Safety Design of Steering Systems for Autonomous Driving

N. KAIHARA K. KIMURA A. ISHIHARA H. NAKAMURA

Fail-operational design is the key technology that ensures safety in case of autonomous driving system failure. In order to extract required issues for such fail-operational design, the steering system was developed as an example with reference to ISO 26262. In this activity, required issues and safety design case study for autonomous driving system have been obtained by applying ISO 26262, and the effectiveness of fail-operational design has been evaluated. This report summarizes the results relating to safety design for autonomous driving systems obtained through a project commissioned by the Ministry of Economy, Trade and Industry.

***Key Words**: autonomous driving, functional safety, ISO 26262, fail-operational, steering system*

1. Introduction

Currently, technological development relating to CASE (Connected, Autonomous, Shared & Services, Electric) is accelerating and the reduction of road accidents has been identified as one of the benefits obtainable through the realization of autonomous driving. This is because the normal principal driving authority would be the system, and there is expectation that the occurrence of accidents typically caused by humans due to so-called human error, etc., would be suppressed. However, there is concern regarding the risk of new types of accidents if this system (especially the electrical and electronic system) fails, because it would be difficult to continue autonomous driving. In other words, the establishment of safety design technology (fail-operational) that can ensure safety by continuing function in the event of an autonomous driving system failure is a key issue that must be addressed.

In response, Japan's Ministry of Economy, Trade and Industry (METI) planned a research on fail-operational corresponding to autonomous driving as one measure of the "Next Generation Advanced Driver Assistance System Research and Development and Demonstration Project" from FY2014 to FY2015, and the "Research and Development and Demonstration Project for the Social Implementation of Advanced Autonomous Driving Systems" from FY2016 to FY2018. As a project assigned to us from the Japan Automobile Research Institute (JARI), which was entrusted with this theme by METI, JTEKT researched and developed the steering system's safety design supporting autonomous driving. Based on ISO 26262:2011, which is the international standard for automotive functional safety, this project aims to clarify the issues of safety design/verification evaluation, indicate the "concepts and method examples" to realize these issues, and utilize as supporting data for "discussion of standards/criteria", "development in individual companies" and "demonstration projects".

This paper describes the results of the safety design of the autonomous driving system obtained in the project undertaken for METI.

2. Issues of Autonomous Driving Systems and the Countermeasures Thereof

In this section, we describe typical safety designs and challenges obtained from development in accordance with ISO 26262:2011, using the steering system of autonomous driving as an example. First, the development flow of Part. 3 to Part. 6 ISO 26262:2011 is shown in **Fig. 1**.

**1 This report was prepared based on the report regarding the results of the FY2014/2015 Next Generation Advanced Driver Assistance System Research and Development and Demonstration Project, report regarding the results of the FY2016 Smart Mobility System Research, Development and Demonstration Project, and report regarding the results of the FY2017/2018 Research and Development and Demonstration Project for the Social Implementation of Advanced Autonomous Driving Systems; which are all the accomplishments of METI's consigned projects.*

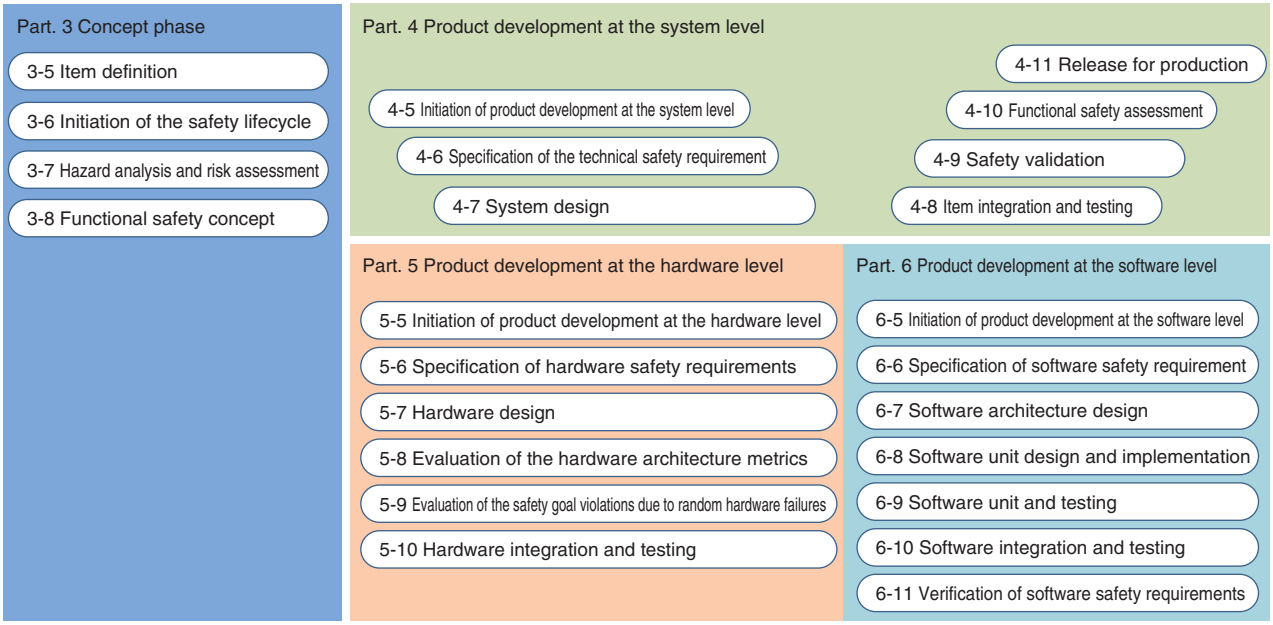
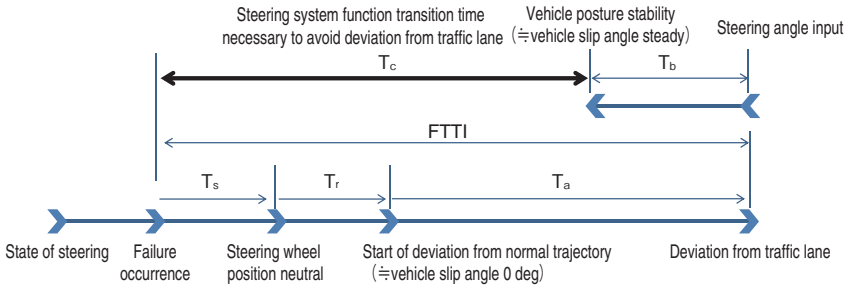


