July 7, 2022

A New Method for Mathematically Proving the Safety of Automated Driving Vehicles:

-- Accelerating Social Acceptance of Automated Driving by Efficiently Deriving Logical Safety Rules --

The research team led by HASUO Ichiro at the National Institute of Informatics (NII, Japan) developed a methodology to provide strong mathematical safety guarantees to automated driving vehicles, together with its underlying theory on formal logic. This research was conducted under the ERATO MMSD project (*1) funded by the Japan Science and Technology Agency (JST, Japan).

Building on the existing methodology called "Responsibility-Sensitive Safety (RSS)" for mathematical proofs of automated driving safety, the research established its extension called "Goal-Aware RSS (GA-RSS)" that expands RSS's application domain to a variety of real-world driving scenarios. Specifically, the techniques in GA-RSS derived from theoretical results in formal logic (*2) enable one to provide mathematical safety proofs to more complex driving scenarios than before, especially those which require achievement of certain goals such as an emergency stop.

The outcome of this research was published in IEEE Transactions on Intelligent Vehicles, a top journal on automated driving on July 5, 2022 (US Eastern Time).

Summary

- For society to accept automated driving vehicles, both guarantees of safety and traceable explanations for safety assurances (in which one can logically track arguments) are necessary.
- Mathematical proofs are a rigorous means of guaranteeing safety; they are the ultimate form of safety guarantees. However, writing such proofs for actual automated driving systems has proven challenging.
- Formal logic has been used to extend an existing methodology called Responsibility-Sensitive Safety (RSS), and software support for the derivation of safety rules has been designed to enable mathematical proofs of safety even in complex driving scenarios.
- We expect that our results will accelerate society's acceptance and adoption of automated driving vehicles.

Japan Science and Technology Agency（JST）

Public Relations Division
5-3 Yonban-cho Chiyoda-ku, Tokyo
102-8666 JAPAN
TEL：+81(0)3-5214-8404　FAX：+81(0)3-5214-8432
E-Mail：jstkoho@jst.go.jp

Research Organization of Information and Systems
National Institute of Informatics
Publicity Team
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo
101-8430 JAPAN
Direct: +81(0)3-4212-2164　FAX：+81(0)3-4212-2150
E-Mail: media@nii.ac.jp

Background

To realize the adoption of automated driving technology, simply improving the safety of automated driving vehicles is not enough. Guaranteeing a high level of safety and explaining to the public why the vehicles are safe will be necessary before automated driving vehicles will be accepted on public roads. At present, mainstream approaches to guaranteeing safety focus on analyzing accident statistics and testing using computer simulations. However, these empirical and statistical approaches are haunted by questions such as "How do we know that it is safe enough?" and "Can it be explained in a way that society finds convincing?" It thus follows that the creation of a logical approach to explaining safety in a way that is easy for people to understand is highly desirable.

In this context, RSS, a methodology proposed by Intel Corporation and detailed in Figure 1, has recently been attracting attention. RSS is intended to provide mathematical proofs for the safety of automated driving vehicles by expressing traffic safety rules in the form of explicit mathematical formulas and then proving the validity of those formulas. Mathematical proofs are the ultimate form of safety guarantee, both in terms of the degree of assurance provided and in the fact that tracing each logical step of a proof can explain why its conclusion is correct.

Though mathematically proving the safety of complex systems such as automated driving vehicles is generally quite difficult, RSS makes it possible by focusing on "logical safety rules" that vehicles must follow. Because the logical safety rules established by RSS are general and independent of manufacturer or vehicle type, they can be used as international standards, industry standards, and traffic regulations; hence, these rules are expected to greatly accelerate the social acceptance of automated driving vehicles. Although RSS is currently the focus of considerable interest in both industry and academia, the technical basis for formulating and proving logical safety rules has yet to be developed. Consequently, RSS has thus far only been applied to simple driving scenarios, such as following the vehicle ahead on a road without intersections.

