Transactions of KSAE, Vol. 28, No. 8, pp.515-520 (August, 2020)

pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2020.28.8.515

압력센서 Use Case 분석을 통한 SEooC 적용 연구

이 승 환*·박 병 규

에스피아이디 엔지니어링 사업본부

The Study on Application SEooC by Use Case Analysis of Pressure Sensor

Seunghwan Lee* • Byoungkyu Park

Engineering Division, SPID Co. Ltd., 145 Gasan digital1-ro, Geumcheon-gu, Seoul 08506, Korea
(Received 10 October 2019 / Revised 23 January 2020 / Accepted 10 April 2020)

Abstract : SEooC(Safety Element out of Context) is a method that assumes higher requirements in the application of automotive functional safety. To improve the quality of the assumed requirements, a method of applying SEooC through use case analysis is proposed. This study examined the basic SEooC methodology and defined how to apply the use case analysis method in detail. Through the case of developing a pressure sensor by applying SEooC, the upper requirements were derived by analyzing the use case. In addition, assuming system design, the internal safety requirements and requirements of use of SEooC target products were derived, and the hardware architecture was designed. When applying SEooC through use case analysis, the upper system can be defined and the safety goals, ASIL, and safety requirements can be derived based on clear evidence. In addition, the safety status and FTTI(fault-tolerant time interval) can be assumed in detail.

Key words : SEooC(에스이오오씨), ISO 26262 functional safety(기능 안전), Use case(사용 사례), Assumption(가정), Assumed safety requirement(가정된 안전 요구사항), TSR(기술안전요구사항), HSR(하드웨어 안전요구사항), AoU(사용의 가정), Architecture(아키텍처)

Nomenclature

GSN	: goal structuring notation
TSR	: technical safety requirement
HSR	: hardware safety requirement
HDL	: hardware description language
IP	: intellectual property
FMEA	: failure mode effect analysis
FTA	: fault tree analysis
DFA	: dependent failure analysis
FMEDA	: failure mode effect diagnostic analysis
HAM	: hardware architectural metric
PMHF	: probabilistic metric for random hardware failures
SPFM	: single point fault metric
LFM	: latent fault metric
FTTI	: fault tolerant time interval
FSR	: functional safety requirement
AoU	: assumption of use

1. 서 론

자동차 기능 안전(Functional Safety)을 구현하기 위하여 국제적인 표준(ISO 26262)이 수립되어 적용되고 있다. 이러한 적용에 대하여 적용 차종, ITEM 등이 명확하지 않고 적용되는 응용을 가정하여 기능안전을 수행하는 것을 SEooC(Safety Elements out of Context)[1-5]라고 한다. 안전 목표 및 안전 요구사항이 결정되거나 주어진 상태에서 개발하는 것을 In context에 의해 개발이라고 하고, 안전목표 및 안전 요구사항을 가정하여 개발하는 것을 Out of context라고 한다. SEooC는 여러 다른 응용과 여러 다른 고객을 위하여 일반적인 엘리먼트를 개발할 경우에 해당되며, 이것은 ITEM 개발과는 다른 조직에서 개발될 수 있다. SEooC로 개발되는 제품은 시스템, 서브시스템, 소프트웨어 컴포넌트, 하드웨어 컴포넌트, 하드웨어 파트(part) 등이 있다. 산업계 실무에 SEooC를 적용하기 위해 Opencoss platform을 이용하여 자체 프로세스를 수립

*Corresponding author, E-mail: shlee@espid.com

하여 적용[1]하고 있으며, GSN을 이용하여 프로세스를 수립하여 적용[2]하고 있다. 그러나 이러한 프로세스 측면의 접근도 SEooC 기능안전 수행에 필요하지만, SEooC를 상세하게 적용하기에는 어려움이 있으며, 특히 가정된 요구사항의 품질을 높일 수는 없다.[2]

본 논문에서는 SEooC를 적용하여 기능안전을 수행 시에 상위 요구사항을 가정하는 단계에서 가정된 상위 요구사항의 품질을 높이기 위한 Use Case 분석을 통한 SEooC 적용 방안에 대하여 제안하고자 한다.