Fig. 1 Development flow of ISO 26262:2011 (Part. 3-Part. 6)



T_s : Time from when failure occurs to when tires/steering wheel are returned to center (set as zero seconds for bench test calculation)
T_r : Time until vehicle center-of-gravity starts deviating from normal trajectory after the tires/steering wheel are returned to the center by SAT
T_a : Time from when vehicle center-of-gravity starts deviating from normal trajectory until part of vehicle contacts the white line center
T_b : Time from when steering angle is inputted until vehicle posture becomes stable again from a state of steering (set to 0.5 s on bench test calculation)

Fig. 2 Status of deviation from traffic lane

2. 1 Concept and Setting of Fault Tolerant Time Interval (FTTI)

In Part 3 of **Fig. 1**, the Safety Goals (SG) required of steering systems were established from behavior in autonomously-driven vehicles as follows.

- Prevent steering failure leading to deviation from traffic lane during autonomous driving
- Prevent unnecessary steering leading to deviation from traffic lane in autonomous driving

Here, "steering failure" refers to stopping of the function for automatic steering, and "unnecessary steering" refers to excessive steering beyond the extent necessary for automatic steering. To achieve these Safety Goals, there is a need to formulate Functional Safety Requirements (FSR) and Technical Safety Requirements (TSR) to enable the steering system to continue functioning in the event of a failure. For such formulation, it is important to quantitatively express the SGs; in other words, the calculation of "the time from the occurrence of the autonomously-driven vehicle failure until deviation from the traffic lane (FTTI)" and "the timing that should be complied with to continue the function." In this section, we show the concept and settings for these by using steering failure as an example of the implementation for this problem.

First, the travelling condition was set to "turning and maintaining steering on an expressway". This is based on the line of thinking that the severity of an accident (the degree of harm) is greater if the deviation from the traffic lane caused by the failure occurs on an expressway. In addition, the movement of the vehicle at this time is established as "failure occurs during steering, the tire and steering wheel return to the neutral position by Self Aligning Torque (SAT), the vehicle starts to travel straight and deviates from the traffic lane." Based on these, **Fig. 2** shows the time from failure to deviation from traffic lane

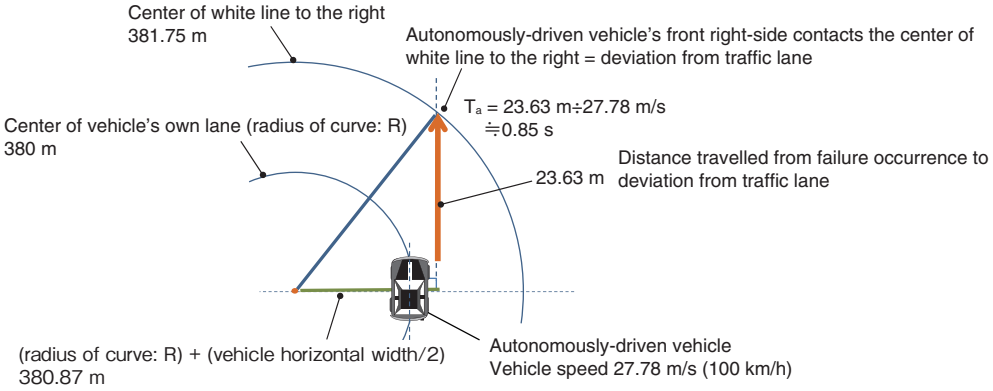


Fig. 3 Movement of deviation from traffic lane

Table 1 Time until deviation from traffic lane

Road conditions				Steering angle, deg	FTTI (T_a+T_r)		T_b, s	T_c, ms
Place	Radius of curve, m	Design vehicle speed, km/h	Width, m		T_a, s	T_r, s		
Expressway	380	100	3.50	16.8	0.85	0.14	0.50	490
	230	80	3.50	21.9	0.80	0.11	0.50	410
	88	50	3.25	40.6	0.67	0.07	0.50	240

and the length of time the steering system must function to avoid deviation from the traffic lane inferred from there.

The T_r of **Fig. 2** is calculated from a vehicle motion equation for a typical two-wheeled model, while T_a is based on the concept shown in **Fig. 3**. It should be noted that **Fig. 3** uses an example of turning on an expressway where the radius of curve is 380 m, and the design vehicle speed is 100 km/h. In addition, the time the function must continue in order to avoid lane deviation, T_c, is FTTI (sum of T_r and T_a) minus the time from steering angle input until the vehicle posture stabilizes (T_b). **Table 1** shows the results of calculating the respective times in relation to the travelling conditions assumed for expressways and metropolis expressways complying with the Government Order on Road Design Standards. T_c being the shortest time in each of these conditions was set as one of the targets of safety design for this theme (T_c = 240 ms with a radius of curve 88 m on a metropolitan expressway). In addition, a steady circle turn was used for the travelling model in the calculation. In this way, it is possible to perform detailed design tied to SGs by clarifying SGs in advance not only in the system safety design for steering systems, but also other systems equipped on autonomously-driven vehicles.

2. 2 Fail-operational during Operational Function Failure

The steering system architecture developed in this theme is shown in **Fig. 4**. This is based on the Functional Safety Requirement (FSR) at the vehicle level needed to achieve the Safety Goals (SG). For example, continued system functionality upon failure occurrence is possible by implementing FSRs such as "providing a function to detect failure of the steering angle control function (main system)" and "continuing to function by providing a redundant steering angle control function," on the Safety Mechanisms (SM) relative to the Intended Functionality (IF) of the steering system architecture. The description of FSR is omitted in this report.

The following is a case study of the issues responding to autonomous driving with the steering system architecture of **Fig. 4**. As mentioned in the preceding paragraph, in order to ensure safety in the event of the autonomous driving system failing, it is necessary to continue the function of the steering system until the vehicle deviates from the traffic lane (240 ms or less in the case of this theme: See **Table 1**).

