J Electr Eng Technol.2015; 10(4): 1915-1920
http://dx.doi.org/10.5370/JEET.2015.10.4.1915

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Design and Development of a Functional Safety Compliant Electric Power Steering System

Kyung-Jung Lee*, Ki-Ho Lee*, Chanwoo Moon†, Hyuk-Jun Chang* and Hyun-Sik Ahn*

Abstract – ISO 26262 is an international standard for the functional safety of electric and electronic systems in vehicles, and this standard has become a major issue in the automotive industry. In this paper, a functional safety compliant electronic control unit (ECU) for an electric power steering (EPS) system and a demonstration purposed EPS system are developed, and a software and hardware structure for a safety critical system is presented. EPS is the most recently introduced power steering technology for vehicles, and it can improve driver's convenience and fuel efficiency. In conformity with the design process specified in ISO 26262, the Automotive Safety Integrity Level (ASIL) of an EPS system is evaluated, and hardware and software are designed based on an asymmetric dual processing unit architecture and an external watchdog. The developed EPS system effectively demonstrates the fault detection and diagnostic functions of a functional safety compliant ECU as well as the basic EPS functions.

Keywords: Functional safety, Electric power steering system, ISO 26262, Electronic control unit

1. Introduction

Recently, electric and electronic (E/E) systems represent an increasing proportion of vehicle parts. Cars produced today have multiple E/E systems such as electrically controlled steering, automatic windows and doors, antilock brakes, and electronic engine controllers, etc. Usually, these E/E systems are controlled with embedded controllers; these embedded controllers have achieved enhancements in vehicle comfort, fuel efficiency, and safety. Although many of these systems facilitate significant improvements in vehicle safety, they are safety related systems, and unexpected failures and interactions in the software and hardware could lead to potentially hazardous situations [1]. ISO 26262, published in 2011, provides a standard approach to the functional safety management of electrical and electronic systems of passenger cars under a maximum weight of 3500 Kg [2].

An electric power steering (EPS) system is a safety critical system. EPS is the latest power steering technology for vehicles, and it can improve a driver's convenience and fuel efficiency. An EPS system reduces steering torque and provides various steering feels by a torque assist motor. Steering torque is defined as the torque a driver applies on the steering column while turning the steering wheel. When an appropriate assistant torque by an assist motor is applied in the same direction as the driver's steering direction, the amount of steering torque required for steering can be significantly reduced [3-6]. In addition, adjustment of the characteristics of the assistant torque allows the driver to experience various steering feels [7]. Many research and technical papers on the EPS system have been published: basic principle and control algorithms were introduced in [3], a reference model based control strategy was proposed in [8], and a fuzzy logic based control method was presented in [9]. The EPS system has a mechanical steering, an ECU, and an assist motor, as illustrated in Fig. A in the appendix. When the driver turns the steering wheel, the column torque is detected by a torque sensor. The ECU determines the motor current reference by using an assist torque table and controls the motor current. In addition to assist control, an EPS system has two more basic functions, namely, damping control and return-to-center control. The former reduces overshoot and oscillation of the steering wheel, while the latter makes the steering wheel return to the center quickly.

In this paper, a design method for ECU that complies with functional safety requirements is proposed and an EPS system for demonstration purposes with the presented ECU is developed. While many studies have been carried out on ECUs that meet the functional safety requirements [10-12], few systems show how the functional safety related hardware and software works. The purpose of the proposed EPS system is to demonstrate the operation of the functional safety compliant system, and to test the integration of the EPS system and the safety related hardware (H/W) and software (S/W). In addition, to comply with ISO 26262, a hazard analysis and risk assessment are first performed to assign a proper ASIL to the ESP systems, and an ECU hardware and software system that satisfies the H/W and S/W requirements of ISO

† Corresponding Author: Dept. of Electronic Engineering, Kookmin University, Korea. (mcwnt@kookmin.ac.kr)
* Dept. of Electronic Engineering, Kookmin University, Korea (streizin@kookmin.ac.kr, thomeyorke@naver.com, {hchang, ahs} @kookmin.ac.kr)

Received: November 26, 2014; Accepted: May 1, 2015

26262 is then designed. Finally, experiments are conducted to verify the validity of the design process and to evaluate the performance of the developed EPS system.