2. SEooC 방법론

SEooC의 방법론을 이해하기 위해 SEooC로 하드웨어 컴포넌트를 개발할 경우를 살펴보면, Fig. 1 Hardware Component SEooC Process와 같은 프로세스[7,9]는 적용할 수 있다. 먼저 1)단계인 “Assumption on system level”에서 상위요구사항인 TSR(Technical Safety Requirement)를 가정한다. Hardware Component 입장에서는 최상위 요구사항은 TSR로 정의된다. 도출된 상위 요구사항에 따른 시스템 설계를 가정하여 SEooC 제품의 역할을 분석하고 설계하는데 유용한 도움을 줄 수 있다. 2)단계에서는 정의된 TSR을 구현하기 위해 Hardware Component의 내부 요구사항으로 Hardware Safety Requirement(HSR)을 도출한다. HSR은 Hardware component 내부의 안전 메커니즘(Safety mechanism)을 구현하기 위한 요구사항이다. 3)단계에서는 도출된 HSR을 구현하기 위한 설계 단계로서 하드웨어 아키텍처 설계와 하드웨어 상세설계를 실시한다. 반도체 컴포넌트 인 경우는 Chip design을 위한 HDL 설계가 해당되며, IP(Intellectual Property) 설계도 여기에 해당된다.

4)단계에서는 앞서서 설계된 하드웨어 설계를 검증하기 위해 안전분석을 실시한다. 안전목표를 위배하는 단일점 결함(Single Point Fault) 위주로 부석하는 FMEA (Failure Mode Effect Analysis),[10,11] 이중점 결함(Dual Point Fault)도 식별할 수 있는 FTA(Fault Tree Analysis),[12,13] 공통원인고장(Common Cause Failure)와 연계고장(Cascading Failure)을 분석하는 DFA(Dependent Failure Analysis)[8]를 실시한다. 5)단계에서는 하드웨어 우발고장(random hardware failure) 분석을 위하여 FMEDA(Failure Mode Effect Diagnostic Analysis)[14-16]을 실시한다. FMEDA 분석은 위험한 고장률의 비율을 분석하는 HAM(Hardware Architectural Metric)분석[7,14]과 위험한 고장률의 잔존량을 분석하는 PMHF(Probabilistic Metric for random Hardware Failures)[7,14]로 구성되어 있다. HAM은 단일점 결함의 비율을 분석하는 SPFM(Single Point Fault Metric)[7,14]

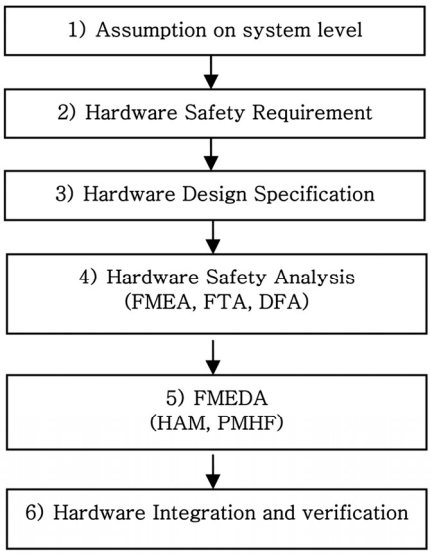

Fig. 1 Hardware component SEooC process

과 잠재결함의 비율을 분석하는 LFM(Latent Fault Metric)[7,14]을 분석하며, PMHF은 단일점 결함, 잔존 결함과 이중점 결함의 잔존량으로 분석한다. 6)단계에는 개발된 하드웨어가 하드웨어 안전 요구사항에 부합하는 것을 보장하기 위하여 하드웨어 수준의 통합 및 검증을 수행한다. 수행 방안으로는 하드웨어 안전 요구사항 구현의 완전성 및 정확성을 검증하는 시험[7]과 스트레스 상황에서의 내구성, 강건성 및 운용을 검증하기 시험[7]이 있다.

3. Use Case 분석 방법

SEooC 방법론을 적용하여 제품을 개발할 때, Assumption on system level 에서 상위 요구사항을 경험과 직관적으로 도출할 수 있지만, 품질이 높은 상위 요구사항을 도출하기 위해서는 Use Case 분석을 고려해야 한다. 이러한 Use Case는 아래와 같은 항목을 고려하여 분석할 수 있다.