For example, if the operational function (main) in **Fig. 4** stops functioning due to a failure, the operational function (sub) performs control instead of the operational function (main), thus making it possible to continue the steering system function and prevent deviation from the traffic lane. However, if the operational function (sub) takes control instead of the operational function (main),

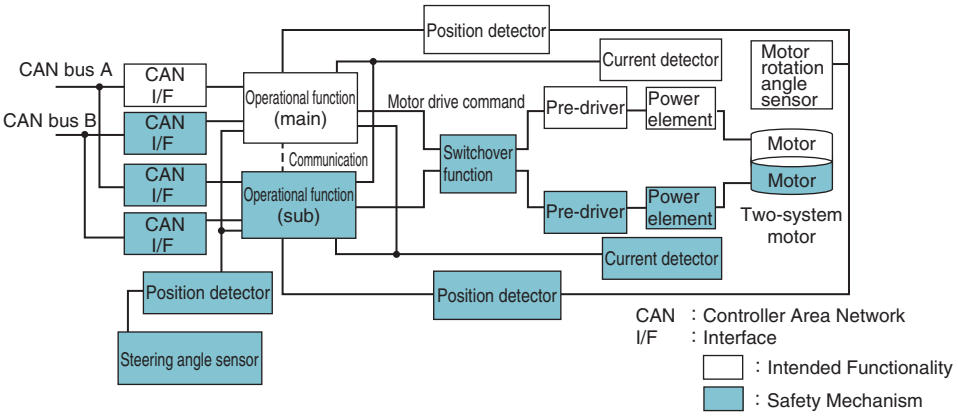


Fig. 4 Steering system architecture

there is a need to implement measures to avoid violations of SGs. Such violations include "switching after deviation from traffic lane" and "vehicle behavior changing suddenly at the moment of switching from main to sub causing deviation from traffic lane." For this theme, in order to avoid such SG violations, the standby state of the operational function (sub) during normal times was made "hot standby." **Figure 5** shows the concept of hot standby implemented in the operational function.

As shown in **Fig. 5**, the operational function (sub) is constantly performing operations with the same timing and control parameters as the operational function (main) even while on standby. In other words, since the main and sub operational functions are always in the same control state, the switchover from main to sub can be performed safely and swiftly, minimizing the impact on the vehicle. Based on this idea, failure detection to completion of switchover is achieved in 10 ms or less in the actual design of the operational function. The concept of hot standby for operational function is effective in autonomous driving systems that require high-speed switching, especially drive motor control systems, steering systems, and detection, cognition, and judgment systems.

3. Verification of Autonomous Driving System Issues

In response to the issues described in the previous section, we built a prototype product (steering system prototype controller) that incorporates the steering system architecture shown in **Fig. 4**. We verified this prototype through a bench test or using a simulator and actual vehicle. The verifications discussed in this section were carried out with reference to Section 8 of ISO 26262-4: 2011 "Item integration and testing". **Table 2** shows the list of test environments constructed in this theme.

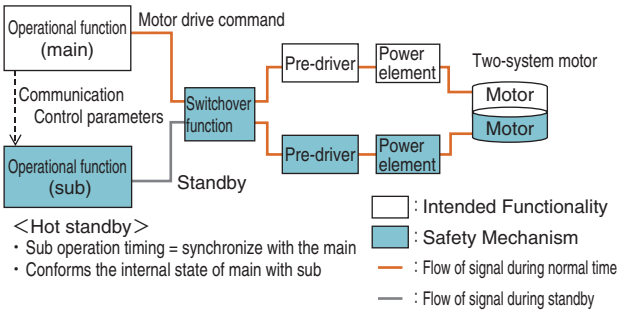


Fig. 5 Concept of hot stand-by for operational function

3. 1 Verification on a Steering Angle Control System Bench (Bench Test)

The purpose of bench verification is to evaluate the implementation and performance of the Safety Mechanisms (SM) incorporated in the steering system prototype controller. Using the steering angle control system bench shown in **Table 2**, a simulated failure was injected into the relevant function of the steering system prototype controller, and the fault detection and switching procedures were evaluated to see if they were working as designed. The test cases required for evaluation were prepared with reference to ISO 26262-4:2011 8.4.1 and 8.4.3. In this report, in relation to the fail-operational in the case of operational function failure (the issue described in **Section 2. 2**), **Fig. 6** and **Fig. 7** show the failure injection method and confirmation results.

Figure 7 shows that, by injecting a simulated failure into the operational function (main), a failure is detected and the output of the operational function (main) is stopped within the function continuation period required to avoid deviation from traffic lane T_c (240 ms), and the output to the motor (PWM signal) switches to the operational function (sub). This indicates that the SMs implemented based on each Safety Requirement are functioning as intended. Furthermore, for this theme, we confirmed that fail-operational existed for not only the

Table 2 List of testing environments

	Features of the evaluation environment				
Evaluation environment	Automatic steering function	Road load	Surrounding environment	Vehicle movement	Driving sovereignty
Steering angle control system bench	Controller + motor	Load motor	–	–	–
Autonomous driving simulator	Controller + motor	Load motor + scenario preparation tool	Scenario creation tool	Vehicle motion simulation tool	System
Actual vehicle evaluation	Controller + motor	Actual road load	Actual environment	Actual vehicle	System

