Transactions of KSAE, Vol. 29, No. 7, pp.609-620 (July, 2021)

Copyright © 2021 KSAE / 188-02
pISSN 1225-6382 / eISSN 2234-0149
DOI http://dx.doi.org/10.7467/KSAE.2021.29.7.609

〈응용논문〉

엑셀 페달 센서의 하드웨어 엘리먼트 평가 수행을 위한 SEooC 적용 사례 연구

박 병 규[*1] · 주 백 수[1] · 정 규 원[2] · 박 재 석[2]

에스피아이디 엔지니어링 사업본부[1] · 트루윈 선행연구팀[2]

A Case Study on The Application of SEooC to Evaluate Hardware Element for the Accel Pedal Sensor

Byoungkyu Park[*1] · Baegsu Joo[1] · Kyuwon Jung[2] · Jeasuok Park[2]

[1]*Engineering Division, SPID Co. Ltd., 145 Gasan Digital1-ro, Geumcheon-gu, Seoul 08506, Korea*
[2]*Advanced Research Team, TRUWIN Co. Ltd., 385 Expo-ro, Yuseong-gu, Daejeon 34051, Korea*
(Received 3 September 2020 / Revised 5 March 2021 / Accepted 15 March 2021)

Abstract : To perform a hardware element evaluation, hardware safety requirements in relation to the hardware element were identified. Nevertheless, in the automotive industry, performing hardware element evaluations without these hardware safety requirements can sometimes occur. To solve this problem, this paper proposed the SEooC technique, which is applied to the evaluation of the hardware element. To illustrate the proposed method, this paper introduced an example of a hardware element evaluation for the Accel Pedal Sensor by applying SEooC.

Key words : Accel pedal sensor(엑셀 페달 센서), Functional Safety(기능안전) ISO 26262(자동차 기능 안전성 국제표준), Evaluation of hardware elements(하드웨어 엘리먼트 평가), Safety elements out of context(컨텍스트 밖 안전 엘리먼트), Assumed context(가정된 컨텍스트), Assumed safety requirements(가정된 안전 요구사항), Quantitative safety analysis(정량적 안전 분석)

Nomenclature

APS : accel pedal sensor
ASIL : automotive safety integrity level
DC : diagnostic coverage
ECU : engine control unit
FM : failure mode
FMEDA: failure modes effects and diagnostics analysis
FSR : functional safety requirement
FHTI : fault handling time interval
FTTI : fault tolerant time interval
HAM : hardware architecture metric
HARA : hazard analysis and risk assessment
HSR : hardware safety requirement
MPFDI : multiple-point fault detection time interval
NA : not applicable
PMHF : probabilistic metrics for random hardware failure
QM : quality management
SEooC : safety elements out of context
SG : safety goal
SM : safety mechanism
TSR : technical safety requirement

Subscripts

O. Time : operation time
PPS 1 : APS output signal 1
PPS 2 : APS output signal 2

1. 서 론

ISO 26262-8:2018, 13절의 하드웨어 엘리먼트 평가는 기능안전 ISO 26262 표준을 준수하여 개발되지 못한

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

QM 수준의 하드웨어 엘리먼트가 기능안전 ISO 26262 표준을 준수하여 개발하고자 하는 아이템, 시스템 또는 엘리먼트의 일부로서 사용(통합)할 때 그 하드웨어 엘리먼트가 사용(통합)에 적합하다는 증거를 제공하기 위한 것이다.[1,2] 이러한 하드웨어 엘리먼트 평가는 아이템이 정의되어 있는 어플리케이션 컨텍스트 내에서 수행되어야 함으로,[1] 대게 아이템으로부터 도출되어 하드웨어 엘리먼트로 할당된 안전 요구사항을 기반으로 평가를 수행하게 된다. 하지만, 자동차 산업 현장에서는 때때로 평가 대상 하드웨어 엘리먼트에 대한 특정 하드웨어 안전 요구사항이 없이, 단지 '기능안전 ISO 26262 표준을 준수하여 특정 ASIL 수준을 만족 할 것'이라는 매우 포괄적이고 모호한 요구사항만 주는 경우가 있다.[2] 사실 이 경우는 요구사항 개발 및 관리에 있어서 적절하지 못한 사례이다. 왜냐하면, 하드웨어 안전 요구사항에 따른 분석 및/또는 시험(기능, 성능, 신뢰성 시험)을 수행해야만 이 평가 대상 하드웨어 엘리먼트가 적절한 기능적 성능을 가지고 있어, 이러한 하드웨어 엘리먼트를 적용하려는 아이템 또는 시스템의 하드웨어 설계에서 의도된 기능을 제공하는데 적합하다는 증거를 제공할 수 있기 때문이다.[1,2] 그럼으로 평가 대상 하드웨어 엘리먼트에 주어진 하드웨어 안전 요구사항 없이는 평가 수행이 어렵다. 하지만 그러함에도 불구하고, 이러한 사례는 자동차 시장에 적절한 시기의 제품 출시 요구와 더불어 수많은 다양한 제품의 개발을 위해 종종 직면하게 되는 상황이기도 하다. 이러한 상황을 그나마 적절히 대처할 수 있는 수단이 ISO 26262-10에서 제시된 SEooC방안[3]이다. SEooC 기법을 적용함으로써, 하드웨어 엘리먼트 평가 수행을 위한 하드웨어 안전 요구사항을 생성할 수 있다.

SEooC는 말 그대로, 안전 관련 엘리먼트를 컨텍스트 밖에서 개발하는 것을 말한다.[3] 여기서 컨텍스트 밖(Out of context)이란 적용되는 차종 및 아이템이 명확하지 않는 상태에서 설계에 대한 적절한 가정(Assumption)을 통해 안전 요구사항을 도출하여 기능 안전을 수행하는 것을 말한다.[3,4] 이와 반대되는 경우가 컨텍스트 내(In context)이다. 이 경우는 차종 및 아이템이 명확하고 이에 따른 안전 목표 및 안전 요구사항이 주어진 상태로서 기능안전 ISO 26262 표준을 준수하는 개발의 일반적인 형태이다.[4] 하지만, 범용 엘리먼트의 개발과 같은, 어느 특정 안전 관련 엘리먼트는 종종, 최종적으로 적용될 차종 및 아이템에 대한 정보를 정확하게 알 수 없는 경우가 발생하게 되는데, 이러한 상황을 적절하게 대처하기 위한 수단으로 컨텍스트 밖(Out of context) 기법을 활용한다.[3,4] 물론, SEooC가 하드웨어 엘리먼트 평가를 위해 제안된 것은 아니나, 자동차 메이커 또는 시스템 통합 업체로 부터 주어진 하드웨어 안전 요구사항이 없는 하드웨어 엘리먼트 평가에도 응용이 가능하다.