2. Development Phase of Functional Safety Compliant EPS System

2.1 Hazard analysis/risk assessment of EPS system

In the concept development phase, safety goals are defined and hazard analysis and risk assessment is carried out [2]. ISO 26262 outlines the process of assessing risks and hazardous events by evaluating three factors: severity of potential harm to individuals (S), probability of exposure in the driving and operating situations (E), and the controllability by the driver to control the hazardous situation (C). For the EPS system, the majority of hazard caused by malfunctions in the city could be allocated to ASIL D as shown in Table 1 [2, 3]. Here, a request means that the driver operates the system in a vehicle.

Table 1. Vehicle level ASIL assigned in driving scenario

Scenario

Level	Request	Failure Mode	Driving Scenario	Failure Impact
Vehicle	Steering request	Unintended steering assist	City	Over or under steering

S	E	C	ASIL	Safety Goal
S3	E4	C3	D	Intended steering assist

A failure mode is defined as the manner in which a system component could potentially fail to meet the design intent. A failure impact is a maneuver of the vehicle in faulty conditions. A safety goal is defined as a top-level safety requirement, and is a result of hazard analysis and risk assessment.

2.2 Hardware and software requirements for a safety critical system

Generally, an automotive E/E system consists of hardware elements such as a power supply, CPU, memory, digital I/O, RAM, actuators, sensors and so on. ISO 26262-5:2011 (Annex D) summarizes the typical faults associated with each hardware element and the guidelines for diagnostic coverage (DC). Additionally, the standard lists the typical safety mechanisms associated with these element faults, and categorizes the effectiveness of the safety mechanisms by ranking the DC as low, medium, or high. The rankings correspond to typical coverage levels at 60%, 90%, and 99%, respectively.

The analyzed faults or failures modes of a control logic part of ECU for each DC are shown in Table 2. Five factors need to be detected for control logic to achieve 99% of diagnostic coverage. In addition, safety mechanisms for the processing unit faults are as shown in Table 3 [2]. Even though the diversity and redundancy of the safety measures are implemented in both primary and redundant/monitoring paths within one processing unit as specified in Table 3, an additional external watchdog processor with an independent clock source and power supply should be used to verify the primary processing unit operation and to avoid the risks associated with potential common-cause failures. ISO 26262-5:2011(Annex D) lists the guidelines for ensuring that typical safety mechanisms achieve the required DC level. Table 4 lists examples of external watchdog processors.

Table 2. Typical faults of hardware elements and diagnostic coverage

Element		Control logic
DC for failure modes	Low (60%)	No code execution, Execution too slow, Stack overflow/underflow
	Medium (90%)	Wrong coding or no execution, Execution too slow, Stack overflow/underflow
	High (99%)	Wrong coding, Wrong or no execution, Execution out of order, Execution too fast or too slow, Stack overflow/underflow

Table 3. Safety mechanism for elements faults

Safety mechanism/measure	Typical DC considered achievable
Self-test by software: limited number of patterns (one channel)	Medium
Software diversified redundancy (one hardware channel)	High
Reciprocal comparison by software	High
HW redundancy (e.g., dual-core lockstep, asymmetric redundancy, coded processing)	High

Table 4. Safety mechanisms for program sequence monitoring / clock

Safety mechanism/measure	Achievable Typical DC
Watchdog with separate time base and time window	Medium
Logical monitoring of program sequence	Medium
Combination of temporal and logical monitoring of program sequences with time dependencies	High

An ASIL D system has to assure a high level of diagnostic coverage; therefore, it has to have a watchdog with sequence and time monitoring, software based self-test, and software/hardware diversified redundancy, as listed in Tables 2, 3 and 4.

3. Functional Safety-Compliant Hardware Architecture Design

The designed ECU architecture has an asymmetric dual processing unit architecture with an external watchdog as shown in Fig. 1. The primary processing unit performs the

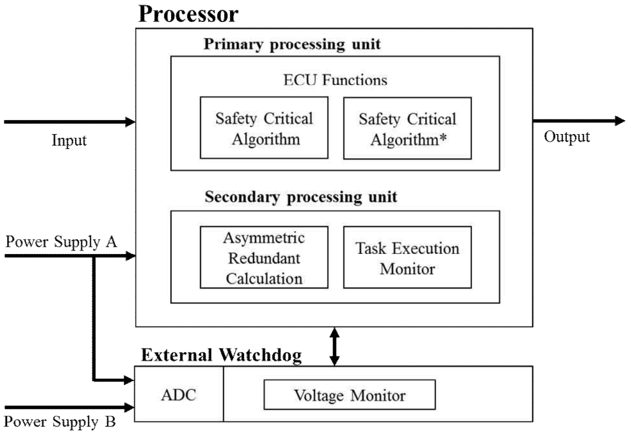

Fig. 1. Asymmetric dual-core architecture with an external watchdog

application software, while the secondary processing unit monitors the results of the operation on the primary processing unit. The external watchdog monitors the supply voltages of the devices and task execution time of the primary processing unit. The processor and external watchdog communicate with each other over a serial peripheral interface (SPI). Also, if a safety critical failure is detected, the external watchdog can drive the system to a safe state using safety path control [13-15].

