April 10, 2024

Mathematical Formulation of ISO 34502 Hazardous Scenarios for Automated Driving Systems

— Automation and Streamlining of Safety Assurance Tasks Accelerate Social Acceptance of Automated Driving —

A research group including Professor HASUO Ichiro of the Information Systems Architecture Science Research Division of the National Institute of Informatics (NII, Director-General: KUROHASHI Sadao, Chiyoda-ku, Tokyo, Japan), Dr. WAGA Masaki, Assistant Professor of the Department of Informatics in the Graduate School of Informatics of Kyoto University (President: MINATO Nagahiro, Kyoto-shi, Japan) and others has mathematically formulated the hazardous scenarios specified in ISO 34502,[*1] an international standard that stipulates a framework for the safety assurance of vehicles with automated driving systems as a part of the Exploratory Research for Advanced Technology (ERATO) HASUO Metamathematics for Systems Design project[*2] (ERATO MMSD, Research Director: HASUO Ichiro, Information Systems Architecture Science Research Division at the NII) implemented by the Japan Science and Technology Agency (JST, President: HASHIMOTO Kazuhito, Chiyoda-ku, Tokyo, Japan).

This research translates hazardous scenarios traditionally described in English and other natural languages into descriptions in a formal language called signal temporal logic (STL)[*3]. This fixes the meanings of hazardous scenarios that may cause differences in interpretation and opens the way to the automation and streamlining of safety evaluation tasks using hazardous scenarios. This achievement has positive effects on the safety assurance of automated driving vehicles. It also suggests that mathematics plays a significant role in the utilization of requirements likened to contracts between information systems and the human society.

The research findings were presented on April 9, 2024 (central European time) at the 39th ACM/SIGAPP Symposium on Applied Computing (SAC), a major international conference on application of informatics.

Key Points

- For the full ubiquitization of automated driving vehicles, it is imperative that we establish social trust in them based on extensive and detailed safety assurance activities.
- For this purpose, hazardous scenarios faced by automated driving vehicles are comprehensively defined in ISO 34502. Given that they are described in natural language, it

情報・システム研究機構 国立情報学研究所
京都大学 情報学研究科
科学技術振興機構（JST）

is possible that difference may occur in the interpretation of their meanings. It is also difficult to process them mechanically using software tools.

- This research employs a formal language called STL to mathematically formulate the hazardous scenarios in ISO 34502. This fixes the meanings of the hazardous scenarios and opens the way toward the automation and streamlining of monitoring and other safety evaluation tasks.
- It has positive effects on safety assurance of automated driving vehicles. It also suggests the significant role that mathematics may play in the social acceptance of automated driving and other new technologies.

Background

To make the automated driving technologies widely accepted in society, merely improving the safety of automated driving vehicles is insufficient. It is necessary to guarantee their high level of safety and explain this to society to persuade society to accept automated driving vehicles operating on public roads. In Japan and abroad, many different safety assurance frameworks have been proposed. Among them, ISO 34502 is a framework that originated in Japan based on the efforts of Japan Automobile Manufactures Association, Inc. (“JAMA”).

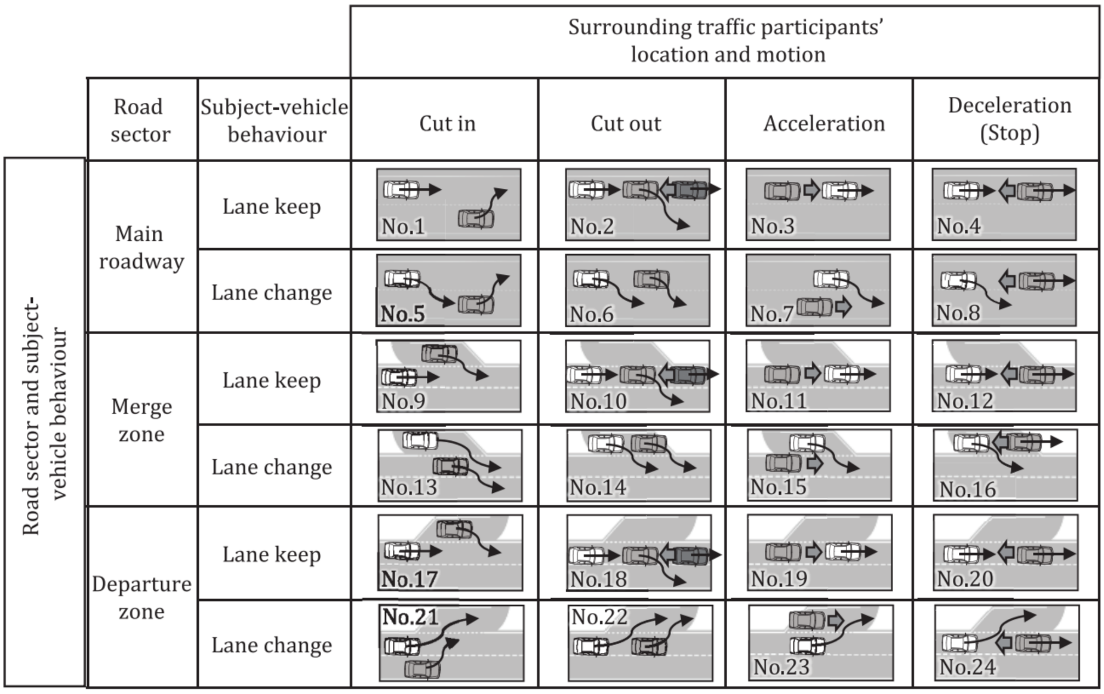
ISO 34502 provides a comprehensive list of hazardous scenarios faced by automated driving vehicles. They are based on a combination of hazardous elements at each of the three phases, perception, decision and control, that the operations of vehicles equipped with automated driving systems are divided into. This stance takes the approach of guaranteeing the safety of automated driving vehicles by assessing whether or not proper safety actions can be taken in these hazardous scenarios.