본 논문에서는 기능안전 ISO 26262 표준을 준수하여 개발되지는 않았으나, 지난 십 수년간 자동차 시장에서 문제없이 사용해 왔던 APS 센서에 대하여 SEooC 기법을 적용한 하드웨어 엘리먼트 평가 방안을 제시한다. 이를 위해서, 특정 어플리케이션 컨텍스트를 가정하여 APS 센서 수준의 하드웨어 안전 요구사항을 도출하고, 도출된 하드웨어 안전 요구사항에 기반한 하드웨어 엘리먼트 평가 수행 과정을 설명한다.

2. 용어 정의

APS 센서에서 사용되는 주요 용어를 다음과 같이 정의하였다.

Table 1 Term & description

Term	Description
Idle	· State of maintaining the vehicle with minimum force to prevent the engine from turning off.
WOT (wide open throttle)	· State of fully open the Throttle valve in order to enable internal combustion with maximum output. · APS output no longer increases when pedal is pressed above the limit.
PPS	· Output voltage of APS sensor · The ECU recognizes the APS sensor output value as % unit using the formula below. $\frac{\text{APS output voltage}}{\text{APS input voltage (supplied by the ECU)}} \times 100\ (\%)$
Limp-home mode	· Mode to limit engine RPM by ECU (RPM does not increase above a certain level)

3. 하드웨어 엘리먼트 평가 대상

평가 대상 하드웨어 엘리먼트는 Fig. 1에서 나타낸 바와 같이 차량의 가속 페달에 장착되어 운전자의 가속 의지를 전자 신호 형태로 출력하는 APS(Accel Pedal Sensor) 센서이다.

안전상의 이유로 출력은 완전히 분리된 두 개의 아날

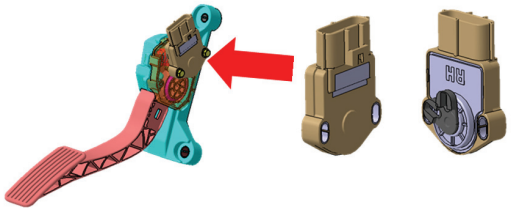


Fig. 1 Accel pedal assy & Accel pedal sensor

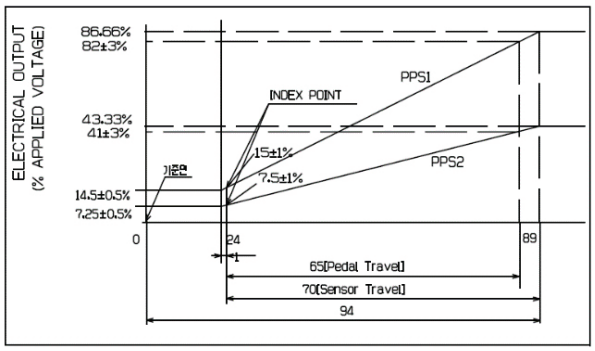


Fig. 2 APS sensor output graph

로그 출력인 PPS 1과 PPS 2를 가진다. PPS 2의 출력은 PPS 1의 1/2이다. 이는 두 출력 간의 상관관계를 통해 APS 센서에 대한 유효성을 ECU가 확인하기 위함이다. Fig. 2는 APS 센서의 페달 각도에 따른 PPS 1과 PPS 2에 대한 출력 그래프이다. Table 1에 기술된 PPS에 대한 설명에 보다시피 PPS 전압 값의 범위는 ECU로부터 공급받은 전압에 따라 달라진다.

4. 어플리케이션 컨텍스트의 가정

APS 센서에 대한 안전 요구사항을 명세하기 위하여 SEooC 기반의 가정(Assumption)[3]을 통해 아이템을 정의하고 HARA 분석[5]을 수행한다. APS 센서의 최종 어플리케이션은 엔진 제어시스템이다. HARA 분석[5]의 결과로 안전 목표가 도출되고 ASIL 등급이 지정되었다면, 안전 목표로 부터 파생된 FSR 및 TSR을 명세한다. 이후 명세 된 TSR로 부터 APS 센서에 대한 안전 요구사항은 명세 되어진다.

단, 적절하지 못한 가정은 잘못된 하드웨어 엘리먼트 평가로 이어지게 됨으로 주의해야 한다.

4.1 아이템의 가정

4.1.1 아이템 정의

Fig. 3은 아이템의 아키텍처를 나타낸 그림이다. APS 센서가 적용될 아이템은 각종 센서로 부터 수집된 정보를 분석하여 엔진의 출력을 최적의 상태로 제어하는 엔진 제어 시스템이다.

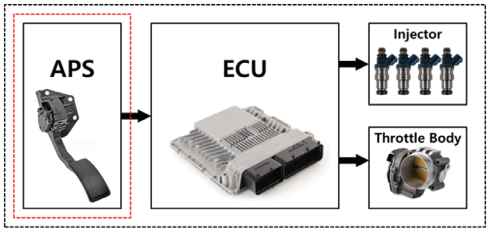


Fig. 3 ITEM architecture

4.1.2 아이템의 주요 기능

① 차량의 엔진 출력 증가 기능:
운전자의 가속 의지를 반영하여 차량의 엔진 출력을 증가시킴.

a. APS 센서의 증가된 회전각에 상응하는 만큼 Throttle Body의 열림을 증가시킨다.
b. APS 센서의 증가된 회전각에 상응하는 만큼 Injector의 연료 분사를 증가시킨다.

② 차량의 엔진 출력 감소 기능:
운전자의 감속 의지를 반영하여 차량의 엔진 출력을 감소시킴.

a. APS 센서의 감소된 회전각에 상응하는 만큼 Throttle Body의 열림을 감소시킨다.
b. APS 센서의 감소된 회전각에 상응하는 만큼 Injector의 연료 분사를 감소시킨다.

