

DEVELOPMENT OF A SAFETY ASSURANCE PROCESS FOR AUTONOMOUS VEHICLES IN JAPAN

Jacobo, Antona-Makoshi

Nobuyuki, Uchida

Kunio, Yamazaki

Japan Automobile Research Institute (JARI)

Japan

Koichiro, Ozawa

Honda R&D Co. and Japan Automobile Manufacturers Association, Inc. (JAMA)

Japan

Eiichi, Kitahara

Nissan Motor Co. and JAMA

Japan

Satoshi, Taniguchi

Toyota Motor Co. and JAMA

Japan

Paper Number 19-0000

ASBTRACT

In order to introduce autonomous driving systems into the market, socially acceptable and technically sound safety assurance methodologies need to be agreed. In Japan, vehicle manufacturers and traffic safety experts have gathered regularly under the auspice of the Ministry of Economy, Trade and Industry, in a coordinated initiative to harmonize the required collaborative research, methodology development and standardization activities. Within this initiative, a comprehensive safety assurance process is to be agreed and made publicly available. The process shall be driven by top safety goals defined by authorities, shall consider the systems' performance limitations, and must be supported by state-of-the-art methodologies and real-world data. At this point, consensus on the overall safety assurance process for SAE Level 3+ autonomy in motorways as well as on the methodology to develop testing scenarios has been achieved and the results are hereby reported. The process and methodology are directly applicable to support the development of systems towards a safer autonomous driving society.

INTRODUCTION

Socially acceptable and technically feasible safety assurance methodologies and criteria need to be established as state-of-the-art global standards for a safe deployment of Autonomous Driving (AD) vehicles into the market. In order to guide this deployment in different regions, corresponding authorities such as the US National Highway Traffic Safety Administration, the UN Economic Commission for Europe, and the Ministry of Land Infrastructure, Transportation and Tourism of Japan have released their own safety guidelines [1, 2].

Product failures and design errors can be covered by an existing functional safety standard ISO26262:2011 [3]. This standard is used to evaluate if a process conforms and hence can be considered safe. In particular, the Safety of the Intended Functionality (SOTIF) process contained within the standard provides coverage of SAE Level 2 AD systems. However, a specific safety assurance process for non-failure conditions that considers SAE Level 3 and higher (3+) AD systems and their performance limitations has not been established yet.

Traditional proving ground and field operation testing are insufficient to proof safety for vehicles with highly autonomous vehicles [4], and the incorporation of complementary virtual testing methodologies is essential. To support the development of these methodologies, joint efforts between industry and authorities are required.

In Japan, vehicle safety and AD experts have gathered regularly supported by the Ministry of Economy, Trade and Industry under the umbrella of the JAMA AD safety assurance working group, in a coordinated initiative to harmonize the required collaborative research, methodology development and standardization activities. A first scope for application of the developed methodologies has been set to SAE level 3+ AD systems on motorways [1].

Within this initiative and scope, our aim is to propose an AD system safety assurance engineering process for non-failure conditions that considers the system's performance limitations. A summary of the overall process is provided, followed by detailed description of the methodology to define virtual test scenarios and related criteria required to assure AD systems safety.

ENGINEERING FRAMEWORK FOR AD VEHICLE TEST SCENARIOS

A schematic of the overall safety assurance process developed is shown in Figure 1. The schematic is based on the project management V-model typically applied to develop connected vehicles, advanced driver assistance systems (ADAS) and AD systems [5]. The process covers all the product development stages from planning, design, implementation, evaluation (verification and validation), to release. Descriptions of each of these steps are provided below.

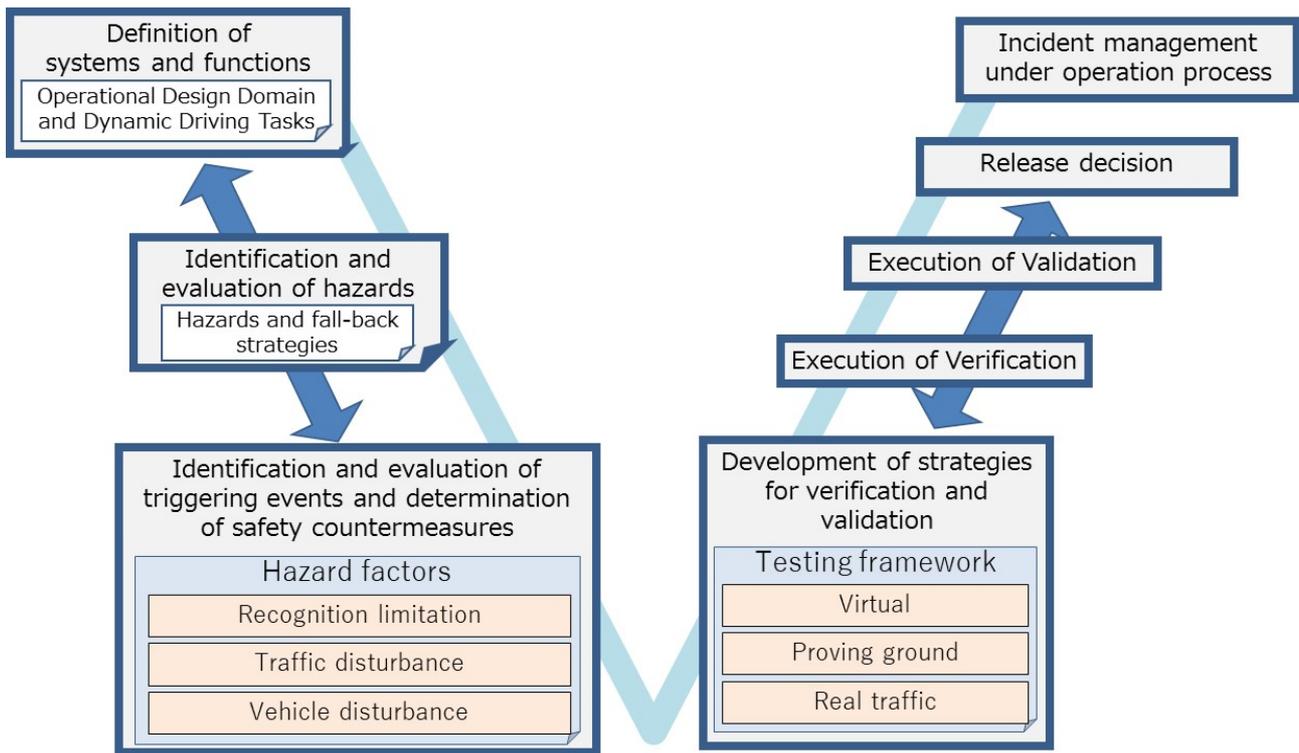


Figure 1 Overall scheme of the safety assurance process

Definition of systems and functions: Operational Design Domain and Dynamic Driving Tasks

The complete safety assurance process is to be conducted within well-defined and pre-determined operational and responsibility share boundaries. Therefore, upon the collection of existing information concerning the purpose and specification of different AD systems and functions, the Operational Design Domain (ODD), defined as the boundaries within the system is intended to operate, is described at the initial stage. ODD contents shall include at least information on roadway types, location within the road, vehicle speed ranges, and environmental conditions. The ODD definition needs to be structured in a way that the user can understand and operate the AD system safely. On the other hand, the test scenarios that will be developed shall consider the ODD in a technically comprehensive way based on the physics of the system. For example, when rainy conditions are included in the ODD, the term 'rain' may be enough to communicate with the user, but the scenario might consider the effect of rain from different physical viewpoints such as the possible influence of raindrops on sensor performance, or the influence of rain on vehicle dynamics due to a decrease of the friction coefficient between the tires and the wet road surface. In order to organize all the ODD related information concerning the vehicle and its surroundings in a systematic manner, the Goal Structuring Notation methodology is applied [6]. This methodology is a standardized graphical argumentation technique widely applied to document and present safety goals and arguments in a clearer format than plain text [6].