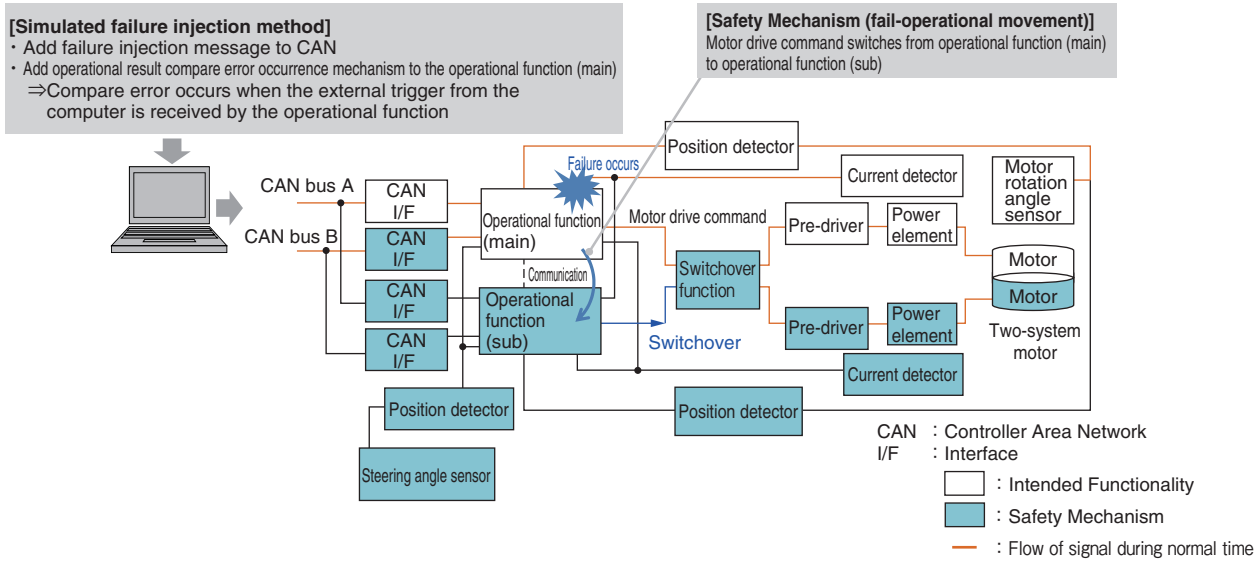


Fig. 6 Fault injection method to the operational function

operational function, but also for all implemented SMs, however a description of this is omitted in this report.

3. 2 Verification in an Autonomous Driving Simulator

The purpose of verification in a simulator is to check the accuracy of the time from failure to deviation from traffic lane calculated in **Section 2. 1** (FTTI), and evaluate the impact of the Safety Mechanism (SM) required for fail-operational on the behavior of the autonomously-driven vehicle. These details are described in **Sections 3. 2. 1** and **3. 2. 2** below. First, **Fig. 8** shows the configuration of the autonomous simulator.

As **Fig. 8** shows, the scenario creation tool creates the vehicle's travelling scene and describes vehicle behavior, while the vehicle motion simulation tool calculates the vehicle motion from the given vehicle control value, vehicle specifications, and road conditions. The integrated

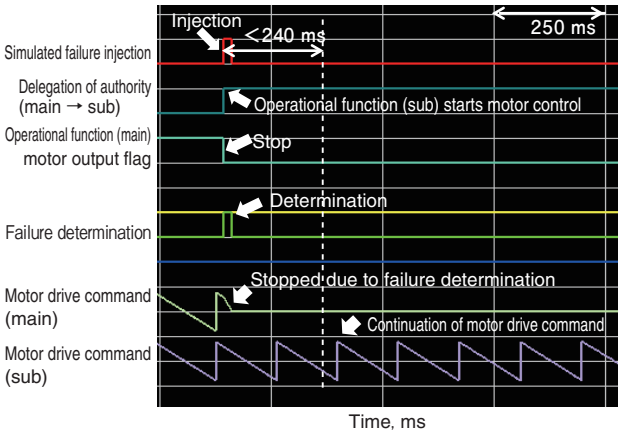


Fig. 7 Fail-operational confirmation result

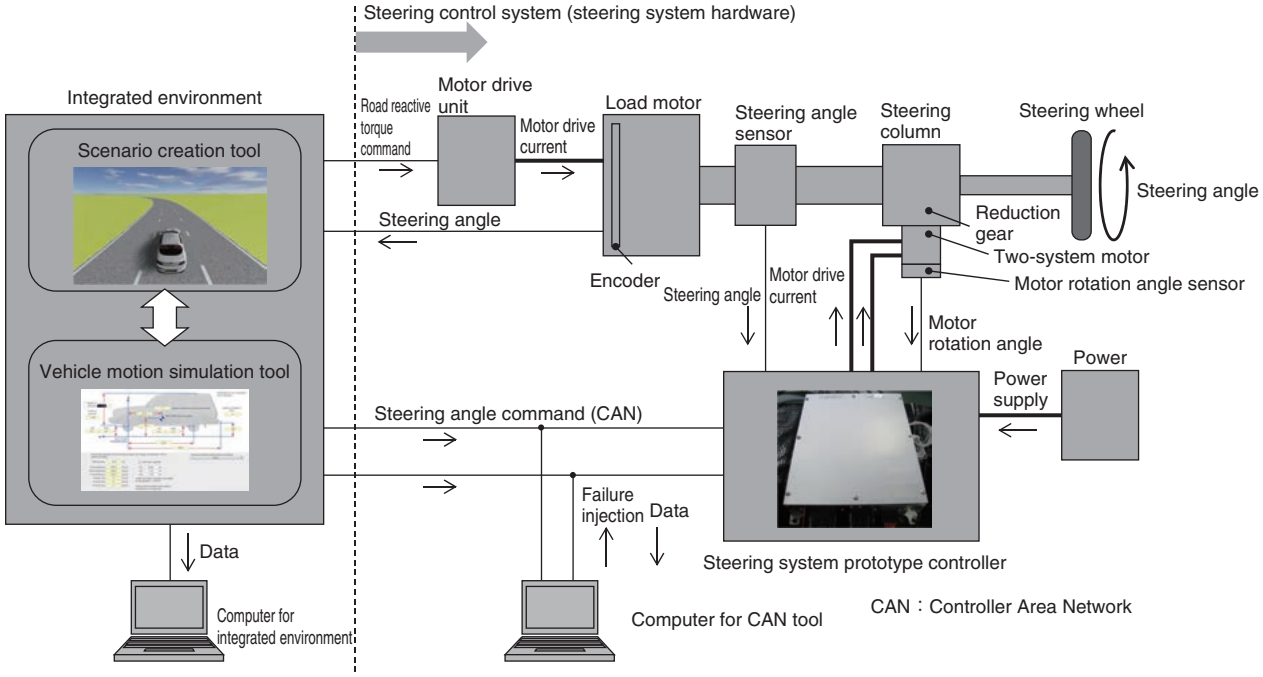
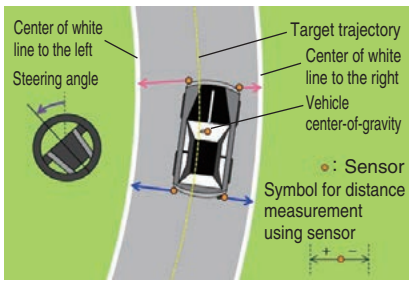