4.2 위험원 분석 및 리스크 평가

위험원 분석 및 리스크 평가인 HARA 분석[5]을 통해 APS 센서가 적용될 아이템의 안전 목표와 ASIL 등급을

Table 2 HARA analysis results 1 for APS

	Contents
Functional unit	APS(Accel Pedal Sensor)
Feature under consideration	When the driver presses the accel pedal, the driver's willingness to accelerate is transmitted to the ECU according to the angle at which the pedal moves.
Hazard	Unintended maximum of the APS output during pedal operation by the driver. (Unintended work)
Effect of the failure	The maximum output of the APS, regardless of the driver's willingness, can be a danger to the driver, nearby vehicles, and pedestrians.
Scenario	Mid-speed driving on city roads (>30 km/h, <80 km/h)
Severity	S3
Comment for severity	Difficult to avoid due to rapid acceleration. Life threat from vehicle and object collision during speeding.
Exposure	E4
Comment for exposure	>10 % of average operating time
Controllability	C1
Comment for controllability	The driver can avoid dangerous situations by reducing the speed by pressing brake pedal after recognizing rapid acceleration.
ASIL	B

Table 3 HARA analysis results 2 for APS

	Contents
Functional unit	APS(Accel Pedal Sensor)
Feature under consideration	When the driver releases the accel pedal, the driver's willingness to decelerate is transmitted to the ECU according to the angle at which the pedal moves.
Hazard	Unintended minimum of the APS output during pedal operation by the driver. (Unintended Stop)
Effect of the failure	Vehicle speed can be reduced due to the minimum of APS output regardless of the driver's willingness. Eventually, it can be a danger to nearby vehicles.
Scenario	High-speed driving on highway (>80 km/h)
Severity	S3
Comment for severity	Life threat from collision with rear vehicle due to unintentional speed drop when driving at high speed
Exposure	E4
Comment for exposure	>10 % of average operating time
Controllability	C1
Comment for controllability	The driver can avoid dangerous situations by moving to the shoulder of a road and turn-on the hazard warning lamp after recognizing a rapid deceleration.
ASIL	B

가정한다. 엔진 제어 시스템에서의 위험원은 APS 센서 결함이며, 리스크는 이로 인한 주행 중 의도치 않는 차량의 가속 또는 감속에 따른 차량 추돌이다. Table 2와 Table 3은 APS 센서에 대한 HARA 분석 내용을 보여준다. 참고로 HARA 분석에 대한 수행 절차 및 방안은 ISO 26262-3:2018[5]에 자세히 설명되어 있다.

4.3 안전 목표 및 ASIL 등급

4.2 HARA 분석[5]의 결과로 다음과 같은 안전 목표(SG) 및 ASIL 등급을 도출하였다.

Table 4 Safety goal and ASIL level

ID	Requirement	ASIL
SG1	Unintentional increase in engine power must not be allowed.	B
SG2	Unintentional reduction in engine power must not be allowed.	B

4.4 안전 상태 및 FHTI

APS 센서 고장이 발생한 경우라도 엔진 제어시스템에 대한 리스크가 비합리적인 수준이 없는 운영 모드인 안전 상태(Safe state)는 Table 5에 나타나 있다. 그리고, APS 센서 결함으로 부터 엔진 제어시스템이 안전 상태로 도달하기까지의 시간인 FHTI(결함 처리 시간 간격)는 500 ms 로 가정하였다.

아래 Table 5에서 나타낸 바와 같이 안전 상태 및 FHTI 시간은 SG1과 SG2에 대해 동일하다.

Table 5 Safety status and FHTI

ID	Safe state	FHTI
SG1	· Warning lamp ON (cluster indicate) · Limp-home Mode	500 ms
SG2		

4.5 기능 안전 요구사항

'4.3 안전 목표 및 ASIL 등급'에서 정의된 안전 목표로 부터 기능 안전 요구사항을 도출하여 명세한다.[5] ASIL 분해는 적용하지 않는다. 모든 FSR에 대한 ASIL등급은 B이며, Safe state 및 FHTI는 '4.4 안전 상태 및 FHTI'와 같다.

4.5.1 ID: FSR_APS_01

운전자의 가속 의지에 따라 엔진 출력을 증가하여야 한다. (Related SG: SG2)

4.5.2 ID: FSR_APS_02

운전자의 감속 의지에 따라 엔진 출력을 감소하여야 한다. (Related SG: SG1)

4.5.3 ID: FSR_APS_03

장치는 모니터링 되어야 하며, 문제 발생시 적절한 조치를 취하여야 한다. (Related SG: SG1, SG2)

4.5.4 ID: FSR_APS_04

장치는 내외부로 부터의 잡음 및 스트레스로 부터 강건해야 한다. (Related SG: SG1, SG2)

4.6 기술 안전 요구사항

'4.5 기능 안전 요구사항'으로 부터 기술 안전 요구사항을 도출하여 명세한다.[6] ASIL 분해는 적용하지 않는다. 모든 TSR에 대한 ASIL등급은 B이다.

4.6.1 ID: TSR_APS_01

ECU는 APS 센서로부터 독립적이고 이중화 된 두 개

의 아날로그 입력을 받아야 한다. (Related FSR: FSR_APS_01, FSR_APS_02)

4.6.2 ID: TSR_APS_02

ECU는 APS 센서의 이중화 된 두개의 아날로그 신호 입력에 따라 엔진 출력을 제어하여야 한다. (Related FSR: FSR_APS_01, FSR_APS_02)

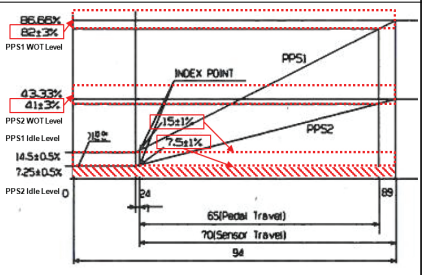
4.6.3 ID: TSR_APS_03

ECU는 APS 센서를 모니터링하여 이상 발견 시 경고 등을 점등하고 엔진 출력 상태를 Limp-home Mode로 전환시켜야 한다. (Related FSR: FSR_APS_03)

4.6.4 ID: TSR_APS_04

APS 센서는 페달 회전 범위에 상응하는 두 개의 서로 독립된 아날로그 출력을 ECU로 전달해야 한다. (Related FSR: FSR_APS_01, FSR_APS_02)

Table 6 Assumption for external safety mechanism 1

ID	E_SM_APS_01		
Name	APS output validity monitoring		
O. Time	200 ms	Implementation part	SW
Safe Status	Warning lamp ON and Limp-home Mode		
Purpose	To check the validity of the APS output signals.		
Relative SG	SG1, SG2		
Relative TSR	TSR_APS_03, TSR_APS_05		
Defense against failure modes	Out of Range (Under & Over)		
Claim to DC (%)	・If 'Out of Range Under' occurs, the ECU will detect it 99 %. ・If 'Out of Range Over' occurs, the ECU will detect it 99 %.		
SM type	Avoid to single point fault		
Architecture			
Description	Monitoring whether the APS output signals are outside the effective range. ・PPS 1 Under : 15 % under ・PPS 1 Over : 82 % excess ・PPS 2 Under : 7.5 % under ・PPS 2 Over : 41 % excess		

4.6.5 ID: TSR_APS_05

APS 센서는 출력 신호의 유효성을 보장 하기 위해서 유효한 출력 범위 값을 가져야 하며, 독립된 두 출력 간에는 서로 상관관계가 있어야 한다. (Related FSR: FSR_APS_03)

4.6.6 ID: TSR_APS_06

APS 센서는 내외부로 부터의 잡음 및 스트레스로 부터 강건해야 한다. (Related FSR: FSR_APS_04)

4.7 외부 안전 메커니즘의 가정(Assumption)

하드웨어 엘리먼트 평가 대상인 APS 센서는 내부 진단을 위한 안전 메커니즘이 없다. 그럼으로 ECU는 APS 센서의 출력 신호 품질에 문제가 없음을 보장하기 위하여 필연적으로 APS 센서를 모니터링 하고, 모니터링 결과에 따른 조치를 수행하여야 한다. APS 센서 입장에서 ECU의 이러한 행위는 외부 안전 메커니즘에 해당된다. Tables 6~8에 나타난 바와 같이 3가지의 외부 안전 메커니즘이 ECU 측에 구현되어 있을 것으로 가정한다.

