Paper ID # AP-TP2329

A Safety Assurance Process for Automated Driving Systems

Jacobo Antona-Makoshi[1*], Nobuyuki Uchida[1], Eiichi Kitahara[2, 3] , Koichiro Ozawa[2, 4] , Satoshi Taniguchi[2, 4,]

1. Japan Automobile Research Institute, ajacobo@jari.or.jp, Japan
2. Japan Automobile Manufacturers Association, Japan
3. Nissan Motor Co., e-kitahara@mail.nissan.co.jp, Japan
4. Honda R&D Co., koichiro_ozawa@n.t.rd.honda.co.jp, Japan
5. Toyota Motor Co., satoshi_taniguchi_ad@mail.toyota.co.jp, Japan

Abstract

In order to introduce Automated 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 SAKURA project (Safery Assurance KUdos for Relieable Autonomous vehicles), 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 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 safety assurance process for SAE Level 3+ automation in motorway environments has been achieved and the results are hereby outlined. The process can be used as a guidance to continue developing the systems and related standards towards a safer Automated Driving society.

Keywords: Automated Driving, Safety Assurance Process, Standard

Background and aim

The Traffic Agency of the Ministry of Land, Infrastructure, Transportation and Tourism of Japan [1], the US National Highway Traffic Safety Administration [2], the UN Economic Commission for Europe [3], and the UN World Forum for Harmonization of Vehicle Regulations (WP29) [4] are gradually releasing technical safety guidelines to support the development of regulatory and standardization work to ensure safety of Automated Driving (AD) systems.

A functional safety standard ISO26262:2011 [5] exists for failure and design errors. The 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 a specific coverage of SAE Level 2 AD systems. However, a safety assurance process for non-failure conditions that considers SAE Level 3 and higher AD systems and their performance limitations has not yet been established.

This technical paper aims to propose an AD system safety assurance process for non-failure conditions that considers the system's performance limitations. The scope of the report comprises SAE level 3 and higher AD systems in motorways [1].

Methodology

In the current paper, a complete AD systems safety assurance engineering management process from product planning to release decision has been outlined. Throughout the paper, we incorporated terms and definitions according to DIN/SAE [6] and to ISO26262 [5].

Overall safety assurance process

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 advanced driver assistance systems (ADAS) and AD systems [7]. 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.

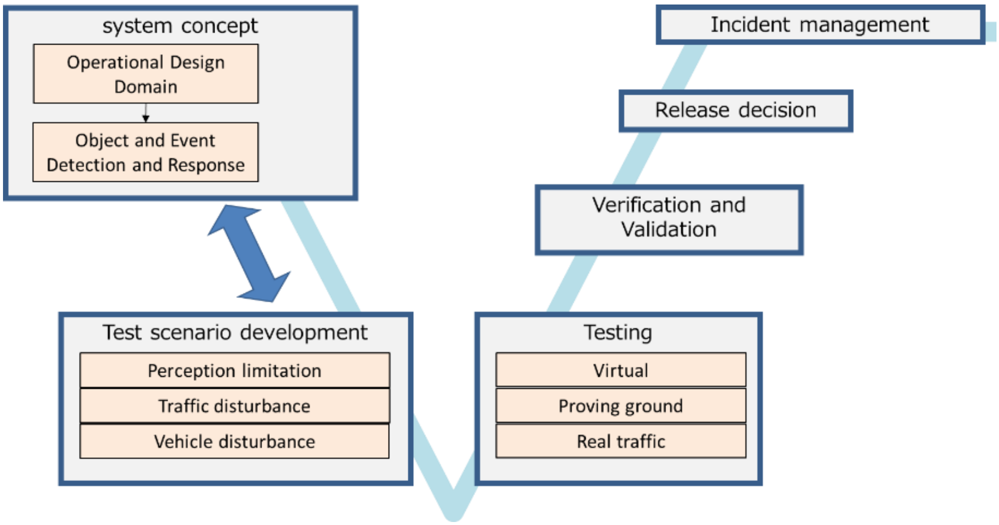

Figure 1. Overall schematic of the safety assurance process

Operational Design Domain

The complete safety assurance process is to be conducted within well-defined and pre-determined operational boundaries. Therefore, upon the collection of existing information concerning the purpose and specification of different AD systems and functions, the Operational Design Domain (ODD) is defined at the initial stage. ODD contents shall include at least information on roadway types, location within the road, vehicle speed ranges and environmental conditions.

Scenario development

Figure 2 summarizes the test scenario development process by using real-world data. The definitions for functional, logical, and concrete scenarios are adopted from DIN/SAE [6]. The structure for functional scenarios is developed following a systematic combinatorial approach that defines all possible elements of a scenario and their combinations, as well as be described within different layers. Logical scenarios are defined by combining the structuralized functional scenarios with parameter ranges which can be defined by means of a data-driven approach that systematically extracts and processes vehicle trajectories from traffic monitoring data. Concrete scenarios are defined from the logical scenarios, by means of a parameter search engine, e.g. sampling methodologies or stochastic algorithms to select concrete values from the parameter distribution.