- Use case ID
- Use case name
- Functionalities
- Input information
- Output information
- Parameters
- Assumed application system
- Assumed dangerous failure modes
- Assumed ASIL
- Assumed safety requirement
- Assumed safe state
- Assumed FTTI

Use case도 제품의 기능별로 여러 분석이 가능하기 때문에 고유의 ID가 필요하여 먼저, Use case ID를 정의한다. Use case 구분하기 위해 ID 뿐만 아니라 고유의 이름을 Use case Name으로 정의한다. SEooC를 적용하고자 하는 하드웨어 컴포넌트의 기능은 여러 개가 있을 수 있으며, 기능 별로 Use case를 분석하는 것이 적절하다. 해당 하드웨어 컴포넌트의 기능을 Functionalities에 정의를 한다. 그러한 기능이 구현되기 위한 입력 정보를 Input information에 정의하고, 출력 정보를 Output information에 정의한다. 해당 하드웨어 컴포넌트의 기능의 주요 인자를 Parameters에 정의를 한다. Assumed application system에서는 해당 하드웨어 컴포넌트가 사용되는 System(Item)을 정의한다. 상위 요구사항을 가정하기 위해서는 SEooC 컴포넌트가 사용되는 System(Item)을 가정해야 한다. Assumed dangerous failure modes에서는 SEooC 컴포넌트의 결함으로 인한 가정된 System(Item)의 위험한 고장을 정의한다. Assumed ASIL에서는 가정된 System(Item)의 위험한 고장으로 인한 운전자 상해의 정도(Severity), 그러한 위험한 상황의 노출정도(Exposure), 위험한 상황을 제어할 수 있는 정도(Controllability)를 고려하여 ASIL을 결정[6]한다. Assumed Safety Requirement에서는 앞서 정의한 System(Item)의 위험한 고장을 방지하기 위한 요구사항을 도출한다. 요구사항은 System (Item) 레벨의 안전 목표(Safety Goal)와 이를 만족하기 위한 SEooC 컴포넌트의 안전 요구사항을 도출한다. 여기서 도출한 SEooC 컴포넌트 안전 요구사항이 해당 하드웨어 컴포넌트의 Top 요구사항으로 TSR에 해당된다. Assumed Safe State는 위험한 상황을 방지하거나 회피하여 궁극적으로 도달하고자 하는 안전 상태를 정의한다. Assumed FTTI(Fault Tolerant Time Interval)은 위험한 결함을 감지하여 안전 상태까지 허용되는 시간을 정의하며, Application System 레벨과 Component 레벨을 정의해 준다.

4. Use Case 분석 사례

하드웨어 컴포넌트를 SEooC로 개발할 때 아래와 같이 Use Case 분석을 통한 SEooC 적용을 제시하고자 한다.

4.1 SEooC 대상 제품

SEooC로 개발될 제품은 압력 센서이며, 압력 센서의 주요 기능 ID와 기능은 아래 Table 1과 같다.

Table 1 Function of pressure sensor

Function ID	Function
FN.PRE.01	Measure the air pressure
FN.PRE.01	Transmits measured air pressure to serial communication

4.2 Use Case 분석

SEooc로 개발할 압력 센서에 대한 Use Case 분석은 Table 2와 같다. 압력 센서의 Use Case 분석 결과 압력 센서의 가정된 적용은 엔진 제어 장치의 입력 센서로 사용되며, 가정된 위험한 고장은 압력 센서 내부 부품의 결함으로 인한 잘못된 압력 측정 값을 ECU 쪽으로 출력하거나 외부 전기적 노이즈에 의해 압력 센서와 ECU의 통신 불가로 분석되었다. ASIL을 가정하기 위해 위험한 상황에 대한 시나리오를 예측해 보면 고속도로 운행시 압력 센서가 잘못된 압력 값을 전달하거나 압력 값을 전달하지 못하여 엔진 엔진 제어시스템의 공연비 제어 오동작으로 인하여 급가속이 발생하여 운전자의 생명에 위협을 줄 수 있다. 이러한 ISO 26262-3[3]에서 Hazardous events를 분류하면 생명에 위협을 주는 경우 Severity 3, 고속도로 노출인 경우, Exposure 4, 급가속의 상황을 운전자가 제어하기 어려운 경우, Controllability 3에 해당되어 ISO 26262-3,[6] Table 4 ASIL determination에 의해 ASIL B로 정의되며, 본 Use Case는 ASIL B로 가정된다. 이에 따른 엔진제어장치의 가정된 안전 목표는 “(SG.PRE.01) 의도하지 않은 급가속은 방지되어야 한다. (ASIL B)”로 도출되며, 압력 센서의 가정된 안전 요구사항은 “(TSR.PRE.01) 압력 센서의 잘못된 압력 출력신호가 방지되어야 한다. (ASIL B)”와 “(TSR.PRE.02) 압력 센서의 ECU 쪽으로 통신불가가 방지되어야 한다. (ASIL B)”로 도출된다. 본 Use Case의 초점은 압력 센서의 최상위 요구사항(TSR)을 도출하는 것이며, FSR(Functional Safety Requirement)는 생략했지만, 필요시 도출할 수도 있다. 결함이 발생하고 안전 상태까지 허용되는 시간(FTTI)는 엔진 제어 장치의 Application level은 1000 ms, 압력 센서 레벨은 10 ms로 가정한다. Use Case 분석을 통하여 압력 센서의 상위 요구사항이 가정되었다.