Table 7 Assumption for external safety mechanism 2

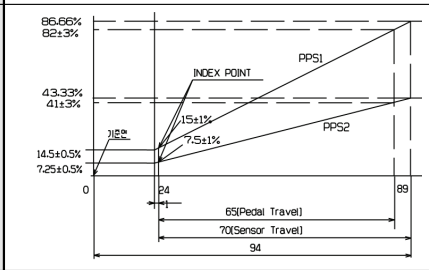
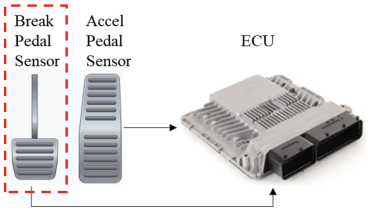
ID	E_SM_APS_02		
Name	Monitoring correlation between two output signals		
O. Time	200 ms	Implementation part	SW
Safe status	Warning lamp ON and Limp-home Mode		
Purpose	To check whether the APS is abnormal status through the correlation between the two output signals.		
Relative SG	SG1, SG2		
Relative TSR	TSR_APS_03, TSR_APS_05		
Defense against failure modes	Stuck in range / Offset / Drift		
Claim to DC (%)	・If 'Stuck in range' occurs, the ECU will detect it 90 %. ・If 'Offset/Drift' occurs, the ECU will detect it 90 %.		
SM type	Avoid to single point fault		
Architecture			
Description	・Monitoring whether the correlation between the two output signals exceeds the specifications below. $\text{Correlation} = \frac{\text{PPS1}}{2} - \text{PPS2} < 1.0\,(\%)$		

Table 8 Assumption for external safety mechanism 3

ID	E_SM_APS_03		
Name	Monitoring sensor faults by other sensors		
O. Time	200 ms	Implementation part	SW
Safe status	Warning lamp ON and Limp-home Mode		
Purpose	If the APS output signals are 'Stuck' within the effective range, to check whether fault of APS by using other sensors.		
Relative SG	SG1, SG2		
Relative TSR	TSR_APS_03		
Defense against failure modes	Stuck in range		
Claim to DC (%)	· In the case of a 'Stuck in range' fault, the worst-case scenario is that the correlation between the two outputs is maintained. · Generally, in this case, the ECU cannot detect a fault with the APS sensor. · However, if the brake switch signal is used, the ECU will detect 60 % of APS sensor fault.		
SM type	Avoid to multiple point fault		
Architecture			
Description	· The ECU determines whether there is a fault with the APS sensor compared to other sensors connected to the vehicle, such as the brake sensor. · Ex) If the APS output signals are Stuck at a 50 % output, the vehicle will drive according to the 50 % output. At this time, when the driver presses the brake pedal for deceleration, the ECU recognizes that the accel pedal and the brake pedal are simultaneously pressed, then determines that the APS is malfunctioning. In addition, even if the brake pedal is pressed, if the APS sensor signal output remains the same for a certain period of time, it may be determined that the APS is malfunctioning.		

4.8 하드웨어 안전 요구사항

'4.6 기술 안전 요구사항'으로 부터 하드웨어 안전 요구사항을 도출하여 명세한다.[7] ASIL 분해는 적용하지 않는다. 모든 HSR에 대한 ASIL등급은 B이다. 다음의 Tables 9~13은 APS 센서에 대한 하드웨어 안전 요구사항을 명세한 것이다.

Table 9 Hardware safety requirement 1 for APS

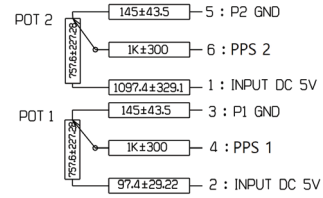
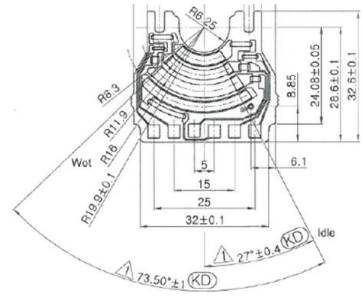
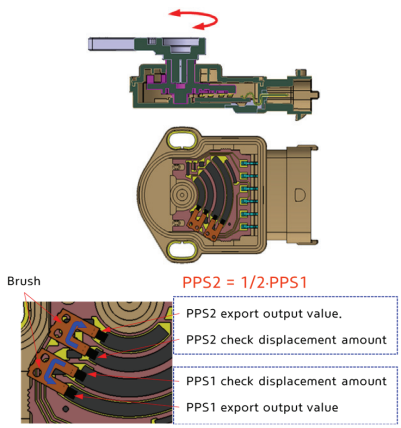
Status	☐ Proposed ☐ Assumed ☒ Accepted		
ID	HSR_APS_01	Related TSR	TSR_APS_02, TSR_APS_04
HSR	The sensor shall have a variable output depending on the rotational displacement of the accelerator pedal.		
Satisfaction condition	· Carbon track shall have the following resistance values.  · The Carbon Track shall be printed as shown in the following drawings in order to ensure that the resistance values are variable according to the rotational displacement of the accelerator pedal. 		
Related SM	NA		
O. Time	Immediately	MPFDI	NA
Limit range	The resistance value error of each carbon track shall be within 30 %.		
Constraints	Carbon track must be applied uniformly to ensure linearity when printing.		
Expected fault or malfunction	· Carbon Track print poor. · Damage and departure of Brush. · Open circuit, short circuit of pattern printed on PCB. · Output signal different from pedal displacement.		
Hardware architecture			
Verification method	· Review : PCB drawing review · Testing : Check the resistance value.		