The Dynamic Driving Tasks (DDT) and the responsibility share between the system and the driver are also defined at this point. It is noted that clarifying the responsibility share in accidents involving other vehicles that committed traffic rule violations or emergency rescue operations is particularly challenging, and solutions beyond vehicle development

engineering may be required (e.g. crashes involving roads with potholes due to lack of road maintenance; crashes involving vehicles running in the wrong direction; or recognition limitations to take appropriate interventions in crashes involving emergency vehicles such as ambulances or police cars).

Identification and evaluation of hazards

Hazards, defined as potential sources of harm [2], are identified and evaluated at this point. Since hazards can be expressed at the vehicle behavior level, the ISO 26262 framework may be applied and the standardized hazard and risk assessment results may be diverted for the current purpose. If the hazards identified are judged unacceptable, a validation target shall then be specified for further analysis in the validation process. In addition, actuation strategies can be implemented at this stage to ensure safety for all traffic participants for the cases that fall within the ODD ranges but face hazards that the system is not designed to cope with (eg. when the system detects that the accuracy of a sensor measurement is lower than specified), or for cases that fall outside the ODD range (eg. when the vehicle enters a road type in which the system is not intended to work).

Triggering events and determination of safety countermeasures

Triggering events, defined as events that cause a risk to take place, are accounted for in this step. For hazards that have been judged unacceptable, the triggering events are analyzed under vehicle control categories, including traffic disturbance, recognition limitations, and vehicle disturbance sub-categories.

Traffic disturbance relates to traffic scenarios that may lead to a hazard as a combination of "road geometry", "ego-vehicle behaviour", and "surrounding vehicle location and motion". In order to handle a large amount of possible traffic disturbances, a well structured catalogue of foreseeable scenarios is jointly built by AD vehicle developers and traffic safety experts. The following sections in this paper elaborate in detail on the construction of such catalogues.

Recognition limitations refer to conditions in which the sensor system fails to correctly recognize hazard factors. Examples include part mounting conditions (e.g. unsteadiness related to sensor mounting or manufacturing variability), environmental conditions (e.g. sensor cloudiness, dirt, light, etc), or vehicle conditions (e.g. vehicle inclination due to uneven loading that modifies sensor orientation, or vehicle state due to sensor shielding with external attachments such as bicycle racks).

Vehicle disturbance relates to situations in which, recognition and vehicle control command works correctly, but the vehicle fails to follow the control command. These may include vehicle conditions (e.g. total weight, weight distribution, mechanical functions) and driving environment including aspects that may affect vehicle dynamics (e.g. road surface irregularities and inclination, road friction, wind).

The safety countermeasures that will be applied and the systems and features that will intervene to avoid or mitigate the identified risk need to be decided for the triggering events that have been judged to require intervention. In addition, after

confirming that the intervention is valid for the triggering event, the necessary functions may be either improved or newly developed according to the definition of systems and functions, and the system shall be updated accordingly.

Strategies for verification and validation

The strategies to validate and verify the system and to secure its safety are defined at this point. These strategies combine intensive virtual testing, with comparatively limited amount of physical tests in proving grounds and real-traffic environments.

The verification sub-process shall check the mathematical and physical correctness of the systems and functions developed and the safety countermeasures applied. It shall also confirm that all the safety specifications and requirements from the perspective of sufficiency of sensor-, algorithm- and actuator-related countermeasures are fulfilled.

The validation sub-process confirms that the systems and components including the safety countermeasures applied do not lead to an unreasonable risk for the traffic participants, and that the validation target previously defined is achieved, therefore demonstrating safety of the AD System.

Release decision

The release decision sub-process confirms that the safety of the AD system can be explained and that the remaining risk (if any) falls within an acceptable tolerance by reviewing whether adequate actions were implemented according to the results of the safety assurance process. Finally, based on the review results, it is decided whether the release of the system is acceptable or not.

Social contextualization of the engineering framework

The corresponding authorities in different regions are releasing safety guidelines. For example, the Japanese government recently released a technical safety guideline for AD systems, which reads ‘Automated vehicle systems, under their Operational Design Domain (ODD), shall not cause any traffic accidents resulting in injury or death, that are rationally foreseeable and preventable’ [1]. By contextualizing the AD systems safety assurance engineering framework proposed (Figure 1) with respect to governmental safety guidelines proposed by authorities, it is possible to develop engineering workframe that covers both social acceptance and technical aspects of the AD vehicles.