4. Implementation of Functional Safety-Compliant Software

To achieve a high level DC, the implemented code has a software based self-test and monitor functions. The software structure required to meet the functional safety requirement is shown in Fig. 2. The software related to safety functions checks the memory, special functions registers (SFR), and OP codes in the primary and secondary processing unit cyclically. The software related to safety functions has three monitor functions. First, the asymmetric redundant calculation ensures the reliability of safety-critical algorithms. The safety-critical algorithms code has the redundant implementations of two differently-ordered algorithms. The asymmetric redundant monitor compares the results of two safety critical algorithms (for example, that of the torque assist motor controller), and reports it to the system as shown in Fig. 3. Second, the task monitor ensures the correct sequence of tasks such as algorithms and their allowed run time. The asymmetric redundant calculation and the task monitor are non-critical

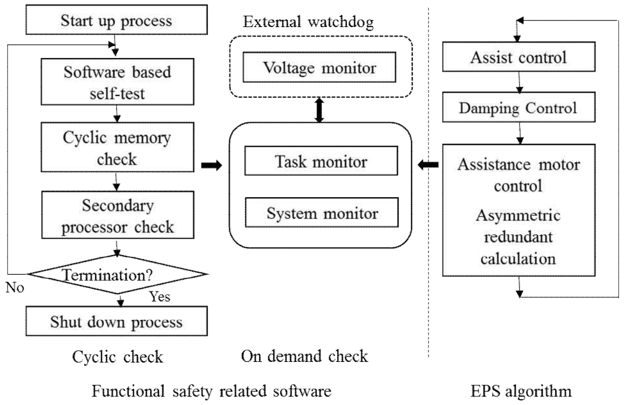

Fig. 2. Software structure for the proposed EPS system

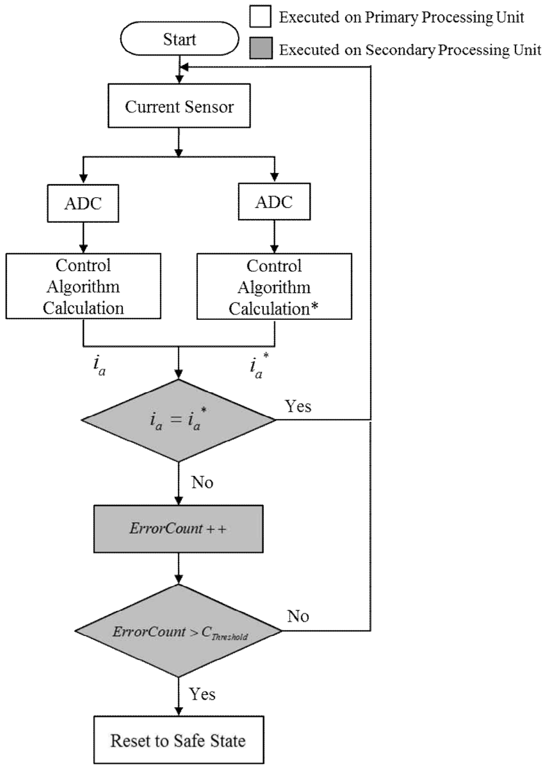
Executed on Primary Processing Unit
Executed on Secondary Processing Unit
Start
Current Sensor
ADC
ADC
Control Algorithm Calculation
Control Algorithm Calculation*
i_a
i_a^*
$i_a = i_a^*$
Yes
No
ErrorCount++
ErrorCount > $C_{Threshold}$
No
Yes
Reset to Safe State