Table 10 Hardware safety requirement 2 for APS

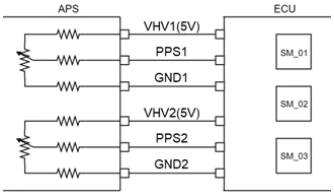
Status	☐ Proposed ☐ Assumed ☒ Accepted		
ID	HSR_APS_02	Related TSR	TSR_APS_01, TSR_APS_02, TSR_APS_04
HSR	Sensors shall have physically separate power inputs for independent and redundant outputs.		
Satisfaction condition	Power-line of output 1 and Power-line of output 2 should be separated from each other.		
Related SM	NA		
O. Time	NA	MPFDI	NA
Limit range	NA		
Constraints	The sensor shall have at least 6 connector pins in order to have physically separated power terminals.		
Expected fault or malfunction	・Carbon Track print poor ・Open circuit, short circuit of pattern printed on PCB		
Hardware architecture			
Verification method	・Review : PCB drawing review ・Testing : Functional test		

Table 11 Hardware safety requirement 3 for APS

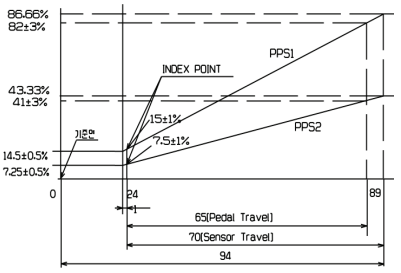
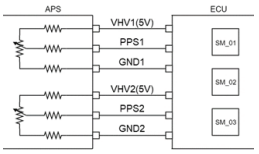
Status	☐ Proposed ☐ Assumed ☒ Accepted		
ID	HSR_APS_03	Related TSR	TSR_APS_03, TSR_APS_05
HSR	For the ECU to determine whether the sensor is abnormal according to the correlation between the two outputs, PPS 2 (output 2) must have a value of 50 % (less than 1.5 % tolerance) of PPS 1 (output 1).		
Satisfaction condition	・The two outputs shall be physically completely separated. ・The output specifications are as follows. 		
Related SM	E_SM_APS_02		
O. Time	Immediately	MPFDI	200 ms
Limit range	・Do not deviate from the output specifications		
Constraints	・To prevent damage to the Brush, print a carbon track with a 70° displacement that is wider than the rotational displacement of the pedal. ・The ECU must make a judgment for a fault that has a broken correlation between the two outputs.		
Expected fault or malfunction	・Output signal different from pedal displacement. ・The correlation between the two outputs is broken		
Hardware architecture			
Verification method	・Review : PCB drawing review ・Testing : Functional and Performance Test		

Table 12 Hardware safety requirement 4 for APS

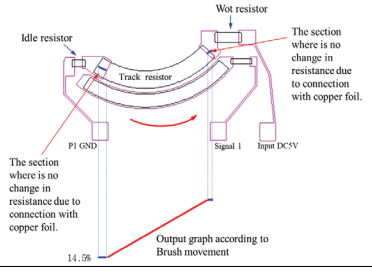
Status	☐ Proposed ☐ Assumed ☒ Accepted		
ID	HSR_APS_04	Related TSR	TSR_APS_03, TSR_APS_05
HSR	APS shall have an Idle/WOT Level so that the ECU can recognize the failure of the sensor. (If output is below Idle level or above WOT level, the ECU determines that the sensor has failed.)		
Satisfaction condition	The two outputs of the sensor must meet the following Idle level and WOT level. Idle / WOT PPS1: source voltage * 15% / source voltage * 82% PPS2: source voltage * 7.5% / source voltage * 41%		
Related SM	E_SM_APS_01		
O. Time	Immediately	MPFDI	NA
Limit range	・Idle level tolerance rate : ± 1 % ・WOT level tolerance rate : ± 3 %		
Constraints	It is the ECU's responsibility to determine APS failures of deviant the tolerance rate for the Idle level and the WOT level.		
Expected fault or malfunction	・Out of tolerance rate of Idle level ・Out of tolerance rate of WOT level		
Hardware architecture			
Verification method	・Review : PCB drawing review ・Testing : Functional and performance test		

Table 13 Hardware safety requirement 5 for APS

Status	☐ Proposed ☐ Assumed ☒ Accepted		
ID	HSR_APS_05	Related TSR	TSR_APS_06
HSR	The APS shall meet the specifications of ES 35190-02 to demonstrate robustness from internal and external noise and stress.		
Satisfaction condition	Must meet ES 35190-02 specification.		
Related SM	NA		
O. Time	NA	MPFDI	NA
Limit range	NA		
Constraints	NA		
Expected fault or malfunction	ES 35190-02 Specification meet fail.		
Hardware architecture	NA		
Verification method	・Testing: Reliability test		

5. 하드웨어 엘리먼트 평가 수행

‘4.8 하드웨어 안전 요구사항’을 기반으로 APS 센서에 대한 하드웨어 엘리먼트 평가를 수행한다. APS 센서는 내부 고장을 제어 또는 검출하기 위한 자체 안전 메커니즘이 없음으로 ISO 26262-8:2018, 13절에 따라 Class Ⅱ로 분류된다.[1] 이에 따라 평가는 분석과 시험을 적절히 선택하여 수행한다.[1]

5.1 하드웨어 엘리먼트 평가 계획 및 시험 계획

ISO 26262-8:2018, 13.4.3.2 절에 따라 하드웨어 엘리먼트 평가 계획서를 작성하고, ISO 26262-8:2018, 13.4.3.5 절에 따라 하드웨어 엘리먼트 시험 계획서를 작성한다.[1] 시험 계획서에는 ‘4.8 하드웨어 안전 요구사항’ 기반으로 기술된 테스트 케이스 명세를 포함시킨다. 본문에는 지면상의 이유로 APS 센서에 대한 하드웨어 엘리먼트 평가 계획서 및 시험 계획서를 생략하였다. 참고로 이와 관련된 세부적인 절차 및 내용은 ‘하드웨어 엘리먼트 평가에 의한 하드웨어 통합의 이해와 사례 연구[2]’를 참조하기 바란다.

5.2 시험에 의한 하드웨어 엘리먼트 평가 수행

‘5.1 하드웨어 엘리먼트 평가 시험 계획’에 따라 시험에 의한 하드웨어 엘리먼트 평가를 수행하여 시험 결과서를 작성한다.[1] 시험에는 가정된 요구사항에 따른 기능 및 성능 시험과 환경 시험을 포함하는 신뢰성 시험이 있다.[2]

5.3 고장 모드 및 고장 시나리오

하드웨어 고장 분석을 수행하기에 적합한 정보를 제공하기 위하여 평가 대상인 APS 센서에 대한 고장 모드 및 고장 시나리오를 기술한다. 이를 위해 ISO 26262-5, Annex Table D.1[7]과 ISO 26262-11, Table 53[8]을 참조하였으며, 전문가의 현장 경험을 최종 반영하여 기술 하였다. Table 14와 Table 15는 APS 센서 출력인 PPS 1과 PPS 2에 대한 고장 모드 및 고장 시나리오를 보여준다.