However, under ISO 34502, these hazardous scenarios are described in natural language, in English specifically. This poses an obstacle to their large-scale application. The first issue comes from the vagueness of natural language. Take “forcible lane change” for example. There are different interpretations of what exactly it means.

The second issue is the difficulty of software processing. To evaluate safety using the hazardous scenarios it is necessary to execute a huge number of safety evaluation tasks, including monitoring to detect occurrences of hazardous scenarios and creating test data to simulate the operating conditions in which a hazardous scenario may occur. We need software to automate them. However, regarding the hazardous scenarios described using natural language, it is necessary to freshly create software to execute the tasks from scratch for each scenario. This requires a huge amount of labor.

Research method and achievements

To resolve the issues above, the research team mathematically formulated some of the hazardous scenarios described in ISO 34502, particularly those arising from hazardous elements in the decision phase (Fig. 1). This process created mathematical definitions for individual hazardous scenarios and fixed their meanings.



Road sector and subject-vehicle behaviour		Surrounding traffic participants' location and motion			
Road sector	Subject-vehicle behaviour	Cut in	Cut out	Acceleration	Deceleration (Stop)
Main roadway	Lane keep	No.1	No.2	No.3	No.4
	Lane change	No.5	No.6	No.7	No.8
Merge zone	Lane keep	No.9	No.10	No.11	No.12
	Lane change	No.13	No.14	No.15	No.16
Departure zone	Lane keep	No.17	No.18	No.19	No.20
	Lane change	No.21	No.22	No.23	No.24

Fig. 1: Table of ISO 34502 hazardous scenarios which arise particularly from hazardous elements in the decision phase. This table is cited from ISO 34502:2022.