Fig. 8 Diagram of an autonomous simulator



If the white line center or target trajectory is (relative to the vehicle front)
on the left: + (positive) value output
on the right: – (negative) value output

However, vehicle right side sensor senses the center of white line to the right
Sensor on vehicle's left side senses the center of white line to the left.

Fig. 9 Measurement sensor mounting positions

environment is a collaboration between the two tools described above, and communication is performed with elements outside of the integrated environment (steering system hardware), thus ultimately simulating a state of autonomous driving.

Next, we show the sensing method for measuring the deviation of the autonomously-driven vehicle from traffic lane. Sensors were added to the vehicle in the scenario creation tool in a total of five locations; the front left, front right, back left, back right, and vehicle center-of-gravity in order to make it possible to measure the shortest distance between the boundary line of the vehicle's own lane (hereinafter "white line center") and the target trajectory (see **Fig. 9** and **10**). The sensor attached to the right side of the vehicle senses the distance to the center of the white line to the right, and the sensor attached to the left side of the vehicle senses the distance to the center of the white line to the left. If the object (white line center or target trajectory) is on the left relative to the front side of the vehicle, the sensor outputs a + (positive) value and, alternatively, if the object is on the right relative to the front side of the vehicle, the sensor outputs a – (negative) value. Also, the value is + (positive) when the steering angle is counterclockwise.

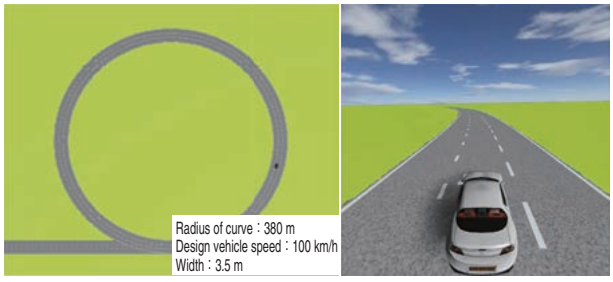


Fig. 10 Vehicle behavior confirmation screen

3. 2. 1 FTTI Accuracy Verification

This section discusses the results of confirming the accuracy of the time from the failure occurring to deviation from the traffic lane (FTTI) calculated by the bench test in **Section 2. 1** using the autonomous driving simulator. As shown in **Section 2. 1**, the FTTI at the time steering failure occurs indicates the time from simulated fault injection during turning and steering to the time it takes for the vehicle to deviate from the center of the white line. The occurrence of steering failure by simulator was configured to send a stop operation command from the outside to the steering system controller. The steering system controller that receives the stop operation command stops the driving current to the motor, which in turn eliminates motor torque, resulting in a steering failure condition during travel. Using this steering failure generation method, we confirmed the accuracy of the FTTI calculated in the bench test in addition to the driving conditions shown in **Table 3**. Here, in addition to the expressway condition of **Table 1**, the condition simulating a left turn on a general road verifiable using the same model was also used for reference evaluation.

Table 4 shows a comparison between the value calculated in the bench test in **Section 2. 1** and the result of confirmation in a simulator carried out in this section. Moreover, **Fig. 11** is a graph showing some of these result plotted identically.

From **Table 4**, when comparing the value calculated in the bench test and the simulation results, it can be confirmed that T_a, which has a high contribution to FTTI (the time until the autonomously-driven vehicle starts to deviate from the normal trajectory until it overlaps the center of the white line: See **Fig. 2**) demonstrates similar characteristics when it is assumed that the vehicle is travelling on an expressway. This represents the static behavior of the vehicle assuming that T_a is in a straight direction, and can be calculated using a simple vehicle motion equation. In addition, in the expressway where the radius of curve is larger than a general road, the steering angle in a maintained-steering state is small while driving

Table 3 Autonomous driving conditions (FTTI confirmation)

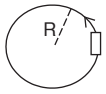
Road conditions				Reference	Travelling model
Place	Radius of curve, m	Design vehicle speed, km/h	Width, m		
Expressway	380	100	3.50	Government Order on Road Design Standards	
	230	80	3.50	Government Order on Road Design Standards	
	88	50	3.25	Sangubashi, Metropolitan Expressway	
General road	15	20	3.50	Government Order on Road Design Standards	

Table 4 FTTI comparison results

Road conditions				Steering angle, °	FTTI calculation result			
Place	Radius of curve, m	Design vehicle speed, km/h	Width, m		Environment	FTTI, s	T_a, s	T_r, s
Expressway	380	100	3.50	16.80	Bench test	0.99	0.85	0.14
					Simulator	1.08	0.85	0.23
	230	80	3.50	21.90	Bench test	0.91	0.80	0.11
					Simulator	1.06	0.85	0.21
	88	50	3.25	40.60	Bench test	0.74	0.67	0.07
					Simulator	1.03	0.74	0.29
General road	15	20	3.50	185.40	Bench test	0.59	0.56	0.03
					Simulator	1.23	0.99	0.24

Bench test: Bench test calculation result
Simulator: Autonomous driving simulator result