4.3 시스템 설계 가정

SEooC에 의해 압력 센서를 설계하는 데 있어 도출된 상위 요구사항에 따른 가정된 시스템의 아키텍처를 설계한다. 가정된 시스템은 엔진 제어시스템으로 특히 인터페이스를 세부적으로 설계하면 Fig. 2와 같다.

압력 센서는 엔진제어시스템에서 엔진에 흡입되는 공기의 압력을 계측하여 ECU에 전달함으로 ECU는 가속에 필요한 Fuel Injector를 통하여 연료 분사량을 제어하고 Ignition Coil을 통하여 점화시기를 제어한다.[17]

4.4 HSR 도출

Use Case를 통하여 도출한 TSR은 아래와 같으며, 이것은 SEooC 대상인 압력 센서에 할당된 안전 요구사항이 된다.

Table 2 Use case analysis of pressure sensor

Use case ID	UC.PRE.01
Use case name	Use case of pressure sensor
Functionalities	The pressure sensor measures the pressure of the air and transmits the data to serial communication.
Related function ID	FN.PRE.01, FN.PRE.02
Input	Air pressure
Output	Serial communication signal
Parameters	Air pressure (kpa)
Assumed application	- Assembled from the intake manifold of the engine, measured the pressure of the mass air flow and sent to the ECU. - Input sensor for engine control.
Assumed dangerous failure modes	- When the diaphragm inside the pressure element is damaged, the pressure is incorrectly measured and transferred to the ECU, and rapid acceleration or rapid acceleration due to incorrect control of the air-fuel ratio. - Unable to communicate to the ECU due to circuit loss caused by external electrical noise
Assumed ASIL	- Scenario: When the vehicle wants to turn left/right at a national highway intersection at a medium speed, the pressure sensor transmits the wrong pressure value, resulting in rapid acceleration or rapid acceleration due to misbehaving of the engine control system's air/fuel ratio, which causes rear-end/front collision with another vehicle, threatening the driver's life. - Severity: S3 (Rear/Front collision with another vehicle at medium speed threatens the driver's life) (cf. ISO26262-3, Table B.1) - Exposure : E2 (National Road Intersection) (cf. ISO26262-3, Table B.2) - Controllability: C3 (control is difficult or uncontrollable) (cf. ISO26262-3, Table B.6) - ASIL: B (cf. ISO26262-3, Table 4)
Assumed safety requirement	Application Level Safety Goal : (SG.PRE.01) Unintentional rapid acceleration shall be prevented. (ASIL B) Component Level Safety Requirement : (TSR.PRE.01) Incorrect pressure output signal from the pressure sensor shall be prevented. (ASIL B) (TSR.PRE.02) Communications failure to the ECU of the pressure sensor shall be prevented. (ASIL B)
Assumed safe state	Application Level: Eliminate rapid acceleration/sudden acceleration Component Level: Send error messages to the ECU through serial communication or recognize non-communication at the ECU
Assumed FTTI	Application Level FTTI : 1000 ms Component Level FTTI : 10 ms

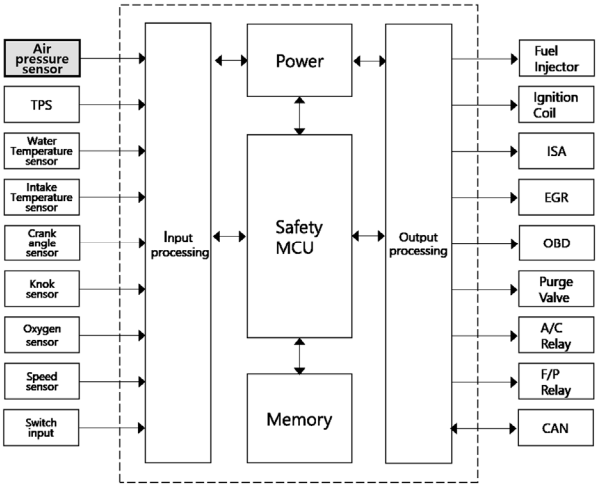

Fig. 2 Assumed system architecture

(TSR.PRE.01) 압력 센서의 잘못된 압력 출력신호가 방지되어야 한다. (ASIL B)