Table 14 Failure mode and failure scenario for PPS 1

ID	FM	Scenario
FM1	Out of range (under)	· Output is lower than Idle Level (14.5 %) due to PPS 1 and GND being shorted. (GND short) · Power or/and PPS 1 signals are open.
FM2	Out of range (over)	· Output is higher than WOT Level (82 %) due to PPS 1 and Battery/VHV1 being shorted. (Power source short) · GND open.
FM3	Stuck in range	· Output is fixed to a random value within the effective range of 14.5 % to 82 % due to damage or/and departure of PPS 1 brush.
FM4	Offset	· Offset occurs due to positional deviation of PPS 1 Brush. · Variation of resistance value due to damage of PPS 1 Carbon Track. Eventually, an offset occurs.
FM5	Drift	· Variation of resistance value due to damage of PPS 1 Carbon Track. Eventually, a drift occurs.

Table 15 Failure mode and Failure scenario for PPS 2

ID	FM	Scenario
FM6	Out of range (under)	· Output is lower than Idle Level (14.5 %) due to PPS 2 and GND being shorted. (GND short) · Power or/and PPS 2 signals are open.
FM7	Out of range (over)	· Output is higher than WOT Level (82 %) due to PPS 2 and Battery/VHV2 being shorted. (Power source short) · GND open.
FM8	Stuck in range	· Output is fixed to a random value within the effective range of 14.5 % to 82 % due to damage or/and departure of PPS 2 brush.
FM9	Offset	· Offset occurs due to positional deviation of PPS 2 Brush. · Variation of resistance value due to damage of PPS 2 Carbon Track. Eventually, an offset occurs.
FM10	Drift	· Variation of resistance value due to damage of PPS 2 Carbon Track. Eventually, a drift occurs.

5.4 정량적 안전 분석

하드웨어 우발 고장에 대한 정량적 평가는 아이템 수준에서 평가되어야 함으로, 일반적으로 하드웨어 엘리먼트 평가 수준에서 이루어지는 것은 아니다.[1,2,6] 하지만, 본 논문에서는 SEooC 기법[3]을 적용하여 어플리케이션 컨텍스트를 가정하였을 뿐만 아니라, 이러한 상황에서 APS 센서를 적용할 것으로 기대 하였기 때문에 가정된 아이템 수준의 APS 센서에 대한 정량적 평가를 수행하였다.

5.4.1 기본 고장율(Base Failure Rate) 산출

정량적 안전 분석을 수행하기 위하여 APS 센서의 두 출력 단인 PPS 1과 PPS 2에 대한 기본 고장율 값을 산출한다. 기본 고장율 계산은 ‘IEC TR 62380, 11.7 Non wire wound cermet potentiometer(one or several turn)’에 근거하였고, 미션 프로파일은 ‘IEC TR 62380: Table 11- Mission profiles for automotive’를 적용하였다.[9] 그리고 보수적으로 계산하기 위하여 De-rating factor의 τ_{off}를 ‘0’으로 적용하였으며, 계산 수식은 다음과 같다.[9] 단, 계산 과정은 생략하였다.

$$\lambda = 0.3 \times \left(\left[\frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right] \times \pi_Y + 1.2 \times 10^{-3} \times \left[\sum_{i=1}^{j} (\pi_n)_i \times (\Delta T_i)^{0.68} \right] \right) \times 10^{-9} / h$$

① PPS 1의 기본 고장율 값

0.3* (3.9634* 1 + 1.2 * 10^{-3}* 3038.541) = **2.283** Fit

② PPS 2의 기본 고장율 값

0.3* (6.3298* 1 + 1.2* 10^{-3}* 3038.541) = **2.993** Fit

5.4.2 FMEDA 수행

SG1과 SG2에 대한 FMEDA를 수행한다. 차량 수명 시간 $T_{Lifetime}$은 10만 시간(차량의 년중 운행시간인 500 h[9] X 차량의 수명 시간인 20년 X 보수적으로 평가하기 위해서 10배를 곱해 줌)으로 하였다. 다음의 Fig. 4, Fig. 5는 SG1과 SG2에 대한 FMEDA 수행 결과를 보여주는 FMEDA 결과서이다. 참고로 FMEDA 분석 기법에 관한 참고할 만한 문헌은 ISO26262-5: 2018 Annex E[7]와 ISO26262-11:2018 Annex C, Annex D[8]이다.

5.5 하드웨어 엘리먼트 평가 결과

ISO 26262-8:2018, 13.4.3.6 절을 참조하여 하드웨어 엘리먼트 평가 결과서를 작성한다.[1] 다음은 APS 센서에 대한 평가 결과이다.

① SG1 - 의도하지 않은 엔진 출력의 증가는 방지되어야 한다.

	Component Name	Base Failure rate/FIT**		Safety-related component to be considered in the calculations?	Failure Mode	Failure rate distribution	Failure mode that has the potential to violate the safety goal in absence of safety mechanisms?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal?	Failure mode coverage wrt. violation of safety goal	Single-Point Fault failure rate/FIT	Residual Fault failure rate/FIT	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component?	Detection means? Safety mechanism(s) allowing to prevent the failure mode from being latent?	Failure mode coverage with respect to latent failures	Latent Multiple-Point Fault failure rate/FIT**
1	PPS1	2.2829	2.2829	Y	out of range (under)	0.2	N		0.00	0.000	0.000	N			0.000
			2.2829		out of range (over)	0.2	Y	E_SM_APS_01 E_SM_APS_02	0.99	0.000	0.005	Y	E_SM_APS_02	0.90	0.045
			2.2829		stuck in range	0.2	Y	E_SM_APS_02 E_SM_APS_03	0.99	0.000	0.005	Y	E_SM_APS_02 E_SM_APS_03	0.90	0.045
			2.2829		offset (+3% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.046	Y	E_SM_APS_02	0.90	0.041
			2.2829		drift (+3% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.046	Y	E_SM_APS_02	0.90	0.041
2	PPS2	2.9928	2.9928	Y	out of range (under)	0.2	N		0.00	0.000	0.000	N			0.000
			2.9928		out of range (over)	0.2	Y	E_SM_APS_01 E_SM_APS_02	0.99	0.000	0.006	Y	E_SM_APS_02	0.90	0.059
			2.9928		stuck in range	0.2	Y	E_SM_APS_02 E_SM_APS_03	0.99	0.000	0.006	Y	E_SM_APS_02	0.90	0.059
			2.9928		offset (+1.5% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.060	Y	E_SM_APS_02	0.90	0.054
			2.9928		drift (+1.5% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.060	Y	E_SM_APS_02	0.90	0.054

