A customizable dynamic scenario modeling and data generation platform for autonomous driving," *arXiv preprint arXiv:2011.14551*, 2020.

[4] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a formal model of safe and scalable self-driving cars," *arXiv preprint arXiv:1708.06374*, 2017.

Joelle Abou Faysal received the M.S. degree in computer science and telecommunication engineering from Antonine University (UA), Lebanon, in 2017. She also received her Masters and Research degree in Université Franche-Comté, in Belfort-Monbéliard, France, in 2018. She is currently pursuing the Ph.D. Cifre degree with the Université Côte d'Azur, Cnrs, Inria, I3S and Renault Software Labs in Sophia Antipolis.

Nour Zalmai received the Electrical Engineering Diploma in 2013 from Supélec, Gif-sur-Yvette, France, and the MSc and PhD degrees in electrical engineering, both from ETH Zurich, Zurich, Switzerland, in 2013 and 2017, respectively. His research interests include signal processing and graphical models for learning sparse signal decompositions. He is currently working in engineering at Renault for Algorithm & Embedded SW ADAS/AD.

Ankica Barisic was born in Zagreb in 1983. She is a Postdoctoral researcher at Université Côte d'Azur, Cnrs, Inria, I3S. She also occupied a Postdoctoral researcher at NOVA-LINCS. She obtained PhD degree in computer science, specializing in software systems, from Universidade Nova de Lisboa in 2017 and MSc degree in mathematics, specializing in computer science, from the University of Zagreb in 2010. From 2007 till 2010, she was working as a designer of information systems for the financial industry.

Frederic Mallet (M'99) received the Ph.D. degree from Université Nice Sophia Antipolis, Nice, France, in 2000, and the Habilitation degree in 2010. He is currently a Professor of Computer Science with Université Nice Sophia Antipolis. He researches on the definition of sound models and tools for the design and analysis of embedded systems and cyber-physical systems. He is a Permanent Member of the Aoste Team, a joint team between Inria Sophia Antipolis Research Center, Valbonne, France, and I3S Laboratory (Cnrs UMR), Sophia Antipolis.