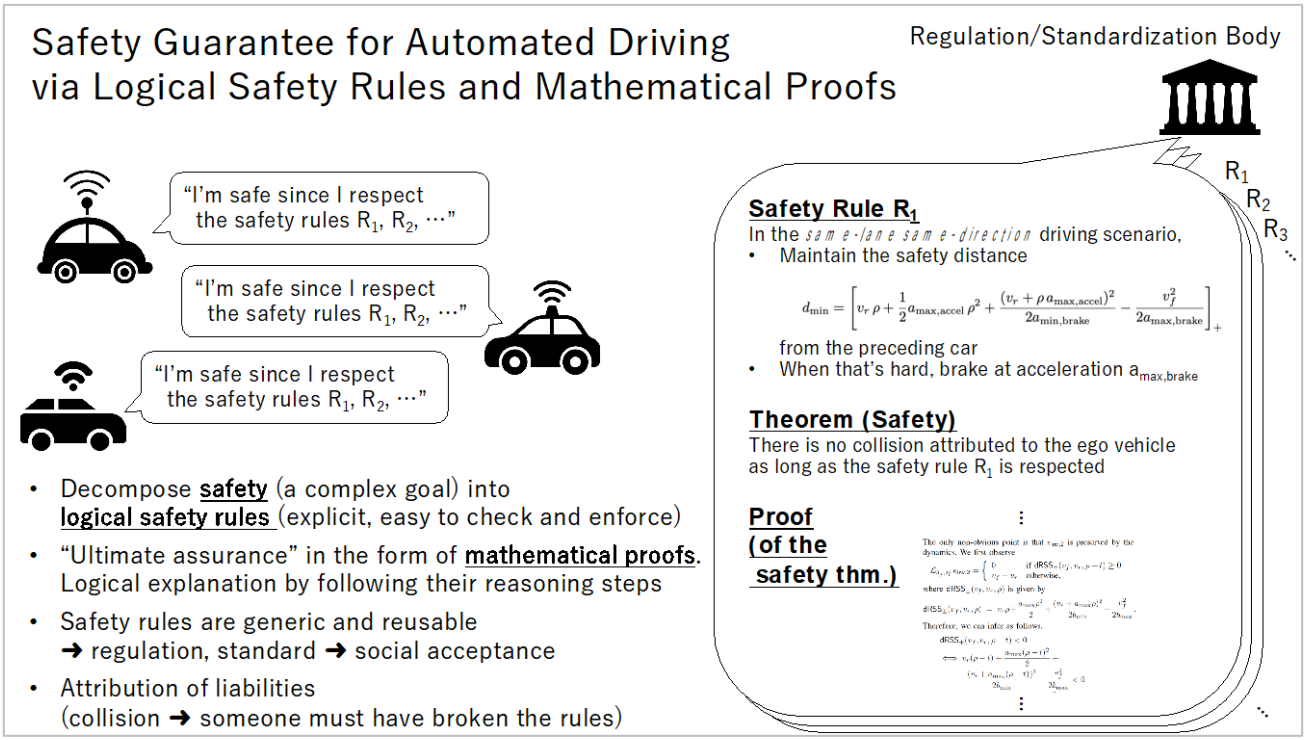

Fig. 1: A proof-based approach to automated driving safety, shared by RSS and our proposed method, GA-RSS. In addition to proposing a rigorous logical safety rule, we mathematically prove a safety theorem that guarantees no accidents will occur as long as this logical safety rule is followed.

Methods and Results

We utilized our expertise in formal logic to establish a new technical foundation for RSS and proposed a novel extension that overcomes the weaknesses of RSS. Our extension is called goal-aware RSS (GA-RSS). While the conventional RSS only covered collision avoidance in simple driving scenarios, GA-RSS can formulate logical safety rules and prove their correctness for complex driving scenarios that require the achievement of goals such as an emergency stop at a safe point while avoiding collision with other vehicles. This extension is an essential technology for the full-fledged deployment of the RSS methodology and its application to a diverse and complex set of real-world driving scenarios.

We proposed a system of formal logic called "differential Floyd-Hoare logic" (dFHL) as the technical basis for enabling GA-RSS, and designed and implemented a workflow and software support for deriving logical safety rules based on it (Figure 2). Conceived of as an extension of the well-known "Floyd-Hoare logic" in software research, dFHL is a system of formal logic for efficiently proving the safety of digital/analog hybrid systems [(*3)], such as automotive control. dFHL greatly expands the scope of applications of RSS by making it possible to partition and sequentially analyze complex control plans for automated vehicles.