Fig. 3. Safety mechanism of the asymmetric redundant calculation

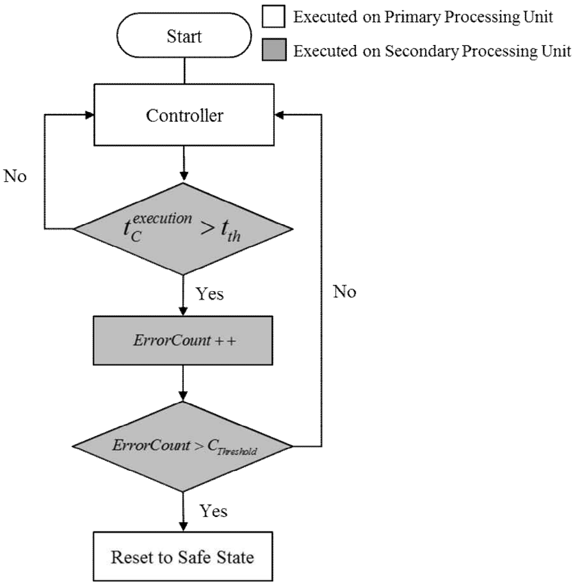
Executed on Primary Processing Unit
Executed on Secondary Processing Unit
Start
Controller
No
$t_C^{execution} > t_{th}$
Yes
No
ErrorCount++
ErrorCount > $C_{Threshold}$
Yes
Reset to Safe State

Fig. 4. Safety mechanism of the task monitor tests. If these non-critical tests fail, an error count of these monitor functions is incremented. When the error count is greater than the threshold count, the external watchdog is set to the disabled state. The entire system also resets to the safe state [14]. Fig. 4 shows the task monitor flow, where $t_c^{execution}$ and t_{th} are the task execution time and threshold time, respectively. Third, the external watchdog monitors the voltage inputs of the safety critical systems. If any voltages are outside of the predetermined threshold voltage range, because the voltage monitor is critical in the tests, the external watchdog directly enters the disabled state to reset the system [13].

5. Experimental Results

The developed experimental EPS system is shown in Fig. 5. The system consists of a wheel, an assist BLDC motor, an ECU, a torque and angle sensor (TAS) on the steering column, and a geared DC motor that simulates reaction force. The structure of the ECU for the EPS is shown in Fig. 6. The TAS sensor measures the steering torque on the steering column, and the BLDC motor then generates the assist torque in such a direction that it reduces the steering torque.

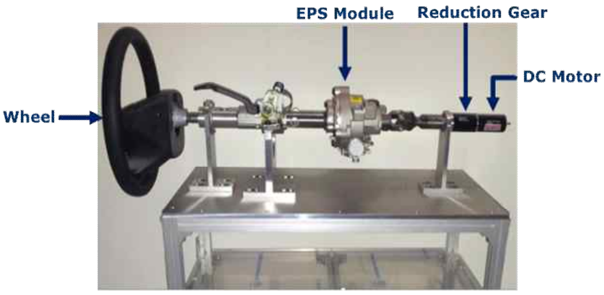

Fig. 5. Experimental EPS system

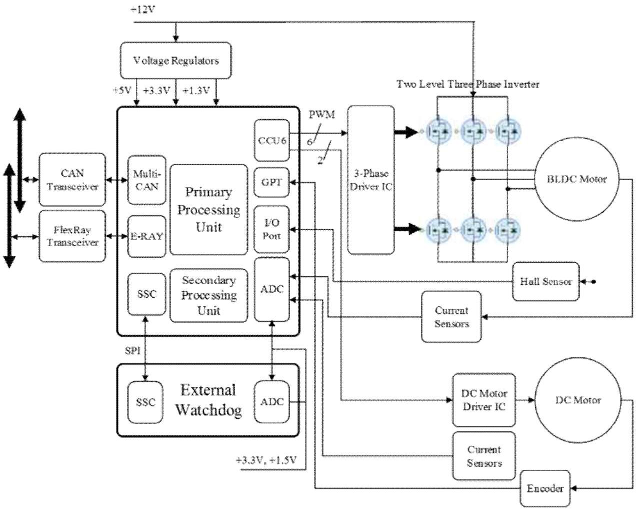

Fig. 6. Structure of the Experimental EPS system

Monitoring functions for functional safety such as the asymmetric redundant calculation, task monitor, and voltage monitor are verified using a hardware-in-the-loop simulation (HILS). Assistant motor control loops, which are safety critical codes, are redundantly implemented. Two independent and differently ordered instances of the same control algorithm calculate the current reference on motor. The system monitor compares the results from two redundant codes. To test the function of the system monitor, an incorrect result is generated by one motor control instance on purpose, so that the calculation results from the two instances do not coincide. The system monitor reports the mismatch, and the system is then reset at 3.35s, as in Fig. 7. This shows that the system monitor works properly. Next, an experiment is conducted to test the voltage monitor. The external watchdog monitors the supply voltage to the motor driver, and the upper and lower threshold voltages are set to 2.7V and 1.3V, respectively. In the case the supplied voltage to the motor driver goes