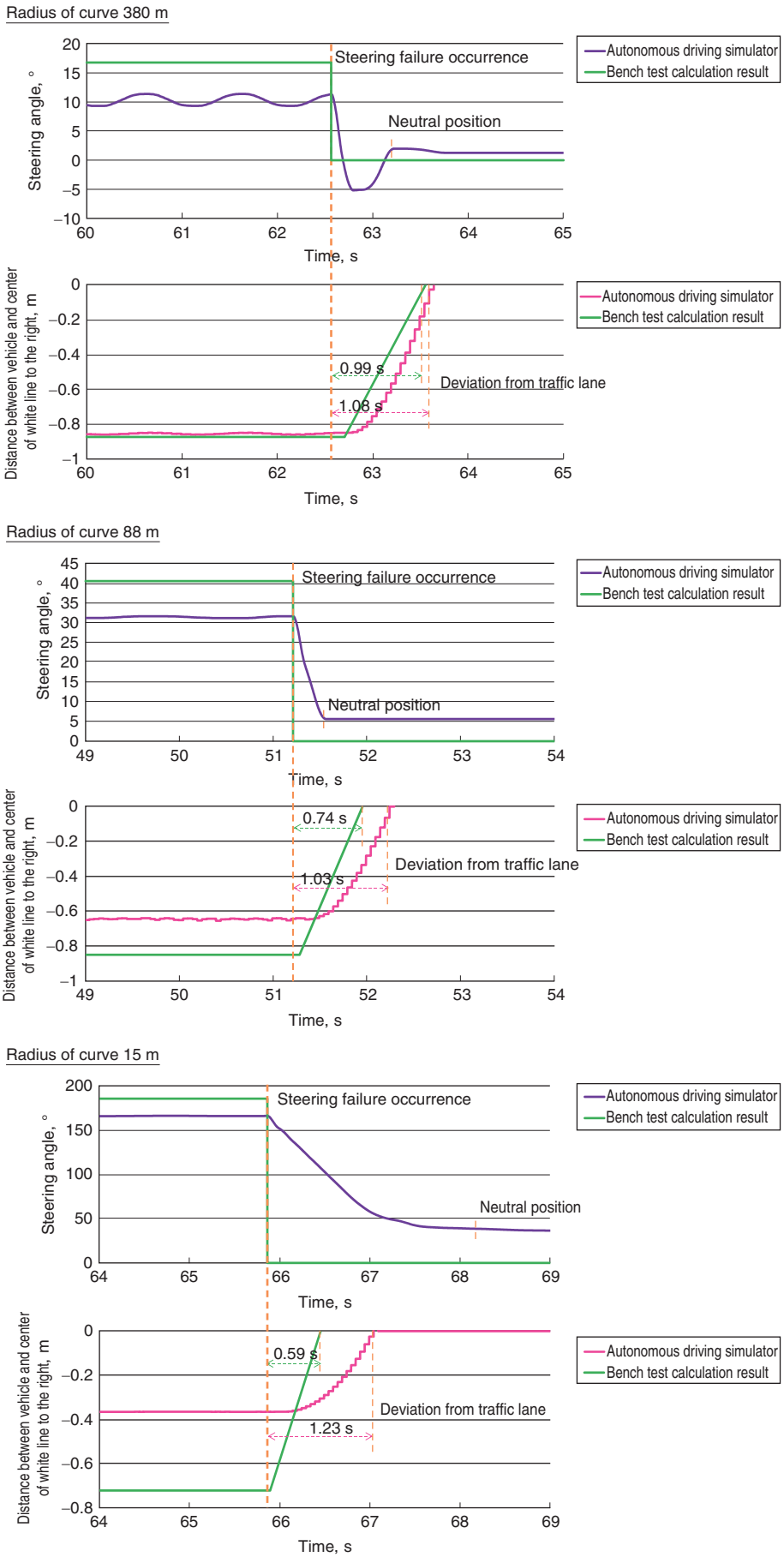


Fig. 11 FTTI comparison diagram (excerpt)

in a circular curve, and the time to return the steering angle to the vicinity of neutral by SAT is short. This is one of the reasons why correlations appeared in T_a.

On the other hand, as **Fig. 11** shows, the result in the autonomous driving simulator assuming a general road with a radius of curve 15 m, is that the autonomously-driven vehicle departs from its own lane before the steering angle returns to a position in the vicinity of neutral. Therefore, in conditions where the steering angle before steering failure is large, such as at low speed, there is a need to add the interval placed as zero seconds under the bench test calculation condition (time for steering angle to reach neutral position by Self Aligning Torque (SAT) from a maintained-steering state). Moreover, it can be seen that the difference between the FTTI of the bench test calculation result and the autonomous driving simulator result increases as the vehicle speed decreases and the steering angle increases.

From the above results, it can be established that FTTI can be a reference value even in bench test calculations using a simple formula under conditions assuming expressway travel, however to widen the vehicle travelling conditions to the low speed range assuming a general road, it would be necessary to confirm using a simulator.

3. 2. 2 Confirmation of Effect of Fail-operational on Behavior of an Autonomously-driven Vehicle

This section describes results of a verification utilizing an autonomous driving simulator to ascertain the presence or absence of a Safety Goal (SG) violation (deviation from traffic lane) in the period between a fail-operational operation due to injection of a simulated failure until the posture of the autonomously-driven vehicle stabilizes. In regards to the travelling scene for the verification, the same conditions as **Table 3** in **Section 3. 2. 1** were selected, and simulated failures during turning were injected in each scene. Some of the confirmation results are shown in **Fig. 12**. A simulated fault is injected into the operational function (main), and other injection results are omitted.

From **Fig. 12**, the vehicle behavior at the time of fail-operational due to failure of the operational function can be confirmed to not have reached the point of deviation from the traffic lane as there is no variation in the travelling trajectory (the shortest distance between each of the vehicle's four corners and the center of the white line) before and after the simulated failure injection. As with the verification results by the steering angle control system bench in **Section 3. 1**, this is believed to be