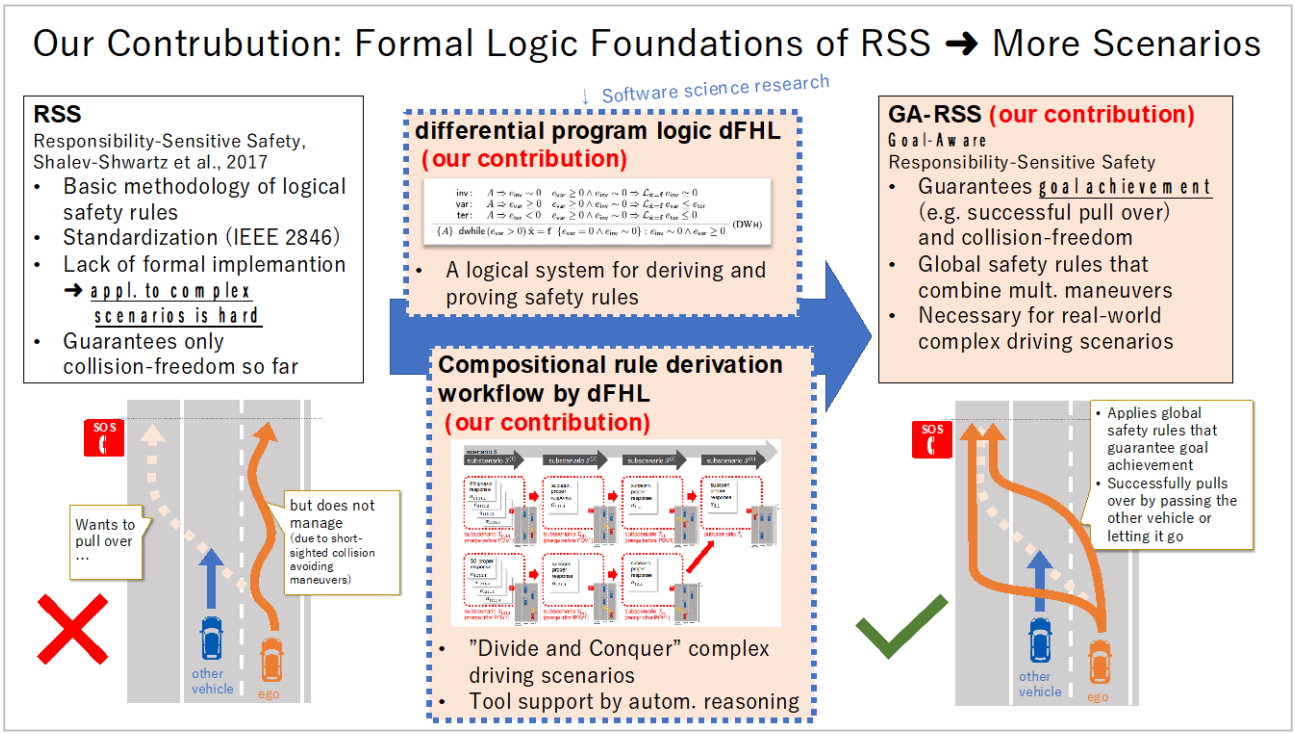

Fig. 2: An example of an emergency stop. RSS (left) was combined with our differential program logic dFHL (middle) to realize GA-RSS (right), making it applicable to a variety of automated driving situations. In the example shown here, the conventional RSS safety rules enforced short-sighted collision avoidance behavior and the emergency stop was not achieved because other vehicles were in the way and lane changes could not be executed. The proposed GA-RSS safety rules incorporated overarching control plans for passing other vehicles by accelerating—or letting them go by braking—to achieve the goal of an emergency stop.

Future outlook

Active attempts to apply RSS to real-world automated driving are already underway, with Intel applying RSS to its products and IEEE P2846 facilitating discussions of international standardization. We believe that our development of GA-RSS will greatly expand the scope of RSS from simple scenarios to realistic and complex scenarios that require the achievement of objectives through a combination of multiple actions, such as emergency stops, and will make a significant contribution to the efforts of the industry to guarantee safety and the development of international standards. If the use of GA-RSS enables broader application of the concept of RSS, and if the ultimate guarantee of safety by mathematical proofs can be provided for various automated driving situations, society's concerns can be dispelled, the adoption of automated driving vehicles can be facilitated, and the development of the industry can be stimulated.

Logical safety rules must be developed and proven for each and every one of the many possible driving scenarios. Use of the rule derivation workflow and software support designed in this research makes it possible to develop logical safety rules for a complex scenario in a realistic timeframe of only a few weeks.

Because the logical safety rules created in this way are general, that is, independent of manufacturer, vehicle type, etc., they can be used for many years and constitute valuable assets for society.

As part of the ERATO MMSD project, we will utilize the workflow and software support proposed here to develop logical safety rules for more driving scenarios. In addition, we will conduct theoretical research and software development to make the formulation of logical safety rules more efficient and less labor-intensive.

Comment from HASUO Ichiro

"Our mission is to contribute to society through our research in formal logic by designing a language (logic system) for writing proofs and providing software to support the activity of writing proofs. We had the opportunity to collaborate on this endeavor with Mazda Motor Corporation and contribute to the important field of automated driving vehicles. I believe that our theoretical research, refined over many years, is now seeing the light of day (in terms of application), and, at the same time, it stands as an example of the importance of basic mathematical and theoretical research.