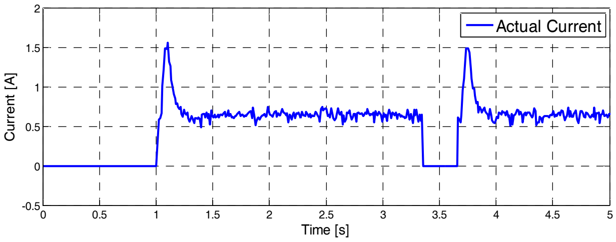

Fig. 7. Asymmetric redundant calculation – current control response

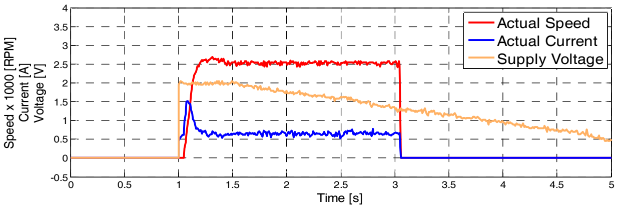

Fig. 8. Voltage monitor

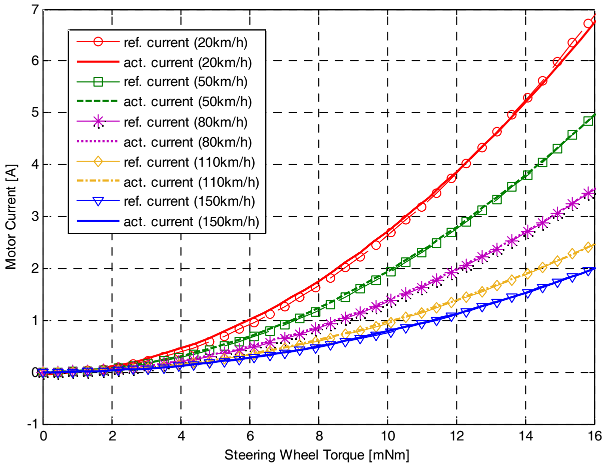

Fig. 9. EPS assist motor current with respect to steering wheel torque

outside the voltage range, the external watchdog resets the system. As shown in Fig. 8, the supplied voltage drops to 1.3V at 3.1 s, the motor controller is stopped. Finally, the basic EPS function is tested. Fig. 9 shows the results of EPS assist control. The assist torque reference is obtained from an assistance control table that is stored in the ECU, according to the steering torque and vehicle speed. Fig. 9 depicts the reference current and actual current that is directly proportional to the assist motor torque; the figure shows that the actual current follows the reference current. Figs. 7, 8 and 9 show that the EPS function works properly while the safety related software cyclically checks the CPU for faults or failures, and this result verifies that the EPS algorithm is well integrated with functional safety related software.

6. Conclusion

In this paper, a functional safety-compliant design approach for an ECU was presented, and an EPS system was developed for the purpose of demonstration. This EPS system demonstrates the functions of the functional safety compliant hardware and software. The EPS system was assigned at ASIL D, and it must have high DC. The developed ECU consisted of a dual processing unit and external watchdog to achieve high DC. It also has a software base self-test, asymmetric redundancy, and a task monitor. A voltage monitor was also used for the monitoring of faults in the controller. Verification of the proposed functional safety-compliant hardware and software was performed by inserting intentional false data. The asymmetric redundancy and tasks were checked periodically by the system, and when a mismatch or timer overrun was detected, a system reset was attempted. If the supplied voltage to the CPU reaches outside of the voltage range, the system enters the disabled state. The developed EPS is a system used for demonstration purposes, not for actual use, and it is suitable for demonstrating the functions of the hardware/software for functional safety as well as the control algorithm of an EPS system.