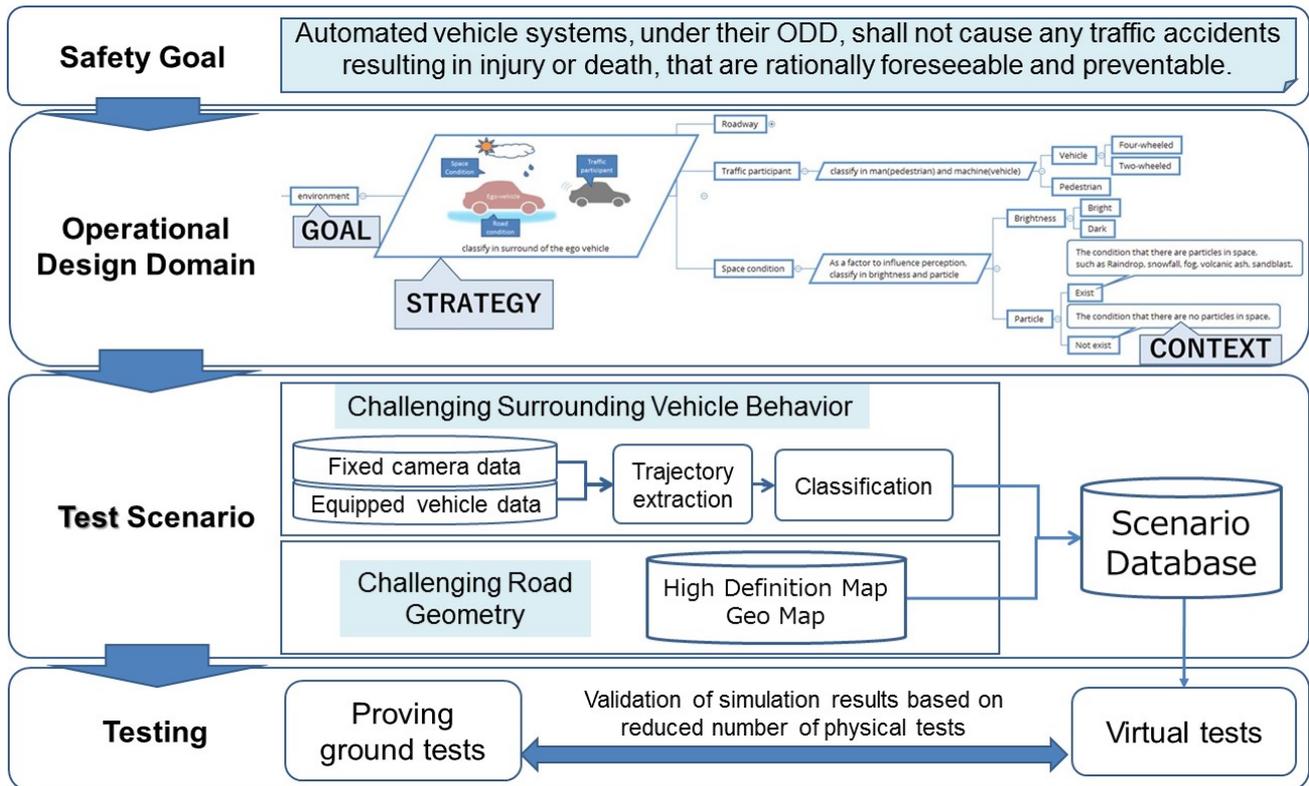


Figure 2 Top-down approach for social contextualization of the engineering framework for AD safety assurance

A scheme that illustrates such contextualization is shown in Figure 2. The scheme follows a top-down approach in which the ODD is defined considering the top safety goal, and test scenarios and validation strategies are developed under the same framework based on real-world data.

In order for AD test scenarios to be able to address the safety guidelines by the Japanese government, technical definitions for foreseeability and preventability becomes necessary. Foreseeable conditions are described as technically possible scenarios with quantitative parameter ranges. Preventable conditions are described as avoidable scenarios by means of technical intervention. The inter-relation between foreseeability and preventability is illustrated in Figure 3. The focus of the scenario catalogue development in the current paper focuses on foreseeable and preventable scenarios according to the figure. It is noted at this point that preventing crashes in situations that involved other vehicles that committed traffic rule violations or extreme maneuvers is particularly challenging, and strategies complementary to vehicle engineering may be required (e.g. crashes involving vehicles running in the wrong direction at very high speeds).

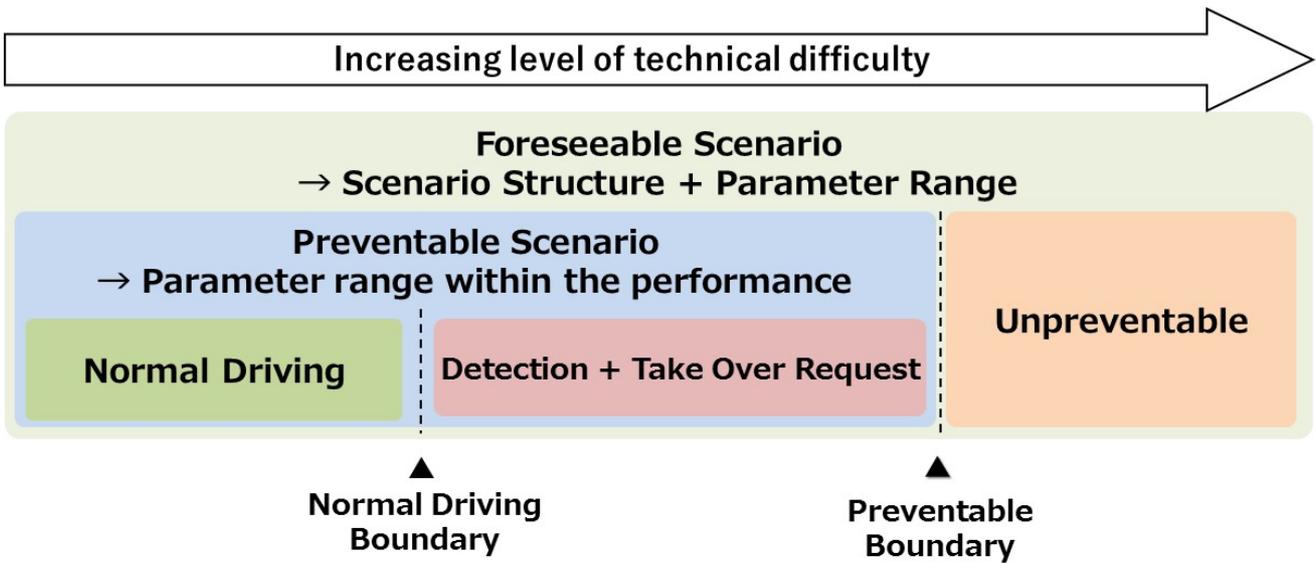


Figure 3. Foreseeable and preventable scenarios and their inter-relations

Approach to AD safety test scenarios

Figure 4 summarizes the technical approach to develop test scenarios including quantified parameter ranges for AD vehicle safety assurance. First, scenarios are structured in order to cover holistic root causes from the point of view of the physics of the AD systems.

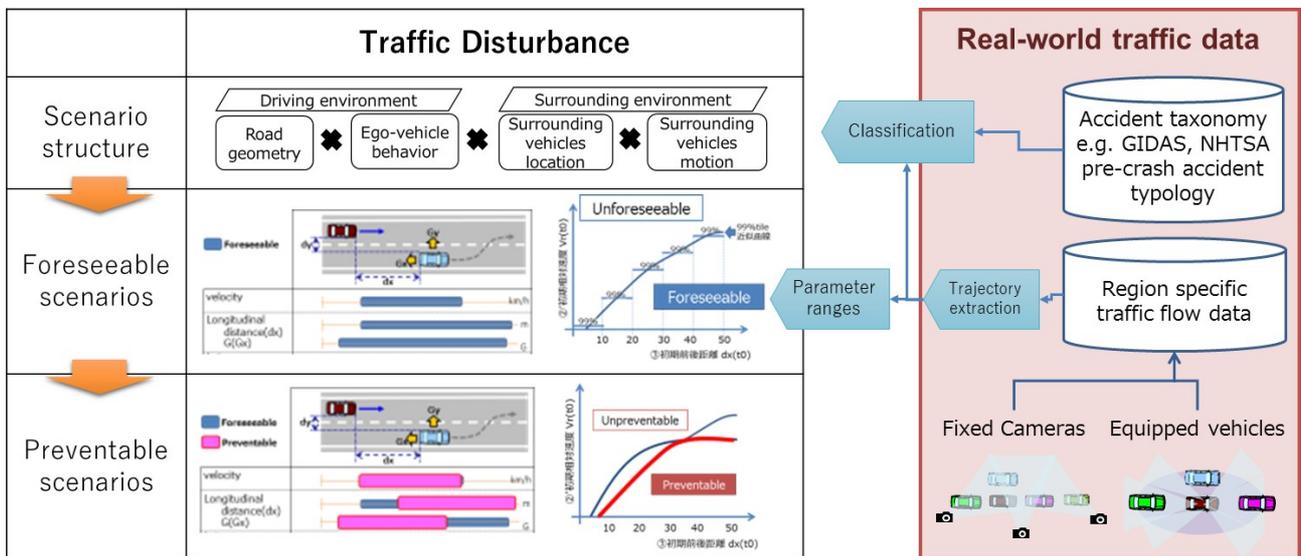


Figure 4 Approach to test scenarios for AD safety assurance

For each structured scenario, parameters and their ranges for foreseeable conditions are defined based on real-world traffic monitoring data. Among the foreseeable conditions, the ranges are narrowed down to those that correspond with