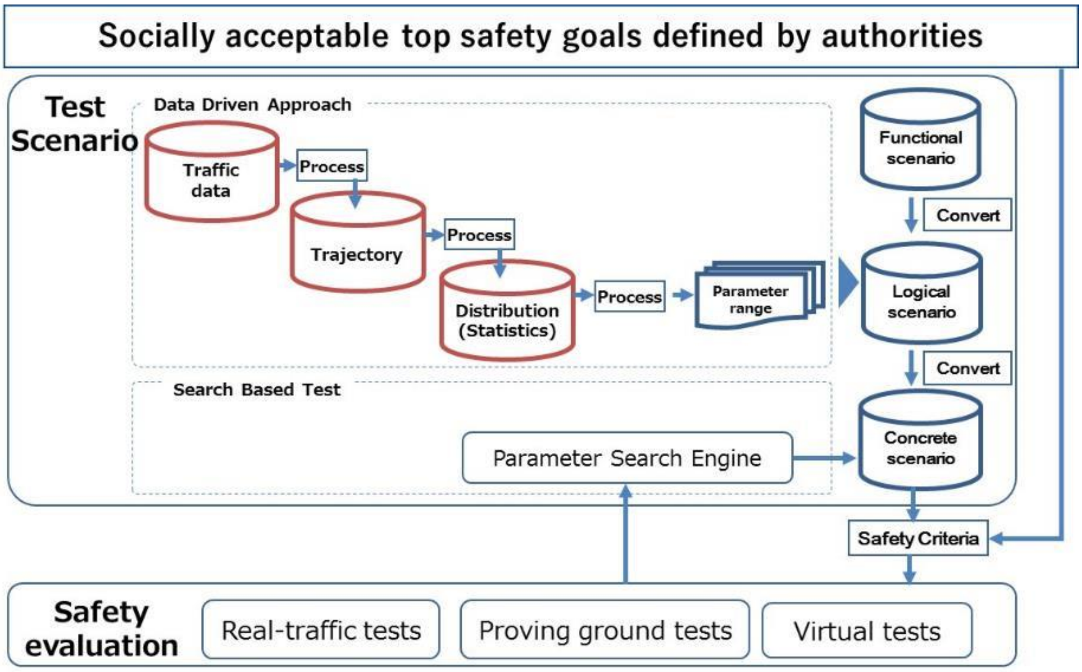

Figure 2. Test scenario development using real world data

Scenario structure

The ODD definition shall 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 [6].

Due to the large amount of information required to determine all possible scenarios of interest and the identification of automation risks, standardized ontology-based and graphical argumentation techniques commonly applied to document and present safety goals and arguments in a clearer format than plain text (e.g. Goal Structuring Notation [8]), may be applied to organize the ODD and the detailed scenario related information.

Within the AD system safety analysis, possible disturbances to three categories related to the physics of the system are accounted for developing the scenarios: perception disturbance, traffic disturbance, and vehicle disturbance (Figure 3). By following this approach, it is possible to conduct the AD system safety analysis that covers holistic safety-relevant root causes from the view point of the physics of the system.

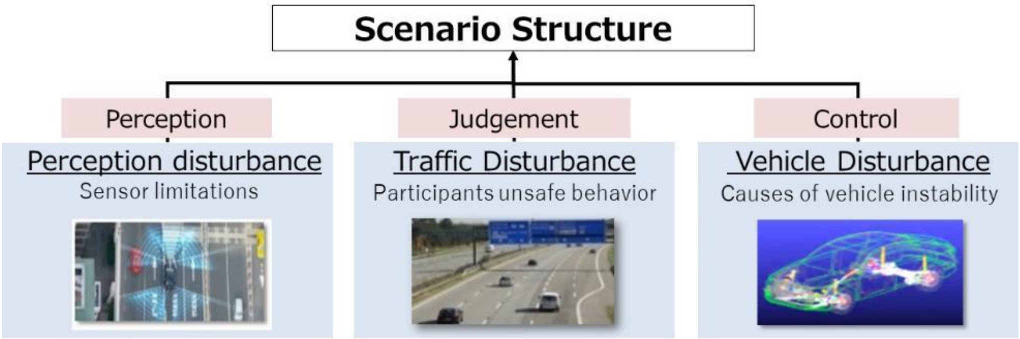

Figure 3. Test scenario development from inside of the AD system

Perception disturbance refers to conditions in which the sensor system fails to correctly recognize a hazard due to sensor malfunctioning, sensor blind spots or misinterpretation. Examples include part mounting (e.g. unsteadiness related to sensor mounting or manufacturing variability), environmental (e.g. sensor cloudiness, dirt, light, etc.), or vehicle conditions (e.g. vehicle inclination due to uneven loading that modifies sensor orientation, or sensor shielding with external attachments such as bicycle racks).

Traffic disturbance relates to traffic conditions that may lead to a hazard as a combination of road geometry factors (e.g. branches or ramps in highways), ego-vehicle behavior (e.g. lane change maneuver), and surrounding vehicle location and motion (e.g. cut-in from a near side vehicle).