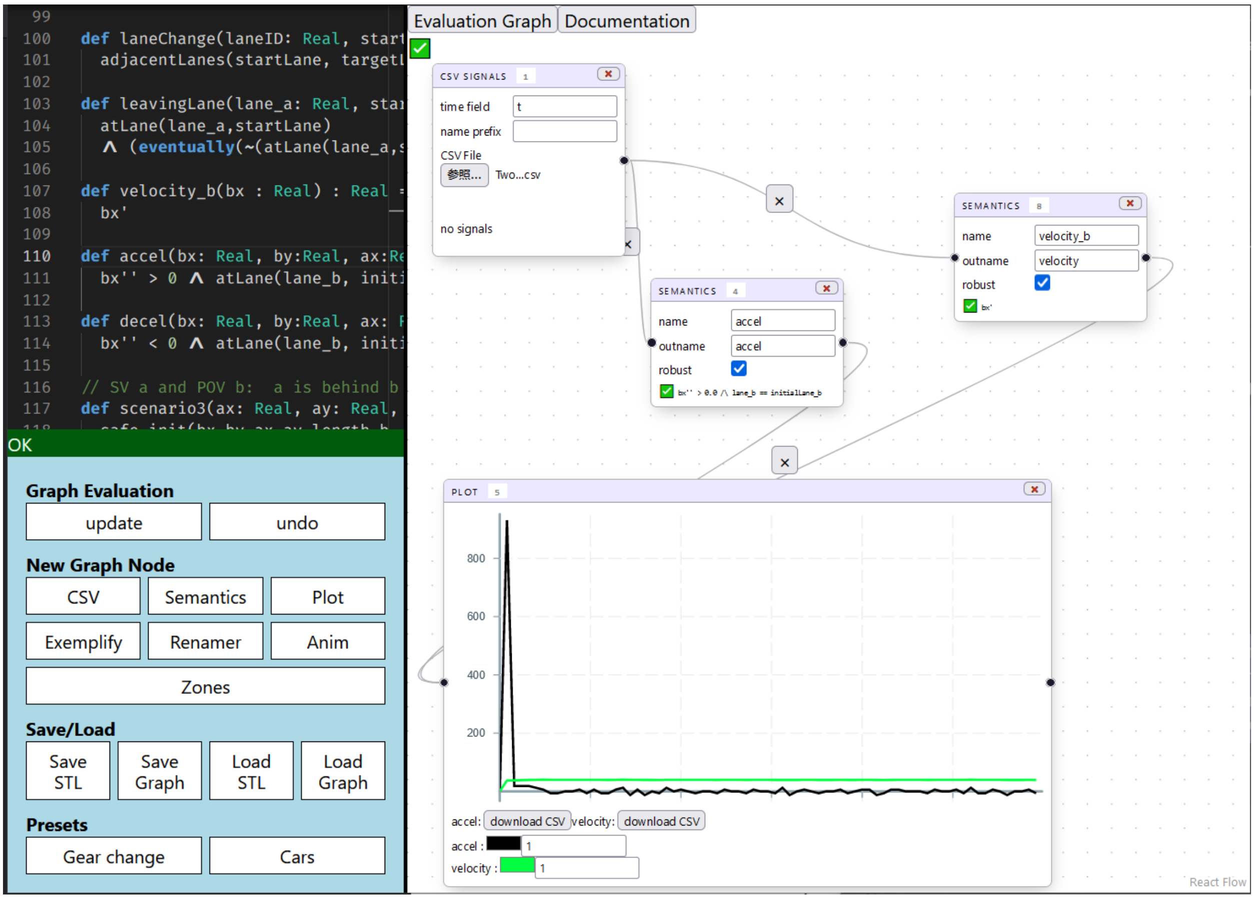
The research employed STL to mathematically formulate the scenarios (Fig. 2). When writing programs, one uses some programming language which is a formal language. Similarly the hazardous scenarios are expressed in a formal language called STL. Since the meanings of the vocabulary of STL are already defined mathematically, the meanings of the hazardous scenarios get defined mathematically. In addition, the formulation process was carried out while checking whether or not the mathematical meanings described matched the original intentions of ISO 34502 using STL Debugger, an interactive tool being developed by the research group (Fig. 3).

$scenario_i(SV, POV, L) \;:=\; initSafe(SV, POV) \wedge roadSector_i(SV, POV) \wedge disturb_i(SV, POV, L)$, $i = 1, \ldots, 24$ (cf. this is (1). *initSafe* is from §4.3)

$disturb_i(SV, POV, L) \;:=\; initialCondition_i(SV, POV, L) \wedge behaviourSV_i(SV, L) \wedge behaviourPOV_i(POV, SV, L)$, $i = 1, \ldots, 24$ (cf. (2) in §3)

i	$roadSector_i$ (cf. §4.1)	i	$initialCondition_i$ (cf.§4.2)	$behaviourSV_i$ (cf.§4.4)	$behaviourPOV_i$ (cf.§4.5)
$1-8$	$mainRoad(SV, POV)$	1	$\top$	$laneKeep(SV, L)$ $\mathcal{U} danger(SV, POV)$	$cutIn(POV, SV)$
		2	$sameLane_3(SV, POV_1, POV_2, L)$ $\wedge aheadOf(SV, POV_1)$ $\wedge aheadOf(POV_1, POV_2)$	$laneKeep(SV, L)$ $\mathcal{U}(\neg sameLane(SV, POV_1, L))$	$leavingLane(POV_1, L)$ $\wedge(laneKeep(POV_2, L)$ $\mathcal{U}(\neg sameLane(POV_2, POV_1, L)$ $\wedge danger(SV, POV_2)))$
		3	$aheadOf(POV, SV)$ $\wedge(sameLane(SV, POV, L)$ $\vee inAdjLanes(SV, POV, L))$	$laneKeep(SV, L)$ $\mathcal{U} danger(SV, POV)$	$accel(POV, SV, L)\ \mathcal{U}\ danger(SV, POV)$
		4	$aheadOf(POV, SV)$ $\wedge(sameLane(SV, POV, L)$ $\vee inAdjLanes(SV, POV, L))$	$laneKeep(SV, L)$ $\mathcal{U} danger(SV, POV)$	$decel(POV, SV, L)\ \mathcal{U}\ danger(SV, POV)$
		5	$\top$	$leavingLane(SV, L)$	$cutIn(POV, SV)$
		6	$\top$	$leavingLane(SV, L)$	$cutOut(POV, SV, L)$
		7	$aheadOf(POV, SV)$	$enteringLane(SV, L)$	$accel(POV, SV, L)\ \mathcal{U}\ danger(SV, POV)$
		8	$sameLane(SV, POV, L)$ $\wedge aheadOf(SV, POV)$	$leavingLane(SV, L)$	$decel(POV, SV, L)\ \mathcal{U}\ danger(SV, POV)$
9–16	$mergeZone(SV, POV)$	9–16	$initialCondition_{i-8}$	$behaviourSV_{i-8}$	$behaviourPOV_{i-8}$
17–24	$departZone(SV, POV)$	17–24	$initialCondition_{i-16}$	$behaviourSV_{i-16}$	$behaviourPOV_{i-16}$