preventable conditions. Both the evaluation of the completeness of the structured scenarios as well as the steps to define ranges for foreseeable and preventable conditions are developed based on real-world traffic monitoring and accident data. The completeness of the structured scenarios is conducted based on accident data that contains information on pre-crash conditions. Traffic monitoring data is utilized to define the parameter ranges representative of foreseeable scenarios. Detailed descriptions of the methodologies to structure and to generate test scenarios for AD safety assurance purposes follow.

STRUCTURE OF AD VEHICLE TEST SCENARIOS FOR SAFETY ASSURANCE

This chapter provides a description and practical guidance on the development of test scenario structure for AD safety assurance purposes. The scenario structure aims to cover all foreseeable root causes of traffic accidents that may possibly caused by AD vehicles. The applicability of the methodology proposed is limited, at this moment, to motorways.

Traffic scenario structure systematization

A scheme of the traffic scenario structure developed is presented in Figure 5. By analyzing and classifying traffic disturbances systematically and considering the driving environment and the surrounding environment, lists of traffic scenarios can be developed. Driving environment comprises Road geometry and Ego-vehicle behavior. Surrounding environment comprises surrounding vehicles location, and surrounding vehicles motion.

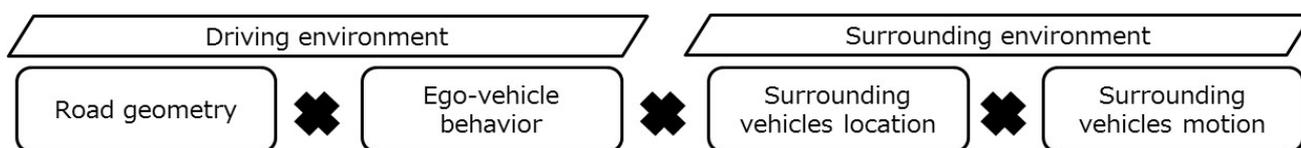


Figure 5. Structure for traffic scenarios

Road geometry classification and parameterization: Basic road geometry structure is defined according to the Japanese road structure ordinance [7], which provides technical standards for the development of roads in the country. In addition to road geometry related information such as cross sections, horizontal sections, sight distances, or speed changes, the ordinance includes parameters to ensure traffic safety and traffic flow smoothness.

Using the ordinance as a basis, road geometry sectors are categorized into Main road, Merging lane, Departure lane, and Ramp (Figure 6). Following this basic scheme, the corresponding critical road parameters for each of these components and for each scenario are defined based on expertise. As a result, critical parameters for traffic disturbances including the number of lanes, lane width, speed change lane and vertical gradients are proposed. Although the ordinance is generic, minor adaptations of the road structure may be required to become applicable to regions outside Japan.

Ego-vehicle behavior classification and parameterization: A lane change maneuver from a contiguous line or from a merging lane may differ in road geometry category, but share the ego-vehicle behavior. The same holds for lane keeping. Therefore, possible ego-vehicle behaviors are categorized in Lane Keep and Lane Change categories. This simple categorization of vehicle behaviours, in combination with the road geometry information provided previously, lead to a number of combinations (Figure 6).

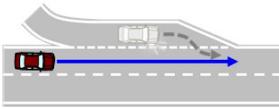
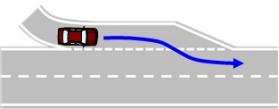
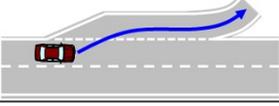
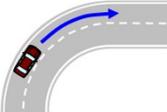
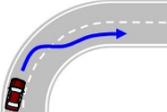
		Ego-vehicle behavior	
		Lane keep	Lane change
Road geometry	Main road	 Free driving Following	 Lane change Overtaking
	Merging lane	 Being merged	 Merging
	Departure lane		 Departure
	Ramp	 Free driving Following	 Lane change Overtaking

Figure 6. Road geometry and ego-vehicle behaviour parameters

Surrounding vehicle location classification and parameterization: The location of surrounding vehicles to be considered in the safety evaluation is defined according to adjacent locations in eight directions around the ego-vehicle, as these may invade the ego-vehicle’s trajectory. In addition, when there is a large speed difference between the leading vehicle and the vehicle ahead of the leading vehicle, the former may cut out to avoid a collision. If this cut out occurs suddenly, the oncoming ego-vehicle may also need to intervene for crash avoidance. To account for this possible scenarios, the location of the vehicles ahead of the leading vehicle is also considered and is noted as ‘+1’ (Figure 7, left).

Surrounding vehicle motion classification and parameterization: Possible motion of the surrounding vehicles is categorized in five groups: cut-in, cut-out, acceleration, deceleration, and synchronization. From the perspective of safety evaluation, it is possible to minimize the number of evaluation tests by focusing on the motion of the target participants that may obstruct the ego-vehicle's behavior (Figure 7, right chart).

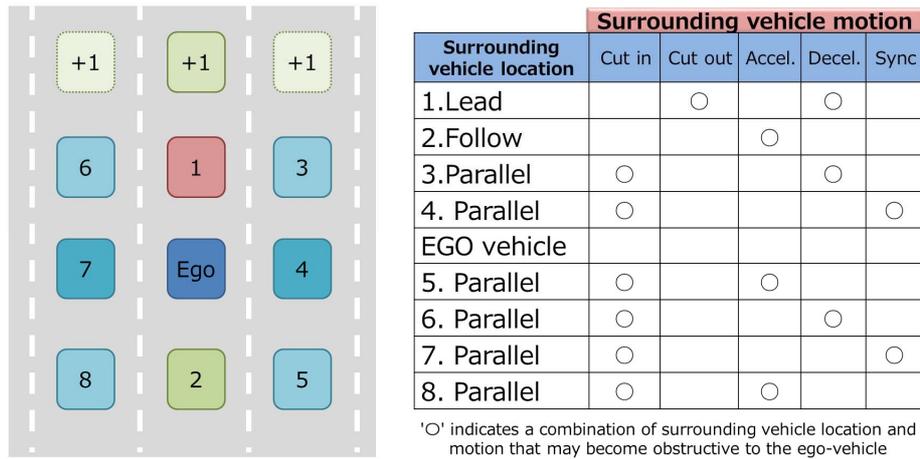


Figure 7. Surrounding vehicles locations (left) and cases that may become obstructive to the ego-vehicle (right)

Resulting structure for Autonomous Driving vehicle scenario

As a result of the systematization process described, a methodology to structure scenarios as a combination of road geometry, ego-vehicle behavior, and surrounding vehicles location and motion is proposed. Following this structure, a matrix containing 32 test scenarios was developed based on expert discussions (Figure 8). The completeness of this matrix may be evaluated based on comparative accident taxonomy. The critical parameters and ranges for each of the scenarios can be defined and quantified based on traffic monitoring data.