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

Data driven approach

For each of the three scenario structure categories, logical scenarios including relevant parameters and their ranges are defined based on real-world traffic monitoring data (Figure 4). The completeness of the structured scenarios is conducted by establishing a taxonomy based comparison between accident data that contains information on pre-crash conditions and the scenarios. Traffic monitoring data is utilized to define the parameter ranges representative from real traffic.

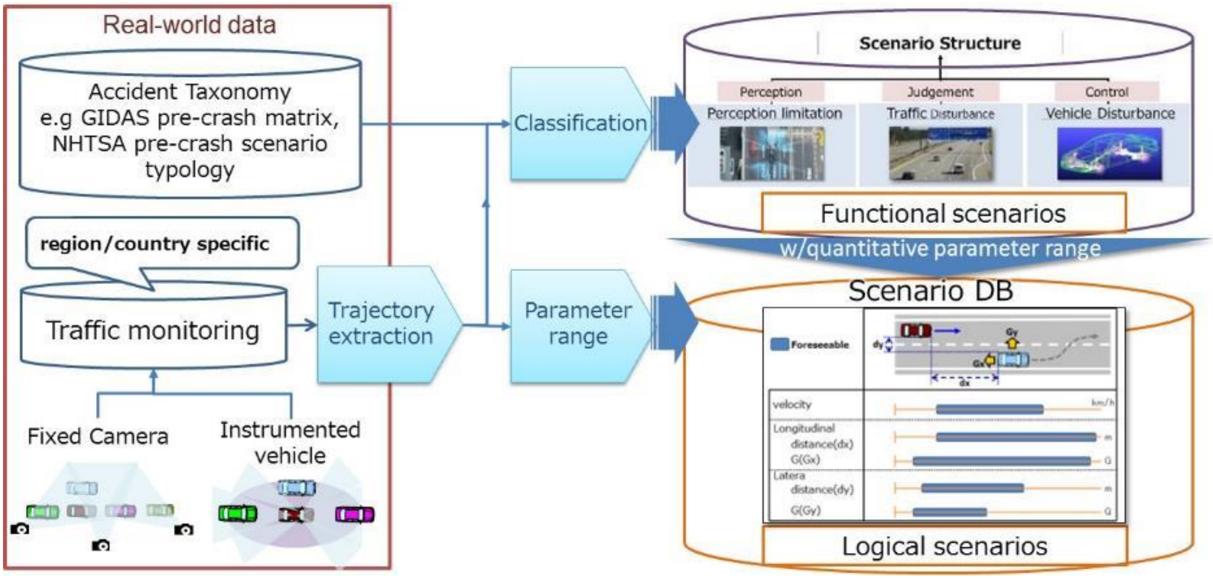

Figure 4. Field data application to develop a database of scenarios

Testing

Based on the developed scenarios, safety evaluation is conducted by combining intensive virtual testing, with comparatively limited amount of physical tests in proving grounds and real-traffic environments.

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 on proving grounds and under real-traffic environments.

The verification sub-process shall check the mathematical and physical correctness of the systems, developed functions and the applied safety countermeasures. 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 applied safety countermeasures, do not lead to an unreasonable risk for all traffic participants, and that the validation target previously defined has been 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 using a Behavioural Safety Assessment (BSA). BSA focuses on the assessment of the AD in individual test-cases. Thereby, for each individual test-case different metrics are applied to confirm the AD compliances with pre-defined behavioural criteria at different stages. Finally, based on the review of the results, it is decided whether the release of the system is acceptable or not and incident management needs to be defined and deployed.

Conclusion

An AD system safety assurance process for non-failure conditions that considers the system's performance limitations is proposed with a main focus on SAE Level 3+ AD systems for motorways. The process can be used as a guidance to continue developing the systems and corresponding standards towards a safer AD society.

Acknowledgement

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

References

1. Japan (2018). Japan Traffic Agency of the Ministry of Land Infrastructure and Transportation. Guideline regarding safety technology for Automated Vehicles in Japan.
2. NHTSA (2017). Automated Driving Systems 2.0: A Vision for Safety.
3. EU (2019). "Guidelines on the exemption procedure for the EU approval of Automated Vehicles." Retrieved from: https://ec.europa.eu/docsroom/documents/34802?locale=en.
4. UN/WP29 (2019). "Framework document on automated/autonomous vehicles. Informal document WP.29-177-19." Retrieved from: https://www.unece.org/fileadmin/DAM/trans/.../WP29-177-19e.pdf.
5. ISO (2018). 26262: Road vehicles-Functional safety. International Organization for Standardization.
6. DIN/SAE (2019). DINSAE SPEC 91381: Terms and Definitions Related to Testing of Automated Vehicle Technologies.
7. Themann, P., et al. (2016). "Holistic Assessment of Connected Mobility and Automated Driving." *ATZ worldwide*, vol.118, pp.26-31.
8. Kelly, T. and R. Weaver (2004). The goal structuring notation–a safety argument notation. Proceedings of the dependable systems and networks 2004 workshop on assurance cases. Citeseer.