(TSR.PRE.02) 압력 센서의 ECU 쪽으로 통신불가가 방지되어야 한다. (ASIL B)

이러한 압력 센서의 안전 요구사항을 만족하기 위하여 압력 센서 내부 안전 요구사항, 즉 HSR(Hardware Safety Requirement)를 도출해야 한다. HSR은 주로 압력 센서 내부 구현되는 안전 메커니즘 위주로 도출하면 Table 3과 같다.

압력 센서가 외부 통신으로 오류 메세지를 전송하면 ECU가 받아서 시스템의 안전상태가 유지되도록 해야 한다. 그리고 ECU는 압력 센서와 Serial 통신이 두절되는 경우도 감지하여 안전상태를 유지해야 한다. 이것은 SEooC로 개발된 압력 센서를 사용함에 있어 필요한 요구사항이다. 이러한 요구사항을 AoU(Assumption of Use)[18]를 위한 요구사항으로 표현할 수 있으며 Table 4와 같다. 또는 Use Case 분석 시 가정된 요구사항(Assumed Safety Requirement)에서 ECU의 요구사항으로 도출될 수도 있다.

4.5 하드웨어 설계

도출된 HSR에 따라 압력 센서를 설계하면 Fig. 3의 아키텍처와 같다.

Table 3 3 HSR of pressure sensor

HSR ID	Requirement
HSR.PRE.01	The pressure sensor shall detect a fault in the power supply through under/over voltage monitoring and send an error message to the external communication.
HSR.PRE.02	The pressure sensor shall detect defects in the pressure sensing part and A/D through the self test and send an error message to the external communication.
HSR.PRE.03	The pressure sensor shall detect a fault in the DSP through the watchdog and send an error message to the external communication.
HSR.PRE.04	The pressure sensor shall detect a fault in the memory (ROM) through the ECC and send an error message to the external communication.
HSR.PRE.05	The pressure sensor shall detect a fault in serial communication through the CRC.

Table 4 AoU of pressure sensor

AoU ID	Requirement
AoU.PRE.01	The ECU connected to the pressure sensor shall receive data via serial communication and detect errors in the data transmitted over the CRC.
AoU.PRE.02	The ECU connected to the pressure sensor shall maintain the system in a safe state within xxx msec after receiving an error message via serial communication.
AoU.PRE.03	The ECU connected to the pressure sensor shall periodically communicate via serial communication, detect it when communication is lost, and keep the system safe in xxx msec.

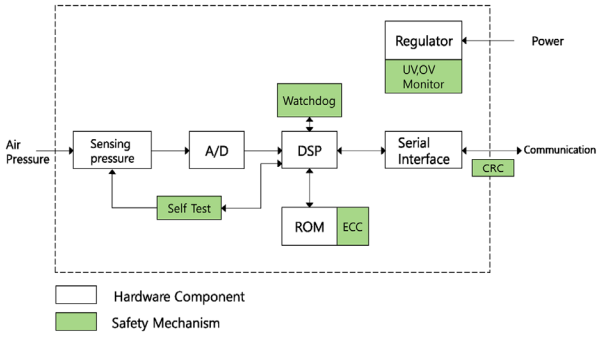

Fig. 3 Hardware architecture of pressure sensor

5. 결 론

본 논문에서는 SEooC를 적용하여 기능안전을 수행 시에 가정된 상위 요구사항의 품질을 높이기 위한 Use Case 분석을 통한 SEooC 적용 방안에 대하여 제시하였으며 다음과 같은 결론을 얻었다.

1) Use Case 분석을 통해 가정된 상위 시스템에 대한 정의와 발생할 수 있는 위험한 고장모드를 정의하여 분석할 수 있다.
2) Use Case 분석을 통해 명확한 근거를 기반으로 ASIL을 가정할 수 있다.
3) Use Case 분석을 통해 가정된 안전 목표와 안전요구사항을 도출할 수 있다.
4) Use Case 분석을 통해 가정된 안전 상태(Safe Sate)와 FTTI를 Application level와 Component level로 세부적으로 가정할 수 있다.