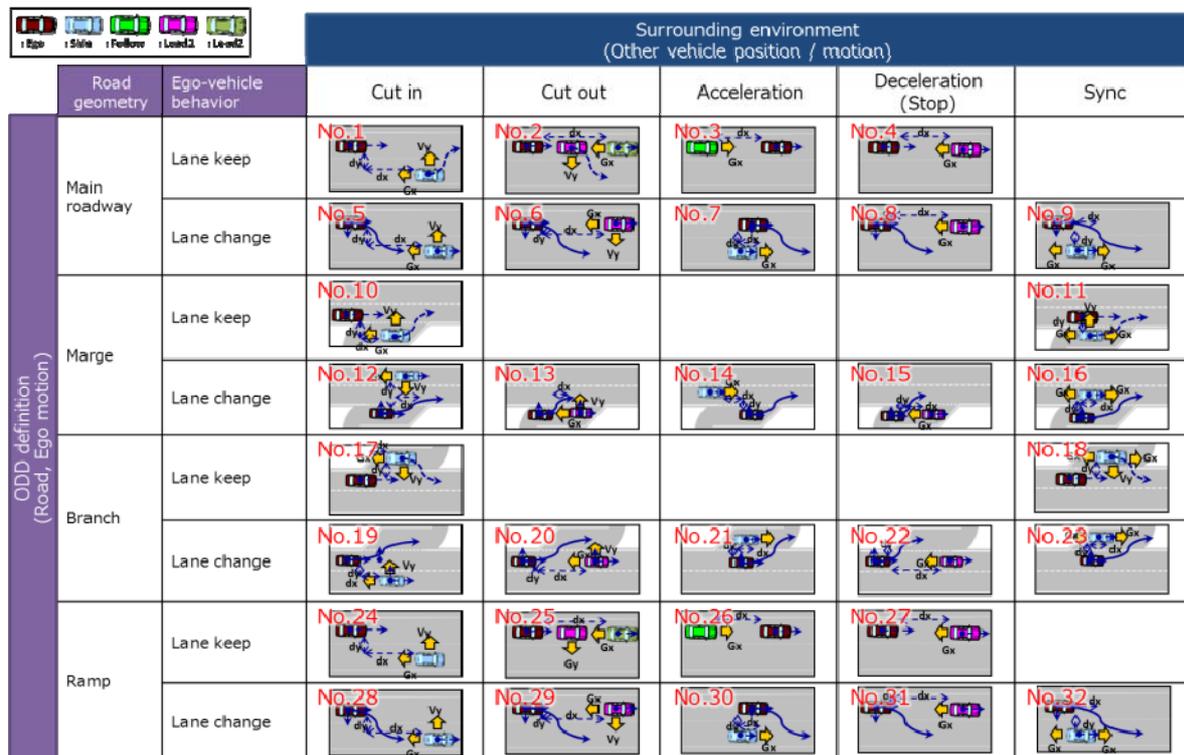


Figure 8. Traffic scenario matrix and corresponding parameters

Scenario matrix completeness evaluation based on accident data

The completeness of the scenario matrix proposed (Figure 8) may be evaluated by comparing its ability to cover accidents as reported in, for example, German in-depth accident study (GIDAS) database [8]. The underlying assumption of such comparison is that the accidents contained and classified in GIDAS represent all foreseeable scenarios in the German traffic environment.

GIDAS classifies traffic accidents according to predefined codes related to crash characteristics. Through a comparative taxonomy analysis between the GIDAS codes and the matrix of scenarios proposed (Figure 8), a relationship is established.

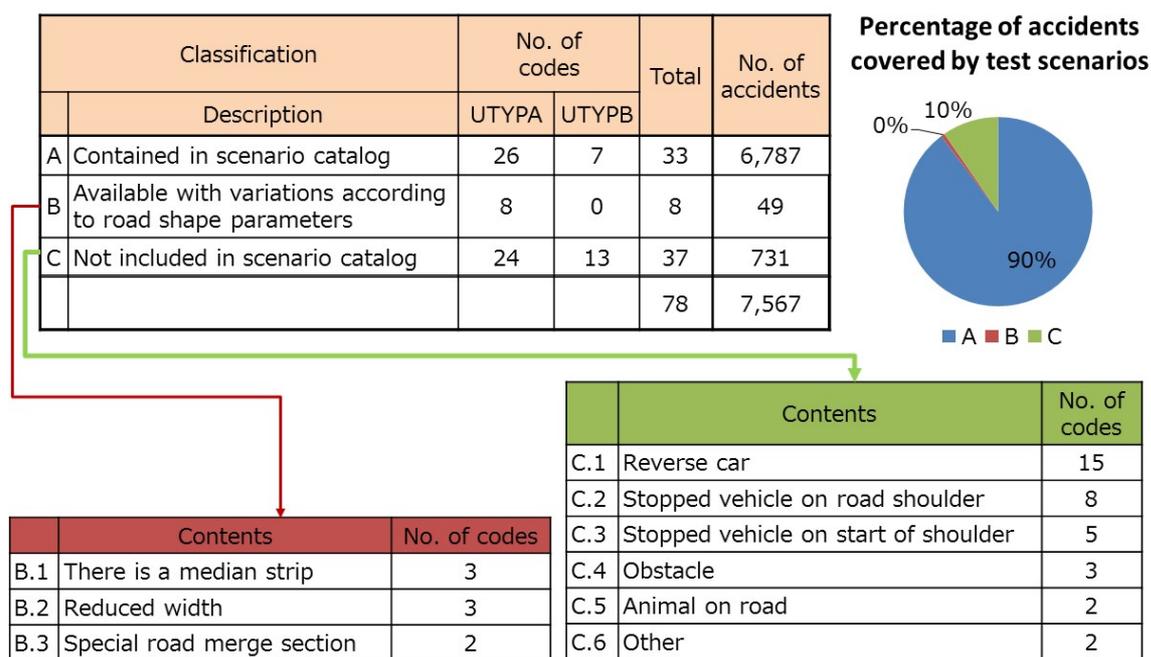


Figure 9. Scenario matrix evaluation based on GIDAS accident taxonomy

The upper left table in Figure 9 shows GIDAS accident code counts categorized based on the comparative taxonomy analysis. Categories A, B and C represent together 78 codes and 7,567 accidents in motorways contained in the dataset analyzed. From these accidents, the comparative analysis shows that 33 codes and 6,787 accidents can be analyzed under the proposed matrix of scenarios (Figure 8), suggesting that the proposed matrix may potentially address nearly 90% of the motorway accidents reported in German motorways.

