講演番号	248

文献番号	20225248

The redundant system for fail-safe operation in the event of malfunction

Takefumi Yamada [1)] Naoki Isokane [1)] Keita Kinoshita [2)] Satoshi Takahashi [2)]

1) Woven Core, Inc
Nihonbashi Muromachi Mitsui Tower, 3-2-1 Nihonbashi Muromachi, Chuo-ku, Tokyo, 103-0022, Japan
2)TOYOTA MOTOR CORPORATION
1 Toyota-cho, Toyota, Aichi, 471-8572, Japan

KEY WORDS:**Electronics and control, Control system/autonomous land system/autonomous driving, System Electronics,** Software Architecture (E1)

In order to realize an advanced driver assistance system in hands-off driving, in the event of a malfunction, the system is requires to continue its assistance until the driver regains the driving operation. In the advanced driver assistance system, it is essential to ensure high reliability with redundant design within the restrictions on component mounting. The following three functions are redundantly designed to achieve a fail-safe operation. Firstly, braking function to avoid or reduce the severity of a collision with moving or stationary vehicles in front of the vehicle along with front object recognition system. Secondly, steering function to keep the current lane as much as possible along with lane recognition system. Finally, notification function to let the driver know that the driver's take-over is required.

The system has redundant configuration, as shown in Fig.1 for components necessary for the fail-safe operation such as sensors for recognizing surrounding vehicles and lanes, actuators for braking and steering, and sensors for information on vehicle motion. It also has redundant power supplies and communications. In the event of a malfunction and a bad condition such as heavily rain, the remaining components are available for continued the fail-safe operation.

The ADS-ECU (Advanced Drive System ECU) consists of the SoC (System on a Chip) and the MCU (Micro Controller Unit). Functions that require high computing power for recognition and judgement are placed in the SoC, and functions that require high reliability are placed in the MCU. The SoC has functions that require high computing power, such as Localization that estimates the vehicle position, Sensor fusion that determines object information based on the results of multiple sensors, and Planner that generates the trajectory and speed plan. MCUs are redundant between MCU2 (Main System) and MCU1 (Backup System) , and the functions necessary for the fail-safe operation such as the Controller that commands the actuators from the ADS-ECU, the Human Machine Interface that notifies the driver takes over driving operation, and the System State Manager that manages the system state of the ADS-ECU, are arranged. The system can continue the fail-safe operations using the functions of the remaining MCU even if one of the MCUs fails.

In order to confirm the effects of the redundant system described above, all these components were implemented onto the newly designed system. Use of CPU resources were evaluated in the condition of maximum CPU usage, which shows that all functions were processed within the target values. The fail-safe operation was evaluated by simulating component malfunctions using a real vehicle and a simulator, which confirmed that avoid collision, lane keeping, and notification function work as required for the fail-safe operation.

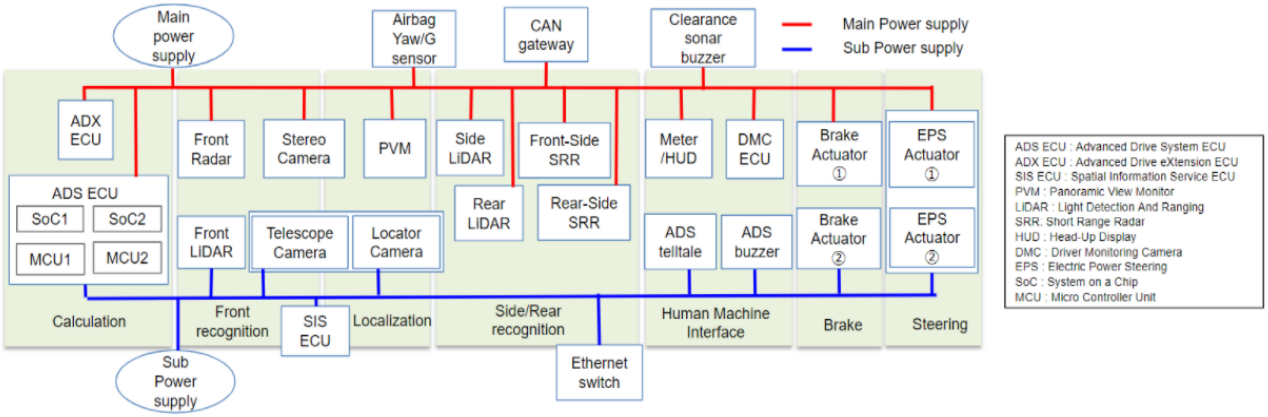

Fig.1 Redundant system configuration