Appendix

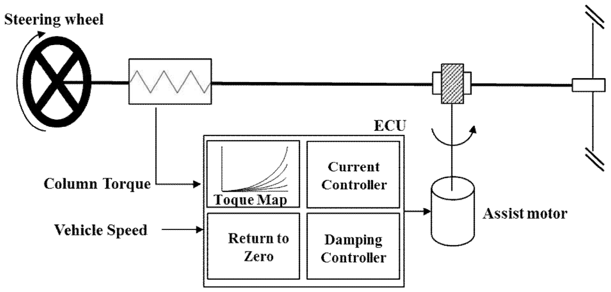

Fig. A. Structure of the EPS system

Acknowledgements

This work was partly supported by Infineon Technologies.

This research was partly supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the C-ITRC (Convergence Information Technology Research Center) (IITP-2015-H8601-15-1005) supervised by the IITP (Institute for Information & communications Technology Promotion)

This research was partly supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2040141)

References

[1] M. Bellotti and R. Mariani, "How future automotive functional safety requirements will impact microprocessors design," Microelectronics Re-liability, vol. 50, no. 9-11, pp. 1320-1326, 2010.

[2] ISO 26262, Road Vehicles-Functional Safety, 2011.

[3] A. Badawy, J. Zuraski, F. Bolourchi, and A. Chandy, "Modeling and analysis of an electric power steering system," SAE Tech. Paper 1999-01-0399, 1999.

[4] Y. Hu, X. Ji, K. Chen and X. Ma, "Elementary Study on BLDC Controller for Electric Power Steering System," SAE Tech. Paper 2004-01-1096, 2004.

[5] J. Lee, H. Moon, and J. Yoo, "Current Sensorless Drive Method for Electric Power Steering," International Journal of Automotive Technology, Vol. 13, No. 7, pp. 1141-1147, 2012

[6] M. Lee, H. Lee, K. Lee, S. Ha, J. Bae, J. Park, H. Park, H. Choi and H. Chun, "Development of a Hardware In The Loop Simulation System for Electric Power Steering in Vehicles," International Journal of Automotive Technology, Vol. 12, No. 5, pp. 733-744, 2011

[7] J. Kim and J. Song, "Control Logic for an Electric Power Steering System Using Assist Motor," Mechatronics, vol. 12, no. 3, pp. 447-459, Apr. 2002.

[8] Alaa Marouf, Mohamed Djemaï, Chouki Sentouh, and Philippe Pudlo, "A New Control Strategy of an Electric-Power-Assisted Steering System," IEEE Transaction on Vehicular Technology, vol. 61, no. 8, pp. 3574-3588, October 2012

[9] Hui Chen, Leilei Zhang, Bolin Gao, "Active Return Control of EPS Based on Model Reference Fuzzy Adaptive Control", Proceedings of the 2011 IEEE International Conference on Mechatronics, pp. 194-199, 2011,

[10] P. O. Jacob, "Design & Safety Considerations for Electrical Power Steering (EPS) Systems Based on Automotive Safety Integrity Levels," SAE Technical Paper, 2010-01-0994, 2010.

[11] S. Seo, "ISO26262 application to electric steering development with a focus on Hazard Analysis," In Proc. of Systems Conference, IEEE International, pp. 655-661, 2010.

[12] K. Lee, Y. Ki, H. Ahn, G. Hwang and J. Cheon, "Functional Safety Compliant ECU Design for Electro-Mechanical Brake (EMB) System," SAE Int. J. Passeng. Cars - Mech. Syst., pp. 1476-1483, 2013.

[13] Infineon Technologies, TC1798 User's Manual, 2009.

[14] Infineon Technologies, CIC61508 User's Manual, 2012.

[15] Infineon Technologies, SafeTcore Safety Driver, 2012.

Kyung-Jung Lee He received B.S. and M.S. degrees from Kookmin University. He is currently working towards the Ph.D. degree at Kookmin University. His research interests automotive electronic control and motor control.

Ki-Ho Lee He received the B.S. and M.S. degrees from Kookmin University. His research interests automotive electronic control and motor control.

Chanwoo Moon He received the B.S., M.S. and Ph.D. degrees from Seoul National University. His research interests are motor control and intelligent robot system.

Hyuk-Jun Chang He received the B.S. and M.S. degrees from Seoul National University. He was awarded the Ph.D. degree from Imperial College London. His research interests include nonlinear control theory and nonlinear systems

Hyun-Sik Ahn He received the B.S., M.S. and Ph. D. degrees in control and instrumentation engineering from Seoul National University. His research interests are automotive electronics, electronic chassis control, and motor control applications.