Category B comprises a total of 8 codes and 49 accidents (0.006% of all motorway accidents) that are related with road characteristics not covered by the matrix of scenarios. It is noted that the road geometry data applied to develop the list of scenarios was based on the Japan road structure ordinance [7], which may not cover some characteristics of German motorways. In order to provide coverage of the 8 remaining codes, adaptations of the proposed methodology to the German road characteristics may be required.

Category C comprises 37 codes and 731 accidents (10% of the total) that are not covered by the safety methodology proposed. Further analysis of the codes reveals that three code sub-categories (adding up to 28 codes) involved illegal maneuvers such as reversing in the motorway or illegal parking on the motorway shoulder (C1 to C3). The remaining 7 codes include obstacles or animals on the road and other unknowns (C4 to C6). The preventability of the crashes in this category (C) remains challenging for AD engineering intervention and call for complementary approaches that also involve, for example, rule enforcement.

GENERATION AND FORMATION OF AD VEHICLE TEST SCENARIOS FOR SAFETY ASSURANCE

This chapter provides a description and practical guidance on the process to generate test scenarios for AD vehicle safety evaluation by means of application of real-traffic data. The tests scenario structure is based on the previously proposed and the focus is on defining foreseeable scenarios including quantitative critical parameter ranges.

Road geometry parameter settings based real-world map data

To determine road geometry parameters, baseline road geometry critical parameters were assigned the most demanding values based on the Japan road structure ordinance, according to

Table 1.

Table 1. Baseline road geometry parameters from the road structure ordinance of Japan

Road parameters			Demanding value		
Cross section	Number of lanes		3		
	Width (m)		3.25		
	Center zone	Median (m)	1.25		
		Shoulder (m)	0.25		
	Side strip (m)		1.25		
Linear gradient (%)		2.5			
Linear	Velocity (km/h)		120	100	
	Horizontal alignment	Curve section	Radius (m)	570	380
			Transition section (m)	100	85
			Superelevation (%)	10	
		Speed change lane	Type	Direct	Parallel
			Direction	Deceleration	Acceleration
			Taper length (m)	70	60
			Pre-determined length (m)	110	220
	Vertical Alignment	Vertical Curve	Radius curve convex (m)	11000	6500
			Radius curve concave (m)	4000	3000
			Length (m)	100	85
		Vertical gradient (%)		5	6
Sight distance	Velocity (km/h)		120	100	
	Sight distance (m)		210	160	

In practice, real road geometries may not strictly comply with the road structure ordinance due to different reasons (e.g. merging lane length may be shorter than stipulated by the road ordinance due to limited construction space in crowded cities). Therefore, the previously defined baseline values for road geometry parameters need to be updated to reflect the actual strict road geometry conditions. With this purpose, dynamic map data are incorporated into the process. For example, a search of motorway characteristics in the region of Tokyo for “legal speed limit of 100 km/h” and “minimum curve section radius lower than 100 m” (Figure 10, left) shows numerous locations (resulting blue spots on the right of Figure 10). This exemplary search indicates that the baseline parameter values for road geometry (

Table 1) need to be updated from 380 m to no more than 100 m, to better reflect the actual road demanding parameter for curve radius in the region of Tokyo.

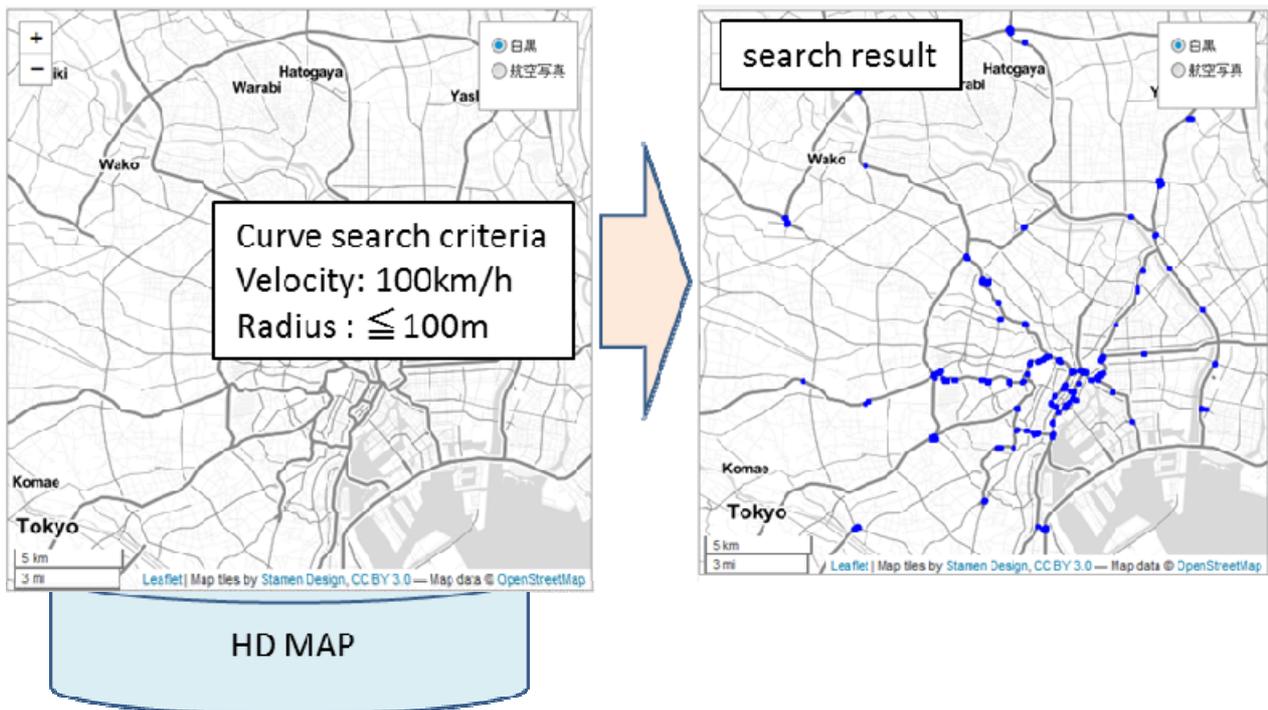


Figure 10. Data extraction utilizing dynamic map data

Surrounding vehicle foreseeable parameter ranges based on real-world traffic data

The process to derive critical parameter ranges in a cut-in test scenario (No.1 in Figure 8) is described in Figure 11. The basic idea is to define a list of surrounding vehicle motion critical parameters, and a simplistic model of the evolution of these parameters in time. In parallel, collection of real traffic data with stationary cameras and vehicles equipped with data collection devices is conducted, and correlation analysis between the simple surrounding vehicle behavior model and the corresponding field data measurements is conducted. Thereafter, parametric simulation studies are conducted to develop statistical distributions of a wide range of possible combinations of parameters. Based on these distributions, the parameter ranges that correspond with foreseeable scenarios are defined.