$\sum_{SR,HW}(\lambda_{SPF}) =$	0.00	$\sum_{SR,HW}(\lambda_{RF}) =$	0.23	$\sum_{SR,HW}(\lambda_{MPF,latent}) =$	0.40	$\sum_{SR,HW}(\lambda_{MPF,detected}) =$	3.59	$\sum_{SR,HW}(\lambda_{MPF}) =$	3.99

Results of HAM (Hardware Architectural Metrics) analysis

Total failure rate	5.28
Total Safety Related failure rate (λ)	5.28
Total Not Safety Related failure rate	0.00

Target			
	SPFM	90	% (over)
	LFM	60	% (over)

Single-Point Fault Metric 95.60 % Result: **Satisfied**

$1 - \sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF}) / \sum_{SR,HW}\lambda$

Latent Fault Metric 92.09 % Result: **Satisfied**

$1 - \sum_{SR,HW}(\lambda_{MPF,latent}) / \sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})$

Results of PMHF (Probabilistic Metric for random Hardware Failures) analysis

$T_{Lifetime}$ (Vehicle life time) 100,000

Target			
	PMHF	100	FIT (under)

$PMHF_{est} = \Sigma\lambda_{SPF} + \Sigma\lambda_{RF} + \Sigma\lambda_{DPF\_det} \times \Sigma\lambda_{DPF\_latent} \times T_{lifetime}$ = 0.23 FIT Result: **Satisfied**

Fig. 4 FMEDA Result for SG1

② SG2 - 의도하지 않은 엔진 출력의 감소는 방지되어야 한다.

	Component Name	Base Failure rate/FIT**		Safety-re lated component to be considered in the calculations?	Failure Mode	Failure rate distribution	Failure mode that has the potential to violate the safety goal in absence of safety mechanisms?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal?	Failure mode coverage wrt. violation of safety goal	Single-Point Fault failure rate/FIT	Residual Fault failure rate/FIT	Failure mode that may lead to the violation of safety goal in combination with an independ ent failure of another component?	Detection means? Safety mecha nism(s) allowing to prevent the failure mode from being la tent?	Failure mode coverage with respect to latent failures	Latent Multiple-Point Fault failure rate/FIT**
1	PPS1	2.2829	2.2829	Y	out of range (under)	0.2	Y	E_SM_APS_01 E_SM_APS_02	0.99	0.000	0.005	Y	E_SM_APS_02	0.90	0.045
			2.2829		out of range (over)	0.2	N		0.00	0.000	0.000	N		0.90	0.000
			2.2829		stuck in range	0.2	Y	E_SM_APS_02 E_SM_APS_03	0.99	0.000	0.005	Y	E_SM_APS_02 E_SM_APS_03	0.90	0.045
			2.2829		offset (-3% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.046	Y	E_SM_APS_02	0.90	0.041
			2.2829		drift (-3% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.046	Y	E_SM_APS_02	0.90	0.041
2	PPS2	2.9928	2.9928	Y	out of range (under)	0.2	Y	E_SM_APS_01 E_SM_APS_02	0.99	0.000	0.006	Y	E_SM_APS_02	0.90	0.059
			2.9928		out of range (over)	0.2	N		0.00	0.000	0.000	N		0.90	0.000
			2.9928		stuck in range	0.2	Y	E_SM_APS_02 E_SM_APS_03	0.99	0.000	0.006	Y	E_SM_APS_02	0.90	0.059
			2.9928		offset (-1.5% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.060	Y	E_SM_APS_02	0.90	0.054
			2.9928		drift (-1.5% over)	0.2	Y	E_SM_APS_02	0.90	0.000	0.060	Y	E_SM_APS_02	0.90	0.054

$\sum_{SR,HW}(\lambda_{SPF})=$	0.00	$\sum_{SR,HW}(\lambda_{RF})=$	0.23	$\sum_{SR,HW}(\lambda_{MPF\_latent})=$	0.40	$\sum_{SR,HW}(\lambda_{MPF\_detected})=$	3.59	$\sum_{SR,HW}(\lambda_{MPF})=$	3.99

Results of HAM (Hardware Architectural Metrics) analysis

Total failure rate	5.28
Total Safety Related failure rate (λ)	5.28
Total Not Safety Related failure rate	0.00

Target			
	SPFM	90	% (over)
	LFM	60	% (over)

Single-Point Fault Metric 95.60 % Result: Satisfied

$1 - \sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF}) / \sum_{SR,HW}\lambda$

Latent Fault Metric 92.09 % Result: Satisfied

$1 - \sum_{SR,HW}(\lambda_{MPF,latent}) / \sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})$

Results of PMHF (Probabilistic Metric for random Hardware Failures) analysis

$T_{Lifetime}$ (Vehicle life time) 100,000

Target			
PMHF	100	FIT (under)	

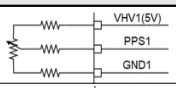
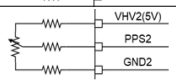
$PMHF_{est} = \Sigma\lambda_{SPF} + \Sigma\lambda_{RF} + \Sigma\lambda_{DPF\_det} \times \Sigma\lambda_{DPF\_latent} \times T_{lifetime}$ = 0.23 FIT Result: Satisfied

Fig. 5 FMEDA Result for SG2

5.5.1 하드웨어 엘리먼트 정보

Table 16은 APS 센서 출력 단인 PPS 1, PPS 2에 대한 내부 회로와 Class 등급을 보여준다.

Table 16 Hardware element information for APS

No	Class	Name	Description	Circuit
1	Class Ⅱ	PPS 1	APS output 1	
2	Class Ⅱ	PPS 2	APS output 2	

5.5.2 기본 고장율, 고장 모드, 고장 모드 분포율

Table 17은 '5.3 고장 모드 및 고장 시나리오'에 기술된 10개의 고장 모드에 대한 기본 고장율, 고장 모드, 고장

Table 17 Base failure rate, failure mode, failure mode distribution for APS

No	Fit	Failure Mode	Distribution	R. SG
FM1	2.283 Fit	Out of range (under)	20 %	SG1, SG2
FM2		Out of range (over)	20 %	SG1, SG2
FM3		Stuck in range	20 %	SG1, SG2
FM4		Offset	20 %	SG1, SG2
FM5		Drift	20 %	SG1, SG2
FM6	2.993 Fit	Out of range (under)	20 %	SG1, SG2
FM7		Out of range (over)	20 %	SG1, SG2
FM8		Stuck in range	20 %	SG1, SG2
FM9		Offset	20 %	SG1, SG2
FM10		Drift	20 %	SG1, SG2

모드 분포율을 나타낸 것이다. 기본 고장율은 위의 '5.4 정량적 안전 분석'에서 계산 되어졌으며, 고장 모드 분포율은 전문가 판단에 의해 균등 분할되었다.