Fig. 2: An example mathematical formula for an ISO 34502 hazardous scenario, an achievement of this research project. The table shows a template for scenarioᵢ (i = 1, 2, ..., 24), which represents the individual hazardous scenarios, and their constituents.



```
def laneChange(laneID: Real, start
  adjacentLanes(startLane, targetL

def leavingLane(lane_a: Real, star
  atLane(lane_a,startLane)
  ∧ (eventually(~(atLane(lane_a,s

def velocity_b(bx : Real) : Real =
  bx'

def accel(bx: Real, by:Real, ax:Re
  bx'' > 0 ∧ atLane(lane_b, initi

def decel(bx: Real, by:Real, ax: R
  bx'' < 0 ∧ atLane(lane_b, initi

// SV a and POV b:  a is behind b
def scenario3(ax: Real, ay: Real,
```

OK

CSV SIGNALS 1
time field: t
name prefix:
CSV File: 参照... Two...csv
no signals

SEMANTICS 4
name: accel
outname: accel
robust: ☑
☑ bx'' > 0.0 /\ lane_b == initialLane_b

SEMANTICS 8
name: velocity_b
outname: velocity
robust: ☑
☑ bx'

PLOT 5
accel: download CSV velocity: download CSV
accel : ■ 1
velocity : 🟩 1

Fig. 3: STL Debugger screenshot. The GUI section on the right side interactively shows the meaning of the STL logic formula entered in the text section in the upper left part.

The mathematical formulation in STL solve the second issue above as well. There are a large number of algorithms that can conduct monitoring and generate test data from the data expressed in STL as input, including the previous results of the research group. The current research findings have opened the way toward the application of these algorithms to the evaluation of safety under the ISO 34502 standard.

Outlook

STL is a formal language that is expected to be broadly applied in the manufacturing industry. An ecosystem of STL-based quality assurance software tools is rapidly arising. The current research findings link the software ecosystem and the ISO 34502 framework for the safety assurance of automated driving vehicles. This not only improves the social acceptance of automated driving but also accelerates automation and digitalization in the manufacturing industry.

Meanwhile, it was a common belief that the intended descriptions can only be formalized by engineers familiar with STL. This has hindered the utilization of STL in the industrial world. STL is by no means a difficult formal language. Even so, a learning process is much like that of a new programming language. Used in the research project, the STL Debugger plays the same role as the debuggers used for general programming languages. It aids the process of learning STL and the use of the language in industry.

The research employs the notion of responsibility-sensitive safety (RSS)[*4] distance to define the notion of hazard in the formulation process. RSS is in the spotlight as a method for mathematically proving the safety of automated driving vehicles. It is hoped that the current research achievements will further demonstrate the practical relevance of RSS.

More generally, the mathematical formulation of properties, requirements, specifications, expected usage scenarios etc. of various information systems helps clarify the meanings and automate data processing. It has tremendous industrial and social significance as it aids the development of highly reliable and efficient products. The research group will work to broadly disseminate this specific form of the application of mathematics in society and to enhance the technologies and software tools that support it. It will thus continue its research efforts with a view toward the establishment of reliable information systems and the social acceptance of these systems.

Statement from Professor HASUO Ichiro:

This research was inspired by a collaboration with Mitsubishi Electric Corporation. It proposed ISO 34502 for a case study on the mathematical formulation of requirements in STL which made these achievements possible.