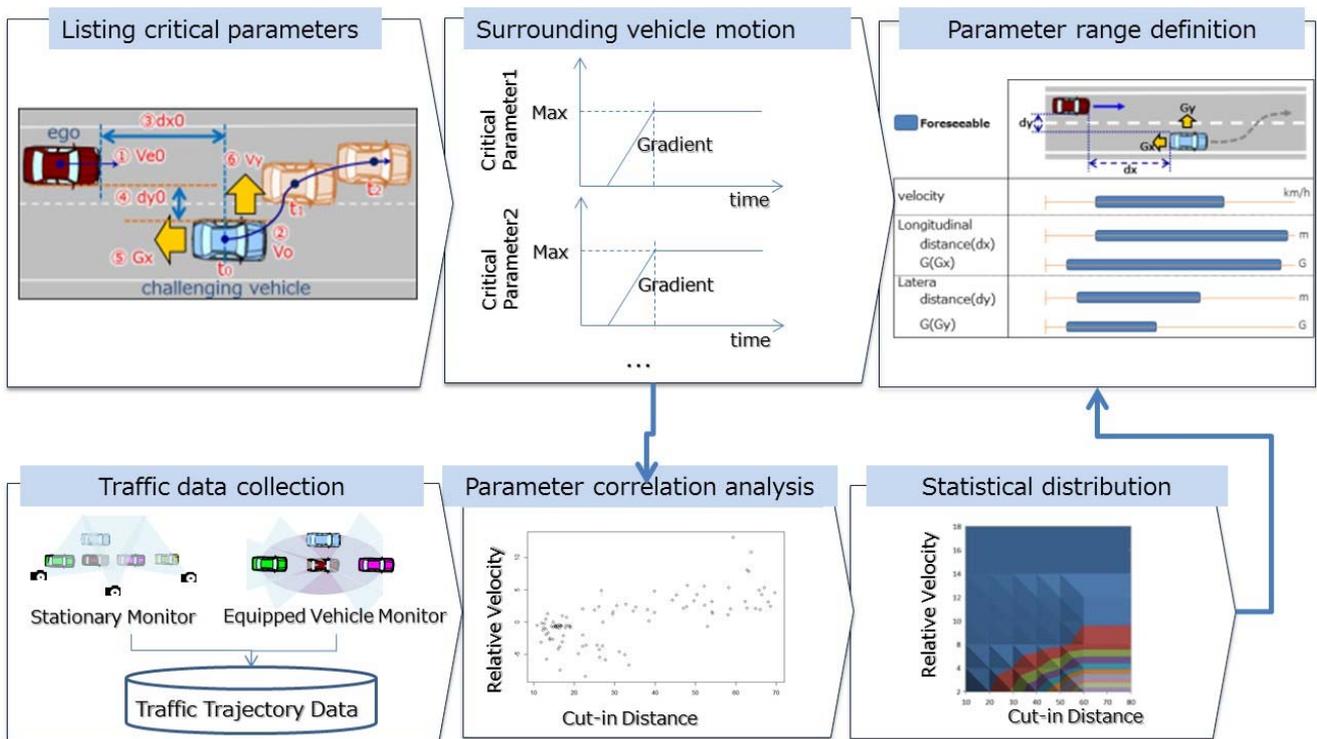


Figure 11. Process to extract surrounding vehicles motion to determine foreseeable scenario parameter ranges

Critical parameters and ranges: The same cut-in scenario is used to further elaborate on the process to define critical parameter ranges. Similar processes are applied to extract the critical parameters for other scenario.

Two main aspects regarding the process to define critical parameter ranges are considered. The first one concerns the definition of the start and end time for the test scenario based on trajectory data (Figure 12, left). In this example, the start time of the scenario is defined by first identifying the lateral velocity of the challenging vehicle (V_y) at the timing (t_1) in which the relative lateral distance between both vehicles (dy) becomes zero, and then by tracking back the lateral velocity (V_y) until the point in which it becomes zero. The end time is defined as the time in which the difference between the longitudinal velocities of the challenging and the ego-vehicle ($V_o - V_e$) becomes zero.

The second aspect regarding the process concerns to the definition of critical parameter ranges from the recorded trajectories. These ranges are defined by extracting cumulative ratios for large amounts of data cases (Figure 12, right). In the example, the cumulative ratio of lateral velocity (V_y) is obtained for different initial longitudinal distances (dx).

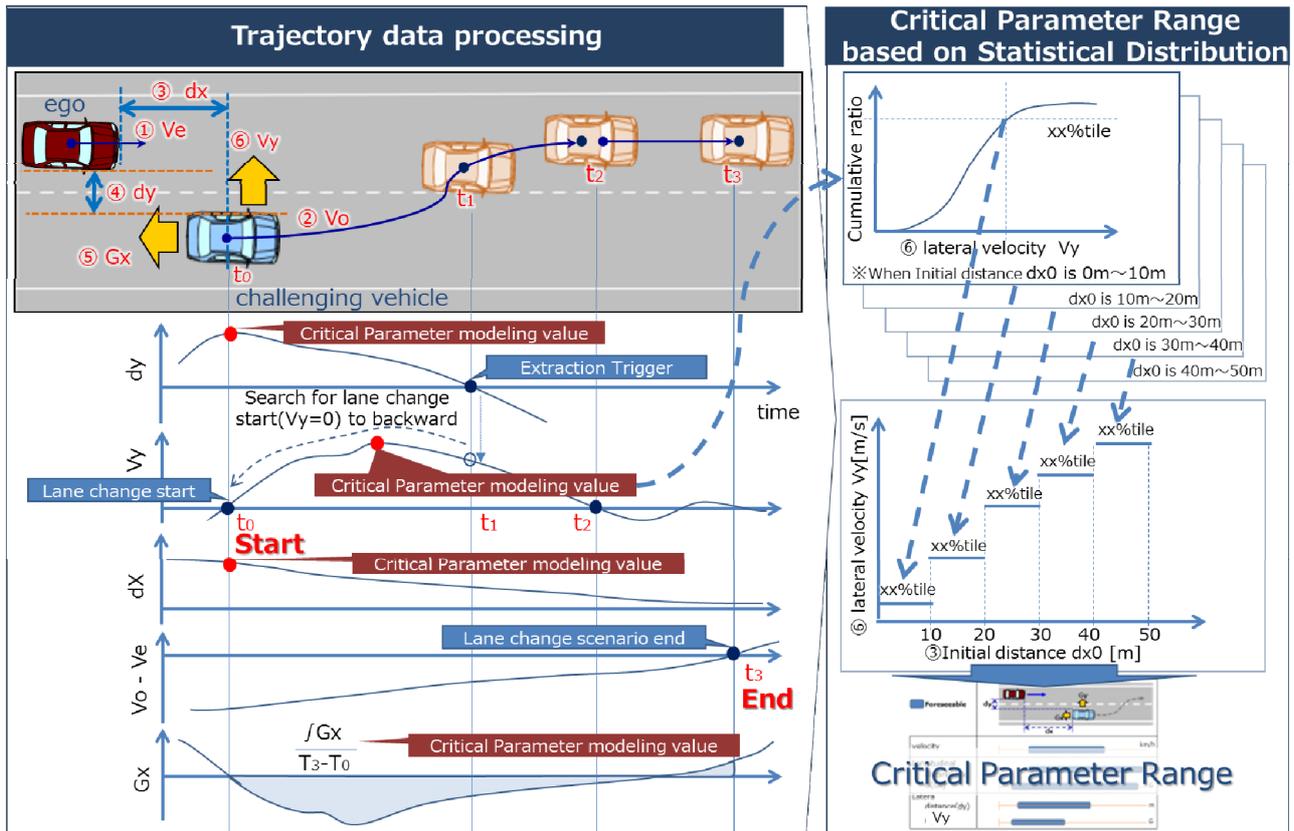


Figure 12. Definition of scenario start and end based on trajectory data processing (left) and critical parameter ranges definition based on cumulative ratios (right)