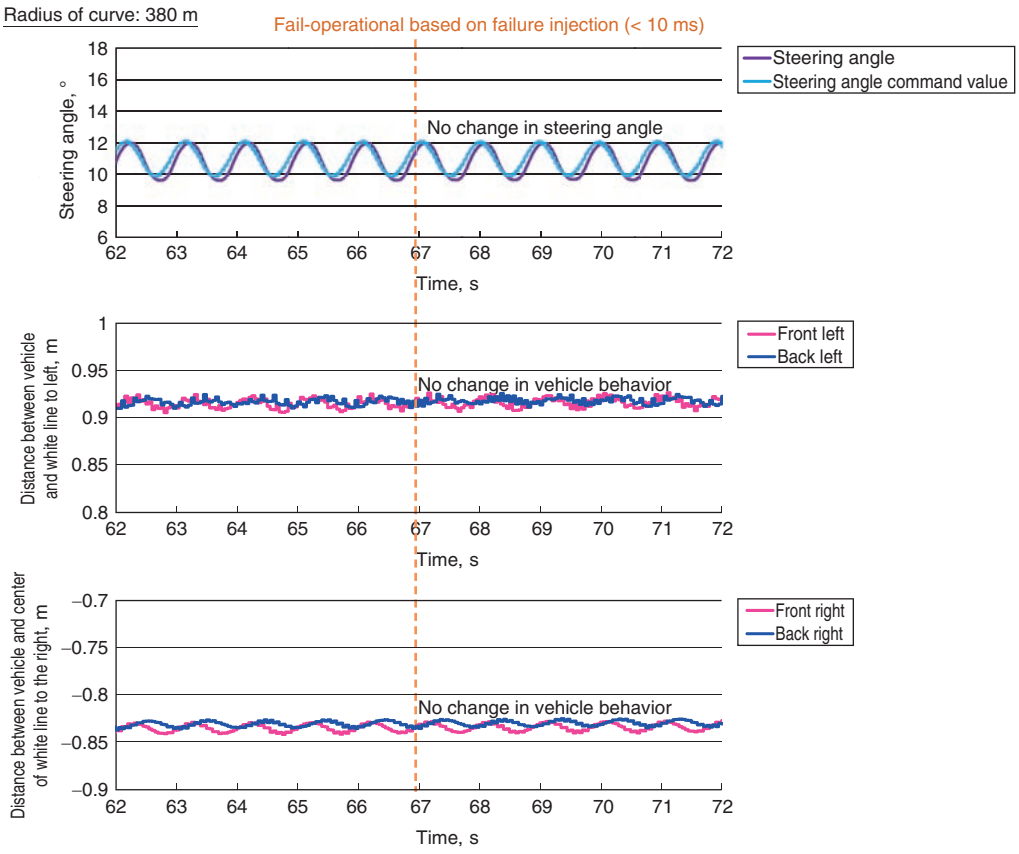


Fig. 12 Results of confirming vehicle behavior through fail-operational

because the transition from operational function (main) to operational function (sub) is completed in 10 ms or less, therefore there is no effect on the vehicle behavior.

Thus, by using a simulator, it is possible to easily simulate autonomous driving scenes, as well as confirm the behavior of the fail-operational and autonomously-driven vehicle in the event of a failure with good reproducibility even in high-risk and severe conditions. In the future, as the development of autonomous driving accelerates further, we believe that the examples of problem verification shown in this section will be useful.

3. 3 Verification on an Actual Vehicle

Verification on the actual vehicle was carried out from the position that it was the final confirmation of the ISO 26262 V-shaped model. The purpose of this verification is to confirm the effectiveness of each verification method by comparing the bench test calculation results and the autonomous driving simulator verification results described in each section.

The autonomous driving system mounted on the actual vehicle utilizes open source autonomous driving control software based on a real-time OS (Operating System) and is equipped with a LiDAR (Light Detection and Ranging) on its peripheral environment recognition device so that the vehicle can grasp its own position. In addition, the steering system is equipped with column-type electric power steering including a steering system prototype controller with fail-operational, and a motor. **Figure 13** shows the autonomously-driven vehicle used for verification.

Measurement of the distance between the autonomously-driven vehicle and the center of the white line was performed using a 3D map and the same sensing as **Fig. 9**, while travelling conditions were made the same as the general road condition of **Table 3** to match the comparison conditions with simulation results. **Figure 14** shows the results of confirming actual vehicle behavior when a simulated failure is injected into the operational function (main), and **Fig. 15** shows comparison results of the bench test calculated value, autonomous driving simulator value, and actual car measurement value for the time from the failure occurring to deviation from the traffic lane (FTTI).

In **Fig. 14**, the vehicle behavior at the time of fail-operational due to failure of the operational function (main) can be confirmed to not have reached the point of deviation from the traffic lane as there is no variation in the travelling trajectory before and after the simulated failure injection. This is roughly consistent with the verification results obtained from the autonomous driving simulator in **Section 3. 2. 2**, and the transition from the operational function (main) to the operational function (sub) is also the same on the actual vehicle as it can be