New information technologies such as automated driving systems and generative AI always face the issue of social trust. In other words, they are tested to see if they are safe enough to be accepted by society. In this process, the requirements that should be met by those information systems act as contracts with society and as the foundation for social trust. Mathematical formulation as in The research project is very important in this respect. We will advance our research and development of mathematical technologies to the organize relationships between information technologies and society and to realize a human-centered society where information technologies are used safely.

Research Project

This research was conducted as part of the HASUO Metamathematics for Systems Design project (JPMJER1603), a part of the Exploratory Research for Advanced Technology (ERATO) program of the Japan Science and Technology Agency (JST), the project for the Realization of Full-Scale Spread of Automated Driving Using Technologies for the Logical Explanation of Software Quality (JPMJST2213), a project promotion type (commercialization support) project in the JST's Program for Creating Start-ups from Advanced Research and Technology (START), and the Formal Analysis and Design of AI-intensive Cyber-Physical Systems (JPMJCR2012) project that is a part of the JST Strategic Basic Research Program CREST. This research involved collaboration with the Information Technology R&D Center of Mitsubishi Electric Corporation.

Title and Authors

Title: Temporal Logic Formalisation of ISO 34502 Critical Scenarios: Modular Construction with the RSS Safety Distance

Authors: Jesse Reimann, Nico Mansion, James Haydon, Benjamin Bray, Agnishom Chattopadhyay, Sota Sato, Masaki Waga, Étienne André, Ichiro Hasuo, Naoki Ueda, Yosuke Yokoyama

Venue: The39th ACM/SIGAPP Symposium On Applied Computing (SAC) 2024

Date: April 9, 2024 (Central European Time)

<Media Contact>

National Institute for Informatics Research Organization of Information and Systems
Publicity Team, Planning Division, General Affairs Department
Tel: +81-3-4212-2164 E-mail: media@nii.ac.jp

Kyoto University
International Public Relations Office, Public Relations Division, External Affairs Department
Tel: +81-75-753-5729
E-mail: comms@mail2.adm.kyoto-u.ac.jp

<JST's Business Contact>

Japan Science and Technology Agency (JST)
IMABAYASHI Fumie,
Department of Research Project
Tel: +81-3-3512-3528 E-mail: eratowww@jst.go.jp

(*1) ISO 34502: A framework that originated in Japan for the safety assurance of automated driving vehicles based on the Automated Driving Safety Evaluation Framework developed by Japan Automobile Manufactures Association, Inc. For more information, see the news release from the Ministry of Economy, Trade and Industry at:
https://www.meti.go.jp/english/press/2022/1116_003.html

(*2) ERATO Hasuo Metamathematics for Systems Design project: A project selected by the Japan Science and Technology Agency (JST) as a part of its Exploratory Research for Advanced Technology (ERATO) program. It carries out academic research on quality assurance methods for cyber physical systems (CPS) which will be a significant pillar of Society 5.0. Specifically, it defines automated driving systems as a priority technology to be used in the future, as they are attracting attention as typical examples of CPSs. It works on the research and development of methods for modeling, formal verification and testing to support the assurance of the reliability of these systems, and technologies for the practical verification and validation (V&V) of these methods. A major ambitious project like this requires people in multiple academic disciplines, such as software, control and artificial intelligence (AI), to collaborate. In the research process, it also emphasizes metamathematical theories that provide a foundation for inter-disciplinary integration. This is abbreviated as ERATO MMSD. For more information about the project, see https://www.jst.go.jp/erato/hasuo/en/. The research period of the project terminated in March 2022. Currently, research is being continued in the additional support period that ends in March 2025.

(*3) Signal Temporal Logic (STL): A system of logic for describing the characteristics of time-varying signals obtained by adding $F_{[0, T]}$ (not later than T seconds from now), $G_{[0, T]}$ (constantly for a period of T seconds from now) and other temporal operators to propositional logic, which is a fundamental system of logic using operators such as $\wedge$ (and) and $\vee$ (or). It was introduced in 2004 by Oded Maler and Dejan Nickovic.

(*4) Responsibility-Sensitive Safety (RSS): A methodology that was first proposed by a researcher working for Mobileye Technologies Limited to mathematically demonstrate the safety of automated driving vehicles. When it is applied to the specific driving scenario of averting a rear-end collision, a formula for the inter-vehicular distance at which the rear-end collision can be avoided without fail by properly applying the brake (RSS safety distance) is obtained. The ERATO MMSD research achievements in 2022 paved the way for its application to complicated driving scenarios such as a lane change and an emergency stop. For details, refer to the news released at:
https://www.nii.ac.jp/en/news/release/2022/0707.html