Catalogue of functional scenarios: By applying the same methodology to each of the scenarios in Figure 8, sets of scenario-dependent foreseeable parameter ranges are developed. This provides a complete catalogue of functional scenarios that can be applied for AD safety evaluation. The format of these scenarios is similar to those in the matrix in Figure 8, but includes lists of critical parameter and corresponding quantified ranges for each of the scenarios proposed.

Scenario database

The outcome of the overall process is envisioned as a database that provides the outcome of tests, but that also enables bidirectional traceability of the entire between the raw traffic monitoring data and the critical parameter ranges that define foreseeable conditions (Figure 13). Efforts to harmonize the development, maintenance, and accessibility to such database could lead to a common international database to support the a safe and global deployment of AD vehicles.

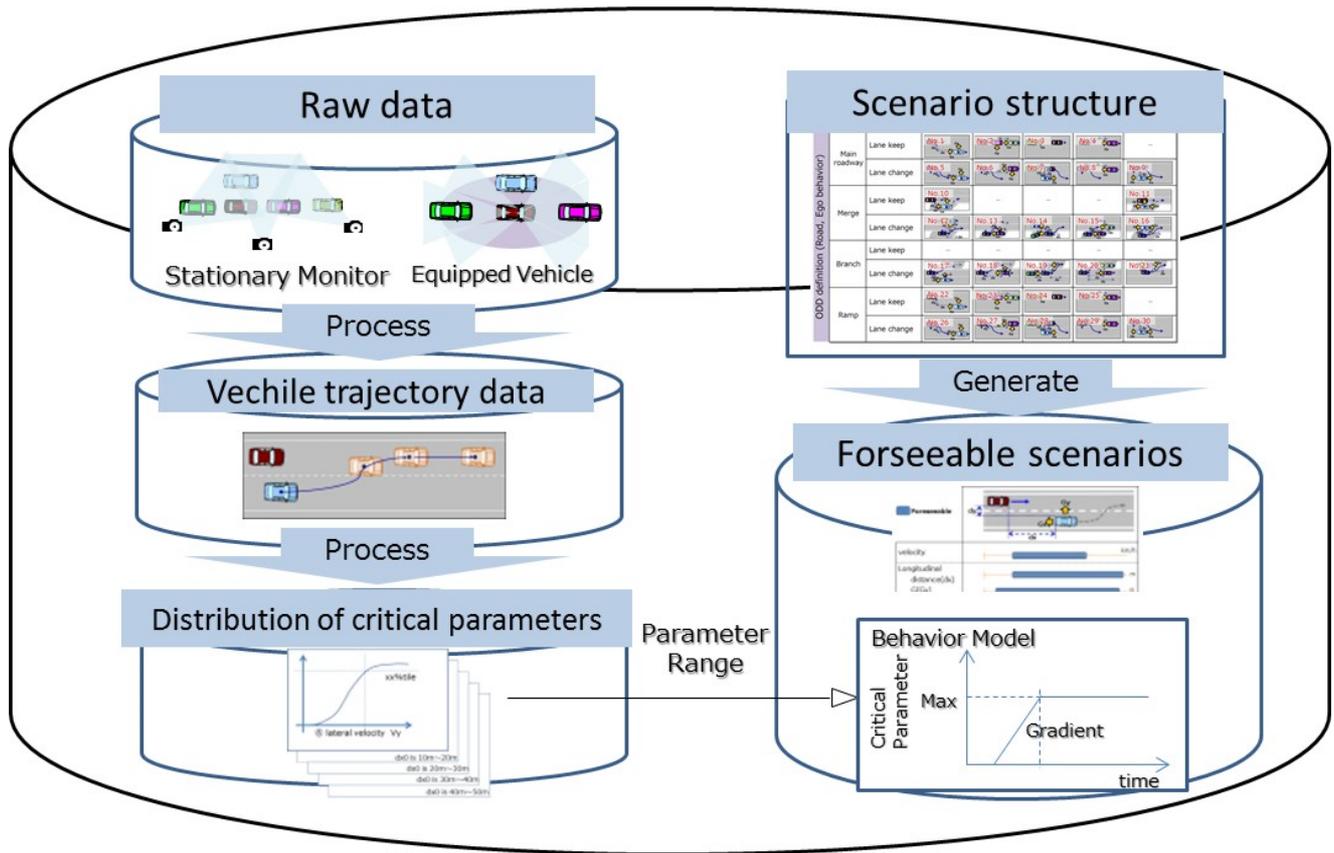


Figure 13 Database scheme with tracability from raw data to critical parameter Range

CONCLUSION

A safety assurance process for AD vehicles has been developed by JAMA and JARI under the auspice of the Japanese government and is hereby proposed. The proposal provides guidance on the overall safety assurance engineering process for Level 3+ AD systems under non-failure conditions on motorways, and on the methodologies to develop test scenarios and related criteria from real traffic monitoring data.

ACKNOWLEDGMENT

The results from a project financed by the Ministry of Economy, Trade and Industry of Japan have been utilized in this paper.

REFERENCES

1. Japan Traffic Agency of the Ministry of Land Infrastructure and Transportation. Guideline regarding safety technology for Automated Vehicles in Japan. September; 2018. Available from: <https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-34.pdf>.
2. NHTSA. Automated Driving Systems 2.0: A Vision for Safety. September; 2017. Available from: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.
3. ISO. 26262: Road vehicles-Functional safety. Geneva, Switzerland: International Organization for Standardization; 2018.
4. Wachenfeld W, Winner H. The release of autonomous vehicles. *Autonomous Driving*: Springer; 2016. p. 425-49.
5. Themann P, Raudszus D, Zlocki A, Eckstein L. Holistic Assessment of Connected Mobility and Automated Driving. *ATZ worldwide*. 2016;118(1):26-31.
6. Kelly T, Weaver R, editors. The goal structuring notation—a safety argument notation. *Proceedings of the dependable systems and networks 2004 workshop on assurance cases*; 2004: Citeseer.
7. Association JR. Explanation and application of road structure ordinance. Maruzen; 2004.
8. Otte D, Krettek C, Brunner H, Zwipp H, editors. Scientific approach and methodology of a new in-depth investigation study in germany called gidas. *Proceedings: International Technical Conference on the Enhanced Safety of Vehicles*; 2003: National Highway Traffic Safety Administration.