가정된 상위 시스템에서 SEooC 제품의 역할과 기능을 명확히하기 위해 시스템 아키텍처를 가정하여 설계하였으며, 가정된 상위 요구사항을 만족하기 위해 SEooC 제품의 내부 안전요구사항(HSR)을 도출하였고, 이 가운데 SEooC 제품을 사용함에 필요한 요구사항(AoU)을 도출하였다. 마지막으로 도출된 HSR에 따른 하드웨어 아키텍처를 제시하였다. Use Case 분석을 통해 적용된 SEooC 제품은 하드웨어 컴포넌트이지만, SEooC로 개발될 소프트웨어 컴포넌트, 시스템에도 적용 가능하며, 이에 대한 향후 적용 및 연구도 필요하다

References

1) A. Ruiz, A. Melzi and T. Kelly, “Systematic Application of ISO 26262 on a SEooC: Support by Applying a Systematic Reuse Approach,” Design, Automation and Test in Europe Conference and Exhibition, pp.393-396, 2015.
2) X. Larrucea, S. Mergen and A. Walker, “A GSN Approach to SEooC for an Automotive Hall Sensor,” EuroSPI 2016: Systems, Software and Services Process Improvement, pp.269-280, 2016.
3) I. Etxeberria-Agiriano, X. Larrucea, P. Gonzalez-Nalda, M. C. Otero and I. Calvo, “ISO26262 SEooC Compliance of a ROS Based Architecture,” Wseas Transactions on Systems, Vol.16, pp.53-63, 2017.
4) X. Larrucea, A. Walker and R. Colomo-Palacios, “Supporting the Management of Reusable Automo-

tive Software," IEEE Software, Vol.34, No.3, pp.40-47, 2017.
5) K. -J. Lee, Y. -H. Ki and H. -S. Ahn, "Automotive ECU Design with Functional Safety for Electro-Mechanical Actuator Systems," World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Vol.7, No.7, pp.912-917, 2013.
6) ISO 26262-3:2018, Road Vehicles Functional Safety Part 3: Concept Phase, 2nd Edn., 2018.
7) ISO 26262-5:2018, Road Vehicles Functional Safety Part 5: Product Development at the Hardware, 2nd Edn., 2018.
8) ISO 26262-9:2018, Road Vehicles Functional Safety Part 9: Automotive Safety Integrity Level (ASIL)-oriented and Safety-oriented Analyses, 2nd Edn., 2018.
9) ISO 26262-10:2018, Road Vehicles Functional Safety Part 10: Guidelines on ISO 26262, 2nd Edn., 2018.
10) H. H. Kim and N. H. Lee, "The Case Study on Software FMEA for the Efficient Improvement of Functional Safety," KSAE Annual Conference Proceedings, pp.1303-1308, 2012.
11) Y. K. Seo, D. H. Jung, S. S. Yu and W. Y. Rha, "The Optimization Study on the Test Method of Remanufactured Power Steering Oil Pump by Using FMEA," Transactions of KSAE, Vol.24, No.1, pp.90-98, 2016.
12) B. S. Seo and D. I. Lee, "Analysis of Electric Vehicle Fault Mode Using Fault Tree Analysis," KSAE Annual Conference Proceedings, pp.1239-1242, 2011.
13) J. J. Baek and K. W. Rhie, "Analysis of Safety and Importance for E/E/PE using RBD and FTA in ISO 26262," KSAE Annual Conference Proceedings, pp.1738-1742, 2009.
14) B. K. Park and S. H. Lee, "The Methods for Describe the Safety Mechanism and Estimate the Diagnostic Coverage in order to Conduct the Efficient FMEDA," Transactions of KSAE, Vol.26, No.6, pp.791-798, 2018.
15) B. C. Kim, "Evaluation of ISO 26262-5 Hardware Architectural Metrics and PMHF(Probabilistic Metric for Random Hardware Failures) using FMEDA," Auto Journal, KSAE, Vol.36, No.10, pp.26-38, 2014.
16) R. Inada, T. Hirotsu, Y. Morita and T. Hata, "Diagnostic Coverage Evaluation Method for Analog Circuits to Comply with Functional Safety Standards," SAE 2015-01-0267, 2015.
17) J. W. Sohn, W. T. Lee, P. J. Yoon, J. I. Lee and M. H. Sunwoo, "An Engine Management System Based on Real-time OS," KSAE Fall Conference Proceedings, pp.1052-1057, 2000.
18) ISO 26262-11:2018, Road Vehicles Functional Safety Part 11: Guidelines on Application of ISO 26262 to Semiconductors, 2nd Edn., 2018.