5.5.3 APS 센서에 대한 기능 및 성능 시험 결과

APS 센서에 대한 기능 및 성능 시험 결과서 및 환경 시험을 포함하는 신뢰성 시험 결과서는 지면상의 이유로 본문에 포함되지 않았다. 하지만, '5.1 하드웨어 엘리먼트 평가 계획 및 시험 계획'에 따라 APS 센서에 대한 기능 및 성능 시험을 수행하였고, 모든 시험 항목을 통과하였다. 이를 통해 APS 센서에 할당된 하드웨어 안전 요구사항의 완전하고 올바른 구현을 검증 하였다. 그리고 신뢰성 시험을 수행하여 스트레스 상황에서의 내구성, 강건성을 입증하였다.

5.5.4 FMEDA 수행결과

안전 목표 1과 2에 대한 하드웨어 우발 고장에 대한 정량적 분석 결과는 Fig. 4, Fig. 5에서 나타낸 바와 같이

SG1 – SPFM: 95.6 %, LFM: 92.09 %, PMHF: 0.23 Fit
SG2 – SPFM: 95.6 %, LFM: 92.09 %, PMHF: 0.23 Fit

으로서, ASIL B 수준의 정량적 목표 값을 만족하였다. 아래 Table 18은 ISO26262-5:2018에 명시된 하드웨어 우발 고장에 대한 ASIL B 수준의 정량적 목표 값이다.

Table 18 Quantitative target value of random hardware failure for ASIL B level

		Value
HAM (Hardware Architecture Matic)	SPFM (Single Point Fault Metric)	≥90 %
	LFM (Latent Fault Metric)	≥60 %
PMHF (Probabilistic Metric for random Hardware Failures)		< 100 Fit

5.5.5 하드웨어 엘리먼트 평가 논거

Table 19는 APS 센서에 대한 하드웨어 엘리먼트 평가 논거이다. 이를 통해 APS 센서가 기능안전 ISO 26262 표준을 준수하여 개발하려는 엔진 제어 시스템에 통합되는 것이 문제가 없음을 보여준다.

- Assumption of application context for APS
  : APS에 대한 어플리케이션 컨텍스트 가정 문서
- APS functional test report
  : 가정된 요구사항에 따른 기능 및 성능 시험 결과서

Table 19 Argument of EHE(Evaluation of hardware elements) for APS

No	Name	Method	Evidence	Compliance check
1	APS	Test & Analysis	· Assumption of application context for APS · APS functional test report · APS reliability test report · FMEDA report	Pass

- APS reliability test report
  : 가정된 요구사항에 따른 신뢰성 시험 결과서
- FMEDA report
  : 가정된 어플리케이션 컨텍스트에 따른 FMEDA 결과서

다음 내용을 근거로 하여, 본 문에서 가정된 상황에 따라 APS 센서를 사용할 경우, 목표한 ASIL B 수준을 만족하였다.

1) 안전 목표 및 기능 안전 요구사항, 그리고, 기술 안전 요구사항을 가정하여 하드웨어 안전 요구사항을 도출하였다.
2) 정량적 평가를 위하여 외부 안전 메커니즘을 가정하였고, 이에 대한 진단 커버리지 값을 산정하였다.
3) 가정된 상황에서 하드웨어 엘리먼트 평가 계획을 수립하고 계획에 따라 하드웨어 엘리먼트 평가를 수행하였다.
4) APS 센서에 대한 기능 및 성능 시험을 통해 APS 센서에 할당된 하드웨어 안전요구사항의 완전하고 올바른 구현을 검증하였다. 그리고 신뢰성 시험을 통하여 스트레스 상황에서의 내구성, 강건성을 검증하였다.
5) APS 센서에 대한 정량적 안전 분석인 FMEDA 수행을 통하여 HAM과 PMHF 값을 평가하여 ASIL B 수준의 목표 값을 만족하였음을 입증하였다.

6. 결 론

본 논문은 지난 십 수년간 자동차 시장에서 문제없이 사용해 왔던 QM 수준의 APS 센서를 기능안전 ISO 26262 표준을 준수하여 개발 하려는 아이템 또는 시스템의 일부로 사용(통합) 할 때 요구되는 하드웨어 엘리먼트 평가 수행에 있어서, SEooC 기법을 적용한 방안을 구체적인 사례를 들어 소개하였다.

서론에서 밝혔듯이, 하드웨어 엘리먼트 평가를 수행하기 위해서는 평가 대상 하드웨어 엘리먼트에 주어진 하드웨어 안전 요구사항이 필요한데, 자동차 산업 현장

에서는 때때로 이러한 하드웨어 안전 요구사항 없이 하드웨어 엘리먼트 평가를 수행해야 하는 경우가 있다. 이를 해결 하기 위해 ISO 26262-10에서 제시된 SEooC 기법을 활용하여 하드웨어 안전 요구사항을 생성하였으며, 생성된 하드웨어 안전 요구사항에 기반한 하드웨어 엘리먼트 평가를 수행하였다.

이를 통해, 가정된 상황에서 APS 센서를 사용할 경우, 통합에 대한 문제가 없음을 입증하였고, 자동차 메이커 또는 시스템 통합 업체로부터 요구된 특정 ASIL 수준이 만족하였음을 증명 하였다.

References

1) ISO 26262-8:2018, Road Vehicles Functional Safety Part 8: Supporting Processes, 2nd Edn., 2018.
2) B. K. Park and S. H. Lee, “Understanding and Case Study of Hardware Integration by Evaluation of Hardware Elements,” Transactions of KSAE, Vol.28, No.10, pp.693-700, 2020.
3) ISO 26262-10:2018, Road Vehicles Functional Safety Part 10: Guidelines on ISO 26262, 2nd Edn., 2018.
4) S. H. Lee and B. K. Park, “The Study on Application SEooC by Use Case Analysis of Pressure Sensor,” Transactions of KSAE, Vol.28, No.8, pp.515-520, 2020.
5) ISO 26262-3:2018, Road Vehicles Functional Safety Part 3: Concept Phase, 2nd Edn., 2018.
6) ISO 26262-4:2018, Road Vehicles Functional Safety Part 4: Product Development at the System Level, 2nd Edn., 2018.
7) ISO 26262-5:2018, Road Vehicles Functional Safety Part 5: Product Development at the Hardware, 2nd Edn., 2018.
8) ISO 26262-11:2018, Road Vehicles Functional Safety Part 11: Guidelines on Application of ISO 26262 to Semiconductors, 2nd Edn., 2018.
9) International Electrotechnical Commission, IEC TR 62380 Edition 1.0: Reliability Data Handbook - Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment, IEC, 2004.