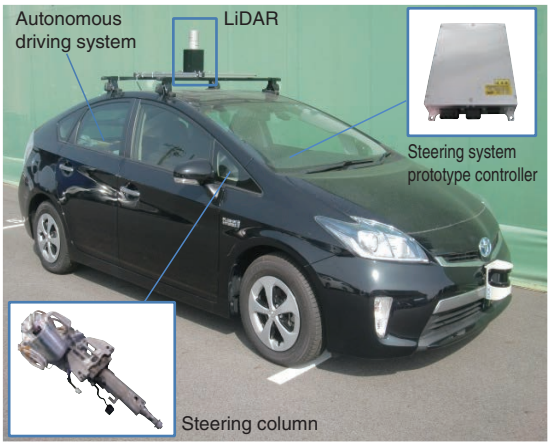


Fig. 13 Actual vehicle for autonomous driving

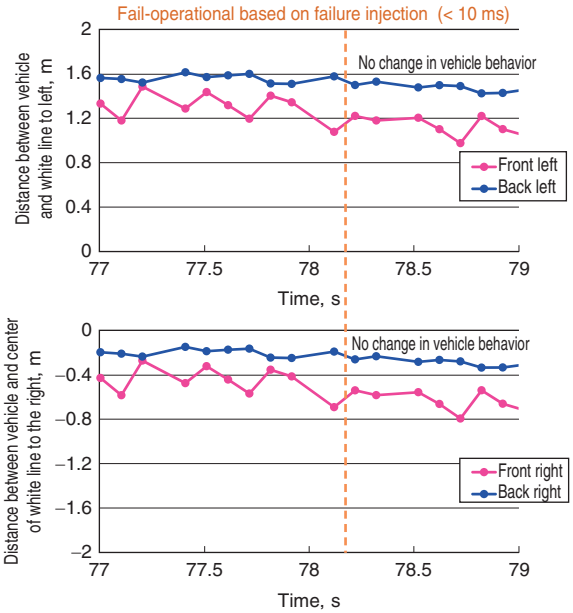
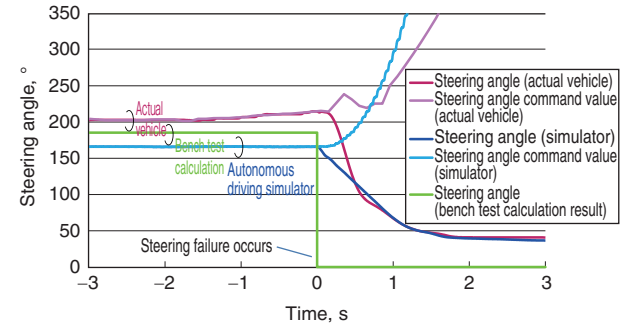


Fig. 14 Results of confirming vehicle behavior through fail-operational (Actual vehicle evaluation)

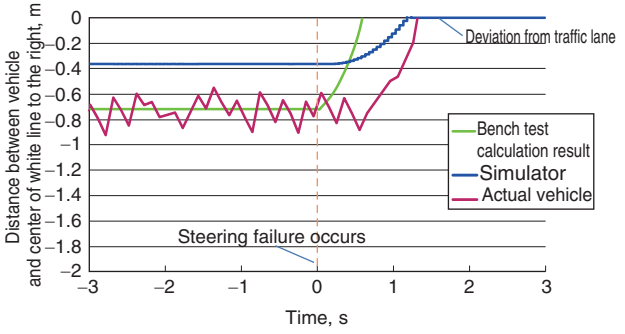
completed within 10 ms, therefore does not affect vehicle behavior.

The three portions of **Fig. 15** show comparison results. **15 (a)** shows a comparison of steering angle command value and steering angle, **(b)** shows a comparison of the distance between the vehicle's front right and center of white line to the right, and **(c)** shows a comparison of the distance between vehicle center-of-gravity and target trajectory. This is adjusted to suit the graph's time axis (x axis) whereby the time of steering failure occurrence is zero seconds.

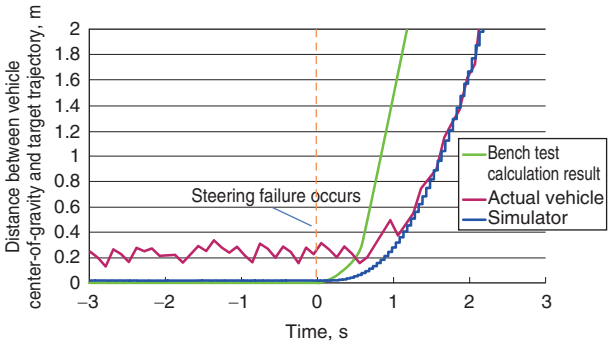
Figure 15 (b) shows that the time from steering failure occurrence to the deviation from traffic lane (FTTI) is close to the results obtained in the actual vehicle evaluation and autonomous driving simulator. However, if the data before zero seconds before steering failure



(a) Steering angle command value and steering angle



(b) Distance between vehicle front right and center of white line to the right



(c) Distance between vehicle center-of-gravity and target trajectory

Fig. 15 Difference due to evaluation environments (FTTI results)

is observed, it is apparent that the distance between the front right of the vehicle and the center of white line to the right varies in the respective evaluation environments. This is because the vehicle slip angle is different during circular curve travel, and when accuracy is improved, it is necessary to combine the parameters of the autonomous driving simulator side.

Figure 15 (c), in contrast to **Fig. 15 (b)**, represents the vehicle behavior without the influence of vehicle slip angle. From **Fig. 15 (c)**, it can be construed that, in an actual vehicle, although the distance with the vehicle center-of-gravity before steering failure and the target trajectory is not consistent and there is room for improvement, the vehicle behavior after steering failure occurs shows the same characteristics as the vehicle behavior observed in the autonomous driving simulator. In other words, it is possible to obtain the same characteristics of vehicle trajectory in the simulator and the actual vehicle. Therefore, when deciding whether to use a simulator or an actual vehicle, it is desirable to use the suitable one for the specific application to be verified. See **Section 3. 2** for a comparison between the bench test calculation result and the simulation result.

4. Conclusion

In this paper, we described case studies of the results of the consigned project from Japan's Ministry of Economy, Trade and Industry. **Section 2**, using the steering system as an example, discussed the concept of time from failure to deviation from traffic lane (FTTI), a requirement to verify Safety Mechanism (SM) taken from the safety design and issues relating to autonomous driving systems extracted from ISO 26262:2011, as well as the bench test calculated value thereof. In addition, a case study was provided regarding a safe switching method (hot standby) in the event of an operational function failure. Furthermore, in **Section 3**, in relation to autonomous driving system issues, we were able to construct verification environments for bench test, autonomous driving simulator, and actual vehicle respectively, and confirm safety design, as well as the effectiveness of each verification method.

These results are available to the general public through the Ministry of Economy, Trade and Industry, and we hope that it will be useful supporting data for individual companies and demonstration projects that will start developing autonomous driving technology in the future.

5. Acknowledgements

The results of this research were obtained from the FY2014/2015 Next Generation Advanced Driver Assistance System Research and Development and Demonstration Project, FY2016 Smart Mobility System Research, Development and Demonstration Project, and the FY2017/2018 Research and Development and Demonstration Project for the Social Implementation of Advanced Autonomous Driving Systems. We would like to express our gratitude to the Japan Automobile Research Institute, a general foundation corporation from whom we received a great deal of cooperation in conducting this research.



N. KAIHARA* K. KIMURA* A. ISHIHARA**

H. NAKAMURA***

* *Future & Frontier Research Dept., Research & Development Division*
** *Systems Innovation R&D Dept., Research & Development Division*
*** *ITS Research Dept., Japan Automobile Research Institute*