The ERATO MMSD project, together with other projects such as the MIRAI eAI(*4), CREST CyPhAI(*5), and CREST ZT-IoT(*6) projects , are all part of the activities of NII as a center for comprehensive software research. In particular, by pursuing the theoretical and mathematical foundations of software science, the ERATO MMSD project will contribute to new application areas, such as cyber-physical systems, artificial intelligence systems, and ICT system security."

Funding and Support

This research has been made possible thanks to the support of the Japan Science and Technology Agency's ERATO MMSD Project (JPMJER1603). It was conducted in collaboration with Mazda Motor Corporation (*7).

Information on Paper

Title: Goal-Aware RSS for Complex Scenarios via Program Logic

Authors: Ichiro Hasuo, Clovis Eberhart, James Haydon, Jeremy Dubut, Brandon Bohrer, Tsutomu Kobayashi, Sasinee Pruekprasert, Xiao-Yi Zhang, Erik Andre Pallas, Akihisa Yamada, Kohei Suenaga, Fuyuki Ishikawa, Kenji Kamijo, Yoshiyuki Shinya, Takamasa Suetomi

Posted: IEEE Transactions on Intelligent Vehicles

DOI: https://doi.org/10.1109/TIV.2022.3169762

Date of Publication: July 5, 2022 (US Eastern Time)

END

<Media Contact>
Research Organization of Information and Systems
National Institute for Informatics
Publicity Team
TEL: +81(0)3-4212-2164; E-mail: media@nii.ac.jp

<About JST>
Japan Science and Technology Agency (JST)
Department of Research Project　IMABAYASHI Fumie
TEL: +81(0)3-3512-3528; E-mail: eratowww@jst.go.jp

(*1) ERATO Hasuo Mathematics for Systems Design Project (ERATO MMSD): A research project in the grant scheme "Strategic Basic Research Program ERATO" by the Japan Science and Technology Agency (JST) to promote basic research on quality assurance methods for cyber-physical systems (CPSs), a major pillar of Society 5.0. This project is engaged in the research and development of modeling, formal verification, and testing methods that support reliability assurance, as well as practical verification and validation (V&V) technologies that encompass these methods, with a focus on automated driving, which have attracted attention as a typical example of CPSs. Because tackling these major challenges requires collaboration across diverse academic fields, from software and control to AI, this project promotes research with an emphasis on mathematical (meta) theory, which forms the basis for the fusion of these fields. This project is abbreviated as ERATO MMSD. For more information, please visit https://www.jst.go.jp/erato/hasuo/en/
The official research period ended in March 2022, but research continues to be conducted thanks to an extension of funding (through to March 2025).

(*2) Formal Logic: A branch of mathematics that takes proofs as its object of study. Major applications include the design of formal systems that make it easier to write proofs, as well as the implementation of software for writing and checking proofs. Beginning with the notion of Turing machine, modern computers were originally born from formal logic.

(*3) Hybrid system: Dynamical systems that combine the characteristics of both the digital, discrete dynamics of computers, and the analog, continuous dynamics of physical systems. Because most modern industrial products are controlled by microcomputers, they are examples of hybrid systems.

(*4) MIRAI eAI Project:　a research project supported by the JST-MIRAI program "Super Smart Society (Society 5.0)" mission area. This project aims at developing engineering techniques for AIs, specifically with deep learning techniques, which can meet the fine-grained demands for safety and reliability of ADS. The official title of the project is "Engineerable AI Techniques for Practical Applications of High-Quality Machine Learning-based Systems," and the principal investigator is ISHIKAWA Fuyuki, Associate Professor at NII. For more, please visit https://engineerable.ai/

(*5) CREST Project CyPhAI: A research project supported by JST's CREST program. This project studies robust formal design methods based on mathematics to ensure the safety and reliability of CPSs that include AI as a component (AI-CPS). The formal title is "Formal Analysis and Design of AI-intensive Cyber-Physical," and the principal investigator is SUENAGA Kohei, Associate Professor in the Graduate School of Informatics at Kyoto University, and a Visiting Associate Professor at NII. In addition, KISHIDA Masako, Associate Professor at NII, is a principal collaborator. For more information, please visit https://www.cyphai.io/

(*6) CREST ZT-IoT Project: A research project supported by JST's CREST program. In accordance with the Zero Trust (ZT) concept, this project aims to realize secure IoT systems by integrating formal verification research and system software research. The official title of the project is "Zero Trust IoT by Formal Verification and System Software," and the principal investigator is TAKEFUSA Atsuko, Professor at NII. SEKIYAMA Taro, Assistant Professor at NII, is a principal collaborator. For more information, please visit https://zt-iot.nii.ac.jp/

(*7) The model we examined is a prototype for research evaluation, and its quality does not have any relationship with the quality of the actual products.